شبکه :

در ساده ترین تعریف میتوان گفت که وقتی حداقل دو سیستم منابعی را با یکدیگر به اشتراک می گذارند (این منابع میتواند شامل : اطلاعات ، اینترنت ، پرینتر و ... باشد) یک شبکه تشکیل داده اند.

معمول ترین اجزاي شبکه ها

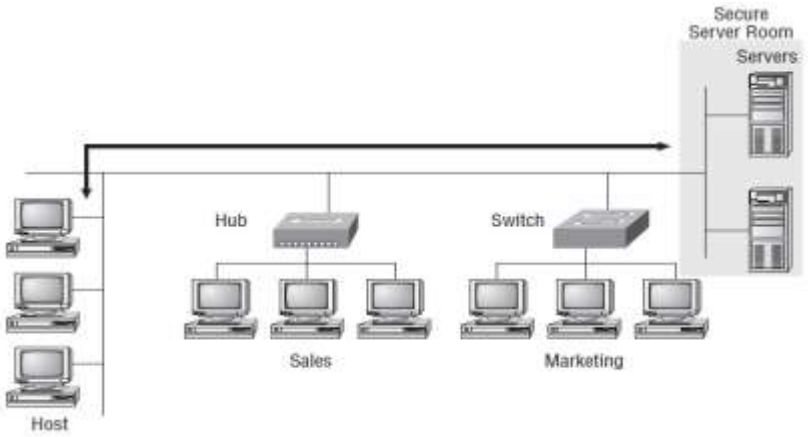
- Servers
- Workstations
- Hosts

Workstations

سیستم هایی قوی هستند که در حالیکه از منابع شبکه مانند client ها استفاده می کنند منابعی را نیز در شبکه share کرده و در اختیار دیگران قرار میدهند.در حقیقت workstationها کمکی برای server ها هستند و قسمتی از وظایف آنها را به دوش میکشند. مثل ایفای نقش به عنوان یک printserver در شبکه

Hosts

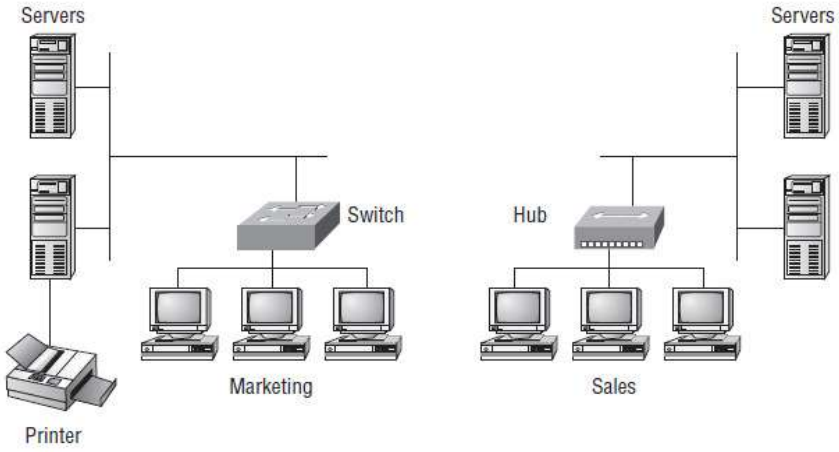
تقریباً تمامی اجزای شبکه که منبعی و یا سرویسی را در شبکه ارائه می کنند host نامیده می شوند Server ها و workstation ها نیز host محسوب میشوند.



Local Area Network (LAN)

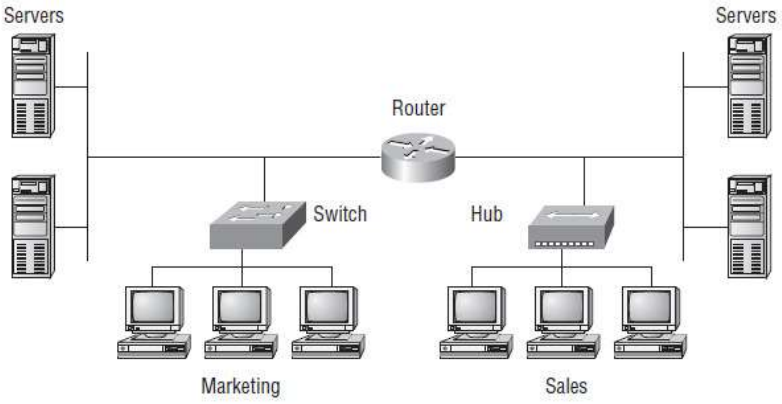
شبکه ای که از لحاظ جغرافیایی در یک مکان مشخص باشد. مثل یک ساختمان ، یک خانه و امثال آنها.

یک شبکه LAN نمیتواند در چندین مکان باشد.در شکل زیر دو شبکه LAN را مشاهده می کنید.



اگر این دو شبکه LAN بخواهند با یکدیگر ارتباط برقرار کنند ، دو مسئله مانع از این کار خواهد شد:

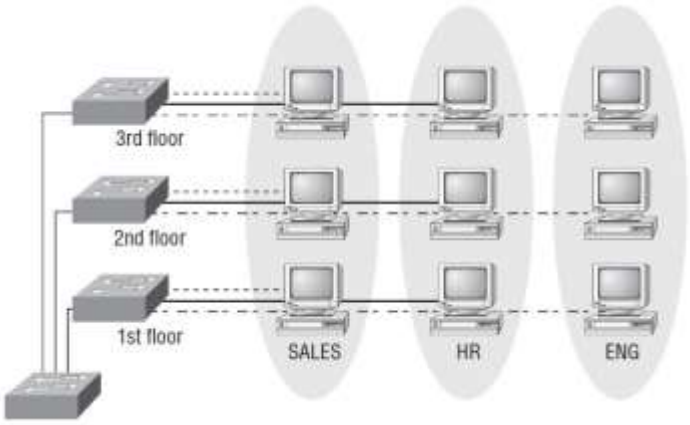
۱. باید هر دو شبکه بصورت فیزیکی به یکدیگر متصل شده باشند
۲. نمی توانند بصورت Remote به Server ها و منابع شبکه دیگر دسترسی پیدا کنند .حلال این مسئله یک سخت افزار بسیار عالی و زیبا و جالب به نام Router است.



Virtual LAN (VLAN)

در دنیای جدید شبکه های کامپیوتری workgroup تعریف قدیمی خود را از دست داده و جای خود را با VLAN تعویض کرده است. بدین صورت که شما میتوانید در طبقه ای دیگر از یک ساختمان باشید) دور از فضای فیزیکی workgroup خود (اما همچنان عضوی از همان workgroup بوده و به منابع آن دسترسی داشته باشید. این حالت در صورتی امکان پذیر است که بتوانید بصورت مستقیم با آن workgroup در ارتباط باشید (این حالت معمولاً توسط administrator که switch را برای این منظور تنظیم کرده است قابل استفاده است). نمونه ای از چند VLAN را در شکل زیر مشاهدی می کنید . جمله ای که میتوان VLAN را با آن تعریف کرد این است:

"Take my host and make it appear local to the remote resources"



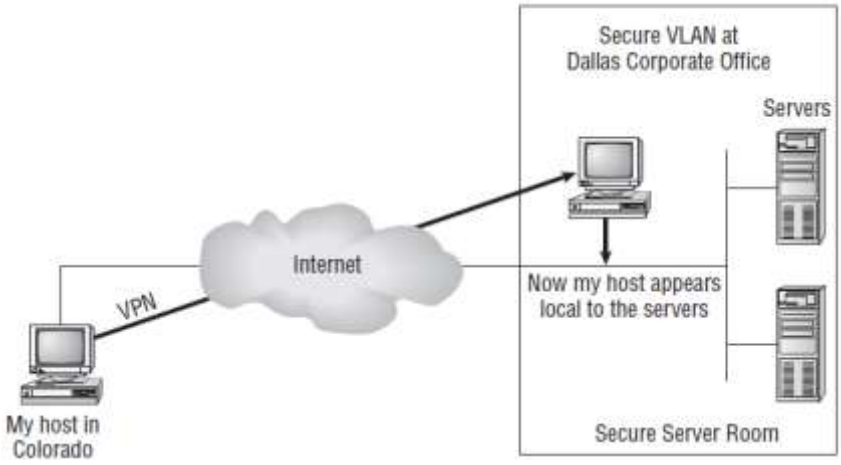
Wide Area Network (WAN)

شبکه های WAN در مقایسه با LAN از لحاظ فیزیکی وسعت بسیار بیشتری دارند. این وسعت میتواند از فاصله بین چند ساختمان تا بین چند قاره باشد. یکی از بزرگترین شبکه های WAN اینترنت است که هر روز با آن سرو کار داریم. در نگاهی تخصصی تر تفاوت WAN و LAN را بررسی میکنیم

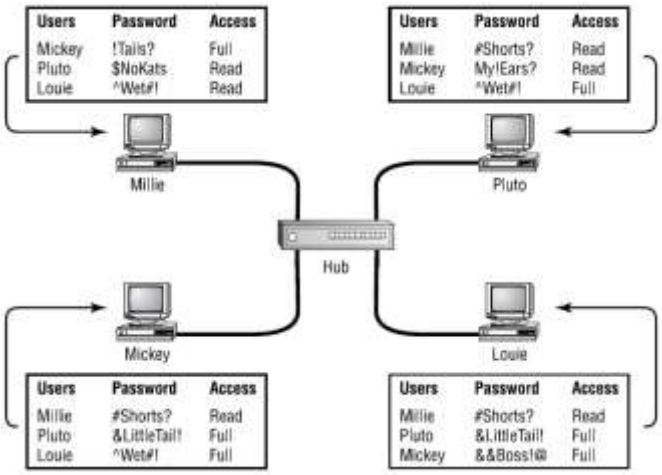
- معمولاً برای برقراری ارتباط به یک یا چند Router نیاز دارند.
- مثل LAN هادارای فضای فیزیکی محدودی نیستند.
- معمولاً سرعتشان پایین تر است.
- زمان برقراری ارتباط در WAN مشخص است در صورتی که شبکه LAN یا همیشه برقرار است یا نیست.
- در WAN نحوه ارتباط به چند صورت می تواند باشد خصوصی و عمومی . مثل شبکه داخلی و یا مودم و...

Virtual Private Network (VPN)

از VPN ها معمولاً برای برقراری ارتباط امن بین LAN ها و WAN ها استفاده می کنیم.در واقع وقتی از طریق ISP به شبکه WAN متصل می شویم از دید شبکه WAN ما یک مراجعه کننده خارجی هستیم ، و سیستم ما را جزئی از شبکه داخلی خود محسوب نخواهد کرد. اما اگر از طریق VPN متصل شده باشیم جزئی از شبکه LOCAL در محل WAN خواهیم بود و میتوانیم از منابع آنجا استفاده کنیم . این حالت به نوعی شبیه VLAN است که پیشتر در مورد آن بحث کردیم.



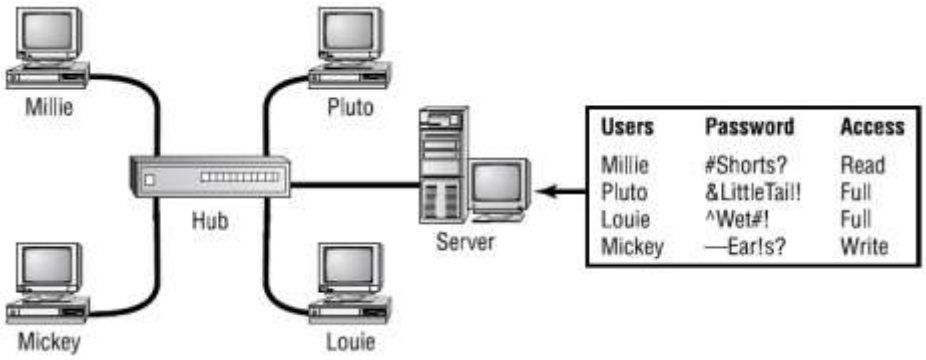
Peer-to-Peer Networks



در شبکه های peer-to-peer سیستم ها بصورت مستقیم با یکدیگر در ارتباط اند قسمت مدیریت مرکزی ندارند ، یعنی هیچ کدام بر دیگری برتری ندارد و فقط هنگامی که یکی از سیستم ها از دیگری منبعی را درخواست میکند سیستم ارائه کننده منبع تعیین کننده نحوه دسترسی و مجوز ها خواهد بود.

Client/Server Networks

این حالت کاملاً برعکس شبکه های peer-to-peer است. در این نوع شبکه ها تمامی قوانین و مجوز ها از طرف یک سیستم مرکزی بنامserver تعیین و ارائه می شود و برتری هر سیستم به مجوز هایی است که از طرف server به او اعطا شده است.

