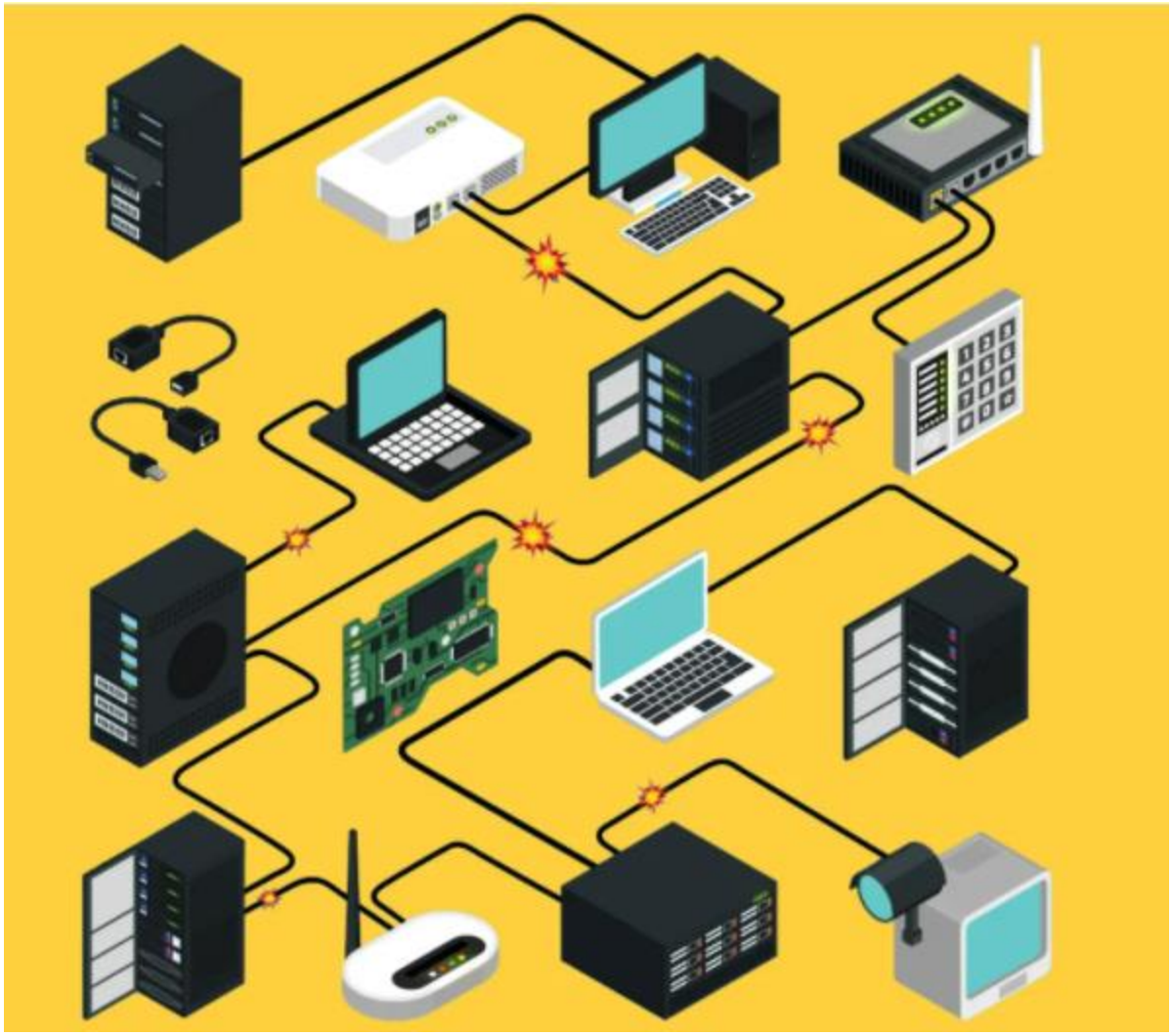
اکتیو شبکه :

اکتیو به معنی فعال است و در حوزه شبکه به معنی تاثیر گذار بودن روی جریان الکتریکی است.

اکتیو شبکه پیکربندی دستگاه‌هایی مثل روتر، سوئیچ و فعالیت‌های نرم افزاری را برعهده می‌گیرد و به تعبیر دیگر روی تجهیزات فیزیکی شبکه اجرا می‌شود.



تقسیم بندی کلی شبکه اکتیو

انرژی شبکه در هر اکتیو نتورک توسط دست‌کم یک منبع ولتاژ یا تامین می‌شود. این منابع قادرند به‌طرز عجیبی انرژی شبکه را نامحدود تامین کنند. اگر بخواهیم اکتیو شبکه را با توجه به نوع تجهیزات به‌کاررفته در آن تقسیم‌بندی کنیم، به این دو نوع می‌رسیم: شبکه اکتیو مسی و شبکه اکتیو نوری.

شبکه اکتیو مسی

در شبکه‌های پسیو یک مشکل بزرگ وجود داشت و آن قدرت سیگنال بود. این شبکه‌ها فقط قادر بودند چند دستگاه محدود را به هم وصل کنند. اما شبکه اکتیو مسی با استفاده از کابلی که به یک تقویت‌کننده وصل شده، توزیع سیگنال را چند برابر بیشتر می‌کند و به قدرت بیشتری نیاز دارد.

در این حالت قدرت سیگنال کابل ورودی را می‌توان با خروجی تقویت‌کننده توزیع یکی دانست. به این ترتیب به جای آنکه از چند سیستم استفاده شود، با یک کابل دسترسی برای تمام دستگاه‌ها فراهم می‌شود. کافی است یک کابل مجزا بین تقویت کننده و تلویزیون‌ها کشیده شود. البته این سیستم ایراداتی هم دارد. مثلا اینکه در صورت خرابی تقویت‌کننده یا قطع برق، سیگنال کل دستگاه‌ها خاموش می‌شود.

شبکه اکتیو نوری

شبکه اکتیو نوری را می‌توان تا حد زیادی مشابه شبکه مسی اکتیو (مورد قبل) دانست؛ با این تفاوت که اینجا خبری از تقویت‌کننده توزیع نیست و برای سیگنال‌رسانی، از فیبر نوری استفاده می‌شود. کابل فیبر هر کاربر مستقیما به سوئیچ متصل است و داده‌ها را از آن می‌گیرد. این یعنی باز هم مشکل قدرت سیگنال که در شبکه‌های پسیو شاهدش بودیم، حل شده است. اما همچنان هرگونه خرابی و قطع برق سوئیچ، عدم دسترسی کاربران به داده‌های ورودی را به همراه خواهد داشت. البته در اکتیو نتورک‌های نوری برای تقویت سیگنال از تقویت‌کننده‌های نوری استفاده می‌شود.

خدمات اکتیو شبکه

به‌محض آنکه خدمات پسیو راه‌اندازی شدند، وقت پیکربندی خدمات Active Network است. تنظیمات و پیکربندی‌های سخت‌افزارها باید در این مرحله انجام شوند. از تضمین امنیت با نصب و راه‌اندازی آنتی‌ویروس گرفته تا پیکربندی نرم افزارها، از تنظیم و پیکر بندی تجهیزات وایرلس تا پیکربندی روتر و سوئیچ بکاپ‌گیر خودکار، از انواع مجازی سازی گرفته تا ارائه سرویس‌های مبتنی بر ویپ، از نصب برنامه‌های مدیریت دسترسی تا راه اندازی سیستم‌عامل‌ها، از نصب و پیکربندی فایروال‌ها گرفته تا ارائه سرویس‌های مجازی خصوصی، همه و همه بخشی از خدمات اکتیو شبکه هستند که در این مرحله صورت می‌گیرند.

خدمات اکتیو شبکه به خدماتی گفته می شود که تجهیزات اکتیو شبکه را نصب و راه اندازی کند که هر کدام از تجهیزات اکتیو نام برده شده در بالا دانش و تخصص خاص خود را برای نصب و راه اندازی نیاز دارد.

به عنوان نمونه بر روی هر سرور می تواند سرویس های تخصصی زیادی نصب شود که هر کدام فرد متخصص مربوط به خود را دارد.

