Subject: شبکه‌های کامپیوتری
Date: دوشنبه ۱۴:۰۰ تا ۱۶:۴۰

۱۴ جزوه پایان ترم

۲ جزوه میان ترم و حضور غیاب

۲ جزوه ارائه

Scanned with CamScanner

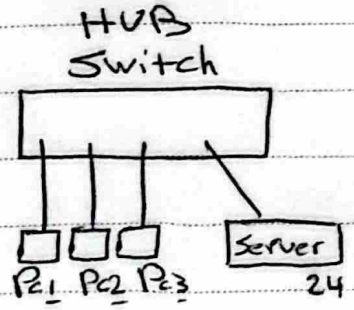
Subject: جلسه اول
Date

جزوه شبکه های کامپیوتری

انواع شبکه از نظر وسعت جغرافیایی:

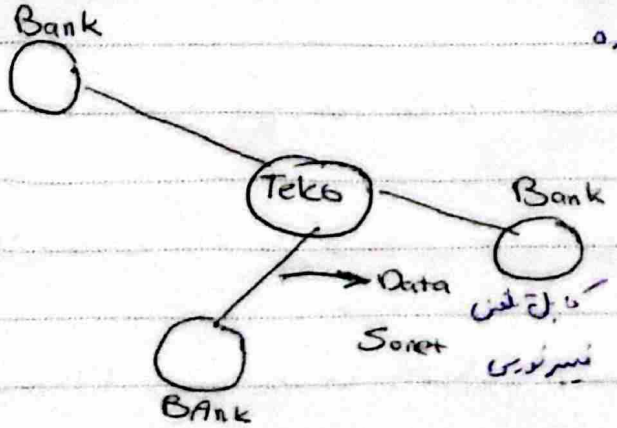
محلی
۱_LAN (Local Area Network)

به شبکه های محلی در وسعت کوچک مانند: شرکت، کارخانه و حتی یک دانشکده، به وسعت کوچکی را شامل می شود شبکه های LAN می گوییم. در این شبکه تمامی Device ها به وسیله کابل شبکه به دستگاه مرکزی به نام Hub یا Switch متصل میشود که میتوانیم به صورت کابل از منابع یکدیگر استفاده کنند



شهری
۲_MAN (MetroPolitan Area Network)

از به هم پیوستن چندین شبکه LAN به یکدیگر متصل میشود شبکه MAN می گوییم ارتباط بین شعب بانک در یک شهر یا به هم پیوستن چند دانشکده

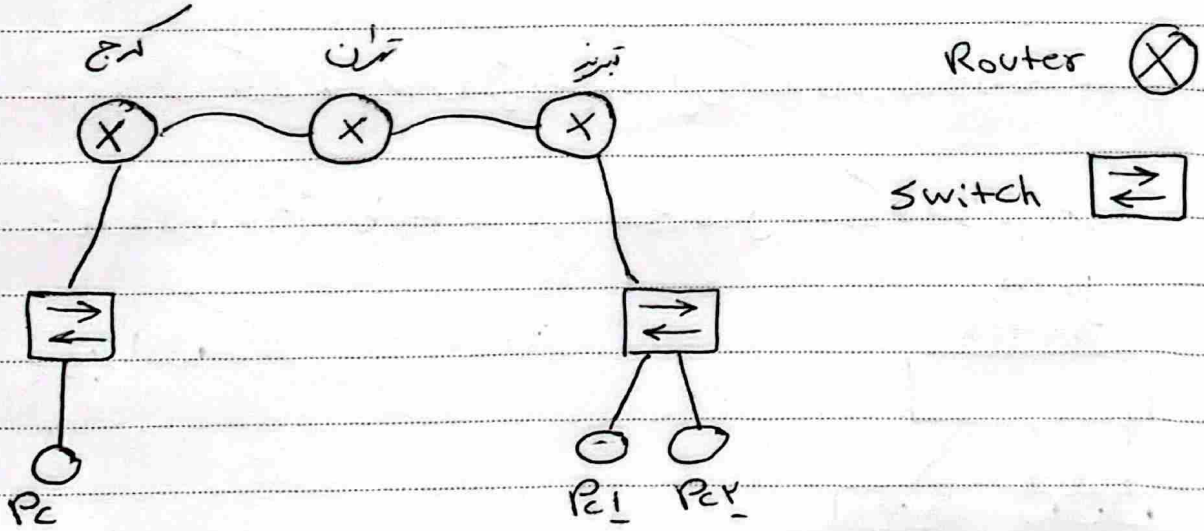


Subject:
Date

۴_WAN (Wide Area Network)

به شبکه هایی که از به هم پیوستن چندین شهر، استان، کشور یا حتی قاره ها به هم تشکیل میشود

شبکه WAN می گوییم. Router ها نقش اساسی در شبکه WAN دارند



بزرگ ترین شبکه WAN اینترنت می باشد.

تاریخچه شبکه:

شبکه در سال ۱۹۶۰ متولد شده و نام اولین شبکه ARPAnet بود که از این شبکه به منظور ایجاد ارتباط بین پایگاه های نظامی با استفاده از خطوط تلگراف و تلفن ایجاد شد که در سال ۱۹۷۰ مراکز علمی و تجاری نیز به این شبکه پیوستند. با پایدار شدن اینترنت در سال ۱۹۸۰ این شبکه ها باهم ادغام شدند و در سال ۱۹۸۹ با به وجود آمدن

Subject:
Date

اولین صفحات وب، شبکه تقریباً ساختاری به خود گرفت (کامل شد).

شبکه چیست؟

از به هم پیوستن کامپیوترها و Device های مختلف مانند مودم، سوئیچ، چاپگرهای تحت شبکه و استفاده از منابع یکدیگر به روش سیمی و بدون سیم (wireless) شبکه پدید می آید.

دلایل استفاده از شبکه:

۱- تبادل اطلاعات ۲- استفاده اشتراکی از منابع (مثل اینترنت، چاپگر، نایل و...)

۳- انجام محاسبات پیچیده (با استفاده از چندین سیستم به صورت هم زمان)

اجزا اصلی شبکه:

۱- End system: به هر وسیله ای که بتواند از منابع شبکه استفاده کند یا سرویسی را در شبکه به بقیه سیستم ها ارائه دهد End system می گوییم. مثل: PC ها، چاپگرها، سرورها، دوربین مداربسته و...

End system ها به دو دسته کلی تقسیم میشوند:
۱- Client
۲- Server

۱- Client: به سیستم هایی اطلاق میشود که به صورت عمومی در شبکه کار می کند و اصولاً

Subject:
Date

سرویس گیرنده هستند. (معمولاً کامپیوترهای کاربران هستند) (سیستمی که سرویس دریافت می‌کند)

۲- Server: به سیستم هایی اطلاق می‌شود که سخت افزار قدرتمندتری نسبت به Client ها دارند و جزء سرویس دهنده ها می‌باشند (مثل وب سرور یا فایل سرور)

۲) IMP: به هر ابزاری که End System ها را به هم وصل می‌کند مانند Router & Hub

IMP می‌گوییم که دو نوع دارد { Core / Edge } Fireman ، Switch

۱- Core: به IMP هایی که در وسط شبکه قرار دارند و برای حجم قابل ملس نیست و اصولاً در اتاق سرورها، دیتا سنترها و ISP ها مستقر هستند

۲- Edge: IMP هایی که به صورت مستقیم با End System ها در تماس هستند. مثل مودم Adsl

۳) Media: به هر دیرایی که سیگنال را از خودش عبور می‌دهد Media گفته می‌شود که در شبکه های سیمی مدیا کابل است و در شبکه های wireless (بی‌سیم) مدیا هوا است.
یا به تعریفی دیگر:

به اجزایی که end system ها را به IMP ها متصل می‌کند و سیگنال را از خود عبور می‌دهد media می‌گوییم

Subject:
Date

انواع IMP ها در مدل OSI:

۱) Layer1 HUB: فقط وظیفه برقراری ارتباط دارند و هیچگونه مدیریتی روی اطلاعات انجام نمی دهند.

۲) Layer2 Switch: علاوه بر وظیفه Hub مدیریت روی داده ها نیز انجام می دهد (یک سری دستور، یک سری config)

۳) Layer3 Router: امکان ارتباط بین ۲ یا چند شبکه متفاوت را برقرار می کند

۴) Layer4 Firewall: توانایی کنترل ورودی و خروجی های یک شبکه، کنترل ترافیک و نظارت بر اعمال کامل کاربران را بر عهده دارد.

مدل OSI: یک مدل مرجع هفت لایه ای است که عام استاندارد های پروتکل های خاص در این لایه فعالیت می کنند که هفت لایه آن عبارتند از:

۷	Application
۶	Presentation
۵	Session
۴	Transport
۳	Network
۲	Datalink
۱	Physical

Scanned with CamScanner

Subject:
Date

۱- لایه فیزیکی (Physical): وظیفه اصلی در لایه فیزیکی انتقال بیت ها به صورت سیگنال الکتریکی و ارسال آن بروی کانال می باشد. واحد اطلاعات در این لایه Bit می باشد و بنابراین این لایه هیچ اطلاعاتی از محتوای پیام ندارد و تنها بیت‌های او را ارسال یا دریافت می کند. در این لایه تقریبا سخت افزاری است مسائل مخابراتی در مبادله‌ی Bit ها تجزیه و تحلیل شده و طراحی های لازم انجام میشود. طراح شبکه می تواند برای طراحی این لایه از استاندارد های شناخته شده انتقال RS-232 RS-422 و RS-423 که سخت افزار آن ها موجود می باشد استفاده کند. این لایه هیچ وظیفه ای در مورد تشخیص و تفهیم خطا ندارد.

۲- لایه پیوند داده (Data Link): وظیفه این لایه این است که با استفاده از مکانیزم های کشف و کنترل خطا داده ها را روی یک کانال انتقال که ذاتا دارای خطا است، بدون خطا و مطمئن به مقصد برساند. در حقیقت میتوان وظیفه این لایه را بیمه اطلاعات در مقابل خطاهای احتمالی دانست. کشف خطا که از وظایف این لایه می باشد میتواند از طریق اضافه کردن Bit های کنترل خطا مثل Bit های Parity check، checksum و CRC انجام شود.

