Computer Networks

فصل یک :مقدمه ای بر سوئیچینگ بسته

M.Zangian

انواع سوئیچینگ

بطور کلی سوئیچینگ به چهار دسته تقسیم می شوند:

۱- سوئیچینگ پیام (Message Switching)

۲- سوئیچینگ سلول (Cell Switching)

۳- سوئیچینگ مداری (Circuit Switching)

۴- سوئیچینگ بسته (Packet Switching)

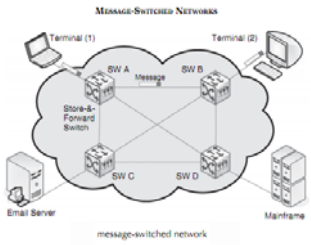
M.Zangian

انواع سوئیچینگ

3

سوئیچینگ پیام

- در تکنیک سوئیچینگ پیام هر پیام بعنوان یک ماهیت مستقل عمل کرده و در طول مسیر با رسیدن به هر ایستگاه در مسیر،ذخیره شده و سپس به ایستگاه بعدی هدایت می گردد.(store-and-forward) بنابراین در این نوع سوئیچینگ ایستگاه های کاری نیاز به بافر بزرگی دارند.هر پیام در این نوع سوئیچینگ مستقلا اطلاعات آدرس مقصد را درخود دارند.این نوع سوئیچینگ عموما برروی سوئیچینگ مداری و یا سوئیچینگ بسته پیاده سازی می شوند.مانند سرویس ایمیل و یا پست صوتی.



M.Zangian

انواع سوئیچینگ

4

سوئیچینگ سلول

- سوئیچینگ سلول از جهات بسیاری شبیه سوئیچینگ بسته است با این تفاوت که در این نوع سوئیچینگ ،بسته ها کوچک و طول بسته ها ثابت است. در این سوئیچینگ سعی شده از قابلیت اطمینان تحویل که مشخصه سوئیچینگ مداری و کارایی که مشخصه سوئیچینگ بسته است استفاده گردد.این نوع سوئیچینگ پهنای باند مناسب باسرعت خوب در اختیار قرار میدهدوبرای انتقال داده و صوت مورد استفاده قرار می گیرد از جمله شبکه هایی که از این نوع سوئیچینگ استفاده می نماید شبکه (Asynchronous Transfer Mode)ATM می باشد.

M.Zangian

انواع سوئیچینگ

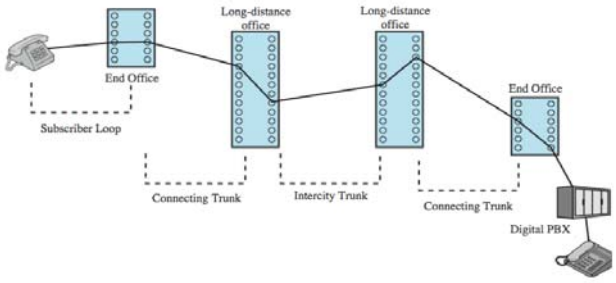
سوئیچینگ مداری Circuit Switching

در این نوع سوئیچینگ قبل از هر گونه تبادل اطلاعات می بایست یک کانال ارتباطی بین مبدا و مقصد رزرو شده و به ارتباط اختصاص یابد.

- کانال رزرو شده بصورت اختصاصی برای یک ارتباط در نظر گرفته می شود و ارتباط دیگری نمی تواند از این کانال بصورت همزمان استفاده نماید.
- در طول تماس کانال ارتباطی بصورت ثابت بین مبدا و مقصد در نظر گرفته می شود و تغییر نمی کند.
- کانال ارتباطی تا قطع تماس بصورت اشغال شده خواهد بود چه اطلاعاتی از کانال عبور کند و چه نکند.
- قبل از برقراری تماس مبدا باید منتظر رزرو یک مسیر از مبدا تا مقصد باشد و در صورتیکه بین مبدا و مقصد کانال ارتباطی و یا ظرفیت کانال آزاد وجود نداشته باشد ارتباط برقرار نخواهد شد.

انواع سوئیچینگ

سوئیچینگ مداری Circuit Switching



- تنهایک مسیر بین مبدا و مقصد وجود دارد و ارتباط از مسیرهای متفاوت برقرار نمی گردد.
- در صورت قطع مسیر در هر نقطه کل ارتباط قطع شده و برای برقراری مجدد آن نیازمند برقراری مجدد تماس خواهیم بود.
- بعد از برقراری ارتباط کانال ارتباطی بصورت Transparent عمل می کند.
- نرخ ارسال اطلاعات از مبدا به مقصد در طول مسیر ثابت است.

انواع سوئیچینگ

7

سوئیچینگ مداری Circuit Switching

- یک ارتباط در سوئیچینگ مداری شامل سه مرحله است:

۱- برقراری مسیر Establish

۲- تبادل اطلاعات Transfer

۳- قطع ارتباط Disconnect

سیستم های ارتباطی مبتنی بر Circuit Switching برای انتقال ترافیک صوتی توسعه یافته است. مانند تلفن

M.Zangian

انواع سوئیچینگ

8

سوئیچینگ بسته Packet Switching

- دراین نوع سوئیچینگ داده درقالب بسته ها انتقال داده می شود.
- داده های با اندازه بزرگ به بسته های کوچکتر تقسیم شده و سپس منتقل می شود.
- هر بسته متشکل از داده ها ی اولیه بعلاوه اطلاعات کنترلی جهت انتقال بسته می باشد.
- اطلاعات کنترلی که به داده های اولیه اضافه می شود جهت کنترل تجهیزات سوئیچینگ برای هدایت بسته ها به مقصد بکار می رود.
- اطلاعات کنترلی اضافه شده ارزش اطلاعاتی نداشته و بعنوان سربار یا Overhead در Packet Switching محسوب می شوند.
- بسته ها ممکن است از مسیرهای متفاوتی از مبدا به مقصد برسد.

M.Zangian

انواع سوئیچینگ

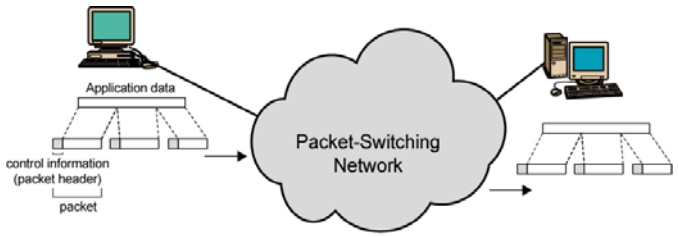
Packet Switching

سوئیچینگ بسته

- هر Node شبکه بسته های رسیده را بافر کرده و سپس آنرا منتقل می کند

(Stored and forward)

- با توجه به اینکه بسته ها ممکن است از مسیرهای متفاوتی از مبدا به مقصد منتقل شود و تاخیر هر مسیر ممکن است متفاوت باشد بنابراین ترتیب بسته ها در مقصد ممکن است با ترتیب ارسال بسته ها از مبدا متفاوت باشد.



انواع سوئیچینگ

Packet Switching

سوئیچینگ بسته

- هر مسیر منفرد ارتباطی از یک نود به نود دیگرمی تواند بین بسته های متفاوت و از ایستگاههای مختلف بصورت مشترک مورد استفاده قرار گیرد بنابراین کانال برای یک ارتباط اشغال نمی گرددو ایستگاههای مختلف می توانند بصورت مشترک از یک کانال استفاده نمایند.
- بسته های مختلف برای انتقال با فر شده و در صف قرار می گیرد بنابراین در صورت ترافیک بالای کانالها بسته ها باز هم پذیرفته می شوند. و در کوتاهترین زمان ممکن به سمت مقصد مسیردهی می شوند.
- هر ایستگاه ارتباطی می تواند به نود محلی خود با نرخ ارسال مربوط به خود متصل گردد اما در طول مسیر نرخ ارتباط بسته به مسیر ارتباطی می تواند متفاوت باشد.

انواع سوئیچینگ

11

سوئیچینگ بسته Packet Switching

- سوئیچینگ بسته می تواند به دو صورت پیاده سازی گردد:
- ۱- مدار مجازی Virtual Circuit (VC)
- ۲- دیتا گرام Datagram

M.Zangian

انواع سوئیچینگ

12

سوئیچینگ بسته مدار مجازی Virtual Circuit

- درروش مدار مجازی قبل از شروع به ارسال بسته های اطلاعاتی از یک ماشین ابتدا یک مسیر بین مبدا و مقصد برقرار می شود،بدینصورت که مبدا ابتدا با ارسال یک بسته کنترلی خاص با یک شماره ویژه برروی شبکه اعلام می کند که خواستار برقراری ارتباط با یک مقصد خاص می باشد.هر مسیر یاب که آن بسته را دریافت کندضمن پیدا کردن یک مسیر مناسب برای آن بسته شماره آنرا در جدولی درج می کندو از آن به بعد هر بسته ای که با این شماره وارد شود از همان مسیری که برای بسته اول انتخاب شده بود به سمت مقصد هدایت می شود.بنابراین تمام بسته های ارتباطی که بعد از برقراری یک مسیر از مبدا به مقصد ارسال می شوند نیاز به مسیریابی جداگانه نخواهند داشت .به این مسیر که فقط یکبار ایجاد می شود مدار مجازی گفته می شود.مدار مجازی تاوقتی با اطلاع طرفین ارتباط و اعلام به مسیریابهای واقع برروی مدار خاتمه داده نشود ،برقرار خواهد ماند از آنجاییکه در روش VC تمام بسته های اطلاعاتی از یک مسیر واحد حرکت می کنندواین تضمین وجود دارد که بسته ها با همان ترتیب ارسال شده در مقصد دریافت شوند.

M.Zangian

انواع سوئیچینگ

13

سوئیچینگ بسته مدار مجازی Virtual Circuit

خصوصیات روش مدارمجازی را می توان به موارد زیر خلاصه نمود:

- برای ارسال بسته های اطلاعاتی به آدرس های جهانی مبدا و مقصد نیازی نیست بلکه فقط به شماره VC نیاز است. بنابراین هر بسته برای انتقال بجای آدرس مقصد حاوی شماره VC است.
- برای هدایت بسته های اطلاعاتی نیاز به اجرای الگوریتم مسیریابی برای تک تک بسته ها نمی باشد و فقط یک جستجو در جدول هر مسیر یاب برای یافتن VC مورد نظر کفایت می کند. بنابراین سرعت مسیر یابی در این سوئیچینگ بالاتر از دیتا گرام است.
- بسته ها الزاما به ترتیب به مقصد خواهند رسید.
- احتمال گم شدن بسته ها ناشی از اشتباه در عمل مسیریابی در شبکه وجود ندارد.
- در صورتیکه یک Node شبکه با مشکل مواجه شود ارتباط تمامVC هایی که از آن Node میگذرد ،قطع خواهد شد بنابراین قابلیت اطمینان پایینتری دارد .

M.Zangian

انواع سوئیچینگ

14

سوئیچینگ بسته دیتاگرام Datagram Packet Switching

درروش دیتاگرام هر ماشین‌میزبـان پـس از آنکـه بسـته‌ای را تولیـد کـرد تحویـل اولیـن مسیریاب در دسترس .می‌دهد مسیریابها مختارند بر اساس شرایط ترافیکی و توپولوژی زیرساخت ارتباطی شبکه ، مسیری را برای آن بسته انتخاب کرده و آن بسته را روی آن مسیر ارسال نماید.بنابراین هیچ مسیر ثابت و از قبل مشخصی برای بسته های متوالی وجود ندارد. یعنی وقتی دو بسته از یک مبدا تولید و به سمت یک مقصد واحد ارسال میشود ممکن است مسیرهای متفاوتی را طی نمایند بنابراین ممکن است بسته ها به ترتیبی که تولید می شوند به مقصد نرسند.

M.Zangian

انواع سوئیچینگ

15

سوئیچینگ بسته دیتاگرام Datagram Packet Switching

هر بستهٔ اطلاعاتی به آدرسهای جهانی مبدأ و مقصد نیازمند است.

برای هر بسته باید مسیریابی جداگانه انجام شود.

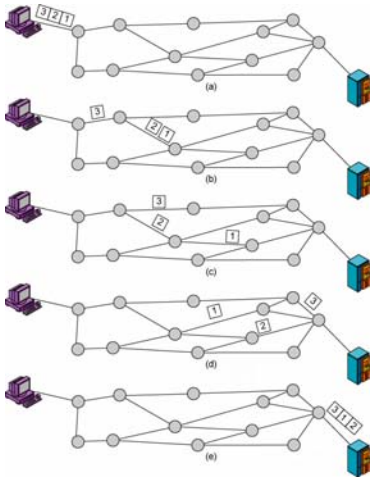
- توزیع و هدایت بسته ها روی مسیرهای متفاوت ، بر اساس شرایط توپولوژیکی و ترافیکی لحظه ای شبکه خواهد بود.
- چون بسته ها به ترتیب نمیرسند باید فرآیندی برای تنظیم ترتیب بسته ها اتخاذ شود.
- در لایهٔ بالاتر باید نظارتهای ویژه بر گم شدن یا دوبله شدن بسته ها انجام شود.
- در صورتیکه یک Nodeشبکه با مشکل مواجه شود مسیریابها می توانند در صورت وجود مسیرهای جایگزین اقدام به ارسال اطلاعات از این مسیرها نمایند.

M.Zangian

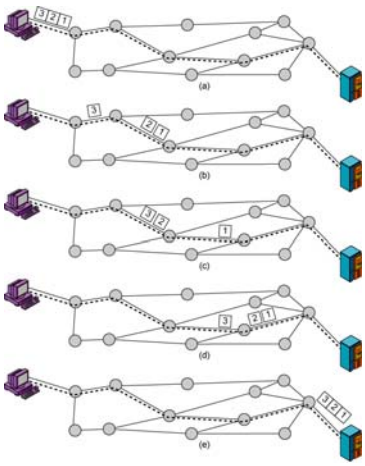
انواع سوئیچینگ

16

Datagram Packet Switching



Virtual Circuit (VC) Packet Switching

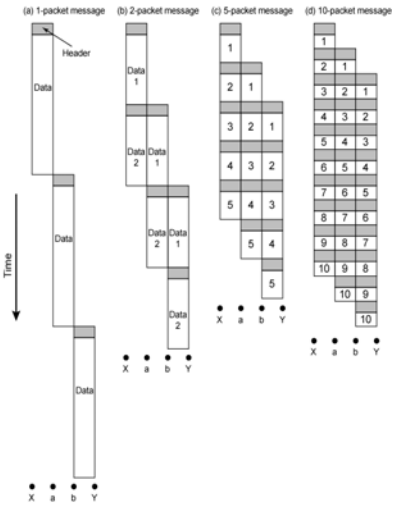


M.Zangian

سوئیچینگ بسته

اندازه بسته ها

Packet Size



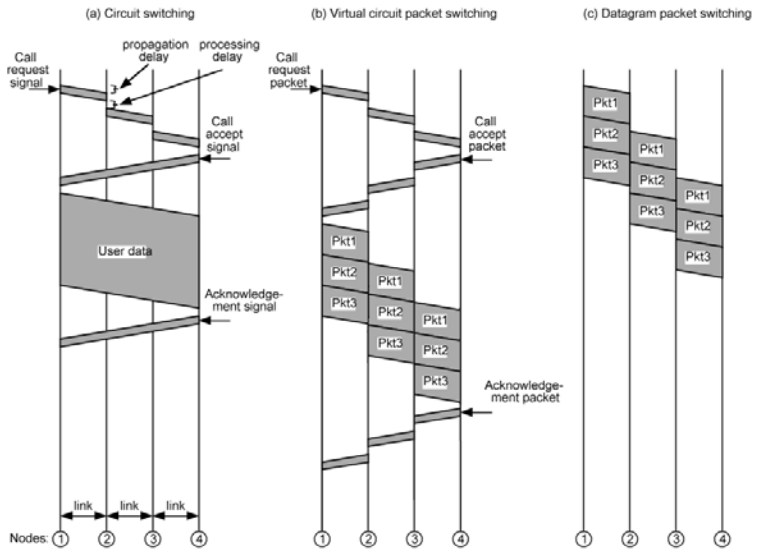
(a) همانطوریکه در شکل مقابل دیده می شود،هر مسیر یاب برای اینکه بتواند یک بسته را از یک لینک به لینک دیگر مسیر دهی نماید می بایست Packet را بطور کامل دریافت نموده و سپس اقدام به ارسال آن برروی لینک دیگر نماید از اینرو در طول دریافت یک بسته مسیر یابهای دیگر نمی توانند بسته جدید را مسیردهی نمایندو در صورتیکه این بسته بزرگ باشد زمان انتظار مسیریابهای دیگر برای دریافت بسته جدید طولانی تر خواهد بود.

(b,c)با کاهش اندازه بسته ها مشاهده می شود زمان انتظار مسیریابها برای دریافت بسته جدید کاهش یافته و در کل زمان مسیریابی بسته ها کاهش می یابد.

(d) با کاهش اندازه بسته ها سربار ناشی از Header بسته ها آنقدر زیاد می گردد که در ازای انتقال اطلاعات کمی سربار ناشی از Header ها حجم قابل توجهی یافته و مشاهده می شود زمان انتقال بسته ها افزایش می یابد.

M.Zangian

سوئیچینگ بسته



مقایسه تاخیر زمانی در سه روش سوئیچینگ (اثرتاخیرانتشارو تاخیر پردازش برروی سوئیچینگ)

M.Zangian

سوئیچینگ بسته

MTU (Maximum Transmission Unit)

- یکی از پارامترهای مهم در کارایی Packet Switching (سوئیچینگ بسته)،تعیین اندازه بسته ها می باشد .هر بسته برای انتقال نیازمند یک سری اطلاعات اضافی برای هدایت بسته می باشد که بصورت Header و یا Tariler به بسته افزوده می شود.این اطلاعات اضافی در واقع تنها برای هدایت بسته ها در شبکه بکار می رود و ارزش اطلاعاتی ندارند.ازاینرو این اطلاعات اضافه به نوعی سربار (Overhead) محسوب شده و برای هر بسته این اطلاعاتی اضافی به داده اصلی افزوده می شود. بنابراین در صورتیکه اندازه بسته ها کوچک انتخاب شود، در قبال انتقال بخش کوچکی از داده Overhead زیادی در شبکه خواهیم داشت که کارایی شبکه را کاهش می دهد. انتخاب مقداری بزرگ برای اندازه بسته ها باعث می گردد سربار هر بسته به نسبت اندازه داده کاهش یابد ولی در صورت بروز خطا و یا نرسیدن بسته به مقصد کل بسته که اندازه بزرگی دارد باید مجددا ارسال گردد که باز هم با عث کاهش کارایی خواهد شد. از طرف دیگر برخی از پروتکلهای شبکه از نظر مکانیزم طوری طراحی شده اند که نمی توان اندازه بسته را از مقداری بزرگتر در نظر گرفت(بعنوان مثال در صورت بزرگ بودن اندازه بسته مدت زمان اشغال کانال افزایش یافته و کامپیوترهای دیگر باید مدت زمان بیشتری برای انتقال بسته های خود منتظر بمانند که باز هم باعث کاهش کارایی در سوئیچینگ بسته ها خواهد شد.). بنابراین اندازه بسته به گونه ای باید باشد که به یک Trade off بین سربار ،امکان بروزخطا و مسائل تکنیکی برسیم.
- پارامتر MTU عبارتست از بزرگترین اندازه بسته برحسب بایت که یک لایه می تواند آنرا به جلو هدایت کند .در واقع بزرگترین اندازه بسته است که یک لایه می تواند آنرا قبول نموده و به جلو انتقال دهد.این واحدMTU بر حسب بایت برای یک لایه مشخص می شود. در صورتیکه طول داده اصلی برای انتقال از MTU بیشتر گردد می بایست داده ها شکسته شده و در بسته های مختلف قرار گیرد.

cisco

Computer Networks

فصل دو :مدل مرجع OSI و TCP/IP

مدل مرجع OSI

OSI(Open System Interconnection)

- برای ایجاد یک ارتباط مطمئن و قابل اعتماد بین ایستگاههای کاری و ایجاد یک شبکه کامپیوتری مسائل و مشکلات گسترده و متنوعی وجوددارد.این مسائل و مشکلات همگی از یک سنخ نیستند و منشاء و راه حل های مشابه نیز ندارند. بخشی از این مسائل توسط سخت افزار و بخش دیگر با استفاده از تکنیکهای نرم افزاری قابل حل هستند.بعنوان مثال در بخشی از ارتباط شبکه ای درگیر مسائل الکترونیکی و مدولاسیون و کدینگ خط هستیم و در بخشی دیگر درگیر مسائل هدایت بسته ها کنترل جریان داده ها ومکانیزمهای تصدیق وتایید بسته ها می باشیم . از اینرو با توجه به تفاوت ماهیت مشکلات و جلوگیری از پیچیدگی و رفع مشکلات بصورت آسانتر ازمعماری لایه ای برای شبکه های کامپیوتری استفاده می گردد. علاوه براین معماری لایه ای این امکان را می دهد که هرلایه بتواند بدون تاثیر برروی لایه های دیگر بهینه سازی شده و یا ارتقاء عملکرد پیدا کند.
- در معماری لایه ای این فرض مطرح است که هر لایه بصورت مستقل از لایه های دیگر باشد و در عملکرد لایه های دیگر مداخله ننماید.

مدل مرجع OSI

OSI(Open System Interconnection)

- طراحی لایه ای شبکه را می توان با برنامه نویسی ماژولار مقایسه کرد.بدین صورت که روالهای حل یک مسئله به اجزای کوچکتری شکسته می شودوبرای آن زیر برنامه نوشته می شود.در توابع صدا زننده این زیر برنامه ها ،جزئیات درونی آنها اهمیت ندارد بلکه فقط نحوه صدا زدن آنها و پارامترهای مورد نیاز ورودی به زیر برنامه وچگونگی برگشت نتیجه به صدازننده زیر برنامه ،مهم است.

مدل مرجع OSI

مفاهیم کلی معماری لایه ای

لایه(Layer):

جهت کاهش پیچیدگی در طراحی شبکه ، اجزاء و مکانیزمهای شبکه در قالب لایه های متفاوت سازماندهی میشوند.هدف هر لایه ارائه خدمات به لایه های بالاتر خود می باشد وهرلایه بصورت مستقل از لایه های دیگر وظایف خود را انجام می دهد.

پروتکل(Protocol):

مجموعه قواعد و قوانین بکاررفته در یک لایه می باشد تا بتواند با لایه نظیر خود در یک ایستگاه کاری دیگر گفتگو نماید.

پردازشهای همتا (Peer-to-Peer Process):

به پردازشهایی که دو لایه متناظر از دوایستگاه مختلف جهت ایجاد ارتباط و گفتگو صورت می گیرد گفته می شود.

واسط (Interface):

بین لایه های مجاور یک اینترفیس وجود دارد که عملیات و خدمات پایه ای که لایه زیر ین به بالایی می دهد را تعریف می کند.

معماری شبکه (network architecture) :

مجموعه پروتکلهای حاکم بر کل لایه و لایه ها را معماری شبکه گویند.

مدل مرجع OSI

اصول طراحی لایه ای شبکه

- هرگاه سرویسهایی که باید ارائه شود از نظر ماهیت متفاوت باشد باید لایه به لایه وجداگانه طراحی شود.
- هر لایه باید وظیفه مشخصی داشته باشد واین وظایف باید توسط معماری شبکه به دقت تشریح گردد.
- وظیفه هر لایه بایستی با در نظر گرفتن قراردادها واستانداردهای جهانی تعریف گردد.
- مرزهای لایه باید بگونه ای انتخاب شود که جریان اطلاعات بین لایه ها حداقل باشد.
- درهرلایه جزئیات لایه های زیرین نادیده گرفته می شود و لایه های بالایی باید در یک روال ساده وماژولار از خدمات لایه زیرین خود استفاده نماید.
- تعداد لایه‌ها نباید به اندازه‌ای زیاد باشدکه تمایز لایه ها از دیدگاه سرویسهای ارائه شده نامشخص باشد و نه آنقدر کم باشد که وظیفه و خدمات یک لایه پیچیده و نامشخص گردد.

مدل مرجع OSI

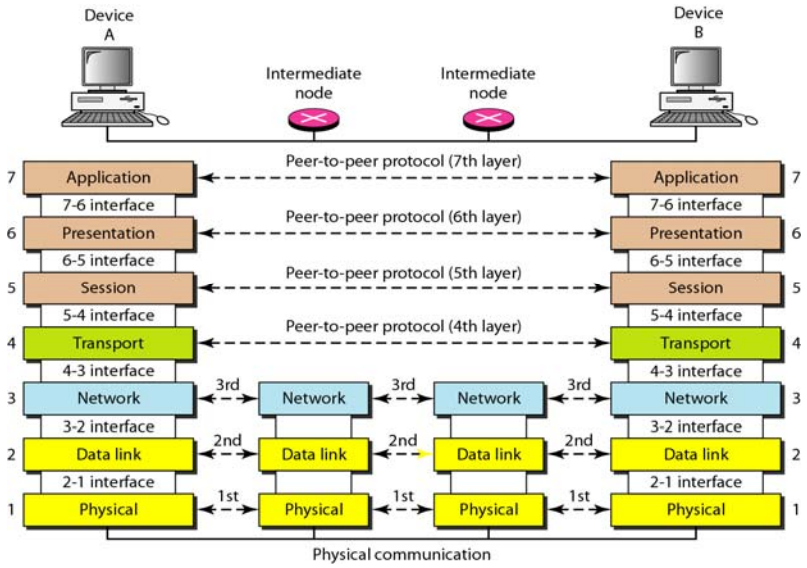
OSI(Open System Interconnection)

- سازمان جهانی ISO- (International Standard Organization) در اوائل دهه ۸۰ ،مدلی هفت لایه را برای شبکه ارائه کرد، که درآن وظایف وخدمات شبکه درهفت لایه مجزا تعریف و ارائه شده است.این مدل هفت لایه ای که در اصل برگرفته از مدل مرجع DOD (متعلق به وزارت دفاع ایلات متحده) بود ، OSI نام گرفت.هرچند که در عمل در شبکه اینترنت از این مدل استفاده نمی گردد و بجای آن از مدلی چهار لایه ای به نام TCP/IP تعریف شده است ،ولی به دلیل دقتی که در تفکیک و تبیین مسائل شبکه در این مدل شده است ، مرجع مناسبی برای درک معماری شبکه در دیگر مدلها می باشد.

M.Zangian

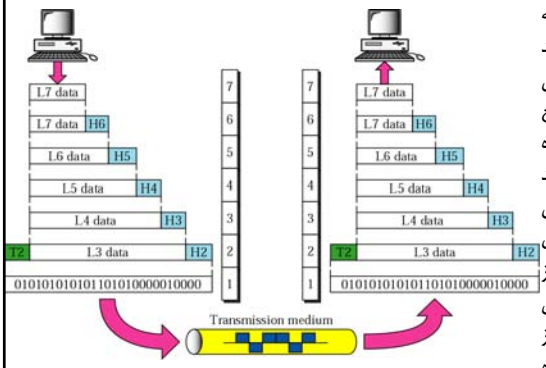
مدل مرجع OSI

Peer-to-Peer Processing



M.Zangian

مدل مرجع OSI



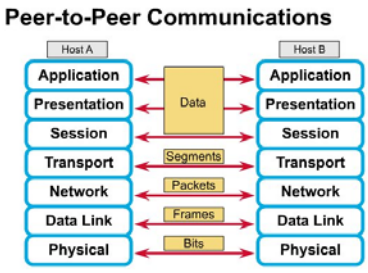
درمدل لایه ای شبکه ،وقتی یک برنامه کاربردی درلایه آخر اقدام به ارسال یک واحد اطلاعات می نماید،Header لازم به آن اضافه شده و از طریق صدا کردن توابع سیستمی استاندارد ، به لایه زیرین تحویل داده می شود.لایه زیر نیز پس از اضافه کردن سرآیند لازم ،آنرا به لایه پایین تحویل می دهد و این روند تکرار می شود تا آن واحد اطلاعات روی کانال فیزیکی ارسال شود.در مقصد پس از دریافت یک واحد اطلاعات از روی خط فیزیکی ، تحویل لایه بالاتر شده و در هر لایه پس از تحلیل و پردازش لازم ،سرآیند اضافه شده راحذف و به لایه بالاتر تحویل می دهد.

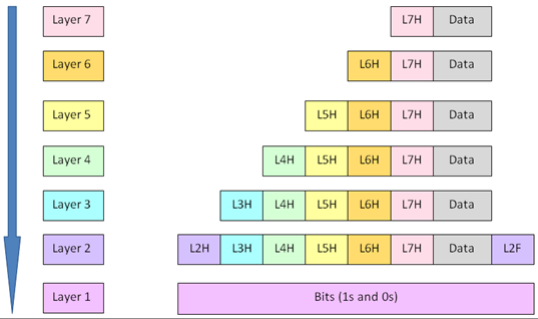
تا در نهایت داده اولیه را که از ایستگاه مبدا ارسال شده را به همان صورت تحویل لایه نظیر خود در مقصد دهد.

در Peer-to-Peer Processing لایه های متناظر با اضافه کردن Header و پردازش آن در طرف مقابل با یکدیگر ارتباط برقرار می کنند.به اضافه کردن Header به بسته اطلاعاتی در هرلایه Encapsulation می گویند.

M.Zangian

مدل مرجع OSI



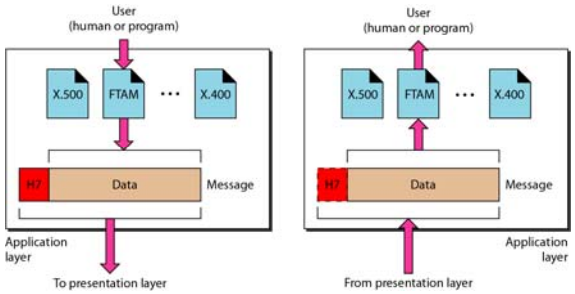


M.Zangian

مدل مرجع OSI

لایه کاربرد Application Layer

- دراین لایه استاندارد مبادله پیام بین برنامه های کاربردی درماشین سرویس گیرنده و سرویس دهنده تعریف می شود. لایه کاربرد شامل تعریف استانداردهایی نظیر مدیریت شبکه ،انتقال مطمئن فایل ،دسترسی به بانکهای اطلاعاتی راه دور ،تحلیل و ترجمه نامهای نمادین و ... می باشد.پروتکلهای لایه کاربرد ی بصورت رابطهای برنامه نویسی برنامه های کاربردی (API) برای فراهم کردن کتابخانه استانداردی به منظور انجام عملیات مهم شبکه ارائه می گردد.

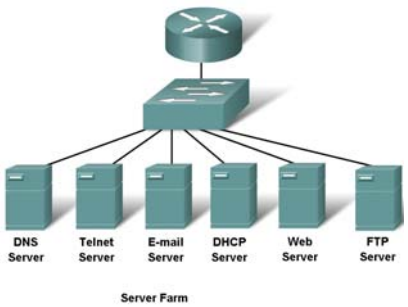


File Transfer Access and Management

مدل مرجع OSI

لایه کاربرد Application Layer

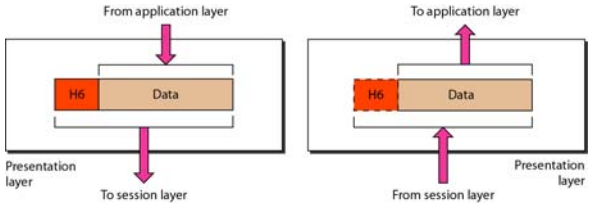
- نمونه ای از پروتکلها و سرویسهای لایه کاربرد عبارتند از:
- سرویس وب (World Wide Web)
- سرویس انتقال فایل (File Transfer Protocol)
- سرویس پستی (E.Mail)
- فراخوانی پروسیجرهای راه دور (Remote Procedure Call)
- Winsock API



مدل مرجع OSI

Presentation Layer لایه ارائه (نمایش)

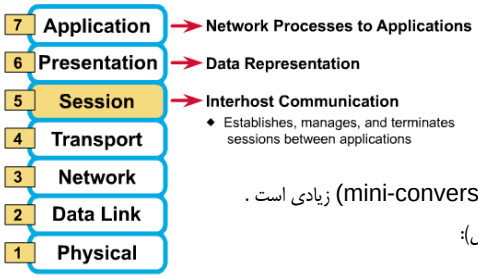
- دراین لایه معمولا کارهایی انجام می شود که اگر چه بنیادی و اساسی نیستند ولیکن نیاز عمومی تلقی می شوند.از جمله عملیاتهایی نظیر فشرده سازی اطلاعات بازکردن از حالت فشرده (Compression,Decompression) ، رمزنگاری و رمزگشایی (Encryption,Decryption) و یا تبدیل کدپیج ها در ماشین هایی که از استانداردهای مختلفی برای متن استفاده می کنند مثل تبدیل متون EBCDIC به ASCII و بالعکس در این لایه صورت می گیرد.
- پروتکلهایی نظیر MP3، Real Audio، JPEG، GIF بصورت گسترده ای در کاربردهای انتقال صورت و تصویر در این لایه تعریف می شوند. این لایه خدماتی نظیر امنیت اطلاعات و نیز استفاده بهینه از پهنای باند را ارائه می نماید.



M.Zangian

مدل مرجع OSI

Session Layer لایه جلسه



گفتگو بین دو کامپیوتر متشکل از محاوره های کوچک(mini-conversations) زیادی است .

بطور کلی هر Host دو نقش را می تواند بازی کند (یا هردونقش):

- درخواست خدمات مانند یک کلاینت
- پاسخگویی یا ارائه خدمات مانند یک سرور
- مشخص نمودن اینکه در هر لحظه کدام یک نقش خود را ایفا نمایند براساس فرآیندی به نام کنترل گفتگو یا Dialogue Control انجام می گیرد.

دوروش کنترل گفتگو عبارتند از:

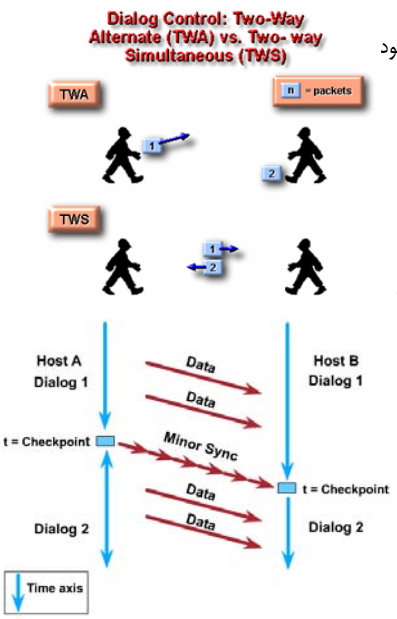
- ارتباط دو طرفه همزمان(Two-Way Simultaneous) (TWS)
- ارتباط دوطرفه متناوب(Two-Way Alternate) (TWA)

لایه جلسه درمورد استفاده یکی از دور روش کنترل گفتگو تصمیم می گیرد.

M.Zangian

مدل مرجع OSI

لایه جلسه Session Layer



درحالت ارتباط دو طرفه ارتباط می تواند همزمان از دو طرف انجام شود

در ارتباط دو طرفه امکان تصادم در سطح لایه session رخ دهد .که باعث بروز اشتباه در یک گفتگوی دوطرفه گردد.

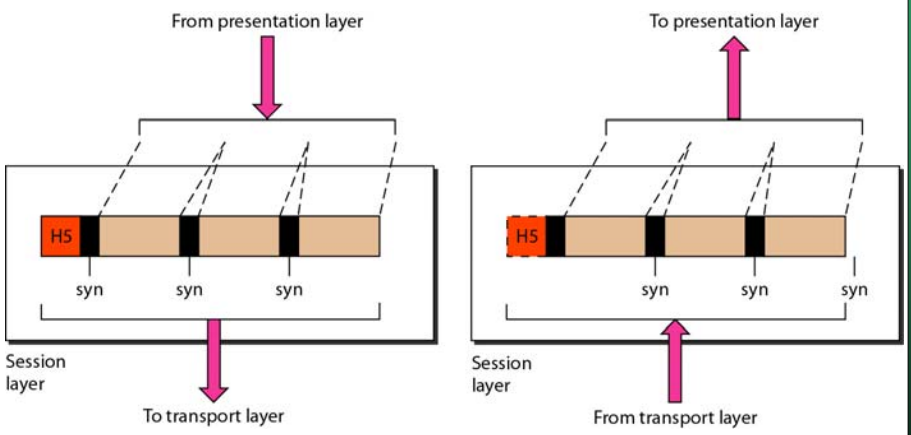
بطور کلی لایه جلسه دو وظیفه عمده را بعهده دارد :

- کنترل گفتگو
- همزمان سازی
- در فرآیند همزمان سازی شروع کننده گفتگو با ایجاد یک فاصله زمانی (CheckPoint)، بین جریان داده وقفه لازم برای برخی از عملیاتهای مورد نیاز را فراهم می آورد برخی از این عملیاتها عبارتند از:
- پشتیبان گیری از برخی از فایلهای ویژه
- ذخیره سازی برخی تنظیمات شبکه
- ذخیره سازی برخی از تنظیمات زمانی
- ایجاد یک توجه برای نقطه پایانی گفتگو

M.Zangian

مدل مرجع OSI

لایه جلسه Session Layer



M.Zangian

مدل مرجع OSI

لایه حمل (Transport Layer)

یکی از لایه های بسیار مهم مدل مرجع OSI لایه حمل می باشد که شامل توابع مهمی برای این منظور می باشد.

لایه حمل با ایجاد یک پردازش نظیر به نظیر با طرف مقابل وظیفه تحویل داده به طرف مقابل را ایفا می کند.

برای این منظور در لایه حمل قابلیتهای زیر دیده شده است :

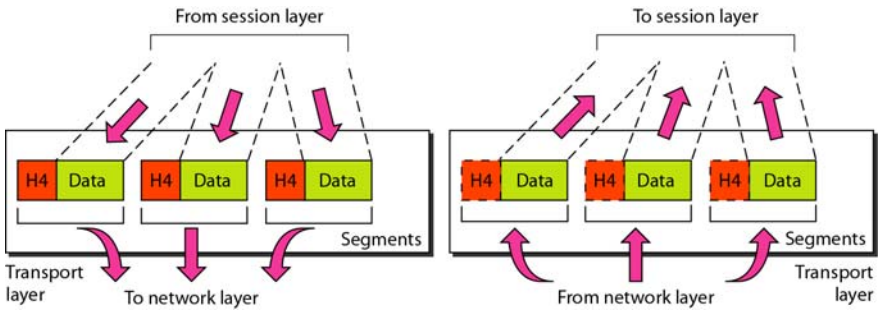
- تمایز سرویس های مختلف با استفاده از آدرس دهی پورت (Service Point Addressing)
- قطعه بندی داده های لایه بالاتر به قطعات کوچکتر در یک طرف و بازسازی داده از روی قطعات در طرف مقابل (Segmentation & reassembly)
- کنترل ارتباط (Connection Control)
- کنترل جریان داده (Flow Control)
- کنترل خطا (Error Control)

مدل مرجع OSI

لایه حمل (Transport Layer)

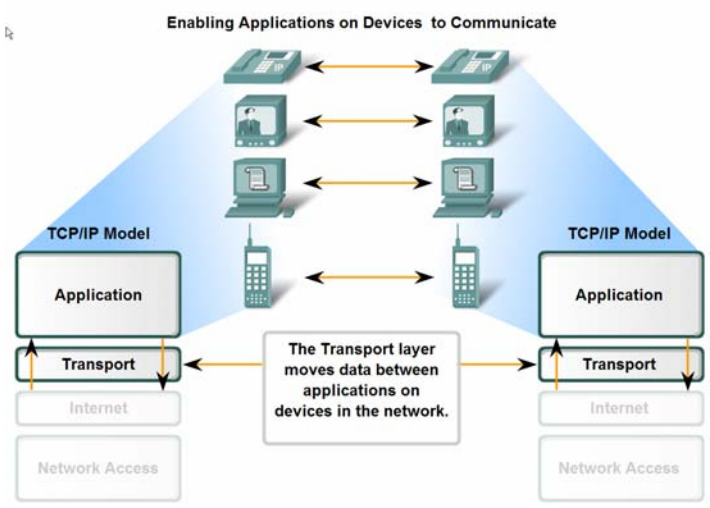
لایه حمل داده مورد نظربرای انتقال ، که در لایه های بالاتر فراهم شده است را در صورت بزرگ بودن به قطعات کوچکتر به نام Segment می شکند .و به هر قطعه یک سرآیند برای پردازش نظیر به نظیر با طرف مقابل می افزاید.

در طرف مقابل لایه حمل قطعات دریافت شده را مرتب کرده و با حذف سرآیند اضافه شده از هر قطعه، یک دیتا گرام یک پارچه را به لایه بالاتر تحویل می دهد.



مدل مرجع OSI

لایه حمل (Transport Layer)



مدل مرجع OSI

لایه حمل (Transport Layer)

بطور کلی در انتقال داده دونوع سرویس ،بسته به کاربردها مختلف قایل تصور است:

- ارائه سرویس مطمئن و اطمینان از تحویل اطلاعات به ترتیب ارسال وبدون خطا

(Connection Oriented)

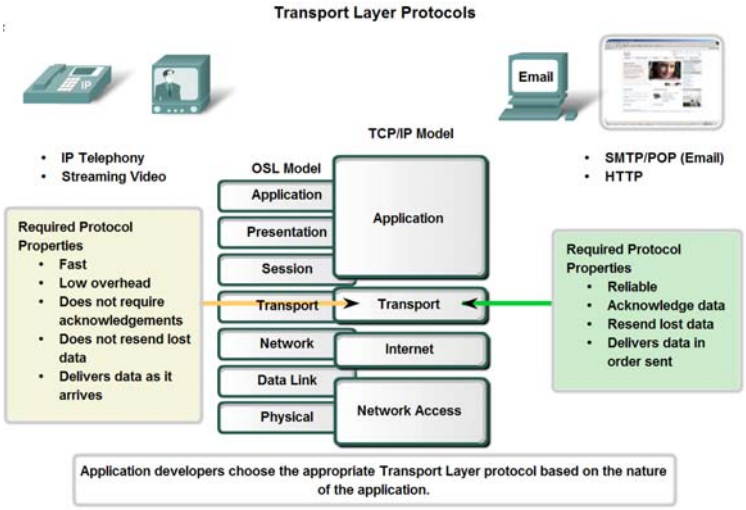
- ارائه سرویس غیر مطمئن و سریع

(Connection Less)

برنامه های ارتباطی بسته به نوع کاربرد مورد نظر از یکی از سرویس های ارائه شده در لایه حمل استفاده می نمایند.

مدل مرجع OSI

لایه حمل (Transport Layer)



مدل مرجع OSI

لایه حمل (Transport Layer)

لایه حمل برای ارائه دونوع سرویس مطمئن و غیر مطمئن از دو پروتکل TCP و UDP استفاده می نماید.

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

مدل مرجع OSI

41

لایه حمل (Transport Layer)

TCP and UDP Headers

TCP SEGMENT & HEADER FIELDS

Bit 0	Bit 15 Bit 16	Bit 31
Source Port (16)	Destination Port (16)	
Sequence Number (32)		
Acknowledgement Number (32)		
Header Length (4) Reserved (6) Code Bits (6)	Window (16)	
Checksum (16)	Urgent (16)	
Options (0 or 32 if any)		
APPLICATION LAYER DATA SEGMENT (Size varies)		

20 Bytes

UDP SEGMENT & HEADER FIELDS

Bit (0)	Bit (15) Bit (16)	Bit (31)
Source Port (16)	Destination Port (16)	
Length (16)	Checksum (16)	
APPLICATION LAYER DATA SEGMENT (Size varies)		

8 Bytes

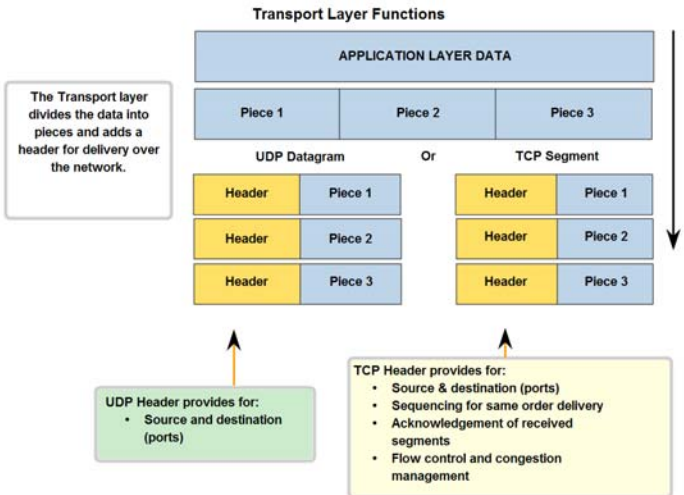
مقایسه سرآیند TCP و UDP

M.Zangian

مدل مرجع OSI

42

لایه حمل (Transport Layer)



در تصویر بالا داده آماده شده در لایه کاربرد به قطعات کوچکتری به نام Segment تقسیم می شوند .به هر سگمنت با توجه به پروتکل مورد نظر یکی از سرآیندهای TCP یا UDP افزوده می گردد.

M.Zangian

مدل مرجع OSI

لایه حمل (Transport Layer)

برای تشریح وظایف لایهٔ انتقال باید کاستی های لایهٔ IPرا بررسی کرده و سپس روشی را که لایهٔ انتقال برای جبران آنها برگزیده است ، توضیح بدهیم. دقت کنید که منشأ کاستی های لایهٔ IP ، ذاتِ کانالهای انتقال و مشکلات فیزیکی در زیرشبکهٔ ارتباطی است. عمدهٔ این کاستی ، ها عبارتند از:

- تضمینی وجود ندارد وقتی بستهای برای یک ماشین مقصد ارسال میشود آن ماشین آمادهٔ دریافت آن بسته باشد و بتواند آنرا دریافت کند.
- تضمینی وجود ندارد وقتی چند بستهٔ متوالی برای یک ماشین ارسال میشود به همان ترتیبی که بر روی شبکه ارسال شده اند ، در مقصد دریافت شوند.
- تضمینی وجود ندارد که وقتی بسته ای برای یک مقصد ارسال میشود ، به دلیل دیر رسیدن مجدداً ارسال نشود و در چنین حالتی ممکن است بستهای به اشتباه دو بار در مقصد دریافت شود. لایهٔ IP قادر نیست تمایزی بین دو بستهٔ عین هم ، که یکی از آنها زائد است قائل شود وهر دو را تحویل ماشین مقصد میدهد.

M.Zangian

مدل مرجع OSI

لایه حمل (Transport Layer)

- لایه IP هیچ وظیفه ای در قبال توزیع بسته ها بین پروسه های مختلفی که بر روی یک ماشین واحد اجرا شده اند ندارد. در یک محیط "چند کاربره" یا "چند وظیفه ای" ممکن است چندین پروسهٔ متفاوت تقاضای ارسال یا دریافت داده داشته باشند. حال فرض کنید بستهای به لایهٔ IP از یک ماشین واحد ، تحویل داده شود. داده های درون این بسته متعلق به کدامین پروسهٔ درحال اجرا روی آن ماشین است؟ از دیدگاه لایهٔ IP مفهومی به نام "پروسه های متفاوتِ در حال اجرا" ، رسمیّت و هویّت ندارد.
- لایه IP هیچ وظیفه ای در قبال تنظیم سرعت تحویل بسته ها به یک ماشین ندارد. مثلاً ممکن است یک ماشین با سرعت بسیار زیاد بسته هایی را تولید کرده و تحویل لایهٔIP بدهد ولی ماشین مقصد قادر نباشد بسته ها را با این سرعت دریافت کند و بسته ها در مقصد به دلیل عدم توانایی در دریافت ، از بین بروند.

M.Zangian

مدل مرجع OSI

لایه حمل (Transport Layer)

راهکارهای پروتکل TCP برای جبران کاستی های لایه IP

رفع مشکل عدم تضمین آماده بودن دریافت داده ها در گیرنده

اولین کاستی در لایهٔ IP عدم تضمین در آماده بودن و توانایی دریافت داده ها توسط ماشین مقصد ، عنوان شد. در پروتکل TCP راهکاری ساده وکارآمد برای این مشکل اتخاذشده است: " برقراری یک ارتباط و اقدام به هماهنگی بین مبدأ و مقصد ، قبل از ارسال هرگونه داده".

شروع ارتباط:

فرض کنید پروسهٔ A تمایل داشته باشد برای پروسهٔ B بر روی یک ماشین مشخص ، داده هایی را ارسال کند؛ قبل از اقدام به ارسال داده به صورت زیر عمل میکند:

- A یک بستهٔ خاص را به عنوان درخواست برای ارتباط ، به آدرس ماشین B میفرستد و منتظر میماند.
- B درخواست ارتباط را دریافت کرده و بر حسب شرایط ، آمادگی یا عدم آمادگی خود را به A اعلام مینماید.(ممکن است B اصلاً وجود خارجی نداشته باشد و طبعاً هیچ پاسخی بر نمیگردد.)
- در صورتی که A در یک مهلت زمان مشخص ، پاسخ مثبت مبنی بر آماده بودن B دریافت نماید میتواند به ارسال داده ها اقدام نماید.

مدل مرجع OSI

لایه حمل (Transport Layer)

راهکارهای پروتکل TCP برای جبران کاستی های لایه IP

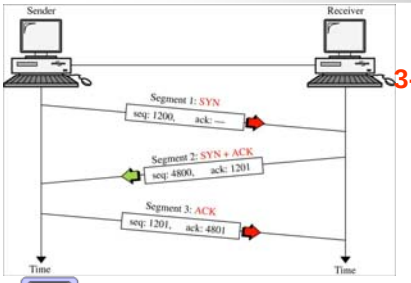
به پروتکلهایی که قبل از مبادلهٔ داده ها سعی در برقراری یک ارتباط و ایجاد هماهنگی قبلی مینمایند پروتکلهای "اتصال گرا" Connectuion Orientedگفته میشود. در این پروتکلها خاتمهٔ مبادلهٔ داده ها نیزبایستی در یک روند هماهنگ و با اطلاع قبلی انجام شود.

خاتمه ارتباط :

A خاتمهٔ ارسال داده های خود را اعلام میکند ولی باید منتظر بماند و به دریافت داده های ارسالی از طرف B ادامه بدهد تا آ نکه B نیز اعلام ختم ارتباط را تایید کند.

B نیز اعلام ختم ارتباط کرده و ارتباط ، در یک روند هماهنگ خاتمه مییابد.

مدل مرجع OSI



لایه حمل (Transport Layer)

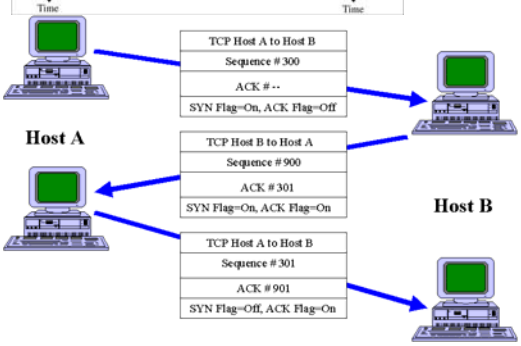
دست تکانی سه مرحله ای 3-way handshaking

فرآیند دست تکانی سه مرحله ای یا 1.SYN-2.SYN,ACK-3.ACK یک فرآیند بین ایستگاههای ابتدا و انتها، برای ایجاد یک ارتباط است.

در پروتکلهای اتصال گرا نظیر TCP قبل از ارسال داده های اصلی ابتدا باید یک ارتباط یا Connection بین مبدا و مقصد بوجود آید از اینرو ایستگاه فرستنده ابتدا یک بسته SYN به سمت گیرنده می فرستند. بسته SYN در واقع یک بسته TCP است که در سرآیند آن پرچم SYN ، ۱ شده است و این به معنی تمایل به ایجاد یک ارتباط است.

SYN=SYNchronize

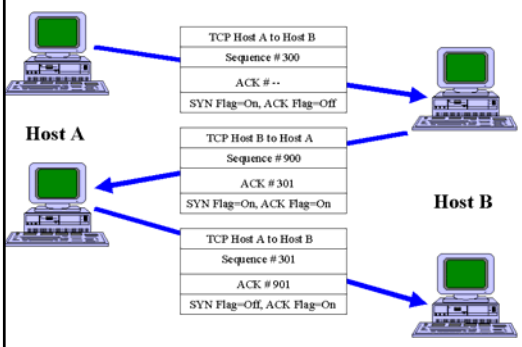
ACK=ACKnowledgement



M.Zangian

مدل مرجع OSI

دست تکانی سه مرحله ای 3-way handshaking



در صورتیکه گیرنده برای دریافت اطلاعات آمادگی داشته باشد ، با ارسال یک بسته با یک کردن پرچم SYN در هدر بسته ، تمایل خود را نیز برای ارسال اطلاعات اعلام داشته وعلاوه بر آن با ۱ کردن پرچم ACK دریافت بسته SYN را از طرف فرستنده تایید می کند.

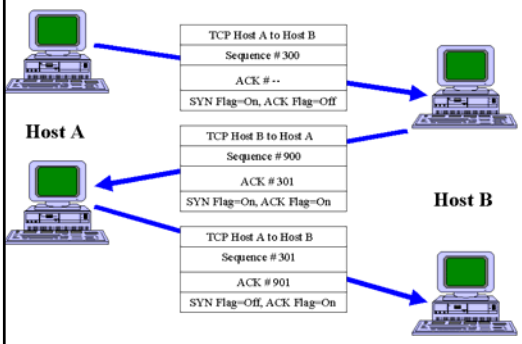
در مرحله آخر فرستنده باید دریافت بسته SYN را از طرف گیرنده تایید نماید بنابراین یک بسته ACK را به سمت گیرنده ارسال می کند.

بعد از این سه مرحله فرستنده و گیرنده می توانند شروع به ارسال و دریافت داده های اصلی بنمایند.علاوه براین در حین مراحل دست تکانی سه مرحله ای اطلاعات دیگری نیز بین فرستنده و گیرنده ردو بدل می شوند که برای ادامه ارتباط کاملا ضروری است.

M.Zangian

مدل مرجع OSI

دست تکانی سه مرحله ای 3-way handshaking

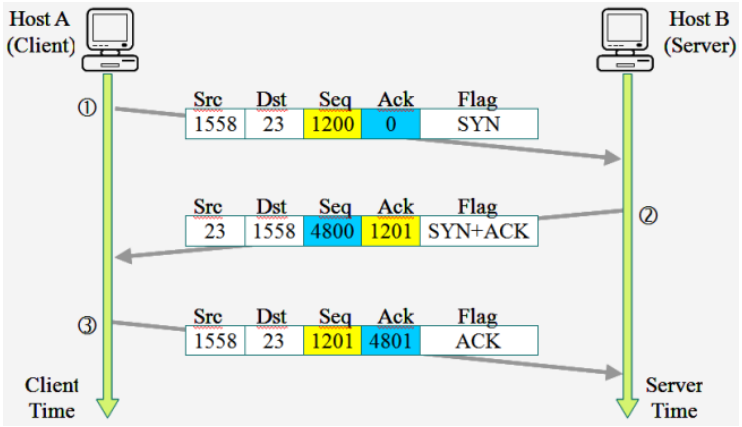


از جمله اطلاعاتی که در حین فرآیند دست تکانی سه مرحله ای بین فرستنده و گیرنده ردو بدل می شود Sequence Number است. Seq.Number . یک شماره است که بصورت اتفاقی تولید می شود و بدین معنی است که بسته های ارسال از طرف من از این به بعد از این شماره ، شماره گذاری می گردد. علت انتخاب اتفاقی Seq.Number دراینستکه احتمال اشتباه در بسته های دیگری که از ایستگاههای کاری مختلف ارسال شده است ، به حداقل برسد.

