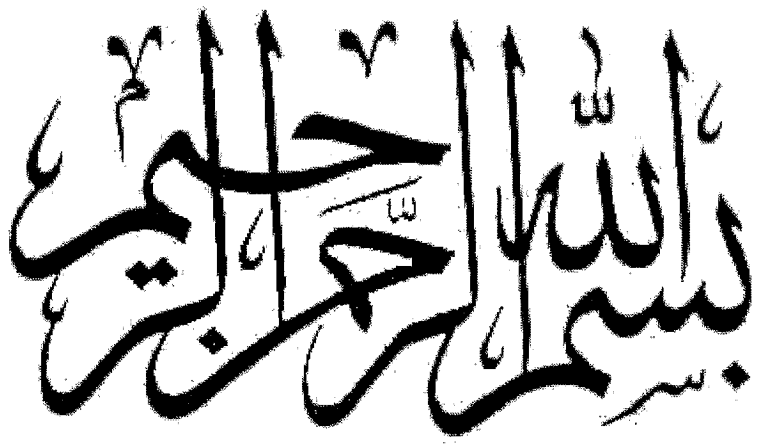

دانشکده مهندسی برق و کامپیوتر
گروه مهندسی کامپیوتر

پایان نامه

برای دریافت درجه کارشناسی ارشد

مهندسی فناوری اطلاعات-شبکه‌های کامپیوتری

ارزیابی کارآئی پروتکل AODV در مقابل حملات DDoS در شبکه‌های ویژه

استاد راهنما : **دکتر فضل‌الله ادیب‌نیا**

استاد مشاور : **دکتر محمد قاسم زاده**

پژوهش و نگارش : شیده سرائیان

شهریور ۱۳۸۷

این پایان‌نامه با حمایت‌های مالی

مرکز تحقیقات مخابرات ایران

به انجام رسیده است.

تقدیم به

مادر مهربان و دلسوزم و پدر صبورم

که در دنیا بهتر از آن دو پیدا نکردم

برادر و خواهر

و

همسر مهربانم

دوستانی که هر چه بر سر ما می رود محبت اوست

و تمام آنهایی که دوستشان داریم و نمی دانند چقدر

و آنهایی که دوستمان دارند و نمی دانیم چقدر

پروردگارا! برایم سرنوشتی خیر بنویس، تقدیری مبارک،

تا زود نخواهم آنچه را تو دیر می خواهی.

خداوند مهربان را سپاسگزارم که توانستم یکی دیگر از مقاطع علم‌آموزی را پشت سر بگذارم، بر خود لازم می‌دانم از استادان بزرگوار جناب آقای دکتر فضل الله ادیب‌نیا و جناب آقای دکتر محمد قاسم زاده که توفیق استفاده از راهنمائی‌های مدبرانه و دلسوزانه ایشان را برای انجام این پروژه داشتم و همچنین از راهنمائی‌های جناب آقای دکتر مهدی آقا صرام و جناب آقای دکتر ناصر موحدی‌نیا برای پایان رساندن این پایان‌نامه و کلیه عزیزانی که به نوعی من را همراهی نموده‌اند، کمال تشکر و قدردانی را داشته باشم.

مدیریت تحصیلات تکمیلی	**صورتجلسه دفاعیه پایان نامه دانشجوی** **دوره کارشناسی ارشد**	شناسه: ب/ک/۳ شماره: تاریخ: پیوست:

جلسه دفاعیه پایان نامه تحصیلی خانم: ***شیده سرائیان***

دانشجوی کارشناسی ارشد رشته / گرایش: ***مهندسی فناوری اطلاعات گرایش شبکه‌های کامپیوتری***

تحت عنوان: ***ارزیابی کارایی پروتکل AODV در مقابل حملات DDoS در شبکه‌های ویژه***

و تعداد واحد: ۶ در تاریخ ***۱۳۸۷/۶/۲۵*** با حضور اعضای هیأت داوران (به شرح ذیل) تشکیل گردید.

پس از ارزیابی توسط هیأت داوران، پایان نامه با نمره: به عدد ۱۹ به حروف نوزده تام و درجه عالی مورد تصویب قرار گرفت.