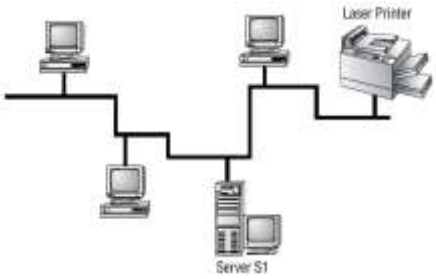


توپولوژي هاي شبکه

توپولوژی شبکه نشان دهنده نحوه چیدمان و اتصالات شبکه است. انواع توپولوژی های شبکه در زیر لیست شده اند:

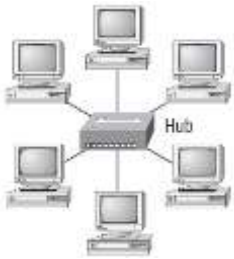
Bus , Star , Ring , Mesh , Point-to-point , Point-to-multipoint , Hybrid

Bus Topology



در توپولوژی Bus تمامی سیستم ها از طریق یک سیم به یکدیگر متصل میشوند که در ابتدا و انتهای شبکه هر کدام یک وسیله بنام ترمینال نصب میشود . نصب و راه اندازی آن بسیار ساده است ، میزان کابل کشی کم است ، در فواصل زیاد troubleshoot آن سخت است. اگر قسمتی از کابل قطع شود همه شبکه از کار خواهد افتاد. این توپولوژی بسیار قدیمی بوده و تقریباً خارج از رده است

Star Topology

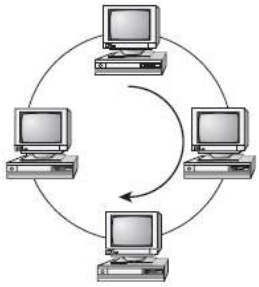


شامل یک مکان مرکزی است (کابلی یا بی سیم) که همه سیستم ها به آن متصل می شوند و از آن طریق ارتباط برقرار می کنند.دارای مزیت های بیشتری نسبت به توپولوژی Bus می باشد از جمله اگر کابل سیستمی دچار اشکال شود فقط آن سیستم ارتباطش را از دست می دهد و بقیه سیستم ها فعالیتشان مختل نخواهد شد ، پس باعث بالا رفتن fault tolerance شبکه خواهد شد.

از مزیت ها و معایب این توپولوژی:

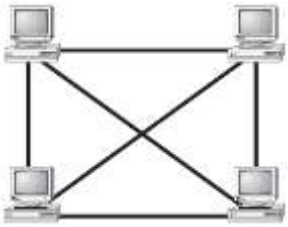
- سیستم های جدید به راحتی میتوانند به شبکه اضافه شوند.
- Troubleshootاین نوع شبکه ها راحتتر است.
- به دلیل طولانی شدن کابل کشی هزینه آن بیشتر است.
- اگر Hub دچار مشکل شود کل شبکه Down خواهد شد.

Ring Topology



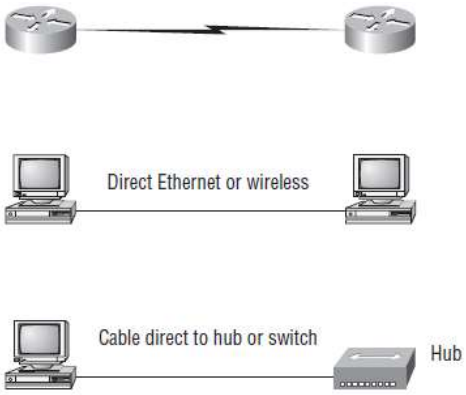
در این حالت تمام کامپیوتر ها در شبکه به یکدیگر متصل شده اند. بزرگترین اشکال این نوع توپولوژی بغیر از شباهت آن به Busاین است که هنگام اضافه کردن یک سیسنم به شبکه باید کابل اتصال را قطع کرد که باعث Down شدن کل شبکه خواهد شد . از سال ۱۹۹۰ به بعد به ندرت از این توپولوژی استفاده می شود.

Mesh Topology



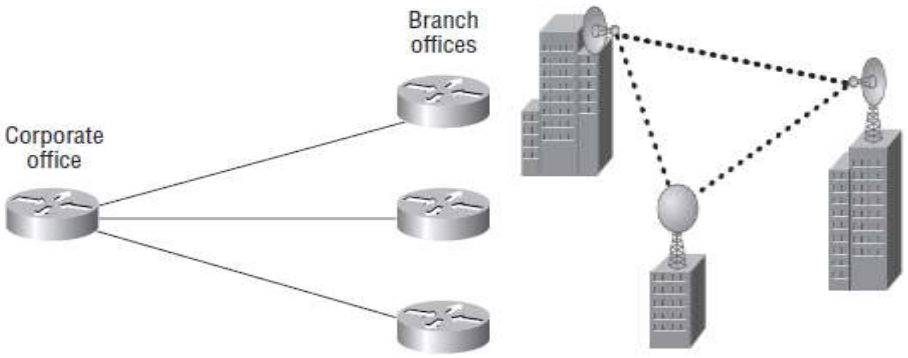
در این حالت تمامی سیستم ها بصورت فیزیکی به یکدیگر متصل می شوند. معمولاً در شبکه های LAN از این نوع توپولوژی استفاده نمی شود. اگر تمامی دستگاه ها در شبکه مستقیماً به یکدیگر متصل نباشند نمیتوان گفت توپولوژی Mesh بصورت کامل اجرا شده است . هر چقدر تعداد سیستم ها بیشتر باشد این تشخیص و اجرای این توپولوژی پیچیده تر می شود .برای محاسبه تعداد Connection ها در شبکه به ازای هر سیستم از فرمول n(n-1)/2 استفاده می کنیم بدین صورت که n نشان دهنده هر host یا Location بوده و جواب بدست آمده از فرمول مشخص کننده تعداد connection های آن خواهد بود . برای مثال در شکل زیر با استفاده از این فرمول خوایم داشت : 4(4-1)/2=6 ،یعنی ۶ اتصال. دراین نوع توپولوژی Tolerance Faultبسیار بالا است.

Point-to-Point Topology



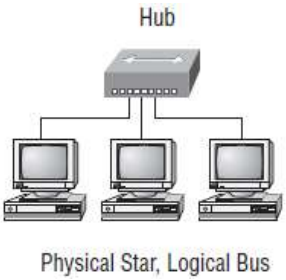
همان گونه که از نام این توپولوژی معلوم است ، در این حالت دو Router با یکدیگر ارتباط مستقیم برقرار می کنند. اتصال این دو از هر نوعی میتواند باشد.

Point-to-Multipoint Topology



در این نوع توپولوژی ، ارتباط بین یک router با چند router برقرار می شود.

Hybrid Topology



توپولوژی hybrid در واقع تلفیق بین چند توپولوژی مختلف است که با یکدیگر مرتبطند.

انتخاب توپولوژي درست

انتخاب توپولوژی درست به چند مورد بستگی دارد ، از جمله:

* هزینه

* راحتی یا پیچیدگی در نصب

* نحوه نگهداری

*میزان Fault Tolerance مورد نیاز

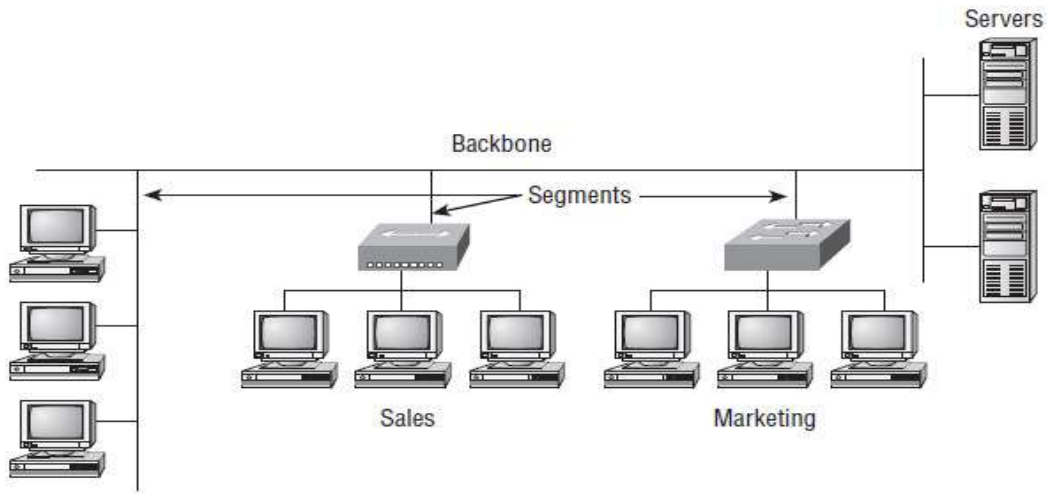
Network Backbone

برای هرچه دور تر شدن از پیچیدگی در نصب و فهم شبکه ، ما آن را به چند قسمت تقسیم میکنیم که آنها را backbone و segmentمی نامیم.

Backbone

تمام server ها و segment های شبکه به backbone متصل می شوند که ساختار اصلی شبکه را تشکیل می دهند .
Backboneشبکه باید قوی و سریع باشد (معمولاًgigabit Ethernet)

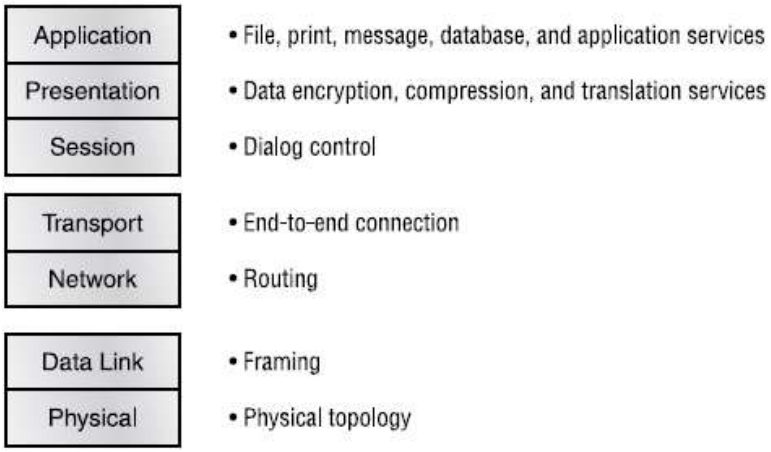
Segment



تمام قسمت های کوچک شبکه که به یکدیگر متصل شده اند اما جزء backbone شبکه نمی باشند.

پروتکل شبکه و لایه هاي آن

لایه های موجود در پروتکل شبکه را مثل شرکتی در نظر بگیرید که هر لایه مثل بخشی در شرکت است که وظیفه ای را بر عهده دارد. لایه های موجود در این پروتکل را به ۷ لایه تقسیم میکنیم که به ترتیب عبارتند از:



این ۷ لایه به دو گروه تقسیم می شود که سه لایه بالا تعیین کنندۀ نحوه ارتباط برنامه ها و کاربران با یکدیگر و چهار لایه باقیمانده(۴ لایه پایینی) تعیین کننده نحوه تبادل اطلاعات می باشند.

Application Layer

وقتی برنامه ای میخواهد با شبکه ارتباط برقرار کند ، نیاز خود به برقراری ارتباط را از طریق قسمت Application اعلام میکند و این لایه مقدمات کار را می چیند . برای مثال اگر شما بخواهید از طریق IE محتویات یک فایل HTML را بصورت Local مشاهده کنید و پروتکل یاد شده هم در سیستم موجود نباشد مشکلی به وجود نخواهد آمد اما اگر بخواهید همان صفحه را از

طریق شبکه ببینید در صورت نبود این پروتکل و این لایه قادر به انجام این کار نخواهید بود . همچنین بررسی موجود بودن منابع مورد درخواست و یافتن آنها نیز از وظایف این لایه می باشد.

Presentation Layer

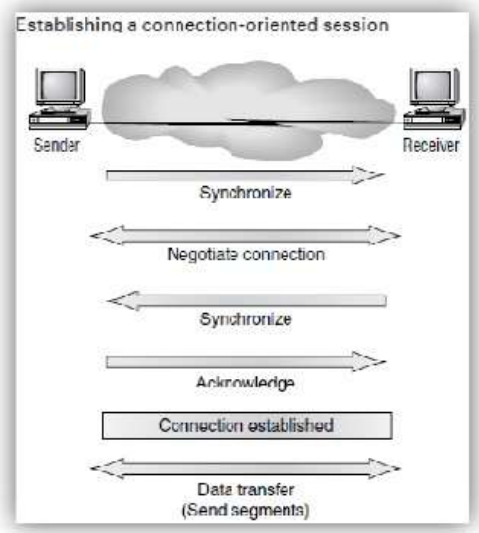
وظیفه این لایه معرفی ماهیت اطلاعات به لایه App بوده و انجام کارهای translation و formatting code نیز بر عهده این لایه است . این لایه هنگام تبادل اطلاعات باید مطمئن شود که اطلاعات از سیستم مبداء صحیح و سالم به مقصد transmit شده و درمقصد decode خواهد شد . برخی از ارتباطات Multimedia هم بر عهده این لایه می باشد.

