

۱/۶
موسسه تخصصی (Network +) CompTIA

☑️ (موسسه تخصصی)

☉ MCTP EA

☉ MCSA 2008, 2012

☉ MCP

☉ MCTS

☉ CCNA R8S

☉ CCNP

- MCP members (Society)

Server : کامپیوتری است از لحاظ سخت افزار ای قدرتمند تر از سایرین بوده و

افزون داشته می باشد و می تواند خدماتی مختلف بدهد مانند webservice

File service, Mail service, VPN Service

رایج است

Client : کامپیوتری است که می تواند توسط کاربران شبکه استفاده

شوند و این انجام امور روزمره کاربران شبکه می کند

Data : بهترین انتخاب Data می باشد

Media : به طبع تجهیزات سخت افزار می باشد

Protocol : زبان مشترک اجزای شبکه است در واقع کاری هر دو

قواعد رفتاری می باشد که سیستم از آن برای برقراری ارتباط و تبادل

اطلاعات استفاده می کنند

تعریف شبکه: گروهی توصیف شده‌ی حداقل دو کامپیوتر است که هم

ارتباط داشته باشند و بتوانند منابعی مانند اطلاعات، نرم افزار، سخت افزار

اشتراک کنند. به همین منظور اینها را "شبکه" می‌نامند.

انواع شبکه از نظر فیزیکی، منطقی =

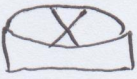
Local Area Network (LAN): به شبکه‌ای که در محدوده‌ی کوچک

LAN می‌گویند.

نمونه‌های رایج شبکه =

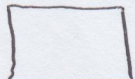
Hub : 


LAN : 

Router : 

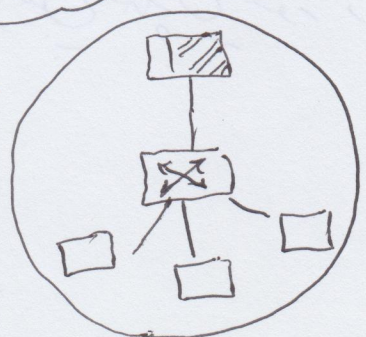
Server : 

Cable : 

Client : 

Internet : 

Switch : 

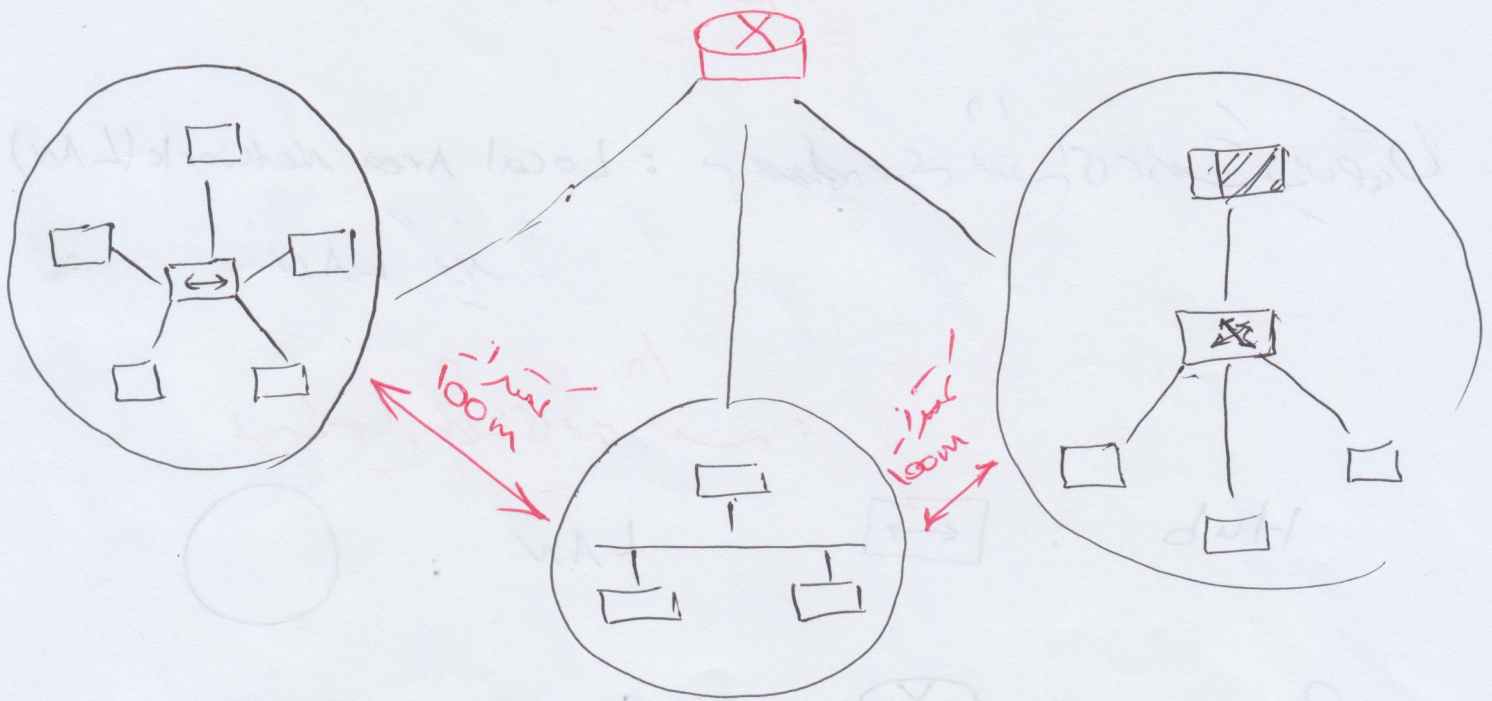


Campus Area Network (CAN) : منطقه چندان وسیع نیست

در باطن آن چند سرور قرار دارد و به یکدیگر متصل است و از یک سرور LAN

مخزن داده دارد و به این ترتیب ترافیک در آن به گردش در می آید

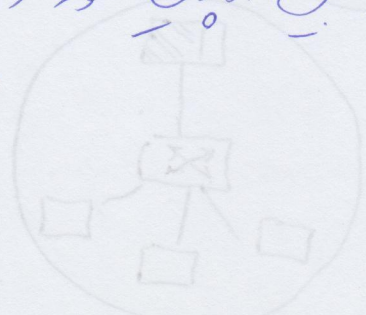
شبکه اصلی یک CAN خواهد بود



Metropolitan Area Network (MAN) : تلف فون منطقه وسیع است 100 km

Wide Area Network (WAN) : یک منطقه جغرافیایی وسیع است

چندین سرور و شبکه در آن قرار دارد و به یکدیگر متصل است



تقسیم بندی شبکه از نظر نرم افزاری :

Peers - to Peer (workgroup) : به سبب این گفته می شود که مدیرین این صورت

کنند مدیریت همزمانی که مدیر شبکه کوچک تغییراتی در سیستمها را به سبب
سایرند که سیستمی برای تک تک سیستمها ضرورت پیدا کرده و تنظیمات
مربوطه را انجام دهد.

Client - Server (Domain Model) : در این سبب مانند مدیرین

صورت کارها متمرکز می باشد و کل کار مدیرین شبکه از روی یک سرور مرکزی
انجام می شود.

کودکی مشخص Workgroup و Domain مدل بودن

Right click on my computer → This PC →

→ - compute name, domain and workgroup setting

Unmanagable Switches : تنظیم کنیوت غیر قابل تنظیم

Managable Switches : تنظیمات کنیوت قابل تنظیم

نوعه‌های سوئچ ۲ : Unmanagable , Managable

وجود پورت Port (پورت سوئچ) پورت های Console , mgmt , ...

متغیر ریزنده‌های مختلف برای اتصال سیستم ، کاربرد های آن و غیره

تعمیرات

Routers : روترها ، شبکه های گسترده

! کاربرد WAN , MAN

Network Interface Card : شبکه های گسترده

کاربرد روترها در شبکه های گسترده

استفاده از کارت شبکه در شبکه های گسترده

نقاط : Switch , Hub

Switch ها فقط ارسال می کنند و اطلاعات را از Source به Destination ارسال می کنند اما Hub ها با ارسال Broadcast از همه سیستم های شبکه اطلاعات را برای تمام سیستم ها ارسال می کنند Broadcast و در نتیجه Signal اطلاعات به همه سیستم ها

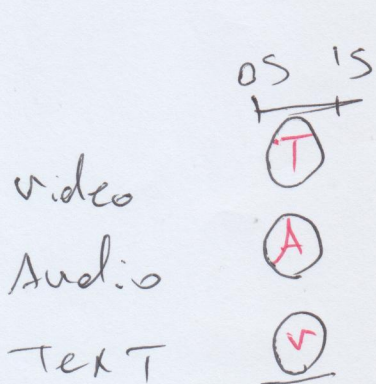
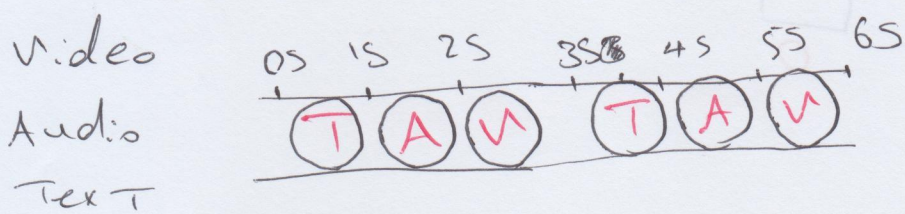
نقطه بندی سرعتی ارتباط : در دنیای ارتباطات از نظر نحوه ارسال

در نتیجه Signal در انواع سرعتی Baseband و

Broadband سرعت را در یک خط می دهد اما در دنیای ما هم داریم

Baseband : در هر خطی می توانیم در یک باند فرکانسی تنها یک نوع سیگنال

ارسال می کنیم و انتقال می دهیم و این انتقال سیگنال هم نوع دیگر خطی را ندارند

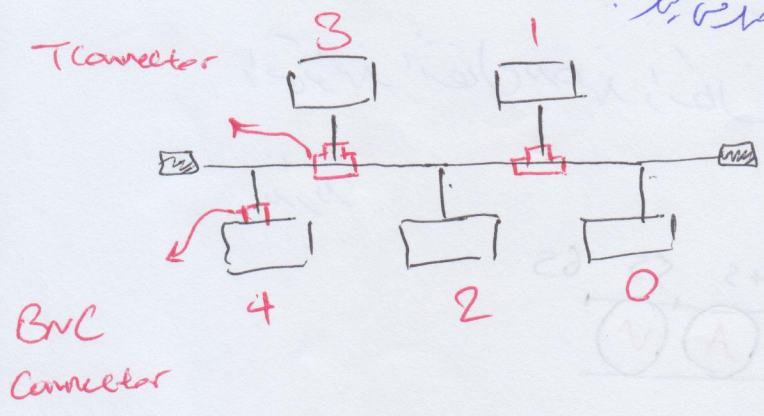


Broadband : به سرعتی گفته می شود که در یک باند فرکانسی می توانیم در یک خط انتقال می دهیم و این انتقال سیگنال هم نوع دیگر خطی را ندارند

Topology : وضع و تقسیم شبکه است که نحوه انتقال و توزیع داده را مربوط به مشخص می کند

انواع Topology : Bus - Star - Token ring - Hybrid - Mesh

توپولوژی (Bus) : توپولوژی خطی قدیمی در کم کاربرد است به دلیل آن تمام کامپیوترهای شبکه از مسیر یک خط اصلی که در یک نقطه مشخص شده است بهم متصل می شوند هر چقدری که کامپیوتری تعداد سیل داشته باشد بیشتر احتمال دارد که در آن خط یا این اصل فاصله از مرکز و علاء الحضور تمام کامپیوترهای به دسترس قرار ندهد و محدودیت