فرستنده و گیرنده هرکدام Seq.Number مربوط به خود را دارنددرواقع بسته های فرستنده از یک شماره اتفاقی و بسته های گیرنده از یک شماره اتفاقی دیگر شماره گذاری می شوند.بعد از این توافق بسته ها بصورت ترتیبی شماره گذاری می شوند. Seq.Number در بسته های داده به شماره اولین بایت داده موجود در آن بسته اشاره دارد.

M.Zangian

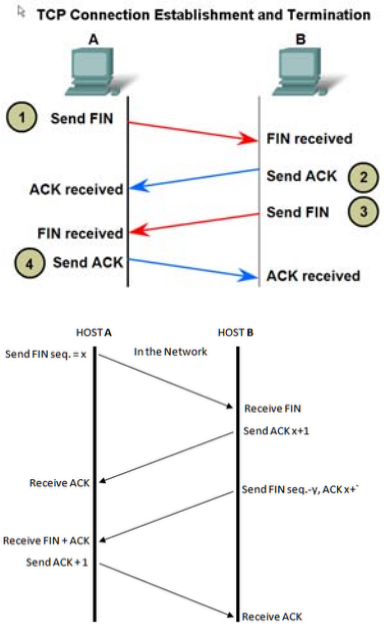
مدل مرجع OSI



علاوه بر این شماره پروسه (پورت) مبدا و مقصد نیز در این مرحله مشخص می شود و بعد از برقراری ارتباط در طول مرحله ارسال و دریافت داده بین مبدا و مقصد ، شماره پروسه ها ثابت باقی می ماند.

M.Zangian

مدل مرجع OSI



لایه حمل (Transport Layer)

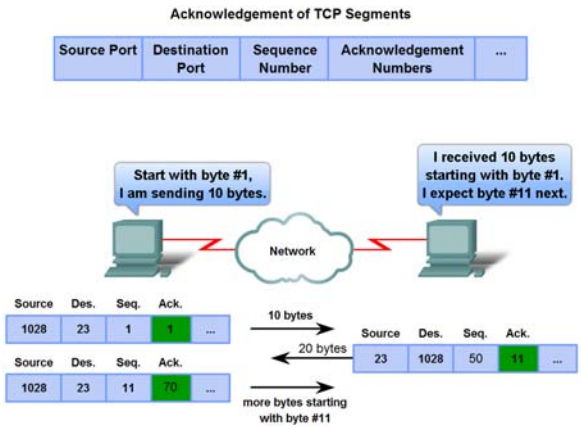
فرآیند قطع ارتباط

همانطوریکه برقراری ارتباط در یک سرویس اتصال گرا می بایست بین مبدا و مقصد هماهنگی شود و مورد توافق واقع شود، بعد از تبادل اطلاعات ، پایان ارتباط نیز باید به اطلاع برسد ، از اینرو هر طرف ارتباط ،در صورتیکه بخواهد ارتباط را پایان دهد ، در آخرین بسته ارسالی با یک کردن پرچم FIN(FINish) آنرا به اطلاع طرف مقابل می رساند و طرف مقابل با ارسال ACK دریافت آنرا تایید می کند. با این کار طرف درخواست کننده پایان ارتباط ، داده ای را ارسال نمی کند ولی تا زمانیکه طرف مقابل اطلاعاتی برای ارسال داشته باشد آنرا می پذیرد. در صورتیکه طرف مقابل هم داده ای برای ارسال نداشته باشد ، با ۱ کردن پرچم FIN آنرا به اطلاع طرف مقابل می رساند و با تایید دریافت این بسته ارتباط از دو طرف بسته می شود.

در صورتیکه این دو ایستگاه مجددا بخواهند داده ای را ردو بدل کنند ، دوباره باید فرآیند دست تکانی سه مرحله ای را برای شروع ارتباط مجدد انجام دهند.

مدل مرجع OSI

لایه حمل (Transport Layer)



بعد از انجام دست تکانی سه مرحله ای و برقراری ارتباط دو طرف براساس توافقات انجام شده ،اقدام به ارسال و دریافت داده می نمایند.توجه نمایید در هر مرحله Seq.Number به شماره اولین بایت موجود در ان بسته اشاره می کند.

مدل مرجع OSI

لایه حمل (Transport Layer)

رفع مشکل عدم دریافت بترتیب بسته ها(سگمنت ها)

- فرستنده بعد از شکستن داده به سگمنت برای هرکدام یک شماره ترتیب مشخص می کند و در سرآیند آن این شماره ترتیب را قرار می دهد.شماره ترتیب برای اولین بار از یک شماره تصادفی آغاز می شود.
- سگمنتها برای ارسال به سمت گیرنده به ترتیب در یک بافر قرار می گیرند.
- با ارسال هر سگمنت فرستنده یک تایمر(زمانسنج) تنظیم می نماید تا در صورت عدم دریافت تایید ارسال در این زمان نسبت به ارسال مجدد بسته اقدام نماید.
- به سرآیند هر بسته یک کد ۱۶ بیتی کشف خطا (CheckSum) برای کشف خطای احتمالی اضافه می گردد.
- گیرنده با دریافت هربسته و بعد از اطمینان از سالم بودن بسته یک پیغام تایید (Ack)به سمت فرستنده ارسال می گردد.
- فرستنده بعد از دریافت تایید ارسال یک سگمنت بافر مربوط به آنرا آزاد می نماید.و فرآیند ارسال را ادامه می دهد.

مدل مرجع OSI

لایه حمل (Transport Layer)

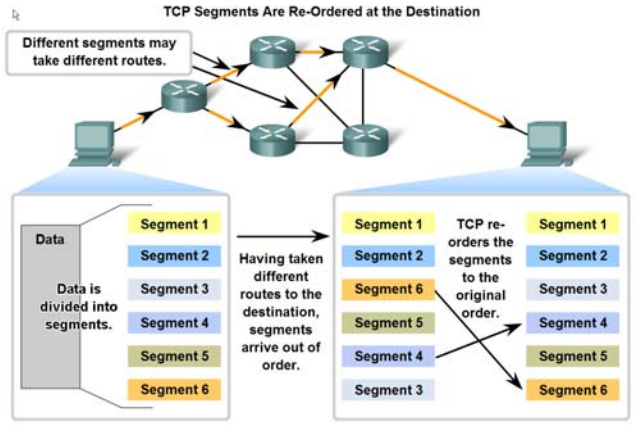
- در گیرنده در صورتیکه یک بسته دوبار دریافت شود (در اثر تاخیر در دریافت تایید یک بسته ممکن است با به پایان رسیدن تایمر مربوطه بسته مجدد ارسال گردد.) با کنترل شماره ترتیب Seq. Number یکی از بسته ها حذف می گردد.

ارسال Ack معمولا بصورت مجزا انجام نمی شود بلکه گیرنده تایید یک بسته ارسال شده(Ack) را به سرآیند بسته پاسخ اضافه می کند، مگر آنکه گیرنده داده ای را برای ارسال نداشته باشد.به این روش که باعث صرفه جویی در زمان می گردد Piggy Backing گفته می شود.

به پروتکلهایی که فقط در هنگام دریافت صحیح بسته ها پیغام Ack را بر می گردانند و در صورت بسته های خراب یا عدم دریافت بسته ساکت می مانند، پروتکلهای PAR(Positive Acknowledgement with Retransmission) می گویند.

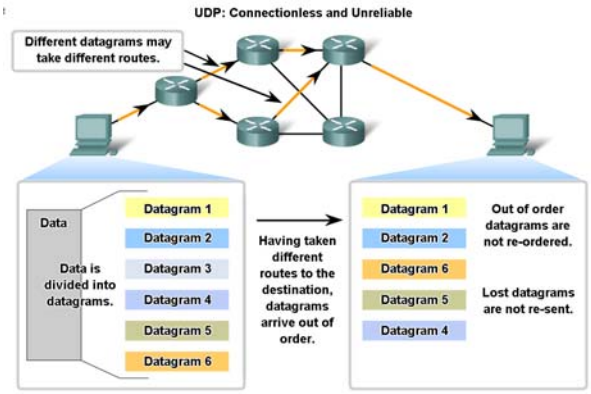
مدل مرجع OSI

مرتب کردن سگمنتهای دریافتی بر اساس Seq.Number در مقصددر پروتکل TCP



مدل مرجع OSI

عدم وجود مکانیزم مرتب سازی و نیز دریافت مجدد بسته های گم شده در UDP



در UDP در صورت نیاز لایه Application متولی درست رسیدن بسته ها خواهد بود.

مدل مرجع OSI

لایه حمل (Transport Layer)

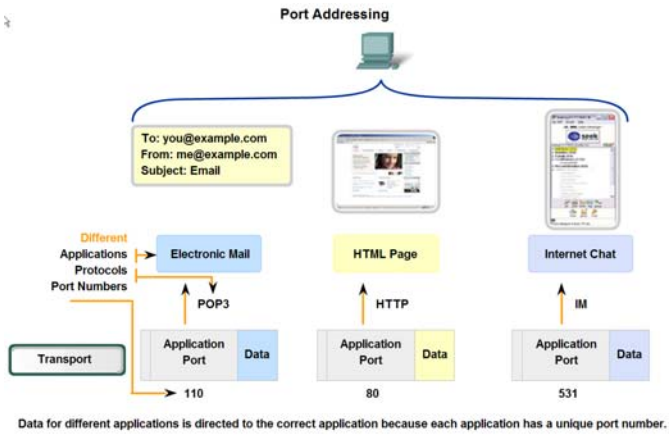
رفع مشکل عدم تفکیک پروسه های همزمان و متفاوت

هر پروسه برای تقاضای برقراری یک ارتباط با پروسهای دیگر روی شبکه ، یک شمارهٔ شناسایی برای خود برمی گزیند. به این شمارهٔ شناسایی "آدرس پورت" گفته می شود.

- **شماره پورت در هرسیستم برای یک پروسه یکتا ست و پروسه دیگر نمی تواند شماره پورت مشابه با پروسه دیگر را انتخاب نماید.**
- **سیستم عامل شماره پورت انتخاب شده برای یک پروسه را در جدولی نگهداری می کند و اجازه نمی دهد پروسه دیگربرروی همان ماشین شماره پورت یکسان داشته باشد.**
- **در سرآیند هر بسته TCP یک شماره پورت برای پروسه مبدا و یک شماره پورت برای پروسه متناظر در مقصد در نظر گرفته می شود.**
- **از ترکیب آدرس IP و آدرس پورت برای تفکیک هر پروسه بین تمام پروسه های موجود در شبکه ای مانند اینترنت استفاده نمود.(پروسه یکتا بصورت جهانی) به این ترکیب آدرس سوکت گفته می شود.**

مدل مرجع OSI

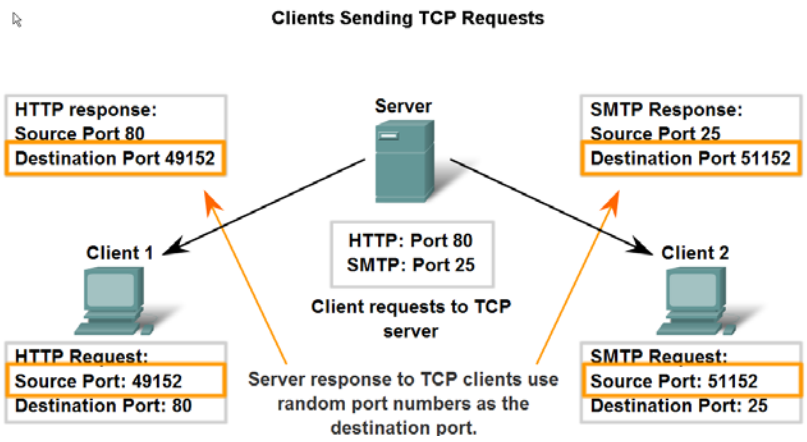
لایه حمل (Transport Layer)



در این تصویرنقش شماره پورت برای ارائه سرویس های مختلف نشان داده شده است .هر برنامه کاربردی برای ارائه سرویس از یک پورت منحصر بفرد استفاده می نماید.

مدل مرجع OSI

لایه حمل (Transport Layer)

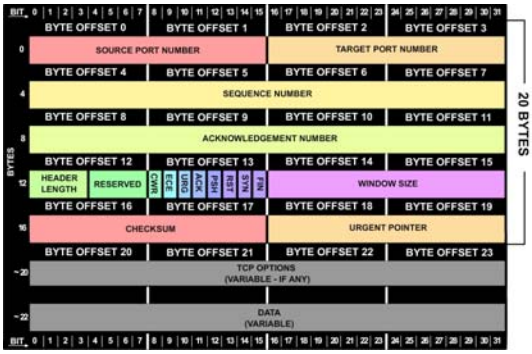


در تصویر بالا نقش شماره پورت در ایجاد نشست TCP و هدایت سگمنتها به پردازشهای سرور نشان داده شده است.

مدل مرجع OSI

لایه حمل (Transport Layer)

بررسی فیلدهای سرآیند TCP



- Source Port: در این فیلد یک شمارهٔ ۱۶ بیتی بعنوان آدرس پورت پروسهٔ مبدأ که این بسته را جهت ارسال ، تولید کرده ، قرار خواهد گرفت.
- Target Port: در این فیلد ، آدرس پورتِ پروسهٔ مقصد که آنرا تحویل خواهد گرفت ، تعیین خواهد شد.

مدل مرجع OSI

لایه حمل (Transport Layer)

•شماره پورت عددی بین ۰ تا ۶۵۵۳۵ می باشد که برنامه های کاربردی مختلف برای تمایز پروسه های همزمان از شماره پورت های مختلفی برای تمایز استفاده می نمایند. برخی از برنامه های کاربردی رایج از شماره پورتهای استاندارد که عددی بین ۰- ۱۰۲۳ می باشد استفاده می نمایند.پورتها با شماره ۱۰۲۴ تا ۶۵۵۳۵ می تواند برای سایر برنامه های کاربردی مورد استفاده قرار گیرد.

آدرس سوکت

استفاده از آدرس IP به همراه شماره پورت می تواند یک پروسه یکتا را برروی هرماشین در دنیا مشخص نمایدبه این ترکیب آدرس سوکت می گویند.

(IP Address : Port Number) = Socket Address

مثال : 193.142.22.121:80

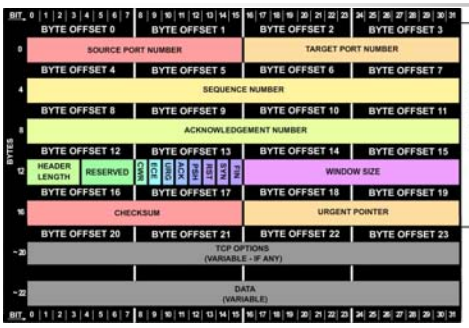
IP بسته را تا کامپیوتر مقصد مسیریابی میکندو Port درون کامپیوتر بسته را به پروسس مورد نظر می رساند.

مدل مرجع OSI

توجه نمایید شماره پورت برای ایستگاههایی که بعنوان سرویس دهنده مورد استفاده قرار می گیرند باید از یک استاندارد مشخص پیروی نماید چرا که سرویس گیرنده های مختلف که می خواهند از یک سرویس دهنده سرویس بگیرند باید شماره پورت سرویس مورد نظر را بدانند از اینرو با انتخاب استاندارد پورت ، این کار به سهولت انجام می شود.

البته در برخی مواقع برای افزایش امنیت از شماره پورت استاندارد برای ارتباط اختصاصی استفاده نمی شود بنابراین سرویس گیرنده باید از شماره پورت سرویس در سمت سرویس دهنده مطلع باشد. بنابراین این موضوع کمی امنیت را بالاتر خواهد برد.

مدل مرجع OSI



لایه حمل (Transport Layer)

• Sequence Number : این فیلد سی و دو بیتی ، شمارهٔ ترتیب اولین بایتی را که در "فیلد داده" از بستهٔ جاری قرار دارد ، نشان میدهد.

در اولین سگمنت ارسالی یک عدد تصادفی درون Sequence Number قرار می گیرد و این فیلد از صفر شروع نمی شود.

Acknowledgement Number:

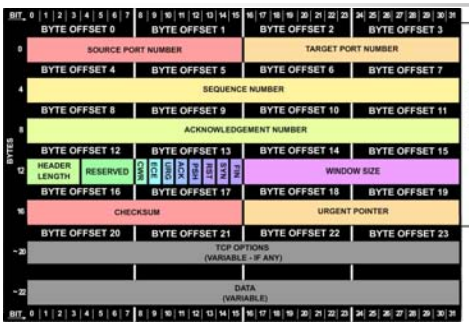
این فیلد ۳۲ بیتی نیز شمارهٔ ترتیب بایتی که گیرنده بسته منتظرِ دریافت آن است را تعیین میکند.

Header Length: عددی که در این فیلد قرار میگیرد ، طول سرآیندبستهٔTCP را بر مبنای کلمات ۳۲ بیتی تعیین میکند . بعنوان مثال اگر در این فیلدعدد ۷ قرار بگیرد طول سرآیند مقدار۴×۷ برابر ۲۸ بایت خواهد بود. طول این فیلد ۴ بیت است بنابراین طول سرآیند TCP حداقل ۲۰ و حداکثر ۶۰ بایت می باشد.

•بدلیل اینکه ممکن است طول سرآیند بیش از ۲۰ بایت باشد و اطلاعات اضافی در قسمت Option قرار گیرد طول سرآیند محل دقیق شروع داده را دریک سگمنت مشخص می نماید.

M.Zangian

مدل مرجع OSI



لایه حمل (Transport Layer)

• Reserved : ۶ بیت رزرو شده برای استفاده های آتی.

•Flag Bits: ۶ بیت flag هر کدام بعنوان یک پرچم مورد استفاده قرار می گیرند که معانی خاص خود را دارند.

بیت URG(Urgent Pointer) :

در صورتیکه این بیت مقدار ۱ را داشته باشد به معنی معتبر بودن مقدار موجود در فیلد Urgent Pointer است و می بایست این فیلد مورد پردازش قرار گیرد در صورتیکه این بیت صفر باشد به معنی غیر معتبر بودن فیلد Urgent Pointer است و از آن چشم پوشی می شود.

بیت ACK:

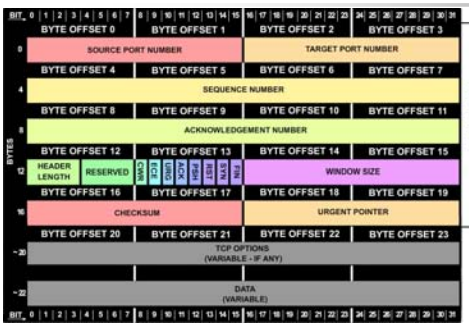
اگر در این بیت مقدار ۱ قرار گیرد به معنی معتبر بودن مقدار موجود در فیلد Acknowledgement Number است.

M.Zangian

مدل مرجع OSI

65

لایه حمل (Transport Layer)



- بیت PSH:فرستنده با یک کردن این بیت از گیرنده می خواهد که داده های موجود در این بسته را بافر نکند و در اسرع وقت برای پردازشهای برنامه کاربردی به لایه های بالاتر منتقل نماید.در پروتکل TCP معمولا داده های کوچک بافر می شوند تا زمانیکه حجم داده به مقدار معینی برسد و سپس اطلاعات را یکجا تحویل لایه های بالاتر بدهد. این موضوع دربرخی از موارد ایجاد مشکل می نماید .

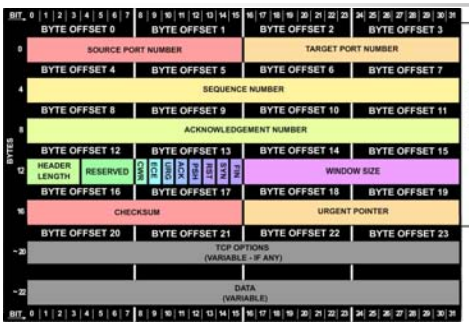
بعنوان مثال در برنامه ای نظیر telnet ممکن است بخواهیم با فرستادن علامت ؟ گیرنده فهرستی از فرامین ماشین را برای ما بفرستد درصورتیکه گیرنده بخواهد این کاراکتر را بافر کرده و منتظر رسیدن آن به مقدار معینی باشد، ایجاد مشکل می کند در این حالت باید از گیرنده بخواهیم داده را بافر نکرده و سریعا به برنامه کاربردی منتقل نماید.

M.Zangian

مدل مرجع OSI

66

لایه حمل (Transport Layer)



- بیت RST:

در صورتیکه یکی از طرفین ارتباط به هر دلیلی (نقص نرم افزاری یا سخت افزاری) بخواهد ارتباط را بصورت یکطرفه قطع نماید با یک کردن این بیت به طرف مقابل قطع یکطرفه ارتباط را اعلام می نماید و برای از سرگیری ارتباط باید دوباره فرایند شروع ارتباط انجام شود.علاوه بر این RST میتواند بعنوان علامت عدم پذیرش ارتباط مورد استفاده قرار می گیرد.

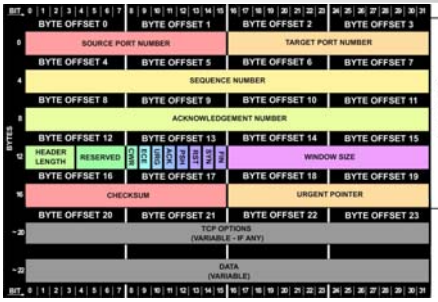
بیت SYN:

این بیت نقش اساسی در برقراری یک ارتباط بازی می کند.شروع کننده ارتباط با ارسال یک بسته TCP بدون داده و با تنظیم SYN=1,Ack=0 تقاضای برقراری ارتباط را به طرف مقابل اعلام میکند.

M.Zangian

مدل مرجع OSI

لایه حمل (Transport Layer)



بیت FIN:

اگر یکی از طرفین ارتباط داده ای را برای ارسال به طرف مقابل نداشته باشد در آخرین بسته خود این بیت را یک می کند.و در واقع ارسال اطلاعات را بصورت یکطرفه قطع مینماید. در این حالت طرف مقابل می تواند همچنان به ارسال اطلاعات ادامه دهد و در نهایت با یک کردن بیت FIN در آخرین بسته خود ارتباط بصورت کامل قطع خواهد شد.

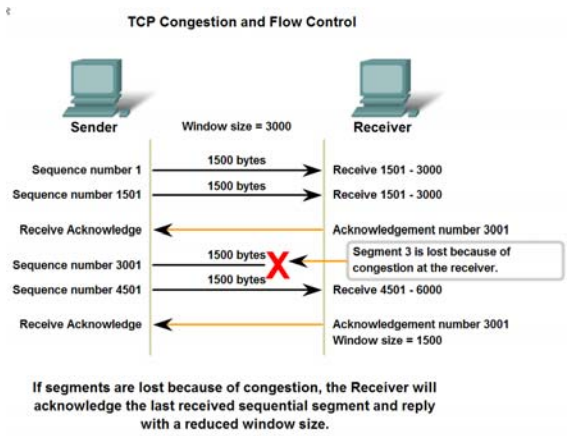
فیلد Windows Size:

مقدار قرار داده شده در این فیلد بیانگر میزان فضای خالی بافر گیرنده می باشد و گیرنده به طرف مقابل اعلام میکند که از بایت با شماره Acknowledgement Number حداکثر تا Windows Size میتواند ارسال داشته باشد و ارسال بیش از این مقدار باعث سرریز شدن بافر و نادیده گرفتن آن خواهد شد.مقدار صفر در این فیلد به معنی پر شدن کامل بافر گیرنده است.و فرستنده با دریافت این مقدار ارسال خود را متوقف می نماید.

M.Zangian

مدل مرجع OSI

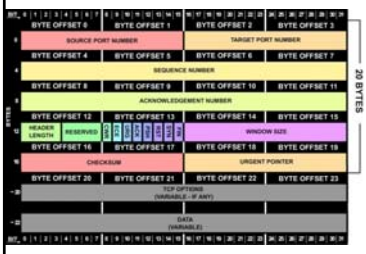
لایه حمل (Transport Layer)



استفاده از Window Size برای کنترل جریان

M.Zangian

مدل مرجع OSI



Checksum:

یک فیلد ۱۶ بیتی، برای کشف خطاست که با محاسبه تولید میشود. این فیلد با قرار دادن صفر بجای فیلد Checksum محاسبه شده و با قراردان نتیجه در Checksum به سمت گیرنده ارسال می شود.در گیرنده با دریافت کل سرآیندو داده ، Checksum به ترتیب که گفته خواهدشد، مجددا محاسبه شده و اگر تمام بیتهای نتیجه ۱ باشد(معادل صفر در مکمل ۱) نتیجه بدون خطاست.

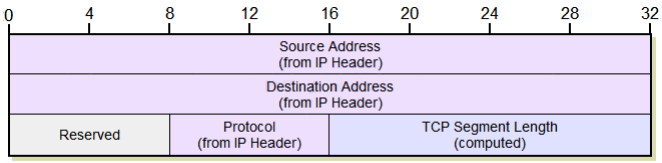
برای محاسبه Checksum:

۱- ابتدا یک سرآیند فرضی (به صورت زیر) به مجموعه سرآیند و داده سگمنت TCP منهای قسمت Checksum اضافه می گردد(۱۶ بیت checksum صفر در نظر گرفته می شوند.). و کل مجموعه بصورت کلمات ۱۶ بیتی در نظر گرفته می شوند.

Source IP Address		
Destination IP Address		
00000000	00000110	TCP Segment Length

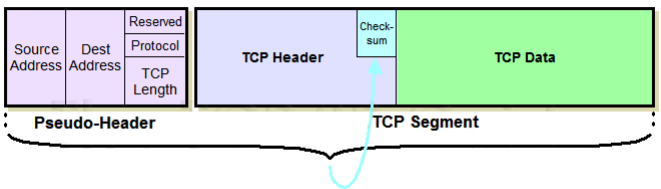
Pseudo-Header

مدل مرجع OSI



TCP "Pseudo Header" For Checksum Calculation

سرآیند کاذب که برای محاسبه Checksum به سرآیند TCP اضافه می شود.



Checksum Calculated Over Pseudo Header and TCP Segment

قرار دادن checkSum در سرآیند TCP

مدل مرجع OSI

TCP pseudo-header (IPv4)

Bit offset	0–3	4–7	8–15	16–31
0	Source address			
32	Destination address			
64	Zeros		Protocol	TCP length
96	Source port			Destination port
128	Sequence number			
160	Acknowledgement number			
192	Data offset	Reserved	Flags	Window
224	Checksum			Urgent pointer
256	Options (optional)			
256/288+	Data			

۲-داده های ۱۶ بیتی در سیستم مکمل یک با یکدیگر جمع می شوند.

۳- نتیجه حاصل جمع مکمل یک می گردد(صفرها به یک و یکها به صفر تبدیل میشوند.)

۴- checksum به سرآیند اضافه شده و به سمت مقصد ارسال می گردد.

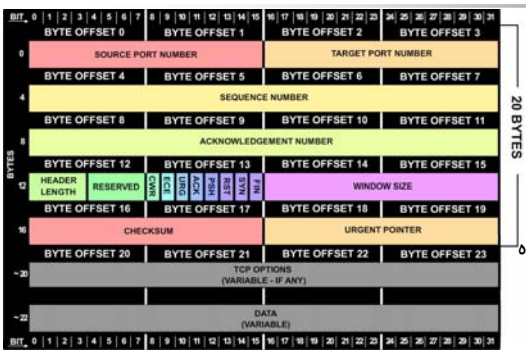
۶- در مقصد بیتهای سرآیند و دیتا (بهمراه Checksum) در سیستم مکمل یک با هم جمع می شوند ودر صورتیکه تمامی بیتها برابر یک شد اطلاعات صحیح درغیر اینصورت اطلاعات اشتباه است.

مدل مرجع OSI


```
      1000 0110 0101 1110
      1010 1100 0110 0000
      0111 0001 0010 1010
      1000 0001 1011 0101

First, we add the 16-bit values 2 at a time:

         1000 0110 0101 1110   First 16-bit value
      +  1010 1100 0110 0000   Second 16-bit value
        --------------------
        1 0011 0010 1011 1110  Produced a carry-out, which gets added
      + \----------------> 1   back into LBb
        --------------------
          0011 0010 1011 1111
      +   0111 0001 0010 1010  Third 16-bit value
        --------------------
        0 1010 0011 1110 1001  No carry to swing around (**)
      +   1000 0001 1011 0101  Fourth 16-bit value
        --------------------
        1 0010 0101 1001 1110  Produced a carry-out, which gets added
      + \----------------> 1   back into LBb
        --------------------
          0010 0101 1001 1111  Our "one's complement sum"


      0010 0101 1001 1111   Our "one's complement sum"

      1101 1010 0110 0000   The "one's complement"
```

درسیستم مکمل یک معادل صفر است 259F(H)+DA60(H)=FFFF(H)

مدل مرجع OSI



Urgent Pointer:

در این فیلد عددی به عنوان اشاره گر قرار میگیرد که موقعیت داد ه های اضطراری را درون بسته TCP جاری معین میکند، مانندداده های مربوط به وقفه ها که درون بسته جاری ارسال می شوند وبدون قطع ارتباط فعلی توسط برنامه کاربردی در لایه بالاتر پردازش می شود و در لایه TCP پردازش نمی گردد.

فیلد Option:

این فیلد اختیاری است و می تواند برای منظورهای مختلفی مورد استفاده قرار گیرد بعنوان مثال این فیلد می تواند حاوی اطلاعات حداکثر اندازه مجاز بسته TCP باشد.

Urgent:فوری-اضطراری

M.Zangian

مدل مرجع OSI

فیلد Option:

طول فیلد Option متغییر بوده و می تواند از صفر تا ۳۲۰ بیت (۴۰ بایت)باشد. طول این فیلد حتما باید مضربی از ۳۲ بیت (مضارب صحیح از ۴ بایت) بوده و در صورتیکه طول این فیلد کمتر از مضرب صحیح از ۳۲ بیت بود باقیمانده با داده اضافی پر می گردد.

M.Zangian

مدل مرجع OSI

لایه حمل (Transport Layer)

رفع مشکل کنترل جریان و خطا

- عدم کنترل جریان در ارتباط بین دو ایستگاه کاری باعث اتلاف منابع سیستم و شبکه می شود.

کنترل جریان وخطا در دوسطح قابل انجام است:

- کنترل جریان و خطا در سطح یک خط(لینک) ارتباطی(بین دو دستگاه متصل به دو سر یک خط ارتباطی)
- کنترل جریان و خطا بین دو گره نهایی در شبکه (فرستنده و گیرنده نهایی)

- کنترل خطا و جریان در لایه حمل در نقاط انتهایی و ایستگاههای ابتدا و انتهای یک ارتباط انجام می گیرد.
- کنترل جریان میزان داده قابل انتظار در هر زمان را مشخص می کند
- کنترل خطا مشخص می کند خطاها چگونه باید تصحیح شوند.
- مباحث کنترل جریان داده و خطا در دو لایه پیوند داده و لایه حمل و در دو سطح مختلف پیاده سازی می شود .بنابراین مباحث مربوط به این بخش می تواند بصورت مشترک باشد.

مدل مرجع OSI

- کنترل جریان داده

جریان داده ارسال شده از طرف فرستنده باید بگونه ای باشد که گیرنده را در خود غرق نکند.

داده های ورودی می بایست قبل از استفاده بررسی و پردازش شونداغلب سرعت پردازش کمتر از سرعت ارسال داده هاست بنابراین هر دستگاه گیرنده، دارای حافظه ای به نام بافر است که داده های ارسال شده را پیش از پردازش بافرمینماید. اگر بافر در حال پر شدن باشد گیرنده باید بتواندا فرستنده بخواهد ارسال را تا زمانیکه امکان دریافت آن وجود داشته باشد متوقف نماید.

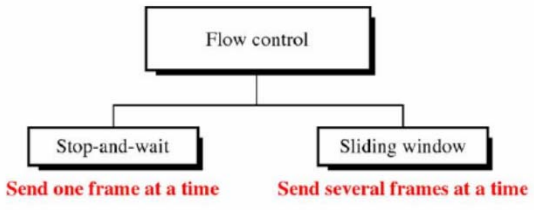
مدل مرجع OSI

روشهای کنترل جریان و خطا :

بطور کلی دو روش کنترل جریان مورد استفاده قرار می گیرد:

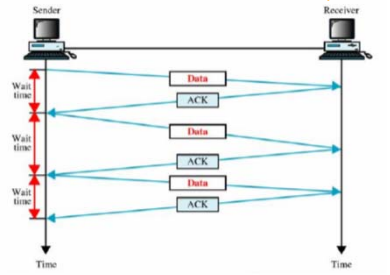
۱- توقف و انتظار (Stop-and-Wait)

۲- پنجره های لغزان (Sliding Window)



مدل مرجع OSI

روشهای کنترل جریان و خطا – توقف و انتظار

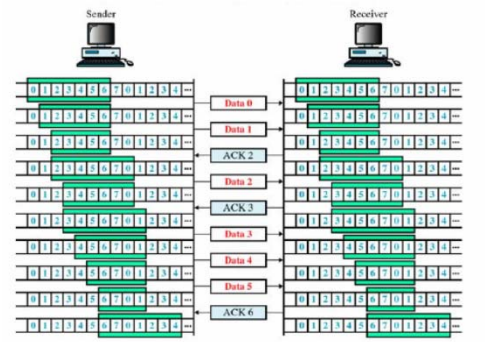


درروش توقف و انتظار فرستنده بعد از هر ارسال منتظر دریافت یک تصدیق می ماند.

فریم (سگمنت) بعدی تنها در صورتی ارسال می شود که تصدیق فریم قبلی دریافت شده باشد. این فرآیند ارسال و انتظار آنقدر ادامه پیدا می کند که فرستنده فریم انتهای ارسال را بفرستد.مزیت این روش سادگی آنست اما عیب مهمی که مطرح است ،کارایی پایین و کند بودن این روش است بخصوص زمانی که تاخیر ارسال بین فرستنده و گیرنده زیاد باشد (ارتباطات ماهواره ای)

مدل مرجع OSI

روشهای کنترل جریان و خطا – روش پنجره لغزان(Sliding Window)



• در روش توقف و انتظارفرستنده با ارسال هر بسته منتظر دریافت تایید از گیرنده می شود و تا زمانیکه پیغام تایید دریافت نشود بسته بعدی ارسال نخواهد شد اما در روش پنجره لغزان فرستنده در محدوده یک پنجره فرضی ارسال را شروع می کند و تا پایان پنجره به ارسال خود ادامه میدهد و متوقف نمی گردد. سپس با دریافت هر بسته تایید از طرف گیرنده پنجره یکی بطرف جلو شیفت پیدا میکند و می تواند محدوده خود را به سمت بسته های جدید گسترش دهد.

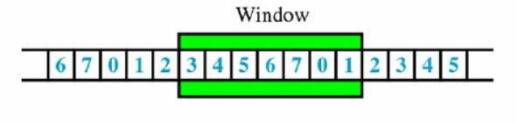
مدل مرجع OSI

روشهای کنترل جریان و خطا – روش پنجره لغزان

•گیرنده می تواند برای چند فریم دریافت شده تنها یک پیغام Ack ارسال نماید و با دریافت Ack با یک شماره به معنای دریافت تمامی فریمهای قبل از آن شماره خواهد بود.

•شماره گزاری فریمها با پیمانه n صورت می گیرد و فریمها از ۰ تا n-1 شماره گزاری می گردند. یعنی اگر n=5 باشد فریمها بصورت 0,1,2,3,4,0,1,2,3,4,... شماره گزاری می شوند.

•در شروع فرآیند هر دو پنجره فرضی n-1 فریم خواهد داشت .بنابراین پیش از نیاز به هرگونه تصدیق n-1 فریم می تواند ارسال شود.

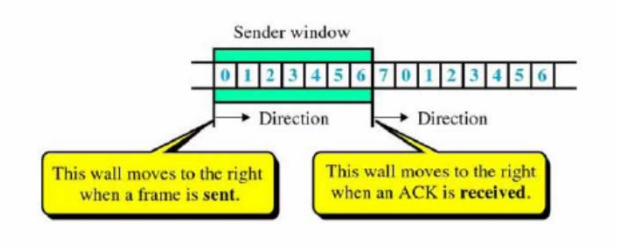


مدل مرجع OSI

روشهای کنترل جریان و خطا – روش پنجره لغزان

پنجره فرستنده

• در سمت فرستنده با آغاز ارسال، پنجره شامل w=n-1 فریم است با ارسال هر فریم سمت چپ پنجره به سمت داخل حرکت کرده و اندازه پنجره کاهش می یابد. بنابراین اگر اندازه پنجره را w بگیریم با ارسال ۳ فریم بدون دریافت Ack اندازه پنجره w-3 خواهد شد.حال با دریافت هر پیغام Ack به ازای هر فریم پنجره مورد نظر از سمت راست گسترش می یابد.

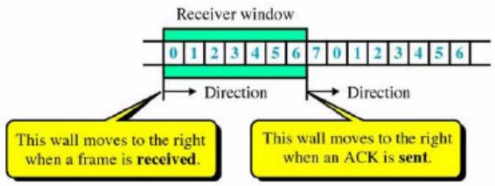


مدل مرجع OSI

روشهای کنترل جریان و خطا – روش پنجره لغزان

پنجره گیرنده

• در ابتدای دریافت پنجره گیرنده به تعداد n-1 فضای خالی برای دریافت فریمها در نظر گرفته است.زمانیکه یک فریم دریافت گردد اندازه پنجره گیرنده کم می شود.در صورتیکه گیرنده به ازای دریافت فریمها پیغام Ack ارسال نماید به تعداد فریمهای تایید شده پنجره از سمت راست گسترش می یابد و فضای خالی برای دریافت فریمهای جدید ایجاد می گردد.



مدل مرجع OSI

روشهای کنترل جریان وخطا- روش پنجره لغزان

• سئوال: چرا اندازه پنجره یکی کمتر از اندازه پیمانه در نظر گرفته می شود؟ (W=n-1)

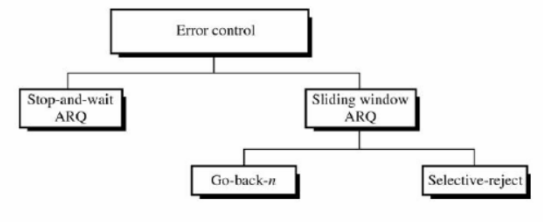
فرض کنید n=8 و اندازه پنجره نیز مساوی آن یعنی ۸ انتخاب شود. با ارسال فریم ۰ و دریافت یک Ack=1 پنجره یکی به سمت راست حرکت می نماید.یعنی شامل فریمهای 1,2,3,4,5,6,7,0 حال اگر به هر دلیل پیغام Ack=1 (بمعنی دریافت فریم 0) تکرار شود مشخص نیست این پیغام تایید برای فریم 0 قبلی است یا تایید برای 0 فریم جدید.بنابراین برای رفع هر گونه ابهامی اندازه پنجره w=n-1 در نظر گرفته می شود.

مدل مرجع OSI

روشهای کنترل جریان و خطا

درخواست خودکار تکرار(Automatic Repeat Request)ARQ

• در صورتیکه فریم ارسال شده در گیرنده دریافت نشود و یا با خطا دریافت گردد می بایست فریم مورد نظر دوباره فرستاده شود.از اینرو مکانیزمی برای ارسال مجدد فریمها باید پیش بینی شود.



روشهای کنترل خطا

مدل مرجع OSI

روشهای کنترل جریان و خطا

درخواست خودکار تکرار(Automatic Repeat Request)ARQ

توقف و انتظار ARQ

در روش توقف و انتظار گفتیم فرستنده با ارسال هر فریم منتظر دریافت پیغام تصدیق از سمت گیرنده است بنابراین در صورت عدم دریافت فریم فرستنده باید بتواند آنرا مجددا ارسال نماید برای این منظور می بایست چهار ویژگی به سازوکار کنترل جریان در روش توقف و انتظار افزوده شود.

۱- فرستنده یک نسخه از فریم ارسالی را تازمانیکه تصدیق آنرا دریافت نکرده است نگهداری می کند تا در صورت نیاز بتواند مجددا آنرا ارسال نماید.

۲- بمنظور شناسایی فریمها فریمهای داده جهت ارسال به ترتیب با الگوی 0,1,0,1,… شماره گزاری می گردد.(شماره فریمهای صفر با Ack1 و شماره فریمهای یک با Ack0 تایید می شوند.

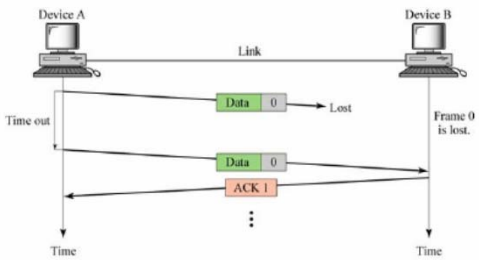
۳- در صورتیکه خطایی در فریم دریافت شده وجودداشته باشدگیرنده یک پیغام NAK را که بمعنی درخواست ارسال مجدد آخرین فریم ارسال شده است به فرستنده ارسال می کند.

مدل مرجع OSI

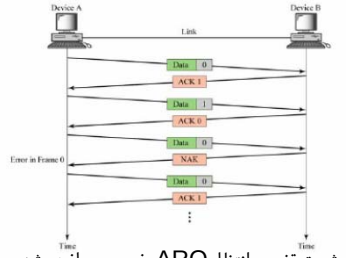
روشهای کنترل جریان و خطا

توقف و انتظار ARQ

۴- دستگاه فرستنده برای هر فریم ارسالی یک زمانسنج در نظر می گیرد اگرزمان تصدیق یک فریم از مدت زمان تعیین شده بیشتر شودفرستنده با فرض گم شدن فریم ،مجددا آنرا می فرستد.



روش توقف و انتظارARQ، فریم گم شده(ویا تصدیق گم شده)



روش توقف و انتظارARQ، فریم دریافت شده با خطا

مدل مرجع OSI

روشهای کنترل جریان و خطا – روش پنجره لغزان

روش پنجره لغزان ARQ

برای پیاده سازی ARQ در روش پنجره لغزان ، الگوریتمهای مختلفی مورد استفاده قرار می گیردکه از میان این روشها دو روش بیش از همه مورد استفاده قرار می گیرد که در ادامه به بررسی این روشها خواهیم پرداخت.

روش بازگشت به n : (Go Back n)

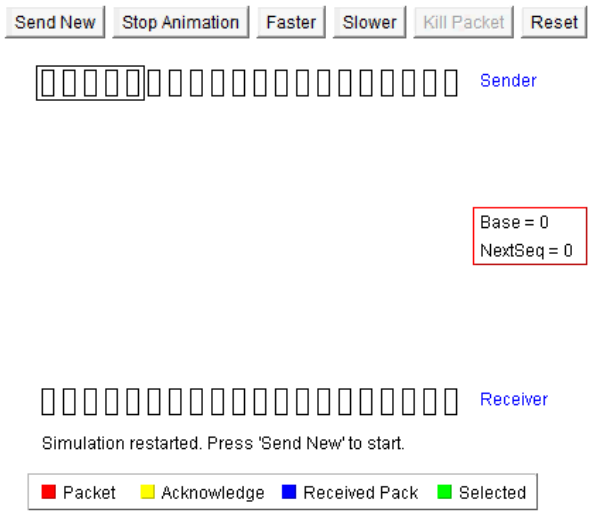
دراین روش در صورتیکه درگیرنده یک فریم بطور صحیح دریافت نگردد از آن فریم به بعد دیگر پیغام Ack ارسال نخواهد شد تا جاییکه فرستنده به انتهای پنجره برسد و بدلیل اینکه پیغام Ack دریافت نداشته پنجره گسترش پیدا نمی کند و متوقف می شود. این توقف تا زمانی ادامه پیدا می کند که تایمر مربوطه به پایان زمان خود برسد با پایان این زمان فریم تصدیق نشده و تمامی فریمهای بعد از آن مجددا ارسال می شود حتی اگر فریم های بعدی قبلا دریافت شده باشد.

M.Zangian

مدل مرجع OSI

روشهای کنترل جریان و خطا – روش پنجره لغزان

روش بازگشت به n : (Go Back n)



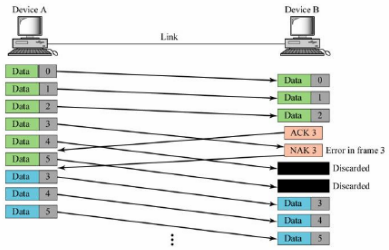
M.Zangian

مدل مرجع OSI

روشهای کنترل جریان و خطا – روش پنجره لغزان

روش بازگشت به n : (Go Back n)

•درروش Go Back n می توان بجای ارسال Ack به ازای هر فریم دریافت شده، از یک پیغام Ack برای چند فریم ،استفاده نمود و در صورت عدم دریافت صحیح یک فریم با استفاده از یک پیغام NAck فرستنده را از موضوع مطلع کرد. دریافت NAck x به معنی دریافت فریم ها تا X-1 و عدم دریافت صحیح X است.

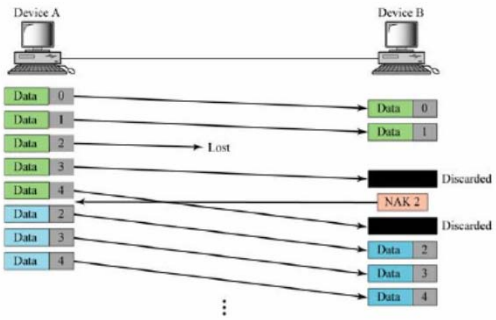


روش بازگشت به n–فریم آسیب دیده

مدل مرجع OSI

روشهای کنترل جریان و خطا – روش پنجره لغزان

روش بازگشت به n : (Go Back n)

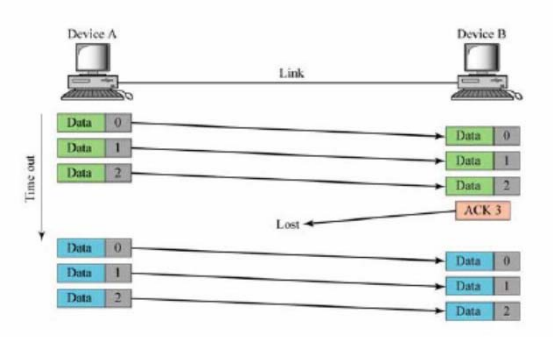


روش بازگشت به n–فریم گم شده

مدل مرجع OSI

روشهای کنترل جریان و خطا – روش پنجره لغزان

روش بازگشت به n : (Go Back n)



روش بازگشت به n– تصدیق گم شده

مدل مرجع OSI

روشهای کنترل جریان و خطا – روش پنجره لغزان

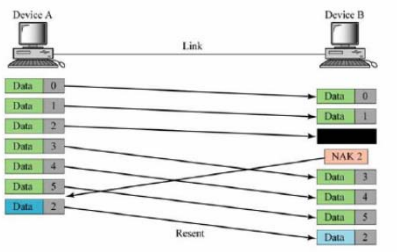
روش رد انتخابی(Selective Reject)

• در روش بازگشت به n بعد از عدم دریافت صحیح یک فریم فریمهای بعدی مورد پذیرش قرار نمی گیرند و می بایست تمام فریمهای پنجره ارسال بعد از فریم آسیب دیده مجددا ارسال گردد اما در روش رد انتخاب تنها ارسال فریم آسیب دیده درخواست می شودو فریمهایی بعدی که صحیح دریافت شده اند مجددا ارسال نخواهد شد.(به این روش ، روش تکرارانتخاب Selective Repeat نیز گفته می شود.)

مدل مرجع OSI

•در این روش هر چند می توان فریمها را خارج از نوبت دریافت کرد اما نمی توان آنها را خارج از نوبت تصدیق نمود.اگر یک فریم گم شود .فریم بعدی خارج از نوبت دریافت شده است و گیرنده هنگام مرتب سازی فریمها متوجه فقدان یک فریم شده و یک NACK رابرای فرستنده ارسال می نماید.گیرنده تا فریم های بعدی را دریافت نکند متوجه فقدان یک فریم نخواهد شد. اگر فریم مفقود شده آخرین فریم باشدگیرنده هیچ عملی را انجام نمی دهد و فرستنده با آن همانند یک تصدیق گم شده رفتار می کند.

•در صورتیکه پیغام تصدیق گم شود و یا به فرستنده نرسد بعد از رسیدن فرستنده به پایان پنجره ، زمانسنج را بکار می اندازد و بعد از سپری شدن زمان تمام فریمهای تصدیق نشده مجددا ارسال می شود.



روش رد انتخابی ارسال مجدد فریم آسیب دیده

M.Zangian

مدل مرجع OSI

روشهای کنترل جریان و خطا – روش پنجره لغزان

روش رد انتخابی(Selective Reject)

سیستم مبتنی بر رد انتخاب می بایست برای پیاده سازی این روش ویژگیهای زیر را در خود داشته باشد:

• چون تنها فریمهای آسیب دیده درخواست و مجددا ارسال می گردد در این روش می بایست مکانیزمی برای مرتب سازی فریمها وجود داشته باشد.

•دستگاه فرستنده باید مکانیزمی برای جستجو و ارسال مجدد فریم درخواست شده فراهم آورد.

•یک بافر می بایست در گیرنده فریمهای دریافتی را نگه دارد تا بتواند درخواست ارسال مجددو حذف داده های تکراری و مرتب سازی فریمها را انجام دهد.

•در اینجا پیغام ACK به همان فریم تایید شده اشاره می کند و نه به شماره فریم بعدی(همانند NAck در مورد فریمهای تایید نشده) .

M.Zangian

مدل مرجع OSI

روشهای کنترل جریان و خطا – روش پنجره لغزان

روش رد انتخابی(Selective Reject)

• بدلیل پیچیده بودن این روش توصیه شده است اندازه پنجره در این روش کوچکتر از اندازه پنجره در روش بازگشت به n باشد.و اگر اندازه پنجره در روش بازگشت به n را برابر n-1 در نظر بگیریم انداز پنجره در این روش (n+1)/2توصیه شده است.

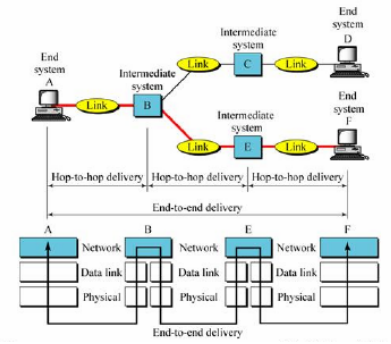
تحقیق:

در روش Selective Reject مقصد چگونه بسته NAck را برای ارسال مجدد به مبدا اعلام می کند؟
(شماره بسته را در کدام یک از فیلدهای سرآیند به مقصد اعلام می کند؟)

مدل مرجع OSI

لایه شبکه (Network Layer)

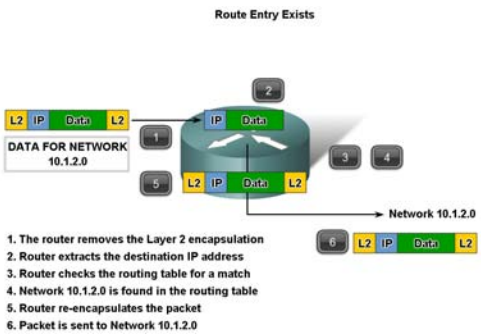
لایه شبکه مسئول تحویل بسته از مبدا به مقصد نهایی از میان شبکه ای متشکل از تعداد زیادی خط ارتباطی (لینک) است.تفاوت این لایه با لایه پیوند داده در این است که لایه شبکه وظیفه انتقال بسته ها را بین نقاط انتهایی مبدا و مقصد را بعهده دارد در حالیکه لایه پیوند داده انتقال بسته(فریم) بین نقاط دوسر یک لینک را بعهده دارد.



در شکل روبرو انتقال بسته ها بین دو نقطه انتهایی ارتباط یعنی A وF مدنظر می باشد.بسته تولید شده در لایه شبکه A می بایست به لایه شبکه ایستگاه B برسد و بالعکس.لایه شبکه این نقاط اهمیتی به نحوه انتقال بسته درون فریم در ایستگاههای میانی نمی دهند.

مدل مرجع OSI

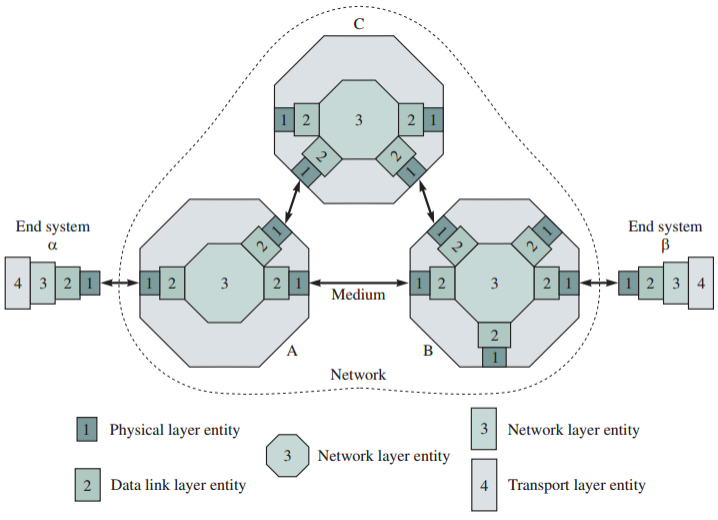
لایه شبکه (Network Layer)



درواقع نقاط انتهایی در ایستگاههای انتهایی به دنبال ایجاد یک ارتباط منطقی نقطه به نقطه بین لایه های شبکه مبدا و مقصد هستند.در هر یک از ایستگاههای بین راه بعد از دریافت هر فریم از لایه فیزیکی و پیوند داده ، اطلاعات درون فریم ،که Packet لایه شبکه می باشد استخراج شده و با بدست آوردن آدرس مقصد در سرآیند بسته ، مسیری که باید بسته هدایت شود تعیین شده و دوباره بسته درون فریم دیگر(متناسب با پروتکل پیوند لایه مورد نظر) کپسوله شده و به سمت لایه پیوند داده ایستگاه مسیر یابی شده هدایت می گردد.

M.Zangian

مدل مرجع OSI



ارتباط بین لایه ها وچگونگی هدایت بسته بین لایه های ۱و۲و۳

M.Zangian

مدل مرجع OSI

لایه شبکه (Network Layer)

ویژگی ها و مسئولیت های لایه شبکه:

- ایجاد یک اتصال منطقی انتها به انتها.

لایه شبکه در ایستگاههای ابتدا و انتها به کمک لایه شبکه ایستگاههای میانی می بایست قادر باشند که امکان هدایت بسته ها از مبدا به مقصد را فراهم آورد .

- پنهان کردن جزئیات لایه های فیزیکی و پیوند داده از لایه های بالاتر

تغییر پروتکل های لایه پیوند داده و لایه فیزیکی نباید تاثیری برروی عملیات و سرویسهای ارائه شده به لایه حمل گردد.