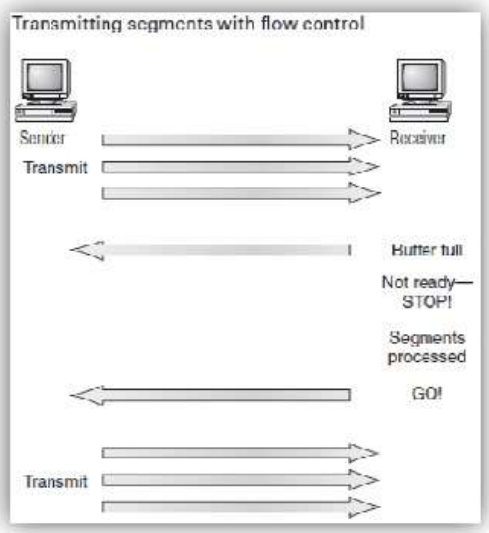
Session Layer

مسئولیت کارهایی از قبیل برقراری ، مدیریت و قطع ارتباط میان این لایه و layer presentation و کنترل ارتباط به سخت افزار ها و node ها بر عهده این لایه است .هماهنگی بین server ها و client ها و ارتباط میان آنها از سه طریق simplex ، duplex half وduplex full انجام می شود. در کل وظیفه این لایه جدا سازی اطلاعات برنامه های مختلف از یکدیگر می باشد.

Transport Layer

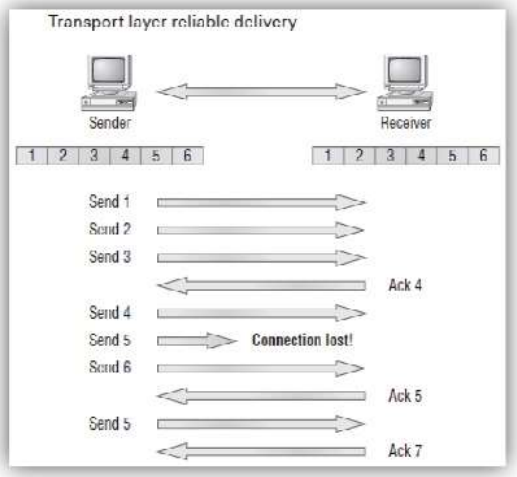
قبل از شروع تبادل اطلاعات بین دو سیستم ، ابتدا لایه Transport سیستم مبداء با لایه Transport سیستم مقصد تماس برقرار می کند. ارتباط ایجاد شده در این مرحله (Virtual circuit ارتباط مجازی) نامیده می شود و از نوع-oriented connectionمی باشد. در واقع این ارتباط مثل بستن قرار دادی است که در آن مقدار تبادل اطلاعات توافق شده و در صورت موافقت طرفین ارتباط پایدار و قابل اعتماد برقرار می شود . شکل زیر نحوهٔ برقراری ارتباط oriented-connection را نشان می دهد . وقتی ارتباط برقرار شد هر از چند گاهی پیوسته بودن اتصال و تبادل صحیح اطلاعات بررسی می شود.





Acknowledgments

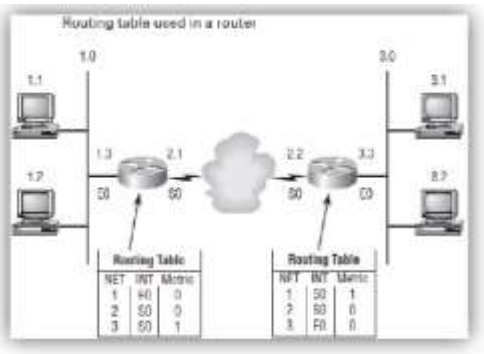
یک پیام است. پیامی که پوسته بودن اتصال و تبادل اطلاعات را تضمین می کند. هر segment از اطلاعات فرستاده شده از طرف سیستم فرستنده منتظر جواب (Acknowledgments)از سیستم گیرنده می شود و بعد از دریافت آن segment بعدی را ارسال می کند. شکل زیر نمونه ای از این رابطه و پیام دریافت است.



Network Layer

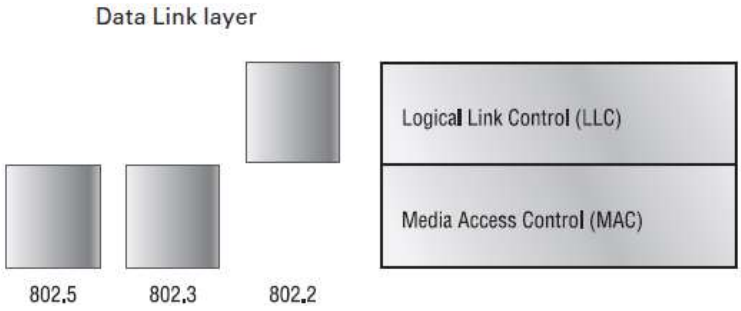
این لایه آدرس device ها را یافته ، مکان آنها را در شبکه ردیابی می کند و بهترین مسیر را برای برقراری ارتباط و حمل و نقل اطلاعات انتخاب می کند. Router ها هم در همین لایه فعالیت می کنند. نحوه کار این لایه بدین صورت است که ابتدا یک Packet به Router فرستاده می شود و IP آن چک می شود . اگر IP مورد نظر در جدول Routerموجود بوده و در همان مکان در شبکه نیز باشد packet به آنجا فرستاده می شود در غیر اینصورت به Router های دیگر مراجعه خواهد شد. دو نوع packet در این لایه از شبکه مورد استفاده قرار می گیرد:

۱. Packets Data: برای انتقال اطلاعاتی که از طرف کاربران رد و بدل می شود استفاده می شود.
برای مثال پروتکل های IP (Protocol Internet)وInternet، Protocol version 6 (IPv6) .
۲. packets update-Route: برای مطلع ساختن Router های همسایه از شبکه ها و IP های متصل شده به آنان مورد استفاده قرار می گیرد .
مثل Open Shortest : و Enhanced Interior Gateway Routing Protocol (EIGRP) ، RIPv2 ، Routing Information Protocol (RIP) . Path First (OSPF)



Data Link Layer

شامل حمل و نقل فیزیکی اطلاعات و کنترل topology network , notification error و control flow می باشد. یعنی این لایه اطلاعات را به bit تبدیل کرده و از رسیدن اطلاعات به آدرس فیزیکی واقع در LAN اطمینان حاصل می کند. این لایه اطلاعات را به قسمت های کوچکتر بنام frame data تبدیل کرده و یک header که شامل آدرس سخت افزاری مبداء و مقصد است را به آن اضافه می کند. شکل زیر نشان دهنده عملکرد این لایه بر اساس IEEE می باشد.



802.x نشان دهنده استاندارد مربوطه می باشد

Control Access Media(MAC): مشخص می کند که چگونه packet ها در سخت افزار قرار گرفته و خارج شوند. ضمناً آدرس فیزیکی کارت شبکه نیز می باشد.

Control Link Logical(LLC): وظیفه شناسایی لایه های شبکه در پروتکل مربوطه و encapsulate کردن اطلاعات را بر عهده دارد. در حقیقت مشخص می کند که وقتی یک frame می رسد لایه Link Data چه رفتاری با آن بکند.

Physical Layer

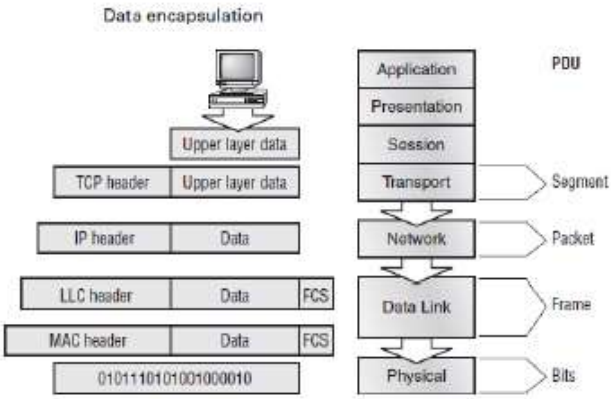
این لایه دو عمل مهم انجام میدهد

1. Send bits

2. Receive bits

Bit ها با مقدار ۰ و ۱ وارد و خارج می شوند. نحوه ارسال و دریافت این بیت ها در سخت افزار های مختلف فرق می کند (موج پالس و .....،)

نحوه Encapsulation



اتصالات شبکه ها

Coaxial

Twisted pair

Fiber optic

Coaxial Cable

این کابل ها از سیم مسی که با پلاستیک پوشیده شده اند تشکیل می شوند.

10Base-2عنوان با کهThin Ethernet نیز شناخته می شوند و از کابل coaxial استفاده می کنند. این کابل ها با عنوان ۵۸ RG-نیز شناخته می شوند. این کابل ها با connectorهای BNC به یکدیگر متصل می شوند.

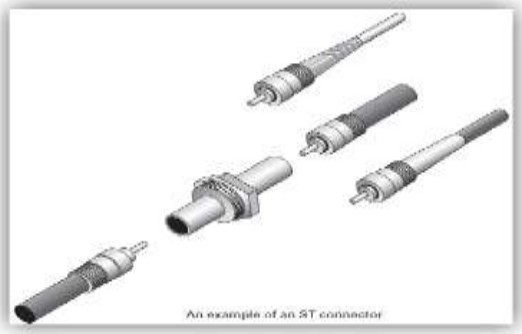
Twisted-Pair Cable

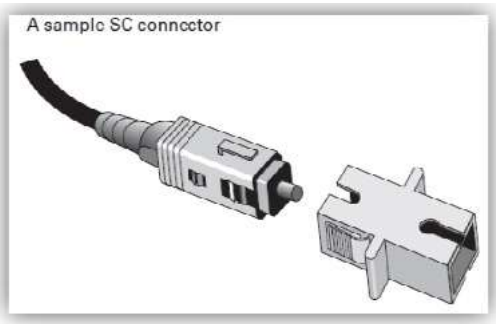
متشکل از چندین کابل که به یکدیگر پیچانده شده اند و با روکش پلاستیکی پوشانده شده اند. این کابل ها در شبکه های10Base-T 100Base-TX, 1000Base-TX مورد استفاده قرار می گیرند. نام این شبکه ها با فرمتx-<Signaling> k نوشته می شوند که درآن نشان دهنده سرعت و سیگنال است که با حالت Mbps نشان داده می شود و<signaling> مشخص کننده basebandیا broadband بوده و X نشان دهنده نوع کابل می باشد. برای مثال100base-x یعنی شبکه ای که سرعت آن ۱۰۰Mbps وx می تواند معانی مختلفی داشته باشد .T نیز می تواند به معنی جفت کابل های به هم تابیده شده مثلcat5، 5e و6utp باشد.

Fiber-Optic Cable

کابل های فیبر نوری از سیگنال های نوری بجای سیگنال های دیجیتالی استفاده می شود. این سیگنال های می توانند از طریق هسته ای شیشه ای یا پلاستیکی عبور کنند که کیفیت فیبرهای شیشه ای به مراتب بیشتر از پلاستیکی هابوده و البته قیمت آن نیز بیشتر است.این کابل ها در دونوع multimode fiber (MMF)وsingle-mode fiber (SMF) ارائه میشوند. تفاوت این دو در تعداد اشعه های قابل حمل توسط آنهاست از MMF . ها برای فواصل کوتاه و از SMF ها برای فواصل طولانی استفاده می شود. از مزایا و معایب این کابل هامیتوان به موارد زیر اشاره کرد:

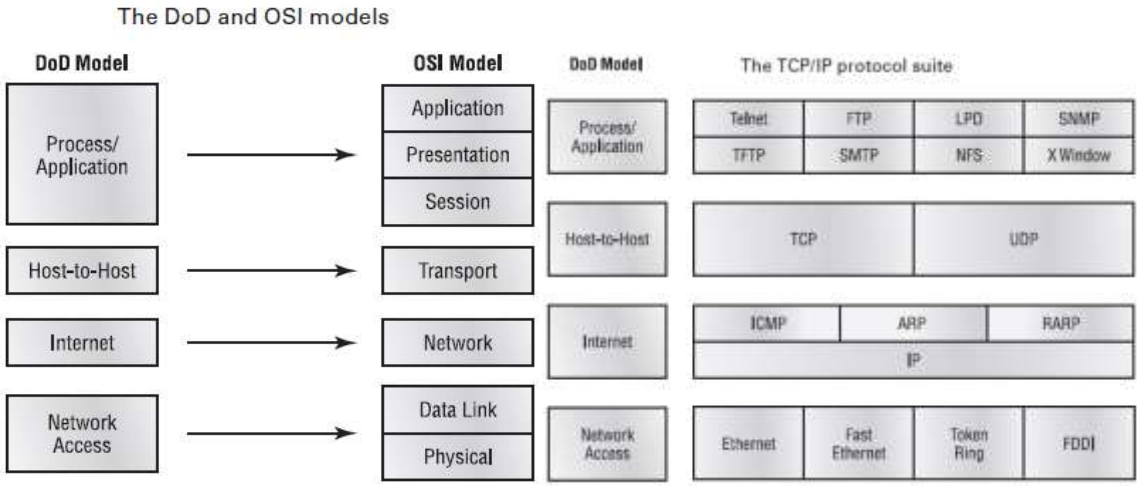
- در مقابل EMI و RFI مصون هستند
- میتواند تا ۴۰ کیلومتر یا ۲۵ مایل اطلاعات راtransmit کند
- راه اندازی آن سخت است
- نسبت به کابل هزینه بیشتری دارد
- Troubleshoot آنها سخت و گران است





TCP/IP

برای اولین بار در سال ۱۹۷۳ و به صورت دو پروتکل مجزا TCP و IP و در سال ۱۹۸۳ در قالب IP/TCP DOD (Department of Defense) . ارائه شد شرکت تولید کننده IP/TCP این پروتکل را در ۴ لایه تقسیم کرد که در OSI به ۷ لایه طبقه بندی شده بود.



