به نام خدا

محمد عرفان آراسته

۱ - CSMA ، در شبکه های سیمی و بی سیمی متفاوت است ، این پروتکل در شبکه های بی سیم و سیمی چه اسمی دارد و چه فرقی دارند؟

همانطور که میدانید زمانیکه اطلاعات بر روی بستر شبکه های کامپیوتری در حال حرکت به سوی مقاصد خود میباشند احتمال بروز تصادم و برخورد بین این اطلاعات و پکت ها وجود دارد. مخصوصاً زمانی شبکه بین دو دستگاه به صورت فیزیکی مشترک باشد و دو دستگاه نتوانند همزمان با هم ارتباط داشته باشند.

برای کمتر کردن یا از بین بردن این مشکل الگوریتم هایی طراحی شده است، و به صورت پروتکل در آمده است :

این پروتکل ها در لایه ۲ و بوسیله لایه MAC اجرا می شوند.

Carrier-sense multiple access:

به صورت خلاصه در این الگوریتم هر دستگاهی که می‌خواهد در شبکه اطلاعاتی ارسال کند باید ابتدا چک کند که دستگاه دیگری اطلاعاتی ارسال نمی‌کند و شبکه مشغول نیست. (carrier sense)

Carrier-sense multiple access with collision detection (CSMA/CD):

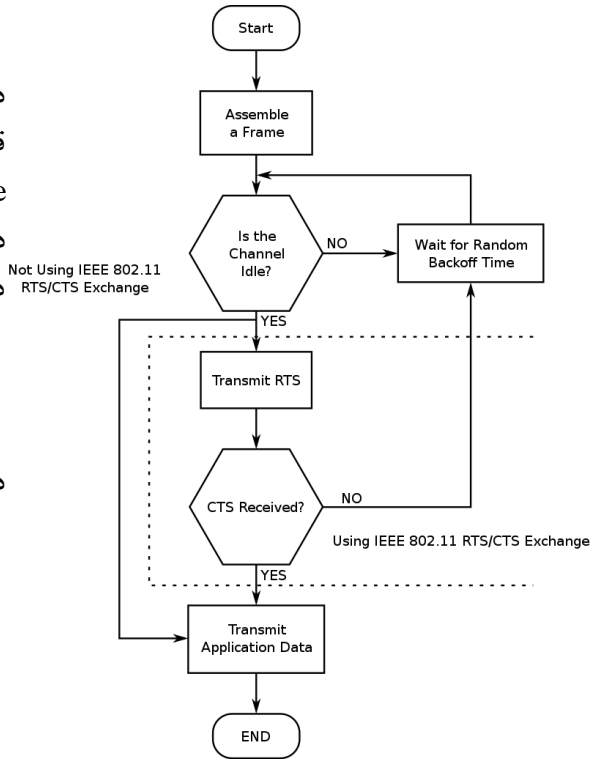
در این پروتکل علاوه بر اینکه یک دستگاه منتظر خالی شدن بستر شبکه برای ارسال اطلاعات می‌شود (carrier-sense)، پروتکلی برای وقتی که در وسط ارسال اطلاعات تداخل رخ دهد نیز دارد و می‌تواند این تداخل را شناسایی کند (collision detection) ،

بعد از اینکه این تداخل در هنگام ارسال فریم شناسایی شد ، ارسال فریم را متوقف می‌کند و یک jam signal (سیگنالی حاوی ۳۲ بیت که به بقیه ایستگاه ها هشدار می‌دهد تا آن‌ها نیز اطلاعاتی ارسال نکنند) ارسال می‌کند و سپس قبل از اینکه بخواهد دوباره آن فریم را ارسال کند یک زمان رندوم متنظر می‌شود.

این پروتکل بیشتر در شبکه‌های سیمی استفاده می شود.

Carrier-sense multiple access with collision avoidance (CSMA/CA):

در این پروتکل نیز علاوه بر اینکه از carrier sensing استفاده می‌شود (یعنی قبل از ارسال دیتا بررسی می کند که شبکه مشغول نباشد) ، از collision avoidance نیز استفاده می‌شود یعنی هر کسی قبل از ارسال دیتا با ارسال درخواست مطمئن می‌شود که شبکه مشغول نیست و دستگاه متناظر باید پاسخ دهد که آیا شبکه برای ارسال اطلاعات خالی هست یا خیر.



RTS: Request to send

CTS: Clear to Send

از این پروتکل بیشتر در شبکه‌های وایرلس استفاده می شود.

در این پروتکل به جای تشخیص تداخل تلاش می‌شود که از آن جلوگیری کرد.

(به غیر از این پروتکل ها، پروتکل های دیگری نیز هستند.)