Subject:
Date

وظیفه دیگر این لایه کنترل جریان یا به عبارت دیگر تنظیم جریان ارسال فریم (Frame) ها به گونه ای است که اگر یک دستگاه Imp کند باشد Data را از دست ندهد و با تنظیم جریان از هدر رفت دیتا جلوگیری شود. واحد اطلاعات در این لایه فریم (Frame) می باشد

۳- لایه شبکه (Network): یکی از مهم ترین لایه های OSI لایه شبکه می باشد

در این لایه اطلاعات به صورت بسته های سازمان دهی شده و برای انتقال مطمئن تحویل لایه دوم میشود. یکی از وظایف اصلی این لایه Routing یا مسیریابی می باشد که هر مسیریاب به صورت ایستا (Statick) و پویا (Dynamic) بسته ها را تا رسیدن به مقصد نهایی مسیریابی می کند این لایه ذاتاً بدون اتصال است.

Connection less oriented (بدون اتصال)

Connection oriented (اتصال گرا)

یعنی پس از تولید یک بسته اطلاعاتی در مبدأ بدون هیچ تضمینی آن بسته تا مقصد نهایی پیش می رود

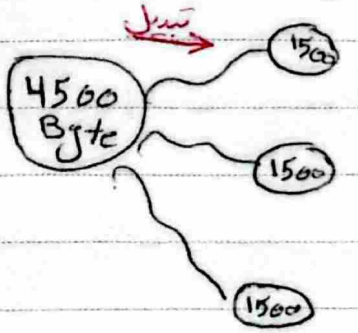
یکی از پروتکل های مهم و حیاتی در لایه شبکه IP (Internet Protocol) می باشد

واحد اطلاعاتی در این لایه Packet یا بسته می باشد.

PAPCO

Subject:
Date

۴- لایه انتقال (Transport) : لایه انتقال در این لایه براساس خدمات لایه زیرین یک سرویس انتقال بسیار مطمئن و اتصال گرا (Connection oriented) ارائه میشود. از وظایف مهم این لایه میتوان به موارد زیر اشاره کرد:



۱- تقسیم بسته بزرگ تر به کوچک تر (Fragmenting)

۲- بازسازی بسته های اطلاعاتی و تشکیل یک پیام کامل

۳- شماره گذاری بسته های کوچک تر جهت بازسازی

۴- تعیین مکانیزم ناگ گذاری ایستگاه هایی که در شبکه اند.

نکته: دو پروتکل مهم در این لایه فعالیت می کنند TCP, UDP می باشد

UDP: Connection Less oriented (بدون اتصال گرا) - تضمین ارسال ندارد (تضمین نداریم تو رسیدن بسته ها) - معیار آن سرعت است (سرعت ↑) - امنیت ↓

TCP: Connection oriented (اتصال گرا است) - تضمین میکند (تضمین دایم در رسیدن بسته ها) - سرعت ↓ - امنیت ↑



دقت مهم

PAPCO

Subject:
Date

۵- لایه نشست (session) : وظیفه این لایه فراهم آوردن یک جلسه هاست

ورود به سیستم از راه دور، احراز هویت طرفین، نگهداری این نشست و توانایی از سرگیری

یک نشست در هنگام قطع ارتباط. در این لایه واحد ارتباط پیام می باشد.

وظایف این لایه را میتوان در مراحل زیر خلاصه کرد:

۱- برقراری و مدیریت یک جلسه

۲- شناسایی طرفین

۳- مشخص نمودن اعتبار پیام ها

۴- اتمام جلسه

۵- حسابداری مشتری ها

مثل ورود کارت بانکی در ATM که پردازش اولیه انجام میشود و یک نشست فعال

انجام میشود برای مثال رمزچه درست چه غلط اون نشست برقرار میشه،

مثلا تا پرداخت میره، رمز غلط باشه میله غلطم

PAPCO

Subject:
Date

۶- لایه ارائه (Presentation) : در این لایه وظایف عمومی نسبتاً مهمی انجام می پذیرد. چهار وظیفه مهم به شرح زیر اجرا می گردد:

۱- فشرده سازی

۲- رمزنگاری برای ارسال داده های محرمانه

۳- رمزگشایی

۴- تبدیل کدها به یکدیگر وقتی دو ماشین از استانداردهای مختلفی استفاده می کنند.

مثل تبدیل متن EBCDie به کد اسکی (ASCII) و برعکس

۷- لایه Application : لایه کاربرد یا کاربرد بالاترین لایه OSI است

استاندارد مبادله پیام بین نرم افزارهایی که در اختیار کاربر بوده و به نحوی با شبکه در ارتباط اند تعریف می شوند. این لایه شامل تعریف استانداردهایی نظیر انتقال نامه های الکترونیکی، انتقال مطمئن فایل، دسترسی به بانک های اطلاعاتی و ارتباطی از راه دور، مدیریت شبکه و انتقال صفحات وب است

Subject:
Date

توپولوژی (Topology) ، به تفاهم نامه مشترک بین تجهیزات گفته می شود که در آن یک سری از استانداردهای تعریف و دستگاه های مختلف ملزم به رعایت آنند.

به تفاهم نامه مشترک بین تجهیزات که طبق استاندارد همان توپولوژی فعالیت کنند توپولوژی می گویند.

ا- Topology Bus : یک توپولوژی قدیمی که اولین بار در شبکه ساخته شد (اولین توپولوژی Bus نود)

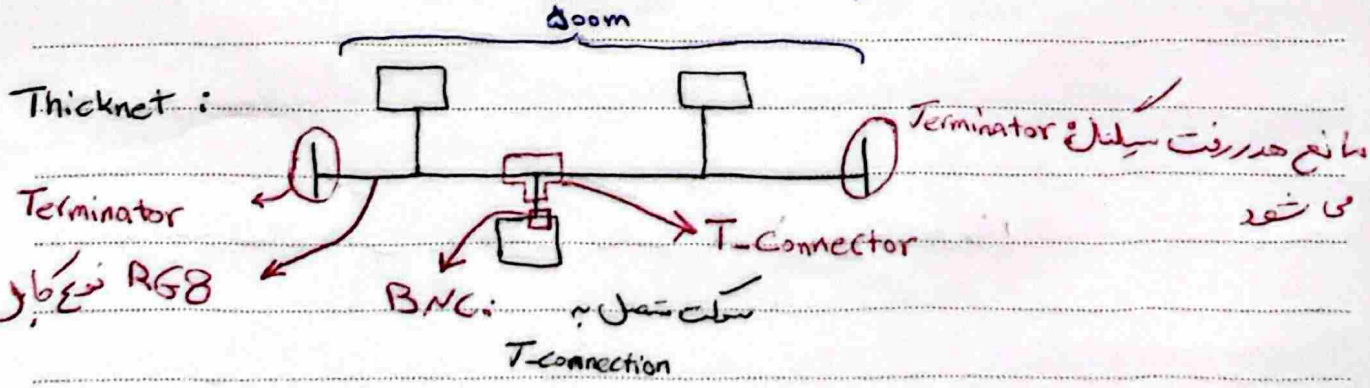
اولین شبکه Topology که نصب و راه اندازی و گسترش آن نیز بسیار ساده است

و کابل های مسی دارد که در این روش همه computer ها پشت سرهم و در یک خط با

کابل Coaxial متصل می شوند. کابل کشی ها در توپولوژی Bus با در استاندارد

Thicknet برای شبکه های ضخیم و Thinnet برای شبکه های نازک هستند

Thicknet :

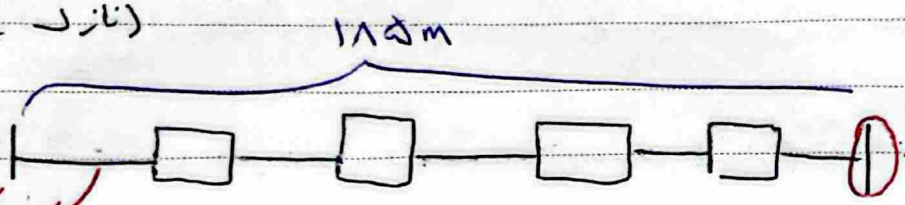


Thicknet (ضخیم) ، در نهایت (max) اندازه ۵۰۰ متری دارد. جنس سیم RG8

و به دستگاه مدلزی AUI متصل می شود

Subject:
Date

Thinnet (نازک)



نوع کابل
RG59

مانع هدررفتن سیگنال می‌شود

طول (max) نهایت ۱۸۵m و نوع کابل RG59

مزایا: ۱- راه اندازی سریع و گسترش آن آسان است

۲- نصب و راه اندازی ارزان قیمت

۳- به دانش تخصصی زیادی نیاز ندارد

۴- امنیت بالای آن به دلیل عدم دسترسی به اینترنت

معایب: ۱- اگر به هر علتی هرجای کابل قطع، سوختگی یا پاره شود کل شبکه Down یا مختل می‌شود

۲- سرعت بسیار پایین آن نهایت حداکثر ۱۰Mbps

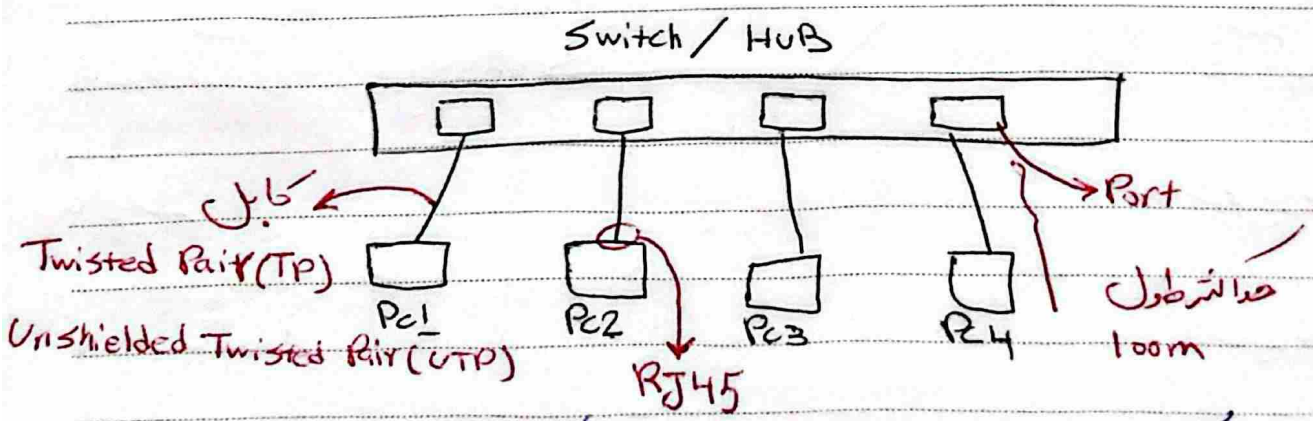
Subject:
Date

۲- Topology Star: در این نوع Topology همه سیستم ها به صورت مجزا با کابل Twisted Pair یا UTP و با سوکت RJ45 به دستگاه مرکزی به نام Hub یا Switch متصل می شوند. Topology Star معمولاً در شبکه های LAN استفاده می شود.

