هدف اصلی فناوری اطلاعات: IT

گردآوری،سازماندهی و فراوری داده ها و دانش پراکنده در سطح دنیاست به گونه ای که بتوان از این دانش گردآوری شده،معرفت و دانش جدید تولید کرد.

شبکه های کامپیوتری:

مجموعه ای از کامپیوترهای مستقل است که از طریق یک رسانه انتقال با یکدیگر به تبادل اطلاعات می پردازند.

رسانه انتقال یا کانال مخابراتی: Media

به هر محیط مادی یا غیر مادی اطلاق میشود که داده ها از طریق آن از مبدا به مقصد منتقل میشوند.

لینک: **Link**

وقتی دو یا چند دستگاه بر اساس قواعد از قبل مشخص و استاندارد ،داده ها را به روشی قانونمند نشانه گذاری (encode) ،سازماندهی و سپس بین یکدیگر مبادله میکنند میگوئیم لینک (پیوند) پدید آمده است.

Internet

مجموعه ای از شبکه های مستقل و مرتبط با یکدیگر است که ارتباطات همگانی را میسر کرده است.

Web

روشی برای سازماندهی اطلاعات است به گونه ای که غیر از کنار هم قرار دادن متن،صدا،تصویر،گرانیک، سادگی دسترسی به اطلاعات پراکمده دنیا،ازطریق مفهومی بنام ابرپیوند hyperlink

Interanet

شبکه ای داخلی(با تملک سازمانی یا خصوصی) است که از پروتکلهای مرتبط با اینترنت و مخصوصا تکنولوژی وب برای سازماندهی شبکه استفاده میکند.(TCP/IP-HTTP-WWW)
Interanet الزاما به internet وصل تمیباشد.

کاربردهای شبکه های کامپیوتری

1-اشتراک منابع: به اشتراک گذاشتن سخت افزار ،نرم افزار و داده های مورد نیاز در شبکه

2- حذف محدودیتهای جغرافیایی در تبادل داده ها: شبکه های ...,WAN

3- کاهش هزینه ها: پست الکترونیک و استفاده مشترک از سخت افزارهای گران قیمت

4- بالا رفتن قابلیت اعتماد سیستمها: Reliability کانالهای انتقال در زیر ساخت ارتباطی شبکه ،باعث شده که قطع یکی از کانالها منجر به از دست رفتن کل شبکه نشود.

5- افزایش کارائی سیستم: توزیع وظائف سازمانی یک مجموعه همانند بانک به ماشینهای متفاوت در آن شبکه ضمن حفظ استقلال کارائی سیستم را ازلحاظ دسترسی اطلاعات ،سرعت پذازش و ذخیره و بازیابی اطلاعات افزایش خواهد داد

خدماتی که شبکه ها ارائه میکنند.

Remote access-Email-File transfer-Remote login,News groups-Information seek-Advertisement-Ebanking-Teleconference-People finding

دسته بندی سخت افزار شبکه های کامپیوتری

دیدگاه اول تکنولوژی انتقال

تکنولوژی انتقال

شبکه های پخش فراگیر Broadcast

-انتقال اطلاعات از طریق یک کانال فیزیکی که بین تمام ایستگاههای شبکه مشترک است انجام میشودو ایستگاهها موظفند بطور دائم به خط گوش دهند.

معایب

مدیریت پیچیده کانال:

-هر ایستگاه عنصری مستقل محسوب میشود و هیچگونه حاکمیت بیرونی بر آنها وجود ندارد ،رعایت قانون و نوبت استفاده از کانال بر عهده ایستگا هاست

امنیت کم:

-با توجه به اینکه تمام ایستگاهها موظف به گوش دادن به خط هستند بنابراین اطلاعات روی کانال توسط همه ایستگاهها شنیده میشود و امکان استراق سمع وجود دارد.

کارائی پایین:

-چون تمام ایستگاهها فقط یک کانال در اختیار دارند ،لذا سهم کوچکی از کل پهنای باند در اختیار یک ایستگاه قرار میگیرد و اگر تصادم نیز وجود داشته باشد که چه بدتر

شبکه های نقطه به نقطه Point to Point

-در شبکه های نقطه به نقطه هرگاه بین دو ماشین خط مستقیمی وجود نداشته باشد بسته های حاوی داده میتوانند با گذر از چند ماشین میانی دست به دست و تحویل مقصد شوند

- عناصر سوئیچ یا مسیر یاب وظیفه دارد بسته های حاوی اطلاعات را به گونه ای هدایت کند که در رسیدن به مقصد کمترین تاخیر و کوتاهترین مسیر را تجربه کنند Routing

دیدگاه دوم مقیاس بزرگی شبکه و ناحیه تحت پوشش PAN-LAN-MAN-RAN-WAN

دیدگاه دوم مقیاس بزرگی شبکه و ناحیه تحت پوشش

شبکه های شخصی PAN:personal area network

- برای محدوده زیر 10 متر در نظر گرفته شده است و مالکیت فردی دارد.،تکنولوژی USB (سیمی) و بلوتوث(بی سیم) برای این رده از شبکه ها توسعه داده شده اند.

شبکه های محلی LAN:local area network

- در فواصل محدود جغرافیایی حداکثر یکی دو کیلومتر و تحت تملک سازمانهای کوچک،نهادها،ادارات و محیطهای آموزشی کوچک نصب و راه اندازی میگردد.
- با توجه به کوتاه بودن طول کانال1- افت سیگنال کم 2- نرخ خطا بسیار پایین است.
- نرخ ارسال میتواند بسیار با لا باشد و تاخیر انتشار بسیار ناچیز است(propagation delay).
- با توجه به محدود بودن تعداد ایستگاهها ،مدیریت شبکه اسانتر از بقیه شبکه هاست
- هزینه نصب و راه اندازی این شبکه ها چندان بالا نیست و دارای شاخصی به اسم توپولوژی هستند. Topology

(IEEE 802.3) Token ring (IEEE 802.11)Wi-Fi

شبکه های بین شهری MAN:metropolitan area network

- شبکه های بین شهری در گستره یک منطقه وسیع مانند یک شهر پیاده سازی میگردد(حدود 100 الی 200 کیلومتر)

(IEEE 802.16) DQDB FDDI

شبکه های منطقه ای RAN:regional area network

- در در گسترده وسیعی از یک کشور(مانند شبکه استانی یا ایالتی) و عموما با هدف خاص پیاده سازی میشود

(IEEE 802.22)

شبکه های گسترده WAN:wide area network

- در در گسترده وسیعی از یک کشور،قاره و یا جهان پیاده میشود و شبکه های محلی و بین شهری را به هم متصل می نماید و یک زیر ساخت ارتباطی یا ستون فقرات است

توپولوژی:

چگونگی اتصال ماشینها از طریق کانال فیزیکی به یکدیگر (توپولوژی) آن شبکه گفته میشود.
چگونگی همبندی و اتصال ماشینها به کانال انتقال و ایجاد یک شبکه واحد را اصطلاحا توپولوژی شبکه گویند.

توپولوژیهای رایج

توپولوژی خطی (BUS) - تمام ماشینها از طریق یک کانال فیزیکی مشترک به همدیگر متصل شده اندو بعلت سادگی در نصب و راه اندازی و ارزان بودن ،یکی از شبکه های پر رونق دنیا محسوب میشد.

توپولوژی حلقه (Ring) - توپولوژی حلقه از لحاظ ظاهری نقطه به نقطه به نظر میرسد ولی باطنا از نوع پخش فراگیر میباشد Broadcast

توپولوژی ستاره (Start) - ارتباط تمام ماشینهای شبکه از طریق یک گره مرکزی برقرار میشود. این گره میتواند یک سوئیچ بسیار سریع و هوشمند باشد یا یک هاب معمولی یا یک کامپیوتر

توپولوژی درختی یا سلسله مراتبی (Hierarchy) - از بهم پیوستن چند شبکه با توپولوژی ستاره پدید می آید

توپولوژی با اتصال کامل یا توری شکل(Full connected) - بین هر دو ماشین در شبکه یک کانال انتقال مستقیم وجود دارد. - هر ماشین حداقل با چهار ماشین همسایه خود دارای کانالی اختصاصی است

شبکه های بین شهری (MAN) - در یک منطقه وسیع و برای اتصال چند شبکه محلی استفاده میشود ،طول کانال زیاد است(بیش از 100 کیلومتر)،و معمولا رسانه دیجیتال آن فیبر نوری میباشد.

شبکه های گسترده (WAN) - این شبکه ساختار همگون و یکسان ندارد.پس ماشینها از سخت افزار و نرم افزار متنوعی استفاده میکنند که بطور ذاتی با هم سازگار نیستند.

- در WAN به ماشینهای نهایی که در اختیار کاربر قرار دارد و برنامه های کاربردی اورا اجرا میکند ماشین میزبان گویند Host
- آنچه بین همه ماشینهای میزبان یکسان است زبان مشترکی برای مبادله اطلاعات ،نحوه گفتگو و قالب پیام هاست.

وظیفه (communication Subnet) زیر شبکه نقل و انتقال داده های یک ماشین میزبان به ماشینی دیگر بر روی شبکه های پراکنده در جهان است

زیر ساخت ارتباطی در شبکه WAN

عناصر سوئیچ Switching elements

- عناصر سوئیچ و مسیر یابها در زیر شبکه از روش (سوئیچ بسته) استفاده میکنند ،این عناصر اصطلاحا از قاعده (دریافت،ذخیره،و هدایت به جلو) پیروی میکند.
- هرگاه مسیر یابها در زیر ساخت شبکه یک بسته را بطور کامل دریافت و در حافظه خود ذخیره کنندو سپس به پردازش و هدایت آن مشغول شوند اصطلاحا به روش (ذخیره /ارسال) عمل کرده اند. Store & Forward
- هر گاه دو یا چند شبکه محلی از طریق یک زیرساخت ارتباطی بهم متصل شده و یک شبکه یکپارچه واحد پدید آید اصطلاحا یک Internetwork پدید آمده است.
- به عمل یکپارچه سازی چند شبکه از طریق یک زیر ساخت ارتباطی اصطلاحا همبندی شبکه ها Internetworking گفته میشود.

خطوط ارتباطی یا کانالها Trunk-Channels-circuit

- این خطوط ،کانالهای انتقال با پهنای باند بالا هستند که ارتباط عناصر سوئیچ را برقرار میکنند.و اغلب از نوع نقطه به نقطه هستند.

روشهای انتقال اطلاعات بین دو ماشین در زیر ساخت شبکه

سوئیچینگ مداری (Circuit Switching)

- ابتدا برای انتقال اطلاعات بین دو ماشین ابتدا یک اتصال فیزیکی مابین آنها برقرار میشود و یک مدار بسته بین گیرنده و فرستنده پدید می آید (مانند سوئیچینگ تلفن)
- پس از شماره گیری مدار برقرار میشود و پس از پایان ارتباط کلیه سوئیچهای میانی به حالت باز بر میگردند.

سوئیچینگ پیام (Message Switching)

- در ان روش که صرفا مختص داده ای دیجیتالی است ،هر ایستگاه یک اتصال دائمی و همیشه وصل با مرکز سوئیچ خود دارد.
- مرکز سوئیچ یک کامپیوتر با تعداد زیادی پورت دیجیتال (ورودی/خروجی) است و مجهز به حافضه اصلی و حافضه جانبی
- این روش یک عیب اساسی دارد و آنهم **(عدم محدودیت طول پیام)** است و اشکالات عمده آن بشرح زیر است.

معایب

- هر مرکز سوئیچ باید فضای حافظه بسیار زیادی برای ذخیره سازی حجم انبوه پیام ها داشته باشد.
- در صورت بروز حتی یک بیت خرابی در پیام(ناشی از خطای کانال) حجم بسیار زیادی از داده ها باید مجددا ارسال شود.
- چون هر مرکز سوئیچ موظف است کل پیام را دریافت کرده و سپس آنرا به کانال مناسب هدایت نماید لذا تاخیر رسیدن پیام زیاد خواهد شد.

سوئیچینگ بسته و سلول(Packet Switching/Cell Switching)

- در هر بار ارسال کل پیام بزرگ به قطعات کوچکتری بنام (بسته) تقسیم شده و ضمن اضافه شدن اطلاعات لازم برای بازسازی اصل پیام به هر بسته آنها را جداگانه به مرکز سوئیچ ارسال میشود.
- مجموع تاخیر در روش سوئیچ بسته کمتر از روش سوئیچ پیام خواهد بود.
- در مراکز سوئیچ مدرن که با سرعت بسیار بالا عمل میکند **طول بسته ها ثابت و بسیار کوچک** است مانند بسته ATM با 48 بایت داده و 5 بایت سرایند مجموعا 53 بایت.
- سوئیچهای ATM با نرخ ارسال 155.52 Mbps و 622.08 Mbps و بالاتر در دسترس است.
- مراکز سوئیچ بسته یا سلول ، اصطلاحا از قاعده (دریافت،ذخیره، و هدایت به جلو) پیروی میکنند.

