دانشگاه علوم پزشکی و خدمات بهداشتی درمانی کاشان
معاونت درمان
واحد مدیریت اطلاعات سلامت

## عنوان مطلب:

# شبکه کامپیوتر و امنیت سیستم ها

## فهرست


مقدمه ۳

تقسیم بندی شبکه ها ۴

- تقسیم بر اساس نوع وظایف ۴
- تقسیم بر اساس گره ۴
- تقسیم بر اساس توپولوژی ۵
  - توپولوژی BUS ۶
  - توپولوژی STAR ۷
  - توپولوژی RING ۸
  - توپولوژی Mesh ۹
- تقسیم بر اساس حوزه جغرافیایی ۱۰
  - شبکه LAN ۱۰
  - شبکه MAN ۱۱
  - شبکه WAN ۱۲

کابل شبکه ۱۲
- کابل UTP ۱۳
- کابل کواکسیال ۱۴
- فیبر نوری ۱۵

آشنایی با مدل OSI ۱۶
- لایه Physical ۱۶
- لایه Data Link ۱۶
- لایه Network ۱۶
- لایه Transmission ۱۶
- لایه Session ۱۶
- لایه Presentation ۱۶
- لایه Application ۱۶

پروتکل ها ۱۷
- پروتکل Physical ۱۷
- پروتکل Transmission ۱۷
- پروتکل Application ۱۷

امنیت شبکه های کامپیوتری ۱۸
- امنیت فیزیکی ۱۹
- امنیت منطقی ۲۲
- ملزومات و مشکلات امنیتی ارائه دهندگان خدمات ۲۳

## مقدمه

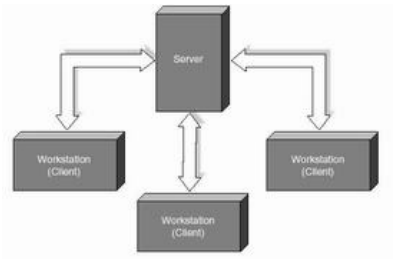
یک شبکه شامل مجموعه ای از دستگاه ها ( کامپیوتر، چاپگر و ... ) بوده که با استفاده از یک روش ارتباطی (کابل، امواج رادیوئی، ماهواره) و به مظور اشتراک منابع فیزیکی (چاپگر) و اشتراک منابع منطقی (فایل) به یکدیگر متصل می گردند. شبکه ها می توانند با یکدیگر نیز مرتبط شده و شامل زیر شبکه هائی باشند.

# تفسیم بندی شبکه ها

شبکه های کامپیوتری را بر اساس مولفه های متفاوتی تقسیم بندی می نمایند. در ادامه به برخی از متداولترین تقسیم بندی های موجود اشاره می گردد.

## تقسیم بندی بر اساس نوع وظایف

کامپیوترهای موجود در شبکه را با توجه به نوع وظایف مربوطه به دو گروه عمده : سرویس دهندگان (Servers) و یا سرویس گیرندگان (Clients) تقسیم می نمایند. کامپیوترهائی در شبکه که برای سایر کامپیوترها سرویس ها و خدماتی را ارائه می نمایند و هسته اساسی سیستم عامل بر روی آن نصب خواهد شد، سرویس دهنده نامیده می گردند. کامپیوترهائی که از خدمات و سرویس های ارائه شده توسط سرویس دهندگان استفاده می کنند ، سرویس گیرنده نامیده می شوند . در شبکه های Client-Server ، یک کامپیوتر در شبکه نمی تواند هم به عنوان سرویس دهنده و هم به عنوان سرویس گیرنده ، ایفای وظیفه نماید.

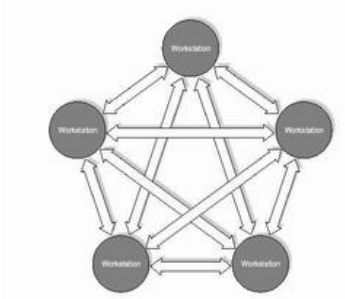



## تقسیم بندی براساس گره:(Node)

این نوع از تقسیم بندی شبکه ها براساس ماهیت گره ها یا محل های اتصال خطوط ارتباطی شبکه ها انجام می شود. در این گروه بندی شبکه ها به دو نوع تقسیم بندی می شوند. تفاوت این دو گروه از شبکه ها در قابلیت های آن نهفته است .این دو نوع اصلی از شبکه ها، شبکه هایی از نوع نظیر به نظیر (Peer to Peer) و شبکه های مبتنی بر Server یا Server Based نام دارند .

در یک شبکه نظیر به نظیر یا Peer to Peer ، بین گره های شبکه هیچ ترتیب یا سلسله مراتبی وجود ندارد و تمام کامپیوتر های واقع در شبکه از اهمیت یا اولویت یکسانی برخوردار هستند. به شبکه Peer to Peer یک گروه کاری یا Workgroupنیز گفته می شود. در این نوع از شبکه ها هیچ کامپیوتری در شبکه به طور اختصاصی وظیفه ارائه خدمات همانند سرور را ندارد. به این جهت هزینه های این نوع شبکه پایین بوده و نگهداری از آنها نسبتاً ساده می باشد. در این شبکه ها براساس آن که کدام کامپیوتر دارای اطلاعات مورد نیاز دیگر کامپیوتر هاست، همان دستگاه نقش سرور را برعهده می گیرد. و براساس تغییر این وضعیت در هر لحظه هر یک از کامپیوتر ها می توانند سرور باشند. و بقیه سرویس گیرنده. به دلیل کارکرد دوگانه هر یک از کامپیوتر ها به عنوان سرور و سرویس گیرنده، هر کامپیوتر در شبکه لازم است تا بر نوع

کارکرد خود تصمیم گیری نماید. این فرآیند تصمیم گیری، مدیریت ایستگاه کاری یا سرور نام دارد. شبکه هایی از نوع نظیر به نظیر مناسب استفاده در محیط هایی هستند که تعداد کاربران آن بیشتر از ۱۰ کاربر نباشد .




برای بهره گیری از مزایای هر دو نوع از شبکه ها، معمولاً سازمان ها از ترکیبی از شبکه های نظیر به نظیر و مبتنی بر سرور استفاده می کنند. این نوع از شبکه ها، شبکه های ترکیبی یا Combined Network نام دارند. در شبکه های ترکیبی دو نوع سیستم عامل برای تامین نیازهای شبکه مورد استفاده قرار می گیرند.

یک شبکه LAN در ساده ترین حالت از اجزای زیر تشکیل شده است :

- دو کامپیوتر شخصی . یک شبکه می تواند شامل چند صد کامپیوتر باشد. حداقل یکی از کامپیوترها می بایست به عنوان سرویس دهنده مشخص گردد. (در صورتی که شبکه از نوع Client-Server باشد).
- یک عدد کارت شبکه (NIC) کارت شبکه مسئول دریافت، انتقال، سازماندهی و ذخیره سازی موقت اطلاعات در طول شبکه است . به منظور انجام وظایف فوق کارت های شبکه دارای پردازنده ، حافظه و گذرگاه اختصاصی خود هستند.