حداکثر طول آن ۱۰۰ m است و اگر بیشتر شود افت سیگنال اتفاق می افتد.

سرعت این شبکه ها با توجه به رعایت کردن استاندارد های کابل کشی و نوع کابل ها

۱۰ / ۱۰۰ / ۱۰۰۰ می باشد



راه اندازی این شبکه نسبت به توپولوژی Bus به دانش شبکه نیاز دارد.

اولین مزیت توپولوژی Star این است که به دلیل این که Computer ها با کابل مجزا به Switch متصل است تحمل خطا بالاتری دارد و اگر یک کابل دچار ایراد شود فقط همان Pc یا Computer دچار ایراد می شود. یکی از اشکالات آن نیز در این است که اگر Switch یا HUB خراب شود کل شبکه مختل (Down) می شود

Scanned with CamScanner

Subject:
Date

طریقه سوکت زدن با کابل های شبکه با دو استاندارد A و B به شرح زیر می باشد:

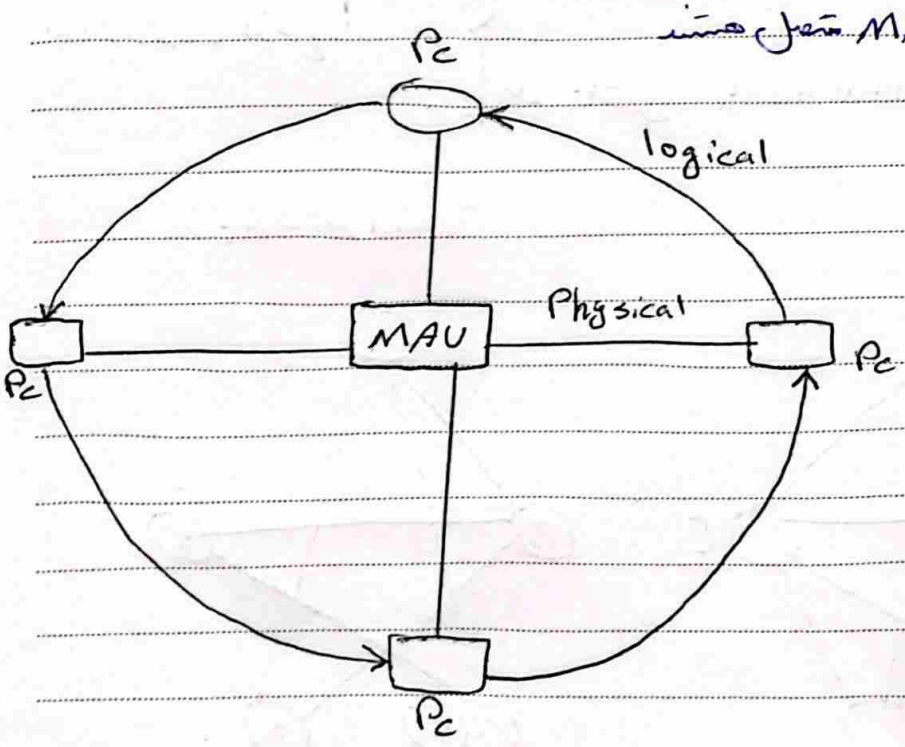
class A:		class B:
۱- سفید سبز		۱- سفید نارنجی
۲- سبز	change	۲- نارنجی
۳- سفید نارنجی		۳- سفید سبز
۴- آبی		۴- آبی
۵- سفید آبی	change	۵- سفید آبی
۶- نارنجی		۶- سبز
۷- سفید قهوه ای		۷- سفید قهوه ای
۸- قهوه ای		۸- قهوه ای

نکته: به ایستگاه کاری شبکه های Star ← Keystone Box گفته می شود.

Scanned with CamScanner

Subject:
Date

۲- Topology Ring (توپولوژی حلقه): از نظر انتقال سیگنال یک شبکه ی حلقه ای به این دلیل که هر کامپیوتر منطقاً به کامپیوتر همسایه خود وابسته است مانند شبکه Bus است اما در این نوع شبکه برخلاف توپولوژی Bus که انتهای کابل ها با Terminator بسته می شود به یکدیگر متصل میشوند و یک حلقه تشکیل میدهند. تمام کامپیوترها به دستگاه مرکزی به نام MAU متصل هستند



انتقال بسته در این روش به صورت ساعتگرد است. MAU که نوعی کابل می باشد اطلاعات را از یک Port گرفته و به نوبت به تک تک Port های دیگر می فرستد.

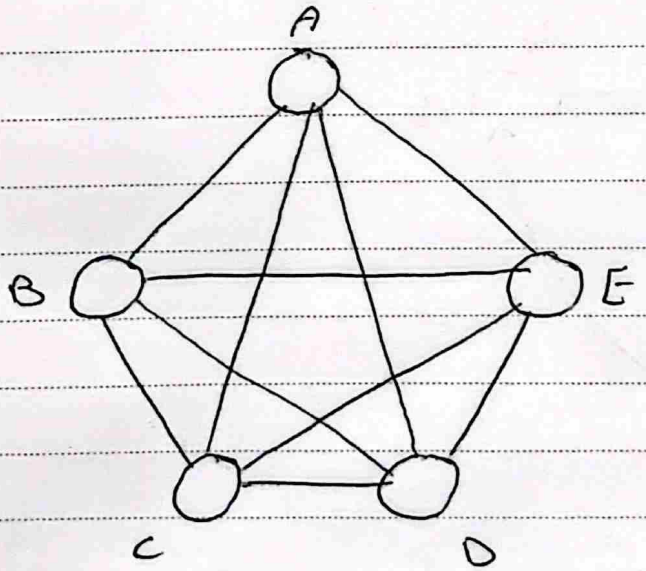
در این شبکه کد بسته ای به نام token که در دستگاهی قرار دارد دور حلقه تشکیل می شود که در نهایت Device ای آن را قبول کند یا بین بست رخ بدهد این شبکه به Token Ring هم معروف است

Subject:
Date

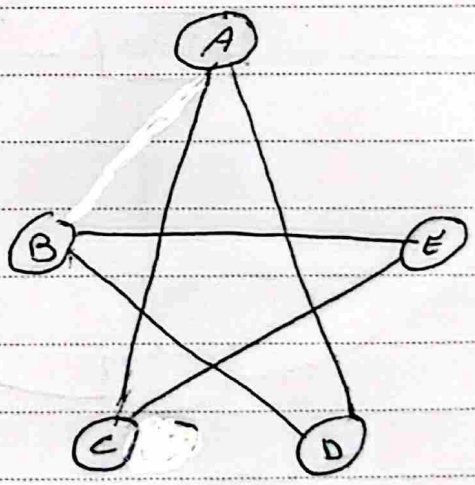
۴. Topology Mesh (توپولوژی مش): اگر در شبکه ای تعمل خطا بالایی را بخواهیم و آن شبکه همیشه باید پایدار بماند از توپولوژی mesh استفاده می کنیم. در این شبکه اگر قطعی به هر نحوی رخ دهد باز هم ارتباط بین دستگاه ها باقی می ماند و فقط نیاز کمتری داشته باشد ولی بی ارتباطیت ملدهه قطع شدند.

این توپولوژی دو نوع دارد:
۱- کامل full mesh
۲- ناقص Partial mesh

Full mesh:



Partial mesh:



عیب: پر هزینه است

Scanned with CamScanner

Subject:
Date

ل- Wireless Topology (توپولوژی بی سیم): این توپولوژی سن کمتری نسبت به توپولوژی های کیبل دار مدیا آن هوا است و دو نوع می باشد:

- Wireless
  - AD Hoc (محلی و کوچک) ارتباط سودم
  - infrastracture شبکه های BTS سل های مخابراتی یا شبکه های بزرگ
    مثل شبکه های MAN که به صورت Wireless به همدیگر متصل اند

انواع مدیا کابلی: ۱- Coaxial ۲- Twisted Pair ۳- ISDN ٤- X25

۵- fiber optic

۱- Coaxial: در این نوع کابل هسته مسی جهت انتقال اطلاعات استفاده می شود و روکش آن Shield است. نهایت سرعت آن 10Mb/Ps است و در دو نوع RG8 و RG58, RG59 می باشد

۲- Twisted Pair یا UTP: به کابل های شبکه امدوزی که ۸ رشته و ٤ زوج دارد کابل های Twisted Pair می گوییم. نحوه کابل کشی آن ها بر دو استاندارد A, B است و حداکثر طول کابل 100m است.

Subject:
Date

تقسیم بندی آن ها با category های مختلف مشخص می کنیم مثلا:

- category
  - cat 5
  - cat 5e
  - cat 6
  - cat 6e
  - cat 7

در سرعت ها شون متفاوت هستند. سرعت آن ها

10mb/ps و 100mb/ps و 1000mb/ps است.

