



شبکه های کامپیوتری

(آمادگی برای آزمون Network+)

اسلاید سوم

«پخش اطلاعات در شبکه، کانال های انتقال داده، آدرس مک، هاب و سویچ، پروتکل ARP»



محمد سعید صفایی صادق

(استفاده از اسلایدها صرفاً برای دانشجویان مجاز می باشد!)

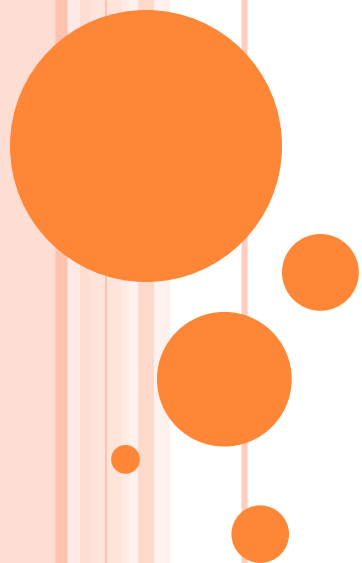
۱۴۰۳

درس
شبکه های
کامپیوتری

۳

پخش اطلاعات در شبکه

Network Casting



رابطه چند به چند (مدل داده) یا Many to Many

در ریاضیات، کاردینالیتی یک مجموعه، یک اندازه‌گیری برای «تعداد عناصر مجموعه» است.

رابطه چند به چند در تحلیل سامانه‌ها نوعی از کاردینالیتی است که به رابطه بین دو موجودیت اشاره دارد؛ مثلاً A و B، که در آن A ممکن است شامل یک نمونه والد باشد که برای آن فرزندان زیادی در B وجود دارد و برعکس. به عنوان مثال، A را به عنوان نویسنده و B را به عنوان کتاب در نظر بگیرید. یک نویسنده می‌تواند چندین کتاب بنویسد و یک کتاب می‌تواند توسط چندین نویسنده نوشته شود.



پخش اطلاعات در شبکه

در شبکه‌های رایانه‌ای، پخش کردن به معنای انتقال یک بسته به نحوی است که توسط همه دستگاه‌های موجود در شبکه دریافت شود.

در عمل، پخش کردن به یک دامنه پخش محدود می‌شود.

پخش کردن عمومی‌ترین روش ارتباطی است، و همچنین فشرده‌ترین است، به این معنا که ممکن است پیام‌های زیادی تقاضا شود و بسیاری از دستگاه‌های شبکه درگیر شوند.

پخش کردن ممکن است برای انجام یک نوع حمله بندآوری خدمات DoS به نام حمله اسمورف Smurf مورد سوء استفاده قرار بگیرد.



انواع روش های پخش اطلاعات در شبکه (معرفی ارتباطات موجود)

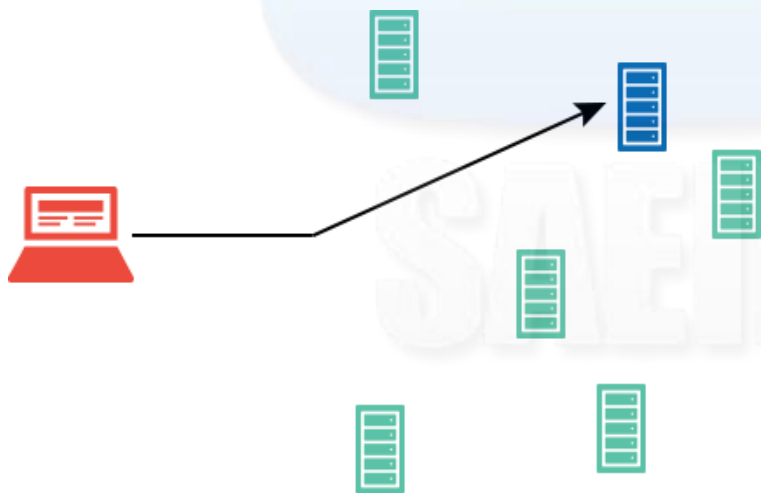
۱- روش Unicast یا تک پخشی :

در ساختار ارتباطات m به m ، یا همه به همه، به Unicast در اصطلاح ارتباط یک به یک گفته می شود.

در Unicast ارتباطات یک کامپیوتر به عنوان فرستنده و گیرنده و کامپیوتر دیگر نیز به عنوان گیرنده، فرستنده و گیرنده با همدیگر ارتباط برقرار می کنند و بسته های داده خود را رد و بدل می کنند.

هر آدرس مقصد به طور منحصر به فرد

یک نقطه پایانی گیرنده را شناسایی می کند.



انواع روش های پخش اطلاعات در شبکه (معرفی ارتباطات موجود)

۱- روش Unicast یا تک پخشی :

برای مثال در Unicast زمانیکه شما یک صفحه وب سایت را باز می کنید شما به یک آدرس IP که مربوط به وب سایت است اطلاعات را ارسال می کند و از آن اطلاعات را دریافت می کنید، حتی دانلود کردن یک فایل از یک فایل سرور هم نوعی از ارتباطات یک به یک محسوب می شود.

برای ساده تر شدن موضوع فرض کنید یک تلفن دارید و یک شماره تلفن ، شما این شماره را می گیرید و با شخص مورد نظر تماس برقرار می کنید.

این ارتباط بین شما و شخص صاحب خط برقرار می شود و به آن یک به یک گفته می شود زیرا کسی غیر از شما دو نفر از محتویات تماس با خبر نیست.

مثال تلفن بهترین مثال برای شناخت بهتر موضوع Unicast است .

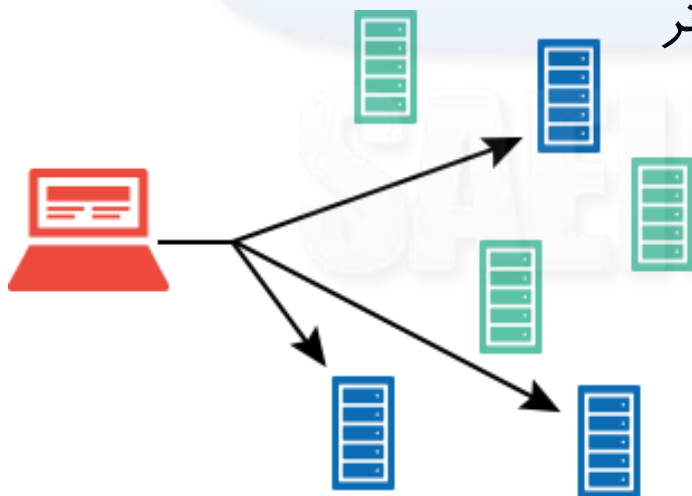
انواع روش های پخش اطلاعات در شبکه (معرفی ارتباطات موجود)

۲- روش Multicast یا چند پخشی :

در ساختار ارتباطات m به m به Multicast در اصطلاح ارتباط یک به چند گفته می شود.

