آشنایی با

آی پی ورژن 6

IPv6

فـصل اول

IPV 6

چکیده :

پروتکل اینترنت نسخه ۶ (به انگلیسی: Internet Protocol version 6) یا به اختصار IPv6 جدیدترین نسخه پروتکل اینترنت (Internet Protocol) است که ارتباط‌های اینترنتی بر پایه آن شکل می‌گیرد. این نسخه قرار است جای نسخه ۴ این پروتکل (IPv4) را که هم‌اکنون استفاده می‌شود بگیرد.

IPv4 از فضای آدرسی ۳۲ بیتی استفاده می‌کند. این فضای اجازه‌ی آدرس‌دهی ۲۳۲ یعنی حدود ۴ میلیارد آدرس در اینترنت را می‌دهد. با توجه به این‌که امروزه بسیاری از دستگاه‌ها افزون بر کامپیوترها مانند موبایل‌ها، دوربین‌ها و حتا لوازم خانگی و قاب عکس‌های دیجیتال به اینترنت متصل می‌شوند، این فضا رو به اتمام است و تاکنون با تمهیداتی مانند NAT سعی در جبران این کمبود داشته اند. IPv6 اما از فضای آدرس‌دهی ۱۲۸ بیتی استفاده می‌کند که اجازه داشتن ۲۱۲۸ آدرس یگانه را به ما می‌دهد و مشکل فضای آدرسی که هم‌اکنون با آن روبرو هستیم را رفع می‌کند.

مقدمه :

نشاني پروتكل اينترنت (Internet Protocol Address) يا به اختصار نشاني آي‌پي (IP Address) نشاني عددي است كه به هريک از دستگاه ها و رايانه‌هاي متصل به شبكه ي رايانه اي كه بر مبناي مدل مرجع TCP/IP (از جمله

اینترنت) کار میکند، اختصاص داده میشوند. پیام هایي که دیگر رایانه ها براي این رایانه میفرستند با این نشانه ي عددي همراه است و مسیر یاب هاي شبکه آن را مانند «نشاني گیرنده» در نامه هاي پستي تعبیر میکنند، تا بالاخره پیام به رابط شبکه رایانه مورد نظر برسد.

تاریخچه :

با این تصمیم که اینترنت به طور جدي نیاز به ظرفیت و فضاي آدرسدهي بالایي دارد گروه معماري اینترنت سه پیشنهاد اصلي در این زمینه ارائه نمود. اولین پیشنهاد تحت عنوان TUBA بود. این پیشنهاد بر اساس سوئیچینگ IP بر روي CLNP به عنوان پروتکل لایه اینترنت بود. CLNP یك پروتکل OSI میباشد که داراي آدرس 20 هشتتایي میباشد و تمامي پروتکلهاي مسیریابي تعریف شده را پشتیباني مینماید. این پروتکل مورد قبول واقع نشد زیرا CLNP در آن زمان هم (زمان پیشنهاد) یك پروتکل قدیمي و غیر موثر محسوب میشد و حتي در بازار IPv4 هم به صورت یك پروتکلي که به طور گسترده در بازار پروتکلهاي IP کاربرد داشته باشد مورد قبول نبود. پیشنهاد دوم IPv7 نامیده میشد که بعداً به TP/IX تغییر نام داد و سرانجام CATNIP نامیدند، این پیشنهاد بر اساس این ایده پایه‌ریزي شده‌بود که یك بسته‌ي اطلاعاتي با قالب مشترك تعریف شود که با

IPT، CLNP و IPX سازگاري داشته باشد، اين پيشنهاد به علت عدم رشد سريع آن مورد توجه و استقبال واقع نشد. سومين و آخرين پيشنهاد كه موفقترين آنها نيز بود با عنوان IP در IP زندگي خود را آغاز نمود، اساس اين پيشنهاد اين بود كه در آن براي اينترنت دو لايه جداگانه، يكي به عنوان لايه زيرساخت و ديگري به عنوان لايه گسترش محلي تعريف كنند. در اين پيشنهاد در واقع يك نوع بستهبندي آدرس IP صورت گرفته است كه مكانيزم خوبي براي انتقال IP ساده نيز ميباشد، انتقال آدرسها با اين روش از IPv4 به راحتي انجام ميگيرد اين روش در واقع به افزايش فضاي آدرس دهي IP از 32 بيتي به 64 بيتي و از بين بردن بعضي از مشخصه هاي منسوخ شده IPv4 براي كاهش اندازه سرآيندهاي پروتكل IP ميباشد. SIP را با پيشنهادي كه آن را PIP ميگفتند تركيب دادند و اثرات مسيريابي IPv4 را بهبود بخشيدند و پيشنهاد جديدي را ارائه نمودند كه آنرا SIPP ناميدند. با تغييرات به وجود آمده و با اعمال تغييراتي روي آن بعدها آن را IPv6 ناميدند، از اسم IPv5 استفاده نكردند چون قبلاً از آن در جاي ديگر و براي پروتكل جاري ديگر استفاده شده بود. يكي از عمومي‌ترين مزايا و منافع IPv6 گستردگي و ازدياد فضاي آدرس‌دهي آن است و اين نسخه از فضاي آدرس‌دهي 128 بيتي استفاده ميكند در صورتيكه IPv4

از فضاي آدرس‌دهي 32 بيتي استفاده مي‌نمود. IPv6 داراي فواید زيادي براي شبکه‌ها مي‌باشد. از جمله اين فواید مي‌توان به امنيت بالاي آن در شبکه، بهبود و تقليل جداول مسيريابي، و در نتيجه کاهش حافظه و پردازنده لازم براي مسيريابها، و بهبود بخشيدن به استفاده از آدرس‌دهي اتوماتيك براي کاربران متحرك اشاره نمود.

انواع آيپي

دو نسخه آيپي درحال استفاده مي باشد: آيپي نسخه 4 و آيپي نسخه 6 که هر يک نشاني آيپي را به روش متفاوتي ارائه مي نمايند.

نشاني آيپي نسخه 4

نشاني آيپي نسخه چهارم يک عدد 32 بيتي است که براي سادگي آن را به شکل چهار بخش عددي در مبناي ده مي‌نويسند که با نقطه از هم جدا مي‌شوند (مانند 199.211.45.5). اين روش نشاني‌دهي را ده‌دهي نقطه‌دار مي‌نامند هر يک از چهار بخش را يک هشتايي (Octet) مي‌گويند زيرا طول آن 8 بيت (يا 1 بايت) است و مي‌تواند عددي از 0 تا 255 باشد. پس 2 به توان 32 آدرس مختلف داريم.

اصولاً هر نشاني آيپي 32 بيتي به دو بخش تقسيم مي‌شود: يک پيشوند و يک پسوند. اين دو سطح به منظور ايجاد يک روش مسيريابي کارآمد طراحي شده

است. پیشوند آدرس، شبکه‌اي را که رایانه به آن متصل است مشخص مي‌کند (Network) در حالیکه پسوند یک رایانه یکتا را روي شبکه مشخص مي‌کند (Host). یعني به هر شبکه در اینترنت یک مقدار یگانه که تحت عنوان شماره شبکه شناخته شده است، اختصاص دارد. شماره شبکه به عنوان یک پیشوند در نشاني هر رایانه‌اي که به شبکه وصل است ظاهر مي‌شود. بعلاوه به هر رایانه روي یک شبکه، یک پسوند نشاني یکتا تخصیص یافته است.

هر نشاني کامل، شامل یک پیشوند و یک پسوند است و طوري تخصیص داده مي‌شوند که یکتا باشند، بنابراین ویژگي اول تضمین مي‌گردد. اگر دو رایانه به دو شبکه مختلف وصل شده باشند، نشاني‌هایشان پیشوندهاي متفاوت خواهند داشت. اما اگر دو رایانه به یک شبکه وصل باشند، نشاني‌هایشان داراي پسوندهاي متفاوت خواهد بود.

آي‌پي ایستا و پویا

آي‌پي پویا با هر بار وصل‌شدن به شبکه داخلي و یا اینترنت تغییر مي‌کند. اما آي‌پي ایستا (Static) اینطور نیست. آي‌پي پویا (Dynamic) در هر شبکه توسط کارساز پروتکل پیکربندي پویاي میزبان (DHCP Server) به رایانه‌ها در شبکه اختصاص داده مي‌شود. یعني وقتي شما به اینترنت و یا شبکه داخلي وصل

مي‌شويد، كارساز پروتكل پيكربندي پوياي ميزبان به شما يک نشاني آي‌پي اختصاص مي‌دهد.

DHCP Server مي‌تواند يک سرويس در سيستم‌عامل‌هاي سرور باشد يا يک قطعه سخت‌افزاري مانند مسيرياب (Router) و يا نقطه دسترسي (Access Point) در شبکه باشد.

براي ديدن نشاني آي‌پي رايانه خود مي‌توان از برنامه winipcfg.exe (در ويندوز 95 و 98 و ME) يا ipconfig.exe (در ويندوز 2000 و XP) کرد. در لينوکس يا يونيکس (يا سيستم‌هاي مبتني بر آن‌ها) نيز مي‌توان از دستور ifconfig استفاده کرد.

آي پي نسخه 6

گسترش روز افزون اينترنت و نياز به آدرس هاي بسيار بيشتر تيم Internet Engineering Task Force را برآن داشت تا به فکر تکنولوژي هاي جديدي باشند تا امکان تعريف آدرس هاي آي پي بيشتري فرآهم گردد. بهترين راه ساخت مجدد نشاني پروتکل اينترنت بود . در سال 1995 ميلادي نسخه جديد نشاني پروتکل اينترنت با نام آي پي نسخه 6 معرفي گرديد . اندازه آدرس از 32 بيت به 128 بيت افزايش يافت وامکان آدرس دهي تا 2به توان 128 آدرس افزايش يافت. اين کار تنها تعداد آدرس هاي اينترنتي را گسترش نداد، بلکه باعث خواهد شد جدول مسيرياب هاي

اینترنتي (روترها) کوچکتر شود . کلیه سیستم‌عامل‌هاي جدید سرور و خانگي از جمله ویندوز ویستا به طور کامل پشیباني مي‌شود ولي متاسفانه هنوز توسط بسیاري از مسیریاب هاي شبکه هاي خانگي و تجهیزات شبکه عادي پشتیباني نشده است.

بررسی IPV6

از دیگر مشکلاتی که NAT ایجاد می کند ، اختلال در عملکرد نرم افزارهایی است که بر پایه سیستم Peer-to-Peer عمل می کنند . به طور کلی در NAT به QOS با کیفیت خدمات توجه چندانی نمی شود ، که با رشد کاربردهای چندرسانه ای در اینترنت این موضوع جدی تر و حساس تر به نظر می رسد .

این مشکلات به سادگی قابل حل خواهند بود ، در صورتی که هر کامپیوتر بر روی شبکه دارای یک آدرس IP واقعی مربوط به خود باشد . چیزهایی که امروزه برای IPv4 غیر ممکن است دلیلی برای تولد IPv6 خواهد بود . در دنیایی با IPv6و بدون NAT هر کامپیوتر آدرس IP یگانه مربوط به خود را خواهد داشت ، این بدین معنی است که یک PC در یک نقطه می تواند با PC دیگر در جایی دیگر یک ارتباط مستقیم (peer to peer) داشته باشد و هر کامپیوتر از هر جایی قابل کنترل شدن را داشته باشد . علاوه بر این امکان استفاده از آنها وجود نداشته بوجود خواهد آمد به خاطر NAT ، اکثر متخصصان دیگر

نگران کمبود فضای آدرس دهی IP نبودند ، اگر شما یک شبکه خانگی داشته باشید ؛ آنوقت تهویه مطبوع ، یخچال ، تلویزیون و دیگر وسائل شما می توانند به شبکه محلی شما اضافه شوند و با تولید کنندگان خود ارتباط برقرار کنند به طوری که هر وسیله در آدرس IP فایر وال با آن شریک خواهد شد . با وجود تمام این دستاوردها ، NAT واقعاً یک شیطان است . یک تکنولوژی که برای پاسخ گویی به تمام مشکلات مهندسان آمده ولی باعث مشکلاتی می شود ، عمیق تر از آنکه NAT ادعای حل آن را دارد . در حقیقت یکی از بزرگترین دلایلی که تکنولوژی های اولیه اینترنت خواهان توسعه IPv6 در سال 1990 شدند جلوگیری از پذیرش گسترش عرضی NAT و گسستگی حاصل از آن و ایجاد یک اتحاد تقریباً کامل بین اجزای اینترنت بود .

در یک تجسم ساده ، NAT یک سری از موانع را ایجاد می کند ، کامپیوترهایی که در محدوده فایروال NAT قرار می گیرند می توانند با وب سرور و سرورهای دیگر بر روی اینترنت ارتباط برقرار کنند و حمله های پراکنده ای که روی شبکه صورت می گیرد نمی توانند از NAT گذشته و به کامپیوترهای بدون محافظ داخل NAT آسیبی برساند ، تا این جا این سیستم بسیار خوب کار می کتد . در حقیقت بسیاری از سازمانها از NAT به عنوان سیستم دفاعی اولیه در

مقابل هکرها استفاده می کنند . این تکنولوژی باعث می شود که مؤسسات از این که سیستم امنیتی خود را بدین وسیله ارتقاء داده اند به هیجان در آیند . اما امنیتی که به وسیله NAT ایجاد می شود سرابی بیش نیست ، ازدیاد کامپیوترهای کیفی ، ضمیمه های پست و شبکه های بی سیم باز فرصت های زیادی را برای هکر های زبر دست فراهم می کند که پشت یک NAT پنهان شده و تدارک یک حمله از داخل را ببینند . پس به راحتی مشخص می شود که تنها با اعتماد به یک سیستم دفاعی محیطی نمی توان به یک امنیت نسبی رسید .