V A T V A T

T
A
V

9

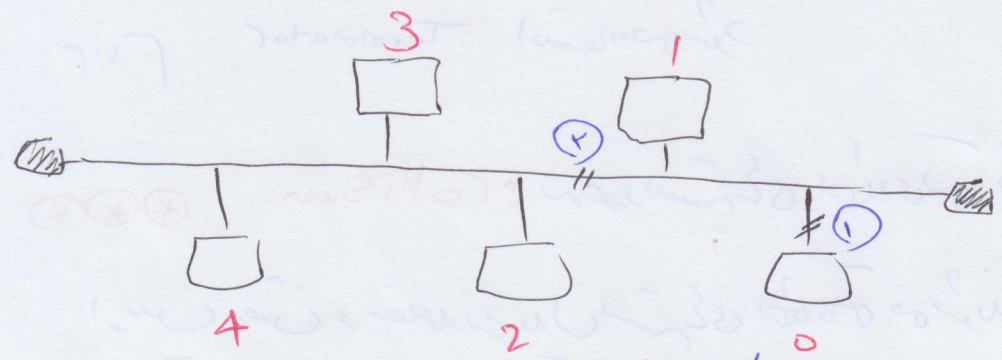
کابل توپولوژی Bus از نوع کابل Coaxial دو سیمه

Connector ها :

BNC (RG 58) ها : اتصال کابل به کابل

T Connector : برای اتصال کابل به سیمت متصل شده (مثل شبکه)

Failure ها :



- ① : قطعی سیم - Failed می شود
- ② : توپولوژی به Failed می شود

استانداردهای Bus :

(Thinnet) 10 Base 2 (1)

(Thick net) 10 Base 5 (2)

Baseband

<p>10 Base 5</p> <p>↓</p> <p>5x100 = 500m</p>	<p>↑</p> <p>10 Base 2</p> <p>↓</p> <p>Speed [mb/s]</p> <p>x100 = 200m</p> <p>185m</p> <p>(حد اکثر سیم کشی)</p>
---	--

Atenuation : پدیده افت سیگنال

⊗ ⊗ ⊗

10

Tranciever Base 5

Base 2

Tranciever Base 2

Signal Bouncing

Terminator

Terminator

Collision

Collision

Collision

Carrier Sense Multiple Access with Collision Detection

Carrier Sense Multiple Access with Collision Detection

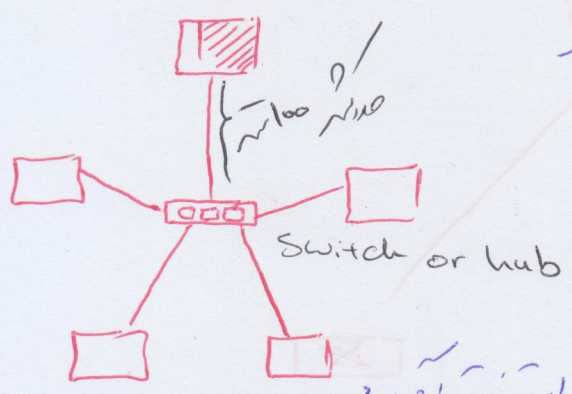
Source Destination

Signal Bouncing

Terminator

تولودوی Star: تعداد کم در خط درین

تولودوی کسب جوسوند

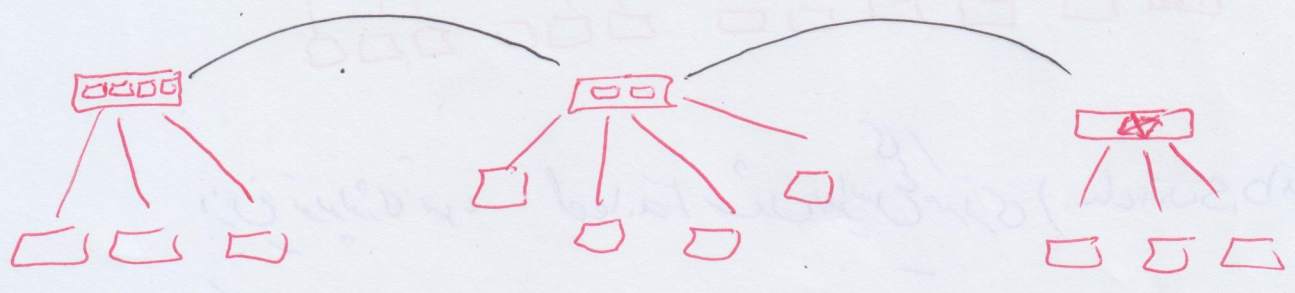


انواع تولودوی Star:

1) Star: تعداد کم سوچ جوسوند

2) Cascade Star: سترایک سوچ جوسوند

(A) اتصال صورت گیری کسب برای تعدادی عدد سوچ جوسوند:

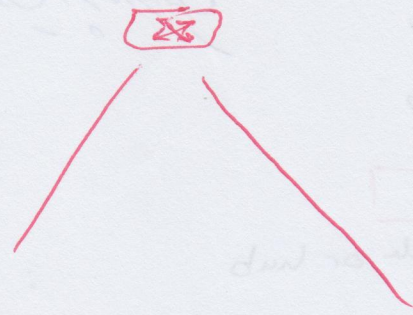


(B) مدل سوچ جوسوند Cisco:

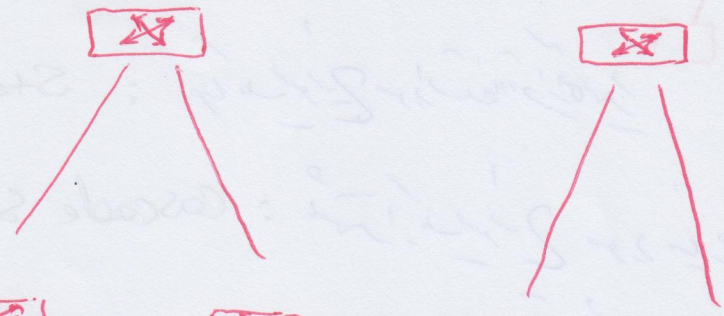
دایره سه لایه Access به با سه لایه Distribution (سه لایه ۲)، لایه Core

محل جوسوند . لایه Distribution (سه لایه ۲)، لایه Core

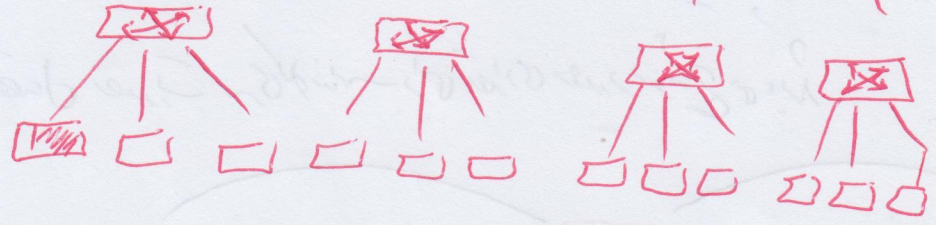
Core :



Distribution :



Access :



داین توپولوژی نہی، Failed سٹن انوائس عمیری (Hub, Switch) کی
 کل سسٹم Failed ہوئو

نہی، نہی* توپولوژی Star :

- نہی:
- (1) ٹریبل شوٹنگ (Trouble Shooting) نہی
- (2) کولیشن (Collision) نہی
- (3) توپولوژی نہی

بسیار

۱) از باقی مانده سیستم با این تکنیک می توان به یک مرکز (Switch, Hub) متصل کرد

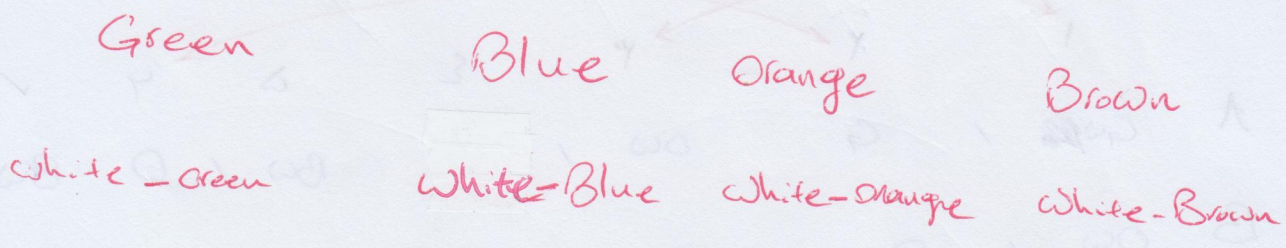
۲) هزینه کمتر (بدون نیاز به کابل شبکه و سوزن است)

کابل توپولوژی Star :

Twisted Pair

کابل مورد استفاده در این توپولوژی از نوع

ستاره است که در آن یک سر به همه



انواع Twisted Pair از نظر ظاهری :

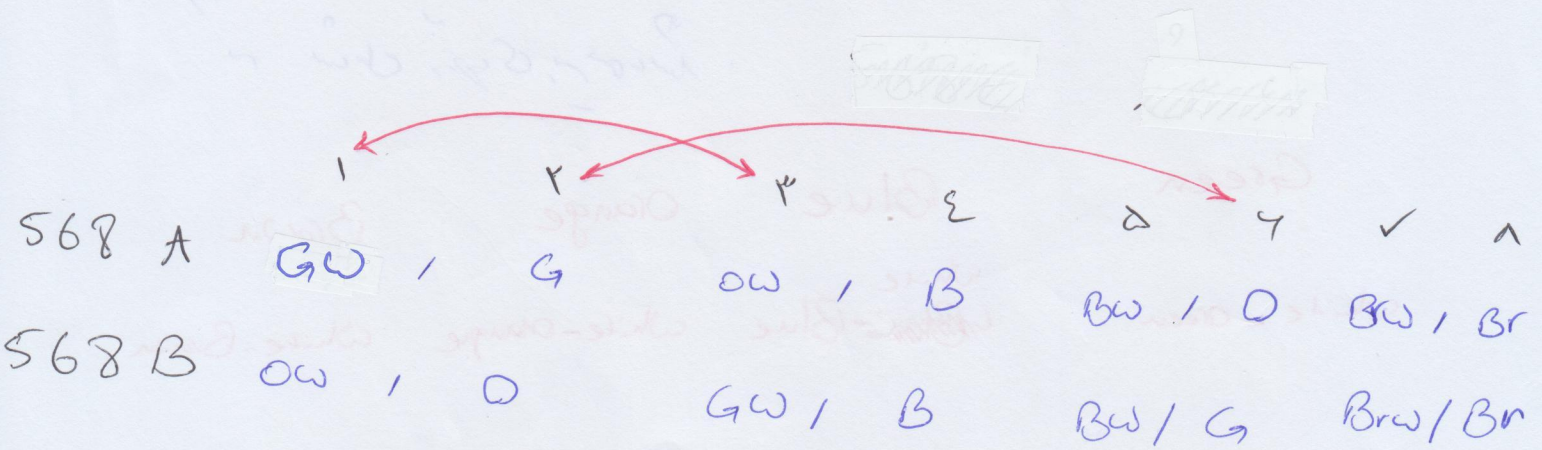
(Unshielded Twisted Pair) UTP * (۱)

(Shielded Twisted Pair) STP (۲)