بخشی از مسائل در طراحی لایه های شبکه

معماری و عملکرد لایه ای شبکه

- به دلیل پیچیدگی بسیار زیاد و گستره مولفه هائی که پیکره یک شبکه را تشکیل میدهند ،معماری یک شبکه کامپیوتری بصورت لایه ای طراحی میشود.
- تبدیل بیت ها به یک سیگنال متناسب با کانال انتقال (کانالهای مسی،فیبر نوری،ماهواره ای،رادیویی)
- ماهیت انتقال در ارتباط بین دو موجودیت(Entity) می باشد. در سه رده زیر

Simplex - ارتباط یکطرفه(یکطرف همیشه فرستنده و طرف دیگر همیشه گیرنده)

Half Duplex - ارتباط دو طرفه غیر همزمان(هر دو ماشین میتوانند فرستنده یا گیرنده باشند ولی نه بصورت همزمان

Full Duplex - ارتباط دو طرفه همزمان

- مسئله خطا و وجود نویز در کانالهای مخابراتی و کنترل خطا Error Control
- پیدا کردن بهترین مسیر و هدایت بسته ها از طریق آن مسیر
- هماهنگی سرعت مبدا و مقصد Flow Control
- موضوعاتی همچون ازدحام،تداخل و تصادم باید در سطح سخت افزار و نرم افزار بررسی شود.
- تحلیل توزیع داده و تضمین امنیت دادهای در حال جریان و مدیریت نشستها

اصول طراحی لایه های شبکه

- هر لایه وظیفه مشخصی دارد و طراح شبکه باید به دقت تشریح کند
- هرگاه سرویسهایی که باید ارائه شود از نظر ماهیتی متفاوت باشد باید لایه به لایه و جداگانه طراحی شود.
- وظیفه هر لایه باید با توجه به قراردادها و استانداردهای جهانی مشخص شود.
- تعداد لایه ها نباید آنقدر زیاد باشد که تمایز لایه ها از دیدگاه سرویسهای ارائه شده نامشخص باشدو نه آنقدر کم باشد ،که وظیفه و خدمات یک لایه،پیچیده و نامشخص شود
- باید مرزهای هر لایه به گونه ای انتخاب شود که جریان اطلاعات بین لایه ها ،حداقل باشد.

لایه های همتا **Peer**

-لایه های n ام از هر دو ماشین همتای یکدیگر هستند.
- هر پردازش و فعل و انفعالی که در لایه nام از ماشین مبداء بر روی داده ها انجام میشود فقط در لایه همتا در ماشین مقصد قابل بهره برداری است.

پروتکل **Protocol** - عبارت است از کلیه قراردادهای توافق شده بین دو لایه همتا برای برقراری و پیشبرد یک ارتباط(قالب پیامها،نحوه تبادل بسته ها)

سرویس **Service**

- عبارت است از مجموعه کارهایی که یک لایه برای لایه های بالاتر از خود انجام میدهد.
- سرویس در واقع بین دو لایه مجاور بر روی یک اشین واحد تعریف میشود،لایه پایینی لایه ارائه دهنده سرویس و لایه بالایی مصرف کننده آن سرویس است.

معماری شبکه **Network Architecture** - به مجموعه لایه ها و پروتکلهای آن معماری شبکه گفته میشود.

PDU protocol data unit - به قطعه داده ای که در هر لایه (طبق پرتکل مربوطه) سازماندهی و تحویل لایه زیرین میشود بطور عام و انتزاعی PDU گفته میشود.

مدل مرجع **Reference Model** - عبارتست از توصیف انتزاعی معماری لایه ای شبکه

مدل مرجع **OSI (open system interconnection)** - در این مدل وظائف و خدمات شبکه در هفت لایه مجزا تعریف(طراحی) و ارائه میشود.

Hardware Layer	***لایه*** 1	***لایه فیزیکی***	**Physical Layer**	
	لایه 2	***لایه پیوند داده ها***	**Data Link Layer**	
	لایه 3	***لایه شبکه***	**Network Layer**	
Software Layer	***لایه*** 4	***لایه انتقال***	**Transport Layer**	
	لایه 5	***لایه نشست(جلسه)***	**Session Layer**	
	لایه 6	***لایه نمایش(ارائه)***	**Presentation Layer**	
	لایه 7	***لایه کاربرد***	**Aplication Layer**	

OSI Layers

① Physical Layer

- وظیفه اصلی انتقال بیتها بر روی کانال مخابراتی است (ارسال یا دریافت بیتهای 0 و 1)
- ماهیت فیزیکی خط انتقال (مسی،فیبر نوری،...)
- ظرفیت کانال فیزیکی و نرخ ارسال Channel Capacity and Bit rate
- چگونگی نمایش بیتها در قالب سیگنالی متناسب با کانال
- نوع مدولاسیون
- مسائل مکا نیکی و الکتریکی مانند نوع کابل ،باند فرکانسی و نوع رابط کابل(کانکتور)
- این لایه هیچ وظیفه ای در مورد تشخیص خطا ندارد

② Data Link Layer

- بیمه اطلاعات در مقابل خطاهای احتمالی(مکانیزمهای کشف و کنترل خطا)
- تبدیل اطلاعات ارسالی از لایه های بالاتر به فریم frame و ارسال آن به لایه فیزیکی بصورت بیت به بیت
- کشف خطا از طریق اضافه کردن بیتهای کنترل خطا مثل بیتهای Parity ،Cheksum و CRC
- کنترل جریان (تنظیم جریان ارسال فریم به گونه ای که یگ گیرنده کند نیز بتواند فریمها را دریافت نماید. Flow Control
- تایید وصول داده ها یا عدم دریافت صحیح هر فریم به فرستنده (مشترک با لایه انتقال)
- پس از تحویل یک واحد اطلاعاتی به مقصد وظیفه این لایه تمام میشود.
- راه اندازی ،سرویس گیری و کنترل سخت افزار لایه فیزیکی بر عهده این لایه است

③ Network Layer

- مهمترین وظیفه این لایه مسیر یابی است.
- اگر بین دو ماشین در شبکه مسیر های گوناگونی وجود داشته باشد هدایت بسته های اطلاعاتی بسمت مقصد بر عهده این واحد است.
- مسیر یابی به دو صورت ایستا (تعیین و پیکره بندی توسط عامل انسانی) و همشمند میتواند باشد.
- در این لایه تمام ماشینهای شبکه نیازمند یک آدرس جهانی و یکتا هستند IP Global Address

④ Transport Layer

- وظیفه کلیدی این لایه آنست که داده ها را از لایه بالاتر دریافت کرده و در صورت نیاز آنرا به با اندازه متناسب تقسیم بندی کرده و پس از ضمیمه کردن شناسنامه لازم آ«ها را جهت ارسال تحویل لایه شبکه دهد.

- مطمئن شود که ماشین گیرنده آماده دریافت اطلاعات است
- شماره گذاری جریان ارسال اطلاعات
- حفظ ترتیب جریان اطلاعات
- هر پروسه بر روی یک ماشین واحد هویت مستقلی برای ارسال و دریافت داده دارد.

Segment Detail

- کنترل جریان هوشمند در سطح پروسه (نه در سطح یک ماشین)
- کنترل مجدد خطا برای اطمینان نهایی
- تقسیم پیامهای بزرگ به بسته های اطلاعاتی کوچک
- شماره گذاری بسته های قطعه قطعه شده جهت بازسازی
- بازسازی بسته های اطلاعاتی و تشکیل یک پیام کامل
- تعیین و تبیین مکانیزم نامگذاری ایستگاههایی که در شبکه هستند
- حفظ ترتیب جریان بایتها

⑤ Session Layer

Session- به مجموعه عملیاتی که پس از برقراری یک ارتباط بین دو پروسه وبا یک توافق اولیه آغاز و سپس با انجام یکسری تراکنش ادامه می یابد و سپس در روالی هماهنگ و مورد توافق ختم میشود نشست گویند.

وظایف کلی

- برقراری و مدیریت یک نشست
- شناسایی طرفین
- سنکرونیزاسیون تماسها و فعل و انفعالات همزمان
- مشخص نمودن اعتبار پیامها
- اتمام نشست
- حسابداری مشتری ها

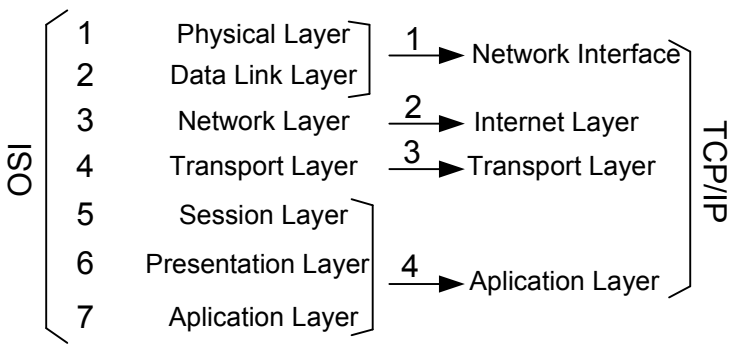
⑥ Presentation Layer

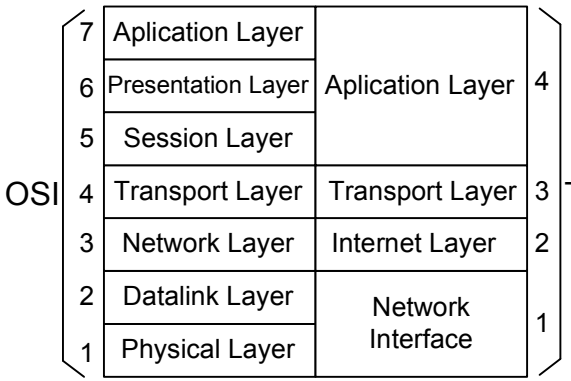
- عملیاتی که در این لایه انجام میگیرد عموما بر روی محتوا و مفهوم پیامها متمرکز است.
- تبدیل قالب Format پیامها ،فشرده سازی،رمز نگاری و رمزگشایی پیامها ،تبدیل کد ها به یکدیگر ASCII to EBCDIC

⑦ Aplication Layer

- انواع سرویسهای کاربردی سطح بالا
- انتقال فایل ،انتقال صدا، انتقال نامه های الکترونیکی

OSI Layers





TCP/IP

① **Network Interface** ***لایه واسط شبکه***

- پروتکلها میتوانند مبتنی بر ارسال رشته بیت یا رشته بایت باشند Byte oriented Bit oriented
- MAN-LAN-PPP-SLIP Wireless IEEE 802.11 ,Token Ring IEEE 802.5

② **Internet** ***لایه شبکه***

- بسته های IP زا از مبداء تا مقصد هدایت میکند.
- IGMP-ARP-RARP-RIP-ICMP-BOOTP-DHCP
- در این لایه یک واحد اطلاعاتی که باید تحویل مقصد گردد دیتا گرام گویند Datagram
- ارسال یک بسته IP بر روی شبکه ،عبور از مسیر خاصی را تضمین نمیکند و از سالم به مقصد رسیدن آن هیچ اطلاعی بدست نخواهد آمد.
- حالت چند پخشی :یعنی یک ایستگاه بتواند به چندین مقصد گوناگون که در قالب یک گروه سازماندهی شده اند ،بسته یا بسته هایی را ارسال کند.
- حالت سرویس در لایه اتصال گرا نیست.

روش اتصال گرا
Reliable

- یک مسیر فیزیکی و مستقیم بین مبداء و مقصد وجود دارد
- ترتیب جریان بایتها حفظ میشود
- اطلاع از وصول یا عدم وصول پیام وجود خواهد داشت
- دارای سرعت پایین و دقت بالاست

روش بدون اتصال
Unreliable

- در این روش ارتباط از طریق عناصر میانی و سوئیچ انجام میشود.
- ترتیب جریان بایتها حفظ نمیشود
- اطلاعی از وصول یا عدم وصول پیام نیست
- روش سریعی بوده و دارای خطای زیادی است.

③ **Transport** ***لایه انتقال***

- این لایه ارتباط ماشینهای انتهایی (میزبان) را در شبکه برقرار میکند و میتواند اتصال گرا Reliable (TCP) و بدون اتصال باشد Unreliable (UDP)

④ **Aplication** ***لایه کاربرد***

- در این لایه بر اساس خدمات لایه های زیرین ،سرویس سطح بالایی برای خلق برنامه های کاربردی ویژه و پیچیده ارائه میشود.
- WEB-FTP-TELNET,..

Network Interface

مفاهیم مرتبط با لایه واسط شبکه

- مسائل مربوط به ارتباط فیزیکی بین دو ماشین در یک شبکه
- اتخاذ تدابیری برای اینکه یک کانال دارای خطا به یک خط بدون خطا و مطمئن تبدیل شود.
- اطلاعاتی که قرار است بر روی یک خط ارسال شوند در قالب یک فریم سازماندهی شده و ابتدا و انتهای آن با علائم ویژه نشانه گذاری میشود Delimiter برای درک فریمهای متوالی
- به ابتدا و انتهای هر فریم ،اطلاعات لازم مانند آدرس آدرس گیرنده و فرستنده و کد کشف خطا اضافه میگردد.
- جلوگیری از تصادم Collision و مدیریت کانال در شبکه هایی که از کانال اشتراکی استفاده میکنند.
- هر یک از مسیر یابها یا سوئیچها خط اختصاص با دیگر سوئیچها دارند که لینک گویند
- دو شبکه مجزا با استفاده از مسیر یاب و خطوط نقطه به نقطه به هم وصل میشوند
- یک بسته برای طی مسیر از یک ماشین مبدا به ماشین مقصد گاه از شبکه های میانی و کانالهای متفاوت عبور میکند

مفاهیم کانالهای انتقال

Bandwith ***پهنای باند***

- پهنای باند هر کانال را میتوان توانایی و ظرفیت آن در ارسال اطلاعات با نرخ B بیت در ثانیه ،تعریف کرد.