عنوان	نام و نام خانوادگی	امضاء
استاد / استادان راهنما	دکتر فضل ا... ادیب نیا	
استاد / استادان مشاور	دکتر محمد قاسم زاده	
متخصص و صاحبنظر داخلی	دکتر مهدی آقا صرام	
متخصص و صاحبنظر خارجی	دکتر سید مرتضی بابامیر (از دانشگاه کاشان)	

نماینده تحصیلات تکمیلی دانشگاه (ناظر)

نام و نام خانوادگی: منصور رضیعیان

امضاء:

چکیده

شبکه‌های ***MANET***، یک الگوی شبکه‌بندی بی‌سیمی جدید برای کاربران سیار هستند. این شبکه‌ها، از جمله سیستم‌های خودگردانی هستند که از یکسری گره‌های متحرک تشکیل شده‌اند و این گره‌ها به وسیله کانال‌های بی‌سیم به یکدیگر اتصال می‌یابند. هر گره عمل کننده در این شبکه‌ها، فقط به عنوان یک سیستم انتهائی به حساب نمی‌آید، بلکه می‌تواند به عنوان یک مسیریاب نیز برای هدایت بسته‌ها در نظر گرفته شود.

مهمترین مسأله در طراحی این شبکه‌ها، آسیب‌پذیری آنها در مقابل حملات امنیتی است. بایستی دقت نمود که این حملات همیشه از خارج از شبکه انجام نمی‌گیرند، بلکه گاهی اوقات، ممکن است بعضی از گره‌های موجود در شبکه، خود نقش حمله‌کننده را ایفا نمایند. یکی از این نوع حملات، حملات ***DDoS***[1] است که بنا بر نوع عملکردشان، تأثیر جدی بر روی شبکه‌های ویژه گذاشته و آنها را دچار اشکال می‌کنند. در این پروژه، به ارزیابی یکی از قراردادهای آسیب‌پذیر این نوع شبکه‌ها به نام ***AODV***[2] در مقابل حمله ***Blackhole*** که یکی از انواع مهم دسته حملات ***DDoS*** است، می‌پردازیم.

این ارزیابی با استفاده از شبیه‌سازهای ***OMNET++*** و ***Mobility Framework*** در قالب چندین سناریو انجام شده است. برای ارزیابی قرارداد فوق، از معیارهای مختلفی مانند نرخ تحویل بسته، تأخیر انتها به انتها و توان بهره گرفته شده است.

در شبیه‌سازی این نوع حمله در شبکه‌های ویژه، اثر حمله ***Blackhole*** بر روی معیارهای مختلف و در شرایط گوناگون بررسی گردیده است. نتایج حاصل شده، حاکی از تأثیر بالای این نوع حمله بر روی شبکه‌های ***MANET*** می‌باشد. آنچه که در نمودارهای حاصل شده از شبیه‌سازی مشاهده می‌گردد، آن است که حمله فوق سبب کاهش نرخ تحویل بسته، تأخیر انتها به انتها و توان شده و در ادامه فعالیت خود، عملکرد صحیح شبکه را دچار اشکال می‌سازد.

---

[1] Distributed Denial of Service
[2] Advanced On-demand Distance Vector

در نتایج حاصل از شبیه‌سازی سناریوهای دیگر، مشاهده می‌شود که هر چه تعداد حمله کنندگان و تعداد گره‌ها افزایش می‌یابد، اثر این حمله نیز زیاد شده، معیارهای در نظر گرفته شده شدیداً کاهش یافته و شبکه در سطح وسیعی، تحت تأثیر قرار می‌گیرد. از طرفی، با افزایش تعداد اتصالات، اثر این حمله و موفقیت آن، به شدت کاهش می‌یابد.