The Process/Application Layer Protocols

Telnet

به user های Remote اجازه ارتباط و دسترسی به منابع را صادر می کند. کاربران با اجرای برنامه Client Telnet و ورود به Server Telnetارتباط را برقرار می کنندTelnet .هیچگونه امنیت یا encryption را پشتیبانی نمی کند

File Transfer Protocol (FTP)

FTPپروتکلی است که فایلها از این طریق Transfer می شوند. البته فقط یک پروتکل نیست و یک نرم افزار نیز است. دسترسی اولین قدم است و در مرحله بعدی باید عمل Authenticateانجام شود.

Secure File Transfer Protocol (SFTP)

FTPهمراه با encryption را گویند.

Trivial File Transfer Protocol (TFTP)

نوع ساده تری از FTP است که اگر آدرس دقیق منبع مورد نظر را داشته باشید مورد استفاده قرار می گیرد. بااین پروتکل نمی توانید Browsing Directoryانجام دهید. امنیت تعریف نشده است و فایلهای با حجم کوچک را می توان با این پروتکل Transfer کرد.

Network File System (NFS)

شرایط برقراری ارتباط بین دو سیستم عامل مختلف را برقرار می کند. برای مثال یک طرف NT و طرف دیگر UNIX

Simple Mail Transfer Protocol (SMTP)

برای ارسال ایمیل استفاده می شود.

Post Office Protocol (POP)

برای دریافت ایمیل مورد استفاده قرار می گیرد . آخرین نسخه این پروتکل POP3 نام دارد.

Internet Message Access Protocol, Version 4 (IMAP4)

دارای امنیت و انتخاب های بیشتری در مورد نحوه تبادل ایمیل ها دارد. می توانید انتخاب کنید که قسمتی از ایمیل را دریافت کنید (مثلاً Header) یا کل آن را. در صورتی که در دو پروتکل قبلی تمام ایمیل ارسال و دریافت می شود. همچنین این پروتکل امکان searchبین تمام یا قسمتی از ایمیل را می دهد. امنیت این پروتکل نیز بیشتر است(Kerberos) .

Transport Layer Security (TLS)

هم TLS و هم SSL برای ایجاد امنیت در تبادل اطلاعات بصورت آنلاین مورد استفاده قرار می گیرند.

SIP (VoIP)

Protocol Initiation Session(SIP)پروتکلی بسیار قوی برای شکل دهی و برقراری ارتباطات Multimedia مثل , Voice ,Video conferencing , Messaging Instant ,video و Games Online می باشد

RTP (VoIP)

Real-time Transport Protocol (RTP) اعمالی از قبیل vedio conferencing و push to talk system را انجام می دهدو بطور کل voice over ip

Line Printer Daemon (LPD)

برای Sharing Printer طراحی شده است.

X Window

برای برنامه هایی که به حالت interface user graphical(GUI) در دو طرف مورد استفاده قرار می گیرند طراحی شده است

Simple Network Management Protocol (SNMP)

وظیفه monitoring شبکه را بر عهدا دارد . بصورتی که Admin را از تمامی اتفاقات در شبکه مطلع می کند و اطلاعات شبکه را جمع آوری می کند.

Secure Shell (SSH)

یک ارتباط امن Telnet از طریق IP/TCP برقرار می کند. ازاین طریق می توان به یک سیستم Remote ، login کرده برنامه ای را اجرا و فایل هایی را ارسال و دریافت کرد.

Hypertext Transfer Protocol (HTTP)

با استفاده از این پروتکل می توان text ، Imageو لینک ها را در Browser تبدیل کرد. در کلام کلی برای برقراری ارتباط بین Browserو server-web مورد استفاده قرار می گیرد

Hypertext Transfer Protocol Secure (HTTPS)

به نسخه Secure پروتکل HTTP اطلاق می شود.

Network Time Protocol (NTP)

برای Synchronize ساعت بین شبکه ها مورد استفاده قرار می گیرد. شاید ساده به نظر بیاید اما اکثر ارتباطات در حال حاضر به صورت time – or date -stamped هستند.

Network News Transfer Protocol (NNTP)

برنامه های Reader News از این فناوری برای مطلع ساختن Client هایشان استفاده می کنند.(search engine)

Secure Copy Protocol (SCP)

FTPراهی بسار ساده برای تبادل اطلاعات است اما امن نیست. چرا که Information Account ها به همراه خود فایلها و بصورت clearفرستاده و در نتیجه encrypt نمی شوند .این پروتکل رسیدن اطلاعات به مقصد بصورت امن را تظمین می کند

Lightweight Directory Access Protocol (LDAP)

Clientها به این صورت با Directory Active مرتبط می شوند و می بینند. البته نحوه برقراری ارتباط و تعیین روش ها نیز توسط این پروتکل استفاده می شود.

Internet Group Management Protocol (IGMP)

برای مدیریت ip multicast sessionsها استفاده می شود

Line Printer Remote (LPR)

پروتکلی است که در هر دو طرف clientو printer نصب می شود. این پروتکل job print ها را از client دریافت و تا اتمام عملprintآن را پیگیری می کند.

Domain Name Service (DNS)

عمل Resolution Name را انجام می دهد

Dynamic Host Configuration Protocol (DHCP)

IP Address assigning

Transmission Control Protocol (TCP)

حجم بزرگی از اطلاعات را از برنامه ها دریافت و آنها را بهsegmentهای کوچکتر تقسیم می کند.

User Datagram Protocol (UDP)

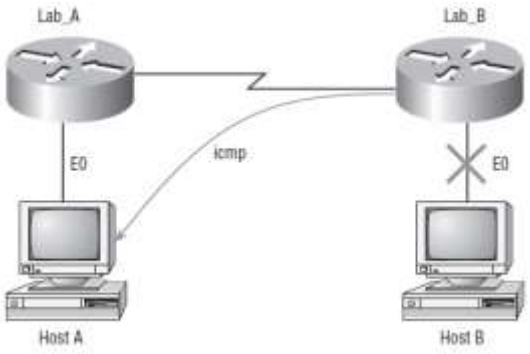
نسبت به IP/TCP دارای ضعف های زیادی است در تعریف کلی UDF داده های با حجم کم را می تواند برای تبادل بر عهده بگیرد و از لحاظ امنیتی نیز مزیتی ندارد.

Internet Protocol (IP)

IPیک تصویر کلی از اطلاعات است. یعنی تمامی سیستم هایی که دارای Address IP می باشند از این طریق اقدام به برقراری ارتباط می کنند. این پروتکل ابتدا IP مقصد را چک کرده سپس با استفاده از جدول Routing آن را به طرف مقصد راهنمایی می کند. بطور کلی ابتدا با در نظر گرفتن آدرس شبکه ، شبکه مقصد را یافته و سپس با استفاده از آدرس سخت افزاری Address MAC، packetرا به مقصد نهایی می فرستد.

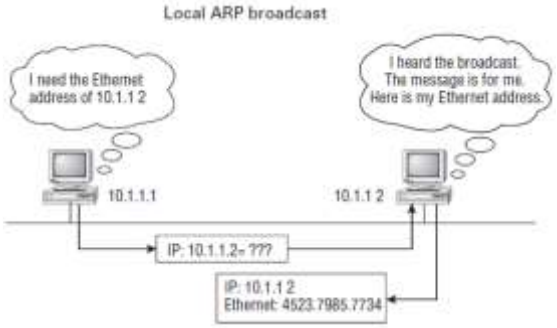
Internet Control Message Protocol (ICMP)

Network layer و IP برای سرویس دهی استفاده می کند. وظیفه این پروتکل جمع آوری و گزارش مشکلات شبکه می باشد. برای مثال اگر Router به هر دلیلی نتواند با یک IPارتباط برقرار کند ، از این پروتکل برای فرستادن گزارش Unreachable Destinationبه مبداء استفاده می کند. اگر buffer receiving در router گیرنده پر باشد از این پروتکل برای ارسال پیام Full Bufferاستفاده می کند.



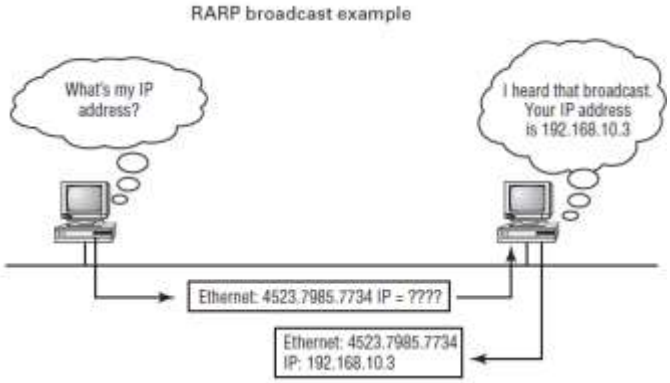
Address Resolution Protocol (ARP)

از یک IP آدرس Address MAC آن را بدست می آورد. این پروتکل از طریق broadcast این اطلاعات را جمع آوری می کند.



Reverse Address Resolution Protocol (RARP)

سیستم هایی که بصورت (diskless بدون دیسک) هستند و برای ذخیره IP مکانی ندارند اما از Address MAC خود مطلع اند از طریق RARP ، IPخود را به دیگران معرفی می کنند.



Proxy Address Resolution Protocol (Proxy ARP)

در یک شبکه نمی توان بیشتر از یک Gateway Defualt داشت . این پروتکل بدون معرفی کردن یک آدرس خاص این وظیفه را بر عهده می گیرد .

برای اینکه به استانداردی در خصوص Network و Host برسند ، تصمیم گرفتند که کلاس دسته بندی های مشخصی را برای آدرس های IP در نظر بگیرند .

Class A

NETWORK	HOST		
1 TO 126	X	X	X

Class B

NETWORK		HOST	
128 TO 191	X	X	X

Class C

NETWORK			HOST
192 TO 223	X	X	X

هدف از این دسته بندی این بود که مشخص شود دو آدرس IP از یک خانواده (در یک شبکه اند) یا خیر.

سوال) آیا آدرس های 80.83.26.70 و 80.81.25.32 در یک شبکه قرار دارند ؟

جواب) ابتدا نگاه می کنیم که این آدرس ها عضو کدام کلاس می باشند . چون می خواهیم بخش Network را از Host جدا کنیم. هر دو آدرس ، کلاس A می باشند بنابراین:

NETWORK	HOST
80.	81.25.32

NETWORK	HOST
80.	83.26.70

حالا باید ببینیم آیا قسمت Network یکسان است ؟

بله ، هر دو ۸۰ است ، پس دو آدرس فوق داخل یک شبکه می باشند.

سوال) آیا آدرس ها 130.42.39.50 و130.41.35.50 در یک شبکه قرار دارند ؟

جواب) ابتدا نگاه می کنیم که این آدرس ها عضو کدام کلاس می باشند ، چون می خواهیم بخش Network را از Host جدا کنیم. هر دو آدرس ، Class B می باشند بنا بر این

NETWORK	HOST
130.42.	39.50

NETWORK	HOST
130.41.	35.50

حالا باید ببینیم آیا قسمت Network یکسان است ؟

خیر، پس دو آدرس فوق داخل یک شبکه قرار ندارند.