در این نوع ارتباطات یک کامپیوتر ارتباط خود را بصورت همزمان با چندین کامپیوتر دیگر برقرار می کند و شروع به ارسال و دریافت داده می کند.

در واقع زمانیکه صحبت از Multicast می شود منظور گروهی از کامپیوترهای مشخص هستند که یک کامپیوتر با آنها ارتباط برقرار کرده است.



انواع روش های پخش اطلاعات در شبکه (معرفی ارتباطات موجود)

۲- روش Multicast یا چند پخشی :

در Multicast اطلاعات صرفاً به گروه یا مجموعه ای منتقل می شود که در آن گروه قرار دارند و اطلاعات به همه کامپیوترهای شبکه منتقل نخواهد شد.

دستگاه هایی که می خواهند اطلاعات مربوط به Multicast را دریافت کنند بایستی به عضویت این گروه Multicast در بیایند.

در ادامه خواهیم خواند که IPv4 Class D برای استفاده در موارد Multicasting مورد استفاده قرار می گیرد.

انواع روش های پخش اطلاعات در شبکه (معرفی ارتباطات موجود)

۲- روش Multicast یا چند پخشی :

برای راحت تر شدن درک موضوع فرض کنید یک تلفن دارید که قابلیت کنفرانس شدن دارد.

شما ابتدا افرادی که می خواهید در این کنفرانس باشند را شماره گیری می کند و هر کس که در این کنفرانس قرار دارد صدای افراد دیگر را خواهد شنید و افرادی که نمی توانند صدا را دریافت کنند.

پس بایستی به عضویت این گروه کنفرانس در بیایند تا بتوانند صدا را دریافت کنند.

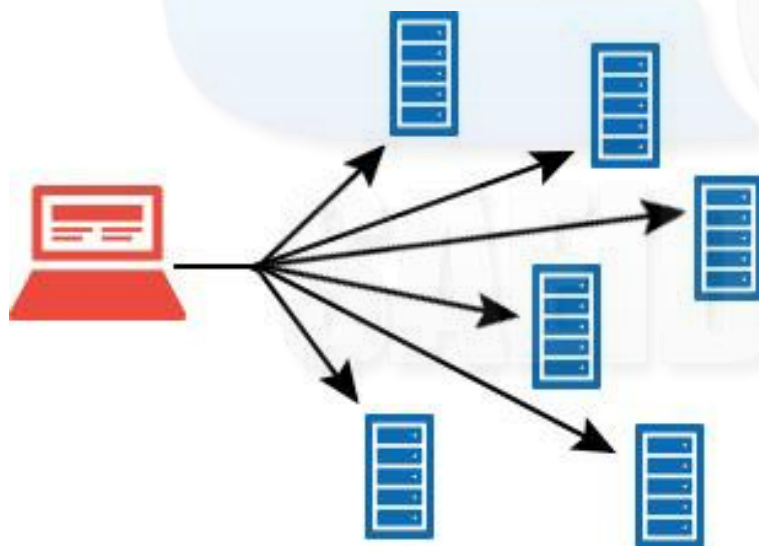
این بهترین مثال برای درک مفهوم Multicasting یا ارتباط یک به چند است.

انواع روش های پخش اطلاعات در شبکه (معرفی ارتباطات موجود)

۳- روش Broadcast یا همه پخشی :

در ساختار ارتباطات m به m Broadcast در اصطلاح ارتباط یک به همه گفته می شود.

در این نوع ارتباطات یک کامپیوتر ارتباط خود را بصورت همزمان با همه کامپیوترهای موجود در شبکه برقرار می کند و شروع به دریافت و ارسال داده می کند.



انواع روش های پخش اطلاعات در شبکه (معرفی ارتباطات موجود)

۳- روش Broadcast یا همه پختی :

در واقع زمانیکه صحبت از Broadcast می شود منظور همه کامپیوترهای موجود در شبکه هستند بدون استثناء ، یک کامپیوتر زمانیکه اطلاعات خود را Broadcast می کند تمامی کامپیوترهای شبکه این اطلاعات را دریافت می کنند.

در ساختار ارتباطات Broadcast یک کامپیوتر تنها یکبار اطلاعات را Broadcast می کند و در این لحظه اگر کامپیوتری روشن باشد این اطلاعات را در همان یکبار دریافت خواهد کرد.

در ادامه خواهیم خواند که هاب در شبکه بسته های اطلاعاتی Broadcast را از خود عبور می دهند.

انواع روش های پخش اطلاعات در شبکه (معرفی ارتباطات موجود)

۳- روش Broadcast یا همه پختی :

اما روترها یا همان مسیریاب های شبکه بصورت پیشفرض بسته های اطلاعاتی Broadcast را از خود عبور نمی دهند و آنها را در اصطلاح فنی Drop می کنند.

به عبارت دیگر Router ها اجازه عبور ترافیک Broadcast از یک Segment از شبکه LAN شما به Segment دیگر را نمی دهند.

زمانیکه می خواهیم در خصوص مثالی درباره Broadcast صحبت کنیم من همیشه می گویم فرض کنید در یک سالن بزرگ فریاد می زنید: سعید صفایی...

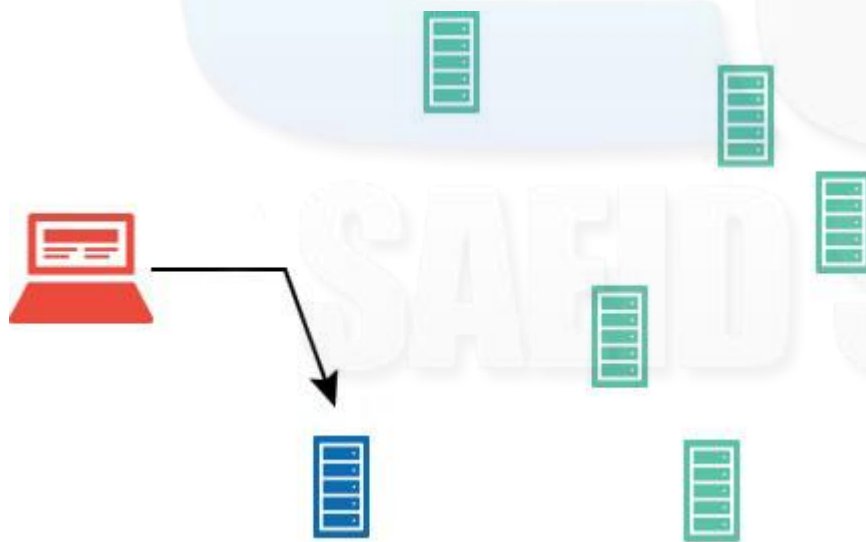
همه افراد سالن صدای شما را می شنوند ، در اینجا شخصی که فریاد زده است اطلاعات خود را Broadcast کرده است.