C: ظرفیت کانال بر حسب بیت در ثانیه
B: پهنای باند کانال بر حسب هرتز
S: متوسط توان سیگنال
N: متوسط توان نویز

$$C=B.\log_2(1+S/N)$$

BER (bit error rate) ***نرخ خطای بیت***

- میانگین تعداد بیتهایی که در حین انتقال از طریق یک کانال دچار خطا میشوند نرخ خطای بیت گویند.(مثلا فرستنده بیت 1 بفرستد و در گیرنده اشتباها بیت 0 آشکارسازی شود و بلعکس)

Multiplexing ***تسهیم***

- به عمل تقسیم پهنای باند یک کانال بین چند ایستگاه مالتی پلکس یا تسهیم گفته میشود و به دو روش قابل انجام است.

Multiplexing

FDM ***تسهیم در حوزه فرکانس*** **(Ferquency Division Multiplexing)**

- اگر حداکثر N استگاه در شبکه وجود داشته باشد پهنای باند فرکانسی کانال به N باند مجزا تقسیم میشود.
- هر ایستگاه موظف است در یکی از این باندهای فرکانسی ارسال و دریافت داشته باشد بنابراین هر گونه تصادم و داخل سیگنال منتفیست.

TDM ***تسهیم در حوزه زمان*** **(Time Division Multiplexing)**

- هر ایستگاه مجاز است فقط در برش زمانی (Time Slot) متعلق به خودش اطلاعات را روی کانال بفرستد.

- با توجه به انفجاری بودن Bursty Traffic بودن ارسال داده ها و تعداد نامشخص ایستگاهها روشهای TDM,FDM مناسب نیستند و از استاندارد IEEE 802.X استفاده میشود.

کابلهای شبکه

Twisted Pair

STP ***سیم زوج بهم تابیده زره دار*** **Shielded Twisted Pair**

ScTP ***سیم زوج بهم تابیده دارای فویل*** **Screened Twisted Pair**

UTP ***سیم زوج بهم تابیده بدون زره*** **Unshielded Twisted Pair**

UTP — **50 Ohm**

Cat 1	پهنای باند 100KHz	بالاترین نرخ ارسال 144Kbps	مودم معمولی و دورنگار	استفاده در مودم و دورنگار
Cat 2	پهنای باند 1MHz	بالاترین نرخ ارسال 2Mbps	ISDN	
Cat 3	پهنای باند 16MHz	بالاترین نرخ ارسال 10Mbps	سیستم تلفن 10Base-T4	
Cat 4	پهنای باند 20MHz	بالاترین نرخ ارسال 16Mbps	Token Ring	
Cat 5	پهنای باند 100MHz	بالاترین نرخ ارسال 100Mbps	100Base-T	
Cat 6	پهنای باند 250MHz	1Gbps		
Cat 7	پهنای باند 600MHz	10Gbps		

Fiber Optic ***فیبر نوری***

- تارهای بسیار نازکی از جنس شیشه یا پلاستیک هستند که پرتوهای نور را از مبداء به مقصد منتقل میکنند.

سه بخش اصلی فیبر نوری ⟵ 1) Core ***هسته*** 2) **Cladding** ***روکش*** 3) **Buffer Coating** ***پوشش محافظ***

Fiber Optic

فیبرهای نوری چند حالته با تغییر ناگهانی در مرز هسته و روکش **Step Index Multi Mode Fiber**

فیبرهای نوری چند حالته با تغییر تدریجی ضریب شکست در مرز هسته و روکش **Grade Index Multi Mode Fiber**

فیبرهای نوری تک حالته **Single Mode Fiber**

ویژگی

- پهنای باند فوق العاده بالا
- ایمنی فوق العاده در مقابل نویز
- عدم ارتباط الکترونیکی گیرنده و فرستنده
- امنیت اطلاعات(انشعاب سخت)
- وزن ،حجم ، و قیمت پایین مواد اولیه
- ایمنی محیط(عدم تولید جرقه)
- تضعیف پایین

امواج طیف نور

نور مادون قرمز Infrared

- این نور میتواند بصورت هدایت نشده Unguided (بدون نیاز به کابل) برای انتقال بکار گرفته میشود، در چند متر

خطا در شبکه

نویز حرارتی - به دلیل حرکت اتفاقی الکترونها بوجود می آید و با افزایش دما،شدت این نویز هم بصورت خطی تقویت میشود،اثر این خطا کاملا تصادفی است.

شوکهای الکتریکی - بدبلیل قطع و وصل کلیدها ،سیمها،سوئیچهای الکتریکی یا رعد و برق بوجود می آید و نوعی خطای انفجاری را پدید می آورد

نویز کیهانی - ناشی از حرکات کیهانی ،کهکشانها ، وضعیت ستارگان ،خورشید و امثال آن میباشد و تاثیر آن بیشتر در کانالهای رادیویی است.

روشهای کشف خطا

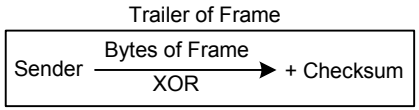
بیت توازن Parity bit

بیت توان فرد 1 Odd Parity
بیت توان زوج 0 Even Parity

- در این روش به ازای هر بایت از اطلاعات یک بیت توازن اضافه میشود.این بیت به گونه ای باید انتخاب و اضافه شودکه مجموع تعداد بیتهای 1 ،همیشه زوج یا فرد باشد.
- این روش وقتی موثر است که تعداد خطاهای رخ داده زوج نباشد.

روش کشف خطا ی Checksum جمع کنترلی

- این روش وقتی موثر است که تعداد خطاهای رخ داده در بیتهای هم ارزش زوج نباشد.

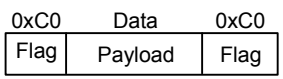


کدهای کشف خطای CRC Cyclic Redundancy Check

- به ازای مجموعه بیتهای کل یک فریم ، تعداد بین کنترلی بنام کد CRC محاسبه و به انتهای فریم اضافه میکند،تعداد بیتهای CRC ثابت است.

استانداردهای انتقال روی خطوط نقطه به نقطه

پرتکل SLIP Serial Line IP

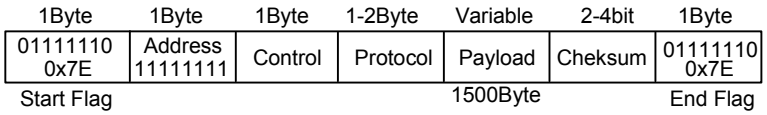


- برای اتصال ایستگاههای Sun بوسیله یک خط سریال مثل خط تلفن ابداع شد و فوق العاده ساده و در عین حال سریع است.

معایب

- در این پرتکل هیچگونه کد کشف خطا گنجانیده نشده و به لایه های بالاتر سپرده شده است.
- درون فیلد داده صرفا میتواند بسته های IP قرار بگیرد.
- دو ماشین نقطه به نقطه باید آدرس IP ثابت و شناخته شده ای داشته باشند.
- این پرتکل فقط برقرار کننده ارتباط را بعنوان ماشین معتبر میشناسد و هیچ راهی برای تایید هویت کاربر برقرار کننده ارتباط نیست
- بسیاری از سیستم عاملها این پروتکل را پشتیبانی نمیکنند

پرتکل PPP Point to Point Protocol



تنظیم و ایجاد یک اتصال PPP

- استفاده از یکسری بسته های کنترلی LCP بعد از شماره گیری و اتصال خط Link Control Packet
- مرحله دوم احراز هویت شروع کننده به طرف مقابل
- مرحل سوم استفاده از پرتکل NCP برای برقراری لایه شبکه (گرفتن IP) Network Control Protocol

Control → 00000011 No Ack Normal frames

Protocol → -عدد این فیلد مشخص کننده آنست که بسته درون فیلد داده ،مربوط به چه پرتکلی در لایه بالاتر است

Payload → - اندازه آن پس از اتصال توافق میشود پیش فرض 1500Byte

IEEE802.1

- پرتکل نیست، بلکه استانداردی شامل یکسری تعاریف ،تشریح برخی از روشها و مقدمه ای در مورد مجموعه استانداردهاست.(استاندارد های لایه اول و دوم)

IEEE802.2

- یک زیر لایه بنام LLC **(Logical Link Control)**

LLC

1- یکسان سازی توپولوژیهای مختلف برای یکسان سازی سرویس به لایه بالاتر

2- سرویس انتقال فریمها مطمئن خواهد شد.

IEEE802.3(10Mbps)

CSMA/CD

Carrier Sense Multiple Access with Collision Detection

1- هر ایستگاه در شبکه ابتدا به کابل گوش میدهد ودر صورت آزاد بودن کانال اجازه ارسال دارد

2-در صورت اشغال بودن خط پس از انتظار 9.6 میکروثانیه مجددا ارسال میکند وباز به خط گوش میدهد و در صورت باز بودن کانال تا انتهای فریم را ارسال میکند.

3- تمام ایستگاهااگر در لحظه آغازین ارسال فریم تشخیص تصادم دهد سیگنال نویز گونه JAM را ارسال میکنند (بعنوان خطا و اخطار) و مجددا به مرحله اول میروند.

- بمحض آنکه ایستگاهها از وقوع تصادم آگاه شدند ارسال خود را نیمه کاره رها میکنند ،قطع سریع فرایند ارسال در زمان و پهنای باند صرفه جویی میکند.
- یکی از بنیادیترین پارامترهای موثر در کارایی این الگوریتم مدت زمانی است که طول میکشد تا ایستگاهی که ارسال خود را آغاز کرده متوجه تصادم شود.
- کشف تصادم بصورت آنالوگ انجام میگرد به سه روش

کشف تصادم

1- بررسی توان مصرفی

2- اندازه گیری پهنای پالس سیگنال دریافتی از سیگنال و مقایسه آن با پهنای واقعی سیگنال ارسالی

3- اندازه گیری سطوح ولتاژ پالسها

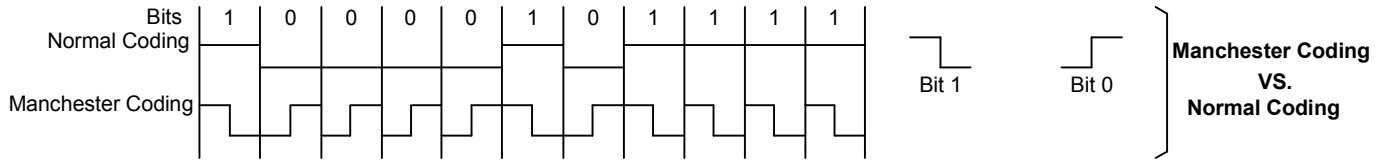
- حداکثر طول کانال 2500 متر در نظر گرفته شده بود که پس از 500متر از Regenerate برای جلوگیری از تضعیف استفاده میشود.

کاهش راندمان کانال

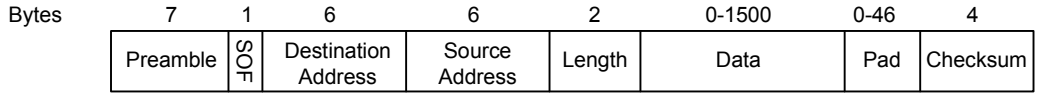
- باکاهش طول فریم (زمان تلف شده برای رقابت و تصرف کانال روی حجم کمی از داده سرشکن میشود)
- با افزایش طول کانال (زمان تلف شده برای رقابت و تصرف کانال به نسبت طول کانال افزایش میابد.)
- با افزایش نرخ ارسال (در زمان تلف شده برای رقابت و تصرف کانال حجم داده بیشتری از بین می رود)

10Base5 ⟶ Thick Ethernet ⟶ 500m ⟶ 100node (in one segment)
10Base2 ⟶ Thin Ethernet ⟶ 185m ⟶ 30node (in one segment)
NIC=Network Interface Card
MAC address in ROM=6 Byte

- سرعت انتقال در اولین نسخه اترنت 10Mbps بود با استفاده از روش کدینگ منچستر Manchester Coding
- اشکال روش منچستر نسبت به روش معملی اینست که به پهنای باند دو برابر نیاز دارد چرا که طول هر پالس نصف یک بیت است(برای ارسال هر بیت دو پالس ارسال میشود)



Manchester Coding VS. Normal Coding



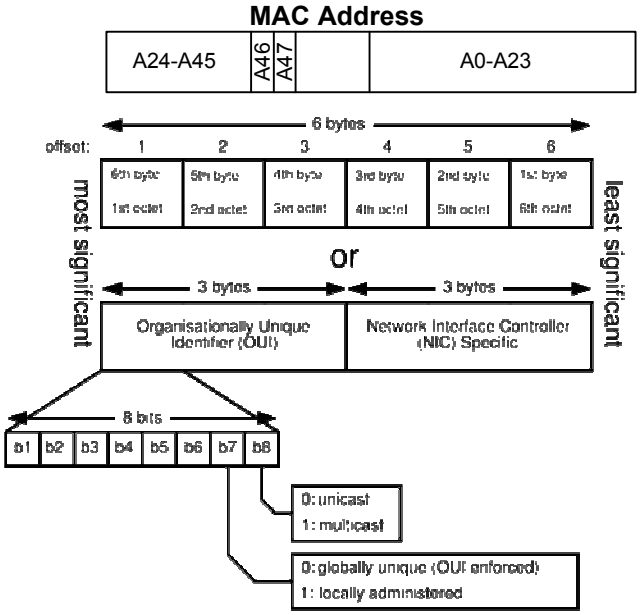
IEEE Standard 10Mbps

- فیلد زیر 64Byte ارسال نمیشود و مجاز نیست

IEEE802.3

MAC Address

آدرسهای ارسال فریم



A0-A23 شماره سریال کارت شبکه

A24-A45 شماره شناسایی شرکت سازنده کارت شبکه

A46 آدرس توسط مدیر شبکه تعیین شده و در خارج از شبکه هیچ ارزشی ندارد (Bit=0)

آدرس توسط IEEE به ثبت رسیده و اعتبار دارد (Bit=1)

دلایل برداشت فریم از روی کانال توسط یک ایستگاه

- در فیلد آدرس مقصد فریم دریافتی، آدرس خود را ببیند.
- در فیلد آدرس مقصد تمامی بیتها 1 باشد.
- در فیلد آدرس مقصد شماره گروهی را ببیند که در آن عضو است.

