تسلط بر مفاهیم پایه شبکه منطبق با استانداردهای بین‌المللی

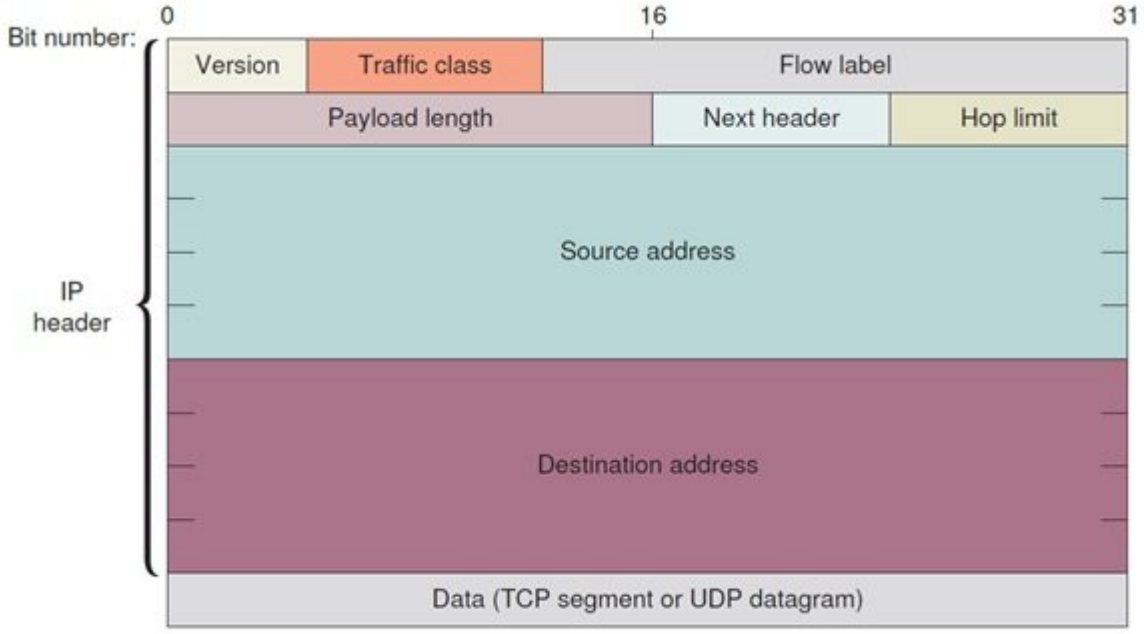
آموزش رایگان دوره نتورک‌پلاس (Network+) آشنایی با بسته‌های IPv6، دامنه تصادم/پخشی، پروتکل ICMP (بخش 27)

در مقاله شماره گذشته آموزش نتورک‌پلاس با دست دادن سه مرحله‌ای در پروتکل TCP، نحوه ارسال پیام‌ها از طریق پروتکل UDP و فیلدهایی که درون یک بسته IPv4 قرار دارند آشنا شدیم. در این شماره قصد داریم به سراغ پروتکل IPv6 رفته، فیلدهای یک بسته Ipv6 را بررسی کرده، نگاه دقیق‌تری به پروتکل ICMP داشته و با دامنه تصادم بیشتر آشنا شویم.

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

بسته‌های IPv6

با توجه به این‌که IPv6 اطلاعات بیشتری را حمل می‌کند، در نتیجه بسته‌های آن قالب متفاوتی نسبت به بسته‌های IPv4 دارند. فیلدهای درون یک سرآیند IPv6 در شکل زیر نشان داده شده‌اند.