- آدرس دهی

سیستم آدرس دهی در لایه پیوند داده برای آدرس دهی محلی استفاده می شودو اگر بسته از محدوده یک شبکه خارج شود نیاز به سیستم آدرس دهی دیگری خواهیم بود تا موقعیت و هدایت بسته ها را بین مبدا و مقصد امکان پذیر سازد.

مدل مرجع OSI

لایه شبکه (Network Layer)

ویژگی ها و مسئولیت های لایه شبکه:

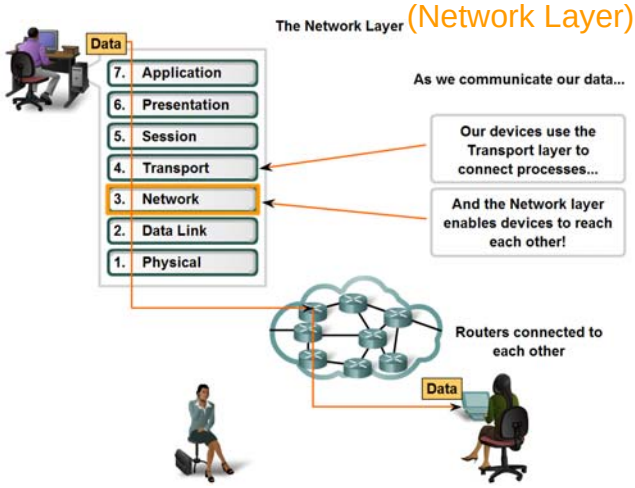
- مسیر یابی

معمولا بین مبدا و مقصد شبکه های متعددی وجود دارد که این شبکه ها با ارتباطات و لینکهای متعددی به هم متصل شده اند و این شبکه ها ، در کنار هم شبکه های بزرگتری را سازمان می دهند برای هدایت بسته ها به اتصال دهنده های بین شبکه ای نیاز است(مانند روترها) که هدایت بسته ها را بین شبکه های مستقل فراهم آورد .یکی از کارکردهای لایه شبکه ایجاد مکانیزمی برای هدایت بسته ها از مبدا به مقصد بین ایستگاههای واسط است.

تقسیم شبکه ای یکپارچه و بزرگ به شبکه های کوچکتر و برقراری ارتباط بین این شبکه های کوچکتر کارایی را در شبکه یکپارچه (اینترنت) افزایش می دهد.

مدل مرجع OSI

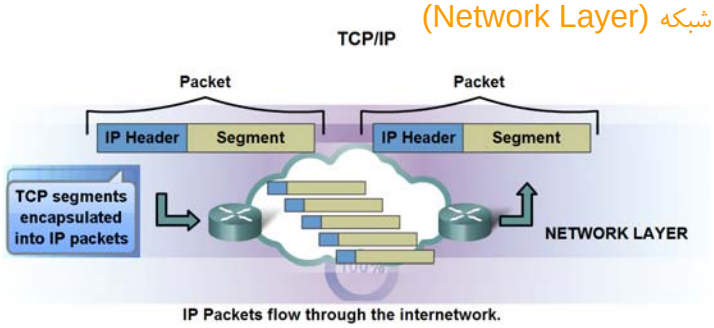
لایه شبکه (Network Layer)



وظیفه اساسی لایه شبکه هدایت بسته ها بین ایستگاههای میانی و رساندن آن به ایستگاههای انتهایی است.

مدل مرجع OSI

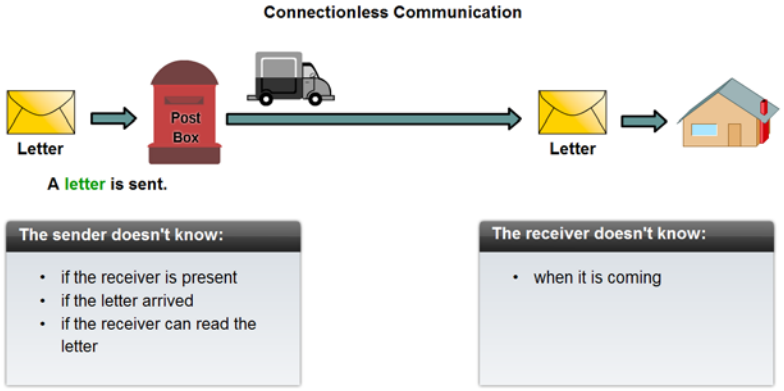
لایه شبکه (Network Layer)



- Connectionless - No connection is established before sending data packets.
- Best Effort (unreliable) - No overhead is used to guarantee packet delivery.
- Media Independent - Operates independently of the medium carrying the data.

مدل مرجع OSI

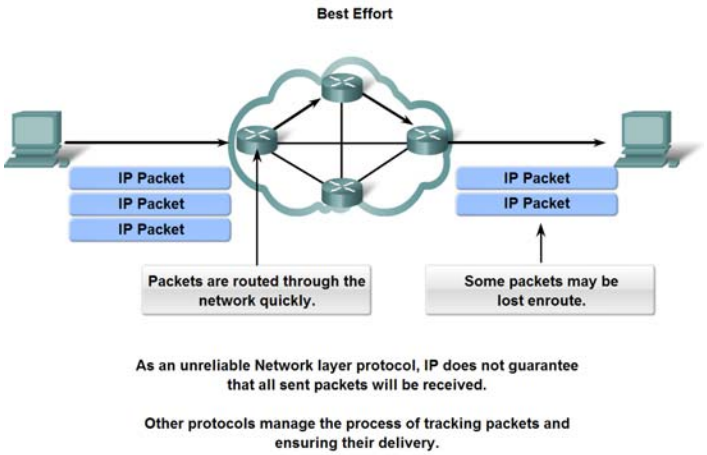
لایه شبکه (Network Layer)



تشابه عملکرد لایه شبکه و سیستم انتقال پستی

مدل مرجع OSI

لایه شبکه (Network Layer)

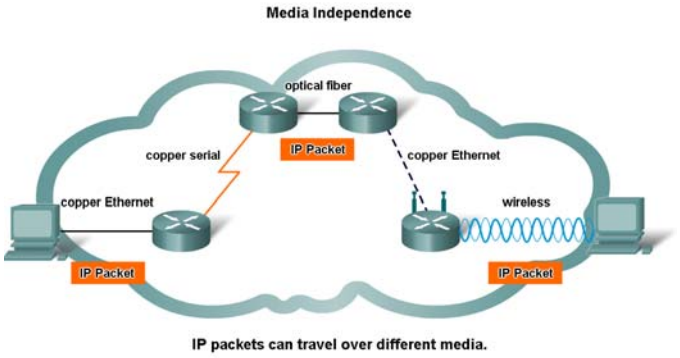


پروتکل های لایه شبکه درمورد رسیدن همه بسته های ارسالی تضمینی ندارندو اصولا این وظیفه به عهده لایه حمل گذاشته شده است.

مدل مرجع OSI

105

لایه شبکه (Network Layer)



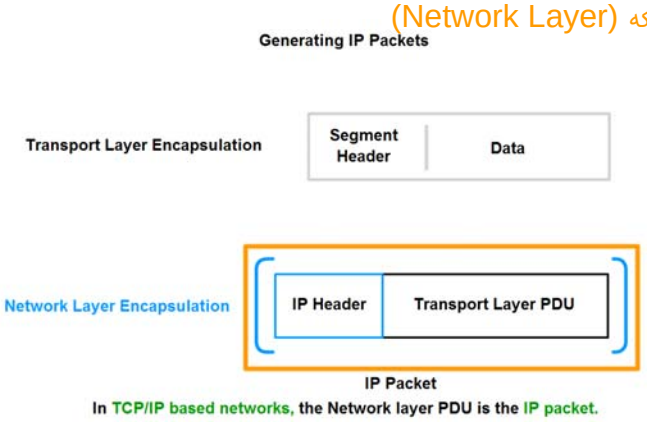
مستقل بودن لایه شبکه و عدم وابستگی به شرایط و پروتکل های لایه فیزیکی

M.Zangian

مدل مرجع OSI

106

لایه شبکه (Network Layer)



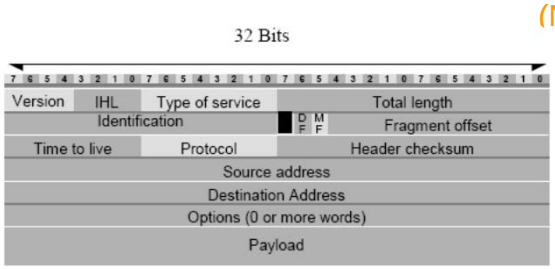
کپسوله کردن سگمنت لایه حمل درون IP Packet در لایه شبکه

M.Zangian

مدل مرجع OSI

لایه شبکه (Network Layer)

بررسی سرآیند بسته IP



Version: این فیلد نسخه پروتکل IP را که این بسته بر اساس آن ایجاد شده است را نشان می دهد این فیلد ۴ بیت است و برای بسته های IP V4 عدد 2(100) در آن قرار می گیرد از دیگر نسخه های بسته IP ، IP V6 یا IPng است.

IHL: این فیلد ۴ بیتی بوده و طول کل سرآیند (Header)را برحسب word(۳۲ بیت) نشان می دهد.

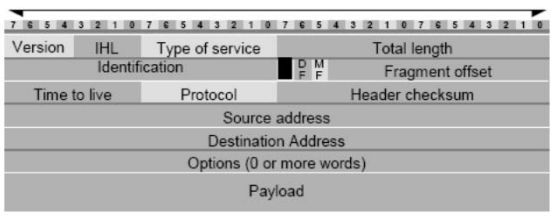
حداقل طول سرآیند ۲۰ بایت یا ۵ word است بنابراین حداقل مقداری که در این فیلد قرار می گیرد ، 2(0101) می باشد. طول قسمت اختیاری (Option) ۱۰ کلمه یا ۴۰ بایت می باشد.بنابراین طول سرآیند حداقل ۲۰ بایت و حداکثر ۶۰ بایت خواهد بود.

M.Zangian

مدل مرجع OSI

لایه شبکه (Network Layer)

بررسی سرآیند بسته IP



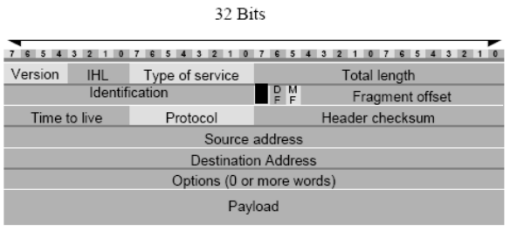
Type Of Service:

یک فیلد ۸ بیتی است . توسط این فیلد فرستنده از مسیریابهای مسیر تقاضای سرویسهای ویژه برای ارسال دیتاگرام می نماید.بعنوان مثال تعیین اولویت برای داده هایی که باید سریع ارسال شوند مانند صوت و تصویر و یا تعیین قابلیت اطمینان برای برخی از داده ها این فیلد خود به بخشهای دیگری تقسیم می شوند . سه بیت سمت چپ(MSB) اولویت بسته ها را تعیین می نماید .عدد ۰ کمترین اولویت و ۷ بیشترین اولویت را مشخص می نماید.مسیریابها بادریافت بسته ای با اولویت بالاتر آنرا در اولویت مسیریابی قرار می دهند.

P2	P1	P0	D	T	R	–	–
تقدّم بسته			تأخیر	توان خروجی	قابلیّت اطمینان	بلا استفاده	

M.Zangian

مدل مرجع OSI



لایه شبکه (Network Layer)

بررسی سرآیند بسته IP

بیت D(Delay) : فرستنده با یک کردن بیت D از مسیر یابهای مسیر می خواهد حتی الامکان از مسیرهای دارای تاخیرهای بالا (مثل ارتباطات ماهواره ای) استفاده ننماید.

بیت T (Throughput):

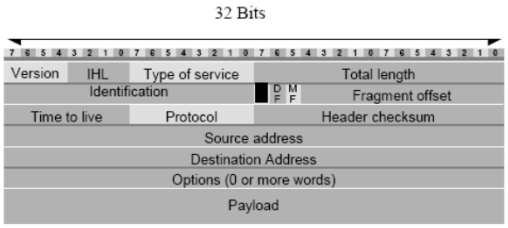
با یک کردن بیت T فرستنده از مسیر یاب های مسیر می خواهد که بسته را از مسیرهایی با توان عملیاتی ارسال بالا هدایت نماید.(ارتباطات ماهواره ای دارای توان عملیاتی ارسال و تاخیر بالاست.)

بیت R (Reliability):

فرستنده با یک کردن این بیت از مسیر یابها می خواهد که قابلیت اطمینان را مورد توجه قرار داده و در صورت امکان از مسیرهای دارای خطای پایین تر استفاده نماید.

M.Zangian

مدل مرجع OSI



لایه شبکه (Network Layer)

بررسی سرآیند بسته IP

اغلب مسیریابهای تجاری از فیلد Type Of Service صرفنظر می کنند.

Total Length:

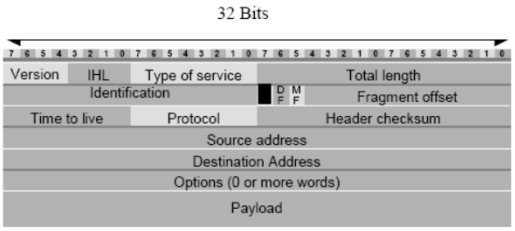
در این فیلد یک عدد ۱۶ بیتی قرار می گیرد که طول کل بسته IP را که شامل طول سرآیند به همراه داده می شود را بر حسب بایت تعیین می کند.بنابراین در پیش بینی انجام شده در سرآیند حداکثر طول بسته IP، ۶۵۵۳۵ بایت می باشد.

Identification:

برخی مواقع مسیریابها یا ماشینهای میزبان مجبورند که یک دیتاگرام را به قطعات کوچکتری بشکنندو ماشین مقصد مجبور است آنها را بازسازی کند.بنابراین وقتی یک دیتاگرام واحد شکسته می شودباید مشخصه ای داشته باشد تا در مقصدبتوان قطعه های دیتاگرام را از بقیه جدا کرد.در این بیت ۱۶ بیتی عددی قرار می گیردکه شماره یک دیتاگرام واحد را مشخص می نماید.کلیه بسته های IP که با این شماره وارد می شوند ، قطعه های مربوط به یک دیتاگرام بوده وباید با گردآوری قطعات مجددا آنرا بازسازی نمود.البته شماره ترتیب قطعات باید مشخص گرددکه در ادامه به آن می پردازیم.

M.Zangian

مدل مرجع OSI



لایه شبکه (Network Layer)

بررسی سرآیند بسته IP

Fragment Offset :

شامل ۳ بخش است ،بیت DF ،بیت MF ، Fragment Offset، بیت اول مورد استفاده قرار نمی گیرد.(بیت تیره شده)

(Don't Fargment):DF

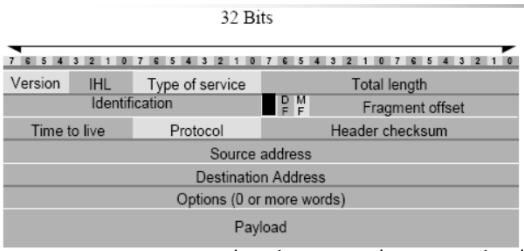
با یک شدن این بیت در سرآیند یک بسته IP ،هیچ مسیریابی نباید آنرا قطعه قطعه نماید.چرا که مقصد امکان بازسازی قطعات را ندارد.در صورتیکه این بیت یک باشدو مسیریابی نتواند آنرا بدلیل بزرگی اندازه آن انتقال دهد ناگزیر آنرا حذف می نماید.

(More Fargment):MF

این بیت مشخص می کند که آیا یک بسته IP ،آخرین قطعه از یک دیتاگرام است یا قطعه دیگری نیز وجوددارد.در آخرین قطعه این بیت صفر ولی در قطعات میانی این بیت الزاما یک است.

M.Zangian

مدل مرجع OSI



لایه شبکه (Network Layer)

بررسی سرآیند بسته IP

:Fragment Offset

این قسمت که سیزده بیتی است،

درحقیقت شماره ترتیب هر قطعه در دیتاگرام شکسته شده را مشخص میکند.باتوجه به ۱۳ بیتی بودن این فیلد یک دیتاگرام حداکثر می تواند به ۸۱۹۲ قسمت تقسیم شود.نکته بسیار مهم در مورد این فیلد این ست که اندازه هر قطعه به استثناء قطعه آخر باید ضریبی از ۸ باشد.عددی که در این فیلد قرار می گیردضربدر ۸ آدرس محل قرار گرفتن قطعه در دیتاگرام را مشخص می نماید.

مثال : فرض کنید مسیریاب بخواهد دیتاگرامی به اندازه ۵۰۰۰ بایت راقطعه قطعه کند بطوریکه هر قطعه کوچکتر از ۱۵۰۰ بایت گردد. اندازه ۱۲۵۰ بایت برای هر قطعه مناسب نمی باشد ولی اندازه ۱۲۸۰ بایت مناسب است .بنابراین دیتاگرام به ۴ قطعه شامل ۳ قطعه ۱۲۸۰ بایتی و یک قطعه ۱۱۶۰ بایتی تقسیم می شود .در این مثال فرض کنید مسیریاب شماره ۲۳۲۲ را بعنوان مشخصه دیتاگرام ،انتخاب کرده است. بنابراین فیلدهای آفست و مشخصه قطعات به صورت زیر خواهد بود.

M.Zangian

مدل مرجع OSI

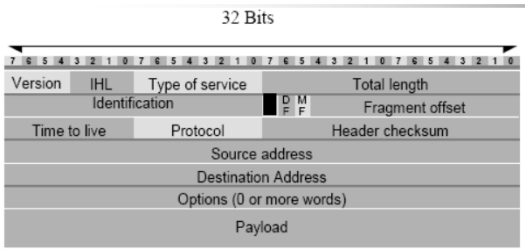
لایه شبکه (Network Layer)

بررسی سرآیند بسته IP

شمارهٔ قطعه	Identification	Fragment Offset	بیت MF	آدرس محّل قرار گرفتن قطعه در دیتاگرام	طول هر قطعه
قطعهٔ شماره ۱	2322	0	1	8*0=0	۱۲۸۰
قطعهٔ شماره ۲	2322	160	1	8*160=1280	۱۲۸۰
قطعهٔ شماره ۳	2322	320	1	8*320=2560	۱۲۸۰
آخرین قطعه	2322	480	0	8*480=3840	۱۱۶۰

عمل شکسته شدن یک بسته IP ممکن است در طول مسیر در هر جای شبکه اتفاق بیافتند ولی وظیفه بازسازی آن بعهده ماشین مقصد است.

مدل مرجع OSI



لایه شبکه (Network Layer)

بررسی سرآیند بسته IP

فیلد Time To Live(TTL):

این فیلد ۸ بیتی در واقع یک شمارنده است که طول عمر بسته را مشخص می کند،

طول عمر بسته به طور ضمنی به زمانی اشاره می کند که یک بسته IP در شبکه می تواند سرگردان بماند.حداکثر طول عمر یک بسته IP می تواند ۲۵۵ باشد. باعبور بسته از هر مسیریاب مسیر یک واحد از این فیلد کاسته می شود، علاوه بر این اگر یک بسته IP به دلیل بافر شدن در حافظه مسیر یاب زمانی را منتظر بماند به ازای هر ثانیه یک واحد از این فیلد کم می شود. به محض اینکه مقدار این فیلد صفر گردد بسته در هر جای شبکه باشد توسط مسیریاب دریافت کننده بسته حذف خواهد شدو از ادامه مسیر بازخواهد ماند.البته یک پیغام هشدار به ماشینی که بسته را تولید کرده بازپس فرستاده می شود.

این فیلد نقش حیاتی در پاکسازی شبکه از بسته های IP سرگردان که در مسیرهای بسته در حال چرخش هستند بازی می کند.بسته گاها بدلیل جداول مسیریابی نادرست ،ممکن است درون حلقه های بینهایت بیافتد.در صورت عدم وجود چنین فیلدی ممکن است شبکه با انبوهی از بسته های سرگردان مواجه خواهد شد.

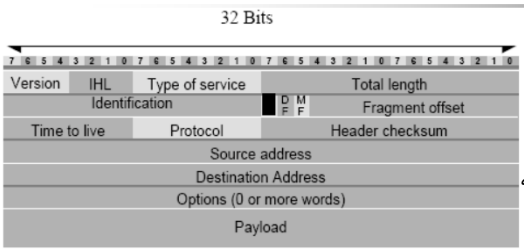
مدل مرجع OSI

لایه شبکه (Network Layer)

بررسی سرآیند بسته IP

فیلد Protocol:

دیتاگرامی که در یک فیلد داده از یک بسته IP حمل می شود،با ساختمان داده خاصی



مبتنی بر یک پروتکل استاندارد از لایه شبکه و یا لایه های بالاتر است که تحویل لایه IP می گردد.بسته ها پس از دریافت در مقصد باید تحویل پروسه متناظر با پروتکل تعیین شده گردد.در جدول زیر برخی از پروتکلهای تولید کننده و دریافت کننده دیتاگرام ارائه شده است.

0	Reserved		[JBP]
1	ICMP	Internet Control Message	[RFC792,JBP]
2	IGMP	Internet Group Management	[RFC1112,JBP]
3	GGP	Gateway-to-Gateway	[RFC823,MB]
4	IP	IP in IP (encasulation)	[JBP]
5	ST	Stream	[RFC1190,IEN119,JWF]
6	TCP	Transmission Control	[RFC793,JBP]
7	UCL	UCL	[PK]
8	EGP	Exterior Gateway Protocol	[RFC888,DLM1]
9	IGP	any private interior gateway	[JBP]
10	BBN-RCC-MON	BBN RCC Monitoring	[SGC]
11	NVP-II	Network Voice Protocol	[RFC741,SC3]
12	PUP	PUP	[PUP,XEROX]
13	ARGUS	ARGUS	[RWS4]
14	EMCON	EMCON	[BN7]
15	XNET	Cross Net Debugger	[IEN158,JFH2]
16	CHAOS	Chaos	[NC3]
17	UDP	User Datagram	[RFC768,JBP]

M.Zangian

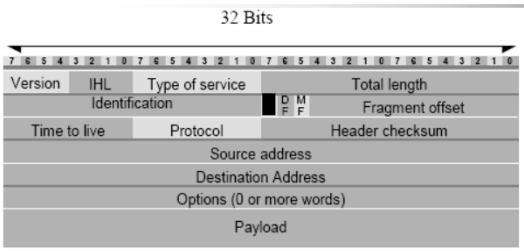
مدل مرجع OSI

لایه شبکه (Network Layer)

بررسی سرآیند بسته IP

فیلد (Header Checksum):

این بیت که ۱۶ بیتی است به منظور کشف خطای احتمالی ***در سرآیند*** هر بسته IP



مورد استفاده قرار می گیرد.برای محاسبه کد کشف خطا کل سرآیند بصورت ۱۶ بیتی (دوبایت دوبایت) با یکدیگر جمع می شوند.نهایتا حاصل جمع بصورت مکمل یک منفی می شود.و عدد حاصل شده در این فیلد قرار می گیرد.

در هر مسیریاب قبل از پردازش و مسیر یابی ابتدا صحت اطلاعات درون سرآیند بررسی می شود (بدین صورت که دوبایت دوبایت در مبنای مکمل یک بیتهای سرآیند با هم جمع می شوند .حاصل باید عدد صفر باشد در غیر اینصورت بسته حذف می گردد.)

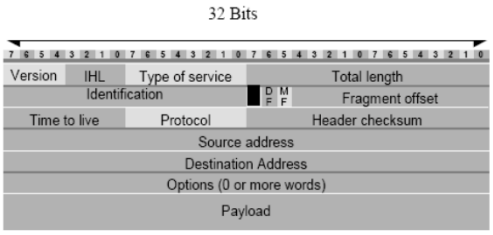
نکته: فیلدChecksum در هر مسیر یاب می بایست بصورت مجدد محاسبه و مقداردهی گرددزیرا وقتی بسته ای وارد یک مسیر یاب می شود حداقل فیلد TTL از آن تغییر می کند.فیلد Checksum برای کشف خطا در Payload استفاده نمی شود ،چراکه اینگونه خطاها در لایه های پایینتر (لایه Data link یا لایه ای فیزیکی) توسط کدهای CRC و یا لایه های بالاتر بررسی میگردد

M.Zangian

مدل مرجع OSI

لایه شبکه (Network Layer)

بررسی سرآیند بسته IP



فیلد(Source Address):

هر ماشین میزبان در شبکه اینترنت بایددارای یک آدرس ۳۲ بیتی یکتا باشد(IP V4) که می بایست در هنگام تولید یک بسته IP آدرس خود را (آدرس مبدا) در این فیلد قرار دهد.

فیلد (Destination Address):

در این فیلد آدرس ۳۲ بیتی مربوط به ماشین مقصد، که باید بسته به آن تحویل شود ، قرار می گیرد.

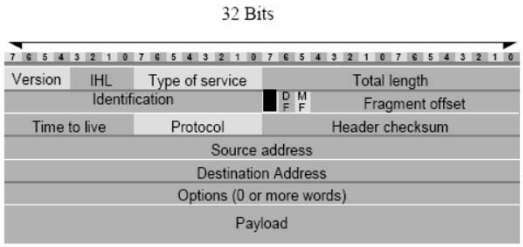
نکته : در طول مسیر از مبدا تا مقصد فیلدهای مربوط به آدرس مبدا و مقصد ثابت وبدون تغییر میماند.

M.Zangian

مدل مرجع OSI

لایه شبکه (Network Layer)

بررسی سرآیند بسته IP



فیلد(Options):

در این فیلد اختیاری که حداکثر تا ۴۰ بایت می تواند اندازه آن باشدو محتوی اطلاعاتی است که می تواند مسیریابها را در یافتن مسیر مناسب کمک کند.در صورتیکه اندازه این فیلد مضرب صحیحی از ۳۲ بیت نباشدتا رسیدن به این مضرب اطلاعات اضافی دربیتها قرار داده میشود (Padding)

فیلد Payload :

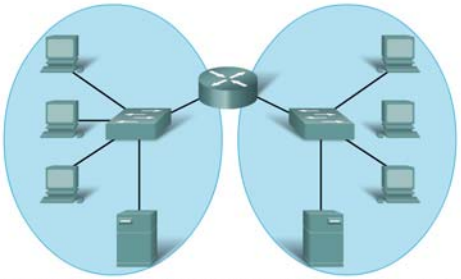
در این فیلد داده های دریافتی از لایه بالاتر قرار می گیرد.

M.Zangian

مدل مرجع OSI

:Broadcast Domain

حوزه همه پخشی یک تقسیم منطقی از شبکه است که تمام Node ها و ایستگاههای این حوزه ،می تواند در دسترس ایستگاههای دیگر با استفاده از ارسالهای همه پخشی در لایه پیوند داده باشند.در واقع یک بسته همه پخشی (در لایه ۲) می تواند به همه ایستگاههای این حوزه تحویل شود.افزایش حوزه همه پخشی می تواند اثر منفی در کارایی شبکه و ایجاد ازدحام داشته باشد بنابراین با شکستن حوزه همه پخشی بزرگ به چند حوزه همه پخشی کوچکتر کارایی افزایش خواهد یافت.



Replacing the middle switch with a router creates 2 IP subnets, hence, 2 distinct broadcast domains. All devices are connected but local broadcasts are contained.

ایجاد دو حوزه همه پخشی وشکستن حوزه های همه پخشی با استفاده از روتر.روترها تحت عنوان Broadcast Killer اجازه عبور بسته های همه پخشی را از یک زیر شبکه به زیر شبکه دیگر نمی دهد.

مدل مرجع OSI

:Default Gateway

بطور کلی ارسال بسته ها به دو شکل می تواند مورد نظر باشد:

۱- ارسالهایی که ایستگاههای مبدا و مقصد در یک subnet (زیر شبکه) هستند.

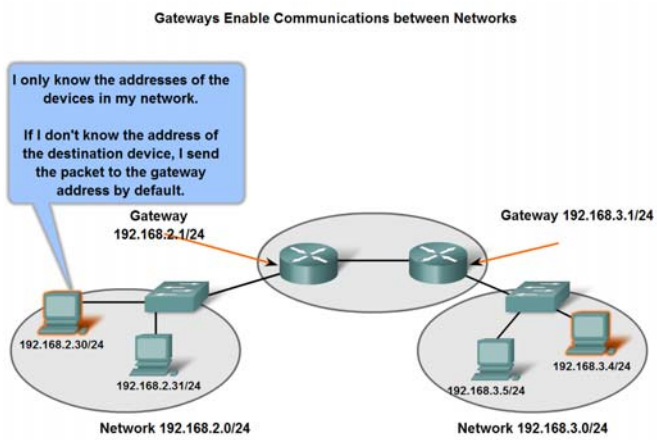
۲- ارسالهایی که ایستگاههای مبدا و مقصد در یک زیر شبکه قرار ندارند.

در مورد اول که ایستگاههای مبدا و مقصد در یک زیر شبکه هستند ارسال می تواند از طریق پروتکلهای لایه پیوند داده و لایه فیزیکی بصورت مستقیم و بدون واسطه صورت گیرد .

در صورتیکه ایستگاههای مبدا و مقصد در یک subnet نباشندایستگاه مبدا نمی تواند بسته را بصورت مستقیم به مقصد ارسال کند چراکه مقصد در زیر شبکه مبدا نیست بنابراین نیاز به ایستگاههای واسطی داریم که بتواند در زیر شبکه های مختلف قرار گرفته و آنها را به یکدیگر مرتبط نماید.چنین ایستگاه واسطی تحت عنوان دروازه پیش فرض یا Default Gateway شناخته می شود.بنابراین ایستگاه مبدا بدون هیچ نگرانی در صورتیکه با مقصد در یک زیر شبکه واقع نباشند بسته را تحویل Default Gateway می دهد بنابراین وظیفه ارسال بسته به مقصد به عهده Default Gateway خواهد بود.

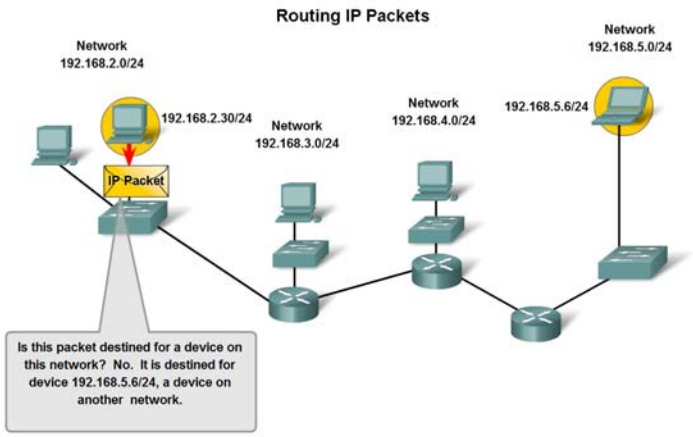
دروازه پیش فرض دارای اینترفیسهای مختلفی است که هر کدام از این اینترفیسها می تواند در زیر شبکه های مختلف قرار گیرد.

مدل مرجع OSI



Gateway ها امکان ارتباط شبکه های مختلف را با یکدیگر فراهم می آورد.

مدل مرجع OSI



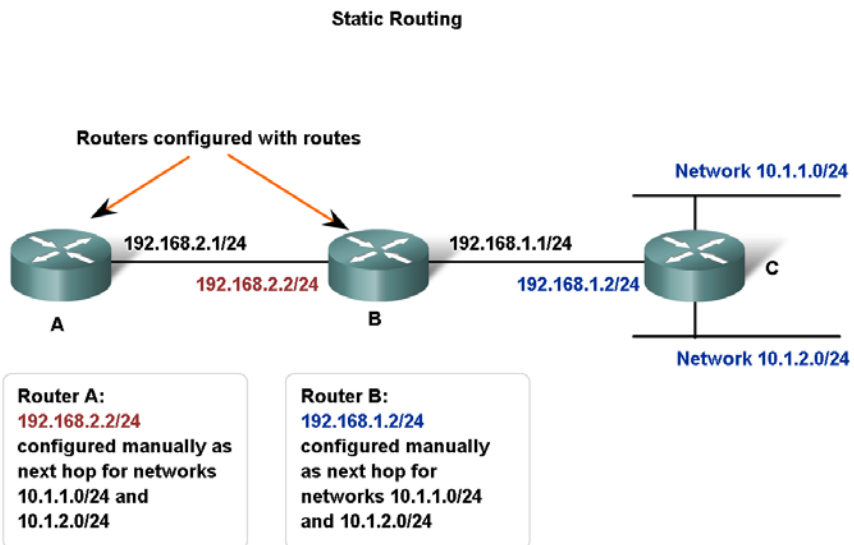
مسیریابی بسته های IP

مدل مرجع OSI

جداول مسیر یابی (Routing Tables):

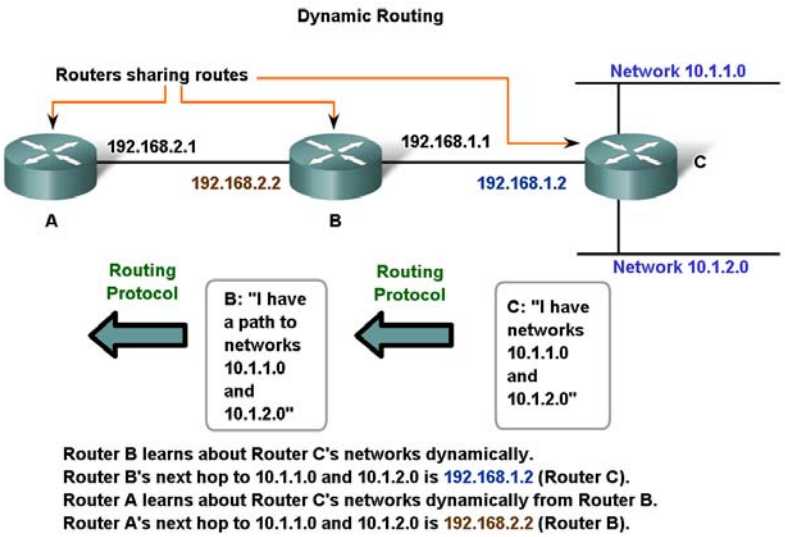
هر مسیر یاب برای اینکه بداند بسته ای که متعلق به یک زیر شبکه است را از کدام یک از مسیرها(اینترفیسهای خود) انتقال دهد نیاز مند اطلاعاتی برای مسیر یابی بسته است.این اطلاعات در جداولی تحت عنوان جداول مسیریابی در تمام مسیریابهای شبکه قرار دارد. این جداول یا بصورت استاتیک توسط مدیر شبکه تعریف می شوندویا با استفاده از پروتکلهای مسیریابی دینامیک ایجاد می شوند.

مدل مرجع OSI



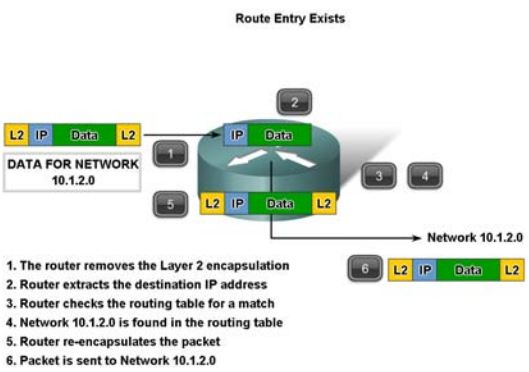
مسیر یابی استاتیک

مدل مرجع OSI



مسیر یابی پویا(دینامیک)

مدل مرجع OSI



مسیر یابی

باارسال بسته بسمت یک مسیریاب ،بسته بصورت زنجیره ای از بیتها از یکی از اینترفیس ها وارد روتر میشود.این بسته ها همان فریمهای لایه ۲ شبکه هستند که بسته به پروتکل لایه ۲ ، براساس یک الگوی خاص شکل یافته است.روتر ابتدا بسته لایه ۲ را دریافت میکند،سپس کپسول لایه ۲ را حذف نموده و داده محتوی آن که یک بسته IP لایه ۳ است را از درون آن استخراج می نماید.

سپس آدرس مقصد واقع در سرآیند بسته IP ، را استخراج می نماید.سپس روتر جدول مسیر یابی خود را چک می کند تاآدرس شبکه مقصد را در آن بیابد .با یافتن آدرس شبکه مورد نظر ، روتردر می یابد بسته را به کدام یک از اینترفیسهای خود هدایت کند، بنابراین بسته را متناسب با پروتکل لایه دو تعریف شده برای اینترفیس مورد نظر کپسوله سازی کرده و آنرا به طرف مقصد هدایت می کند.

مدل مرجع OSI

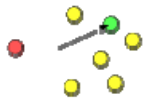
نکته

در صورتیکه مبدا و مقصد (متعلق به یک Broadcast Domain)
در یک زیر شبکه باشند نیازی به Default Gateway نیست
و ارتباط بصورت مستقیم و در لایه ۲ (ویا لایه فیزیکی TCP/IP)
می تواند برقرار شود که در ادامه بخش بررسی می گردد.

برای بررسی نحوه رسیدن بسته ها به مقصد ،لازم است برخی تعاریف و اصطلاحات در اینجا مطرح گردد که برخی از این مباحث در لایه Data Link مورد بحث است ولی برای پیوستگی مبحث در اینجا طرح می گردد.

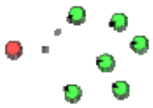
مدل مرجع OSI

انواع ارسال بسته ها در شبکه:



Unicast:

در این نوع ارسال ، بسته ها از یک میزبان در مبدا تنها به یک میزبان مقصد ارسال می شوند. (Host To Host)



Broadcast:

در این نوع ارسال بسته ها از یک میزبان به تمام ایستگاههایی که متعلق به یک Broadcast Domain باشند ارسال خواهد شدو تمامی ایستگاههای این محدوده، بسته ها را دریافت خواهند کرد.

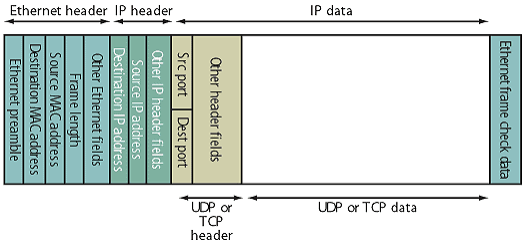
Multicast:

در این روش ارسال یک بسته از یک میزبان به مجموعه ای انتخاب شده از میزبانهای دیگر ارسال می گردد. در این روش ایستگاهها با عضویت در گروههای مختلف با ارسال بسته به یک گروه ،تمامی اعضاء گروه بسته را دریافت خواهند کرد. مباحث مربوط به ارسال Multicast بسیار گسترده است که مورد نظر این درس نمی باشد. ازمهمترین پروتکلهای مطرح در Multicast پروتکل IGMP می باشد.

مدل مرجع OSI

هدایت بسته ها در لایه ۲ ، OSI:

یکی از پروتکلهای مهم و مطرح در لایه Data Link از مدل مرجع OSI و یا لایه Network Access مدل مرجع TCP/IP پروتکل اترنت است ، همانطوریکه گفتیم داده های هر لایه در لایه زیرین خود درون سرآیند (Header) و یا پی آیند (Trailer) کپسوله می شوند و به لایه بعدی منتقل می گردند. فریم اترنت نیز بسته های IP که از لایه IP ، به لایه پیوند داده منتقل می شود را درون Header و Trailer ، کپسوله می کند و فریم اترنت را ایجاد می کند.در شکل زیر قالب فریم اترنت قابل مشاهده است.

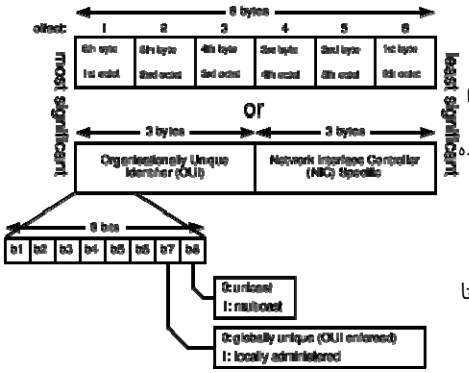


همانطوریکه در فریم اترنت مشاهده می گردد ازدو آدرس جدید در Header استفاده شده است. Destination MAC Address,Source MAC Address

مدل مرجع OSI

آدرس فیزیکی (Physical Address/MAC Address):

اینترفیسهای تجهیزات شبکه در لایه ۲ که بخواهند برای ارتباط از پروتکل Ethernet(و برخی از پروتکل های دیگر) استفاده نمایند، می بایست از یک آدرس منحصر بفرد استفاده کنند تابتواند فریمهای اترنت را دریافت کرده و از طریق این آدرس ، در لایه ۲ با تجهیزات دیگرارتباط برقرارکنند.این آدرس منحصر بفرد آدرس فیزیکی یا MAC Address نامیده می شود.در شکل زیر فرمت آدرس فیزیکی نشان داده شده است.



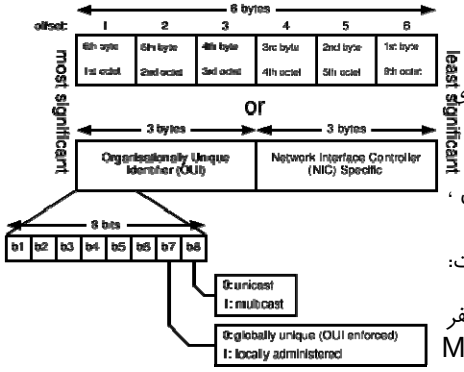
MAC Address یک آدرس ۶ بایتی است (۴۸ بیت)که بصورت ۲ قسمت ۳ بایتی تقسیم بندی می شود. 3 اکتت ،اول (OUI) یک عدد منحصر بفرد است که به هر شرکت تولید کننده تجهیزات (مثل کارت شبکه) اختصاص داده شده است و آن شرکت برای تجهیزات خود از این شناسه استفاده می نماید.

۳ اکتت بعدی در اختیار شرکت سازنده است تا به هر ترتیب مورد نظر آدرس های منحصر بفرد را برای هر اینترفیس آدرس گذاری شده خود انتخاب نماید.

MAC:Media Access Control

مدل مرجع OSI

آدرس فیزیکی (Physical Address/MAC Address):



آدرس فیزیکی برای هر اینترفیس یک آدرس منحصر بفرد است که بصورت ماندگار در حافظه فقط خواندنی آن توسط شرکت سازنده برنامه ریزی و یا اصطلاحا سوزانده می شود.

در فرمت استاندارد شده برای آدرس فیزیکی ، دو بیت LSB از اکتت اول آدرس معانی خاصی دارد که بصورت زیر تعریف شده است:

B8: این بیت برای ارسالهای Unicast ، صفر و برای ارسالهای Broadcast و Multicast یک می باشد.

B7: صفربودن این بیت به معنی اعتبار جهانی آدرس فیزیکی است به عبارت دیگر در صورتیکه این بیت یک باشد به این معنی است که آدرس فیزیکی یک آدرس رجیستر شده است. در صورتیکه این بیت ۱ باشد به این معنی است که آدرس اعتبار محلی دارد و توسط مدیر شبکه و برای مقاصد آزمایشی قرار داده شده است ویک آدرس رجیستر شده نیست.

M.Zangian

مدل مرجع OSI

آدرس فیزیکی معمولا بصورت ۶ اکتت در مبنای ۱۶ که با – و یا : از یکدیگر جدا می شوند نوشته می شود. مثال : 00-14-0B-32-FF-BE

سئوال:

همانطوریکه در مورد آدرس فیزیکی گفته شد،در پروتکل اترنت برای ارسال یک بسته در این لایه احتیاج به آدرس فیزیکی مقصد است، اما در مورد ارسال همه پخشی که یک میزبان خاص مد نظر نیست آدرس فیزیکی مقصد چگونه انتخاب می شود؟

قرارداد:

برای ارسال های همه پخشی آدرس فیزیکی FF-FF-FF-FF-FF-FF در نظر گرفته شده است بعبارت دیگر وقتی تمام بیتهای آدرس فیزیکی برابر ۱ باشد بمعنی یک ارسال همه پخشی است.

M.Zangian

مدل مرجع OSI

تحقیق

آدرس فیزیکی برای ارسالهای Multicast چگونه تعیین می شود؟

مدل مرجع OSI

با مطرح شدن فریم اترنت و بحث آدرس فیزیکی ممکن است ابهاماتی در مورد اینکه نقش آدرس IP در مورد ارتباط ایستگاهها در این میان چگونه تعریف می شود ، بوجود آید. برخی از سئوالاتی که ممکن است در این زمینه مطرح شود را می توان به صورت زیر خلاصه نمود:

- نقش آدرس IP وآدرس فیزیکی چگونه تعریف می شود؟
- ما در ارتباط بین میزبانها در شبکه آدرس IP مبدا و مقصد را داریم، واطلاعاتی در مورد آدرس فیزیکی مقصد نداریم.این اطلاعات چگونه بدست می آید؟
- در این میان نقش Default Gateway چگونه تعریف می شود؟

قبل از پاسخگویی به این سئوالات ، ابتدا ارسال از مبدا به مقصد را به دو شکل مطرح می کنیم:

۱- مبدا و مقصد در یک زیر شبکه (Subnet)باشند.

۲- مبدا و مقصد در زیر شبکه های متفاوتی واقع باشند.

مدل مرجع OSI

بحث مربوط به زیر شبکه ها و الگوهای شبکه ، را در آینده در یک فصل مستقل بررسی خواهیم کرد اما برای ادامه ، ابتدا به سئوال زیر پاسخ می دهیم:

سئوال :

چگونه یک ایستگاه می تواند تشخیص دهد که مقصد در زیر شبکه خودش قرار دارد یا خیر به عبارت دیگر چگونه تشخیص دهیم مبدا و مقصد در یک زیر شبکه واقع شده اند؟

پاسخ: تشخیص اینکه مبدا و مقصد در یک Subnet واقع شده اند یا خیر به راحتی و توسط عملگر AND قابل تشخیص است .برای این منظور از رابطه زیر استفاده می نماییم:

اگر

(Source IP Address) AND (Source Subnet Mask)

=

(Destination IP Address)AND(Source Subnet Mask)

باشد ،در اینصورت مبدا و مقصد در یک Subnet واقع شده اند.در غیر اینصورت در یک Subnet نیستند.

مدل مرجع OSI

نکته

در ارتباط شبکه ای ارتباط یکطرفه معنی ندارد بنابراین شرایط ارتباط باید چه از مبدا به مقصد و چه از مقصد به مبدا مورد بررسی قرار گیرد. بنابراین برای بررسی اینکه مبدا و مقصد در یک subnet هستند یکبار این بررسی باید از دید مبدا و یکبار از دید مقصد مورد بررسی قرار گیرد.

تا اینجا تشخیص دادیم که مبدا و مقصد در یک Subnet هستند یا خیر .با تشخیص این مورد ارسال بسته از مبدا به مقصد به دو شکل صورت می گیرد. در شکل اول زمانیست که مبدا و مقصد در یک Subnet باشند .در اینصورت مبدا با یافتن آدرس فیزیکی مقصد بسته را در یک فریم اترنت کپسوله کرده و به سمت مقصد می فرستد. بارسیدن چنین فریمی به هر ایستگاه، ایستگاه مورد نظر آدرس فیزیکی مقصد واقع در سرآیند فریم را بررسی می کند و در صورتیکه این آدرس برابر آدرس فیزیکی خودش بود آنرا دریافت می کند و به لایه های بالاتر خود منتقل می نماید. در غیر اینصورت فریم حذف می گرددو به لایه های بالاتر منتقل نمی گردد.

مدل مرجع OSI

درشکل دوم ، ایستگاه مبدا با بررسی IP مقصد در می یابد که با مقصد در یک Subnet قرار ندارد در اینصورت ،آدرس فیزیکی مقصد در دسترسی نخواهد بود تا در فریم اترنت آنرا قراردهد.

بنابراین در این حالت نیاز به یک دستگاه واسط است که بتواند در هدایت فریم به سمت مقصد کمک نماید .این دستگاه واسط همان Default Gateway است که قبلا نیز به آن اشاره شده بود.

بنابراین :

زمانیکه ایستگاه مبدا و مقصد در یک Subnet نباشند،برای ارسال بسته بین آنها باید از تجهیزاتی به نام Gateway استفاده نمود.در واقع مبدا با سپردن فریم اترنت به Gateway مسئولیت ارسال بسته را از خود آزاد نموده و به Gateway محول می نماید.

پس در شکل دوم که مبدا و مقصد در یک زیر شبکه قرار ندارند ایستگاه مبدا آدرس فیزیکی اینترفیس اترنت Gateway را که در Subnet خودش قرار دارد را بجای آدرس فیزیکی مقصد قرارداده و فریم به سمت Gateway ارسال می شود. در Gateway فریم باز شده و از درون آن Packet ، IP استخراج می شود و مقصد اصلی در لایه ۳ مسیر دهی می شود.

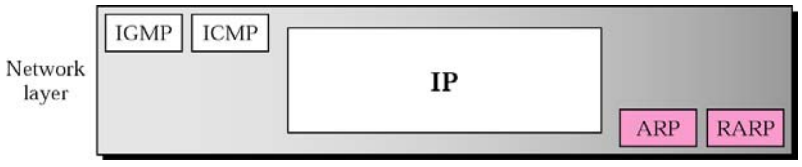
M.Zangian

مدل مرجع OSI

پروتکل ARP (Address Resolution Protocol):

در بحث گذشته دو حالت ارسال را بررسی کردیم و در هر دو نوع کپسوله شدن Packet ، IP را درون فریم اترنت و ارسال به سمت مقصد(درحالت اول)و یا Gateway (در حالت دوم) را خاطر نشان کردیم .حال سئوال اینجاست ایستگاه مبدا از کجا باید آدرس فیزیکی مقصد و یا Gateway را بداند؟ تنها چیزی که ما از ایستگاه مقصد می دانیم IP مقصد است و نه آدرس فیزیکی آن.

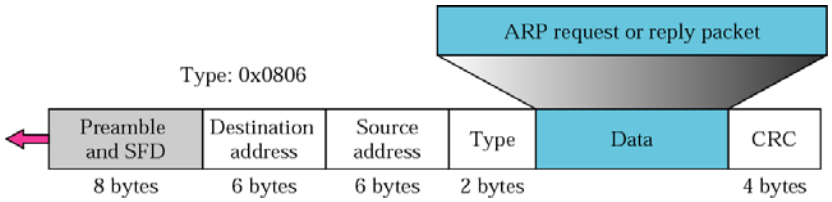
برای پاسخگویی به این نیاز، پروتکلی در لایه ۳ (لایه شبکه از مدل OSI) به نام ARP پیاده سازی گردید در این پروتکل با داشتن آدرس IP مقصد ، آدرس فیزیکی آن جستجو و یافت می شود.



M.Zangian

مدل مرجع OSI

فریم ARP در واقع یک بسته ARP است که درون فریم Ethernet، کپسوله می گردد.



Frame Type برای بسته ARP برابر 0x806 می باشد.

مدل مرجع OSI

EtherType	Protocol
0x0800	Internet Protocol, Version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x0842	Wake-on-LAN Magic Packet, as used by ether-wake and Sleep Proxy Service
0x1337	SYN-3 heartbeat protocol (SYNdog)
0x22F3	IETF TRILL Protocol
0x6003	DECnet Phase IV
0x8035	Reverse Address Resolution Protocol (RARP)
0x809B	AppleTalk (Ethertalk)
0x80F3	AppleTalk Address Resolution Protocol (AARP)
0x8100	VLAN-tagged frame (IEEE 802.1Q) & Shortest Path Bridging IEEE 802.1aq[3]
0x8137	Novell IPX (alt)
0x8138	Novell
0x814C	Simple Network Management Protocol (SNMP)[4]
0x8204	QNX Qnet
0x86DD	Internet Protocol, Version 6 (IPv6)
0x8808	Ethernet flow control
0x8809	Slow Protocols (IEEE 802.3)
0x8819	CobraNet
0x8847	MPLS unicast
0x8848	MPLS multicast
0x8863	PPPoE Discovery Stage
0x8864	PPPoE Session Stage

EtherType	Protocol
0x886F	Microsoft NLB heartbeat [5]
0x8870	Jumbo Frames
0x887B	HomePlug 1.0 MME
0x888E	EAP over LAN (IEEE 802.1X)
0x8892	PROFINET Protocol
0x889A	HyperSCSI (SCSI over Ethernet)
0x88A2	ATA over Ethernet
0x88A4	EtherCAT Protocol
0x88A8	Provider Bridging (IEEE 802.1ad) & Shortest Path Bridging IEEE 802.1aq[6]
0x88AB	Ethernet Powerlink
0x88CC	LLDP
0x88CD	sercos III
0x88D8	Circuit Emulation Services over Ethernet (MEF-8)
0x88E1	HomePlug AV MME
0x88E3	Media Redundancy Protocol (IEC62439-2)
0x88E5	MAC security (IEEE 802.1AE)
0x88F7	Precision Time Protocol (IEEE 1588)
0x8902	IEEE 802.1ag Connectivity Fault Management (CFM) Protocol / ITU-T Recommendation Y.1731 (OAM)
0x8906	Fibre Channel over Ethernet
0x8914	FCoE Initialization Protocol
0x9000	Configuration Test Protocol (Loop)[7]
0x9100	Q-in-Q
0xCAFE	Veritas Low Latency Transport (LLT)[8]

شماره پروتکل (Type)برای برخی از پروتکلها

مدل مرجع OSI

ARP Packet:

HW Type		Prot. Type
HW Addr Len	Prot Addr Len	Operation
Sender's HW Addr (1-4)		
SHA (5-6)		SIP (1-2)
SIP (3-4)		THA (1-2)
Target HW Addr (3-6)		
Target IP Addr		

Hardware Type:

اشاره به نوع رابط سخت افزاری برای اتصال به بستر فیزیکی است. برای اترنت این مقدار برابر ۱ است .اندازه این فیلد ۱۶ بیت (۲ بایت است)

شماره نوع	عنوان سخت افزار کارت شبکه
1	Ethernet
2	Experimental Ethernet
3	X.25
4	Proteon ProNET (Token Ring)
5	Chaos
6	IEEE 802.X
7	ARCnet

مدل مرجع OSI

HW Type		Prot. Type
HW Addr Len	Prot Addr Len	Operation
Sender's HW Addr (1-4)		
SHA (5-6)		SIP (1-2)
SIP (3-4)		THA (1-2)
Target HW Addr (3-6)		
Target IP Addr		

Protocol Type:

شماره پروتکل لایه شبکه را مشخص می نماید که برای پروتکل IPV4 عدد ۲۰۴۸ و یا 0x800 می باشد.

Hardware Address Length:

طول آدرس سخت افزاری یا به عبارت دیگر طول آدرس فیزیکی را مشخص می نماید که برای پروتکل اترنت، طول این آدرس ۶ بایت است.

Protocol Address Length:

اندازه طول آدرس پروتکل لایه شبکه است. برای پروتکل IP این عدد برابر ۴ است.