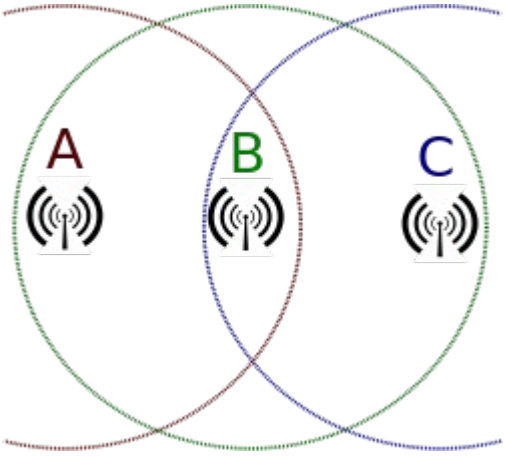
حال چرا در شبکه‌های وایرلس از CSMA/CD استفاده نمی‌شود و از CSMA/CA استفاده می شود؟

۱.شبکه های وایرلس طبق استاندارد IEEE 802.11 ،معمولا یک‌طرفه (half-duplex) هستند:

در نتیجه هر دستگاه در شبکه هنگام ارسال اطلاعات نمی‌تواند چیزی را دریافت کند پس نمی‌تواند collision detection به آن شکلی که در پروتکل CSMA/CD داریم داشته باشد.

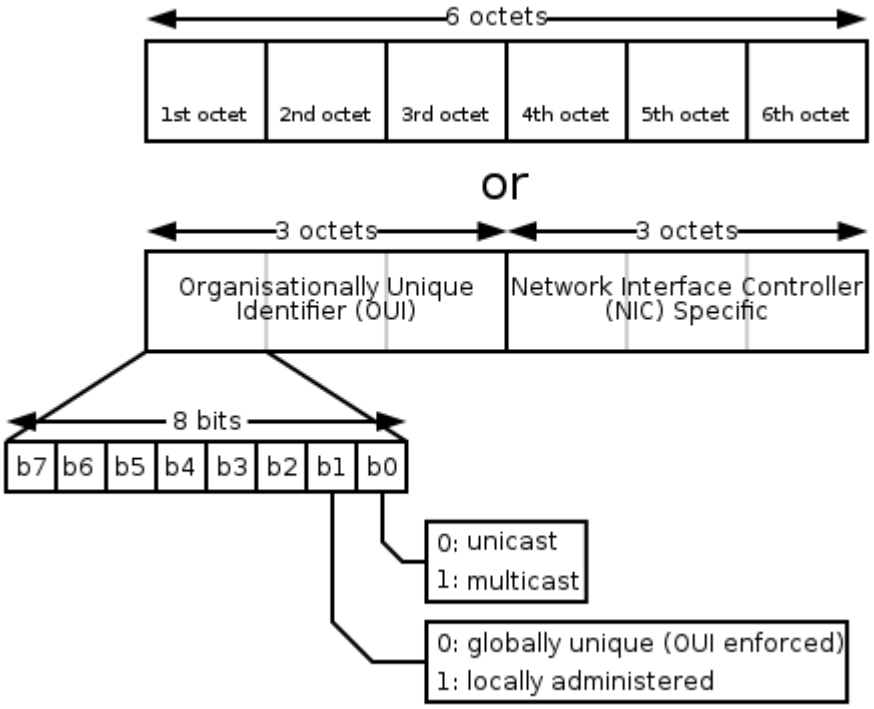
۲.کامپیوتر هایی که به وسیله وایرلس به یک Access point متصل هستند می‌توانند Access point را ببینند ولی شاید نتوانند یکدیگر را ببینند. (Hidden Node Problem)

در نتیجه برای اینکه در این شبکه، کامپیوترها با یکدیگر ارتباط برقرار کنند نیاز به یک پروتکل بهتر است تا اجازه ندهد برای مثال ۲ فرستنده در یک کانال برای Access point داده ارسال کنند ، زیرا این باعث می‌شود دیتای آن‌ها تداخل پیدا کند و Access Point نتواند دیتا هر دو را به درستی دریافت کند. همچنین دو فرستنده نمی‌توانند بفهمند که با یکدیگر تداخل دارند.



