



جزوه : Network+

مدرس : مهندس رجایی

گردآورنده : یاسمن هادوی

آموزشگاه مهندسی کندو پیشرو در ارائه آموزشهای شبکه، امنیت شبکه

سیسکو ، مایکروسافت ، لینوکس ، میکروتیک ، برنامه نویسی و ...

تلفن : 021 43810 و 021 66176517

www.CanDo.ac

[Telegram.me/CanDo_ac](https://t.me/CanDo_ac)

[Instagram.com/CanDo.ac](https://www.instagram.com/CanDo.ac)

[Facebook.com/www.CanDo.ac](https://www.facebook.com/www.CanDo.ac)

مقدمه

اولین بار در زمان جنگ جهانی دوم که روسیه در حال موشک فرستادن بود و خیلی پیشرفت کرده بود آمریکا گفت یک کاری کنیم که بتوانیم در سطح اطلاعاتی ارتباطات بهتری داشته باشیم، اولین بار پروژه شبکه یک پروژه نظامی و امنیتی بود که در DOD¹ (وزارت دفاع آمریکا) شکل گرفت. برای اینکه خودشان را از لحاظ ارتباطی ارتقا بدهند این پروژه را در سطح اطلاعاتی به دانشگاه MIT که بهترین و برجسته ترین دانشگاه آمریکاست دادند، این دانشگاه شبکه را روی این پروژه که ARPA² نام داشت تحقیق و بررسی کرد و توانست یک بسته ای که بتواند جابجا شود را بوجود آورد (منظور از بسته یک سیگنال الکترونیکی است که از یک طرف کابل به طرف دیگر کابل منتقل می شود). در نتیجه شبکه به وجود آمد اما در حوزه نظامی و اطلاعاتی بود و به صورت محرمانه، وقتی این پروژه از حالت نظامی و اطلاعاتی خارج شد سه تا شرکت بودند به نام های Xerox³, Dec³, Intel آمدند دانش شبکه را گرفتند و گسترش دادند مخصوصاً شرکت Xerox که آزمایشگاه پیشرفته ای برای تحقیقات علمی داشت، این سه شرکت توانستند شبکه را به آن شکلی که ما امروزه می شناسیم بوجود بیاورند اسم آن چیزی که بوجود آوردند را گذاشتند Ethernet.

¹Department of Defense

² Advanced Research Projects Agency

³Digital Equipment Corporation

DOD وقتی شبکه را شکل داد با یک قانونی صحبت می کرد فعلاً به آن قانون DOD می گوییم که وقتی بخواهیم در یک شبکه send و receive داشته باشیم یک قانونی برایش بگذاریم، این سه شرکت نیاز به یک قانون داشتند، چون هر کدام قانون خودشان را می گفتند و نمی توانستند با هم سازگاری داشته باشند نیاز بود که این سه شرکت بیایند و یک حرف مشترک بزنند از آنجاییکه باهم تفاهم نداشتند از شرکت ISO که کارش ساختن استاندارد است خواستند یک قانون مشترک تعریف کند این شرکت یک مدلی تعریف کرد به نام مدل استاندارد OSI⁴.

* دیدی که از OSI باید داشته باشیم خیلی مهم است اگر OSI را فهمیدیم می توانیم Network کار خوبی شویم اگر این قسمت را نفهمیم در زمینه Network هیچی نمی شویم!

تقسیم بندی شبکه از لحاظ وسعت یا Scale:

¹LAN, ²WAN: در دنیای امروزی فقط همین ۲ نوع را مورد استفاده قرار می دهیم.

اگر شبکه وسعت کمی داشت مثلاً در حد وسعت کلاس میتواند LAN باشد اگر یک سرتهران به سردیگر آن وصل باشد لزوماً شبکه WAN نیست باز هم می تواند LAN باشد چون

⁴ Open System Interconnection

⁵ Wide area Network

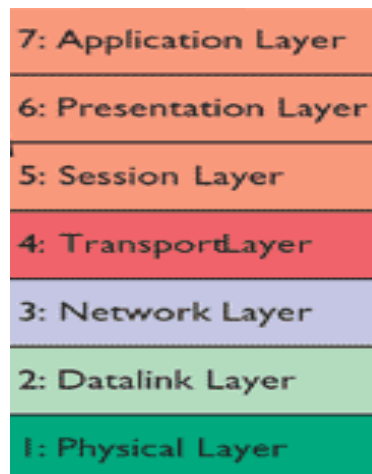
⁶ Local area Network

ممکن است ما یک لینک wireless داشته باشیم و قادر باشیم دو سر تهران را بهم وصل کنیم! (در ادامه خواهیم فهمید به چه صورت) اگر شبکه داخلی را در حوزه مخابرات ببریم و از ارتباطاتی استفاده کنیم که بسته از یک دستگاه ارتباطی خاصی رد شود می شود شبکه WAN.

امروزه ممکن است یک شبکه محلی LAN داشته باشیم که از یک طرف تهران وصل باشد به طرف دیگر تهران و ممکن است از یک طرف خیابان به طرف دیگر خیابان وصل شویم اما شبکه مان WAN باشد.

Topology

به چگونگی قرارگیری سیستم ها در شبکه و نحوه اتصال آنها به هم را توپولوژی شبکه می گویند، مدل OSI شامل ۷ لایه است که شبکه در قالب این ۷ لایه کار می کند.



- حالا این مدل یعنی چی؟ اصلاً این مدل کجاست؟ اگر شبکه در قالب این لایه ها کار می کند پس چرا ما تو کامپیوتر ندیدیمش؟

جواب: فرض کنید نشستید پشت کامپیوترتان و در **Browser** کامپیوتر خود وارد می کنید

www.Google.com اتفاقات زیادی پس از زدن این فرمان رخ می دهد تا این سایت برایمان باز شود، ما به عنوان یک کاربر می گوییم که چه می خواهیم ، کامپیوتر و سیستم های شبکه موظفند بگویند برای خواسته ما چه چیزی لازم است، این آدرسی که وارد می کنیم لازمه اما کافی نیست! باید به کفایت برسد تا در دنیای شبکه بتواند راه خود را طی کند و به **Google** برسد و برای ما جواب برگرداند پس اگر وظایف موجود در لایه ها در شبکه نباشد این بسته به جایی نمی رسد یعنی : ما این آدرس www.Google.com را در

بالاترین لایه شبکه یعنی **Application** قرار می دهیم این بسته باید طبقه طبقه راه خودش را طی کند و به پایین بیاید در هر لایه توقف کند و یه سری چیز بهش اضافه شود که این کار ساده ای نیست. آخرش می رسد به لایه **physical** . ما این لایه رو غالباً به صورت یک سیم دیدیم که به پشت کامپیوترمان وصله و از آن بیرون آمده (این تعریف درستی نیست اما فعلاً تصور کنید!) یا یک چیزی پشت کامپیوترمان هست که امواج را می فرستد به یک دستگاهی که در خانه مان هست، منظور این است که ما در اینجا **media** یا **carrier** (حامل، حامل بسته ای که از لایه **application** فرستادیم و می خواهد وارد سیم شود) داریم، ما که نمی توانیم www.Google.com را وارد سیم کنیم چون سیم فقط سیگنال

الکترونیکی را می فهمد، لایه ها صفر و یک (باینری) می فهمند توی لایه physical باید کاری کنیم که صفر و یک تبدیل به سیگنال شده و وارد media شود به این تبدیل که در لایه physical انجام می شود مدولاسیون می گویند. ما در کامپیوتر خود احتیاج به یک قطعه داریم که ما را وصل کند به media .

اگر پشت کامپیوترمان را دقت کنیم یک سیم پشت case می بینیم که بیرون آمده ، به آن قطعه ای که این سیم از آن بیرون آمده و داخل کامپیوتر هست را کارت شبکه میگویند، حالا اگر سیم بهش وصل باشد می گویند LAN Card و اگر بی سیم بود می گویند Wireless LAN Card یا WLAN .

پس این قطعه ای که داخل کامپیوترمان هست و با آن وصل به media می شویم و کار مدولاسیون را انجام می دهد می گوئیم NIC⁷ (مودم، LAN Card ، WLAN Card و ... نوعی NIC هستند، یعنی interface ی که می خواهد به Network وصل شود).

پس ما در هر کامپیوتر برای اینکه بتوانیم پا به دنیای شبکه بگذاریم احتیاج به یک NIC داریم که بتواند صفر و یک را به سیگنال تبدیل کرده و وارد media کند.

پس تا اینجا فهمیدیم که وظیفه لایه physical تبدیل بیت به سیگنال و سیگنال به بیت است.

⁷NetworkInterface Card

Media ها می توانند شکل های مختلف داشته باشند :

مثال: طبق شکل زیر فرض کنیم ما در خانه خود نشستیم و با WLAN Card وصل

هستیم به مودم ، مودم ما از طریق خط تلفن به مخابرات محله مان وصل است آن کسی که برای ما اینترنت را محیا میکند و بهش می گویند ⁸ISP در مخابرات محله برای خودش یک دستگاهی دارد (البته اگر مستقیماً از خود مخابرات اینترنت نگرفته باشیم) مثلاً فرض می

کنیم از شاتل اینترنت گرفتیم، از طریق لینک wireless به شاتل وصل هست و شاتل هم

به زیرساخت مخابرات کشور از طریق فیبرنوری وصل است و بعد از آن باز از طریق فیبرنوری

به دبی می رسد، از آنجا به بعد اطلاعات VSAT ی شده و به ماهواره رفته و بعد پایین می

آید، پس ما می بینیم با زدن یک دستور www.Google.com در داخل کشور این همه

اتفاق برای بسته اطلاعاتی افتاد، می بینیم که media دائم در حال تغییر کردن است اول

media امواج رادیویی بود بعد سیگنال الکترونیکی شد(چون داخل سیم مسی است) بعد

دوباره شد ماکروویو (رادیو) بعد از آن شد نور دوباره نور و بعد امواج ماهواره ای، پس ما می

توانیم دنیای اینترنت را اصطلاحاً Mixed of Media (ترکیب media های مختلف)

بنامیم .

⁸Internet Service Provider



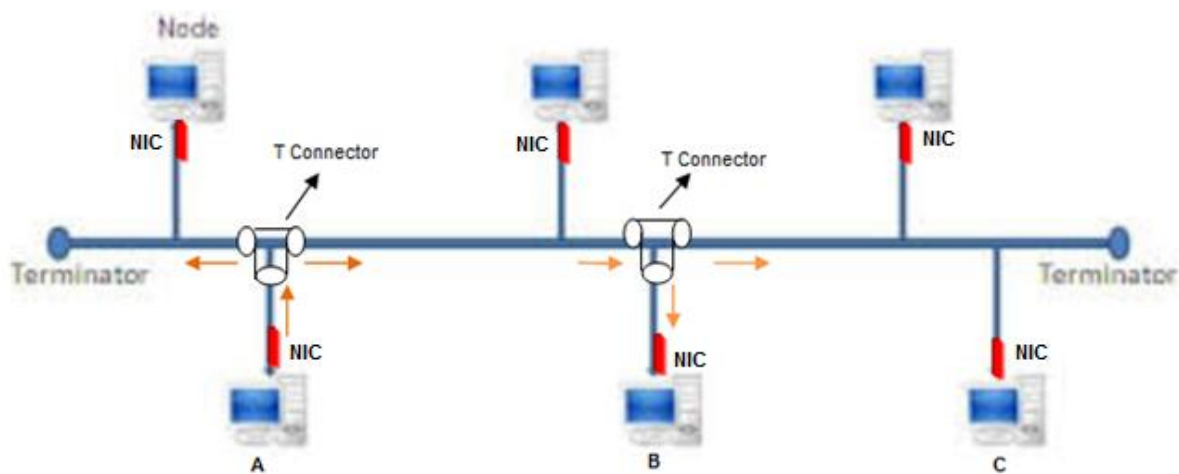
× منظور از نور سیگنالینگ نور است.

گاهی می گویند LAN Card بصورت Onboard است یعنی Motherboard

بصورت already روی خودش LAN Card را دارد حالا اگر نداشت می توانیم اضافه

کنیم. پس فهمیدیم Media داخل کارت شبکه می رود و تغییرات زیادی می کند اولین

شبکه هایی که از نظر توپولوژی بوجود آمدند شبکه های Bus بودند به شکل زیر :



- media شکل نشان داده شده کابل Coaxial است. (این کابل را در جاهایی مثل پشت

بام خانه مان دیدیم که بصورت یک سیم رفته به یک بشقاب گرد وصل شده است، همچنین

در دوربین های مدار بسته که به روش آنالوگ set می شوند)

- Terminator ها جمع کننده ولتاژ در ابتدا و انتهای کابل هستند.

طبق شکل اگر قصد داشته باشیم از سیستم A بسته ای را به سیستم C ارسال کنیم باید

داده خود را به صورت سیگنالینگ وارد سیم کنیم مشکل اینجاست که پایانه هایی که ولتاژ یا

بسته به آنها تعلق ندارد ممکن است بسته را بردارند.

ما سیم Coaxial دو نوع داریم: << 10Base2 , 10Base5 به پهنای باند

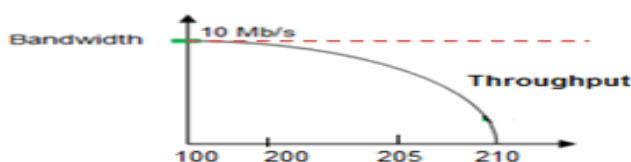
10Mb/s اصطلاحاً Ethernet گفته می شود، و به 100Mb/s می گویند Fast

Ethernet و به 1000Mb/s می گویند Gigabit Ethernet .

منظور از Ethernet شبکه ای است که روی سیم مسی واقع شده است.

در 10Base 2 عدد ۲ همان طول کابل است که هر چقدر طول کابل بیشتر باشد افت ولتاژ

بیشتر می شود، مطابق نمودار زیر:



تعریف **Throughput** و **Bandwidth** :

Bandwidth یا پهنای باند رابطه مستقیمی با **media** مصرفی دارد به طور مثال می تواند **10Mb/s** را از خود عبور دهد اما این ربط مستقیمی به قدرت و لتاژ موجود درون **media** دارد که می تواند در اثر زیاد شدن مسافت **media** کاهش یابد به میزان استفاده و لتاژ از **Bandwidth**، **Throughput** گفته می شود .

- برای اینکه بتوانیم **10Base2** و **10Base5** را به کابل وصل کنیم نیاز به یک **Connector** داریم که به کارت شبکه وصل شود، کانکتور **10Base2** را **Connector BNC** و کانکتور **10Base5** را **Connector Vampire Tap** می گویند.
- به **10Base2** اصطلاحاً **thinnet** و به **10Base5** اصطلاحاً **thicknet** می گویند.

تصادف یا **Collision** در شبکه :

در شبکه های **Bus** تصادف اتفاق می افتد چون کلاً یک **media** داریم و آن **media** یک رشته فلزی دارد که همه سیستم ها از همان رشته برای ارسال بسته استفاده می کنند. در این **media** اصطلاحاً گفته می شود **Collision** برای همه **share** است.

توپولوژی Bus خوب نیست و با این توپولوژی نمی توانیم کاری بکنیم که Collision نداشته باشیم تنها کاری که می توانیم بکنیم این است که بیاییم media را مدیریت کنیم یک قانون می گذاریم به نام CSMA/CD⁹ (حس کن media را برای درخواست های چندگانه جهت تشخیص Collision)

مراحل تشخیص تصادف با استفاده از CSMA/CD

(۱) Listening

(۲) Jam Signal

(۳) Random Time

CSMA/CD سه مرحله دارد مرحله اول Listening به منزله این است که سیستم وسیله NIC خود به ولتاژ موجود در media گوش کند طبق این قانون اگر ولتاژی در شبکه حس نشد سیستم مجوز آن را در شبکه پیدا می کند که بسته خود را بفرستد اما احتمال Listening همزمان و ارسال همزمان وجود دارد در این صورت در شبکه Collision ایجاد می شود و سیستمی که از همه زودتر متوجه آن می شود اقدام به انتشار Jam Signal می کند این سیگنال برای تمامی سیستم ها Collision را بازگو می کند و از میان تمام سیستم ها آن دسته از سیستم هایی که اقدام به انتشار سیگنال

⁹Carrier Sense Multiple Access With Collision Detection

همزمان نموده اند موظفند پس از گذشت مرحله سوم و گرفتن یک **RandomTime** آخرین بسته خود را مجدد ارسال کند با این روش **Collision** از بین نمی رود تنها احتمال آن کم می شود.

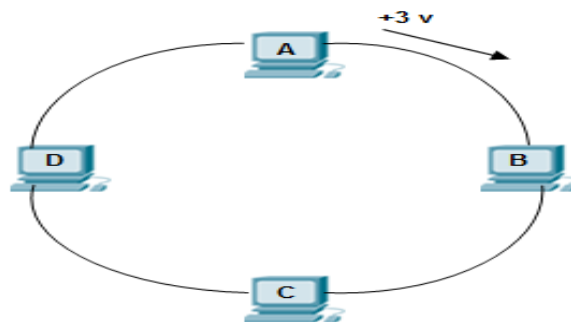
در شبکه های امروزی این مراحل از بین رفته اما در اثر پیاده سازی اشتباه ممکن است پیش بیاید.

اشکالات شبکه Bus :

- اگر Terminator از بین برود کل شبکه مختل می شود.
 - اگر قسمتی از کابل خراب شود کل شبکه مختل می شود.
 - اگر سیگنالی توسط یک سیستم برای سیستم دیگر بخواهد ارسال شود به جز آن سیستمی که طالب بسته است تمام سیستم ها در جریان قرار می گیرند و ممکن است به اشتباه بسته را دریافت کنند.
 - وجود Delay هست که در اثر Collision می تواند رخ بدهد.
- پس دیدیم که این توپولوژی مناسب نبود و رفتیم سراغ توپولوژی بعدی:

توپولوژی Ring

در این روش Terminator را حذف کردند در اینجا media همان Coaxial است در این شبکه یک ولتاژی می چرخد و به همه سیستم ها می رسد مثلاً ولتاژ +۳۷ ، اولین سیستمی که در شبکه روشن شود این ولتاژ را generate می کند این ولتاژ بصورت already در شبکه وجود دارد در شبکه Bus نبودن ولتاژ به معنی خالی بودن شبکه بود اما در این شبکه بودن +۳۷ به معنی خالی بودن شبکه است ، فرض کنیم طبق شکل سیستم B می خواهد به سیستم D بسته بفرستد نمی تواند این کار را بکند تا زمانی که Token به دستش برسد یا ولتاژ +۳۷ را ببیند و بداند که شبکه خالی است که اصطلاحاً می گویند Token خالی است.



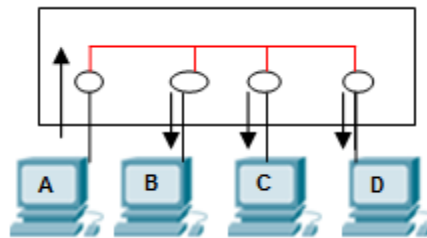
وقتی که Token به دستش رسید ولتاژ خودش را القا می کند مثلاً +۵۷ این ولتاژ از سیستم B حرکت کرده در جهت عقربه های ساعت به دست سیستم C می رسد می بیند بسته مال خودش نیست بر نمی دارد دست سیستم D می رسد از روی آدرس های بسته

می فهمد بسته مال خودش است بسته را بر می دارد بعد ولتاژ می رسد دست سیستم A می بیند ولتاژی غیر از ۳۷+ است پس بسته را بر نمی‌دارد بسته می رسد باز دست آن سیستمی که القای ولتاژ کرده یعنی سیستم B خودش، بارش را از روی شبکه بر می‌دارد، پس همه سیستم‌ها باید منتظر باشند که Token خالی باشد تا بتوانند بسته خودشان را بفرستند در اینجا برای مدیریت Collision دیگر CSMA/CD نداریم بلکه Token Passing داریم.

× در این روش Terminator را چگونه از بین بردیم؟

به این صورت که هر ایستگاه که ولتاژ خود را القا می‌کند همان ایستگاه دوباره ولتاژ خودش را جمع می‌کند، در این شبکه هم مانند Bus اگر یک جای کابل خراب شود کل شبکه مختل می‌شود.

: Hub



یک سری NIC بر رویش هست که مداری داخلش آمده اینها را به هم دیگر وصل کرده است که می شود توپولوژی Bus بعد اینها وصل می شوند به سیستم ها فایدهش این است که Terminator داخل Hub است و دیگر روی شبکه رها نیست و دیگر اینکه خود Hub، Repeater است یعنی سیگنال را می گیرد تقویت می کند و بیرون می دهد به توپولوژی که سیستم ها به یک دستگاه متمرکز وصل شدند و امروزه معروف ترین توپولوژی حال حاضر است Star گفته می شود این شکل به صورت Physical (چشم ما این طوری می بیند)، Star است اما به صورت Logical (منطقی)، Bus است.

عملکرد Hub :

مطابق شکل نشان داده شده در بالا اگر ایستگاه A بخواهد بسته ای را به ایستگاه B بفرستد Hub بسته را از ایستگاه A گرفته به همه ایستگاههای موجود می فرستد، بسته مربوط به هر ایستگاهی بود بر میدارد دوباره از طریق Hub جواب بسته را به مبدا بر می گرداند.

سوال : ارتباطات بی سیم با بی سیم بصورت ۲ طرفه است اما غیرهمزمان؛ چه کار کنیم که به ارتباط دوطرفه همزمان مانند تلفن برسیم؟

جواب : باید به جای اینکه یک رشته داشته باشیم ، ۴ رشته داشته باشیم به این صورت که

۲ تا از آنها را مسئول ارسال و ۲ تا را مسئول دریافت کنیم پس media شبکه دیگر نباید

Coaxial باشد در نتیجه Category ها بوجود آمدند و ما آنها را به عنوان Cat-1، Cat-2، Cat-3 و ... می شناسیم.

Cat-5 هم نوع 4 Pair (۸ رشته) دارد و هم 2 pair.

Cat-5 نوع 4 pair به صورت ۴ زوج به هم تابیده است به همین دلیل به آن می گویند twisted pair.

رنگ هایشان هم به صورت استاندارد است.