هنوز یک مشکل دیگر با IPv6 باقی مانده و آن این است که باید با تمام مشکلات امنیتی که این تغییر احتمالاً باعث آن می شود مقابله کرد . اجرای IPv6 امنیت رمزنگاری را پیشنهاد می کند که از زمان استاندارد (IP sec) اجباری شده است،این خصوصیات IPv6 باید با این استاندارد هماهنگ باشد ، پس همه سرورهای DNS،سرورهای شبکه و جستجوگرهای شبکه کد های جدیدی خواهند داشت(هر مشکل امنیتی کد مخصوص به خود را خواهد داشت) گرچه ممکن است در نگاه اول کد شدن مشکلات باعث ایجاد دردسر شود ولی مشکلات مربوط به امنیت مشخص خواهند بود و وقتی که ، پی آمد های امنیتی با سرورهای IPv6 پیش بیاید ، اطمینان بیشتری در کشف آن خواهیم داشت .

ولی آن چه که می تواند ضربه مهلک نهایی را به IPv6 بزند و آن را در تابوت مرگ گرفتار کند یک تکنولوژی سیاه جادویی است که اهمیت افزایش تعداد آدرس های IP را از آن مقدار که در گذشته داشته کاهش می‌دهد . این تکنولوژی NAT یا Network Address Translation نام دارد که اجازه می دهد یک دو جین یا حتی هزاران کامپیوتر با یک آدرس IP واحد پشتیبانی شوند . NAT تکنولوژی کلیدی است که در بسیاری از فایروال‌های شرکتها و خصوصاً در مسیر یاب های کوچک استفاده می شود .

NAT از یکی از اساسی ترین قوانین اینترنت تخطی کرده است ، با NAT این حقیقت که هر کامپیوتر بر روی شبکه باید دارای آدرس واحد باشند ، انکار خواهد شد .

در اینترنت امروزی ، استفاده کامپیوتر ها از این روش Private Addresses نامیده می شود که این خصوصی سازی آدرس ها در پناه یک فایروال انجام می شود . فایروال مانند دروازه ای عمل می کند که تمام ورودی ها و خروجی ها را کنترل می کند و بسته هایی را که از خارج به داخل و یا بالعکس خارج می شوند را بازنویسی و پیکربندی مجدد می کند .

گرچه ممکن است در نگاه اول کد شدن مشکلات باعث ایجاد دردسر شود ولی مشکلات مربوط به امنیت مشخص خواهند بود و وقتی که ، پی آمد های امنیتی با

سرورهای IPv6 پیش بیاید ، اطمینان بیشتری در کشف آن خواهیم داشت . هنوز یک مشکل دیگر با IPv6 باقی مانده و آن این است که باید با تمام مشکلات امنیتی که این تغییر احتمالاً باعث آن می شود مقابله کرد . اجرای IPv6 امنیت رمزنگاری را پیشنهاد می کند که از زمان استاندارد (IP sec) اجباری شده است،این خصوصیات IPv6 باید با این استاندارد هماهنگ باشد ، پس همه سرورهای DNS،سرورهای شبکه و جستجوگرهای شبکه کد های جدیدی خواهند داشت(هر مشکل امنیتی کد مخصوص به خود را خواهد داشت)

یک مشکل دیگر برای IPv6 این است که مسیر یاب ها به مدارهای مجتمع خاصی مجهز هستند که به راحتی می توانند بسته های اطلاعاتی IPv4 را هدایت کنند ولی این مسیریاب ها سخت افزارهای مشابهی برای V6 ندارند و همانطور که قبلاً اشاره شد هدایت این بسته ها به صورت نرم افزاری باعث کندی روند حرکت خواهد شد . در نتیجه بسیاری از متخصصان معتقد هستند که مسیر یاب های V4 به سادگی نمی توانند از عهده یک تغییر و تحول ناگهانی و وسیع در اسکلت اصلی اینترنت بر آیند . مسیر یاب ها باید ارتقاع پیدا کنند و تمام شرکتها باید از استانداردهای تقریباً مشابهی پیروی کنند که بسیار پر هزینه خواهد بود . در یک مقیاس تجاری متوسط با مسیریاب های Hight- 16

Speed قیمت تمام شده به راحتی به حدود یک میلیون دلار خواهد رسید .

توسعه IPv6 بدین معنی است که هر نرم افزاری که از اینترنت استفاده می کند احتیاج دارد مجدداً پیکربندی شود .

همه جستجوگرهای اینترنت بر روی تمام کامپیوتر ها ، تمامی Outlook Express ها و همه سرورهای اینترنت برای پاسخ گویی به آدرس های 128 بیتی احتیاج به ارتقاء پیدا می کنند . یکی از راه حل های موجود برای تغییر حالت این است که همه کامپیوترها آدرس های IPv4 و IPv6 را باهم داشته باشند . با این روش مشکل یافتن زمان مناسب برای توسعه عمومی سیستم ها به IPv6 حل خواهد شد . چون ممکن است بعضی از افراد در بعضی از جاها هنوز دارای سیستم V4 باشند که در نتیجه قادر به ایجاد ارتباط با شما که سیستم خود را به V6 ارتقاء داده اید نخواهند بود .

کارکرد سیستم در این روش بدین طریق است که :

فیلد Versionشماره نسخه پروتکل برای IPv6 همیشه 6 است . کما اینکه برای IPv4 نیز همیشه 4 است !!!

در دوران گذار از IPv4 به نسخه جدید که ممکن است یک دهه طول بکشد ، مسیریابها قادرند با بررسی این فیلد تشخیص بدهند که با چه نوع بسته ای روبرو

هستند . البته از آنجایی که بررسی این فیلد به چندین دستور اجرایی CPU نیاز دارد و این کار زمان مفید پردازش هر بسته را هدر می دهد لذا در بسیاری از پیاده سازی های عملی برای اجتناب از این زمان تلفاتی ، تشخیص اینکه یک بسته از نوع IPv4 است یا IPv6 ، با استفاده از فیلد خاصی در سرآیند لایه پیوند داده ها بر عهده سخت افزار گذاشته شده است . بدین ترتیب بسته ها بر اساس نوعشان مستقیماً به نرم افزار مناسب در لایه شبکه هدایت می شوند . البته این الزام که لایه پیوند داده از جزئیات نوع بسته های لایه شبکه آگاه باشد با این اصل اساسی که «هر لایه نباید از فضای بیت هایی که از لایه بالاتر به آن تحویل داده می شود ، آگاه باشد» در تناقض است . بدون شک بحث و مناقشه بین طرفداران ایده های «انجام اصول گرایانه و صحیح کار» و «تسریع کار» همانطور که در ادامه مطالب متوجه آن خواهید شد به شدت ادامه خواهد داشت .

فصل دوم

امنیت در IPv6

امنیت در IPv6

امنیت یکی از مشخصات داخلی پروتکل IPv6 است که دارای هر دو مشخصه تصدیق هویت (Authentication) و رمزنگاری (Encryption) در لایه IP پروتکل جدید است. IETF سازمانی است که به گروه کاری امنیت در IP معروف است. این سازمان وظیفه دارد که مکانیزمهای امنیتی مورد نیاز در لایه‌های مختلف IP را هم در IPv6 و هم در IPv4 جهت گسترش و بهبود استانداردهای مورد نیاز بر عهده گیرد. همچنین این گروه وظیفه دارد پروتکل‌های مدیریتی کلید عمومی (Key Management Protocols) را جهت استفاده بیشتر در شبکه جهانی اینترنت توسعه و گسترش دهد. تصدیق (Authentication) این قابلیت را به گیرنده بسته می‌دهد که مطمئن شود آدرس مبدا معتبر بوده و بسته در طول زمان انتقال دچار تغییر و دستکاری نخواهد شد. رمز نگاری (Encryption) اطمینان می‌بخشد که تنها گیرنده اصلی بسته می‌تواند به محتویات آن دست یابد. به عبارت دیگر رمز نگاری باعث می‌شود که تنها گیرنده‌ای که بسته به نام او ارسال شده است، می‌تواند به محتویات آن دسترسی داشته باشد. برای بررسی و تحلیل این مزایا یک سیستم کلیدی بکار گرفته می‌شود که به موجب آن فرستنده‌ها و گیرنده‌ها بر روی یک مقدار کلیدی که مورد استفاده قرار می‌گیرد با هم به توافق می‌رسند. سیستم مدیریت کلید عمومی که توسط طراحان IPv6 پذیرفته شده است،

مکانیزم ISAKMP می‌باشد، که با ایجاد و تولید کلید رمز سر و کار دارد و روشهای اجرای عمومی پروتکل مدیریت کلید را تامین می‌کند. پیغامهای ISAKMP با استفاده از پروتکل UDP رد و بدل می‌شوند و از شماره پورت ۵۰۰ استفاده می‌کند. [4]

IPv6 لزوم IPSEC را اجباری می‌کند و در نتیجه یک قالب امنیتی یک پارچه برای ارتباطات اینترنتی ایجاد می‌کند. IPSEC برای پیاده‌سازی رمزنگاری و نیز تصدیق استفاده می‌شود. در بسیاری از پیاده‌سازی‌های IPv4 امکان فعال سازی IPSEC نمی‌باشد و در نتیجه سطح امنیت کاهش می‌یابد.

پروتکل امنیت در لایه شبکه IPSec

همانگونه که ذکر شد، بحث امنیت داده‌ها و اطلاعات در IPv6 از اهمیت بالایی برخوردار است. با گسترش حملات کامپیوتری، اصالت، جامعیت، هویت‌شناسی و محرمانگی اطلاعات خصوصاً اطلاعات حیاتی افراد و سازمانها در معرض خطر قرار خواهد گرفت. از این رو استفاده از پروتکل IPSec، باعث ایمن سازی فضای اطلاعات خواهد شد. پروتکل IPSec یکی از استانداردهای VPN است که با استفاده از مکانیزم های هویت‌شناسی و رمزنگاری مانع از گوش دادن به داده‌ها یا دستکاری و خراب کاری آنها می‌شود. قابل توجه‌ترین موارد استفاده از آن به صورت شبکه به شبکه و نیز دسترسی از راه

دور(کامپیوتر به شبکه) می‌باشند. در واقع امنیت شبکه‌های خصوصی مجازی VPN از چندین روش امکانپذیر می‌باشد که عبارتند از دیوار آتش, IPSec , AAA Server و کپسوله سازی. اما روش IPSec به علت امن بودن، پایداری بالا، ارزان بودن، انعطاف پذیر بودن و مدیریت بالا مورد توجه قرار گرفته است. مطابق با تعریف IETF پروتکل IPSec به این شکل تعریف می‌شود: "یک پروتکل امنیتی در لایه شبکه که خدمات رمزنگاری را تامین می‌کند. خدماتی که بصورت منعطف به پشتیبانی ترکیبی از تایید هویت، جامعیت، کنترل دسترسی و محرمانگی می‌پردازد" . پروتکلIPSec از IKE به عنوان مدیریت کلید استفاده می‌کند. این پروتکل مخصوصا برای بسته‌های پروتکل IP طراحی شده و بر خلاف PPTP امنیت را برای سایر پروتکل‌ها فراهم نمی‌آورد. بعلاوه شامل دو مد رمزنگاری است که transport و tunnel نام دارند و هر یک سطحی از امنیت را فراهم می‌آورند. امروزه این پروتکل یکی از مورد توجه‌ترین پروتکل‌های امنیتی محسوب می‌شود و از جمله اینکه هر دو شرکت بزرگ Cisco و Microsoft در محصولات خود پشتیبانی از IPSec را گنجانده‌اند...

پروتکل IPSec از دیدگاه شبکهIPSec

این پروتکل در لایه ۳ عمل می‌کند و شامل پروتکل‌های AH و ESP می‌باشد. IPSec از AH به منظور هویت‌شناسی و جامعیت مبدا بدون استفاده از رمزنگاری بهره

می‌گیرد، درحالیکه ESP هویت‌شناسی و جامعیت مبدا را به کمک رمزنگاری فراهم می‌آورد. پروتکل IPSec دارای دو مد عملیاتی انتقال و تونل است. در مد انتقال مکانیزم رمز نگاری روی قسمت داده ای بسته IP اعمال می‌شود و سرآیند بسته IP تغییر نخواهد کرد. بنابراین مبدا و مقصد نهایی بسته ممکن است توسط افراد غیر مجاز مشاهده شود، اما چون در این مد سرآیند لایه ۴ رمزنگاری شده است، اطلاع دقیق از نوع و کیفیت بسته ارسالی برای کابران غیر مجاز امکانپذیر نخواهد بود. معمولاً از این مد زمانی استفاده می‌شود که هم مبدا و هم مقصد پروتکل IPSec را پشتیبانی نماید. در مد تونل، تمامی بسته IP رمزنگاری می‌شود و سپس یک سرآیند جدید به بسته رمزنگاری شده الحاق می‌گردد. از این مد زمانی استفاده می‌شود که یک یا هر دو طرف اتصال IPSec دروازه های امنیتی باشند که از این پروتکل حمایت می‌کنند، در حالی که مبدا و مقصد اصلی که در پشت این دروازه ها قرار دارند پروتکل IPSec را پشتیبانی نمی‌کنند. در این حالت مبدا و مقصد اصلی بسته ها از دید کاربران غیر مجاز پنهان خواهد ماند.

