نام و نام خانوادگی دانشجو: رحمت اله انصاری

شماره دانشجویی: ۹۹۱۲۳۷۷۳۳۱

Date: 1402-01-22

گزارش کار جلسه پنجم:

در این جلسه دو پروتکل ارسال پکت ARP و ICMP بررسی شد.

پروتکل چیست؟

در پاسخ به پروتکل چیست و protocol به فارسی بایستی گفت پروتکل یعنی مجموعه ای استاندارد از قوانین که به دستگاه های الکترونیکی امکان برقراری ارتباط با یکدیگر را می دهد. این قوانین شامل چه نوع داده ای می توانند منتقل شوند، چه دستوراتی برای ارسال و دریافت داده ها و چگونگی تأیید انتقال داده ها، است.

پروتکل ICMP

پروتکل icmp که مخفف عبارت internet control message protocol است که در فارسی آن را پروتکل کنترل پیام های اینترنتی ترجمه می کنند. icmp جهت خطایابی در کامپیوترها ، روترها و هاست، بررسی وجود سیگنال و به طور کلی بررسی وضعیت ارتباطی بین روتر و سرور ها مورد استفاده قرار می گیرد.

از ICMP به چه منظوری استفاده می‌شود؟

هدف اصلی Internet Control Message Protocol گزارش خطا است. زمانی که دو دستگاه از طریق اینترنت با یکدیگر ارتباط برقرار می‌کنند، در صورت عدم رسیدن هر یک از داده‌ها به مقصد مورد نظر، ICMPخطاهایی را برای اشتراک با سایر دستگاه‌های ارسال کننده ایجاد می‌کند. به عنوان مثال، در صورتی که یک پکت داده برای روتر خیلی بزرگ باشد، روتر پکت را رها نموده و پیام ICMP را به مبدا اصلی باز می‌گرداند.

استفاده دیگر پروتکل ICMP در امور مربوط به تشخیص شبکه است Traceroute .و ping هر دو با این پروتکل کار می‌کنند. از ابزار traceroute برای نشان دادن مسیر بین دو دستگاه اینترنتی استفاده می‌شود.

مسیر انتخاب شده، مسیر واقعی فیزیکی روترهای متصل است که یک درخواست می‌بایست قبل از رسیدن به مقصد از آن عبور کند. سفر بین یک روتر و دستگاه دیگر، تحت عنوان hop شناخته می‌شود و traceroute نیز زمان مورد نیاز برای هر "هاپ" را در طول مسیر گزارش می‌کند. این امر می‌تواند برای تعیین منابع تاخیر شبکه مفید باشد.

ابزار ping نسخه‌ی ساده شده‌ی traceroute است. یک ping سرعت اتصال بین دو دستگاه را بررسی نموده و به طور دقیق اعلام می‌کند که یک پکت چقدر طول می‌کشد تا به مقصد خود برسد و مجددا به دستگاه فرستنده برگردد.

هرچند کهping ، داده‌های مربوط به مسیریابی یا هاپ را ارائه نمی‌دهد، اما هنوز هم یک معیار بسیار مفید برای اندازه‌گیری تاخیر بین دو دستگاه به شمار می‌رود. پیام‌های echo-request و echo-reply به طور معمول برای انجام یک ping مورد استفاده قرار می‌گیرند.

متاسفانه حملات شبکه می‌توانند از این فرایند سوء استفاده کرده و ابزارهایی جهت ایجاد اختلال مانند ICMP flood attack و ping of death attack تولید نمایند.

پروتکل ARP

پروتکل arp در شبکه مخفف عبارت Address Resolution Protocol بوده و به عنوان یک پروتکل ارتباطی جهت پیدا کردن لایه آدرس و پیوند آن مورد استفاده قرار می‌گیرد. عملکرد پروتکل arpچیزی شبیه به پروتکل MAC بوده که در لایه اینترنت از آدرس IPV4 استفاده می‌کند.

پروتکل arp چه وظیفه ای بر عهده دارد ؟

برای درک اینکه پروتکل ARP چگونه کار می‌کند مثال زیر را باید در نظر بگیرید. دو کامپیوتر در کی دفتر وجود دارد. آن‌ها با نام کامپیوتر ۱۴ و کامپیوتر ۲ شناخته می شوند. این کامپیوتر ها با استفاده از کابل های

اترنت و سوئیچ شبکه به هم متصل هستند. این اتصال به صورت یک شبکه محلی است. در این اتصال هیچ روتاری دخالت نمی کند. کامپیوتر ۱ بسته ای را برای کامپیوتر ۲ ارسال می کند. این ارسال از طریق DNS انجام می شود. در این فرایند DNS مشخص می کند که کامپیوتر ۲ دارای آدرس ۱۹۲.۱۶۸.۰.۵۵ به عنوان IP آدرس است.

برای ارسال بسته به مک آدرس کامپیوتر ۲ نیاز است. در ابتدا رایانه ۱ با استفاده از جدول ARP ذخیره شد در خود آدرس ۱۹۲.۱۶۸.۰.۵۵ را جست و جو می کند. در این حالت در سوابق موجود در این IP به دنبال مک آدرس است. آدرس مک کامپیوتر ۲ به عنوان مثال eb: 24: b2: 05: ac ۰۰ :است. در صورت یافتن مک آدرس کامپیوتر ۱ یک فریم را در اترنت به مقصد آدرس eb: 24: b2: 05: ac ۰۰ :ارسال می کند. در این فریم یک بسته IP وجود دارد. کامپیوتر ۲ این فریم را دریافت می کند و یک پیام پاسخ به IP ای که در فریم قرار داشت ارسال می کند. به این ترتیب هر دو رایانه آدرس های مک خود را در جداول ARP خود قرار می دهند و برای یکدیگر ارسال می کنند.

کامپیوتر ۱ اطلاعات پاسخ را دریافت می کند در جدول خود ذخیره می کند. اکنون هر دو رایانه یکدیگر را در شبکه شناخته اند و می توانند برای یکدیگر بسته های داده را ارسال کنند. این مثال نمونه کوچکی از عملکرد پروتکل ARP بود که به ساده ترین شکل ممکن توضیح داده شد.