انواع روش های پخش اطلاعات در شبکه (معرفی ارتباطات موجود)

۴- روش Anycast یا هریابی:

در ساختار ارتباطات m به m به Anycast در اصطلاح ارتباط یک به نزدیکترین گفته می شود.

در واقع تمامی مواردی که تا کنون بررسی کردیم در مفاهیم مسیریابی مورد استفاده قرار می گیرند و Anycast هم به همین شکل است.



انواع روش های پخش اطلاعات در شبکه (معرفی ارتباطات موجود)

۴- روش Anycast یا هریابی:

Anycast در واقع یک تکنیک شبکه ای است که یک آدرس IP از مسیرهای مختلفی در شبکه قابل دستیابی می شود.

بر اساس الگوریتم های مسیریابی که در شبکه ها استفاده می شود تصمیم گیری می شود که درخواست کاربر از کدام مسیر بهتر است برود تا به مقصد مورد نظر برسد.

Anycast دارای یک سری مزایا می باشد ، مزیت اصلی این سرویس این است که کاربران همیشه به نزدیکترین سرویس در دسترس متصل خواهند شد چیزی که به عینه در ساختار DNS مشاهده می کنید.

انواع روش های پخش اطلاعات در شبکه (معرفی ارتباطات موجود)

۴- روش Anycast یا هریابی:

اینکار باعث کاهش زمان دسترسی به اطلاعات می شود و همچنین باعث ایجاد شدن Load Balancing در شبکه نیز می شود.

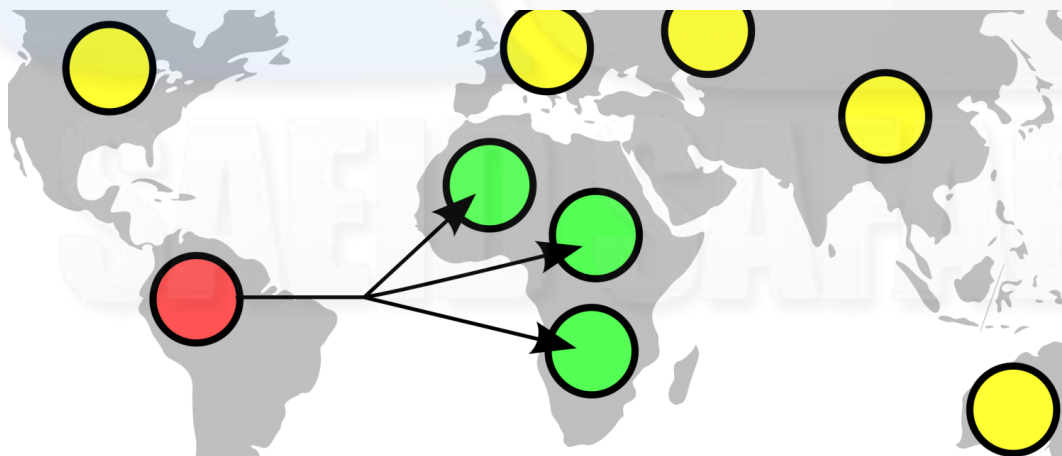
مزیت دوم این سرویس سادگی پیاده سازی آن است، شما بدون اینکه دغدغه محل قرارگرفتن سرور DNS خود را داشته باشید با استفاده فقط ای یک آدرس IP می توانید چندین سرویس DNS را دسترسی پیدا کنید.

انواع روش های پخش اطلاعات در شبکه (معرفی ارتباطات موجود)

۵- روش Geocast یا نشر جغرافیایی:

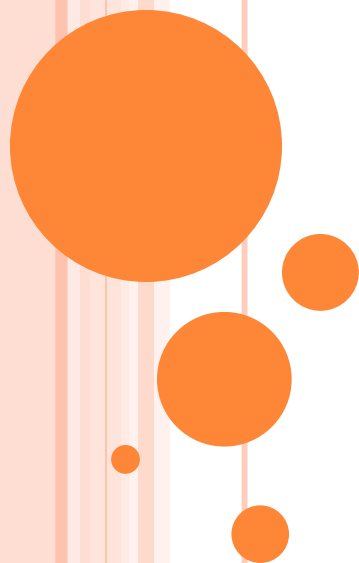
در واقع Geo مخفف کلمه Geography است و Geocast به ارسال اطلاعات به گروهی از شبکه های مقصد می باشد که با استفاده از موقعیت جغرافیایی شناسایی می شوند.

در واقع Geocast یک حالت ویژه از Multicast است که با استفاده از پروتکل های مسیریابی برای شبکه های موبایل و ad-hoc پیاده سازی می شود.



کانال های انتقال داده

Data Transfer Channels



کانال های انتقال داده در شبکه

انتقال داده یا **Data Transfer** یعنی اطلاعاتی که به روش ارتباطی از یک مکان به مکان دیگر منتقل می شوند.

به عنوان مثال برای این که یک صفحه وب سایت قابل مشاهده باشد باید تمام متن ها، تصاویر و سایر داده ها از طریق اینترنت به رایانه منتقل شوند.

لازم به ذکر است که ساده ترین روش **Data Transfer**، انتقال داده با وای فای می باشد.

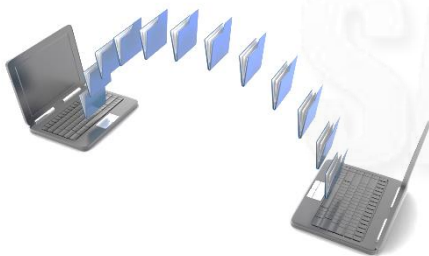


کانال های انتقال داده در شبکه

Data transfer فرایند استفاده از تکنیک ها و فناوری های محاسباتی برای انتقال داده های الکترونیکی یا آنالوگ از یک گره رایانه به دیگری می باشد.

داده ها به صورت بیت و بایت بر روی یک رسانه دیجیتال یا آنالوگ منتقل می شوند و این فرایند ارتباطات دیجیتال یا آنالوگ و حرکت آن بین دستگاه ها را امکان پذیر می کند.

اصولا Data Transfer دستگاه ها یا مؤلفه های موجود در دستگاه ها را قادر می سازد تا با یکدیگر صحبت کنند و ارتباط برقرار کنند.



کانال های انتقال داده در شبکه

شبکه انتقال داده ها

از قالب های مختلف ارتباطی برای انتقال داده بین یک یا چند گره استفاده می شود.

داده های منتقل شده ممکن است از هر نوع، اندازه و ماهیتی برخوردار باشند.

Data transfer های آنالوگ به طور معمول داده ها را به صورت سیگنال های آنالوگ ارسال می کنند، در حالی که انتقال داده های دیجیتال داده ها را به جریانهای بیت دیجیتال تبدیل می کنند.

به عنوان مثال ، Data transfer ها از یک سرور راه دور به رایانه محلی نوعی Data transfer های دیجیتال است.