## تقسیم بندی بر اساس توپولوژی

الگوی هندسی استفاده شده جهت اتصال کامپیوترها، توپولوژی نامیده می شود. توپولوژی انتخاب شده برای پیاده سازی شبکه ها، عاملی مهم در جهت کشف و برطرف نمودن خطاء در شبکه خواهد بود.. نوع توپولوژی انتخابی جهت اتصال کامپیوترها به یکدیگر، مستقیماً بر نوع محیط انتقال و روش های استفاده از خط تاثیر می گذارد. با توجه به تأثیر مستقیم توپولوژی انتخابی در نوع کابل کشی و هزینه های مربوط به آن، باید با دقت و تأمل به انتخاب توپولوژی یک شبکه همت گماشت . عوامل مختلفی جهت انتخاب یک توپولوژی بهینه مطرح می شود. مهمترین این عوامل بشرح ذیل است :

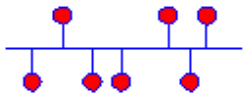
- - هزینه . هر نوع محیط انتقال که برای شبکه LAN انتخاب شود، در نهایت باید عملیات نصب شبکه در یک ساختمان پیاده سازی گردد. عملیات فوق فرآیندی طولانی جهت نصب کانال های مربوطه به محل عبور کابلها در ساختمان است. در حالت ایده آل کابل کشی و ایجاد کانال های مربوطه باید قبل از بکارگیری ساختمان انجام شود.
- - انعطاف پذیری . یکی از مزایای شبکه های LAN ، توانائی پردازش داده ها و گستردگی و توزیع گره ها در یک محیط است. توپولوژی انتخابی می بایست بسادگی امکان تغییر پیکربندی در شبکه را فراهم نماید. مثلا" ایستگاهی را از نقطه ای به نقطه دیگر انتقال و یا قادر به ایجاد یک ایستگاه جدید در شبکه باشیم .

چهار نوع توپولوژی رایج در شبکه های LAN استفاده می گردد :

- BUS
- STAR
- RING
- Mesh

## توپولوژی BUS

یکی از رایجترین توپولوژی ها برای پیاده سازی شبکه های LAN است . در مدل فوق از یک کابل به عنوان ستون فقرات اصلی در شبکه استفاده شده و تمام کامپیوترهای موجود در شبکه ( سرویس دهنده ، سرویس گیرنده ) به آن متصل می گردند.



Bus Topology

### مزایای توپولوژی BUS

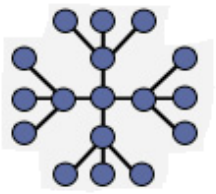
- کم بودن طول کابل . بدلیل استفاده از یک خط انتقال جهت اتصال تمام کامپیوترها ، در توپولوژی فوق از کابل کمی استفاده می شود.موضوع فوق باعث پایین آمدن هزینه نصب و ایجاد تسهیلات لازم در جهت پشتیبانی شبکه خواهد بود.
- ساختار ساده . توپولوژی BUS دارای یک ساختار ساده است . در مدل فوق صرفا" از یک کابل برای انتقال اطلاعات استفاده می شود.
- توسعه آسان . یک کامپیوتر جدید را می توان براحتی در نقطه ای از شبکه اضافه کرد. در صورت اضافه شدن ایستگاه های بیشتر در یک سگمنت ، می توان از تقویت کننده هائی به نام Repeater استفاده کرد.

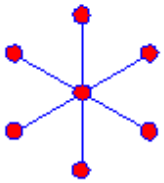
### معایب توپولوژی BUS

- مشکل بودن عیب یابی . با اینکه سادگی موجود در تویولوژی BUS امکان بروز اشتباه را کاهش می دهند، ولی در صورت بروز خطاء کشف آن ساده نخواهد بود. در شبکه هائی که از توپولوژی فوق استفاده می نمایند، کنترل شبکه در هر گره دارای مرکزیت نبوده و در صورت بروز خطاء می بایست نقاط زیادی به منظور تشخیص خطاء بازدید و بررسی گردند.
- ایزوله کردن خطاء مشکل است . در صورتی که یک کامپیوتر در توپولوژی فوق دچار مشکل شود، باید کامپیوتر را در محلی که به شبکه متصل است رفع عیب نمود. در موارد خاص می توان یک گره را از شبکه جدا کرد. در حالتیکه اشکال در محیط انتقال باشد ، تمام یک سگمنت می بایست از شبکه خارج گردد.
- ماهیت تکرارکننده ها . در مواردیکه برای توسعه شبکه از تکرارکننده ها استفاده می گردد، ممکن است در ساختار شبکه تغییراتی نیز داده شود. موضوع فوق مستلزم بکارگیری کابل بیشتر و اضافه نمودن اتصالات مخصوص شبکه است .

## توپولوژی STAR

در این نوع توپولوژی همانگونه که از نام آن مشخص است ، از مدلی شبیه "ستاره" استفاده می گردد. در این مدل تمام کامپیوترهای موجود در شبکه معمولا" به یک دستگاه خاص با نام " هاب " متصل خواهند شد.





Star Topology

### مزایای توپولوژی STAR

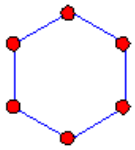
- سادگی سرویس شبکه . توپولوژی STAR شامل تعدادی از نقاط اتصالی در یک نقطه مرکزی است . ویژگی فوق تغییر در ساختار و سرویس شبکه را آسان می نماید.
- در هر اتصال یکدستگاه . نقاط اتصالی در شبکه ذاتا" مستعد اشکال هستند. در توپولوژی STAR اشکال در یک اتصال ، باعث خروج آن خط از شبکه و سرویس و اشکال زدائی خط مزبور است . عملیات فوق تاثیری در عملکرد سایر کامپیوترهای موجود در شبکه نخواهد گذاشت .
- کنترل مرکزی و عیب یابی . با توجه به این مسئله که نقطه مرکزی مستقیما" به هر ایستگاه موجود در شبکه متصل است ، اشکالات و ایرادات در شبکه بسادگی تشخیص و مهار خواهند گردید.
- روش های ساده دستیابی . هر اتصال در شبکه شامل یک نقطه مرکزی و یک گره جانبی است . در چنین حالتی دستیابی به محیط انتقال جهت ارسال و دریافت اطلاعات دارای الگوریتمی ساده خواهد بود.