در زیر به برخی از سرویس های مختلف سرور اشاره می کنیم :

- سرویس اکتیو دیرکتوری(Active Directory)
- سرویس اشتراک گذاری فایل ها
- سرویس آنتی ویروس
- سرویس نرم افزار های مالی
- سرویس اتوماسیون های مالی
- سرویسCRM
- سرویس بکاپ گیری
- سرویس تلفنVOIP

همچنین خدمات نصب و راه اندازی هر کدام از تجهیزات نام برده شده خود زیر مجموعه خدمات اکتیو شبکه حساب می شوند ، همانند موارد زیر:

- خدمات نصب و راه اندازی روتر میکروتیک
- خدمات نصب و راه اندازی مودم اینترنت
- خدمات نصب و راه اندازی سرور
- خدمات نصب و راه اندازی دیواره آتش(Firewall)
- خدمات نصب و راه اندازی دستگاه ذخیره سازی اطلاعات در شبکه(NAS)

از چه تیمی خدمات اکتیو شبکه بگیریم؟

خدمات شبکه اکتیو درست مثل تمام بخش‌های مرتبط با شبکه به علم و هنر دست متخصصان کاربلد و حرفه‌ای اکتیوکار نیاز دارد. دقت کنید لزوما هرکسی که مدتی در زمینه پیکربندی فعالیت کرده یا درسش را خوانده، از عهده این کار تخصصی برنمی‌آید و کارشناسان تیم انتخابی باید سابقه تجربی در این زمینه داشته باشند. چرا می‌گوییم این مسئله از اهمیت و جدیت بالایی برخوردار است؟

چون علاوه بر پیکربندی، مستندسازی تجهیزات سخت‌افزاری و نرم‌افزاری یک گام بسیار مهم است که هرکسی دانش این کار را ندارد. شبکه به یک نقشه جامع شامل تمام تجهیزات سخت‌افزاری و زیرساختی به‌کار رفته احتیاج دارد تا مرجعی برای رفع ایرادات پیش‌آمده باشد. تیم خدمات شبکه اکتیو باید این سطح از پشتیبانی را ارائه دهند تا مدیر سرور همواره یک آگاهی نسبی از وضعیت شبکه داشته باشد و

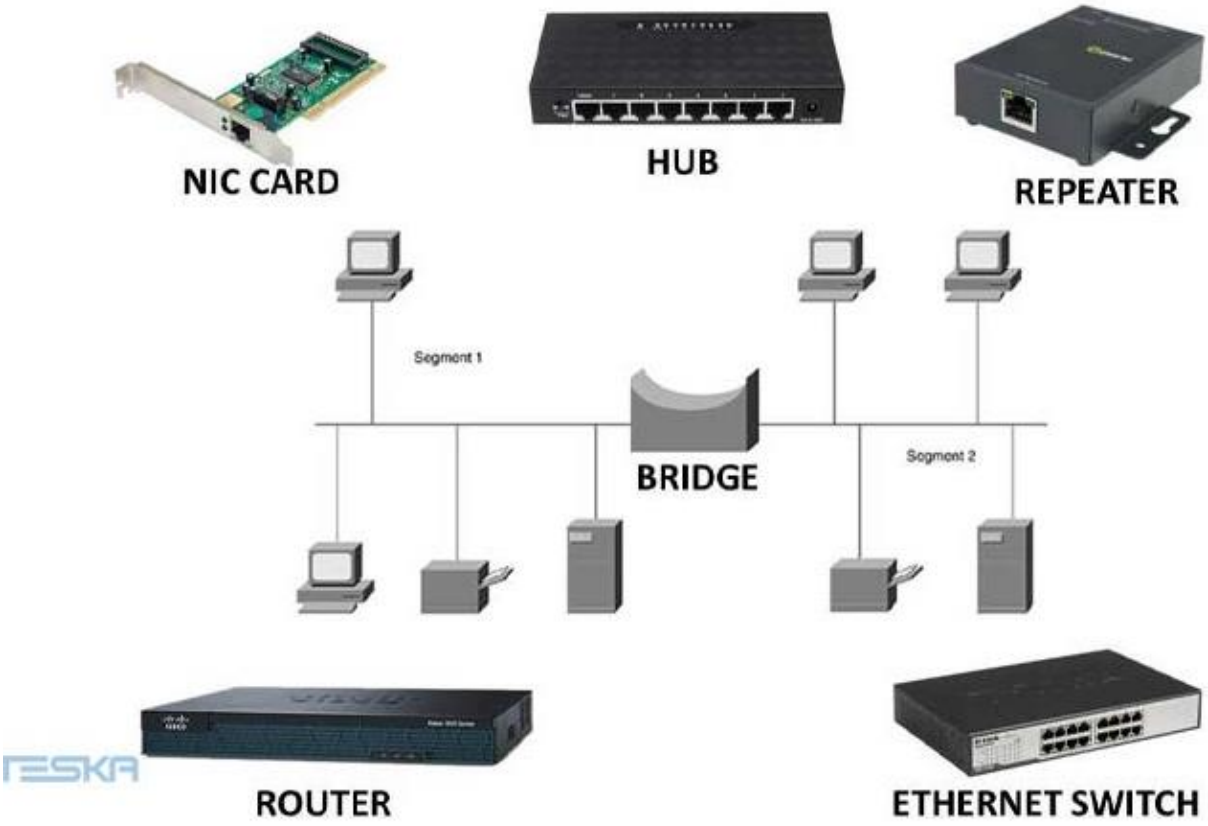
جلوی هدررفت زمان و سرمایه را به‌موقع بگیرد. دقت کنید که اهمیت مسئله مستندسازی با گسترش وسعت شبکه بیشتر و بیشتر می‌شود.

مراحل راه اندازی خدمات اکتیو شبکه

راه اندازی خدمات اکتیو شبکه به صورت استاندارد باید از تجهیزات کلیدی تر شروع شوند و به تجهیزات کم اهمیت تر خطم شود، اما در بسیاری از موارد به دلیل وضعیت کاری ممکن این الویت بندی دچار تغییر شود و نیاز باشد تا تجهیزاتی همانند پرینتر ها و کامپیوتر در ابتدا نصب و راه اندازی شوند و سپس نسبت به نصب و راه اندازی تجهیزات کلیدی تر همانند سرور اقدام شود.

در برخی از موارد نیز ممکن است مثلا بخشی از سرور مالی راه اندازی شود، سپس یکی از کامپیوتر ها راه اندازی شود و در ادامه تجهیزات دیگری که نیاز به آن بیشتر از بقیه تجهیزات احساس می شود.

تجهیزات اکتیو شبکه



تجهیزات اکتیو شبکه : به معنی تجهیزات تاثیر گذار بر روی سیگنال بیان کرد، به عبارتی دیگر تجهیزات اکتیو شبکه می تواند بر روی سیگنال شبکه تغییرات ایجاد کنند و نسبت به تجهیزات پسیو شبکه که تنها منتقل کننده سیگنال هستند متفاوت عمل می کنند.

تجهیزات اکتیو شبکه تجهیزاتی هستند که در نبود برق فعالیت آنها منحل می‌شود و برای کارکردن به جریان برق احتیاج دارند.

تجهیزات اکتیو شبکه بر روی جریان الکتریکی تاثیر گذارند و می توانند آن را قطع و وصل کنند، به عبارتی دیگر تمامی تجهیزاتی که بر روی آن ها نرم افزاری وجود دارد که نیاز به تنظیم شدن دارد را می توان زیر مجموعه تجهیزات اکتیو شبکه قرار داد.

اگر بخواهیم تعریف تخصصی‌تری از این تجهیزات ارائه کنیم، می‌توان گفت این تجهیزات می‌توانند حالت خاصی روی یک سیگنال داده عبوری ایجاد کنند و آنها را تغییر دهند.

اگر بخواهیم چند نمونه از تجهیزات اکتیو شبکه را نام ببریم می توانیم به موارد زیر اشاره کنیم:

- سرور
- سوئیچ
- روتر
- مودم اینترنت
- دستگاه های ذخیره سازی اطلاعات همانندNAS
- کامپیوتر
- پرینتر
- اکسزپوینت

لازم به ذکر است که هر کدام از تجهیزات نام برده شده به انواع بسیار گسترده ای تقسیم بندی می شوند.

انواع تجهیزات شبکه اکتیو عبارت‌اند از :

۱- رپیتر در تجهیزات اکتیو در شبکه(Repeater)

از ریپیتر یا تکرارکننده برای ارسال اطلاعات در فواصل طولانی بدون از بین‌رفتن داده‌ها و ضعف سیگنال‌ها استفاده می‌شود. داده‌های انتقالی روی شبکه به‌طور کامل بازسازی و تقویت می‌شوند تا بدون کوچک‌ترین تغییر و با بالاترین کیفیت به کاربر برسند.

ریپیتر در لغت به معنی تقویت کردن است و در شبکه های کامپیوتری نیز همین کار را انجام می دهد. به عبارتی دیگر در قسمت هایی از شبکه که با محدودیت هایی مواجه باشیم که باعث بشوند سیگنال ما ضعیف شود، از ریپیتر استفاده می کنیم.

ریپیتر ها انواع مختلفی دارند که از پر کاربرد ترین های آن ها می توان به ریپیتر در سوئیچ شبکه و ریپیتر امواج وای فای اشاره کرد. ریپیتر در سوئیچ شبکه به طور پیش فرض در تمامی سوئیچ های شبکه وجود دارد و زمانی که فواصل کابل های شبکه بیشتر از ۱۰۰ متر باشد، میتوان در بین راه از سوئیچ شبکه استفاده کرد تا امواج الکترومغناطیسی را تقویت کند.

همچنین در مکان هایی که امواج وای فای ضعیف باشد و امکان کابل کشی برای اضافه کردن اکسس پوینت های دیگر وجود نداشته باشد می توان از ریپیتر امواج وای فای استفاده کرد، به گونه ای که می تواند امواج نسبتا ضعیف وای فای را دریافت کند و آن ها را تقویت کرده و سپس منتشر کند. برخی از اکسس پوینت ها به طور پیشرفت این حالت را دارند و میتوان آن ها را برای این کار تنظیم کرد.


TP-LINK
RE
Wireless
Power
Ethernet


Wi Fi
AP/ROUTER
WLAN
Power/WPS
WAN/LAN
LAN
WPS

تکرار کننده یک دستگاه الکترونیکی است که سیگنال دریافتی را تقویت می‌کند. شما می‌توانید تکرار کننده را دستگاهی تصور کنید که یک سیگنال دریافت می‌کند و آن‌را با قدرت بیشتری ارسال می‌کند تا سیگنال بتواند مسافت‌های طولانی‌تری را پوشش دهد. تکرارگرها روی لایه فیزیکی کار می‌کنند.