Analog Signal



Digital Signal

حالت های انتقال در شبکه های کامپیوتری

روشی که در آن داده ها از یک دستگاه به دستگاه دیگر منتقل می شوند به عنوان حالت های انتقال در شبکه های کامپیوتری شناخته می شود.

حالت انتقال در لایه فیزیکی تعریف می شود و در سه دسته زیر طبقه بندی می شوند:

۱- **حالت ساده Simplex** : این کانالها فقط در یک جهت انتقال انجام می دهند.

۲- **نیمه دو طرفه Half-Duplex** : این کانالها امکان برقراری ارتباطات دو طرفه را امکان پذیر می کنند، اما سیستم های هر دو طرف اتصال باید به نوبت از طریق رسانه ارتباطی ارسال انجام دهند.

۳- **دو طرفه کامل Full-Duplex** : در این روش انتقال همزمان داده ها بین سیستم های متصل امکان پذیر است.

حالت های انتقال در شبکه های کامپیوتری

۱- حالت ساده Simplex :

در حالت Simplex ارتباط یک طرفه است، یعنی جریان داده یک طرفه است.

یک دستگاه می تواند داده ارسال کند ولی نمی تواند داده ای دریافت کند و یا می تواند داده دریافت کند ولی نمی تواند داده ای ارسال کند.

این نوع حالت انتقال چندان محبوب نیست زیرا در اکثر ارتباط ها لازم است تا داده ها به صورت دو طرفه تبادل شوند.

حالت Simplex در زمینه هایی که نیازی به دریافت پاسخ متناظر نیست استفاده می شود.

Simplex



حالت های انتقال در شبکه های کامپیوتری

۱- حالت ساده Simplex :

ایستگاه رادیویی در این حالت یک کانال ارتباطی ساده است که فقط به Listener ها پیام ارسال می کند اما اجازه دریافت پیام از طرف آن ها را نمی دهد.

مزایای حالت Simplex

در حالت Simplex، ایستگاه می تواند از کل پهنای باند کانال ارتباطی استفاده کند، به طوری که داده های بیشتری را می توان در یک زمان منتقل کرد.

معایب حالت Simplex

ارتباط یک طرفه است، بنابراین هیچ ارتباطی بین دستگاه ها وجود ندارد.

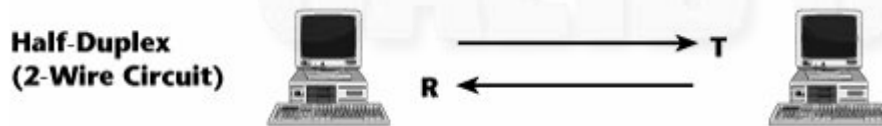
حالت های انتقال در شبکه های کامپیوتری

۲- نیمه دو طرفه Half-Duplex :

در حالت Half-Duplex جهت انتقال داده می تواند دو طرفه باشد. یعنی ایستگاه می تواند داده را ارسال و دریافت کند.

جریان انتقال داده در این حالت دو طرفه است اما نمی تواند همزمان باشد. کل پهنای باند کانال ارتباطی در یک جهت و در یک زمان مورد استفاده قرار می گیرد.

در حالت نیمه دوبلکس امکان تشخیص خطا وجود دارد و در صورت بروز هر گونه خطایی، گیرنده از فرستنده درخواست می کند تا دوباره داده را ارسال کند.



حالت های انتقال در شبکه های کامپیوتری

۲- نیمه دو طرفه Half-Duplex :

مزایای حالت Half-duplex

در حالت نیمه دوبلکس، هم دستگاه ها می توانند داده ها را ارسال و دریافت کنند و هم می توانند از کل پهنای باند کانال ارتباطی در حین انتقال داده استفاده کنند.

معایب حالت Half-duplex

نمی توان به صورت همزمان داده ارسال کرد

حالت های انتقال در شبکه های کامپیوتری

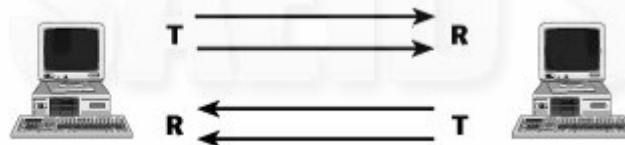
۳- دو طرفه کامل Full-Duplex :

در حالت Full-duplex ارتباط دو طرفه است و امکان ارسال و دریافت داده به صورت همزمان وجود دارد.

حالت Full-duplex از دو کانال Simplex تشکیل شده است که یکی ترافیک را به یک طرف انتقال می دهد و دیگری همان کار را در جهت مخالف انجام می دهد.

این حالت از نظر کارایی سریع ترین حالت انتقال در بین دستگاه ها است.

Full-Duplex
(4-Wire Circuit)



حالت های انتقال در شبکه های کامپیوتری

۳- دو طرفه کامل Full-Duplex :

برای نمونه در شبکه تلفن از این حالت انتقال داده استفاده می شود. زمانی که افراد با هم در ارتباط اند همزمان هم آن ها می توانند صحبت کنند و هم میتوانند گوش کنند.

مزایای حالت Full-duplex

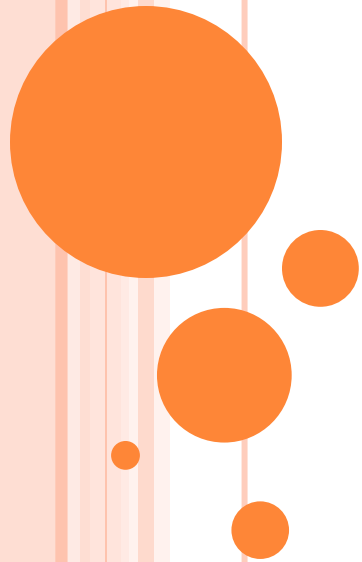
هر دو ایستگاه می توانند داده ها را به طور همزمان ارسال و دریافت کنند.

معایب حالت Full-duplex

اگر مسیر اختصاصی بین دستگاه ها وجود نداشته باشد، ظرفیت کانال ارتباطی به دو بخش تقسیم می شود.

آدرس مک، هاب و سویچ

Mac Address, Hub & Switch



آدرس فیزیکی شبکه MAC Address

هر دستگاهی که به شبکه متصل می‌شود، نه فقط برای اتصال و دسترسی، بلکه برای شناسایی در شبکه به شناسه‌ای نیاز دارد که آن را از دستگاه‌های دیگر متمایز کند.

مفهومی تحت عنوان آدرس فیزیکی یا Mac Address که مثل کد ملی یا اثر انگشت انسان، برای هر عضو شبکه متفاوت است.

آدرس MAC مخفف عبارت Media Access Control و یک آدرس فیزیکی کاملاً یونیک است که دستگاه‌های متصل به شبکه را از هم متمایز می‌کند.