مدل مرجع OSI

Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request 1, Reply 2
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled in a request)		
Target protocol address (For example, 4 bytes for IP)		

Operation:

نوع عملیات تعریف شده برای پروتکل را تعریف می نماید:

1 : فاز Request (درخواست) پروتکل ARP

2: فاز Reply (پاسخ) پروتکل ARP

3 : فاز Request پروتکل RARP

4: فاز Response پروتکل RARP

Sender Hardware Address: آدرس فیزیکی مبدا (ارسال کننده)

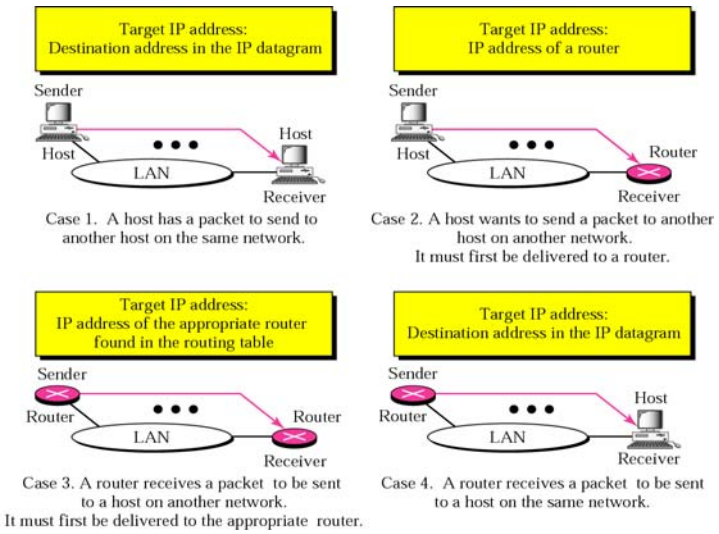
Sender Protocol(IP) Address:آدرس IP مبدا

Target Hardware Address: آدرس فیزیکی مقصد(دریافت کننده)

Target Protocol(IP) Address: آدرس IP مقصد

M.Zangian

مدل مرجع OSI



چهار شکل استفاده از پروتکل ARP

M.Zangian

مدل مرجع OSI

مراحل اجرای پروتکل ARP:

۱- دستگاه مبدا برای ارسال یک بسته به مقصد با IP مشخص ابتدا بررسی می کند مقصد در Subnet خودش قرار دارد یا خیر؟

۲- در صورتیکه مقصد با مبدا در یک Subnet باشند مبدا به دنبال آدرس فیزیکی مقصد و در صورتیکه مبدا و مقصد در یک Subnet نباشند مبدا به دنبال آدرس فیزیکی Default Gateway است.

۳- مبدا برای یافتن آدرس فیزیکی مقصد(ویا Gateway) ابتدا به ARP Cache خود مراجعه می کند در صورتیکه برای IP مورد نظر قبلا آدرس فیزیکی پیدا شده باشد و در ARP cache ثبت شده باشد ،دیگر نیازی به استفاده از پروتکل ARP نیست و مبدا می تواند فریم اترنت را با همان آدرس فیزیکی موجود ایجاد نماید.

۴- در صورتیکه مبدا آدرس فیزیکی مقصد را در ARP Cache خود نیابد باید با استفاده از پروتکل و بسته ARP آنرا بیابد.

۵- مبدا قبل از ارسال بسته اصلی بسته دیگری بر اساس پروتکل ARP می سازد تا ابتدا آدرس فیزیکی مقصد را بیابد.

مدل مرجع OSI

مراحل اجرای پروتکل ARP:

۶- از آنجاییکه مبدا نمی داند که مقصد با IP مشخص چه آدرس فیزیکی دارد و در کجای شبکه قرار دارد بنابراین باید یک اعلان همگانی بفرستد تا هر ایستگاهی که آدرس IP مقصد را داراست اعلام وجود نموده و آدرس فیزیکی خود را به مبدا گزارش نماید. از اینرو مبدا یک فریم Broadcast ساخته و پیام ARP را درون آن جای میدهد.برای ارسال یک فریم همه پخشی مبدا از آدرس فیزیکی همه پخشی یعنی FF:FF:FF:FF:FF:FF استفاده می نماید. این نوع اعلان همه پخشی را ARP Request می نامند.

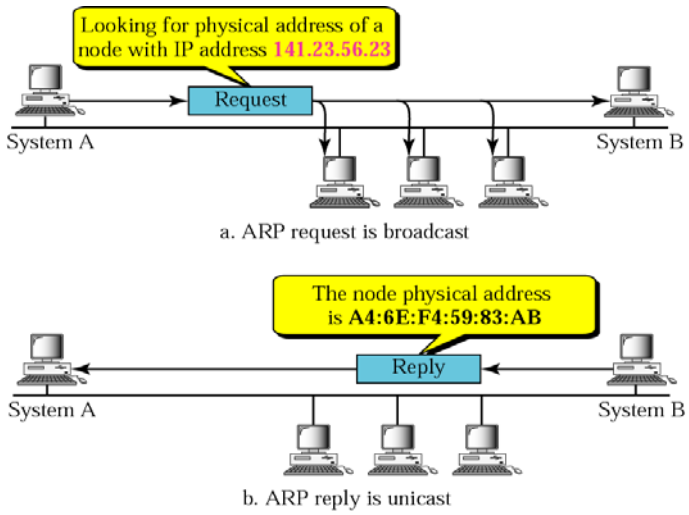
۷- همه ایستگاههای موجود در حوزه همه پخشی این درخواست (ARP Request)را دریافت می نماید. و هر ایستگاهی که IP آن با IP مقصد که در بسته ARP قرار دارد ،یکی بود، آدرس فیزیکی خود را درون بسته ARP قرار داده و باساخت بسته ARP Reply و کپسوله کردن آن آنرا به سمت مبدا درخواست کننده می فرستد.علاوه بر این مقصد اطلاعات IP و MAC Address مبدا را که در ARP Request قرار دارد را در ARP Cache خود ثبت می نماید.

۸- مبدا با دریافت ARP Reply ، آدرس فیزیکی معادل آدرس IP مقصد را در ARP Cache خود ثبت می نماید.

۹- مبدا بسته اصلی را در فریم اترنت با آدرس فیزیکی مقصد که دیگر وجود دارد را به مقصد ارسال می نماید.

مدل مرجع OSI

147

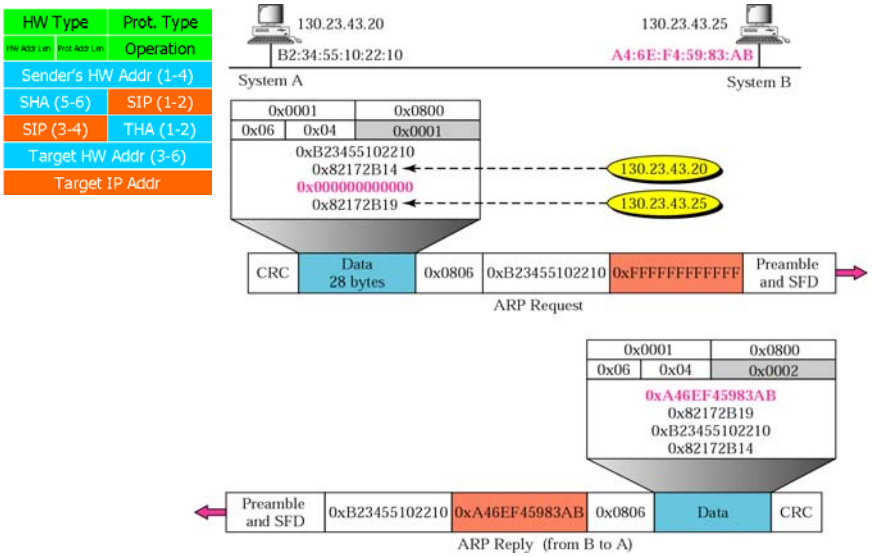


نوع ارسال فریم های ARP Request,Arp Reply

M.Zangian

مدل مرجع OSI

148



مرحله درخواست ARP و پاسخ ARP

M.Zangian

مدل مرجع OSI

حافظه ARP Cache:

دریک شبکه ارسال های Broadcast منابع سیستم و شبکه را به نحو چشمگیری مورد استفاده قرار می دهند.از اینرو تا جایی که ممکن است در صدد هستیم ارسال های Broadcast را در شبکه کاهش دهیم.از آنجاییکه بسته ARP Request از ارسال همه پخشی استفاده می نماید، سعی می شود این ارسالها نیز در شبکه کاهش یابد از اینرو بعد از یافتن آدرس فیزیکی مقصد ، مبدا این آدرس را در حافظه خود نگه می دارد تا در ارسالهای بعدی به همان آدرس IP از آدرس فیزیکی بدست آمده استفاده نماید. به حافظه ای که اطلاعات ARP را در خود نگه می دارد ، حافظه ARP Cache می گویند.

برای هر ورودی حافظه ARP ،یک تایمر Set می شود تا بعد سپری شدن زمان آن ورودی مورد نظر آزاد گردد. (معمولا ۲۰ دقیقه)

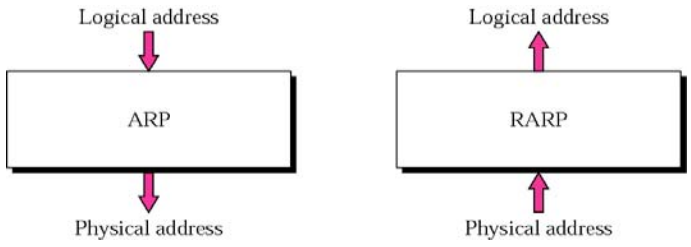
مدل مرجع OSI

تحقیق

در صورتیکه بعد از ثبت آدرس فیزیکی و آدرس IP یک میزبان در ARP Table، IP Address مورد نظر تغییر یابد چگونه این تغییرات در ARP Table بروز می شود؟

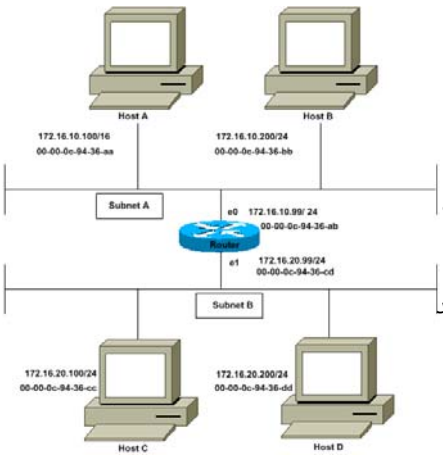
پروتکل RARP(Reverse Address Resolution Protocol)

این پروتکل عکس عمل پروتکل ARP را انجام می دهد یعنی با داشتن آدرس فیزیکی آدرس IP را بدست می آورد.



مدل مرجع OSI

وقتی مسیریابی که به یک شبکه متصل است می بیند آدرس مقصدی که توسط ARP سوال شده ،متعلق به شبکه ای است که به آن (مسیریاب)متصل است ،آدرس فیزیکی خودش را به ایستگاه سوال کننده در پاسخ ARP ارسال میدارد؛ به این روش Proxy ARP گفته میشود.



در شکل روبرو فرض کنید ایستگاه A بخواهدبسته ای رابه ایستگاه D ارسال نماید.باتوجه به IP های تعیین شده ایستگاه A تصور می کند ایستگاه D در Subnet خودش است و نیازی به Default Gateway ندارد .بنابراین برای یافتن MAC ایستگاه D بسته ARP را ، Broadcast می نماید. اما ایستگاه D درSubnet ایستگاه A نیست که به آن پاسخ دهد و روتر هم بسته های همه پخشی را هدایت نمی کند. در اینجا در صورتیکه تنظیمات Proxy ARP روی روتر انجام شده باشد بجای ایستگاه D روتر به بسته ARP پاسخ می دهدو اعلام میکند که بسته را به من بده تا آنرا به ایستگاه D برسانم.در روتر Cisco ، Proxy ARP بصورت پیش فرض فعال است.

M.Zangian

آدرس IP

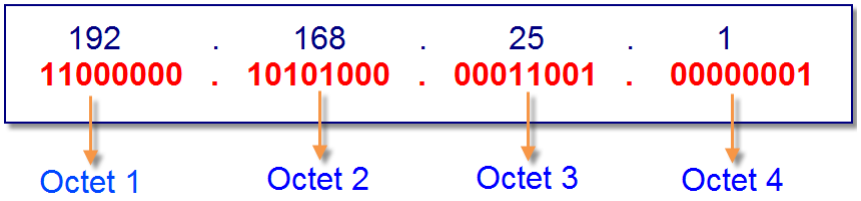
برای شناسایی ایستگاههای کاری که از پروتکل IP در لایه شبکه برای هدایت بسته ها استفاده می نمایند، از آدرس IP استفاده می گردد.این آدرس به هر ایستگاه کاری اختصاص یافته و به کمک آن هر ایستگاه موقعیت مشخصی در شبکه پیدا می نمایدکه امکان شناسایی آن توسط ایستگاههای کاری دیگر و نهایتا هدایت بسته ها از ایستگاه مورد نظر به ایستگاههای دیگر و برعکس را فراهم می سازد.

برای آدرسهای IP درحال حاضر دونسخه IPV4 و IPV6(IPng) ،استاندارد شده است.که در شبکه های کامپیوتری ابتدا IPV4 مورد استفاده قرار گرفت ولی بدلیل محدودیتهایی که این نسخه از آدرس دهی شبکه دارد ، IPV6 که ساختاری کاملا متفاوت با آن داشته و همانند IPV4 محدودیت تعداد آدرس برای ایستگاهها را ندارد، استانداردسازی شد.درحال حاضر در شبکه جهانی از هر دو نسخه استفاده شده است .اما اغلب شبکه های موجود هنوز از نسخه ۴ آدرس IP استفاده می کنند،که ما نیز در این درس به بررسی این نسخه خواهیم پرداخت.

M.Zangian

آدرس IP V4.0

نسخه ۴ آدرس IP از ۳۲ بیت برای آدرس دهی ایستگاههای کاری استفاده می نماید.که برای راحتی کار با آدرس های IP ، این ۳۲ بیت به ۴ قسمت ۸ بیتی تقسیم می گردد که به هریک از این ۴ قسمت یک اکتت(Octet) گفته می شود. در نمایش آدرس IP ، این ۴ اکتت با . از یکدیگر جدا شده و برای سهولت کار ،از معادل دهدهی هر اکتت برای نمایش آدرس IP استفاده می شود.



اگر بخواهیم با این ۳۲ بیت ،ایستگاههای کاری را آدرس دهی کنیم جمعا به تعداد ۲ به توان ۳۲ ایستگاه را می توانیم آدرس دهی کنیم که حدود ۴ میلیارد آدرس را در اختبار ما قرار خواهد داد.

$$2^{32} = 4,294,967,296$$

آدرس IP V4.0

آنچه که در اینجا می بایست مورد توجه قرار گیرد اینستکه تنها آدرس دهی ایستگاههای کاری ،انتظارات ما را از یک سیستم آدرس دهی برآورده نمی کند،چراکه آدرس باید بگونه ای باشد که بتوان به کمک آن محل قرار گیری ایستگاه را مشخص نمودتا با داشتن آدرس IP مقصد، امکان هدایت بسته ها به سمت آن فراهم شود.

در شبکه های کامپیوتری دو مفهوم از لحاظ آدرس دهی مورد توجه می باشد.

۱- شبکه در برگیرنده ایستگاه کاری(Network)

۲- ایستگاه کاری(Host)

بنابراین اگر برای این دو مشخصه یک شناسه در آدرس دهی تعریف نماییم ،امکان یافتن هر ایستگاه در یک شبکه عظیم کامپیوتری فراهم می شود.

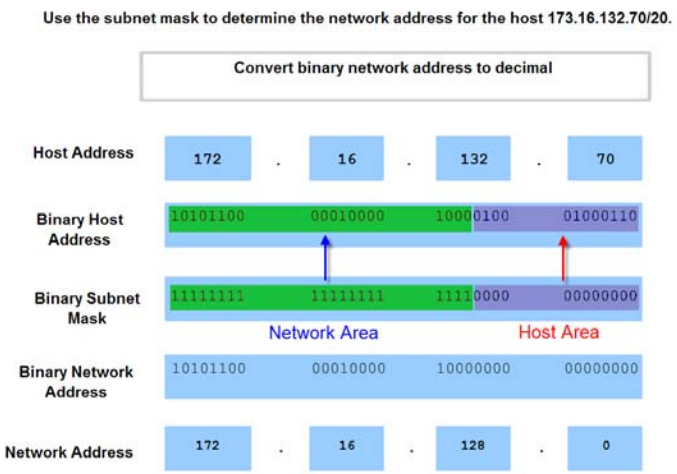
برای این منظور دو شناسه Network ID که منحصر بفرد می باشد برای مشخص کردن یک شبکه خاص و Host ID برای مشخص کردن شماره ایستگاه در یک Network با مشخصه Net Id مورد استفاده قرار می گیرد.بنابراین اگر ما شماره(شناسه) یک شبکه را بدانیم بدلیل اینکه منحصر بفرد است شبکه مورد نظر را یافته و با داشتن شناسه ایستگاه مورد نظر ، مستقیما ایستگاه کاری مورد نظر را درون آن شبکه خواهیم یافت.

آدرس IP V4.0

اما سئوالی که مطرح می شود اینست که کدام بخش از آدرس IP مربوط به شناسه شبکه (Net Id) و کدام بخش مربوط به شناسه میزبان (Host Id) می باشد. مشخص است که تنها از روی آدرس IP نمی توان این دوقسمت را تفکیک کرد بنابراین احتیاج به اطلاعات دیگری داریم که این دوبخش را در آدرس IP مشخص نماید.این اطلاعات اضافی الگوی شبکه ویا Subnet Mask نامیده می شود.بکمک الگوی شبکه می توان شناسه شبکه و میزبان را از هم تفکیک نمود.

الگوی شبکه متناظر با آدرسIP متشکل از ۳۲ بیت است.این ۳۲ بیت، بیت به بیت متناظر را آدرس IP می باشد.الگوی شبکه از دورشته پیوسته 1 و 0 در کنار هم تشکیل شده است.این رشته های 1 و 0پیوسته بوده وبین آنها مقدار دیگری قرار نمی گیرد.حال آن قسمت از آدرس IP که بیتهای متناظرش در الگوی شبکه 1 قرارگرفته محدوده Net Id را مشخص می کند و آن قسمت ازآدرس IP که متناظر با آن در الگوی شبکه صفر است محدوده Host Id را مشخص می کند.

آدرس IP V4.0



برای بدست آوردن آدرس Network محدوده Network را در IP آدرس بیت به بیت نوشته و تمام بیتهای محدوده Host را در IP صفر قرار می دهیم. به عبارت دیگر با AND آدرس IP و Subnet Mask آدرس شبکه بدست می آید.

آدرس IP V4.0

دو آدرس IP که آدرس شبکه آنها یکسان باشد متعلق به یک زیر شبکه هستند ومی توانند در لایه ۲ با یکدیگر ارتباط برقرار کنند.

در هر زیر شبکه دو آدرس رزرو شده است که نمی تواند بعنوان IP هیچ ایستگاهی مورد استفاده قرار گیرد.این دو آدرس عبارتند از آدرس شبکه و آدرس همه پخشی

1.Network Address
2.Broadcast Address

برای بدست آوردن آدرس شبکه کافی است تمام بیتهای آدرس IP را که درمحدوده Host است ، رابرابر صفر قرار دهیم.

برای بدست آوردن آدرس همه پخشی بدین صورت عمل می کنیم که تمام بیتهای آدرس IP را که در محدوده Host قرار دارد را برابر یک قرار می دهیم.

آدرسهای بین Network Address و Broadcast Address در هر زیر شبکه می تواند بعنوان آدرس ایستگاههای کاری مورد استفاده قرار گیرد.

آدرس IP V4.0

اگر تعداد بیتها محدوده Hostرا برابر n بگیریم تعداد ایستگاههایی که می توانند آدرس دهی شوند $2^n - 2$ خواهد بود

که دو آدرس کم شده همان آدرسهای شبکه و همه پخشی هستند که نمی تواند بعنوان آدرس ایستگاه مورد استفاده قرار گیرد.

اگر تعداد بیتهای محدوده Network برابر n باشد تعداد شبکه های مستقل از هم دو به توان n خواهد بود.

آدرس IP V4.0

زمانیکه IPV4.0 استانداردسازی شد، آدرسهای IP در پنج کلاس تقسیم بندی شدند که دارای الگوی شبکه (Subnet Mask) مشخص بودند.شکل زیر این ۵ کلاس و الگوی شبکه مربوط به هر یک را نشان می دهد.

IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

** All zeros (0) and all ones (1) are invalid hosts addresses.

M.Zangian

آدرس IP V4.0

Class	High Order Bits	Start	End
Class A	0	0.0.0.0	127.255.255.255
Class B	10	128.0.0.0	191.255.255.255
Class C	110	192.0.0.0	223.255.255.255
Multicast	1110	224.0.0.0	239.255.255.255
Experimental	1111	240.0.0.0	255.255.255.255

کلاسهای استاندارد شده با الگوی شبکه مشخصی (Subnet Mask)تعریف می شوند.از اینرو در صورتیکه ازکلاسهای کامل استفاده نماییم(Class Full) بدون داشتن الگوی شبکه می توان الگوی شبکه را بدست آورد.

در هر کلاس ،اکتت اول با الگویی از بیتها شروع می شود که به کمک این الگو می توان کلاس و درنهایت الگوی شبکه را بدست آورد.(اولین اکتت در کلاس A با 0،کلاس B با 10 کلاس C با 110 کلاس D با 1110 و کلاس E با 1111 شروع می شود.)

M.Zangian

آدرس IP V4.0

Subnet Mask based on Class

	1st Octet	2st Octet	3st Octet	4st Octet	Subnet Mask
Class A	Network	Host	Host	Host	255.0.0.0 or /8
Class B	Network	Network	Host	Host	255.255.0.0 or /16
Class C	Network	Network	Network	Host	255.255.255.0 or /24

Number of Networks and Hosts per Network for Each Class

Address class	First Octet Range	Number of Possible Networks	Number of Host per Networks
Class A	0 to 127	128 (2 are reserved)	16,777,214
Class B	128 to 191	16,348	65,534
Class C	192 to 223	2,097,152	254

آدرس IP V4.0

بطور کلی فضای آدرسهای IP به چند گروه تقسیم بندی می شود:

۱- آدرسهای عمومی (Public IP Addresses)

۲- آدرسهای اختصاصی(Private IP Addresses)

۳- آدرسهای خاص(Special IP Addresses)

۱- آدرسهای عمومی آدرسهایی هستند که در شبکه جهانی (اینترنت) پذیرفته شده هستند و قابل Route شدن هستند.این مجموعه بزرگترین مجموعه از فضای آدرس را تشکیل می دهند وآدرسهای این مجموعه توسط موسسات مشخصی اختصاص می یابند(IANA).(به این آدرسها IP های Valid نیز گفته می شود.)

۲- آدرسهای اختصاصی آدرس هایی هستند که در شبکه جهانی اینترنت اعتبار ندارند و می توانند جهت آدرس دهی شبکه های اختصاصی و اینترانت ها مورد استفاده قرار گیرد.

به این آدرسها IP Invalid نیز گفته می شود.)

۳- آدرسهای خاص آدرسهایی هستند که برای منظورهای خاصی مورد استفاده قرار می گیرندو هر یک تعریف مشخص و کاربرد معینی دارند.

آدرس IP V4.0

جدول زیر محدوده IPهای Private را نشان میدهد.

RFC1918 name	IP address range	number of addresses	classful description	largest CIDR block (subnet mask)	host id size
24-bit block	10.0.0.0 – 10.255.255.255	16,777,216	single class A	10.0.0.0/8 (255.0.0.0)	24 bits
20-bit block	172.16.0.0 – 172.31.255.255	1,048,576	16 contiguous class Bs	172.16.0.0/12 (255.240.0.0)	20 bits
16-bit block	192.168.0.0 – 192.168.255.255	65,536	256 contiguous class Cs	192.168.0.0/16 (255.255.0.0)	16 bits

Class	Start	End
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

آدرس IP V4.0

یکی دیگر از محدوده IP هایی که بعنوان Private IP Addresses شناخته می شود-Link local addresses هستند وزمانی مورد استفاده قرار می گیرد که برای ایستگاههای کاری بصورت استاتیک IP تعریف نشده باشد ویا اینکه نتوانند IP خود را از DHCP اختیار کنند در اینصورت بصورت اتوماتیک از این محدوده IP اختیار می کنند.این محدوده عبارتست از: 169.254.1.0- 169.254.254.255 این محدوده آدرس توسط روترها Route نمی شوند.

IP های خاص:

۱- Loopback Address

آدرسی است برای تست اینترفیس شبکه(کارت شبکه)، که در واقع ارسال بسته به این آدرس ارسال بسته از یک کامپیوتر به خودش است.این برگشت بسته بصورت فیزیکی نیست بلکه بصورت نرم افزاری است و برای تست صحت درایور و برخی از اشکالات سخت افزاری بکار می رود.محدوده در نظر گرفته شده برای کاربردهای Loopback 127.0.0.0-127.255.255.255 می باشدبا این حال اختصاصا IP ، 127.0.0.1 برای اشاره کامپیوتر به کارت شبکه خودش است.این آدرس تحت عنوان localhost نیز شناخته می شود.این آدرس همچنین اجازه کار به برخی نرم افزارهای شبکه را بدون داشتن شبکه امکانپذیر می کند که در این حالت سرویس دهنده و سرویس گیرنده خود کامپیوتر است.

آدرس IP V4.0

IP های خاص:

۲- Local Network

آدرس 0.0.0.0 بعنوان آدرس شبکه محلی است و تا زمانی که ایستگاه آدرسی اختیار نکرده است ،از این آدرس استفاده می نماید.این آدرس تنها می تواند بعنوان IP، ایستگاه مبدا در برخی از بسته ها بکار رود.

۳- Local Broadcast Address

آدرس 255.255.255.255 بعنوان آدرس همه پخشی برای هر شبکه محلی بکار می رود. و هر ایستگاهی در شبکه محلی با دریافت بسته ای که آدرس مقصد آن این آدرس باشد، آنرا می پذیرد.

آدرس IP V4.0

اولین اکتت هر کلاس مشخص کننده کلاس IP می باشد .در صورتیکه اکتت اول آدرس با بیت 0 شروع شود کلاس A و در صورتیکه دوبیت MSB اکتت اول 10 باشد کلاس Bو همینطور برای کلاسهای C,D,E به ترتیب 110,1110,1111 بیتهای شروع کننده خواهند بود.

الگوی شبکه برای هر کلاس ثابت بوده و تعداد مشخصی و ثابتی ایستگاه و شبکه در هر کلاس می تواند تعریف شود.که در شکل نشان داده شده است. از آنجاییکه بخشی از بیتهای هر کلاس ثابت است بنابراین در محاسبه تعداد شبکه هر کلاس باید بیتهای ثابت را حذف کرد بعنوان مثال در کلاس A تعداد بیتهای بخش Network ۸ بیت است اما از آنجاییکه بیت اول همیشه 0 است و تغییر نمی کند تعداد شبکه های قابل تعریف در این کلاس دو بتوان ۷ خواهد بود.

کلاسهای DوE کاربردهای خاص دارند و مانند سایر کلاسها مورد استفاده قرار نمی گیرند.

کلاس D برای آدرس دهی ارسالهای Multicast مورد استفاده قرار می گیرد و کلاس E تا کنون مورد استفاده قرار نگرفته است و جهت کاربردهای آزمایشی است.

آدرس IP V4.0

Subnetting:

استفاده از الگوهای ثابت کلاسهای تعریف شده تحت عنوان آدرس دهی Class Full نامگذاری می گردد.
اما استفاده از الگوهای شبکه Class Full محدودیتهای زیادی دارد بعنوان مثال کوچکترین زیر شبکه در این کلاسها 254 ایستگاه را می تواند آدرس دهی کند و برای شبکه هایی با تعداد Host های کوچکتر مجبوریم از یک کلاس کامل (یک کلاس C) استفاده نماییم،که آدرسهای محدود IP بیهوده در یک شبکه کوچک مورد استفاده قرار می دهد.
در مقابل الگوهای شبکه Class Full الگوهای شبکه Class Less یا الگوهای بدون کلاس هستند که می توانند از هر الگوی شبکه ای متناسب با نیاز استفاده نمایند.

نکته

تعداد Host ها و نیز شبکه ها می بایست توانی از دو باشد .بعنوان مثال برای طراحی زیر شبکه ای با 3 ،Host می بایست ۳ بیت در نظر گرفته شود.بعبات دیگر زیر شبکه ای با ۶ ایستگاه . برای طراحی زیر شبکه ای با ۳ ،host قبل از هر چیز می بایست 3+2 شود.چراکه دو آدرس برای آدرس شبکه و آدرس همه پخشی در هر زیر شبکه باید رزرو شود.و برای ۵ آدرس نزدیکترین عدد توان ۲ ، ۸ می باشد که ۳ بیت برای آدرس دهی آن مورد نیاز است.

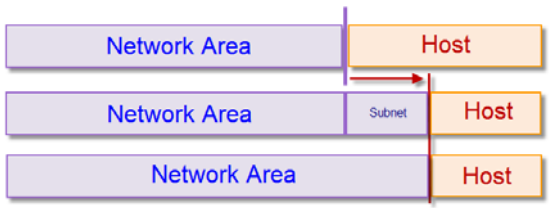
M.Zangian

آدرس IP V4.0

الگوهای شبکه Class Less این امکان را فراهم می آورد که زیر شبکه هایی با تعداد ایستگاههای متناسب با نیاز خود را آدرس دهی نماییم.

به عمل تقسیم آدرسهای یک کلاس و یا زیر شبکه، به چندزیر شبکه مستقل و کوچکتر Subnetting می گویند.

برای تقسیم یک کلاس و یا زیر شبکه به تعدادی زیر شبکه کوچکتر و درعین حال مستقل کافی است تعدادی بیت از محدوده Host را به بیتهای محدوده Network اختصاص دهیم.با این عمل به تعداد دو به توان بیتهای اختصاص داده شده از Host به Network می توان زیر شبکه های مستقل ایجاد کرد.بعبارت دیگر اگر دو بیت از محدوده Host به Network اختصاص دهیم تعداد ۴ یعنی دو به توان دو زیر شبکه کوچکتر خواهیم داشت.



M.Zangian

آدرس IP V4.0

با تقسیم یک کلاس یا زیر شبکه به زیر شبکه های کوچکتر الگوی شبکه یا همان Subnet Mask تغییر خواهد کرد و محدوده مربوط به Network افزایش خواهد یافت.(تعداد یک های Subnet Mask)

بطور کلی دو نوع طراحی در مسائل مربوط به Subnetting مطرح می شود که در زیر به بررسی هر یک خواهیم پرداخت:

۱- یک کلاس یا زیر شبکه داده می شود و خواسته می شود این محدوده آدرس را به تعداد مشخصی زیر شبکه تقسیم نماییم.در این نوع مسائل تعداد Host هر زیر شبکه اهمیتی ندارد و تنها تعداد مشخصی زیر شبکه مستقل مورد نظر است.

مثال:

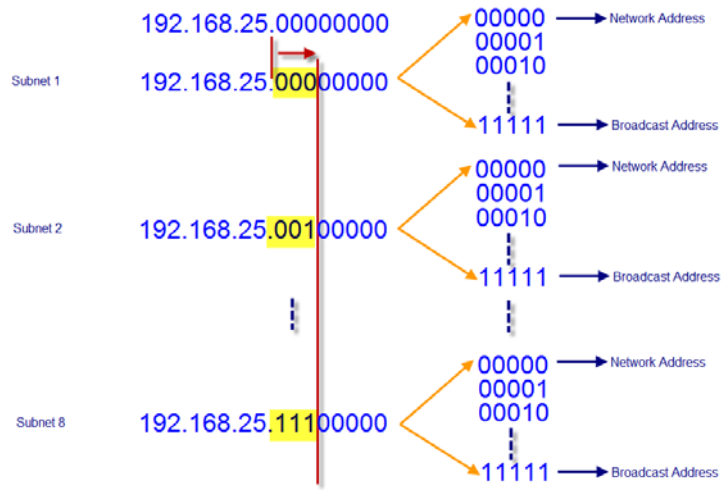
می خواهیم یک کلاس C به آدرس 192.168.25.0/24 را به 5 زیر شبکه مستقل از هم تقسیم نماییم:

آدرس IP V4.0

در این مثال یک کلاس Cداده شده است و میخواهیم آنرا به ۵ زیر شبکه مستقل تقسیم نماییم.محدوده Host در یک کلاس C شامل ۸ بیت است که می تواند 254 ایستگاه کاری را با آن آدرس دهی کرد.حال ما می خواهیم این ۲۵۴ آدرس را در زیر شبکه هایی قرار دهیم که مستقل از هم باشند.

برای حل این مسئله باید تعدادی بیت را از انتهای محدوده Host به Network اختصاص دهیم. در این مسئله کوچکترین توان ۲ که بتواند ۵ زیر شبکه را شامل شود ۸ است بنابراین ۳ بیت(۲ بتوان ۳ برابر ۸)از محدوده Host باید به Network اختصاص یابد.

آدرس IP V4.0



تقسیم یک کلاس Cبه ۸ زیر شبکه (Subnet)کوچکتر

آدرس IP V4.0

همانطوریکه در شکل صفحه قبل دیده می شود،با اختصاص ۳ بیت به Network ۸ زیر شبکه مستقل ایجاد می گردد که در هر یک از این زیر شبکه ها ۵ بیت محدوده Host می توانند از ۰ تا ۳۱ یعنی ۳۲ آدرس (۲ به توان ۵) آدرس را به خود اختصاص دهد.

دو آدرس ابتدا و انتهایی هر زیر شبکه بعنوان آدرس شبکه و آدرس همه پخشی مفهوم مجازی داشته و نمی تواند بعنوان آدرس ایستگاهی انتخاب شود بنابراین در هر زیر شبکه ۳۰ آدرس Host می توانیم داشته باشیم.

با تقسیم یک کلاس C به ۸ زیر شبکه الگوی شبکه ، برای هر یک از زیر شبکه ها تغییر می کند.

255 . 255 . 255 . 0
11111111.11111111.11111111.00000000

11111111.11111111.11111111.11100000

255 . 255 . 255 . 224

آدرس IP V4.0

همانطوریکه در مثال قبل مشاهده می گردد تمام زیر شبکه ها با یک الگوی شبکه ثابت تعریف می شوند این نوع تقسیم زیر شبکه ها را تقسیم به روش FLSM (Fixed Length Subnet Mask) می گویند.

۲- نوع دیگر مسائلی که در طراحی شبکه مطرح می باشد،مسائلی است که در آن تعداد Host در هر شبکه مشخص شده و تعداد شبکه در اهمیت دوم قرار دارد.

البته باید توجه نمود در اینگونه مسائل تعداد بیتهای باقیمانده برای تقسیم زیر شبکه ها به اندازه ای باشد که نیاز ما را برطرف نماید.

آدرس IP V4.0

مثال:

یک کلاس C به آدرس 192.168.25.0/24 را بگونه ای تقسیم نمایید که درهر زیر شبکه بتوان ۳۲ ،ایستگاه را آدرس دهی نمود.

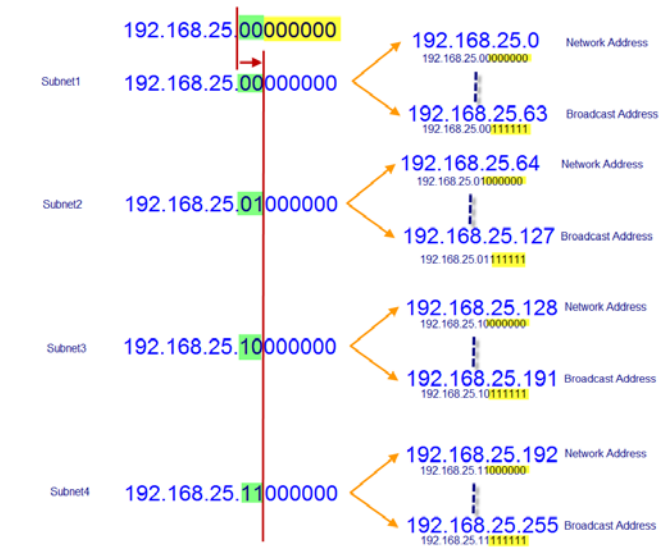
دراین مسئله بجای تعداد زیر شبکه تعداد ایستگاه در هر زیر شبکه داده شده است.

برای حل این مسئله ابتدا باید به تعداد آدرسهای مورد نیاز 2 آدرس اضافه نمود .این دو آدرس همان آدرسهای شبکه و همه پخشی هستند بنابراین در هر زیر شبکه ۳۲+۲=۳۴ آدرس نیاز داریم برای رسیدن به این تعداد آدرس احتیاج به ۶ بیت داریم(نزدیکترین عدد توان ۲ به ۳۴). در این نوع مسائل ۶ بیت را از سمت Host جدا می کنیم تا تعداد آدرسهای خواسته شده تضمین شود.

بنابراین ۲ بیت برای Subnetباقی می ماند یعنی ۴ Subnet خواهیم داشت.

آدرس IP V4.0

:FLSM

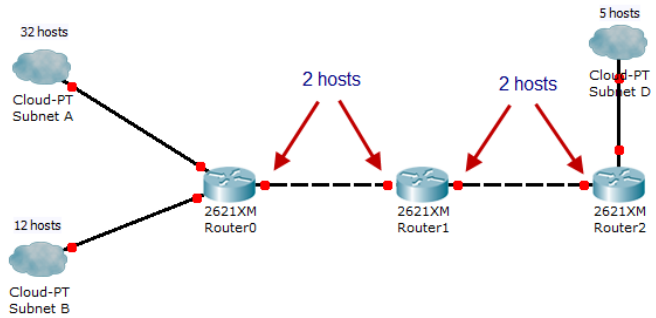


Subnet Mask:255.255.255.192

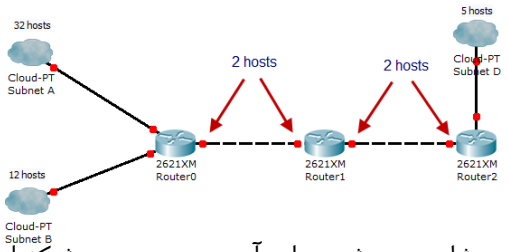
آدرس IP V4.0

مثال:

می خواهیم دیاگرام منطقی زیر را با استفاده از کلاس C: 192.168.25.0/24 آدرس دهی کنیم:



آدرس IP V4.0



همانگونه که در شکل مشاهده می شود برای آدرس دهی چنین شبکه ای ۵ ، زیر شبکه مستقل نیازداریم .از آنجاییکه در روش FLSM الگوی شبکه ثابت است ،بنابراین اندازه زیر شبکه ها باید بگونه ای باشد که بزرگترین گروه را در بر بگیرد.

Subnet 1:32+2=34 Addresses

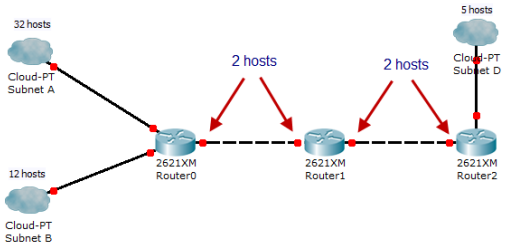
Subnet 2:12+2=14 Addresses

Subnet 3: 5+2=7 Addresses

Subnet 4: 2+2=4 Addresses

Subnet 5:2+2=4 Addresses

آدرس IP V4.0



با در نظر گرفتن آدرسهای مورد نیاز بزرگترین زیر شبکه باید بتواند ۳۴ آدرس را در اختیار قرار دهد.برای ۳۴ آدرس ما ۶ بیت از سمت Host Area نیاز داریم بعبارت دیگر:

مشاهده می شود که با محاسبات انجام شده تنها ۴ زیر شبکه را می توانیم آدرس دهی نماییم.اما در مسئله ما ۵ زیر شبکه نیاز داریم. چگونه باید این مشکل را برطرف کرد؟

192.168.25.00000000

Subnet 1 192.168.25.00000000

Subnet 2 192.168.25.01000000

Subnet 3 192.168.25.10000000

Subnet 4 192.168.25.11000000

آدرس IP V4.0

VLSM:

در مثال صفحه دیدیم به روش FLSM نمی توان مسئله را حل کرد.با واکاوی مسئله

می بینیم آدرس ها به دلیل محدودیت FLSM به صورت صحیح توزیع نشده است.بلوکهای زیر شبکه می بایست به اندازه ای بزرگ باشد که بزرگترین گروه آدرس را شامل شود یعنی بلوکهای ۶۴ آدرسی ،مشکل FLSM از همین جا آشکار می شود ما برای همه زیر شبکه ها حتی زیر شبکه هایی که ۴ آدرس نیاز دارند یک زیر شبکه ۶۴ آدرسی اختصاص داده ایم بنابراین آدرسها نتوانستند ۵ زیر شبکه را پوشش دهند.

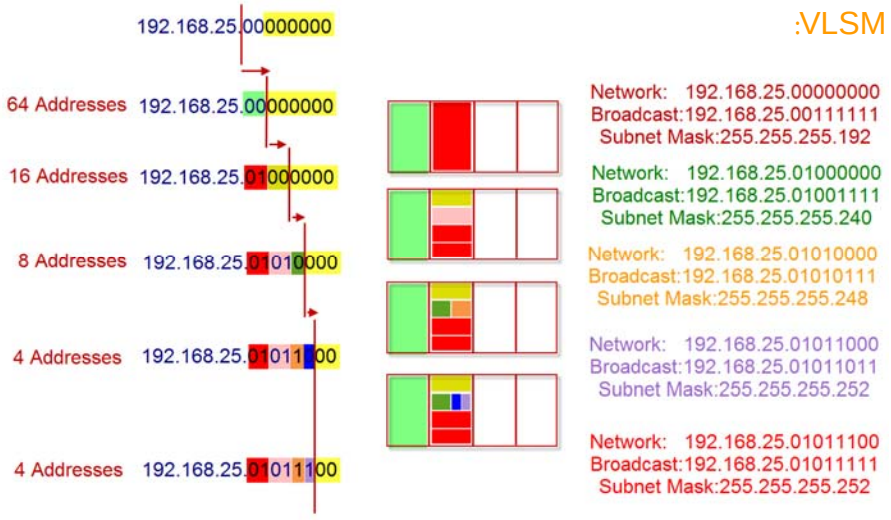
اگر ما بتوانیم به روشی در هر زیر شبکه تنها به تعداد آدرسهای مورد نیاز آدرس اختصاص دهیم بنابراین آدرسهای لازم برای زیر شبکه های دیگر هم فراهم می گردد و اینگونه استفاده از IP ها بهینه می شود.

در روش VLSM بر خلاف روش FLSM الگوی شبکه (Subnet Mask) در هر زیر شبکه می تواند تغییر نماید.

VLSM:Variable Length Subnet Mask

آدرس IP V4.0

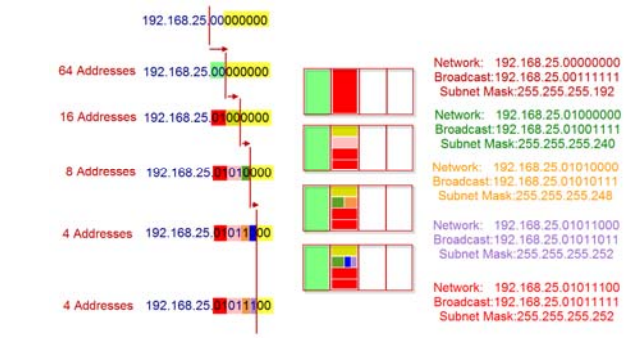
VLSM:



اولین مرحله در VLSM اینستکه تقسیمات را به ترتیب آدرس Sort نزولی نماییم.یعنی ابتدا تقسیمات را از دسته های بزرگتر شروع می کنیم.

آدرس IP V4.0

VLSM:

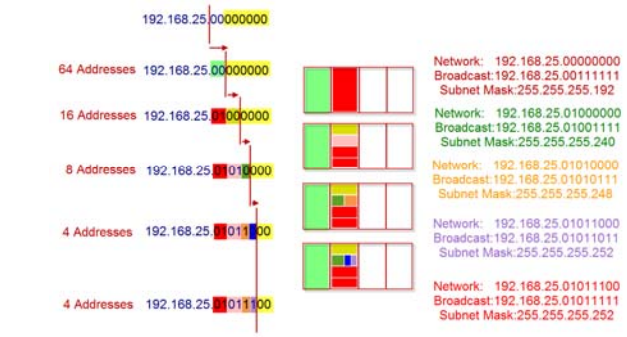


بنابراین کلاس داده شده را به ترتیب با ۶۴ آدرس،۱۶ آدرس، ۸ آدرس ، ۴ آدرس ، ۴ آدرس آدرس دهی می کنیم. اگر برای اولین زیر شبکه ۶ بیت در نظر بگیریم،۴ زیر شبکه ۶۴ آدرسی خواهیم داشت اولین قسمت را برای ۳۴ آدرس اول استفاده می کنیم(سیزرنگ). اما زیر شبکه دوم که ۶۴ آدرس را در اختیار قرار می دهد(قرمز رنگ) برای ۱۴ آدرس مورد نیاز ما بزرگ است بنابراین اگر ۴ بیت را برای ۱۴ آدرس کنار بگذاریم ۲ بیت باقی می ماند که تکه دوم را به ۴ قسمت تقسیم می کند.

M.Zangian

آدرس IP V4.0

VLSM:



اولین زیر شبکه از این ۴ قسمت را برای ۱۴ آدرس بعدی کنار می گذاریم (زیتونی)و سراغ دومین دسته می رویم(صورتی) که تعداد ۱۶ آدرس به ما می دهد که برای ۷ آدرس مورد نیاز ما بزرگ است. بنابراین این دسته را نیز تقسیم می کنیم برای ۷ آدرس ۳ بیت نیاز داریم بنابراین اگر سه بیت را کنار بگذاریم ۱ بیت باقی می ماند که می تواند ۲ زیر شبکه که هر کدام ۸ آدرس را در اختیار قرار دهد داشته با شیم. اولین زیر شبکه ۸ آدرسی را برای ۷ آدرس مورد نیاز کنار می گذاریم (سبز رنگ)و دومین زیر شبکه (نارنجی رنگ) را برای آدرسهای بعدی مورد استفاده قرار می دهیم.برای آدرسهای بعدی ما ۴ آدرس می خواهیم که سه بیت موجود ۸ آدرس را در اختیار می گذارد و برای ۴ آدرس ۲ بیت کافی است بنابراین یک بیت باقیمانده دو زیرشبکه ۴ ادرسی را در اختیار می گذارد.

M.Zangian

آدرس IP V4.0

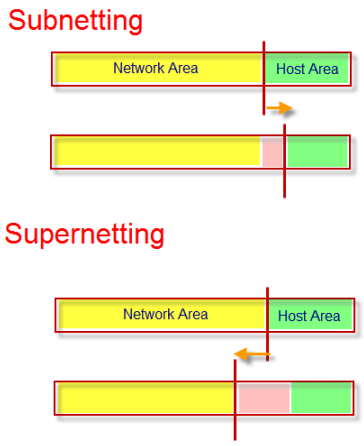
Supernetting:

در اسلایدهای قبل مباحث مربوط به Subnetting و ایجاد شبکه های مستقل کوچک از یک کلاس ویا زیر شبکه بزرگتر را بررسی کردیم.

اما گاهی اوقات لازم است برای ایجاد شبکه های یکپارچه بزرگتر ،از چند کلاس و یا زیر شبکه کوچکتر استفاده نماییم و با ادغام آنها یک شبکه یکپارچه با تعداد آدرسهای بیشتر ایجاد نماییم.دراین حالت مباحث Supernetting مطرح می شود.

آدرس IP V4.0

در Subnetting برای ایجاد چند زیر شبکه از یک کلاس بیتهایی از قسمتHost جدا می کردیم و به Network Area اختصاص می دادیم .اما در Supernetting برای ایجاد شبکه با Host های بیشتر باید بیتهایی را از قسمتNetwork به Host اختصاص دهیم.



آدرس IP V4.0

Supernetting:

مثال:

میخواهیم شبکه ای یکپارچه با تعداد ۶۰۰ ، Host طراحی نماییم.
از آنجاییکه یک کلاس C تنها 254 ،آدرس را دراختیار قرار می دهد یک راه برای ایجاد شبکه ای با تعداد ۶۰۰ آدرس استفاده از یک کلاس B است .دراینصورت می توان شبکه ای طراحی نمودکه بسیار بیشتر از ۶۰۰ آدرس یعنی ۶۵,۵۳۴ آدرس را در اختیار قرار دهد.در نگاه اول در می یابیم چنین راه حلی غیر منطقی بوده وبا توجه به محدودیت آدرسهای IP شاید غیر ممکن باشد.

راه حل دوم اینست که از چند کلاس C استفاده نماییم بطوریکه بتواند تعداد آدرسهای مورد نیاز ما را تامین نماید و با ادغام آنها شبکه مورد نظر خودرا طراحی نماییم.

اما ما شبکه ای یکپارچه می خواهیم و نباید بین آدرسها گسستگی وجود داشته باشد. از اینرو باید شروطی را برای ادغام مجموعه آدرسهای کوچکتر و ایجاد یک مجموعه بزرگتر در نظر بگیریم.

آدرس IP V4.0

شرایط استفاده از Supernetting برای ایجاد شبکه های بزرگتر
۱. بلوکهایی از آدرس که با هم ادغام می شوند باید توانی از دو باشند(2,4,8,...)
۲. بلوکهای آدرس که با هم ادغام می شوند بایستی پیوسته بوده وبین آنها فاصله نباشد.
۳.بیتهایی که از قسمت Network به Host اختصاص می دهیم در کوچکترین بلوک می بایست تماما صفر باشد.

آدرس IP V4.0

مثال : کدام یک از کلاسهای C زیر می توانند برای ایجاد شبکه ای با ۶۰۰ آدرس با هم ادغام (Supernet) شوند؟

1) 198.47.32.0 198.47.33.0 198.47.34.0
2) 198.47.32.0 198.47.42.0 198.47.52.0 198.47.62.0
3) 198.47.31.0 198.47.32.0 198.47.33.0 198.47.34.0
4) 198.47.32.0 198.47.33.0 198.47.34.0 198.47.35.0

برای ایجاد شبکه ای با ۶۰۰ آدرس با توجه به اینکه هر کلاس C تنها ۲۵۴ آدرس دراختیار قرار می دهد ۳ بلوک C نیاز داریم اما طبق شرایط Supernet کردن کلاسها تعدا بلوکها باید توانی از دو باشد بنابراین ۴ بلوک نیاز داریم بنابراین گزینه ۱ نمی تواند برای این منظور بکاررود.

گزینه ۲ شرط دوم را ندارد چون بلوکها پیوسته نیستند.

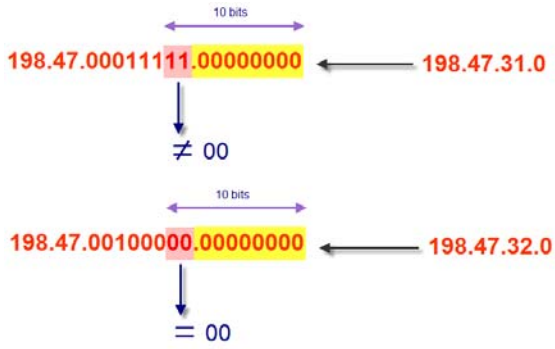
گزینه ۳ دو شرط اول را داراست اما در مورد شرط سوم ما باید بررسی نماییم. برای ۶۰۰ آدرس ما ۱۰ بیت برای Host نیاز داریم .کلاسهای C ، ۸ بیت برای Host دارند بنابراین باید دوبیت از قسمتNetwrok با Host اختصاص یابد.

M.Zangian

آدرس IP V4.0

حال ببینیم این دوبیت در کوچکترین بلوک صفر است یا خیر؟

در گزینه ۳ کوچکترین بلوک **198.47.31.0** می باشدپس خواهیم داشت:



مشاهده می شود که گزینه ۳ شرط دوم را ندارد اما گزینه چهارم هر سه شرط را داشته و می تواند Supernet شود.

M.Zangian

آدرس IP V4.0

برای Supernet کردن ۴ بلوک که شروط گفته شده را دارا هستندکافی است الگوی شبکه Supernet شده را بیابیم از اینرو کوچکترین بلوک را در نظر گرفته به طریق زیر عمل می کنیم.

198.47.32.0

198.47.00100000.00000000 255.255.11111111.00000000

198.47.00100000.00000000 255.255.11111100.00000000

255.255.252.0

مشاهده می شود بلوک 198.47.32.0/22 یک بلوک یکپارچه خواهد بود.

آدرس IP V4.0

چگونگی اختصاص IP Address به یک Host از نوع ویندوز(در اینجا XP)

به دو طریق می توان به یک ایستگاه کاری از نوع ویندوز IP Address اختصاص داد :

۱- بصورت اتوماتیک

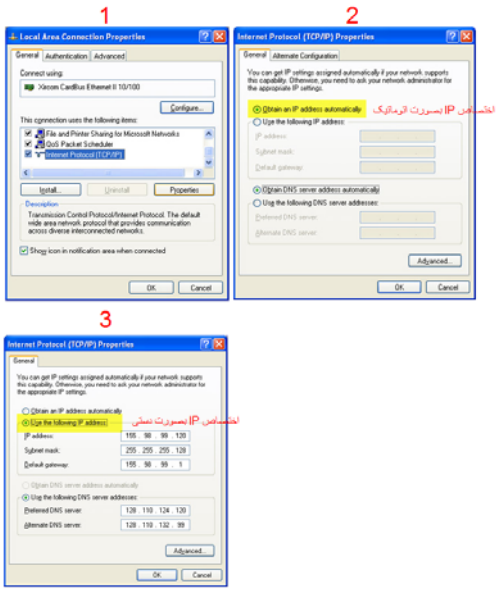
۲- اختصاص آدرس بصورت دستی

در حالت اول ایستگاه کاری با استفاده از پروتکل DHCP از یک سرویس دهنده DHCP ، IP Adress و سایر اطلاعات نظیر Subnet Mask، Default Gateway،DNS Server Address را دریافت می نماید.

درحالت دوم آدرسها می بایست بصورت دستی تنظیم شود . اسلاید بعدی نحوه اختصاص آدرسهای مورد نیاز بصورت دستی را نشان می دهد.

DHCP: Dynamic Host Configuration Protocol

آدرس IP V4.0



مدل مرجع OSI- لایه پیوند داده

لایه پیوند داده لایه دوم مدل مرجع OSI و قسمتی از لایه Network Access (لایه ۱) مدل مرجع TCP/IP می باشد.