اگر دو ساختمان بزرگ از طریق شبکه به هم وصل شوند و فاصله بین کاربران زیاد باشد، ممکن است هنگام انتقال، داده‌ها از بین برود یا سیگنال‌ها ضعیف شود. در چنین شرایطی سرپرستان شبکه برای حل مشکل از repeater استفاده می‌کنند. ریپیتر وظیفه تقویت و بازسازی داده‌های انتقالی را در شبکه وایرلس بر عهده دارد، به‌گونه‌ای که سیگنال‌ها به خوبی و بدون دست خوردگی به مقصد برسند.

۲- سوئیچ در تجهیزات اکتیو شبکه(Switch)

سوئیچ از جمله دستگاه‌های اساسی هر شبکه است که اجزا و دستگاه‌های شبکه را به هم وصل می‌کند. به کمک سوئیچ، این عضو شبکه اکتیو، هر کاربر به‌جای آنکه خود کابل شبکه را به سرور متصل کند، به سوئیچ وصل می‌شود و به سرور و دستگاه‌های دیگر دسترسی پیدا می‌کند. این‌طوری کل دستگاه‌های شبکه قابل مشاهده‌اند، کاربرها می‌توانند هم‌زمان داده بفرستند، وجود دیگر کاربران، سرعت دستیابی کاربران دیگر را کم نمی‌کند.

سوئیچ شبکه نسخه ارتقا یافته هاب شبکه محسوب می شود، با این تفاوت که اطلاعات ارسال از یکی از تجهیزات شبکه به تجهیزات دیگر متصل به شبکه ارسال نمی شود و سوئیچ این قابلیت را دارد تا آدرس اطلاعات ارسالی در شبکه را تشخیص دهد و اطلاعات را تنها به مقصد اصلی هدایت کند.

سوئیچ ها در شبکه به دو نوع رایج غیر مدیریتی و مدیریتی تقسیم بندی می شوند که در نوع غیر مدیریتی شما تنها کاری که لازم است انجام دهید اتصال دستگاه های مختلف به سوئیچ برای برقراری ارتباط است اما در سوئیچ های مدیریتی شما می توانید تنظیمات مختلف مدیریتی را نیز نسبت به سوئیچ های غیر مدیریتی اعمال کنید که بیشتر این تنظیمات باعث ارتقا امنیت شبکه می شوند.

شرکت Cisco را می توان معروف ترین شرکت تولید سوئیچ های شبکه قابل برنامه ریزی در دنیا نامید. همچنین برند های مثل D-linkو TP-Linkدر تولید سوئیچ های شبکه فعال هستند و سوئیچ هایی را در نوع مدیریتی و غیر مدیریتی به بازار عرضه می کنند که در برخی از مجموعه به چشم میخورند

عملکرد سوئیچ شبیه به هاب است با این تفاوت که هوشمند است. سوییچ هنگامی که بسته‌ای را دریافت می‌کند بر مبنای مک‌آدرس یا آدرس آی‌پی دستگاه بسته را برای گره درست ارسال می‌کند و در نتیجه بسته برای همه پورت‌ها ارسال نمی‌شود. با توجه به این‌که بسته برای پورت مشخصی ارسال می‌شود مشکل تصادم، ازدحام و مصرف بیش از اندازه ترافیک به وجود نمی‌آید.

سوئیچ یک دستگاه چند پورتی است که کارایی شبکه را بهبود می‌بخشد. سوئیچ اطلاعات مسیریابی محدود در مورد گره‌های شبکه داخلی را حفظ می‌کند و به سیستم‌ها امکان اتصال به روتر را می‌دهد.

به‌طور کلی، سوئیچ‌ها می‌توانند آدرس سخت‌افزاری بسته‌های ورودی را بخوانند و بسته‌ها را به مقصد مناسب انتقال دهند.

سوئیچ‌ها به دلیل قابلیت مدار مجازی و هوشمندی که دارند، کارایی شبکه را بهبود می‌بخشند. سوئیچ‌ها امنیت شبکه را افزایش می‌دهند، زیرا از طریق الگوریتم‌های مسیریابی، بهترین مسیر را انتخاب می‌کنند و قابلیت دفع حملات سایبری شناخته شده را دارند. شما می‌توانید یک سوئیچ را به عنوان دستگاهی در نظر بگیرید که بهترین قابلیت‌های روترها و هاب‌ها را دارد، البته بدون وجود روتر قادر به اتصال به اینترنت نیست.

یک سوئیچ می‌تواند در لایه پیوند داده (data link) یا لایه شبکه (network) مدل osi کار کند. سوئیچ چند لایه سوئیچی است که می‌تواند در هر دو لایه کار کند یعنی می‌تواند به عنوان سوئیچ و روتر عمل کند. پس سوئیچ چند لایه یک دستگاه با کارایی بالا است که از پروتکل‌های مسیریابی مشابه روترها پشتیبانی می‌کند.

سوئیچ‌ها می‌توانند در معرض حملات انکار سرویس توزیع شده (DDoS) قرار بگیرند. البته سوییچ‌های امروزی راهکارهایی برای محافظت از شبکه در برابر حمله‌های سیلابی دارند. امنیت پورت سوئیچ یکی از مهم‌ترین نکاتی است که باید به آن دقت کنید، بنابراین مطمئن شوید که پورت‌های بلااستفاده غیرفعال هستند و از جستجوی dhcp ، بازرسی arp و فیلتر آدرس مک استفاده می‌کنید.

از مهم‌ترین نکاتی که در زمان خرید سوییچ باید به آن دقت کنید مدیریتی، غیر مدیریتی، نیمه هوشمند بودن، تعداد پورت‌ها، توانایی پشتیبانی از فناوری PoE و... است. علاوه بر این باید به نوع سوییچ نیز

دقت کنید که قابل استفاده در کدام لایه است. همان طور که گفتیم برخی از سوییچ‌ها در لایه ۲ و برخی دیگر در لایه ۳ کار می‌کنند.

سوییچ ها در شبکه نقش بسیار مهمی را ایفا می کنند و آن ارتباط دستگاه ها به هم است

۳ - بریج در تجهیزات شبکه اکتیو(Bridge)

بریج یعنی پل و از آن برای اتصال و برقراری ارتباط میان دو شبکه کاملا جداگانه استفاده می‌شود. برای آنکه کارکنان یک ساختمان از شبکه ساختمان دیگری استفاده کنند، دو شبکه محلی آنها به وسیله بریج به یکدیگر وصل می‌شوند. این دستگاه برای شبکه‌سازی میان کامپیوترها مورد استفاده قرار می‌گیرد.

بریج یا پل به نوعی همان سوئیچ شبکه بود با این تفاوت که تنها دو پورت داشت و قبل از سوئیچ ها طراحی و به بازار عرضه شد که به واسطه آن زمانی که دو تا شبکه داشتیم و میخواستیم آن ها را به

یکدیگر متصل کنیم از بریج استفاده میشد. به این گونه که یکی از پورت های شبکه اولی به یه پورت بریج متصل میشد و یک پورت از شبکه دوم به پورت دوم بریج متصل میشد.

دلیل متصل کردن دو شبکه یه یکدیگر و ترکیب نکردن آن ها از طریق هاب به یک شبکه بزرگ تر این بود که در شبکه های کوچک ترافیک کمتری از هر نود شبکه به نود های دیگر شبکه ارسال میشد و ترافیک در حدی بود که شبکه می توانست به کار عادی خود ادامه دهد، اما زمانی که تعداد نود ها در یک شبکه افزایش پیدا می کرد ترافیک با افزایش مواجه میشد و سرعت کاهش در شبکه کاهش پیدا می کرد.

به همین دلیل استفاده از بریج باعث شد دو شبکه به یکدیگر متصل شوند، به گونه ای که تنها در زمان هایی که لازم بود اطلاعات از یک شبکه به شبکه دیگر انتقال پیدا کند، بریج اطلاعات را از یک شبکه به شبکه دیگر منتقل می کرد و در مواقع عادی ترافیک یک شبکه را بی دلیل به شبکه دیگر منتقل نمی کرد.

برای اتصال دو شبکه مجزا از هم یک پل ارتباطی ایجاد می‌شود که به آن پل (bridge) می‌گویند. در این حالت شبکه محلی A می‌تواند از طریق دستگاه بریج به شبکه محلی B متصل شود. از پل‌ها می‌توان برای اتصال دو lan فیزیکی به یک lan منطقی بزرگ‌تر نیز می توان استفاده کرد. همچنین پل‌ها برای تقسیم شبکه‌های بزرگ‌تر به بخش‌های کوچک‌تر با قرار گرفتن بین دو بخش فیزیکی شبکه و مدیریت جریان داده بین هر دو نیز استفاده می‌شوند.

bridgeفقط در لایه‌های فیزیکی (physical) و پیوند داده (data link) مدل osi کار می‌کند. نقش اساسی پل‌ها در معماری شبکه، ذخیره و ارسال فریم‌ها بین بخش‌های مختلف است. آن‌ها از مک آدرس‌ها برای انتقال فریم استفاده می‌کنند. با مشاهده مک آدرس پل‌ها می‌توانند داده‌ها را به سمت دستگاه‌های متصل به هر بخش هدایت کنند.