آدرس فیزیکی شبکه MAC Address

برای درک بهتر مک آدرس، شبکه را مثل پارکینگ و آدرس مک را مثل پلاک خودروها در نظر بگیرید.

هرچقدر هم که پارکینگ پر شود، پلاک هیچ دو اتومبیلی مشابه نخواهد بود. این موضوع در مورد آدرس MAC هم صدق می‌کند. حتی اگر صدها دستگاه به یک شبکه متصل شوند، باز هم می‌توان دستگاه را با آدرس MAC پیدا کرد.

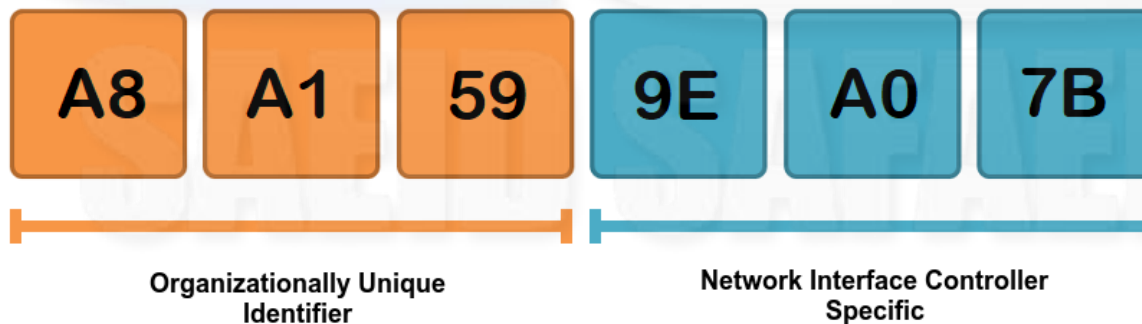
مک آدرس Media Access Control یک شناسه یکتا برای دستگاههای شبکه است که به هر دستگاه در شبکه تخصیص داده میشود. این آدرس برای شناسایی دستگاه در لایه دسترسی به شبکه استفاده شده و شامل یک مجموعه 48 بیتی از اعداد شناور است.

آدرس فیزیکی شبکه MAC Address

اولین ۳ بایت از MAC آدرس مربوط به سازنده دستگاه Vendor است و ۳ بایت دیگر مربوط به شناسه منحصر به فرد دستگاه است. از طریق مک آدرس، دستگاهها در شبکه تشخیص داده و بسته‌های دیتا به مقصد مورد نظر ارسال میشوند.

MAC

Media Access Control Address



آدرس فیزیکی شبکه MAC Address

با توجه به ۴۸ بیت و این که هر بیت می تواند دو حالت ۰ و ۱ باشد، در مجموع ۲ به توان ۴۸ دستگاه واسط شبکه را شماره گذاری می کند که برابر ۲۸۱۴۷۴۹۷۶۷۱۰۶۵۶ می باشد، یعنی چیزی حدود ۲۸۱ هزار میلیارد دستگاه.



مهمترین کاربردهای آدرس MAC

۱- شناسایی دستگاه ها در شبکه های محلی LAN:

در شبکه های اترنت، آدرس مک برای شناسایی و ارتباط بین دستگاهها استفاده می شود.

هر دستگاهی که به شبکه متصل می شود، با استفاده از آدرس مک خود می تواند داده ها را ارسال یا دریافت کند.

۲- فیلتر کردن دسترسی به شبکه (Mac Filtering):

مدیران شبکه می توانند با استفاده از آدرس مک، دسترسی دستگاههای خاصی را به شبکه محدود کنند.

این روش به افزایش امنیت شبکه کمک میکند.

جدول مک آدرس سوئیچ شبکه چیست؟

جدول مک آدرس یا همان جدول آدرس سوئیچ شبکه، یک جدول است که در سوئیچهای شبکه قرار دارد.

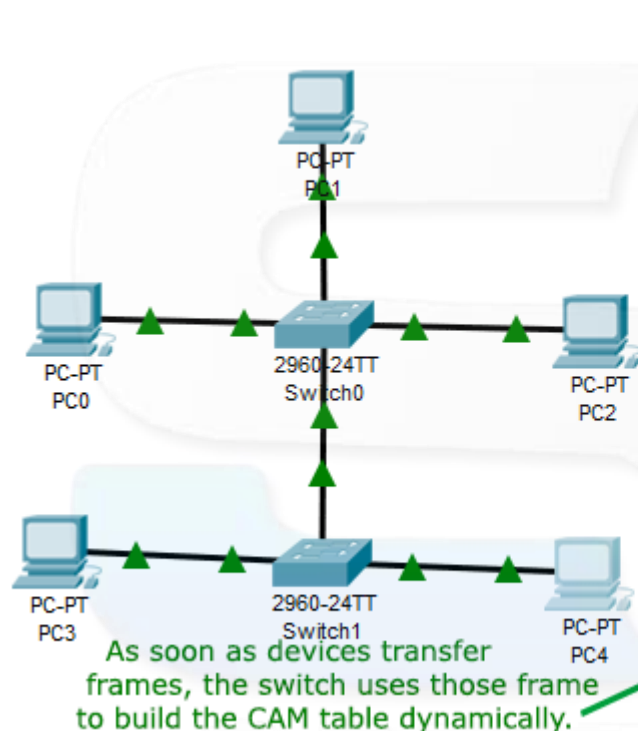
این جدول آدرسهای MAC دستگاههایی که به سوئیچ متصل هستند را به همراه پورتهایی که به آنها متصل شده اند ذخیره میکند.

وقتی یک بسته دیتا از یک دستگاه به سوئیچ میرسد، سوئیچ مشخص میکند که بسته باید به کدام پورت ارسال شود.

برای این کار، سوئیچ به جدول مک آدرس خود نگاه میکند و مشخص میکند که آیا آدرس MAC مقصد در جدول وجود دارد یا خیر.

اگر آدرس MAC در جدول وجود داشته باشد، سوئیچ بسته را به پورت مربوط به آن آدرس ارسال میکند؛ در غیر این صورت، بسته به تمام پورتها منتشر میشود (برای پیدا کردن دستگاه مقصد (پروتکل ARP)).