فهرست مطالب

فصل اول: شبکه‌های ویژه

۱-۱ مقدمه..... ۱

۱-۲ معرفی شبکه‌های ویژه..... ۱۶

۱-۳ خصوصیات شبکه‌های ویژه..... ۱۹

۱-۴ امنیت در شبکه‌های ویژه..... ۲۰

۱-۵ قراردادهای مسیریابی مورد استفاده در شبکه‌های ویژه..... ۲۳

فصل دوم: حملات DDoS

۲-۱ امنیت ۳۳

۲-۲ حملات DDoS ۳۹

فصل سوم: قرارداد AODV

۳-۱ بررسی قرارداد AODV ۴۷

۳-۲ حمله Blackhole..... ۵۴

فصل چهارم: ارزیابی و شبیه‌سازی

۴-۱ معرفی شبیه‌سازهای به کار گرفته شده..... ۸۵

۴-۲ ارزیابی و شبیه‌سازی..... ۶۱

۴-۳ تحلیل نتایج حاصل از شبیه‌سازی..... ۷۳

فصل پنجم: نتیجه‌گیری و پیشنهادها

۵-۱ نتیجه‌گیری..... ۷۵

۵-۲ پیشنهادها..... ۷۸

فهرست اشکال

شکل (۱-۱) تغییر توپولوژی شبکه در شبکه‌های ویژه..... ۱۸

شکل (۳-۱) فرمت بسته RREQ..... ۵۰

شکل (۳-۲) فرمت بسته RREP..... ۵۱

شکل (۳-۳) فاز کشف مسیر قرارداد AODV..... ۵۲

شکل (۳-۴) فاز کشف مسیر در قرارداد AODV در زمان وجود حمله Blackhole ۵۶

شکل (۳-۵) ارتباط گره مقصد به گره‌های دیگر..... ۵۷

شکل (۴-۱) معماری به کارگرفته شده در شبیه‌سازهای Mobility Framework و OMNET++ ... ۶۲

شکل (۴-۲) توپولوژی فرضی ۶۴

شکل (۴-۳) نرخ تحویل بسته در زمان حمله Blackhole - یک فرستنده و یک گیرنده..... ۶۸

شکل (۴-۴) تأخیر انتها به انتها در زمان حمله Blackhole - یک فرستنده و یک گیرنده ۶۹

شکل (۴-۵) میزان توان در زمان حمله Blackhole - یک فرستنده و یک گیرنده ۶۶

شکل (۴-۶) نرخ تحویل بسته در زمان حمله Blackhole - دو فرستنده و یک گیرنده ۶۷

شکل (۴-۷) تأخیر انتها به انتها در زمان حمله holeBlack- دو فرستنده و یک گیرنده ۶۸

شکل (۴-۸) میزان توان در زمان حمله Blackhole- دو فرستنده و یک گیرنده ۶۸

شکل (۴-۹) نرخ تحویل بسته در زمان حمله Blackhole - پنج فرستنده و یک گیرنده ۷۰

شکل (۴-۱۰) تأخیر انتها به انتها در زمان حمله Blackhole- پنج فرستنده و یک گیرنده ۷۰

شکل (۴-۱۱) میزان توان در زمان حمله Blackhole- پنج فرستنده و یک گیرنده ۷۱

شکل (۴-۱۲) نرخ تحویل بسته در زمان حمله Blackhole - پنج فرستنده و یک گیرنده ۷۲

شکل (۴-۱۳) نرخ تحویل بسته در زمان حمله Blackhole - پنج فرستنده و یک گیرنده ۷۲

شکل (۴-۱۴) نرخ تحویل بسته در زمان حمله Blackhole - پنج فرستنده و یک گیرنده ۷۳

فهرست جداول

جدول (۳-۱) نتایج حاصل از فاز کشف مسیر ۵۳
جدول (۳-۲) نتایج حاصل از فاز کشف مسیر در زمان وجود حمله Blackhole..... ۵۷
جدول (۴-۱) پارامترهای محیط شبیه‌سازی ۶۴

فصل اول
شبکه‌های ویژه

۱-۱. مقدمه

شبکه‌های کامپیوتری از چندین کامپیوتر متصل به هم تشکیل شده است که از یک سیستم ارتباطی به هدف به اشتراک گذاری داده‌ها، منابع و ارتباطات استفاده می‌کند. برای مثال شبکه کامپیوتر خانگی ممکن است از دو یا چند کامپیوتر تشکیل شده باشد که با استفاده از شبکه، فایل‌ها و یک چاپگر را به اشتراک گذاشته‌اند. اندازه و مقیاس هر شبکه از روی سخت‌افزار مورد استفاده و همچنین پروتکلهایی که پیاده‌سازی شده‌اند، تعیین می‌شوند.