پروتکلهای IPSec

خانواده پروتکل IPSec شامل دو پروتکل است. یعنی سرآیند احراز هویت یا AH (Authentication Header) وESP

هر دوی این پروتکل‌ها از IPSec مستقل خواهد بود. این پروتکل از متد ESP جهت کپسوله استفاده میکند.

پروتکل AH

بطور خلاصه پروتکل AH در واقع تأمین کنندهٔ سرویسهای امنیتی زیر خواهد بود: ۱.تمامیت داده ارسالی ۲.احراز هویت مبدا داده ارسالی ۳. نادیده گرفتن بسته‌های دوباره ارسال شده

این پروتکل برای تمامیت داده ارسالی از HMAC استفاده می‌کند و برای انجام این کار مبنای کارش مبتنی بر کلید سری است که payload بسته و بخشهایی تغییر ناپذیر سرآیند IP شبیه IP آدرس خواهد بود. بعد از این کار این پروتکل سرآیند خودش را به آن اضافه می‌کند در شکل زیر سرآیندها و فیلدهای AH نمایش داده شده است.

سرآیند AH، 24 بایت طول دارد. حال به توضیح فیلدهای این پروتکل می‌پردازیم.

اولین فیلد همان Next Headerمی باشد. این فیلد پروتکلهای بعدی را تعیین می‌کند. در حالت Tunnel یک دیتاگرام کامل IP کپسوله می‌شود بنابراین مقدار این فیلد برابر ۴ است. وقتی که کپسوله کردن یک دیتا گرام TCP در حالت انتقال(Transport mode) باشد، مقدار این فیلد برابر ۶ خواهد شد

فیلد payload length همانطوریکه از نامش پیداست طول payload را تعیین می‌کند.

فیلد Reserved از دو بایت تشکیل شده است.برای آینده در نظر گرفته شده است.

فیلد security parameter Index یا SPI از ۳۲ بیت تشکیل شده است. این فیلد از SA تشکیل شده که جهت باز کردن پکت‌های کپسوله شده بکار می‌رود. نهایتاً ۹۶ بیت نیز جهت نگهداری احراز هویت پیام Hash یا (HMAC) بکار می‌رود.

HMAC حفاظت تمامیت دادهٔ ارسالی را برعهده دارد. زیرا فقط نقاط نظیر به نظیر از کلید سری اطلاع دارند که توسط HMAC بوجود آمده و توسط همان چک می‌شود.

چون پروتکل AH حفاظت دیتاگرام IP شامل بخشهای تغییر ناپذیری مثل IP آدرسها نیز هست، پروتکل AH اجازه ترجمه آدرس شبکه را نمی‌دهد. NAT یا ترجمه آدرس شبکه در فیلد IP آدرس دیگری (که معمولاً IP آدرس بعداً می‌باشد) قرار می‌گیرد. وبه این جهت تغییر بعدی HMAC معتبر نخواهد بود. در شکل زیر حالتهای انتقال و تونل در پروتکل AH به نمایش در آمده است.همان طور که می‌بینید این پروتکل در این دو حالت ارتباط امن بین دو نقطه انتهائی که در دو شبکه مجزا قرار دارند را فراهم می‌آورد، همچنین

ارتباط امن بین دو نقطه در یک شبکه داخلی و یک نقطه انتهائی و یک مسیر یاب یا حفاظ دیواره آتش (Firewall) را ممکن می‌سازد.

پروتکل Encapsulation Security Payload(ESP)

پروتکل ESP سرویسهای امنیتی زیر را ارائه می‌کند:

محرمانگی

احراز هویت مبدا داده ارسالی

رد بسته‌های دوباره ارسال شده

در واقع پروتکل ESP هم امنیت تمامیت داده (سلامت داده‌های ارسالی) پکت‌هایی که از HMAC استفاده می‌کنند را تامین کنید و هم محرمانگی از طریق اصول رمزنگاری (Encryption principle) بکار گرفته شده .بعد از رمزنگاری پکت و محاسبات مربوط به HMAC، سرآیند ESP محاسبه و به پکت اضافه می‌شود. سرآیند ESP شامل دو بخش است که مطابق شکل زیر نمایش داده شده است.

اولین ۳۲ بیت سرآیند ESP همان SPI است که درSA بکار گرفته شده و جهت بازگشایی پکت کپسوله شده ESP بکار می‌رود.

دومین فیلد همان شماره توالی یا Sequence Number می‌باشد که به جهت حفاظت از تهاجمات داده‌های بازگشتی استفاده می‌شود.

سومین فیلد همان بردار مقدار اولیه یا Initialization Vector (IV) می‌باشد. این فیلد نیز برای پردازش رمزنگاری بکار می‌رود. الگوریتمهای رمزنگاری متقارن اگر از IV استفاده نکنند، مورد تهاجم متوالی روی پکت قرار می‌گیرد. IV این اطمینان را می‌دهد تا دو مشخصه Payload روی دو Payload رمز شده مختلف قرار گیرد. پردازش رمزنگاری در IPSec در دو بلوک رمز (Cipher) بکار می‌رود. بنابراین اگر طول Payloadها تک تک باشند. , Payload IPSecها را به شکل لایه لایه قرار می‌دهد. و از اینرو طول این لایه‌ها همواره در حال اضافه شدن است. طول لایه (2 Pad length) بایت است.

فیلد بعدی که همان Next header می‌باشد، سرآیند بعدی را مشخص می‌کند.

این پروتکل HMAC است که مانند پروتکل HA از تمامیت و سلامت داده‌های ارسالی حفاظت می‌کند. فقط این سرآیند است که می‌تواند به Payload اعتبار دهد. سرآیند IP شامل پروسه محاسبه نمی‌باشد.

NAT هیچ ارتباطی به کار ESP ندارد و این بخش هنوز هم ممکن است بخشی از IPSec باشد و با آن ترکیب گردد. NAT پیمایشی (NAT-Traversal) راه حلی است در کپسوله کردن پکت‌های ESP به همراه پکت‌های

UDP. در شکل زیر حالتهای انتقال و تونل در پروتکلESP به نمایش در آمده است.

همان طور که می‌بینید این پروتکل در این دو حالت ارتباط امن بین دو نقطه انتهائی که در دو شبکه مجزا قرار دارند را فراهم می‌آورد، همچنین ارتباط امن بین دو نقطه در یک شبکه داخلی و یک نقطه انتهائی و یک مسیر یاب یا حفاظ دیواره آتش(Firewall) را ممکن می‌سازد.

پروتکل IKE

IKE پروتکلی است که چندین مسئله مهم در ارتباط امن را تنظیم می‌کند. احراز هویت نقاط نظیر و کلید تبادلی متقارن. این پروتکل مجمع امنیت (SA) را ایجاد کرده و درSAD یا پایگاه مجمع امنیت (Security Association data base) قرار می‌دهد. IKE پروتکلی است که عموماً نیازمند فضای کاربر فوق العاده‌ای است و روی سیستم‌های عامل پیاده سازی نمی‌شود. پروتکل IKE، از پورت شماره UDP/500 استفاده می‌کنند. IKE از دو مرحله تشکیل شده است. اولین مرحله همان تشکیل مجمع امنیت مدیریت کلید (Internet Security Association and key) یا (ISAKMP SA) می‌باشد. در مرحله دوم ISAKMPSA، برای مذاکره و تنظیم IPSec , SA بکار می‌رود. احراز هویت مرحله اول نقاط نظیر معمولاً بر

مبنای کلیدهای پیش اشتراک شده (Per shared Keys)، کلیدهای RSA و گواهینامه X509 بوجود می‌آید. مرحله اول از دوحالت پشتیبانی می‌نماید. حالت اصلی (main mode) و حالت تهاجمی (aggressive mode) این دو حالت نقاط نظیر را احراز هویت کرده و ISAKMP SA را تنظیم می‌نمایند. در حالت تهاجمی تنها نصف تعداد پیامها در این مورد تحت پوشش قرار می‌گیرد. به هر حال این خود یک اشکال محسوب می‌شود، زیرا این حالت نمی‌تواند از هویت نقاط نظیر پشتیبانی حفاظت نماید و از این جهت است که این حالت با داشتن کلید پیش اشتراکی (PSK) مستعد حملات میان راهی (man-in-the-middle) خواهد بود. از طرف دیگر تنها منظور از حالت تهاجمی همین است. در حالت اصلی نه تنها از کلید پیش شرط مختلف نمی‌تواند پشتیبانی نمایدبلکه نقاط نظیر به نظیر را نیز نمی‌شناسد. در حالت تهاجمی که از حفاظت هویت افراد / نقاط حمایت نمی‌کند و هویت کاربران انتهایی را چنین شفاف انتقال می‌دهد. بنابراین نقاط نظیر هر چیز را خواهد دانست پیش از آنکه احراز هویتی در مورد جا و کلیدهای پیش شرط بتواند بکار برد. در مرحله دوم پروتکل IKE که SAهای پیشنهادی تبادل می‌شوند و توافقاتی بر پایه ISAKMP SA برای SA انجام خواهد شد. ISAKMP SA احراز هویت برای حفاظت از تهاجمات میان راهی را تهیه می‌بینند. دومین مرحله از حالت سریع استفاده می‌کند. معمولاً دو نقطه نظیر روی

SAKMP SA با هم مذاکره و توافق می‌کنند که هر دو طرف معمولاً روی چندین مذاکره (حداقل ۲ تا) بطور غیر مستقیم توافق کنند.

مفاهیم اساسی

با استفاده از پروتکل IPsec شما می‌توانید پنهان کردن داده‌ها، صحت داده‌ها، اعتبار یا سندیت و Anti Reply Protection را برای ترافیک شبکه به صورت زیر ایجاد کنید:

-ایجاد امنیت انتها به انتها از کاربر به کارگزار، از کارگزار به کارگزار و از کاربر به کاربر در مد انتقال IPSec

-ایجاد دسترسی راه دور امن از کاربر به دروازه بر روی اینترنت با استفاده از پروتکل تونل سازی لایه ۲ (L2TP) امن شده بوسیله IPSec .

-IPSec یک اتصال دروازه به دروازه امن را روی WAN اختصاصی یا یک اتصال تحت اینترنت با استفاده از تونل L2TP/IPSec یا مد تونل IPSec فراهم می‌کند. (مد تونل IPSec برای کار با VPN دسترسی راه دور طراحی نشده است.) سیستم‌عامل WIN2000 پیکربندی و مدیریت امنیت شبکه را بوسیله IP Security آسان کرده است.

SSL چیست؟

(SSL یا Secure Socket Layer) راه‌حلی جهت برقراری ارتباطات ایمن میان یک سرویس‌دهنده و یک سرویس‌گیرنده است که توسط شرکت Netscape ارائه شده است. در واقع SSL پروتکلی است که پایین‌تر از لایه کاربرد (لایه ۴ از مدل TCP/IP) و بالاتر از لایه انتقال (لایه سوم از مدل TCP/IP) قرار می‌گیرد. مزیت استفاده از این پروتکل بهره‌گیری از موارد امنیتی تعبیه شده آن برای امن کردن پروتکل‌های غیرامن لایه کاربردی نظیر HTTP، LDAP، IMAP و... می‌باشد که براساس آن الگوریتم‌های رمزنگاری بر روی داده‌های خام (plain text) که قرار است از یک کانال ارتباطی غیرامن مثل اینترنت عبور کنند، اعمال می‌شود و محرمانه ماندن داده‌ها را در طول کانال انتقال تضمین می‌کند. به بیان دیگر شرکتی که صلاحیت صدور و اعطاء گواهی‌های دیجیتال SSL را دارد برای هر کدام از دو طرفی که قرار است ارتباطات میان شبکه‌ای امن داشته باشند، گواهی‌های مخصوص سرویس‌دهنده و سرویس‌گیرنده را صادر می‌کند و با مکانیزم‌های احراز هویت خاص خود، هویت هر کدام از طرفین را برای طرف مقابل تأیید می‌کند، البته غیر از این‌کار می‌بایست تضمین کند که اگر اطلاعات حین انتقال مورد سرقت قرار گرفت، برای رباینده قابل درک و استفاده نباشد که این‌کار را با کمک الگوریتم‌های رمزنگاری

و کلیدهای رمزنگاری نامتقارن و متقارن انجام می‌دهد.

ملزومات یک ارتباط مبتنی بر پروتکل امنیتی SSL

برای داشتن ارتباطات امن مبتنی بر SSL عموماً به دو نوع گواهی دیجیتال SSL یکی برای سرویس‌دهنده و دیگری برای سرویس‌گیرنده و یک مرکز صدور و اعطای گواهینامه دیجیتال یا CA نیاز می‌باشد. وظیفه CA این است که هویت طرفین ارتباط، نشانی‌ها، حساب‌های بانکی و تاریخ انقضای گواهینامه را بداند و براساس آن‌ها هویت‌ها را تعیین نماید.

اجزای پروتکل SSL

پروتکل SSL دارای دو زیر پروتکل تحت عناوین زیر می‌باشد.

SSL Record Protocol که نوع قالب‌بندی داده‌های ارسالی را تعیین می‌کند.