### معایب توپولوژی STAR

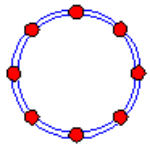
- زیاد بودن طول کابل . بدلیل اتصال مستقیم هر گره به نقطه مرکزی ، مقدار زیادی کابل مصرف می شود. با توجه به اینکه هزینه کابل نسبت به تمام شبکه ، کم است ، تراکم در کانال کشی جهت کابل ها و مسائل مربوط به نصب و پشتیبنی آنها بطور قابل توجهی هزینه ها را افزایش خواهد داد.
- مشکل بودن توسعه . اضافه نمودن یک گره جدید به شبکه مستلزم یک اتصال از نقطه مرکزی به گره جدید است . با اینکه در زمان کابل کشی پیش بینی های لازم جهت توسعه در نظر گرفته می شود ، ولی در برخی حالات نظیر زمانیکه طول زیادی از کابل مورد نیاز بوده و یا اتصال مجموعه ای از گره های غیر قابل پیش بینی اولیه ، توسعه شبکه را با مشکل مواجه خواهد کرد.
- وابستگی به نقطه مرکزی . در صورتی که نقطه مرکزی ( هاب ) در شبکه با مشکل مواجه شود ، تمام شبکه غیرقابل استفاده خواهد بود.

## توپولوژی RING

در این نوع توپولوژی تمام کامپیوترها بصورت یک حلقه به یکدیگر مرتبط می گردند. تمام کامپیوترهای موجود در شبکه ( سرویس دهنده ، سرویس گیرنده ) به یک کابل که بصورت یک دایره بسته است ، متصل می گردند. در مدل فوق هر گره به دو و فقط دو همسایه مجاور خود متصل است . اطلاعات از گره مجاور دریافت و به گره بعدی ارسال می شوند. بنابراین داده ها فقط در یک جهت حرکت کرده و از ایستگاهی به ایستگاه دیگر انتقال پیدا می کنند.



Ring Topology



Dual Ring Topology

## مزایای توپولوژی RING

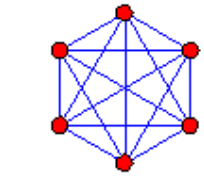
- کم بودن طول کابل . طول کابلی که در این مدل بکار گرفته می شود ، قابل مقایسه به توپولوژی BUS نبوده و طول کمی را در بردارد. ویژگی فوق باعث کاهش تعداد اتصالات ( کانکتور) در شبکه شده و ضریب اعتماد به شبکه را افزایش خواهد داد.
- نیاز به فضائی خاص جهت انشعابات در کابل کشی نخواهد بود. بدلیل استفاده از یک کابل جهت اتصال هر گره به گره همسایه اش ، اختصاص محل هائی خاص به منظور کابل کشی ضرورتی نخواهد داشت .
- مناسب جهت فیبر نوری . استفاده از فیبر نوری باعث بالا رفتن نرخ سرعت انتقال اطلاعات در شبکه است. چون در توپولوژی فوق ترافیک داده ها در یک جهت است ، می توان از فیبر نوری به منظور محیط انتقال استفاده کرد.در صورت تمایل می توان در هر بخش ازشبکه از یک نوع کابل به عنوان محیط انتقال استفاده کرد . مثلا" در محیط های اداری از مدل های مسی و در محیط کارخانه از فیبر نوری استفاده کرد.

## معایب توپولوژی RING

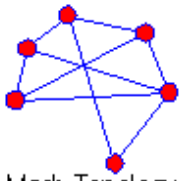
- اشکال در یک گره باعث اشکال در تمام شبکه می گردد. در صورت بروز اشکال در یک گره ، تمام شبکه با اشکال مواجه خواهد شد. و تا زمانیکه گره معیوب از شبکه خارج نگردد ، هیچگونه ترافیک اطلاعاتی را روی شبکه نمی توان داشت .
- اشکال زدائی مشکل است . بروز اشکال در یک گره می تواند روی تمام گرههای دیگر تاثیر گذار باشد. به منظور عیب یابی می بایست چندین گره بررسی تا گره مورد نظر پیدا گردد.
- تغییر در ساختار شبکه مشکل است . در زمان گسترش و یا اصلاح حوزه جغرافیائی تحت پوشش شبکه ، بدلیل ماهیت حلقوی شبکه مسائلی بوجود خواهد آمد .
- توپولوژی بر روی نوع دستیابی تاثیر می گذارد. هر گره در شبکه دارای مسئولیت عبور دادن داده ای است که از گره مجاور دریافت داشته است . قبل از اینکه یک گره بتواند داده خود را ارسال نماید ، می بایست به این اطمینان برسد که محیط انتقال برای استفاده قابل دستیابی است .

## توپولوژی Mesh

در این نوع توپولوژی که تمامی نقاط ارتباطی با دیگر نقاط در ارتباط هستند، هرگونه اختلال فیزیکی در سطوح دسترسی منجر به اختلال عملکرد شبکه نخواهد شد، با وجود آنکه زمان‌بندی سرویس‌دهی را دچار اختلال خواهد کرد. پیاده‌سازی چنین روش با وجود امنیت بالا، به دلیل محدودیت‌های اقتصادی، تنها در موارد خاص و بحرانی انجام می‌گیرد.



Fully Connected Topology



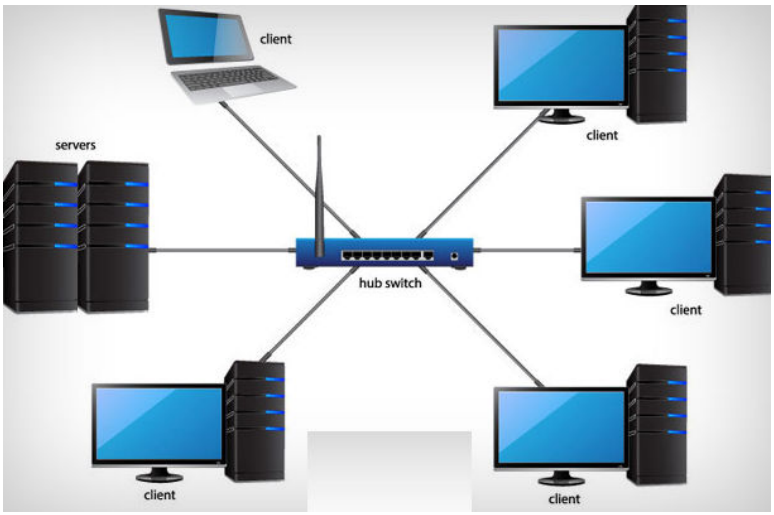
Mesh Topology

## تقسیم بندی بر اساس حوزه جغرافی تحت پوشش

شبکه های کامپیوتری با توجه به حوزه جغرافیائی تحت پوشش به سه گروه تقسیم می گردند :