وظایف این لایه عبارتند از:

۱- کپسوله سازی Packet ها با استفاده از Header و Trailer

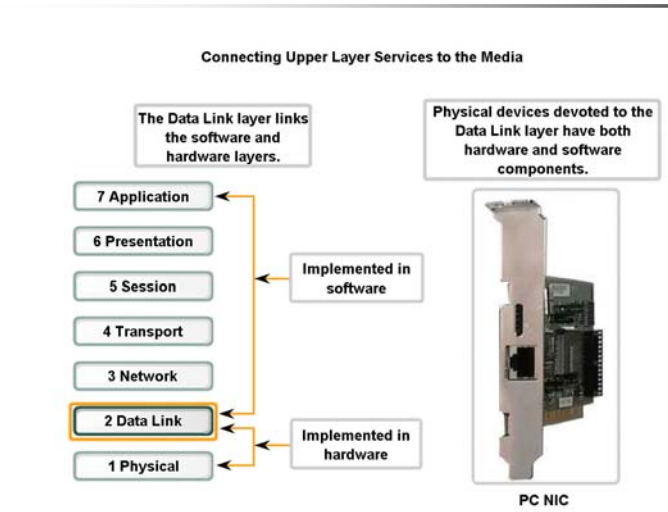
۲- آدرس دهی مناسب برای ارتباط ایستگاهها در این لایه

۳- کنترل دسترسی به رسانه (Media)

۴- کنترل جریان داده

۵- کنترل خطا (Error Detection &Correction)

مدل مرجع OSI- لایه پیوند داده



بخشی از لایه پیوند داده بصورت نرم افزار و بخشی بصورت سخت افزاری پیاده سازی می شود.

مدل مرجع OSI- لایه پیوند داده

۱- کپسوله سازی بسته ها درون فریم

متناسب با نوع رسانه انتقال ،پهنای باند،نوع لینک ارتباطی پروتکلهای متفاوتی برای ارتباط ایستگاههای کاری در این لایه تعریف شده اند که هر یک ویژگی های خاص خود رادارند . اما تمام این پروتکلها بسته (Packet) دریافت شده از لایه شبکه را درون Header و Trailer ، کپسوله سازی می کنند. فرمت و فیلدهای اطلاعاتی در heder و Trailer بسته به پروتکل استفاده شده متفاوت است . از مهمترین پروتکلهای لایه پیوند داده عبارتند از :Ethernet,PPP,HDLC

,SLIP,...

بنابراین پروتکلهای متفاوت در این لایه فریمهای مختص خود را دارند. روتر که از تجهیزات لایه ۳ محسوب می شود فریم دریافت شده از فرستنده باهر پروتکلی که باشد را حذف و مجددا آنرا براساس پروتکل Next Hop فریم بندی می کند.

مدل مرجع OSI- لایه پیوند داده

Standards for the Data Link Layer

ISO:	HDLC (High Level Data Link Control)
IEEE:	802.2 (LLC), 802.3 (Ethernet) 802.5 (Token Ring) 802.11(Wireless LAN)
ITU:	Q.922 (Frame Relay Standard) Q.921 (ISDN Data Link Standard) HDLC (High Level Data Link Control)
ANSI:	3T9.5 ADCCP (Advanced Data Communications Control Protocol)

برخی از استانداردهای لایه پیوند داده

مدل مرجع OSI- لایه پیوند داده

۲- آدرس دهی لایه پیوند داده

از آنجاییکه تجهیزات و ایستگاههای کاری ممکن است بخواهند در لایه دو با یکدیگر ارتباط برقرار کنند بنابراین می بایست آدرس دهی مستقل از لایه شبکه برای این لایه در نظر گرفت تا تجهیزات بتوانند در این لایه بصورت مستقل از لایه شبکه فریمها را دریافت و انتقال دهند.

براساس نوع لینک ارتباطی و پروتکل لایه پیوند داده این سیستم آدرس دهی می تواند بصورت ساده و خلاصه و یا سیستم آدرس دهی کاملتری را شامل شود.

مهمترین آدرس استفاده شده در این لایه لایه فیزیکی(MAC Address) است که قبلا مفصلا راجع به آن صحبت شده است.

مدل مرجع OSI- لایه پیوند داده

۲- کنترل دسترسی به رسانه مشترک

بطور کلی دونوع لینک ارتباطی را برای ارتباط یک ایستگاه با ایستگاه دیگر می توان متصور شد.

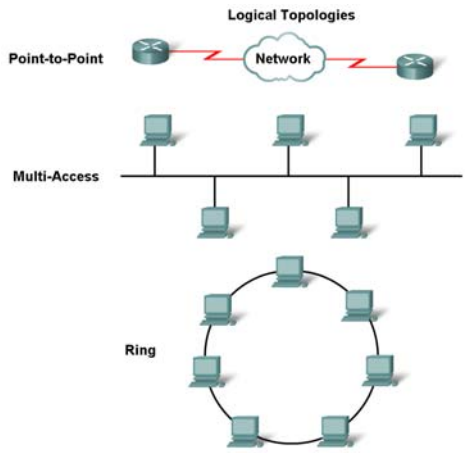
۱- لینک ارتباطی نقطه به نقطه(Point-to-Point)

۲- رسانه مشترک (Shared Medium)

لینک ارتباطی نقطه به نقطه بدین معنی است که بین دو دستگاه یا ایستگاه کاری تنها یک لینک ارتباطی وجود دارد.

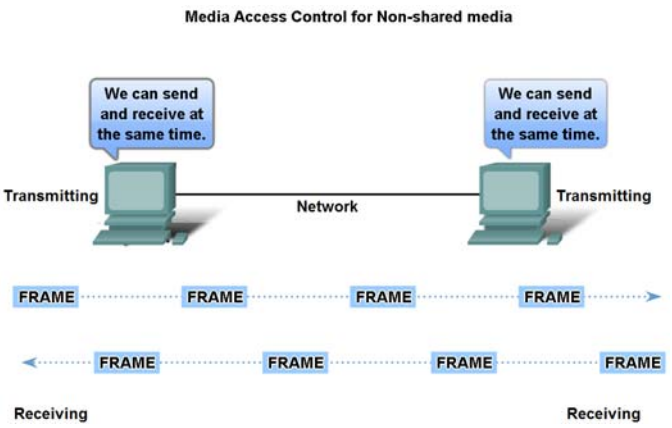
بنابراین پروتکلهای تعریف شده برای این نوع لینکها ساده بوده و سیستم آدرس دهی آن مختصر و ساده می باشد.از مهمترین پروتکلهای ارتباطی نقطه به نقطه می توان به پروتکلهای PPP,HDLC اشاره کرد.

مدل مرجع OSI- لایه پیوند داده



توپولوژی های مختلف دسترسی به رسانه

مدل مرجع OSI- لایه پیوند داده



کنترل دسترسی به رسانه برای ارتباط نقطه به نقطه بسیار ساده است

مدل مرجع OSI- لایه پیوند داده

کنترل دسترسی به رسانه مشترک

ارتباط بین دو ایستگاه کاری در ارتباط نقطه به نقطه به دو صورت می تواند انجام شود:

۱- ارتباط بصورت دو طرفه (Full Duplex)

در این نوع ارتباط دو ایستگاه در دو سر لینک می توانند هر زمان که بخواهند به ارسال فریمها بپردازند و بصورت دو طرفه و همزمان با یکدیگر به تبادل اطلاعات بپردازند.در این روش در دسترسی به رسانه ارتباطی مشکلی بوجود نخواهد آمد.

۲- ارتباط بصورت یک طرفه (Half Duplex)

در این نوع ارتباط دو ایستگاه نمی توانند همزمان به ارسال فریم بپردازند و می بایست زمان ارسال برای هر ایستگاه تعیین شود تا تصادم بین فریمها بوجود نیاید.

بنابراین در این نوع ارتباط کنترل ساده دسترسی به رسانه مورد نیاز است.

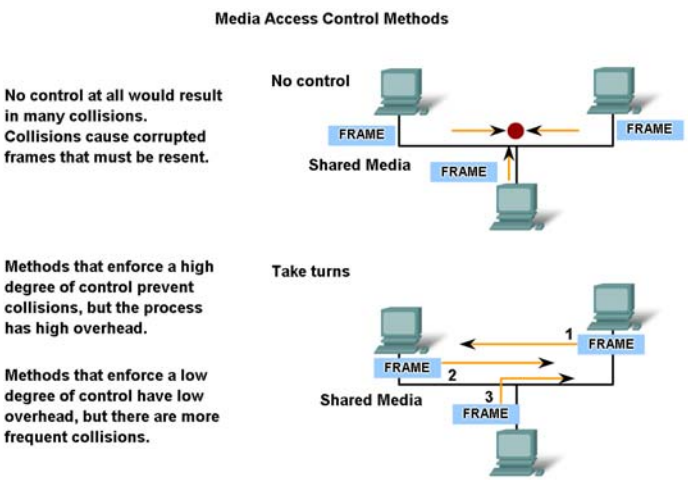
مدل مرجع OSI- لایه پیوند داده

کنترل دسترسی به رسانه مشترک

در ارتباط ایستگاهها بصورت رسانه مشترک ،ایستگاهها برروی یک محیط مشترک که بین تمام ایستگاهها وجود دارد به تبادل اطلاعات می پردازند از اینرو کنترل دسترسی به رسانه در این روش بسیار حائز اهمیت ،همچنین به سیستم آدرس دهی کاملتری در این روش نیاز است چون تعداد ایستگاههای کاری بیش از دو ایستگاه است. علاوه براین برای ارتباط بین ایستگاهها توپولوژی ارتباطی متفاوتی وجود دارد که هر یک شرایط خاصی را برای کنترل دسترسی به رسانه مشترک تعریف می کنند.

عدم وجود کنترل دسترسی به رسانه مشترک ، باعث بوجود آمدن تصادم (Colision) بین فریمها و از بین رفتن اطلاعات فریمها می شود.

مدل مرجع OSI- لایه پیوند داده



وجود پروتکل دسترسی به رسانه باعث کاهش Colision می شود.

مدل مرجع OSI- لایه پیوند داده

کنترل دسترسی به رسانه مشترک

از لحاظ روش و تکنولوژیهای مورد استفاده ، روشهای دسترسی به رسانه مشترک به دو دسته کلی تقسیم می شوند:

۱- روش ایستا (Static) تخصیص کانال

۲- روش پویا (Dynamic) تخصیص کانال

مدل مرجع OSI- لایه پیوند داده

۱- روش ایستا تخصیص کانال

در این روش کانال از لحاظ زمانی ویا باند فرکانسی بین استفاده کننده ها تقسیم می شود. در روش تسهیم زمانی (TDM:Time Division Mutiplex) کانال بصورت لحظات کوتاه به ترتیب در اختیار یکی از استفاده کننده ها قرار می گیردوهر استفاده کننده تنها در زمان مربوط به خود می تواندبه ارسال اطلاعات بپردازد.و در روش(FDM:Frequency Division Multiplex)کانال به باندهای فرکانسی مجزا تقسیم شده و هر باند فرکانسی به یکی از استفاده کننده ها اختصاص می یابد.
این روش دو عیب بزرگ دارد یکی اینکه اگر تعداد استفاده کننده زیاد باشد و ظرفیت کانال محدود ، ظرفیت اختصاص یافته به هر کانال محدود می شود.

روش ایستا تخصیص کانال- Multiplexing

عیب دیگر این روش اینستکه در بسیاری از زمانها ایستگاههای کاری داده ای برای ارسال ندارند بنابراین در زمان اختصاص یافته (و یا باند فرکانسی تخصیص یافته) برای آن ایستگاه داده ای ارسال نمی گردد.که این باعث کاهش بهره وری و بازدهی کانال می شود.

مدل مرجع OSI- لایه پیوند داده

روش پویا (Dynamic) تخصیص کانال :

در این روش ، کانال بصورت دینامیک به ایستگاهها تخصیص می یابد . برای استفاده از چنین روشهایی فرضها و شرایط زیر متصور است:

۱-فرض مدل ایستگاه: N ایستگاه در شبکه موجود است که هریک در هر زمان ممکن است احتیاج به ارسال اطلاعات داشته باشد.

۲- فرض کانال انتقال یکتا:فقط یک کانال مشترک برای تبادل اطلاعات موجود است.

۳- فرض برخورد (Colision) ممکن است دو یا چند ایستگاه بطور همزمان اطلاعات خود را روی کانال قرار دهند که در این صورت برخورد روی خواهد دادومی بایست عمل ارسال مجدد صورت گیرد.ضمن اینکه فرض می کنیم تنها خطای ممکن خطای برخورد باشد.

۴- مدل زمانی می تواند بصورت پیوسته و یا گسسته باشد.در مدل زمانی پیوسته ایستگاهها در هر زمانی می توانند اقدام به ارسال فریم نمایند.در حالت مدل زمانی گسسته زمان به بازه های زمانی مشخص (Time Slot) تقسیم شده و ایستگاهها فقط مجاز به ارسال فریم در ابتدای هر بازه زمانی هستند.اگر چه می توانند در طول بازه چندین فریم ارسال کنند.

مدل مرجع OSI- لایه پیوند داده

روش پویا (Dynamic) تخصیص کانال – شرایط متصور

۵- مدل شنود سیگنال حامل :

الف) باقابلیت شنود :ایستگاههای کاری می توانند متوجه شوند که کانال اشغال است . در نتیجه می توانند قبل از ارسال در صورت اشغال بودن از ارسال اجتناب کنند.

ب) بدون قابلیت شنود: ایستگها قابلیت تشخیص اشغال بودن کانال را ندارند بنابراین پس از ارسال در صورت رخداد Colision مجددا فریم را ارسال می کنند.

مدل مرجع OSI- لایه پیوند داده

کنترل دسترسی به رسانه مشترک (روش های پویا)

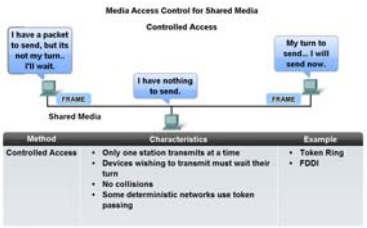
بطور کلی می توان روشهای کنترل دسترسی به رسانه مشترک را به دو گروه تقسیم بندی کرد:

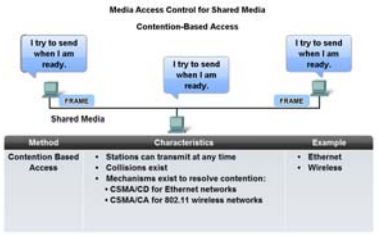
۱- روشهای دسترسی کنترل شده به رسانه

Controlled media access

۲- روشهای دسترسی به رسانه مبتنی بر رقابت

Contention based media access





M.Zangian

مدل مرجع OSI- لایه پیوند داده

کنترل دسترسی به رسانه مشترک

۱- روشهای های دسترسی کنترل شده به رسانه

در این روش هر ایستگاه کاری بصورت کنترل شده اقدام به ارسال فریمها می نماید.بنابراین هیچ یک از ایستگاهها نمی تواند هر زمان که بخواهد اقدام به ارسال اطلاعات نماید و باید منتظر بماند تا مجوز دسترسی به رسانه را دریافت نماید.

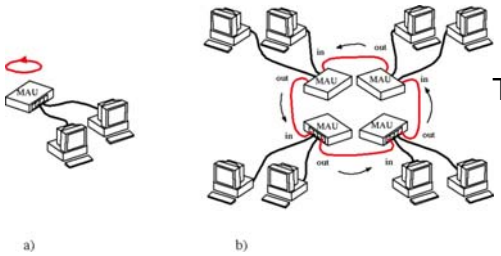
ویژگیهای چنین روشهایی عبارتند از :

- قابل پیش بینی بودن و قطعی بودن
- هر دستگاه تنها در زمان تعیین شده ای می تواند داده را ارسال نماید و در مابقی زمانها باید منتظر بماند تا مجددا زمان دسترسی به رسانه به آن ایستگاه داده شود.
- اینگونه روشها ی کنترل دسترسی سربار (Overhead) زیادی تحمیل می کنند.
- در چنین شبکه هایی تصادم (Colision) وجود ندارد.

از جمله این روشهای دسترسی به رسانه مشترک روش Token Ring است که با استفاده از Token کنترل می شود.Token بین ایستگاههای مختلف درون حلقه جابجا می شود و هر ایستگاه که Token را دریافت نماید می تواند اقدام به ارسال اطلاعات نماید.

M.Zangian

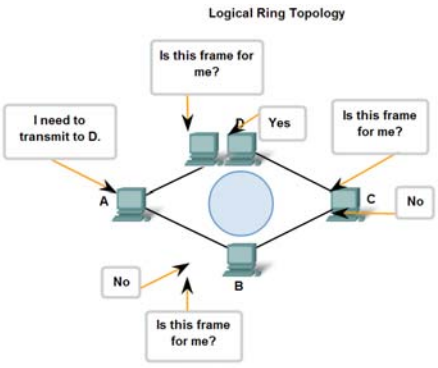
مدل مرجع OSI- لایه پیوند داده



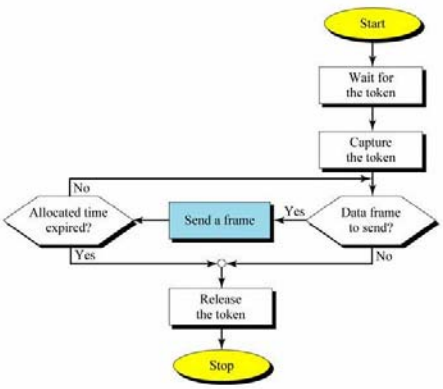
Token Ring Access Unit

Token Ring سوئیچ

مدل مرجع OSI- لایه پیوند داده



دریافت فریم در توپولوژی Ring



گردش عملیات Token Ring

مدل مرجع OSI- لایه پیوند داده

کنترل دسترسی به رسانه مشترک

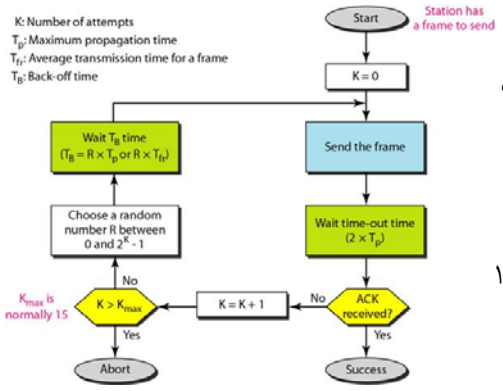
روشهای دسترسی به رسانه مبتنی بررقابت Contention based media access

- قابل پیش بینی نمی باشد.هر کس اول شروع کند ، رسانه را در اختیار می گیرد.
- هر ایستگاه به رسانه مشترک گوش می کند وزمانیکه رسانه مشترک را خالی بیابد می تواند اقدام به ارسال اطلاعات نماید.
- سربار در اینگونه روشها کم است.
- احتمال وقوع تصادم Colision وجوددارد.
- احتیاج به سیستمی برای باز ارسال فریمهای آسیب دیده دارد.
- برای شبکه های بزرگ به هیچ عنوان مناسب نمی باشد.

از پروتکلهایی که از اینگونه روشها استفاده می نماید می توان به اترنت قدیمی اشاره نمود.

مدل مرجع OSI- لایه پیوند داده

پروتکل ALOHA:



۱- Pure ALOHA

در این پروتکل مدل زمانی پیوسته بوده و شنود سیگنال حامل وجود ندارد. فرستنده در صورت برخورد یک زمان تصادفی منتظر می شود و مجددا فریم را ارسال می کند. در این روش بازدهی استفاده از کانال مشترک در حدود ۱۸.۴ درصد است که چندان مطلوب نیست.

۲- Slotted ALOHA

این پروتکل مانند Pure ALOHA است با این تفاوت که مدل زمانی در این روش گسسته است .بازدهی این روش دوبرابر حالت قبل است زیرا در طول Time Slot ها برخورد یا Colision نخواهیم داشت.

مدل مرجع OSI- لایه پیوند داده

کنترل دسترسی به رسانه مشترک

پروتکل دسترسی چندگانه با قابلیت شنود سیگنال حامل (Carier Sense Multiple Access-CSMA

بطور کلی سه روش دسترسی چند گانه با قابلیت شنود سیگنال حامل مورد استفاده قرا گرفت:

۱- با سماجت Persistent

۲-بدون سماجت Non-Persistent

۳- باسماجت P P-Persistent

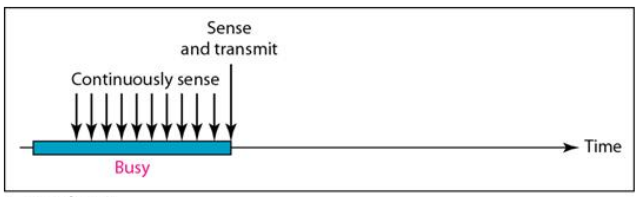
مدل مرجع OSI- لایه پیوند داده

کنترل دسترسی به رسانه مشترک

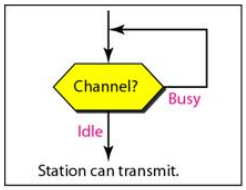
دسترسی چندگانه با قابلیت شنود سیگنال حامل

۱- Persistent: (با سماجت)

در این پروتکل که مدل زمانی پیوسته با قابلیت شنود است،فرستنده بصورت مستمروبا سماجت وضعیت خط را چک می کند و هر زمان خط را آزاد ببیند با احتمال (۱۰۰٪) اقدام به ارسال اطلاعات می نماید.بازدهی این روش حدود 50% است.



a. 1-persistent



a. 1-persistent

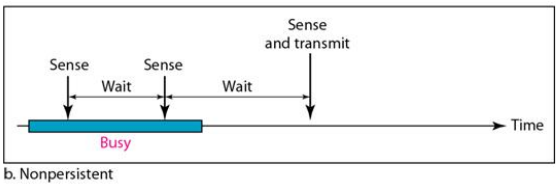
مدل مرجع OSI- لایه پیوند داده

کنترل دسترسی به رسانه مشترک

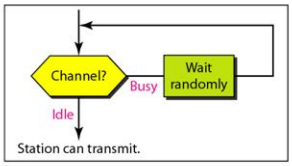
دسترسی چندگانه با قابلیت شنود سیگنال حامل

۲- None-Persistent(بدون سماجت)

این روش مانند روش Persistent است با این تفاوت که بجای چک مستمر خط توسط فرستنده ،خط در فاصله های زمانی تصادفی چک وبررسی می شود و در صورت آزاد بودن خط ، فرستنده اقدام به ارسال اطلاعات می نماید.بازدهی این روش حدود ۹۰٪ است.



b. Nonpersistent

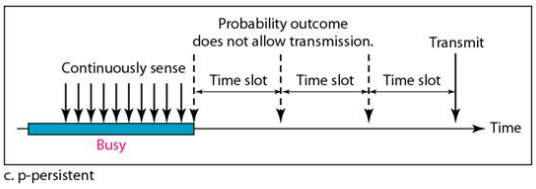


b. Nonpersistent

مدل مرجع OSI- لایه پیوند داده

کنترل دسترسی به رسانه مشترک

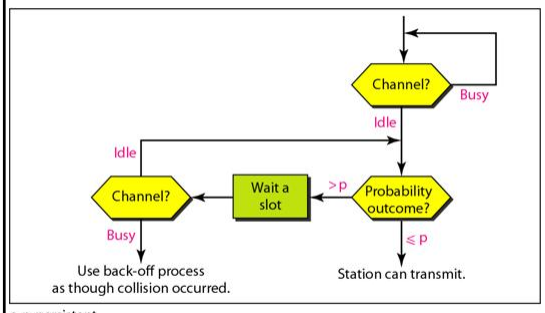
دسترسی چندگانه با قابلیت شنود سیگنال حامل



c. p-persistent

۳- P-Persistent(با سماجت P)

مدل زمانی در این روش ،بصورت گسسته است. در این روش فرستنده اگر خط را آزاد ببیند به احتمال P اقدام به ارسال می نماید.بازدهی این روش بسته به مقدار Pمتغییر است مثلا برای P=0.1 بازدهی حدود ۹۰٪ وبرای P=0.01 بازدهی حدود ۹۹٪ است.



c. p-persistent

مدل مرجع OSI- لایه پیوند داده

کنترل دسترسی به رسانه مشترک

دسترسی چندگانه با قابلیت شنود سیگنال حامل با قابلیت تشخیص تصادم

Carrier Sense Multiple Access/Colision Detection(CSMA/CD)

این روش علاوه بر قابلیت های روشهای قبلی توانایی تشخیص Colision را دارد.در این روش ابتدا ایستگاههایی که تمایل به ارسال فریم دارند موظفند به خط گوش دهند و تا آزاد شدن کانال صبر کنند این مرحله یعنی Carrier sense می تواند براساس یکی از روشهای توضیح داده شده یعنی None Persistent, P Persistent, Persistent صورت گیرد.بعد از آزاد شدن کانال و ارسال فریم امکان بوجود آمدن تصادم وجود دارد.در صورت بروز تصادم هر ایستگاه که برخورد را تشخیص داده است ،ابتدا یک سیگنال هشدار دهنده به نام سیگنال Jam را برای اطلاع به سایر ایستگاهها مبنی بر بروز تصادم برروی کانال مشترک قرار میدهد.سپس هر کدام از ایستگاههایی که در تصادم نقش داشته اند موظف هستند براساس الگوریتم عقب گرد نمایی Exponential Backoff یک عدد تصادفی بر مبنای ضریبی از زمانهای 51.2 میکروثانیه صبر کرده و مجددا کانال را بررسی نمایند.

M.Zangian

مدل مرجع OSI- لایه پیوند داده

کنترل دسترسی به رسانه مشترک

الگوریتم عقب گرد نمایی (Exponential Backoff)

طبق الگوریتم عقب گرد نمایی . در بار اول تصادم، از بین اعداد (0,1) یک عدد انتخاب شده و به اندازه ضریب آن در واحد زمانی 51.2 میکرو ثانیه تاخیر انجام می شود در بار دوم تصادم ،عدد تصادفی از بین اعداد (0,1,2,3) انتخاب خواهد شد و در تکرار k ام عدد تصادفی از بازه $(0,2^k-1)$ انتخاب می شود.

تاخیر انتشار (Propagation Delay)

مدت زمانی که طول می کشد تا سیگنالی از یک نقطه از رسانه انتقال به نقطه دیگر منتشرشده و در آن نقطه قابل شنود باشد تاخیر انتشار گفته می شود.تاخیر انتشار به سرعت سیر امواج الکترومغناطیسی و طول مسیر بستگی دارد.

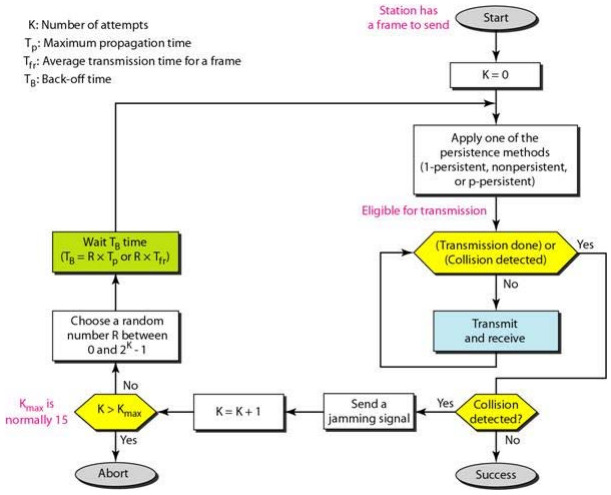
L: طول کانال برحسب متر

C: سرعت سیر امواج الکترومغناطیسی بر حسب متر بر ثانیه

تاخیر انتشار: $\tau = L/c$

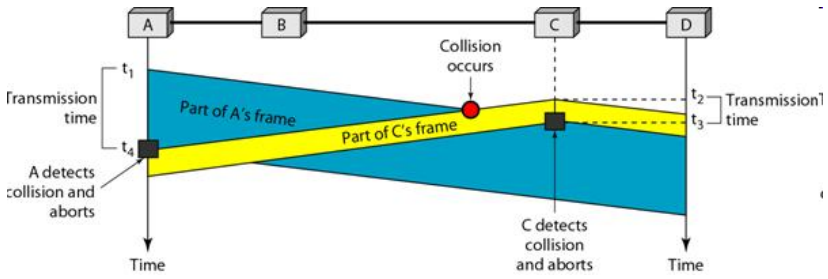
M.Zangian

مدل مرجع OSI- لایه پیوند داده



گردش کار الگوریتم CSMA/CD

مدل مرجع OSI- لایه پیوند داده



ایستگاههای ارسال کننده به محض تشخیص Colision از ارسال فریمها خودداری می کنند و با این کاردراستفاده از منابع شبکه و سیستمی بطور قابل توجهی صرفه جویی می شود.

مدل مرجع OSI- لایه پیوند داده

221

لایه پیوند داده به دو زیر لایه ،کنترل دسترسی به رسانه انتقال MAC Sublayer

که وظیفه مدیریت و کنترل دسترسی ایستگاه به رسانه انتقال را بعهده دارد و زیر لایه LLC(Logical Link Control) تقسیم می شود. که زیر لایه LLC در قسمت بالایی لایه پیوند لایه و درواقع بین لایه شبکه و زیر لایه MAC قرار دارد.

لایه پیوند داده می تواند دو نوع سرویس اتصال گرا و سرویس غیر اتصال گرا را ارائه نماید البته سرویس اتصال گرا در لایه پیوند داده hop-to-hop می باشدو می تواند بین یک ایستگاه و ایستگاه بعدی صورت گیرد . مکانیزم کنترل جریان و کنترل خطا توسط این لایه قابل انجام است که این وظایف در زیر لایه LLC تعریف شده است.

البته با توجه به اینکه برای انتقال بسته های IP ، سرویس اتصال گرا و تضمین صحت دریافت در لایه Transport انجام می شود .در برخی از پروتکلها از جمله پروتکلهای مختلف اترنت تلاش می کنند سرویس دیتاگرام عرضه کنند یعنی در لایه دو سرویس غیر اتصالگرا ارائه داده و مسائل آنرا به لایه Transport واگذار می نمایند.اما برخی از سیستمها وجوددارند که به پروتکلهایی با قابلیت های اتصالگرا در لایه ۲ نیاز دارند.

M.Zangian

مدل مرجع OSI- لایه پیوند داده

222

از اینرو برای هماهنگی پروتکلها ،IEEE پروتکلی را درزیر لایه LLC و بهمین نام (Logical Link Control) تعریف کرده که می تواند برروی پروتکلهای مختلف لایه ۲ قرار گرفته و مقتضیات لازم را برای ارائه سرویس های زیر فراهم می آورد:

۱- خدمات ارسال نامطمئن دیتاگرام

۲- خدمات دیتا گرام با تصدیق وصول

۳- خدمات ارسال اتصالگرای مطمئن

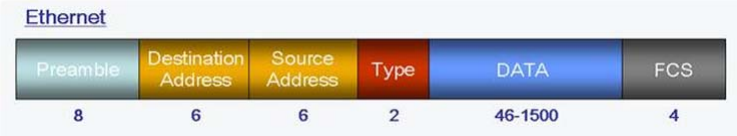
درواقع زیر لایه LLC که در قسمت بالایی زیر لایه MAC در لایه دو قرار می گیرداز طریق تعریف یک قالب و اینترفیس واحد می تواند تفاوت پروتکلهای مختلف را از دید لایه های بالاتر (لایه شبکه) مخفی نگه دارد.

M.Zangian

اترنت Ethernet

قالب فریم اترنت:

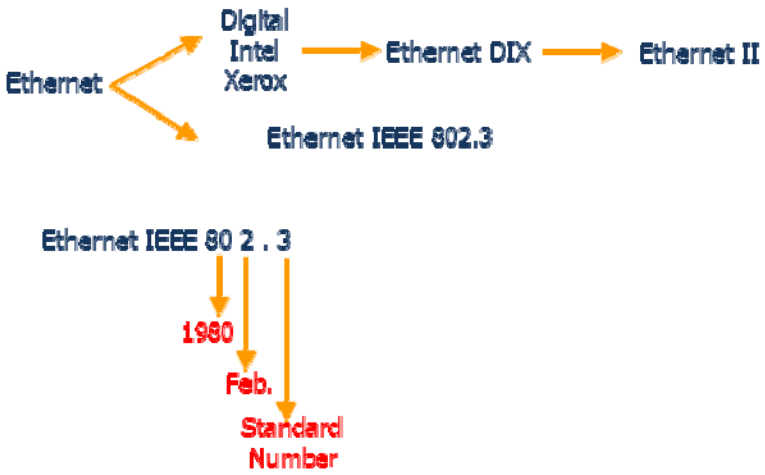
همانطوریکه قبلا گفتیم یکی از پروتکلهای مهم لایه دو پروتکل اترنت است.که امروزه از پرکاربردترین پروتکلها در شبکه های کامپیوتری است.این پروتکل در ابتدا توسط سه شرکت DEC(Digital Equipment Corporation),Intel,Xerox استاندارد سازی شد و فریم آن تحت عنوان فریم DIX بصورت زیر معرفی گردید.



استاندارد DIX یک قرارداد بین چند شرکت برای تولید تجهیزات شبکه بود اما بعدها در ابتدای دهه ۸۰ کمیته IEEE ، برای استانداردسازی وجهانی کردن اترنت اقدام نمود و نهایتا با تغییرات اندکی نسبت به فریم DIX فریم اترنت را با شماره IEEE 802.3 تصویب نمود.

M.Zangian

اترنت Ethernet



M.Zangian

قالب فریم اترنت 802.3:

استاندارد 802.3 با اندک تغییراتی نسبت به فریم DIX معرفی شدکه بعدها این تناقضات نیز برطرف شد و این دو استاندارد با هم ساز گار شدند. قالب فریم تصویب شده IEEE به شکل زیر می باشد.

فیلد Preamble:

این فیلد ۷ بایتی درواقع اطلاعات خاصی را در برندارد وبعنوان مقدمه فریم تعریف شده است که تمام ۷ بایت با الگوی 10101010 به دنبال هم آورده شده است علت انتخاب این الگو صفرویک بودن متوالی بیتهاو در نتیجه امکان سنکرون کردن فرستنده و گیرنده است.گیرنده با دریافت این بیتها خود را با ساعت فرستنده سنکرون کرده و موظف است تا پایان فریم خود را سنکرون نگه دارد.

M.Zangian

فیلد Preamble:

تفاوت این فیلد در فریم DIX در اینستکه در فریم DIX این فیلد ۸ بایتی است و در عوض فریم DIX فیلد ۱ بایتی SOF را ندارد.در قالب DIX هر ۸ بایت الگوی 10101010 را دارد.

فیلد SOF(Start Of Frame):

این فیلد مشخص کننده شروع فریم است و گیرنده می فهمد بعد از الگوی SOF فریم شروع شده و داده های آن معتبر است و باید آنرا برای پردازش مورد استفاده قرار دهد. طول SOF یک بایت است و الگوی آن بصورت 10101011 می باشد.

تا اینجا می بینیم تفاوت فریم DIX و Ethernet 802.3 در یک بیت است.

M.Zangian

Destination Address :

فیلد بعدی ۶ بایت (۴۸ بیت) است که مشخص کننده آدرس فیزیکی ایستگاه مقصد است.این فیلد در ابتدای فریم قرار گرفته است تا گیرنده با دریافت ۶ بایت ابتدای فریم تشخیص دهد این فریم متعلق به خودش است یا نه در صورتیکه فریم متعلق به یک ایستگاه باشد باید آدرس مقصد فریم با آدرس فیزیکی ایستگاه گیرنده باشد.در صورتیکه فریم متعلق به یک ایستگاه نباشد،ایستگاه می تواند از دریافت ادامه فریم صرفنظر کند.

Source Address:

این فیلد نیز ۶ بایتی است و مشخص کننده هویت (آدرس فیزیکی) تولید کننده فریم (مبدا) است.

M.Zangian

فیلد Length:

این فیلد ۲ بایت است و طول داده های معتبر جاسازی شده در فیلد DATA رابرحسب بایت مشخص می کند.

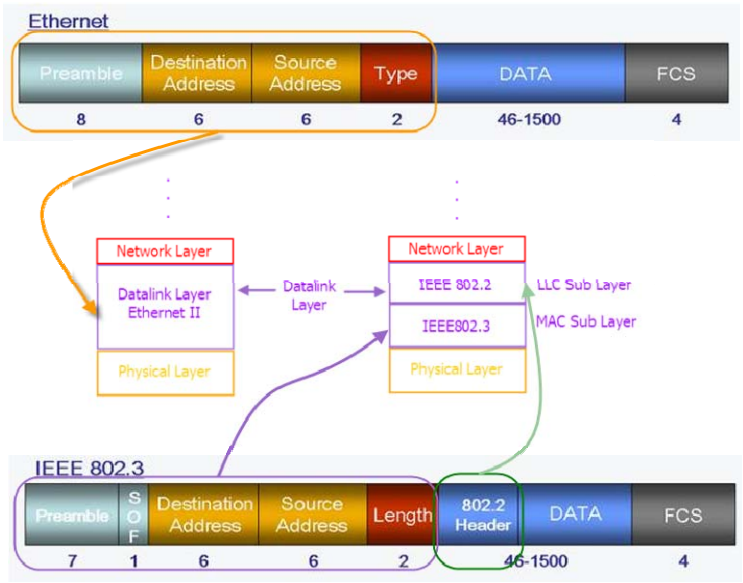
فیلد DATA:

این فیلد که همان بسته لایه ۳ است که درون فریم اترنت قرار می گیرد.این فیلد حداقل می بایست ۶۴ و حداکثر 1500 بایت باشد.علت انتخاب حداقل ۶۴ بایت برای امکان تشخیص تصادم در تجهیزات است.

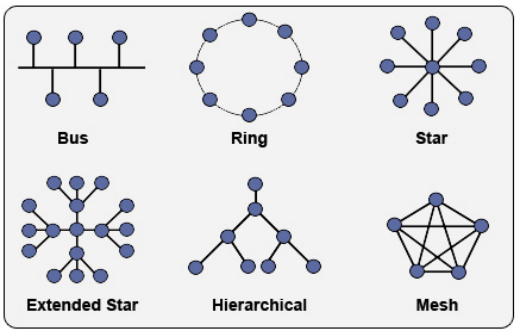
فیلد FCS(Frame Check Sequence):

این فیلد ۴ بایت است وبرای کشف خطا در فریم بکار برده می شود.

M.Zangian



M.Zangian



انواع توپولوژی LAN:

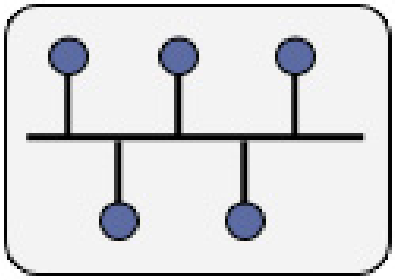
توپولوژی شبکه مشخص می کند که ایستگاههای کاری در یک شبکه مانند کامپیوترها ، پرینترهای شبکه ،سرورها و دستگاههای دیگر ،چگونه به یکدیگر مرتبط می شوند

در واقع توپولوژی شبکه ارتباط بین سیم ها ،تجهیزات و مسیرهای هدایت بسته ها را توصیف می کند.بطور خلاصه ۶ توپولوژی مختلف را می توان مطرح نمود.

M.Zangian

اترنت Ethernet

انواع توپولوژی LAN:



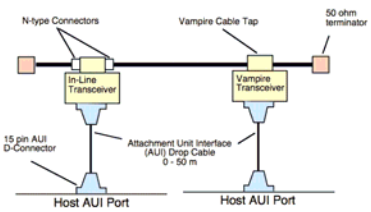
۱- توپولوژی BUS:

در این توپولوژی تمام ایستگاهها به یک کانال (کابل) مشترک تحت عنوان BUS یا Backboneمتصل می گردد.این توپولوژی ساده ،ارزان بوده و ایستگاهها باید برای دسترسی به کانال مشترک باید

با یکدیگر رقابت کنند.باید توجه نمود که

در این توپولوژی انتهای کابل بایستی Terminate شود چراکه سیگنال با رسیدن به انتهای کابل به شکل آینه ای برگشت می کند و با سیگنال اصلی برخورد می کند و باعث خراب شدن سیگنال می شود از اینرو نقاط انتهایی باید با یک مقاومت ۵۰ اهمی به زمین متصل شود تا از اثر بازگشت سیگنال جلوگیری شود.ایستگاههای کاری توسط دستگاه کوچکی به نام ترانسیور به کابل اصلی متصل می شوند.

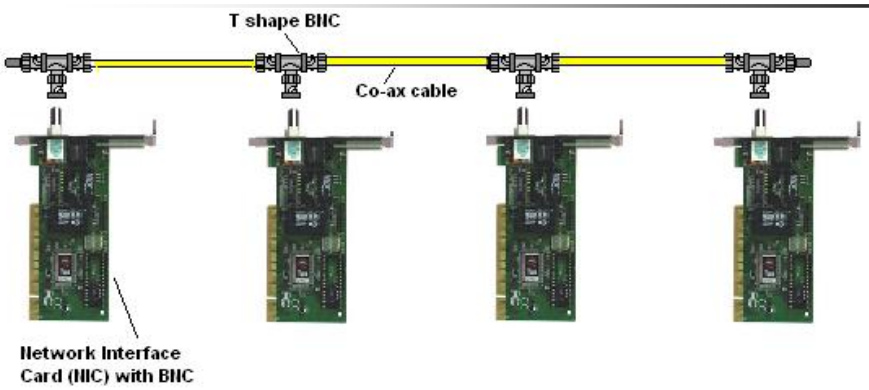
اترنت Ethernet



Thick Ethernet- 10 Base 5

50 Ohm Terminator

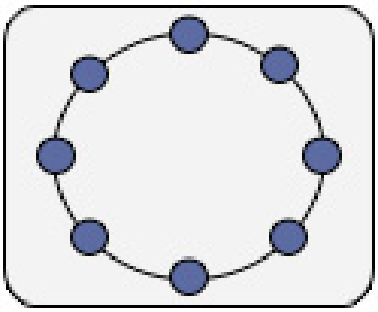
اترنت Ethernet



10 Base 2 – Thin Ethernet

M.Zangian

اترنت Ethernet



انواع توپولوژی LAN:

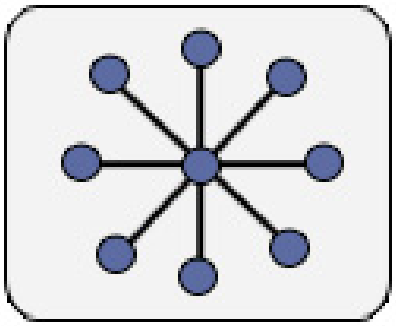
۱- توپولوژی Ring:

این توپولوژی برخلاف توپولوژی BUS نقطه انتهایی نداردبنابراین نیازی به Terminator ندارد.پیاده سازی این توپولوژی پیچیده است.فریم در حلقه ایجاد شده از یک Node به Node دیگر منتقل شده تا به مقصد برسد.

از مهمترین ویژگیهای این توپولوژی افزونگی و قابلیت اطمینان بالاتر این روش است چراکه برای رسیدن به هر Node دو مسیر وجود دارد و در صورتیکه یک مسیر با مشکل مواجه شود ارتباط می تواند از مسیر دیگر برقرار گردد.

M.Zangian

انواع توپولوژی LAN:

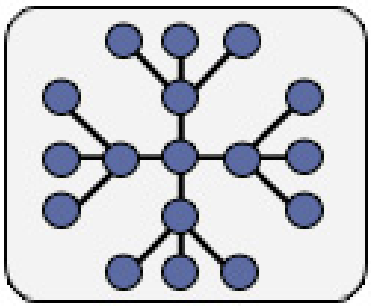


۱- توپولوژی Star:

این توپولوژی پرکاربردترین توپولوژی LAN است.پیاده سازی این توپولوژی بسیار ساده است و افزونگی و قابلیت اطمینان بالاتری نسبت به توپولوژی BUS دارد.در این توپولوژی هر Node بصورت مستقل به یک تجهیز شبکه مرکزی متصل می گردند.

در این توپولوژی حتی اگرایستگاه کاری در هر Node با مشکل مواجه شود ایستگاههای دیگر بدون هیچ مشکلی می توانند به ارتباط خود ادامه دهند.تنها در صورتیکه دستگاه مرکزی با مشکل مواجه شود کل شبکه با مشکل مواجه خواهد شد.

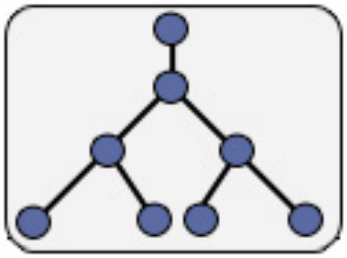
انواع توپولوژی LAN:



۱- توپولوژی Extended Star:

دراین توپولوژی قابلیتهای بیشتری نسبت به توپولوژی Star بدست می دهد.و این توپولوژی مناسب بسط و توسعه شبکه در ساختمانهای یک سازمان است.این توپولوژی از تضعیف سیگنال در اثر افزایش طول شبکه در توپولوژی Star جلوگیری می کند.

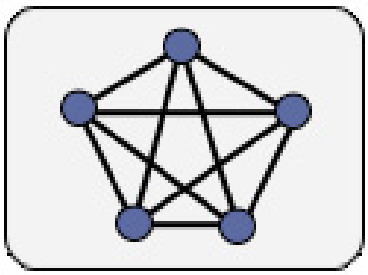
توپولوژی Star مناسب برای شبکه های کوچک و کوتاه است در صورتیکه توپولوژی Extended Star مناسب برای شبکه های بزرگ و با طول بیشتر است.در این توپولوژی نقاطی که ممکن است با مشکل مواجه شود توزیع شده و احتمال اینکه کل شبکه با مشکل مواجه شود کمتر است.



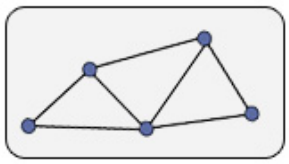
انواع توپولوژی LAN:

۱- توپولوژی Hierarchical:

این توپولوژی بیشتر شبیه توپولوژی Star است با این تفاوت که در این توپولوژی از Node مرکزی استفاده نمی شود.به این توپولوژی ، توپولوژی Tree(درخت) نیز گفته می شود.این توپولوژی همان مشکل توپولوژی Star را دارد .در صورتیکه Node اصلی در بالاترین نقطه زنجیر با مشکل مواجه شودو این Node ارتباط اصلی شبکه با شبکه های دیگر باشد، ارتباط کل شبکه با شبکه های دیگر با مشکل مواجه می شود.



Fully Mesh



Partial Mesh

انواع توپولوژی LAN:

۱- توپولوژی Mesh:

این توپولوژی به دو صورت Fully Mesh و Partial Mesh تقسیم می شود .در Fully Mesh هر Node شبکه یک مسیر با تمامی Node های دیگر دارد.در این توپولوژی افزونگی و قابلیت اطمینان تا بالاترین حد ایجاد شده است اما پیاده سازی این شبکه پیچیده و سخت است.این توپولوژی بیشتر در شبکه های WAN و بین روترها پیاده سازی می شود.

تجهیزات انتقال لایه ۲:

239

هاب(HUB):

تجهیزاتی هستند که ایستگاههای مختلف با اتصال به آن به یک BUS مشترک وصل می شوند.هابها عملیاتهای زیر را برروی یک فریم ورودی انجام می دهند:

- سیگنال ورودی را قبل از اعمال برروی کانال مشترک تقویت و باز تولید (Regenerate) می کند .تا سیگنالی که برروی کانال منتقل می شود بدون تضعیف و دارای سطوح ولتاژ و بدون نویز باشد.
- عملیات کشف تصادم (Colision Detection) وتولید سیگنال نویزگونه JAM در صورت تشخیص تصادم
- عملیات مربوط به ترانسیور که در شبکه های BUS دیدیم برعهده HUB قرار داده شده است.یعنی خطوط ارسال و دریافت را جداگانه و مستقل وارد Hub شده (Full Duplex) و بعد از تقویت برروی کانال مشترک داخلی قرار می گیرد و سپس آنچه را که برروی کانال مشترک قرار دارد را بطور جاگانه برروی تمامی پورتها باز تولید و تکرار می کند.
- در صورتیکه یک ایستگاه معیوب بوده و حاوی داده های معتبر نباشد .Hub ایستگاه خراب را از مدار خارج می سازد.

M.Zangian

تجهیزات انتقال لایه ۲:

240

هاب(HUB):

Hub ها قیمت بسیار پایینی دارندواز هوش پایینی برخوردارندو در واقع تنها لایه ۱ مدل OSI را می توانند درک کنند وهر کامپیوتر متصل به هاب تمام بسته هایی را که کامپیوترهای دیگر به Hub می فرستند را می تواند دریافت کند.(از لحاظ امنیتی در سطح بسیار پایینی است.)

در هاب تصادم وجود دارد چون ایستگاهها در درون Hub برروی یک کانال مشترک قرار می گیرند .الگوریتم CSMA/CD در شبکه هایی که از Hub استفاده می کنند پیاده سازی می شود.

معمولا برروی Hub ها یک چراغ نارنجی رنگ به نام Colision وجود دارد که در صورت تشخیص تصادم چشمک می زند و هر چه ریتم آن سریعتر باشد یعنی تصادم بیشتری صورت گرفته است.

بدلیل اینکه Hub از یک کانال مشترک بین ایستگاههای مختلف استفاده می نماید به هیچ عنوان مناسب شبکه های بزرگ(بیش از ۸ ایستگاه) نیست .چراکه تصادم به حدی بالا می رود که عملا ارسال داده ها را بسیارکند و یا غیر ممکن می سازد.

M.Zangian

تجهیزات انتقال لایه ۲:

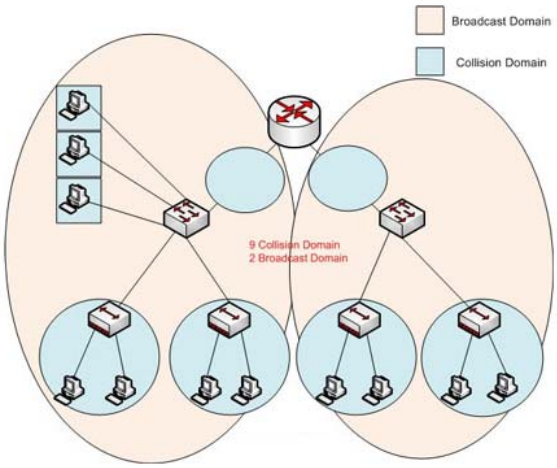
حوزه تصادم (Colision Domain)

حوزه تصادم ،تمام ایستگاههایی که به یک کانال مشترک متصلندو به روش CSMA/CD در تصاحب کانال با یکدیگر رقابت میکنند حوزه تصادم می گویند بعنوان مثال اگر حوزه تصادم ۱۶ باشد یعنی ۱۶ ایستگاه برای دسترسی به کانال مشترک با هم رقابت می کنند .هر چه حوزه تصادم شامل ایستگاههای بیشتری باشد احتمال وقوع Colision بیشتر است وما مایلیم تعداد ایستگاههای هرحوزه تصادم در کوچکترین مقدار خود یعنی ۱ باشد. بعبارت دیگر مایلیم تعداد حوزه های تصادم مستقل بیشتر شود.

حوزه پخش فراگیر (Broadcast Domain)

تمام ایستگاههایی که به یک کانال مشترک گوش می کنندو میتوانند بسته های Broadcast را دریافت کنند برروی یک حوزه پخش فراگیر واقع هستند.

تجهیزات انتقال لایه ۲:



Colision Domain و Broadcast Domain در یک شبکه فرضی

تجهیزات انتقال لایه ۲:

243

یک Hub ، یک Colision Domain ویک Broadcast Domain دارد.
یک سوئیچ بدون VLANمتعدد یک Broadcast Domain وبه ازای هر پورتش یک Colision Domain دارد.
یک سوئیچ با VLAN به تعداد VLAN هایش Broadcast Domain و به تعداد پورتهایش Colision Domain دارد.

توجه :تعداد ایستگاههای یک Colision Domain با تعداد Colision Domain در یک شبکه مفاهیم متفاوتی دارد

M.Zangian

تجهیزات انتقال لایه ۲:

244

سوئیچ لایه ۲:

این سوئیچها قابلیت های بسیار بالاتری نسبت به هاب دارند.این تجهیزات می توانند فریم اترنت را بفهمندو قابلیت یادگیری آدرس را دارند.عملیاتی که یک سوئیچ انجام می دهد عبارتست از:

- هر ایستگاه دو لینک مستقل ومجزا برای ارسال و دریافت با سوئیچ دارد.چون هیچگونه کانال اشتراکی وجود ندارد مسئله تصادم در سوئیچها وجود ندارد بنابراین ارسال همزمان ایستگاهها امکانپذیر است
- در ورودی و خروجی هر پورت بافر وجود دارد.
- سوئیچ ،آدرس مبدا و شماره پورتی که فریم دریافت شده بهمراه شماره VLAN پورت ورودی را در صورتیکه در جدول محلی (MAC Address Table) وجود نداشته باشد .برای شناسایی بعدی ثبت می کند (عملLearning).

M.Zangian

تجهیزات انتقال لایه ۲:

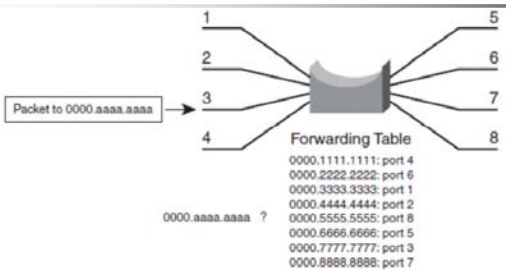
سوئیچ لایه ۲:

•پس از انتقال فریم به بافر ورودی (Ingress Queues) سوئیچ آدرس مقصد فریم، استخراج شده و در درون یک جدول محلی جستجو می شود (CAM Table) تا پورتی که ایستگاه مقصد به آن متصل شده است پیدا شود. سپس از طریق یک Backplane پرسرعت فریم به بافر خروجی (Egress Queues)پورت مقصد منتقل می شود(عمل Forwarding).

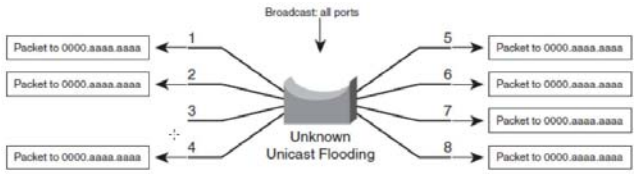
• در صورتیکه آدرس مقصد در جدول محلی وجود نداشته باشد و سوئیچ نداند که مقصد به کدام پورت متصل است .فریم را برروی تمامی پورتهایش بغیر از پورت مبدا ارسال می کند.(ارسال به تمام پورتها بصورت UniCast) تا ایستگاهی که بسته برای آنست پاسخ بدهد که در این صورت آدرس آن و پورت متصل به آن چون در مبدا قرار می گیرد ثبت می شود و در مراجعات بعدی از آن استفاده می نماید. به این عمل، Unknown UniCast Flooding گفته می شود.

•سوئیچ در دوحالت یک فریم ورودی را Broadcast می نماید.یکی حالتی که آدرس مقصد یک آدرس پخش همه گیر باشد.FF-FF-FF-FF-FF-FF و دیگر اینکه اطلاعی در باره پورتی که مقصد به آن متصل است نداشته باشد.در اینصورت فریم برروی همه پورتها بغیر از پورت ورودی بصورت Unicast ارسال می شود.

تجهیزات انتقال لایه ۲:



زمانیکه مقصد یک فریم در جدول MAC Address (CAM) یافت نشود.



قراردادن فریم در بافر خروجی تمام اینترفیس ها بغیر از اینترفیس ورودی در صورتیکه مقصد در جدول CAM وجود نداشته باشد. (Unknown UniCast Flooding)

تجهیزات انتقال لایه ۲:

247

نکته:

سوئیچها عمل

Learning

(یاد گرفتن MAC-Address ها) را براساس

Source MAC Address

فریم ورودی انجام می دهندو عمل

Forwarding

هدایت بسته ها به سمت مقصد

را بر اساس

Destinatiopn MAC Adress

فریم ورودی انجام می دهند.