علت تاباندن این سیم ها این است که یک حریمی را ایجاد می کند که القای بار جانبی را کم کند (نویز نباید داشته باشیم) چون ممکن است در اثر این القای ولتاژ یک بیسی از صفر یک شود و برعکس، این تاباندن باعث می شود که این مسئله کمتر اتفاق بیفتد.

کابل های Category ۳، نوع دارند: (۱) UTP^{۱۰} (۲) STP^{۱۱} (۳) FTP^{۱۲}

(۱) UTP: کابلی که یه سری رشته وسطش هست و هیچ چیز دیگری ندارد.

(۲) STP: یک رشته فلزی دارد که گیرنده نویز است.

(۳) FTP: یک رشته فویل مانند است که مقاومتش کابل را در مواقع آتش سوزی بالا

می برد و گیرنده نویز هم هست و ...

¹⁰Unshielded Twisted Pair

¹¹Shielded Twisted Pair

¹²Foiled Twisted Pair

حالا ممکن است یک کابلی ۲ نوع از این استاندارد ها را داشته باشد مثلاً SFTP باشد هرکدام بنا به جای استفاده می تواند کاربرد داشته باشد

کابل	پهنای باند	سوکت	
Cat-5	→ 100 mbit/ps	→ RJ45	} 4 Pair
Cat-5e	→ 1000 mbit/ps	→ RJ45	
Cat-6	→ 1000 mbit/ps	→ RJ45	
Cat-6A	→ 10 Gigbit/ps	→ RJ45	

- همه این ها سوکت RJ45 می خورند اما اگر خواستیم به بازار برویم و برای خودمان

سوکت RJ45 بخریم باید حتماً بگوییم که RJ45 برای چه کابلی می خواهیم مثلاً برای

Cat-5 یا Cat-6 یا ... می خواهیم.

- تفاوت Cat-6 و Cat-5e در طول کابل و کیفیتشان است.

- در تلفن خانه از سوکت RJ11 استفاده می شود.

کامپیوتر ما باید شامل NIC باشد که این NIC دارای ۸ رشته است بین ۲ سیستم A , B

بین NIC ها اگر خواهیم دو سیستم را شبکه کنیم نیاز به media است.

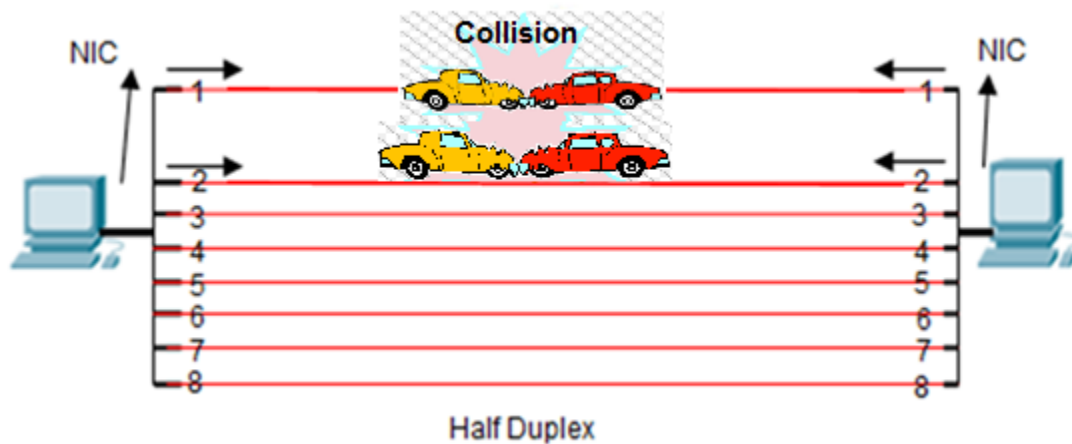
برای شبکه کردن ۲ سیستم به ۲ Step کلی نیاز است :

(۱) برقراری بستر (۲) Set کردن logic

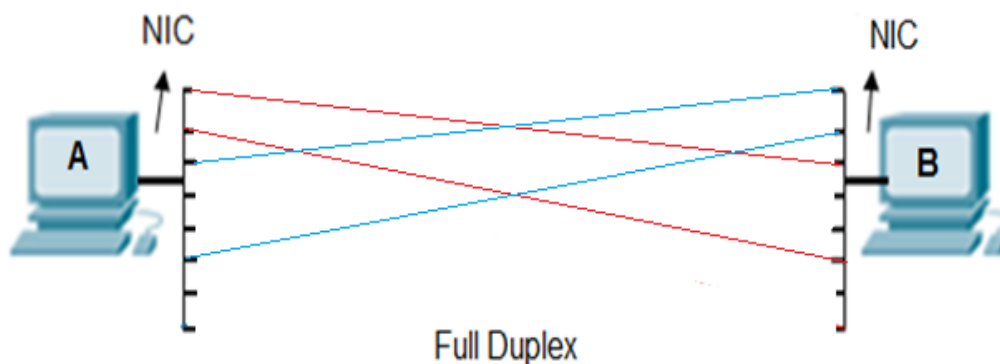
اگر media را نظیر به نظیر جلو ببریم مثلاً به ترتیب نارنجی به نارنجی، سبز به سبز، آبی به

آبی و به همین صورت جلو برویم با توجه به اینکه کارت شبکه درون PC ها از یک قانون

کلی تبعیت می کنند رشته ۱ و ۲ وظیفه ارسال اطلاعات و پایه های ۳ و ۶ وظیفه دریافت اطلاعات را دارند.



در این مرحله باعث می شود که وقتی سیستم A , B بخواهند همزمان ارسال Data کنند Collision ایجاد می شود و همچنین آن رشته ای که وظیفه ارسال یا دریافت را ندارد مجبور شود این کار را انجام دهد.



این مرحله که همان تکنولوژی خط تلفن است که رشته ۱ و ۳ وظیفه ارسال و رشته ۲ و ۶ وظیفه دریافت اطلاعات را بر عهده دارند و دو سیستم می توانند به صورت همزمان ارسال و دریافت اطلاعات را داشته باشند یعنی اگر نرنجی بگذاریم رو ۱ طرف دیگر باید روی ۳ بگذاریم ، اگر آبی را گذاشتیم روی ۲ طرف دیگر روی ۶ بگذاریم.

× اگر رشته ها را نظیر به نظیر بگذاریم اصطلاحاً کابل را **Straight** زدیم.

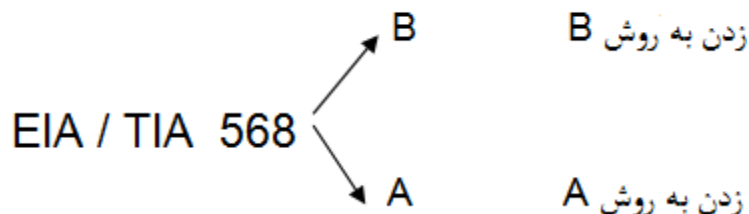
× اگر رشته ها را ضربدری بگذاریم اصطلاحاً کابل را **Cross** زدیم.

برای اینکه شبکه بهینه شود و به **Full Duplex** بودن برسیم :

× اگر رشته های **Send** و **Received** در دو طرف ارتباط متفاوت بود **Straight** می زنیم.

× اگر رشته های **Send** و **Received** در دو طرف ارتباط یکسان بود **Cross** می زنیم.

برای رسیدن به **Full Duplex** بودن ۲ قانون می گذاریم :

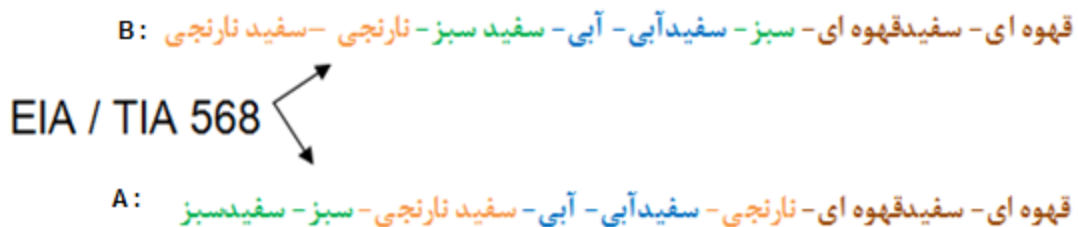


یک کمپانی آمد و این ۲ استاندارد را گذاشت ، حالا منظور از زدن کابل به روش A یا B چیست؟

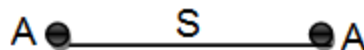
یعنی این کابلی که پشت کامپیوتر ماست یک سوکت دارد، این سوکت ۲ نوع است یک نوع یعنی مترایش به همان گونه که از کارخانه آمده است مثلاً کابل نیم متری یا ۲ متری : می رویم به بازار و می گوییم یک کابل آماده ۲ متری Cross می خواهیم یا اینکه سوکت را بر می داریم و کابل ها را بر اساس رنگی که می خواهیم می چینیم داخل سوکت می کنیم و بعد با آچار مخصوص آن را پانچ می کنیم.

قانون B می گوید اگر سوکت شبکه را از سمت پین های فلزیش (طرف جکش پشت به ما است) به سمت ما باشد یعنی ما pin های فلزی را ببینیم از چپ به راست می شود :

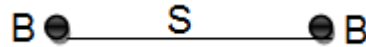
1-2-3-4-5-6-7-8



به شکل های زیر توجه کنید:



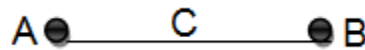
اگر دو طرف کابل استاندارد A باشد می شود Straight

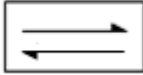



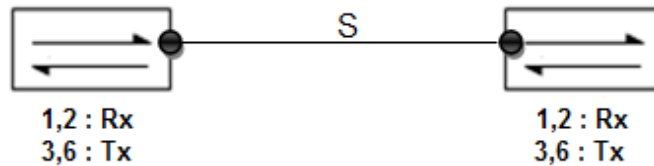
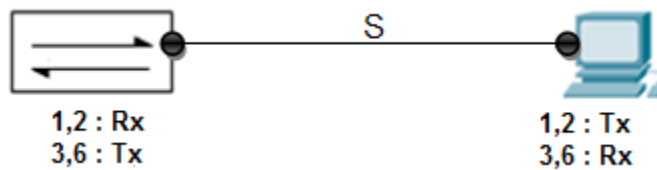
همین طور اگر دو طرف کابل استاندارد B باشد می شود Straight

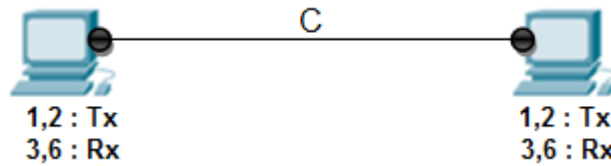
× از بین A و B ، B عمومیت بیشتری دارد.

اگر یک طرف کابل را به صورت A و طرف دیگر را به صورت B بزنیم می شود Cross



× بدانیم نحوه نمایش سوئیچ به صورت  است و نحوه نمایش Hub بصورت  می باشد.





ما در یک ارتباط در کابل، دو سر داریم با توجه به دیدی که از دستگاه‌ها داریم کابل را می‌زنیم.

تکنولوژی Auto-MDIX^{۱۳}:

امروزه این تکنولوژی در همه NIC ها وجود دارند یعنی مهم نیست C بزنی یا S. NIC می‌آید می‌گوید هر وقت از رشته‌های Send و Receive ، Collision دریافت کردی بیا negotiation کن و یک طرف رشته‌های Send و Receive را بیا خودت عوض کن اگر پشت دستگاه را نگاه کنیم و نوشته بود MDIX دیگه مهم نیست کابل را C بزنی یا S.

فیبرنوری

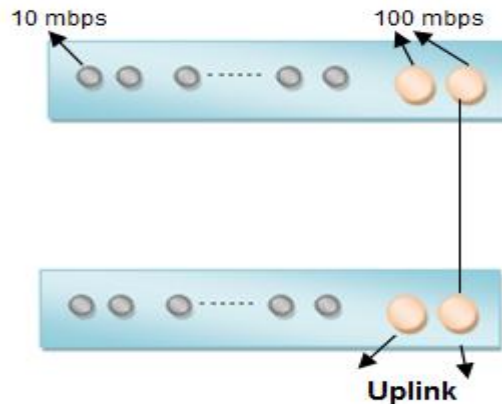
به اندازه 10 Gig پهنای باند می‌دهد، 70km هم به ما Throughput می‌دهد در دو حالت Single Mode و Multi Mode می‌باشد که فرق این دو حالت در نوع منبع نوری شان است که از شکست نور استفاده کند یا از منبع نور مستقیم، دارای دو رشته است که Rx و Tx جدا از هم هستند رشته چپ معمولاً Send و رشته راست معمولاً Receive است، فیبرنوری به یک جوش نیاز دارد که با دستگاه خاصی انجام می‌شود، قابلیت شنود کم و امنیت بالا از ویژگی‌های این media می‌باشد.

¹³Media Dependent Interface X

توپولوژی Expand Star

سوئیچ می تواند 48 port ، 24 port و ... داشته باشد (همان NIC ها هستند) که برای کاربران تعبیه شده است حالا اگر ۶۰ کاربر داشته باشیم دیگر یک Switch کافی نخواهد بود کاری که باید بکنیم این است که ۲ سوئیچ را به هم وصل کنیم که به این توپولوژی Expand Star می گویند. با کابل Cross این دو سوئیچ را به هم وصل می کنیم (چون رشته های Send , Receive دو طرف یکسان است)

*Uplink ها به منظور اتصال بین Switch ها می باشند و برای ارتباطات با پهنای باند بالاتر بین سوئیچ ها تعبیه می شوند. که روی هر سوئیچ معمولاً ۲ تا Uplink موجود است ممکن است سوئیچی هم باشد که Uplink نداشته باشد.



همان طور که در شکل می بینیم هر سوئیچ علاوه بر 24 port که دارد و می تواند به ۲۴ کاربر سرویس دهد دارای 2 port uplink، می باشد ، به طور مثال:

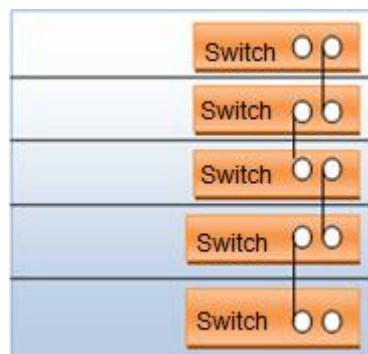
اگر فرض کنیم Port های معمولی سوئیچ ها پهنای باند 10 Mb/s باشد port های uplink دارای پهنای باند 100 Mb/s می باشد.

× به این دلیل پهنای باند port های uplink ها بیشتر از port های معمولی می باشد که در شبکه ترافیک ایجاد نشود.

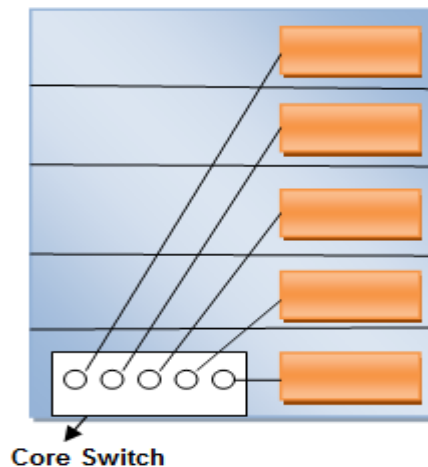
× Backbone شبکه جایی است که بیشتر ارتباطات کابل های شبکه از آنجا شکل می گیرد.

فرض کنید یک ساختمان داریم در هر طبقه ۴۰ کاربر داریم چگونه می توانیم شبکه ایجاد نماییم؟

راه اول) در هر طبقه یک Switch بگذاریم بعد Uplink به Uplink آنها را به هم وصل کنیم این روش بهینه نیست و مدیریتش خوب نیست و اگر آن وسط یک سوئیچ خراب شود کل شبکه مختل می شود و عیب یابی نمی توان کرد.



راه دوم) علاوه بر سوئیچ های هر طبقه یک سوئیچ مرکزی بگذاریم کلیه سوئیچ ها را به آن وصل می کنیم، port های سوئیچ مرکزی باید 1000 Mb/s و port های معمولی سوئیچ ها 100 Mb/s باشد که ترافیک بوجود نیاید. به سوئیچ مرکزی Core Switch می گویند.



یادمان باشد که :

× Hub دستگاه لایه ۱ هست یعنی هیچی نمی فهمد ولتاژ را می گیرد و بیرون می دهد.

× Computer ۷ لایه را می فهمد.

× Switch دستگاه لایه ۲ هست.

× Router (که در ادامه تعریفش می کنیم) دستگاه لایه ۳ هست.

شکل زیر را در نظر بگیرید :



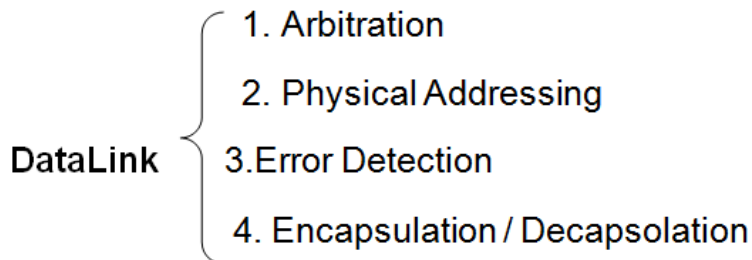
توضیح: اولین دستگاه که کامپیوتر است دومی سوئیچ هست سومی Router چهارمی

سوئیچ و پنجمی هم باز کامپیوتر، وقتی می گویند که OSI، ۷ لایه است یه نکته ای دارد در هر دستگاه به ازای هر لایه که مورد بررسی قرار می گیرد یک process انجام می شود یعنی اگر یک دستگاهی باشد که کلاً یک لایه را بفهمد می تواند خیلی سریع کار کند(چون لایه ۱ سیگنالینگ هست و بصورت ولتاژ هست) تا دستگاهی که لایه ۵ را می فهمد. منظور این است که هر دستگاه که لایه های بیشتری را قرار باشد بفهمد باید دستگاه هوشمندتری باشد پس هرچقدر Process و Ram دستگاه بالاتر برود دستگاه قیمت بالاتری پیدا می کند.

با توجه به شکل بسته از لایه ۷ حرکت کرده به لایه ۱ می رسد تبدیل به ولتاژ شده و بعد به سمت media می آید بعد می رسد به سوئیچ که قالباً ۲ لایه را می فهمد بعد که تا لایه ۲ را بررسی کرد و فهمید چه چیزهایی باید به بسته اضافه شود دوباره به سمت لایه ۱ آمده تبدیل به ولتاژ می شود و داخل media می رود باز به دستگاه بعدی می رسد (Router) در این دستگاه بسته آدرس خودش را بر اساس لایه ۳ می فهمد و باز مورد بررسی قرار می گیرد و در نهایت وارد media می شود.

نتیجه : همه دستگاه ها لزوماً نباید هر ۷ لایه OSI را بشناسند و مورد بررسی قرار دهند
 بعضی از دستگاه ها برای اینکه از نظر اقتصادی هم مقرون به صرفه باشند کفایت به آن
 اندازه که لازم است لایه ها را بشناسند.

لایه ۲ (DataLink)



Arbitration : به مکانیزم های مختلف مقابله با Collision در توپولوژی های مختلف
 گفته می شود مانند: CSMA/CD در توپولوژی Bus یا Token Passing در
 توپولوژی Ring .

× همان طور که گفتیم لایه ۱ فهمی ندارد که بتواند در مواقع وقوع Collision با آن مقابله
 کند فقط می تواند خبرش را به لایه ۲ بدهد. لایه ۲ فهمش از لایه ۱ بیشتر، لایه ۳ فهمش از
 لایه ۲ بیشتر و ...

Physical Addressing : کارت شبکه ها بر روی خود یک cheapset دارند

درون این cheapset ها یک آدرس فیزیکی از طرف کمپانی شبکه ثبت شده است که به

آن ها می گویند: physical address که اسم های مختلفی دارد :

physical address – Burn in Address(BIA) – Media Access Control(Mac)

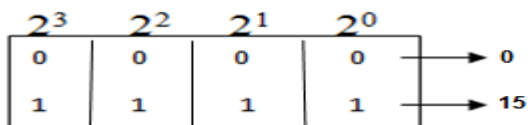
این آدرس فیزیکی از طرف کمپانی شبکه در داخل cheapset حک می شود.

آدرس فیزیکی آدرسی است به طول ۴۸ بیت که از لحاظ ساختار به شکل زیر است:

XX_XX_XX_XX_XX_XX

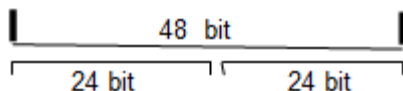
طول هریک از X ها ۴ بیت است. و از لحاظ مقدار هر کدام می تواند عددی بین ۰-۹ یا

A_F باشد.



x هر کدام از این ۴ بیت ها می توانند ۱۶ مقدار (۱ + اولی - آخری) را به خود اختصاص

دهند.



از لحاظ ساختار به ۲ تا ۲۴ بیتی تقسیم می شود ۲۴ بیت اول استاندارد شرکت IEEE است که این استاندارد روی ۲۴ بیت اول نظارت می کند و به آن می گویند OUI^{۱۴} ، ۲۴ بیت دوم برای Vendor است که میتواند ۲^{۲۴} حالت ایجاد کند.

هر NIC که در لایه ۲ بتواند فعالیت کند این mac address را دارد ، کمپانی IEEE می گوید من اولین بار ۲۴ بیت به صورت رایگان بهت می دهم تو خودت (کمپانی سازنده) برو ۲^{۲۴} احتمال کنار آن ۲۴ بیت قرار بده بگذار و mac address های مختلف را تولید کن بعد که تمام شد بیا ۲۴ بیت دیگر بهت بدهم و احتمالات خودت را کنارش بگذار با این کار چون ۲۴ بیت اول unique است،

نتیجه : Mac Address های کارت شبکه بصورت unique هستند.