- شبکه های محلی کوچک یا LAN
- شبکه های متوسط یا MAN
- شبکه های گسترده یا WAN

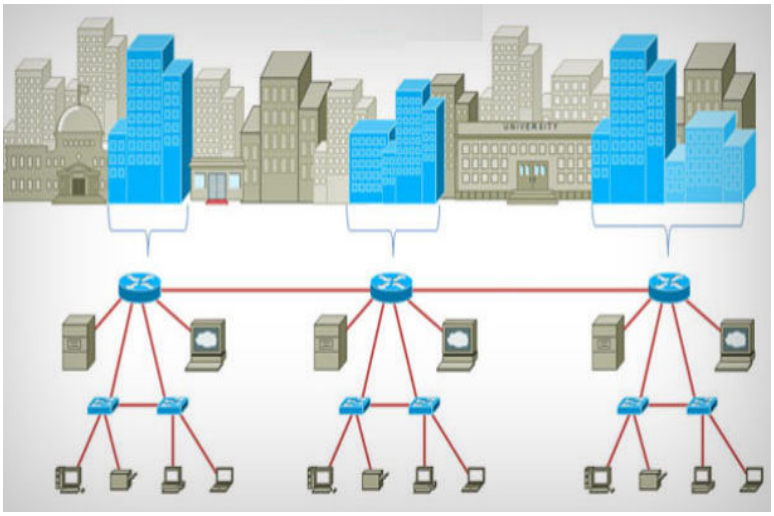
## شبکه های LAN




شبکه LAN یا Local Area Network کوچکترین نوع شبکه کامپیوتر است. حوزه جغرافیائی که توسط این نوع از شبکه ها پوشش داده می شود ، یک محیط کوچک نظیر یک ساختمان اداری، مدرسه، شرکت، ساختمان مسکونی و یا تجاری است . این شبکه برای انتقال اطلاعات در داخل یک مجموعه کوچک راه اندازی می شود و نیازی به هماهنگی با مخابرات یا سایر سازمان ها نمی باشد. این نوع از شبکه ها دارای ویژگی های زیر می باشند :

- توانائی ارسال اطلاعات با سرعت بالا
- محدودیت فاصله
- قابلیت استفاده از محیط مخابراتی ارزان نظیر خطوط تلفن به منظور ارسال اطلاعات
- نرخ پایین خطا در ارسال اطلاعات با توجه به محدود بودن فاصله
- عیب یابی سریع در شبکه

## شبکه های MAN



شبکه MAN یا Metropolitan Area Network از مجموع چند شبکه LAN بوجود می آید. این شبکه برای راه اندازی نیاز به مجوز مخابرات و سازمان ها یی مثل سازمان تنظیم قوانین و مقررات ارتباطات رادیویی دارد. حوزه جغرافیائی که توسط این نوع از شبکه ها پوشش داده می شود ، یک مجموعه شهری می باشد. این شبکه برای انتقال اطلاعات در بین شعبات یک شرکت، مؤسسه یا اداره در یک شهر راه اندازی می شود. این نوع از شبکه ها دارای ویژگی های زیر می باشند :

- پیچیدگی بیشتر نسبت به شبکه های محلی
- قابلیت ارسال تصاویر و صدا
- قابلیت ایجاد ارتباط بین چندین شبکه
- هزینه راه اندازی بیشتر نسبت به LAN
- سرعت پایین تر نسبت به LAN
- نرخ بالای خطا در ارسال اطلاعات
- عیب یابی سخت تر در شبکه

## شبکه های WAN

شبکه WAN یا World Area Network بزرگترین و پیچیده ترین نوع شبکه است. حوزه جغرافیائی که توسط این نوع شبکه ها پوشش داده می شود ، در حد و اندازه کشور و قاره است. مجوز این شبکه برای راه اندازی به دولت ها و شرکت بزرگ داده می شود. شبکه اینترنت، بزرگترین شبکه WAN در جهان است. این نوع از شبکه ها دارای ویژگی های زیر می باشند :

- قابلیت ارسال اطلاعات بین کشورها و قاره ها
- قابلیت ایجاد ارتباط بین شبکه های LAN
- سرعت پایین ارسال اطلاعات نسبت به شبکه های LAN و MAN
- نرخ خطای بالا با توجه به گستردگی محدوده تحت پوشش
- عیبا یابی خیلی سخت تر در شبکه

## کابل در شبکه

در شبکه های محلی از کابل به عنوان محیط انتقال و به منظور ارسال اطلاعات استفاده می گردد. ازچندین نوع کابل در شبکه های محلی استفاده می گردد. در برخی موارد ممکن است در یک شبکه صرفاً از یک نوع کابل استفاده و یا با توجه به شرایط موجود از چندین نوع کابل استفاده گردد. نوع کابل انتخاب شده برای یک شبکه به عوامل متفاوتی نظیر: توپولوژی شبکه، پروتکل و اندازه شبکه بستگی خواهد داشت . آگاهی از خصایص و ویژگی های متفاوت هر یک از کابل ها و تاثیر هر یک از آنها بر سایر ویژگی های شبکه، به منظور طراحی و پیاده سازی یک شبکه موفق بسیار لازم است.

## کابل UTP (Unshielded Twisted pair)

متداولترین نوع کابلی که در انتقال اطلاعات استفاده می گردد ، کابل های بهم تابیده می باشند. این نوع کابل ها دارای دو رشته سیم به هم پیچیده بوده که هر دو نسبت زمین دارای یک امپدانش یکسان می باشند. بدین ترتیب امکان تاثیر پذیری این نوع کابل ها از کابل های مجاور و یا سایر منابع خارجی کاهش خواهد یافت . کابل های بهم تابیده دارای دو مدل متفاوت : Shielded ( روکش دار ) و Unshielded ( بدون روکش ) می باشند. کابل UTP نسبت به کابل STP بمراتب متداول تر بوده و در اکثر شبکه های محلی استفاده می گردد.کیفیت کابل های UTP متغیر بوده و از کابل های معمولی استفاده شده برای تلفن تا کابل های با سرعت بالا را شامل می گردد. کابل دارای چهار زوج سیم بوده و درون یک روکش قرار می گیرند. هر زوج با تعداد مشخصی پیچ تابانده شده ( در واحد اینچ ) تا تأثیرپذیری آن از سایر زوج ها و یاسایر دستگاههای الکتریکی کاهش یابد.

کابل های UTP دارای استانداردهای متعددی بوده که در گروه های (Categories) متفاوت زیر تقسیم شده اند:

| Type | کاربرد |
|---|---|
| Cat 1 | فقط صوت ( کابل های تلفن ) |
| Cat 2 | داده با سرعت ۴ مگابیت در ثانیه |
| Cat 3 | داده با سرعت ۱۰ مگابیت در ثانیه |
| Cat 4 | داده با سرعت ۲۰ مگابیت در ثانیه |
| Cat 5 | داده با سرعت ۱۰۰ مگابیت در ثانیه |

### مزایای کابل های بهم تابیده :

- سادگی و نصب آسان
- انعطاف پذیری مناسب
- دارای وزن کم بوده و براحتی بهم تابیده می گردند.

### معایب کابل های بهم تابیده :

- تضعیف فرکانس
- بدون استفاده از تکرارکننده ها ، قادر به حمل سیگنال در مسافت های طولانی نمی باشند.
- پایین بودن پهنای باند
- بدلیل پذیرش پارازیت در محیط های الکتریکی سنگین بخدمت گرفته نمی شوند.