یک بسته **IPv6**

جزییات مربوط به هر یک از فیلدهای عکس بالا به شرح زیر هستند:

فیلد		طول	عملکرد
سرآیند	Version	bits 4	نسخه‌ای از پروتکل IPv که بسته‌ها از آن استفاده می‌کنند را نشان می‌دهد.
	Traffic class	bits 8	حق اولویت بسته‌ها را مشخص می‌کند. این فیلد مشابه با فیلد DiffServ در بسته‌های IPv4 است، اما شبیه به آن نیست.
	Flow label	bits 20	جریان یا توالی بسته‌ها از مبدا به سمت یک یا چند مقصدی که بسته‌ها به آن تعلق دارند را نشان می‌دهد. روترها این اطلاعات جریانی را ترجمه می‌کنند تا مطمئن شوند که بسته‌ها به درستی در حال انتقال هستند. اطلاعات جریانی ممکن است به اولویت‌بندی ترافیک نیز کمک کنند.
	Payload length	bits 16	اندازه بارداده یا داده‌هایی که توسط یک بسته حمل می‌شوند را مشخص می‌کند. برعکس فیلد Total length در بسته‌های Ipv4 فیلد Payload length در بسته‌های IPv6 به اندازه کل یک بسته اشاره‌ای نمی‌کند.
	Next header	bits 8	نوع سرآیند یک بسته IP را مشخص می‌کند که به‌طور معمول TCP یا UDP است.
	Hop limit	bits 8	مدت زمانی که بسته‌ها می‌توانند از سوی روتری در یک شبکه فوروارد شوند را مشخص می‌کند. این فیلد عملکردی شبیه به فیلد TTL در بسته‌های IPv4 دارد. زمانی که hop limit به 0 برسد، بسته از دست رفته محسوب می‌شود.
	Source address	bits 128	آدرس کامل آی‌پی مبدا را نشان می‌دهد.
	Destination address	bits 128	آدرس کامل آی‌پی مقصد را نشان می‌دهد.
	Data	Variable	شامل داده‌های اصلی است که مبدا ارسال کرده، همراه با سرآیندهایی که از لایه‌های بالاتر آمده‌اند. فیلد داده‌ای بخشی از سرآیند IPv6 نیست، بلکه درون سرآیند IPv6 کپسوله شده است. به یاد داشته باشید که فیلد داده‌ای در سطر پایین جزیی از سرآیند HPv6 نیست.

اگر فیلدها و عملکردها آن‌ها در IPv6 را با فیلدهای درون یک بسته IPv4 که در شماره گذشته بررسی کردیم، ارزیابی کنید، ممکن است شباهت‌ها و تفاوت‌هایی را مشاهده کنید. به‌طور مثال، هر دو بسته با یک فیلد 4 بیتی Version آغاز می‌شوند. سایبر فیلدها همچون TTL در Ipv4 و hop limit در Ipv6 شبیه هستد، اما تفاوت‌هایی دارند. یک تفاوت قابل توجه بین هر دو نسخه این است که بسته‌های IPv6 آدرس‌هایی به مراتب طولانی‌تر دارند. همچنین در یک بسته IPv6 ما فیلد Fragment offset نداریم، زیرا میزبان‌ها در IPv6 اندازه بسته‌ها را پیش از آن‌که پیام‌ها را ارسال کنند، متناسب با وضعیت شبکه تنظیم می‌کنند.

پروتکل کنترل پیام اینترنتی (ICMP) سرنام Internet Control Message Protocol

در حالی که پروتکل IP کمک می‌کند تا داده‌ها به مقصد درستی برسند، پروتکل کنترل پیام اینترنتی (ICMP) که پروتکل لایه شبکه است یکی از پروتکل‌های زیربنایی بوده که گزارش موفقیت‌آمیز بودن یا شکست در تحویل داده‌ها را گزارش می‌دهد. این پروتکل می‌تواند نشان دهد چه زمانی بخشی از شبکه پر ازدحام بوده، زمانی که داده‌ها