چگونگی دیدن Mac Address در pc :

Windows + R → cmd

ابتدا وارد محیط cmd می شویم

getmac

دستور زیر را وارد می کنیم :

چگونگی دیدن NIC در pc :

¹⁴Organizationally Unique Identifier

ncpa.cpl^{۱۵}

در محیط cmd با استفاده از دستور زیر:

یا از طریق مسیر زیر:

Control Panel → Network and Internet → Network and Sharing Center →
Change adapter settings

چگونگی دیدن Mac Address های pc بر اساس NIC های سیستم:

ipconfig /all

در محیط cmd با دستور زیر:

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Faraz>ipconfig/all

Windows IP Configuration

    Host Name . . . . . : Yasaman-PC
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Bluetooth Device (Personal Area Network)
    Physical Address. . . . . : 00-08-C9-3A-56-2B
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Anghezi:

    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Atheros AR9002WB-1NG Wireless Network Adapter
    Physical Address. . . . . : 00-08-C9-39-D5-38
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::f53a:a040:ad74:991a%12(Preferred)
    IPv4 Address. . . . . : 192.168.1.101(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Saturday, April 26, 2014 1:25:30 PM
    Lease Expires . . . . . : Thursday, May 01, 2014 10:49:24 AM
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.1
    DHCPv6 IAID . . . . . : 301992138
    DHCPv6 Client DUID. . . . . : 00-01-00-01-18-B6-4D-EF-54-04-A6-75-23-F1

    DNS Servers . . . . . : 8.8.8.8
    NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Local Area Connection:

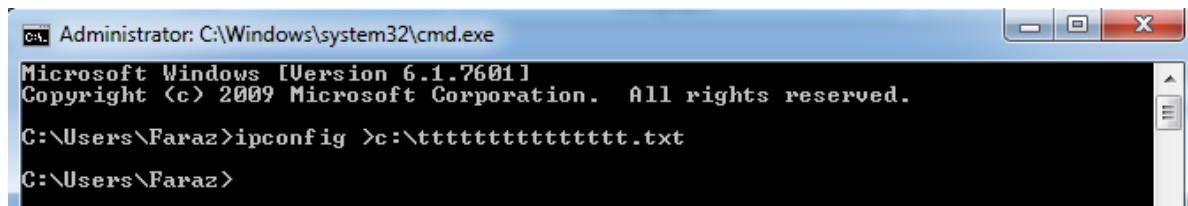
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Atheros AR8151 PCI-E Gigabit Ethernet Controller (NDIS 6.20)
    Physical Address. . . . . : 54-04-A6-75-23-F1
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
  
```

¹⁵Network Connection Properties administration. Control Panel

اگر بخواهیم دستور در محیط cmd نوشته نشود و داخل یک فایل save کند جلوی دستور با استفاده از دستور زیر:

>C:\نام.txt

مثال:



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Faraz>ipconfig >c:\tttttttttttttt.txt
C:\Users\Faraz>
```

این دستور mac address های سیستم را در فایل بنام ttttttttttt.txt در C به ما نشان می دهد.

جلسه دوم :

ابزارهای زیر را در کلاس بررسی کردیم:

آچار شبکه دیدیم که ۲ نوع است یکی مانند انبردست فشار به بالا می آورد و یک مدل از بغل فشار وارد می کرد.

سوکت RJ45 ، وقتی یک کابل می گیریم سرش سوکت ندارد(مگر اینکه از کمپانی بگیریم) سر کابل را می بُریم و می بینیم که ۴ زوج به هم تابیده است، با دست تاییدگیشان را باز می کنیم، به صورت A یا B سیم ها را به ترتیب رنگشان کنار هم گذاشته و داخل سوکت می کنیم و با آچار شبکه پانچ می کنیم.

Striper : یک لبش تیغ است طرف دیگرش حفره مانند، هرچقدر کابل را داخلش جلوتر بیاوریم مقطع دستگاه نازکتر می شود یعنی اگر کابل را خیلی جلو ببریم ممکن است به رشته هایش آسیب وارد کند، با یک چرخش دست لایه رویی کابل برداشته می شود.

کارت شبکه و cheapset روی آن را بررسی کردیم که mac address داخل cheapset حک شده است.

فیبر نوری دیدیم که غلاف داخل فیبر ترکیبات سمی دارد شیشه داخل فیبر اگر وارد دستمان شود آسیب وارد می کند، فیبر یک قرقره دارد که دور قرقره بسته می شود.

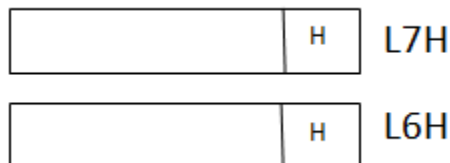
Switch : ۲ نوع دارد manageable و unmanageable ، D-Link هر دو نوع را دارد

و سوئیچ ارزانی است و احتمال اینکه در شبکه خراب شود زیاد است در بین سوئیچ های manageable سوئیچ مناسبی نیست، تفاوت قیمتش با سوئیچ Cisco این است که مثلاً سوئیچ 24 port نوع D-Link را اگر بخریم ۳۰۰۰۰۰ تومان سوئیچ Cisco را می خریم ۳۰۰۰۰۰۰.

_ شبکه از لحاظ اجرا به دو قسمت تقسیم می شود : active _ Passive

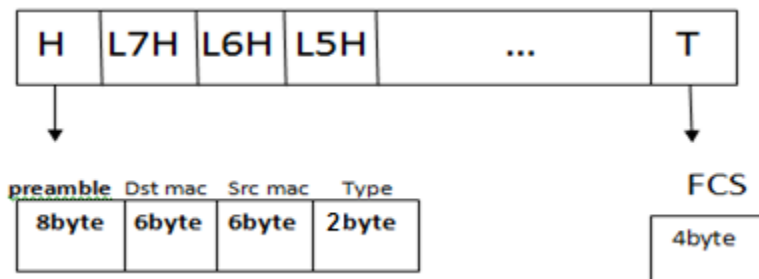
دستگاه هایی که برق واردش می شود active و دستگاه هایی که power ندارد و برق داخلش وارد نمی شود می شود passive . کارت شبکه یک دستگاه passive است .

هر بسته در لایه های شبکه که از بالا به پایین می آید در هر لایه Header مخصوص به خودش را اضافه می کند هر لایه فقط از Header مربوط به خود خبر دارد به طور مثال لایه ۵ از Header لایه ۶ خبر ندارد فقط Header مربوط به خودش را می تواند اضافه کند و بردارد و ...



لایه ۲ به جز Header، Footer یا Trailer هم دارد، ابتدای سیگنال شدن بیت‌های لایه ۲ از Header اتفاق می‌افتد یعنی بیت‌ها را از Header می‌گیرد و شروع می‌کند به سیگنال کردن.

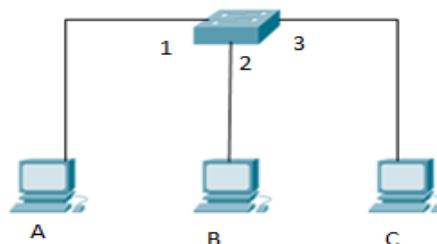
اولین سیگنالی که وارد شبکه می‌شود Header است.



اسم این استاندارد را گذاشتند: Dix (Digital Equipment Corporation, Intel, Xerox)

Preamble: کدینگی هست که بهش می‌گویند کدینگ منچستر، Preamble می‌گوید که بیت‌های ۱ با چه ریتی به دست ما می‌رسد و مشخص می‌کند که چگونه باید خوانده شود (به صورت Synchronization است).

مثال) طبق شکل بسته از سیستم A به سیستم C چگونه می‌تواند برسد؟



جواب: Switch برخلاف Hub بسته را به همه نمی فرستد بلکه فقط به همان مقصد مورد

Src mac	Dst Mac
Mac A	Mac C

نظر می فرستد می دانیم که در لایه ۲ در PCA بسته ای به شکل

شکل می گیرد Switch وقتی این بسته را می گیرد mac کسی را که بسته را می فرستد می فهمد داخل خودش mac table تشکیل می دهد (اگر Switch این جدول را نداشته باشد Hub است) می نویسد Port1 و Port2 و .. وقتی بسته از A می رسد به Switch اولین کاری که می کند Src بسته را نگاه می کند و هر دفعه می نویسد که با mac چه کسی دارد صحبت می کند به تدریج که هر بسته جابجا می شود جدولش را پر می کند، حالا موضوع اینکه که اگر اولین بار mac مقصد را نداشته باشد چکار کند؟

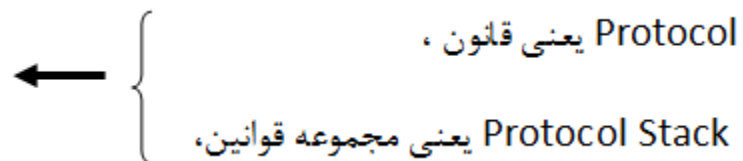
1	MacA
2	MacB
3	MacC

فعلاً فرض می کنیم که جدول پر باشد وقتی بسته از A به سمت Switch می آید بررسی می شود که یک نفر از mac A آمده و می خواهد برود به Mac C در جدول نگاه می کند و می بیند باید از Port3 بیرون برود در نتیجه بسته را از Port3 بیرون می دهد و بسته دیگر از port2 عبور نمی کند.

می گیرد و می گذارد داخل CRC خودش اگر FCS که در آمد با قبلی برابر شد یعنی بسته دچار هیچ Error نشده اگر حتی کمی فرق کند این 4byte بسته لایه ۲ دور انداخته می شود.

Type: اشاره گر به پروتکل لایه بالایی .

واحد اندازه گیری پروتکل در هر لایه را PDU^{۱۸} می گویند.



Protocol ها زیر مجموعه Protocol Stack ها هستند.

PDU لایه های مختلف به شکل زیر است :

Layer 5,6,7	Data	
Layer 4	Segment	
Layer 3	Packet	
Layer 2	Frame	→ بسته لایه ۲
Layer 1	Bit	

¹⁸Protocol Data Unit

× اگر بگویند packet هایی که از لایه ۲ رد می شود غلط است باید بگوییم packet هایی که از لایه ۳ رد می شود.

× مهمترین قسمت header لایه ۲ چیست؟ جواب: Mac Address .

^{۱۹}IP: یک سری کدها هستند که به صورت Logical تعریف شده اند و جایی حک نشده است (می توانند تغییر کنند) مثلاً ۰۰۹۸ که کد ایران است برای اینکه از آمریکا به ایران زنگ بزنیم باید در شبکه مدل زیر را داشته باشید تا بتوانیم سیستم را صدا بزنیم:

0098 21 8887 5551
سایبر تک مخابرات تهران IRAN
بهشتی

وظایف لایه ۳:

- _ Logical Addressing
- _ Routing
- _ Error Detection
- _ Encapsulation

¹⁹Internet Protocol

IP به دو Version تقسیم می شود: (v4 , v5 , v6)

IP در دنیا ۲ ورژن را می شناسد: (V4 , V6)

V5 بعد از V4 بوجود آمد اما فقط در حد تحقیق ماند و به نتیجه ای نرسید اما شروعی شد برای V6.

V6 طولش ۱۲۸ بیت است یعنی می تواند 2^{128} حالت تولید کند!

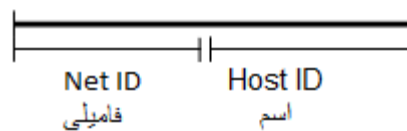
طول V4 ، ۳۲ بیت و به شکل زیر می باشد :

XXX.XXX.XXX.XXX
8 bit 8 bit 8 bit 8 bit

× مثالی از IP v4 : 10.0.0.1 ، 192.168.01

: Host ID , Net ID

هر IP یک اسم دارد و یک فامیلی ، هیچ دو سیستمی یافت نمی شود که هم Host ID و هم Net ID برابر داشته باشند، Host حکم اسم را دارد و Net ID حکم فامیلی .



$$\left\{ \begin{array}{l} \text{Net ID} + \text{Host ID} = 32 \text{ Bit} \\ 32 \text{ Bit} - \text{Net ID} = \text{Host ID} \end{array} \right.$$

کنار IP باید یک چیزی داشته باشیم که نشان گر این است که چه قدر از IP جز Net ID و چقدرش جز Host ID می باشد.



Prefix Notation تعداد بیت هایی که از ابتدای IP تا به آنجا متعلق به Net ID است را

نشان می دهد. مثال: 192.168.0.1/16

Net ID = 192.168 , Host ID = 0.1

این مدل را کارفرما می فهمد ولی سیستم نمی فهمد.

× در یک سوئیچ تنها IP هایی می توانند ارتباط بگیرند که دارای Net ID برابر باشند .

می خواهیم مدل صفر و یکی IP را بگوییم که سیستم می فهمد:

	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1
192.168.0.1/24	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1
Prefix	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0
Value Prefix or Subnet Mask	255	255	255	0

توضیح:

به ۲ روش می توان Net ID را بر روی IP مشخص کرد:

روش اول یا Prefix Notation: که در جلوی هر IP با یک عدد نمایان می شود می گوید چه تعداد بیت از ابتدای IP متعلق به Net ID است.

روش دوم: ارزش بیت های متعلق به Net ID یا همان Subnet Mask.

به عنوان مثال:

Prefix	Subnet Mask
/8	255.0.0.0
/16	255.255.0.0
/24	255.255.255.0

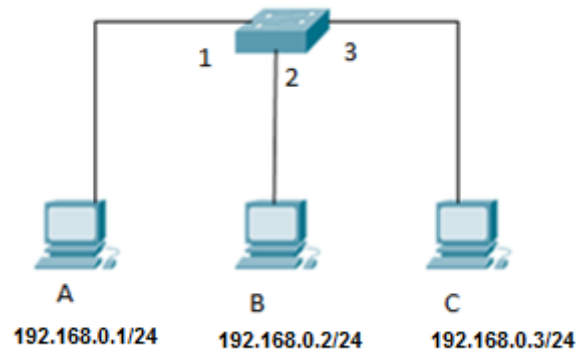
سیستم ها اولین معیار برقراری ارتباطشان IP است، ما هر آدرسی (مثلاً

www.google.com) به سیستم بدهیم آن تبدیل به IP می کند، در لایه ۲ بر اساس IP

که ما دادیم Mac Address ثبت می شود حالا سوال اینجاست Mac Address یک

سیستمی که IP آن را می دانیم چگونه پیدا کنیم؟

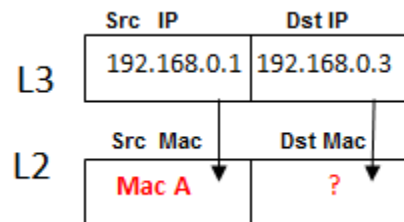
مثال (فرض کنیم شکل زیر را داریم



قرار است بسته ای از سیستم A به سیستم C بفرستیم.

توضیح :

مرحله ۱: در PC A بسته در لایه ۳ می آید با توجه به IP که صدایش کردیم و می دانیم، بعد به لایه ۲ آمده و Process لایه ۲ برویش انجام می شود، Mac خودش را که می داند ولی مقصد را نمی داند(اگر بخواهد ثبت شود در حافظه RAM ثبت می شود که حافظه ماندگار نیست) پس بسته فعلاً قابلیت ارسال ندارد.



مرحله ۲ : بسته اصلی کنار رفته بسته ARP^{۲۰} می آید (برای پیدا کردن Mac Dst) که پروتکل لایه ۳ می باشد داد می زند و می گوید من Dst Mac را بدست می آورم و بهت میدهم حالا ARP به چه صورت کار می کند؟

به این صورت که توی لایه ۳ همان را می گذارد ولی در لایه ۲ به جای Dst Mac ، ۱۲ تا F می گذارد، این ۱۲ تا F توهمی به سوئیچ می دهد که سوئیچ فکر می کند Hub است و بسته را به همه می فرستد (Broadcast).

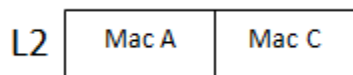
این ۱۲ تا F ، Mac آدرس عمومی - Mac آدرس Broadcast است .

L3	192.168.0.1	192.168.0.3
L2	Mac A	FF : FF : FF : FF : FF : FF

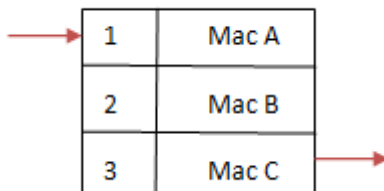
مرحله ۳ : بسته به سمت سوئیچ آمده ، سوئیچ بسته را به همه می فرستد سیستم B بسته را باز می کند و تا لایه ۳ نگاه می کند و می گوید 192.168.0.3 من نیستم پس قرار نیست جواب ARP را بدهم ، سیستم C بسته را باز می کند و می بیند که 192.168.0.3 خودش است و چون توی بسته قسمت type نوشته شده ARP می گوید پس من باید جواب بدهم .

²⁰Address Resolution Protocol

مرحله ۴: می آید به جای ۱۲ تا F ، Mac خودش را می گذارد و بعد جای Src و Dst را عوض می کند و بسته را تحویل کسی که سوال پرسیده بود می دهد بدین صورت Table Switch دو طرف پر می شود حالا می داند توی لایه ۲ بسته اصلی باید بزند Mac A , Mac C حالا بسته به این شکل زیر می رود داخل سوئیچ.



مرحله ۵: سوئیچ در Table خود نگاه می کند و می فهمد که بسته از Port 1 آمده از Port 3 قرار است بیرون برود جواب را پیدا کرده و بسته را می فرستد ، پس سیستم ها باتوجه به IP آدرسشان می توانند Mac خودشان را در یک شبکه پیدا کنند.



× جدول سوئیچ به مرور پر می شود .

× ARP بسته اصلی نیست و کار آن به دست آوردن آدرس لایه ۲ مجهول از روی آدرس لایه ۳ معلوم می باشد با توجه به مثال بالا کارش این است که برود Mac مقصد را پیدا کند بعد بسته اصلی ارسال می شود توی این ارسال اتفاقی که می افتد این است که A , C می توانند Mac همدیگر را در کنار IP شان ثبت کنند که باعث می شود سرعت ارتباط بیشتر شود و

به آن ARP Cache می‌گوییم، اگر بخواهیم دوباره بسته‌ای را ارسال کنیم دیگر لنگ ARP نمی‌مانیم مگر اینکه ARP Cache را Delete کنیم یا اینکه سیستم را reset کنیم (چون RAM حافظه موقته و سیستم را که Reset کنیم این حافظه پاک می‌شود یا با زدن فرمان Arp -d).

× بعضی از ارتباطات به صورت اتوماتیک برقرار می‌شوند مثلاً فرض کنیم ۲ سیستم در ارتباطند در یک شبکه و در یک سیستم یک Printer داریم و این Printer در سیستم دیگر تعریف شده سیستم وقتی بالا می‌آید برای اینکه Printer خود را پیدا کند ARP می‌کند، داخل شبکه یک سری چیزها هست که خود به خود ARP می‌شوند، به جز ARP یک سری بسته‌ها هستند در شبکه که به صورت اتوماتیک جابجا می‌شوند.

یکی از مشکلات ARP:

این که همه سیستم‌ها باید تا لایه ۳ را بررسی کنند تا ببینند بسته با آنها کار دارد یا خیر.

Run menu >> cmd>>

با Command زیر می‌توانیم arp cache سیستم را ببینیم:

arp -a

و با دستور زیر می توان arp cache سیستم را خالی کرد:

arp -d

× کارت شبکه می تواند داخل شبکه ای که سوئیچ هست سه چیز را دریافت کند:

(۱) هر چیزی که مال خودش است

(۲) چیزهایی که از خودش به کسی قرار است برود

(۳) چیزهایی که مال همه هست مانند ARP.

حالا چگونه این ها را می توانیم ببینیم؟ با استفاده از یک سری نرم افزارها مانند

. Wireshark

: Router

امروزه در دنیای اینترنت حتماً Router ها هستند.

اینکه Router چیست و فرقی با سوئیچ در چیست و چرا بوجود آمد مثال زیر را در نظر

بگیرید:

فرض کنیم در یک شبکه جهانی اگر یک سیستم بخواهد به سیستم کنار خودش که در

یک شبکه است بسته ای بفرستد یعنی باید به تمام سیستم های شبکه ها ARP بدهد!!!

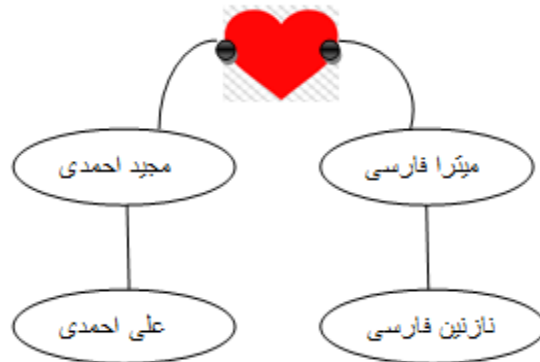
این طوری که همه دنیا می فهمند !! چون ARP منتقل می شود به همه ، یک نفر هم که در دنیا ARP نمی کند و خیلی ها ممکن است در حال ARP کردن باشند این طوری که شبکه جهانی از بین می رود!

Router علاوه بر اینکه وظیفه اش مسیریابی است ARP یک شبکه ای که به خودش مربوط نیست را از خودش عبور نمی دهد و جلوی آن را می گیرد. عبور از یک شبکه به شبکه دیگر با استفاده از Router ها انجام می پذیرد، Router متعلق به لایه ۳ است.

اگر می گویند تمام دنیا با هم در ارتباط هستند یعنی Net ID آنها با هم برابر است؟! یعنی IP ها به اندازه تمام دنیاست؟! اصلاً اگر کمترین مقدار مورد نظر را هم بخواهیم برای Net ID در نظر بگیریم که ۸ بیت باشد در نتیجه ۲۴ بیت Host خواهیم داشت یعنی می شود 2^{24} . آیا این 2^{24} حالت می تواند پاسخ گوی تمام دستگاه های توی دنیا باشد؟

به خاطر همین موضوع لازم می شود که دستگاهی باشد که اگر دو سیستم Net ID هایشان با هم برابر نبود بتوانند با هم ارتباط برقرار کنند در نتیجه Router ها آمدند.