منابع:
https://en.wikipedia.org/wiki/Carrier-sense_multiple_access
https://en.wikipedia.org/wiki/Carrier-sense_multiple_access_with_collision_detection
https://en.wikipedia.org/wiki/Carrier-sense_multiple_access_with_collision_avoidance
https://www.quora.com/Why-does-wireless-networking-use-CSMA-CA-instead-of-CSMA-CD?share=1
https://askinglot.com/why-csma-cd-is-not-used-for-wireless-network
https://www.ionos.com/digitalguide/server/know-how/csmaca-carrier-sense-multiple-access-with-collision-avoidance/?
https://www.geeksforgeeks.org/difference-between-csma-ca-and-csma-cd/
https://www.datisnetwork.com/csma-ca-vs-csma-cd.html

۲ـ بیت هفتم و هشتم مک آدرس از سمت چپ (شروع از ۱) چه کاربردی دارند؟ و چرا بیت هفتم در تولید آدرس ipv6 کاربرد دارد؟



(universal-bit) u-bit یا همان بیت هفتم مک آدرس می‌باشد که می‌تواند ۲ چیز را مشخص می‌کند :
۱. اینکه یک مک آدرس به صورت پیش‌فرض بر اساس تنظیمات کارخانه است (OUI enforced) یا به صورت جهانی بی همتاست و فقط یکی از آن ساخته شده (globally unique)
۲. یا اینکه این مک آدرس برای مصارف داخلی در شبکه‌ها استفاده می‌شود (locally administered)

و اما بیت هشتم unicast بودن یا grouping مک آدرس را مشخص می کند.

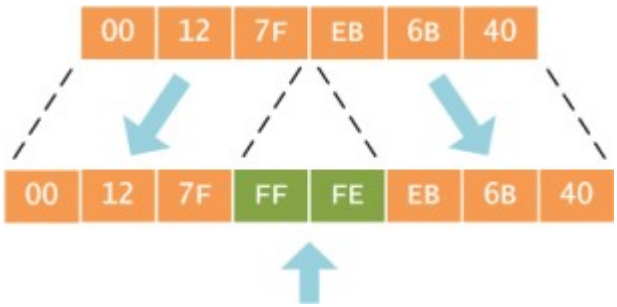
برای مثال wireshark برای یک مک آدرس مربوط به یک کارت وایرلس چنین چیزی را می گوید:

```
Address: IntelCor_76:12:09 (7c:50:79:76:12:09)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
```

(همانطور که مشاهده می‌کند بیت هفتم و هشتم این مک آدرس هر دو صفر اند به این معنی که این مک آدرس در جهان unique است و یک مک آدرس unicast محسوب می شود)

یکی از خوبی‌های ipv6 نسبت به ipv4 این است که می‌تواند به interface ها به صورت آتومات آدرس لایه ۳ (ip) بدهد. به این معنی که بر خلاف ipv4 که نیاز به dhcp یا کانفیگ های دستی دارد (اگرچه می‌توان از dhcpv6 برای ipv6 نیز استفاده کرد)، ipv6 می‌تواند بر اساس مک آدرس به راحتی یک ip برای خودش تولید کند و از آنجایی که مک

آدرس یک آدرس بی همتاست، در نتیجه آی پی های ورژن ۶ نیز بی همتا خواهند بود و از این نظر نیست مشکلی وجود نخواهد داشت. به این فرمت آدرس دهی فرمت EUI-64 می گویند.
در RFC2373 این تبدیل مک آدرس به آی پی ورژن ۶ توضیح داده شده:
ابتدا در وسط مک آدرس ۱۶ بیت (FF:FE) را طزریق می کنیم، به این شکل ما یک آدرس ۶۴ بیتی خواهیم داشت:



سپس بیت هفتم که مربوط به کاربری مک آدرس می‌باشد را برعکس می کنیم:

به این شکل ما یک نصفه از آدرس ipv6 درست کردیم. نصفه دیگر آدرس ipv6 مربوط به network ما می باشد.
تمام پروسه این تبدیل را خود کامپیوتر بر اساس مک آدرس انجام می‌دهد و نیاز نیست ما این کار را بکنیم.

منابع:
https://packetlife.net/blog/2008/aug/4/eui-64-ipv6/
https://en.wikipedia.org/wiki/IPv6_address#Modified_EUI-64
https://en.wikipedia.org/wiki/MAC_address

۳ـ پروتکل ARP چگونه کار می کند؟

Address resolution protocol ، هدف این پروتکل پیدا کردن آدرس‌های لایه link مثل MAC Address می‌باشد، برای مثال ما از این پروتکل استفاده می‌کنیم تا بتوانیم مک آدرس مربوط به یک آی پی مربوط به یک شبکه داخلی را پیدا کنیم.

این پروتکل یک پروتکل از نوع درخواست_پاسخ می باشد . همچنین پکت های مربوط به این پروتکل فقط درون شبکه داخلی انتقال داده می‌شوند و به خارج از شبکه منتقل نمی شوند.

