تسلط بر مفاهیم پایه شبکه منطبق با استانداردهای بین‌المللی

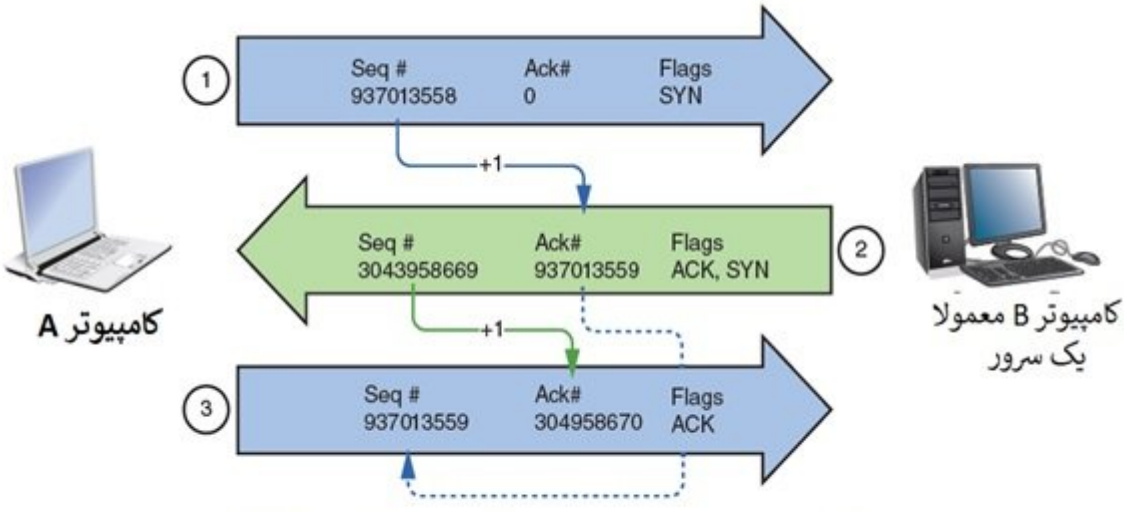
آموزش رایگان دوره نتورک‌پلاس (Network+) بررسی دست دادن سه مرحله‌ای در TCP، واکاوی یک سگمنت UDP (بخش 26)

در مقاله گذشته آموزش نتورک‌پلاس به سراغ پروتکل TCP/IP رفته و فیلدهای درون یک سگمنت TCP را بررسی کردیم. اکنون قصد داریم فیلدهای درون بسته آی‌پی و نحوه ارسال و دریافت یک سگمنت TCP را بررسی کنیم.

برای مطالعه بخش بیست و پنجم آموزش رایگان و جامع نتورک پلاس (Network+) اینجا کلیک کنید

دست دادن سه مرحله‌ای در TCP

دست دادن سه مرحله‌ای به معنای شروع نشست/جلسه‌ای است که پیش از آن‌که TCP داده‌های واقعی را انتقال دهد ایجاد می‌شود. برای درک بهتر این موضوع به زمانی که فرد جدیدی را ملاقات می‌کنید فکر کنید. شما ابتدا دست خود را جلو می‌برید، اما مطمئن نیستید که فرد مقابل به شما پاسخ خواهد داد. اگر شخص مقابل دست خود را جلو بیاورد، شما دو نفر با یکدیگر دست داده و گفت‌وگو را آغاز می‌کنید. شکل زیر انتقال سه مرحله‌ای در یک فرآیند دست‌دهی TCP را نشان می‌دهد.



فرآیند دست دهی سه مرحله ای در یک نشست TCP

جزییات مراحل نشان داده شده در تصویر بالا به شرح زیر است:

مرحله 1، SYN (درخواست برای یک ارتباط) کامپیوتر A پیامی برای کامپیوتر B همراه با اطلاعات زیر ارسال می‌کند.

- در فیلد Sequence number، کامپیوتر A یک عدد تصادفی برای همگام‌سازی ارتباط انتخاب و ارسال می‌کند. در شکل بالا این عدد 937013558 است.
- بیت SYN به 1 تظیم شده است که نشان می‌دهد فلگ SYN فعال شده است. فعال بودن این فلگ نشان می‌دهد که هر دو طرف آماده هستند یک ارتباط را برقرار کنند. کامپیوتر A دست خود را به نشانی برقراری ارتباط برای کامپیوتر B دراز می‌کند تا ببیند آیا پاسخی دریافت می‌کند یا خیر.
- بیت ACK در حالت کلی در اولین انتقال به 0 تنظیم می‌شود، زیرا هنوز هیچ اطلاعاتی از کامپیوتر B برای تایید وجود ندارد.