برای اینکه با کارایی Router بهتر آشنا شوید مثال زیر را در نظر بگیرید:



مثال) فرض کنیم مجید و میترا با هم ازدواج می کنند و در مراسم عروسیشان علی و نازنین همدیگر را می بینند و به هم علاقه مند می شوند بعد از عروسی اگر این دو بخواهند از هم دیگر خبر بگیرند باید از طریق مجید و میترا این کار را بکنند چون علی دستش در یک شبکه هست و نازنین در شبکه دیگر (شبکه هایی که Net ID (فامیلی هایشان) شان حتما متفاوت است وگرنه Router می خواستیم چه کار همان سوئیچ را می گذاشتیم)

چون مجید و میترا با هم ازدواج کردند این دو می شوند دستهای Router .

مجید برای علی Default Gateway محسوب می شود یعنی جایی که پیغام علی می تواند رد شود و بیرون برود همچنین برای نازنین هم میترا این نقش را برعهده دارد و نازنین و علی را با هم ارتباط می دهد! یعنی مجید و میترا می شوند IP های روی Router (دقت کنید که IP روی Switch نمی توانستیم Set کنیم اما Router روی Port خودش IP می پذیرد)

× Mac Address و IP سیستم را می توانیم خودمان Set کنیم.

× Mac address از داخل شبکه بیرون نمی رود.

× Default Gateway برای زمانی هست که Net ID دو سیستمی که قرار است ارتباط برقرار کنند با هم برابر نباشد.

جهت تنظیم کارت شبکه :

Network Address >> Advanced >> Configure >> Properties >> بر روی NIC دستگاه کلیک راست

اگر بر روی Not Present باشد یعنی همانی که روی خودش هست.

Set کردن IP :

>> Properties >> Internet Protocol Version 4 >> Properties >> بر روی NIC دستگاه کلیک راست
IP Address

در خانه یک ADSL Modem Router داریم که

(۱) آدرس های خودش را از طریق لایه ۳ بررسی می کند.

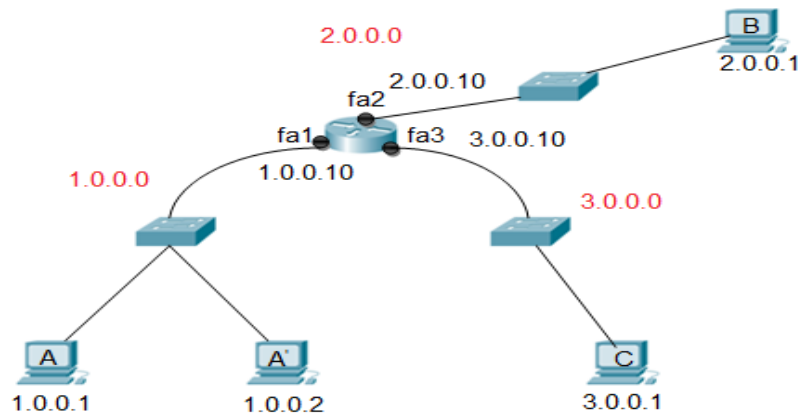
(۲) دستگاهی است که حداقل ۲، Interface دارد (یکی سیم تلفن که وصل به مخابرات

است و دیگری به صورت کابل یا Wireless)

Router ها معمولاً تعداد Port زیادی ندارند و کار اصلی شان این است که بین چند

شبکه ارتباط برقرار کنند.

مثال) شکل زیر را در نظر بگیرید :



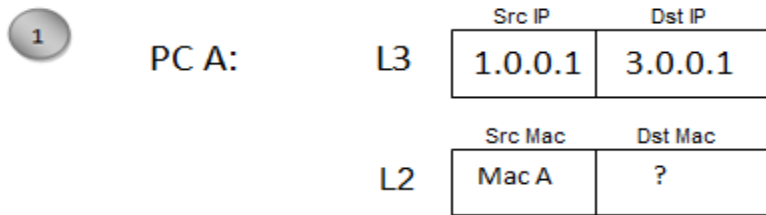
الف) قرار است بسته ای از سیستم A به سیستم A' منتقل شود :

توضیح: اگر قرار باشد بسته از سیستم A به سیستم A' برسد و Mac A' را نداشته باشد ARP می کند داخل شبکه و می گوید 1.0.0.2 مال کی هست؟ بسته از دو طرف سوئیچ رد می شود یکی بالا می رود به سمت دست Router و آن می گوید که من 1.0.0.2 نیستم، یکی هم به سمت پایین سوئیچ آمده و دست A' رسیده می بیند 1.0.0.2 مال خودش هست در نتیجه Mac خودش را جای ۱۲ تا F می گذارد و جای مبدا و مقصد را عوض می کند در نتیجه بسته از A به A' ارسال می شود.

دیدیم که بسته ARP از Router رد نشد.

ب) حالا می خواهیم بسته ای را از سیستم A به سیستم C بفرستیم :

مرحله اول: بسته در سیستم A به شکل زیر تشکیل می شود:

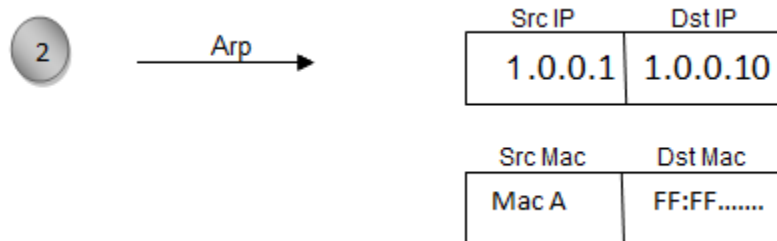


در لایه ۲ چون Mac مقصد را نمی داند قبل از اینکه Arp کند می گوید 3.0.0.1 که توی شبکه من نیست! (دو نوع Arp از لحاظ مکانیزم اجرا داریم: ۱) Arp که مبدا و مقصد داخل یک شبکه هست ۲) Arp که مبدا و مقصد داخل یک شبکه نیستند) در نتیجه بسته اصلی فعلا کنار می رود و بسته Arp می آید.

مرحله دوم: بسته Arp می گوید چون بسته قرار است به یک شبکه دیگر برود (چون Src IP و Dst IP هم خانواده نیستند) پس من باید Arp را برای پیدا کردن Mac Gateway بفرستم!

× IP Gateway در کارت شبکه به عنوان Default Gateway ثبت شده است.

در مرحله دوم بسته به صورت زیر شکل می گیرد:



مرحله سوم: بسته Arp به سمت سوئیچ آمده و سوئیچ در Mac Address Table خود

نگاه می کند (فرض کنیم پر شده) می گوید من Arp ی که آمده به سمتم را از همه Port هایم بیرون می دهم بسته دست A' رسیده و می گوید من که 1.0.0.10 نیستم پس نباید

جواب Arp را بدهم، بسته می رسد به دست Router Port می گوید تو

1.0.0.10 هستی؟ می گوید بله در نتیجه Mac خودش می فرستد برای سیستم A (فرض

کنید در Arp Cache نداشته باشد)

مرحله چهارم: بسته اصلی Mac Address خودش را پیدا می کند می گوید می خواهم

از 1.0.0.1 به 3.0.0.1 بروم، بسته به صورت زیر شکل می گیرد:

4

Src IP	Dst IP
1.0.0.0	3.0.0.1
Src Mac	Dst Mac
Mac A	Mac fa 1

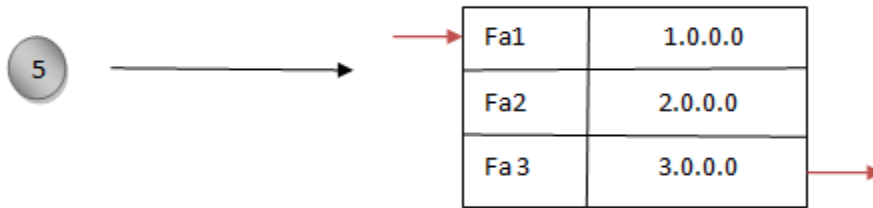
بسته اصلی با این شکل به دست سوئیچ رسیده سوئیچ در Mac Address Table

خودش نگاه می کند و می گوید بسته می خواهد برود به سمت Mac fa1 در نتیجه بسته

را سمت Router می فرستد (Router دستگاهی است که مسیریابی خودش را از طریق

IP انجام می دهد با استفاده از Routing Table) در Routing Table ، IP های شبکه

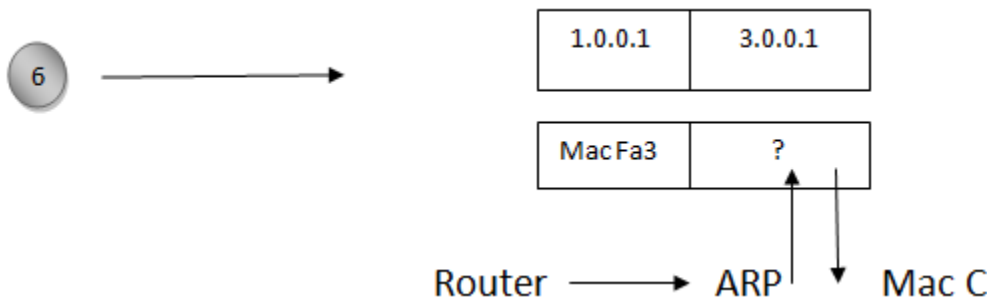
ها به صورت کلی گفته شده به شکل زیر :



مرحله پنجم: Router وقتی بسته به دستش می رسد اولین کاری که می کند این است که لایه ۲ بسته را که Mac ها نوشته است را جدا می کند و بعد با استفاده از **Routing Table** خود در لایه ۳ به صورت کلی می گوید یک نفر از 1.0.0.0 آمده و می خواهد به 3.0.0.0 برود بسته را می آورد سر دست 3.0.0.0 نگه می دارد:

x به این عملیات که Router بسته را از یک دستش به دست دیگری می دهد می گویند Routing که براساس IP های موجود در بسته این کار را می کند.

مرحله ششم: حالا دوباره بسته به صورت زیر شکل می گیرد:



اگر Router، Dst Mac را نداشته باشد داخل شبکه Fa 3، Arp می کند (بسته دیگر به سمت شبکه بالایی نمی رود) و نتیجه اش را می نویسد، حالا بسته را به سوئیچ می دهد بعد سوئیچ داخل **Mac Address Table** خود نگاه می کند و بسته را به سیستم C می دهد.

جلسه سوم

× سوئیچ هایی داریم که Uplink ندارند.

× اگر دو سوئیچ را به هم وصل کنیم که همه Port های معمولی سوئیچ 100 Mb/s ولی Uplink ها 1000 Mb/s باشد بیایم کابل اتصالشان را Cat5 بزنیم در واقع اشتباه بزرگی کردیم چون سوئیچ ها توانایی انتقال 1000 mb/s را داشته اند اما کابل توانایی انتقال 100 mb/s بیشتر را ندارد باید دقت کنیم که چه کابل هایی را در کجا بکار ببریم .

یک سری دسته بندی برای IP وجود دارد که یک نوع آن Class-full است که امروزه در بسته بندی ها اصلاً Class-full وجود ندارد، در این نوع تقسیم بندی گفته می شود که IP با کلاس های مختلف شناخته می شود : A-B-C-D-E

A	1-126	<u>Net ID</u> . <u>Host ID</u> . <u>Host ID</u> . <u>Host ID</u> / 8
B	128-191	<u>Net ID</u> . <u>Net ID</u> . <u>Host ID</u> . <u>Host ID</u> / 16
C	192-223	<u>Net ID</u> . <u>Net ID</u> . <u>Net ID</u> . <u>Host ID</u> /24
D	224-239	
E	240-255	

× D برای کارهای خاصی به کار می رود و به صورت multicast می باشد.

× E بصورت آزمایشی است و در آزمایشگاه های تست IP استفاده می شود.

سوال: اگر بخواهیم برای شبکه خودمان یکی از دسته بندی های بالا را انتخاب کنیم بهتر است کدام را انتخاب کنیم؟

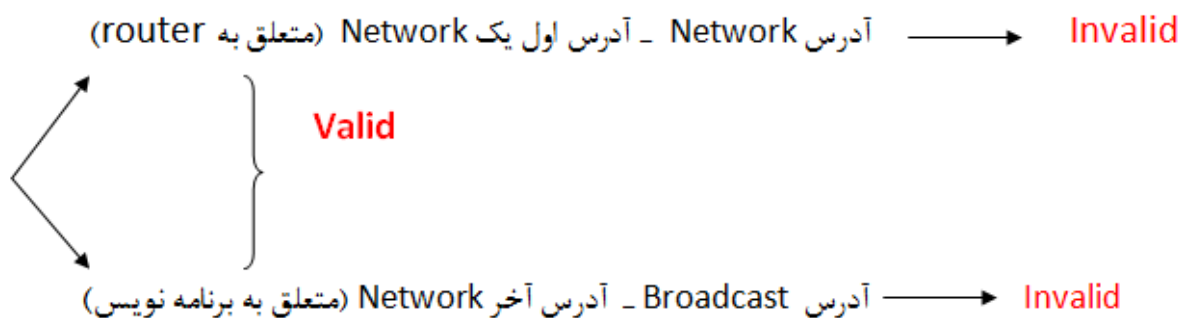
جواب: A، چون 2^{24} حالت IP به ما می دهد و در نتیجه تعداد Host بیشتری را می توانیم IP دهی کنیم.

تقسیم بندی IP از نظر وجود یا عدم وجود:

Valid: یعنی IP که وجود دارد و می توان آن را به یک Host داد.

Invalid: یعنی IP که وجود ندارد و نمی توان آن را به یک Host داد.

در شبکه ۲ تا آدرس داریم که Invalid هستند.



این دو آدرس را نمی توان در یک سیستم، Set کرد چون برای کاربرهای خاص بکار می روند

باتوجه به Subnet Mask هرگاه تمام بیت های مربوط به Host ID را مقدار صفر قرار

دهیم می شود آدرس Network.

همین طور با توجه به Subnet Mask هرگاه تمام بیت های مربوط به Host ID را مقدار یک قرار دهیم می شود آدرس Broadcast .

مثال) در IP داده شده آدرس Network و آدرس Broadcast را مشخص کنید.

192.168.0.X/24

جواب :

{	192.168.0.0	آدرس Network
	192.168.0.255	آدرس Broadcast

مثال : در IP داده شده آدرس Network و آدرس Broadcast را مشخص کنید.

10.0.0.0/8

جواب :

آدرس >> Invalid >> Network 10.0.0.0

آدرس Broadcast >> Invalid >> 10.255.255.255

بین این دو آدرس هرچه باشد valid است مانند: 10.0.0.1 ، 10.1.1.0 ، 10.50.60.1

و ...

مثال : 172.16.1.1/16 را داریم آدرس Network و آدرس Broadcast آن را بنویسید.

جواب :

آدرس Network >> 172.16.0.0/16

آدرس Broadcast >> 172.16.255.255/16

مثال : با 16 / prefix چه تعداد IP تولید می شود و چه تعداد Host را می توان IP دهی نمود.

جواب :

Valid range

Total IP range (تعداد کل IP های تولید شده)

$2^H - 2$

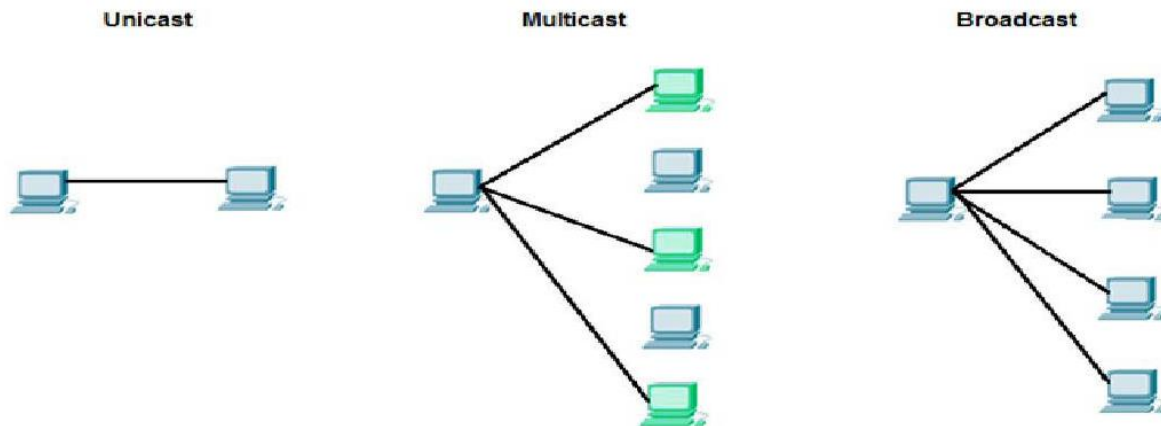
2^H

سوال : فرق Broadcast لایه ۲ با Broadcast لایه ۳ چیست؟

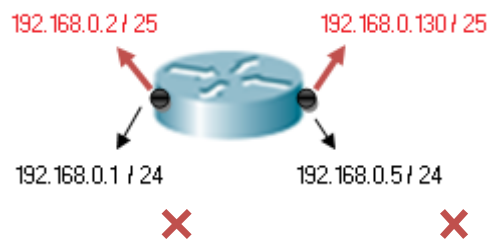
جواب : وقتی در لایه ۲ یک IP را با Mac Broadcast می دهیم درسته که Switch آن را از همه Port هایش خارج می کند ولی فقط یک سیستم خودش را صاحب Packet می داند، فریم به دست همه می رسد ولی فقط یک نفر خودش را صاحب Packet می داند.

توی Broadcast لایه ۳ درسته که Switch باید آن را به همه بفرستد یعنی Broadcast لایه ۳ باید وصل شود به Mac Broadcast ، یک Packet به دست همه می رسد و همه فکر می کنند که صاحب Packet هستند.

انواع ترافیک در شبکه :

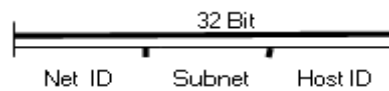


فرض کنید ما به 10 Host نیاز داشته باشیم آن وقت 8 Bit برایش زیاد است که خواهیم جا بگذاریم در این جا می آییم از بیت‌های قسمت Host به قسمت Net ID قرض می دهیم.

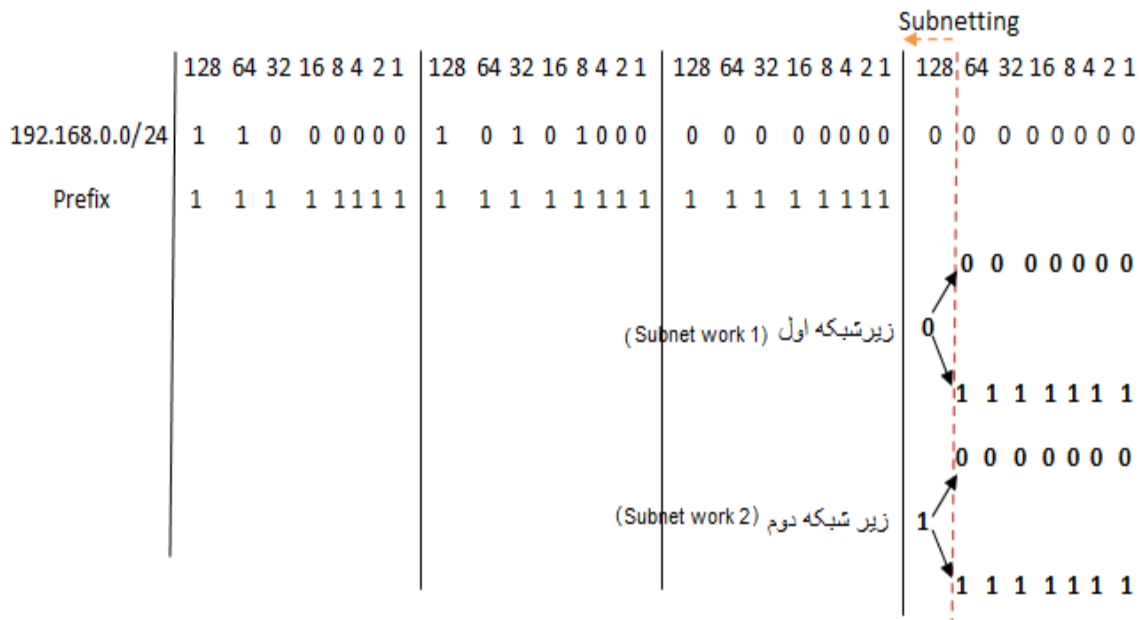


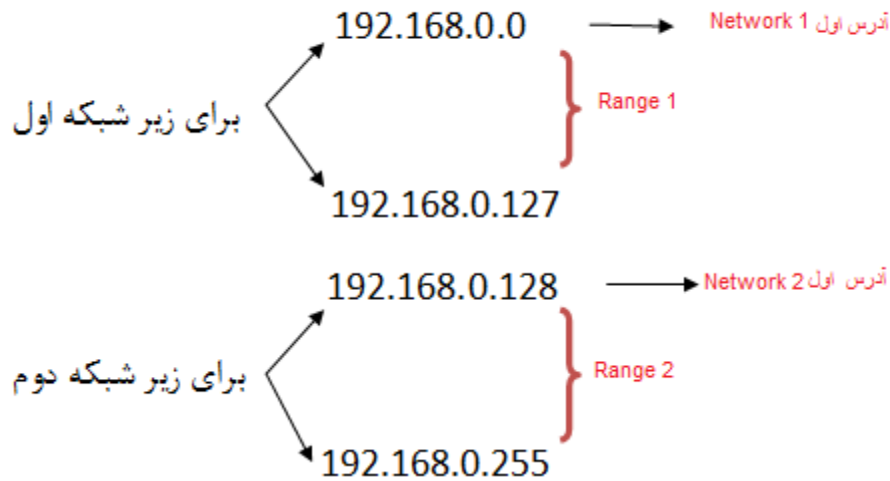
با توجه به شکل اگر Router ، 10 تا دست هم داشته باشد باید IP دست ها دارای Net ID برابر باشند اگر غیر از این خواهیم IP دهی کنیم Router نپذیرفته و پیغام Overlap (همپوشانی) می دهد و نمی توانیم اینگونه عمل کنیم پس باید چکار کنیم؟

فرض کنید 192.168.0.0/24 را خریده ایم اگر اعتقاد داریم که 8 bit برای Host است و دست ماست می توانیم از بیت های Host ببخشیم به Net ID. اگر یک بیت قرض بدهیم دو احتمال بوجود می آید اگر دو بیت قرض بدهیم 4 احتمال بوجود می آید:



به عملیات قرض دادن از بیت های Host به Net ID به منظور تولید Subnet Work های بیشتر و به طبع آن کم شدن تعداد Host در هر Range، Subnetting گفته می شود.