* نوع سوکت به رایج ترین نوع کابل استفاده از سوکت RJ45 استفاده می شود

تربندی سوئیچی Twisted Pair

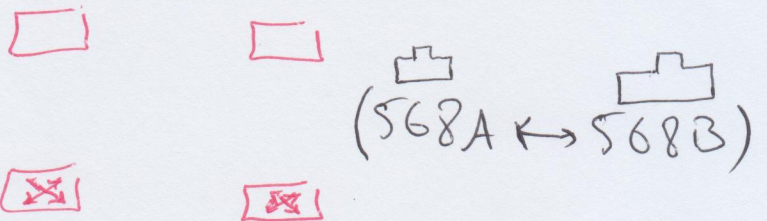
568 A ۱) روغن
 568 B ۲) روغن



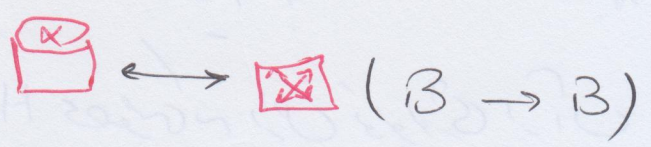
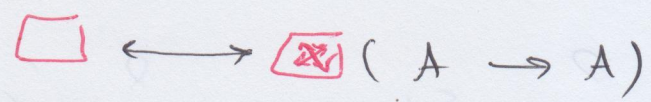
کلمه استاندارد سوئیچینگ استاندارد IEEE تعین می شود

نوع تربندی سوئیچی : بستن اتصال در روغن از نوع سوئیچ

Cross :



Straight :



Twisted Pair سیم‌های سیم‌چین

100m : Cat 1 : 1 mb/s : قوت انتقال داده در صورت نیاز کمتر است

100m : Cat 2 : 4 mb/s : قوت انتقال داده در صورت نیاز کمتر است

100m : Cat 3 : 10 mb/s : قوت انتقال داده در صورت نیاز کمتر است

10BaseT Twisted Pair

100m : Cat 4 : 16 mb/s : قوت انتقال داده در صورت نیاز کمتر است

100m : Cat 5 : 100 mb/s : قوت انتقال داده در صورت نیاز کمتر است

55m : Cat 5e : 1000 mb/s : قوت انتقال داده در صورت نیاز کمتر است

works Cat 5 wire

100m : Cat 6 : 1 Gb/s : قوت انتقال داده در صورت نیاز کمتر است

100m : Cat 6+ (6a) : 10 Gb/s : قوت انتقال داده در صورت نیاز کمتر است

works

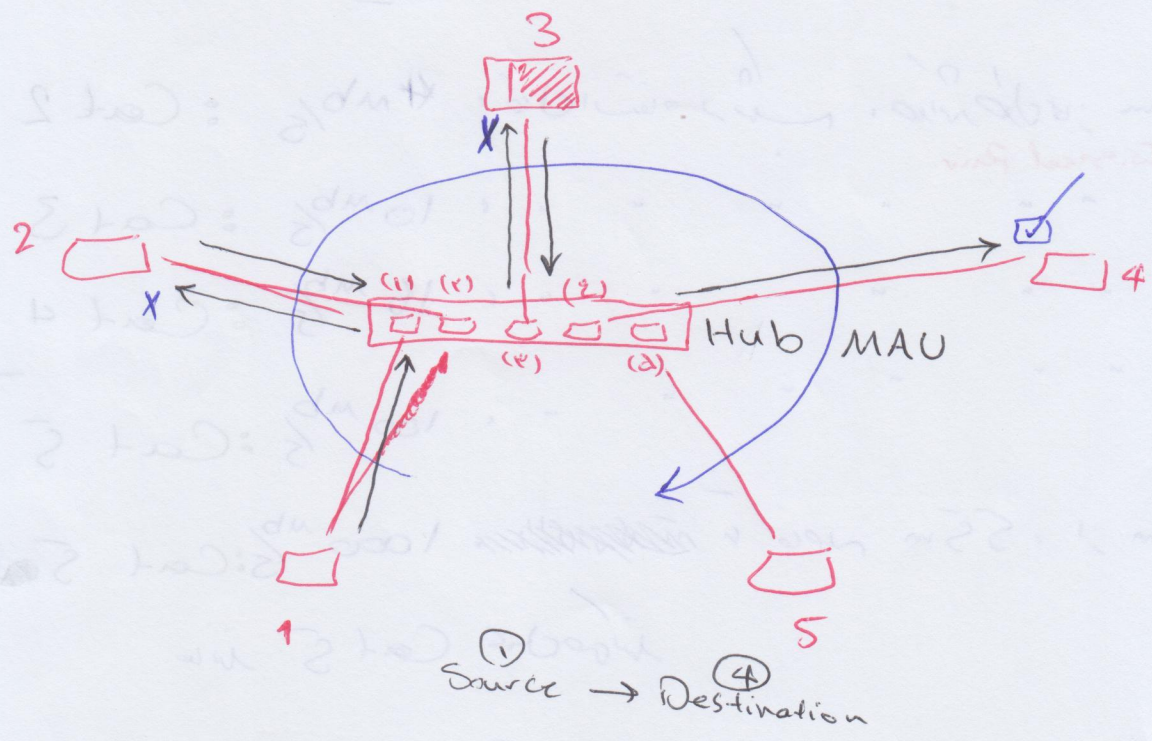
100m : Cat 7 : 10 Gb/s : قوت انتقال داده در صورت نیاز کمتر است

سیم‌های سیم‌چین (Cat 6 و Cat 5)

- 10mb/s ← Ethernet
- 100mb/s ← Fast Ethernet
- 1Gb/s ← Gigabite Ethernet

توپولوژی Token Ring :

این فنیکال این توپولوژی صد است
 این فنیکال این توپولوژی صد است
 استفاده صورت (Hub MAU) یک صورت زنده ای شکل ارسال
 داده، اطلاعات از سر بردن گونه ای شکل، ارسال
 بسته به هر عدد



Failure :

اگر سیستم (Client) هر استند کل است این خط و در
 که با کلین سیستم از پورت Hub MAU این مقدار است

توقف Token :

یک سیستم یا Frame است که در این توپولوژی از آن برای ارسال

اطلاعات استفاده می شود. این سیستم یک Token را میگیرد و در حال

گردش است. در هر کامیونیتی تعداد ارسال Data را مشخص میکند

و در این سیستم Token آن را متوقف کرده و سیستمی اصلی می

باشد که خود از آن استفاده می کند و آن اضافه می کند سپس Token

به یک خود از آن استفاده می کند تا به سیستم مقدار میدهد

در این توپولوژی دلیل وجود یک Token (Frame) دیگر

Collision به هیچ وجه اتفاق نمی افتد. این تنها توپولوژی است

که بدون Collision در آن اتفاق نمی افتد.

توپولوژی Mesh :

این توپولوژی در شبکه LAN کاربرد دارد و بیشتر در شبکه های

WAN از آن استفاده می شود. با استفاده از این توپولوژی بین

محلین Location بین Link (ارتباط) ایجاد می کنیم

تا در صورت Failed شدن یکی از Link ها ارتباط با آن

برقرار باشد. در صورتی که در Mesh یک توپولوژی از آن می باشد

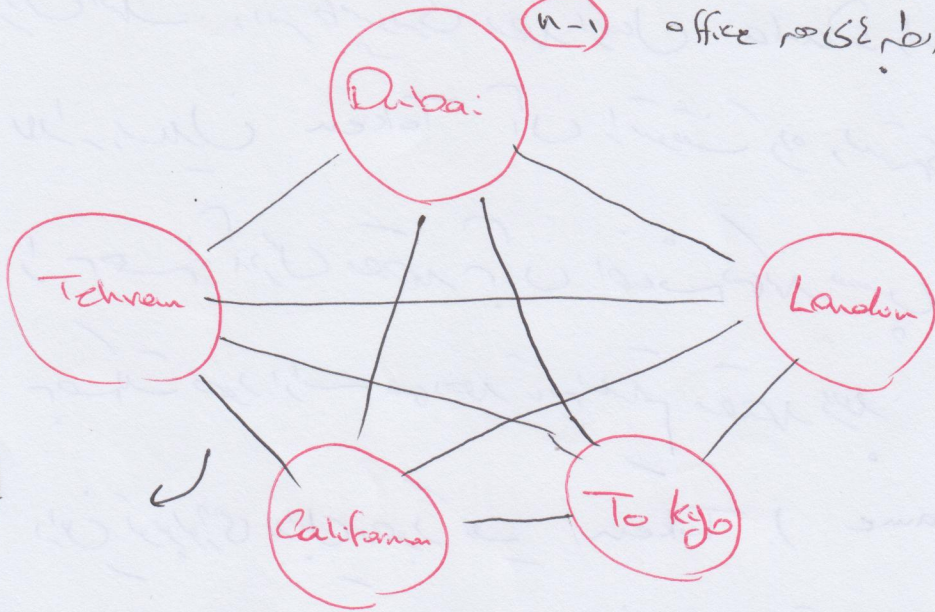
نشان دادن نحوه راه اندازی Back up Link های شبکه

WAN استفاده می شود

تعداد کل شبکه
مردمان

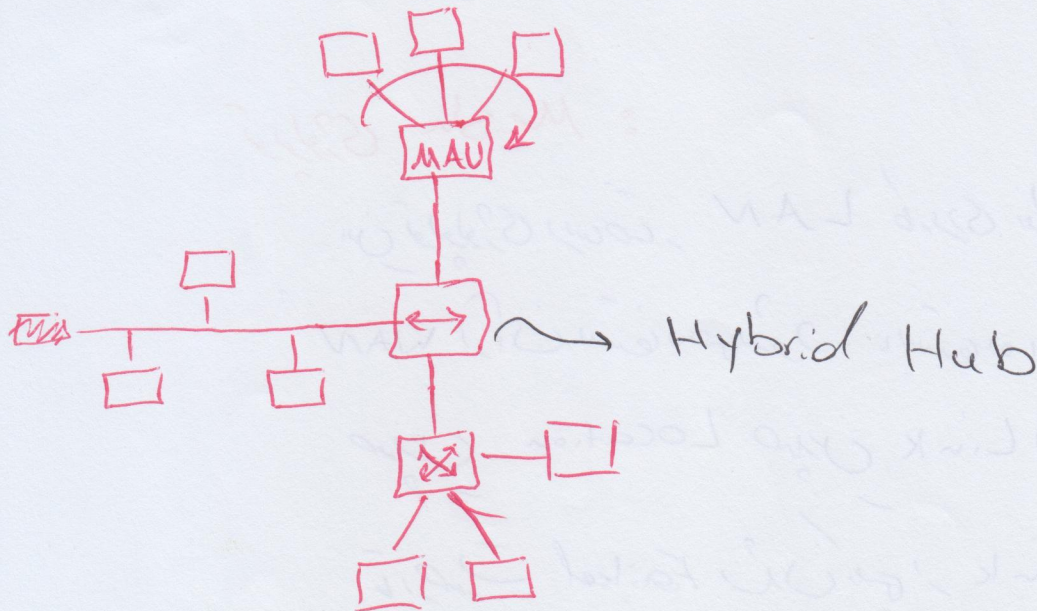
$$= \frac{n(n-1)}{2}$$

تعداد استفاده office n
تعداد راه های به office n-1



Reliability

توپولوژی Hybrid: ترکیبی از هر دو توپولوژی Hybrid



تعریف Backbone, Segment :

Segment: هرین طبقه است که از آن برای انتقال Client ها
استفاده می شود

Backbone: هرین طبقه است که Server ها از آن استفاده می کنند

Switch ها به کمک آن انتقال می دهند (Load ها، ترافیک ها)

انواع Hub :