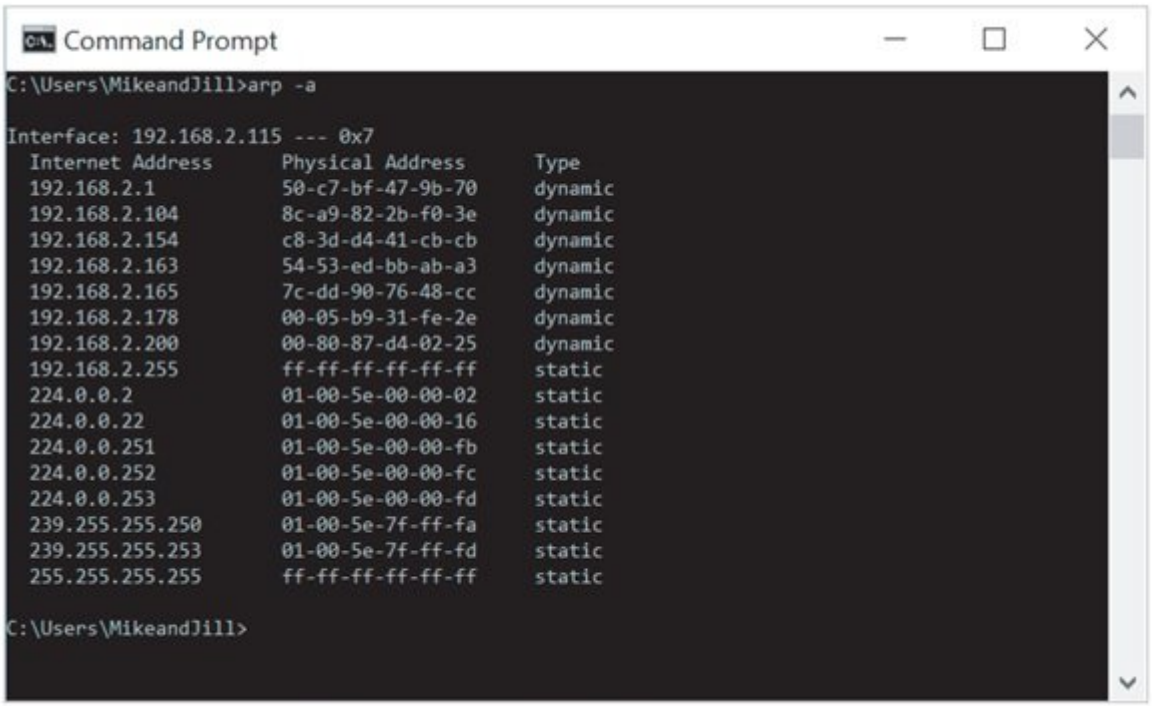
نتوانسته‌اند به مقصد برسند را مشخص کرده و زمانی که داده‌ها به واسطه منقضی شدن زمان تعیین شده در فیلد TTL از دست رفته‌اند را مشخص می‌کند. ICMP خطاهای مربوط به انتقال را به ارسال‌کننده داده گزارش داده، اما خطاهای شناسایی شده را برطرف نکرده و این‌کار را به پروتکل‌های لایه بالاتری همچون TCP محول می‌کند.
گزارش‌هایی که پروتکل ICMP منتشر می‌کند دارای اطلاعات مهمی هستند که برای حل مشکلات شبکه استفاده می‌شوند. پیام‌های ICMP به‌طور خودکار از سوی دستگاه‌های درون شبکه همچون روترها و ابزارهایی همچون ping تولید می‌شود. از آن‌جایی که این پروتکل در لایه 3 و در کنار پروتکل IP کار می‌کند، پیام‌های ICMP شامل سرآیند IP و سرآیند ICMP هستند. شکل زیر یک سرآیند ICMP را نشان می‌دهد.

یک بسته ICMP

فیلدهای تصویر بالا در جدول زیر تشریح شده‌اند. دقت کنید که فیلد داده‌ای در سطح پایین جزیی از سرآیند ICMP نیست.

فیلد		طول	عملکرد
سرآیند	Type	bits 8	نوع پیام ICMP را مشخص می‌کند. به‌طور مثال عدم دریافت پیام در مقصد
	Code	bits 8	زیرنوع یک پیام را مشخص می‌کند. به‌طور مثال میزبان مقصد شناخته شده نیست
	Checksum	bits 16	به گره دریافت‌کننده اجازه می‌دهد تا مشخص کند که آیا بسته ICMP در مدت زمان انتقال خراب شده یا به درستی دریافت شده است.
	Rest of header	bits 32	به نوع پیام و زیرپیام بستگی دارد
	Data	Variable	به‌طور معمول حاوی سرآیند آی‌پی و 8 بایت نخست بخش داده‌ای یک بسته آی‌پی بوده که یک پیام ICMP آن‌را ارسال کرده است.