پل‌ها از بسیاری جهات مانند هاب‌ها هستند، از جمله این که مولفه‌های lan را با پروتکل‌های یکسان به یکدیگر متصل می‌کنند، با این تفاوت که پل‌ها بسته‌های داده ورودی را به عنوان فریم می‌شناسند و قبل از ارسال آدرس، آن‌ها را فیلتر و بسته‌بندی می‌کنند. از آن‌جایی که بسته‌های داده را فیلتر می‌کنند، پل هیچ تغییری در قالب یا محتوای داده‌های ورودی ایجاد نمی‌کند. جدول بریج در ابتدا خالی است، اما به مرور زمان آدرس هر کامپیوتر متعلق به شبکه محلی و آدرس‌های هر رابطی که شبکه محلی به سایر شبکه‌ها را متصل می‌کند نگه‌داری می‌کند. پل‌ها، مانند هاب‌ها می‌توانند چند پورته باشند. پل‌ها در سال‌های اخیر به ندرت استفاده می‌شوند و سوئیچ‌ها جایگزین آن‌ها شده‌اند که عملکرد بهتری دارند. در واقع، سوئیچ‌ها به‌علت نحوه عملکرد خود به‌عنوان پل چند پورته (multiport bridges) نامیده می‌شوند.


Landis+Gyr
NETWORK BRIDGE N2250
CLASS-B
DC Input: 12-24 VDC,1.66-0.83amp
Catalog No:
Assembled in México
LT-80200F4B
LT-80200F4B
Patent Notices
www.landisgyr.com/about/patent-notices/
SERIAL 1
SERIAL 0
ETHERNET 1
10/100
ETHERNET 0
10/100/1000
POWER
WAN
LAN
WI-FI
LAN
RADIO
WI FI
LTE 1
LTE 2

۴ - هاب در تجهیزات شبکه اکتیو(Hub)

اگر در سطح لایه فیزیکی به هاب نگاه کنیم، شبیه سوئیچ وظیفه اتصال تجهیزات شبکه را به یکدیگر دارد. اما یک فرق عمده بین سوئیچ و هاب هست که مربوط به ارتباط بین دستگاه‌هاست. سوئیچ می‌تواند داده‌ها را برای مقصد خاصی ارسال کند، اما هاب داده‌ها را به همه پورت‌ها می‌فرستد که خود عامل کندی شبکه است.

هاب شبکه وسیله است که تجهیزات مختلف در شبکه را به وسیله کابل شبکه به یکدیگر متصل می کند و تشکیل یک شبکه کامپیوتری را میدهد. هاب های شبکه حاوی چند عدد پورت شبکه هستند و هر یک از آن ها برای اتصال یک دستگاه اکتیو شبکه استفاده می شود.

زمانی که یکی از تجهیزات متصل در شبکه شروع به ارسال اطلاعات می کنند، تمامی تجهیزات شبکه متصل شده به هاب می توانند اطلاعات ارسال شده را دریافت کنند و این موضوع یکی از ایرادات در هاب ها بود که باعث ترافیک زیاد در شبکه، کاهش سرعت و کاهش امنیت در شبکه میشد که در سوئیچ ها این موضوع برطرف شد و امروزه دیگر از هاب های شبکه استفاده نمی شود.

هاب شبیه به سوئیچ عمل میکند با این تفاوت که تکنولوژی آن قدیمی بوده و عملکرد و سرعت آن پایین است. در حقیقت hub وظیفه ی اتصال تجهیزات شبکه را بر عهده دارد.

از هاب میتوان به عنوان تقویت کننده برای آن دسته از سیگنالهایی که بعد از مسافتهای طولانی ضعیف میشوند نیز استفاده کرد. در صورت ورود داده ها بصورت آنالوگ هاب آنها را به سیگنال منتقل میکند. هابها به دو مدل پورت ساده و چندگانه تقسیم میشوند.

یکی از مشکلاتی که هاب در شبکه ایجاد میکند مصرف و تداخل بیش از حد پهنای باند میباشد.

hubدستگاهی است که امکان اتصال تجهیزات مختلف به شبکه را می‌دهد. امکان استفاده از هاب به عنوان یک تکرارکننده وجود دارد زیرا سیگنال‌هایی که پس از طی مسافت‌های طولانی روی کابل‌ها ضعیف می‌شوند را تقویت می‌کند. هاب ساده‌ترین عضو دنیای شبکه است، زیرا مولفه‌های یک شبکه محلی را بر مبنای پروتکل‌های یکسانی به یکدیگر متصل می‌کند. در مقایسه با سوئیچ سرعت و کارایی پایین‌تری دارد و تقریبا منسوخ شده است.

یک هاب می‌تواند با داده‌های دیجیتالی و آنالوگ مورد استفاده قرار گیرد، به شرطی که تنظیمات آن برای آماده‌سازی قالب‌بندی داده‌های ورودی پیکربندی شده باشد. به عنوان مثال، اگر داده‌های ورودی به صورت دیجیتال باشد، هاب باید آن‌را به عنوان بسته منتقل کند، اما اگر داده‌های ورودی آنالوگ باشند، هاب آن‌را به شکل سیگنال منتقل می‌کند. هاب‌ها عملکردهای فیلترینگ یا آدرس‌دهی بسته‌ها را انجام نمی‌دهند. آن‌ها فقط بسته‌های داده را برای همه دستگاه‌های متصل ارسال می‌کنند. هاب‌ها در لایه فیزیکی مدل Open Systems Interconnection (OSI) کار می‌کنند. هاب‌ها به دو نوع پورت ساده و چندگانه تقسیم می‌شوند.

هاب فاقد هرگونه مولفه هوشمندی است به همین دلیل مشکل بزرگی که ایجاد می‌کند تداخل و مصرف بیش از اندازه پهنای باند است، زیرا هنگامی که گره‌ای قصد دارد یک بسته اطلاعاتی را برای گره دیگری ارسال کند از رویکرد همه پخشی استفاده می‌کند که باعث می‌شود یک بسته اطلاعاتی برای همه گره‌های متصل به هاب ارسال شود.

۵ - روتر در تجهیزات اکتیو شبکه(Router)

روتر یا مسیریاب، همانطور که از نامش پیداست، وظیفه مسیریابی اطلاعات بین شبکه‌های مختلف را بر عهده دارد. البته از این دستگاه در شبکه‌های LAN و WAN که بیش از یک شبکه فعال وجود دارد و فعالیت کاربران بیرون شبکه است، استفاده می‌شود. در دنیای امروز و عصر اینترنت، اتصال دو یا چند شبکه یک نیاز هم و اجتناب ناپذیر است.

روتر به معنی مسیریاب است و برای ارتباط یک شبکه با شبکه دیگر مورد استفاده قرار میگرد.

شما زمانی که به اینترنت متصل می شوید، به شبکه اینترنت متصل شده اید! این مثال ساده ای است از اتصال یک شبکه (شبکه داخلی مثل خونه یا سازمان) به یک شبکه ی دیگر مثل اینترنت. باید به این نکته توجه کنید که شبکه ی دیگر لزوما اینترنت نیست، بلکه ممکن است شما به دلایل مختلفی از چند شبکه استفاده بکنید و که از یکدیگر مجزا شده اند اما نیاز به اتصال این دو شبکه به یکدیگر وجود دارد.

تفاوت روتر و بریج این است که در روتر هر کدام از شبکه ها به طور مستقل می توانند کار بکنند و وابستگی به یکدیگر ندارد اما زمانی که از بریج برای اتصال دو شبکه به یکدیگر استفاده می شود، هر شبکه نمی تواند بدون وابستگی به شبکه دیگر کار بکند و انگار هر دو شبکه یک شبکه را تشکیل داده اند.

هنگامی که قصد اتصال دو شبکه محلی به یکدیگر را دارید به ابزاری برای اتصال شبکه‌ها به یکدیگر نیاز دارید. برای این منظور باید از مودم‌روتر استفاده کنید. مودم‌روتر وسیله‌ای است که برای برقراری ارتباط سامانه‌ها به یکدیگر از طریق کابل یا شبکه وای‌فای استفاده می‌شود.

روترها در انواع مختلفی به بازار عرضه می‌شوند و در زمان خرید روتر باید به استانداردهای مخابراتی که پشتیبانی می‌کند، فرکانس‌ها و تعداد آنتن‌ها دقت کنید. به‌عنوان یک قاعده کلی، پیشنهاد می‌شود به سراغ خرید روترهایی بروید که از استاندارد ۸۰۲.۱۱ acپشتیبانی می‌کنند. علاوه بر این، اگر در نظر دارید در آینده از اینترنت سیار استفاده کنید باید به توانایی روتر در پشتیبانی از سیم‌کارت دقت کنید.

روترها با ترسیم مسیری برای دستگاه‌های متصل به شبکه و از طریق توپولوژی‌های مختلف شبکه به انتقال بسته‌ها به مقاصد کمک می‌کنند. روترها دستگاه‌های هوشمندی هستند و اطلاعات مربوط به شبکه‌هایی که به آن‌ها متصل هستند را ذخیره می‌کنند. اکثر روترها را می‌توان طوری پیکربندی کرد که به عنوان فایروال فیلتر بسته‌ها عمل کند و از فهرست کنترل دسترسی (ACL) نیز پشتیبانی می‌کنند.