Passive Hub: هر دو طرف برای انتقال به یکدیگر استفاده می کنند

Source و Destination هر دو طرف در یک لاین

Active Hub: به یک منبع برای انتقال به هر دو طرف

Source و Destination هر دو طرف در یک لاین

Hybrid Hub: یک نوع خاص از Active Hub است که در آن

از آن برای انتقال به یک طرف و به هم استفاده می کنند

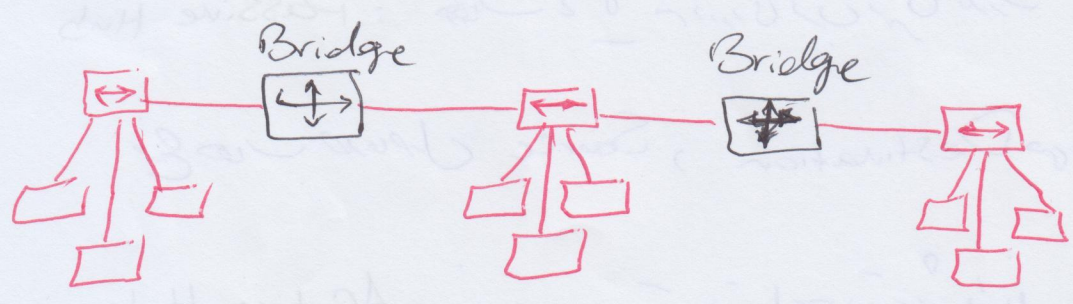
Repeater: هر دو طرف در یک لاین Bus

از آن برای انتقال به یک طرف و به هم استفاده می کنند

Switch ها از آن استفاده می کنند و Repeater ها از آن استفاده می کنند

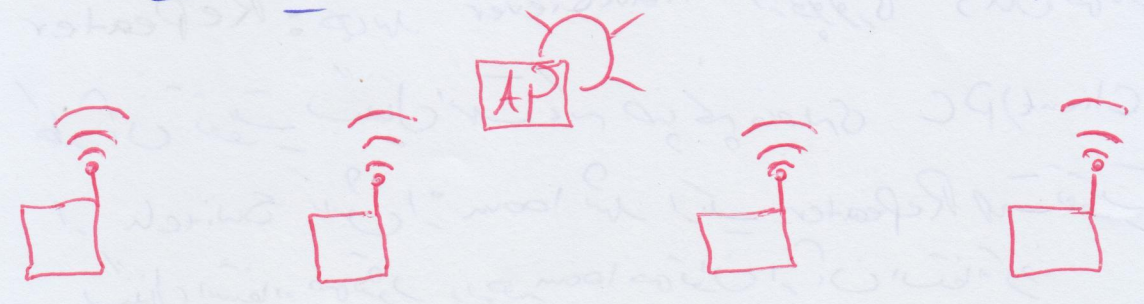
Bridge : از این دستگاه برای اتصال چندین Hub به یکدیگر استفاده

میکنیم زیرا که هر آن هم بخشی است که جدا در حالت بسته ای اصلی است از یک Hub نیز یعنی آن را به Hub های مختلف میزنند و بسته متعلق به کامپیوترهای مختلف Hub میزند و بسته در این شبکه گسترش پیدا میکند و بسته در این شبکه گسترش پیدا میکند و بسته در این شبکه گسترش پیدا میکند



WAP (Wireless Access Point) : این دستگاه مرکزی است که به Hub

دارد و در شبکه های Wireless از آن برای اتصال سیستم به یکدیگر استفاده می شود. این تفاوت که برای ارتباط با Access Point استفاده می شود، ارتباط به هم به هم برقرار می شود. تنها به وسیله ارتباط کامپیوتری به اتصال Access Point می توان به هم وصل شدن دارند



Wireless

Service Set Identifier (SSID)

Preshare key

wireless range

wireless rate

Range

Rate و Range بین بیس * فرکانس و پهنای باند

Access Point : Range

Rate

wireless

Speed : کارایی و پهنای باند

استاندارد های wireless : استانداردهای wireless

۸۰۲.۱۱ استاندارد

(11)

(Fast / Short range) 802.11a

54 mb/s

5 GHz

(Slow / Average) 802.11b

11 mb/s

(Fast / low) 802.11g

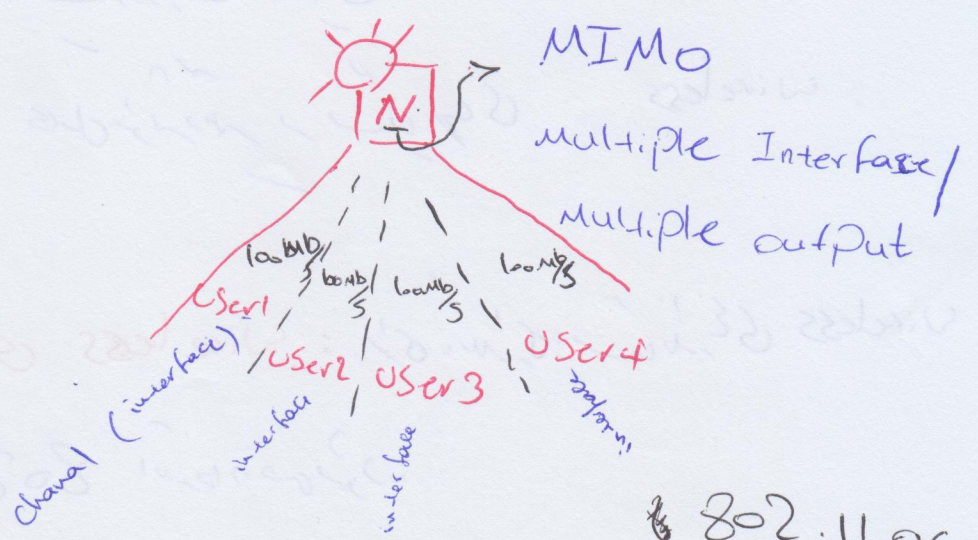
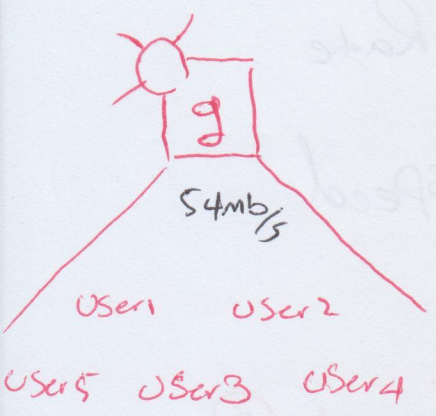
54 mb/s

2.4 GHz

(Fast / Short & low) 802.11n

100-600 Mb/s

2.4 & 5 GHz



interface 4 (Fast / Short or low)

433 mb/s

2.4 or 5

SSID Broadcast (4) : این قابلیت را می توان در تنظیمات شبکه بی سیم خود غیرفعال کرد تا شبکه شما را از دید دیگران مخفی نگه دارید.

این قابلیت می تواند به عنوان یک روش امنیتی اضافی استفاده شود. اگرچه این قابلیت به تنهایی برای امنیت کامل شبکه کافی نیست.

SSID Broadcast

MAC Filtering

- Black list
- White list

MAC Filtering

Name	MAC Address
my Smartphone	- - - - -
my Laptop	- - - - -

White list : این لیست فقط دستگاه های مجاز را به شبکه اجازه دسترسی می دهد.

Black list : این لیست دستگاه های غیر مجاز را از شبکه حذف می کند.

WEP (Wireless Equivalent Protection)

Pre shared key : این کلید را باید در هر دو طرف شبکه به اشتراک گذاشت.

Encryption : فرآیند رمزنگاری داده ها برای جلوگیری از دسترسی غیر مجاز.

Encryption

a ADSL : امکان استفاده از تلفن اینترنت سرعت کمین

سرعت Download بیشتر از سرعت Upload میباشد

b SDSL : عدم امکان استفاده از تلفن اینترنت سرعت کمین

c VDSL : ۱۵-۵۵ mb/s سرعت

d Satellite : از همه آهسته تر امکان دسترسی به اینترنت بسیار در کف

با استفاده از ارتباطات دیجیتال محفوظه های مهم میزند این فناوری بسیار زیست است.

e Wireless : این روش همسایگان و دستگاه های قابل حمل (Portable)

لین Smart Phone ها Tablet ها Laptop ها

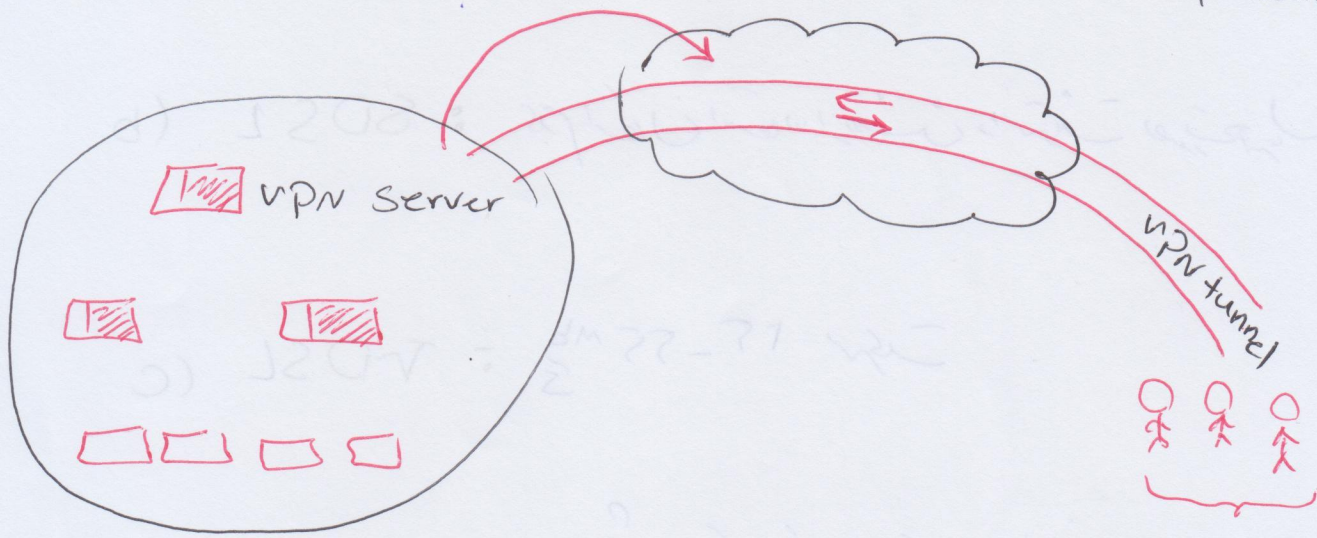
مهاکت امکان دسترسی اینترنت از هر جگه در دنیا نیز امکان پذیر هست
این آرد به هم میزند

۱ share : بهریت و امکان دانلود، آپلود میفرم - دلیل استفاده محدودتر

۲ dedicated : دانلود، آپلود میفرم و بهریت و بهریت میزند
مشخص شده تخصیص خود متعصب میباشد

رشته VAN - فناوری:

VPN (Virtual Private Network): یک تکنولوژی است که امکان برقراری دور



برقراری VPN:

- PPTP: قدیمی ترین پروتکل - مناسب برای موبایل - امنیت پایین و سرعت خوب
- L2TP: امنیت بالا و سرعت خوب
- IPsec: امنیت بالا و سرعت خوب