جدول مک آدرس سوئیچ شبکه چیست؟



changed state to up
When the switch starts, the CAM table is empty.

```
Switch>enable
Switch#show mac-address-table
      Mac Address Table
```

Vlan	Mac Address	Type	Ports
----	-----	-----	-----

```
Switch#show mac-address-table
      Mac Address Table
```

Vlan	Mac Address	Type	Ports
----	-----	-----	-----
1	0001.6462.12ce	DYNAMIC	Fa0/3
1	0001.c965.b519	DYNAMIC	Gig0/1
1	0007.ecdd.4128	DYNAMIC	Fa0/2
1	0060.3e7d.d194	DYNAMIC	Gig0/1
1	0090.2b22.9cc1	DYNAMIC	Gig0/1
1	00e0.8fad.629a	DYNAMIC	Fa0/1

Switch#



MAC Address

AA:AA:AA:AA:AA:AA

BB:BB:BB:BB:BB:BB

Switch Port

g1/0/1

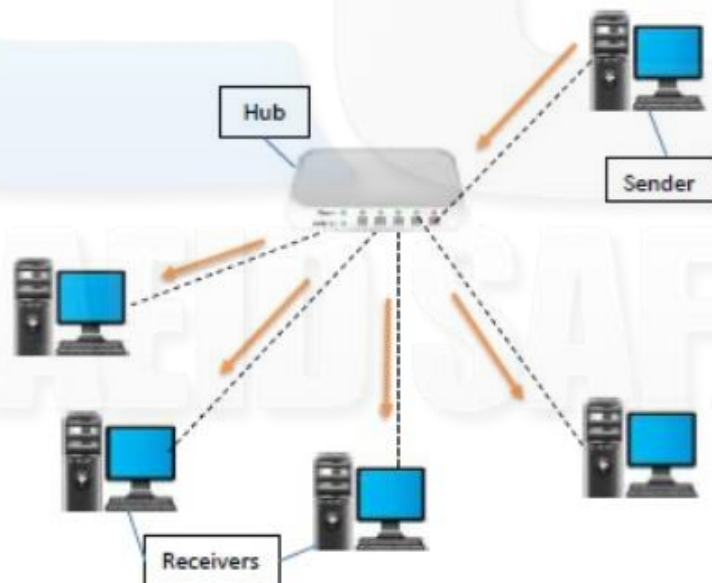
g1/0/27

هاب Hub :

هاب Hub در شبکه‌های کامپیوتری یک دستگاه است که برای اشتراک گذاری اطلاعات بین دستگاه‌های متصل به شبکه استفاده می‌شود.

هاب‌ها به عنوان تجهیزات فیزیکی در لایه فیزیکی مدل OSI قرار دارند.

وظیفه اصلی هاب، دریافت داده‌ها از یک دستگاه و ارسال آن به تمامی دستگاه‌های دیگر متصل به شبکه، بدون در نظر گرفتن آدرس مقصد است.



کاربرد های هاب Hub :

۱- اتصال دستگاهها

هابها برای اتصال دستگاههای مختلف به یکدیگر و ایجاد شبکههای کامپیوتری استفاده می شوند. این اتصالات می توانند شامل کامپیوترها، لپ تاپها، پرینترها، دوربینها و دستگاههای دیگر باشند.

۲- تقویت سیگنال

هابها توانایی تقویت سیگنالهایی که از دستگاهها دریافت می کنند را دارند. این ویژگی به جبران افت سیگنال در طول شبکه کمک می کند.

کاربرد های هاب Hub :

۳- آزمایش و تست شبکه

هاب‌ها برای انجام تست و آزمایش‌های شبکه به کار می‌روند. زمانی که نیاز به تست کابل‌ها یا اطمینان از اتصال دستگاه‌ها به یکدیگر وجود دارد، می‌توان از هاب شبکه استفاده کرد.

۴- سازگاری با شبکه‌های کوچک

در شبکه‌های کوچک و ساده، هاب‌ها به عنوان تجهیزات ارتباطی موثر عمل می‌کنند و می‌توانند به طور کامل نیازهای اتصال دستگاه‌ها را برطرف کنند.

کاربرد های هاب Hub :

۵- کاهش هزینه‌ها

در برخی مواقع، اگر نیاز به مدیریت پیچیده شبکه نباشد و ترافیک شبکه محدود باشد، استفاده از هاب ممکن است باعث کاهش هزینه‌های نصب و پیکربندی شبکه شود.

معایب هاب Hub :

۱- عدم تشخیص بهترین مسیر شبکه: هاب‌ها قادر به تشخیص و انتخاب بهترین مسیر برای انتقال داده‌ها نیستند و به صورت یکنواخت داده‌ها را به تمام دستگاه‌ها ارسال می‌کنند.

۲- عدم کار به صورت دوطرفه: اطلاعات در هاب‌ها به صورت یکطرفه انتقال پیدا می‌کنند و هر دستگاه فقط می‌تواند در یک زمان اطلاعات ارسالی را دریافت کند.

۳- عدم قابلیت فیلتر کردن اطلاعات: هاب‌ها قابلیت فیلتر کردن اطلاعات را ندارند و همه بسته‌های اطلاعات را به تمام دستگاه‌ها ارسال می‌کنند.

۴- عدم قابلیت اتصال به شبکه مختلف: هاب‌ها نمی‌توانند به معماری‌های شبکه‌های مختلف مانند اترنت، توکن، و رینگ به صورت اتوماتیک متصل شوند.

سویچ Switch:

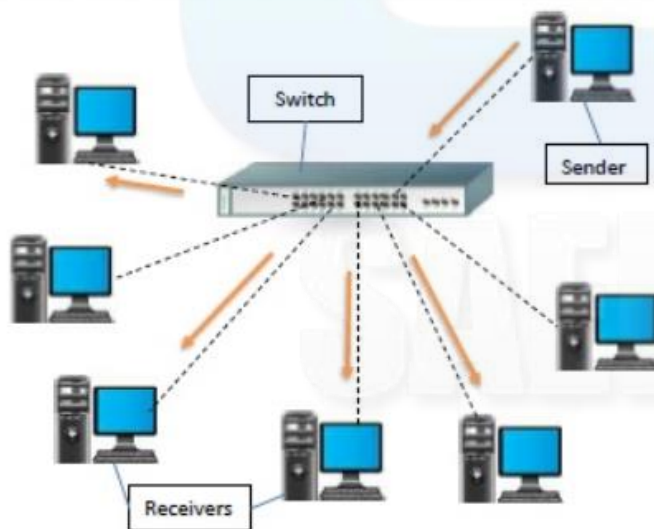
سوئیچ شبکه در مفهوم کلی، یک وسیله سخت‌افزاری است که چندین دستگاه را در یک شبکه متصل می‌کند.

این ابزار مهم در لایه پیوند داده مدل OSI، که وظیفه انتقال مطمئن داده‌ها بین دستگاه‌ها را در اختیار دارد، عمل می‌کند.

سوئیچ شبکه بسته‌های داده را از یک دستگاه دریافت کرده و آنها را به دستگاه مقصد ارسال می‌کند.

این فرآیند با بررسی آدرس MAC

مقصد هر بسته و ارسال آن به پورت مناسب انجام می‌شود.



Multicasting by a Switch

مزایای سویچ Switch:

۱- بهبود عملکرد شبکه: سوئیچ با ایجاد یک اتصال اختصاصی بین دستگاه‌ها، تراکم شبکه را کاهش داده و عملکرد کلی را بهبود می‌بخشد.