روترها، همراه با واحد سرویس کانال/واحد سرویس داده (CSU/DSU) توانایی ترجمه فریم LAN به فریم WAN را دارند، این فرایند ضروری است، زیرا شبکه‌های محلی و شبکه‌های گسترده از پروتکل‌های

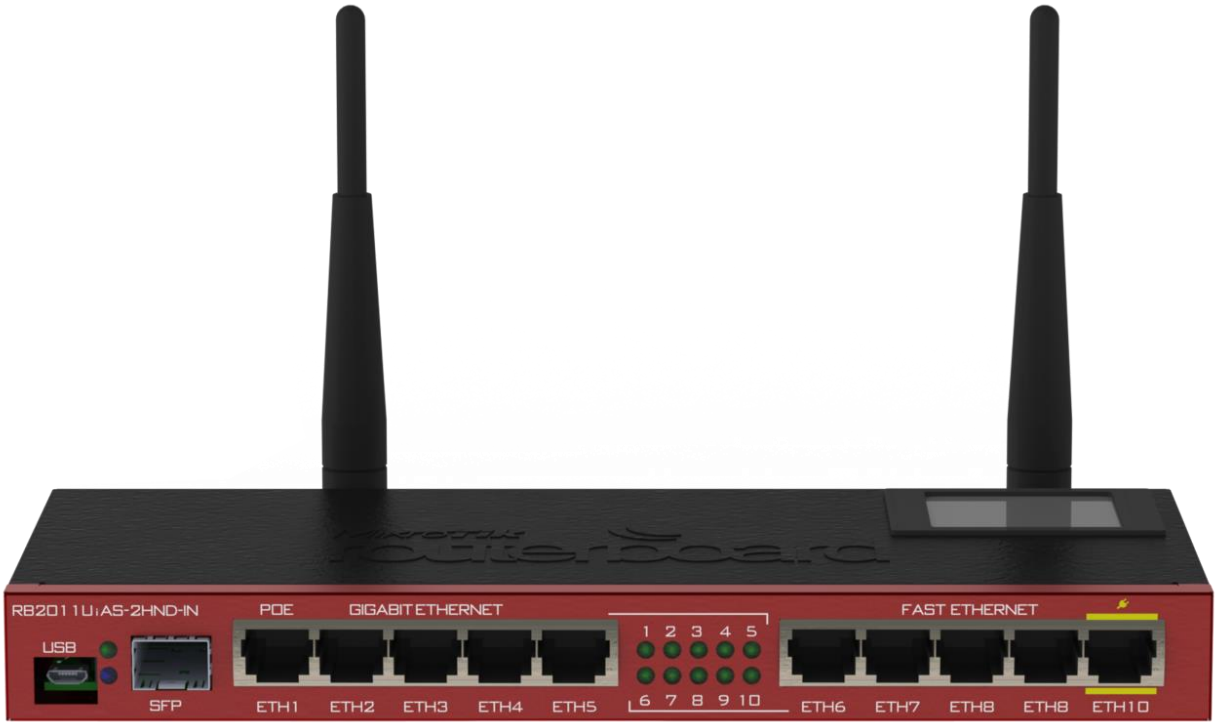
مختلف شبکه استفاده می‌کنند. این روترها به‌نام روترهای مرزی نیز شناخته می‌شوند. این روترها توانایی برقراری ارتباط شبکه‌های LAN به WAN را دارند.

روتر برای تقسیم شبکه‌های داخلی به دو یا چند زیر شبکه استفاده می‌شود. روترها می‌توانند به‌صورت داخلی به سایر روترها متصل شوند و مناطقی را ایجاد کنند که مستقل عمل می‌کنند. روترها با حفظ جداول در مورد مقاصد قابلیت برقراری ارتباطات محلی را فراهم می‌کنند. برای این منظور روتر حاوی اطلاعاتی در مورد سیستم‌های متصل به آن است و در صورت عدم تشخیص مقصد، محل ارسال درخواست‌ها را حدس می‌زند.

روترها معمولاً مسیریابی را با استفاده از یکی از سه پروتکل استاندارد پروتکل اطلاعات مسیریابی (RIP)، پروتکل دروازه مرزی (BGP) یا ابتدا کوتاهترین مسیر (OSPF) را انتخاب کن انجام می‌دهند.

روتر ها معمولاً در جاهایی استفاده می شوند که بیش از یک شبکه وجود دارد

از معروف ترین شرکت های تولید کننده روتر می توان به Cisco و MikroTik اشاره کرد.



۶ - اکسس پوینت در تجهیزات شبکه اکتیو(Access point)

اکسس‌پوینت یا نقطه دسترسی برای اتصال از راه دور در شبکه‌های خیلی بزرگ استفاده می‌شود تا حرکت کارکنان در محیط کار، دسترسی به شبکه را مختل نکند. در واقع اکسس پوینت در شبکه‌های وایرلس نقش سوئیچ را ایفا می‌کند.

اکسس پوینت به واسطه فناوری WiFi تجهیزات بیسیم شبکه را به شبکه متصل می کنند، به عبارتی دیگر اکسس پوینت همان سوئیچ شبکه است، با این تفاوت که اتصال شبکه را به صورت بیسیم برقرار می کند و تجهیزات شبکه بیسیم در شبکه به واسطه اکسس پوینت به شبکه و تمامی تجهیزات دیگر شبکه متصل می شوند.

بیشترین کاربر اکسس پوینت ها اتصال به شبکه اینترنت است، به عبارتی دیگر شما زمانی که دستگاه بیسیم خود را به واسطه اکسس پوینت به شبکه ای وصل می کنید در آن اتصال به اینترنت برقرار است، شما هم می توانید از اینترنت آن شبکه استفاده کرده و نیاز های خود را برآورده کنید.

برخی از دستگاه ها به خودی خود شامل اکسس پوینت هستند و دیگر نیاز نیست شما برای اتصال دستگاه های خود به صورت بیسیم اکسس پوینت جداگانه تهیه کنید. مودم ها و برخی از روتر ها شامل اکسس پوینت هستند و با تنظیم آن ها می توانید به شبکه مورد نظر متصل شوید.

به‌طور معمول در شبکه کابلی برای برقراری ارتباط تجهیزات با شبکه به یک سوئیچ نیاز داریم، اما در شبکه‌های وایرلس به اکسس پوینت نیاز داریم تا به کلاینت‌هایی که دورتر از روتر قرار دارند اجازه اتصال

به شبکه وای‌فای را بدهد. پس اکسس پوینت در شبکه‌های وایرلس همان کاری را انجام می‌دهد که سوئیچ در شبکه‌های کابلی انجام می‌دهد.

اکسس پوینت می‌تواند از نظر فنی شامل اتصال سیمی یا بی سیم باشد اما معمولاً به دستگاه بی سیم اشاره دارد. یک Access Point در لایه دوم مدل osi کار می‌کند و می‌تواند یا به عنوان پلی که یک شبکه سیمی استاندارد را به دستگاه‌های بی سیم متصل می‌کند یا به عنوان یک روتر انتقال داده‌ها از یک نقطه به نقطه دیگر استفاده شود.

اکسس پوینت‌های بی‌سیم (WAP) شامل یک دستگاه فرستنده و گیرنده هستند که برای ساخت شبکه محلی بی‌سیم (WLAN) استفاده می‌شود. اکسس‌پوینت‌ها دستگاه‌های مجهز به آنتن، فرستنده و آداپتور داخلی هستند. آن‌ها دارای چند پورت هستند که به شما این امکان را می‌دهند تا شبکه را برای پشتیبانی از کلاینت‌های بیشتر گسترش دهید. بسته به اندازه شبکه، ممکن است یک یا چند اکسس پوینت برای پوشش کامل مورد نیاز باشد.

اکسس پوینت‌ها ممکن است پورت‌های زیادی را برای افزایش وسعت شبکه، قابلیت‌های دیوار آتش و سرویس DHCP ارائه دهند. بنابراین، ما اکسس‌پوینت‌هایی در بازار داریم که یک سوئیچ، سرورdhcp ، روتر و فایروال هستند.

شرکت های Linksysو Unifiدر زمینه تولید اکسس پوینت در جهان معروف هستند و محصولات باکیفتی در این زمینه تولید می کنند که در بازار ایران هم می توانید نسبت به خرید آن ها اقدام کنید.


cisco
abg WiFi n
CERTIFIED

۷ - مودم در تجهیزات اکتیو شبکه(Modem)

مودم وسیله است که وظیفه آن تبدیل سیگنال دیجیتال به آنالوگ و برعکس می باشد. کار اصلی مودم ها اتصال شما با شبکه اینترنت است، اطلاعات در شبکه اینترنت از طریق کابل ها و به صورت آنالوگ منتقل می شوند و کامپیوتر های ما توانایی فهم امواج آنالوگ را ندارند. در نتیجه مودم ها این کار را انجام داده و اطلاعات آنالوگ منتقل شده را به دیجیتال تبدیل می کنند تا توسط کامپیوتر ها قابل فهم شود.

همچنین اطلاعات ارسالی کامپیوتر ها به شبکه اینترنت به صورت دیجیتال است و مودم ها اطلاعات ارسالی را از دیجیتال به آنالوگ تبدیل می کنند تا از طریق کابل تلفن به مرکز تلفن برسد.