آدرس تک پخشی **Unicast address** (A47 (Bit=0))

- فرستنده یکی –گیرنده یکی A47 الزاما صفر است.

آدرس چند پخشی **Multicast address**

- فریم برای یک گروه از ایستگاهها ارسال میگردد.

آدرس پخش فراگیر **Broadcast address**

- گیرنده فریم تمامی استگاههای متصل به کانال خواهند بود.

Hub

هاب غیر فعال **Passive Hub**

- بهم وصل کردن کابل ایستگاهها به یکدیگر و ایجاد کانالی مشترک
- هوشمند نیست (عدم کشف تصادم یا تقویت سیگنال ورودی)

هاب فعال **Active Hub**

- تقویت و بازتولید سیگنال ورودی ایستگاهها Regenerate
- عملیات کشف تصادمCollision Detection
- بر خلاف 10base-5 داده ها بطور جدا و مستقل وارد هاب میشوند
- هاب هوشمندانه ایستگاه خراب را از مدار خارج میکند
- الگوی جدیدی برای کابل کشی اترنت10Base-F

5-4-3 Rule

There are only maximum 5 segments between any two terminal nodes.
There are only maximum 4 repeaters between any two terminal nodes.
There are only three segments could be used to connect nodes.
There are two inter-hub segments could not be used to connect nodes.
There forms one collision domain that could contain maximum 1024 nodes.

5 Segments + 4 Hub + 3 Segments for Workstation + 2 Segments for Trunk Extention

IEEE802.3u

IEEE802.3u (100Mbps)

- کاهش زمان یک بیت از 100 نانو ثانیه به 10 نانو ثانیه Bit Time=10ns
- ارتقاء سرعت به 100 مگابیت در ثانیه
- 100Base-FX Up to 2000 meter

حالت دو طرفه غیرهمزمان **Hulf Duplex**

- تفاوتی با اترنت 10Mbps ندارد و قواعد CSMA/CD حکمفرماست
- اتصال ایستگاهها با هاب یا سوئیچ توسط یک کانال مشترک

حالت دو طرفه همزمان **Full Duplex**

- ایستگاهها از طریق 2 لینک مستقل به سوئیچ متصل میشوند.
- ایستگاهها همزمان ارسال و دریافت با سوئیچ دارند

سوئیچ اترنت

- سوئیچ ابزاری است هوشمند که فریمهای دریافتی از پورتها را میگیرد و بر اساس آدرس مقصد درج شده در فریم آنرا مستقیما بر روی پورتی منتقل میکند که ماشین مقصد بدان پورت متصل است.
- هر ایستگاه دو لینک مستقل و مجزا (برای ارسال یا دریافت) با سوئیچ دارد. Full Duplex
- در ورودی و خروجی هر پورت بافر وجود دارد.
- پس از ورود فریم به بافر سوئیچ پورت مقصد پیدا میگردد و فریم بر روی آن پورت ارسال میگردد.
- قالب فریمها با فریمهای عادی اترنت فرقی ندارند
- اگر به هر پورت تنها یک ایستگاه متصل باشد حوزه تصادم وجود ندارد Collision Domain
- به عمل انتقال فریم ورودی یک پورت به بافر پورت خروجی مقصد عمل سوئیچینگ گفته میشود. Switching

سوئیچ متقارن Symmetric

- عمل سوئیچینگ را بین پورتهایی با نرخ ارسال مساوی انجام میدهد

سوئیچ نامتقارن Asymmetric

- میتواند فریمها را بر روی پورتهایی منتقل کند که سرعت یکسانی ندارند.

- **Full Duplex+Half Duplex**

مکانیزم سوئیچها

سوئیچهای ذخیره و هدایت Store & Forward

Store & Forward

1- یک فریم را بطور کامل دریافت میکند

2- کد کشف خطا مورد بررسی قرار میگیرد و در صورت سالم بودن به مرحله بعد میرود و در غیر اینصورت حذف میگردد

3- پورت سوئیچ برای ایستگاه مقصد مشخص میشود با استفاده از فیلد آدرس مقصد MAC Address

4- فریم از طریق یک Backplane بسیار سریع از بافر ورودی پورت مبداء به بافر خروجی پورت مقصد منتقل میشود ،سرعت این انتقال چند صد برابر سرعت ارسال داده ها بر روی کانال است

5- فریم از درون بافر خروجی بصورت سریال بر روی لینک ایستگاه مقصد ارسال میگردد.

سوئیچهای میانبر Cut-Through

Cut-Through

1- بمحض دریافت شش بایت اول از فریم MAC Address عملیات جستجو برای پورت مقصد آغاز میگردد.

2- بلافاصله پس از پیدا شدن پورت مقصد ،داده ها بر روی پورت خروجی منتقل میشود.

3- سوئیچ هیچ وظیفه ای در مقابل فریمهای خراب ندارد (این مشکل در لایه های بالاتر رفع میگردد)

4- اگر پورت مقصد مشغول باشد فریم در بافر منتظر مانده و تا آزاد شدن پورت به صف انتقال میابد.

IEEE802.3z

اترنت گیگابایت

- 1Gbps
- Same Frame قالب فریم یکسان با اترنت عادی
- Full Duplex-Half Duplex
- پشتیبانی از سیمهای مسی و فیبر نوری
- امکان استفاده از کابلهای UTP cat 5

مکانیزمهای اترنت گیگابایت

مکانیزم توسیع حامل Carrier Extension

- سخت افزار سوئیچ آنقدر داده های زائد به انتهای داده میچسباند تا طول فریم حداقل 512 بایت شود.

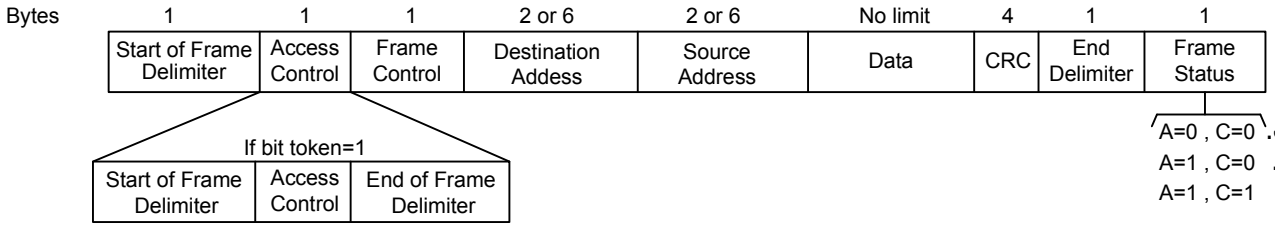
مکانیزم ارسال انفجاری فریمها Frame Bursting

- به فرستنده اجازه داده شده در یکبار ارسال چندین فریم متوالی بفرستد تا طول مجموع آن 512 بایت شود و اگز باز هم به 512 بایت نرسید ،سخت افزار داده های زائد را اضافه میکند

IEEE802.4 ***شبکه های محلی توکن باس***

IEEE802.5 ***شبکه های محلی حلقه***

IEEE802.5



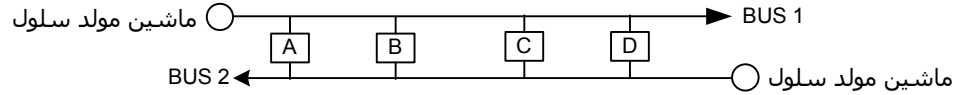
A=0 , C=0 ایستگاه مقصد ،در شبکه نیست و فریم دریافت نشده است.

A=1 , C=0 ایستگاه مقصد ،در شبکه وجود دارد ولی فریم پذیرفته نشد.

A=1 , C=1 فریم توسط ایستگاه مقصد سالم دریافت شد.

IEEE802.6 ***استاندارد شبکه بین شهری*** **DQDB** (Distributed queue Dual Bus)

IEEE802.6



- پوشش ناحیه ایMAN
- 160Km 44.736Mbps
- 9 Byte Header

بیت اشغال **(Busy)**

Bit=1 - در صورتی که این بیت 1 باشد مشخص کننده اینست که سلول خالی نیست و محتوی داده ایستگاه دیگری است.

بیت تقاضا **(Request)**

Bit=1 - با یک کردن این بیت ایستگاه تقاضای ارسال خود را اعلام میکند مشروط به اینکه کسی این بیت را 1 نکرده باشد.

- هر ایستگاه دارای دو شمارنده سخت افزاری است که در ابتدای کار صفر به صفر تنظیم میشود.CD&**RC(Request counter)**

RC —Copy→ DC ——→ RC-1

IEEE802.6

IEEE802.11 ***استاندارد شبکه های بی سیم*** **WiFi**

- محیطهای بی سیم سرشار از نویز محیطی ،موانع تضعیف کننده توان ،سطوح منعکس کننده سیگنال رادیویی و.....بود ،نرخ خطای فریم متجاوز از 90%
- پهنای باند کانالهای بی سیم بسیار ناچیز خواهد بود.(تداخل فرکانسی ایستگاهها)
- طیف امواج الکترومغناطیسی بعنوان یک سرمایه ملی ،مصرفی و نیاز به مجوز و هزینه بسیار داشت
- رنج بردن از مشکل **Capture effect**

مشکل Capture effect

- هر گاه دو سیگنال حامل داده یک با توان زیاد و دیگری با توان کم به یک گیرنده برسد به جای بروز پدیده تصادم سیگنال با توان زیاد دریافت شده و سیگنال با توان کم نقش نویز را بازی میکند.
- بعبارت دیگر وقتی دو فرستنده هم توان ،یکی در فاصله کم و دیگری در فاصله زیاد از گیرنده واقع شده باشند ،حضور فرستنده دوم احساس نمیشود و فرستنده اول در هر لحظه که بخواهد میتواند کانال را تصرف کند (capture)

رفع مشکل Capture effect

- ثابت نگه داشتن تمام سیگنالها در برد بسیار محدود(ریر 300 متر)
- استفاده از روشهای جدید مدولاسیون دیجیتال HR-DSSS & OFDM
- افزایش نرخ ارسال در پهنای باند محدود

حوزه های انتقال بی سیم

- حوزه WAN بیسیم IEEE 802.16
- حوزه LAN بیسیم IEEE 802.11
- حوزه ارتباطات بیسیمی IEEE 802.15 (Bluetooth)

IEEE802.11Wireless WiFi

- هیچگونه توپولوژی خاصی بر آن حاکم نیست.

مشکل CSMA/CD

- مشکل ایستگاههایی که ناخودآگاه از چشم هم پنهان می مانند(مشکل ایستگاه پنهان) -A تمایل دارد برای B ارسال داشته باشد ولی قادر به شنود اینکه B مشغول است نمیباشد.
- مشکل ایستگاههایی که به اشتباه (همچون سراب) در چشم هم آشکار میشود (مشکل ایستگاه ،آشکار) -A تمایل دارد برای B ارسال داشته باشد ولی فکر میکند ارسال او با شکست روبرو خواهد شد.

IEEE802.11

IEEE802.X

الگوریتم CSMA/CA در شبکه بی سیم IEEE802.11

CSMA/CA

1- ایستگاه A به کانال گوش کرده و در صورت آزاد بودن خط ،یک فریم کوتاه به نام RTS به طول 20 بایت در فضای پیرامون خود منتشر میکند(Request to Send)RTS

RTS
- آدرس ایستگاه A ،ایستگاهی که تمایل به دریافت فریم دارد
- آدرس ایستگاه B ،ایستگاهی که بایستی فریم را دریافت کند
- مدت زمانی که ارسال فریم داده ها طول خواهد کشید.
- مقداری اطلاعات کنترلی و کد کشف خطا

2- اگر فریم RTS توسط B دریافت شد ،ایستگاه B در پاسخ فریم کوتاه CTS را در جهت آمادگی بر میگرداند.(Clear to Send)CTS

3- تمامی ایستگاههایی که فریم CTS را دریافت کرده اند برای خودداری از تصادم به اندازه زمان مشخص شده در فریم CTS از ارسال هر سیگنالی خودداری میکنند. دستگاه A در اینحالت شروع به ارسال سیگنال میکند

4- ایستگاههایی که RTS را میشنوند ولی CTS را نمیشنوند احتمالا در برد A هستند ،ولی در برد B قرار نگرفته اند.

5- به محض پایان انتقال فریم ،ایستگاه B موظف است پس از بررسی سلامت فریم ،در یافت موفق آنرا با ارسال فریم کوتاه ACK تصدیق کند.

6- کانال آزاد و رقابت ایستگاههایی که تمایل به ارسال دارند شروع خواهد شد.

- هر گاه دو یا چند ایستگاه بطور همزمان فریم RTS بفرستد تصادم رخ میدهد.
- مکانیزمی برای کشف تصادم وجود ندارد
- اگر ایستگاهی RTS فرستاد و در مهلت مقرر پاسخ CTS برنگشت آنرا تصادم فرض میکند اگر چه ممکن است از خطای کانال باشد.
- اگر ایستگاهی RTS فرستاد و در مهلت مقرر پاسخ CTS برنگشت ایستگاه یک مدت زمان تصادفی صبر کرده و در صورت آزاد بودن خط RTS را مجددا ارسال میکند.