به نوع داخلی (indoor) آن جهت کابل کشی داخلی ساختمان UTP و به کابل های خارجی (outdoor) STP می گویند که روکش آلومینیومی دارد.

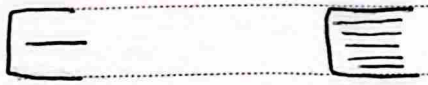
۳- ISDN: کاربرد اصلی این کابل انتقال تصویر می باشد به عنوان مثال آیفون های تصویری از این نوع کابل استفاده می کنند و سرعت انتقال آن 128Kb/ps است و حداکثر طول کابل 100m است.

۴- X25: این کابل برای انتقال فکس با سرعت بالا استفاده می شود. نوعی دیگر از کابل های تلفن است که به مراتب سرعت آن جهت انتقال فکس از کابل های تلفن بالاتر است. نهایت سرعت آن 1.5 Mb/ps است و طول کابل آن 75m می باشد

PAPCO

Subject:
Date

۵) fiber optic: در این نوع کابل دیتاها به وسیله یک رشته لیزر یا چند رشته لیزر کار انتقال دیتا را انجام میدهد.



Single mode multi mode

انواع مدیا بی سیم: ۱- wifi ۲- Wimax ۳- micro wave ۴- infrared (مادون قرمز)

۵- laser

۱- wifi: به عنوان اولین منادی انتقال دیتا به روش بی سیم مطرح گردید.

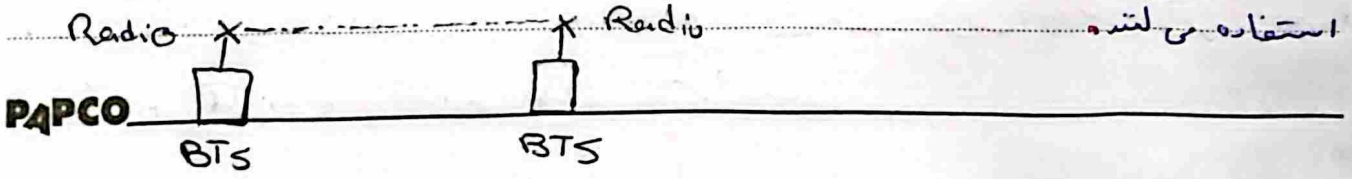
wifi
- Modem wifi
- Access Point

این ها دیوایس هایی هستند که در این شبکه کار می کنند دیوایس ها در این شبکه:

و از استاندارد IEEE 802/11 استفاده می کنند

۲- wimax: یکی دیگر از روش های انتقال دیتا به صورت بی سیم می باشد در آن از رادیو (radio) به عنوان دستگاه های انتقال سیگنال و دیتا استفاده می شود. سرعت به مراتب بالاتر از wifi دارد و تجهیزات آن روی کدل ها نصب می گردد.

۳- micro wave: رادیو ها در این روش حتماً باید دید به روی هم دیگر قرار بگیرند و هم دیگر را ببینند. اکثر پدافندهای هوایی از این روش برای ارسال داده های حساس به صورت لیزری استفاده می کنند.



Scanned with CamScanner

Subject:
Date

۴- مادون قرمز (infrared): مادون قرمز شعاع کمتر از ۱m را پوشش میدهد در ضمن دستگاه ها در این روش حتما باید روبه روی هم دیگر قرار بگیرند و در نهایت سرعت آن 1mb/ps است

d- laser: سرعت آن مانند فیبر نوری و گاهی بالاتر است مبدأ و مقصد حتما باید روبه روی یکدیگر باشند به صورت پرتاب تلی و چند رشته ای کار می کند.

انواع سیستم عامل های شبکه:

۱- Windows NT, 2000: اولین سیستم عامل های تحت شبکه که برمبنا هسته Dos در سال ۱۹۹۳ شرکت Microsoft ویندوز NT ۱ معرفی و در سال 2000 اولین ویندوز سرور به نام Windows 2000 طراحی و اجرا کردید بعدها در سال 2003 اولین و کامل ترین نسخه ویندوز سرور Windows server 2003 بود که سرویس های متعدد سرویس مثل DHCP و Active Directory را ارائه داد.

۲ Novell

نکته ۱: سیستم عامل های Novell برای توپولوژی و شبکه های Bus طراحی و اجرا کردیده و هسته آن نیز Dos است به Netware معروف شدند شرکت Novell طراحی و توسعه داد پروتکل IP در Netware نام IPX داشت

Subject:
Date

۲- سیستم عامل های Unix: Unix یک سیستم عامل تحت شبکه و در سال ۱۹۷۰ عرضه شد و امروزه در نسخه و اشکال گوناگونی وجود دارد و برخلاف Windows, Novell متعلق به شرکت خاصی نیست. جزء سیستم عامل های open source می باشد

انواع سیستم عامل Unix:

۱- Nix System: جزء اولین برنامه های توسعه یافته Unix می باشد که توسط شرکت AT&T در سال ۱۹۷۰ شروع به کار کرد مالک اصلی این شرکت SCO می باشد

۲- BSD Unix: یکی از اولین اشکال Unix می باشد که از Unix اصلی AT&T تولید شده است و همیشه از متداول ترین محصولات Unix بوده است

متداول ترین نسخه های BSD Unix عبارتند از: ۱ Open BSD ۲ Net BSD ۳ Free BSD که نسخه رایگان و قابل دانلود می باشد

۳- Sun Solaris: شرکت Sun micro System این نسخه جهت معارف نظامی در آمریکا استفاده می شود. یکی از محبوب ترین سیستم عامل های تجاری Unix است و همچنین یکی از بهترین رابط های گرافیکی Unix یعنی Open windows را دارا می باشد

Subject:
Date

۴- Linux: بهترین و محبوب ترین نسخه سیستم عامل های Unix نسخه linux می باشد که به صورت رایگان است. Open source (قابل گسترش به صورت شخصی برای کاربران)

۳- macintosh: اپل سیستم عامل ها از همان ابتدا قابلیت شبکه بندی قوی ای داشتند به عنوان بخشی از تجهیزات استاندارد خود دارای یک رابط شبکه به نام local Talk است و سیستم عامل آن macos نام دارد و دو پروتکل اختصاصی appletalk و appleshare را دارد.

کانال های انتقال: ۱- گیرنده ۲- فرستنده ۳- کانال های فیزیکی

وظیفه سخت افزار مخابراتی در لایه ی واسط شبکه آن است که بدون توجه به نوع و محتوا داده، بیت های داده را بر روی کانال های فیزیکی منتقل کند. سخت افزار انتقال در این لایه بیشتر با مسائل الکتریکی و مخابراتی سروکار دارد.

کانال های ارتباطی که برای اتصال بین دو ماشین استفاده می شود عبارتند از:

۱- خطوط تلفن: خطوط تلفن که به کابل های زوج سیم معروف اند سرویس تلفن های ثابت و خطوط دیتا بین سازمان های مختلف از این نوع می باشند

Subject:
Date

۲- سیم های به هم تابیده شده زوجی (Twisted Pair): سیم های به هم تابیده شده زوجی که به کابل های Twisted Pair (UTP, STP) معروف اند دارای ۸ رشته ی به هم تابیده شده به صورت ۴ زوج و در یک شیلد یا PVC آلمینیومی قرار دارد. دلیل به هم تنیدگی این نوع کابل ها جلوگیری از تداخل صوتی (crosstalk) و غیره می باشد

۳- کابل های هم محور (Coaxial): کابل های هم محور (coaxial) که در انواع مختلفی است که در مدل ضخیم آن ۵۰Ω و در نوع نازک آن ۷۵Ω می باشد.

۴- کانال های ماهواره ای: کانال های ماهواره ای که در ترکانس های گیرنده و فرستنده به شرح زیر خدمات ارسال می کنند:

۱- باند C: ارسال از زمین به ماهواره در باند ۵,۹GHz تا ۶,۴GHz (۵,۹GHz ~ ۶,۴GHz) و دریافت از ماهواره در باند ۳,۷GHz تا ۴,۲GHz (۳,۷GHz ~ ۴,۲GHz)

۲- باند KU: ارسال از زمین به ماهواره ۱۴,۵GHz ~ ۱۴GHz و دریافت از ماهواره ۱۲,۲GHz ~ ۱۱,۷GHz

۳- باند KA: ارسال از زمین به ماهواره در باند ۳۰GHz ~ ۲۷,۵GHz و دریافت از ماهواره ۲۱,۷GHz ~ ۱۷,۷GHz

P4PCO

Subject:
Date

۵- کانال های رادیوی: کانال های رادیویی شامل باندهای فرکانسی مختلف مثل VHF , UHF

۶- امواج طیف نوری: شامل ماندن قرمز که با استفاده از نور و محیط شفاف و رو به روی یکدیگر دیتا را تا کمتر از 10m انتقال میدهد.

نکته: تمام کانال های گفته شده دارای مشخصه ای به نام پهنای باند هستند.

پهنای باند را میتوان توانایی و ظرفیت آن کانال در ارسال اطلاعات با نرخ B بیت در ثانیه تعریف کرد یعنی اگر می گوییم پهنای باند یک کانال 1Mb/s می باشد یعنی نمیتوان بالاتر از این ظرفیت دیتا ارسال کرد.

تسهیم: با توجه به اینکه پهنای باند بعضی از کانال ها بسیار زیاد است مثل کانال های ماهواره ای میتوان یک کانال فیزیکی را بین چندین ایستگاه تقسیم کرد این تقسیم باعث میشود که از یک کانال مشترک چندین ایستگاه استفاده کنند و هزینه های ارتباط کاهش یابد. به عمل تقسیم پهنای باند یک کانال بین چند ایستگاه عمل تسهیم یا سالتی پلکس می گوییم که تسهیم به دو روش قابل انجام است:

Subject:
Date

۱ـ تسهیم در میان فرکانس (FDM) ۲ـ تسهیم در میان زمان (TDM)

۱ـ FDM : در روش FDM با فرض اینکه حداکثر n ایستگاه 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 را انجام دهد و چون این باند فرکانسی به صورت ثابت متعلق به خودش خواهد بود هرگونه تصادم و تداخل منتفی خواهد شد (غیرممکن میشود)

TDM : در روش TDM زمان به بازه های کوچک (Time slot) تقسیم شده و هر ایستگاه مجاز است فقط در بازه ی زمانی متعلق به خودش اطلاعات را روی کانال بفرستد.