M.Zangian

تجهیزات انتقال لایه ۲:

248

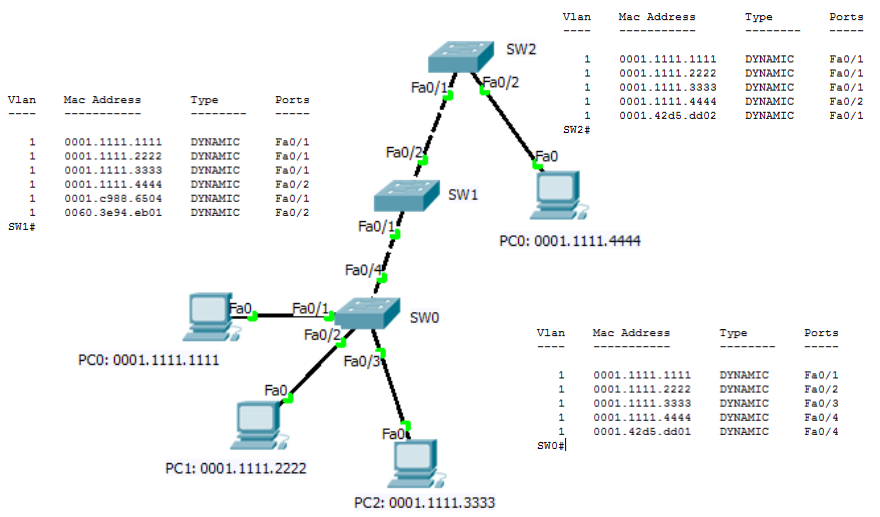
نکته:

در صورتیکه یک پورت سوئیچ غیرفعال گردد و یا ایستگاه کاری متصل به آن از آن جدا گردد . رکوردویا رکوردهای Learn شده مربوط به پورت از جدول CAM حذف می گردد.

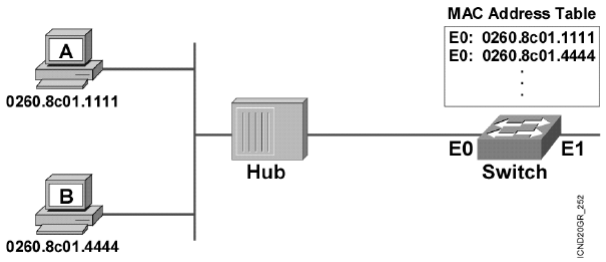
در صورتیکه آدرس MAC ثبت شده در جدول CAM ، در پورت دیگری از سوئیچ Learn شود،رکورد ثبت شده قبلی حذف می گردد.(یک MAC مشابه نمی تواند همزمان به دو پورت مختلف سوئیچ متصل گردد.)

M.Zangian

تجهیزات انتقال لایه ۲:



تجهیزات انتقال لایه ۲:



در شکل بالا یک سوئیچ توسط یک HUB به دو ایستگاه متصل است ،(دو ایستگاه به یک سگمنت سوئیچ متصل است.) همانطوریکه قبلا گفتیم Hub با دریافت هر فریم آنرا برروی تمامی پورتها غیر از پورت ورودی باز پخش می کند. بنابراین اگر ایستگاه A بخواهد فریمی را برای ایستگاه B بفرستد ، این فریم به سوئیچ هم خواهد رسید از آنجاییکه در تبادل اطلاعات قبلی سوئیچ MAC آدرس ایستگاههای A و B را در جدول MAC Address خود دارد می داند که هر دو ایستگاه برروی یک سگمنت سوئیچ است ، بنابراین فریم دریافتی را حذف می کند و به سگمنتهای دیگر منتقل نمی کند به این عمل Filtering گفته می شود.

تجهیزات انتقال لایه ۲:

همانطورکه در مبحث سوئیچ گفتیم سوئیچها با دریافت یک فریم آدرس Source را به همراه اطلاعات مربوط به پورت ورودی و نیز VLAN پورت ورودی در جدول MAC Address یا جدول CAM خود نگهداری می کند .علاوه بر این ، سوئیچ یک زمانسنج را برای این اطلاعات در نظر می گیرد که به آن Hold Time یا Aging Time گفته می شود. این زمان بصورت نزولی کاهش یافته تا به صفر برسد.در صورتیکه تا صفر شدن زمان Aging بسته دیگری با همان Source و همان پورت وارد شود ، Aging Time مجددا با مقدار پیش فرض مقدار دهی می گرددودر غیر اینصورت با صفر شدن Aging Time اطلاعات مورد نظر از جدول پاک می شود.به این عمل سوئیچ ، Aging گفته می شود.

عمل Aging سوئیچ ازپر شدن بافر سوئیچ از ایستگاههایی که برای مدت طولانی به ارسال اطلاعات نمی پردازند جلوگیری می کند.

در سوئیچهای قریمی تر سیسکو بدلیل محدود بودن حافظهCAM ، Aging Time برابر 5 دقیقه یا ۳۰۰ ثانیه بود.

تجهیزات انتقال لایه ۲:

سوئیچ لایه ۲:

- اگر هر پورت تنها به یک ایستگاه متصل باشد هیچ رقابتی برای دسترسی به کانال وجود نداردوحوزه تصادم در سوئیچها (Colision Domain) ۱ است و هیچ بخشی از پهنای باند کانال تلف نخواهد شد.(یعنی یک ایستگاه در هر حوزه تصادم شرکت دارد.)
- قالب فریم اترنت برای سوئیچها هیچ تفاوتی با اترنت ندارد بنابراین ضمن حفظ سازگاری با تجهیزات هاب کارایی شبکه به نحو چشمگیری افزایش می یابد.
- سوئیچها می توانند در دونوع متقارن Symmetric و نامتقارن Asymmetric پیاده سازی شوند. در سوئیچهای متقارن سوئیچ تنها قادر است عمل سوئیچینگ را بین پورتها و ایستگاههای با نرخ ارسال یکسان انجام دهد .در صورتیکه در سوئیچهای Asymmetric فریمها را می توان برروی پورتهایی که سرعت یکسانی ندارند نیز ارسال نمود.بعنوان مثال پورتهای با سرعت 100Mbps می توانند با تجهیزات با سرعت 10Mbps نیز ارتباط برقرار کنند.

تجهیزات انتقال لایه ۲:

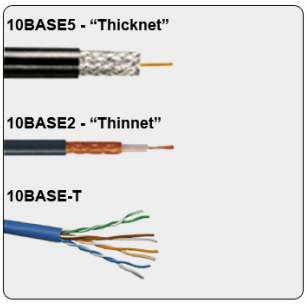
تعریف

به عمل انتقال فریم ورودی یک پورت به بافر خروجی پورت مقصد عمل سوئیچینگ می گویند.

تجهیزات انتقال لایه ۲:

اتصال ایستگاهها به سوئیچ:

اترنت در طول تکامل خود از کابلهای متفاوتی برای ارتباط ایستگاهها با یکدیگر استفاده کرد. کابلهای کواکسیال قطور تا نازک و تکامل آن به سمت کابلهای شبکه امروزی که بصورت ۴ زوج بهم تابیده (Twisted Pair) همه متناسب با توپولوژی و افزایش سرعت انتقال تکامل یافته اند. هر چند مراحل تکامل محیط های انتقال بحث مفصلی را می طلبد، دراینجا با آخرین و متداولترین این محیط ها آشنایی مختصری پیدا خواهیم کرد.



Cable	Transfer Rate	Max. Length	Connector used
Thinnet	10 Mbps	185 meters	BNC
Thicknet	10 Mbps	500 meters	Vampire Tap
Cat 3 UTP	10 Mbps	100 meters	RJ-45
Cat 5 UTP	100 Mbps	100 meters	RJ-45
Cat 5e UTP	1 Gbps	100 meters	RJ-45
Cat 6 UTP	1 Gbps	100 meters	RJ-45
Fiber	1+ Gbps	Over 2 km	SC, ST, LC

تجهیزات انتقال لایه ۲:

انواع مختلف پورتهای اترنت:

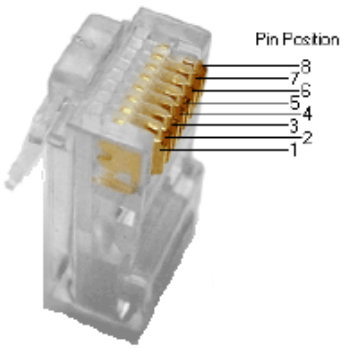
۱- پورتهای لینک مسی Copperlink (به این پورتها Electrical نیز می گویند.)

۲- پورتهای فیبر نوری Fiber(به این پورتها Optical نیز می گویند)

۳- پورتهای بی سیم(Wireless)

تجهیزات انتقال لایه ۲:

معمولترین پورتهای روی یک سوئیچ پورتهای copper link هستند این پورتها بصورت ۸ کنتاکت مسی (پوشیده شده با لایه نازکی از طلا) سیگنالها را از کابلهای ۴ زوجی (۸ رشته ای) به درون تجهیزات منتقل می کند. اتصال کابل شبکه به این پورتها توسط یک سوکت RJ45 امکانپذیر می گردد.



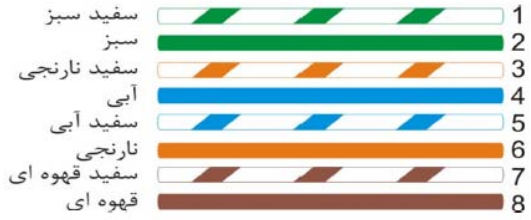
سوکت Rj45 - شبکه

آچار شبکه Network Crimp

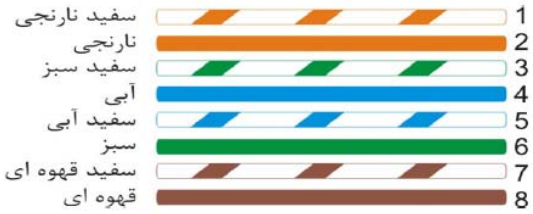
تجهیزات انتقال لایه ۲:

استاندارد رنگ بندی در کابلهای شبکه :

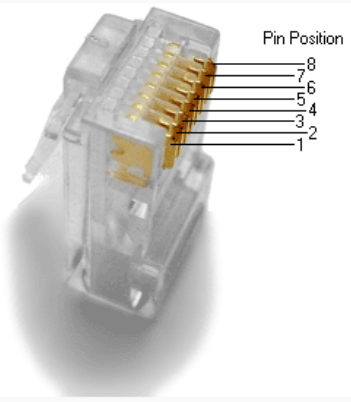
استاندارد:EIA/TIA 568 A



استاندارد:EIA/TIA 568 B

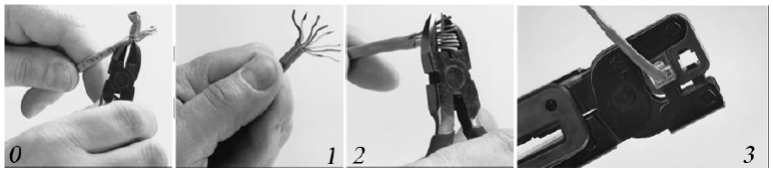


تجهیزات انتقال لایه ۲:

T568A Color	T568B Color	Pins on plug face (socket is reversed)
white/green stripe	white/orange stripe	
green solid	orange solid	
white/orange stripe	white/green stripe	
blue solid	blue solid	
white/blue stripe	white/blue stripe	
orange solid	green solid	
white/brown stripe	white/brown stripe	
brown solid	brown solid	

مقایسه رنگ بندی دو استاندارد

تجهیزات انتقال لایه ۲:



مراحل سوکت زنی کابل شبکه

تجهیزات انتقال لایه ۲:

همانطوریکه در Workshopها دیدیم تجهیزات شبکه به دو دسته DCE و DTE تقسیم می شوند .تجهیزات DCE(Data Comminucations Equipment) Data Forwarder هستند وجهت انتقال داده و یا سیگنال مورد استفاده قرار می گیرند.در مقابل DTE(Data Terminal Equipment)، Data Generator هستند.

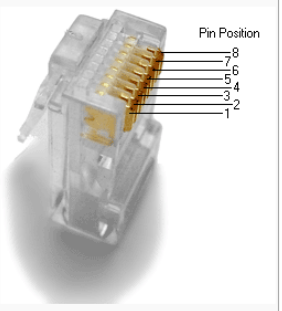
کامپیوتر ، روتر تجهیزات DTE محسوب می شوند.درمقابل سوئیچها و مودمها تجهیزات DCE هستند.در اینجا می خواهیم ببینیم تجهیزات DCE و DTE چگونه به یکدیگر مرتبط می شوند.

اگر دو تجهیز از یک نوع باشند یعنی هر دو DTE و یا DCE باشندباید به کابل Cross به یکدیگر متصل شوند.

اگر دوتجهیز دونوع متفاوت باشند یعنی یکی DTE و دیگری DCE باشد.از کابل Straight (Direct) استفاده می شود.

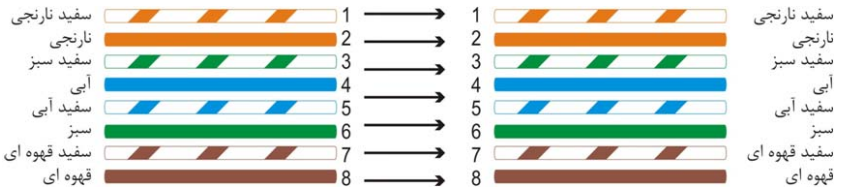
تجهیزات انتقال لایه ۲:

Two pairs crossed, two pairs uncrossed
10BASE-T or 100BASE-TX crossover

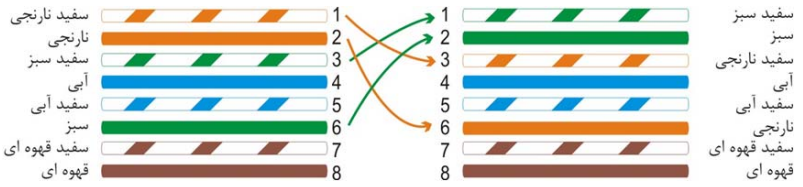
Pin	Connection 1: T568A			Connection 2: T568B			Pins on plug face
	signal	pair	color	signal	pair	color	
1	Bl_DA+	3	white/green stripe	Bl_DB+	2	white/orange stripe	
2	Bl_DA-	3	green solid	Bl_DB-	2	orange solid	
3	Bl_DB+	2	white/orange stripe	Bl_DA+	3	white/green stripe	
4		1	blue solid		1	blue solid	
5		1	white/blue stripe		1	white/blue stripe	
6	Bl_DB-	2	orange solid	Bl_DA-	3	green solid	
7		4	white/brown stripe		4	white/brown stripe	
8		4	brown solid		4	brown solid	

رنگ بندی کابلCross-Over

تجهیزات انتقال لایه ۲:



شبکه از نوع Straight Patch Cord



شبکه از نوع Cross Patch Cord

تجهیزات انتقال لایه ۲:

نوع دیگر پورتهای سوئیچ پورتهای Optical یا پورتهای نوری هستند.این پورتها ممکن است بصورت ماژولار و یا بصورت ثابت برروی سوئیچ متصل باشند. در نوع ثابت سیستم دریافت و ارسال بصورت فیبر برروی بدنه سوئیچ ثابت است در حالیکه در نوع ماژولار ، این سیستم بصورت یک ماژول جداگانه در محل های خاصی که برای این منظور ساخته شده است نصب می شود.

محل نصب ماژول GBIC

تجهیزات انتقال لایه ۲:

ماژول فیبر نوری GBIC

ماژول فیبر نوری SFP(Mini GBIC)

SFP:Small Form-factor Pluggable

GBIC:Giga Bit Interface converter

هر ماژول دو محل اتصال یکی برای Send(Tx) و دیگری برای Receive(RX) دارد

برای اتصال دو سوئیچ به یکدیگر می بایست Send یک ماژول به Recieve ماژول دیگر متصل شود در غیر اینصورت ارتباط برقرار نخواهد شد.

انواع سوئیچ لایه ۲

انواع سوئیچ لایه ۲:

1.Stored And Forward

2.Cut-Throught:

3.Fragment Free

4.Adaptive Switch

انواع سوئیچ لایه ۲

انواع سوئیچ لایه ۲ از نظر هدایت فریمها:

مکانیزم هدایت در سوئیچهای Stored And Forward:

1. ابتدا یک فریم بطور کامل به درون بافر ورودی از پورت مبدا منتقل می شود(Store)
2. کد کشف خطای فریم بررسی و در صورت عدم صحت و سلامت فریم ،بلافاصله فریم حذف شده و نادیده گرفته می شود و در وصورت سالم بودن فریم مرحله بعدی دنبال می شود.
3. فیلد آدرس مقصد (Destination Address) از فریم استخراج شده و درون یک جدول محلی (MAC Address Table) جستجو می شود.تا مشخص شود ایستگاه مقصد به کدام پورت متصل است.
4. فریم از طریق یک Backplane سریع از بافر ورودی پورت مبدا به بافر خروجی پورت مقصد منتقل می گردد .
5. فریم از درون بافر خروجی به صورت سریال برروی لینک مقصد ارسال می گردد.

سرعت انتقال فریمها برروی Backplane چند ده ویا چند صد برابر سرعت ارسال داده ها برروی کانال است .که تحت عنوان Backplane Through put در مشخصه فنی سوئیچها ثبت می شود.

انواع سوئیچ لایه ۲

مکانیزم هدایت در سوئیچهای Cut-Throught:

۱. به محض دریافت شش بایت اول از فریم که حاوی ۴۸ بیت آدرس مقصد است ،عملیات جستجو برای پیدا کردن پورت مقصد آغاز می گردد.

۲. بلافاصله پس از پیدا شدن پورت مقصد ،داده ها برروی پورت خروجی منتقل می شود و این درحالیست که دریافت مابقی فریم از پورت ورودی در جریان است.(اگر بتوان از زمان جستجو آدرس مقصد در درون جدول محلی صرفنظر کرد،تاخیر بین ورود و خروج فریم معادل ۶ بایت یا همان ۴۸ بیت خواهد بود.

نکته ۱: در صورتیکه در سوئیچای Cut-Through پورت مقصد مشغول باشد فریم در بافر منتظر شده و تا آزاد شدن پورت در صف قرار می گیرد.

نکته ۲: در سوئیچهای Cut-Throght فریم ورودی از نظر صحت بررسی نخواهد شد و سوئیچ هیچ وظیفه ای در برابر دریافت قریمهای خراب ندارد.

این نوع سوئیچ ها بیشتر در سطح Core که احتیاج به سرعت در Forward فریم داریم مورد استفاده قرار می گیرند.این سوئیچ ها تاخیر (Latency) کم و نیز قابیلیت اطمینان (Reliability) پایین دارند.

M.Zangian

انواع سوئیچ لایه ۲

مکانیزم هدایت در Fragment Free:

1. سوئیچ اجازه میدهد ۶۴ بایت اول (۵۱۲ بیت) فریم به با فر وارد شود.این ۶۴ بایت کلیه سرآیندهای اولیه را در بر می گیرد(سرآیند اترنت ، TCP،IP) . سوئیچ ایت ۶۴ بایت را برای تشخیص رخداد Colision بررسی می کند در صورتیکه فریم دچار Colision شده باشد می بایست در این ۶۴ بایت تاثیر بگذارد.در وصرت وجود اشکال فریم دورریخته می شود در غیر اینصورت عمل جستجو برای یافتن پورت خروجی در جدول محلی آغاز می شود. بررسی کامل فریم از نظر وجود خطا (CRC Check) در سوئیچ صورت نمی گیردو در مقصد انجام خواهد شد.
2. پس از پیدا شدن پورت مقصد ،فریم از طریق پورت خروجی ارسال می شود.

M.Zangian

انواع سوئیچ لایه ۲

Adaptive Switch:

در این نوع سوئیچها در ابتدا سوئیچ بصورت Cut-Through شروع به Forward فریمها می نماید.و در صورتیکه میزان Error در یک پورت بالا رود سوئیچ به مود Store-and-Forward سوئیچ می کند. این نوع سوئیچ مزیت های سوئیچ Cut-Through و Stored- And- Forward را باهم در اختیار قرار میدهد.

از نظر سرعت: Cut-Through>Fragment Free>Store and Forworad

از نظر قابلیت اطمینان: Store and Forworad>Fragment Free>Cut-Through

سوئیچ لایه ۲

Auto Negotiation:

پروسه ای در لایه فیزیکی است که در آن دو اینترفیس که به یکدیگر متصل می گردند،درمورد پارامترهای مشترک خود نظیر سرعت ارتباط،Duplex Mode وچگونگی Flow Control به توافق می رسند.در این پروسه پورتهایی که به یکدیگر متصل می گردند در مورد حداقل های پارامترمشترک توافق می کنند .این قابلیت در استاندارد Fast Ethernet تعریف گردید که بواسطه آن پورتها می توانند با پورتهای Fast Ethernet، Gigabit Ethernet و نیز اترنت های قدیمی تر 10 Base T ارتباط برقرار کنند.

در صورتیکه در طرف مقابل این قابلیت وجود نداشته باشدویا غیرفعال شود ،طرفی که دارای این قابلیت است می تواند سرعت خود را با طرف مقابل هماهنگ کند ولی در مورد Duplex تصوری از طرف مقابل ندارد و بنابراین بصورت حداقلی یعنی Half Duplex عمل می کند.

آشنایی با سوئیچهای Cisco:

بطور کلی سوئیچهای سیسکو در لایه های مختلف (OSI) طراحی می شوند.این سوئیچها بطور معمول لایه های ۲ ، ۳ وبعضا لایه ۴ (OSI) را پشتیبانی می کنندکه بسته به کاربردهای مختلف می بایست سوئیچ مناسب را انتخاب کرد.

سوئیچهای لایه ۲ پرکاربردترین سوئیچها هستند این سوئیچها مبتنی بر پروتکل اترنت بوده و قابلیت forward فریمهای اترنت را دارند. از اینرو اینترفیسهای (پورتها)سوئیچ همگی اترنت هستند.

پورتهای سوئیچ می توانند سرعتهای مختلفی را در اختیار قرار دهند، که بطور معمول پورتهای سوئیچ ممکن است سرعتهای 10Mbps ، 100Mbps و گاها 1000 Mbps (1Gbps)و در برخی از سوئیچهای Core تا 10GBps را پشتیبانی کنند.

10 Mbps:Ethernet(10 BaseT)	IEEE 802.3
100Mbps:Fast Ethernet	IEEE802.3u
1000Mbps:Gigabit Ethernet	IEEE802.3z;IEEE802.3ab
10000Mbps:10 Gigabit Ethernet	IEEE802.3ae

آشنایی با سوئیچهای Cisco:

انواع حافظه در تجهیزات سیسکو:

ROM:قسمتی از مدل حافظه تجهیزات سیسکو را تشکیل می دهد که ممکن است برروی یک یا چند Chip برروی برد اصلی قرار داده شود.این حافظه فقط خواندنی است و نمی توان برروی آن اطلاعاتی را نوشت.اطلاعات اولیه این حافظه توسط شرکت سازند برروی آن قرار می گیرد.از جمله اطلاعاتی که برروی این حافظه قرار می گیرد،نرم افزار Bootstrap است . Bootstrap نرم افزاری است که برای مقدار دهی اولیه (Initial) تجهیز بارگزاری IOS و شروع کار تجهیز مورد استفاده قرار می گیرد و تنها در ابتدای روشن شدن تجهیز و تا بارگزاری IOS کنترل تجهیز را در دست دارد.

Flash: این حافظه برروی ماژول Single Inline Memory Module(SIMM) قراردارد.دومی تواند از طریق اسلات *Personal Computer Memory Card International Association* نیز بصورت خارجی اضافه شود(قابل تعویض).این حافظه برای قرار دادن IOS Image تجهیز مورد استفاده قرار می گیرد . برروی این حافظه می تواند بیش از یک IOS Image نیز قرار گیرد.فایلهای سیستمی موردنیاز در این حافظه قرار می گیرد.در برخی از تجهیزات در قسمت بالایی و انتهایی این حافظه برنامه Bootstrap قرار داده می شود.

آشنایی با سوئیچهای Cisco:

RAM: حافظه RAM یک حافظه با سرعت بالاست . این حافظه زمانیکه سیستم Restart شود اطلاعات آن از بین می رود .در تجهیزات شبکه این حافظه برای نگهداری جداول (Routing Tables,MAC-Address Tables ,..) و بافرها قرار داده می شود و اصولا هر زمان نیاز به حافظه موقت باشد از این حافظه استفاده می شود.Running Config در این حافظه قرار می گیرد و با Restart شدن تجهیز پاک می شود.

NVRAM:این حافظه در تجهیزات سیسکو برای نگهداری Startup Config مورد استفاده قرار می گیرد.که در زمان روشن شدن تجهیز فایل پیکربندی از این حافظه خوانده شده و بار گزاری می شود.

آشنایی با سوئیچهای Cisco:

انواع فایل پیکربندی:

بطور کلی در تجهیزات سیسکو دو نوع فایل پیکربندی وجود دارد که در حافظه های مختلفی قرار داده می شوند.این فایلها عبارتند از :

۱- Startup Config

۲- Running Confg

Startup Config:

این فایل پیکربندی درون حافظه NVRAM قرار داده می شودو بصورت ماندگار حتی بعد از خاموش شدن تجهیز اطلاعات آن از بین نمی رود.

Running Config :

این فایل در واقع در ابتدا وجود خارجی ندارد و بصورت مقیم در حافظه RAM قرار می گیرد. زمانیکه تجهیز روشن می شود .فایل پیکربندی از Startup Config خوانده شده و بصورت یک کپی درون حافظه RAM قرار می گیرد و از آن پس هر نوع تغییراتی در پیکربندی درون این فایل موقت انجام می شود.این قابلیت که در تجهیزات سیسکو وبرخی برندهای دیگر وجود دارد چند مزیت دارد.

آشنایی با سوئیچهای Cisco:

یکی از مزیتهای این روش اینستکه ممکن است مدیر سیستم تغییراتی در پیکربندی دهدکه دسترسی به تجهیز را از دست بدهیم این مورد، بخصوص در ارتباط راه دور به تجهیز (telnet,ssh) زیاد اتفاق می افتد در اینصورت تنها راه ارتباطی اینستکه از طریق کنسول که ارتباطش بستگی به تنظیمات شبکه ندارد تنظیم انجام شده را تصحیح کنیم .اما اشکال استفاده از کنسول برای پیکربندی اینستکه حتما باید در کنار تجهیز باشیم و اگر این تجهیز در راه دور قرار داشته باشد،ناگزیریم آنرا را انتقال داده و یا خود به محل نصب تجهیز مراجعه نماییم و یا از یک متخصص شبکه کمک بگیریم که دسترسی به تجهیز داشته باشد.اما باتوجه به اینکه تغییرات نهایی در Running Config قرار گرفته است واین تنظیمات به Startup Config منتقل نشده است ، در صورتیکه سوئیچ یکبار خاموش و روشن شود تنظیمات قبلی که در Startup Config قرار دارد در Running Config قرار گرفته و مجددا ارتباط ما برقرار می گردد.پس تنها باید یک نفر غیر متخصص تجهیز را خاموش و روشن کند که کار راحتی است!

آشنایی با سوئیچهای Cisco:

البته باید توجه نمود که در صورتیکه پیکربندی کامل شد برای اینکه در صورت خاموش شدن تجهیز پیکربندی از دست نرود باید اطلاعات Running Config در Startup Confg کپی شود. اینعمل با دستورات زیر امکان پذیر است:

write memory

ویا copy running-config startup-config

POST(Power On Self Test):

وقتی یک تجهیز سیسکو روشن می شود ،تجهیز شروع به تست خود می کند.در این مرحله روترپردازنده، اینترفیسها ،حافظه ،ماژولها و قسمتهای مختلف تجهیز را تست می کند. و به تناوب LED های مربوط به پورتها روشن و یا خاموش می شوند که هر یک بسته به سوئیچ معانی خاص خود را دارد.فرآیند POST در حدود 50 تست مختلف را برای اطمینان از کارکرد صحیح تجهیز انجام می دهد.هر نوع خطایی بصورت یک پیام خطادر console قابل مشاهده خواهد بود.

آشنایی با سوئیچهای Cisco:

مراحل روشن شدن (Boot) روتر:

۱- روتر عملیات POST(Power On Self Test) را جهت تشخیص کارکرد صحیح CPU و Memory و اینترفیسها انجام می دهد.

۲- برنامه Boot Strap اجرا می شود(از ROM به RAM منتقل می شود).

۳-بررسی رجیستر Confreg واقع در NVRAM برای مشخص شدن نحوه بوت شدن.

۴- بسته به محتویات Confreg جستجو برای پیدا کردن IOS آغاز می گردد.در این حالت چند احتمال وجود داردکه در قسمت بعدی توضیح داده می شود.

۵- در صورت یافتن IOS معتبر (Valid) سیستم آنرا از حالت فشرده خارج کرده (Decompress)و بارگزاری می نماید .سیستم به جستجوی فایل پیکربندی Startup Config از دورن حافظه NVRAM می پردازد.

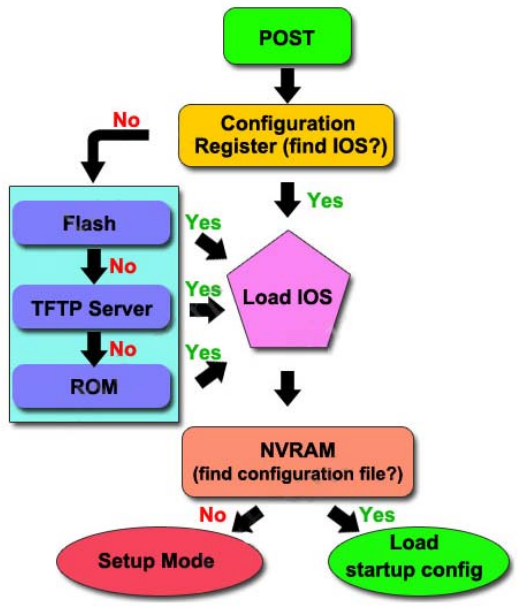
آشنایی با سوئیچهای Cisco:

مراحل روشن شدن (Boot) روتر ادامه:

۶- در صورت پیدا نکردن Startup Config معتبر روتر وارد محیط Dialog Configuration (Setup Mode) می شود در این حالت روتر پرسشی مطرح می کند که آیا می خواهید پیکربندی را از طریق Dialog انجام دهید یا خودتان پیکربندی می کنید.در صورت انتخاب Yes روتر تعدادی سئوال پیش فرض از شما می پرسد و با پاسخ به این سئوالات تجهیز شما پیکربندی اولیه می شود .در صورتیکه خود می خواهید روتر را پیکربندی نمایید به این سئوال جواب منفی دهید.

Continue with configuration dialog? [yes/no]:

در صورتیکه برای بار نخست روتر را پیکربندی می کنید نیز چنین سئوالی مطرح می شود.




```
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
```

POST

```
Self decompressing the image :
############################################################################ [OK]
            Restricted Rights Legend
```

Locate & extract IOS into RAM

مراحل POST و بارگزاری IOS در RAM

آشنایی با سوئیچهای Cisco:

احتمالاتی که ممکن است در یافتن IOS پیش بیاید:

•اگر محتویات Confreg برابر 0x2102 (باید به User Manual هر تجهیز مراجعه شود.) بدین معنی است که برای یافتن IOS به پارامترهای سیستمی Startup Config مراجعه شود. اگر تنظیمات مربوط به Boot System یاقت شود با توجه به تنظیمات آن ، IOS از مکان داده شده بارگزاری می گردد.

ولی اگر پارامترای لازم در Startup Confg یافت نشود و یا این فایل مشکل داشته باشد.جستجو برای یافتن IOS از مکانهای زیر دنبال می شود.

۱- Flash(مکان پیش فرض)

۲- TFTP Server

آشنایی با سوئیچهای Cisco:

احتمالاتی که ممکن است در یافتن IOS پیش بیاید(ادامه):

در صورتیکه فایل IOS در هیچ از مکانهای گفته شده یافت نشود،روتر بسته به مقدار Configure Register وارد مود ROM Monitor می گردد و یا از حافظه ROM ،برنامه RXboot(Mini IOS) را بارگزاری می کند (در تجهیزات قدیمی) و این برنامه Mini IOS اقدام به بارگزاری IOS اصلی می نماید . درمود ROM Monitor امکان انجام تنظیماتی برای کپی IOS بر روی روتر وجوددارد.

Operating Environment	Common Name	Stored In	Used in...
ROM Monitor	ROMMON	ROM	Old and new routers
Boot ROM	RxBoot, boot helper	ROM	Only in older routers

آشنایی با سوئیچهای Cisco:

283

درجدول روبرو بیتهای مهم کنترلی رجیستر Configure Register نشان داده شده است .

نکته: در (برخی) سوئیچهای سیسکو امکان تغییر Configure Register وجود ندارد و برای ورود به مود Boot Loader از مکانیزمهای دیگر استفاده می شود.

M.Zangian

آشنایی با سوئیچهای Cisco:

284

بیتهای 0-3 از Configure Register تحت عنوان Boot Field شناخته می شود که نحوه Boot شدن و یافتن IOS را مشخص می کند.

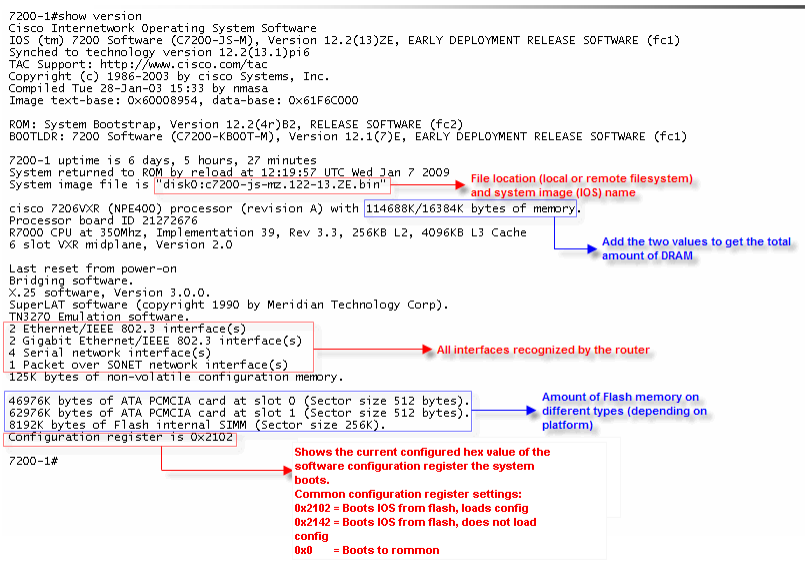
تا زمان بارگزاری IOS بسته به تنظیمات Conf.reg در صورتیکه کلید Break رابفشارید روتر مستقیما وارد مود ROMMonitor می گردد.

در محیط شبیه ساز از کلید Ctrl+C بجای Break استفاده شود.

در مورد سوئیچها برای ورود به مود ROMMonitor از مکانیزمهای دیگری استفاده می شود. بعنوان مثال در برخی از سوئیچهای دکمه ای به نام Mode برروی پنل جلویی سوئیچ وجود دارد که اگر سوئیچ خاموش گرددو این دکمه فشرده نگه داشته شود و سپس سوئیچ روشن شود وارد مود Boot Loader خواهید شد. که در این رابطه باید به User Manual دستگاه مراجعه شود.

M.Zangian

آشنایی با سوئیچهای Cisco:



مشاهده مقدار Conf Reg با استفاده از فرمان show version

M.Zangian

آشنایی با سوئیچهای Cisco:

زمانیکه یک دستگاه سیسکو نتواند IOS را پیدا نماید ، وارد مود ROM Monitor می شود در این مود می توان با استفاده از پروتکل TFTP و یک TFTP Server ، که فایل IOS برروی آن قرار گرفته است ، فایل IOS را به Flash دستگاه کپی نمود برای این کار پارامترهای TFTP می بایست به شکل زیر وارد گردد.دراین حالت ،برروی سیستمی که بعنوان TFTP Server معرفی می شود ،یک برنامه که این سرویس را ارائه دهد نصب می گرددو با استفاده از یک کابل شبکه به یکی از پورتهای سوئیچ یا روتر متصل می گردد.

```
rommon11>TFTP_FILE=c2600-i-mz.120-7.T.bin
```

```
rommon 16 > IP_ADDRESS=10.1.1.1
!--- This is the temporary IP address assigned to the router.
rommon 17 > IP_SUBNET_MASK=255.255.255.0
!--- Same as on the TFTP server.
rommon 18 > DEFAULT_GATEWAY=10.1.1.2
!--- Use the IP address of the TFTP server.
rommon 19 > TFTP_SERVER=10.1.1.2
!--- TFTP server's IP address.
rommon 20 > TFTP_FILE=c2600-is-mz.120-7.T.bin
!--- Exact name is case sensitive.
rommon 21 > TFTP_CHECKSUM=0
!--- This prevents checksum errors with earlier 2600 boot ROMs.
rommon 22 > tftpdnld
!--- This command must be lower case.
```

M.Zangian

آشنایی با سوئیچهای Cisco:

با اجرای فرمان tftpdnld پورتی که به TFTP Server متصل شده است فعال شده و عملیات انتقال فایل IOS شروع می گردد و فایل درون Flash تجهیز کپی می گردد.

با پایان عمل انتقال با استفاده از فرمان reset می توان سیستم را Restart نمود در این حال IOS جدید بارگزاری خواهد شد.

```
IP_ADDRESS: 10.1.1.1
          IP_SUBNET_MASK: 255.255.255.0
          DEFAULT_GATEWAY: 10.1.1.2
          TFTP_SERVER: 10.1.1.2
          TFTP_FILE: c2600-is-mz.120-7.T.bin

    Invoke this command for disaster recovery only.
    WARNING: all existing data in all partitions on flash will be lost!
    Do you wish to continue? y/n:  [n]:  y

    Receiving c2600-is-mz.120-7.T.bin from 10.1.1.2 !!!!!.!!!!!!!!!!!!!!!!!!!!.!!
    File reception completed.
    Copying file c2600-is-mz.120-7.T to flash.
    Erasing flash at 0x607c0000
    program flash location 0x60440000
    rommon 22 >reset
```


آشنایی با سوئیچهای Cisco:

در صورتیکه چند فایل IOS درون Flash قرار داشته باشد همواره قدیمی ترین IOS بارگزاری می شود مگر اینکه رجیستر Conf Reg بگونه ای تنظیم شده باشد که محتویات Startup Config برای بارگزاری IOS در نظر گرفته شود و در این تنظیمات ، تنظیمات مربوط به معرفی فایل IOS وجود داشته باشد.

با استفاده از فرمان boot system در مود Config می توان تنظیمات مربوط به محل قرار گیری فایل IOS را انجام داد. بسته به نوع روتر و حافظه های آن این فرمان می تواند پارامترهای مختلفی داشته باشد.معمولا توسط این فرمان فایل قرار گرفته شده در Flash بعنوان IOS معرفی می گردد.

Router(config)# boot system flash [*device:*][*filename*]

```
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#boot system flash flash:c2600-i-mz.122-28.bin
Router(config)#
```

آشنایی با سوئیچهای Cisco:

بازیابی کلمه عبور Password Recovery:

در مدیریت شبکه مواقعی پیش می آید که بعد از تنظیمات امنیتی یک تجهیز ، کلمه عبور تجهیز ،فراموش می شود . Password Recovery بدین معنی است که بدون از دست دادن تنظیمات پیکربندی یک دستگاه ، بتوان Password فراموش شده را تغییر داد.

همانطوریکه در تنظیمات Conf-reg گفته شد می توان این رجیستر را بگونه ای تنظیم نمود که سیستم بعد از boot شدن محتویات NVRAM را نادیده بگیرد.

می دانیم تنظیمات مربوط به کلمه عبور در startup-config قرار گرفته و بصورت یک فایل در NVRAM ذخیره می شود، بنابراین زمانیکه سیستم NVRAM را نادیده بگیرد ، بنابراین تصور می نماید که فایل config وجود ندارد و وارد مود setup می شود.

نکته: تنها زمانی می توان Password Recovery را انجام داد که این قابلیت در تجهیز غیر فعال نشده باشد.در غیر اینصورت یا باید Password را بخاطر آورد و یا دسترسی به تجهیز باعث از دست دادن اطلاعات پیکربندی موجود در تجهیز خواهد شد.

M.Zangian

آشنایی با سوئیچهای Cisco:

اما می خواهیم فرآیند بازیابی کلمه عبور را بگونه ای انجام دهیم که اطلاعات پیکربندی تجهیز از بین نرود و تنها کلمه عبور را تغییر دهیم .مراحلی که برای این منظور می بایست انجام شود به صورت زیر قابل بیان است.

۱- برای بازیابی کلمه عبور می بایست دسترسی فیزیکی به تجهیز امکان پذیر باشد.

۲- از طریق پورت کنسول و بصورت سریال به تجهیز متصل شوید.

۳- تنظیمات ارتباط سریال را بصورت زیر انجام دهید:

Bits per sec : 9600
Data bits : 8
Parity : none
Stop bits : 1
Flow control : none

M.Zangian

آشنایی با سوئیچهای Cisco:

۴- تجهیز را خاموش و سپس روشن نمایید

۵- در ۶۰ ثانیه ابتدایی بعد از روشن شدن تجهیز (زمانیکه تجهیز درحال انجام فرآیند bootstrap است) کلید Break برروی صفحه کلید را بفشارید.

۶- سیستم وارد مود ROMMonitor می گرددو اعلان سیستم به شکل زیر نمایش داده می شود.

```
rommon 1 >
```

۷- با استفاده از فرمان زیر تنظیمات Conf-reg را بگونه ای انجام می دهیم که محتویات NVRAM را نادیده بگیرد.

```
rommon 1 >confreg 0x2142
```

۸- سپس با استفاده از فرمان reset ، تجهیز را ریست نمایید.

```
rommon 2 >reset
```

۹- اجازه دهید تجهیز reset شود و IOS را بارگزاری نماید.

آشنایی با سوئیچهای Cisco:

۱۰- بعد از Reset شدن، تجهیز IOS را از حافظه بارگزاری می نماید.فایل IOS بصورت Image از حافظه دریافت و از حالت فشرده خارج شده و در RAM بارگزاری می گردد.

۱۱- بدلیل نادیده گرفتن محتویات NVRAM ، تجهیز تصور می نماید که فایل پیکربندی نشده است بنابراین وارد مود setup می شود.

```
Continue with configuration dialog? [yes/no]:
```

با پاسخ منفی به پیغام تجهیز ، ویا فشردن کلیدهای ctrl+c از مود setup خارج شوید.

بنابراین حرف n را وارد کرده و وارد مود User Exec Mode شوید.

۱۲- با وارد کردن فرمان enable وارد مود Priviledge شوید.

آشنایی با سوئیچهای Cisco:

۱۳- فرمان زیر را وارد نمایید تا محتویات startup-config در running-config کپی گردد.

Router# copy startup-config running-config

با این عمل ، ما بدون کلمه عبور وارد مود Priviledge شده ایم و محتویات startup-config که پیکربندی قبلی تجهیز را در بر دارد را در running-config کپی می نماییم.

توجه نمایید بجای دستور بالا ،دستورات زیر را **هرگز** بکار نبرید. چراکه باعث ازبین رفتن محتویات فایل پیکر بندی خواهد شد.

Router# copy running-config startup-config استفاده نکنید.

ویا

Router# wr mem استفاده نکنید.

آشنایی با سوئیچهای Cisco:

۱۳- دستورات زیر را به ترتیب وارد نمایید.

Router# configure terminal

Router(config)#enable secret کلمه عبور جدید

Router(config)#config-register *0x2102*

Router(config)#end ویا ctrl +z

Router#write memory ویا copy running-config startup-config

آشنایی با سوئیچهای Cisco:

غیر فعال کردن امکان Password Recoveryدر تجهیزات:

در صورتیکه در یک سوئیچ سرویس Password Recover غیر فعال شود دیگر نمی توان عملیات Password Recovery را انجام داد. این بدین معنی نیست که دیگر تجهیز غیر قابل استفاده است بلکه بدین معنی است که تنها زمانی می توانید از تجهیز استفاده نمایید که محتویان پیکربندی قبلی تجهیز پاک گردد.

با استفاده از فرمان زیر می توان Password Recovery را در یک تجهیز غیر فعال نمود:

1. Router> enable
2. Router# configure terminal
3. Router(config)# no service password-recovery

و برای استفاده از امکان Password Recovery از فرمان زیر استفاده می کنیم که بصورت پیش فرض نیز همین حالت فعال است.

Router(config)# service password-recovery

بعد از وارد کردن دستور no service password recovery نمی توان مقدار Conf.Reg را تغییر داد بنابراین قبل از این دستور Conf.Reg راتغییر می دهیم.

آشنایی با سوئیچهای Cisco:

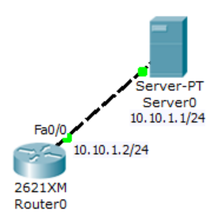

```
Initializing Hardware ...
System integrity status: 00000610
Rom image verified correctly
System Bootstrap, Version 15.3(3r)S, RELEASE SOFTWARE
Copyright (c) 1994-2013  by cisco Systems, Inc.
Current image running: Boot ROM1
Last reset cause: LocalSoft
Cisco ASR 1000 platform with 4194304 Kbytes of main memory

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
..
telnet> send brk
..

PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to the factory default
configuration and proceed [y/n] ?y

Router clearing configuration.  Please wait for ROMMON prompt...

File size is 0x17938a80
Located isr4400-universalk9.BLD_V153_3_S_XE310_THROTTLE_LATEST_20130623_234109.SSA.bin
Image size 395545216 inode num 26, bks cnt 96569 blk size 8*512
################################################################################
```

دسترسی به روتر و پاک شدن محتویات Startup-Config در صورت تایید.

```
Initializing Hardware ...
System integrity status: 00000610
Rom image verified correctly
System Bootstrap, Version 15.3(3r)S, RELEASE SOFTWARE
Copyright (c) 1994-2013  by cisco Systems, Inc.
Current image running: Boot ROM1
Last reset cause: LocalSoft
Cisco ASR 1000 platform with 4194304 Kbytes of main memory

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
..
telnet> send brk
..

PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to the factory default
configuration and proceed [y/n] ?y

Router clearing configuration.  Please wait for ROMMON prompt...

File size is 0x17938a80
Located isr4400-universalk9.BLD_V153_3_S_XE310_THROTTLE_LATEST_20130623_234109.SSA.bin
Image size 395545216 inode num 26, bks cnt 96569 blk size 8*512
##########################################################################
```

دسترسی به روتر ونیاز به یادآوری Password در صورت عدم تایید.

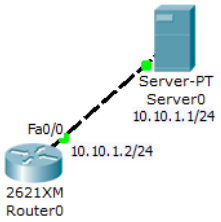

```
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int f0/0
Router(config-if)#ip address 10.10.1.2 255.255.255.0
Router(config-if)#no sh

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up

Router(config-if)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#dir ?
  WORD    Directory or file name
  flash:  Directory or file name
  nvram:  Directory or file name
  <cr>
Router#dir flash:
Directory of flash:/

    3  -rw-     5571584          <no date>  c2600-i-mz.122-28.bin
    2  -rw-       28282          <no date>  sigdef-category.xml
    1  -rw-      227537          <no date>  sigdef-default.xml

64016384 bytes total (58188981 bytes free)
Router#copy flash: tftp:
Source filename []? c2600-i-mz.122-28.bin
Address or name of remote host []? 10.10.1.1
Destination filename [c2600-i-mz.122-28.bin]?

Writing c2600-i-mz.122-28.bin....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 5571584 bytes]

5571584 bytes copied in 3.406 secs (1635000 bytes/sec)
Router#
```



پشتیبان گیری از IOS

آشنایی با سوئیچهای Cisco:


```
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int f0/0
Router(config-if)#ip address 10.10.1.2 255.255.255.0
Router(config-if)#no sh
Router(config-if)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy sta
Router#copy startup-config tftp:
Address or name of remote host []? 10.10.1.1
Destination filename [Router-confg]?

Writing startup-config....!!
[OK - 453 bytes]

453 bytes copied in 3.061 secs (0 bytes/sec)
Router#
```



پشتیبان گیری از Startup Config

پروتکل CDP:

پروتکل CDP(Cisco Discovery Protocol)

پروتکل CDP یک پروتکل لایه ۲ است که بکمک آن یک تجهیز سیسکو می تواند اطلاعاتی راجع به همسایگان خود که بصورت مستقیم به تجهیز متصل است را بدست بیاورد.

پروتکل CDP مخصوص تجهیزات سیسکو است و تجهیزات با برندهای دیگر این پروتکل را پشتیبانی نمی کنند.(از پروتکلهای خاص خود استفاده می کنند.)

تجهیزات سیسکو با استفاده از آدرس Multicast: 01-00-0c-cc-cc-cc اطلاعات خود را از طریق فریمهای CDP به تجهیزات دیگر متصل به خود ارسال کرده و در صورتیکه تجهیزات دیگر که بصورت مستقیم به آن متصل هستند پروتکل CDP را پشتیبانی نمایند به آن پاسخ می دهند.

بصورت پیش فرض فریم CDP هر ۶۰ ثانیه یکبار برروی اینترفیسهای فعالی که هدرهای Subnetwork Access Protocol (SNAP) را پستیبانی کند ارسال می گردد. از جمله لینکهایی از نوع Ethernet,PPP,Hdlc,Frame Relay,ATM,Token Ring .

پروتکل CDP:

هر تجهیز سیسکو اطلاعات دریافتی را در یک جدول برای مدت زمان معینی که بصورت پیش فرض ۱۸۰ ثانیه است (Hold Time) نگهداری می کند و با دریافت هر فریم CDP جدید اطلاعات خود را بروز کرده و زمان Hold Time بصورت مجدد set می شود. در صورتیکه زمان Hold Time برای اطلاعات یک تجهیز در جدول به پایان برسد و در این مدت اطلاعات CDP جدید دریافت نشده باشد، اطلاعات آن تجهیز از جدول CDP حذف می گردد.

CDP اطلاعات مختلفی از یک تجهیز را دراختیار همسایگان خود قرار می دهد که بسته به نسخه IOS و نوع تجهیز می تواند متفاوت باشد.

از جمله این اطلاعات می توان به نسخه سیستم عامل (IOS) ، Hostname، هر آدرس لایه شبکه نظیر IP Address ، نام پورت ارسال کننده اطلاعات ، نوع دستگاه و مدل آن ،نوع Duplex (Full/Half) لینک مورد نظرو اطلاعات دیگر اشاره کرد.

پروتکل CDP:

دستورات مرتبط با CDP:

```
Switch#show cdp
Global CDP information:
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
Switch#
```

این دستور که در Priviledge مود قابل اجراست وضعیت تنظیمات کلی CDP را نشان می دهد.

از جمله زمان پیش فرض برای ارسال فریمهای CDP ، زمان پیش فرض Hold Time که مشخص کننده طول عمر اطلاعات CDP در صورت عدم دریافت فریم CDP جدید از یک دستگاه است و نیز نسخه اطلاعات CDP ، که منتشر شده را نشان می دهد.

زمانهای پیش فرض را می توان بصورت زیر تغییر داد:(این دستورات در محیط شبیه سازی فعال نیست)

```
(config)#cdp holdTime 255
(config)#cdp timer 120
```

پروتکل CDP:

با استفاده از دستور زیر تنظیم زمان ارسال فریمهای CDP ،به حالت پیش فرض باز می گردد.(60s)

```
(config)# no cdp timer
```

با استفاده از این دستور زمان Holdtime به حالت پیش فرض تنظیم می شود.(180s)

```
(config)# no cdp holdTime
```

تعیین نسخه CDP منتشر شده

```
Switch(config)# cdp advertise-v2
```

Default CDP Configuration

Feature	Default Setting
CDP global state	Enabled
CDP interface state	Enabled
CDP timer (packet update frequency)	60 seconds
CDP holdtime (before discarding)	180 seconds
CDP Version-2 advertisements	Enabled

پروتکل CDP:

CDP بصورت پیش فرض برروی تجهیزات سیسکو فعال است . در صورت غیر فعال بودن CDP با دستور زیر CDP فعال می شود.

```
Switch(config)# cdp run
```

برای غیر فعال کردن کلی CDP از دستور زیر استفاده می شود:

```
(config)# no cdp run
```

CDP بصورت پیش فرض برروی اینترفیس های تجهیزات سیسکو فعال است . در صورت غیر فعال بودن این پروتکل برروی یک اینترفیس با استفاده از دستور زیر CDP فعال می شود:

```
Switch(config)#interface f0/2
Switch(config-if)#cdp enable
```

```
Switch(config)#interface range f0/1-24
Switch(config-if-range)#cdp enable
```

پروتکل CDP:

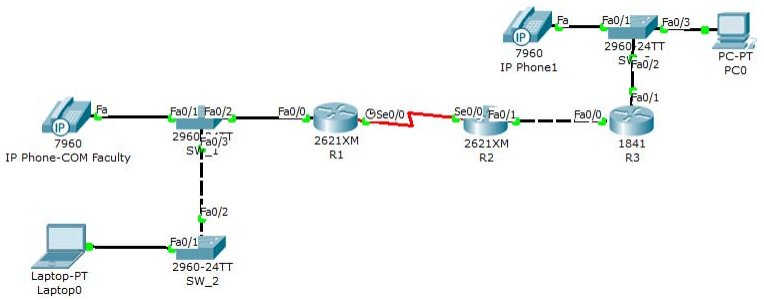
با استفاده از دستور زیر CDP برروی یک اینترفیس غیر فعال می شود:

```
Switch(config)#interface f0/2
Switch(config-if)#no cdp enable
```

با دستور زیر فهرستی از اینترفیسها که CDP برروی آنها فعال است نمایش داده می شود.

```
Router#show cdp interface
FastEthernet0/0 is up, line protocol is up
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
FastEthernet0/1 is administratively down, line protocol is down
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0/0 is up, line protocol is up
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```


پروتکل CDP:



با استفاده از دستور زیر می توان همسایگان یک تجهیز که از نوع سیسکو باشند را مشاهده نمود.

```
SW_1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID     Local Intrfce   Holdtme    Capability   Platform    Port ID
IP Phone      Fas 0/1          149           H P      7960
SW_2          Fas 0/3          149           S        2960        Fas 0/2
R1            Fas 0/2          149           R        C2600       Fas 0/0
```

پروتکل CDP:

با استفاده از دستور زیر اطلاعات بیشتری از همسایگان یک تجهیز سیسکو می توان بدست آورد.