شبکه‌های کامپیوتری مجموعه‌ای از کامپیوترهای مستقل متصل به یکدیگرند که با هم ارتباط داشته و تبادل داده می‌کنند. مستقل بودن کامپیوترها بدین معناست که هر کدام دارای واحدهای کنترلی و پردازشی مجزا بوده و وجود یا عدم وجود یکی بر دیگری تأثیرگذار نیست. متصل بودن کامپیوترها یعنی از طریق یک رسانه فیزیکی مانند کابل، فیبر نوری، ماهواره و ... به یکدیگر وصل می‌باشند. دو شرط فوق از شرایط لازم برای ایجاد یک شبکه کامپیوتری می‌باشند، اما شرط کافی برای تشکیل چنین شبکه، برقراری ارتباط و تبادل داده بین کامپیوترهاست.

این موضوع در بین متخصصین قلمرو شبکه مورد بحث است که آیا دو کامپیوتر که با استفاده از نوعی رسانه ارتباطی به یکدیگر متصل شده‌اند، تشکیل یک شبکه می دهند؟ در این رابطه گفته شده است که یک شبکه نیازمند دست کم سه کامپیوتر متصل به هم است. در جای دیگری، یک شبکه کامپیوتری را به صورت شبکه‌ای از گره‌های پردازشگر داده که جهت دریافت و ارسال داده به یکدیگر متصل شده‌اند، تعریف شده است. کامپیوتری که به وسیله‌ای غیرکامپیوتری متصل شده

است، مثلاً از طریق ارتباط اترنت به یک پرینتر متصل شده است، ممکن است که یک شبکه کامپیوتری به حساب آید.

در مواردی هم به دو یا چند کامپیوتر متصل به هم نیازمند است تا یک شبکه تشکیل شود. در مورد تعداد بیشتری کامپیوتر که به هم متصل هستند، عموماً توابع پایه‌ای مشترکی دیده می‌شود. از این رو برای آنکه شبکه‌ای به وظیفه‌اش عمل کند، سه نیاز اولیه بایستی فراهم گردد که عبارتند از : اتصالات، ارتباطات و خدمات.

اتصالات به بستر سخت‌افزاری اشاره دارد، ارتباطات به روشی اشاره می‌کند که به وسیله آن وسایل با یکدیگر صحبت کنند و خدمات نیز برای بقیه اعضای شبکه به اشتراک گذاشته شده‌اند.

ممکن است شبکه‌های رایانه‌ای مطابق مدلهای مرجع پایه‌ای که در صنعت به عنوان استاندارد شناخته می‌شوند مانند مدل مرجع هفت لایه OSI و مدل چهار لایه TCP/IP، بر اساس نوع لایه شبکه‌ای که در آن عمل می‌کنند، طبقه‌بندی شوند.

گاهی اوقات نیز، شبکه‌های کامپیوتری بر اساس اندازه یا گستردگی ناحیه‌ای که شبکه پوشش می‌دهد، طبقه‌بندی شوند. برای نمونه شبکه شخصی[1]، شبکه محلی[2]، شبکه کلان‌شهری[3] یا شبکه گسترده[4].

شبکه‌های کامپیوتری بر اساس فناوری سخت‌افزاری که جهت اتصال هر دستگاه در شبکه استفاده می‌شود نیز، طبقه‌بندی می‌گردند. نمونه‌هایی از این فناوری‌ها عبارت‌اند از: اترنت[5]، شبکه محلی بی‌سیم[6]، شبکه ارتباط از طریق خطوط برق[7].

در بعضی موارد نیز، شبکه‌های کامپیوتری بر اساس معماری موجود بین اعضای شبکه، دسته‌بندی می‌شوند.

---

[1] PAN
[2] LAN
[3] MAN
[4] WAN
[5] Ethernet
[6] WLAN
[7] HomaPNA

شبکه‌های کامپیوتری بر اساس نوع توپولوژی شبکه نیز طبقه‌بندی می‌گردند. این شبکه‌ها عبارتند از :

۱) شبکه باس[1].

۲) شبکه ستاره[2].

۳) شبکه حلقه‌ای[3].

۴) شبکه توری[4].

۵) شبکه ستاره- باس[5].

۶) شبکه درختی[6].

۷) شبکه سلسله مراتبی[7].