L2TP: امنیت خوب - مناسب برای موبایل و اینترنت، امنیت بالا و سرعت خوب

در این VPN Server یک سرور IPsec هست با این امنیت بسیار قوی

سرعت خوب، امنیت بالا، بیت بیت امنیت بسیار بالا

سرور IPsec نیاز به دانش فنی بالا دارد

SSTP: جدیدترین و قویترین و امنترین پروتکل

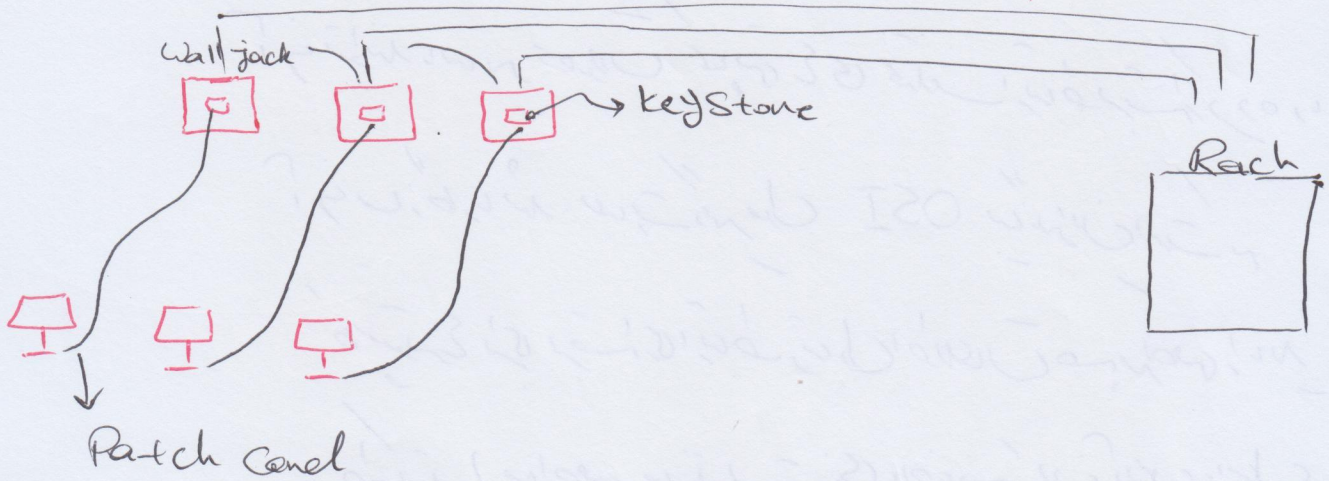
در این نوع پروتکل نیاز به سرور توسط CA هست

در این سرور توسط Certificate هست، هر کسی که می‌خواهد

بازرسی

- اینجیل Point to Point (سویچ بود مستقماً دارد و ریسک بالایی دارد)
- طرح Access Point, خودنژاد

تجهیزات لازم است: راه اندازی کابینت



Patch Panel :

تعداد کمی کابل در ردیف ۲ Rack در کابینت مستقماً به سوئیچ اختصاص داده می شود و در ردیف ۱، کابل که به کابینت وصل است Port های سوئیچ هستند. استفاده از Patch Panel این امکان را فراهم می کند که کابل های داخل کابینت به صورت منظم تر و صورت بهتری در کابینت قرار داده شود. Port های سوئیچ را می توان داخل کابینت قرار داد.

1	Physical
2	Data Link
3	Network
4	Transport
5	Application

مدل OSI (Open System Interconnection)

بطور کلی این مدل برای استاندارد سازی و برقراری ارتباط بین سیستم‌های

مختلف است. این مدل به گونه‌ای طراحی شده است که بتواند ارتباطات بین سیستم‌های مختلف

را برقرار کند و همچنین به عنوان یک راهنما برای طراحی سیستم‌های ارتباطی

است. این مدل به گونه‌ای طراحی شده است که بتواند ارتباطات بین سیستم‌های مختلف

را برقرار کند. این مدل به گونه‌ای طراحی شده است که بتواند ارتباطات بین سیستم‌های مختلف

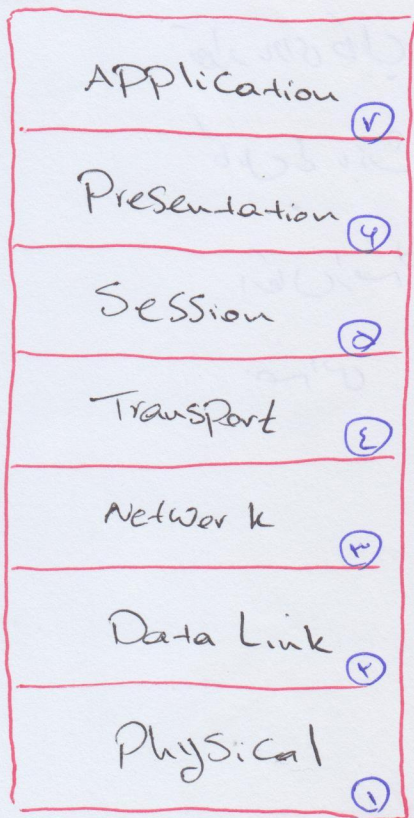
را برقرار کند. این مدل به گونه‌ای طراحی شده است که بتواند ارتباطات بین سیستم‌های مختلف

را برقرار کند. این مدل به گونه‌ای طراحی شده است که بتواند ارتباطات بین سیستم‌های مختلف

صورت می‌گیرد...

All People Seem to need Data

Processing



Encapsulation

اگر کاربری قصد ارسال دیتای را داشته باشد، دیتای اصلی آن را با دیتای

لایه (Application) شروع به صحبت کرده و بگوید از چه لایه ای

بگیرم یا دیتای خاصی به آن اضافه می شود تا اینکه بسته به دیتای

فیزیکی ارسال شده، داده آماده ارسال از طریق Media می شود. این

راستن Encapsulation گویند.

Decapsulation

بعد از اینکه بسته به مقصد رسید صورت عکس را با بین گرفتن بسته شروع

به صحبت کرده و بگوید از چه لایه ای بگیرم یا دیتای خاصی از آن کم می شود

تا اینکه بسته به لایه Application به دست کاربر برسد

لایحه Physical

Physical : این لایحه تأثیری در محتوای بسته‌های اطلاعاتی ندارد

فقط وظیفه انتقال اطلاعات را بر عهده دارد و هیچ تغییری در محتوا ایجاد نمی‌کند

(bit) : کوچک‌ترین واحد اطلاعاتی است که در این لایحه انتقال می‌دهد

در این لایحه هیچ تغییری در این داده‌ها ایجاد نمی‌شود. فقط وظیفه ارسال و دریافت داده‌ها را بر عهده دارد. در این لایحه هیچ تغییری در این داده‌ها ایجاد نمی‌شود.

لایحه Data Link

Data Link : وظیفه این لایحه

Physical Network : انتقال بسته‌های اطلاعاتی از طریق

Physical : انتقال و مدیریت داده‌ها در سطح

این لایحه وظیفه ای است که در Sublayer (زیر لایحه) می‌باشد تا از تأثیرات فیزیکی خود استنباط کند

Physical Link = Physical Link

LLC (Logical Link Control)

MAC (Media Access Control)

وظیفہ LLC :

1) فریم کے ساتھ ساتھ Frame

2) Media Collision اور Error سے نمٹنا

3) فریم کی دوبارہ بھیجنا

4) فریم کی رفتار اور سائز کا کنٹرول

Physical Address = MAC Address = MAC کا پتہ

1) کسی بھی نیٹ ورک میں کسی بھی نیٹ ورک پر کسی بھی نیٹ ورک پر

MAC Address کا پتہ

MAC Address کی شکل

Decimal	Binary	Hexa Decimal
0	0	0
...	...	9
1	1	A
...	...	f
9	2	f
10	2 بیٹے Base 2	16
↓	Base 2	16 بیٹے Base 16
10 بیٹے Base 10		

Decimal: 486
 Binary: 111110110
 Hexa Decimal: 313F

MAC آدرس 12 رقم ذاتیوع Hexa Desimal میں

13-6A-D1-BB-0b-DC

MAC Address سے

IP Config / all

12 x 4b = 48b = 6B

get mac: MAC آدرس

13-6A-D1-BB-0b-DC

OUI

NIC

Organizational Unit ID

Network Interface Control

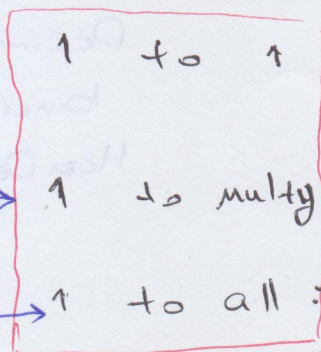
OUI سے

Frame MAC، ڈیٹا فریم، اتصال سے

Data Link سے

Switch, Bridge

یہ ہے کہ یہ ہے



Unicast: ایک سے ایک

Multicast: ایک سے کئی

Broadcast: ایک سے سب

یہ ہے کہ یہ ہے

Switch →

Hub →

پروتکل های قدیمی لایه ۱ Data Link:

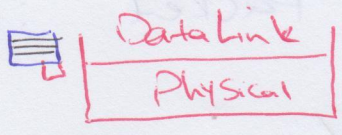
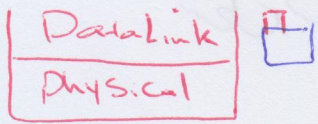
SLIP: این پروتکل هنگام عبور بسته های اصلی از لایه ۱

Data Link که فایل ۱۸ (بسته) را به لایه ۱ آن اضافه

می کند، علاوه بر آن بسته ها تعداد بسته ها را نیز مشخص از دریافت

آن یک بایت مشخص به هر بسته را به صورت طول دریافت کرده

است



Source

PPP: زمانی که بخواهیم با استفاده از ریس Dial up به اینترنت متصل

شویم این پروتکل به عنوان واسطه در دایال آپ استفاده می شود، اطلاعاتی که برای اتصال

Dial up به آن نیاز است (Username و Password)

برای سدر و مقصد ارسال می کند

* MAC Address, Switch صرفاً برای ارتباط داخلی است

گاهی اوقات در رای ارتباط شبکه های خاص نیز به سمت مقصد

لازم می آید

۱) تبدیل اسم میسر به آدرس های منطقی و منطقی

۲) مسیریابی در شبکه و انتخاب بهترین مسیریابی محسوس

اطلاعاتی که این کار توسط دستگاه انجام Router می شود

سطح بسته اطلاعاتی : Packet

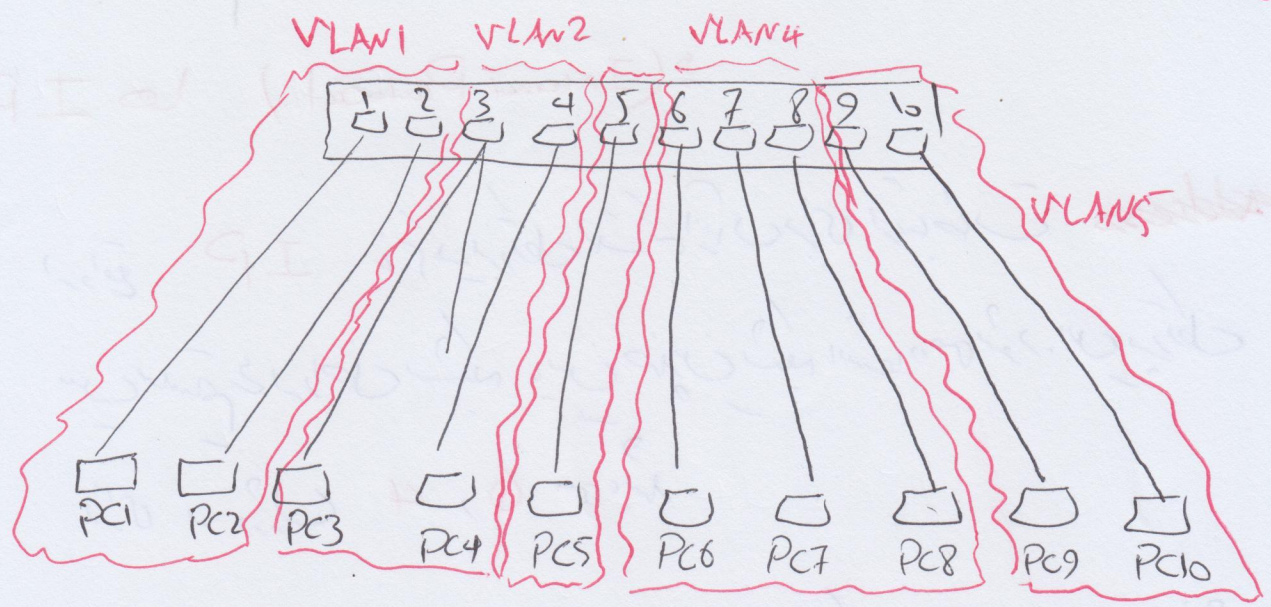
در صورت اشتباهی، می این سطح کار می کند :

سوئیچ لایه ۳، (Layer 3 Switch)

کامپیوترهای نیز در این سطح می باشد

۳۵

b : VLANing



VLAN3

Cisco Router Roleover
 Cisco Router Roleover

$$\begin{aligned}
 & 10 \times 1 + 5 \times 0 + 5 \times 1 + 5 \times 1 + 5 \times 1 + 5 \times 0 \\
 & 10 + 0 + 5 + 5 + 5 + 0 = 35
 \end{aligned}$$

IP ها (Internet Protocol)

IP ~~Address~~ **IP** نام و پورت است که برای ارتباط
 بین سیستم‌ها در داخل شبکه یا بین شبکه‌ها استفاده می‌شود. این پورت
 دارای درون 4, 6 می‌باشد.