SSL Handshake Protocol که براساس قالب تعیین شده در پروتکل قبلی، مقدمات ارسال داده‌ها میان سرویس‌دهنده‌ها و سرویس‌گیرنده‌های مبتنی بر SSL را تهیه می‌کند.

بخش‌بندی پروتکل SSL به دو زیر پروتکل دارای مزایای چندی است. ازجمله:

اول: در ابتدای کار و طی مراحل اولیه ارتباط (Handshake) هویت سرویس‌دهنده برای سرویس‌گیرنده مشخص می‌گردد.

دوم: در همان ابتدای شروع مبادلات، سرویس‌دهنده و گیرنده بر سر نوع الگوریتم رمزنگاری تبادلی توافق می‌کنند.

سوم: در صورت لزوم، هویت سرویس گیرنده نیز برای سرویس‌دهنده احراز می‌گردد.

چهارم: در صورت استفاده از تکنیک‌های رمزنگاری مبتنی بر کلید عمومی، می‌توانند کلیدهای اشتراکی مخفی را ایجاد نمایند.

پنجم: ارتباطات بر مبنای SSL رمزنگاری می‌شوند. الگوریتم های رمزنگاری پشتیبانی شده درSSL در استانداردSSL، از اغلب الگورتیم های عمومی رمزنگاری و مبادلات کلید (Key Exchcenge Algorithm) نظیر DES، DSA، KEA، MD5، RC2،RC4، RSA و RSA Key Exchauge، SHA-1، Skipjack و DES3 پشتیبانی می‌شود و بسته به این‌که نرم‌افزارهای سمت سرویس‌دهنده و سرویس‌دهنده نیز از موارد مذکور پشتیبانی نمایید، ارتباطاتSSL می‌تواند براساس هر کدام این از الگوریتم ها صورت پذیرد. البته بسته به طول کلید مورد استفاده در الگوریتم و قدرت ذاتی الگوریتم

می‌توان آن‌ها را در رده‌های مختلفی قرار دارد که توصیه می‌شود با توجه به سناریوهای موردنظر، از الگوریتم‌های قوی‌تر نظیر DES3 با طول کلید ۱۶۸ بیت برای رمزنگاری داده‌ها و همچنین الگوریتم SHA-1 برای مکانیزم‌های تأیید پیغام MD 5 استفاده شود و یا این‌که اگر امنیت در این حد موردنیاز نبود، می‌توان در مواردی خاص از الگوریتم رمزنگاری RC 4 با طول کلید ۴۰ بیت و الگوریتم تأیید پیغام MD 5 استفاده نمود. (شکل زیر) با تشکر امیر علی انوری :-)

نحوه عملکرد داخلی پروتکلSSL

همان‌طور که می‌دانید SSL می‌تواند از ترکیب رمزنگاری متقارن و نامتقارن استفاده کند. رمزنگاری کلید متقارن سریع‌تر از رمزنگاری کلیدعمومی است و از طرف دیگر رمزنگاری کلید عمومی تکنیک‌های احراز هویت قوی‌تری را ارایه می‌کند. یک جلسه SSL (SSL Session) با یک تبادل پیغام ساده تحت عنوان SSL Handshake شروع می‌شود. این پیغام اولیه به سرویس‌دهنده این امکان را می‌دهد تا خودش را به سرویس‌دهنده دارای کلید عمومی معرفی نماید و سپس به سرویس‌گیرنده و سرویس‌دهنده این اجازه را می‌دهد که یک کلید متقارن را ایجاد نمایند که برای رمزنگاری‌ها و رمزگشایی سریع‌تر در جریان ادامه مبادلات مورد استفاده قرار می‌گیرد. گام‌هایی که قبل

از برگزاری این جلسه انجام می‌شوند براساس الگوریتم RSA Key Exchange عبارتند از:

- سرویس گیرنده، نسخه SSL مورد استفاده خود، تنظیمات اولیه درباره نحوه رمزگذاری و یک داده تصادفی را برای شروع درخواست یک ارتباط امن مبتنی بر SSL به سمت سرویس‌دهنده ارسال می‌کند.

- سرویس‌دهنده نیز در پاسخ نسخه SSL مورد استفاده خود، تنظیمات رمزگذاری و داده تصادفی تولید شده توسط خود را به سرویس‌گیرنده می‌فرستد و همچنین سرویس‌دهنده گواهینامه خود را نیز برای سرویس‌گیرنده ارسال می‌کند و اگر سرویس‌گیرنده از سرویس‌دهنده، درخواستی داشت که نیازمند احراز هویت سرویس‌گیرنده بود، آن را نیز از سرویس‌گیرنده درخواست می‌کند.

- سپس سرویس‌گیرنده با استفاده از اطلاعاتی که از سرویس‌دهنده مجاز در خود دارد، داده‌ها را بررسی می‌کند و اگر سرویس‌دهنده مذکور تأیید هویت شد، وارد مرحله بعدی می‌شود و در غیراین‌صورت با پیغام هشداری به کاربر، ادامه عملیات قطع می‌گردد.

- سرویس‌گیرنده یک مقدار به نام Secret Premaster را برای شروع جلسه ایجاد می‌کند و آن را با استفاده از کلید عمومی (که اطلاعات آن معمولاً در سرویس‌دهنده موجود است) رمزنگاری می‌کند و این مقدار رمز شده را به سرویس‌دهنده ارسال می‌کند.

- اگر سرویس‌دهنده به گواهینامه سرویس‌گیرنده نیاز داشت می‌بایست در این گام برای سرویس‌دهنده ارسال شود و اگر سرویس‌گیرنده نتواند هویت خود را به سرویس‌دهنده اثبات کند، ارتباط در همین‌جا قطع می‌شود.

- به محض این‌که هویت سرویس‌گیرنده برای سرویس‌دهنده احراز شد، سرویس‌دهنده با استفاده از کلید اختصاصی خودش مقدار Premaster Secret را رمزگشایی می‌کند و سپس اقدام به تهیه مقداری به نام Master Secret می‌نماید.

- هم سرویس‌دهنده و هم سرویس‌گیرنده با استفاده از مقدار master Secret کلید جلسه (Session Key) را تولید می‌کنند که در واقع کلید متقارن مورد استفاده در عمل رمزنگاری و رمزگشایی داده‌ها حین انتقال اطلاعات است و در این مرحله به نوعی جامعیت داده‌ها بررسی می‌شود.

- سرویس‌گیرنده پیغامی را به سرویس‌دهنده می‌فرستد تا به او اطلاع دهد، داده بعدی که توسط سرویس‌گیرنده ارسال می‌شود به وسیله کلید جلسه رمزنگاری خواهد شد و در ادامه، پیغام رمز شده نیز ارسال می‌شود تا سرویس‌دهنده از پایان یافتن Handshake سمت سرویس‌گیرنده مطلع شود.

- سرویس‌دهنده پیغامی را به سرویس‌گیرنده ارسال می‌کند تا او را از پایان Handshake سمت سرویس‌دهنده آگاه نماید و همچنین این که داده بعدی که ارسال خواهد شد توسط کلید جلسه رمز می‌شود.

- در این مرحله SSL Handshake تمام می‌شود و از این به بعد جلسه SSL شروع می‌شود و هر دو عضو سرویس‌دهنده و گیرنده شروع به رمزنگاری و رمزگشایی و ارسال داده‌ها می‌کنند.

حملات تأثیرگذار برSSL

SSL نیز از حملات و نفوذهای مختلف در امان نیست. بعضی از حملات متداولی که براین پروتکل واقع می‌شود عبارتند ازTraffic Analysis : یا تحلیل ترافیک، حملات Certification Injection و حملات از نوع Man in the middle.

SSH چیست؟

به عنوان یک تعریف بسیار ساده می‌توان SSH را این گونه بیان کرد : SSH یک روش قدرتمند و پر استفاده و البته نرم‌افزاری است که برای دستیابی به امنیت شبکه طراحی شده‌است. هربار که داده‌ای از طرف کامپیوتر به شبکه فرستاده می‌شود، به صورت خودکار توسط SSH کدگذاری می‌شود. هنگامی که داده به مقصد خود می‌رسد به صورت خودکار کدگشایی می‌شود. نتیجه‌ای که خواهد داشت کدگذاری نامرئی خواهد بود.

بدین صورت کاربران نهایی درگیر پروسه کدگذاری و کدگشایی نخواهند شد و از ارتباط امن خود می‌توانند به خوبی استفاده کنند. امنیت سیستم کدگذاری SSH با استفاده از الگوریتم های پیچیده و مدرن تضمین می‌شود. تا آنجا که امروزه در سیستم های حیاتی و بسیار حساس از این سیستم استفاده می‌شود. به صورت معمول محصولاتی که از SSH استفاده می‌کنند از دو بخش خادم و مخدوم (Client/Server) تشکیل می‌شوند. Clientها با استفاده از تنظیمات سرور مربوطه به آن وصل می‌شوند و سرور وظیفه تایید هویت و قبول و یا رد ارتباط را به عهده دارد. نکته : باید توجه داشته باشید تشابه نام Secure Shell با محیطهایی مانند Bourne shell و یا C Shell نشان دهنده این نیست که SSH نیز محیطی است که وظیفه تفسیر فرامین برای سیستم‌عامل را بر عهده دارد. با اینکه SSH تمامی مشکلات را حل نخواهد کرد، اما در مورد بسیاری از موارد می‌تواند راه حل مناسبی باشد. برخی از این موارد عبارتند از :

یک پروتکل خادم/مخدوم امن برای کدگذاری و انتقال داده‌ها در شبکه.

تعیین هویت کاربران به وسیله کلمه عبور ، host ، public key و یا استفاده از PGP،Kerberos و یا PAM

قابلیت امن کردن برنامه‌های ناامن شبکه مانند Telnet، FTP و در کل هر برنامه‌ای که بر اساس پروتکل TCP/IP بنا شده است.

بدون هیچ تغییر در استفاده کاربر نهایی (End User) پیاده شده و قابلیت پیاده سازی بر روی بیشتر سیستم‌عامل‌ها را دارد.

یژگی های امنیتی Windows XP Service Pack 2

هدف اصلی SP2، بهبود امنیت کاربران ویندوز XP است که این کار را با 4 رویکرد انجام می دهد:

- محافظت بهتر از شبکه
- بهبود حفاظت از حافظه
- ایمن سازی امور مربوط به E-Mail
- امنیت در مرور اینترنت توسط Internet Explorer

محافظت از شبکه با فایروال پیشرفت کرده ویندوز است (که قبلا تحت عنوان Internet Connection Firewall وجود داشت) که به صورت پیش فرض فعال می باشد. این فایروال در مراحل اولیه بوت شدن ویندوز، قبل از اینکه Network Stack فعال شود، شروع به کار می کند و نفوذ گر در مراحل اولیه بالا آمدن سیستم هم نمی تواند آن را مورد حمله قرار دهد. همچنین هنگام خاموش شدن سیستم نیز، این فایروال بسیار دیر خاموش می شود و بعد از اینکه لایه های شبکه غیر

فعال شدند، این فایروال کار خود را پایان می دهد. این فایروال دارای واسط کاربری قابل قبولی برای مدیریت آن می باشد و قابل مدیریت و اعمال سیاست از سوی مدیر شبکه یا همان Domain Administrator می باشد. همچنین از IPv6 که در این نسخه از ویندوز ارائه شده است نیز پشتیبانی می کند

فصل سوم

شباهت ها ،تفاوت ها و پیکربندی

IPV6

اینترنت پروتکل ویرایش 6 یک پروتکل packet-switched لایه ای شبکه ای برای کارهای اینترنتی می باشد. این نسخه از IP به اندازه IP V.4 ،که نسخه فعلی پروتکل اینترنت برای کاربردهای عمومی در اینترنت است ،موفق طراحی شده است.

مهمترین بهبودی که در IP V.6 ایجاد شده است ، افزایش تعداد آدرسهای در دسترس برای تجهیزات شبکه شده است ، برای مثال ، هر تلفن همراه و وسیله الکترونیکی متحرک دارای آدرس خاص خود می باشد. IP V.4 از 232 آدرس (در حدود 4/3 بیلیون آدرس) پشتیبانی میکند ، که برای تخصیص یک آدرس برای هر فرد زنده ناکافی است، و فقط برای وسایل نصب شده و تجهیزات پورتابل کفایت می کند . با اینحال ، IP V.6 از 2128 آدرس (در حدود 340 بیلیون بیلیون بیلیون بیلیون آدرس) پشتیبانی میکند ، یعنی برای هر کدام از 6/5 بیلیون فرد زنده ، 1028 ×5 آدرس تخصیص داده می شود. با چنین حجم بالایی از آدرسها ی در دسترس ،گره های IP V.6 می توانند آدرسهای گسترده در سطح جهانی را بدون اینکه نیازی به انتقال آدرس شبکه باشد ،داشته باشند.

خصوصیات IP V.6

IP V.6 یک نمونه گسترش یافته محافظه کارانه از IP V.4 است. پروتکلهای انتقالی و لایه ای برای کار با IP V.6 نیاز به تغییرات خیلی کم یا اصلاً نیازی به تغییر ندارند ، استثنا در این زمینه فقط شامل پروتکلهای کاربردی که آدرسهای لایه ای / شبکه ای را شامل میشوند ،می باشد. (همانند FTP یا NTPv3).

با اینحال ، کاربردها اغلب نیاز به تغییرات کوچکی و کامپایلر مجدد دارند تا بتوانند در IP V.6 کار کنند.