روش کار این پروتکل به این شکل است:

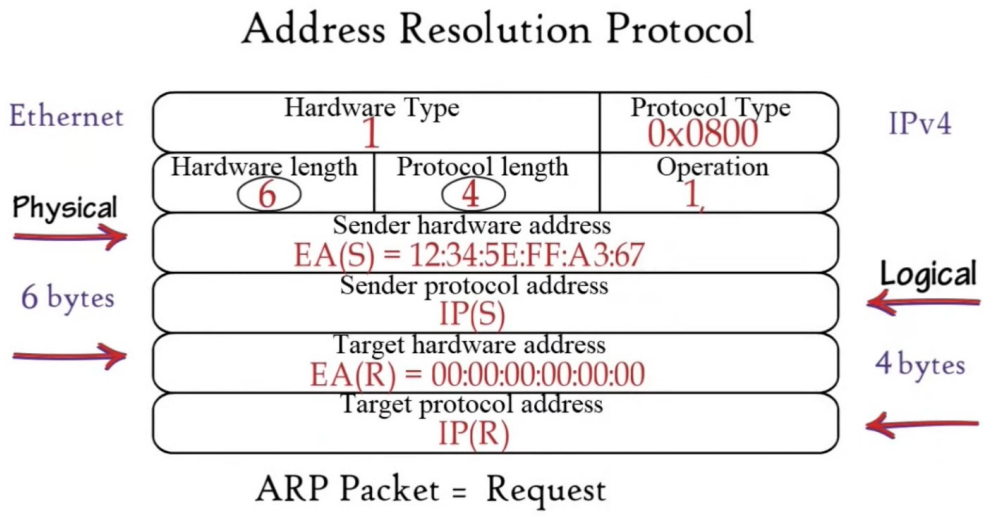
۱ . کامپیوتری که نیاز به دانستن مک آدرس مربوط به یک آی پی داخلی را دارد ، درخواستی بر اساس آی پی هدفش می‌سازد و در شبکه broadcast می کند.

۲ . تمام کامپیوتر های درون شبکه داخلی این درخواست را دریافت می‌کنند.

۳ . ولی فقط کامپیوتری که همان آی پی مورد نظر را دارد به این درخواست به صورت unicast پاسخ می‌دهد ، و مک آدرس خود را برای کامپیوتر درخواست کننده ارسال می کند. ولی بقیه کامپیوتر های درون شبکه این فریم را نادیده می گیرند.

۴ . بعد از اینکه کامپیوتر درخواست کننده مک آدرس هدف خود را پیدا کرد می‌تواند به صورت unicast با هدف خود ارتباط برقرار کند.

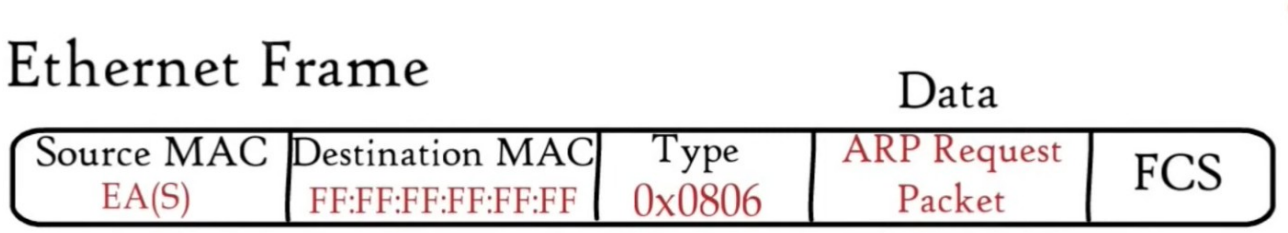
یک پکت arp برای مثال:



(همانطور که مشاهده می‌شود، در این درخواست ما مک آدرس هدف خود را نداریم، درنتیجه Target Hardware Address با یک مک آدرس کاملاً صفر پر شده.)

Hardware Type	==> Link Layer Protocol (Ethernet is 1)
Protocol Type	==> Network layer Protocol (ipv4 is 0x0800)
Hardware Length	==> Length of Link layer address (Ethernet MAC address is 6 bytes)
Protocol Length	==> Length of Network layer address (IP address is 4 bytes)
Operation	==> Specifies the operation that the sender is performing: 1 for request, 2 for reply.
Sender Hardware Address	==> Media address of the sender.
Sender Protocol Address	==> Network layer Address of sender.
Target hardware address	==> Media address of the receiver.
Target protocol address	==> Network layer Address of receiver.

که در نهایت در لایه ۲ در یک فریم به این شکل قرار می گیرد:



Type ==> type of Data carried by this frame (ARP is 0x0806)

منابع:
https://en.wikipedia.org/wiki/Address_Resolution_Protocol
https://www.youtube.com/watch?v=EC1slXCT3bg
https://www.youtube.com/watch?v=cn8Zxh9bPio
https://www.youtube.com/watch?v=tXzKjtMHgWI