ساختار فریم در استاندارد IEEE802.11

کاربردهای فریم
- فریمهای داده (Data Frame)
- فریمهای کنترلی (Control Frame)
- فریمهای مدیریتی (Management Frame)
- فیلد (Frame Control)

IEEE802.11 Frame

Frame Control	Duration (or ID)	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	FCS
Byte → 2	2	6	6	6	2	6	0-2312	4

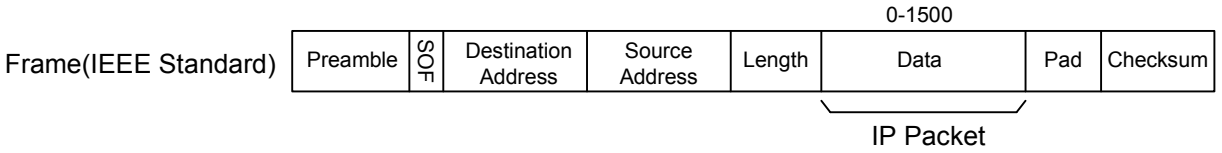
Frame Control

2Byte

16 Bit →

2	2	4	1	1	1	1	1	1	1	1
Protocol Verision	Type	Sub Type	To DS	From DS	More Flag	Retry	PWR Mgt.	More Data	Wep	Order

- وظیفه لایه سوم (شبکه) هدایت بسته های اطلاعاتی از شبکه ای به شبکه دیگر میباشد.
- وظیفه یک مسیر یاب (Router) هدایت بسته های اطلاعاتی از مبداء به مقصد می باشد.(مسیر یابی)
- لایه شبکه ،همان لایه ای است که تمامی کارتهای واسط ،داده های خود را تحویل وی میدهند و در ضمن کنترل تمام این کارتهای واسط را در اختیار دارد و میتواند به خدمت بگیرد.
- لایه شبکه را میتوان نقطه همگرایی و اتحاد لایه های زیرین دانست.
- تمام کارتهای واسط در یک مسیر یاب داده های درونی یک فریم را برای پردازشهای آتی و مسیر یابی ،تحویل لایه 3 میدهند.
- در مدل TCP/IP به یک واحد اطلاعات که باید درون فیلد داده از لایه پیوند داده قرار بگیرد بسته IP (IP Packet) گویند.



مسیر یاب Router

- مسیر یاب ماشینی است که دارای تعدادی پورت ورودی و خروجی دارد است و بسته های اطلاعاتی را از ورودیها تحویل میگیرد و بر اساس آدرس IP مقصد یکی از کانالهای خروجی را برای انتقال بسته انتخاب میکند بنحوی که بسته را به مقصد نزدیک نماید.
- ماشینی که هیچ نقشی در هدایت بسته های اطلاعاتی روی شبکه ندارد و فقط تولید کننده یا مصرف کننده بسته های اطلاعاتی است را ماشین میزبان (Host Machine) یا ماشین نهایی (End System) میگویند.
- مجموعه مسیریابها و کانالهای ارتباطی بین آنها ،توپولوژی زیر شبکه را تشکیل میدهند.
- ترافیک یک مسیر یاب میانگین مجموع کل بسته های است که در واحد زمان به آن وارد میشوند.

پرتکل IP

- قراردادی که حمل و تردد بسته های اطلاعاتی و همچنین مسیر یابی صحیح آنها را از مبداء به مقصد ، مدیریت و ساماندهی مینماید پرتکل IP گویند.

قطعه Fragment

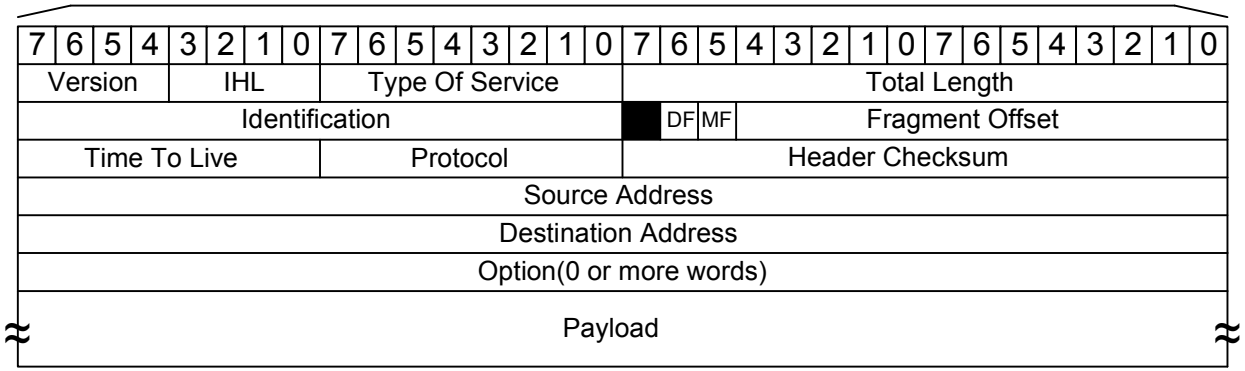
- لایه IP دیتاگرام بزرگ تحویل گرفته از لایه بالاتر را به واحدهای کوچکتری بنام قطعه (Fragment) شکسته و با تشکیل یک بسته IP به ازای هر قطعه ،اطلاعات لازم برای طی مسیر در شبکه را به آنها اضافه میکند ،بدین ترتیب قطعات داده دارای هویت و شناسنامه میشوند.
- هر چند طول هر بسته IP میتواند 64Kbyte باشد ولی عموما طول بسته ها حدود 1500 بایت است.
- اندازه متعارف قطعات عموما 512 بایت است.

قالب یک بسته IP

- یک بسته IP از دوقسمت سرآیند (Header) و قسمت حمل داده ها (Payload) تشکیل شده است.
- مجموعه اطلاعاتی که در سرآیند بسته IP درج میشود توسط مسیر یابها مورد استفاده و پردازش قرار میگیرد.

IP Header

32bit



Version (4 bit) ⟶ IP Ver 4(0100),IP Ver 6(0110)

IHL(ip header length) (4 bit) ⟶ IHL*32=IP header length

Example:(1111)=15*32=480bit طول سرآیند

Type Of Service (8 bit) بعنوان مثال تقاضای ارسال سریع و به موقع (برای ارسال صوت یا تصویر) یا قابلیت اصمینان صد در صد (ارسال نامه الکترونیکی) به مسیر یاب

P2	P1	P0	D	T	R	-	-

Priority=P1,P2,P3 تقدم بسته

Throughput=T ظرفیت خروجی

Delay=D تاخیر

Reliable=R قابلیت اطمینان

Total Length (16 bit) طول کل بسته IP : حداکثر 64kbyte میباشد ولی عموما زیر 1500 بایت است.

Identification (16 bit) مشخص کننده قطعه های مربوط به یک دیتا گرام ،کل قطعه ها ی یک دیتا گرام دارای یک شماره واحد هستند

Fragment Offset (13bit) مشخص کننده شماره ترتیب هر قطعه در دیتاگرام شکسته شده، با توجه به 13 بیتی بودن این فیلد یک دیتا گرام حداکثر به 8192 قطعه میتواند تقسیم شود

DF(don't fragment) (1bit) با 1 شدن این بیت در یک بسته ip هیچ مسیر یابی حق ندارد آن را قطعه قطعه کند.

MF(more fragment) (1bit) اگر قطعه بعدی وجود داشته باشد این بیت الزاما 1 میباشد.

Time To Live (TTL 8 bit) شمارنده طول عمر بسته میباشد ،حد اکثر طول عمر یک بسته 255 میباشد که با گذشتن از هر مسیر یاب از مقدار این فیلد 1 واحد کم میشود.

Protocol (8 bit) شماره پرتکلی (TCP,UDP) است که در لایه بالاتر تقاضای ارسال یک دیتاگرام کرده است.

Header Checksum (16 bit) بمنظور کشف خطاهای احتمالی در سرآیند هر بسته IP استفاده میشود.

Source Address (32 bit) آدرس IP ماشین میزبان

Destination Address (32 bit) آدرس IP ماشین مقصد

Option(0 or more bits Total 40byte) محتوی اطلاعاتی است که میتواند به مسیر یابها در یافتن مسیر مناسب کمک کند یا اطلاعاتی را از آنها طلب میکند

Payload در این فیلد داده های در یافتی از لایه های بالاتر قرار میگیرد

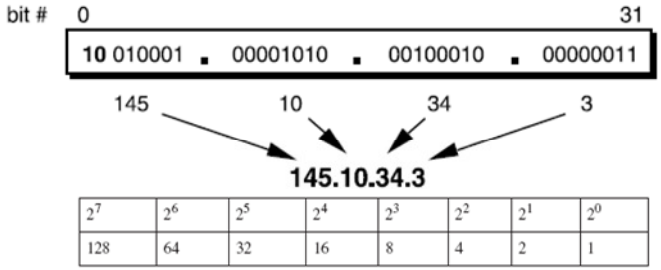
آدرسهای IP

- یک آدرس IP بصورت استاندارد را به صورت چهار عدد دهدهی که با نقطه از هم جدا شده اند مینویسند.

- بخشی از فضای 32 بیتی آدرس به شماره شناسایی یک شبکه (Network Number)اختصاص یافته و مابقی بیتها ،شناسه ماشین میزبان (Host ID) را مشخص میکند.

- شماره شناسایی شبکه برای تمام ماشینهای متعلق به یک شبکه واحد،یکسان و مشترک است.

- طول بخش شماره شناسایی شبکه شبکه در یک آدرس IP متغییر بوده و به کلاس آدرس بستگی دارد.



آدرسهای خاص (غیر قابل استفاده)

- 0.0.0.0 - این آدرس غیر معتبر بوده و در پرتکلی مثل RIP برای مسیر یابی از آن استفاده میشود
- 255.255.255.255 - از این آدرس برای پخش فراگیر Broadcast استفاده میشود.
- 127.0.0.1 - آدرس Loop back نام دارد و برای اشکال زدایی و تست پشته پرتکل از آن استفاده میشود.

- InterNIC (Internet Network Information Center) - مرکز کنترل و نظارت بر آدرسهای IP
- IANA (Internet Assigned Number Authority) - قدرت اجرایی و تصمیم گیری برای آدرسهای IP منحصر بفرد

Classful IP Address
کلاسهای آدرسهای IP

Class A

A
- $2^{7}-2=126$ - تعداد آدرسهای زیر شبکه
- $2^{24}-2=16,777,214$ - تعداد ماشینهای میزبان

Subnet Mask 255.0.0.0

32	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	7bit Network ID							24bit Host ID																							

First Octet in Decimal **0-127**
- **1-126** Valid Address
- **0** 0 is invalid
- **127** Qdrdqudc enqknnoa`bj sdrshmf

Class B

B
- $2^{14}-2=16,382$ - تعداد آدرسهای زیر شبکه
- $2^{16}-2=65,534$ - تعداد ماشینهای میزبان

Subnet Mask 255.255.0.0

32	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
1	0	14bit Network ID														16bit Host ID															

First Octet in Decimal **128-191** Valid Address

Class C

C
- $2^{21}-2=2,097,150$ - تعداد آدرسهای زیر شبکه
- $2^{8}-2=254$ - تعداد ماشینهای میزبان

Subnet Mask 255.255.255.0

32	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
1	1	0	21bit Network ID																					8bit Host ID							

First Octet in Decimal **192-223** Valid Address

Class D

32	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
1	1	1	0	28bit Multicast address																											

First Octet in Decimal **224-239** Valid Address

Class E

32	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
1	1	1	1	0	27bit Reserved for future use/testing																										

First Octet in Decimal **240-255** Valid Address

آدرسهای خاص (قابل استفاده)

0.HostID	- این آدرس زمانی بکار میرود که ماشین میزبان ،پیش شماره شبکه ای که بدان متعلق است را نداند.
NetID.255	- برای ارسال یک پیام فراگیر برای تمام ماشینهای یک شبکه راه دور که ماشین میزبان فعلی متعلق به آن نیست

الگوی زیر شبکه Subnet Mask

- برای تفکیک آدرس زیر شبکه و آدرس میزبان، از الگوی زیر شبکه استفاده میشود (در حقیقت IP ماشین میزبان با الگوی زیر شبکه AND جبری میشود)

	32	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
215.50.31.0	1	1	0	1	0	1	1	1	0	0	1	1	0	0	1	0	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0
AND																																
255.255.255.0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
215.50.31.0	1	1	0	1	0	1	1	1	0	0	1	1	0	0	1	0	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0

/8	255.0.0.0	Class A
/16	255.255.0.0	Class B
/24	255.255.255.0	Class C

Subnet Mask for Classful IP address

215.50.31.0/24
/24 or 255.255.255.0

24/ بدین معنی میباشد که تعداد 24bit بعنوان Subnet Mask در نظر گرفته شده است.

زیر شبکه های غیر استاندارد Classless

- اگر تعدادی از بیتهای HostID را به NetID نسبت دهیم در حقیقت یک آدرس IP با کلاس (Classful)را به تعدادی مشخص زیر شبکه (Classless)تقسیم کرده ایم.

بعنوان مثال اگر بخواهیم آدرس IP کلاس B ذکر شده را به 9 زیر شبکه تقسیم کنیم ابتدا از فرمول زیر استفاده میکنیم.

Rsdo 09 $2^N - 2 \geq 9$ → $2^4 - 2 = 14$ N= تعداد بیتهایی که باید از HostID قرض گرفت.