IPv6 با تکیه بر پروتکل ICMPv6 همان کارهایی را انجام می‌دهد که پروتکل‌های ICMPv4 و ARP روی IPv4 عهده‌دار انجام آن است. این وظایف شامل شناسایی و گزارش‌دهی خطاهای رخ داده در زمان انتقال، کشف سایر گره‌ها روی یک شبکه و مدیریت چندوظیفگی است. برای درک بهتر تفاوت‌های ICMPv4 و ICMPv6 باید اطلاع دقیقی درباره پروتکل ARP روی شبکه‌های IPv4 داشته باشیم. پیشنهاد می‌کنم مطلب **هر آنچه که باید در مورد پروتکل تفکیک آدرس یا ARP بدانید** را مطالعه کنید تا اطلاعات دقیق‌تری به دست آورید. برای مشاهده جدول ARP روی یک ایستگاه کاری ویندوز، پنجره خط فرمان را باز کرده و فرمان arp -a را درون آن وارد کنید.

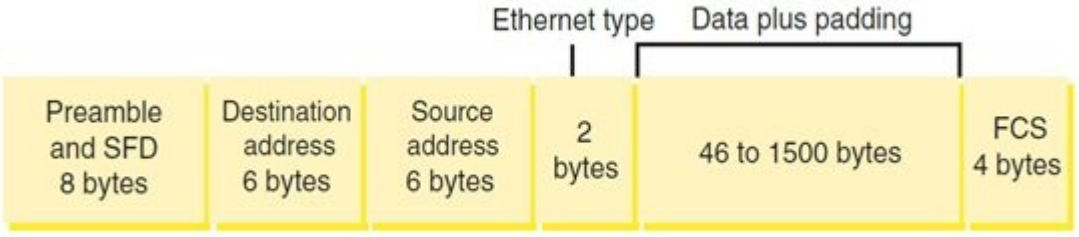


فرمان arp -a فهرستی از دستگاه های متصل به شبکه را نشان می دهد

اترنت (Ethernet)

مهم‌ترین استاندارد لایه پیوند داده، اترنت، وفق‌پذیر بوده، روی بیشتر مدیاهای شبکه اجرا شده و هزینه‌های مقرون به صرفه‌ای دارد. مزایای متعدد اترنت باعث شده است تا به یکی از محبوب‌ترین و مهم‌ترین فناوری‌های شبکه‌های محلی مدرن امروزی تبدیل شود.

Ethernet II استاندارد جاری است که شرکت‌های دل، اینتل و Xerox پیش از آن‌که IEEE شروع به استانداردسازی اترنت کند آن‌را معرفی کردند. برعکس پروتکل‌های لایه بالاتر، اترنت سرآیند و دنباله فریم را به بارداده‌ای که از لایه پایین‌تر از خود به ارث برده است اضافه می‌کند. این‌کار باعث می‌شود تا فریمی پیرامون یک بارداده ساخته شود. شکل زیر یک فریم Ethernet II را نشان می‌دهد.



جزییات مربوط به فیلدهای اترنت 2 به شرحی است که در جدول زیر آماده است.

نام فیلد		طول	توضیح
Preamble		bytes 7	ساعت دریافت‌کننده پیام را همگام‌سازی می‌کند.
(SFD (start frame delimiter		byte 1	نشان می‌دهد که فریم آماده به کار است.
سرآیند	Destination address	bytes 6	مک آدرس دریافت‌کننده را ارائه می‌کند.
	Source address	bytes 6	مک آدرس ارسال‌کننده را ارائه می‌کند.
	Type field	bytes 2	پروتکل بالادستی که فریم را حمل کرده است را مشخص می‌کند. به‌طور مثال، یک بسته IP مقدار 0x0800 را درون فیلد Type قرار می‌دهد.

Data		bytes to 46 1500 bytes	اگر داده‌ها حداقل 46 بایت نیستند، آن‌را تکمیل می‌کند.
دنبال کننده	FCS (frame check (sequence	bytes 4	اطمینان حاصل می‌کند که داده‌ها در مقصد دقیقا مطابق با داده‌های ارسال شده از مبدا هستند، برای این منظور از الگوریتم CRC (یک چرخه اضافی بررسی) برای بررسی و مطابقت دادن استفاده می‌شود.