Scanned with CamScanner

Subject:
Date

IP (internet Protocol):

هر کدام مربع یک Device

IP { IPv4 ۳۲ بایت
IPv6 128 } IANAL (سازمان یانا)

قابل تغییر مثل اسم زنابیل

328it | ۸ | ۸ | ۸ | ۸ بایت | xxxxxxxx

Range

هر کدام مربع ۱۰۲۴ Device

MAC Address: آدرسی ۱۲ بایتی است که ۶ بایت اول آن مولفه کارخانه سازنده است و ۶ بایت شماره سریال دستگاه است.

Mac Address تغییر نمی‌کند ولی IP قابل تغییر است
به جز موارد خاص نظامی و دزدی

غیرقابل تغییر مثل کدملی

به هر بخش Octed می‌گویند

Mac Address → XXXXXX XXXXXX
مولفه کارخانه سازنده — شماره سریال

مثال: FFB9G8 4825AZ

تبدیل ۱۱۸ به مبنا دودویی در ۸ بایت:

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
X	✓	✓	✓	X	✓	✓	X
۰	۱	۱	۱	۰	۱	۱	۰

PqPCO

Scanned with CamScanner

Subject:
Date

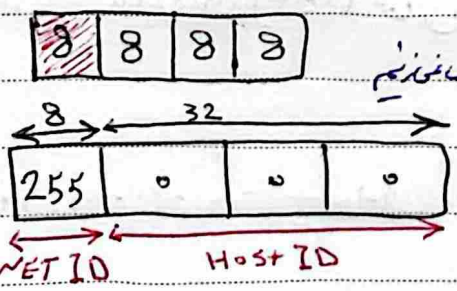
+ باید به کامپیوترها و سرورهای مختلف IP بدهیم تا کار کنند

هر IPv4 ۴ بخش دارد که هر بخش ۸ بایت است و کلاس‌ها بر اساس Net ID تقسیم‌بندی می‌شوند

+ یک IP در ابتدا و انتها نمی‌تواند به صفر ختم شود یعنی Range شبکه Octed اول و آخر آن نمی‌تواند صفر باشد ۱۹۲.۱۶۸.۰.۵ X ۰.۱۶۸.۰.۱.۱ X

این سازمان (IANA) IP ها را در تعداد مهمان‌پذیری به کلاس‌های مختلفی تقسیم‌بندی کرده:

کلاس A: از لحاظ تعداد مهمان‌پذیری بزرگ‌تر از سایر کلاس‌ها است و در اختیار سازمان‌های بزرگ است زمانی استفاده می‌شود که به تعداد بالایی IP نیاز داشته باشیم. * داخل کلاس A به این خوبی دست نمی‌زنیم



اولین عدد IP در این بازه عددی باشه می‌گیم توی

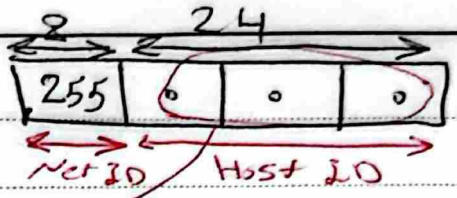
این کلاس هست ۱ تا ۱۲۶ Class A: 1 ~ 126

مشخصه اصلی Net ID آست که ۱ تا ۱۲۶ است که تعداد زیر شبکه آن است و این کلاس ۱۶۷۷۷۲۱۴ = $(۲۵۴)^۳$ Host ID را می‌پذیرد. مثال از کلاس A: ۱.۰.۰.۱ تا ۱۲۶.۲۵۴.۲۵۴.۲۵۴ (میلیون)

Subject:
Date

A: ۱ تا ۱۲۶

Subnet Mask: ۲۵۵.۰.۰.۰

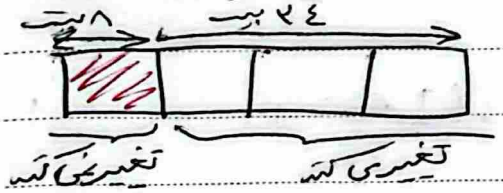


Host ID: $(۲۵۴)^۳ = ۱۶$ میلیون ← تعداد میزبان

Net ID: تعداد اولین شبکه (شناسه شبکه) Host ID: تعداد میزبان

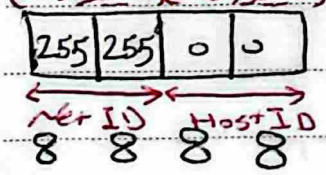
هر خانه یک اوکتت (octet) نام دارد در کلاس A اوکتت اول از سمت چپ

بین ۱ تا ۱۲۶ است از ۱۲۷ استفاده نمی‌کنیم چون loop back است.



کلاس B: برای شبکه‌های متوسط و بزرگ استفاده می‌شود.

مشخصه اصلی ۱۹۱ تا ۱۲۸ است. Net ID هم ۱۶ بیت است Host ID هم ۱۶ بیت



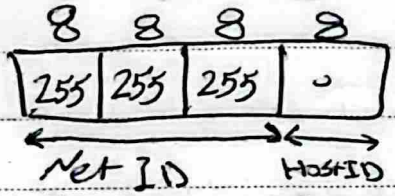
به طوری که ۱۶ تا $۶۴ = (۲۵۴)^۲$ میزبان می‌پذیرد

B کلاس: ۱۹۱ تا ۱۲۸

Subnet Mask: ۲۵۵.۲۵۵.۰.۰

Host ID: $(۲۵۴)^۲$ یا ۶۴ تا ۱۶

کلاس C: معمولی‌ترین کلاس است و عمومی‌تر است کلاس C: ۱۹۲ تا ۲۲۳



Host ID: ۲۵۴

Subnet Mask: ۲۵۵.۲۵۵.۲۵۵.۰

Scanned with CamScanner

Subject:
Date

کلاس D: از این آدرس برای ارسال یک دیتاگرام به طور همزمان برای چندین ماشین میزبان کاربرد دارد به منظور عملیات رسانه ای و چند بخشی به کار میرود.

کلاس E: فعلاً از این کلاس جهت مصارف عمومی استفاده خاصی نمی شود و گاهی جهت مصارف آزمایشگاهی و نظامی به صورت آزمایشی استفاده می شود.

آدرس های خاص: در بین تمامی کلاس های IP پنج گروه از آدرس ها معنای ویژه ای دارند و با آن ها نمی توان یک شبکه خاص را تعریف کرد یا آدرس دهی کرد

۱- 0.0.0.0: هر ماشین میزبان که از آدرس IP خودش مطلع نیست این آدرس را به عنوان آدرس خودش فرض می کند البته از این آدرس فقط به عنوان آدرس مبدأ و برای ارسال یک بسته میتوان استفاده کرد و گیرنده بسته نمی تواند پاسخی به مبدأ بسته برگرداند.

۲- 0. HostID: زمانی به کار میرود که ماشین میزبان آدرس مشخصه شبکه ای که به آن متعلق است را نداند در این حالت در قسمت NetID مقدار ۰ و در قسمت HostID شماره ی مشخصه خود را قرار میدهد

Scanned with CamScanner

Subject:
Date

۳- 255.255.255.255: برای ارسال پیام های فراگیر برای تمامی ماشین های میزبان بر روی شبکه محلی که ماشین ارسال کننده به آن متصل است.

۴- Net ID.255: برای ارسال پیام های فراگیر برای تمامی ماشین های یک شبکه ی راه دور که ماشین میزبان فعلی به آن متصل نیست.

۵- 169.254.xx.yy APIPA: هرزمانی که سیستم من با تنظیمات DHCP نتواند از مودم یا سرور یا سوئیچی که سرویس DHCP روی آن فعال است تواند IP بگیرد IP ← APIPA را می گیرد

۶- 127.0.0.1 : Local است (test LoopBack)

دستور Ping: دستوری است در شبکه که یکی از مهم ترین دستورات اشکال یابی و دسترسی به سیستم های دیگر در شبکه می باشد که سه فرمان خروجی آن به شرح زیر می باشد:

Run → CMD (Command Prompt) → Ping IP (مقصد Destination)

مثال: Ping 192.168.125

1- Reply Time: IP: TTL: (Time To Live) طول عمر بسته در میلیثانیه ✓

2- Reply Destination Host Unreachable ✗

PAPCO

Subject:
Date

۳- Request Timed Out ✗

* در این فرمان Packet 4 ارسال میشود (4 Packet Sent) (Recive 4 Packet)
(lost : 0)

برقراره Packet Sent : 4 Recive : 4 Lost : 0

برقرار نیست Sent : 4 Recive : 0 Lost : 4

پروتکل ARP : هرگاه بخواهیم آدرس MAC یک کامپیوتر را از روی آدرس IP آن بدست آوریم از پروتکل ARP استفاده می کنیم برای این کار کامپیوتر فرستنده یک ARP Request تولید کرده و داخل آن پیامی به این مضمون که چه کسی آدرس mac کامپیوتری با این IP را دارد را در شبکه (پخش همگانی) Broad cast می کند یعنی آدرس mac آن را می گذارد تمام کامپیوترهای شبکه این پیام را دریافت کرده و تنها کامپیوتری به آن پاسخ میدهد که صاحب آدرس IP فوق است و گیرنده پیغام ARP Reply تولید می کند و آدرس mac خود را در آن قرار میدهد و آن را به تولید کننده ARP Request ارسال می کند

Subject:
Date

☆ آدرس های دریافت شده از هر کامپیوتر که به صورت ARP می باشد در جدولی به نام MacTable در Switch یا Router ذخیره می شود

پروتکل ICMP (پروتکل مخصوص IP): این پروتکل که برای IP دهی از آن استفاده می کنیم و ساختار کلی آن به شکل زیر میباشد:

check sum	Code	TyPe
Parametrs		
Data		

TyPe: داخل این فیلد یک عدد قرار می گیرد که نوع پیام ارسفن می کند و ساختار فیلدهای پارامتر و دیتا به این فیلد بستگی دارد حتی اگر نوع پیام Destination Host Unrechable باشد

Code: هر نوع پیام ممکن است چند اگزدوه داشته باشد مثلا اگر Host مورد نظر در دسترس نباشد یا کلا آن شبکه غیر قابل دسترس باشد.

check sum: تقریبا مانند IP عمل می کند و بیشتر برای کنترل خطا کاربرد دارد.