سوال) آیا آدرس ها 190.25.35.42و 190.25.30.48 در یک شبکه قرار دارند ؟

جواب) ابتدا نگاه می کنیم که این آدرس ها عضو کدام کلاس می باشند ، چون می خواهیم بخش Network را از Host جدا کنیم. هر دو آدرس ،Class B می باشند. بنا بر این:

NETWORK	HOST
190.25.	30.48

NETWORK	HOST
190.25.	35.42

حالا باید ببینیم آیا قسمت Network یکسان است ؟

بله هر دو ۱۹۰,۲۵ است.پس دو آدرس فوق داخل یک شبکه می باشند.

سوال) آیا آدرس های 220.34.32.48 و 220.34.30.42 در یک شبکه قرار دارند ؟

جواب) ابتدا نگاه می کنیم که این آدرسها عضو کدام کلاس می باشند ، چون می خواهیم بخش Network را از Host جدا کنیم. هر دو آدرس ، Class C می باشند. بنا براین:

NETWORK	HOST
220.34.30.	42
NETWORK	HOST
220.34.32.	48

حالا باید ببینیم آیا قسمت Network یکسان است ؟

خیر ، پس دو آدرس فوق داخل یک شبکه قرار ندارند.

سوال) آیا آدرس های 200.42.50.30 و200.42.50.102 در یک شبکه قرار دارند ؟

جواب) ابتدا نگاه می کنیم که این آدرسها عضو کدام کلاس می باشند ، چون می خواهیم بخش Network را از Host جدا کنیم.
هر دو آدرس ، Class C می باشند بنا براین:

NETWORK	HOST
200.42.50.	102

NETWORK	HOST
200.42.50.	3

حالا باید ببینیم آیا قسمت NETWORK یکسان است؟

بله،هر دو ۲۰۰,۴۲,۵۰ است . پس دو آدرس فوق داخل یک شبکه می باشند.

تبدیل اعداد دسیمال به باینری و بلعکس

برای اینکه بتوانیم یک آدرس IP را تحلیل کنیم و یا در جلوتر Subnet کنیم ، بایستی یاد بگیریم که با اعداد باینری کار کنیم.
هر قسمت از چهار قسمت دسیمال آدرس IP را به یک عدد ۸ بیتی باینری تبدیل خواهیم نمود.

و آن را در بیت های ۰ تا ۷ قرار خواهیم داد

بیت۷	بیت۶	بیت۵	بیت۴	بیت۳	بیت۲	بیت ۱	بیت۰

دو را به توان شماره هر بیت برسانید و مقدار عددی آن را یادداشت کنید :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
دو به توان۷	دو به توان٦	دو به توان٥	دو به توان٤	دو به توان۳	دو به توان۲	دو به توان۱	دو به توان۰
بیت۷	بیت۶	بیت۵	بیت۴	بیت۳	بیت۲	بیت۱	بیت۰

حالا وقتی می خواهیم یک عدد دسیمال را به باینری تبدیل کنیم ، عدد را بصورت متوالی به مقادیر بالا ، از چپ به راست ، کسر

می کنیم. در صورتیکه مقادیر توانی دو قابلیت کسر شدن از عدد باقیمانده را داشت ، در جدول مربوطه عدد یک و اگر نداشت عدد صفر را قرار می دهیم. برای اینکه درک بهتری داشته باشیم عدد ۲۴۹ را به باینری تبدیل می کنیم :

مرحله اول)

249 -128 = 121

بنابراین ۱۲۸ در ۲۴۹ وجود دارد. بنا بر این :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
۱							

مرحله دوم)

121 - 64 = 37

بنابراین ۶۴ داخل ۱۲۱ وجود دارد پس :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
۱	۱						

مرحله سوم)

57 -32 = 25

بنابراین ۳۲ داخل ۵۷ وجود دارد پس :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
۱	۱	۱					

مرحله چهارم)

25 - 16 = 9

بنابراین ۱۶ داخل ۲۵ وجود دارد پس :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
۱	۱	۱	۱				

مرحله پنجم)

9 - 8 = 1

بنابراین ۸ داخل ۹ وجود دارد پس :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
۱	۱	۱	۱	۱			

مرحله ششم)

1-4 = ERROR

بنابر این ۴ داخل ۱وجود دارد پس :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
۱	۱	۱	۱	۱	۰		

مرحله هفتم)

1-2 = ERROR

بنابراین ۲ داخل ا وجود دارد پس :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
۱	۱	۱	۱	۱	۰	۰	

مرحله آخر

1-1 = 0

بنابراین ا داخل ا وجود دارد پس :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
۱	۱	۱	۱	۱	۰	۰	۱

به عبارتی عدد دسیمال ۲۴۹ به باینری می شود : ۱۱۱۱۱۰۰۱

تمرین) عدد دسیمال ۶۳ را به باینری تبدیل کنید.

مرحله اول)

63 - 128 = ERROR

بنابراین ۱۲۸ در ۶۲ وجود ندارد. بنا بر این :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
۰							

مرحله دوم)

63-64 = ERROR

بنابراین ۶۴ داخل ۶۳ وجود دارد پس :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
۰	۰						

مرحله سوم)

63 -32 = 31

بنابراین ۳۲ داخل ۶۳ وجود دارد پس :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
۰	۰	۱					

مرحله چهارم)

31- 16 = 15

بنابراین ۱۶ داخل ۳۱ وجود دارد پس :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
۰	۰	۱	۱				

مرحله پنجم)

15 - 8 = 7

بنابراین ۸ داخل ۱۵ وجود دارد پس :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
۰	۰	۱	۱	۱			

مرحله ششم)

7- 4 = 3

بنابراین ۴ داخل ۷ وجود دارد پس :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
۰	۰	۱	۱	۱	۱		

مرحله هفتم)

3 - 2 = 1

بنابراین ۲ داخل ۳ وجود دارد. پس :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
۰	۰	۱	۱	۱	۱	۱	

مرحله آخر)

1- 1 = 0

بنابراین ۱داخل ا وجود دارد پس :

۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
۰	۰	۱	۱	۱	۱	۱	۱

به عبارتی عدد دسیمال ۶۳ به باینری می شود :۰۰۱۱۱۱۱۱

Network ID & Broadcast address

هر Range آدرس IP داخل یک شبکه واحد ، مجموعه ای از یک سری آدرس IP است که همگی داخل آن شبکه اند . از این مجموعه ، دو آدرس منحصر به فرد وجود دارد؛

Network ID : که مشخصه و معرف آن شبکه است.

Broadcast address که برای دسترسی به همه نود های آن شبکه استفاده می شود.

این دو آدرس را نمی توان به عنوان آدرس معتبر، به نود ها اختصاص داد.

برای محاسبه NetID تمام بیت های Host را صفر می کنیم.

و برای دسترسی به Broadcast address تمام بیت های Host را یک می کنیم.

مثال) NetID و Broadcast address شبکهای که آدرس IP 80.32.51.60 در آن وجود دارد را پیدا کنید.

ابتدا نگاه می کنیم که این آدرس ها عضو کدام کلاس می باشند ، چون می خواهیم بخش Network را از Host جدا کنیم.

این آدرس متعلق به Class A است . بنا بر این :

NETWORK	HOST
80.	32.51.60

اگر آدرس را بصورت باینری بنویسیم خواهیم داشت :

NETWORK	HOST
01010000	00100000.00110011.001111100

حال برای اینکه NET ID را به دست آوریم،تمام بیت های HOST را صفر می کنیم.

NETWORK	HOST
01010000	00000000.00000000.00000000

پس NET ID می شود : 80.0.0.0

برای بدست آوردن آدرس Broadcast همه بیت های Host را یک می کنیم

NETWORK	HOST
01010000	11111111.11111111.11111111

پس Broadcast address می شود : 80.255.255.255

چون این دو آدرس را نمی توانیم به تود ها اختصاص دهیم ، بنابر این اولین آدرس قابل استفاده می شود یکی بالاتر از NetID به

عبارتی :

NETWORK	HOST
01010000	00000000.00000000.00000001

اولین آدرس این شبکه می شود :80.0.0.1

آخرین آدرس شبکه نیز می شود یکی مانده به آدرس Broadcast یعنی :

NETWORK	HOST
01010000	11111111.11111111.11111110

آخرین آدرس قابل استفاده در این شبکه می شود : 80.255.255.254

بنا براین وقتی می خواهیم تعداد آدرسهای قابل استفاده در یک شبکه را حساب کنیم از فرمول

$$2^n-2$$

استفاده می کنیم که h در آن،تعداد بیت های host می باشد.

تمرین) شبکه ای که آدرس IP 201.202.32.40 در آن وجود دارد را تحلیل کنید:

ابتدا نگاه می کنیم که این آدرسها عضو کدام کلاس می باشند ، چون می خواهیم بخش Network را از Host جدا کنیم.

این آدرس متعلق به Class C است . بنا بر این :

NETWORK	HOST
201.202.32.	40

اگر آدرس را بصورت باینری بنویسیم خواهیم داشت :

NETWORK	HOST
11001001.11001010.00100000	00101000

حالا برای اینکه NetIDرا بدست آوریم ، تمام بیت های Host را صفر می کنیم.

NETWORK	HOST
11001001.11001010.00100000	00000000

پس NetID می شود : 201.202.32.0

برای بدست آوردن آدرس Broadcast همه بیت های Host را یک می کنیم.

NETWORK	HOST
11001001.11001010.00100000	11111111

پس Broadcast address می شود : 201.202.32.255

چون این دو آدرس را نمی توانیم به نود ها اختصاص دهیم ، بنابر این اولین آدرس قابل استفاده می شود یکی بالاتر از NET ID به عبارتی :

NETWORK	HOST
11001001.11001010.00100000	00000001

اولین آدرس این شبکه می شود :201.202.32.1

آخرین آدرس شبکه نیز می شود یکی مانده به آدرس Broadcast یعنی :

NETWORK	HOST
11001001.11001010.00100000	11111110

آخرین آدرس قابل استفاده در این شبکه می شود : 201.202.32.254

تعداد آدرس IP قابل استفاده در شبکه :2-(8^2)

می شود ۲۵۴ آدرس IP

وقتی از شما می خواهند که شبکه ای را تحلیل کنید ، بایستی موارد زیر را حساب کنید ؛

class	**c**
Network id	**201.202.32.0**
First ip address	**201.202.32.1**
Last ip address	**201.202.32.254**
Broadcast address	**201.202.32.255**
Number of Available IP addresses	**254**

تمرین) شبکه ای که آدرس IP 130.64.33.25 در آن وجود دارد را تحلیل کنید.

ابتدا نگاه می کنیم که این آدرسها عضو کدام کلاس می باشند ، چون می خواهیم بخش Network را از Host جدا کنیم.

این آدرس متعلق به Class B است . بنا بر این :

NETWORK	HOST
130.64.	33.25

لزومی ندارد قسمت Network را نیز به باینری تبدیل کنیم ، پس اگر آدرس را بصورت باینری بنویسیم خواهیم داشت:

NETWORK	HOST
130.64.	0010001.00011001

حالا برای اینکه NetIDرا بدست آوریم ، تمام بیت های Host را صفر می کنیم.

NETWORK	HOST
130.64.	00000000.00000000

پس NetID می شود : 130.64.0.0

برای بدست آوردن آدرس Broadcast همه بیت های Host را یک می کنیم.

NETWORK	HOST
130.64.	11111111.11111111

پس broadcast address می شود: 130.64.255.255

چون این دو آدرس را نمی توان به نود ها اختصاص دهیم ،بنابراین اولین آدرس قابل استفاده می شود یکی بالاتر از NET ID به عبارتی :

NETWORK	HOST
130.64.	00000000.00000001

اولین آدرس این شبکه می شود : 130.64.0.1

آخرین آدرس شبکه نیز می شود یکی مانده به آدرس Broadcast یعنی :

NETWORK	HOST
130.64.	11111111.11111110

آخرین آدرس قابل استفاده در این شبکه می شود : 130.64.255.254

تعداد آدرس IP قابل استفاده در شبکه: 2- (2^16)

می شود ۶۵۵۳۴ آدرس IP

وقتی از شما بخواهند که شبکه ای را تحلیل کنید بایستی موارد زیر را محاسبه کنید

class	**B**
Network id	**130.64.0.0**
First ip address	**130.64.0.1**
Last ip address	**130.64.255.254**
Broadcast address	**130.64.255.255**
Number of Available IP addresses	**65534**

Subnet Mask

آموختیم که چگونه می توانیم بفهیم دو آدرس IP متعلق به یک شبکه اند یا خیر. کامپیوتر برای اینکه این موضوع را بفهمد از مفهومی به نام Subnet Mask استفاده می کند. به این صورت که تمام بیت های Network را یک و تمام بیت های Host را صفر در نظر می گیرد تا Subnet mask را بسازد. سپس Subnet Mask را در آدرس Boolean IP AND می کند.