مثال: معادل Prefix ، Subnet Mask های زیر را بنویسید.

الف) 25: 255.255.255.128/25

ب) 26: 255.255.255.192/26

ج) 27: 255.255.255.224/27

نکته: از Octet آخر نمی توانیم ۷ بیت قرض بگیریم:

چون احتمالات تعداد Host می شود: $2^1 - 2 = 0$

پس نمی شود.

مثال: IP ، 10.0.1.0 / 24 را در اختیار داریم آن را تبدیل به 26/ می نمایم.

الف) در هر Range چه تعداد IP تولید می شود؟

ب) در هر Range چه تعداد Host را می توان IP دهی کرد؟

ج) Range های آن را بنویسید.

جواب:

الف) $2^6 = 64$ $/24 \longrightarrow /26$

ب) $2^6 - 2 = 62$

ج) $\left\{ \begin{array}{l} 10.0.1.0 \text{ _ } 10.0.1.63 \\ 10.0.1.64 \text{ _ } 10.0.1.127 \\ 10.0.1.128 \text{ _ } 10.0.1.191 \\ 10.0.1.192 \text{ _ } 10.0.1.255 \end{array} \right.$

مثال (آیا با $/26$ آدرس IP : 10.0.1.63، valid است ؟

جواب : خیر چون این آدرس Broadcast ، Range 1 هست و Invalid است.

مثال (با توجه به Subnet Mask 255.255.255.224 کدام 3 ، IP زیر Valid هستند ؟

- A) 172.22.243.127
- B) 172.22.243.191
- C) 172.22.243.190
- D) 10.16.33.98
- E) 10.17.64.34
- F) 192.168.1.160

جواب: C,D,E

نکته: ۳ تا Octet اول هرچی میخواهد باشه به آن کاری نداریم فقط Octet چهارم را نگاه می کنیم.

هر آدرسی که بین Range های زیر باشد قابل قبول است:

آدرس Network ها	آدرس Broadcast
0	31
32	63
64	95
96	127
128	159
160	191
192	223
224	255

مثال) IP ، 192.168.0.94/27 را داریم آدرس Network آن را بنویسید .

Range:

0	31	
32	63	
64	95	→ IP داده شده در این Range است
96	127	
128	159	
160	191	
192	223	
224	225	

آدرس Network : 192.164.0.64/27

مثال : IP ، 1.0.0.0/30 را در اختیار داریم (24/ بوده که به Subnet/30 تبدیل شده

است) چند Subnet work تولید شده است؟ 4 ، Range اولیه آن را بنویسید.

Range یا Subnet Work تعداد کل یا IP های تولید شده در هر range $2^2 = 4$ $32 - 30 = 2$

Range :

1.0.0.0 تا 1.0.0.3

1.0.0.4 تا 1.0.0.7

1.0.0.8 تا 1.0.0.11

1.0.0.12 تا 1.0.0.15

چگونه بفهمیم کدام IP ، Private یا Public است ؟

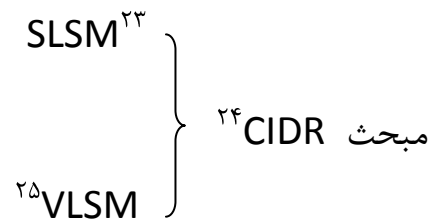
Private IP Range	}	10.0.0.0/8	10.0.0.0 _ 10.255.255.255
		172.16.0.0/12	172.16.0.0 _ 172.31.255.255
		192.168.0.0/16	192.168.0.0 _ 192.168.255.255

سوال : اگر آدرس Public را در شبکه Private بگذاریم چی می شود؟

هیچی نمی شود کار هم می کند اما هر چیزی که از عرفش خارج شود قطعاً مشکلاتی را در بر خواهد داشت مثلاً: وبسایت هایی که Service می دهند همگی IP Public دارند بعد اگر ما IP سایت یاهو را در شبکه داخلی گذاشته باشیم از آن به بعد هر وقت که آن IP را بزنیم دیگر نمی رود یاهو را باز کند بلکه PC شبکه داخلی را باز می کند.

جلسه چهارم

تا حالا می گفتیم که مثلاً 25/ داریم که می شد 7 تا بیت برای Host که می توانستیم 2^7 ،
IP داشته باشیم و $2^7 - 2$ تا Host حالا می خواهیم برعکسش را عنوان کنیم.

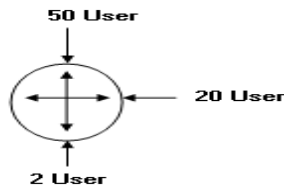


SLSM وقتی کاربرد دارد که بازه User ها نزدیک به هم باشد مثلاً {55, 50, 60}، می آید
بیشترین تعداد کاربر را در نظر می گیرد برای بقیه هم همان را محاسبه می کند مهم هم
نیست چقدر می خواهد هدر برود.

VLSM زمانی که بخواهیم با کمترین هدر رفت IP دهی کنیم.

مثال: فرض کنید یک IP به ما دادند: 10.0.0.0

این IP را چگونه بین User ها تقسیم کنیم که کمترین هدررفت IP را داشته باشیم.



²³ Same Length Subnet Mask

²⁴ Classless Inter-Domain Routing

²⁵ Variable Length Subnet Mask

جواب:

دقت کنید که وقتی یک IP به ما می دهند آدرس Network را می دهند.

$$2^H - 2 \geq n \rightarrow \text{تعداد user ها}$$

$$2^H - 2 \geq 50 \rightarrow 2^H \geq 52 \rightarrow \boxed{H = 6} \quad 2^6 = 64 \text{ تعداد پرش}$$

$$32 - 6 = 26 : \text{Prefix}$$

Subnet Mask : 255.255.255.192

Net 1 : 10.0.0.0/26 تا 10.0.0.63/26

$$2^H - 2 \geq 20 \rightarrow 2^H \geq 22 \rightarrow \boxed{H = 5} \quad 2^5 = 32 \text{ تعداد پرش}$$

$$32 - 5 = 27 \rightarrow 8.8.8.3 \rightarrow \text{Subnet Mask : 255.255.255.224}$$

تعداد بیت های Net ID در هر Octet

Net 2 : 10.0.0.64/27 تا 10.0.0.95/27

$$2^H - 2 \geq 2 \rightarrow 2^H \geq 4 \rightarrow \boxed{H = 2} \quad 2^2 = 4 \text{ تعداد پرش}$$

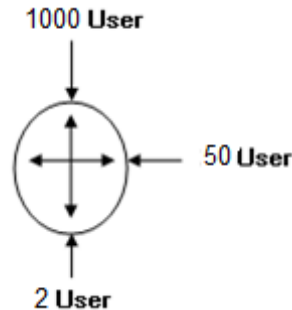
$$32 - 2 = 30 \rightarrow \boxed{8.8.8.6} \rightarrow \text{Subnet Mask: 255.255.255.252}$$

تعداد بیت های Net ID در هر Octet

Net 3 : 10.0.0.96/30 تا 10.0.0.99/30

مثال: فرض کنید یک IP به ما دادند: 10.0.0.0

این IP را چگونه بین User ها تقسیم کنیم که کمترین هدررفت IP را داشته باشیم.



$$2^H - 2 \geq 1000$$

$$2^H \geq 1002 \rightarrow \boxed{H=10} \rightarrow 2^{10} = 1024 \text{ تعداد پرش}$$

$$32 - 10 = 22 \rightarrow \text{8.8.6.0} \rightarrow \text{Subnet Mask : 255.255.252.0}$$

$H=2$ $H=8$
 $2^2 = 4$ پرش $2^8 = 256$ پرش

Net 1 : 10.0.0.0/22 تا 10.0.3.255

$$2^H - 2 \geq 50$$

$$2^H \geq 52 \rightarrow \boxed{H=6} \rightarrow 2^6 = 64 \text{ تعداد پرش}$$

$$32 - 6 = 26 : \text{Prefix} \rightarrow \text{8.8.8.2}$$

$H=0$ $H=0$ $H=0$ $H=6$
 $2^6 = 64$ پرش

Net 2 : 10.0.4.0/26 تا 10.0.4.63/26

$$2^H - 2 \geq 2 \rightarrow 2^H = 4 \rightarrow H = 2 \quad 2^2 = 4 \text{ تعداد پرش}$$

Net 3 : 10.0.4.64/30 تا 10.0.4.67/30

برای اینکه بینیم دو کامپیوتر در یک شبکه با هم ارتباط دارند یا نه

با استفاده از دستور زیر در محیط Cmd :

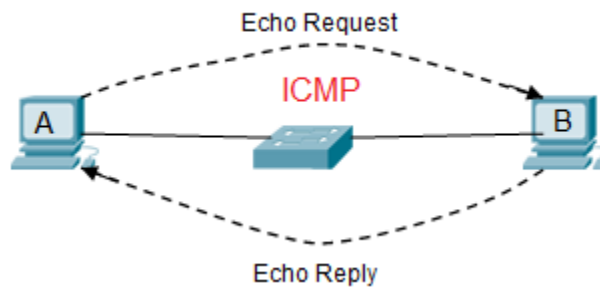
C:\> ping <Dst IP>

مثلاً نشستیم پشت PC A می خواهیم بینیم با PC B ارتباط داریم یا نه با استفاده از دستور زیر در محیط Cmd :

ping 1.0.0.2

PCB IP

در این Command یک فرآیند دو مرحله ای پیش می آید:



از PC A بسته ای به PC B فرستاده می شود و منتظر جواب برگشتش می ماند به بسته ای که می فرستد اصطلاحاً می گویند Echo Request و به بسته ای که بر می گردد اصطلاحاً Echo Reply می گویند .

این دو فرآیند متعلق به پروتکلی است به نام ICMP^{۲۶} پس ICMP پروتکل Ping است و Ping با پروتکل ICMP کار می کند.

در اثر زدن دستور Ping ، 4 خط یا بیشتر ایجاد می شود، حالت های مختلفی ممکن است پیش آید :

1

Echo Request رفته اما Echo Reply بر نگشته این یعنی ارتباط برقرار نیست اما مشکل از طرف مقابل است و به دلایلی نتوانسته بسته را برگرداند : Request Time out

```
C:\Users\Faraz>ping 192.168.40.30
Pinging 192.168.40.30 with 32 bytes of data:
Request timed out. |
Request timed out. |
Request timed out. |
Request timed out. |
```

ممکن است ۴ خط را به صورت زیر ببینیم:

2

```
C:\Users\Faraz>ping yahoo.com
Pinging yahoo.com [98.138.253.109] with 32 bytes of data:
Reply from 98.138.253.109: bytes=32 time=335ms TTL=44
Reply from 98.138.253.109: bytes=32 time=711ms TTL=44
Reply from 98.138.253.109: bytes=32 time=328ms TTL=44
Reply from 98.138.253.109: bytes=32 time=291ms TTL=44
```

²⁶Internet Control Message Protocol

این یعنی دو سیستم همدیگر را شناختند و با هم در ارتباطند و با Time ی که بسته Echo Request می رود و برمی گردد ارتباط دارند حجم بسته ای که برای IP B قرار داده می شود 32 byte است (که حجم بسته قابلیت تغییر هم دارد)، TTL عمر بسته است.

فرض کنید به ما به عنوان Admin شبکه گفته می شود که D pc به شبکه وصل نیست.

ما از D pc ، ping می گیریم که ۴ خط برای ما نشان می دهد بعد می رویم پشت سیستم D ببینیم مشکل چیست و نیاز داریم که بیشتر از ۴ خط نشان داده بشود با گذاشتن یک -t

کنار دستور ping این کار انجام می شود: `ping<ip>-t`

بعد شروع می کنیم به عیب یابی سیستم D مثلاً فرض کنید که کابلش قطع بوده کابل رو وصل می کنیم و می بینیم که ارتباط وصل می شود.

این دستور ادامه پیدا می کند تا زمانی که ما `ctrl + c` را بزنیم.

3

اگر یک سیستم کابلش وصل نباشد و بدین صورت اتصال برقرار نباشد در این حالت Echo Request نمی رسد و پیغام برگشت می آید که من نرسیدم!



یعنی مشترک مورد نظر در دسترس نمی باشد.

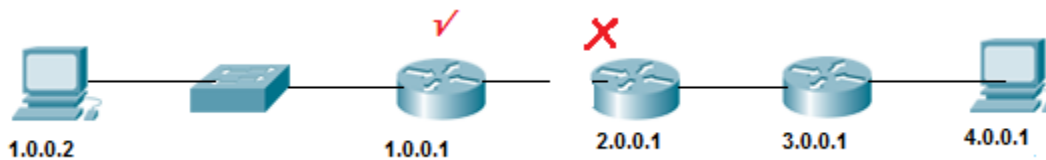
درواقع می داند Network را چکار کند اما نمی داند آن Host در آن Network کجاست می گوید:

Reply: Destination Host unreachable

```
C:\Users\Faraz>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.
```

4

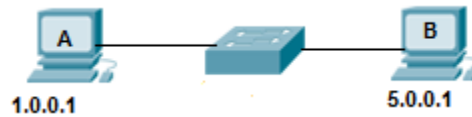
با توجه به شکل اگر خواهیم بسته ای را از 1.0.0.2 به 4.0.0.1 بفرستیم



اما بسته تا Router 1.0.0.1 رفته و از آنجا به بعد نرفته این دستور می گوید که آخرین IP که رسیدیم و Ack ش را گرفتیم 1.0.0.1 است اگر router table خودش نمی دانست 4.0.0.1 را چکار کند یعنی Net ID اش را نمی شناخت ما 4 خط را به صورت زیر می بینیم :

Reply From 1.0.0.1: Destination net unreachable

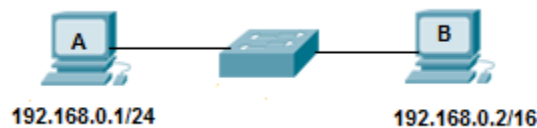
نکته: در شکل زیر هر جور که حساب کنیم دو سیستم نمی توانند باهم ارتباط داشته باشند:



اما اگر PC A ، ARP کند ، ARP به دست PC B می رسد و سیستم B تا لایه ۳ بالا می آورد و می بیند هم Net ID نیستند پس جواب ARP را نمی دهد.

نتیجه اینکه در هر صورت ARP از همه port های سوئیچ رد می شود.

نکته: با توجه به شکل زیر آیا بسته می تواند از سیستم A به سیستم B برسد؟

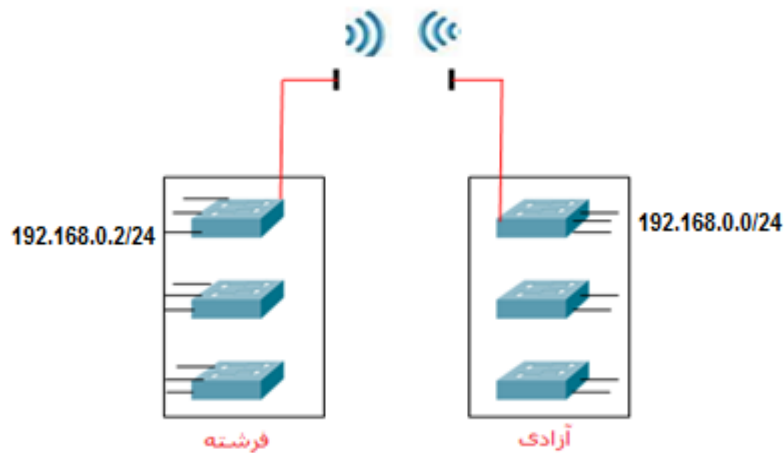


بله ، در یک ارتباط در شبکه LAN (یعنی شبکه ای که وسطش سوئیچ باشد) کامپیوتر فرستنده IP مقصد را با mask خودش مقایسه می کند و نتیجه می گیرد که آیا با کامپیوتر مقصد هم Net ID می باشد یا خیر.

یعنی در این شکل برای ارسال بسته از سیستم A به سیستم B ، 192.168.0.1 ، 192.168.0.2 را به چشم /24 می بیند ، بعد می بیند که آیا هم Net ID هستند یا نه در مسیر برگشت هم 192.168.0.2 می گوید که طرف مقابل به صورت /16 باید با من هم Net ID باشد.

ادامه مبحث LAN و WAN :

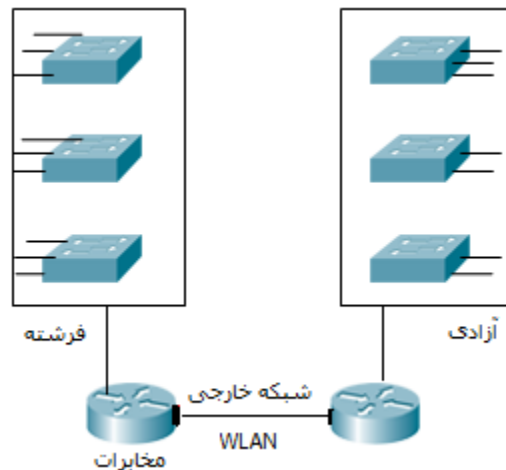
فرض کنیم بالای هر ساختمان یک دکل گذاشته ایم داخل هر ساختمان یک سری سوئیچ داریم که ارتباطات داخلی را در یک شبکه شکل می دهند به کامپیوترهای زیادی وصل هستند که می آییم ۲ تا دستگاه Wireless می گذاریم که این ۲ همدیگر را می بینند و یک سیم از یکی از سوئیچ ها رفته به آن دستگاه .



این یک شبکه LAN است یعنی هر دو طرف Net ID یکسان دارند.

یک مشکلی وجود دارد و آن این است که اگر فردا یک برج بین این دو ساختمان ساخته شد دیگر این ۲ دستگاه به همدیگر دید نداشته و این ارتباط قطع می شود.

این مشکل را این گونه می شود حل کرد که بیاییم و از مخابرات یک router اجاره کنیم مثلاً 64k که ارتباط را از ۲ طرف بگیرد >> در این صورت یک شبکه خارجی خواهیم داشت که Range ها متفاوت می شود. به این شبکه خارجی WAN می گویند.



نتیجه اینکه یک شبکه LAN می تواند WAN هم باشد بعضی جاها نمی توانیم از LAN استفاده کنیم چون همه جا دید مستقیم نداریم.

× کسی که مودم ما را در خانه تنظیم کند می گوید IP مودم (Gateway) هست مثلاً: 192.168.0.1، ما بلد نیستیم چگونه باید این IP مودم را عوض کنیم حالا باید چکار کنیم؟

می توانیم بیایم IP شبکمان را عوض کنیم مثلاً: (هر چیزی). 192.168.0.5 مثلاً:

(با توجه به IP مودم این کار را کردیم Net ID را برابر همان IP مودم گذاشتیم مقدار Host را دلخواه) پس ما باید یا IP کامپیوترمان را بگذاریم روی range Gateway یا برعکس.

حالا فرض کنید ما هزار تا کامپیوتر در یک شبکه داریم عوض کردن IP همه این 1000 کامپیوتر که سخت است! مجبوریم که IP خود Gateway را عوض کنیم.

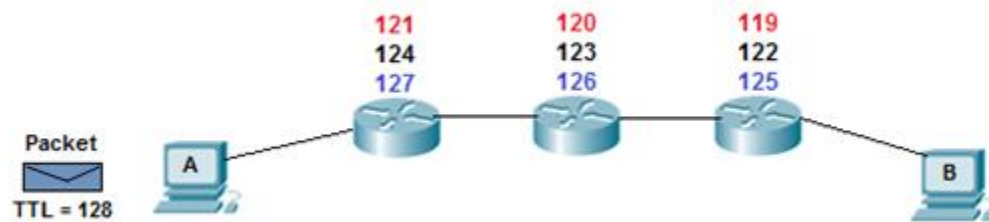
نحوه تغییر دادن Default Gateway :

در محیط cmd ، با زدن دستور ipconfig /all ، Default Gateway IP را پیدا می کنیم و آن IP را کپی کرده و می بریم داخل Browser خود paste می کنیم، در صفحه ای که باز می شود user و password را admin می زنیم باز می شود!

بعد در صفحه تنظیمات router قسمت WLAN آدرس Gateway را تغییر می دهیم.

TTL (مدت زمان عمر بسته)

این مقدار درون packet وجود دارد و به ازای هر دستگاه لایه ۳ یک عدد از مقدار آن کم می شود با این حساب اگر بسته ای در یک تبادل به هر دلیل به مقصد خود نرسد و مجدد ارسال شود (این قسمت در لایه ۴ اتفاق می افتد) به ازای هر router که در مسیر رفت رد می کند آن قدر این مقدار کم می شود تا این مقدار به صفر برسد و در اینجا عمر بسته به پایان می رسد.



مثلاً: با توجه به شکل فرض کنید یک بسته ای از سیستم A قرار است به سیستم B فرستاده شود با TTL = 128 (این مقدار را مقصد تعیین می کند و بین 0-255 است) آنقدر فرستاده

می شود تا TTL صفر شود بعد اگر پیدا نشد می نویسد The page cannot Display

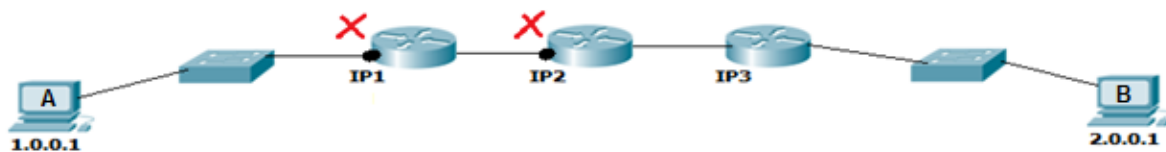
سایت هایی که بیشتر طول می کشد تا این پیغام بیاید یعنی TTL بیشتری روی آنها Set شده است که مقدارش قابل تغییر است اما کلاً به صورت اتوماتیک Set می شود.

ولی در شبکه داخلی ثانیه دارد مثلاً می گوید بعد از چند بار ارسال مدتش تمام می شود.