مودم آن ها انواع مختلفی دارند که هر کدام از آن ها به می تواند به نوع داخلی و خارجی تقسیم شود. در ابتدا تنها مودم ها به صورت داخلی و Internal ساخته می شدند و پس از آن مودم ها به صورت خارجی و external هم طراحی و روانه بازار شدند و متصل کردن آن به کامپیوتر ها ساده تر شود و توانایی اتصال به لپ تاپ ها را نیز داشته باشد.


TP-LINK


TP-LINK

مودم‌ها برای انتقال سیگنال‌های دیجیتال از طریق خطوط تلفن آنالوگ استفاده می‌شوند. بنابراین، سیگنال‌های دیجیتال توسط مودم به سیگنال‌های آنالوگ با فرکانس‌های مختلف تبدیل شده و به مودم مقصد انتقال داده می‌شوند. مودم دریافت‌کننده سیگنال آنالوگ را به دیجیتال تبدیل کرده و خروجی دیجیتال را به دستگاهی متصل به مودم که معمولاً کامپیوتر است تحویل می‌دهد. داده‌های دیجیتالی معمولاً از طریق رابط کاربری استاندارد RS-232 به مودم یا از طریق خط سریال انتقال داده می‌شوند. مودم‌ها روی هر دو لایه فیزیکی و پیونده داده کار می‌کنند.

به زبان ساده مودم، ارتباط شما را با مراکز ارائه دهنده اینترنت برقرار می کند.

مودم های جدید هم نقش روتر را بازی می کنند و هم مودم

۸ - POE .در تجهیزات شبکه اکتیو(Power E-Net)

POEمعرفی شده تا مشکل عدم دسترسی به پریز برق در نقاط کور را برطرف کند و راه‌اندازی شبکه بی هیچ مشکلی امکان‌پذیر باشد. امروزه کابل‌های شبکه از امکان انتقال جریان برق نیز برخوردارند و بی‌برقی مانعی برای پوشش‌دهی شبکه نیست.

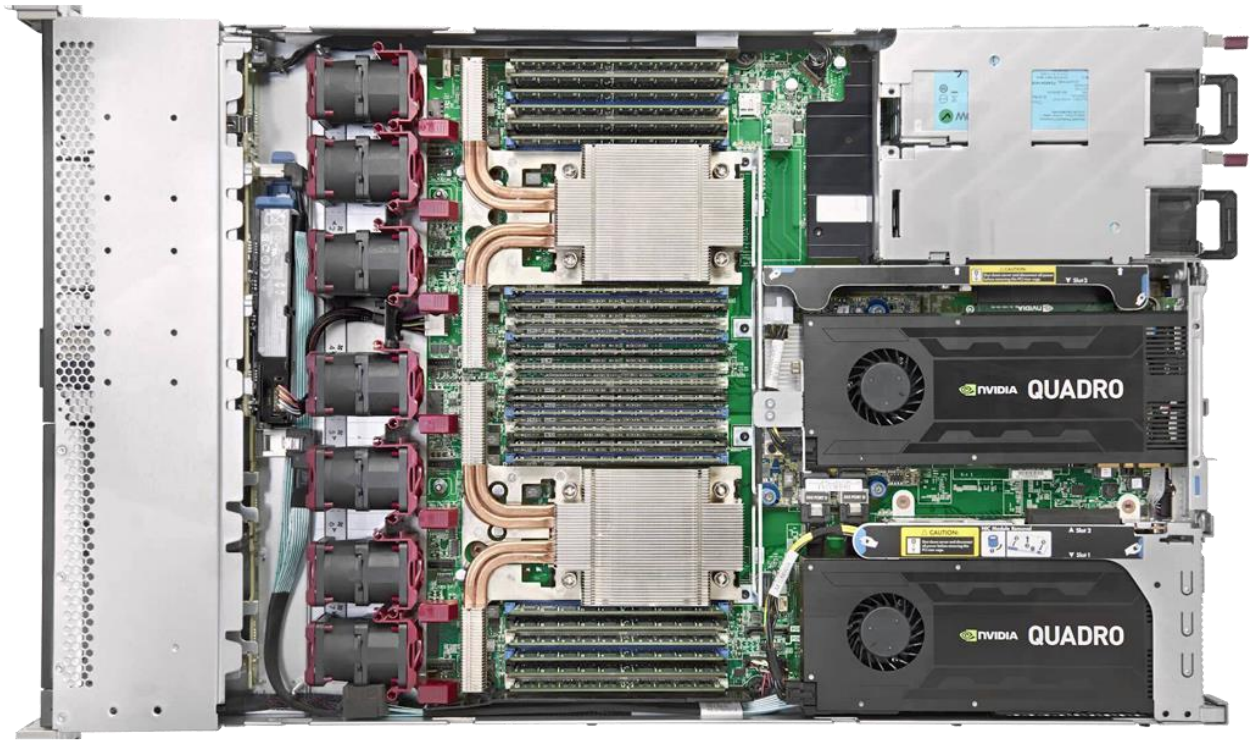
۹ - سرور(Server)

سرور در شبکه یک کامپیوتر تقویت شده و ارتقا داده شده با قابلیت های خاص خود است که همیشه روشن است و در حال سرویس دادن به کامپیوتر ها و تجهیزات دیگر شبکه می باشد. به عبارتی دیگر تمام قطعاتی که در یک کیس کامپیوتر وجود دارند در سرور تقویت شده اند و حتی از برخی از این تجهیزات مانند کارت شبکه، منبع تغذیه و فضای ذخیره سازی به صورت چند تایی استفاده شده است تا ضمن افزایش قدرت، زمانی که یکی از این تجهیزات دچار ایراد شد فعالیت اصلی تعلیق نشود و تجهیز جایگزین ادامه فعالیت را انجام دهد.

سرور مرکزیت یک شبکه را تشکیل می دهد و وظیفه سرویس دادن به تجهیزات و کاربران دیگر در شبکه را بر عهده دارد. سرویس های بسیار زیادی بر روی سرور نصب و راه اندازی می شوند که از مهم ترین آن ها می توان به سرویس مجازی سازی، سرویس اکتیو دیرکتوری، سرویس اشتراک گذاری فایل، سرویس نرم افزار های مالی و اداری اشاره کرد.

به عنوان مثال در سرویس نرم افزار های مالی، نرم افزار اصلی نسخه سرور بر روی سرور نصب می شود و کاربران برای اینکه به صورت همزمان با هم بتوانند بر روی اطلاعات ویرایش انجام دهند توسط نرم افزار های کلاینت به سرور متصل شده و نرم افزار مالی را اجرا می کنند.

سرور ها از جمله تجهیزات گرون قیمت شبکه هستند و نیاز به نگهداری مناسب دارند تا بتوانند به درستی فعالیت کنند ، همچنین سرور های برند های مختلفی دارند که شرکت HP بزرگترین آن ها محسوب می شود و اکثر شرکت ها در دنیا از سرور های این شرکت استفاده می کنند.



اصلیترین نقش در شبکه بر عهده ی سرورها میباشد. سروها در انواع مختلفی از جمله ایستاده، تیغه ای، ابری و... تولید و عرضه میشوند. از جمله بهترین برندهای سرور میتوان به hp اشاره کرد.

در واقع سرورها نقش اصلی را در برقراری ارتباطات شبکه دارند، سرور با تامین منابع پردازشی مورد نیاز کاربر، تخصیصIP ، اشتراک گذاری فایلها و استفاده از منابع سخت افزاری در اختیار کاربران **قلب اصلی شبکه های کامپیوتری** می باشد.

سرور قلب تپنده شبکه‌های ارتباطی است. اصلی‌ترین وظیفه سرور خدمت‌رسانی به کاربران است. در محیط‌های بزرگ و پیچیده سرور وظیفه تامین منابع پردازشی موردنیاز کلاینت‌ها را دارد. به‌طور مثال،

در محیط‌های ابری یا مبتنی بر فناوری‌های مجازی‌ساز، کاری که سرور انجام می‌دهد تخصیص منابع موردنیاز به کلاینت‌ها است. این فرایند می‌تواند امکان دسترسی به ماشین‌های مجازی میزبانی شده روی سرور، دسترسی به دسکتاپ‌های مجازی‌ساز یا دسترسی ساده به اطلاعاتی باشد که روی بانک‌های اطلاعاتی ذخیره‌سازی شده‌اند.

سرورها در انواع مختلفی به بازار عرضه می‌شوند که سرورهای تیغه‌ای، رک‌مونت، ایستاده، ابری و.... از مهم‌ترین آن‌ها هستند. در میان برندهایی که اقدام به تولید سرور می‌کنند محصولات hp و به ویژه سرورهای پرولیانت به دلیل کیفیت و طول عمر بالا مورد توجه سازمان‌ها قرار دارند. سرورهای پرولیانت نسل نهم و دهم از گزینه‌های اصلی سازمان‌ها هستند.

از معتبرترین برندهای تولیدکننده سرور، شرکت HP است.

از معتبرترین برندهای تولیدکننده سرور، شرکت HP است.

۱۰ - چاپگر (Printer)

چاپگر از تجهیزات اصلی شبکه های کامپیوتری محسوب می شوند و در همه ی شبکه های کامپیوتری می توانید اثری از حداقل یک چاپگر در شبکه را ببینید.