دقت کنید در جدول بالا مقادیر فیلدهای SFD در زمان محاسبه اندازه فریم لحاظ نشده‌اند. بیشتر ابزارهای تحلیل‌گر شبکه شبیه به Wireshark نمی‌توانند دو فیلد اول را بررسی کنند، زیرا این داده‌ها در زمان انتقال و وارد شدن از سوی سخت‌افزارها حذف می‌شوند.

ترکیب سرآیند و FCS در مجموع یک فریم 18 بایتی را پیرامون داده‌ها ایجاد می‌کنند. بخش داده‌ای از یک فریم اترنت شامل 46 تا 1500 بایت اطلاعات است. بنابراین، ما می‌توانیم حداقل و حداکثر اندازه یک فریم را به یکی از دو روش زیر محاسبه کنیم:

• 18-byte frame + 46 bytes minimum data size = 64 bytesminimum frame size

• 18-byte frame + 1500 bytes maximum data size = 1518 bytesmaximum frame size

بیشینه واحد انتقال (MTU) سرنام Maximum Transmission Unit

بیشینه واحد انتقال مقداری بر حسب بایت بوده و حداکثر اندازه قابل انتقال واحدهای اطلاعاتی در یک رابط را مشخص می‌کند. MTU مقداری را مشخص می‌کند که روترها در یک مسیر انتقال پیام در لایه شبکه مجاز به استفاده از آن هستند. بنابراین، MTU حداکثر اندازه بارداده که یک فریم لایه 2 قادر به کپسوله کردن آن است را تعریف می‌کند. برای اترنت، مقدار پیش‌فرض MTU برابر با 1500 بایت است که استاندارد رایج اینترنت است. با این حال، سایر فناوری‌های لایه 2 ممکن است اجازه دسترسی به مقادیر بالاتر یا پایین‌تر برای MTU را ارائه کنند. از آن‌جایی که همواره احتمال وجود سرباره در هر فریم وجود دارد و همین مسئله باعث می‌شود تا کارت شبکه زمانی را برای مدیریت فریم صرف کند، به‌کارگیری اندازه‌های بالاتر فریم روی یک شبکه به‌طور معمول باعث افزایش سرعت می‌شود. با این وجود استثناءهایی نیز وجود دارد که باعث می‌شوند اندازه فریم اترنت را محدود در نظر بگیریم.

- فریم‌های اترنت روی یک شبکه محلی مجازی (VLAN) می‌توانند یک فیلد اضافی 4 بایتی میان فیلد آدرس مبدا و فیلد Type داشته باشند که این فیلد برای مدیریت ترافیک شبکه محلی می‌تواند استفاده شود.
- برخی از شبکه‌های خاص از یک نسخه اختصاصی از اترنت استفاده می‌کنند که اجازه می‌دهد اندازه فریم را بیشتر در نظر بگیرید. در این حالت MTU می‌تواند اندازه‌ای برابر با 9198 بایت داشته باشد که البته این موضوع به نوع معماری اترنتی که استفاده شده است بستگی دارد.