دستور Trace Route: در لینوکس به این صورت نوشته می شود اما در مایکروسافت

Tracert نوشته می شود.

× نرم افزار visual route را دانلود کنیم رد شدن بسته را بصورت گرافیکی نشان می دهد.
 به طور مثال: با توجه به شکل زیر اگر در pc A دستور Tracert را بزنیم بسته 1 تولید می شود، بعد می آید می رسد به router می بیند چون بسته از نوع Trace است جواب اطلاعات IP 1 خودش را بر می گرداند IP 1 را با IP Dst مقایسه می کند اگر یکسان بود تمام می شود در غیر این صورت بسته 2 تشکیل می شود سمت router 2 رفته اطلاعات IP 2 را بر می گرداند می شود خط 2، IP 2 را با IP Dst مقایسه می کند اگر یکسان بود تمام می شود در غیر این صورت بسته 3 تشکیل می شود این قدر این کار را می کنیم تا IP N = IP Dst شود.



	IP1	TTL
1	1.0.0.1 2.0.0.1	1
2	1.0.0.1 2.0.0.1	2
3	1.0.0.1 2.0.0.1	3

این دستور دستگاه های لایه ۳ را که از آنها رد می شویم را نشان می دهد. مثلاً می خواهیم ببینیم چگونه به Google رسیده ایم :

در محیط cmd می زنیم : `tracert Google.com`

یک سری مسیر و IP برای ما نشان داده می شود ، برای اینکه ببینیم بعضی IP ها برای کجاست می توانیم IP مورد نظر را کپی کرده (mark + Enter) و بعد در Google ، Search کنیم `where is my ip` یک سری سایت های را نشان می دهد که آن ها قادر هستند مکان IP را به ما نشان دهند، IP کپی کرده را در کادر قرار داده شده در این سایت ها Paste می کنیم.

× اگر از یک جایی به بعد ستاره گذاشته شده بود یعنی از آنجا به بعد بسته نتوانسته عبور کند.

× اگر یک خط ستاره بود دوباره ادامه پیدا کرده بود 2 حالت دارد:

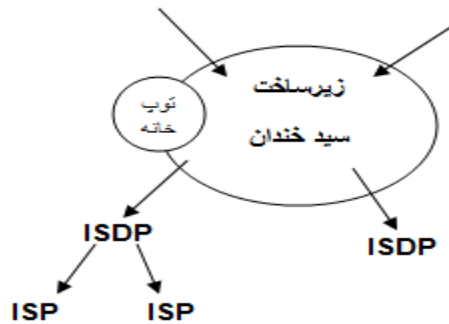
(۱) یا router ی بوده که load آن پر شده و داده به router بعدی.

(۲) این دستگاه نمی خواهد خودش را به ما بشناساند و نمی خواهد جواب `trace` را

برگرداند که دستگاه های امنیتی به این شکل هستند.

× زیرساخت مخابرات کجاست؟

جایی است که اینترنت ما می آید در آنجا و آن موظف است در ایران که به همه ISDP ها اینترنت دهد و IP در اختیارشان قرار دهد فرقی با مخابرات در این است که مخابرات کارهای تلفنی را انجام می دهد ولی زیر ساخت مسائل شبکه و IP را انجام می دهد.



بعد از زیرساخت شبکه اینترنت را داریم.

لینک های اصلی اینترنت می آید تو زیرساخت بعد زیر ساخت می دهد به ISDP ها که یک سری مجوز هستند که از سازمان مقررات رادیویی گرفته می شود مانند شاتل ، ISP شرکت های کوچکتر هستند مانند شهرداد (شهرداد از شاتل مجوز می گیرد)
× در حال حاضر دیگر مجوز ISP صادر نمی شود.

سوال مهم: اگر اتصال به اینترنت قطع بود چکار کنیم؟

اول بصورت فیزیکی media را چک می کنیم بعد IP ، 8.8.8.8 را ping می کنیم اگر پیغام General Gateway داد یعنی gateway نداریم یا اشتباه است باید برویم و

Gateway را Set کنیم مثال کلاس را فرض کنید باید برویم از بخش فنی سایبر تک
 بپرسیم IP router چیست آن را که بدست آوردیم Set می کنیم بعد دوباره ping می
 کنیم 8.8.8.8 را ببینیم جواب می دهد.

× به هر router در اصطلاحات شبکه Hop می گویند.

× اسم دیگر Default Gateway ، Next Hop IP است.

× اگر IP در Octet اول 127.x.x.x بود یعنی برو خودت را ping کن به این IP، Local

Host می گویند که برای تست کارت شبکه است، اگر در Browser مرورگر کامپیوتر

خود 127.9.9.1 را بزنیم منظور این است که برو به یک وبسایتی از کامپیوتر خودم را باز

کن اگر روی کامپیوتر خود وبسایت داشته باشیم باز می شود در غیر این صورت نمی شود.

سوال: فرق Error Detection لایه ۲ با Error Detection لایه ۳ چیست؟

جواب: فرقی نمی کند، Error Detection لایه ۲، Header لایه ۲ را چک می کند،

جواب Fcs را در Trailer می گذارد.

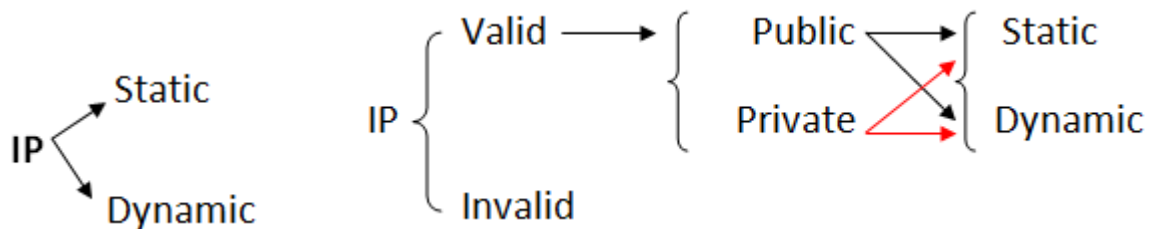
Error Detection لایه ۳، Header لایه ۳ را چک می کند و جواب Fcs را در

Header خود می گذارد.

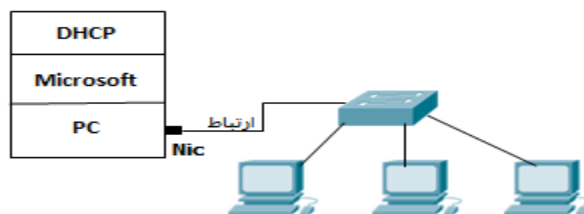
: Decapsulation_Encapsulation

به عمل اضافه شدن Header در هر لایه از OSI و در غالب یک package تحویل لایه پایینی دادن Encapsulation و به عملیات باز شدن Header در لایه مقصد و خوانده شدن Header توسط لایه نظیر Decapsulation گفته می شود.

: تقسیم بندی IP از لحاظ Assign یا تخصیص دادن IP



یک سرویسی هست بنام DHCP^{۲۷} که کارش IP دادن به صورت اتوماتیک است. هر دستگاه لایه ۳ می تواند این سرویس را ارائه دهد اما خودش یک application لایه ۷ است.



²⁷Dynamic Host Configuration Protocol

فرض کنید یک کامپیوتر داریم که بر رویش مایکروسافت نصب باشد و بر رویش سرویس DHCP ، run باشد و یک کارت شبکه داشته باشد که این کارت شبکه خود یک سوئیچ و یک تعدادی pc به آن وصل باشد و به تعداد pc ها تنظیمات IP Address آنها در حالت obtain باشد در این صورت چه اتفاقی می افتد؟

تمام سیستم ها شروع می کنند به Request فرستادن ، این Request به دست همه فرستاده می شود و DHCP پاسخ می دهد که از روی type بسته می فهمد که باید جواب دهد DHCP داخل خودش Scope(Pool) دارد ، استخر IP را ادمین تعریف می کند مثلاً می گوید من یک Pool دارم از 192.168.0.1 تا 192.168.0.10 ، اولین درخواست که می آید سمتش 192.168.0.1 را به آن می دهد دومین که می آید 192.168.0.2 را به آن می دهد و ثبت می کند که من این IP Address را دادم به این Mac Address و در یک جایی داخل جدول خودش نگهداری می کند تا یک زمانی به نام Lease Duration که می توانیم این زمان را تغییر دهیم مثلاً وقتی pc ها ثابت هستند و همیشه همان ها هستند زمان Lease Duration را بالا می بریم و جاهایی مثلاً فرودگاه که دستگاه هایی که می آید و می رود متنوع هستند برای اینکه range مان تمام نشود Lease Duration را پایین می آوریم مثلاً ۱ ساعت یعنی ۱ ساعت این IP برای فلان دستگاه باشد اگر تمدید نکرد IP ش را می دهیم به دستگاه بعدی حالا چند تا شک بوجود می آید :

۱) اگر سیستم ها در حالت obtain قرار بگیرند درخواست بفرستند اما این ارتباط برقرار نشود چه می شود؟ سیستم ها شروع می کنند به درخواست دادن چندین بار، وقتی درخواست بر نمی گردد داخل شبکه LAN بنا را می گذاریم به حساب نبودن DHCP . در صورتی که تنظیمات یک سیستم بر روی obtain باشد اما DHCP در شبکه موجود نباشد پس از گذشت یک مدت زمانی آن سیستم به صورت اتوماتیک از رنجی بنام APIPA²⁸، IP می گیرد این Range با 169.254 شروع شده و به صورت 16/ می باشد و دو Octet آخر را به صورت random می گذارد.

169.254.X.X/16

× در خانه ما DHCP روی مودم است که به pc ما IP می دهد که اگر بخواهیم IP هایش را ببینیم ipconfig /all می گیریم.

۲. در صورتی که تنظیمات مربوط به DHCP در یک شبکه تغییر یابد برای اینکه این تغییرات بر روی سیستم ها اعمال شود می توان از چند راه استفاده کرد :

الف) خاموش و روشن کردن pc !!

ب) Enable / Disable کردن کارت شبکه

ج) زدن دستور ipconfig /release (سیستم هر IP که از DHCP گرفته را رها می

کند) و در ادامه ipconfig /renew (دوباره گرفتن IP) .

²⁸Automatic Private IP Address

× Server ها باید قابلیت شناسایی یک جا باشند در نتیجه IP Static می گیرند.

جلسه پنجم

ابزارهایی که در کلاس بررسی کردیم:

- یک Point Wireless دیدیم بنام Nanostation ، انواع مختلفی دارد یک نوع loco دارد که کوچکتر است یک آنتن wireless دارد که قادر است مسافت زیادی مثلاً 2km یا بیشتر را از لحاظ شبکه به هم اتصال بدهد.

- دستگاهی به نام tester کابل شبکه دیدیم که ۲ قسمتی بود کابل شبکه را برای ما تست می کند که ببینیم همه سیم هایش را درست زدیم یا نه، یک طرف کابل شبکه را می زنیم به یک قسمت دستگاه طرف دیگرش را به قسمت دیگر دستگاه می زنیم بعد با on کردنش شروع می کند به پالس فرستادن توی تک تک رشته های کابل بعد می گوید مثلاً ۱ این طرف روشن می شود باید ۱ طرف دیگر هم روشن شود اگر ۲ یک طرف روشن شود ۲ طرف دیگر هم باید روشن شود مگر اینکه کابل Cross خورده باشد که در این صورت ۱ این طرف روشن شود ۳ طرف مقابل باید روشن شود ۲ یک طرف روشن شود ۶ طرف دیگر باید روشن شود ، مزیتش این است که مثلاً در یک شبکه که یک تعداد زیادی کابل پشت PC ها وجود دارد که همه آنها رفتند در یک سوئیچ می رویم کابل شبکه پشت PC A را می کشیم و می زنیم به دستگاه کابل های داخل سوئیچ را هم یکی یکی امتحان می کنیم دستگاه را نگاه می

کنیم با زدن کدام کابل چراغ ها روشن می شود راه دیگر این است که یکی را بفرستیم کنار سوئیچ که به آن نگاه کند بعد کابل PC مورد نظر را بکشیم و بعد بپرسیم که کدام port سوئیچ خاموش شد!!!!!!

- سوئیچ ها دو نوع هستند :

Manageable, unmanageable

سوئیچ های D-Link اغلب جز سوئیچ های مدیریت ناپذیر هستند که به جز port های LAN جای Port دیگری ندارند که بخواهیم با دستگاه ارتباط کنیم و تنظیمش کنیم.

سوئیچ های مدیریت پذیر یک port دارند که برویش نوشته Console که با استفاده از آن می توانیم به محیط ترمینال دستگاه وصل شویم.

- شبکه کلاس را خودمان Set کردیم، سناریو این گونه بود که تمامی کامپیوترهایمان از کابل شبکه خودش در آمد ، کابل جدید برداشتیم یک سرش را در کارت شبکه PC خودمان و سر دیگرش را در port سوئیچ کردیم ، سوئیچ ها را به هم وصل کردیم همه وصل شدن به هم و جلو آمده در نهایت رفتند در داخل یک سوئیچ زیر میز استاد، بعد 192.168.40.30 (IP یکی از سیستم های موجود در شبکه) را ping گرفتیم و دیدیم که ارتباط داریم تا اینجا توانستیم بستر شبکه را بوجود آوریم.

4_Transport

لایه ۴

TCP IP : تعیین کننده سرویس درخواستی از کامپیوتری که ما از آن درخواستی کردیم،

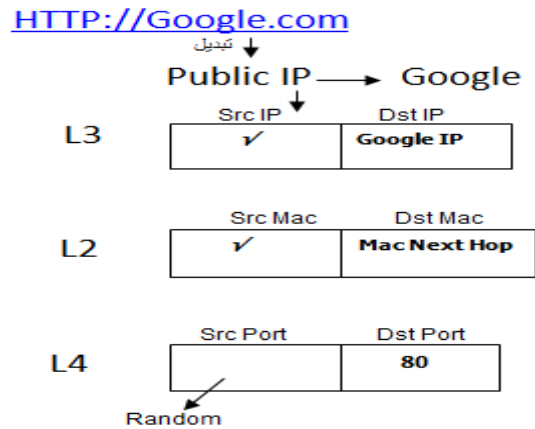
برای این کار در لایه ۴ چیزی داریم به اسم Port Number (این port با port سوئیچ فرق می کند)

این یک مفهوم logic است، Port Number یک عدد است، ما می توانیم از 0_65535 (یعنی ۱۶ بیت) تا port داشته باشیم، در سیستم از 0_1024 آن را اصطلاحاً Well Known Ports که port های معروف هستند می گویند.

تعریف Port : به حفره های Logic ی (منطقی) در دل سیستم عامل Port گفته می شود.

هر Port با توجه به سرویس یا نرم افزار خاصی در یک سیستم گشوده می شود به عنوان مثال اگر نرم افزار VNC بر روی کامپیوتر نصب نباشد Port مربوط به آن باز نخواهد بود و سایر کامپیوترهای شبکه نمی توانند به آن متصل شوند.

مثال: اگر در Browser کامپیوتر خود آدرس [HTTP://Google.com](http://Google.com) را وارد کنیم



در واقع گفتیم:

1. Google.com باید تبدیل شود به IP (Public IP مربوط به Google).
2. کامپیوتر ما می آید به عنوان Src IP ، IP خودش را می گذارد و به عنوان Dst IP ، Google IP را می گذارد توی لایه ۲ بسته اصلی می آید Src Mac که دارد را گذاشته و به جای Dst Mac ، Mac Next Hop را می گذارد ، اتفاق دیگری که می افتد این است که در لایه ۴ یک چیز دیگری به بسته اضافه می کند و می گوید دارم Src Port ، Dst Port بعد نگاه می کند می بیند چون آدرس داده شده HTTP هست باید Dst Port را بنویسیم 80 چون Port 80 برای سرویس HTTP تعریف شده است.

نحوه نوشتن Port به این صورت است: IP:Port

با دستور زیر می توانیم Port های باز سیستم خود را در لحظه و ارتباطاتی که در لحظه با هم گرفته شده است را مشاهده کنیم :

C:\>netstat-na


```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Faraz>netstat -na

Active Connections

Proto Local Address           Foreign Address         State
TCP    0.0.0.0:80               0.0.0.0:0               LISTENING
TCP    0.0.0.0:135              0.0.0.0:0               LISTENING
TCP    0.0.0.0:445              0.0.0.0:0               LISTENING
TCP    0.0.0.0:554              0.0.0.0:0               LISTENING
TCP    0.0.0.0:1025             0.0.0.0:0               LISTENING
TCP    0.0.0.0:1026             0.0.0.0:0               LISTENING
TCP    0.0.0.0:1027             0.0.0.0:0               LISTENING
TCP    0.0.0.0:1029             0.0.0.0:0               LISTENING
TCP    0.0.0.0:1030             0.0.0.0:0               LISTENING
TCP    0.0.0.0:1037             0.0.0.0:0               LISTENING
TCP    0.0.0.0:1433             0.0.0.0:0               LISTENING
TCP    0.0.0.0:2869             0.0.0.0:0               LISTENING
TCP    0.0.0.0:5357             0.0.0.0:0               LISTENING
TCP    0.0.0.0:10243            0.0.0.0:0               LISTENING
TCP    127.0.0.1:1028           127.0.0.1:5354          ESTABLISHED
TCP    127.0.0.1:1033           127.0.0.1:27015         ESTABLISHED
TCP    127.0.0.1:1434           0.0.0.0:0               LISTENING
TCP    127.0.0.1:2559           0.0.0.0:0               LISTENING
TCP    127.0.0.1:5354           0.0.0.0:0               LISTENING
TCP    127.0.0.1:5354           127.0.0.1:1028          ESTABLISHED
TCP    127.0.0.1:27015         0.0.0.0:0               LISTENING
TCP    127.0.0.1:27015         127.0.0.1:1033          ESTABLISHED
TCP    192.168.1.101:139       0.0.0.0:0               LISTENING
TCP    [::]:80                  [::]:0                  LISTENING
TCP    [::]:135                 [::]:0                  LISTENING
TCP    [::]:445                  [::]:0                  LISTENING
TCP    [::]:554                  [::]:0                  LISTENING
TCP    [::]:1025                 [::]:0                  LISTENING
TCP    [::]:1026                 [::]:0                  LISTENING
TCP    [::]:1027                 [::]:0                  LISTENING
TCP    [::]:1029                 [::]:0                  LISTENING
TCP    [::]:1030                 [::]:0                  LISTENING

```

طرف سرویس گیرنده Port را برای اینکه می خواهد یک سرویسی درخواست کند مقدار Port خود را یک مقدار Random که از طرف کامپیوتر Set می شود که بالاتر از 1024 است، بسته برود و برگردد بعد رها می کند آن Port صرفاً برای بردن و برگرداندن درخواست است.

حالا این Src Port به چه دردی می خورد؟

برای مبدا است و برگرداندن درخواست به آنجا مثلاً فرض کنید توی Firefox دو تا Tab باز می کنیم هر کدام از Tab هایی که باز می کنیم Port مخصوص به خودشان را بر میدارند شماره Port های معروفی که باید حفظ باشیم:

Protocol	Port Number	Protocol	Port Number
HTTPS	443	²⁹ Pop3	110
³¹ SMTP	25	³⁰ DNS	53
³³ RDP	3389	³² IMAP	143

× وقتی یک وبسایت راه می افتد Port 80 را به سمت دنیای بیرون باز می کند. مثلاً فرض کنید ما یک وب سرور داریم که می خواهد به دنیای شبکه ارائه سرویس کند در مایکروسافت سرویسی هست به نام ³⁴IIS (در لینوکس سرویسی هست به نام APACHI که می تواند Port 80 را باز کند) که اگر برویم آن را فعال کنیم Port 80 روی PC ما باز می شود و ما خواهیم توانست سرویس Web ارائه دهیم.

²⁹ Post Office Protocol

³⁰ Domain Name System

³¹ Simple Mail Transfer Protocol

³² Internet Message Access Protocol

³³ Remote Desktop Protocol

³⁴ Internet Information Services

چگونگی فعال شدن IIS :

Start > Control Panel > Programs > Programs and Features
(Turn windows features on or off) > Internet Information
Service

این قسمت را تیک کلی زدیم. حالا port 80 روی pc ما باز شده و می توانیم سرویس web ارائه دهیم.

وقتی سرویس IIS را راه می اندازیم به صورت اتوماتیک داخل درایو نصب ویندوز یک Folder ساخته می شود به نام Inetpub داخلش یک پوشه هست به نام wwwroot فایل های سایت مان در این قسمت قرار می گیرند. اگر در Browser مرورگر خود بزنیم 127.0.0.1 یعنی برو وبسایت داخل pc خودم را نشان بده در این حالت ما Hosting هستیم که داریم سرویس وب می دهیم.

Hosting یک تیکه از Hard Disk است که یک کمپانی به ما اجاره می دهد ، سایت Google اولین بار از اتاق خواب مدیر عامل روی وب منتشر شد !

پس چرا ما می رویم سالیانه پول می دهیم به یک کمپانی که از آن Hosting اجاره کنیم؟ اینترنت خانه ما قابلیت این را ندارد که یک دفعه 1000 تا user به سمت وبسایت ما بروند پهنای باند ما کلاً اشغال می شود پس آن کمپانی پهنای باند قوی دارد ، کمپانی یک

دستگاهی دارد که امنیت و بسایت ما را تامین می کند ، کمپانی از فایل های ما Back up می گیرد و ...

پس ما پول یک سری خدمات را می دهیم وگرنه ما وبسایتمان را از اتاق خانه خودمان هم می توانیم بفرستیم بیرون!

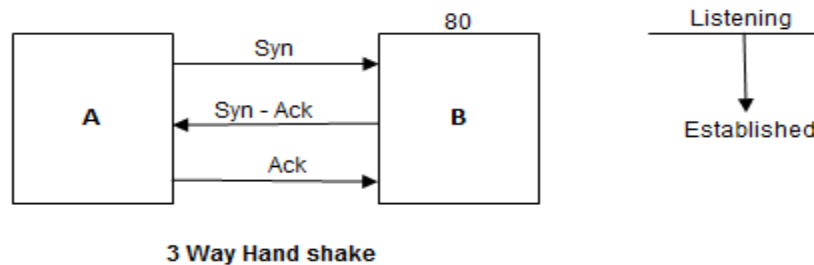
کسانی که می خواهند سایت طراحی کنند و روی اینترنت بگذارند باید بروند IP Public Static بخرند(چون اگر Dynamic باشه دائم عوض می شود که مناسب نیست.) و ببرند بگذارند روی یک Server و برروی آن IIS نصب کنند .