## کابل کواکسیال

یکی از مهمترین محیط های انتقال در مخابرات کابل کواکسیال و یا هم محور می باشد . این نوع کابل ها از سال ۱۹۳۶ برای انتقال اخبار و اطلاعات در دنیا به کار گرفته شده اند. در این نوع کابل ها، دو سیم تشکیل دهنده یک زوج، از حالت متقارن خارج شده و هر زوج از یک سیم در مغز و یک لایه مسی بافته شده در اطراف آن تشکیل می گردد. در نوع دیگر کابل های کواکسیال ، به حای لایه مسی بافته شده ، از تیوپ مسی استوانه ای استفاده می شود. ماده ای پلاستیکی این دو هادی را از یکدیگر جدا می کند. ماده پلاستیکی ممکن است بصورت دیسکهای پلاستیکی یا شیشه ای در فواصل مختلف استفاده و مانع از تماس دو هادی با یکدیگر شود و یا ممکن است دو هادی در تمام طول کابل بوسیله مواد پلاستیکی از یکدیگر جدا گردند.

### مزایای کابل های کواکسیال :

- قابلیت اعتماد بالا
- ظرفیت بالای انتقال ، حداکثر پهنای باند ۳۰۰ مگاهرتز
- دوام و پایداری خوب
- پایطن بودن مخارج نگهداری
- قابل استفاده در سیستم های آنالوگ و دیجیتال
- هزینه پائین در زمان توسعه
- پهنای باند نسبتا" وسیع که مورد استفاده اکثر سرویس های مخابراتی از جمله تله کنفرانس صوتی و تصویری است .

### معایب کابل های کواکسیال :

- مخارج بالای نصب
- نصب مشکل تر نسبت به کابل های بهم تابیده
- محدودیت فاصله
- نیاز به استفاده از عناصر خاص برای انشعابات

## فیبر نوری

یکی از جدیدترین محیط های انتقال در شبکه های کامپیوتری ، فیبر نوری است . فیبر نوری از یک میله استوانه ای که هسته نامیده می شود و جنس آن از سیلیکات است تشکیل می گردد. شعاع استوانه بین دو تا سه میکرون است . روی هسته ، استوانه دیگری ( از همان جنس هسته ) که غلاف نامیده می شود ، استقرار می یابد. ضریب شکست هسته را با M1 و ضریب شکست غلاف را با M2 نشان داده و همواره M2<M1 است . در این نوع فیبرها ، نور در اثر انعکاسات کلی در فصل مشترک هسته و غلاف ، انتشار پیدا خواهد کرد. منابع نوری در این نوع کابل ها ، دیود لیزری و یا دیودهای ساطع کننده نور می باشند.منابع فوق ، سیگنال های الکتریکی را به نور تبدیل می نمایند.

### مزایای فیبر نوری :

- حجم و وزن کم
- پهنای باند بالا
- تلفات سیگنال کم و در نتیجه فاصله تقویت کننده ها زیاد می گردد.
- فراوانی مواد تشکیل دهنده آنها
- مصون بودن از اثرات القاهای الکترو معناطیسی مدارات دیگر
- آتش زا نبودن آنها بدلیل عدم وجود پالس الکتریکی در آنها
- مصون بودن در مقابل عوامل جوی و رطوبت
- سهولت در امر کابل کشی و نصب
- استفاده در شبکه های مخابراتی آنالوگ و دیجیتال
- مصونیت در مقابل پارازیت

### معایب فیبر نوری :

- براحتی شکسته شده و می بایست دارای یک پوشش مناسب باشند. مسئله فوق با ظهور فیبر های تمام پلاستیکی و پلاستیکی / شیشه ای کاهش پیدا کرده است .
- اتصال دو بخش از فیبر یا اتصال یک منبع نور به فیبر ، فرآیند دشواری است . در چنین حالتی می توان از فیبرهای ضخیم تر استفاده کرد اما این مسئله باعث تلفات زیاد و کم شدن پهنای باند می گردد.
- از اتصالات T شکل در فیبر نوری نمی توان جهت گرفتن انشهاب استفاده نمود. در چنین حالتی فیبر می بایست بریده شده و یک Detector اضافه گردد. دستگاه فوفق می بایست قادر به دریافت و تکرار سیگنال را داشته باشد.
- تقویت سیگنال نوری یکی از مشکلات اساسی در زمینه فیبر نوری است . برای تقویت سیگنال می بایست سیگنال های توری به سیگنال های الکتریکی تبدیل ، تقویت و مجددا" به علائم نوری تبدیل شوند.

## آشنایی با مدلOSI (هفت لایه شبکه)

انتقال اطلاعات بین کامپیوترهای مختلف در شبکه وابسته به انتقال اطلاعات بین بخش های نرم افزاری و سخت افزاری درون هر یک از کامپیوترهاست. هر یک از فرایند های انتقال اطلاعات را می توان به بخش های کوچک تری تقسیم کرد. هر یک از این فعالیت های کوچک را سیستم عامل براساس دسته ای از قوانین مشخص انجام می دهد. این قوانین را پروتکل می نامند .برای استانداردسازی پروتکل های ارتباطی، سازمان استاندارد های بین المللی (ISO) در سال ۱۹۸۴ اقدام به تعیین مدل مرجع OSI یا Open Systems Interconnection نمود. مدل مرجع OSI ارائه دهنده چارچوب طراحی محیط های شبکه ای است و در آن کلیه فعالیت های شبکه ای در هفت لایه مدل سازی می شود. در نظر گرفتن عملیات انتقال اطلاعات بین لایه های متناظر مدل OSI واقع در کامپیوتر های مبدا و مقصد را انتقال مجازی یا Virtual می نامند. حرکت اطلاعات در کامپیوتر مبدأ از لایه فوقانی به طرف لایه تحتانی مدل OSI و از آنجا به لایه زیرین مدل OSI واقع در کامپیوتر مقصد صورت می گیرد. در کامپیوتر مقصد اطلاعات از لایه های زیرین به طرف بالاترین لایه مدل OSI حرکت می کنند. عمل انتقال اطلاعات از یک لایه به لایه دیگر در مدل OSI از طریق واسطه ها یا Interface ها انجام می شود. این واسطه ها تعیین کننده سرویس هایی هستند که هر لایه مدل OSI می تواند برای لایه مجاور فراهم آورد.

### ۱- لایه فیزیکی یاPhysical

لایه زیرین در مدلOSI است. این لایه اطلاعات را بصورت جریانی از رشته های داده ای و بصورت الکترونیکی روی کابل هدایت می کند. این لایه تعریف کننده ارتباط کابل و کارت شبکه و همچنین تعیین کننده تکنیک ارسال و دریافت داده ها نیز هست .

### ۲- لایه پیوند یاData Link

لایه دوم مدلOSI است. این لایه وظیفه دارد تا اطلاعات دریافت شده از لایه شبکه را به قالبی منطقی به نام فریم (Frame)تبدیل کند.