۲- امنیت پیشرفته: سوئیچ‌های شبکه ویژگی‌های امنیتی پیشرفته‌ای ارائه می‌دهند که باعث شده مدیران شبکه بتوانند دسترسی به منابع شبکه را کنترل کرده و از دسترسی غیرمجاز به داده‌ها شبکه جلوگیری کنند.

۳- مقیاس پذیری: سوئیچ‌های شبکه را می‌توان به راحتی برای افزودن دستگاه‌های اضافی با رشد شبکه گسترش داد و آنها را به یک راه حل مقیاس پذیر برای شبکه‌های کوچک و بزرگ تبدیل کرد.

تفاوت هاب و سوئیچ:

تفاوت سوئیچ با هاب به این صورت خواهد بود که هاب یک دستگاه ساده می باشد که همه ترافیک ورودی به خود را به تمام پورت هایی که دارد، ارسال می کند.

این جریان مقدار بسیار زیادی می باشد که می تواند باعث بروز مشکل در شبکه شود. ولی سوئیچ ها عملکردی متفاوت دارند.

در واقع سوئیچ اطلاعاتی را در مورد دستگاه های متصل شده به خود جمع آوری کرده و سپس ترافیک های ورودی را به کمک پورت های مرتبط با آن، هدایت می کند.

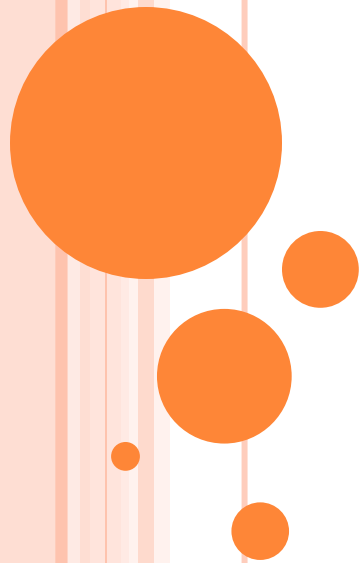


تفاوت هاب و سویچ: Comparison of Hub & Switch

Sr No	Hub	Switch
1	It is a broadcast device.	It is a point to point device.
2	It operates at physical layer.	It operates at datalink layer.
3	It is not an intelligent device.	It is an intelligent device.
4	It simply broadcasts the incoming packet.	It uses switching table to find the correct destination.
5	It cannot be used as a repeater.	It can be used as a repeater.
6	Not a sophisticated device.	It is a sophisticated device.
7	Not very costly.	Costly.

پروتکل ARP

Address Resolution Protocol



تعریف کلی و گذرا از پروتکل

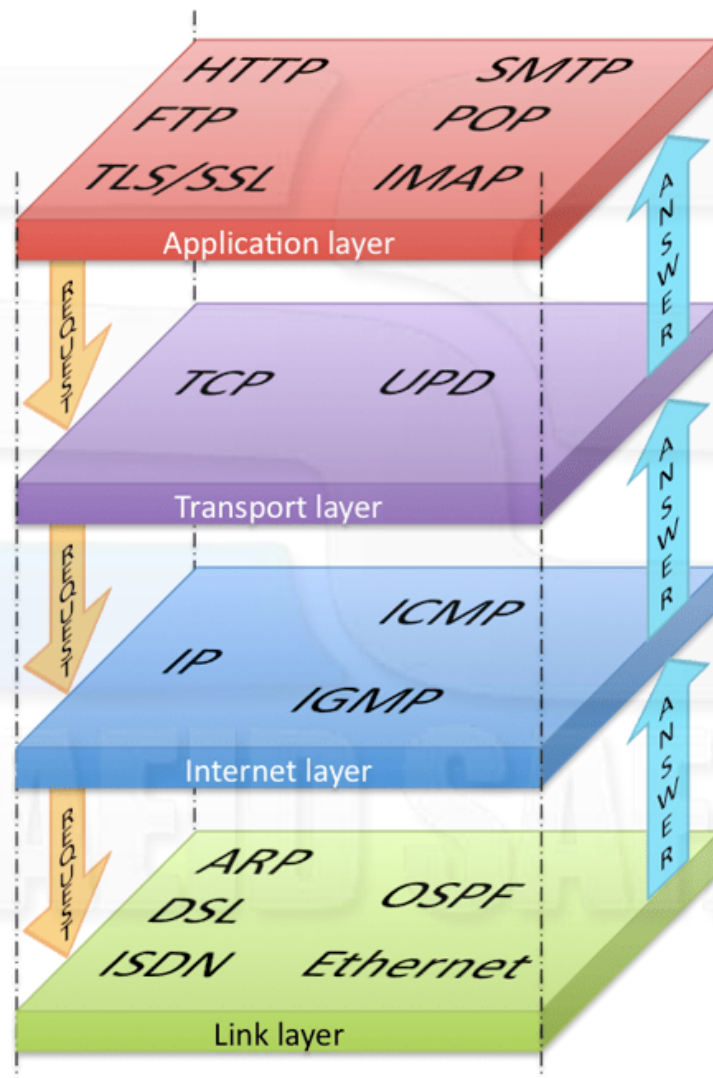
پروتکل یعنی مجموعه ای استاندارد از قوانین که به دستگاه های الکترونیکی امکان برقراری ارتباط با یکدیگر را می دهد.

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.

در تبادل داده ها، دستگاه ها براساس قوانین مشخص شده Protocol داده هایشان را به بسته های کوچک تر تقسیم و آن ها را به صورت سریالی یا موازی ارسال می کنند.

هنگام دریافت، دستگاه مقصد داده ها را با استفاده از فرمت های مشخص شده پروتکل تجزیه و تحلیل و آن ها را بازسازی می کند.

انواع پروتکل های پر کاربرد شبکه



تعریف پروتکل ARP (در جستجوی آدرس فیزیکی در شبکه)

Address Resolution Protocol به اختصار ARP یک پروتکل بسیار مهم در شبکه های کامپیوتری است.

وقتی سیستم شخصی می خواهد پیامی را از طریق شبکه ارسال کند، باید داده ها را در لایه های مدل OSI + Open Systems Interconnection قرار دهد.

در هر لایه، باید تمام اطلاعات header مانند پورت های TCP/UDP در header لایه ۴، آدرس و آدرس IP مقصد در سربرگ لایه ۳ و آدرس های MAC مبدا و مقصد را در سربرگ لایه ۲ پر کند.