توپولوژی شبکه را می‌توان بر اساس نظم هندسی ترتیب داد. توپولوژی‌های شبکه، طرح منطقی شبکه هستند. واژه منطقی در اینجا بسیار پرمعنی است. این واژه به این معنی است که همبندی شبکه به طرح فیزیکی شبکه بستگی ندارد. مهم نیست که کامپیوترها در یک شبکه به صورت خطی پشت سر هم قرار گرفته باشند، ولی زمانیکه از طریق یک هاب به یکدیگر متصل شده باشند، تشکیل همبندی ستاره را می‌دهند نه باس. شبکه‌های کامپیوتری بر اساس پروتکل ارتباطی نیز قابل تقسیم هستند.

انواع شبکه‌های کامپیوتری بر اساس اندازه عبارتند از:

۱) شبکه شخصی[8]: این شبکه، یک شبکه کامپیوتری است که برای ایجاد ارتباطات بین وسایل کامپیوتری که اطراف یک فرد هستند، مانند تلفن سیار، کامپیوترهای جیبی[9] و ... استفاده می‌شود. این‌که این وسایل ممکن است، متعلق به آن فرد باشند یا خیر، جای بحث خود را

---

[1] BUS
[2] STAR
[3] Ring
[4] Mesh
[5] BUS-STAR
[6] Tree
[7] Hierarchical
[8] Personal Area Network
[9] PDA

دارد. برد یک شبکه شخصی عموماً چند متر بیشتر نیست. موارد مصرف شبکه‌های خصوصی می‌تواند جهت ارتباطات وسایل شخصی چند نفر با یکدیگر و یا برقراری اتصال این وسایل به شبکه‌ای در سطح بالاتر و شبکه اینترنت باشد. ارتباطات شبکه‌های شخصی ممکن است به صورت سیمی از طریق گذرگاه کامپیوتر مانند USB و FireWire برقرار شود. همچنین با بهره‌گیری از فناوری‌هایی مانند بلوتوث و ... می‌توان شبکه‌های شخصی را به صورت بی‌سیم ساخت.

۲) شبکه محلی[1] : شبکه محلی، یک شبکه کامپیوتری است که محدوده جغرافیائی کوچکی مانند یک خانه، یک دفتر کار یا گروهی از ساختمان‌ها را پوشش می‌دهد. در مقایسه با شبکه‌های گسترده[2] از مشخصات تعریف شده شبکه‌های محلی می‌توان به سرعت (نرخ انتقال) بسیار بالاتر آنها، محدوده جغرافیایی کوچکتر و عدم نیاز به خطوط استیجاری مخابراتی اشاره کرد. دو فناوری اترنت روی کابل جفت به هم تابیده بدون محافظ[3] و وای‌فای[4] رایج ترین فناوری‌هائی هستند که امروزه استفاده می‌شوند.

۳) شبکه شهری[5] : شبکه شهری معمولاً در سطح یک شهر گسترده می‌شود. در این شبکه‌ها معمولاً از زیرساخت بی‌سیم و یا اتصالات فیبر نوری جهت ایجاد ارتباط بین محل‌های مختلف استفاده می‌گردد.

۴) شبکه گسترده : شبکه گسترده، نسبتاً ناحیه جغرافیایی وسیعی را پوشش می‌دهد. (برای نمونه از یک کشور به کشوری دیگر یا از یک قاره به قاره‌ای دیگر.) این شبکه‌ها معمولاً از امکانات شرکت‌هائی که به ارائه خدمت می‌پردازند، مانند شرکت‌های مخابرات استفاده می‌کنند. به عبارت دیگر، این شبکه‌ها کمتر از مسیریاب و کانال‌های ارتباطی عمومی استفاده می‌نمایند. شبکه‌های گسترده برای اتصال شبکه‌های محلی یا دیگر انواع شبکه به یکدیگر استفاده می‌شوند. بنابراین کاربران و کامپیوترهای یک مکان می‌توانند با کاربران و

---

[1] LAN
[2] WAN
[3] UTP
[4] WiFi
[5] MAN

کامپیوترهایی در مکانهای دیگر در ارتباط باشند. بسیاری از شبکه‌های گسترده برای یک سازمان ویژه پیاده‌سازی می‌شوند و خصوصی هستند. بعضی دیگر به‌وسیله سرویس دهندگان اینترنت[1] پیاده‌سازی می‌شوند تا شبکه‌های محلی سازمانها را به اینترنت متصل کنند.