Scanned with CamScanner

Subject:
Date

Parametrs: گاهی اوقات در بعضی از پیام ها استفاده می شود و گاه ممکن است هیچ نوع کاربردی نداشته باشد و خالی بماند.

Data: داده ای است که قرار است ارسال شود.

انواع پیام های Icmp:

۱- Destination Host Unreachable: یعنی مقصد غیرقابل دسترس است

۲- Time Exceeded: یعنی در زمان بیت بین شده ی TTL (Time To Live) به مقصد نمیرسد پس دور ریخته میشود و در نتیجه یک پیام Icmp فرستاده میشود

۳- Source Quench: با دریافت این پیام مبدأ یا مسیریاب باید حجم و سرعت ارسال بسته ها را پایین بیاورد.

۴- Redirect: زمانی ارسال میشود که یکی از مسیریاب های شبکه بسته دریافتی اش را مجدد باید به همان مسیریاب یا گره ای که بسته را از آن دریافت کرده است بازگرداند.

نکته: پروتکل Icmp یکی از پروتکل های مدیریتی لایه IP است و در کنار پروتکل IP برای گزارش انواع خطا و ارسال پیام به مبدأ بسته در هنگام بروز مشکلات استفاده میشود. در حقیقت Icmp یک سیستم گزارش خطا است.

PAPCO

Subject:
Date

DHCP: پروتکلی است جهت تخصیص دادن آدرس های IP و سایر تنظیمات شبکه مانند:

IP:

Subnet Mask:

DG:

DNS 1:

DNS 2:

مکانیزم کاری DHCP: ۱- Client در هنگام بوت (Boot) شدن یک پیغام DHCP Discover تولید کرده و آن را در شبکه broad cast می کند (فاز شناسایی تمام DHCP های شبکه) ۲- سپس تمام DHCP Server های شبکه آدرس پیشنهادی خود را درون یک پیام به client ارسال می کند. ۳- Client پس از جمع آوری تمامی پیشنهادها یکی را انتخاب کرده و یک پیام DHCP Request تولید می کند و آدرس را از سرور درخواست می کند جهت اطلاع تمامی سرورها ۴- سروری که کلاینت به آن درخواست داده با دادن یک پیام DHCP Ack به صورت Unicast (پخش تکی) IP را به client تخصیص میدهد در اینجا مراحل تخصیص IP کامل شده است.

۵- کلاینت میتواند با ارسال یک Reply به سرور ارسال Mac Address خود بگوید IP را دریافت کردم و به نشست خاتمه دهد.

Scanned with CamScanner

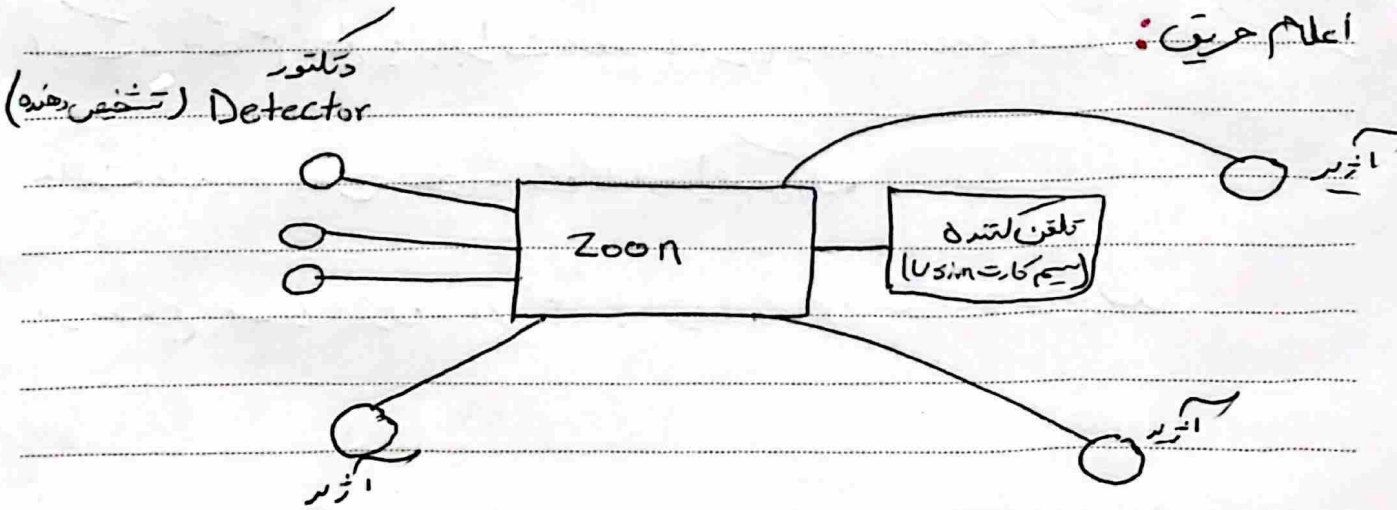
Subject:
Date

Data center: به استاندارد سازی اتاق سرورهای قدیمی و رعایت نکات اصولی استاندارد یک اتاق سرور Data center می گوییم.

استانداردهای Data center: دیواره های کف و سقف پوشیده از مواد نسوز (ePoxy) با تایل های مختلف و ابعاد مختلف به صورت چیدمانی نصب و اجرا میشود که دارای درجه حرارت بالای ۶۷۰° درجه میباشد

۲- درب ضد سرقت و ضد حریق: این درب با فولاد منجم که داخل آن از پشم شیشه فشرده پر شده است نصب و راه اندازی می گردد. روی این در از قسمت بیرون یک دستگیره دیجیتال که هوشمند می باشد نصب می گردد که با رمزنگاری کلیدی و اثر انگشت (Finger Print) و NFC و عنبیه چشم کار میکند.

اعلام حریق:



P4PCO

Subject:
Date

در این سیستم دتکتورها به عنوان سنسور دود و حرارت بر روی سقف یا داخل رک (Rack) راه اندازی میشود و به وسیله ی سیم کشی به دستگاه مرکزی Zoon متصل میشود که این دستگاه نیز به صورت کانال بندی می باشد یعنی می گوییم دستگاه ۴ کاناله، ۸ کاناله، ۱۶ کاناله. از دستگاه Zoon تعدادی آژیر نیز به وسیله ی سیم کشی که در هنگام حریق شروع به آژیر کشیدن کند وصل میشود. یک دستگاه دیگر به نام تلفن کننده نیز در کنار دستگاه Zoon نصب میشود و قابلیت نصب سیم کارت و تعریف کردن چندین شماره تلفن را دارد که در هنگام حریق به این شماره تلفن ها زنگ و پیامک زده میشود.

UPS: سیستم برق دهی به صورت آنلاین و یک منبع تغذیه بدون وقفه و دستگاهی است که هنگام قطع یا تغییرات شدید یا جزئی ولتاژ ورودی امکان ادامه کار در حالت عادی و بدون قطعی را برای کاربر فراهم می کند.

این دو نوع ۱- با باتری داخلی ۲- با باتری خارجی موجود می باشد

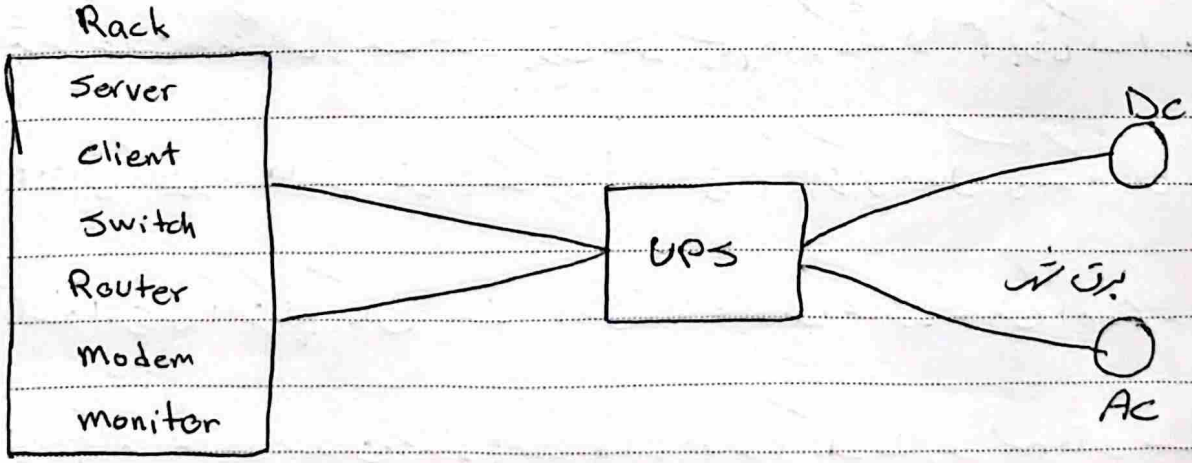
Scanned with CamScanner

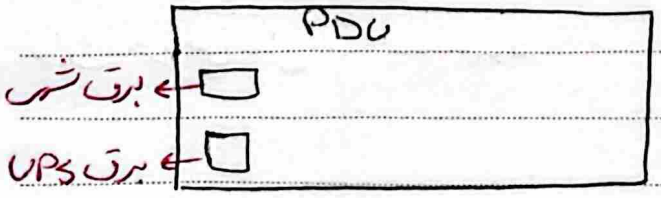
Subject:
Date

طراحی UPS: طراحی UPS به این صورت است که ذخیره برق 220v را طوری در نظر بگیرد که بتواند سیستم ها را از شوک ناگهانی ناشی از قطعی برق محفوظ بدارد و در نتیجه سیستم‌ها و دستگاه ها از خرابی ناشی از قطعی برق و از دست دادن ناگهانی برق شبکه در امان بمانند.