مرحله 2: SYN/ACK (پاسخ به یک درخواست)- زمانی که کامپیوتر B این پیام را دریافت می‌کند با سگمنتی که حاوی اطلاعات زیر است پاسخ می‌دهد:

- بیت‌های ACK و SYN هر دو به 1 تنظیم می‌شوند. این‌کار به زبان ما می‌شود: "بله، من این‌جا حضور دارم و در حال گوش دادن هستم."
- فیلد Acknowledgment number حاوی عددی است برابر با یک شماره توالی که کامپیوتر A قبلا ارسال کرده است. (به‌علاوه 1). آن‌چنان‌که در شکل بالا نشان داده شده است، کامپیوتر B مقدار 937013559 را ارسال کرده است. به این ترتیب، کامپیوتر B سیگنالی برای کامپیوتر A ارسال می‌کند که به معنای درخواست برقراری ارتباط است. اکنون کامپیوتر B انتظار دارد تا کامپیوتر A دومرتبه با شماره ترتیبی 937013559 به او پاسخ دهد.
- در فیلد Sequence number، کامپیوتر B شماره تصادفی خود را ارسال می‌کند. در تصویر بالا این شماره برابر با 3043959669 است.

مرحله 3: ACK (اتصال برقرار شد)- کامپیوتر A سگمنتی که حایل اطلاعات زیر است را منتشر می‌کند.

- Sequence number برابر با 937013559 است، زیرا این شماره‌ای است که کامپیوتر B انتظار دارد آن‌را دریافت کند.
- فیلد Acknowledgment number برابر با شماره توالی کامپیوتر B به‌علاوه 1 است. در این مثال این شماره برابر با 3043959670 است.
- بیت ACK به 1 تنظیم شده است. این ارتباط در حال حاضر برقرار شده و در پیام بعدی، کامپیوتر A شروع به ارسال داده‌ها خواهد کرد.

تا این نقطه، هیچ بارداده‌ای در هیچ‌یک از پیام‌های سه مرحله‌ای ضمیمه نشده و تعداد توالی‌ها در هر مرحله 1 واحد افزایش پیدا کرده‌اند. پس از این سه مرحله انتقال، بارداده یا داده‌ها ارسال می‌شود. این‌کار می‌تواند در قالب یک پیام واحد برای حجم کوچکی از داده‌ها از قبیل درخواست برای یک صفحه وب، یا در قالب پیام‌های چندگانه شکسته شده از قبیل ارسال ارسال داده‌هایی که متعلق به یک صفحه وب هستند انجام شود. در این مرحله تعداد توالی‌ها با تعداد بیت‌های موجود در هر سگمنت دریافت شده افزایش پیدا می‌کنند تا مشخص شود طول پیام دریافتی به شکل صحیحی افزایش پیدا کرده است. در شکل بالا، کامپیوتر A پیام بعدی را ارسال خواهد کرد که شامل بارداده‌ای (همچون یک درخواست HTTP) از یک لایه بالاتر است. فرض کنید کامپیوتر A درخواست دسترسی به یک صفحه وب را در قالب یک پیام ارسال کند، چهارمین پیام در این نشست اندازه‌ای برابر با 725 بیت خواهد داشت. کامپیوتر B این پیام را دریافت کرده، تعداد بیت‌ها را شمارش کرده و 725 بیت به شماره توالی پیام دریافت شده یعنی 937013559 اضافه می‌کند. شماره جدید برابر با 937014284 خواهد بود که شماره تایید پیام بازگشتی خواهد بود. (که پنجمین پیام در این نشست خواهد بود.) دو میزبان ارتباط را به همین روش ادامه خواهند داد تا وقتی که کامپیوتر A سگمنتی که بیت FIN آن برابر با 1 است را ارسال کند. یک بودن این بیت نشان می‌دهد که انتقال داده‌ها به پایان رسیده است.