### ۳- لایه شبکه یا Network

لایه سوم در مدلOSI است. این لایه مسئول آدرس یا نشانی گذاری پیام ها و تبدیل نشانی های منطقی به آدرس های فیزیکی و نیز مدیریت مشکلات مربوط به ترافیک شبکه نظیر کند شدن جریان اطلاعات است.

### ٤- لایه انتقال یاTransmission

لایه چهارم مدل OSI است. این لایه مسئول ارسال و دریافت اطلاعات و کمک به رفع خطاهای ایجاد شده در طول ارتباط است که در صورت بروز خطا در حین ارتباط، این لایه مسئول تکرار عملیات ارسال داده است .

### ۵- لایه جلسه یاSession

لایه پنجم مدل OSI است. این لایه بر برقراری اتصال بین دو برنامه کاربردی روی دو کامپیوتر مختلف واقع در شبکه نظارت دارد. همچنین تأمین کننده همزمانی فعالیت های کاربر نیز هست .

### ۶- لایه نمایش یا Presentation

لایه ششم مدل OSI است. این لایه تعیین کننده فرمت یا قالب انتقال داده ها بین کامپیوتر های واقع در شبکه است. این لایه در کامپیوتر مبدا داده هایی که باید انتقال داده شوند را به یک قالب میانی تبدیل می کند. این لایه در کامپیوتر مقصد اطلاعات را از قالب میانی به قالب اولیه تبدیل می کند .

### ۷- لایه کاربرد یا Application

بالاترین لایه مدل OSI یا لایه هفت، است. این لایه تأمیین کننده سرویس های پشتیبانی برنامه های کاربردی نظیر انتقال فایل، دسترسی به بانک اطلاعاتی و پست الکترونیکی است .

## پروتکل ها

فرآیند به اشتراک گذاشتن اطلاعات، نیازمند ارتباط همزمان شده ای بین کامپیوتر های شبکه است. برای ایجاد سهولت در این فرایند، برای هر یک از فعالیت های ارتباط شبکه ای، مجموعه ای از دستور العمل ها تعریف شده است. هر دستورالعمل ارتباطی یک پروتکل یا قرارداد نام دارد. یک پروتکل تأمین کننده توصیه هایی برای برقراری ارتباط بین اجزای نرم افزاری و سخت افزاری در انجام یک فعالیت شبکه ای است. هر فعالیت شبکه ای به چندین مرحله سیستماتیک تفکیک می شود. هر مرحله با استفاده از یک پروتکل منحصر به فرد، یک عمل مشخص را انجام می دهد. این مراحل باید با ترتیب یکسان در تمام کامپیوترهای واقع در شبکه انجام شوند. در کامپیوتر مبدا مراحل ارسال داده از لایه بالایی شروع شده و به طرف لایه زیرین ادامه می یابد. در کامپیوتر مقصد مراحل مشابه در جهت معکوس از پایین به بالا انجام می شود. در کامپیوتر مبدأ، پروتکل، اطلاعات را به قطعات کوچک شکسته، به آن ها آدرس هایی نسبت می دهند و قطعات حاصله یا بسته ها را برای ارسال از طریق کابل آماده می کنند. در کامپیوتر مقصد، پروتکل ها داده ها را از بسته ها خارج کرده و به کمک نشانی های آن ها بخش های مختلف اطلاعات را با ترتیب صحیح به هم پیوند می دهند تا اطلاعات به صورت اولیه بازیابی شوند .

پروتکل های مسئول فرآیندهای ارتباطی مختلف برای جلوگیری از تداخل و یا عملیات ناتمام، لازم است که به صورت گروهی به کار گرفته شوند. این عمل به کمک گروه بندی پروتکل های مختلف در یک معماری لایه ای به نام Protocol Stack یا پشته پروتکل انجام می گیرد. لایه های پروتکل های گروه بندی شده با لایه های مدل OSI انطباق دارند. هر لایه در مدل OSI پروتکل مشخصی را برای انجام فعالیت های خود بکار می برد. پروتکل ها براساس آن که به کدام لایه از مدل OSI متعلق باشند، سه نوع طبقه بندی می شوند.

۱- پروتکل های مربوط به سه لایه بالایی مدل OSI به پروتکل های Application یا کاربرد معروف هستند. پروتکل های لایه Application تأمین کننده سرویس های شبکه در ارتباط بین برنامه های کاربردی با یکدیگر هستند .این سرویس ها شامل انتقال فایل، چاپ، ارسال پیام و سرویس های بانک اطلاعاتی هستند. پروتکل های لایه نمایش یا Presentation وظیفه قالب بندی و نمایش اطلاعات را قبل از ارسال بر عهده دارند. پروتکل های لایه جلسه یا Session اطلاعات مربوط به جریان ترافیک را به داده ها اضافه می کنند .

۲- پروتکل های نوع دوم که به پروتکل های انتقال Transmission معروف هستند، منطبق بر لایه انتقال مدل OSI هستند. این پروتکل ها اطلاعات مربوط به ارسال بدون خطا یا در واقع تصحیح خطا را به داده ها می افزایند.

۳- وظایف سه لایه زیرین مدل OSI بر عهده پروتکل های شبکه است. پروتکل های لایه شبکه تامین کننده فرآیندهای آدرس دهی و مسیریابی اطلاعات هستند. پروتکل های لایه Data Link اطلاعات مربوط به بررسی و کشف خطا را به داده ها اضافه می کنند و به درخواست های ارسال مجدد اطلاعات پاسخ می گویند. پروتکل های لایه فیزیکی تعیین کننده استاندارد های ارتباطی در محیط مشخصی هستند.

## امنیت شبکه های کامپیوتری

امنیت ، مبحثی کاملا پیچیده ولی با اصولی ساده است . امنیت یک پردازش چند لایه است. تعیین نوع و نحوه تلقین لایه های دفاعی مورد نیاز ، فقط پس از تکمیل ارزیابی قابل ارائه است . تهیه لیستی از سیاست های اجرایی بر مبنای اینکه چه چیزی برای سازمان مهم تر و انجام آن ساده تر است در اولویت قرار دارد. پس از آنکه این اولویت ها به تایید رسیدند هر یک از آنها باید به سرعت در جای خود به اجرا گذارده شود. ارزیابی امنیتی یک بخش بسیار مهم تر از برنامه ریزی امنیتی است. ارزیابی امنیتی خطوط اصلی را برای پیاده سازی طرح امنیتی مشخص می کند.