پیکربندی خودکار هاستهای بدون تابعیت :

هاستهای IP V.6 می توانند بهنگام اتصال به یک شبکه IP V.6 در حال اجرا به صورت خودکار پیکر بندی گردند. زمانی که برای اولین بار به یک شبکه متصل میشوید، هاست یک درخواست مولتی کاست لینک محلی را برای پیکربندی پارامترها ارسال می کند ؛ اگر پیکربندی مناسب باشد ، روتورهای به هر درخواست در بسته آگهی روتور که در بردارنده پارامترهای پیکربندی شده شبکه – لایه باشد ،پاسخ می دهد.

اگر پیکر بندی خودکار IP V.6 مناسب نباشد، هاست می تواند از پیکربندی خودکار مناسب (DHCP v.6) یا پیکر بندی دستی استفاده کند.

پیکر بندی خودکار بدون تابعیت فقط برای هاستها مناسب است و روتورهای باید به صورت دستی پیکربندی شوند.

مولتی کاست (Multicast) :

Multicast بخشی از پروتکل مبنا در IP V.6 است. این بخش در طرف مقابل IP V.4 قرار دارد که در آن مولتی کاست به صورت اختیاری می باشد.

بیشتر محیطها در حال حاضر زیرساختارهای شبکه ای خود را به گونه ای تنظیم نم کنند که مولتی کاست را انجام دهند. به این معنا که ، جنبه لینکی مولتی کاست کار خواهد کرد ولی جنبه مکانی، جنبه سازمانی و جنبه جهانی مولتی کاست انجام نخواهد شد.

IP V.6 فاقد یک وسیله لینک-محلی است ، همان اثری که از طریق مولتی کاست کردن گروه تمام هاست بدست میآید. (FF::1).

m6bone برای گسترش یک شبکه جهانی مولتی کاست IP V.6 مورد استفاده قرار می گیرد.

Jumbograms :

در IP V.4 بسته ها به اندازه 64 کیلو بایت محدود شده است . هنگام ارتباط بین بخشها یا ارتباط بین لینک ها باحداکثر واحد انتقال بیش از 65576 گروه

هشت تایی ،IP V.6 برای بسته هایی که با این محدودیت مواجه هستند بهترین پشتیبانی را انجام می دهد،به این حالت jumbograms می گویند که می تواند تا 4 گیگا بایت را پشتیبانی نماید. استفاده از jumbograms می تواند بازده را در شبکه های با MTU بالا بهبود بخشد.

امنیت شبکه – لایه :

IPsec ،پروتکل مربوط به رمزگذاری و تعیین اعتبار IP شبکه – لایه ، یک بخش مرتبط با پروتکل مبنای مورد استفاده در IP V.6 است ، که بر عکس IP V.4 می باشد که در آن این بخش اختیاری است (ولی معمولاً مورد استفاده قرار می گیرد).

پویایی:بر خلاف IP V.4 موبایل ، IP V.6 موبایل (MIP V.6) از مسیرگذاری سه جانبه دوری میکند و بنابراین دارای بازده ای به اندازه IP V.6 معمولی است. این مزیت به شدت فرضی است ، زیرا نه MIP و نه MIP V.6 امروزه به طور گسترده ، توسعه نیافته اند.

وضعیت گسترش :

از دسامبر 2005 ، IP V.6 برای بخش کوچکی از آدرسهای فعال در اینترنت قابل دسترسی برای عموم اعمال شد ، البته همزمان از IP V.4 نیز استفاده میشود. پذیرشIP V.6 با معرفی مسیرگزینی دورن دومینی بدون

طبقه بندی (CIDR) و انتقال آدرس شبکه (NAT) ،که هر کدام دارای تاثیر جزیی بر خروج فضای آدرسی دارند ، کاهش یافته است. پاول میلسون ،(مدیر APNIC) در سال 2003 گفت که ،بر آورد میشود که میزان آدرسهای در دسترس IP V.4 بر اساس نرخ رشد فعلی ، کم خواهد شد ، تا این که در سال 2023 فضای در دسترسی نخواهیم داشت. در حالي که در سپتامبر 2005 گزارشی از سیسکو نشان میداد که میزان فضای آدرسی در دسترس ظرف مدت 4 تا 5 سال دیگر به اتمام می رسد. همچنین در نوامبر 2006 ،در یک گزارش به روز شده ، اعلام شد که مقدار IANA از آدرسهای اختصاص داده نشده ، در می 2011 به اتمام خواهد رسید، که با توجه به رجیسترهای اینترنت منطقه ای این وضعیت در آگوست 2012 اتفاق خواهد افتاد. این گزارش همچنین نشان داد که اگر آدرسهای تخصیص یافته استفاده نشده باز پس گرفته شود و برای تقاضای فعلی مورد استفاده قرار گیرند ، تخصیص آدرس IP V.4 می تواند تا سال 2024 ادامه پیدا کند. دولت ایالات متحده ،اعلام کرده است که زیرساختهای شبکه ایی تمام موسسات فدرال باید تا سال 2008 ، IP V.6 را ساپورت کنند. اما برای انجام این کار دو چالش وجود دارد:

1- هیچ بودجه فدرال در دسترسی برای انتقال IP V.6 وجود ندارد. بنابراین انتظار می رود که شرکتها از

خرید تجهیزات و به روز رسانی شبکه شانه خالی کنند. بیشتر شرکتها این طرح انتقال را در دست اجرا دارند ولی ارزیابیها نشان داده است که در صورت اجرای عملی این انتقال بسیاری از شرکتها و موسسات دارای تاخیر هستد .

2- بودجه موسسات IT به شدت مورد توجه قرار گرفته است ، مخصوصاً بودجه جاری سال 2007 برای IT با توجه به ادامه تفکیک ، ثابت مانده است.

در حالیکه چین برنامه ریزی کرده است که پی قراول استفاده از IP V.6 طی برنامه 5 ساله برای نسل بعدی اینترنت چین ،باشد.

بدون توجه به پیکربندی خودکار بدون تابعیت ، آدرس دهی انعطاف پذیرتر و کشف امنیت همسایه (SEND) ، سایر خصوصیات IP V.4 بدون تغییر یا با تغییر کوچکی به IP V.6 منتقل می شود. بنابراین توسعه IPV6 با به اتمام رسیدن فضای آدرس ،شروع می شود.

مشخص کردن شبکه :

شبکه های IP V.6 با استفاده از نکات CIDR نوشته می شود.

هر شبکه IP V.6 (یا زیر شبکه) مجموعه ای از آدرسهای IP V.6 است،بیتهای ابتدایی آدرسها ، که

برای شناسایی تمامی هاستها در شبکه مورد استفاده قرار می گیرند ،پیشوند شبکه نامیده می شوند.

یک شبکه با اولین آدرس در شبکه و اندازه بیتهای پیشوند (در مبنای دو) که بوسیله ممیز از هم جدا شده اند ، مشخص می شود.

برای مثال : db8:1234::/482001:0 نشان دهنده شبکه ای با آدرس های از db8:1234:0000:0000:0000:0000:00002001:0

تا db8:1234:FFFF:FFFF:FFFF:FFFF:FFFF2001:0 می باشد.

با توجه به اینکه یک هاست می تواند به صورت یک شبکه با پیشوند 128 بیتی مشاهده شود ، برخی اوقات شما می توانید آدرسهای هاستی را ببینید که به صورت 128 بیتی نوشته شده است.

بسته IP V.6 :

بیت

flow label	traffic class	version
hop limit	next header	pay load lenth
source address		
destination address		

ساختار یک عنوان بسته IP V.6

بسته IP V.6 شامل دو بخش اصلی است: عنوان و متن پیام

عنوان در اولین 40 هشت تایی/بایت بسته قرار دارد و شامل منبع و آدرسهای مقصد است(هر کدام 128 بیت) است و همانند ورژن (IP نسخه 4 بیتی)،مقدار ترافیک (8 بیتی ،حق تقدم بسته)،برچسب مسیر(20 بیتی ، مدیریت QOS)، طول متن پیام بر حسب بایت(16 بایت) ، عنوان بعدی (8 بیتی)و محدوده هاپ (8 بیتی ، زمان ماندن) می باشد.متن پیام می تواند در حالت استاندارد تا 64 کیلوبایت ، یا در حالت "متن بزرگ" مقادیر بزرگتری را داشته باشد.

آدرس دهی در IPV6

در IP v.4 از روش معروف هشتتايي براي آدرس‌دهي استفاده مي‌كرديم و با استفاده از آن كلاس‌هاي آدرس A، B، C، D و E را تعريف مي‌كرديم و با توجه به ماسك زير شبكه‌اي كه اعمال مي‌كرديم مي‌توانستيم شبكه، زير شبكه و شماره‌هاي گره‌ها را تشخيص دهيم. IP v.6 مقداري با اين مفهوم متفاوت است و ما اين تفاوت را در اين‌جا توضيح مي‌دهيم.در IP v.6 سه روش آدرس‌دهي وجود دارد كه عبارتند از: آدرس منحصر به فرد، گروهي و anycast . حالت پخشي وجود ندارد. آدرس منحصر به فرد مانند ارتباط نقطه به نقطه مي‌باشد و يك بسته فقط به يك آدرس مشخص ارسال مي‌شود نه به

آدرس‌هاي ديگر و اين آدرس به يك واسط مشخص و ثابت در شبكه اختصاص پيدا مي‌كند. حالت گروهي به فرآيندي اشاره دارد كه در آن يك بسته به تعدادي از گيرنده‌ها ارسال مي‌شود اين كار متفاوت با حالت پخشي مي‌باشد زيرا در حالت پخشي بسته ارسال شده به تمامي افزارها و دستگاه‌هاي موجود در زير شبكه تحويل داده مي‌شود ولي در حالت گروهي ارسال بسته فقط براي تعداد محدودي از افزارها كه از قبل تنظيم شده‌اند صورت مي‌گيرد بنابراين افزارهايي بسته را دريافت مي‌كنند كه حالت گروهي از قبل براي آن‌ها تعريف شده باشد. حالت anycast مشابه حالت گروهي مي‌باشد با اين تفاوت كه بسته تنها به اولين افزاري كه در گروه anycast مي‌تواند بسته را دريافت كند تحويل داده مي‌شود و به تمامي افزارهاي موجود در گروه anycast تحويل داده نخواهد شد.قراردادي كه براي نشان دادن و نوشتن آدرس‌هاي 128 بيتي در IP v.6 به‌كار مي‌رود استفاده از بلوك‌هايي از 4 عدد هگزا دسيمال است كه با علامت كولن (:) از همديگر جدا مي‌شوند، يك مثال در زير آورده شده است.

FEDC:CD56:6543:7896:F123:2344:9877:7654

نوشتن اين اعداد مقداري پرزحمت است البته نه براي كاربراني كه در هرحالت مي‌توانند از نام ميزبان به‌جاي آدرس آن استفاده كنند بلكه براي مديراني كه مجبورند اين اعداد را براي پيكربندي فايل‌ها و

بانك‌هاي اطلاعاتي و افزارها بنويسند. براي خلاصه كردن اين عدد نويسي، مطابق قرارداد از نوشتن يك بلوك از صفرهاي متوالي آدرس جلوگيري مي‌كنند. اين كار بسيار مفيد واقع خواهد شد مخصوصاً در روزهاي اول عمر IP v.6 كه مقدار زيادي از فضاي آدرس از صفرها تشكيل شده است. قرارداد حذف كردن صفرها به عددنويسي با دو كولن معروف است و آن به اين معنا است كه اگر دو كولن در يك آدرس نشان داده شود آن آدرس را با وارد كردن صفرها بين دو كولن به 128 بيت مي‌رسانيم. مثال زير اين عمل را نشان مي‌دهد.

FF02:0000:0000:0000:0000:0000:0000:0002

كه مي‌توان آدرس فوق را به صورت زير نمايش داد.FF02:2در نوشتن اعداد مربوط به آدرس‌هاي IP v.6 مي‌توان يك پيشوند آدرس، همان‌طور كه در IP v.4 استفاده مي‌شد تعريف نمود، در IP v.4 همان‌طور كه ديديد تعداد بيت‌هايي كه به عنوان پيشوند به آدرس اضافه مي‌شد و آدرس زير شبكه را مشخص مي‌كرد، را مي‌توانستيم با استفاده از علامت / (slash) از آدرس جدا كنيم. در IP v.6 نيز از همان قالب (IP v.6-prefix/prefix-length) مي‌توان استفاده نمود. مثال زير يك آدرس IPv4 كلاس B با تعداد بيت‌هاي 24 تايي (كه معادل با ماسك زير شبكه 255.255.255.0 است) را نشان مي‌دهد.24/173.8.4.3از همان روش در IP v.6 نيز مي‌توان استفاده كرد، مثال زير نشان مي‌دهد كه اولين 64

بيتي كه به عنوان پيشوند مي‌باشد در جدول مسيريابي براي مشخص كردن قسمت‌هاي مجزا و انحصاري شبكه استفاده مي‌شود

FEDC::1234:2345:2222/64

امکانات و ویژگی های IPV6

افزایش فضای آدرس دهی : یکی از مهمترین مزایای IP v.6 ، افزایش تعداد فضای آدرس دهی است. فضای آدرس دهی IP v.6 به اندازه ای زیاد است که شاید نتوان آن را با فضای آدرس دهی IP v.4 مقایسه نمود. در IP v.4 ، تعداد 4,294,967,296 فضای آدرس دهی وجود دارد در حالی که این عدد در IPv.6 به عدد 340,282,366,920,938,463,463,374,607,431,768,211,456 می رسد.