دو یا چند شبکه یا زیرشبکه[2] که با استفاده از تجهیزاتی که در لایه سه، یعنی لایه شبکه عمل می‌کنند مانند یک مسیریاب، به یکدیگر متصل می‌شوند، تشکیل یک شبکه از شبکه‌ها[3] را می دهند. همچنین می‌توان شبکه‌ای که از اتصال داخلی میان شبکه‌های عمومی، خصوصی، تجاری، صنعتی یا دولتی به وجود می‌آید را شبکه شبکه‌ها نامید. در کاربردهای جدید شبکه‌های به هم متصل شده از پروتکل IP استفاده می‌کنند.

بسته به اینکه چه کسانی یک شبکه از شبکه‌ها را مدیریت می‌کنند و اینکه چه کسانی در این شبکه عضو هستند، می‌توان در سه نوع، شبکه شبکه‌ها را دسته بندی نمود :

۱) شبکه داخلی یا اینترانت[4]

۲) شبکه خارجی یا اکسترانت[5]

۳) شبکه اینترنت[6]

شبکه‌های داخلی یا خارجی ممکن است اتصالاتی به شبکه اینترنت داشته باشند و یا نداشته باشند. در صورتی که این شبکه‌ها به اینترنت متصل باشند، در مقابل دسترسی‌های غیرمجاز از سوی اینترنت محافظت می‌گردند. خود شبکه اینترنت نیز، به عنوان بخشی از شبکه داخلی یا شبکه خارجی به حساب نمی‌آید، اگرچه ممکن است شبکه اینترنت به عنوان بستری برای برقراری دسترسی بین قسمت‌هایی از یک شبکه خارجی خدماتی را ارائه دهد.

یک شبکه داخلی مجموعه‌ای از شبکه‌های متصل به هم است که از پروتکل IP و ابزارهای مبتنی بر IP مانند مرورگران وب استفاده می‌کند و معمولاً زیر نظر یک نهاد مدیریتی کنترل

---

[1] ISP
[2] Subnet
[3] internet
[4] Intranet
[5] Extranet
[6] Internet

می‌شود. این نهاد مدیریتی شبکه داخلی را نسبت به سایر قسمت‌های دنیا محصور کرده و فقط به کاربران خاصی اجازه ورود به این شبکه را می‌دهد. به طور معمول‌تر شبکه درونی یک شرکت یا دیگر شرکت‌ها یک شبکه داخلی می‌باشد.

یک شبکه خارجی یک شبکه یا یک شبکه شبکه‌ها است که از لحاظ قلمرو، محدود به یک سازمان یا نهاد است، ولی شامل اتصالات محدود به شبکه‌های متعلق به یک یا چند سازمان یا نهاد دیگر است که معمولاً در بیشتر مواقع، همیشه قابل اعتماد هستند. برای نمونه مشتریان یک شرکت ممکن است که دسترسی به بخش‌هایی از شبکه داخلی آن شرکت داشته باشند که بدین ترتیب یک شبکه خارجی درست می‌گردد، چرا که از نقطه‌نظر امنیتی، این مشتریان برای شبکه قابل اعتماد به نظر نمی‌رسند. همچنین از نظر فنی می‌توان یک شبکه خارجی را درگروه شبکه‌های دانشگاهی، شهری، گسترده یا دیگر انواع شبکه (هر چیزی غیر از شبکه محلی) به حساب آورد، زیرا از نظر تعریف، یک شبکه خارجی، نمی‌تواند فقط از یک شبکه محلی، تشکیل شده باشد، چون بایستی حداقل یک اتصال به خارج از شبکه داشته باشد.

شبکه ویژه‌ای از شبکه‌ها که حاصل اتصالات داخلی شبکه‌های دولتی، دانشگاهی، عمومی و خصوصی در سرتاسر دنیا است، شبکه اینترنت نامیده می‌شود. این شبکه، بر اساس شبکه اولیه‌ای کار می‌کند که آرپانت[1] نام داشت. همچنین مکانی برای وب جهان‌گستر[2] (WWW) است. در لاتین، واژه Internet برای نامیدن آن استفاده می‌شود که برای اشتباه نشدن با معنی عام واژه شبکه شبکه‌ها، حرف اول آن را بزرگ می‌نویسند.