خطر زمانی قابل درک است که یک تهدید، از نقاط ضعف موجود برای آسیب زدن به سیستم استفاده کند. لذا، پس از آنکه خطرات شناخته شدند، می توان طرح ها و روش هایی را برای مقابله با تهدیدات و کاهش میزان آسیب پذیری آنها ایجاد کرد. طرح امنیتی به طور مدام باید به روز شود. به علاوه هر زمان که تغییرات عمده ای در ساختار و یا عملکردها به وجود آمد، می بایست ارزیابی مجددی صورت گیرد. ارزیابی ها حداقل می بایست شامل رویه هایی برای موارد زیر باشند:

۱- رمز های عبور
۲- مدیریت اصلاحیه ها
۳- آموزش کارکنان و نحوه اجرای برنامه ها
۴- نحوه تهیه فایل های پشتیبان و فضای مورد نیاز آن
۵- ضد ویروس
۶- دیواره آتش
۷- شناسایی و جلوگیری از نفوذ گران
۸- فیلترینگ های مختلف برای اینترنت و پست الکترونیکی
۹- تنظیمات سیستمی و پیکره بندی آنها

برای تامین امنیت بر روی یک شبکه، یکی از بحرانی ترین و خطیرترین مراحل، تامین امنیت دسترسی و کنترل تجهیزات شبکه است. تجهیزاتی همچون مسیریاب، سوئیچ یا دیوارهای آتش. موضوع امنیت تجهیزات به دو علت اهمیت ویژه‌ای می‌یابد :

الف – عدم وجود امنیت تجهیزات در شبکه ، به نفوذگران شبکه اجازه می‌دهد که با دستیابی به تجهیزات ، امکان پیکربندی آنها را به گونه‌ای که تمایل دارند آن سخت‌افزارها عمل کنند، داشته باشند. از این طریق هرگونه نفوذ و سرقت اطلاعات و یا هر نوع صدمه دیگری به شبکه، توسط نفوذگر، امکان‌پذیر خواهد شد.

ب – برای جلوگیری از خطرهای DoS (Denial of Service) تأمین امنیت تجهیزات بر روی شبکه الزامی است. توسط این حمله‌ها نفوذگران می‌توانند سرویس‌هایی را در شبکه از کار بیاندازند که از این طریق در برخی موارد امکان دسترسی به اطلاعات با دور زدن هر یک از فرایندهای شبکه فراهم می‌شود. موضوعات فوق در قالب دو بحث اصلی امنیت تجهیزات مورد بررسی قرار می‌گیرند :

## ۱- امنیت فیزیکی

امنیت فیزیکی، حیطه وسیعی از تدابیر را در بر می‌گیرد که استقرار تجهیزات در مکان‌های امن و به دور از خطر حملات نفوذگران و استفاده از افزایش تعداد پشتیبان سیستم، از آن جمله‌اند. با استفاده از افزایش تعداد پشتیبان، اطمینان از صحت عملکرد سیستم در صورت بروز و وقوع نقص در یکی از تجهیزات بدست می‌آید.

### ۱-۱- افزایش تعداد پشتیبان در محل استقرار شبکه

یکی از راه‌کارها در قالب تهیه پشتیبان از شبکه‌های کامپیوتری، ایجاد سیستم ثانویه کاملاً مشابه شبکه اولیه در حال کار است. با استفاده از این دو سیستم مشابه، علاوه بر آنکه در صورت رخداد وقایعی که کارکرد هریک از این دو شبکه را به طور کامل مختل می‌کند (مانند زلزله) می‌توان از شبکه‌ی دیگر به طور کاملاً جایگزین استفاده کرد، در استفاده‌های روزمره نیز در صورت ایجاد ترافیک سنگین بر روی شبکه، حجم ترافیک و پردازش بر روی دو شبکه‌ی مشابه پخش می‌شود تا زمان پاسخ به حداقل ممکن برسد.

با وجود آنکه استفاده از این روش در شبکه‌های معمول که حجم چندانی ندارند، به دلیل هزینه‌های تحمیلی بالا، امکان‌پذیر و اقتصادی به نظر نمی‌رسد، ولی در شبکه‌های با حجم بالا که قابلیت اطمینان و امنیت در آنها از اصول اولیه به حساب می‌آیند از الزامات است.

### ۱-۲- توپولوژی شبکه

طراحی توپولوژیکی شبکه، یکی از عوامل اصلی است که در زمان رخداد حملات فیزیکی می‌تواند از خطای کلی شبکه جلوگیری کند. در این مقوله، سه طراحی که معمول هستند مورد بررسی قرار می‌گیرند :

الف – طراحی سری ( Bus) :

در این طراحی با قطع خط تماس میان دو نقطه در شبکه، کلیه سیستم به دو تکه منفصل تبدیل شده و امکان سرویس دهی از هریک از این دو ناحیه به ناحیه دیگر امکان پذیر نخواهد بود.

ب – طراحی ستاره‌ای ( Star) :

در این طراحی، در صورت رخداد حمله فیزیکی و قطع اتصال یک نقطه از سرور اصلی، سرویس‌دهی به دیگر نقاط دچار اختلال نمی‌گردد. با این وجود از آنجا که سرور اصلی در این میان نقش محوری دارد، در صورت اختلال در کارایی این نقطه مرکزی (مثل حمله فیزیکی به آن)، ارتباط کل شبکه دچار اختلال می‌شود.

ج – طراحی مش ( Mesh) :

در این طراحی هرگونه اختلال فیزیکی در سطوح دسترسی منجر به اختلال عملکرد شبکه نخواهد شد ولی زمان‌بندی سرویس‌دهی را دچار اختلال می کند. پیاده‌سازی چنین روش با وجود امنیت بالا، به دلیل محدودیت‌های اقتصادی، تنها در موارد خاص و بحرانی انجام می‌گیرد.

### ۱-۳- محل‌های امن برای تجهیزات

در مجموع می‌توان اصول زیر را برای تضمین نسبی امنیت فیزیکی تجهیزات در نظر داشت :

- محدود سازی دسترسی به تجهیزات شبکه با استفاده از قفل‌ها و مکانیزم‌های دسترسی دیجیتالی به همراه ثبت زمان‌ها، مکان‌ها و کدهای کاربری دسترسی‌های انجام شده.

- استفاده از دوربین‌های حفاظتی در ورودی محل‌های استقرار تجهیزات شبکه و اتاق‌های اتصالات و مراکز پایگاه های داده.

- اعمال ترفندهایی برای اطمینان از رعایت اصول امنیتی.

### ۱-۴- انتخاب لایه کانال ارتباطی امن

با وجود آنکه زمان حمله‌ی فیزیکی به شبکه‌های کامپیوتری، آنگونه که در قدیم شایع بوده، گذشته است عمل شنود بر روی سیم‌های مسی، چه در انواع Coax و چه در زوج‌های تابیده، هم‌اکنون نیز از راه‌های نفوذ به شمار می‌آیند. با استفاده از شنود می‌توان اطلاعات بدست آمده از تلاش‌های دیگر برای نفوذ در سیستم‌های کامپیوتری را گسترش داد و به جمع بندی مناسبی برای حمله رسید. در حال حاضر، امن ترین روش ارتباطی در لایه‌ی فیزیکی، استفاده از فیبرهای نوری است. در این روش به دلیل نبود سیگنال‌های الکتریکی، هیچگونه تشعشعی از نوع الکترومغناطیسی وجود ندارد، لذا امکان استفاده از روش‌های معمول شنود به پایین‌ترین حد خود نسبت به استفاده از سیم در ارتباطات می‌شود.