ساختار **IP** : از چپ به راست با صحت سلسله شده است. هر بخش از
octed (آکتید) 8 بیت و هر صفت 4 بیت از رقم صفت جدا می‌شود.
 هر آدرس 32 بیت می‌باشد. یعنی به 4 صفت یعنی
 هر بخش 8 بیت دارد که هر یک 32 بیت می‌باشد. برای این سه صفت
 Decimal (رقم) 0 تا 255 می‌باشد.

011101

$$(0 \times 2^5) + (1 \times 2^4) + (1 \times 2^3) + (1 \times 2^2) + (0 \times 2^1) + (1 \times 2^0) = \underline{\underline{29}}$$

A	1-150	0-522	0-522	0-522
B	158-191	0-522	0-522	0-522
C	191-252	0-522	0-522	0-522

در آگهی اول، چهارم 0، 255، و پنجم 255

آدرسهای IP:

رتبب پنج طبقه A، B، C، D، E برای

IP وجود دارد که از سه طبقه A، B، C می توان

برای آدرس دهی استفاده کرد، هر طبقه دارای یک محدوده است

که در کل هم آدرس در یک طبقه باشد یا در آن محدوده قرار گیرد

هر طبقه دارای یک دامنه، دامنه برای تعداد کامپیوترهاست

و با توجه به تعداد کامپیوترهای هر طبقه مناسب است که

آدرس آن مرتب از عدد صفر تا 255 (IPها) طبقه بندی می شود

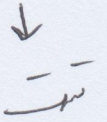
۵ رده با 4th Range

طریق *

A : 1-126 . 0-255 . 0-255 . 0-255

127 = Loop Back

B : 128-191 . 0-255 . 0-255 . 0-255



C : 192-223 . 0-255 . 0-255 . 0-255

* IP آندامه می تواند 255 باشد

طریق

A ← 112.125.2.3

B ← 129.115.0.4

C ← 192.201.205.200

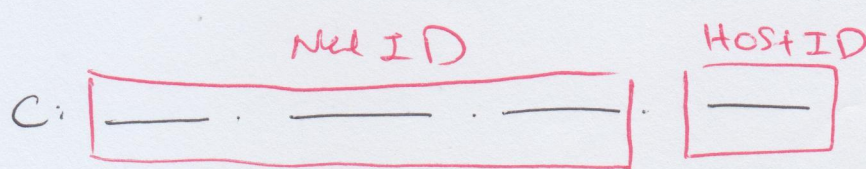
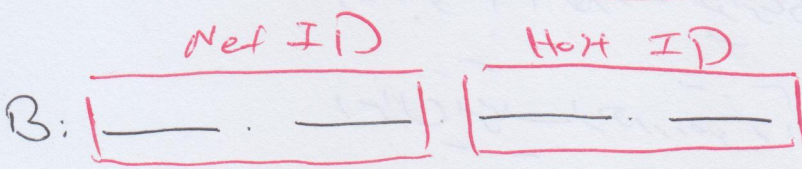
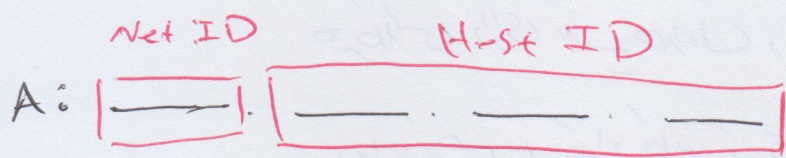
صاف :

وظیفه IP : ۱) به آدرس شبکه مقصد (۲) به آدرس کامپیوتر

Net ID : یعنی Octet ها که در شبکه مشخص می شود
Net ID هر شبکه، همیشه IP صاف است. ID یا شماره شبکه این مشخص می کند

Host ID : یعنی Octet ها (سه تا) A B C (بودن) یا ۵

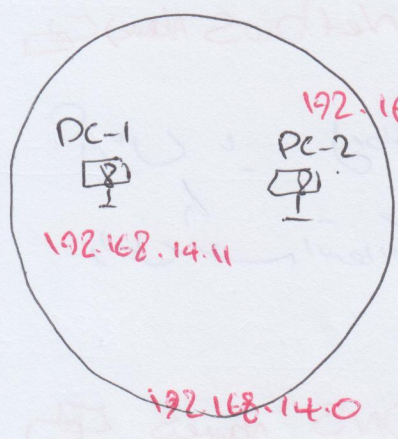
هر شبکه می تواند در صاف باشد یعنی IP نه ID



6 bits Subnet mask

1) Net ID ; Host ID

2) Subnet division



- Default
- A: 255.0.0.0
 - B: 255.255.0.0
 - C: 255.255.255.0

↓

50 IP addresses should be in the same class

Slash notation is used in the form of IP address

A: $\underline{192}.\underline{168}.\underline{14}.0 / \underline{24}$

↓

Net ID

B: $192.168.14.0 / 16$

↓

Net ID

A: $192.168.14.0 / 8$

↓

Net ID

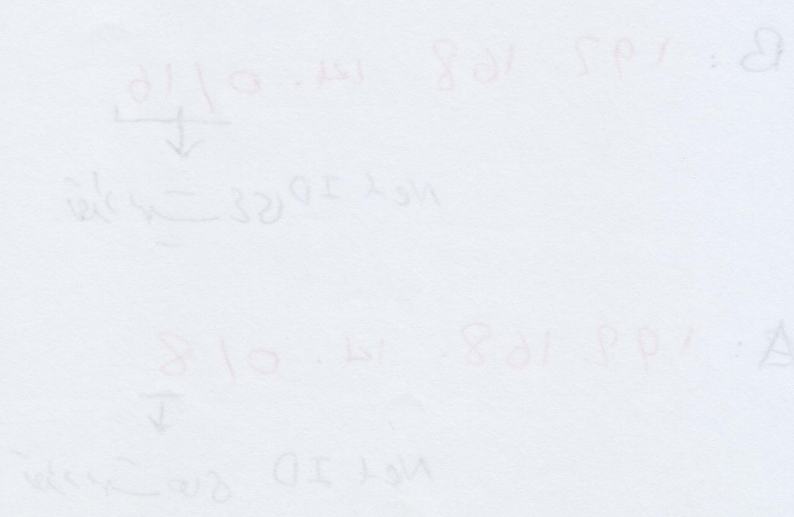
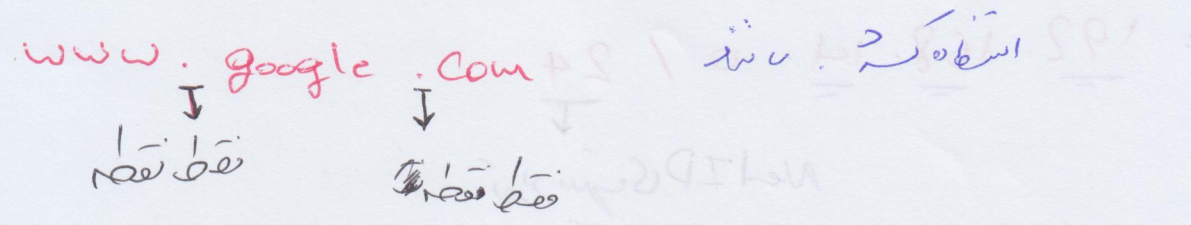
Network Name

* با دستور Host Name در PC یا Client فایل میخواند (اجرا cmd)

انواع اسامی شبکه :

Netbios Name : اسامی که همراه دارای میباشند دیده میشوند
آدرس یا History ندارند این اسامی همراه صورتان برای ارتباط در
داخل شبکه استفاده می شود

DNS Names : اسامی که دارای صفت هستند
تک نقطه ای و سایر صفتها جدا می شوند این اسامی دارای آدرس در History
ظاهر بوده و علاوه بر نام کامپیوتر اسم دیگری که کامپیوتر در آن قرار دارد
نیز در آن ذکر می شود این اسامی صورتان برای ارتباط و جستجو



فتاوحان IP :

Run $\xrightarrow{\text{type}}$ ncpa.cpl $\xrightarrow{\text{Enter}}$ $\xrightarrow{\text{Right click}}$ ok/apply

Properties \rightarrow on IPv4 \rightarrow Properties \rightarrow Obtain IP address automatically

\rightarrow در این ای پی وضعیت اول \rightarrow Subnet mask \rightarrow در این ای پی

دستور Ping : برای اطمینان از اینکه بین دو سیستم (این دستور با اجتناب از IP با هم سیستم) \rightarrow استفاده می شود. Run, Cmd, این دستور

Ping 192.168.14.11

\rightarrow TTL = 128 \rightarrow هج Router بین این است
 \rightarrow TTL = 128
 \rightarrow TTL = 128
 \rightarrow TTL = 128

* اگر بجای 128 یک عدد دیگر بود مثلا 127 یعنی در Router بین Client ها (Host ها) موجود است
میزان اختلاف عدد TTL با عدد 128 بین دستگاهها مقدار Router موجود است

توقف Host : به خاطر اینکه با سایر کامپیوترها که در IP شبکه دراز
مدت زیادی می کشند اصطلاحاً در Host قطع می شوند

پروتکل ICMP : این پروتکل برای تست اتصال، یک پی سی در شبکه

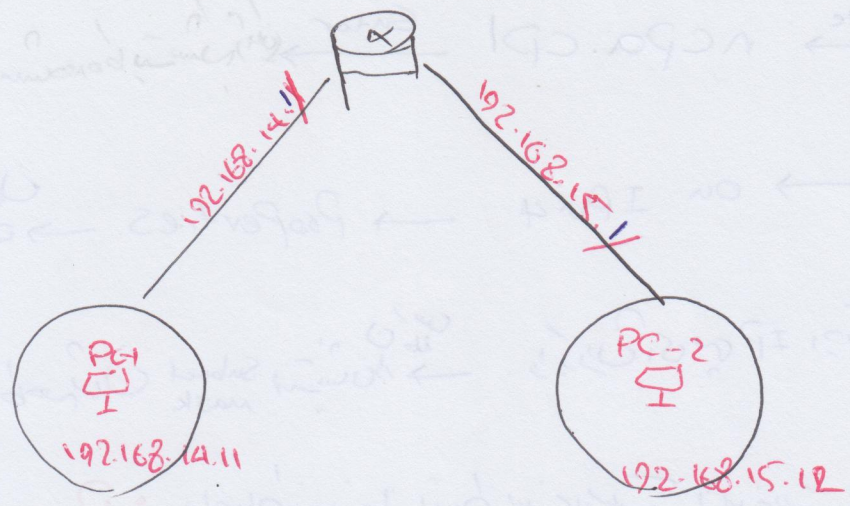
تست ای استفاده می شود. اهمیت اصلی دستور Ping پروتکل ICMP

دارد باری شده در چار یا فتوالی در 32 بیتی است به جهت مقصد ارسال

کرده دستور یا پیغام می سازد. در صورتی که با پیغام مقصد دریافت شود یعنی اینکه

دریافت رتبه است. این پروتکل را می توان دستور در Trace RT

استفاده می شود.