پروتکل بسته داده کاربر (UDP) سرنام User Datagram Protocol

پروتکل بسته داده کاربر موسوم به UDP از یک مدل انتقال ساده بدون ارتباط استفاده کرده که در آن هیچ ارتباط دست‌دهی وجود ندارد، در نتیجه پروتکل قابل اعتمادی نیست. اصطلاح غیر قابل اعتماد بودن به معنای آن نیست که پروتکل UDP بی مصرف بوده و نباید استفاده شود، بلکه منظور این است که این پروتکل هیچ‌گونه تضمینی بابت تحویل داده‌ها ارائه نکرده و پیش از آن‌که فرآیند انتقال داده‌ها آغاز شود هیچ‌گونه اتصالی برقرار نمی‌کند. همان‌گونه که گفتیم پروتکل UDP هیچ‌گونه مکانیزم دست‌دهی در زمان انتشار، تایید دریافت داده‌های منتقل شده، بررسی خطاها، توالی یا کنترل جریان نداشته و به همین دلیل سرعت و کارایی بالاتری نسبت به TCP دارد. عملکرد پروتکل UDP را به جای آن‌که شبیه به یک تماس تلفنی تشریح کنیم، باید شبیه به یک برنامه رادیویی تصور کنیم که سیگنال خود را برای هر کسی که در حال گوش دادن است ارسال می‌کند. UDP برای زمانی که حجم بالایی از داده‌ها باید به سرعت انتقال پیدا کند؛ همچون انتقال داده‌های صوتی یا ویدویی روی اینترنت مناسب است. این پروتکل همچنین برای رسیدگی به درخواست‌های کوچک همچون سامانه نام دامنه یا شرایطی که داده‌ها تغییر پیدا کرده و سرعت نقش مهمی در تکمیل یک پروسه دارد استفاده می‌شود. بازی‌های آنلاین مبتنی بر شبکه از جمله این موارد هستند.
در مقایسه با 10 فیلد سرآیند TCP، سرآیند DUP فقط شامل چهار فیلد پورت مبدا، پورت مقصد، اندازه و Checksum است. دقت کنید که فیلد Checksum این پروتکل به شکل اختیار در شبکه‌های مبتنی بر IPv4 استفاده می‌شود، اما برای تبادلات شبکه‌های مبتنی بر IPv6 ضروری است. شکل زیر دیتاگرام این پروتکل را نشان می‌دهد.

یک دیتاگرام UDP

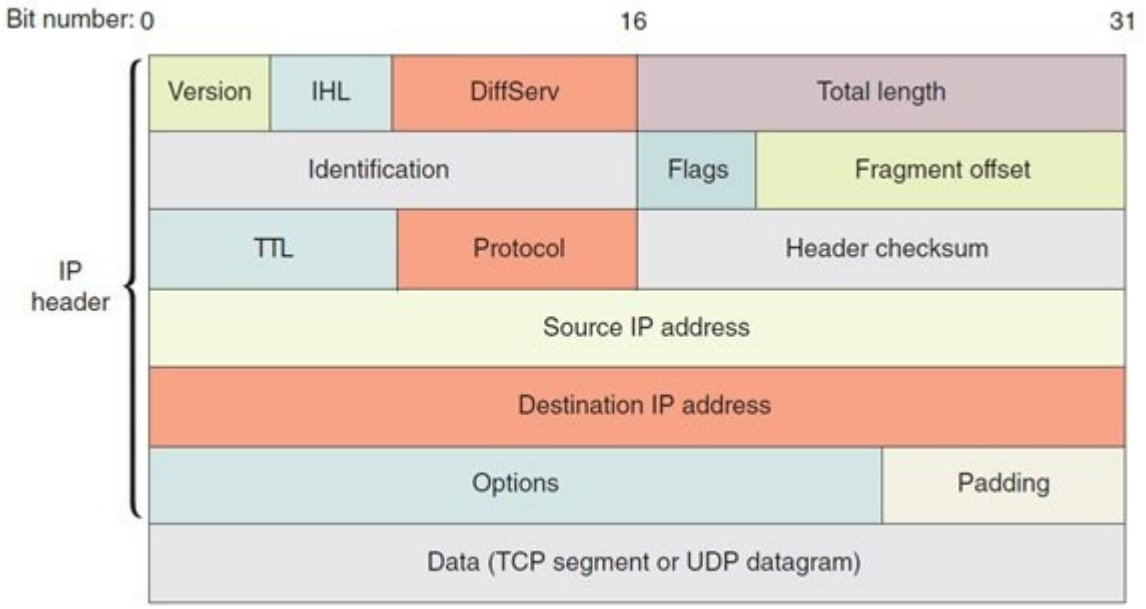
اکنون که با عملکردها و تفاوت‌های دو پروتکل UDP و TCP در لایه چهارم آشنا شدید، اجازه دهید به سراغ پروتکل IP در لایه 3 برویم.