Subnetting a Class B Network Using Binary

172.16.0.0 /16

172.16.0.0 /16

NetID **HostID**

255.255.0.0 → **11111111.11111111.00000000.00000000**

4bit

255.255.240.0 → **11111111.11111111.11110000.00000000**

NetID **HostID**

255.255.0.0 آدرس IP قبل از Subnet **172.16.0.0 /16**

255.255.240.0 آدرس IP پس از Subnet **172.16.0.0 /20**

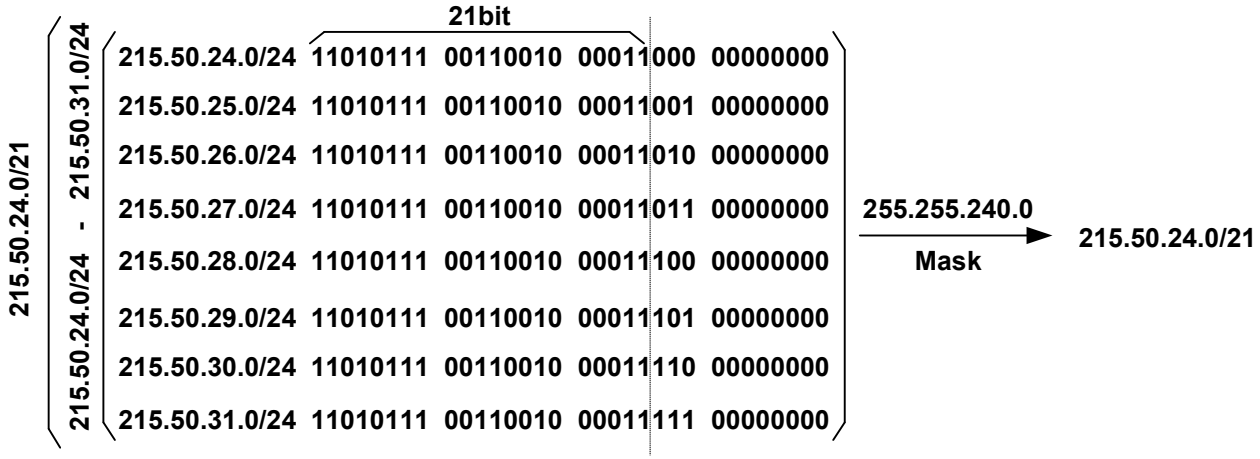
هر کدام از Subnet ها با 20/ بکار گرفته میشود بعنوان مثال 172.16.0.0/20

172.16.0.0 /20

Subnet	Network Address (0000)	Range of Valid Hosts (0001–1110)	Broadcast Address (1111)
0 (0000) invalid	172.16.0.0	172.16.0.1–172.16.15.254	172.16.15.255
1 (0001)	172.16.16.0	172.16.16.1–172.16.31.254	172.16.31.255
2 (0010)	172.16.32.0	172.16.32.1–172.16.47.254	172.16.47.255
3 (0011)	172.16.48.0	172.16.48.1–172.16.63.254	172.16.63.255
4 (0100)	172.16.64.0	172.16.64.1–172.16.79.254	172.16.79.255
5 (0101)	172.16.80.0	172.16.80.1–172.16.95.254	172.16.95.255
6 (0110)	172.16.96.0	172.16.96.1–172.16.111.254	172.16.111.255
7 (0111)	172.16.112.0	172.16.112.1–172.16.127.254	172.16.127.255
8 (1000)	172.16.128.0	172.16.128.1–172.16.143.254	172.16.143.255
9 (1001)	172.16.144.0	172.16.144.1–172.16.159.254	172.16.159.255
10 (1010)	172.16.160.0	172.16.160.1–172.16.175.254	172.16.175.255
11 (1011)	172.16.176.0	172.16.176.1–172.16.191.254	172.16.191.255
12 (1100)	172.16.192.0	172.16.192.1–172.16.207.254	172.16.207.255
13 (1101)	172.16.208.0	172.16.208.1–172.16.223.254	172.16.223.255
14 (1110)	172.16.224.0	172.16.224.1–172.16.239.254	172.16.239.255
15 (1111) invalid	172.16.240.0	172.16.240.1–172.16.255.254	172.16.255.255

آدرس دهی بدون کلاس CIDR(Classless Inter domain Routing)

آدرسهای بدون کلاس که در فضای آدرسهای کلاس C تعریف میشوند در حقیقت از تجمیع آدرسها بعنوان یک آدرس واحد استفاده میشود.



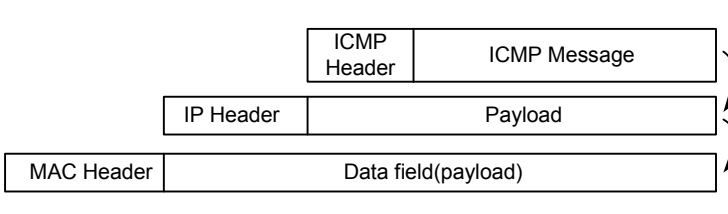
پرتکل ICMP (Internet Control Message Protocol)

-با توجه به اینکه پرتکل IP ،پرتکلی بدون اتصال (connectionless) و غیر قابل اعتماد (unreliable) است از پزتکل ICMP در کنار پرتکل IP ،برای بررسی انواع خطا و ارسال پیام برای مبداء بسته در هنگام بروز اشکالات ناخواسته استفاده میشود.

-ICMP یک سیستم گزارش خطاست که برروی پرتکل IP نصب میشود تا در صورت بروز هرگونه خطا به فرستنده بسته پیام مناسب را بدهد تا آن خطا تکرار نشود.

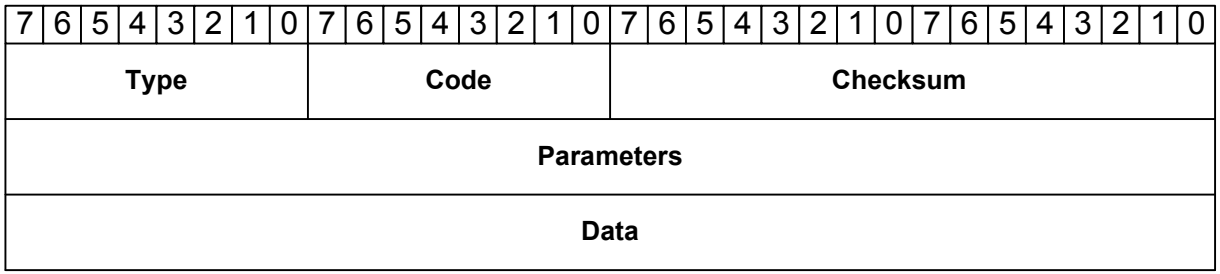
- وقتی پرتکل ICMP درون بسته IP قرار میگیرد در Header IP فیلد Protocol با شماره مشخصه پرتکل ICMP (یعنی 1) تنظیم میشود.

- در صورتیکه بسته ICMP به هر دلیلی دچار خرابی شود پیغام خطایی ارسال نخواهد گردید.



چگونگی قرارگرفتن یک پیام ICMP درون یک بسته IP

قالب پیام ICMP



Type - در این فیلد عددی قرار میگیرد که بیانگر نوع پیام است ساختار فیلدهای Parameters,data با توجه به عددی که در این فیلد قرار میگیرد متفاوت خواهد بود.

Code - گاهی خود نوع پیام به چند نوع فرعی دیگر تقسیم میشود که کد نوع فرعی در این فیلدها قرار میگیرد.

Checksum - برای سنجش اعتبار و سلامت بسته ICMP استفاده میگردد.

پیامهای ICMP

پیام Destination Unreachable

- این پیام زمانی صادر میشود که زیر شبکه یا مسیر یاب نتواند آدرس مقصد را تشخیص دهد یا به هر دلیلی بسته توسط ماشین میزبان تحویل گرفته نشود(مثلا بدلیل بزرگ بودن اندازه بسته ها و عدم اجازه به مسیر یاب برای شکستن آن یا عدم حضور ماشین مورد نظر در شبکه)

پیام Time Exceeded

- این پیام زمانی صادر میشود که مهلت قانونی یک بسته مقتضی شده باشد و یک مسیر یاب مجبور شود آن را حذف کند .این پیام صرفا برای آگاهی ارسال میگردد.

پیام Parameter Problem

- این پیام زمانی صادر میشود که مقداری نامعتبر در یکی از فیلدهای سرایند در بسته IP قرار گرفته باشد و مسیر یلب قادر به تشخیص و تفسیر سرآیند آن بسته IP نباشد.

پیام Source Quench

- این بسته زمانی برای یک ماشین میزبان ارسال میشود که بسته ای در اثر ازدحام در یک مسیر یاب حذف شده باشد و از آن ماشین خواسته شود که حجم ارسال بسته هایش را کاهش دهد.

پیام Redirect

- این پیام زمانی ارسال میشود که یک مسیر یاب احساس کند بسته یا بسته هایی که برای او ارسال شده است در مسیر صحیح نیستند و احتمالا اشکالی در مسیریابی وجود دارد.

پیام Echo Request

- این پیام وقتی صادر میشود که یک مسیر یاب بخواهد بداند که آیا یک ماشین خاص شبکه قابل دسترس و مجود است یا خیر

پیام Echo Reply

- در پاسخ به دریافت Echo Request مقصد با ارسال پیام Echo Reply به آن پاسخ میدهد.

پیام Timestamp Request,Timestamp Reply

- این دو پیام دقیقا شبیه دو پیام تعریف شده در قبل هستند با این تفاوت که دریافت کننده آن،زمان دریافت و زمان ارسال بسته را نیز در پاسخ به آن اضافه خواهد کرد در حقیقیت زمان رفت و برگشت یک بسته نیز تخمین زده میشود.

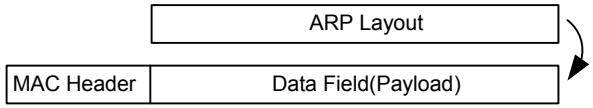
پرتکل ARP (Address Resolution Protocol)

- هر ماشینی روی اینترنت(شبکه) گذشته از اینکه باید آدرسهای IP خودش و مقصدش را بشناسد و بداند ،نیازمند دانستن آدرسهای فیزیکی ماشینهایی که مستقیما با او در ارتباطند ،هم هست.

- وظیفه پرتکل ARP پیدا کردن آدرس فیزیکی یک ماشین براساس آدرس IP آن میباشد.

- پرتکل ARP براساس یک (بسته فراگیر)broadcast بر روی شبکه محلی آدرس فیزیکی ماشین مورد نظر را پیدا میکند.و در جدولی درون حافظه اصلی که ARP Cache نامیده میشود ذخیره میکند.

- پرتکل ARP مستقیما بر روی پرتکل لایه فیزیکی عمل میکند.



- اگر IP بر روی شبکه محلی دیگری قرار داشته باشد به دو حالت ممکن است انجام گردد.

1- مسیر یاب آدرس فیزیکی خودش را به ایستگاه سئوال کننده ارسال میکند. **(Proxy ARP)**

2- ایستگاهها خودشان موظفند بر اساس الگوی زیر شبکه آدرس محلی (local) یا خارجی (global) را تشخیص دهند .و در صورت خارجی بودن آدرس فیزیکی مسیر یاب را انتخاب کنند.

پرتکل **RARP** (Reverse Address Resolution Protocol)

- از این پرتکل برای پرسش در خصوص IP متناظر با یک آدرس فیزیکی خاص استفاده میشود. برعکس پرتکل ARP

- تمام ایستگاههایی که از پرتکل RARP حمایت میکنند درصورتی که بسته شناسایی پخش فراگیر(آدرس IP متناظر با یک آدرس فیزیکی) را دریافت کنند اگر آدرس فیزیکی مورد نظر را بدانند فورا در پاسخ،آدرس IP معادل را در قالب یک بسته **RARP Reply** برمیگردانند.

- بسته های ARP,RARP از نوع فراگیر محلی بوده و توسط مسیریابها به خارج از شبکه منتقل نمیشوند.

پرتکل **BootP**

- این نیاز برای ایستگاههایی بوجود می آید که پس از روشن شدن بایستی از طریق سرویس دهنده شبکه بوت شوند (ایستگاه بدون دیسک)

- این پرتکل از دیتاگرام UDP استفاده میکند و مسیر یابها موظف به انتقال آن هستند .

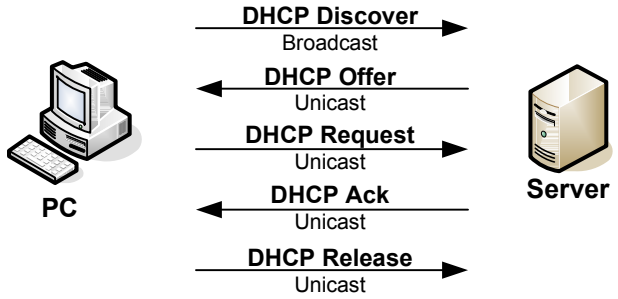
- در پاسخ به بسته های BootP ،علاوه بر آدرس IP ایستگاه مورد نظر،اطلاعات لازم جهت بوت شدن سیستم و همچنین الگوی زیر شبکه و آدرس مسیریاب پیش فرض برای ایستگاه تقاضا کننده در قالب یک بسته UDP ارسال خواهد شد.

- مشکل جدی پرتکل BootP آنست که جدول نگاشت آدرس IP به آدرس اترنت باید بصورت دستی تنظیم و پیکره بندی گردد.

پرتکل **DHCP** (Dynamic Host Configuration Protocol)

- این پرتکل امکانی را فراهم آورده که بتوان آدرس IP ایستگاهها را هم بصورت دستی و هم بصورت خودکار به آنها انتساب داد.

- از آنجایی که ممکن است دسترسی به این سرویس دهنده از طریق پخش فراگیر بسته های تقاضا میسر نباشد فلذا بر روی هر LAN یک عامل رله (DHCP Relay Agent) نیاز است.