Default Gateway : همان روتر است که در شبکه های مختلف

رای سیستم روتر ارتباطات است که در شبکه های مختلف

روش های اختصاص IP دستی :

Static (Manual) :

این روش در شبکه های بزرگ و سیستم های مختلف استفاده می شود و در این روش روترهای مختلف با هم ارتباط برقرار می کنند و در صورت بروز مشکل در شبکه می توان به راحتی آن را حل کرد و در این روش روترها با هم ارتباط برقرار می کنند و در صورت بروز مشکل در شبکه می توان به راحتی آن را حل کرد

Dynamic (DHCP Server):

این روش یک سرور DHCP Server را به کار می‌برد که به کل شبکه IP را به خود اختصاص می‌دهد.

این سرور یک محدوده Range از IPها را به خود اختصاص می‌دهد.

DHCP Server سرور است که به کل شبکه IP را به خود اختصاص می‌دهد. این سرور به صورت Automatic مدیریت می‌کند.

(Automatic Private IP Address) APIPA:

این روش به کامپیوتر اجازه می‌دهد تا خودش یک IP را به خود اختصاص دهد.

این سرور یک محدوده Range از IPها را به خود اختصاص می‌دهد. (APIPA)

[Range 169.254.0.0] خود IP اختصاص می‌دهد.

این سرور به کامپیوتر اجازه می‌دهد تا خودش یک IP را به خود اختصاص دهد.

این سرور به کامپیوتر اجازه می‌دهد تا خودش یک IP را به خود اختصاص دهد. این سرور به صورت Automatic مدیریت می‌کند.

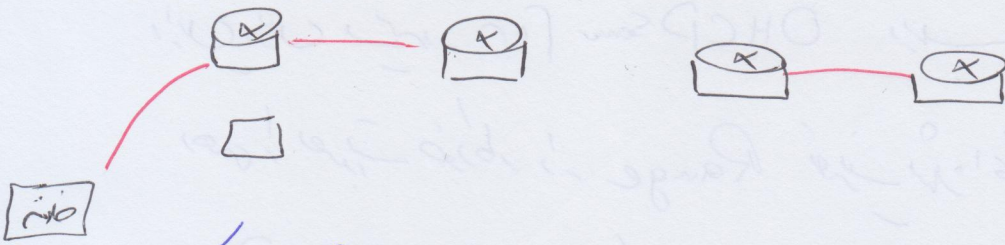
ipconfig /release

ipconfig /renew

Ping 8.8.8.8

درخواست اتصال اینترنت

٧٣
تعیین محل وقوع اتصال (تعیین):



Tracert + IP
تعیین محل وقوع اتصال

تعیین محل وقوع اتصال * * * timeout * * * (تعیین محل وقوع اتصال)

تعیین محل وقوع اتصال (تعیین محل وقوع اتصال)

8.8.8.8

* نکته: در صورت IP ثابت Static این امکان وجود دارد که بر روی سیستم

سپس از آن IP به هم آید و در صورت IP Dynamic این امکان وجود ندارد. هرگز سیستم هرگز ثابت نیست و همیشه

سرور DNS: این سرور می تواند نام را به IP تبدیل کند

زبان نام یا Hostname را در صورتی که در سیستم سرور می توانیم DNS

به کل نام (Name Resolution) نام سرور، Hostname را به IP تبدیل کند

- دستور برای دیدن آدرس DNS:

Run دستور از دستورات nslookup در صورت

دنبال هر Hostname که وارد کنیم IPv4 درج

میگردد و هر وقت که صفحه می شود

پروتکل ARP (Address Resolution Protocol)

کسی از پروتکل های لایه 2 Data Link لایه 3 یعنی تبدیل

IP Address م Mac Address (ایم صده) در این اتفاق

رسانه صده ایم که میسر خواهد یا استفاده از IP Address عنوان

آدرس میسر از عنوان میسر است با سیستم دیگری ارتباط برقرارند

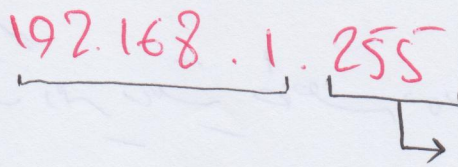
* نکته : دستور های Ping , Tracert از پروتکل

ICMP تهیه می کنند، این پروتکل مربوط به Network می باشد

ارسال بسته بدون IP Broadcast (گسترده)

رابط شبکه را به شبکه سیستم اطلاعاتی ایم ایم سیستم ارسال می کند

IP در هر شبکه ای می تواند ارسال شود



صفت Host ID
 بیت 4 (1) بسته می
 2
 بسته 255

آدرس های Public , Private

Private: یک مجموعه از IP Address حالت به کفوی استفاده

رشته ای خاص بوده در دنیای اینترنت هیچ کاربرد ندارد و صرفاً

مخاطب ما، آدرس های داخلی سیستم های شبکه محلی (شبکه) می باشد

باید این نوع آدرس ها استفاده کنیم. این نوع آدرس ها هم نیز دارای

سه طلاس A, B, C داریم که محدوده های آن به صورت زیر می باشد

A: 10 . 0 . 0 . 0 → 10.255.255.255

B: 172.16.0.0 → 172.31.255.255 , 169.254.0.0 → 169.254.255.255

C: 192.168.0.0 → 192.168.255.255

Public: تمام آدرس های که خارج از محدوده Private هستند

Range Public می باشد کاربرد این آدرس ها در

اینست که مخاطب یک کامپیوتر در دنیای اینترنت نیز قادر به دسترسی
در اینترنت می باشد.

* تبدیل Private → Public

NAT : یعنی آدرس های شبکه های خصوصی را تبدیل به آدرس های عمومی می کند

(Network Address Translation)

معمولاً یک سرور در شبکه های خصوصی قرار می گیرد که وظیفه آن تبدیل آدرس های خصوصی به آدرس های عمومی است

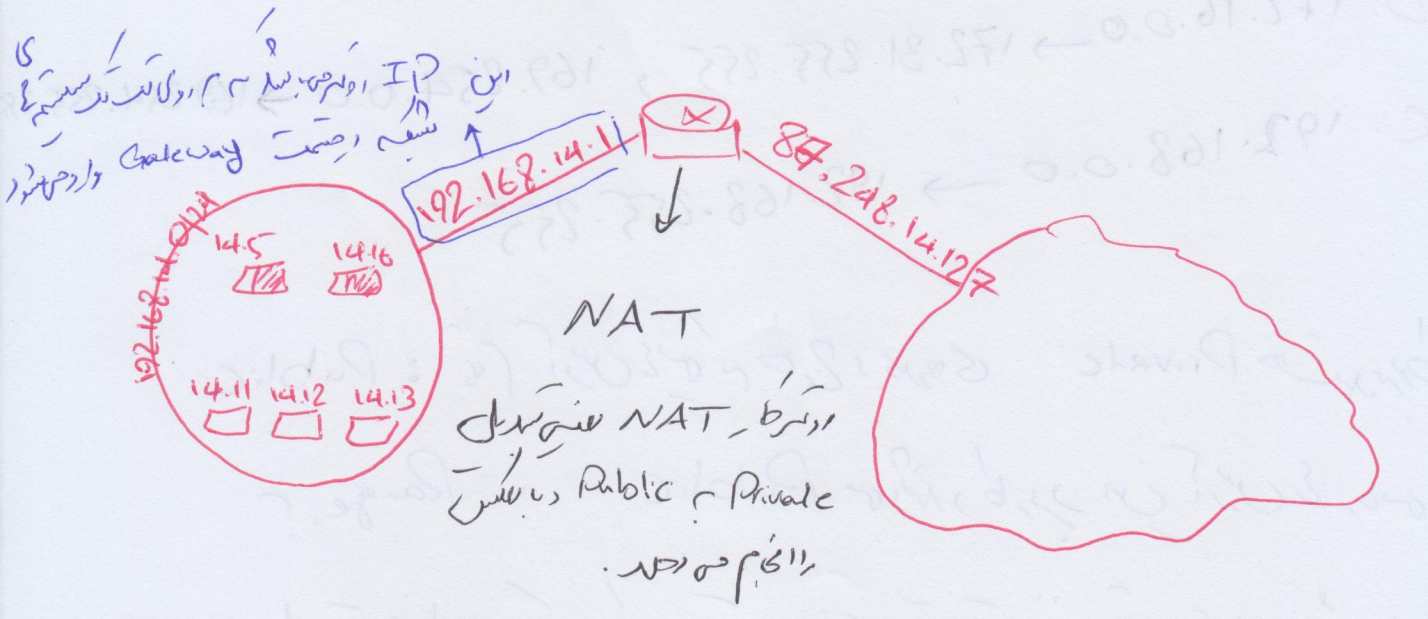
در شبکه های خصوصی هر دستگاه به یک آدرس خصوصی اختصاص می یابد

برای دسترسی به اینترنت از طریق NAT این امکان فراهم می شود

در شبکه های خصوصی هر دستگاه به یک آدرس خصوصی اختصاص می یابد

Public سرورهای Router و NAT Server که وظیفه آن تبدیل آدرس های خصوصی به آدرس های عمومی است

معمولاً یک سرور در شبکه های خصوصی قرار می گیرد که وظیفه آن تبدیل آدرس های خصوصی به آدرس های عمومی است



رابطه: کنترل بسته اطلاعاتی برای صحت از طرف دیگر

مدیریت در طرف دیگر (خطای انتقالی بسته اطلاعاتی) (Error Handling)

(Flow Control)

Segment : بسته اطلاعاتی

صحت بسته را در این لایه چک می کنند؟ صحت اولیه را در لایه سوکت

نبردخلی لایه Transport :

UDP (۲) TCP (۱)

Transmission Control Protocol (۱)

User Datagram Protocol (۲)

رابطه لایه TCP :

Connection oriented : رابطه بسته بسته در این لایه قبل از ارسال هر بسته رابطه

Connection یا رابطه بین سیستم های مبدأ و مقصد است که در سوکت برقرار می شود

(۱) سیستم مقصد وجود داشته باشد

(۲) در دسترس باشد

(۳) آماده دریافت اطلاعات باشد

این ارتباطات با بسته‌های ارسال نمی‌شود یا اگر شود ممکن است گم شود یا به اشتباه
(Reliable Communication) ، بارها در صورت دریافت بسته با خطا اخطار می‌دهد و بسته‌ها را

3-way handshaking : ارتباط با استفاده از پروتکل TCP این نام دارد

در ابتدا هرگاه قبل از ارسال هر بسته ارتباطی، ارتباط بین سیستم‌های مبدأ

مقرر می‌شود تا هر دو طرف از وجود آن مطلع شوند. در اینجا هر طرف یک Acknowledgment

مستطرد می‌دهد.