پروتکل IP سرنام Internet Protocol

پروتکل IP به لایه شبکه در مدل OSI تعلق دارد. این پروتکل مشخص می‌کند که داده‌ها به چه مکانی باید تحویل داده شده و همچنین آدرس‌های آی‌پی مبدا و مقصد را مشخص می‌کند. IP پروتکلی است که TCP/IP را به شبکه متصل می‌کند. به عبارت دقیق‌تر به این پروتکل اجازه می‌دهد از میان شبکه‌های محلی مختلف با اتکا بر روترها عبور کند. همان‌طور که پیش‌تر گفتیم، در لایه شبکه از مدل OSI، داده‌ها درون بسته‌هایی سازمان‌دهی می‌شوند. یک بسته آی‌پی شامل اطلاعات مهمی است که روترها برای انتقال داده‌ها میان سگمنت‌های مختلف شبکه‌های محلی به آن‌ها نیاز دارند. IP یک پروتکل بدون اتصال است، به این معنی که IP نشستی برای ارسال بسته‌های خود منتشر نمی‌کند. هر بسته آی‌پی به‌طور جداگانه از سایر بسته‌هایی که درون مجموعه خودش قرار دارد ارسال می‌شود، در نتیجه برخی از پیام‌ها ممکن است از مسیرهایی متفاوت از دیگری برای رسیدن به مقصد استفاده کنند. تایید این مسئله که آیا آی‌پی پیامی را به میزبان درستی تحویل داده است یا خیر بر عهده پروتکل TCP است. IP با اتکا بر پروتکل TCP یا UDP مطمئن می‌شود که هر پیام به برنامه درستی که روی میزبانی در حال اجرا است، تحویل داده شده است. همان‌گونه که عنوان شد، دو نسخه از پروتکل IP روی شبکه‌های امروزی استفاده می‌شود. IPv4 که اولین بار در سال 1981 معرفی شد و هنوز هم به عنوان استانداردی روی بیشتر شبکه‌ها استفاده می‌شود و IPv6 که در سال 1998 معرفی شد که امنیت بهتر، تنظیمات اولویت‌بندی بهتر، تنظیمات پیکربندی خودکار بهتر و آدرس‌های آی‌پی اضافی‌تر را ارائه می‌کند. بیشتر برنامه‌ها، سرورها، کلاینت‌ها و دستگاه‌های تحت شبکه از IPv6 پشتیبانی می‌کنند. با این حال، هزینه ارتقا زیرساخت‌ها به IPv6 برای بسیاری از سازمان‌ها سنگین بوده و در نتیجه بیشتر سازمان‌ها ترجیح می‌دهند از IPv4 استفاده کنند. به عنوان یک تکنسین شبکه، شما باید اطلاعات کافی در مورد هر دو نسخه این پروتکل به دست آورید. ابتدا اجازه دهید ببینیم بسته‌های IPv4 چگونه ساخته شده و پس از آن به سراغ بسته‌های IPv6 برویم.

بسته‌های IPv4

شکل زیر یک بسته IPv4 را نشان می‌دهد.



توضیح فیلدهای درون تصویر بالا در جدول زیر آماده است. دقت کنید که فیلد داده‌ها در سطر پایین به سرآیند IPv4 تعلق ندارد.