کسانی که وبسایت می گیرند می روند Host و Domain می گیرند.

Domain می شود اسم سایت ، این اسم برمی گردد به IP .

دو سیستم که می خواهند با هم ارتباط برقرار کنند یه کاری می کنند به نام 3 way Hand shake (دست دادن سه طرفه) که متعلق به لایه ۴ هست.

پس برای ایجاد یک ارتباط در فاز اول لازم است مراحل زیر طی شود در غیر اینصورت ارتباط برقرار نخواهد شد :



Syn : Synchronization

Ack : Acknowledgement رسید دریافت بسته

Pc A می گوید Syn (سلام)، Pc B می گوید Syn_Ask (علیک سلام)، Pc A می گوید Ok.

Pc A می گوید من می خواهم ارتباط را ایجاد کنم روی فلان Port تو، می خواهم سرویس بگیرم آیا تو ارائه اش می دهی؟ در جواب Syn Ack بهش برمی گردد که اگر port 80 بر روی کامپیوتر B باز باشد و سیستم A درخواست Port 80 را بخواهد بفرستد سیستم B چون Port 80 بررویش باز است اگر دستور netstat -na از آن بگیریم Port 80 را بصورت Listening نوشته یعنی من روی این Port دارم گوش می دهم و کسی نیامده به سمتش.

اگر بخواهیم از یک سیستمی ارتباط بگیریم ولی Port هنوز به ما جواب نداده باشد می رود در حالت Time wait .

بعد از اینکه ۳ ارتباط 3 Way Hand Shake برقرار شد می رود در حالت Established یعنی ارتباط برقرار شد و 3 way Hand shake انجام شد.

پس کامپیوتر ما وقتی یک Port ش باز است در حالت Listening قرار دارد و منتظر است که یکی بیاید و بگوید که کار دارد.

وقتی ارتباط را گرفت و ۳ مرحله 3 Way Hand Shake طی شد و با هم Syn شدند می آید تو حالت Established (یعنی ارتباط ایجاد شده تا زمانی که آن کار تمام می شود مثلاً می رویم یک سایتی را ببینیم تا وقتی Page down هست این ارتباط وجود دارد ولی بعدش اون خط Establish پاک می شود)

در لایه ۴ دو نوع ارتباط وجود دارد :

1) Connection-Oriented (TCP^{۳۵})

2) Connectionless (UDP^{۳۶})

TCP : ارسال بسته به همراه رسید دریافت بسته. مثلاً به یک پیک موتوری می گوییم که این بسته را که بردی رساندی رسیدش را برایمان برگردان!

³⁵Transmission Control Protocol

³⁶User Datagram Protocol

UDP: ارسال بسته بدون دریافت رسید دریافت بسته، مثلاً به پیک موتوری می‌گوییم این بسته را ببر برسان خداحافظ! در این حالت نمی‌فهمیم بسته رسید یا نه.

در TCP می‌گویند دقت ارتباط مهم‌تر از سرعت ارتباط است چون به ازای هر Sequenc از ارتباطی که می‌رود باید برایمان رسید را برگرداند که من رسیدم اما در UDP می‌گوید من بسته می‌فرستم خواست برسد یا نرسد مهم نیست.

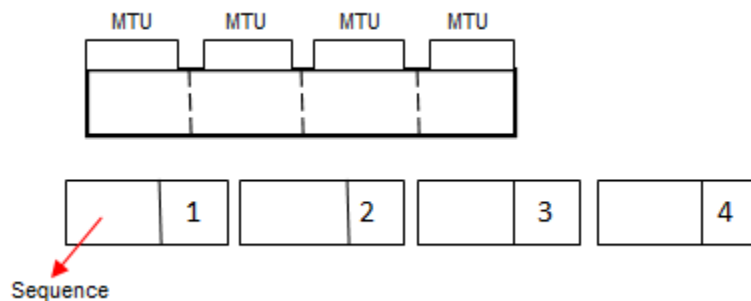
برنامه‌نویس تعیین می‌کند که کدام یک از این ارتباطات استفاده شود مثلاً وقتی یک فایل را می‌خواهیم برای یک نفر ارسال کنیم می‌بینیم اگر فایل از وسطش قطع شود دیگر قابل پخش نیست چون هنوز کامل نشده این از نوع TCP است، اگر بخواهیم ویدیو فوتبال را ببینیم بعضی وقت‌ها تصویر به صورت شطرنجی نمایش داده می‌شود این یعنی یک سری بسته نرسیده که این اتفاق افتاده این ارتباط از نوع UDP است که می‌گوید من می‌خواهم لحظه‌را نشان بدهم حالا می‌خواهد بسته برسد یا نرسد.

در UDP ترتیب ارسال Sequence مطرح نیست.

جهت کنترل ارسال Sequence ها به مقصد در لایه ۴ عملیاتی داریم بنام Fragmentation که بین TCP و UDP مشترک است.

Fragmentation براساس مقداری به نام MTU^{37} که می گوید بسته (که از لایه ۲ در حال خارج شدن است) از یک مقداری بزرگتر نمی تواند باشد بریده می شود.

در لایه ۴ بسته بر اساس سائز استاندارد به نام MTU (بسته یا فریم نمی تواند بیشتر از 1518 Byte باشد در یک مورد خاص تا 1522Byte) تکه تکه می شود و به هر تکه یک Sequence گفته می شود.



وظیفه دیگری در لایه ۴ به نام Ordering ترتیب ارسال Sequence ها براساس شماره آنها برعهده دارد، درارتباط TCP فرستنده به ازای هر Sequence ارسالی منتظر رسید دریافت از طرف مقصد می باشد (acknowledgment) اگر این Ack نیامد فرستنده آن Sequence را مجدد ارسال می کند که در ارتباط UDP مهم نیست، در ارتباطات پایدار طرفین ارتباط مقداری به اسم Window Size را بالا می برند که در این شرایط ack کمتری جابجا می شود و هر Ack معرف رسید تعداد بیشتری Sequence است.

³⁷maximum transmission unit

: Firewall

در شبکه دستگاهی داریم به نام Firewall، (این Firewall با Firewall داخل ویندوز

متفاوت است)

دستگاهی است لایه ۷ ی که حداقل باید لایه ۴ را بفهمد تا بتواند Port Number بفهمد،

بتواند سیستمی را فیلتر کند (Firewall ها توانایی Content Filtering دارند که می

توانند بسته را باز کنند بخوانند و اگر فلان چیز بود داخلش فیلتر کنند) و ...

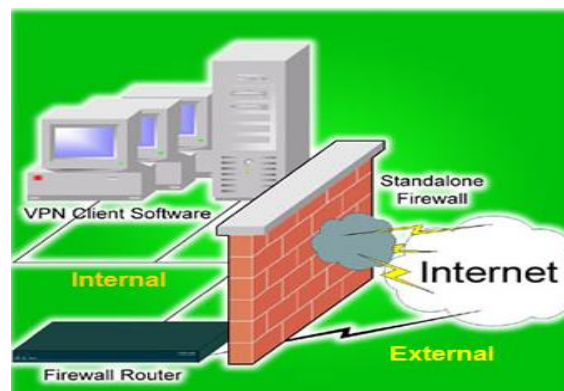
دیواری آجری مانند است، در لبه شبکه قرار می گیرد یعنی جایی که از شبکه به بیرون می

رویم، این دستگاه حداقل باید 2 NIC داشته باشد. در واقع این دستگاه Routing هم انجام

می دهد، پس می توان اصلاً Router وجود نداشته باشد چون Firewall کار Router را

هم می کند. فرقی این است که این Firewall می گوید من جلوی همه Port هایی که از

داخل می خواهند به بیرون بروند و از بیرون می خواهند داخل شوند را می گیرم!



× جدیداً قابلیت های جدیدی آمده برای مکانیزم های Firewall مثلاً می گویند قرار است FaceBook باز شود به این صورت می خواهند باز کنند که الان قابلیت هایی آمده که بسته را باز می کند و می گوید اگر بسته خواست به FaceBook برود و داخل بسته اش فلان چیز نوشته شده بود جلوییش را بگیر!

پس یکی از کارهای Firewall این است که جلوی همه Port های ورودی و خروجی را می بندد.

تمام Firewall ها چه سخت افزاری و چه نرم افزاری از یک قانون تبعیت می کنند:

توی Config Firewall یک خط هست با فرمت زیر:

Action	From	To	Protocol	User

و در آن شروع می کنند به نقش نویسی.

اصول کار Firewall این است که بسته از بالا آمده با خط هایی که وجود دارد یکی یکی خط ها را طی می کند اگر Ok نبود به خط بعد رفته به همین صورت پایین آمده و در آخر اگر با هیچ کدام سازگار نبود بسته دور انداخته می شود.

× در ایران به این صورت Firewall می نویسند کلی پول هم می گیرند که اصلاً مناسب نیست!!

Action	From	To	Protocol	User
Allow	any	any	any	any

این مثل این می ماند که یک دیوار بسازیم و بعد بزنیم خرابش کنیم چون الان هر بسته ای بیاید با این خط match شده و بیرون می رود! ما نیتیمان از Firewall این نیست، این فقط برای دستگاه هایی خوب است که می خواهند شبکه را مانیتور کنند.

۲ مکانیزم Firewall وجود دارد :

(۱) IDS^{۳۸} (۲) IPS^{۳۹}

IDS : فقط Attack را می بیند و مانیتور می کند مثلاً : یک نگهبان بگذاریم و بگوییم هر وقت دزد آمد بگو!

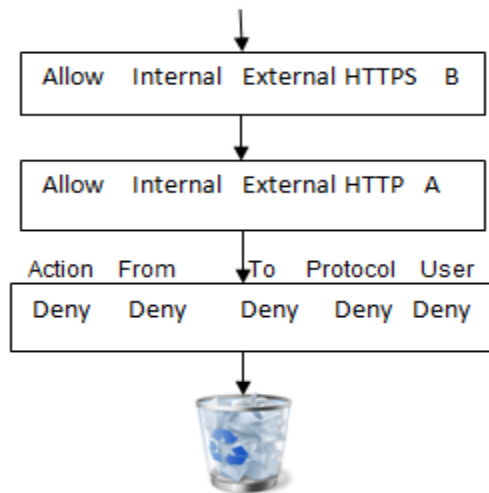
IPS : هم Attack را می بیند و هم جلوی آن را می گیرد مانند نگهبانی که دزد را دید با آن مقابله کند.

هر IPS یک IDS هم هست.

چگونه Firewall را Config می کنند؟

³⁸Intrusion Detection System

³⁹Intrusion Prevention System



این ها Sequence خط ها هستند Sequence اول می گویند اجازه می دهیم به شبکه داخلی که برود به شبکه خارجی فقط برای HTTPS فقط برای User B .

اگر آدرس زیر را داشته باشیم :

B → HTTP:\\ www.yahoo.com

این آدرس با Sequence اول match نیست چون برای HTTP اجازه دارد نه برای HTTPS ، به خط دوم می رود می بیند HTTP درست است اما برای User A مجاز است نه User B در نتیجه به خط بعدی رفته و بسته دور انداخته می شود.

برای آدرس :

B → HTTPS:\\www.Google.com

با خط اول سازگار است در نتیجه بسته از Firewall رد می شود و بیرون آمده.

× در سازمان های دولتی به این صورت Firewall را Config می کنند می گویند اجازه می دهیم به شبکه داخلی که برود به شبکه خارجی فقط برای سایت یا هو فقط برای سیستم B و فقط برای HTTP بدون گستره JPG. که باعث می شود سایت یا هو را نشان دهد بدون عکس.

× نسبت به Scale شبکه می توانیم از انواع Firewall استفاده کنیم.

× در هر کامپیوتر یک Firewall وجود دارد برای دیدن آن دستور firewall.cpl را در run Menu می زنیم این Firewall داخلی سیستم است. در قسمت Advanced Settings و از طریق گزینه های Inbound Rules و Outbound Rules می توانیم تکلیف مشخص کنیم مثلاً بزنینیم : Inbound Rules>>New Rules... در ادامه تعریف کنیم که قصد داریم یک Port یا Program از TCP یا UDP که match شود با Port 80 را Allow بدهیم اگر یا Deny کنیم .

این طوری هیچ کس به سمت Port 80 نمی تواند برود.

× در یک شبکه اولین کاری که می کنند این است که Firewall را off می کنند چون تنظیماتش یک مقدار سخت است و اگر خاموش نباشد ping نمی دهد و نمی فهمیم که فلان pc آمده داخل شبکه یا نه!

معمولاً از یک سری نرم افزار استفاده می کنند که قابلیت Firewall داشته باشد مانند آنتی ویروس Kaspersky .

در خصوص انتخاب آنتی ویروس در شبکه های مختلف تفاوت سلیقه وجود دارد که این به نظر Admin شبکه برمی گردد که چه آنتی ویروسی را پیشنهاد دهد معمولاً برای شبکه آنتی ویروس Kaspersky خوب است چون:

(۱) متعلق به کشور روسیه است که کشور ما رابطه خوبی با آن دارد و Update هایش

میرسد و مشکلی نداریم (اگر یک آنتی ویروس آمریکایی بگیریم ممکن است بعضی از

Update ها نرسد و دچار مشکل شویم!)

(۲) داخل شبکه Load زیادی نمی گذارد.

(۳) قابلیت بستن Port خوبی دارد مثلاً Port USB کامپیوترها را می توانیم با آنتی

ویروس Kaspersky ببندیم اگر قرار بود با خود Windows این کار را انجام بدهیم به

مشکل بر می خوردیم. این آنتی ویروس قادر است Storage USB را ببندد چون یکی از

کارهای واجبی که در هر شبکه باید انجام شود این است که سیستم ها

(a) DVD Writers نداشته باشند.

(b) Port های فلش برای USB بسته باشد یعنی درکل Storage Flash یا Storage

Mobile را ببندد که کاربر نتواند اطلاعات را از داخل شبکه به بیرون منتقل کند و ...

(c) کاری کنیم که کاربر یک حجم محدودی را بتواند ایمیل کند و نه بیشتر.

(d) محدودیت کاربر تا جایی که ممکن است و با اخلاق جور در می آید چون بعضی شرکت ها می گویند تماس های تلفی روی شبکه انجام می شود پس لازم است که شنود شود که این کار باید به کاربر گزارش داده شود وگرنه غیراخلاقی است یا مثلاً دیدن مانیتور کاربر در شبکه (دیدن مانیتور کاربران) یا گذاشتن دوربین مداربسته همه این موارد باید به کاربر گزارش داده شود.

اگر امنیت در شبکه مهم باشد همه این موارد هم اهمیت پیدا می کند

لایه ۵ و ۶ و ۷:

این لایه ها به صورت application می باشند.

همان طور که در ابتدای درس اشاره کردیم Protocol stack داریم به نام TCP IP که ۴ لایه دارد و همه قانون های شبکه حول محور TCP IP کار می کنند.

جریانش این است که کمپانی میکروسافت در حال کردن روی یک پروتکلی بود به نام

NetBeui در آن زمان کمپانی Unix که رقیب میکروسافت بود در حال کار کردن روی

TCP IP بود که بصورت Open Sourc بود و پولی نبود و همه امکاناتش را به صورت رایگان در اختیار کاربران قرار می داد.

TCP IP کم کم در حال محبوب شدن بود همین طور میکروسافت هم از لحاظ ظاهری داشت پیشرفت می کرد ، میکروسافت TCP IP را دزدید و به جای NetBeui خود قرار داد و این طوری شد که محبوب شد! وگرنه TCP IP اصلاً متعلق به میکروسافت نبود!!

کارایی لایه ۵ و ۶ و ۷:

وقتی یک سایتی را باز می کنم که داخلش محتویات SWF وجود دارد که احتیاج به Flash player است اگر در سیستم خود Flash Player نصب نداشته باشیم می بینیم که نوشته می شود Flash Player نداری و بیا روی این لینک کلیک کن تا دانلود شود!

سیستم از کجا فهمید که Flash Player نداریم؟

لایه Presentation وظیفه دارد که فرمت های تبدالی بین یک ارتباط را تعیین کند مثلاً می گوید روی سیستم شما SWF و JPG و ... موجود است.

از وظایف دیگر لایه Presentation }
 Compression (فشرده سازی بسته ها)
 Encryption (رمزنگاری بسته ها)
 می باشد.

Compression: یعنی بسته ها را تاجایی که ممکن است فشرده کرد فشرده سازی بسته

در شبکه به این صورت است که هر متن صفر و یکی که ما به عنوان Data داریم ممکن است شامل یک سری صفر و یک شبیه هم باشد (String های شکل هم) کاری که می کنند این است که به جای این String ها یک نشانه می گذارند و در یک گوشه فایل می نویسند این نشانه یعنی ... ، این کار باعث می شود که حجم بسته کم شود این یکی از مکانیزم های Compression در شبکه است.

Encryption: یکی از نمونه هایش این است که مثلاً تصمیم می گیریم که به جای هر

حرف یک چیز دیگر بنویسیم بعد به طرف مقابل هم بگوییم بدون هر جا که گفتیم A منظور B هست.

در شبکه های امروزه برای ارتباطات امن احتیاج به Security زیادی هستیم چون دنیای اینترنت بی در و پیکر است!

لایه Session یکی از وظایفش چک کردن فرمت های تبادلی است.

× وقتی در سایت یک بانک هستیم و Login هستیم و یک مدتی فعالیتی نمی کنیم و بعد گزینه خلاصه حساب را می زنیم ما را دوباره می برد در صفحه Login و می گوید دوباره

User و Password بزن و Login شو! علت این کار چیست؟ مگر بین مبدا و مقصد 3
Way Handshake انجام نشده و مگر رابطه Established نشده؟

در لایه Session یک ارتباطی پدید می آید به آن می گویند ارتباط Session به
Session، در این Session پسورد ها چک می شود اگر پسورد درست بود Login انجام
می شود.

وقتی Login می شویم یک Session باز ایجاد می شود و با یک زمانی که Programmer
تعیین می کند آن Session باز نگه داشته می شود بعد از گذشت این مدت زمان Session
از بین می رود و ارتباط قطع می شود.

× اگر به عنوان کاربر، Session یک سیستم را در فایروال ببینیم و راست کلیک کنیم و
Disconnect Session را بزنیم آن ارتباط قطع شده و از بین می رود.

وقتی در لایه ۷ دستور صادر می کنیم که HTTPS، بسته در لایه ۶ اتفاقاتی برایش رخ می
دهد.

در ابتدا از طرف Server بعد از فرستادن Certification (از طرف کمپانی های خاصی
صادر می شود که ارائه Certification انجام می دهند) چیزی با آن فرستاده می شود به

نام Public Key که ما بسته های خودمان را با آن رمز می کنیم و می فرستیم برای
، Server

Public Key وقتی یک بسته را قفل کند دیگر نمی تواند باز کند فقط Private Key می
تواند قفل بسته را باز کند حتی اگر این وسط فایروال هم وجود داشته باشد نمی تواند بسته را
باز کند و بخواند مگر در صورت حمله های man in the middle.

× مرورگر Internet Explorer تنها مرورگری است که هویت صادر کننده
Certification را چک نمی کند!

جلسه ۶

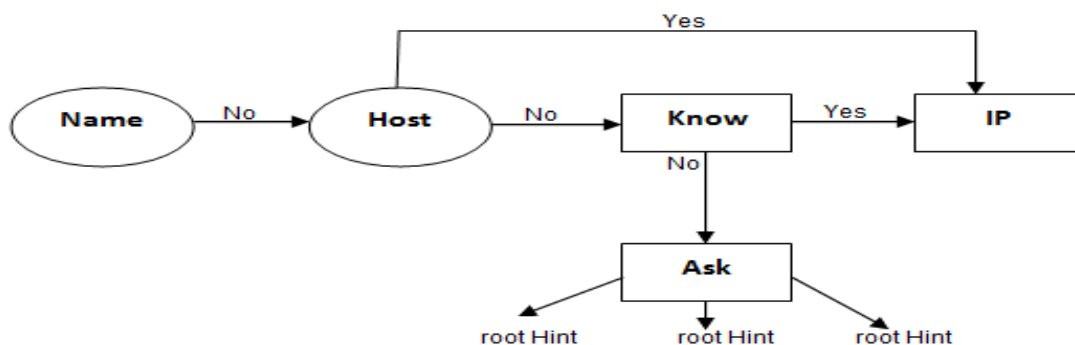
لایه Application ، لایه ای است که کاربر می تواند با آن ارتباط داشته باشد پروتکل های مختلفی مانند DHCP دارد که هر دستگاه لایه ۳ ی هم می تواند آن را راه اندازی کند.

پروتکل های لایه های مختلف به صورت زیر است:

7.Application	HTTP,HTTPS,IMAP,POP3,SMTP,DNS
4.Transport	TCP/UDP
3. Network	IP,ARP,ICMP,IGMP
2.DataLink	PPP,HDLC,Frame,Frame Rely

: DNS^{۴۰}

مکانیزمی برای تبدیل اسم به IP می باشد و عملکرد آن به شکل زیر است :



⁴⁰ Domain Name System

ما DNS را می توانیم به ۲ حالت داشته باشیم:

۱. در شبکه خودمان به عنوان یک سرویس را اندازی کنیم.
 ۲. از سرویس راه اندازی شده توسط یک سری از کمپانی ها استفاده بکنیم.
- کدام یک بهتر است؟ فرقی نمی کند ، در DNS که خودمان راه اندازی می کنیم اگر سوالی را نداند می توانیم برایش Forwarder تعریف کنیم.
- کاربرد DNS چیست؟

ما با داشتن IP درست ، Subnet Mask درست و Gateway درست به اینترنت وصل می شویم اما به IP های اینترنتی ، اگر در قسمت تنظیمات DNS:

run menu> ncpa.cpl> (روی کارت شبکه) right click> properties > Properties

IPv4 > DNS تنظیمات

یک IP DNS بنویسیم که می دانیم سرویس DNS ارائه می دهد با داشتن آن ۳ تا (IP و Subnet Mask و Gateway درست) می توانیم از IP DNS سوال بپرسیم.