DHCP Discover - این بسته را PC بصورت پخش فراگیر می فرستد تا از طریق DHCP Relay Agent ، DHCP Server را پیدا کند.

DHCP Offer - DHCP Server خود را به ماشین درخواست کننده معرفی کرده و پارامترهای مورد نیاز را پیشنهاد میدهد.

DHCP Request - گیرنده تازه وارد از بین پیشنهاد ها فقط یکی را انتخاب کرده و از سرویس دهنده میخواهد که آها راقطعی و ثبت کند.

DHCP Ack - سرویس دهنده با ارسال این پیام پارامترهای لازم را برای سرویس گیرنده می فرستد و آدرس IP آنرا ثبت میکند و سرویس دهنده شروع به کار میکند.

DHCP Release - هرگاه ماشینی بخواهد شبکه را ترک کند با ارسال این پیام تقاضای آزاد شدن آدرس IP خود را به سرویس دهنده اعلام کرده و شبکه را ترک میکند.

سوئیچینگ Switching

- فرایند دریافت یک واحد داده دارای هویت،از یکی از کانالهای ورودی و هدایت آن برروی کانال خروجی مناسب ،بنحوی که بسوی مرکز نهایی خود نزدیک و رهنمون شود.

دستگاههای /ابزار سوئیچ

Repeater *(تکرار کننده)*

- ابزاریست مخابراتی که سیگنال دیجیتال ورودی را دریافت کرده و پس از تشخیص 0 و 1ها آنها را از نو در خروجی خود ،بصورت یک سیگنال دیجیتالی عاری از نویز و بدون تضعیف بازتولید میکند.
- تکرار کننده ها هیچ درکی از فریم،بسته و بایت ندارند و صرفا با مفهوم بیت و سطوح ولتاژ آشنا هستند.

HUB *(هاب)*

- فریمی را که از یک خط ورودی دریافت میشود بدون قید و شرط بر روی تمام خطوط دیگر ارسال میکند. این ابزار در لایه 1 کارمیکند و در آن تصادم رخ میدهد.

Switch *(سوئیچ)*

- سخت افزاری است که فریمهای تولید شده توسط کارت شبکه را گرفته و پس از پردازش سرآیند فریم و بررسی آدرسهای MAC ،آنها را بسوی پورت خروجی مناسب هدایت میکند.
- سوئیچ در درون دارای پردازنده است و در لایه 2 کار میکند.

Bridge *(پل)*

- ابزاریست که دو یا چند شبکه LAN همگون یا غیر همگون را بهم متصل مینماید و در لایه 2 کار میکند.

Router *(مسیریاب)*

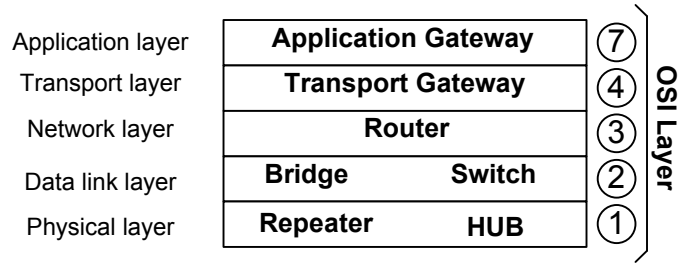
- این ابزار بر اساس سرایند لایه 3 بسته ها را پردازش کرده و بر اساس آدرس جهانی مقصد ،برای آن یک مسیر خروجی مناسب محاسبه و انتخاب مینماید.

Transport Gateway *(در وازه های انتقال)*

- این ابزارها در لایه 4 کار میکنند و بر اساس و هدایت بسته ها را بر اساس سرایند دادهای درونی هر بسته (segment) انجام میدهند.
- سوئیچهای لایه چهارم میتوانند بسته ها را بر اساس تعلق آنها به به یک اتصال خاص (TCP,UDP) هدایت کنند.
- این دروازه ها میتوانند ارتباط دو کامپیوتر که از پرتکلهای اتصال گرای متفاوتی در لایه انتقال استفاده میکنند برقرار سازند. مثلا ارتباط دو کامپیوتربا پرتکلهای اتصال گرای TCP و ATM

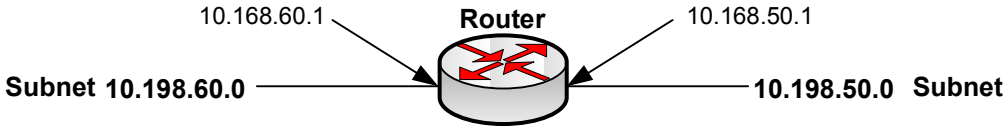
Application Gateway *(در وازه های کاربرد)*

- این نوع دروازه ها عموما نرم افزاری هستند و میتوانند محتوی داده ها را تشخیص داده و پیامی را به پیام دیگر ترجمه کنند. مثلا یک دروازه پست الکترونیکی میتواند یک نامه الکترونیکی را به پیام SMS برای گوشی تلفن همراه تبدیل کرده و به مقصد ارسال نماید..



سوئیچینگ لایه سومی :مسیر یابی

یک مسیریاب به تعداد کارتهای واسط،به آدرس IP احتیاج دارد(زیرا عضو یکایک شبکه هایی است که بدانها متصل میباشد.)پیش شماره آدرس IP هر یک از کارتهای شبکه مساوی پیش شماره تمام اعضای شبکه ای است که به آنها متصل است.



Dynamic & Static Routing

از دیدگاه روش تصمیم گیری و میزان هوشمندی الگوریتم

Static *(ایستا)*

- در این الگوریتم هیچ اعتنایی به شرایط توپولوژیکی و ترافیک لحظه ای شبکه نمیشود.
- برای هدایت یک بسته ،هر مسیریاب از جداولی استفاده میکند که در هنگام پیکره بندی مسیریابها تنظیم شده و در طول زمان ثابت می ماند. IP Route,IPX Route
- این الگوریتمها بسیار سریعند و در صورت تغییر در توپولوژی زیر ساخت ارتباطی شبکه یک مشکل عمده و جدی ایجاد خواهد شد.

Dynamic *(پویا)*

- مسیر یابی بر اساس آخرین وضعیت توپولوژیکی و ترافیک شبکه انجام میشود و جداول مسیر یابی هر T ثانیه یکبار به هنگام میشود.
- با توجه به اینکه پیچیدگی این الگوریتمها برای مسیر یابی زیاد میباشد ،در مسیر یابها از پردازنده های ASIC،تکنیکهای چند پردازنده ای و پردازش موازی استفاده میشود.

از دیدگاه چگونگی جمع آوری و پردازش اطلاعات زیرساخت ارتباطی شبکه

Dynamic

Global Routing Algorithm *(سراسری متمرکز)*

- در الگوریتم متمرکز هر مسیریاب باید اطلاعات کاملی از زیرساخت کل شبکه داشته باشد.(باید تمام مسیریابهای دیگر،ارتباط بین آنها و هزینه هر خط را دقیقا شناسایی نماید)
- برای یافتن بهترین مسیر بین هر دو مسیریاب ،از یکی از الگوریتمهای کوتاهترین مسیر ،نظیر **الگوریتم دایجسترا** (Dijkstra Shortest Path Algorithm) استفاده میشود.
- به الگوریتمهای که برای مسیر یابی به اطلاعات کاملی از زیر ساخت شبکه و هزینه ارتباط بین هر دو مسیریاب نیازمندند اختصارا الگوریتمهای LS (Link State Algorithm) گفته میشود و در مسیر یابهای مدرن و جدید از آن استفاده میشود. مانند IS-IS,OSPF

Decentralized Routing Algorithm *(غیرمتمرکز توزیع شده)*

- در الگوریتم غیر متمرکز مسیریاب اطلاعات کاملی از زیرساخت شبکه ندارد بلکه فقط قادر است هزینه ارتباط با مسیر یابهایی که بطور مستقیم و فیزیکی با آنها در ارتباط است محاسبه و ارزیابی نماید ،سپس در فواصل زمانی منظم هر مسیریاب جدول مسیر یابی خود را فقط برای مسیریابهای مجاور ارسال میکند.
- این الگوریتمها پیچیدگی زمانی Time Complexity بسیار کمی نسبت به الگوریتمهای دایجسترا دارد.
- به این نوع الگوریتمها الگوریتمهای DV (Distance Vector Algorithm) گفته میشود مانند RIP,IGRP,EIGRP,BGP

روش ارسال سیل آسا (Flooding)

- از روش سیل آسا فقط در موارد خاص و برای ارسال پیامهای فراگیر و کنترلی (مثل اعلام جدول مسیر یابی در پروتکلهای LS)استفاده میشود. بسته بر روی تمام مسیرهای خروجی به غیر از مسیری که بسته دریافت شده است ارسال میشود.

(معایب)

- کل شبکه را در ترافیک زائد و بیهوده غرق خواهد کرد بنابراین روشی قابل اتکا و عمومی برای مسیر یابی نخواهد بود.
- اگر همه مسیر یابها یک بسته نوع فراگیر را روی تمام خروجیهای خود ارسال کنند ممکن است پس از چند لحظه خودشان آن بسته را دریافت کنند و چون مجددا آن را روی خروجی های خود ارسال میکنند این تکرار تا بینهایت ادامه خواهد یافت.

روش حل مشکل تکرار بسته های فراگیر

- قرار دادن شماره شناسایی برای هر بسته: (برای هر بسته فراگیر یک شماره منحصر بفرد درج میشود که در صورت دریافت مجدد مسیریاب آنرا نادیده انگاشته و حذف مینماید.)
- قرار دادن طول عمر برای بسته ها: (یک فیلد شمارنده در سرآیند بسته قرار داده میشود و به ازای عبور از هر مسیر یاب یک واحد کاهش می یابد ،هر گاه شماره به 0 رسید بسته از شبکه حذف خواهد شد.)

عملکرد الگوریتمهای LS

1- مسیر یابهای مجاور خود را که بصورت فیزیکی به آنها متصل است شناسایی کرده و آدرس آنها را بدست آورد.

2- هزینه مسیریابهای مجاور خود را اندازه گیری نماید.

3- یک بسته بسازد و تمام اطلاعاتی که از مسیریابهای مجاور خود دارد را در آن قرار بدهد.

4- بسته ساخته شده را به روش سیل آسا برای تمام مسیریابهای شبکه ارسالنماید و همچنین بسته هایی را که از مسیریابهای دیگر میرسد دریافت و ذخیره کند.

5- گراف شبکه را تشکیل داده و با استفاده از الگوریتمی مناسب ،بهینه ترین مسیر را بین هر دو مسیریاب در شبکه پیدا نماید.

Link State Update

- مسیر یاب پس از جمع آوری اطلاعات از مسیریابهای مجاور خود بسته LS را تشکیل میدهد.

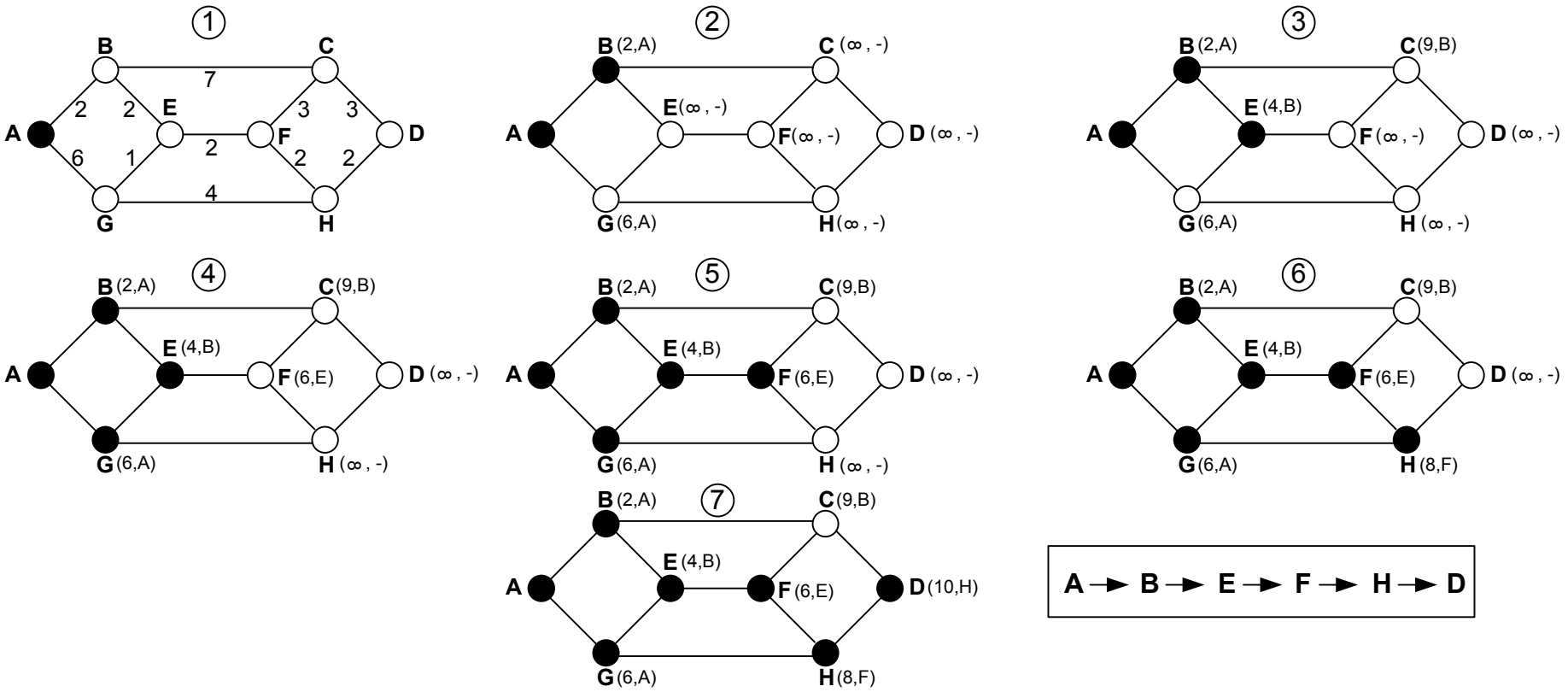
اطلاعات یک بسته LS

1- آدرس جهانی (IP) مسیر یاب تولید کننده بسته

2- یک شماره ترتیب (تا بسته های تکراری از بسته های جدید تشخیص داده شوند)

3- طول عمر بسته (تا اطلاعات بسته ،زمان انقضای اعتبار داشته باشد)

4- آدرس جهانی مسیریابهای مجاور و هزینه تخمینی



- هر مسیر یاب بدون آنکه اطلاعی از هزینه لینکهای ارتباطی در زیر شبکه داشته باشد جدولی را در حافظه خود نگه میدارد که جدول مسیریابی نام دارد Routing Table

- در این جدول به ازای هر مسیریاب درشبکه یک رکورد وجود دارد و هر رکورد دارای دو فیلد مجزا زیر است.