```
SW_1#show cdp neighbors detail

Device ID: IP Phone
Entry address(es):
Platform: cisco 7960, Capabilities: Host Phone
Interface: FastEthernet0/1, Port ID (outgoing port): Switch
Holdtime: 155

Version :
P00303020214

advertisement version: 2
Duplex: full
---------------------------

Device ID: SW_2
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: FastEthernet0/3, Port ID (outgoing port): FastEthernet0/2
Holdtime: 155

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEAS
E SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

advertisement version: 2
Duplex: full
---------------------------
```

M.Zangian

پروتکل CDP:

```
Device ID: R1
Entry address(es):
  IP address : 10.10.1.254
Platform: cisco C2600, Capabilities: Router
Interface: FastEthernet0/2, Port ID (outgoing port): FastEthernet0/0
Holdtime: 155

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

advertisement version: 2
Duplex: full
```

M.Zangian

پروتکل CDP:

```
R1#clear cdp table
```

با استفاده از این دستور جدول اطلاعات CDP در یک تجهیز پاک می گردد و با دریافت اولین فریم CDP اطلاعات مجددا در این جدول قرار می گیرد.

M.Zangian

VLAN

310

Virtual Local Area Network:

VLAN یکی از پرکاربردترین و جالبترین مسائل شبکه به شمار می آید .یکی از مسائل مهمی که شبکه های بزرگ باآن مواجه هستند کنترل بسته های Broadcast در شبکه است و هرچه شبکه بزرگتر باشد این مسئله پررنگ تر می شود.علاوه براین گاهی اوقات در شبکه لازم است بدلیل مسائل امنیتی محدوده دسترسی ایستگاهها از یکدیگر متمایز شود.

بعنوان مثال فرض کنید در یک سازمان اداره حراست که معمولا از حساسیت بالایی برخوردار است ،لازم است از ایستگاههای دیگر جدا شود و دسترسی فقط محدود به پرسنل مربوط به این اداره شود.یک راه حل جداسازی فیزیکی و ایجاد شبکه پسیو مستقل است.این کار علاوه بر تحمیل هزینه های یک شبکه مستقل معایب زیادی دارد .ازجمله این معایب عبارتست از عدم توسعه پذیری شبکه و یا توسعه پذیری سخت چنین شبکه ای است.بعبارت دیگر برای افزودن یک پورت اضافه نیازمند صرف هزینه و زمان برای توسعه دادن به چنین شبکه ای است.

M.Zangian

VLAN

311

مزایای VLAN:

امنیت(Security):

VLAN ها با جداسازی منطقی پورتها ،ایستگاههای متصل به پورتها را از یکدیگر جدا کرده و دسترسی ایستگاههای غیر مجاز را به ایستگاههایی که حاوی اطلاعات حساس هستندغیر ممکن می سازد.

کاهش Broadcast Storm:

گاهی اوقات بسته های Broadcast باعث بوجود آمدن طوفانهای همه پخشی و ایجاد ترافیک در شبکه می شوند که بکمک VLAN می توان با کاهش تعداد ایستگاههای هر Broadcast Domain این اثرات را کاهش داد.

افزایش کارایی:

ایجاد VLAN ها و محدود کردن Broadcast Domain باعث کاهش ترافیکهای ناخواسته و افزایش کارایی شبکه می شود.

مدیریت بهتر شبکه:

با تقسیم بندی و سگمنت کردن یک شبکه FLAT مدیریت شبکه مشکلات شبکه به محدوده های خاصی محدود شده و از تاثیر برخی مشکلات به سگمنتهای دیگر جلوگیری می شودو در نتیجه مدیریت شبکه به مراتب آسانتر می شود.

M.Zangian

VLAN

312

Virtual Local Area Network:

اما راه حل مناسبتر و منطقی استفاده از امکانات موجود وجداسازی منطقی شبکه ها از یکدیگر است.دراین روش احتیاج به هیچگونه تغییر فیزیکی در شبکه نیست و به راحتی با پیکربندی مناسب شبکه می توان به این هدف دست یافت. البته لازمه چنین امری مدیریت پذیر بودن تجهیزات سوئیچ و پشتیبانی از تنظیمات مربوط به VLAN است.در این صورت پورتهایی از سوئیچ که در VLAN های مختلف قرار می گیرند مانند سوئیچ های مجزا عمل می کنند.

همانطوریکه در مبحث مربوط به سوئیچها نیز اشاره شد،تعداد Broadcast Domain با ایجاد VLAN ها و به تعداد VLAN های ایجاد شده افزایش خواهد یافت.

برای تعریف VLAN در یک سوئیچ دو عمل بایستی انجام شود:

۱- ایجاد VLAN

۲- قرار دادن پورتهای مورد نظر در یک VLAN

M.Zangian

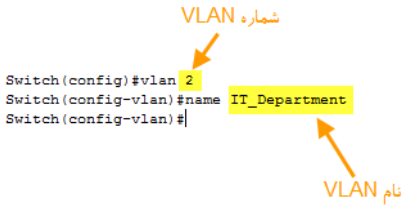
VLAN

Virtual Local Area Network:

باید توجه نمود که ممکن است در برخی موارد نیازی به اختصاص یک پورت به یک VLAN نباشد.که در ادامه مبحث در این باره بیشتر صحبت خواهیم کرد.

تعریف VLAN در سوئیچهای Cisco:

تعریف VLAN در سوئیچهای Cisco به راحتی انجام می شود.با دستورات زیر می توان یک VLAN را تعریف نمود.



در دستور بالا،ابتدا یک VLAN با شماره ۲ ایجاد شده است و در دستور بعدی یک نام برای VLAN در نظر گرفته شده است.

- در عملیات مربوط به VLAN شماره VLAN اهمیت داشته و انتخاب نام جهت ایجاد توضیحی برای VLAN مورد نظر است و تاثیری در عملیات مربوط به VLAN ندارد.

M.Zangian

VLAN

Default VLAN:

تمامی اینترفیسهای سوئیچ در ابتدا متعلق به یک VLAN به نام Default VLAN هستند. VLAN 1 بعنوان Default VLAN تعریف شده است و امکان حذف این VLAN وجود ندارد.

با استفاده از دستور زیر می توان یک VLAN ایجاد شده را حذف نمود.

Switch(config)#no vlan 2

Switch(Config)# no vlan [شماره VLAN]

علاوه بر این می بایست پورت نیز از VLAN خارج شود که در صفحات بعدی راجع به آن صحبت می کنیم.

M.Zangian

VLAN

شماره VLAN:

تعداد VLAN هایی که یک سوئیچ پشتیبانی می کند محدود بوده و در هر سوئیچ ممکن است متفاوت باشد.طبق استاندارد محدوده شماره VLAN به دو محدوده Normal Range وRange Extended تقسیم بندی می شود.طبق استاندارد IEEE802.1q شماره VLAN به 4096 ، VLAN محدود می گردد.

Normal Range:

VLAN ID در این محدوده بین 1و 1005 تعریف می شود.

VLAN ID 1 و 1002 تا 1005 بصورت اتوماتیک ایجاد می شوند و نمی توان را حذف کردو یا پیکربندی نمود.

محدوده 1002 تا 1005 برای استفاده در پروتکلهای Token Ring و FDDI رزرو شده اند.

تنظیمات این محدوده از VLAN ها در یک فایل دیتابیسVLAN ، با نام VLAN.dat ذخیره می شوند.این فایل برروی Flash Memory سوئیچ ذخیره می شود.

VLAN

Extended Range:

VLAN ID در این محدوده بین 1006و 4094 تعریف می شود.

VLAN ID 0 و 4095 توسط استاندارد IEEE 802.1q رزرو شده اند و نمی توان آنها را تغییر داد یا حذف ویا ایجاد نمود.این VLAN ها نمایش داده نمی شوند.

تنظیمات این محدوده VLAN در Running-Configuration ذخیره می شود.

برخی از دستورات و قابلیتهای سوئیچ برای این محدوده ، در دسترس نمی باشد.(مانند VTP)

- VLAN ID
  - Normal-range IDs
    - 1 – 1005
    - 1002 -1005 reserved for Token Ring and FDDI VLANs
    - 1 and 1002 to 1005 are automatically created and cannot be removed
    - Stored in the vlan.dat file in flash memory
  - Extended-range IDs
    - 1006 – 4094
    - Designed for service providers
    - Have fewer options than normal range VLANs
    - Stored in the running configur
- A Cisco Catalyst 2960 switch sup normal and extended range VLANs

VLAN

اختصاص پورت به یک VLAN:

بعد از ایجاد VLAN ممکن است بخواهیم اینترفیسهای مورد نظر را در یک VLAN قرار دهیم. برای این منظور وارد اینترفیس مورد نظر شده و ابتدا مود دسترسی را به Access تغییر می دهیم .بصورت پیش فرض یک پورت در مود Dynamic قراردارد.سپس پورت مورد نظر را در VLAN ی که قبلا آنرا ایجاد کرده ایم قرار می دهیم.

```
Switch(config)#interface fastEthernet 0/1
```
ورود به یک اینترفیس

```
Switch(config-if)#switchport mode access
```
قرار دادن پورت در مود Access

```
Switch(config-if)#switchport access vlan 2
Switch(config-if)#
```
قرار دادن پورت Fa0/1 در VLAN 2

با دستورات بالا اینترفیس Fa0/1 در VLAN 2 قرار گرفت.

در یک سوئیچ اینترفیسهایی که در یک VLAN قرار می گیرند، از پورتهای دیگر که در VLAN های متفاوتی قرار گرفته اند بصورت منطقی مجزا می شوند.

VLAN

در صورتیکه بخواهیم یک پورت را از یک VLAN خارج سازیم از فرمان زیر استفاده می نماییم:

```
Switch(config-if)#no switchport access vlan 2
Switch(config-if)#
```

در اینصورت پورت مورد نظر از VLAN مشخص شده خارج شده و در Default VLAN قرار می گیرد. با استفاده از فرمان زیر می توان اطلاعلتی در مورد VLAN شامل VLAN_ID ، نام VLAN وضعیت آن و نیز پورتهای اختصاص یافته به هر VLAN را مشاهده نمود.

```
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
2    IT_Department                     active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9
3    Engineer_Faculty                  active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

VLAN

با استفاده از دستور زیر می توان اطلاعاتی در مورد یک VLAN خاص (۲)براساس VLAN id بدست آورد:

```
Switch#show vlan id 2

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    IT_Department                    active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Switch#
```

با استفاده از دستور زیر می توان اطلاعاتی در مورد یک VLAN خاص (IT_Department) براساس نام VLAN بدست آورد:

```
Switch#show vlan name IT_Department

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    IT_Department                    active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Switch#
```

M.Zangian

VLAN

ایستگاههایی که به پورتهای متعلق به یک VLAN در سوئیچ متصلند می توانند در لایه ۲ با یکدیگر ارتباط داشته باشند .اما دیگر نمی توانند با ایستگاههای عضو VLAN متفاوت در لایه ۲ ،ارتباط برقرار کنند. در اینصورت مانند اینستکه سوئیچ به چند سوئیچ مجزا تقسیم شده است.

تا اینجا ایجاد یک VLAN را در یک سوئیچ آموختیم وتفکیک منطقی پورتها و قرار دادن آنها را در VLAN های مختلف بررسی کردیم.حال این سئوال مطرح می باشد که ممکن است ایستگاههای کاری که می خواهیم در یک مجموعه قرار گیرندو با یکدیگر ارتباط داشته باشند به یک سوئیچ متصل نباشند حال آنکه مسائلی که تاکنون مطرح شد ایجاد VLAN در یک سوئیچ بود و درشبکه های واقعی معمولا ایستگاههای کاری در شبکه توزیع شده اند و به یک سوئچ محدود نمی شوند.

سئوال: چگونه می توانیم شبکه های مجازی را در سطح سوئیچهای متعدد بوجود آوریم؟

در واقع مسئله به این صورت مطرح می شود که چگونه VLAN های هم شماره را می توان در سوئیچهای مختلف به یکدیگر مرتبط کرد؟

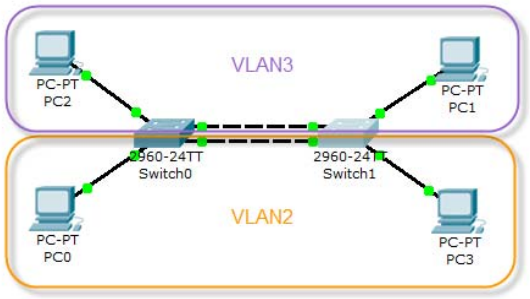
قبلا آموختیم که سوئیچها می توانند با استفاده از ارتباط یک پورت از یک سوئیچ با پورتی از سوئیچ دیگر(uplink) توسعه یا فته و ایستگاههای مرتبط به این سوئیچها به یکدیگر مرتبط شوند. اما در آنجا تمام اینترفیسهای سوئیچها در یک VLAN یعنی Default VLAN واقع بودند و ارتباطها با یک Uplink ساده امکانپذیر می گردید.در اینجا مسئله کمی متفاوت است و دیگر پورتهای مختلف سوئیچ در یک VLAN قرار ندارند.

M.Zangian

VLAN

VLAN Trunking:

همانطوریکه یادآور شدیم با استفاده از یک ارتباط uplink بین دو سوئیچ می توان ارتباط ایستگاههای متصل به آنها را امکانپذیر ساخت. بنابراین ممکن است بنظر برسد که اگر ما در دو سوئیچ uplink را از یک VLAN یکسان انتخاب نماییم VLAN ها به یکدیگر مرتبط می شوند.



اما این روش نمی تواند یک روش مناسب برای برقراری ارتباط بین VLAN های مختلف باشد چراکه به ازای هر VLAN یک Uplink مجزا نیاز داریم که با افزایش تعداد VLAN ها و نیاز به تغییرات در شبکه Passive روشی غیر منطقی و غیر فنی است.

VLAN

VLAN Trunking:

دیدیم برقراری ارتباط بین VLAN های مختلف با استفاده از uplink های مختلف روشی ناکارآمد و غیر منطقی بود بنابراین ما باید بتوانیم به طریقی ارتباط بین VLAN ها را از طریق Uplink موجود امکانپذیر نماییم یعنی تمام VLAN ها از یک Uplink استفاده نموده و در سوئیچ بسته های VLAN های مختلف به VLAN های هم شماره منتقل شود.

انتقال بسته های مربوط به VLAN های مختلف از طریق Uplink مشترک و تحویل آنها به VLAN متناظر در استانداردهای مربوط به مبحث VLAN کاملا پیش بینی شده است و تحت عنوان VLAN Trunking مطرح گردیده است.

بطور کلی در سوئیچهای Cisco از دو پروتکل برای VLAN Trunking استفاده می شود:

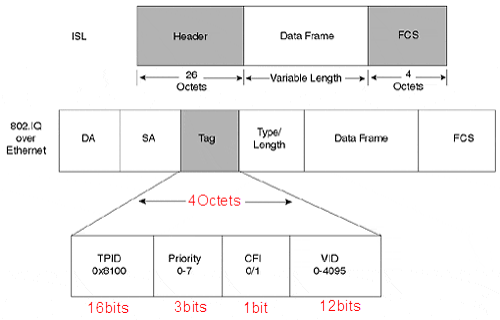
۱- پروتکلISL (Inter-Switch Link Protocol)

۲- پروتکل IEEE 802.1q

پروتکل ISL یک پروتکل اختصاصی برای Cisco است و فقط در تجهیزات سیسکو مورد استفاده قرار می گیرد .اما IEEE 802.1q یک استاندارد جهانی بوده و درتمامی سوئیچهایی که از VLANing پشتیبانی می کنند ،قابل استفاده قرار می گیرد.اگر چه هر دو پروتکل نتیجه یکسانی به همراه دارد ولی از نظر روش کاملا با یکدیگر متفاوتند.

VLAN Trunking:

در اینجا قصد نداریم به تشریح فریمهای ISL و 802.1q بپردازیم اما باید یادآور شویم این دو روش VLAN Trunking از نظر تعریف فریم کاملا متفاوت با یکدیگرند اگر چه نتایج یکسانی را ارائه دهند.در پروتکل ISL فریم اترنت درون فریم ISL کپسوله می شود.اما در پروتکل IEEE 802.1q قسمتی از فریم اترنت برای پشتیبانی از VLAN Trunking باز تعریف می شود.

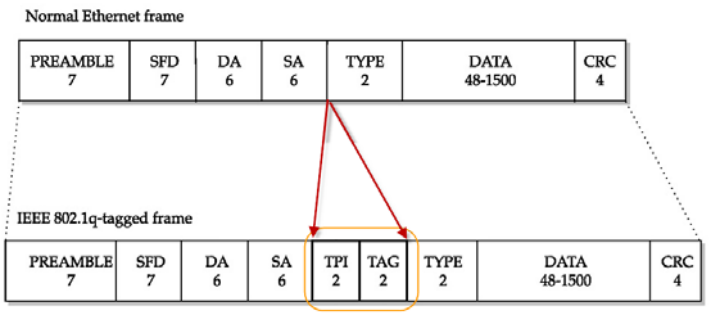


تفاوت ISL و 802.1q در VLAN Trunking

TPID(*Tag Protocol Identifier*):

این فیلد درست در جایگاه Type/Length در فریم اترنت قرار می گیردو برای فریم IEEE802.1q برابر 0x8100 می باشد.

سئوالی که پیش می آید اینستکه چگونه یک سوئیچ می تواند بین فریم معمولی اترنت و فریم اترنتی که حاوی تگ IEEE802.1q است تمایز قائل شود؟



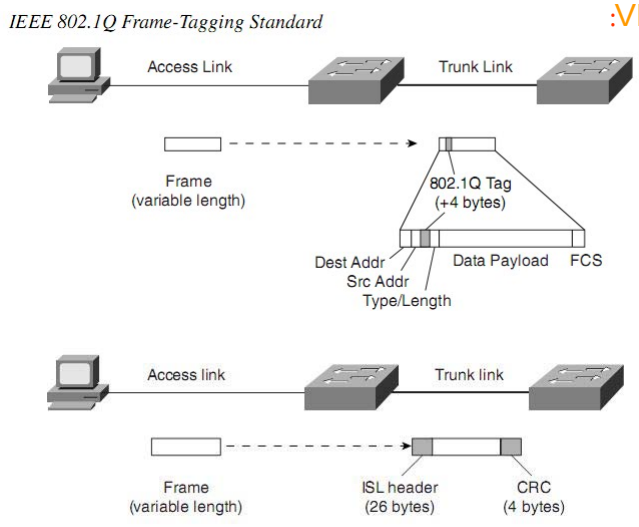
VLAN

در پاسخ به این سئوال باید گفت فیلد TPID (Tag Protocol Identifier) در فریم تگ خورده با Type/Length فیلد در فریم معمولی اترنت هر دو دو بایت هستند .اما معمولا Length در فریم اترنت کوچکتر از 1500 بایت است بنابراین براحتی سوئیچ با مقایسه مقدار در صورتیکه این مقدار کوچکتر یا مساوی 1500 باشد ، این فیلد را بعنوان Length در نظر می گیرد و اگر این فیلد مقداری بیش از 1500 باشد ، فیلد معنی Frame Type را می دهد و در استاندارد تعریف شده تمامی Frame Type ها از مقدار 0x0800 شروع می شود و اگر این مقدار برابر 0x8100 باشد ، بمعنی اینستکه این فریم یک فریم تگ خورده dot1q است.

M.Zangian

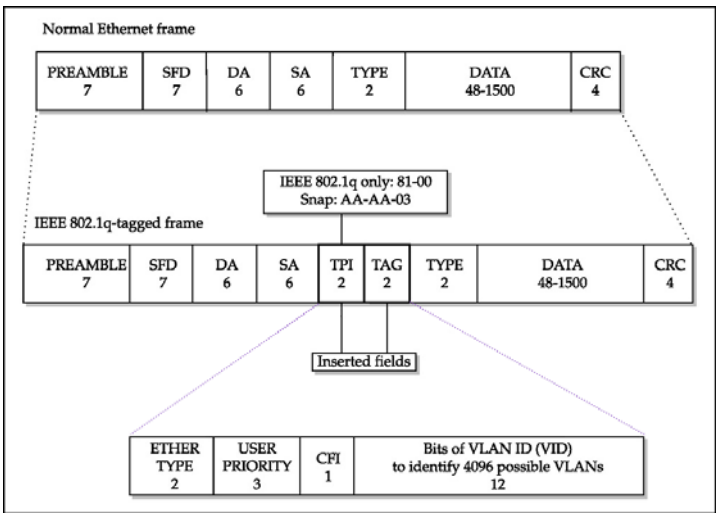
VLAN

VLAN Trunking:

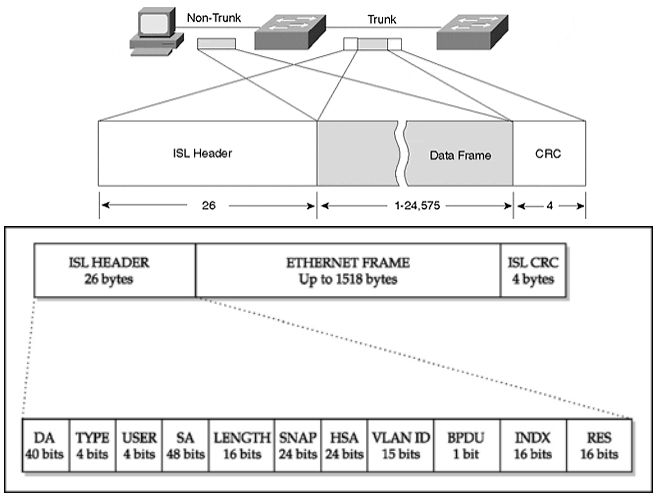


ترانک شدن لینک بین دو سوئیچ

M.Zangian



بازتعریف فریم اترنت و قراردادن تگ 802.1q



کپسوله کردن فریم اترنت در سرآیند ISL

VLAN

329

هردو روشهای VLAN Trunking ،باعث افزایش اندازه فریم می گردد.در 802.1q ، ۴ بایت و در ISL ، ۳۰ بایت (26 Bytes Header+4 Bytes Trailer) به اندازه فریم اضافه می گردد. از آنجاییکه در استاندارد 802.3 فریم های با اندازه بیش از 1518 بایت شامل:

(1500Bytes Payload+6Bytes D.A+6Bytes S.A+2 Bytes Type+4 Bytes FCS)

بعنوان خطا در نظر گرفته شده و حذف می گردد، این افزایش اندازه فریم مشکل ساز می شود از اینرو پورتهای سوئیچ از استاندارد 802.3ac استفاده می کند که از فریمهای 1522 بیت پشتیبانی می نماید.در مورد ISL هم این افزایش سایز فریم توسط سوئیچ سیسکو در نظر گرفته شده و پشتیبانی می شود.

M.Zangian

VLAN

330

802.1q VLAN Trunking:

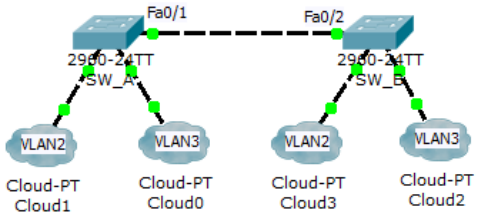
در استاندارد IEEE 802.1q فریمهای متعلق به یک VLAN خاص هنگام انتقال از ترانک (لینک Uplink که بعنوان ترانک تعریف شده است.) با اضافه شدن یک tag که شماره VLAN را مشخص می کند،امکان تحویل فریم به VLAN هم شماره را در سوئیچ دیگر امکانپذیر می کند.

وقتی یک فریم 802.1q در یک سوئیچ دریافت می شود ،سوئیچ با خواندن شماره VLAN ،مقصد را درجدول MAC-Address-Table که مربوط به VLAN مورد نظر است ،جستجو می کند.و در صورت یافت نشدن مقصد برای یافتن مقصد، فریم را بین پورتهای اختصاص یافته به آن VLAN ، Broadcast می کند.

M.Zangian

پیکربندی 802.1q VLAN Trunking:

تعریف VLAN در سوئیچ های سیسکو به راحتی صورت می گیرد کافی است پورتی از سوئیچ که Uplink شده است را در هر دو سوئیچ بعنوان ترانک تعریف کنیم:

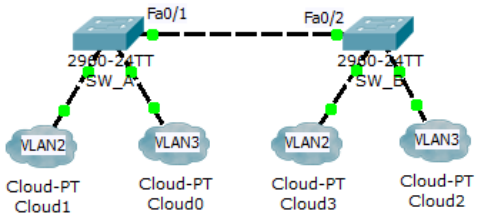



```
SW_A(config)#interface fastEthernet 0/1
SW_A(config-if)#switchport mode trunk
SW_A(config-if)#
```

```
SW_B(config)#interface fastEthernet 0/2
SW_B(config-if)#switchport mode trunk
SW_B(config-if)#
```

M.Zangian

پیکربندی 802.1q VLAN Trunking:



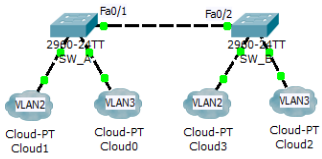

```
SW_A(config)#interface fastEthernet 0/1
SW_A(config-if)#switchport mode trunk
SW_A(config-if)#
```

```
SW_B(config)#interface fastEthernet 0/2
SW_B(config-if)#switchport mode trunk
SW_B(config-if)#
```

با تعریف بالا تمامی VLAN های دو سوئیچ ترانک می شوند.اما اگر بخواهیم VLAN های مشخصی ترانک باشد باید VLAN ها را بصورت مشخص معرفی کنیم.

M.Zangian

در دیاگرام زیر می خواهیم VLAN2 بصورت ترانک و VLAN 3 بصورت VLAN محلی تعریف شود.در اینصورت در دوسوئیچ




```
SW_A(config-if)#interface fastEthernet 0/1
SW_A(config-if)#switchport mode trunk
SW_A(config-if)#switchport trunk allowed vlan 2
SW_A(config-if)#
```

```
SW_B(config)#interface fastEthernet 0/2
SW_B(config-if)#switchport mode trunk
SW_B(config-if)#switchport trunk allowed vlan 2
SW_B(config-if)#
```

در صورتیکه بخواهیم چند VLAN مشخص را ترانک کنیم آنها را با , از هم جدا می کنیم:

```
SW_A(config-if)#switchport trunk allowed vlan 2,3
```

M.Zangian

و در صورتیکه بخواهیم به تعدادی VLAN که VLAN Id آنها پشت سر هم باشد ،اجازه عبور از ترانک را بدهیم از "-" استفاده می نماییم:

Switch(config-if)# switchport trunk allowed vlan 1-3

این دستور اجازه عبور (زدن تگ برروی فریم) فریمهای مربوط به VLAN ، ۱ تا ۳ را برروی ترانک می دهد یعنی VLANهای ۱ ، ۲ ، ۳.

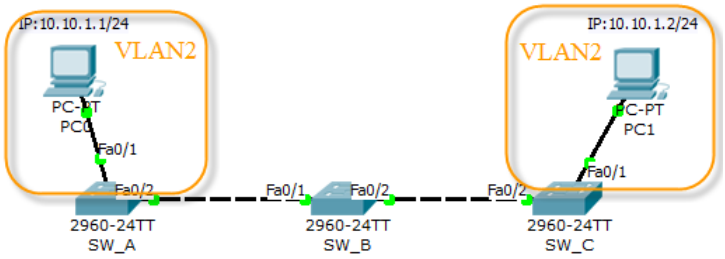
با دستور زیر می توان نوع کپسوله سازی را در ترانک تعیین کرد.تمام سوئیچهای سیسکو IEEE 802.1q را پشتیبانی می کنند .اما ISL پروتکل مخصوص سیسکو است اما در تمامی سوئیچهای سیسکو پشتیبانی نمی شود.در صورتیکه نوع کپسوله سازی را مشخص نکنیم کپسوله سازی 802.1q بصورت پیش فرض در نظر گرفته می شود.

```
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#
```

M.Zangian

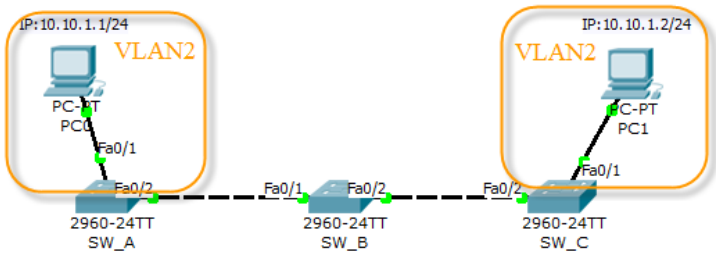
VLAN

مثال: در دیاگرام منطقی زیر می خواهیم ارتباط VLAN های مشابه را با یکدیگر برقرار نماییم.



در این مثال در دو سوئیچ 0 و 2 یک VLAN با VLAN ID ، 2 ایجاد شده است. دراینجا یک سوئیچ واسط بین دو سوئیچ مورد نظر قرار گرفته است بنابراین برای ارتباط دو ایستگاه می بایست دو کار صورت گیرد.

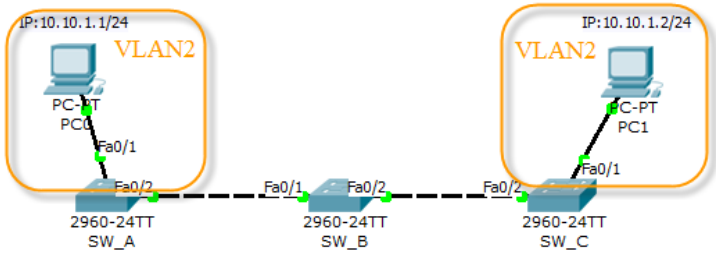
VLAN



ابتدا باید بین هر سوئیچ و سوئیچ واسط ترانک ایجاد گردد.بنابراین در دوسوئیچ پورتهای Fa0/2 را بعنوان ترانک تعریف می کنیم اما در سوئیچ واسط نیز می بایست Fa0/1 و Fa0/2 نیز ترانک شوند تا ترانک از دو طرف برقرار گردد.

علاوه بر این سوئیچ واسط زمانی می تواند یک VLAN را بپذیرد و ترانک نماید که VLAN مربوطه در سوئیچ ایجاد شده است بنابراین هر چند در سوئیچ واسط ایستگاهی متعلق به VLAN2 نباشد می بایست VLAN2 در سوئیچ واسط تعریف شود. بنابراین به راحتی می توان VLAN های مختلف را بین چندین سوئیچ مختلف منتقل کرد و ارتباط ایستگاههای کاری مربوط به VLAN های مشابه را برقرار کرد.

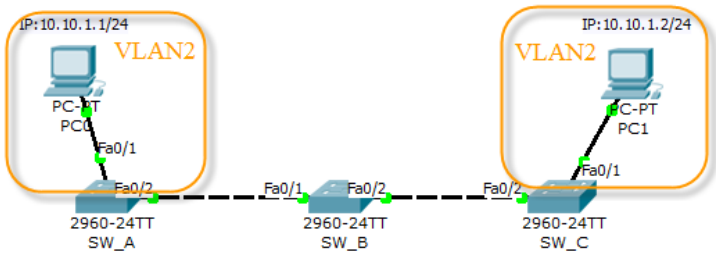
VLAN




```
SW_A(config)#vlan 2
SW_A(config-vlan)#name IT_Department
SW_A(config-vlan)#interface f0/1
SW_A(config-if)#switchport mode access
SW_A(config-if)#switchport access vlan 2
SW_A(config-if)#interface f0/2
SW_A(config-if)#switchport mode trunk
SW_A(config-if)#
```

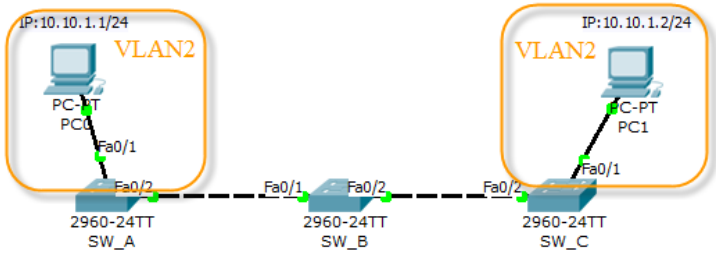
M.Zangian

VLAN




```
SW_C(config)#vlan 2
SW_C(config-vlan)#name IT_Department
SW_C(config-vlan)#interface f0/1
SW_C(config-if)#switchport mode access
SW_C(config-if)#switchport access vlan 2
SW_C(config-if)#interface f0/2
SW_C(config-if)#switchport mode trunk
SW_C(config-if)#
```

M.Zangian




```
SW_B(config)#vlan 2
SW_B(config-vlan)#name IT_Department
SW_B(config-vlan)#interface fastEthernet 0/1
SW_B(config-if)#switchport mode trunk
SW_B(config-if)#interface fastEthernet 0/2
SW_B(config-if)#switchport mode trunk
SW_B(config-if)#
```


DTP(Dynamic Trunking Protocol):

در بحث قبل، برای ایجاد ترانک صراحتا پورتهای دو سر لینک سوئیچ را در مود Trunk قرار دادیم اما پورتهای سوئیچ که در دوسر یک لینک قرار دارند می توانند بصورت دینامیک برای ایجاد ترانک با یکدیگر گفتگو کنند.

پروتکل DTP یک پروتکل جهت گفتگو بین دو سوئیچ برای توافق ایجاد ترانک بین لینک ارتباطی دو سوئیچ و نوع کپسوله سازی VLAN Trunking می باشد. فریم های DTP هر ۳۰ ثانیه در لینک ارسال می گردد.

پورتهای دو سر لینک می توانند در مودهای مختلفی قرار داشته باشند که در امکان ایجاد ترانک بین لینک تاثیر گذار است.


```
interface FastEthernet0/1
 switchport mode dynamic desirable
```

```
interface FastEthernet0/1
 switchport mode dynamic auto
```

VLAN-DTP

341

مودهای مختلف SwitchPort:

Auto:

در این مود پورت سوئیچ در صورتیکه درخواستی برای ایجاد ترانک دریافت کند آنرا می پذیردولی خود پورت تمایل خود را برای ایجاد ترانک اعلام نمی کند.بنابراین پورت مقابل در لینک ارتباطی باید در مودی قرار بگیرد که درخواست ترانک نماید تا یک ترانک بین آندو ایجاد گردد.در صورتیکه پورت طرف مقابل در یکی از مودهای Desirable ، Trunk(On) باشد ترانک بین آندو ایجاد می شود.

Desirable:

دراین مود پورت بصورت فعال تمایل به ایجاد ترانک دارد.در این مد پورت سوئیچ در صورتیکه درخواستی برای ایجاد ترانک دریافت کند آنرا می پذیرد.همچنین پورت در این مد تمایل خود را برای ایجاد ترانک نیز به همسایه خود اعلام می دارد. بنابراین در صورتیکه طرف مقابل پورتی که در این مود قرار دارد در یکی از مودهای Desirable، Auto، Trunk (on) قرار داشته باشد ترانک بین دو سر لینک ایجاد می گردد.

M.Zangian

VLAN-DTP

342

مودهای مختلف SwitchPort:

Trunk(On):

در این مود پورت سوئیچ بصورت ترانک دائمی تعریف می شود و در این صورت پورت جهت ایجاد ترانک با طرف مقابل گفتگو می کند و سعی در ایجاد ترانک دارد حتی اگر طرف مقابل درخواست ترانک را نپذیرد.

Access(Off):

در این مود پورت سوئیچ بصورت دائمی در حالت غیر-ترانک (Access) قرار می گیردو جهت قرار دادن پورت درحالت غیر ترانک با طرف مقابل گفتگو می کند.در این مود حتی اگر طرف مقابل تمایل به ایجاد ترانک داشته باشد، پورت در حالت غیر ترانک قرار می گیرد.

nonegotiate:

این حالت فقط در دو مود Trunkو Access در دسترسی می باشد.و در دو مود دیگر نمی توان حالت nonegotiate را فعال نمود.در صورتیکه این حالت برای یک پورت فعال شود،اجازه ایجادفریم های DTP برای گفتگو به پورت داده نمی شود.

M.Zangian

جدول زیر حالتهای مختلفی که دو پورت می توانند نسبت به هم قرار گیرند و نتیجه ای که در بر خواهد داشت را نشان می دهد

Figure 1 Administrative Mode Combinations and their Operational Modes

Administrative Mode	Auto	Desirable	Trunk (on)	Access (off)	Non-Negotiate (access)	Non-Negotiate (trunk)
Auto	Static access (NT)	Trunk	Trunk	Static access	Static access	Unexpected Results
Desirable	Trunk	Trunk	Trunk	Static access	Static access	Unexpected Results
Trunk (on)	Trunk	Trunk	Trunk	Unexpected Results	Unexpected Results	Trunk
Access (off)	Static access	Static access	Unexpected Results	Static access	Static access	Unexpected Results
Non-Negotiate (access)	Static access	Static access	Unexpected Results	Static access	Static access	Unexpected Results
Non-Negotiate (trunk)	Unexpected Results	Unexpected Results	Trunk	Unexpected Results	Unexpected Results	Trunk

M.Zangian


```
Switch(config-if)#switchport mode dynamic auto
```
قرار دادن یک پورت در مود Auto

```
Switch(config-if)#switchport mode dynamic desirable
```
قرار دادن یک پورت در مود Desirable

```
Switch(config-if)#switchport mode access
```
قرار دادن یک پورت در مود Access

```
Switch(config-if)#switchport mode trunk
```
قرار دادن یک پورت در مود Trunk

```
Switch(config-if)#switchport nonegotiate
```
قرار دادن یک پورت در مود nonegotiate

M.Zangian

VLAN-DTP

بااستفاده از دستور زیر می توان وضعیت Switchport را برای یک اینترفیس مشاهده نمود.

```
Switch#show interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
Switch#
```


VLAN-DTP

فریم های DTP هر ۳۰ ثانیه در لینک ارسال می گردد و برای غیر فعال کردن آن باید از دستور زیر استفاده نمود.

```
Switch(config-if)#switchport nonegotiate
```

DTP تنها بین سوئیچها کار می کند و در صورتیکه یکطرف لینک روتر باشد DTP کار نخواهد کرد و ترانک باید بصورت دستی ایجاد گردد.

VLAN-Native VLAN

Native VLAN:

همانطوریکه در بحث مربوط به VLAN ها گفتیم فریم های عضو VLAN ها هنگام عبور از ترانک tag می خورد تا در سوئیچ دیگر قابل دسترسی توسط VLAN همنام باشد. اما فریمهای عضو Native VLAN ، بصورت پیش فرض هنگام عبور از ترانک tag نمی خورد.در صورتیکه یک فریم بدون tag به یک سوئیچ وارد شود تحویل Native VLAN می شود.

بصورت پیش فرض VLAN1 ، بعنوان Native VLAN در نظر گرفته شده است.علاوه براین VLAN 1 بعنوان Management VLAN نیز می باشد یعنی فریمهای مربوط به CDP,Spanning-tree ، VTP و سایر فریمهای مدیریتی از این VLAN برای عبور استفاده می نمایند و نمی توان آنرا محدود کردویا تغییر داد.

اگر Native VLAN در دو سمت ترانک بین دو سوئیچ متفاوت تنظیم شده باشد ، CDP آنرا کشف واعلام می کند.با استفاده از دستور زیر می توان Native VLAN را در یک پورت ترانک شده تغییر داد.

```
SW_A(config-if)#switchport trunk native vlan 3
```


VLAN-Native VLAN

با استفاده از دستور زیر می توان یک پورت سوئیچ را به Native VLAN اختصاص داد.

```
SW_C(config-if)#switchport native vlan 5
```

ویا

```
SW_C(config-if)#switchport trunk native vlan 5
```

با استفاده از دستور زیر می توان سوئیچ را مجبور کرد برروی تمام VLAN ها از جمله Native VLAN ، تگ بزنند.

```
Switch(config)#vlan dot1q tag native
```

(این دستور توسط Cisco Packet Tracer پشتیبانی نمی شود.)

VLAN-VTP

VTP(VLAN Trunk Protocol):

یکی از مشکلاتی که در پیکربندی VLAN ها وجود دارد ایجاد و تغییر VLAN ها در سوئیچهای یک شبکه است .در صورتیکه تعداد VLAN ها و سوئیچها در یک شبکه زیاد باشد تعریف و تغییرات VLAN کاری زمانبر خواهد بود.بعبارت دیگر برای ایجاد تغییرات برروی VLAN ها در شبکه ای متشکل از ۲۰ سوئیچ بایدتغییرات در این VLAN ها با اتصال به هر یک از سوئیچها بصورت جداگانه انجام پذیرد.

از اینرو امکانی در سوئیچ های سیسکو برای مدیریت لیست VLAN ها در یک شبکه ایجاد شده است تا تعاریف و تغییرات VLAN ها را ساده نماید.

VTP پروتکلی برای مدیریت لیست VLAN ها در یک شبکه است. بعبارت دیگر با این امکان می توان به راحتی ایجاد ، حذف و تغییر نام VLAN ها را در یک شبکه انجام داد.علاوه بر این VTP اشتباهات در تعاریف و نام VLAN ها را به حداقل رسانده ونیز با محدود کردن امکان تغییرات به سوئیچهای خاص امنیت را افزایش خواهد داد.

VLAN-VTP

VTP Domain:

ناحیه مدیریتیVTP بوسیله VTP Domain مشخص می شود. سوئیچهایی که VTP Domain Name آنها یکسان باشنددر ناحیه مدیریتی واحد قرار دارند و میتوانند اطلاعات VLAN ها را با یکدیگر ردو بدل کنند.

اطلاعات VTP درون فریم VLAN1 و از طریق ترانک منتقل می شود. بنابراین برای انتقال فریم VTP بین سوئیچها می بایست بین آنها ترانک برقرار باشد.(در صورتیکه Native Vlan ، بصورت پیش فرض و VLAN 1 باشد ، فریمهای VTP ، tag نمی خورد و درصورتیکه Native VLAN ، VLAN دیگری تعیین شود ، VTP بازهم از VLAN1 اما این بار بصورت Tag خورده منتقل می شود.)

سوئیچها در VTP Domain های مختلف با یکدیگر هیچ اطلاعاتی را به اشتراک نمی گذارند. یک LAN می تواند از چندین VTP Domain مختلف تشکیل شده باشدکه پیغامهایشان را فقط در محدوده Domain خود ردوبدل می کنند. بصورت پیش فرض VTP Domain Name ، Null است.

VLAN-VTP

VTP Version:

سوئیچها بسته به ورژن IOS از VTP Version های متفاوتی پشتیبانی می کنند . بطور کلی سه نسخه از VTP وجود دارد.

در VTP نسخه 1و 2 تنها از VLAN های شماره 1 تا 1000 پشتیبانی می شود.

VTP نسخه 3 از VLAN های 1 تا 4094 پشتیبانی می کند.

VLAN های محدوده Extended Range تنها در نسخه 3 ، VTP پشتیبانی می شوند.

در صورتیکه در یک سوئیچ، نسخه VTP از 3 به 2 تغییر یابد ، VLAN های 1006 تا 4094 از کنترل VTP خارج می شوند.

M.Zangian

VLAN-VTP

مدهای مختلف VTP:

Server Mode:

سوئیچی که در یک VTP Domain بعنوان سرور تعریف می شود،وظیفه مدیریت تعاریف VLAN ها را بعهده دارد.هر VTP Domain حداقل به یک Server نیاز داردتا مدیریت ایجاد ، حذف و تغییر VLAN ها را در Domain خود بعهده می گیرد.هر گونه تغییری در Domain توسط VTP Server به تمام سوئیچهای Domain بصورت Multicast اطلاع داده می شودو سوئیچ های دیگر اطلاعات VLAN را با سرور خود sync می نمایند.

(آدرس Multicast، 01-00-0C-CC-CC-CC)

فهرست کلیه VLAN ها در Flash (ویا NVRAM) سوئیچهای VTP Server ذخیره می شود.(در فایل VLAN.dat) در صورتی که نوشتن در حافظه با مشکل مواجه شود،سوئیچ خود را در مود Clientقرار می دهد تا زمانیکه مشکل بر طرف گردد.

در یک VTP Domain می تواند بیش از یک VTP در مد سرور قرار داشته باشد که بصورت Redundant در شبکه عمل می کنند و اطلاعات خود را با یکدیگر Sync می کنند.

M.Zangian

VLAN-VTP

353

Client Mode:

سوئیچی که در این مود VTP قرار دارد اطلاعات VLAN ها را از سوئیچی که در Domain Name یکسانی قرار دارد دریافت کرده و بر سوئیچ اعمال می کند.علاوه بر این سوئیچی که در این مود قرار دارداطلاعات VTP را بطرف سوئیچهای دیگرنیز ارسال می کند(Relay) .در VTPنسخه ۱ و۲ ، اطلاعات VLAN ، در مود Client ذخیره نمی شود و در RAM قرار دارد و با خاموش شدن سوئیچ از بین می رود و دوباره با دریافت فریم VTP از سمت Server به روز می شود.در این مود سوئیچ نمی تواند بصورت محلی VLAN ی را ایجاد ،حذف و یا تغییر دهد.(در VTP نسخه ۳ ، اطلاعات VLAN در :Flash سوئیچ ذخیره می گردد.)

M.Zangian

VLAN-VTP

354

Transparent Mode:

در این مود سوئیچ تنها فریمهای VTP را دریافت و انتقال میدهد(Relay) ولی اطلاعات دریافت شده را بر روی سوئیچ اعمال نمی کند.در VTP نسخه یک سوئیچ تنهابسته های VTP ، را Relay می کند که هم ، دامنه آنها با دامنه تنظیم شده برروی سوئیچ یکی باشد(Domain هم نام خود) وهم نسخه VTP با نسخه تنظیم شده برروی سوئیچ یکسان باشد .بنابراین در VTP نسخه یک سوئیچ به Domain های دیگر اجازه انتقال نمی دهد.اما در VTP نسخه دو تمامی VTP ها از جمله VTP، Domain های دیگر نیز Relay می شوند.

در این مود می توان برروی سوئیچ VLAN های محلی و مستقل از VTP Domain ایجاد کرد.بنابراین اطلاعات VLAN در این مود بصورت مستقل در NVRAM قرار می گیرد.

M.Zangian

VLAN-VTP

355

جدول زیر قابلیت ایجاد VTP ،گوش دادن واعمال تغییرات ،ایجاد VLAN و ذخیره سازی VLAN ها برای Mode های مختلف نشان داده شده است.

Feature	Server	Client	Transparent
Source VTP Messages	Yes	Yes	No
Listen to VTP Messages	Yes	Yes	No
Create VLANs	Yes	No	Yes*
Remember VLANs	Yes	No	Yes*
*Locally significant only.			

بصورت Default ، در سوئیچ VTP در مد Server قرار دارد. و Domain Name آن Null است.

تازمانیکه نام دامنه یک سوئیچ Null باشد اقدام به ارسال بسته های VTP نمی کند.

M.Zangian

VLAN-VTP

356

Configuration Revision:

VTP در هر سوئیچ دارای پارامتری است که مشخص کننده نسخه تغییرات VLAN هاست. بصورت پیش فرض مقدار 0 برای این پارامتر درنظر گرفته شده و با هر تغییر برروی VLAN های سوئیچ یک واحد به Configuration Revision اضافه می گردد.

- هر سوئیچ که در مود Server یا کلاینت در یک VTP Domain مشترک قرار دارند با دریافت فریم VTP در صورتیکه Configuration Revision آن بیشتر از Conf. Rev.خود باشد آنرا پذیرفته و براساس اطلاعات آن خود را Update می کند. و در صورتیکه Conf. Rev. دریافت شده کوچکتر باشد آنرا در نظر نمی گیرد.
- در صورتیکه Domain Name یک سوئیچ بصورت Null باشد چه در حالت Server باشد و یا Client در صورت دریافت یک فریم VTP با Domain Name غیر Null خود را با آن Sync می کندودر آن دامنه قرار می گیرد.
- تعاریف VTP در Server با خاموش شدن سوئیچ از بین نمی رود.
- در صورتیکه مود VTP تغییر یابد و یا نام VTP Domain تغییر یابد و یا فایل VLAN.dat پاک شود Configuration Revision صفر می شود.

M.Zangian

در صورتیکه در یک VTP Domain، در Server به هر ترتیب Conf. Rev کوچکتر از Conf.Rev ، Client های آن Domain گردد. سرور خود را با کلاینتهای خود Update می کند.

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 6
VTP Operating Mode              : Transparent
VTP Domain Name                 : MyVTP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x00 0xF0 0x6B 0xDA 0x93 0x50 0x23 0xA6
Configuration last modified by 0.0.0.0 at 3-1-93 00:21:47
```

مشاهده وضعیت VTPدر یک سوئیچ

یک سوئیچ در حالت Default
در VTP Mode ، سرور و با Domain Name
Null و پورتهای آن در VLAN 1 می باشدوConf.Rev آن برابر صفر می باشد.

VLAN-VTP

بطور کلی سه نوع VTP Message وجود دارد:

۱- Summary Advertisements

این پیام هر ۳۰۰ ثانیه یکبار (۵ دقیقه) توسط سرور ویا **کلاینت** به سوئیچهایی که به سوئیچ بصورت ترانک متصل است ارسال می شود.علاوه بر این زمانیکه تغییراتی در تعریف VLAN های سرور ایجاد گردد این پیام سریعا توسط سرور به سمت ترانک سوئیچهای همسایه ارسال می گردد و متعاقب آن پیام Subset ارسال می شود.

در این پیام خلاصه اطلاعاتی نظیر VTP Version، Domain Name، Configuration Revision Number، updater identity ، timestamp وMD5 Digest Hash و نیز تعداد رکوردهای پیام Subset که در ادامه آن می آید مشخص می گردد.

VLAN-VTP

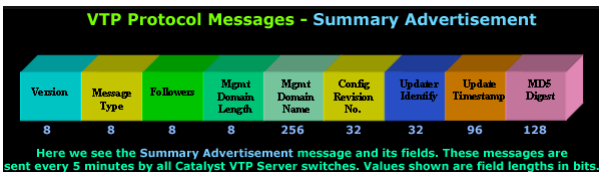
زمانیکه یک سوئیچ یک پیام Summery را دریافت می کند ابتدا نام دامنه پیام را که در فیلد Management Domain Name قرار دارد با نام دامنه خود مقایسه می کند و در صورتیکه این نام یکی نباشد بسته را دور می ریزد.

در صورتیکه نام دامنه پیام و سوئیچ یکی باشد در قدم بعدی سوئیچ Conf.Rev بسته را با Conf.Rev خود مقایسه می کند و اگر Conf.Rev پیام کوچکتر باشد از پیام صرفنظر کرده وآنرا نادیده می گیرد.

Version	Type	Number of Subnet Advertisement Messages	Domain Name Length
Management Domain Name (Padded to 32 Bytes)			
Configuration Revision Number			
Updater Identity			
Update Timestamp (12 Bytes)			
MD5 Digest (16 Bytes)			

بسته Summery Advertisement

در صورتیکه Conf.Rev Number پیام بیشتر از مقدار سوئیچ باشد، سوئیچ در می باید تغییراتی در VLAN شبکه پدید آمده که از آن بی خبر است بنابراین یک پیام Request Advertisement به سمت ارسال کننده می فرستد و بااین کار اعلام می کند نیازمند اطلاعات بیشتری در مورد تغییرات شبکه است.



Message Type(Code): بیانگر نوع پیام VTP است که برای پیام Summery مقدار این فیلد 0x01 است.

Follower(Number Of Subset Advertisement Messages): تعداد Subset هایی که متعاقب Summery Message می آید را معین می کند.

Updater Identifier: اطلاعات مربوط به آدرس IP سوئیچی است که افزایش Conf.Rev را اعلام نموده است.

Update Timestamp: زمان آخرین Update انجام شده را گزارش می نماید.

Md5 Digest:عبارتست از کلمه عبوری که برای نام دامنه درنظر گرفته شده است. این کلمه عبور بصورت hash شده در فیلد قرار می گیرد.

M.Zangian

۱- Subset Advertisements

هنگامی که تغییراتی در VLAN ها برروی سرور ایجادشود این تغییرات سریعا توسط یک پیام Subset Advertisement به سوئیچهای دیگر اطلاع داده می شود.

این پیام زمانیکه یکی از تغییرات زیر برروی شبکه ایجاد شود از طرف سرور ایجاد می شود.

۱- ایجاد یا حذف VLAN

۲- تغییر نام VLAN

۳- فعال یا غیر فعال کردن VLAN

۳- تغییر MTU یک VLAN

با انجام هریک از تغییرات اشاره شده ابتدا سوئیچ یک VTP Summery Message را ارسال نموده و سپس متعاقب آن پیامهای Subset Advertisemnet را ارسال می کند.

M.Zangian

ممکن است برای بروزرسانی اطلاعات VLAN ها در یک شبکه چندین پیام Subset در شبکه ارسال شودتا کلیه تغییرات را به شبکه اعلام نماید.

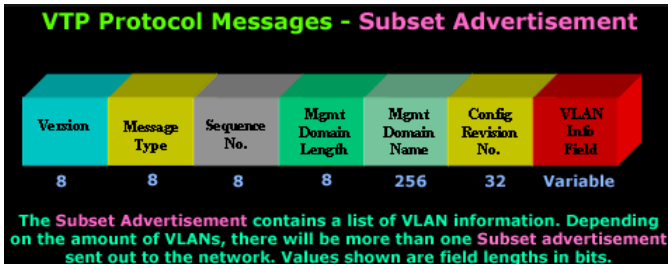
Version	Code	Seq-Number	Domain Name Length
Management Domain Name (Zero-Padded to 32 Bytes)			
Configuration Revision Number			
VLAN-info Field 1			
. . .			
VLAN-info Field N			

بسته

Subset Advertisement

Info Length	Status	VLAN-Type	VLAN-name Len
ISL VLAN-id		MTU Size	
802.10 Index			
VLAN-name (Padded with zeros to Multiple of 4 Bytes)			

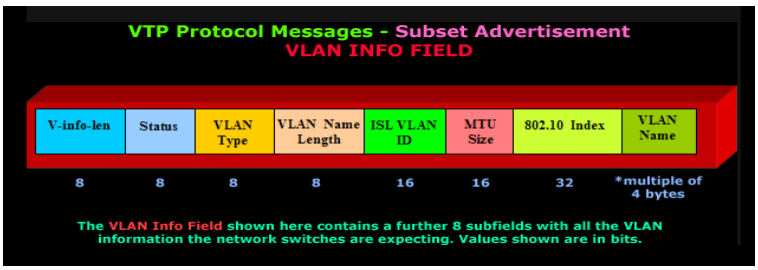
اطلاعات VLAN ها درونVLAN-Info Field



Message Type(code) : برای پیام Subset برابر 0x02 می باشد که بیانگر نوع پیام یعنی Subset است.

Sequence No: شماره ترتیب پیام Subset را در یک مجموعه پیام های Subset ، مشخص می نماید. همانطوریکه گفتیم سوئیچ Updater تعدادی پیام Subset را برای بروزرسانی کامل همسایگان خود ارسال می کند و هر پیام را شماره گذاری کرده و ارسال می نماید و Sequence No شماره ترتیبی پیام را مشخص می نماید که از ۱ شماره گذاری می شود.

M.Zangian



هر VLAN-Info Field درون یک پیام Subset ، دارای مجموعه ای از فیلدهای اطلاعاتی مربوط به VLAN هاست که اطلاعات کاملی از یک VLAN را در بردارد. در یک پیام Subset می تواند چندین VLAN-Info Field وجود داشته باشد که به دنبال هم ارسال می شود.

M.Zangian

۳- Request Advertisement

این پیام زمانی ارسال می گردد که یک سوئیچ احتیاج به اطلاعات تغییرات VLAN ها داشته باشد.زمانیکه یک پیام Request Adv. به یک VTP سرور می رسد ، VTP سرور با ارسال پیامهای Summery Adv. و Subset Adv. به این درخواست پاسخ می دهد.

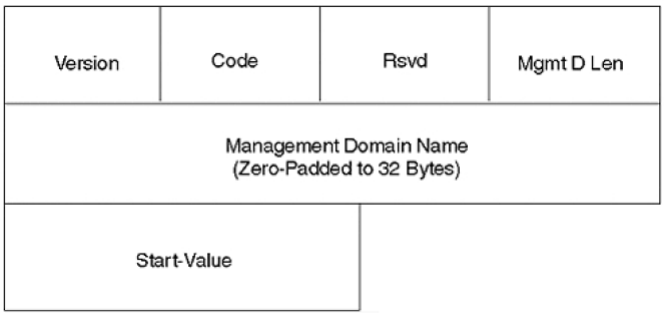
پیام Request Advertisement زمانی ارسال می شود که:

۱-VTP Domain در یک سوئیچ تغییر نماید.(بعبارت دیگر Conf.Rev صفر شود.)

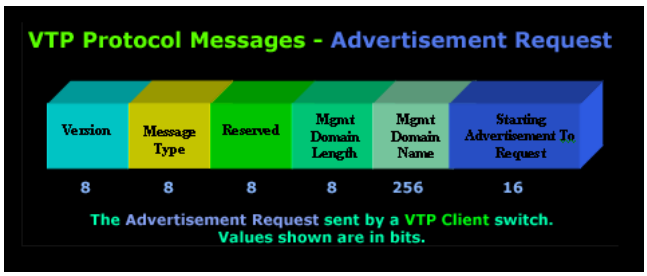
۲-زمانیکه یک سوئیچ یک پیام Summery Adv. با Conf.Rev بالاتر از خود دریافت نماید.

۳- زمانیکه دریافت اطلاعاتSubset با مشکل مواجه شود.

۴- زمانیکه یک سوئیچ Reset شود.



بسته Request Advertisement



Message Type(Code): نوع پیام VTP را مشخص می کند برای پیام Request Advertisement برابر 0x03 می باشد.

Start Advertisement To Request: در صورتیکه در دریافت مجموعه ای از Subset ها بخشی از آن توسط سوئیچ درخواست کننده ، دریافت نگردد، سوئیچ می تواند ازیک پیام مشخص به بعد را درخواست نماید بعنوان مثال اگر N پیام Subset دریافت شده و بقیه دریافت نشود در پیام Request بجای دریافت دوباره تمامی پیامها ،پیام N+1 به بعد ، درخواست می گردد.

امنیت در حالت VTP:

از آنجاییکه با قرار دادن یک سوئیچ در شبکه بطوریکه در مود Server یا کلاینت باشد به راحتی می توان تعاریف VLAN را در شبکه مختل کرد از اینرو باید مسائل زیر را حتما در نظر گرفت.

۱- برای هر VTP Domain حتما می بایست Domain Name را در نظر گرفت و آنرا بصورت Default و Null رها نکرد.

۲- برای هر VTP یک Password انتخاب نمایید.

۳- بعد از انجام تغییرات در شبکه در سوئیچها VTP را در مود Transparent قرار دهید.

توجه نمایید در صورتیکه یک سوئیچ جدید را به شبکه اضافه می نمایید چه VTP در مورد سرور باشد و یا کلاینت .Conf.Rev آنرا صفر نمایید چرا که اگر Conf.Rev آن بیشتر از Conf.Rev سوئیچهای شبکه باشد با قرار دادن نام دامنه هم نام ، تنظیمات VLAN تمام شبکه براساس سوئیچ اضافه شده تغییر خواهد کرد.
با تغییر نام دامنه و برگرداندن نام و نیز با تغییر مود VTP می توان Conf.Rev را برابر صفر قرارداد.

دستورات VTP در سیسکو:

تعیین Domain Name

```
Switch(config)#vtp domain MyVTP
```

تعیین Password برای VTP در صورتیکه Domain Name، Null باشد ، Password را نمی پذیرد.