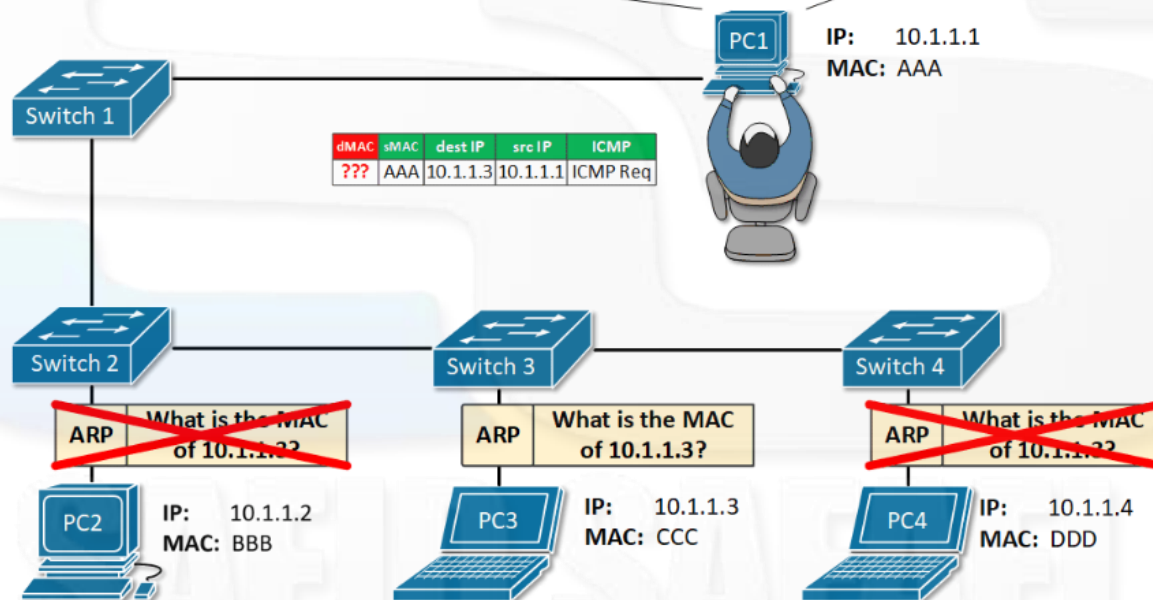
اگر خوب فکر کنید، همه این اطلاعات به جز آدرس MAC مقصد در دسترس کاربر نهایی است.

پروتکل ARP برای تبدیل یک آدرس MAC بر اساس آدرس IP داده شده در یک شبکه محلی معرفی شده است.

مثال پروتکل ARP

Only **PC3** accepts
the ARP request
as it has 10.1.1.3

```
Command Prompt
C:\> ping 10.1.1.3
Pinging 10.1.1.3 with 32 bytes of data:
```



لینک نمایش مثال پروتکل ARP

پروتکل ARP چگونه کار می کند؟

همانطور که در مبحث سویچ ها بحث شد، سویچ ها در لایه ۲ و با Mac کار میکنند.

البته یک سری سویچ هایی هستند که با IP و در لایه ۳ کار میکنند اما جهت دانستن عملکرد پروتکل ARP نظر ما بر روی سویچ های لایه ۲ می باشد و در ادامه مباحث به طور مفصل در رابطه با لایه ها بحث خواهیم کرد.

ARP از ارتباط پخش (یک به همه) Broadcast استفاده می کند تا از تمام کلاینت های نهایی در یک LAN بپرسد که آدرس فیزیکی یک IP مشخص چیست.

پروتکل ARP چگونه کار می کند؟

در مثال قبل، PC1 سعی می کند PC3 را که در همان شبکه محلی و همان زیر شبکه ۱۰.۱.۱.۰/۲۴ قرار دارد، پینگ کند.

هنگامی که کاربر دستور ping 10.1.1.3 را اجرا می کند، PC1 قبل از ارسال آن به شبکه شروع به کپسوله کردن درخواست (ping) ICMP در یک فریم اترنت می کند.



dMAC	sMAC	dest IP	src IP	ICMP
???	AAA	10.1.1.3	10.1.1.1	ICMP Req

چنانچه در آینده خواهیم خواند پروتکل ICMP

یک پروتکل از نوع Echo Request می باشد یعنی در قبال هر درخواست یا Request منتظر پاسخ یا Response می باشد. (برای هر درخواست انتظار جواب دارد)

حال دستور Ping از این نوع پروتکل استفاده میکند.

IP و Mac دستگاه فرستنده و IP دستگاه گیرنده معلوم است اما Mac گیرنده نا مشخص است. اینجاست که پروتکل ARP به کار می آید.

پیام های ARP

دو نوع اصلی بسته در عملیات پروتکل ARP وجود دارد:

۱- درخواست ARP

۲- پاسخ ARP

چهار قسمت در سربرگ ARP وجود دارد:

۱- آدرس سخت افزار منبع MAC

۲- آدرس پروتکل منبع IP

۳- آدرس سخت افزار هدف MAC

۴- آدرس پروتکل هدف IP

ARP Request

Ethernet II Frame

Src: AAAA-AAAA-AAAA

Dst: FFFF-FFFF-FFFF

Address Resolution Protocol (request)

Sender MAC: AAAA-AAAA-AAAA

Sender IP: 10.1.1.1

Target MAC: 0000-0000-0000

Target IP: 10.1.1.3

ARP Reply

Ethernet II Frame

Src: CCCC-CCCC-CCCC

Dst: AAAA-AAAA-AAAA

Address Resolution Protocol (request)

Sender MAC: CCCC-CCCC-CCCC

Sender IP: 10.1.1.3

Target MAC: AAAA-AAAA-AAAA

Target IP: 10.1.1.1

پروتکل ARP چگونه کار می کند؟

در پیام ARP Request آدرس MAC مقصد آدرس broadcast معروف FFFF-FFFF-FFFF است.

این به سوئیچ های LAN نشان می دهد که این ارتباط ارتباطی broadcast شده است و همه دستگاه های متصل در LAN باید یک کپی از فریم را دریافت و پردازش کنند.

مقدار مهم دیگر که باید به آن توجه کنید:

Target MAC 0000-0000-0000 است.

این به صاحب IP Target نشان می دهد که فرستنده در تلاش است آدرس فیزیکی این IP را مشخص کند.

توجه داشته باشید که در پیامهای ARP Reply آدرسهای MAC مبدا و مقصد، آدرسهای unicast هستند.

پروتکل ARP چگونه کار می کند؟

یک درخواست ARP در یک broadcast frame قرار می گیرد.

بنابراین این ارتباط یک به چند است و هر میزبان در LAN یک نسخه از درخواست ARP را دریافت می کند.

اما فقط مالک IP هدف پاسخ می دهد.

پاسخ ARP در یک قاب unicast است.

بنابراین این یک ارتباط یک به یک بین درخواست کننده و ارسال کننده است.

هنگامی که دستگاه آدرس فیزیکی IP را دریافت می کند، یک ورودی در ARP Table خود ARP Cache ایجاد می کند.

هر ارتباط بعدی از ورودی ذخیره شده استفاده می کند.

هر ورودی در جدول ARP به طور پیش فرض ۴ ساعت نگه داشته می شود.
به این ARP Timeout گفته می شود.



با تشکر از همراهی شما

محمد سعید صفایی صادق