اعضای شبکه اینترنت یا شرکت‌های سرویس دهنده آن‌ها، از آدرسهای IP استفاده می‌کنند. این آدرس‌ها از موسسات ثبت آدرس، تهیه می‌شوند تا تخصیص آدرسها قابل کنترل باشد. همچنین سرویس دهندگان اینترنت و شرکت‌های بزرگ، اطلاعات مربوط به، در دسترس بودن آدرس‌هایشان را از طریق پروتکل دروازه لبه[3] با دیگر اعضای اینترنت مبادله می‌کنند.

---

[1] ARPANET
[2] WWW
[3] BGP

همه شبکه‌ها از اجزای سخت‌افزاری پایه‌ای تشکیل شده‌اند تا گره‌های شبکه را به یکدیگر متصل نمایند. این اجزا عبارتند از : کارت شبکه، تکرارگر، هاب، پل، سوئیچ و مسیریاب.

علاوه بر این، روش‌هائی برای اتصال این اجزای سخت‌افزاری لازم است که معمولاً از کابل‌های الکتریکی (از همه رایجتر رده پنج[1] است) و کمتر از آنها، ارتباطات میکروویو و کابل فیبرنوری استفاده می‌شود.

کارت شبکه، آداپتور شبکه یا کارت واسط شبکه[2]، قطعه‌ای از سخت‌افزار کامپیوتر است و این امکان را به کامپیوترها می‌دهد تا بتوانند بر روی یک شبکه کامپیوتری با یکدیگر ارتباط برقرار کنند. این قطعه، دسترسی فیزیکی به یک رسانه شبکه را تأمین می‌کند.

تکرارگر[3] یک قطعه الکترونیکی است که سیگنالی را دریافت کرده و آن را با سطح دامنه بالاتر، انرژی بیشتر، به سمت دیگر ارسال می‌کند. بدین ترتیب می‌توان سیگنال را بدون هیچ تغییری به فواصل دورتری فرستاد. از آنجا که تکرارگرها با سیگنال‌های فیزیکی واقعی سروکار دارند و در جهت تفسیر داده‌ای که انتقال می‌دهند تلاشی نمی‌کنند، در لایه فیزیکی یعنی اولین لایه عمل می‌کنند.

هاب قطعه‌ای سخت‌افزاری است که امکان اتصال قسمت‌های یک شبکه را با هدایت ترافیک در سراسر شبکه فراهم می‌کند. هاب‌ها نیز در لایه فیزیکی عمل می‌کنند. عملکرد هاب بسیار ابتدایی است، به این ترتیب که داده رسیده از یک گره را برای تمامی گره‌های شبکه کپی می‌نماید. هاب‌ها عموماً برای متصل کردن بخش‌های یک شبکه محلی بکار می‌روند. هر هاب چندین درگاه دارد. زمانی‌که بسته‌ای از یک درگاه می‌رسد، به دیگر درگاه‌ها کپی می‌شود، بنابراین همه قسمت‌های شبکه محلی می‌توانند بسته‌ها را ببینند.

یک پل[4] دو زیرشبکه (سگمنت) را در لایه پیوند داده، به هم متصل می‌کند. پل‌ها شبیه به تکرارگرها و هاب‌های شبکه‌اند که برای اتصال قسمت‌های شبکه در لایه فیزیکی عمل می‌نمایند، با

---

[1] Cat 5
[2] Network Interface Card
[3] Repeater
[4] Bridge

این حال پل با استفاده از مفهوم پل زدن عمل می‌کند، یعنی به جای آنکه ترافیک هر شبکه بدون نظارت به دیگر درگاه‌ها کپی شود، آن‌ها را مدیریت می‌کند.

پل‌ها به سه دسته تقسیم می‌شوند:

۱) پل‌های محلی : این پل‌ها، مستقیماً به شبکه‌های محلی متصل می‌شود.

۲) پل‌های دوردست : از این پل‌ها می‌توان برای ساختن شبکه‌های گسترده جهت ایجاد ارتباط بین شبکه‌های محلی استفاده کرد. پل‌های دور دست در شرایطی که سرعت اتصال از شبکه‌های انتهایی کمتر است با مسیریاب‌ها جایگزین می‌شوند.