چاپگر های انواع مختلفی دارند که وابسته به نوع کاری که قرار است با آن ها انجام شود، می تواند متفاوت باشد.


HP LaserJet P1102w

۱۱ - پرینت سرور (Print Server)

پرینت سرور یکی از اجزا مهم شبکه اکتیو است که امکان اشتراک‌گذاری یک پرینتر را بین کاربران شبکه فراهم می‌کند. با استفاده از این وسیله دیگر نیازی به خریداری یک پرینتر به ازای تمام کاربران شبکه نیست، بلکه می‌توان یک پرینتر واحد را در اختیار تمام کاربران اکتیو نتورک گذاشت.

در زمان های قدیم پرینتر ها پورت شبکه نداشتند و برای استفاده از آن ها باید از پورت های دیگری نظیر USB و در قدیم تر از پورت های COM و پورت های LPT استفاده میشد. این موضوع برای یک سیستم کاربردی بود و مشکلی وجود نداشت، اما زمانی که قصد استفاده از چاپگر توسط کامپیوتر های دیگر شبکه مورد نیاز میشد، کامپیوتر متصل به پرینتر حتما می بایستی روشن میبود تا درخواست های چاپ از سیستم های دیگر به سیستم متصل به پرینتر برسد و این سیستم درخواست چاپ را به چاپگر ارسال کند.

به عبارتی دیگر کامپیوتر های دیگر شبکه قادر به ارسال مستقیم درخواست چاپ به پرینتر نبودند و همیشه نیاز به یک کامپیوتر واسط وجود داشت و اگر ان کامپیوتر خاموش بود و یا با مشکلی مواجه میشد، چاپ هم متوقف میشد.

پرینت سرور وسیله بود که این مشکل را برطرف کرد و اجازه ارسال مستقیم درخواست چاپ از تمام سیستم های شبکه به خود پرینتر را به واسطه پرینت سرور برطرف می کرد، این دستگاه حاوی یک پورت شبکه برای اتصال به شبکه و یک یا چند پورت دیگر برای اتصال به پرینتر بود که ارتباط پرینتر با شبکه را برقرار می کرد.

امروزه دیگر اکثر پرینتر ها حاوی پورت شبکه هستند و نیازی به استفاده از پرینت سرور در شبکه وجود ندارد.

در برخی سازمان‌ها لازم است بدون نیاز به کامپیوتر، چاپگری به اشتراک قرار گیرد تا کاربران از طریق شبکه به آن متصل شوند و پرینت‌های خود را ارسال کنند. در چنین سناریویی پرینتر را با کابل یواس‌بی پرینت سرور وصل می‌کنید و پرینت سرور را با یک کابل شبکه به سوئیچ شبکه متصل می‌کنید. این کار باعث می‌شود که پرینت سرور آی‌پی موردنیاز را دریافت کند و در شبکه شناسایی شود. از این به بعد کاربران درخواست‌های چاپ را مستقیما برای پرینتر ارسال می‌کنند.

۱۲ - ذخیره ساز تحت شبکه(NAS Storage)

سرور ها در شبکه به طور پیش فرض فضای ذخیره مناسبی را در اختیار کاربران و انجام کارهای مختلف انجام می دهند اما در استفاده های پیشرفته و کارهای سنگین، سرور با محدودیت های سرعتی و حجمی فضاهای ذخیره سازی خود مواجه می شود و در این حالت نیاز به استفاده از ذخیره ساز های پیشرفته تر NAS احساس می شود.

ذخیره ساز های تحت شبکه در مدل های پیشرفته تعداد و حجم بیشتری از هارد های ذخیره سازی را در اختیار قرار می دهند و همچنین سرعت انتقال اطلاعات در آن ها بیشتر از فضای ذخیره سازی سرور ها می باشد.

شرکت های HP و QNAP در زمینه تولید ذخیر ساز تحت شبکه بسیار معروف هستند.

۱۳ - دوربین تحت شبکه(IP Camera)

دوربین ها مدار بسته مانند خیلی از تجهیزات دیگر قابلیت اتصال به شبکه را نداشتند و به صورت آنالوگ مورد استفاده قرار میگرفتند و توسط دستگاه DVR سینگال آن ها به دیجیتال تبدیل می شد و شما می توانستید فیلم های آن ها را مشاهده کنید.

امروزه دوربین ها می توانند به صورت دیجیتال کار کنند و به صورت مستقل و بدون وابستگی به دستگاه دیگر، تصاویر را به شما نمایش دهند، البته لازم به ذکر است که برای استفاده از امکانات بیشتر نیاز به تهیه NVR در شبکه دارید.

۱۴ - ضبط کننده تصاویر تحت شبکه(NVR)

وظیفه دستگاه NVR علاوه بر ذخیره سازی و مدیریت تصاویر ارائه قابلیت های تصویری ویژه ای همچون تشخیص چهره، تشخیص پلاک، شمارش افراد و ... نیز هست. دستگاه های NVR در واقع عملکردی مشابه سرورهای کامپیوتری دارند با این تفاوت که استفاده و راه اندازی آن ساده تر است. از ویژگی های دیگر NVR می توان به موارد زیر اشاره کرد.

ضبط تصاویر ارسالی از دوربین های تحت شبکه

پخش زنده و یا بازپخش تصاویر

تنظیم ویژگی های تصویر اعم از روشنایی، رنگ و...

برق رسانی به دوربین ها (در صورت POEبودن دستگاه(NVR

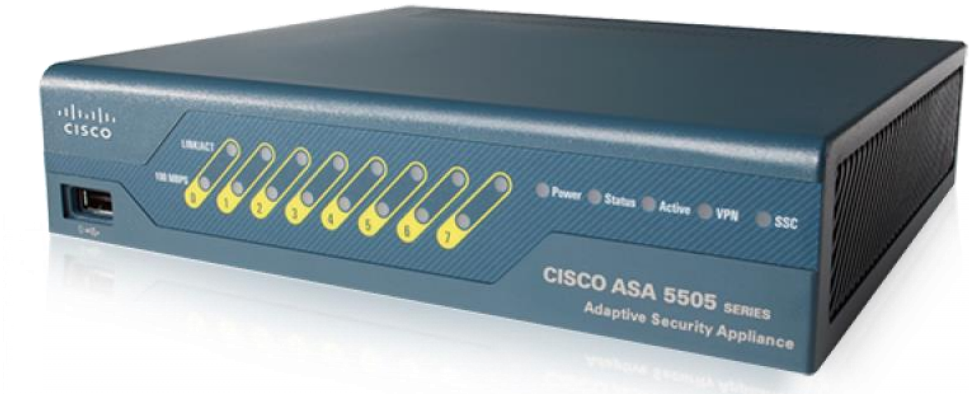
پردازش تصاویر (ویژگی های مختلف اعم از نقشه گرمایی، تشخیص چهره و(...

ذخیره سازی تصاویر با استفاده از انواع حالت های ضبط

۱۵ - دیواره آتش(Firewall)

فایروال شبکه به طور ساده وظیفه کنترل اطلاعات ورودی و خروجی از شبکه را به عهده دارند. به طور پیش در فایروال تمامی موارد ورودی و خروجی به شبکه بسته می شود مگر آن هایی که مورد نیاز است و اگر نباشد کار افراد دچار خلل می شود. در نهایت این موضوع منجر افزایش امنیت شبکه و اطلاعات شبکه می شود.

یکی از کاربرد های فایروال ها، کنترل مصرف اینترنت افراد در یک سازمان است، بگونه ای که میتواند برای هر کاربر سقف مجاز مصرف و یا حداکثر سرعت دانلود و آپلود از اینترنت را مشخص کنید. همچنین در فایروال ها می توانید تنظیم کنید که نرم افزار های قفل شکسته توانایی آپدیت و استفاده از اینترنت را نداشته باشند.



دیوار آتش یا فایروال قادر به نظارت بر داده های ورودی و خروجی بوده و به کاربر کمک میکند تا برنامه ها بدون اطلاع کاربر به اینترنت متصل نشده و از این طریق مانع از ورود هکرها و سرقت اطلاعات توسط آنها خواهد شد.

بطور کلی فایروال نقش مهمی در امنیت شبکه داشته و علاوه بر نرم افزار بصورت سخت افزار نیز در شبکه استفاده میشود. در حقیقت فایروال روتر از جمله تجهیزات سخت افزاری شبکه بوده که مانع از ورود بدافزارها و هکرها خواهد شد .و امنیت شبکه را تامین می کند.

وظیفه اصلی دیوارهای آتش نظارت بر بسته‌های ورودی و خروجی به شبکه سازمانی است. دیوارهای آتش با بررسی و بازبینی بسته‌ها مانع از آن می‌شوند برنامه‌های کاربردی بدون اطلاع کاربر به اینترنت متصل شده و تبادل اطلاعات بپردازند یا هکرها بتوانند به راحتی اقدام به سرقت یا شنود اطلاعات کنند.