شاید این سوال به ذهن‌تان خطور کرده باشد که حداکثر اندازه یک بسته آی‌پی برابر با 65535 بایت است، در حالی که حداکثر اندازه PDU در لایه شبکه و در زمان انتقال روی شبکه اترنت فقط 1500 بایت است. چرا این اختلاف وجود دارد؟ تکه‌تکه کردن به فرآیند تقسیم بسته‌هایی که برای سخت‌افزارهای یک شبکه بیش از اندازه بزرگ هستند اطلاق می‌شود. در این فرآیند بسته‌ها کوچک‌تر می‌شوند تا به شکل مطمئنی روی شبکه انتقال پیدا کنند. در یک شبکه IPv4 روترها بسته‌های وارد شده را آزمایش می‌کنند تا بررسی کنند که آیا اندازه بسته بزرگ‌تر از بیشینه واحد انتقال رابط خروجی است یا خیر، اگر این‌گونه است اجازه شکستن بسته‌ها را صادر می‌کنند. بسته‌هایی که دارای چنین ویژگی باشند به بسته‌های کوچک‌تری شکسته شده که هر یک سرآیند خاص خود را داشته و موقعیت آن‌ها درون مجموعه‌ای که شکسته شده‌اند مشخص می‌شود. فرآیند شکستن بسته‌ها سرعت شبکه را کاهش می‌دهد، به همین دلیل بیشینه واحد انتقال در سطحی تنظیم می‌شود که همه دستگاه‌ها در مسیر دریافت پیام بدون مشکل بتوانند کار کنند. TCP تا جایی که امکان دارد سعی می‌کند در تعامل با MSS سرنام maximum segment size مانع از تکه‌تکه شدن بسته‌ها شود. برای این منظور در زمان ایجاد یک ارتباط سعی می‌کند حداکثر اندازه ممکن برای PDU در لایه انتقال را مشخص کند.