Boolean AND :

1AND 0 = 0

0 AND 1=0

0 AND 0 = 0

1And 1=1

به عبارتی :

SUBNET MASK برای کلاس A

11111111.00000000.00000000.00000000

255.0.0.0

SUBNET MASK برای کلاس B

11111111.11111111.00000000.00000000

255.255.0.0

SUBNET MASK برای کلاس C

11111111.11111111.11111111.0

255.255.255.0

انواع روش هايCommunication

Unicast: packetهای فرستاده شده به یک آدرس فقط به یک interface فرستاده می شوند. برای منظور Balancing Load چند interface از یک آدرس استفاده می کنند

addresses unicast Global: آدرس های عادی قابل Router همانند آدرس های IPv4 در گذشته.

addresses local-Link: معادل address Private ها در IPv4 می باشند. برای استفاده های Local و راه اندازی شبکه های کوچک استفاده می شود

addresses local Unique: آدرس های unique غیر قابل Route می باشند که با هیچ آدرس دیگری overlap نخواهد شد

Multicast: به آدرس های multicast که چند سیستم بصورت همزمان استفاده می کنند اطلاق می شود که با عنوان-many to-oneنیز شناخته می شود. شناسایی این آدرس ها در IPv6 سخت نیست زیرا همه آنها با FF شروع می شوند.

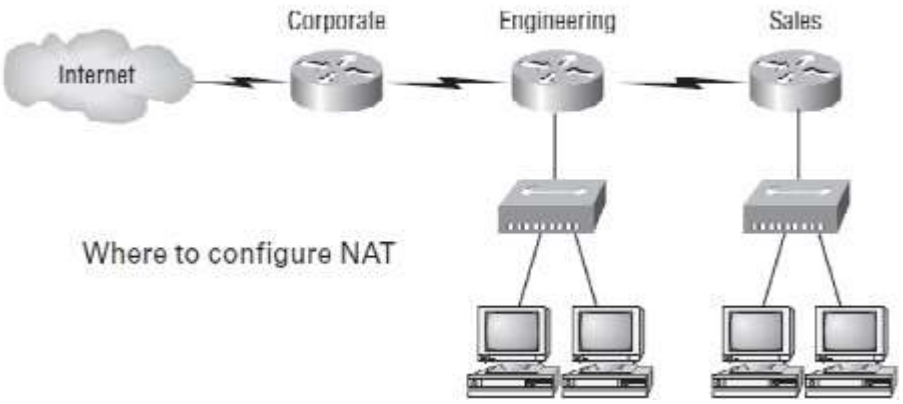
Anycast: مشخص کننده interfaces Multiple است با این تفاوت که به اولین آدرس IPv6 رسیده و در بین بقیه سیستم ها پخش می شود به اصطلاح one-to-one-of- many یا anycast خوانده می شوند) .

(Network Address Translation) NAT

بااستفاده ازNATمی‌توان‌یک‌یاچندValid IPرابه‌تعدادزیادی از clientهایی‌که‌دارایValid IP نیستند به‌اشتراک‌گذاشت درنتیجه‌اینclientهادراینترنت باهمانValid IPهاظاهرخواهندشد.

در حال حاضر NAT باعث کاهش استفاده از IP های Valid در شبکه هاشده است از NAT می توان در موارد زیر استفاده کرد :

- ISP خودراعوض‌کرده اید ومایل‌نیستید که‌تمامIPهایClient هارا دوباره‌عوض‌کنید
- می‌خواهیدبه‌اینترنت متصل‌شویدوclientهای‌شمادارایValid IPنیستند.
- لازم است‌شبکه‌رابایک‌شبکه‌دیگرکه‌دارای‌همانIPهای‌شبکه‌شماهستند،Merge (ادغام) کنید.



این‌روش دارای‌معایبی‌نیزهست.

جدول زیرمزایا ومعایب‌این‌سیستم رابازگومی‌کند :

Advantages and Disadvantages of Implementing NAT

Advantages	Disadvantages
Conserves legally registered addresses	Translation introduces switching path delays
Reduces address overlap occurrences	Loss of end-to-end IP traceability
Increases flexibility when connecting to the Internet	Certain applications will not function with NAT enabled
Eliminates address renumbering as the network changes	

انواعNAT :

(Static NAT (SNAT : one-to-one maping رابین Local وGlobal آدرس‌ها فراهم می‌کند. دراین‌شرایط بایدهرhostدرشبکه‌تان دارای یکValid IPباشد.

Dynamic NAT : اجازه map شدن‌یک‌آدرسValidرابه‌یک آدرس invalid صادرمی‌کند. لازم نیستRouter را مثل‌حالت قبل برای تمام آدرس‌های inside وoutside بصورت دستی‌تنظیم کنید. اما بایدبه تعدادکافی‌آدرسValid برایclient های‌که‌می‌خواهند اقدام به ارسال و دریافت اطلاعات از اینترنت نمایند داشته‌باشید.

Overloading: متداول‌ترین‌حالت استفاده ازNAT است شبیه حالتDynamicNAT است با این‌تفاوت‌که در این روش تمام آدرس‌هایInvalid به‌یک map،ValidIPخواهند شد با استفاده ازport های مختلف. یعنیMANY-TO-ONE دلیل استفاده زیاد از این روش این است که می‌توان هزاران invalid IP را به یک Valid IPمتصل‌کردکه به (PAT (Port Address Translation نیز معروف است .

NAT Names

چنداصطلاح رابه‌خاطربسپارید :

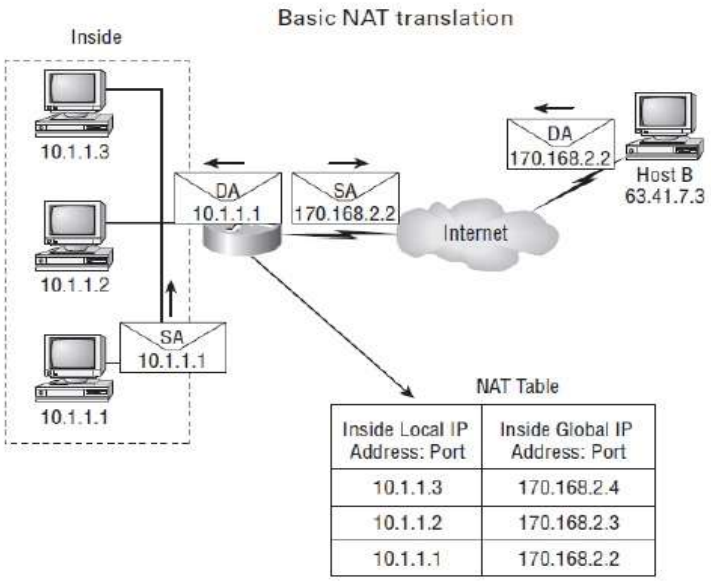
Global Addresses : این‌آدرس‌ها را بعد ازNAT Translation استفاده می‌کنیم

Local Addresses : این‌آدرس‌ها را قبل‌ازNAT Translation استفاده می‌کنیم

Inside Global: نام یک host در داخل شبکه بعد ازNAT Translation

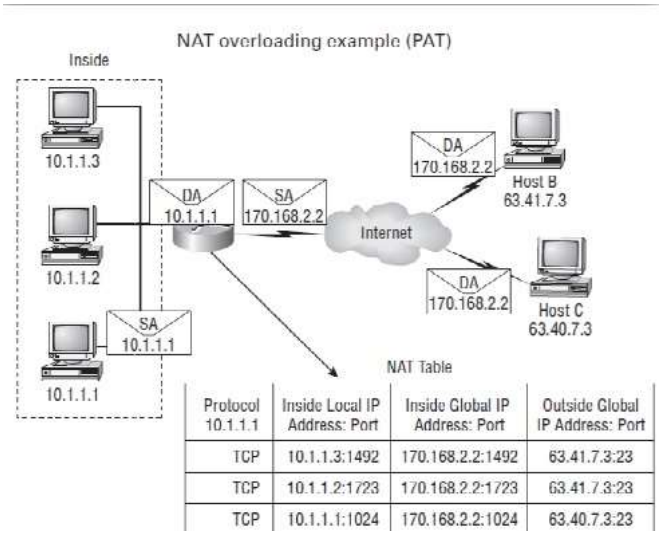
Outside Global: نام‌یک host درخارج از شبکه بعد ازNAT Translation

نحوه‌عملکردNAT



درشکل‌بالاسیستم۱۰،۱،۱،۱یک packet را به‌Routerکه‌NATروی آن‌تنظیم‌شده است می‌فرستد. Router این‌سیستم‌رابه عنوان‌یکinside localکه‌می‌خواهد با خارج ازشبکه ارتباط برقرارکند شناسایی‌می‌کند. آدرس آن راTranslate کرده و در جدولNAT ذخیره می‌کند. Packet به interface خارجیRouter با آدرس Translate.source شده فرستاده می‌شود. External host نیز یکpacket را به همین سیستم داخل NAT می‌فرستد، Router ابتدا آن را دریافت‌کرده و با استفاده از NAT Table به host داخلی (inside global) می‌رساند.

درزیرمثالی‌ازحالت‌پیچیده‌ترPATرامشاهده‌می‌کنید:



gatewayدر شبکه چیست و چه کاری انجام می دهد؟

gatewayدر تنظیمات کارت شبکه سیستم ها یعنی دروازه ورودی

همان طور که از اسمش پیداست کارش اتصال بین دو شبکه است و اغلب از آن بعنوان یک درگاه یاد می شود

Default Gateway اگر نمی خواهیم با کامپیوتر های دیگر در شبکه های دیگر ارتباط داشته باشیم، نیازی نیست که آدرس default gateway تنظیم کنیم

Default Gatewayسیستم یا سروری که ازطریق اون میشه به اینترنت متصل شد،مثلا ISP یک Gatewa به حساب میاد اگر در شبکه ای سیستمی به اینترنت متصل است و اینترنت را به اشتراک گذاشته کاربرانی که میخواهند از اینترنت استفاده کنند بایستی Default Gateway خود را IP آن سیستمی قرار دهند که به اینترنت متصل است تا بتوانند از اینترنت استفاده کنند.

هر شبکه ای که با شبکه های خارجی یا شبکه ی remote در ارتباط هست باید یک پل رابط بین این شبکه ها باشد

مثال: میخواهیم از شبکه ی یک شرکت ایرانی به شبکه ی یک شرکت موجود در آمریکا متصل شویم آیا بین ما کابلی هست؟

امکان نداره که از کابل بتوانیم استفاده کنیم

پس چیکار میکنیم از gateway استفاده میکنیم

باید gateway شبکه ی ما با gateway شبکه ی خارجی هم رنج باشد

gateway شماره ی هست که توسط DNS به صورت Unique (یکتا) در اختیار این نوع سازمانها قرار میگیرد.

بنابراین اگر آدرس default gateway نداشته باشد ، شما نمی توانید به کامپیوتر های دیگر که خارج از شبکه شما هستند ، متصل شوید مگر اینکه از Proxy Server استفاده کنید.

DNSچیست؟

DNS به معنای سیستم نام دامنه که از واژه های Domain Name System گرفته شده در واقع پروتکلی است که چارچوبی را برای گشت و گذار در وب فراهم می کند.

هر وب سایتی یک نام دارد و یک IP آدرس که اولی به هاست (میزبان) معروف است مثلا WWW.IDHCO.COM و دومی یک آدرس عددی است مثل ۱۹۲,۱۶۸,۸,۱

گفتیم DNS مخف Domain Name System است، سیستمی کامپیوتری که زیرساخت لازم برای چرخیدن در پهنه جهانی وب World Wide Webیا همان WWW خومان را فراهم میسازد.

در تعریف ساده آن، سیستم نام دامنه، مجموعه ای از سرورهای ریشه است که در واقع آدرس IP پروتکل اینترنت (Internet Protocol)های سرورهای DNS در آن قرار داشته و به تمام دامنه هایی که در اینترنت ثبت شده اند، دسترسی دارد.

نقش IP چیست و DNS چه کاربردی در این میان دارد؟

تعریف DNS کاربردDNS به زبان ساده بسیاری از مردم نمی دانند که سرور های اینترنتی تنها می توانند با یک آدرس عددی آدرس IP آدرس دهی شوند

نقش کلیدی DNS server names در ترجمه نام دامنه به آدرس های IP است.

با خرید دامنه و ثبت هر وبسایتی در واقع اطلاعات مربوط به آن در مجموعه سرور های ریشه ذخیره میشود.

نقش سرورهای نام DNS که توسط شرکت میزبان (host) شما نگهداری می شود، پاسخ دادن به جست و جو برای یک نام دامنه خاص با محل دقیق در سرور دقیق میزبانی وب با استفاده از آدرس IP سرور میباشد که در آن نام دامنه و بنابراین نام وب سایت، واقع شده است.