افزایش آدرس های سراسری قابل رویت به سازمان ها این اجازه را خواهد داد که مسیر خود را از آدرس های IP غیرقابل روت ارائه شده توسط NAT جدا نموده و برنامه های مورد نیاز خود را در یک محیط واقعی end-to-end استفاده نمایند.

پیکربندی اتوماتیک stateless :

پیکربندی اتوماتیک IP در IP v.4 از طریق سرویس دهنده DHCP انجام می شود. در IP v.6 این کار توسط DHCP v.6 انجام خواهد شد. در IP v.6 این وضعیت توسعه و به پیکربندی اتوماتیک stateless تعمیم یافته است.

با استفاده از پیکربندی اتوماتیک stateless به دستگاه ها اجازه داده می شود که پیکربندی آدرس های IP v.6 خود را از طریق ارتباط با یک روتر مجاور انجام دهند .با این که پیکربندی اتوماتیک stateless برای اکثر محیط ها دارای مزایائی است ،ولی در شبکه هائی که دارای تعداد زیادی از دستگاه ها با قابلیت محدود مدیریتی می باشند، مسائلی را به دنبال خواهد داشت.

یک شبکه مبتنی بر تعداد زیادی سنسور که ممکن است شامل میلیون ها دستگاه بی سیم راه دور باشد که صرفا" بر روی شبکه قابل دسترس می باشند ، نمونه ای در این زمینه است. پیکربندی اتوماتیک به سازمان ها کمک خواهد کرد که هزینه نگهداری و مدیریت شبکه خود را کاهش دهند .با این که پیکربندی اتوماتیک آدرس دهی خصوصی موسوم به APIPA برگرفته از Automatic Private IP Addressing ، دارای خصایص مشابهی در خصوص پیکربندی است ولی ماهیت آن با پیکربندی اتوماتیک stateless کاملا" متفاوت است APIPA از یک محدوده خاص فضای آدرس دهی) IPاز محدوده IP:169.254.0.1 تا (IP:169.254.255.254 در مواردی که یک سرویس دهنده DHCP در شبکه موجود نباشد و یا سرویس گیرنده قادر به برقراری ارتباط با آن نباشد، استفاده می نماید.

پروتکل ARP برگرفته از Address ResolutionProtocol به منظور بررسی منحصربفرد بودن آدرس IP بر روی یک شبکه محلی (LAN) استفاده می گردد. زمانی که یک سرویس دهنده DHCP در دسترس قرار بگیرد، آدرس های IP سرویس گیرندگان به صورت اتوماتیک بهنگام خواهند شد .

Extension header با این که هدر IP v.6 در مقام مقایسه با IP v.4 بسیار ساده تر شده است، ولی امکان ارائه قابلیت های پیشرفته در سطح هدر و بسته اطلاعاتی IP پیش بینی شده است. با اضافه کردن هدر به هدر پایه IP v.6 قابلیت های چشمگیری به آن اضافه شده است. بدین ترتیب، هدر پایه ثابت خواهد ماند و در صورت ضرورت می توان قابلیت های جدید را از طریق extension header به آن اضافه نمود.

امنیت اجباری IPV6

با این که در IP v.4 امکان استفاده از IPsec برگرفته از(Internet Protocol security) وجود دارد ، ولی توجه داشته باشید که ویژگی فوق به عنوان یک قابلیت جدید به پروتکل فوق اضافه می گردد تا از آن در مواردی نظیر tunneling ، رمزنگاری شبکه به منظور دستیابی راه دور VPNs برگرفته از (Virtual Private Networks) و ارتباط با سایت ها استفاده گردد . تعداد زیادی از سازمان ها از پروتکل IPsec در

موارد خاصی استفاده می نمایند ولی وجود موانعی نظیر NAT ، می تواند زمینه بکارگیری آن را با مشکل مواجه نماید

در IP v.6 ، پروتکل IPSec به عنوان بخشی الزامی در پیاده سازی مطرح شده است تا به کمک آن یک زیرساخت امنیتی مناسب به منظور ارائه سرویس های امنیتي نظیر تائید ، یکپارچگی و اعتمادپذیری فراهم گردد . ظرفیت عملیاتی IPsec بگونه ای است که سازمان ها به کمک آن می توانند وضعیت مدل امنیتی خود را بهبود و سیاست های امنیتی خود را توسعه دهند.

فواید IP v.6

ویژگی‌های جدید IP v.6 فواید زیادی را برای کسب و کارهای مختلف به ارمغان می‌آورد:

کاهش هزینه های مدیریت شبکه: ویژگی‌های auto-configurationو آدرس‌دهی سلسله مراتبی مدیریت شبکه IP v.6را آسان می‌کند.بهینه سازی برای شبکه‌های نسل آینده (NGN): رها شدن از NAT مدل Peer-To-Peer را مجدداً فعال می‌کند و به پیاده سازی application ها، ارتباطات و راه‌حل‌های متحرک جدید مثل VOIP کمک می‌کند.

محافظت از دارایی‌های شرکت: IPSec مجتمع، IP v.6 را ذاتاً امن می‌کند و امکان داشتن یک استراتژی متحد برای کل شبکه را فراهم می‌کند.

محافظت از سرمایه‌گذاری: امکان گذر و انتقال آسان و برنامه‌ریزی شده از IP V.4 به IP V.6 . امکان حضور هر دو پروتکل در فاز انتقال وجود دارد.

انواع آدرس های IPV6

آدرسهای IP V.6را می توان به سه گروه تقسیم کرد:

- آدرسهای یونی کاست (UNICAST)
- آدرسهای مولتی کاست
- آدرسهای Anycast

یک آدرس یونی کاست یک رابط واحد را تعریف می کند. این آدرس یک رابط واحد شبکه را معرفی میکند. هر بسته که به یک آدرس یونی کاست ارسال می شود به همان کامپیوتر مشخص شده تحویل داده می شود.

از درسهای مولتی کاست برای مشخص کردن مجموعه ای از رابط ها که به گره های مختلف بجای یک گره تعلق دارند ،استفاده می شود. زمانی که یک بسته به آدرسهای مولتی کاست ارسال می شود ، پروتکل بسته را به تمامی رابط های مشخص شده بوسیله آن آدرس تحویل می دهد. آدرسهای مولتی کاست دارای پیشوند FF00::/8 هستند، و هشت تایی دوم چارچوب آدرس ، مثلاً محدوده ایی که آدرس مولتی کاست در آن گسترش می یابد، را مشخص میکند.چاچوبهای متداولی که مورد استفاده قرار می گیرد عبارتند از :

لینک – محلی (2) ، سایت – محلی (5) و جهانی (E).

آدرسهای Anycast ، نیز برای تخصیص به بیش از یک رابط که به گره های مختلف تعلق دارند در نظر گرفته شده اند. با این وجود ، یک بسته که به آدرس Anycast ارسال شده فقط به یک عضو رابطها تحویل داده می شود که عموماً بر اساس نظر پروتکل مسیر یابی ، از نظر فاصله نزدیکترین عضو است. آدرسهای Anycast را به سانی نمی توان شناسایی کرد. آنها ساختاری همانند آدرسهای یونی کاست معمولی هستند و فقط از نظر پروتکل مسیر یابی در نقاط چند گانه در شبکه با هم متفاوت هستند.

آدرسهای خاص :

در IP V.6 تعدادی آدرس با معانی خاص وجود دارد:

· ::/128 – آدرسی که در آن تمامی صفرها یک آدرس نا مشخص می باشد و فقط برای نرم افزار مورد استفاده قرار می گیرد.

· ::/128 – آدرس لوپ بک که یک آدرس هاست محلی است. اگر یک کاربرد در یک هاست بسته هایی را به این آدرس ارسال کند، IP V.6 این بسته هارا به همان هاست بر می گرداند. (همانند 127.0.0.1 در IP V.4).

· ::/96 – که در IP V.4 با پیشوند صفر مورد استفاده قرار میگیرد – آدرسهای سازگار.که در حال حاضر مورد توجه قرار نمی گیرند.

· ffff:0:0/96:: – از این پیشوند برای آدرسهای طراحی شده در IP V.4 استفاده شده است. (مکانیسمهای انتقال در زیر را ببینید)

· db8::/32:2001 – از این پیشوند برای مستندسازی استفاده میشود. (RFC 3849). هر جایی که بعنوان مثال آدرس IP V.6 داده شده باشد باید از این پیشوند استفاده نمود.

· fc00::/7 – آدرسهای منحصر به فرد محلی (ULA) فقط از طریق سایتهای مشارکتی قابل مسیریابی هستند. آنها در RFC4293 بعنوان جایگزینی برای آدرسهای سایت-محلی تعریف شده آدرسها شامل یک عدد شبه تصادفی 40 بیتی است که ریسک ناسازگاری را در صورت ترکیب سایتها یا رسوخ بسته ها به بیرون کاهش میدهد. این فضای آدرسی شامل دو بخش است:

الف) ULA – fc00::/8 مرکزی که در حال حاضر از آن استفاده نمیشود.

ب) fd00::/8 - تولید و ثبت غیر رسمی ULA بر اساس RFC4193

· fe80::/64 – پیشوند لینک-محلی که فقط آدرسهایی که در لینک فیزیکی محلی معتبر است را مشخص می

کند. این پیشوند با پیکربندی خودکار آدرس IP در IPv4 ،x.x .169.254 قابل قیاس است.

· fec0::/10 – پیشوند سایت – محلی که آدرسهایی که فقط درون سازمان محلی معتبر است را مشخص میکند. کاربرد آن در سپتامبر 2004 بوسیله RFC 3879 مورد توجه قرار نگرفت و سیستمها این نوع خاص از آدرسها را پشتیبانی نکردند.

· ff00::/8 – پیشوند مولتی کاست که برای آدرسهای مولتی کاست همانگونه که بوسیله "ساختار آدرس دهی پروتکل اینترنت نسخه 6 " تعریف شده است، مورد استفاده قرار می گیرد. (RFC 4291)

در IP V.6 هیچ محدوده آدرسی رزرو وجود ندارد و در عوض از کاربردهای مولتی کاست برای مجموعه تمامی هاستها استفاده میشود. IANA فهرست رسمی از فضای آدرسی IP V.6 را نگهداری میکند. واگذاری جهانی یونی کاست را می توان در انواع RIRها یا در صفحات GRHDFP می توان پیدا نمود.

آدرس دهی

طول 128 بیت

اولین تغییر ازIP V.4 به IP V.6 ، طول آدرس شبکه است. همانگونه که توسط RFC4291 تعریف شده است ،

طول آدرس در IP V.6، 128 بیت است در حالي كه آدرسهای IP V.4، 32 بیت است.بنابراین فضای آدرسی IP V.4 به سختی شامل 4 بیلیون آدرس است ،ولی در مورد IP V.6 این فضای آدرسی برای آدرس دهی به 3/4×1038 کفایت می کند.

آدرسهای IP V.6 عموماً شامل دو بخش منطقی است :

یک پیشوند 64 بیتی شبکه یا پیش شبکه و یک بخش 64 بیتی هاست که یا بصورت خودکار از آدرس MAC رابط و یا بصورت متوالی تخصیص داده می شود. با توجه به آدرسهای منحصر بفردی که MAC در سطح جهانی دارد و از این طریق وسیله کاربر و خود کاربردر حین تغییر آدرسهای IP V.6 و زمان دسترسی، قابل جستجو هستند ، RFC3041 برای کاهش جستجوی کاربر توسط یک آدرس IP V.6 توسعه پیدا کرد،بنابراین ترمیم برخی از بی نامي هاي احتمالی در IP V.4 فعلی وجود دارد. RFC3041 مکانیسمی برای سری اتفاقی متغیر با زمان معرفی میکند که بعنوان مشخص کننده مدار رابط ، جابجایی بدون تغییر و آدرسهای MAC قابل جستجو مورد استفاده قرار می گیرد .

نکته :

آدرسهای IP V.6 معمولاً به صورت گروههای هشت تایی برای اعداد چهار رقمی در مبنای شانزده نوشته می شود. برای مثال آدرس

db8:85a3:08d3:1319:8a2e:0370:73342001:0 یک آدرس معتبر در IP V.6 می باشد.

اگر یک گروه چهار رقمی به صورت 0000 باشد ، صفرها می توانند حذف شده و به جای آنها از دو دونقطه (::) استفاده کرد. برای مثال آدرس db8:0000:0000:0000:0000:1428:57ab2001:0 را می توان به صورت خلاصه شده db8::1428:57ab2001:0 نوشت. بر اساس این قاعده هر عدد از 0000های متوالی را می توان با استفاده از دو دونقطه جایگزین کرد تا جالی که در هر آدرس فقط از یک دو کولون (دو نقطه) در آدرس استفاده می شود. صفرهای ابتدایی در یک گروه را می توان نادیده گرفت . بنابراین ،تمامی آدرسهای زیر با هم مشابه و معتبر هستند:

db8:0000:0000:0000:0000:1428:57ab2001:0

db8:0000:0000:0000::1428:57ab2001:0

db8:0:0:0:0:1428:57ab2001:0

db8:0:0::1428:57ab2001:0

db8::1428:57ab2001:0

db8::1428:57ab:2001

داشتن بیش از دو دونقطه در یک آدرس غیر مجاز است زیرا باعث مبهم شدن آن می شود.