سوئیچ وسیله‌ای است که قسمت‌های شبکه را به یکدیگر متصل می‌کند. سوئیچ‌های معمولی شبکه، تقریباً ظاهری شبیه به هاب دارند، اما در مقایسه با هاب از هوشمندی بیشتر و همچنین قیمت بیشتری برخوردار است. سوئیچ‌های شبکه این توانمندی را دارند که محتویات بسته‌های داده‌ای که دریافت می‌کنند را بررسی کرده، دستگاه فرستنده و گیرنده بسته را شناسایی کنند، و سپس آن بسته را به شکلی مناسب ارسال نمایند. با ارسال هر پیام فقط به دستگاه متصلی که پیام به هدف آن ارسال شده، سوئیچ پهنای باند شبکه را به شکل بهینه‌تری استفاده می‌کند و عموماً عملکرد بهتری نسبت به یک هاب دارد.

از نظر فنی می‌توان گفت که سوئیچ در لایه پیوند داده عمل می‌کند، اما بعضی از انواع سوئیچ‌ها قادرند تا در لایه‌های بالاتر نیز به بررسی محتویات بسته بپردازند و از اطلاعات بدست آمده، برای تعیین مسیر مناسب ارسال بسته استفاده نمایند. به این سوئیچ‌ها به اصطلاح سوئیچ‌های چند لایه[1] نیز می‌گویند.

مسیریاب‌ها، تجهیزات شبکه‌ای هستند که بسته‌های داده را با استفاده از سرآیندها و جدول ارسال تعیین مسیر کرده، و ارسال می‌کنند. مسیریاب‌ها در لایه شبکه عمل کرده و اتصال بین بسترهای فیزیکی متفاوت را امکان‌پذیر می‌کنند. این کار با چک کردن سرآیند یک بسته داده انجام می‌شود.

---

[1] Multilayer Switch

مسیریاب‌ها از پروتکلهای مسیریابی مانند OSPF استفاده می‌کنند تا با یکدیگر گفتگو کرده و بهترین مسیر بین هر دو ایستگاه را پیکربندی کنند. هر مسیریاب حداقل به دو شبکه، معمولاً شبکه‌های محلی، شبکه‌های گسترده و یا یک شبکه محلی و یک سرویس دهنده متصل است. بعضی از انواع مودم‌های DSL و کابلی جهت مصارف خانگی، درون خود از وجود یک مسیریاب نیز بهره می‌برند.

وقتی از شبکه اطلاع‌رسانی سخن به میان می‌آید، اغلب کابل شبکه به عنوان وسیله انتقال داده در نظر گرفته می‌شود. در حالیکه چندین سال است که استفاده از شبکه‌سازی بی‌سیم در دنیا آغاز گردیده است.

فناوری ارتباطات سیار به طور پیوسته و سریع در حال رشد است. افراد تمایل دارند تا ترمینال‌های شبکه‌ای خود(مانند Laptopها، PDA[1]ها و...) را در هر مکان و زمان استفاده نمایند. اتصالات بی‌سیمی به کاربران آزادی عمل می‌دهند تا به هر کجا که تمایل دارند و در هر زمان، جابه‌جا شوند. در گذشته، یک شبکه محلی[2] بی‌سیم با سرعت انتقال پایین و خدمات غیرقابل اعتماد، مترادف بود، اما هم اکنون تکنولوژی شبکه محلی بی‌سیم، خدمات قابل قبولی را با سرعتی که حداقل برای کاربران معمولی شبکه کابلی پذیرفته شده می‌باشد، فراهم می‌کند.

شبکه محلی بی‌سیم[3] از امواج الکترومغناطیسی (رادیویی یا مادون قرمز) برای انتقال اطلاعات از یک نقطه به نقطه دیگر استفاده می‌کند. امواج رادیویی اغلب به عنوان یک حامل رادیویی در نظر گرفته می‌شوند، چرا که این امواج، وظیفه انتقال انرژی الکترومغناطیسی را از فرستنده به گیرنده دورتر از خود برعهده دارند. داده، هنگام ارسال برروی موج حامل رادیویی سوار می‌شود و در گیرنده نیز به راحتی از موج حامل تفکیک می‌گردد. به این عمل مدولاسیون اطلاعات به موج حامل گفته می‌شود. زمانی‌که داده با موج رادیویی حامل مدوله می‌شود، سیگنال رادیویی، دارای فرکانس‌های مختلفی علاوه بر فرکانس اصلی موج حامل می‌گردد. به عبارت دیگر فرکانس

---

[1] Personal Digital Assistant
[2] Local Area Network
[3] Wireless Local Area Network (WLAN)