نقش سرورهای ریشه که سیستم نام دامنه (DNS) وب جهان (WWW) را تشکیل می دهند، فرستادن ISP و به تبع آن ارسال مرورگر وب به سرور صحیح دی ان اس است.

با استفاده از این سیستم، کاربران وب فقط باید نام دامنه تان را برای پیدا کردن وب سایت شما بدانند

برای آنها مهم نیست که آدرس IP برای سرور فردی که سایت شما در آن قرار دارد چیست؟

اگر شما، مثلا، سایت خود را به یک سرور بهتر ارتقا دهید، DNSبه روزرسانی میشود تا به آدرس IP سرور جدیدتان مربوط شود. اما بازدیدکنندگان شما هنوز تنها با استفاده از نام دامنه شما از سایت شما بازدید می کنند. یعنی حتی اگر آدرس IP شما تغییر کند، همه چیز برای آنها شفاف و مشخص است.

در دنیای دات کام، این نوع انعطاف پذیری بسیار مهم است.

حال یکبار ببینیم چه اتفاقی میافتد:

من برای استفاده از وب، وارد سیستم ارائه دهنده سرویس اینترنت ISP یا Internet Service Provider می شوم.

نرم افزار مرور وب خود را مثلا اینترنت اکسپلورر یا Google Chrome باز میکنم و در نوار آدرس http://www.idhco.com را وارد میکنم.

کامپیوتر من از سرور (های) DNS مربوط به ISP من درخصوص آدرس آی پی www.idhco.com میپرسد.

تجهیزات ISP من ابتدا حافظه cache خود را بررسی می کند تا متوجه شود آیا اخیرا درخواستی برای این آدرس را بررسی کرده یا نه.

اگر این کار را قبلا نکرده باشد، تجهیزات ISP من با مجموعه سرور های ریشه که سیستم نام دامنه (دی ان اس) را تشکیل می دهند برای پیدا کردن آن سرور DNS ای که آدرس IP نام دامنه را در خود نگه می دارد ارتباط برقرار میکند.

تجهیزات ISP من آدرس ارائه شده را گرفته و درخواستی را به سرور معتبر DNS برای آن دامنه می فرستد.

سرور معتبر DNS با آدرس IP سرور مورد نظر پاسخ می دهد.

تجهیزات ISP من، حافظه cache خود را با آن آدرس به روز می کند تا درخواست های آینده را بدون طی کردن مراحل فوق پاسخ دهد.

تجهیزات ISP من به کامپیوترم با آدرس آی پی سروری که من دنبال آن هستم پاسخ می دهد.

کامپیوتر من حافظه پنهان خود را به روز می کند به طوری که نیازی به جست و جو کردن آدرس برای مدت زمان زیاد نیست.

کامپیوتر من آدرس را به مرورگرش می فرستد، که یک اتصال به سرور با استفاده از آدرس IP مشخص شده باز می شود و اولین صفحه را از سایت درخواستی من بازیابی میشود.مرورگر من صفحه درخواست شده را روی صفحه نمایشم نشان می دهد.اما آیا این تمام کاربرد DNS است ؟

مطمئنا خیر!

وظیفه DNS تنها تبدیل Host Name به IP Address و برعکس نیست.

به لحاظ کاملا کاربردی، هر برنامه ای که از اینترنت برای اتصال دو یا چند هاست به منظور به اشتراک گذاشتن اطلاعات یا برقراری ارتباط استفاده می کند، به استفاده از سرویس های DNS متکی است.

اپلیکیشن هایی که از سرور های DNS استفاده میکنند عبارتند از:

(World Wide Web) WWW

E-mail

دیگر اپ ها مانندinstant messaging

از مورد دوم میتوان دریافت سرور های DNS قادر به ذخیره سوابق نیز هستند.

برای نمونه ایجاد ایمیل آدرس های با هاست جدید مثلا example@idhco.com دقیقا به همین کاربرد DNS برمیگردد.

فراتر از وب و ایمیل، برنامه های بسیاری هستند که وابسته ی خدمات دی ان اس هستند.

این وابستگی می تواند مربوط به پایگاه های داده، برنامه های کاربردی وب ساخته شده با استفاده از middleware یا سرور برنامه، برنامه های اشتراک گذاری، پیام های فوری و بازی های چند نفره باشد

فایروال

فایروال به دو نوع نرم افزاری و سخت افزاری موجود است. فایروال بررسی بسته های ورودی و خروجی بر اساس رول های تعریف شده برای آنرا بر عهده دارد. از دیواره آتش می توان برای اهداف مختلفی بهره برد. از یک کامپیوتر عادی گرفته تا بزرگترین شبکه ها با فایروال در ارتباط هستند.

فایروال چیست

فایروال ابزاری است که توسط آن می توان یک سیستم و شبکه را در مقابل تهدیدات امنیتی و مخرب شامل دسترسی های غیر مجاز ، نفوذ و تخریب و مخصوصا تکذیب سرویس محافظت کرد. علاوه بر موارد و رول های امنیتی امروزه بیشترین کاربرد firewall مخصوصا نوع سخت افزاری آن مقابله با ترافیک مخرب حملات تکذیب سرویس یا DDOS است.

دیواره آتش

دیواره آتش معنی فارسی Firewall است. در زبان فارسی نیز معمولا واژه فایروال ، از دیواره آتش بیشتر مورد استفاده قرار می گیرد. با توجه به اینکه firewall ها سد محکم امنیتی در برابر ترافیک ورودی و خروجی هستند از آنها با نام دیواره آتش یاد می شود.

فایروال نرم افزاری

فایروال نرم افزاری برنامه ای است متکی به سیستم عامل. ترافیک ورودی و خروجی را بر اساس هسته و رول های تعریف شده در آن مدیریت و کنترل می کند. ضعف فایروال نرم افزاری در این است که تنها در لایه Application عمل می کند. بهترین کارایی فایروال نرم افزاری ترکیب با سیستم های امنیتی و نرم افزاری است. دیواره آتش نرم افزاری قابلیت محافظت سیستم در مقابل ورود غیر مجاز ، اجرا و گسترش بدافزار ها و ...را دارد.

فایروال سخت افزاری

فایروال سخت افزاری زیرساخت و تجهیزاتی است قابل مشاهده که برای کنترل و مدیریت یک شبکه کوچک یا بزرگ قابل استفاده هستند. فایروال سخت افزاری عملکرد مستقل دارد. این ابزار در شبکه به عنوان روتر (مسیریاب) عمل کرده و ترافیک مجاز را عبور می دهد. در مقابل از ورود یا حتی از خروج ترافیک غیرمجاز یا مخرب جلوگیری می کند. استفاده از ابزار سخت افزاری مهمترین عامل مقابله با حملات تکذیب سرویس ddos است.

تفاوت فایروال نرم افزاری و سخت افزاری

تفاوت این دو firewall در نوع ساختار و عملکرد است. در نوع سخت افزاری بیشتر حفاظت ، کنترل و مدیریت ترافیک مدنظر است اما در نوع نرم افزاری غالبا حفاظت در مقابل تهدیدات نرم افزاری مطرح است.

فایروال Web Application Firewall – WAF

این نوع بر عملکرد و پردازش اپلیکیشن های تحت وب نظارت مستقیم دارد. این سرویس ها غالبا بصورت ترکیبی و کلی رو وب سرور ، میل سرور ، دیتابیس سرور و بسیاری از سرویس های تحت کار با firewall نظارت دارند و در صورت sync کردن آنها با

firewallاصلی این مورد به بالاترین سطح خود می رسد. از معروف ترین ابزارهای waf می توان به comodo و owasp اشاره کرد.

انواع: Firewall ها

Network-Based Firewalls : برای محافظت از private network در برابرpublic networks مورد استفاده قرار می گیرد برای مثال. ISA Server

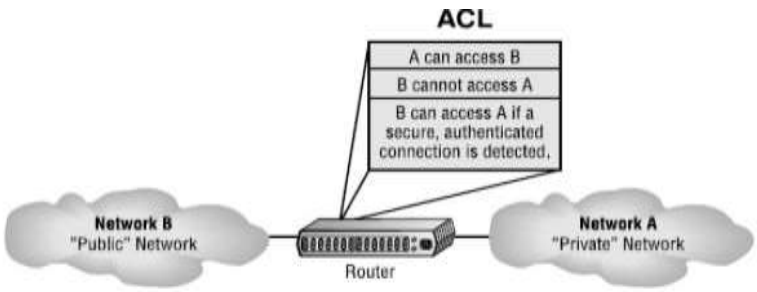
Host-Based Firewalls: برای حفاظت یک سیستم در برابر شبکه های متصل شده مورد استفاده قرار می گیرد برای مثال . Firewall Windows

تکنولوژي هاي Firewall ها

1. Access Control Lists (ACL)

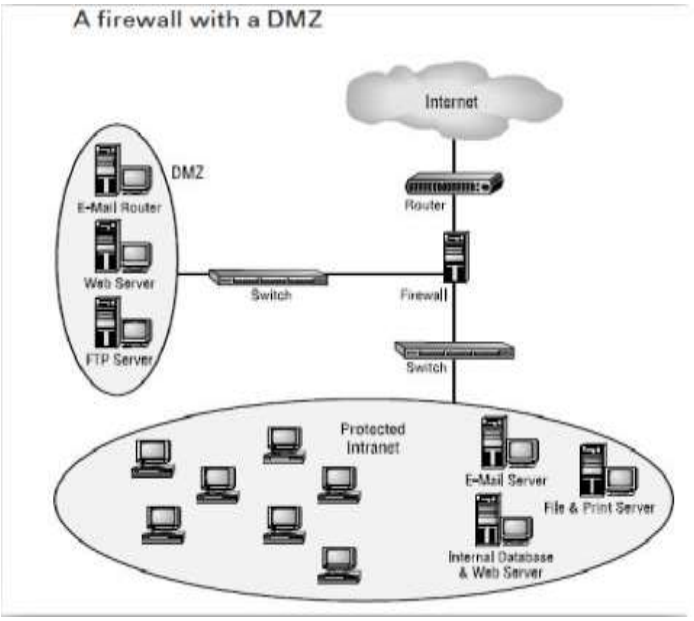
Standard ACLs : با توجه به source IP address اقدام به تصمیم گیری در موردpacket ها می کند.

Extended ACLs : بر حسبsource and destination IP addresses و یا port number ترافیک را کنترل می کند



2. Demilitarized Zone (DMZ)

در این روش معمولاً در Firewall از سه کارت شبکه (معمولاً نه همیشه) استفاده می شود و بدین ترتیب ارتباط بین تمام سیستم ها و شبکه ها را کنترل و segment های مختلف شبکه را از همدیگر جدا می کنند.



شبکه های بی سیم

ایستگاه‌های رادیویی و تلویزیونی برای چند دهه است که سیگنال‌های نامریی آنالوگ را از طریق هوا ارسال می‌کنند. هوای پیرامون ما بستری مناسب برای انتقال و تبادل داده‌ها در اختیار شبکه‌ها قرار داده است. شبکه‌هایی که با اتکا بر فن‌آوری‌های سیمی یا بی سیم به تبادل اطلاعات می‌پردازند. اما اجازه دهید، برای مدتی شبکه‌های سیمی را کنار گذشته و به سراغ شبکه‌هایی برویم که سیگنال‌ها و داده‌ها را همانند ایستگاه‌های رادیویی به شکل نامریی ارسال می‌کنند. اما شبکه‌های بی‌سیم چگونه کار می‌کنند و از چه فناوری‌هایی برای ارسال اطلاعات استفاده می‌کنند؟ ویژگی‌های بی‌سیمی که ماهواره‌ها، بلوتوث، Wi-Fi، تلفن همراه و سایر تجهیزات ارسال و دریافت کننده سیگنال‌های بی‌سیم را بر مبنای آن‌ها مخابره می‌کنند چه هستند و چگونه به دستگاه‌ها اجازه می‌دهند با یکدیگر در تعامل باشند؟

ویژگی‌های شبکه‌های انتقال بی‌سیم

شبکه‌های محلی که سیگنال‌ها را از طریق هوا و از طریق امواج RF (فرکانس رادیویی) انتقال می‌دهند به نامWLAN ها یا شبکه‌های محلی بی‌سیم شناخته می‌شوند. امروزه، رسانه‌های بی‌سیم به یکی از ملزومات مهم شبکه‌های تجاری، خانگی و برخی محیط‌های تخصصی شبکه‌ها تبدیل شده‌اند. درست است که سیگنال‌های سیمی و بی‌سیم شباهت های زیادی دارند و به‌طور مثال هر دو از لایه ۳ و پروتکل‌های بالاتر از آن استفاده می‌کنند، با این حال، ماهیت شبکه‌های بی‌سیم به گونه‌ای است که در برخی موارد به ویژه در لایه‌های پایینی مدل مرجع OSI تفاوت‌هایی با شبکه‌های سیمی دارند. برای روشن شدن بهتر مطلب اجازه دهید به سیگنال‌های بی سیم نگاهی داشته و سپس بررسی کنیم که آن‌ها چگونه ارسال می‌شوند.