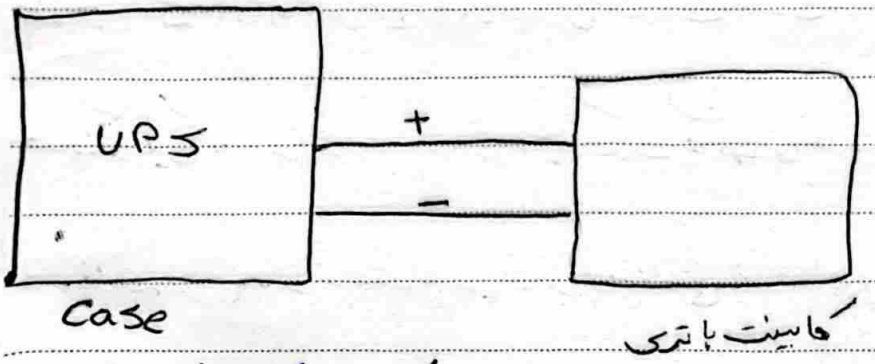
هرچه تعداد باتری ها بیشتر باشد زمان طولانی تری را جهت ذخیره برق به همراه دارد.

به این صورت کار می کند که دائماً به برق شهر وصل می باشد که باتری های خود را شارژ کند زمانی که برق شهر قطع شد UPS میتواند با باتری های خود به مقدار داخل Rack





Subject:
Date



مدل با باتری خارجی آن case اصلی UPS را دارد و در کنار خود یک کابینت باتری جهت گذاشتن باتری های UPS میباشد که این باتری ها را به صورت سری به یکدیگر متصل کرده و یک قطب مثبت و یک منفی را از کابینت باتری به UPS متصل می کنیم. توان باتری ها با توجه به تعداد آن ها تقسیم میشود. مقدار

ژنراتور: دستگاهی است جهت برق دهی سیستم ها و کلیه لوازم برقی که از طریق القای الکترومغناطیسی انرژی مکانیکی را به انرژی الکتریکی تبدیل می کند که این تأمین کننده انرژی الکتریکی ممکن است توربین گاز، توربین بخار، توربین آبی، توربین بادی یا حتی یک موتور دیزل سوز باشد و در دو نوع تک فاز و سه فاز بسته به توان خروجی آن ساخته میشود

Subject:
Date

سیستم اطفاء حریق: به سیستمی که طراحی گردیده است جهت خاموش کردن یا فرونشاندن آتش با سه روش: گاز (FM 200 ، SM 200) و سیستم کشیدن اکسیژن در روش هیبرید (Hybrid) و روش IMC کار می کند در حالت کلی به اقداماتی گفته میشود که با هدف خاموش کردن، کنترل کردن یا هدایت آتش های ناخواسته انجام می گردد.

در حالت کلی آتش سوزی ها در این سیستم به چند کلاس تقسیم میشوند:

کلاس	نوع آتش	مثال	نوع خاموش کننده
class A	مواد جامد	کاغذ، چوب یا پلاستیک	آب، فوم
class B	مایعات قابل اشتعال	بنزین، الکل و نفت	پودر خشک، فوم یا Co_2
class C	گازها	گاز شهری، پروپان	Co_2، پودر خشک
class D	فلزات قابل اشتعال	پتاسیم، منیزیم، سدیم، آلومینیوم	پودر مخصوص اطراف فلزات
class E (K/F)	روغن های آشپزخانه	روغن سرخ کردنی، روغن سویا	خاموش کننده مخصوص مایعات شیمیایی

PAPCO

Subject:
Date

وظایف لایه پیوند داده (Data Link)

کنترل خطا

ایجاد فریم (frame): وظیفه دوم لایه پیوند داده ایجاد فریم است. فریم ها در لایه Data Link از محتویات زیر تشکیل شده اند

type	FSN	ASN	T(x)

نوع فریم را مشخص می‌کند که ۳ ویژگی دارد:

Type: Data: فرستنده به گیرنده ارسال می‌کند

Ack: پاسخ دریافت صحیح که از گیرنده به فرستنده ارسال می‌شود

Nack: پاسخ دریافت غلط که از گیرنده به فرستنده ارسال می‌شود

FSN: در شبکه تمام پیغام هایی که ارسال می‌شوند دارای FSN (شماره فریم ارسالی) هستند. گاهی فرستنده مجبور شود پیام را ۲ یا چند بار ارسال کند برای بار دوم FSN یکی میشود پس میتوان گفت FSN عملا تعداد تکرار از ارسال یک پیام را نشان میدهد

PAPCO

Subject:
Date

ASN: شماره (Ack) ارسالی. وقتی که یک فرستنده یک پیغام را به یک گیرنده میدهد و گیرنده پیام را دریافت کرد ولی با خطا مواجه شد جواب این خطا را داخل پیام ASN ذخیره می کند اما جوابش به گیرنده ارسال نمی شود این اتفاق آنقدر تکرار می شود که ASN جوابش را بشود

نکته: کاربرد ASN و Ack: برای جلوگیری از دریافت پیغام های تکراری و همچنین حفظ ترتیب ارسال و دریافت پیام ها

T(n): مدت زمان ارسال یک پیغام از فرستنده به گیرنده

تشخیص خطا: در لایه DataLink تشخیص خرابی و کنترل خطا وظیفه لایه دوم از مدل OSI می باشد لایه DataLink تشخیص خطاها را با الگوریتم های CRC، Parity، Parity checksum انجام میدهد

وقتی فرستنده یک پیغام را به گیرنده میدهد و گیرنده پیغام را دریافت می کند اگر درست بود که هیچی ولی اگر خطا داشت و قادر به اصلاح خطا بود به فرستنده پیغام میدهد که پیام را درست دریافت نکرده لطفا خطا را برطرف کن و خطا را بده

Subject:
Date

و قادر به اصلاح آن نبود پیغام Nak که سریعا به دریافت پیام خطادار را ارسال می‌کند نسبت به CRC، check sum نیست

اصلاح آن اقدام می‌کند که یکی از راه‌های جلوگیری از خطا که با الگوریتم CRC کار می‌کند فاصله همینگ نام دارد

فاصله همینگ، فاصله رابطه همینگ یعنی تعداد کشف خطا و تعداد اصلاح خطا

فاصله همینگ	تعداد کشف خطا	تعداد اصلاح خطا
d	d-1	(d-1)/2
۳	۲	۱

نکته: اگر در فاصله همینگ بخواهیم یک Bit را اصلاح کنیم باید کاربرد فاصله همینگ را در رابطه‌ی پیدا کردن یک مجهول را بنویسیم که فاصله همینگ با تعداد Bit های ۲ در ارتباط است که ترسول کلی آن به صورت زیر می‌باشد:

$$(m)+(r)+1 \leq 2^r$$

m: تعداد بیت‌های پیام اصلی

r: همان مجهول است و در واقع نشان‌دهنده تعداد بیت‌های اضافه است

2^r: که باید به پیغام فرستنده اضافه شود

مثال:

$M = (\overbrace{10111010}^{M=8}11)$

m در واقع طول رشته است ۸ را از یک میزانیم تا جایی که رابطه درست درباید

$10+(4)+1=15 \leq 2^4=16$

$r=4$

Scanned with CamScanner

Subject:
Date

ماهیت خطا، وقتی که یک پیغام از طرف فرستنده که به صورت M ارسال می‌شود

اما به صورت M' در سمت گیرنده برسد می گوییم خطا رخ داده

M فرستاده ۱۵۱۰۰۱

M' گرفته شده ۱۱۰۰۱

ویژگی های خطا:

۱- یک خطا ناگهانی

۲- خطا انفجاری

۱- وقتی در نهایت یک Bit دچار ایراد و خطا شود که اصلاح آن نیز در همان ابتدا انجام می‌پذیرد می گوییم خطا ناگهانی رخ داده است

۲- اگر یک یا چند بیت پشت سر هم در یک بسته از بین برود می گوییم خطا انفجاری رخ داده است در این گونه خطاها الگوریتم های تشخیص خطا به کار گرفته می‌شود

PAPCO

Subject:
Date

Base band, Broad band: دو روش متفاوت برای انتقال سیگنال هستند که در شبکه های کامپیوتری و مخابراتی استفاده می شوند.

Base band: تنها یک سیگنال داده میتواند در یک زمان انتقال پیدا کند مانند یک راهی که در هر لحظه فقط یک قطار امکان عبور از آن را دارد. این فناوری از داده های دیجیتال در انتقال داده ها استفاده می کند و مقادیر باینری را مستقیماً به عنوان پالس با سطوح مختلف ولتاژ ارسال می کند.

Broad band: سیگنال های داده های متعددی را میتوان هم زمان منتقل کرد مانند بزرگراهی که چندین وسیله نقلیه به طور هم زمان می توانند در آن عبور کنند. فناوری Broad band از سیگنال های آنالوگ در انتقال داده ها استفاده می کند در این فناوری از یک موج آنالوگ مخصوص به نام Carrier wave استفاده می شود. یک Carrier wave هیچ داده ای ندارد اما تمام ویژگی های سیگنال آنالوگ را در خود دارد.