یک زنجیره 4 بیتی در انتهای یک آدرس IP V.6 نیز می تواند به صورت دسیمال نوشته شود ،که با استفاده از نقطه از هم جدا شده اند .از این نکته نیز اغلب برای سازگاریهای آدرسی استفاده می کنند(مطالب زیر را ببینید). بنابراین ffff:1.2.3.4:: معادل آدرس ffff:0102:0304:: است و ffff:15.16.18.31:: نیز مشابه آدرس ffff:0f10:121f:: می باشد.

اطلاعات بیشتر را در این رابطه می توانید در RFC4291 – ساختار آدرس دهی اینترنت پروتکل نسخه 6 – پیدا کنید.

آدرسهای واقعی IP V.6 در URLها :

در یک URL ،آدرسهای IP V.6 درون کروشه قرار می گیرد. برای مثال:

http://[2001:0db8:85a3:08d3:1319:8a2e:0370:7344] /

این نکته این اجازه را می دهد تا یک URL را بدون قاطی کردن آدرسهای IP V.6 و شماره پورت ،تجزیه کرد.

http://[2001:0db8:85a3:08d3:1319:8a2e:0370:7344]:443/

اطلاعات بیشتر را در این رابطه می توانید در RFC2731 – فرمت آدرسهای واقعی IP V.6 در URLها – و RFC3986- شناسایی منابع همشکل (URI) : نوع ترکیب- پیدا کنید.

مشخص کردن شبکه :

شبکه های IP V.6 با استفاده از نکات CIDR نوشته می شود.

هر شبکه IP V.6 (یا زیر شبکه) مجموعه ای از آدرسهای IP V.6 است،بیتهای ابتدایی آدرسها ، که برای شناسایی تمامی هاستها در شبکه مورد استفاده قرار می گیرند ،پیشوند شبکه نامیده می شوند.

یک شبکه با اولین آدرس در شبکه و اندازه بیتهای پیشوند (در مبنای دو) که بوسیله ممیز از هم جدا شده اند ، مشخص می شود.

برای مثال : db8:1234::/482001:0 نشان دهنده شبکه ای با آدرس های از db8:1234:0000:0000:0000:0000:00002001:0 تا db8:1234:FFFF:FFFF:FFFF:FFFF:FFFF2001:0 می باشد.

با توجه به اینکه یک هاست می تواند به صورت یک شبکه با پیشوند 128 بیتی مشاهده شود ، برخی اوقات شما می توانید آدرسهای هاستی را ببینید که به صورت 128 بیتی نوشته شده اند.

انواع آدرسهای IP V.6 :

آدرسهای IP V.6را می توان به سه گروه تقسیم کرد:

- آدرسهای یونی کاست (UNICAST)
- آدرسهای مولتی کاست
- آدرسهای Anycast

یک آدرس یونی کاست یک رابط واحد را تعریف می کند. این آدرس یک رابط واحد شبکه را معرفی میکند. هر بسته که به یک آدرس یونی کاست ارسال می شود به همان کامپیوتر مشخص شده تحویل داده می شود.

از درسهای مولتی کاست برای مشخص کردن مجموعه ای از رابط ها که به گره های مختلف بجای یک گره تعلق دارند ،استفاده می شود. زمانی که یک بسته به آدرسهای مولتی کاست ارسال می شود ، پروتکل بسته را به تمامی رابط های مشخص شده بوسیله آن آدرس تحویل می دهد. آدرسهای مولتی کاست دارای پیشوند FF00::/8 هستند، و هشت تایی دوم چارچوب آدرس ، مثلاً محدوده ایی که آدرس مولتی کاست در آن گسترش می یابد، را مشخص میکند.چاچوبهای متداولی که مورد استفاده قرار می گیرد عبارتند از :

لینک – محلی (2) ، سایت – محلی (5) و جهانی (E).

آدرسهای Anycast ، نیز برای تخصیص به بیش از یک رابط که به گره های مختلف تعلق دارند در نظر گرفته شده اند. با این وجود ، یک بسته که به آدرس Anycast ارسال شده فقط به یک عضو رابطها تحویل داده می شود که عموماً بر اساس نظر پروتکل مسیر یابی ، از نظر فاصله نزدیکترین عضو است. آدرسهای Anycast را به سانی نمی توان شناسایی کرد. آنها ساختاری همانند آدرسهای یونی کاست معمولی هستند و

فقط از نظر پروتکل مسیر یابی در نقاط چند گانه در شبکه با هم متفاوت هستند.

آدرسهای خاص :

در IP V.6 تعدادی آدرس با معانی خاص وجود دارد:

· ::/128 – آدرسی که در آن تمامی صفرها یک آدرس نا مشخص می باشد و فقط برای نرم افزار مورد استفاده قرار می گیرد.

· ::/128 – آدرس لوپ بک که یک آدرس هاست محلی است. اگر یک کاربرد در یک هاست بسته هایی را به این آدرس ارسال کند، IP V.6 این بسته هارا به همان هاست بر می گرداند. (همانند 127.0.0.1 در IP V.4).

· ::/96 – که در IP V.4 با پیشوند صفر مورد استفاده قرار میگیرد – آدرسهای سازگار.که در حال حاضر مورد توجه قرار نمی گیرند.

· ::ffff:0:0/96 – از این پیشوند برای آدرسهای طراحی شده در IP V.4 استفاده شده است. (مکانیسمهای انتقال در زیر را ببینید)

· db8::/32:2001 – از این پیشوند برای مستندسازی استفاده میشود. (RFC 3849). هر جایی که بعنوان مثال آدرس IP V.6 داده شده باشد باید از این پیشوند استفاده نمود.

· fc00::/7 – آدرسهای منحصر به فرد محلی (ULA) فقط از طریق سایتهای مشارکتی قابل مسیریابی هستند. آنها در RFC4293 بعنوان جایگزینی برای آدرسهای سایت-محلی تعریف شده آدرسها شامل یک عدد شبه تصادفی 40 بیتی است که ریسک ناسازگاری را در صورت ترکیب سایتها یا رسوخ بسته ها به بیرون کاهش میدهد. این فضای آدرسی شامل دو بخش است:

الف) ULA – fc00::/8 مرکزی که در حال حاضر از آن استفاده نمیشود.

ب) fd00::/8 - تولید و ثبت غیر رسمی ULA بر اساس RFC4193

· fe80::/64 – پیشوند لینک-محلی که فقط آدرسهایی که در لینک فیزیکی محلی معتبر است را مشخص می کند. این پیشوند با پیکربندی خودکار آدرس IP در IPv4 ،x.x .169.254 قابل قیاس است.

· fec0::/10 – پیشوند سایت – محلی که آدرسهایی که فقط درون سازمان محلی معتبر است را مشخص میکند. کاربرد آن در سپتامبر 2004 بوسیله RFC 3879 مورد توجه قرار نگرفت و سیستمها این نوع خاص از آدرسها را پشتیبانی نکردند.

· ff00::/8 – پیشوند مولتی کاست که برای آدرسهای مولتی کاست همانگونه که بوسیله "ساختار آدرس دهی

پروتکل اینترنت نسخه 6 " تعریف شده است، مورد استفاده قرار می گیرد. (RFC 4291)

در IP V.6 هیچ محدوده آدرسی رزرو وجود ندارد و در عوض از کاربردهای مولتی کاست برای مجموعه تمامی هاستها استفاده میشود. IANA فهرست رسمی از فضای آدرسی IP V.6 را نگهداری میکند. واگذاری جهانی یونی کاست را می توان در انواع RIRها یا در صفحات GRHDFP می توان پیدا نمود.

سرآیند های بسته IPV6

IPv6 بسیاري از ویژگي‌هاي اصلي پروتکل IP .v4 را داراميباشد، اینترنت موفقیت‌هاي لازم را کسب نخواهد کرد مگر اینکه بسیاري از عیب‌ها و نقایص مهم و قابل توجه موجود در طراحي IP v.4 را کنار بگذاریم. بنابراین سرآیندهاي IP v.6 داراي شباهت‌هاي زیادي در مقایسه با هدرهاي IP v.4 ميباشد. هدرهاي IP v.6 ترکیبي از 64 بیت هستندکه بوسیله دو فیلد 128 بیتي یعني آدرس مبداء و آدرس مقصد احاطه شده اند. دیگر فیلدهاي سرآیند یك بسته IP v.6 از قرار زیر ميباشد:

1. Version

2. Class

3. Flow label

4. Length of payload

5. Type

6. Hop limit

برخلاف سرآيندهاي IP v.4 كه شكل و قالب ثابت دارند. سرآيندهاي IP v.6 داراي شكل ثابت نبوده و از انعطاف‌پذيري بيشتري برخوردار است. اين كار باعث مي‌شود سرآيندهايي كه در IP v.4 استفاده مي‌شدند ساده‌تر گردد زيرا IP v.4 يك شكل و قالب ثابت به همه هدرها اختصاص مي‌دهد و تصحيح كننده‌هاي سرآيند را جابجا مي‌كند و اين پروسه و عمل را در همه جهشها تكرار مي‌كند.مهمترين قسمت اين تغييرات، جابجايي و برداشتن پروسه تقسيم‌بندي جهش به جهش مي‌باشد، قبلاً ممكن بود يك ميزبان اطلاعات خود را از طريق چند محيط و مسير به سمت مقصد بفرستد زيرا اين احتمال وجود داشت كه بسته‌اي كه ارسال شده به اندازه‌اي بزرگ باشد كه بعضي از شبكه‌ها نمي‌توانند آن را انتقال دهند. به عنوان مثال ارسال يك بسته از محيط شبكه با توپولوژي حلقه نشانه كه ماكزيمم اندازه بسته آن 4 كيلو بايت است به يك شبكه با استاندارد اترنت كه حداكثر اندازه بسته آن 1.5 كيلو بايت مي‌باشد در نظر بگيريد، در اين حالت مسيريابي كه دو نوع محيط را به همديگر متصل مي‌كند

بسته اصلي را تقسيم خواهد كرد. اين اتفاق در IP v.6 نخواهد افتاد زيرا IP v.6 از پروسه‌اي كه "تشخيص دهنده MTU مسير" گفته مي‌شود استفاده مي‌كند و بنابراين مطمئن است كه هيچ تقسيم بندي لازم نيست.با وجود اينكه IP v.6 داراي سرآيندهاي بسيار ساده‌اي است و لي با اين وجود مفهوم سرآيندهاي توسعه را نيز پشتيباني مي‌كند. زماني كه سرآيندهاي توسعه مورد استفاده قرار مي‌گيرند بخش انتهايي هر سرآيند آدرس سرآيند بعدي را مشخص مي‌كند مگر در حالتي كه نوبت سرآيند آخري، يعني ناحيه داده، باشد. اين مفهوم در شكل زير نشان داده شده است.

Payload

IPv6 headerNext header= payload

Payload

Routing headerNext header= payload

IPv6 header Next header= Routing

Payload

Encryption headerNext header= payload

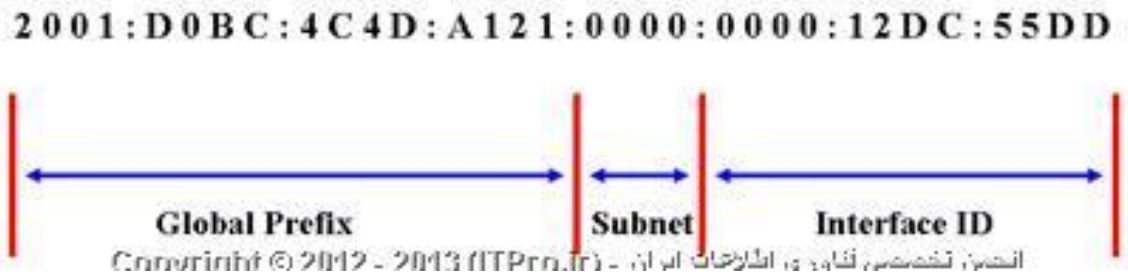
Routing headerNext header=Encryption

IPv6 headerNext header= Routing

سرآیندهای توسعه ای که قابل دسترسی هستند عبارتند از:

1. Routing header
2. Fragment heade
3. Authentication header
4. Encrypted security payload
5. Destination option header

128بیت IPv6 از دو 64 بیت تشکیل شده است.مثالی از ساختار یک آدرس: IPV6



64بیت مربوط به **Interface ID** و کارت شبکه دستگاه است. از این شناسه برای مشخص کردن آدرس منحصربفرد هر اینترفیس شبکه استفاده می شود.64 بیت بعدی به صورت زیر است:

- **FP (Former Perfix)**: به 3 بیت اول آدرس **FP**می گویند.نوع آدرس را مشخص می کند. آدرس global است یا private ، به عنوان مثال **FP**در آدرسهای **Global Unicast**معادل **001** است.

- **TLA_ID (Top Level Aggregator Identifier)**: به 13 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 ISP ها 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 IPv4 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 IPv6 ، تعیین مبدا یک مسیر، بسیار عملی تر و امکانپذیرتر شده است.

فرض کنید که اینترنت شامل 500 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 باشدTLA .).ها در اصل به NAP اشاره می کند .

NAP (Network Access Point) :در سطح دنیای اینترنت 12 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.12تا Backbone اصلی در دنیای اینترنت وجود دارد که اکثرا هم در آمریکا هستند.مثل AT&T یک NAP است.در ساختار اینترنتی بایستی مشخص شود که به کدام یک ازNAP ها متصل می شویم . این قسمت (TLA)توسط سازمان بین المللی تخصیص آدرسهای اینترنتی IANA اختصاص داده می شود .