### ۱-۵- منابع تغذیه

از آنجاکه داده‌های شناور در شبکه به منزله‌ی خون در رگهای ارتباطی شبکه هستند و جریان آنها بدون وجود منابع تغذیه، که با فعال نگاه‌داشتن نقاط شبکه موجب برقراری این جریان هستند، غیر ممکن است، لذا چگونگی پیکربندی و نوع منابع تغذیه و قدرت آنها نقش به سزایی در این میان بازی می‌کنند. در این مقوله توجه به دو نکته زیر از بالاترین اهمیت برخوردار است :

- طراحی صحیح منابع تغذیه در شبکه به گونه‌ای که تمامی تجهیزات فعال شبکه، برق مورد نیاز خود را بدون آنکه به شبکه‌ی برق، فشار بیش از اندازه‌ای وارد شود، بدست آورند.
- وجود منبع یا منابع تغذیه پشتیبان ( UPS) به گونه‌ای که تعداد و یا توان پشتیبانی آنها به نحوی باشد که نه تنها برای تغذیه کل شبکه در مواقع نیاز به منابع تغذیه پشتیبان کفایت کند، بلکه امکان تامین برق بیش از مورد نیاز برای تعدادی از تجهیزات بحرانی درون شبکه را به صورت منفرد فراهم کند.

### ۱-۶- عوامل محیطی

یکی از نکات بسیار مهم در امن سازی فیزیکی تجهیزات و منابع شبکه، امنیت در برار عوامل محیطی است. از مهمترین عواملی در هنگام بررسی امنیتی یک شبکه رایانه‌ای باید در نظر گرفت می‌توان به دو عامل زیر اشاره کرد :

- احتمال حریق (که عموماً غیر طبیعی است و منشأ انسانی دارد)
- زلزله، طوفان و دیگر بلایای طبیعی

تنها راه حل عملی و قطعی برای مقابله با چنین وقایعی، با هدف جلوگیری در اختلال کلی در عملکرد شبکه، وجود یک سیستم کامل پشتیبان برای کل شبکه است.

## ۲- امنیت منطقی

امنیت منطقی به معنای استفاده از روش‌هایی برای پایین آوردن خطرات حملات منطقی و نرم‌افزاری بر ضد تجهیزات شبکه است. در ذیل به مواردی که در اینگونه حملات و ضد حملات مورد نظر قرار می‌گیرند می‌پردازیم.

### ۲-۱- امنیت مسیریاب‌ها

حملات ضد امنیتی منطقی برای مسیریاب‌ها و دیگر تجهیزات فعال شبکه، مانند سوئیچ‌ها، را می‌توان به سه دسته‌ی اصلی تقسیم نمود: حمله برای

غیرفعال سازی کامل  دستیابی به سطح کنترل  ایجاد نقص در سرویس‌دهی

### ۲-۲- مدیریت پیکربندی

یکی از مهمترین نکات در امینت تجهیزات، نگاهداری نسخ پشتیبان از پرونده‌ها مختص پیکربندی است. با وجود نسخ پشتیبان، منطبق با آخرین تغییرات اعمال شده در تجهیزات، در هنگام رخداد اختلال در کارایی تجهزات، که می‌تواند منجر به ایجاد اختلال در کل شبکه شود، در کوتاه ترین زمان ممکن می‌توان با جایگزینی آخرین پیکربندی، وضعیت فعال شبکه را به آخرین حالت بی‌نقص پیش از اختلال بازگرداند.

### ۲-۳- کنترل دسترسی به تجهیزات

دو راه اصلی برای کنترل تجهزات فعال وجود دارد :

- کنترل از راه دور که با اعمال محدودیت در امکان پیکربندی و دسترسی به تجهیزات از آدرس‌هایی خاص یا استانداردها و پروتکل‌های خاص، می‌توان احتمال حملات را پایین آورد.

- کنترل از طریق درگاه کنسول که در صورت عدم کنترل این نوع دسترسی، ایجاد محدودیت‌ها در روش اول عملاً امنیت تجهیزات را تأمین نمی‌کند.

### ۲-۴- امن سازی دسترسی

یکی دیگر از روش‌های معمول امن‌سازی دسترسی، استفاده از کانال رمز شده در حین ارتباط است. یکی از ابزار معمول در این روش، SSH یا Secure Shell است. SSH ارتباطات فعال را رمز کرده و احتمال شنود و تغییر در ارتباط که از معمول‌ترین روش‌های حمله هستند را به حداقل می‌رساند.

از دیگر روش‌های معمول می‌توان به استفاده از کانال‌های VPN مبتنی بر IPSec اشاره نمود. این روش نسبت به روش استفاده از SSH روشی با قابلیت اطمینان بالاتر است.

### ۲-۵- مدیریت رمزهای عبور

مناسب ترین محل برای ذخیره رمزهای عبور بر روی سرور Authentication است. در بسیاری از موارد لازم است که بسیاری از این رموز بر روی خود سخت‌افزار نگاه‌داری شوند.

## ۳- ملزومات و مشکلات امنیتی ارائه دهندگان خدمات

زمانی که سخن از ارائه دهندگان خدمات و ملزومات امنیتی آنها به میان می‌آید، مقصود شبکه‌های بزرگی است که خود به شبکه‌های رایانه‌ای کوچکتر خدماتی ارائه می‌دهند. با وجود آنکه غالب اصول امنیتی در شبکه‌های کوچکتر رعایت می‌شود، ولی با توجه به حساسیت انتقال داده در این اندازه، ملزومات امنیتی خاصی برای این قبیل شبکه‌ها مطرح هستند.

### ۳-۱- قابلیت‌های امنیتی

ملزومات مذکور را می‌توان، تنها با ذکر عناوین، به شرح زیر فهرست نمود :

- قابلیت بازداری از حمله و اعمال تدابیر صحیح برای دفع حملات
- وجود امکان بررسی ترافیک شبکه، با هدف تشخیص بسته‌هایی که به قصد حمله بر روی شبکه ارسال می‌شوند.
- قابلیت تشخیص منبع حملات.

### ۳-۲- مشکلات اعمال ملزومات امنیتی

با وجود لزوم وجود قابلیت‌هایی که بطور اجمالی مورد اشاره قرار گرفتند، پیاده‌سازی و اعمال آنها همواره آسان نیست. یکی از معمول‌ترین مشکلات، پیاده‌سازی IDS (خطر یا ترافیکی که برای یک دسته از کاربران به عنوان حمله تعبیر می‌شود، برای دسته‌ای دیگر به عنوان جریان عادی داده است) می باشد.

در نهایت، تضمین امنیت، از اولین انتظاراتی است که شبکه‌های بزرگ می‌توان داشت.

موفق و پیروز باشید