Subject:
Date

ویژگی	Broad band	Base band
نوع سیگنال	آنالوگ	دیجیتال
روش های تقویت سیگنال	تقویت کننده یا آمپلی فایر (Amplifire)	تکرار کننده یا RePeater
تعداد سیگنال	چندین سیگنال به طور همزمان	یک جریان داده در یک زمان
نوع ارتباط	یک طرفه	دو طرفه
پشتیبانی	FDM (فرکانسی)	TDM
کابل مورد استفاده	کواکسیال (Coaxial) و رادیو فیبر نوری	کواکسیال (Coaxial) فیبر نوری، Twisted Pair
کاربردها	شبکه های کابلی و تلفنی	شبکه های محلی Ethernet

Scanned with CamScanner

Subject:
Date

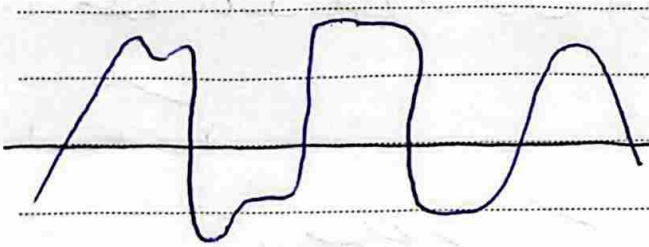
Access Point: دستگاهی است که بتوانی را ایجاد می کند تا دو شبکه به صورت wireless به هم متصل شوند

Modem: مودم یک دستگاه سخت افزاری است که وظیفه اصلی آن تبدیل سیگنال های دیجیتال به آنالوگ و برعکس را برعهده دارد

Analog: از ابتدا هستی وجود داشت هر چیزی که در طبیعت دارای فرکانس باشد در سیستم آنالوگ تعریف می شود مانند نور صدا مغناطیس و ...

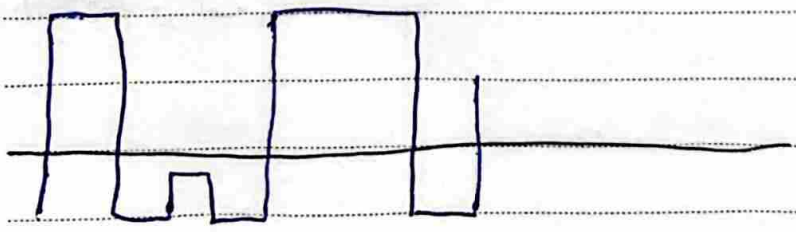
سیستم آنالوگ به طور پیوسته در زمان دارای مقادیر مختلفی است مانند سیگنال برق شهری (220v)

شکل نمونه ای سیستم Analog:



Digital: ساخت بشر است همان امواج آنالوگ است که نمونه برداری شده است اندازه تقریباً دقیقی دارد مثل سامت های دیجیتال امروزی

شکل نمونه ای سیستم Digital:



Scanned with CamScanner

Subject:
Date

تفاوت های سیستم آنالوگ و دیجیتال:

۱- سیستم آنالوگ نویز پذیری بالایی دارد که در دیجیتال اینطور نیست.

۲- پهنای باند دیجیتال بسیار بالاتر از آنالوگ می باشد.

۳- کیفیت بخش صدا و تصویر در دیجیتال بالاتر از آنالوگ می باشد چون در آن سیگنال ها باینری هستند که به آن نیز پالس می گویند.

نکات:

۱- شبکه های امروزی از سیستم دیجیتال استفاده می کنند.

۲- خطوط آنالوگ تلفن از خواص الکتریسیته جهت انتقال و تغییرات صدا بر روی کابل استفاده می کند

۳- برخلاف صدای آنالوگ که از ترکیب سیگنال های الکتریکی برای تعیین شدت صدا استفاده می کند سیگنال های دیجیتال از اعداد برای نشان دادن شدت و سطح صدا استفاده می کند.

Subject:
Date

آنتن های BTS: مجموعه ای از تجهیزات مخابراتی هستند که در شبکه های بی سیم ارتباط مشترک با شبکه را فراهم می کند.

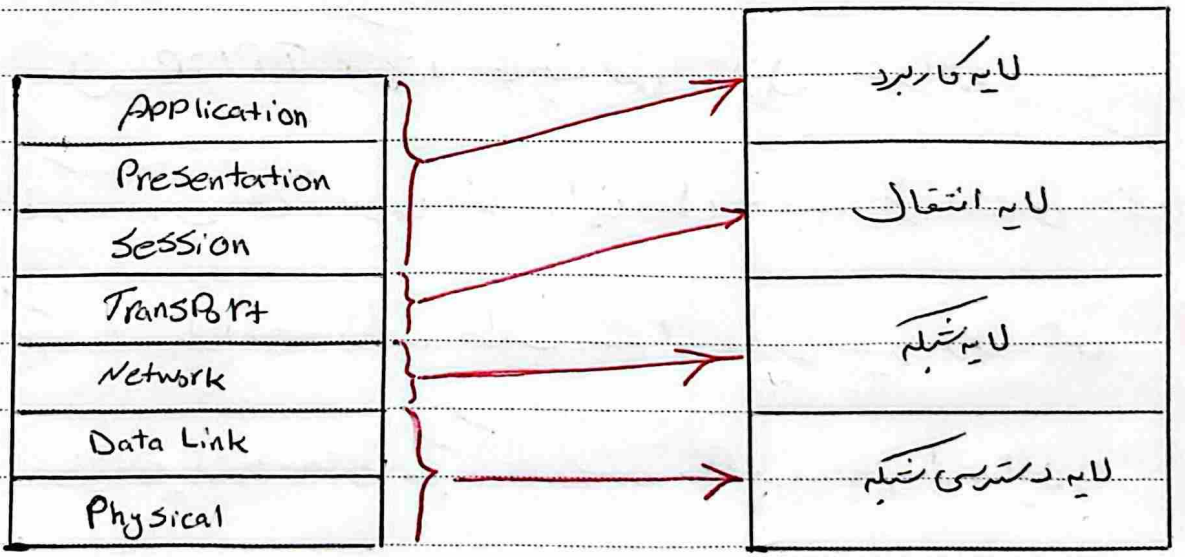
این آنتن ها در مناطقی که سیگنال های مخابراتی ضعیف تری دارند نصب می شوند و به بهبود کیفیت سیگنال های مخابراتی کمک می کنند.

برد مفید این آنتن ها ۲۰km در مناطق شهری و در مناطق مسطح تا ۲۵km نیز می رسد.

Scanned with CamScanner

Subject
Date

مدل TCP/IP: این مدل یک ساختار چهار لایه ای برای ارتباطات گسترده در شبکه و اینترنت فراهم می سازد در لایه TCP/IP یک پشته (Stack) معرفی می گردد که مجموعه ای که شامل بیش از ۱۰۰ پروتکل می باشد برای سازمان دهی کلیه اجزا شبکه اینترنت به کار می رود لایه اول این مدل که لایه دسترسی به شبکه نام دارد تلفیقی از وظایف لایه Physical و Datalink مدل OSI را به نمایش می گذارد لایه دوم آن معادل لایه سوم لایه OSI است و لایه سوم آن نیز همان لایه Transport در مدل OSI می باشد لایه کاربرد آن تلفیقی از لایه ۵، ۶ و ۷ مدل OSI می باشد



Scanned with CamScanner

Subject
Date

لایه دسترسی به شبکه: در این لایه استانداردهای سخت افزار نرم افزارهای راه انداز (Device Driver) و پروتکل های شبکه تعریف می شود این لایه درگیر با مسائل فیزیکی الکتریکی و مخابراتی کانال انتقال نوع کارت شبکه و راه اندازهای لازم برای کارت شبکه می باشد و در شبکه های اینترنت میتواند مجموعه ای از عناصر غیر همگن و نامتشابه را به هم پیوند بزند عام پروتکل های شبکه های LAN و MAN در این لایه قابل استفاده هستند پروتکل های مهمی مثل PPP و SLIP که برای ارسال بسته های اطلاعاتی روی خطوط نقطه به نقطه سریال کاربرد دارد

لایه شبکه: در مدل TCP/IP لایه شبکه وظایف مهمی از قبیل مسیریابی اختصاص IP و آدرس دهی را برعهده دارد در این مدل به بسته های انتقالی در شبکه IP می گوییم که از مبدا تا مقصد وظیفه هدایت بسته از بهترین مسیر برعهده این لایه می باشد برخی از پروتکل های مهم که یک سری وظایف جانبی را در این لایه انجام میدهند عبارتند از پروتکل IGMP, Icmp, RIP, RARP, ARP و Boot P در این لایه فعالیت می کنند

نکته: در این لایه ارتباط بین مبدأ و مقصد از نوع بدون اتصال خواهد بود

Scanned with CamScanner

Subject
Date

نکته: در این لایه مسیریاب ها بایستی از شرایط Topology key و ترانزیتی شبکه اطلاعاتی را کسب نمایند تا بهترین مسیر را برای هر بسته آماده سازند همچنین در این لایه باید اطلاعاتی درباره مشکلات یا خطاهای احتمالی در ساختار زیر شبکه بین مسیریاب ها و ماشین‌های میزبان مبادله شود

لایه انتقال: این لایه ارتباط ماشین های انتهایی (ماشین های میزبان) در شبکه برقرار می کند یعنی میتواند براساس سرویسی که لایه دوم ارائه می کند ارتباط اتصال گرا و مطمئن برقرار کند البته در این لایه برای عملیاتی نظیر ارسال صوت و تصویر که سرعت مهم تر از دقت و خطا است سرویس بدون اتصال سریع و نامطمئن نیز فراهم گردیده است

لایه کاربرد: در این لایه براساس خدمات لایه های زیرین سرویس سطح بالایی برای خلق برنامه های کاربردی ویژه و پیچیده ارائه می شود این خدمات در قالب پروتکل های استانداردی همانند موارد زیر به کاربر ارائه می شود:

۱- شبیه سازی ترمینال (مثل سرویس Telnet) (پورت ۲۳)

۲- انتقال فایل یا FTP (پورت ۲۰,۲۱)

Scanned with CamScanner

Subject
Date

۳- مدیریت پست الکترونیکی

۴- خدمات انتقال صفحات اینترنتی

روش های انتقال Data در انواع شبکه ها:

۱- Simplex: ارسال دیتا در این روش به صورت کاملاً یک طرفه است مثل تلویزیون رادیو کانال های ماهواره.

۲- Half Duplex: ارسال و دریافت دو طرفه غیرهم زمان مثل بی سیم ها، واکی تاکی ها

۴- Full Duplex: ارسال و دریافت دو طرفه به صورت هم زمان مثل تلفن، موبایل و شبکه های کامپیوتری.