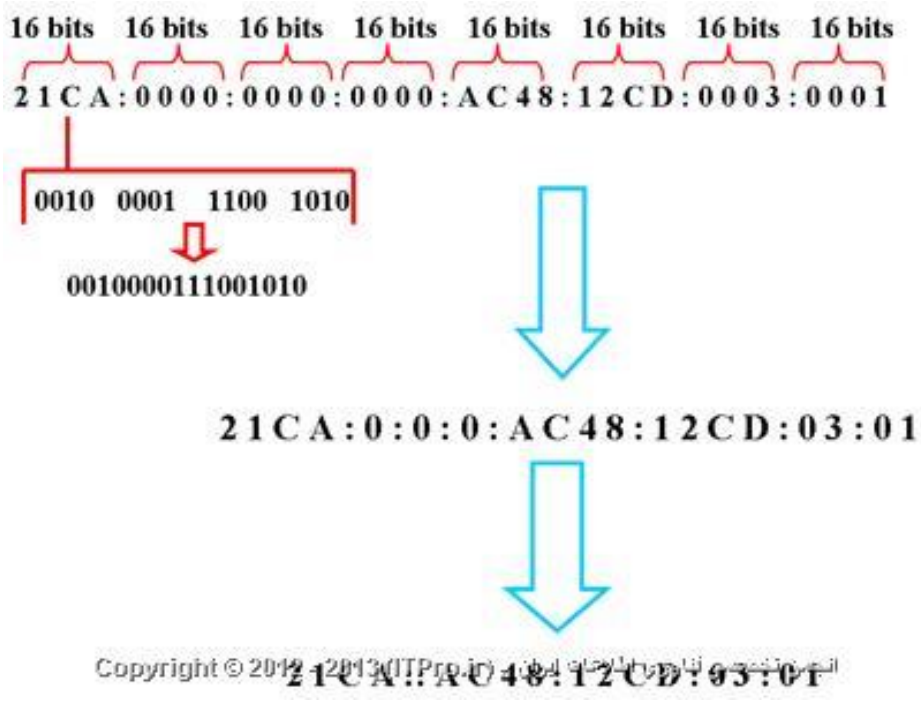
پس اول بایستی معلوم شود که آدرس ما چیست ؟ Global است یا Private ، بعد با فرض اینکه Global باشد حالا باید مشخص شود که این آدرس Global به کدام NAP اینترنتی ختم می شود.تا اینجا از 64 بیت،3 بیت FP و 13 بیت TLA مشخص شد.همانند پروتکلIPv4 ، در پروتکل IPv6 نیز گروهی از آدرسها برای مقاصد خاص

رزرو شده اند. پروتکل IP نسخه 6، 8 بیت رزرو شده دارد که اگر به اینNAP ها در آینده اضافه شود و آدرس های NAP کم بیاد می تواند از این رزروها استفاده کند.مثل 0::0::0::0::0::0::0::0 که معادل "::" بوده و شبیه به آدرس 0.0.0.0 در IPv4 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 24 بیت بعدی **NLA**می گویند. شناسه 24 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 ASمربوطه اشاره می کند.مثلا شماره AS مخابرات ایران NLA.ما می شود یعنی NLA مخابرات ایران.

- **SLA_ ID (Site Level Aggregator Identifier :** به 16 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 IPv6 می توان قسمتهایی از آن را که تماما صفر است، فقط با یک صفر نمایش داد و یا تمام صفرها را به همراه کولن بعد از آن حذف کرد.

فشرده سازیIPv6



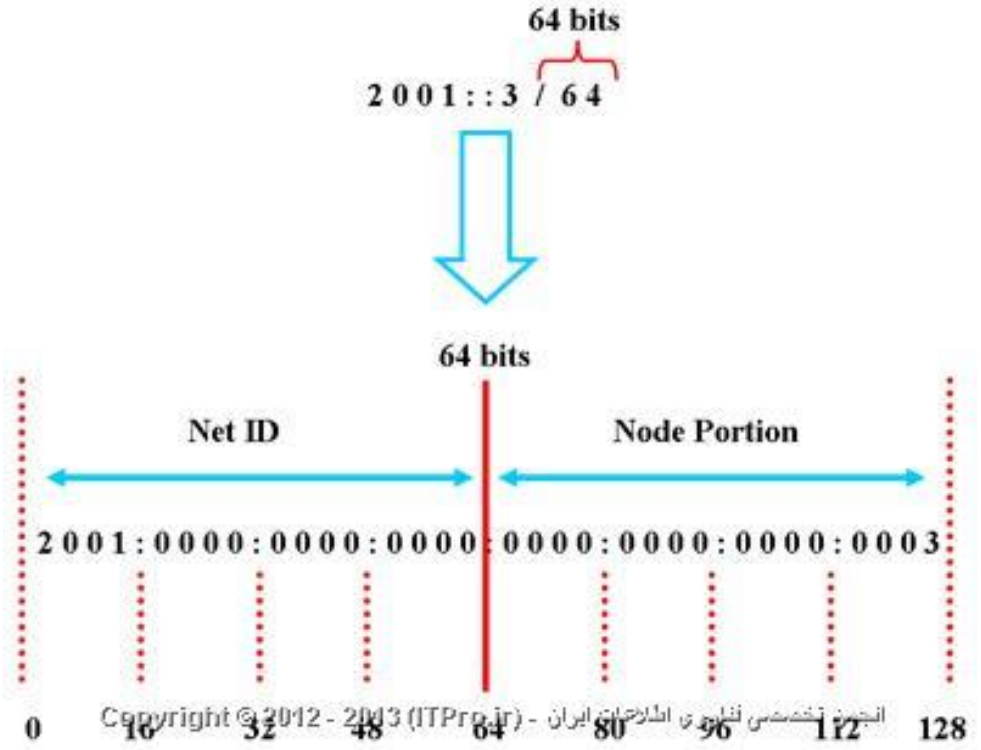
چند نکته :

- IPv6نمی تواند با "::" شروع شود.
- در هر قسمت 16 بیتی می توان حداکثر از عدد **DDDD**و حداقل از **0000**استفاده کرد.
- در **IPv6**چیزی به نام **Subnet Mask**وجود ندارد اما به جای آن **Perfix)پیشوند** (وجود دارد.

به طور مثال IP آدرس 3::2001 با پیشوند 64 بیت به

صورت 2001::3/64 نوشته می شود، مفهوم این است که 64 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، 64 بیت در نظر گرفته می شود.



انـواع آدرس دهی در IPv6

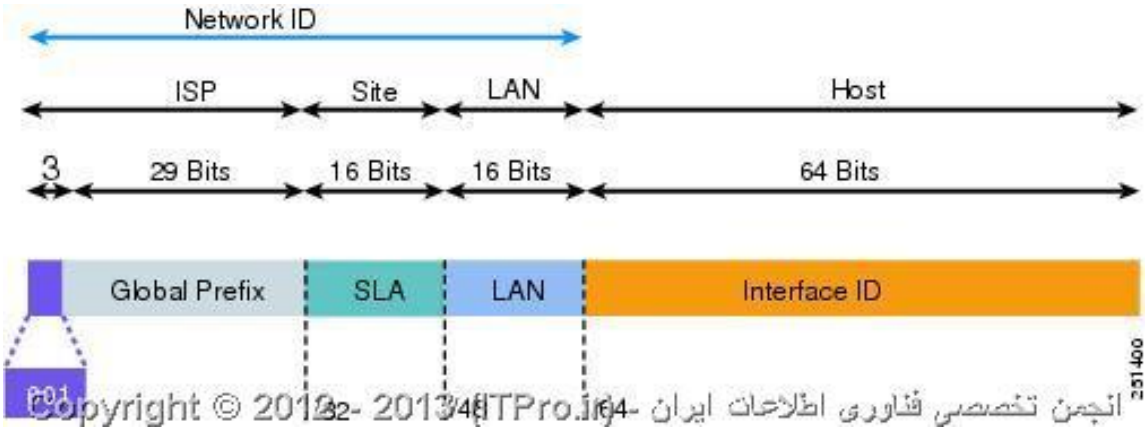
1. **Unicast**
2. **Multicast**
3. **Anycast**

چند نوع مختلف آدرس دهیUnicast

1. **Global Unicast**
2. **Link-Local Unicast**
3. **Unique-Local Unicast**

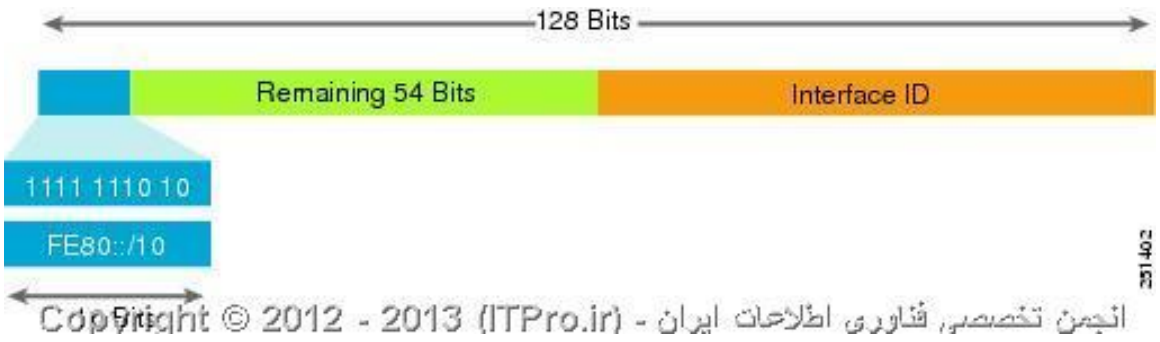
- **Global Unicast** : بـه مفـهوم آدرسهـای unicast قـابـل انـتقـال در اینـترنـت بـوده (قـابـلیت آدرس دهی در

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:

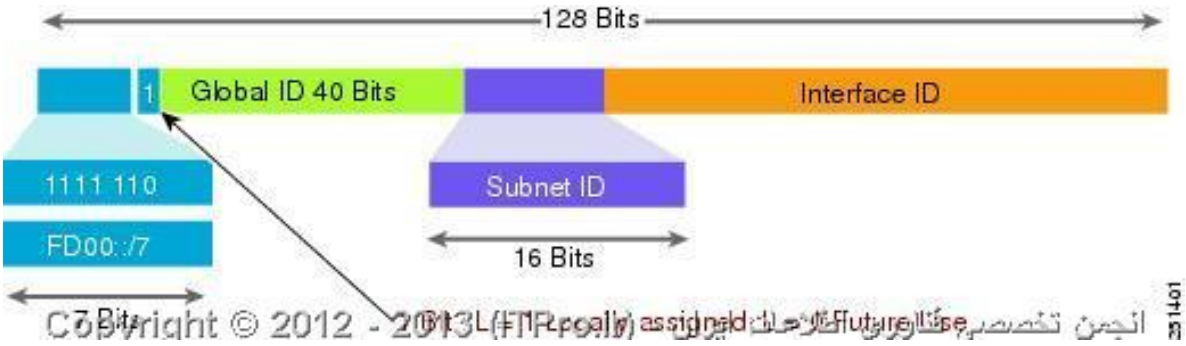


- **Link-Local Unicast** : شبیه به آدرسهای Private یا خصوصی در IPv4 بوده و قابل انتقال در اینترنت نیستند. این آدرسها را می توان به اعضای یک شبکه LAN و یا چند LAN مختلف که قصد برقراری ارتباط با یکدیگر دارند را تخصیص داد. این آدرسها که در غیاب DHCP Server ایجاد می شوند، در IPv6 معادل Fe80::/64 هستند. به بیانی دیگر اگر در هنگام تنظیم IP آدرس ، در کادر محاوره ای **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 16 بیت ثابت (feco) شروع می شوند و به دنبال آن 32 بیت صفر و سپس 16 بیت مربوط به Subnet ID است که معمولا آن را هم صفر در نظر می گیرند. 64 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 Anycastو اختصاص دادن آن به یک routerباید ابتدا بخش NET ID مربوط به IPv6 Addressشبکه 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 2001:4188:1:1::/64 آدرس Anycast برابر با 2001:1:1:0:0:0:0:0یا در حالت فشرده 2001:4188:1:1:: خواهد بود.حال اگر بسته ای به آدرس Anycast ارسال شود ، به دست نزدیکترین آدرسAnycastی که روی روتر تنظیم شده است می رسد.این عمل با استفاده از ساختارهای مسیریابی آدرسهای Anycastو Routing Metric های مسیریابی اتفاق می افتد و زمانیکه یک packetبا 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.

نتیجه گیری :

به آدرس IP نسخه 6 آدرس IP نسل آینده یا Next Generation IP Address نیز گفته می شود . اگرچه تاکنون تقریبا ده سال است که بر روی ویژگی ها و استانداردهای پروتکل IPv6 کار شده، اما اخیرا 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 IPv4 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 IPV4 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 340,282,366,920,938,000,000,000,000,000,000,000 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

یک بخش کلیدی (Internet Control Message Protocol ,version 6) 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 IPv4)

DHCPv6 نسخه جدید DHCP برای IPv6 می باشد.کاملا از نو طراحی شده است فقط از لحاظ مفهومی شبیه به DHCP است.DHCPv6 شامل عملکرد جدید مثل Authentication است.

پروتکلهای مسیریابی برای IPv6 شامل RIPng، OSPFv3