اگر به جای IP DNS بزنیم 8.8.8.8 این IP DNS Server شرکت Google است.

سوال: آیا ایران می تواند همه DNS های رو به خارج را ببیند؟

جواب: بله

برای تست : قسمت تنظیمات IP و DNS رفتیم DNS را برداشتیم ، بعد رفتیم هرسایتی را که باز کردیم دیدیم باز نمی شود.

رفتیم در محیط CMD و 8.8.8.8 را Ping کردیم دیدیم Ping شد ، آمدیم سایت yahoo را Ping کردیم ping yahoo.com نشد!

پس فهمیدیم که مشکل تبدیل اسم به IP داریم (DNS) ، دوباره آمدیم در قسمت تنظیمات DNS و یک DNS که می شناسیم را قرار دادیم مثلاً : 85.15.1.10 که DNS Server شرکت Shatel است.

حالا در محیط CMD سایت یاهو را Ping گرفتیم و دیدیم درست شد.

× اگر IP های اینترنتی را داشته باشیم می توانیم بدون داشتن DNS سایت مورد نظر را باز کنیم اما حفظ کردن IP های Public سایت های مختلف برای ما سخت است و ما راحت هستیم که با اسم کار کنیم در نتیجه DNS که کارش تبدیل اسم به IP است به کار می آید.

× وقتی ما اسم یک سایتی را در Browser خود وارد می کنیم این اسم ابتدا در فایل

hosts موجود در درایو نصب ویندوز رفته و بعد از DNS سوال می کند یعنی:

Drive C > Windows > System32 > drivers > etc > hosts M R T

با استفاده از Notepad این فایل را باز کنید و اگر در آن اضافه کنیم :

1.1.1.1 yahoo.com

با این کار جلوی باز شدن سایت yahoo را می گیریم.

در این حالت اگر بیاییم در محیط CMD بزنی ping yahoo.com به ما 1.1.1.1 را برمی گرداند.

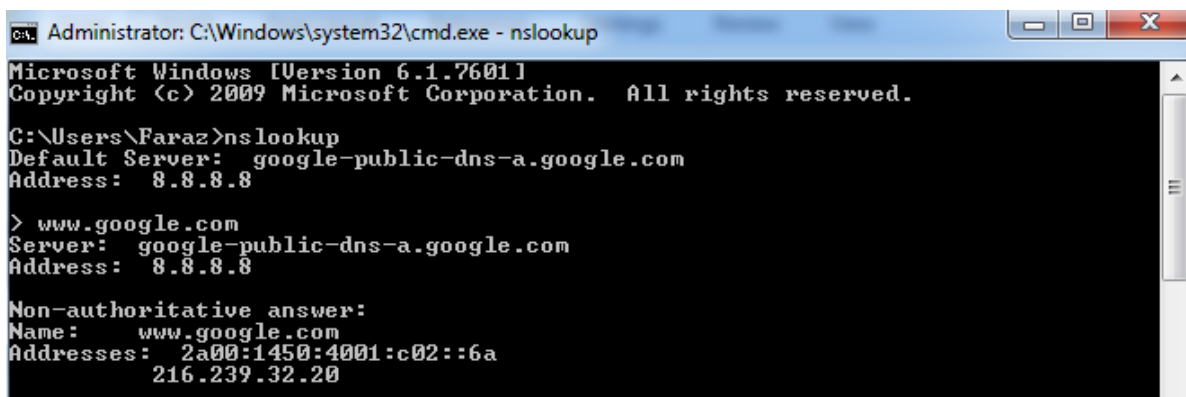
خالی کردن Cache Ram از DNS :

ipconfig /flushdns

دستور زیر توانایی پرسیدن سوال های دامنه ای شما را برعهده دارد یعنی به عنوان مثال می

خواهید بدون باز کردن Browser خود تنها عملکرد DNS خود را تحلیل نمایید :

Nslookup



```

Administrator: C:\Windows\system32\cmd.exe - nslookup
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Faraz>nslookup
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8

> www.google.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: www.google.com
Addresses: 2a00:1450:4001:c02::6a
           216.239.32.20
  
```

برای اینکه بیرون بیاییم دستور زیر را می زنیم:

ctrl + z

× وظیفه اصلی DHCP دادن IP است در کنار این وظیفه یک سری ویژگی نیز دارد که می تواند Gateway و DNS و ... بدهد .

× در شبکه Down Time داریم یعنی وقتی یک Server شبکه پایین آمده و از سرویس دهی می افتد که در ایران زیاد اتفاق می افتد!
Down Time یک سری قانون دارد :

(۱) هر زمانی نمی توان Down Time داد.

(۲) به هر مسئله ای نباید شبکه به Down Time بخورد.

اگر بیایم سایت بانک ملی را Ping کنیم و نشود شاید بتوانیم مبنا رو بگذاریم به اینکه Server آن مشکل دارد ولی وقتی نتوانیم 8.8.8.8 را Ping کنیم می گوئیم اینترنت مان قطع است!

چون این قدر Down Time آن پایین است که نبودن Ping 8.8.8.8 برابر است با نبودن اینترنت.

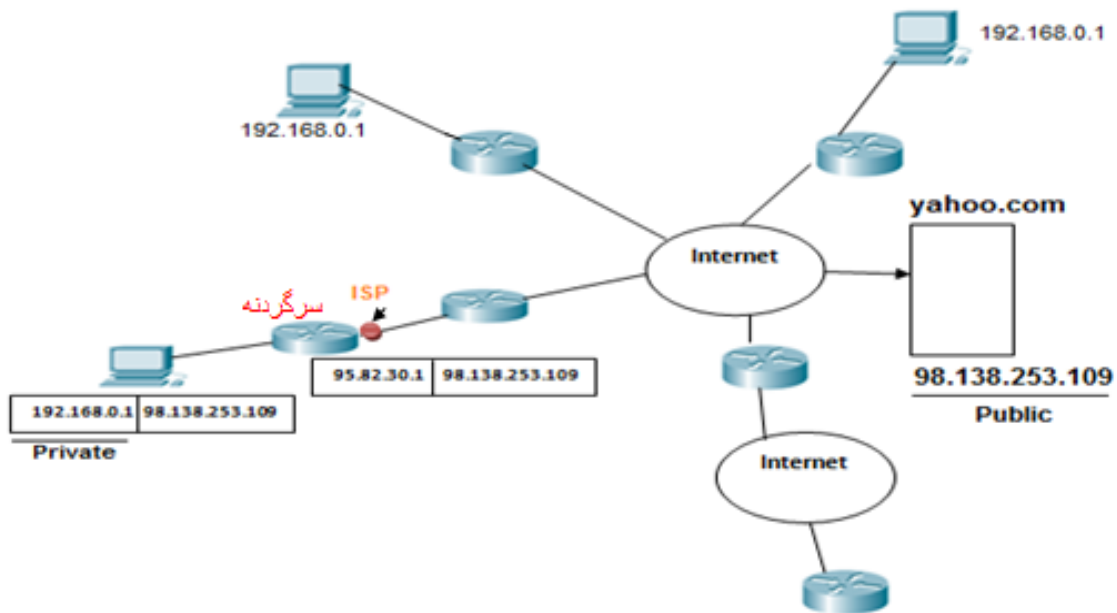
پس اولین معیار ما برای اینکه ببینیم یک سیستم اینترنت دارد یا نه Ping 8.8.8.8 است ، چون ممکن است علت اینکه ما نتوانسته باشیم سایتی را باز کنیم این باشد که اسم را نتوانسته باز کند و مشکل Name Resolution داشته باشد یا DNS .

نکته: به کاری که DNS انجام می دهد می گویند Name Resolution.

آشنایی با فرآیند Nat و Pat:

بدانیم که IP های Private در دنیای اینترنت را ندارند.

شبکه زیر را در نظر بگیرید:



بسته ای قرار است با IP Private : 192.168.0.1 به سایت yahoo برود آیا می تواند؟

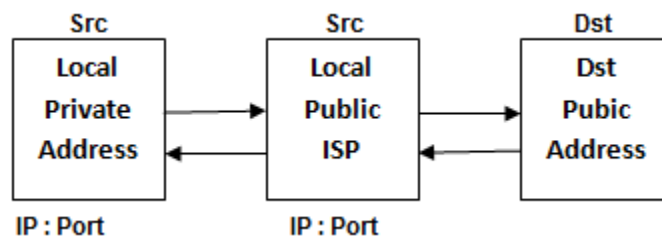
بله می تواند چون به سمت یک IP Public می رود ولی نمی تواند برگردد چون در دنیا IP

Private 192.168.0.1 زیاد است و نمی داند باید به سمت کدام یک برود!

بسته ها که از Router رد می شوند Mac Address، Router آن ها را جدا کرده پس چیزی که اهمیت دارد IP است.

از اول تا آخر ارتباط Logical Address که همان IP Private است به خودی خود عوض نمی شود اما ما می توانیم آن را عوض کنیم، مودم ما برای IP ما به منزله سرگردنه به حساب می آید، سرگردنه IP Private را می گیرد و می گوید من به جای آن، IP دست دیگر خود را می گذارم (یعنی IP که به سمت ISP است و آن را ISP تعیین کرده است). ولی یادم است که تو درخواست داده بودی و می نویسم درخواستی آمد از سمت 192.168.0.1 برای Yahoo.com و من به جایش گذاشتم 95.82.30.1 بسته رفت و برگشت و باز تحویل دادم به خودش به این عملیات تبدیل IP، NAT⁴¹ گفته می شود.

پس بسته که قرار است از شبکه بیرون برود می گوید من با چه IP و چه Port آمدم بعد فرآیند Nat انجام می شود پس علاوه بر IP، Port ها هم تفکیک می شوند که به فرآیند تفکیک Port ها Pat می گویند.



⁴¹Network Address Translation

ISP می تواند در یک دست خودش فرآیند DHCP داشته باشد که به مودم های طرف خود IP بدهد پس یک DHCP داریم که برای اختصاص این Public IP ها است. این Public IP

هایی که از سمت ISP به مودم ما داده می شود Dynamic است که اگر مودم خود را خاموش و روشن کنیم ممکن است عوض شود.

پس ما با استفاده از IP Public پا به دنیای اینترنت می گذاریم و با IP Public بر می گردیم، با همین IP Public است که اگر خواستیم سرویسی در اینترنت ارائه دهیم بتوانیم، اگر یک Server داشته باشیم قرار باشد سرویس Web بدهد و قرار باشد که بر روی آن IIS نصب شود همه دنیا با این IP NAT شده ما را می بینند که توی قرارداد ISP نوشته شده Port 80 بسته می باشد! (این به معنی این نیست که نتوانیم Dst = 80 بزنیم بلکه دیگران نمی توانند به ما Dst = 80 بزنند). یعنی ما نمی توانیم سرویس Web راه بیندازیم چون پول نداده ایم و اگر پول بدهیم این Port برایمان باز می شود.

ما برای اینکه بتوانیم Service Web ارائه دهیم باید یک IP Public Static بخریم که ISP این IP را روی مودم ما ثابت کند.

شبکه از لحاظ مدیریت :

شبکه از لحاظ مدیریت به دو دسته تقسیم می شود :

(۱) مدیریت غیرمتمرکز یا شبکه های Work Group که اصطلاحاً به آن ها Peer to

Peer گفته می شود. در این روش اگر بخواهیم یک قانون تعریف کنیم باید این قانون را روی

تک تک کامپیوترهای موجود در شبکه اعمال کنیم.

(۲) مدیریت متمرکز یا شبکه های Domain Model ، قانون را بر روی یک Server

برای همه کامپیوترها تعریف می کنیم.

در یک شبکه Work Group هر سیستم که با سیستم های دیگر در ارتباط است هر

کامپیوتر هم می تواند سرویس دهنده باشد و هم سرویس گیرنده.

سرویس های همچون File Server ، Print Server ، Web Server ، VNC Server ،

FTP Server ، Mail Server و ... می تواند در یک شبکه وجود داشته باشد. چون تخصص

هر یک از این سیستم ها در یک مورد نیست تعداد کامپیوترهای موجود در این شبکه ها

حداکثر ۱۰ تا می باشد.

در شبکه های Domain Model یک سری دستگاه ها داریم که به آنها Server می گویند

که نقش سرویس دهنده را دارند البته خودشان هم می توانند سرویس بگیرند اما وظیفه

اصلی شان این است که به Client ها سرویس دهند.

قوانین در Server ها تعریف می شوند و به بقیه کامپیوترهای موجود در شبکه انتقال پیدا می کنند.

× سوال: هنگام Login شدن در pc خودمان وقتی Username و Password را می زنیم کجا Login می شویم و احراز هویت (Authentication) کجا انجام می شود؟

جواب: پشت سیستم عامل یعنی داخل Data Base خودمان.

ما در شبکه Work Group فقط پشت DB کامپیوتر خودمان Login می شویم.

اما در شبکه های Domain Model به غیر از DB کامپیوتر خودمان پشت Server.

Login می شویم برای همین است که Server قادر است قانون هایی را وضع کند که

شامل حال کامپیوتر ما شود، چون پشت Server، Login می شویم و کارمان دست آن است.

در این حالت Admin شبکه Login پشت PC خودمان را از ما می گیرد که نتوانیم از پشت

pc خودمان Login شویم و مجبور باشیم از Server، Login شویم تا آن بتواند برای ما

تکلیف تعیین کند.

در شبکه غیرمتمرکز چیزی داریم به نام LSD^{۴۲} که پشت کامپیوتر است.

در شبکه متمرکز GSD^{۴۳} داریم.

چگونه می توان تعیین کرد که یک شبکه Work Group باشد یا Domain Model؟

⁴² Local Security Database

⁴³ Global Security Database

یک شبکه را که با بسترش می سازیم و IP دهی می کنیم already به صورت WG است ،
WB به یک اسم مقید است و اسمش by default همان Work Group است در آدرس
زیر می توان آن را دید:

My Computer $\xrightarrow{\text{Right Click}}$ Properties \rightarrow Advanced system settings \rightarrow Computer
Name \rightarrow Change در این قسمت می توان اسم گروه را تغییر داد

اسم WB باید بین تمام کامپیوترهای WB یکسان باشد.

Computer Name را هم از همین طریق می توان تغییر داد که وقتی تغییر پیدا کند pc
از ما Restart می خواهد که حتماً باید انجام دهیم.

× گزینه Domain برای Windows های Home وجود ندارد.

تغییر دادن پسورد اکانت :

My Computer \rightarrow Manage \rightarrow Local Users and Groups \rightarrow Users \rightarrow
Set Password \rightarrow Proceed \rightarrow ...

اگر در قسمت run Menu کامپیوتر بزنیم gpedit.msc چیزی را برایمان باز می کند که
دری به روی دنیای Group Policy باز می کند یعنی قوانینی که روی pc وجود دارد.

به طور مثال می توانیم در این قسمت تعیین کنیم که Control Panel از منوی Start
حذف شود :

Gpedit.msc \rightarrow Administrative Templates \rightarrow Control Panel \rightarrow Prohibit access to the
Control Panel

این قسمت را باید بخوانیم تا بفهمیم Enable یا Disable کنیم

یا اگر بخواهیم قسمت run را غیر فعال کنیم که اگر cmd زدیم غیرفعال باشد و نشان ندهد:

Gpedit.msc → Administrative Templates → Start Menu and Taskbar → Remove Run menu
Run menu from Start Menu → Enable

در یک کامپیوتر WB باید بیاییم پشت هر pc بشینیم و این کارها را انجام دهیم اما در کامپیوترهای شبکه DM پشت یک Server یک Group تعریف می کنیم و می گوئیم شامل این کامپیوترها باشند، کامپیوترهایی که پشت من Login کردند و همه عضو Domain ما هستند.

مثلاً تعریف کنیم این کامپیوترها را Control Panel شان را ببند << این می شود مدیریت متمرکز.

جهت دسترسی به فایل های به اشتراک گذاشته شده از طرف کامپیوترها

در شبکه های WB :

دو کامپیوتر به ۲ حالت می توانند وارد همدیگر شوند و به منابع همدیگر دسترسی پیدا کنند:

یک راه این است که در My Computer قسمت Network روی Icon های کامپیوترها برویم و تمام کامپیوترهایی که عضو WB هستند را نشان می دهد اگر روی هر کدام از آن اسم ها کلیک کنیم وارد منابعی می شویم که آن کامپیوتر به اشتراک گذاشته اما ما به هر کامپیوتری که بخواهیم وارد شویم باید Username و Password آن کامپیوتر را وارد کنیم. مثلاً اگر کامپیوتر A داشته باشد User: Ali و Password : 123 و کامپیوتر B داشته باشد User: Reza و Password: 456 و کامپیوتر A در شبکه قصد داشته باشد که به کامپیوتر B و منابعش دسترسی پیدا کند باید Password کامپیوتر B را بزند که 456 است.

× اگر Username و Password را نپرسید یعنی دفعه های قبل که وارد آن PC شده ایم remember زده شده و یادش مانده!

راه دیگر روشی است به نام Unc Path به این صورت که در My Computer قسمت Address bar بزنیم :

\\DstIP

نکته : اگر کامپیوتر B پسورد نداشته باشد چه می شود؟ ما نمی توانیم وارد آن شویم چون می گوید (۱) من یادم نیست که آن کامپیوتر چه Username و Password دارد .

(۲) اون کامپیوتر که من در حال وارد شدن به آن هستم Password ندارد.

یک قانونی در کامپیوترها وجود دارد که می گوید ما حق عبور از یک Username و Password خالی را نداریم!

پس اگر می خواهیم وارد کامپیوتری شویم که Password ندارد یا باید برویم و برای آن Username کامپیوتری که می خواهیم واردش شویم Password تعیین کنیم و یا باید برویم و آن قانون را برداریم از طریق مسیر زیر:

gpedit.msc → Windows Settings → Security Settings → Local Policies → Security Options →
Accounts: Limit Local account use of blank passwords to console logon only → Disabled

حالا قادر خواهیم بود که با Username و بدون Password وارد Pc مورد نظر شویم.

پارتیشن های Windows در شبکه های WB که با دسترسی Administrator کامپیوتر مقابل به هم دیگر راه پیدا می کنند دسترسی full دارد و (Share by Default) ، (Share

یعنی اگر کامپیوتری حتی چیزی به اشتراک نگذاشته باشد ما می توانیم مثلاً به درایو C و Desktop کامپیوتر در شبکه دسترسی پیدا کنیم از طریق زدن دستور زیر در Address Bar :

\\192.168.40.1\c\$ → Users → Administrator → Desktop

ما در کامپیوتر سرویسی داریم به نام File and Printer Sharing که می توانیم یک Folder را در شبکه Share کنیم.

نحوه Share کردن Folder به این صورت است که روی Folder مورد نظر راست کلیک کرده و مراحل زیر را طی می کنیم :

Folder → Properties → Sharing → Advanced Sharing ... → Sharing this Folder → تیک این قسمت را می زنیم

در ادامه اسم Folder که Share می کنیم را می گذاریم و تعداد کاربرانی که بتوانند به آن Folder دسترسی پیدا کنند را مشخص می کنیم و یک گزینه Permissions دارد که می توانیم سطح دسترسی کاربران را مشخص کنیم که این گزینه در شبکه های Domain Model خودش را بهتر نشان می دهد.

نحوه Share کردن Printer در شبکه :

Start → Devices and Printers → Add a Printer → Add a local Printer → ...

در ادامه Next می زنیم و Ok می کنیم کار تمام می شود.

حالا بروی Printer که Share شده کلیک راست کنیم Printer Properties را انتخاب کنیم و بعد Sharing و Ok کنیم.

حالا اگر در My Computer و قسمت Address bar ، IP مربوط به سیستمی که Printer ، Share شده است را بزینم مثلاً: 192.168.40.30 \\ می توانیم Printer که Share شده را ببینیم و اگر برروی آن راست کلیک کنیم و گزینه Connect را بزینم به آن متصل می شویم و می توانیم از آن استفاده کنیم.

× وقتی در Word ، ctrl + P (دستور Printer) را می زینم پنجره ای باز می شود و نام printer که نصب کردیم را نشان می دهد به همراه IP سیستمی که در آن Printer به اشتراک گذاشته شده را می بینیم و می توانیم به آن سیستم دستور Print دهیم.

قابلیت مایکروسافت : Remote Desktop

ترکیب remote Desktop و Folder Sharing کار بزرگی می کند که ما مجبور نباشیم برای نصب یک نرم افزار برروی یک سیستم مستقیم پای آن سیستم برویم! مجوز Remote Desktop باید در شبکه داده شود از طریق مسیر زیر:

My Computer → Properties → Remote settings → Remote

در این قسمت تیک گزینه وسط را زده که می گوید به همه و با هر Windows با هر version می تواند دسترسی داشته باشد که معمولاً در شبکه های Work Group این گزینه را انتخاب می کنیم، با انتخاب این گزینه Remote Desktop فعال می شود.

حالا در Run Menu بزنیم ⁴⁴ mstsc که پنجره Remote Desktop Connection باز می شود در این پنجره می توانیم IP آن سیستمی که قصد وارد شدن در آن را داریم وارد می کنیم و در ادامه Username و Password آن سیستم را می زنیم و واردش می شویم و می توانیم Desktop آن را ببینیم (وقتی ما وارد آن سیستم می شویم خود کاربر آن سیستم از Account خود بیرون می افتد)

حالا می توانیم روی Desktop آن سیستم نرم افزار نصب کنیم به این صورت که قبلاً یک نرم افزار در یک Folder ریخته و Folder را Share می کنیم و در کامپیوتری که قرار است وارد آن شویم هم دسترسی اجازه دسترسی داده ایم بعد که وارد کامپیوتر مورد نظر شدیم از قسمت Network وارد کامپیوتر خودمان می شویم و Folder را باز می کنیم و بعد نرم افزار مورد نظر را run می کنیم و بر روی Desktop آن سیستم نصب می کنیم.

پایان

⁴⁴ Microsoft Terminal Services Console