فیلد	طول	عملکرد

سرآیند	Version	bits 4	نسخه پروتکل IP را مشخص می‌کند. به‌طور مثال IPv4 یا Ipv6. یک ایستگاه کاری به فیلد فوق نگاه کرده تا بررسی کند که آیا می‌تواند داده‌های وارد شونده را بخواند یا خیر. اگر موفق نشود بسته را برگشت می‌کند.
	IHL (Internet header (length	bits 4	اندازه سرآیند آی‌پی را در واحد بایت‌ها نشان می‌دهد. این سرآیند می‌تواند حداقل 20 بایت و حداکثر 60 بایت باشد. این فیلد همچنین Data offset نیز نامیده می‌شود، زیرا افست شروع بسته را تاوقتی که داده‌ها از سوی بسته حمل شوند را مشخص می‌کند.
	DiffServ (Differentiated (services	bits 8	برای روترها سطح اولویت‌بندی بسته‌هایی که قرار است پردازش شوند را مشخص می‌کنند.
	Total length	bits 16	طول کل بسته آی‌پی را در واحد بایت مشخص کرده و شامل سرآیند و داده است. یک بسته آی‌پی شامل سرآیند و داده بوده و اندازه آن نباید از 65353 بایت تجاوز کند.
	Identification	bits 16	برخی مواردروترها و میزبان‌های مجبور به شکستن یک دیتاگرام به بسته‌های کوچک‌تر هستند. در این حالت ماشین مقصد مجبور به بازسازی بسته‌ها است. زمانی که یک دیتاگرام واحد شکسته می‌شود، باید ویژگی وجود داشته باشد تا مقصد بتواند بسته‌های دریافتی را بازسازی کرده و آن‌ها را از میان سایر بسته‌های دیتاگرام جدا کند. این فیلد و دو فیلد بعد Flags و Fragment offset به بازسازی بسته‌هایی که جدا دریافت شده‌اند کمک می‌کنند.
	Flags	bits 3	مشخص می‌کند که آیا یک یام شکسته شده و اگر شکسته شده است، آیا بسته‌ای که دریافت شده آخرین قطعه شکسته شده است یا خیر. اولین بیت برای استفاده در آینده رزرو شده است.
	Fragment offset	bits 13	مشخص می‌کند که بسته شکسته شده به چه مکانی در یک مجموعه وارد شده تعلق دارد.
	TTL (Time to (Live	bits 8	حداکثر مدت زمانی را مشخص می‌کند که یک بسته می‌تواند روی یک شبکه پیش از آن‌که از دست برود باقی بماند. درست است که این فیلد واحدی از زمان را نشان می‌دهد، اما روی شبکه‌های مدرن این فیلد تعداد فدعاتی که یک بسته می‌تواند از طریق یک روتر فوروارد شده یا حداکثر تعداد دفعاتی که بسته از هر روتر می‌تواند عبور کند را نشان می‌دهد. مقدار TTL برای هر بسته متفاوت بوده و قابل پیکربندی است. به‌طور معمول این مقدار به 32 یا 64 تنظیم می‌شود. هر بار که بسته‌ای از یک روتر عبور می‌کند، TTL یک واحد کاهش پیدا می‌کند. زمانی که یک روتر یک بسته را با TTL عادل با 0 دریافت می‌کند، آن‌را بسته را حذف کرده و یک پیام اتمام زمان پیام TTL را از طریق پروتکل ICMP برای مبدا ارسال می‌کند.
	Protocol	bits 8	نوع پروتکلی که بسته را دریافت می‌کند را مشخص می‌کند. (به‌طور مثال TCP، UDP یا ICMP)
	Header checksum	bits 16	به میزبان دریافت کننده بسته اجازه می‌دهد تا محاسبه کند که آیا سرآیند آی‌پی در هنگام دریافت بسته خراب شده است یا خیر. اگر فرآیند تطابق و ارزیابی وضعیت بسته‌های دریافتی درست نباشد به معنای آن است که بسته از دست رفته است.
	Source IP address	bits 32	آدرس آی‌پی مبدا را مشخص می‌کند.
	Destination IP address	bits 32	آدرس آی‌پی مقصد را مشخص می‌کد.
	Options	Variable	شامل اطلاعات زمانی و مسیریابی اختیاری است.
	Padding	Variable	شامل بیت‌هایی است که اطمینان می‌دهند که سرآیند دارای بیت‌های 32 است.
	Data	Variable	شامل داده‌هایی است که اساسا از طرف مبدا ارسال شده‌اند و همچنین شامل هر سرآیندی است که از لایه‌های بالاتر دریافت شده‌اند. فیلد داده‌ای بخشی از سرآیند آی‌پی نیست و درون سرآیند آی‌پی کپسوله می‌شود.

در شماره آینده آموزش **نتورک‌پلاس** سراغ بسته‌های IPv6 خواهیم رفت.

معرفی آموزشگاه‌های معتبر دوره نتورک پلاس در سراسر کشور

استان تهران (تهران): آموزشگاه عصر شبکه
برگزار کننده دوره‌ها بصورت حضوری و مجازی هم‌زمان
تلفن: 02188735845 کانال: @Asrehshabakeh

استان گیلان (رشت): آموزشگاه هیوا شبکه
تلفن: 01333241269 کانال: @HivaShabake

تاریخ انتشار:
13 اسفند 1397

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/14738/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D9%88%D8%B1%D9%87-%D9%86%D8%AA%D9%88%D8%B1%DA%A9%E2%80%8C%D9%BE%D9%84%D8%A7%D8%B3-network-%D8%A8%D8%B1%D8%B1%D8%B3%DB%8C-%D8%AF%D8%B3%D8%AA-%D8%AF%D8%A7%D8%AF%D9%86-%D8%B3%D9%87-%D9%85%D8%B1%D8%AD%D9%84%D9%87%E2%80%8C%D8%A7%DB%8C-%D8%AF%D8%B1-tcp%D8%8C