Routing Table Fields

1- فیلد مسیر: این فیلد خط خروجی مناسب برای رسیدن به یک مسیر خاص در شبکه را مشخص میکند.

2- فیلد مقدار تقریبی هزینه: این فیلد هزینه تقریبی رسیدن یک بسته تا مسیریاب مقصد را تعیین میکند.

- هر مسیریاب موظف است هزینه خطوطی را که بصورت فیزیکی با مسیریابهای دیگر دارد محاسبه کرده و در جدول خود درج نماید.

- مسیریابها در بازه زمانی مشخص ستون هزینه از جدول مسیر یابی خوشان را به مسیریابهای مجاور ارسال میکنند.

- در الگوریتم DV جداول با یک الگوریتم بسیار ساده به هنگام میشود.

- پرتکلهای DV دارا مشکل عدم همگرایی سیع جداول مسیریابی در هنگام خرابی یک مسیریاب با یک کانال ارتباطی است این مشکل شمارش تا بینهایت نام گرفته است (count to infinity)

Split Horizon

- برای حل مشکل شمارش تا بینهایت وقتی یک مسیریاب میخواهد اطلاعاتی را به همسایه هایش بدهد هزینه رسیدن به آنهایی را که قطعا باید از همان مسیریاب بگذرد را اعلام نمیکند(یا ∞ اعلام میکند)

- چه در روشهای LS وچه در روشهای DV پس از آنکه مسیرهای بهینه به یکایک شبکه ها پیدا شد نتیجه در جدول مسیریابی جدول هدایت Forwarding Table ذخیره شده و تا زمان بهنگام بهینه سازی بعدی تغییری نخواهد کرد.

تفاوت الگوریتمهای DV & LS

LS

- در الگوریتم LS با فرض داشتن n مسیریاب مجاور و با توجه به اینکه هر مسیریاب نیز دارای K مسیریاب مجاور باشد،جهت نگهداری هزینه کل مسیرها به جدولی با n * K سطر نیازمندیم به همین دلیل این الگوریتم دارای هزینه زمانی اولیه محاسباتی بالایی است و همچنین فضای زیادی نیز اشغال خواهد کرد،اما با داشتن کلیه هزینه ها دارای جستجوی سریعی میباشد.

DV

- در الگوریتم DV هرمسیر یاب فقط هزینه مسیریابهای مجاور را ضبط و نگهداری میکند بهمین دلیل با فرض داشتن n مسیریاب مجاور جدولی با n سطر در هر مسیریاب موجود میباشد پس هزینه زمانی محاسباتی اولیه پایین بوده اما در ادامه جستجو، با توجه به محاسبات درای هزینه بیشتری است.

جداول ارسالی توسط مسیریابهای مجاور J

	A	I	H	K
A	0	24	20	21
B	12	36	31	28
C	25	18	19	36
D	40	27	8	24
E	14	7	30	22
F	23	20	19	40
G	18	31	6	31
H	17	20	0	19
I	21	0	14	22
J	9	11	7	10
K	24	22	22	0
L	29	33	9	9

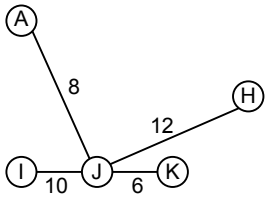
جدول مسیریابی مربوط به مسیریاب J قبل از دریافت جداول مسیریابهای مجاور

	خط	هزینه تقریبی
* A	A	8
B	A	-
C	I	-
D	H	-
E	I	-
F	I	-
G	H	-
* H	H	12
* I	I	10
* J	-	0
* K	K	6
L	K	-

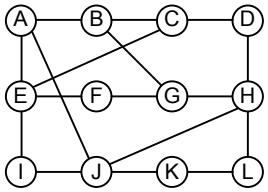
جدول مسیریابی مربوط به مسیریاب J بعد از دریافت جداول مسیریابهای مجاور

	خط	هزینه تقریبی
A	A	8
B	A	20
C	I	28
D	H	20
E	I	17
F	I	30
G	H	18
H	H	12
I	I	10
J	-	0
K	K	6
L	K	15

مسیریابهای مجاور مسیریاب J



زیرساخت ارتباطی شبکه فرضی با 12 مسیر یاب



محاسبه بهترین مسیر J به G

J 8→ A 18→ G 18+8=26
J 10→ I 31→ G 10+31=41
J 6→ K 31→ G 6+31=37
J 12→ H 6→ G 12+6=18

(H,18)

محاسبه بهترین مسیر J به F

J 8→ A 23→ F 8+23=31
J 10→ I 20→ F 10+20=30
J 6→ K 40→ F 40+6=46
J 12→ H 19→ F 19+12=31

(I,30)

محاسبه بهترین مسیر J به C

J 8→ A 25→ C 25+8=33
J 10→ I 18→ C 10+18=28
J 6→ K 36→ C 36+6=42
J 12→ H 19→ C 19+12=31

(I,28)

معایب(کاستیهای) پرتکل IP

- تضمینی وجود ندارد وقتی بسته ای برای یک ماشین مقصد ارسال میشود آن ماشین آماده دریافت آن بسته باشد و بتواند آن را دریافت کند.
- تضمینی وجود ندارد وقتی چند بسته متوالی برای یک ماشین ارسال میشود به همان ترتیبی که برروی شبکه ارسال شده اند در مقصد دریافت گردند.
- تضمینی وجود ندارد که وقتی بسته ای برای یک مقصد ارسال میشود.به دلیل دیررسیدن ،مجددا ارسال نشود .درچنین حالتی ممکن است بسته ای به اشتباه دوبار در مقصد دریافت شود.
- لایه IP هیچ وظیفه ای در قبال توزیع بسته ها بین پروسه های مختلفی که بر روی ماشین واحد اجرا شده اند ندارد.
- لایه IP هیچ وظیفه ای در قبال تنظیم سرعت تحویل بسته ها به یک ماشین ندارد.

***پرتکل اتصال گرا* (Connection Oriented)**

- به پرتکلهایی که قبل از مبادله داده سعی در برقراری یک ارتباط و ایجاد هماهنگی قبلی مینمایند پرتکلهای اتصال گرا گفته میشود.

***پرتکلهای* PAR (Positive Acknowledgement with Retransmission)**

- به پرتکلهایی که فقط در هنگام دریافت صحیح داده ها پیغام Ack برمیگردانند و در صورت دریافت بسته خراب ساکت می مانند پرتکلهای PAR گفته میشود.

***آدرس پورت* (Port Number)**

- هر پروسه برای تقاضای برقرای یک ارتباط با پروسه ای دیگر روی شبکه،یک شماره شناسایی برای خود برمیگزیند به این شماره شناسایی آدرس پورت گفته میشود.

***آدرس سوکت* Socket Address**

- مجموع آدرس IP و آدرس پورت یک پروسه یکتا و واحد را بر روی هر ماشین در دنیا مشخص میکند که آدرس سوکت گفته میشود.

(IP Address:Port Number)=Socket Address

192.168.12.14:8080

ساختار یک بسته TCP

7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Source Port																**Destination Port**															
Sequence Number																															
Acknowledgement Number																															
TCP Header Length				**Unused**				**URG**	**ACK**	**PSH**	**RST**	**SYN**	**FIN**			**Window Size**															
Checksum																**Urgent Pointer**															
Option(0 or more 32-bit words)																															
Data(optional)																															

Source Port (آدرس پورت مبداء) **Destination Port**(آدرس پورت مقصد)

Sequence Number (شماره ترتیب آخرین بایت در فیلد داده از بسته جاری)

Acknowledgement Number (شماره ترتیب بایتی را که فرستنده بسته منتظر دریافت آن است)

TCP Header Length(طول سرایند بسته TCP بر اساس ضریب 32 بیتی)

If bit=1

URG (فیلد Urgent Pointer مقداری قابل استناد و معتبر خواهد داشت)
ACK (عدد فیلد Acknowledgment Number مقداری معتبر خواهد بود)
PSH (فرستنده از گیرنده تقاضا میکند داده های موجود در بسته را بافر نکند.)
RST (ارتباط بصورت یکطرفه و ناتمام قطع خواهد شد)
SYN (مربوط به برقراری ارتباط سه مرحله ای)
FIN (ارسال با آخرین بسته برای قطع ارتباط بصورت یکطرفه)

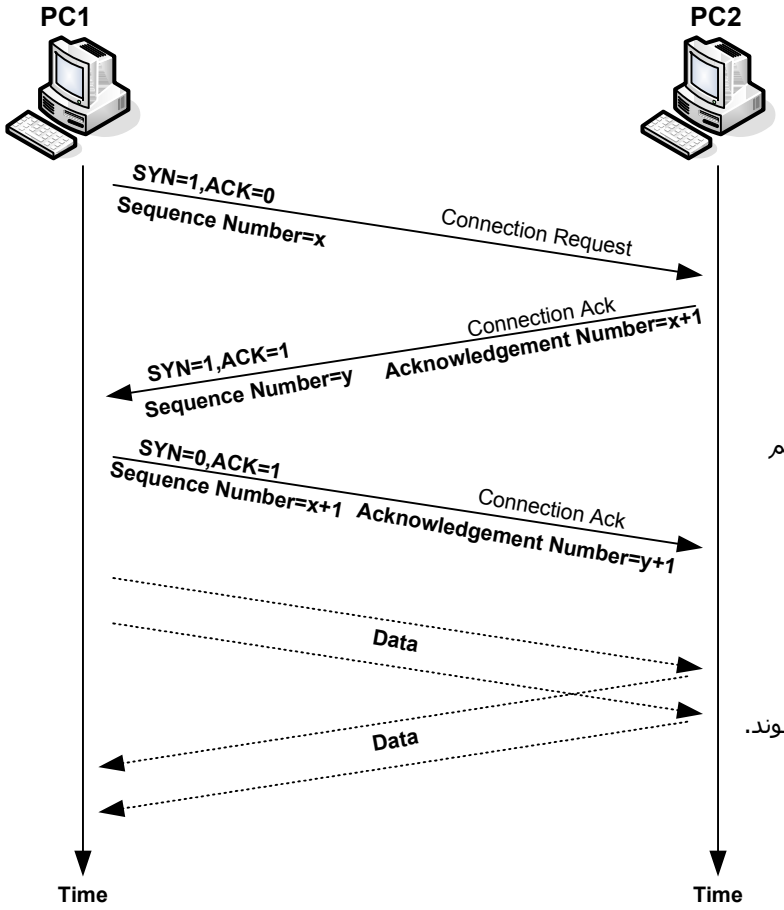
Window Size (برای کنترل جریان داده ها{ارسال همزمان بیشت یا کمتر})

Checksum (کد کشف خطا)

Urgent Pointer (یک عدد بعنوان اشاره گر قرار میگیرد که موقعیت داده های اضطراری درون بسته TCP را معین میکند)

مراحل دست تکانی سه مرحله ای برای برقراری ارتباط در پرتکل TCP

3 Way Handshake in TCP Protocol



ساختار یک بسته UDP

7 6 5 4 3 2 1 0	7 6 5 4 3 2 1 0	7 6 5 4 3 2 1 0	7 6 5 4 3 2 1 0
Source Port		**Destination Port**	
UDP Length		**UDP Checksum**	
Data			

Source Port (آدرس پورت مبداء)

Destination Port(آدرس پورت مقصد)

UDP Length (در این فیلد طول بسته UDP برحسب بایت{شامل سرآیند داده ها} درج میشود)

UDP Checksum (در این فیلد کد کشف خطا درج میشود)

- مناسبترین کاربرد پرتکل UDP برای پروسه هایی است که عملیاتشان مبتنی بر یک تقاضا و یک پاسخ است (مثل سیستم DNS و ارسال تصاویر زنده)

ماشینهای Little Endian

- ماشینهایی که ابتدا بایت کم ارزش و سپس بایت پر ارزش را در حافظه ذخیره میکنند ،ماشینهای Little Endian نامیده میشوند.کامپیوترهای شخصی با پردازنده سری 80X86 و پنتیوم از این دسته هستند.

ماشینهای Big Endian

- ماشینهایی که ابتدا بایت پر ارزش و سپس بایت کم ارزش را در حافظه ذخیره میکنند ،ماشینهای Big Endian نامیده میشوند. کامپیوترهای سری SUN از این دسته هستند.