```
Switch(config)#vtp password MyPassword
```

تغییر مود VTP، سه حالت برای مود VTP وجود دارد:

1. Server
2. Client
3. Transparent

```
Setting device VLAN database password to MyPassword
Switch(config)#vtp mode ?
  client       Set the device to client mode.
  server       Set the device to server mode.
  transparent  Set the device to transparent mode.
Switch(config)#vtp mode server
Device mode already VTP SERVER.
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#vtp mode tran
Switch(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config)#
```

M.Zangian

تغییر نسخه VTP که بسته به نسخه IOS ،سوئیچ می تواند نسخه های متفاوت VTP را پشتیبانی نماید.

```
Switch(config)#vtp version ?
  <1-2>  Set the adminstrative domain VTP version number
Switch(config)#vtp version 2
Switch(config)#
```

نکته

قبل از تعریف VTP در یک شبکه تمام سوئیچهایی که به یکدیگر متصل هستند می بایست با یکدیگر ترانک شوند.

بطور کلی ۳ نسخه برای VTP در سوئیچهای سیسکو وجود دارد که VTP نسخه ۳ تغییرات زیادی نسبت به دو نسخه دیگر داشته و توسط برخی از سوئیچها پشتیبانی می گردد.

M.Zangian

Inter-VLAN:

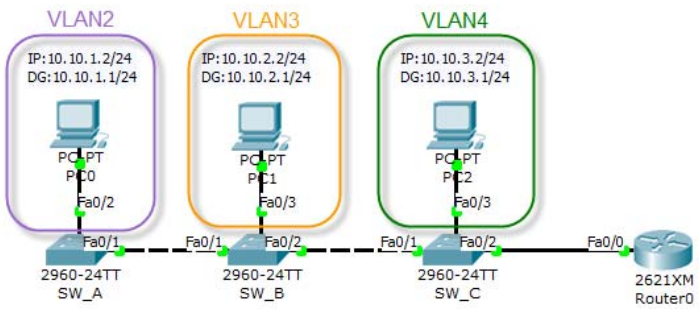
در این بخش آموختیم که چگونه یک شبکه یکپارچه و FLAT را به VLAN های مختلف تفکیک کنیم ودیدیم ارتباط هر VLAN در لایه ۲ محدود به VLAN های همنام در شبکه گردید.اما اغلب اوقات ما می خواهیم ضمن برخورداری از مزایای VLAN نظیر کاهش ایستگاهها در Broadcast Domain و مدیریت ساده تر ، ایستگاههای کاری در VLAN های مختلف با یکدیگر مرتبط باشند.

اما طبق مطالبی که در مورد VLAN ها آموختیم چنین کاری در لایه ۲ امکانپذیر نیست. بنابراین برای ایجاد چنین امکانی می بایست ارتباط بین VLAN های مختلف را در لایه ۳ برقرار سازیم.

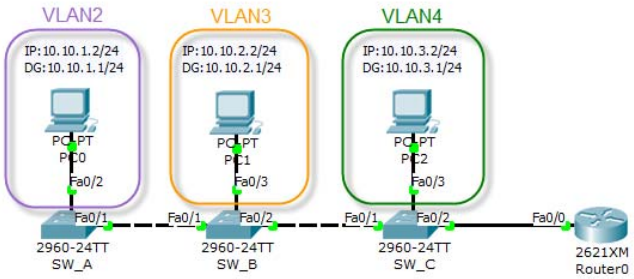
بنابراین برای ایجاد ارتباط بین VLAN ها نیازمند سوئیچ لایه ۳ و یا روتر هستیم. از آنجا که تنظیمات Inter-VLAN در سوئیچ لایه ۳ بسیار ساده است ما در اینجا به تشریح چگونگی ارتباط بین VLAN ها با استفاده از یک روتر می پردازیم.

Inter-VLAN:

در دیاگرام منطقی زیر می خواهیم ارتباط شبکه را بین ایستگاههای کاری در VLAN های 2,3,4 برقرار نماییم.



Inter-VLAN:



برای ایجاد ارتباط بین VLAN ها ابتدا می بایست تعاریف مربوط به لایه دو را انجام دهیم بنابراین باید موارد زیر انجام شود:

۱- تعریف VLAN در سوئیچ های مربوطه

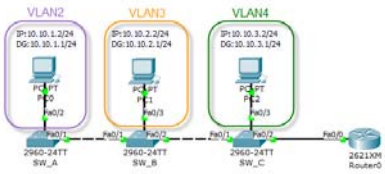
۲- اختصاص پورت های سوئیچ به VLAN

۳- ترانک کردن Uplink بین سوئیچها از هر دو سمت

۴- ایجاد ترانک بین سوئیچ انتهایی و روتر

M.Zangian

Inter-VLAN مراحل ۱-۳:

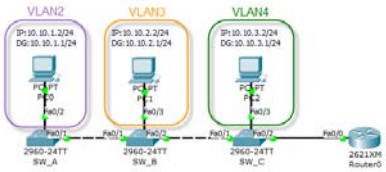



```
SW_A(config)#vlan 2
SW_A(config-vlan)#name V2

SW_A(config-vlan)#vlan 3
SW_A(config-vlan)#name V3

SW_A(config-vlan)#vlan 4
SW_A(config-vlan)#name V4

SW_A(config)#interface fastEthernet 0/2
SW_A(config-if)#switchport mode access
SW_A(config-if)#switchport access vlan 2

SW_A(config)#int f0/1
SW_A(config-if)#switchport mode trunk
```

```
SW_B(config)#vlan 2
SW_B(config-vlan)#name V2

SW_B(config-vlan)#vlan 3
SW_B(config-vlan)#name V3

SW_B(config-vlan)#vlan 4
SW_B(config-vlan)#name V4

SW_B(config)#int f0/3
SW_B(config-if)#switchport mode access
SW_B(config-if)#switchport access vlan 3

SW_B(config-if)#int f0/1
SW_B(config-if)#switchport mode trunk

SW_B(config-if)#int f0/2
SW_B(config-if)#switchport mode trunk
```

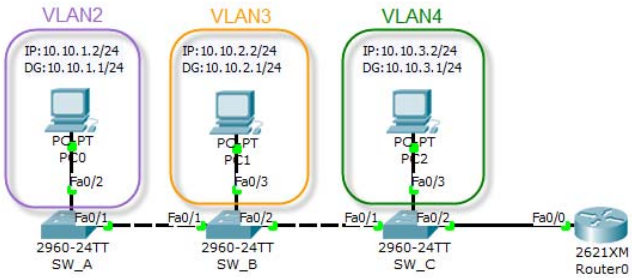
M.Zangian

Inter-VLAN مراحل ۱-۳:



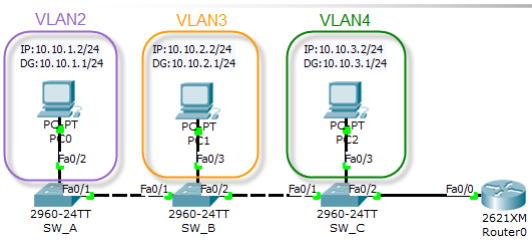

```
SW_C(config)#vlan 2
SW_C(config-vlan)#name V2

SW_C(config-vlan)#vlan 3
SW_C(config-vlan)#name V3

SW_C(config-vlan)#vlan 4
SW_C(config-vlan)#name V4

SW_C(config)#int f0/3
SW_C(config-if)#switchport mode access
SW_C(config-if)#switchport access vlan 4

SW_C(config-if)#int f0/1
SW_C(config-if)#switchport mode trunk

SW_C(config-if)#int f0/2
SW_C(config-if)#switchport mode trunk
```


Inter-VLAN مرحله ٤:



مراحل ۱-۳ در مباحث قبلی بررسی شد اما چگونه می توانیم بین روتر و سوئیچ انتهایی ترانک ایجاد کنیم؟ برای انجام این کار ابتدا می بایست در روتر VLAN های مورد نظر ایجاد شده و سپس ترانک شود. بنابراین می بایست به تعداد VLAN ها ، در روتر اینترفیس داشته باشیم تا ابتدا آنها را در VLAN های متناظر قرار داده و ترانک نماییم.اما اختصاص اینترفیس به تعداد VLAN ها غیر عملی است چرا که اینترفیسهای روتر محدود بوده و عملا چنین کاری منطقی نیست.

Inter-VLAN مرحله ٤:



در روتر می توان یک اینترفیس فیزیکی را بصورت مجازی به تعداد زیادی Sub Interface تقسیم نمود که همگی از اینترفیس فیزیکی موجود استفاده نموده و بعنوان اینترفیس مستقل با آن رفتار می شود بنابراین :

۱- به تعداد VLAN در اینترفیس متصل شده به سوئیچ نهایی ، Sub Interface می سازیم

۲- هر Sub Interface را به یک VLAN اختصاص داده و آنرا ترانک می کنیم.

```
Router(config)#interface fastEthernet 0/0.1
```

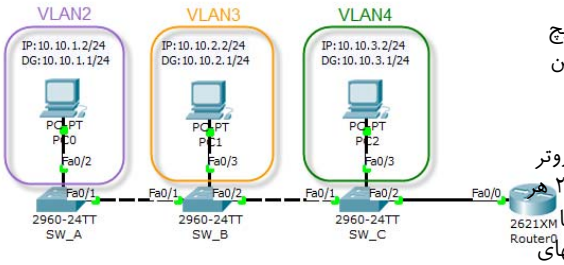
ایجاد Sub Interface

```
Router(config-subif)#encapsulation dot1Q 2
```

قرار دادن Sub Interface در VLAN 2 و ترانک کردن آن با کپسوله سازی dot1.q

M.Zangian

Inter-VLAN مرحله ٤:

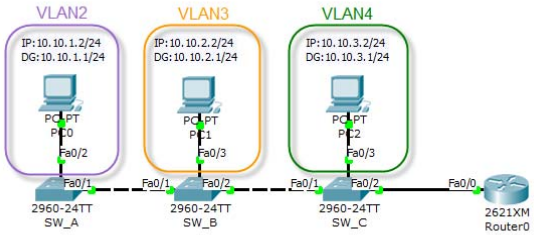


تا اینجا به ازای هر VLAN در سوئیچ یک VLAN در روتر ساختیم بنابراین فریم های مربوط به هر VLAN در سوئیچها از طریق ترانک ها ی بین سوئیچها به VLAN ایجاد شده در روتر منتقل می شود. بنابراین ارتباط لایه ۲ هر VLAN سوئیچ با روتر برقرار شد.اما زمانیکه بخواهیم ارتباط بین ایستگاههای مربوط به VLAN های مختلف که در یک زیر شبکه قرار ندارند را برقرار کنیم ، می بایست این ارتباط در لایه ۳ و توسط Default Gateway برقرار گردد.بنابراین می بایست برای هر ایستگاه آدرس Sub Interface مربوط به VLAN بعنوان Deafult Gateway در نظر گرفته شود.

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#int f0/0.1
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 10.10.1.1 255.255.255.0
Router(config-subif)#int f0/0.2
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip address 10.10.2.1 255.255.255.0
Router(config-subif)#int f0/0.3
Router(config-subif)#encapsulation dot1Q 4
Router(config-subif)#ip address 10.10.3.1 255.255.255.0
```

M.Zangian

Inter-VLAN:



حال فرض کنید بخواهیم از ایستگاه PC0 ایستگاه PC2 را Ping کنیم در این صورت چون IP مقصد و مبدا در یک زیر شبکه واقع نیستند، بسته به سمت Default Gateway فرستاده می شود یعنی آدرس Sub interface مربوط به VLAN2، از آنجاییکه ایستگاه PC0 در VLAN 2 قرار دارد هنگام ترانک شدن Tag می خورد و بین سوئیچها به سمت روتر ترانک می شود با رسیدن فریم به Sub Interface f0/0.1 که مربوط به VLAN 2 است ،فریم توسط روتر باز شده و IP مقصد از درون آن استحراج می شود. روتر در می یابد که مقصد مربوط به Sub Interface f0/0.3 است بنابراین آنرا در فریم اترنت قرار داده Tag ، VLAN4 را به آن اضافه کرده و آنرا به سمت SW_C ترانک می کند .تا فریم بدست PC2 برسد.

M.Zangian

مسیریابی Routing:

در بررسی لایه ۳ ، OSI (لایه شبکه) آموختیم که یکی از وظایف مهم این لایه مسیریابی بسته ها می باشد.بعبارت دیگر یک بسته وقتی به یک مسیر یاب می رسد باید از یکی از اینترفیس های مسیر یاب خارج شود بگونه ای که در نهایت بسته به مقصد مورد نظر برسد. اینکه بسته از کدام یک از اینترفیسهای روتر خارج شود ، توسط فرآیند مسیر یابی مشخص می شود. در فرآیند مسیر یابی ، نهایتا هر مسیر یاب یک جدول مسیر یابی تشکیل می دهد که بر اساس این جدول ،مسیر بعدی بسته مشخص شده و یا در صورت عدم وجود مسیر در این جدول ، بسته دور ریخته می شود.

همانطوریکه دیدیم یکی از پرکاربردترین پروتکل های لایه ۳ ، پروتکل IP است ، در این پروتکل مقصد با یک آدرس منطقی به نام آدرس IP که در هدر هر بسته وجود دارد مشخص می شود. بصورت معمول آدرس مقصد در تمام طول سفر خود به سمت مقصد ،در هدر بسته بدون تغییر می ماند.

M.Zangian

مسیریابی Routing:

وقتی یک مسیر یاب روشن می شود ،جدول مسیر یابی آن که در حافظه RAM قرار دارد فاقد هر گونه اطلاعاتی است . بنابراین مسیر یاب قبل از اینکه بتواند وظیفه هدایت بسته ها را انجام دهد می بایست جدول مسیریابی خودرا تشکیل دهد . سپس توانایی هدایت بسته ها را خواهد داشت.

بطور کلی اطلاعات جداول مسیر یابی با استفاده از سه روش در مسیر یاب ایجاد می گردد.

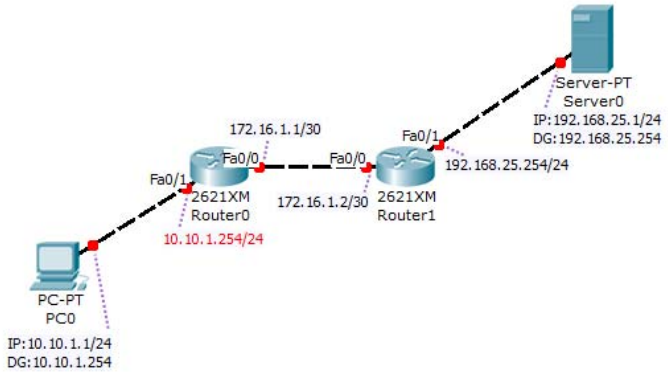
۱- ایجاد مسیربصورت اتوماتیک توسط مسیریاب برای زیرشبکه هایی که بصورت مستقیم به مسیر یاب متصل است.

۱- تنظیمات مسیریابی استاتیک توسط مدیرشبکه

۳- استفاده از روشهای مسیر یابی داینامیک با استفاده از Dynamic Routing Protocols.

مسیریابی Routing:

۱- ایجاد اطلاعات مسیریابی برای زیرشبکه هایی که بصورت مستقیم به مسیر یاب متصل است. به این زیر شبکه ها اصطلاحا Directly Connected می گویند و در جدول مسیر یابی با حرف C مشخص می گردد. در شکل زیریک شبکه فرضی را بررسی می کنیم.



مسیریابی Routing:

قبل از اینکه آدرسهای IP اینترفیس های روترها را تنظیم نماییم جدول مسیریابی یکی از مسیر یابها را مشاهده می کنیم:

برای مشاهده جدول مسیر یابی یک مسیریاب از فرمان زیر استفاده می نماییم:

Route# show ip route

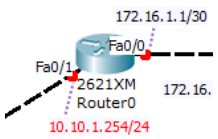
```
Router0#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

Router0#
```

همانطوریکه مشاهده می شود قبل از اختصاص IP به اینترفیس روترها ، در جداول مسیریابی هیچ یک از روترها اطلاعاتی مشاهده نمی گردد.

مسیریابی Routing:

حال IP های مربوط به اینترفیس های روتر را تنظیم می نماییم و تاثیر آنرا برروی جداول مسیر یابی هر یک از روترها بررسی می نماییم.

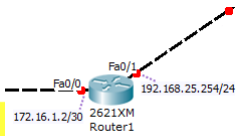
```
Router0#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.1.0 is directly connected, FastEthernet0/1
     172.16.0.0/30 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
Router0#
```



همانطوریکه مشاهده می شود دو ردیف اطلاعات مسیر یابی به جدول مسیر یابی Router0 اضافه گردید.که با حرف C مشخص شده است.

مسیر یابی Routing:


```
Router1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C    192.168.25.0/24 is directly connected, FastEthernet0/1
Router1#
```



و در مورد Router1 مسیر دسترسی به دو زیر شبکه 172.16.1.0/24 و 192.168.25.0/24 مشخص شده است .

اما سئوال اینجاست که این اطلاعات چگونه بوجود آمده است و روتر از کجا در می یابد که مسیر دسترسی به این زیر شبکه ها از کدام اینترفیس است؟

M.Zangian

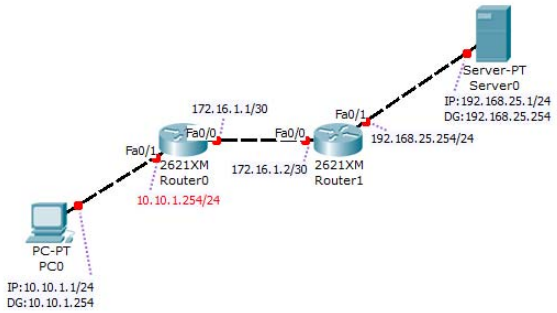
مسیر یابی Routing:

وقتی برروی اینترفیس یک روتر آدرس IP را تنظیم می نماییم ، روتر در می یابد که از طریق آن اینترفیس به یک زیر شبکه متصل است و از طریق آن اینترفیس می تواند به شبکه متصل شده دسترسی داشته باشد. بنابراین آدرس Network ، IP تنظیم شده برروی اینترفیس روتر همان آدرس Network زیر شبکه ای است که بصورت مستقیم به روتر متصل است . برای رسیدن بسته ای با آدرس مقصدی برابر هر یک از آدرس های مربوط به آن زیر شبکه می بایست از طریق اینترفیس عضو آن، بسته را هدایت نماید.

بعبارت دیگر با تنظیم آدرس 10.10.1.254/24 برروی اینترفیس f0/1 روتر 0 ،روتر در می یابد برای رسیدن بسته ها به مقصد هر یک از IP های 10.10.1.0/24 می بایست بسته مورد نظر را از طریق اینترفیس f0/1 خود هدایت کند. بنابراین بصورت خودکار این مسیر را در جدول مسیر یابی خود ایجاد می نماید.

M.Zangian

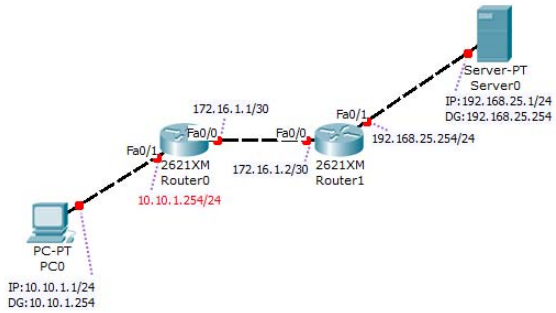
مسیر یابی Routing:



همانطوریکه در شبکه فرضی مشاهده می شود دو زیر شبکه به Router0 و دو زیر شبکه به Router 1 متصل شده است.

Router0: 10.10.1.0/24	از طریق	fa0/1 Router0
172.16.1.0/30	ازطریق	fa0/0 Router0
Router1:192.168.25.0/24	ازطریق	fa0/1 Router1
172.16.1.0/30	ازطریق	fa0/0 Router1

مسیر یابی Routing:

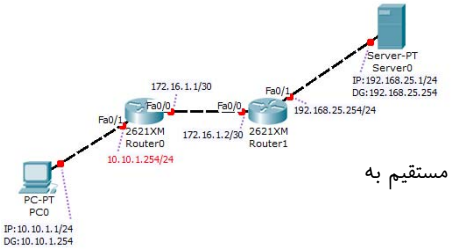


اما Router0 نمی تواند بسته هایی که به مقصد 192.168.25.1 می رسد را مسیر یابی نماید چراکه شبکه 192.168.25.0/24 بصورت بدون واسطه به روتر 0 وصل نیست روتر0 نمی تواند بصورت خودکار مسیری را برای دسترسی به این زیر شبکه ایجاد کند. بنابراین مسیر دسترسی به این زیر شبکه بایستی به روشهای دیگر در جدول مسیر یابی ایجاد گردد.

مسیریابی Routing:

۲- ایجاد جدول مسیر یابی بصورت استاتیک توسط مدیرشبکه

در این روش با استفاده از دستور ip route زیر شبکه هایی که بصورت مستقیم به روترهای شبکه وصل نیستند، بصورت مستقل در هر روترتعریف میگردد. به مثال قبل بر می گردیم:



در این مثال زیر شبکه 192.168.25.0/24 بطور مستقیم به روتر 0 متصل نیست و در مورد روتر 1 زیر شبکه 10.10.1.0/24 بطور مستقیم به روتر ۱ متصل نیست. بنابراین روترها نمی توانند آدرسهای این دو زیر شبکه را بصورت اتوماتیک مسیریابی نمایند ومی بایست جدول مسیر یابی با روشهای دیگر ایجاد گردد.

مسیریابی Routing:

دستور ip route که برای نوشتن static route مورد استفاده قرار می گیرد به شکل زیر می باشد.

ip route prefix mask { next-hop-ip-address | interface-type interface-number } [Administrative-Distance] [name next-hop-name] [Permanent]

در یک دستور Static Route حداقل می بایست ۳ پارامتر مشخص باشد:

۱- prefix

۲- mask

۳- next hop|interface

مسیریابی Routing:

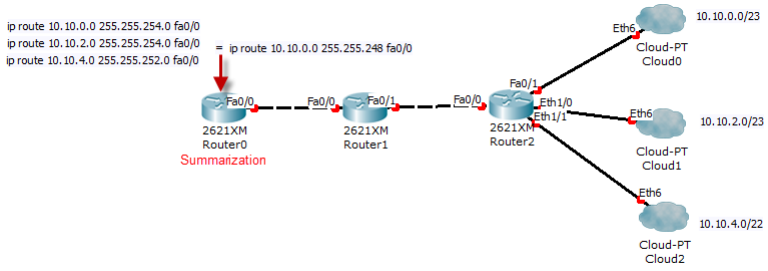
Prefix :این پارامتر به همراه mask ، الگوی زیر شبکه های مقصد را مشخص می کند بعنوان مثال زمانیکه می نویسیم ip route 10.10.1.0 255.255.255.0 ... به این معنی است که تمام بسته هایی که آدرس مقصد آنها واقع در الگوی مورد نظر هستند را route کن.

یعنی آدرسهای 10.10.1.1 تا 10.10.1.254 .

و زمانیکه می نویسیم ip route 10.10.0.0 255.255.0.0 ... به این معنی است که تمام آدرسهایی که در این الگو قرار دارد را با این دستور مسیریابی کن . که این الگو شامل مثلا زیر شبکه های 10.10.1.0/24 و 10.10.2.0/24 ویا 10.10.254.0/24 می شود.

مسیریابی Routing:

بکارگیری الگوی Prefix maskبه ما این امکان را می دهد که
برای چند زیر شبکه که بصورت مستقیم به روتر متصل نیستنددر صورت اختصاص مناسب
IP های زیر شبکه ها ، بجای چند Static Route
یک Static Route بنویسیم و این کار تعداد ردیفهای جدول مسیر یابی
را بطور قابل ملاحظه ای کم خواهد کرد و در نتیجه پردازشهای مسیر یابی
کاهش خواهد یافت به این عمل Summarization و یا خلاصه نویسی
گفته می شود که لازمه اینکار اختصاص صحیح
محدوده IP آدرسها به زیر شبکه هاست. در ادامه در این رابطه مثالی خواهیم داشت.

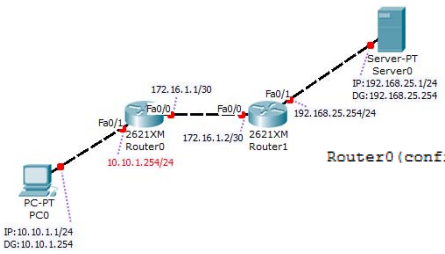


مسیر یابی Routing:

Next hop|interface:

در این قسمت مشخص می کنیم آدرسهای مقصدی که با الگو prefix و mask مشخص شده اند از طرف کدام اینترفیس از روتر ،خارج شوند. در واقع مسیری که نهایتا با خروج از روتر ،بسته به سمت مقصد باید در پیش بگیرد توسط این پارامتر مشخص می شود.

پارامتر مربوط به مسیر خروجی به دو شکل مشخص می شود که می توان هریک از این دوشکل را بکار برد اما این دو شکل استفاده تفاوتهایی با یکدیگر دارند که در ادامه مطرح خواهد شد. بار دیگر مثال قبل را در نظر بگیرید.



حالت ۱: استفاده از اینترفیس خروجی

```
Router0(config)#ip route 192.168.25.0 255.255.255.0 f0/0
```

M.Zangian

مسیر یابی Routing:

با ورود این دستور جدول مسیر یابی (Routing Table) به شکل زیر تغییر می یابد.

```
Router0#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.1.0 is directly connected, FastEthernet0/1
     172.16.0.0/30 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
S    192.168.25.0/24 is directly connected, FastEthernet0/0
```

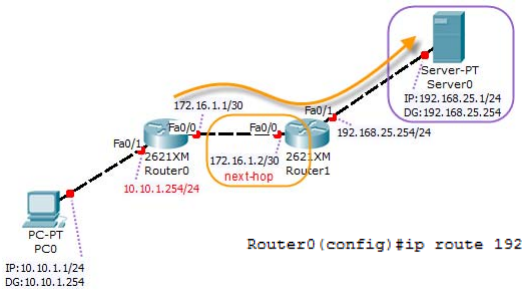
همانطوریکه مشاهده می شود ،در جدول مسیر یابی یک ردیف جدید که با حرف S مشخص شده است به جدول اضافه می گردد. حرف S بمعنی Static است.

M.Zangian

مسیریابی Routing:

حالت ۲: استفاده از next-hop

درحالت دوم ، بجای استفاده از اینترفیس خروجی از آدرس next-hop استفاده می نماییم




```
Router0(config)#ip route 192.168.25.0 255.255.255.0 172.16.1.2
```

در دیاگرام منطقی شبکه یاد شده بسته ها وقتی وارد روتر 0 می شوند برای رسیدن به زیر شبکه 192.168.25.0 می بایست از مسیری که نقطه بعدی آن ، 172.16.1.2 است بگذرند.

M.Zangian

مسیریابی Routing:

در این حالت جدول مسیر یابی روتر را بار دیگر بررسی می کنیم:

```
Router0#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.1.0 is directly connected, FastEthernet0/1
     172.16.0.0/30 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
S    192.168.25.0/24 [1/0] via 172.16.1.2
Router0#
```

در این حالت نیز به جدول مسیر یابی یک ردیف که با حرف S ، یعنی Static مشخص شده است ، اضافه شده است . اما تفاوت هایی در جدول مسیریابی در دوحالت مشاهده می شود.

M.Zangian

مسیریابی Routing:


```
Router0#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.1.0 is directly connected, FastEthernet0/1
     172.16.0.0/30 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
S    192.168.25.0/24 is directly connected, FastEthernet0/0
```

مشخص کردن مسیر بعدی با مشخص کردن اینترفیس خروجی(exit interface)

مشخص کردن مسیر بعدی با مشخص کردن next-hop

```
Router0#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.1.0 is directly connected, FastEthernet0/1
     172.16.0.0/30 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
S    192.168.25.0/24 [1/0] via 172.16.1.2
Router0#
```


مسیریابی Routing:

همانطوریکه مشاهده می شود درحالتیکه مسیر بعدی با اینترفیس خروجی مشخص می شود روتر مسیر را بصورت Directly Connected در نظر می گیرد درحالی که زیر شبکه مقصد ، بصورت Directly Connected نیست . که همین امر باعث ایجاد اختلاف زیادی در این دو روش می گردد.

در حالت دوم که مسیر بعدی با مشخص کردن آدرس Next Hop تعیین می شود ، مسیر بصورت یک رکورد استاتیک در جدول مسیریابی مشخص می گردد.

سیسکو توصیه کرده است که برای مسیریابی استاتیک بجای استفاده از اینترفیس خروجی حتما از آدرس next hop استفاده گردد.

استفاده از اینترفیس خروجی در مواردی که لینک ارتباطی در مسیر خروجی بصورت Point – to – point (نقطه به نقطه) باشد مشکلی ایجاد نمی نماید اما در مواردی که مسیر بعدی یک لینک از نوع shared Medium مانند اترنت باشد مشکلاتی ایجاد می نماید که در ادامه به بررسی آن خواهیم پرداخت.

مسیریابی Routing:

۱- هنگامی که یک مسیر بصورت پورت خروجی ، تعریف شود ، اطلاعات آن زمانی در جدول مسیر یابی قرار می گیرد که پورت مورد نظر Up باشد در غیر اینصورت مسیر مورد نظر در جدول قرار نخواهد گرفت.

۲- همانطوریکه گفته شد ،زمانیکه مسیر خروجی یک مسیر Shared Medium باشد ، در حالتیکه مسیربصورت اینترفیس خروجی تعریف گردد، روتر آنرا در جدول مسیریابی بصورت Directly Connected ثبت می نماید.بنابراین برای اینکه بسته به مقصدی که با prefix و mask مورد نظر match باشد ،ارسال شود روتر با فرض اینکه زیر شبکه مقصد بصورت مستقیم به روتر متصل است ، برای بدست آوردن MAC مقصد ، بسته ARP ایجاد می نمایدو در صورتیکه بر روی روتر بعدی Proxy-Arp فعال باشد ، روتر بعدی اینترفیس خود را بعنوان نماینده مقصد، معرفی می نماید و امکان ارسال به اینترفیس روتر بعدی فراهم می شود و اینکار چندین اشکال دارد. اول اینکه به ازای هر IP در زیر شبکه مقصد مورد نظر یک بسته ARP ، BroadCast می شود و در صورتیکه زیر شبکه مقصد بزرگ باشد ، این کار باعث افزایش پردازش روتر ، ایجاد جدول ARP Cache بزرگ می گردد که

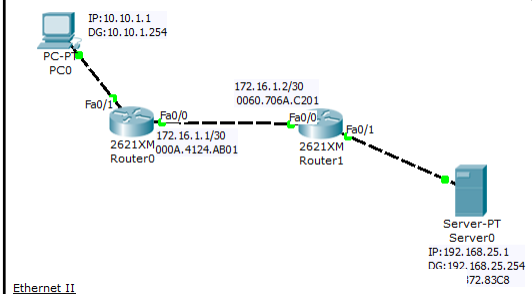
مسیریابی Routing:

در مواردی ممکن است باعث Overload روتر گردد این موضوع بخصوص زمانیکه از Default Route استفاده شود ، مشکل ساز است.

استفاده از IP ، next hop علاوه بر اینکه از ایجاد بسته های ARP جلوگیری می کند ، باعث می گردد در صورتیکه اینترفیس خروجی Down شود ، احتمال اینکه روتر بتواند با استفاده از مسیرهای دیگر به next hop دسترسی داشته باشد وجود دارد و در اینصورت بازهم ارتباط برقرا خواهد بود.

مسیریابی Routing:

۱- استفاده از اینترفیس خروجی



Ethernet II

0	4	8	14	19 Bytes
PREAMBLE: 101010...1011		DEST MAC: FFFF.FFFF.FFFF	SRC MAC: 000A.4124.AB01	
TYPE: 0x806	DATA (VARIABLE LENGTH)			FCS: 0x0

ARP

0	8	16	31 Bits
HARDWARE TYPE: 0x1		PROTOCOL TYPE: 0x800	
HLEN: 0x6	PLEN: 0x4	OPCODE: 0x1	
SOURCE MAC: 000A.4124.AB01 (48 bits)			
		SOURCE IP (32 bits) ==>	
172.16.1.1			
TARGET MAC: 0000.0000.0000 (48 bits)			
TARGET IP: 192.168.25.1 (32 bits)			

Ethernet II

0	4	8	14	19 Bytes
PREAMBLE: 101010...1011		DEST MAC: 000A.4124.AB01	SRC MAC: 0060.706A.C201	
TYPE: 0x806	DATA (VARIABLE LENGTH)			FCS: 0x0

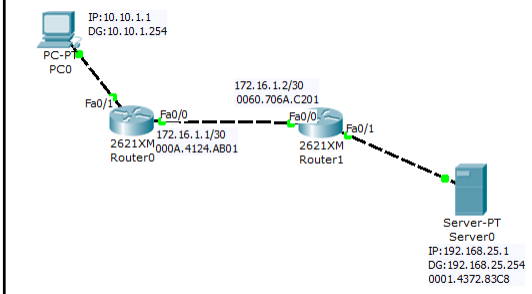
ARP

0	8	16	31 Bits
HARDWARE TYPE: 0x1		PROTOCOL TYPE: 0x800	
HLEN: 0x6	PLEN: 0x4	OPCODE: 0x2	
SOURCE MAC: 0060.706A.C201 (48 bits)			
		SOURCE IP (32 bits) ==>	
192.168.25.1			
TARGET MAC: 000A.4124.AB01 (48 bits)			
TARGET IP: 172.16.1.1 (32 bits)			

M.Zangian

مسیریابی Routing:

۲- استفاده از next-hop



Ethernet II

0	4	8	14	19 Bytes
PREAMBLE: 101010...1011		DEST MAC: FFFF.FFFF.FFFF	SRC MAC: 000A.4124.AB01	
TYPE: 0x806	DATA (VARIABLE LENGTH)			FCS: 0x0

ARP

0	8	16	31 Bits
HARDWARE TYPE: 0x1		PROTOCOL TYPE: 0x800	
HLEN: 0x6	PLEN: 0x4	OPCODE: 0x1	
SOURCE MAC: 000A.4124.AB01 (48 bits)			
		SOURCE IP (32 bits) ==>	
172.16.1.1			
TARGET MAC: 0000.0000.0000 (48 bits)			
TARGET IP: 172.16.1.2 (32 bits)			

Ethernet II

0	4	8	14	19 Bytes
PREAMBLE: 101010...1011		DEST MAC: 000A.4124.AB01	SRC MAC: 0060.706A.C201	
TYPE: 0x806	DATA (VARIABLE LENGTH)			FCS: 0x0

ARP

0	8	16	31 Bits
HARDWARE TYPE: 0x1		PROTOCOL TYPE: 0x800	
HLEN: 0x6	PLEN: 0x4	OPCODE: 0x2	
SOURCE MAC: 0060.706A.C201 (48 bits)			
		SOURCE IP (32 bits) ==>	
172.16.1.2			
TARGET MAC: 000A.4124.AB01 (48 bits)			
TARGET IP: 172.16.1.1 (32 bits)			

M.Zangian

مسیریابی Routing:

405

Administrative Distance:

از آنجاییکه پروتکل های مسیر یابی مختلف ممکن است در یک روتر مورد استفاده قرار گیرد و این پروتکلها بر اساس معیارهای متفاوت ، یک مسیر را برای رسیدن به مقصد در نظر بگیرند ما با تعدادی مسیر مواجه خواهیم بود که برای رسیدن به مقصد وجود دارند و هریک توسط پروتکل های مسیر یابی متفاوت ایجاد شده اند در اینجا پارامتر Administrative Distance این امکان را می دهد که به هر پروتکل مسیر یابی یک عدد بین0 تا 255 اختصاص دهیم که بیانگر قابلیت اطمینان بودن یک پروتکل است . عدد 0 در این پارامتر بیشترین قابلیت اطمینان و عدد 255 بمعنی غیر قابل اعتماد بودن یک پروتکل مسیر یابی است .بنابراین اگر برای یک مقصد دو یا چند مسیر وجود داشته باشد که با پروتکل های مسیر یابی متفاوتی ایجاد شده باشند ، مسیری در نظر گرفته می شود که مربوط به پروتکلی با AD کمتر باشد.

بصورت پیش فرض برای هر پروتکل یک AD در نظر گرفته شده است که این مقدار می تواند توسط مدیر سیستم تغییر یابد.

M.Zangian

مسیریابی Routing:

406

همانطوریکه در جدول مقابل مشاهده می شود مسیرهای Directly Connected بالاترین اولویت را در مسیر ها دارد.

Route Source	Default Distance Values
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown*	255

مقادیر Administrative Distance برای پروتکل های مختلف مسیریابی

M.Zangian

مسیر یابی Routing:

متریک (Metric):

از پارامترهای مهم دیگری که در انتخاب یک مسیر مورد استفاده قرار می گیرد ، متریک است . در واقع متریک عبارتست از **محاسبه هزینه مسیر های متفاوت برای یک پروتکل**. همانطوریکه می دانیم ، هر پروتکل مسیر یابی براساس معیارهایی مشخص و متفاوت ،هزینه مربوط به انتخاب یک مسیر را برای رسیدن به مقصد تعیین می نماید. به این هزینه محاسبه شده متریک گفته می شود.

در واقع براساس متریک مسیرهای مشابه برای رسیدن به یک مقصد مشخص که توسط **یک پروتکل خاص مسیر یابی** ایجاد شده است ، اولویت بندی می شوند.

در واقع متریک اولویت مسیر های مشابه را برای یک پروتکل را تعیین می نماید در حالیکه AD اولویت مسیرهای مشابه را که براساس پروتکل های مختلف ایجاد شده اند را تعیین می نماید.

مسیر یابی Routing:

```
Router0#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.1.0 is directly connected, FastEthernet0/1
     172.16.0.0/30 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
S    192.168.25.0/24 [1/0] via 172.16.1.2
Router0#
```

بار دیگر جدول مسیر یابی را برای مثال قبل بررسی می نماییم . همانطوریکه گفته شد ، زیر شبکه هایی که بصورت مستقیم به روتر متصل اند با حرف C مشخص شده و AD آنها صفر است و دارای بالاترین اولویت بین پروتکل های مسیر یابی هستند . مسیرهایی که توسط مسیریابی استاتیک و بصورت next hop تعیین می شود با حرف S مشخص می شود و به ترتیب اطلاعات مربوط به prefix وmask زیر شبکه مقصد آورده می شود . سپس یک زوج عدد که بصورت [1/0] مشخص شده را می بینیم که این دو پارامتر به ترتیب AD و Metric مربوط به مسیر تعیین شده هستند بعبارت دیگر:

[Administrative Distance/Metric]

مسیر یابی Routing:

AD برای مسیریابی استاتیک برابر ۱ است ، هرچند که ایجاد مسیر یابی استاتیک با روش مشخص کردن اینترفیس خروجی بصورت Directly Connected در نظر گرفته می شود ، اما بازهم AD برای این حالت نیز ۱ می باشد(در IOS های قدیمی تر AD برای این روش صفر در نظر گرفته می شد اما در IOS های جدید این مسئله اصلاح شده است.)

مسیر یابی Routing:

انتخاب بهترین مسیر بر اساس پارامترهای موثر:

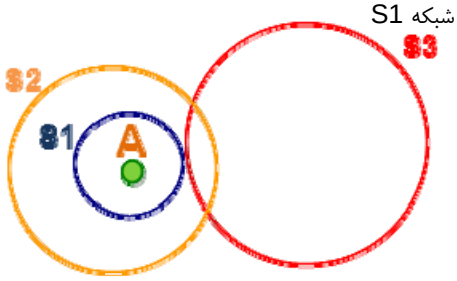
سئوالی که ممکن است در اینجا مطرح شود اینستکه فرض کنیم در یک مسیر یاب بر اساس پروتکلهای مختلف مسیر یابی ، جدول مسیر یابی تشکیل شده است حال سئوال اینجاست از بین مسیرهایی که به مقصد ختم می شوند کدام مسیر در اولویت قرار گرفته و انتخاب می شود؟

در مباحث قبلی پارامترهایی که در اولویت بندی مسیرها موثرند را بررسی نمودیم از جمله AD(Administrative Distance) و Metric .اما قبل از بررسی این دو پارامتر می بایست مسیر هایی در نظر گرفته شوند که الگوی زیر شبکه مقصد،که با Prefix و Mask مشخص می شود ، مقصد را در بر بگیرد و دوم اینکه این الگو از زیر شبکه مقصد ،کوچکترین زیر شبکه باشد. به عبارت دیگر مسیری در اولویت بالاتر قرار می گیرد که در مرحله نخست ، مقصد در الگوی زیر شبکه مقصد وجود داشته باشد و Subnet مورد نظر کوچکترین باشد.

مسیر یابی Routing:

به شکل زیر توجه نمایید:

در این شکل دستیابی به آدرس مقصد A در نظر است اگر ۳ مسیر با سه الگوی زیر شبکه مقصد S1,S2,S3 در جدول مسیر یابی مشخص شده باشد ، از مسیر با الگوی زیر شبکه S3 صرفنظر می گردد چراکه مقصد A درون این زیر شبکه قرار ندارد . اما مسیرهایی با زیر شبکه S1و S2 هر دو مقصد را شامل می شوند سئوال اینجاست کدام مسیر در اولویت قرار می گیرد؟ در اینجا قبل از بررسی هر گونه پارامتر دیگری در یافتن بهترین مسیر ، مسیری انتخاب می شود که مقصد را در برگرفته و زیر شبکه کوچکتری داشته باشد یعنی زیر شبکه S1



A:192.168.1.1/24

S1:192.168.1.0/30

S2:192.168.1.0/24

S3:192.168.2.0/24

مسیر یابی Routing:

مثال:

در یک روتر سه مسیر با پروتکلهای مختلف بدست آمده است برای مقصد های 192.168.32.1 192.168.32.100 , مشخص نمایید نتیجه کدام پروتکل در نظر گرفته می شود.

EIGRP (Internal): 192.168.32.0/19 192.168.32.0-192.168.63.255
RIP: 192.168.32.0/26 192.168.32.0-192.168.32.63
OSPF: 192.168.32.0/24 192.168.32.0-192.168.32.255

```
router# show ip route
     ....
     D   192.168.32.0/19 [90/25789217] via 10.1.1.1
     R   192.168.32.0/26 [120/4] via 10.1.1.2
     O   192.168.32.0/24 [110/229840] via 10.1.1.3
     ....
```

مسیر یابی Routing:

در مثال بالا از نظر AD ، پروتکل EIGRP(AD=90) نسبت به OSPF(AD= 110) و RIP(AD=120) اولویت بالاتری دارد . اما قبل از بررسی AD باید توجه نمود که الگوهای زیر شبکه یکسان نیست.در یک نگاه مشخص است هر سه الگوی زیر شبکه مقصد 192.168.32.1 را در برمی گیرد. پس الگوی با prefix بزرگتر(زیر شبکه کوچکتر) در اولویت قرار می گیرد. بنابراین مسیر مشخص شده توسط پروتکل RIP برای رسیدن به مقصد 192.168.32.1در نظر گرفته می شود. یعنی بسته به سمت Next Hop ، 10.1.1.2 ارسال می گردد.

الگوی زیر شبکه 192.168.32.0/26 ، مقصد 192.168.32.100 را در بر نمی گیرد.بنابراین از انتخابها خارج می شود. بین الگوهای زیر شبکه 192.168.32.0/19 , 192.168.32.0/24 که هر دو مقصد 192.168.32.100 را در بر می گیرند،مسیر تعیین شده توسط پروتکل OSPF در نظر گرفته می شود. یعنی next hop 10.1.1.3

```
router# show ip route
     ....
     D   192.168.32.0/19 [90/25789217] via 10.1.1.1
     R   192.168.32.0/26 [120/4] via 10.1.1.2
     O   192.168.32.0/24 [110/229840] via 10.1.1.3
     ....
```

M.Zangian

مسیر یابی Routing:

بطور خلاصه بهترین مسیر به ترتیب براساس سه پارامتر تعیین می شوند:

۱- بالاترین اولویت مربوط به مسیر هایی است که الگوی مقصد (Prefix , Mask) در جدول مسیر یابی ضمن در برگرفتن مقصد،کوچکترین الگوی مقصد باشد.

۲- در مرحله دوم ، مسیرهای مشابه با اندازه الگوی مقصد یکسان ،که AD کوچکتری داشته باشد در اولویت قرار می گیرد.

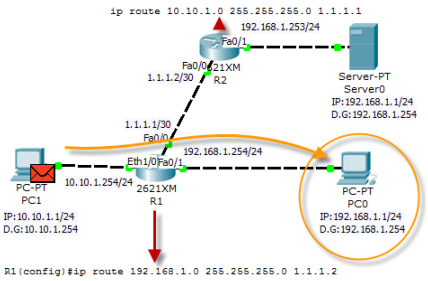
۳- اگر مسیر هایی با الگوی مقصد هم اندازه و در برگیرنده مقصد، AD یکسانی داشته باشند پارامتر تعیین کننده متریک یا هزینه محاسبه شده است . هر میزان متریک کوچکتر باشد مسیر اولویت بالاتری دارد.

نکته:

ترتیب نوشتن Route ها تاثیری در اولویت آنها ندارد.

M.Zangian

مسیریابی Routing:



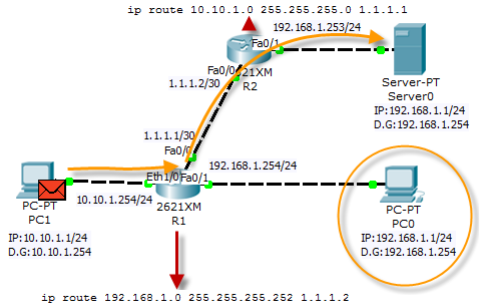
در دیاگرام روبرو در روتر R1 دو مسیر برای دستیابی به مقصد 192.168.1.1مشخص شده است یکی بصورت Directly Connected و دیگری بصورت Route استاتیک .

```
R1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/30 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, FastEthernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.1.0 is directly connected, Ethernet1/0
C    192.168.1.0/24 is directly connected, FastEthernet0/1
R1#
```

با توجه به اینکه اندازه الگوی شبکه در برگیرنده مقصد در هر دو مسیر،به یک اندازه است، AD اولویت مسیریابی را مشخص می کند بنابراین مسیر Directly Connected تعیین می شود. چون AD کوچکتری دارد.توجه نمایید در جدول مسیریابی بدلیل اینکه دو الگوی زیر شبکه مقصد یکسان است ، فقط مسیر با AD کوچکتر نصب می گرددو مسیر استاتیک مورد قبول واقع نمی شود.

M.Zangian

مسیریابی Routing:



در دیاگرام روبرو با وجود اینکه PC0 بصورت Directly Connected است ، بسته ها به مقصد PC0 از مسیر R2 می گذرد و به مقصد Server0 می رسد.

```
R1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/30 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, FastEthernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.1.0 is directly connected, Ethernet1/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, FastEthernet0/1
S       192.168.1.0/30 [1/0] via 1.1.1.2
```

با توجه به تفاوت prefix ها ، الگوهای زیر شبکه یکسان نیست بنابراین هر دو مسیر در جدول نصب می گردد.

علت انتخاب مسیر R2 ، کوچکتر بودن الگوی در برگیرنده مقصد در Route استاتیک است. بنابراین مسیر تعیین شده بصورت استاتیک در اولویت قرار می گیرد.

192.168.1.0/30 <192.168.1.0/24

M.Zangian

مسیریابی Routing:

نکته ۱ : اگر الگوی شبکه مقصد در چند پروتکل مسیر یابی مختلف یکسان باشدو AD پروتکل های مختلف را بگونه ای تغییر دهیم که مقادیر یکسانی داشته باشند. در این حالت روتر بر اساس مقادیر پیش فرض AD ، اولویت را تعیین می کند و به تغییر AD توجهی نمی کند. توجه شود زمانی تغییر AD در نظر گرفته نمی شود که برای پروتکلهای مسیریابی مختلف بصورت دستی AD یکسانی در نظر گرفته شود.

نکته ۲: متریک تنها زمانی در نظر گرفته می شود که الگوی مقصد در برگیرنده مقصد یکسان بوده و مسیرها توسط یک پروتکل مسیریابی تعیین شده باشند.(ADبرای مسیرهای مختلف یکسان باشد.)

مسیریابی Routing:

نکته ۳: اگر الگوی زیر شبکه مقصد، برای چند مسیر یکسان بوده و مسیرها AD یکسانی داشته باشند، یعنی مسیرها از پروتکل مسیر یابی یکسان بدست آمده باشندو متریک مسیرها نیز یکسان باشد، ترافیک بین مسیرهای با متریک یکسان ،توزیع می شود .بعبارت دیگر بین مسیرها Load Balancing انجام می شود.Load Balancing در یک روترسیسکو تا ۶ مسیر مختلف را می تواند در بر بگیرد. (برخی از پروتکلهای مسیر یابی امکان Load Balancing را برای مسیرهای با متریک متفاوت دارند که موضوع بحث نیست.)

مسیریابی Routing:

Default Route:

Default Route یک Route استاتیک است که الگوی شبکه مقصد آن بزرگترین الگوی شبکه بوده و هر شبکه ای را در بر می گیرد. الگوی شبکه مقصد برای Default Route 0.0.0.0 0.0.0.0 می باشد.اگر این Route در تنظیمات مورد استفاده قرار گیرد در صورتیکه هیچ الگویی در جدول مسیریابی، مقصد مورد نظر را در برنگیرد. این Route مورد استفاده قرار می گیرد.

همانطوریکه گفتیم در اولویت Route ها اندازه الگوی زیر شبکه مقصد که مقصد را در بر داشته باشد ،در اولین مرحله مورد بررسی قرار می گیردو الگوهایی انتخاب می شوند که علاوه بر اینکه مقصد را شامل می شود، کوچکترین باشد. Default Route بزرگترین الگوی زیر شبکه مقصدی است که هر مقصدی را شامل می شود.بنابراین تنها در زمانی مورد قبول واقع می شود که هیچ یک از زیر شبکه های جدول مسیریابی ، مقصد مورد نظر را در بر نگیرند. همانند Route استاتیک ،مسیر می تواند با آدرس next hop و یا با مشخص کردن اینترفیس خروجی تعیین شود.

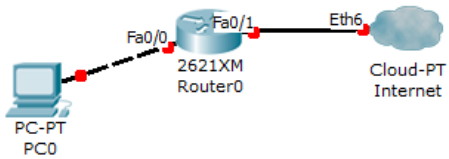
```
R1(Config)#ip route 0.0.0.0 0.0.0.0 10.10.1.1
```

M.Zangian

مسیریابی Routing:

Default Route معمولا در سطح تجهیزات Access بکار می رود بدین معنی که در روتری که نقطه انتهایی یک شبکه محسوب می شودو تنها یک مسیر برای ارتباط با خارج از شبکه وجود دارد.

بعنوان مثال فرض کنید در شبکه زیر ایستگاههای یک شبکه بخواهند به اینترنت دسترسی داشته باشند.



در چنین حالتی اینترنت مجموعه بسیار بزرگی از زیر شبکه های مختلف است و امکان اینکه تمام زیر شبکه ها را بصورت استاتیک برای روتر مشخص کنیم و همگی را به طرف یک next hop هدایت کنیم وجود ندارد. بنابراین در چنین حالتی با نوشتن یک Default Route به روتر می فهمانیم هر بسته که مقصد آن در جدول مسیریابی مشخص نبود را به سمت اینترنت ارسال نماید بنابراین با یک Route تمام آدرسهای مربوط به اینترنت به سمت خارج از شبکه هدایت می شوند.

M.Zangian