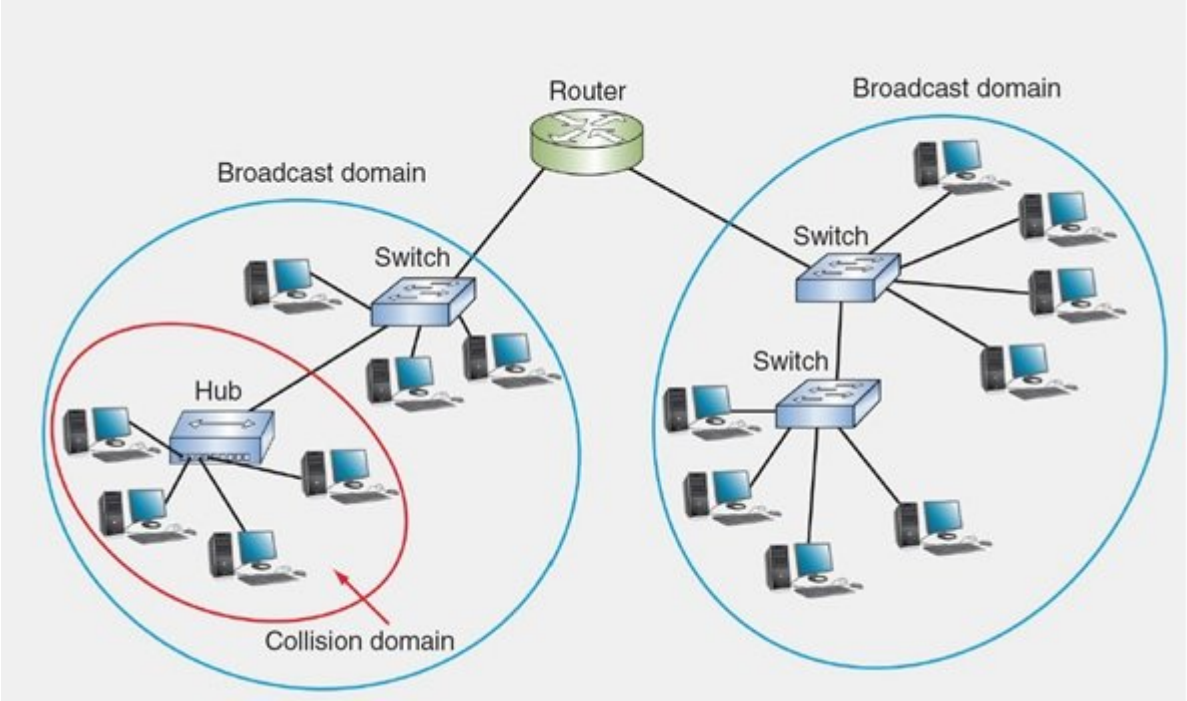
میراثی از گذشته: Collisions و CSMA/CD

زمانی‌که IEEE اولین استاندارد اترنت را در سال 1980 میلادی منتشر کرد، به‌طور رسمی آن‌را استاندارد IEEE 802.3 CSMA/CD نام‌گذاری کرد، اما به شکل غیررسمی اترنت خوانده شد. یک فریم CSMA/CD الگویی متفاوت نسبت به یک فریم اترنت 2 دارد که امروزه در شبکه‌ها از آن استفاده می‌شود. فریم نسل قبلی به نام فریم 802.3 معروف بود، اما فریمی که امروزه در اترنت 2 از آن استفاده می‌شود به نام فریم DIX معروف است. شبکه‌های CSMA/CD اغلب از یک هاب در قالب یک لایه فیزیکی از مدل OSI استفاده می‌کنند. همه گره‌های متصل به هاب برای دسترسی به شبکه در حال رقابت با یکدیگر هستند. گره‌های روی یک شبکه برای آن‌که به درستی بتوانند به منابعی که روی شبکه‌های CSMA/CD (Carrier Sense Multiple Access with Collision Detection) قرار دارند دسترسی پیدا کنند از مک آدرس استفاده می‌کنند. برای چند لحظه وقت گذاشته و به عبارت دسترسی چندگانه با قابلیت شنود/شناسایی سیگنال حامل (Carrier Sense Multiple Access with Collision Detection) فکر کنید. واژگان استفاده شده در این عبارت چه معنایی دارند؟

- Carrier Sense اشاره به کارت شبکه اترنتی دارد که مادامی که هیچ گره‌ای اقدام به ارسال داده‌ها نکند در حال گوش دادن و انتظار کشیدن است.
- Multiple Access اشاره به گره‌های چندگانه‌ای دارد که به مدیایی روی همان شبکه دسترسی دارند.
- Collision Detection اشاره به اتفاقاتی اشاره دارد که در زمان انتقال داده‌ها میان دو گره رخ داده است.

هنگامی که انتقال داده‌ها میان دو گره با مشکل روبرو می‌شود، یک تصادم رخ می‌دهد. پس از یک تصادم/برخورد هر گره بر حسب یک مقدار تصادفی صبر کرده و سپس به ارسال دوباره اقدام می‌کند. یک دامنه تصادم بخشی از یک شبکه است که برخوردها در آن رخ می‌دهد. هاب‌ها چند کامپیوتر را در یک توپولوژی ستاره‌اتوبوسی به یکدیگر متصل می‌کنند که در برخی موارد مشکلات شدیدی را به وجود می‌آورند.

نکته امتحانی: آزمون **نتورک‌پلاس** از شما انتظار دارد که تفاوت‌های میان یک دامنه تصادم (collision) و یک دامنه پخش (broadcast) را مشخص کرده و بدانید در قبال هر یک از این مفاهیم چه تهمیداتی باید در نظر بگیرید. در نتیجه باید اطلاعات کافی در مورد این دو اصطلاح داشته باشید. هر دو دامنه با گروهی از گره‌ها که فرآیند انتقال از/در میان آن‌ها انجام می‌شود تعریف می‌شوند. دامنه پخشی (broadcast) به محدوده یا سگمنتی از شبکه اطلاق می‌شود که اگر یک دستگاه اطلاعات خود را ارسال کند، در آن سگمنت همه دستگاه‌ها قادر به دریافت بسته اطلاعاتی هستند، زیرا همه گره‌ها روی یک شبکه محلی به بسته دسترسی دارند، اما بسته‌ها از طریق روترها فورووارد نمی‌شوند. بنابراین، روترها مرزهای (کرانه‌های) یک دامنه پخشی را تعریف کرده که همراه با تعریف یک شبکه محلی است. در نقطه مقابل، در یک دامنه تصادم (collision) انتقال محدود به گره‌هایی می‌شود که به شکل مستقیم به یک هاب متصل شده‌اند. بنابراین هاب کرانه دامنه تصادم خودش را تعریف می‌کند. شکل زیر تفاوت میان دو دامنه broadcast و collision را نشان می‌دهد.



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:
15 اسفند 1397

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/14762/%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%A2%D8%B4%D9%86%D8%A7%DB%8C%DB%8C-%D8%A8%D8%A7-%D8%A8%D8%B3%D8%AA%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-ipv6%D8%8C-%D8%AF%D8%A7%D9%85%D9%86%D9%87