طیف‌های بی‌سیم

همه سیگنال‌های بی‌سیم توسط امواج الکترومغناطیسی و از طریق هوا ارسال می‌شوند. طیف بی‌سیم، معمولا به نام موج‌های هوایی

شناخته شده و به دامنه فرکانس امواج الکترومغناطیسی اشاره دارد که برای برقراری ارتباطات صوتی و ارسال داده‌ها از آن استفاده می‌شود. در کشوری همچون ایالات متحد کمیسیون ارتباطات فدرال (FCC) که بر نحوه استفاده از طیف‌های بی‌سیم نظارت دارد، محدوده فرکانس‌ها یا پهنای باند طیف‌های بی‌سیم را ۹ کیلوهرتز تا ۳۰۰ گیگاهرتز تعیین کرده است و مشخص کرده است که هر فرکانسی برای چه مقاصدی باید استفاده شود و در چه مکان‌هایی نباید از فرکانس‌های خاصی استفاده شود) .یک هرتز یا Hz یک چرخه در هر ثانیه است. (توجه داشته باشید که ترجمه فرکانس در فارسی بسامد است، اما برای درک بهتر مطلب از همان واژه فرکانس استفاده می‌کنیم.)

نکته: شبکه‌های بی‌سیم از طریق زنجیره‌ای از امواج الکترومغناطیس با یکدیگر ارتباط برقرار کرده که می‌تواند حامل داده‌ها یا می تواند حامل ارتباطات صوتی و تصویری باشد که با طول موج‌های مختلف استفاده می‌شود. اتحادیه بین‌المللی مخابرات (ITU) سازمانی جهانی است که وظیفه قانون‌گذاری و مدیریت فضای فرکانسی را عهده‌دار است. استانداردسازی مخابرات، ارتباطات رادیویی و توسعه مخابرات از وظایف این اتحادیه است. این اتحادیه استانداردهایی برای برقراری ارتباطات بین‌الملل وضع کرده که تخصیص فرکانس های بی‌سیم از جمله آن‌ها است. توجه داشته باشید هر فرکانسی برای هدف خاصی استفاده می‌شود. به‌طور مثال، برخی از باندها تنها برای یک استفاده خاص در نظر گرفته شده‌اند. به‌طور مثال، یک باند برای تلویزیون، FMیا AM در نظر گرفته شده است، در حالی که برخی دیگر همچون باندهای وای‌فای برای استفاده عمومی در دسترس قرار دارند. در موردWi-Fi ، این حرف به معنای آن است که شما می‌توانید دستگاه وای‌فای خودتان را در اختیار داشته و از آن استفاده کنید بدون آن‌که به مجوز سازمان خاصی برای استفاده از این باند نیاز داشته باشید. در ایالات متحده سازمان FCC بر این مسئله نظارت دارد.

مدیریت کانال

باندی که توسط یک دستگاه بی‌سیم استفاده می‌شود توسط دامنه کلی فرکانس خود تعریف می‌شود. برای آن‌که به دستگاه‌های مختلف اجازه دهیم تا باند یکسانی را به‌اشتراک قرار دهند، باند باید به کانال‌هایی تقسیم شود و خود کانال‌ها نیز باید به کانال‌هایی با باند باریک تقسیم شوند. باند باریک (narrow band) یک کانال ارتباطی به وجود آورده که در آن پهنای باند یک پیام ارسال شده فراتر از پهنای باند همبستگی (coherence bandwidth) نخواهد رفت. اما چرا باید یک چنین کاری انجام شود؟ پاسخ ساده است. راهکار فوق به ما اجازه می‌دهد با کاهش پهنای باند، کانال‌های رادیویی بیشتری ایجاد کنیم، با توجه به اینکه ما در عمل اندازه را به نصف کاهش می‌دهیم در یک طیف فرکانس قادر به ایجاد دو کانال رادیویی خواهیم بود. اکثر دستگاه‌های بی سیم یکی از دو فناوری (مدولاسیون) زیر را برای استفاده از مزایای فرکانس‌ها درون باند خود و به منظور جلوگیری از تداخل استفاده می‌کنند.

پرش فرکانسی مبتنی بر طیف گسترده/ طیف گسترده پرش فرکانسی (FHSS) سرنام Spectrum Spreading Frequency Frequency، مدولاسیونی برای ارسال سیگنال در باند فرکانسی رادیویی است. در این مدولاسیون فرکانس موج حامل به شکل پیوسته و شبه تصادفی تعویض می‌شود. انشعابات یا همان پرش‌های کوتاه مدت باعث می‌شوند تا داده‌ها روی فرکانس خاصی درون باند انتقال پیدا کنند، در یک وضعیت دنباله‌دار، پرش بعدی به فرکانس بعدی رفته و این‌کار تکرار می‌شود. پرش از فرکانس می‌تواند صدها بار در ثانیه رخ دهد. دقت کنید که مدولاسیون FHSS ارزان‌تر از DSSS بوده و در محیط‌های پر ازدحام و محیط‌های داخلی

بهتر از DSSS عمل می‌کند. پرش فرکانسی دنباله مستقیم یا طیف گسترده دنباله مستقیم (DSSS) سرنام direct sequence spread spectrum، مدولاسیونی است که در آن جریان‌های داده‌ای به تکه‌های کوچکی تقسیم می‌شوند که این تکه‌های کوچک چیپ ها (chips) نام دارند. چیپ هایی که روی همه فرکانس‌های موجود در یکی از سه کانال عریض به شکل همزمان پخش می شوند. فرایند تقسیم و رمزگذاری داده‌ها چیپ سازی نامیده می‌شود. نرخ توزیع استفاده شده برای انتقال داده‌ها نیز کد چیپ سازی نامیده شده که برای هر دستگاه کدی منحصر به فرد است DSSS .می‌تواند پهنای باند موجود را نسبت به FHSS به شکل کارآمدتری استفاده کرده و در نتیجه توان عملیاتی بالاتری را ارائه می‌کند.

استانداردهای بی‌سیم در محدوده ۲,۴ گیگاهرتز چگونه از باند اختصاصی خود استفاده می‌کنند. برای آشنایی با این موضوع به شکل سریع مروری بر این استانداردها خواهیم داشت و در شماره‌های آتی اطلاعات بیشتری درباره آن‌ها به دست خواهیم آورد.

Wi-Fi، معمولا برای دسترسی به اینترنت بی‌سیم، از مدولاسیون DSSS استفاده می‌کند. در ایالات متحده، سازمان تنظیم مقررات رادیویی (FCC) ۱۱ کانال را در باند ۲,۴ گیگاهرتزی ویژه وای‌فای و ۲۴ کانال را برای باند ۵ گیگاهرتز تعریف کرده است) .کشورهای دیگر ممکن است ۱۴ کانال Wi-Fi را برای باند ۲,۴ گیگاهرتز اختصاص داده باشند (.در ایالات متحده، هر کانال پهنای ۲۰ مگاهرتز دارد. توجه داشته باشید که یک اکسس پوینت وای‌فای (Wi-Fi AP) که یک دستگاه اتصال مرکزی برای کلاینت‌های وای‌فای در یک شبکه است، به صورت دستی برای استفاده از یک گروه انتخاب شده از کانال‌ها پیکربندی شده است. دستگاه‌های کلاینت وای فای کل کانال را برای کانال‌های فعال پویش می‌کنند.

بلوتوث، معمولا برای اتصال دستگاه‌های شخصی بی سیم، از مدولاسیون FHSS استفاده می‌کند تا از ۷۹ کانال اختصاص یافته به گروه بلوتوث استفاده کند. در شبکه‌ای متشکل از دستگاه‌های بلوتوث که piconet نام دارد، یک دستگاه اصلی تعیین می‌شود که این دستگاه زمانی را برای سایر دستگاه‌ها ارائه می‌کند تا دستگاه‌ها بتوانند به شکل درستی به کانال‌ها پرش کرده و از آن‌ها استفاده کنند. از آنجایی که انتقال بلوتوث به‌طور مداوم کانال ها را پر می‌کند، تصادم یا تداخل به ندرت باعث بروز مشکل می‌شوند.

ZigBee، معمولا در دستگاه‌های صنعتی، علمی و پزشکی استفاده شده و از مدولاسیون DSSS و ۱۶ کانال استفاده می‌کند

آنتن‌ها

هوا هیچ مسیر ثابتی برای سیگنال‌ها مشخص نمی‌کند که انتقال پیدا کنند، بنابراین سیگنال‌ها بدون آن‌که هدایت شوند به حرکت خود ادامه می‌دهند. در نقطه مقابل این رویکرد، رسانه‌های سیمی مانند UTP یا کابل فیبر نوری که یک مسیر سیگنال ثابت را فراهم می‌کنند، قرار دارند. فقدان مسیر ثابت باعث می‌شود تا فرآیند ارسال سیگنال‌های بی‌سیم، دریافت، کنترل و تصحیح خطاها از رویکردی متفاوت از سیگنال‌های سیمی پیروی کند. بخشی از این کار در سطح سخت‌افزاری انجام می‌شود. درست مانند سیگنال های سیمی، سیگنال‌های بی سیم از جریان الکتریکی که در طول یک هادی جریان دارد، آغاز می‌شوند. سیگنال الکتریکی از فرستنده به سمت یک آنتن حرکت می‌کند و سیگنال را به عنوان یک سری امواج الکترومغناطیسی در هوا منتشر می‌کند. سیگنال از طریق هوا حرکت می‌کند تا زمانی که به مقصد خود برسد. در مقصد، آنتن دیگری سیگنال را دریافت کرده و گیرنده آن‌را به جریان تبدیل

می‌کند. توجه داشته باشید که آنتن‌ها برای انتقال و دریافت سیگنال‌های بی‌سیم استفاده می‌شوند. همانطور که ممکن است انتظار داشته باشید، برای تبادل اطلاعات، دو آنتن باید به فرکانس یکسانی متصل شوند تا بتوانند از کانال یکسانی استفاده کنند. هر نوع سرویس بی سیم نیاز به یک آنتن اختصاصی برای آن سرویس نیاز دارد. ویژگی‌های سرویس به منظور تعیین خروجی قدرت آنتن، فرکانس، و الگوی تابش آنتن استفاده می‌شوند. یک الگوی تابش آنتن که به نام الگوی تشعشعی نیز معروف است، مقاومت نسبی همه امواج الکترومغناطیسی در یک ناحیه سه بعدی (زوایای مختلف فضای اطرافش) که آنتن قادر به ارسال یا دریافت آن‌ها است را توصیف می‌کند.

الگوهای تشعشع می‌توانند برای طبقه‌بندی آنتن‌ها به دو دسته اساسی زیر تقسیم شوند:

• آنتن تک جهته - (unidirectional antenna) سیگنال‌های بی سیم را در امتداد یک جهت ارسال می‌کند. این نوع آنتن زمانی استفاده می‌شود که منبع نیاز به برقراری ارتباط با مقصد دارد. یک پیوند نقطه به نقطه یا در یک ناحیه خاص از جمله این موارد است. یک اتصال ماهواره‌ای (به‌طور مثال، نوعی که برای دریافت سیگنال‌های دیجیتالی تلویزیون استفاده می‌شود) از آنتن‌های جهت دار استفاده می‌کند.

• آنتن‌های چند جهته/همه جانبه (omnidirectional antenna) – این توانایی را دارند تا سیگنال بی سیم را با قدرت و وضوح چند برابر در همه جهات دریافت کنند. این نوع آنتن‌ها زمانی استفاده می‌شوند که گیرنده‌های زیاد مختلفی مجبور هستند سیگنالی که در جهات مختلف ارسال می‌شود را دریافت کنند. ایستگاه‌های رادیویی و تلویزیونی از آنتن‌ها چند جهته استفاده می‌کنند. درست به همان شکلی که اکثر برج‌ها برای ارسال سیگنال‌های سلولی از آن استفاده می‌کنند. منطقه جغرافیایی که یک آنتن یا سیستم بی سیم می‌تواند به آن دسترسی داشته باشد محدوده سیگنال یا آنتن نام دارد. گیرنده‌ها باید در محدوده وسیعی باشند تا سیگنال‌های دقیق را به‌طور مداوم دریافت کنند. با این حال، حتا در محدوده آنتن نیز ممکن است موانع یا اجسام مختلفی قرار داشته باشند که فرآیند دریافت سیگنال‌ها را با مشکل روبرو می‌کنند.