UDP : ورتیکولی

Connection less : ارتباط نامیدار

- بسته‌های قبلی در دستورالعمل ارسال می‌شوند اما آن‌ها در آن صورتی نیست انجام می‌شوند
در صورت تمام آن‌ها آن صورتی نیست انجام می‌شوند

MTU (Maximum Transfer Unit):

سایه‌های اطلاعاتی که از یک شبکه ارسال می‌شوند را اگر یک سایه بزرگتر از آن باشد

بزرگتر از آن MTU خواهد بود. به این خصوصیت سایه‌های Network گفته می‌شود.

این سایه‌ها که سایه بزرگتر از سایه‌های MTU هستند در روترها (Router) مودا

اگر سایه بزرگتر از سایه‌های MTU در هر قسمت در ID یا اندیس مشخص

موجود باشد روترها قادر به استفاده از همین اندیس‌ها نمی‌شوند.

نقطه‌های سایه بزرگتر از سایه‌های MTU باید در ارسال می‌شوند. این سایه‌ها

IP fragmentation گویند.

1	2
3	4



1 2 3 4

PAT (Port Address Translation):

این پروتکل سایه‌های ورودی در ID یا سایه‌ها Port و Packet سایه‌ها

درخواست‌های سایه‌ها PAT می‌شوند این سایه‌ها یک سایه می‌شوند.

سایه‌ها در طول سایه‌ها می‌شوند در سایه‌ها Port مربوط به این سایه‌ها

درخواست سایه‌ها می‌شوند.

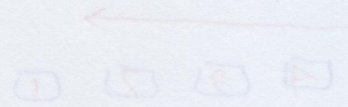
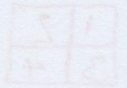
28

PC-1 → Facebook.com

PC-2 → LinkedIn.com

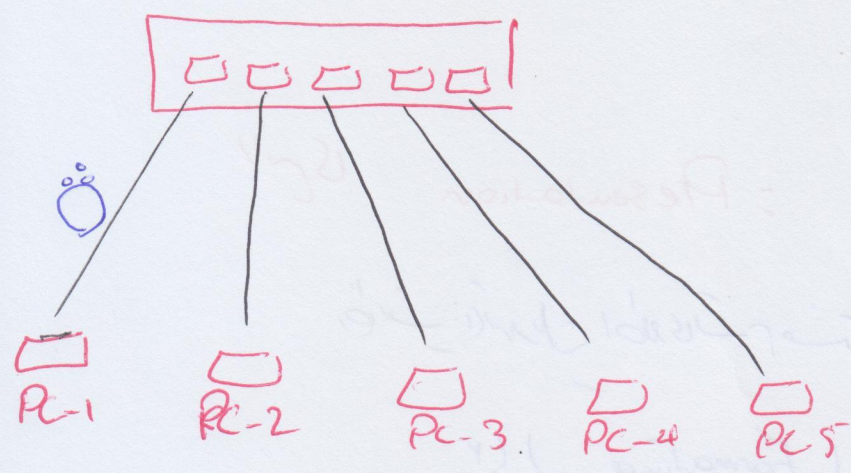
: Table CAM

Client	Private	Public	Port	Server
14.11	14.1	87.248	141	Facebook
14.12	14.1	"	142	linkedin



3 (Port Address Translation) NAT

Detailed NAT table ID and NAT
 NAT & NAT
 NAT & NAT
 NAT & NAT



Port number	MAC Address
1	MAC 1
2	MAC 2
3	MAC 3
4	MAC 4
5	MAC 5

هر کامپیوتر پس از روشن شدن اولین بسته‌ی اطلاعاتی که می‌آید، آدرس MAC آن را در جدول خود ثبت می‌کند.

• Session

۱) هدف: برقراری ارتباط بین سیستم عامل و درگاه‌های فیزیکی

۲) قطعات: برقراری ارتباط شروع در بین آن

۳) هم‌ساز سازی (Synchronization)

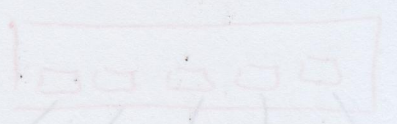
۴) اضافه کردن Check Point (نقطه‌ی کنترل)

۵) بسته‌ها شروع به حرکت می‌کنند و ارسال اطلاعات به درگاه فیزیکی

۶) اطلاعات از فیزیکی شروع به ارسال می‌شود، این کار با هم‌ساز سازی

۷) هم‌ساز سازی کامل می‌شود (تمام شدن فرآیند)

سطح پنجم اطلاعاتی: Data



Presentation : لایه پنجم

وظیفه: تبدیل اطلاعات فرم قابل درک برای کاربر به فرمت قابل

۱) (Formatting) مرتب‌سازی، مرتب‌سازی بصری، مرتب‌سازی

مرتب‌سازی

۲) مرتب‌سازی، مرتب‌سازی، مرتب‌سازی، مرتب‌سازی

مرتب‌سازی

سطح پنجم اطلاعاتی: Data

Application : لایه پنجم OSI

برای برنامه‌های کاربردی، این لایه شامل برنامه‌های کاربردی است.

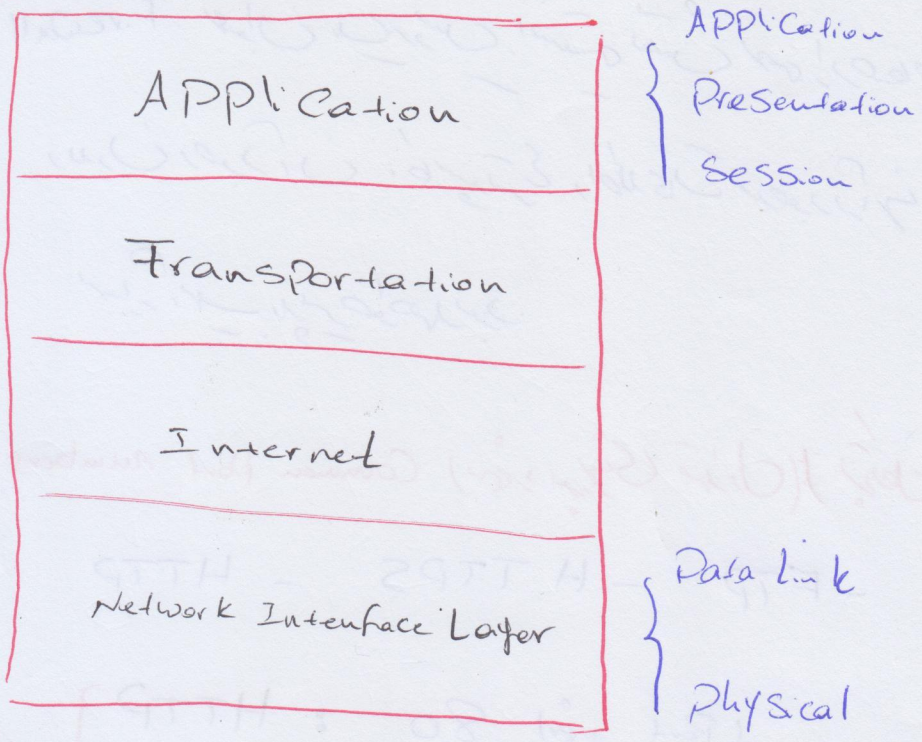
Player ها، E-mail manager ها، مرورگرها، و غیره.

از دیدگاه اطلاعاتی، این لایه شامل Presentation

این لایه برای کاربردهای کاربردی است.

مرتب‌سازی، مرتب‌سازی، مرتب‌سازی، مرتب‌سازی

سطح پنجم اطلاعاتی: Data



Firewall: یک سیستم امنیتی است که طرح ترافیک را بررسی می‌کند و از کامپیوترها، شبکه‌ها و سرورها در برابر

ترافیک نامعتبر (Outbound traffic) یا آن را رد می‌کند (Inbound traffic).

کنترل دسترسی به شبکه‌ها می‌کند و می‌تواند از حملات سایبری جلوگیری کند. در واقع در درون Firewall

تکلیف‌ها انجام می‌دهد. برای هر یک از این موارد، Port (که به آن‌ها Ports گفته می‌شود) دارد (65535 Ports)

هر پورتی که می‌خواهیم به آن دسترسی داشته باشیم، باید از طریق پروتکل یا سیستم امنیتی خاصی مشخص می‌شود.

هر یک از این پورت‌ها باید کار یا سرویس مشخصی داشته باشد. مثلاً پورت ۸۰ برای وبسایت‌ها و پورت ۲۵ برای ایمیل.

شماره‌ها ۱۰۲۴ (۱۹۲۳ - ۰) پورت‌های Well-known هستند.

System Ports (۱۰۲۴ - ۴۹۱۵۱) و پورت‌های اختصاصی دیگر.

Registered Ports (پورت‌های ثبت شده) که برای برنامه‌های خاص استفاده می‌شوند.

اصولاً هر پورتی که در صورت بسته بودن Port می‌تواند ترافیک را رد کند یا Drop یا Reject می‌کند.

Firewall عنوان یک مبروس است که پس از نصب روی ارضاءت - سیستم در کوره داشته
 در بدن وجود آن . کامپیوتری ، اطلاعات موجود در آن را متصل به دیگر است
 بسیار آسان و در صورت وجود

Common Port numbers (به یادگیری مقدماتی) (برای در نظر آید اینی طوری)

TFTP - FTP - HTTPS - HTTP

(Port 80)	:	HTTP	} Web
(Port 443)	:	HTTPS	
TCP 21	:	FTP	
UDP 21	:	TFTP	

mail (برای یادگیری اینی طوری)

25	:	SMTP	} mail
110	:	POP3	
143	:	IMAP	

53 : DNS } Network

68, 67 : DHCP } Services

* ابتدا به شبکه اندیم با هم پوی کاسیویر ما با یک سیستم در آن سیستم می

اصلاحات زنگار دستور - Netstat -> Local PC -> در عمل CMD

در صورتی

بر عمل SNMP در یک سرور

کابل Fiber optic (فیبر نوری) کابلی هستند که از آنجا که می توانیم

بسیار از سرعت و پهنای باند بسیار بالاتر از کابلهای مسی استفاده می شود در آنجا

که می توانیم از آنجا که فیبر نوری از پلاستیک یا شیشه ساخته شده است

اصلاحات استفاده می شود. کابل فیبر نوری خاصیت پهنای باند بسیار

کابل فیبر نوری می تواند اصلاحات را به یک کابل مسی در برتری

این کابل فیبر نوری اصلاحات کابل مسی در برتری

کابل کاسیویر از در نوع کاسیویر SC, ST استفاده می شود

Server Clustering: روشی است که در آن چندین سرور مجزا در یک سرور

بزرگتر قرار می گیرند و در یک سیستم واحد عمل می کنند و هر یک از سرورهای

کلیه درخواست های کاربر را می توانند پاسخ دهند و اگر یکی از سرورها

تعمیر می شود، در این شرایط Load وجود در Serverها کاهش یافته

هر یک از سرورهای موجود در سیستم می توانند به این صورت عمل کنند Load balancing

صحت این است که یک هاست در یک سرور وجود دارد و در کنار آن می تواند سایر سرور ها
 دارد بزرگتر از آن و در صورتی که این سرور ها می توانند با هم کار کنند این سرور ها
 Fault tolerance نام دارد. مانند یک 64 سرور با هم قابل cluster می باشد.

Virtualization

گاهی اوقات برای اینکه سرور های مختلف بتوانند در یک سرور با هم کار کنند
 این سرور ها را می توانیم به کمک Virtualization نام قرار دهیم و این سرور ها را می توانیم

در حد استفاده از فناوری Virtualization می توانیم یک سرور Storage

را بصورت مجزا از سرور اصلی و در کنار سرور اصلی قرار دهیم virtual

در دل آن می تواند استفاده از این فناوری را در یک سرور مجزا قرار دهیم
 به نام سرور مجزا.