فایروال‌ها نقش مهمی در پیشگیری از بروز حمله‌های رایج اینترنتی دارند. به‌طور معمول کاربران، دیوارهای آتش را به شکل نرم‌افزاری می‌شناسند، در حالی که دیوارهای آتش سخت‌افزاری نقش مهمی در تامین امنیت شبکه‌های سازمانی دارند. یکی از شناخته‌شده‌ترین دیوارهای آتش سخت‌افزاری که تقریبا همه کاربران از آن استفاده می‌کنند روترها هستند. فایروال روتر مانع از بروز حمله‌های سیلابی یا حمله‌های بدافزاری می‌شود اما در مقیاس وسیع‌تر، فایروال‌ها در تعامل با سامانه‌های پیشگیری و تشخیص نفوذ در شبکه‌ها نصب می‌شوند تا سرآیندهای مربوط به مبدا و مقصد بسته‌ها را بررسی کنند و اگر محتویات بسته‌ها مغایر با قواعد از پیش تعریف شده برای دیوارآتش بود مانع ارسال یا دریافت بسته‌ها شوند.

فایروال ها هم به صورت نرم افزاری وجود دارند و هم به صورت سخت افزاری

سامانه‌های پیشگیری و تشخیص نفوذ

این سامانه‌ها همانند دیوارهای آتش به شکل نرم‌افزاری و سخت‌افزاری وجود دارند و با ارزیابی بسته‌ها و بر مبنای اطلاعاتی که از قبل دارند حمله‌های سایبری رایج را شناسایی کرده و هشداری برای سرپرستان شبکه ارسال می‌کنند. این سامانه‌ها به انواع مختلفی مثل مبتنی بر میزبان، مبتنی بر شبکه و نمونه‌های مشابه تقسیم می‌شوند که هر یک بسته به نوع شبکه عملکرد خاص خود را دارند. مهم‌ترین نکته‌ای که باید در مورد این سامانه‌ها مکان درست قرارگیری آن‌ها در شبکه است که پهنای باند شبکه را بیهوده مصرف نکنند و از طرفی به شکل درستی قادر به تشخیص موارد مشکوک باشند.

تجهیزات IDS و IPS از جمله تجهیزات امنیتی در شبکه هستند IDS :برای یافتن تهدیدها استفاده می‌شود و IPS برای از بین بردن و قطع دسترسی تهدیدها در شبکه.

مدیریت و تنظیم تجهیزات اکتیو شبکه، نیازمند دانش و تخصص زیادی است.

مدیریت و تنظیم تجهیزات اکتیو شبکه، نیازمند دانش و تخصص زیادی است.

۱۶ - کارت شبکه

از دیگر **تجهیزات اکتیو برای پیاده سازی شبکه،** کارت شبکه است. کارتهای شبکه به ۲ گروه بیسیم یا وایرلس و کابلی تقسیم میشوند، کارتهای وایرلسی نیز شامل ۲ مدل اکسترنال و اینترنال میباشند.

کارتهای شبکه سرعتهای مختلفی دارند و بطور کلی برای برقراری ارتباط هر سیستمی در شبکه به کارت شبکه نیاز میباشد. البته لازم است بدانید مادربردهای جدید کامپیوتر ها و لپتاپ ها دارای کارت شبکه داخلی هستند.

مکانیزم برقراری ارتباط کامپیوتر با شبکه و سایر دستگاه‌های متصل به شبکه است. به‌طور کلی، تمامی تجهیزات برای برقراری ارتباط با شبکه محلی یا اینترنت به کارت شبکه نیاز دارند. بدون کارت شبکه هیچ دستگاهی قادر به برقراری ارتباط با اینترنت نیست. هر کارت شبکه دارای یک مک‌آدرس است که با استفاده از آن در شبکه شناسائی شده و توانائی برقراری ارتباط با سایر دستگاه‌ها را دارد. کارت‌های شبکه در سرعت‌های مختلفی وجود دارند و می‌توانند از استانداردها و پروتکل‌های مختلفی پشتیبانی کنند. نکته مهم در زمان خرید کارت شبکه توانایی پشتیبانی از دو فرکانس کاری و استانداردهای روز است.

۱۷ – گت وی (Gateway)

گیت‌وی‌ها معمولاً در لایه‌های انتقال و نشست (Transport and Session) مدل OSI کار می‌کنند. در لایه انتقال (Transport) و بالاتر، پروتکل‌ها و استانداردهای متعددی از سوی فروشندگان ارایه شده است. گیت‌وی‌ها را باید همانند مترجمی میان توپولوژی‌های شبکه مانند اتصال سیستم باز (OSI) و پروتکل کنترل انتقال/پروتکل اینترنت (TCP/IP) هستند. به همین دلیل، گیت‌وی‌ها دو یا چند شبکه مستقل را متصل می‌کنند که هریک دارای الگوریتم‌های مسیریابی، پروتکل‌ها، توپولوژی، خدمات نام دامنه و رویه‌ها و خط‌مشی‌های مدیریت شبکه هستند.

gatewayبیشترِ عملکردهای روترها را دارند. در حقیقت، یک روتر با قابلیت ترجمه اضافی عملکردی یکسان با یک گیت‌وی دارد. به فرایند ترجمه فناوری‌های مختلف شبکه به شکلی که دستگاه‌ها قادر به درک زبان یکدیگر باشند، مبدل پروتکل (protocol converter) گفته می‌شود.

تفاوت تجهیزات اکتیو و پسیو شبکه چیست؟

تجهیزات شبکه :

تمامی **شبکه ها از تجهیزات سخت افزاری و نرم افزاری** مختلفی تشکیل شده اند که با هدف تبادل اطلاعات به یکدیگر متصل میشوند. در حقیقت بکارگیری تجهیزات شبکه باید به گونه ای باشد تا کلاینتها بتوانند با حفظ کیفیت و سرعت مطلوب به تبادل اطلاعات بپردازند.

اکتیو و پسیو در انگلیسی به معنای (active : فعال) و (passive : غیرفعال) میباشد. در واقع اکتیو و پسیو در الکترونیک از جمله **عبارات رایج در علم شبکه** می باشند با وجود اینکه این دو مفهوم از یکدیگر مجزا هستند اما یکدیگر را کامل کرده و با کمک یکدیگر شبکه را میسازند.

تجهیزات شبکه چیست؟

تجهیزات شبکه یا سخت افزار شبکه، دستگاه‌های فیزیکی هستند که برای ارتباط و تعامل بین سخت‌افزارها در یک شبکه کامپیوتری مورد نیاز هستند.

به طور کلی تجهیزات شبکه به دو دسته ی اکتیو (Active)و پسیو (Passive)تقسیم می‌شوند. تجهیزات اکتیو به تجهیزاتی گفته می‌شود که سیگنال‌های الکترونیکی را تولید، بازتولید، هدایت و مسیریابی می‌کنند. تجهیزات اکتیو یا فعال، در شبکه سیگنال‌ها را تولید می‌کند و از طریق تجهیزات پسیو سیگنال‌ها را در شبکه جابه جا می‌کنند. تجهیزات اکتیو شبکه برای انتقال، مدیریت یا نظارت بر بسته‌هایی که توسط شبکه‌ها ارسال می‌شوند نیز به کار گرفته می‌شوند.

نبود هر یک از تجهیزات اکتیو باعث می‌شود عملکرد شبکه با مشکل روبرو شود. وجود برخی از آن‌ها ضروری است و برخی تنها برای دسترسی ساده‌تر به اطلاعات استفاده می‌شود. مثلا وجود یک NAS در زمان پیاده‌سازی شبکه ضرورتی ندارد، اما هنگامی که صحبت از حجم زیادی از اطلاعات در میان باشد،

وجود یک NAS که قابلیت پشتیبانی از دیسک‌های سخت و حافظه‌های حالت جامد را دارد به میزان قابل توجهی باعث بهبود خدمت‌رسانی و تسریع در روند انجام کارها می‌شود.

برخی از تجهیزات اکتیو و پسیو در شبکه

بطور کلی **تجهیزات پسیو شبکه** به آن دسته از تجهیزاتی گفته میشود که در جریان انتقال داده و اطلاعات شبکه تاثیری بر روی جریان الکتریکی ندارند و تجهیزات اکتیو نیز به آن دسته از تجهیزات اطلاق میشود که در روند انتقال داده ها به جریان الکتریکی نیاز دارند.

پسیو یعنی چه ؟ تجهیزات Passive یا غیرفعال علاوه بر عدم اتصال به برق معمولا در داخل ابزارهای دیگر به کار میروند.

اکتیو یعنی چه؟ تجهیزات active شبکه که در آن انواع تجهیزات الکترونیکی وجود دارد علاوه بر اتصال به برق سیگنالها را نیز تقویت میکنند.

از جمله **تجهیزات اکتیو شبکه** میتوان به موارد ذیل اشاره کرد:

- سرورها
- هاب شبکه
- سوئیچ شبکه
- مودم
- روتر
- اکسس پوینت
- Repeater
- فایروال
- کارت شبکه

تفاوت تجهیزات اکتیو و پسیو

همانطور که از نام تجهیزات اکتیو یا فعال مشخص است نبود این تجهیزات باعث **عدم کارکرد شبکه** خواهد شد، در مقابل تجهیزات غیر فعال یا پسیو به ملزوماتی اطلاق میشوند که کارکرد آنها منوط به وجود و عملکرد مناسب تجهیزات اکتیو است.

تصور کنید از کار افتادن یا نبود یک سوئیچ باعث میشود نتوانید بسیاری از تجهیزات را به شبکه متصل کنید اما وجود یک کابل در صورتیکه سوئیچ یا سروری در شبکه نباشد کاربردی نداشته و عملکرد آن بسته به وجود سوئیچ است.

لازم به ذکر است که تجهیزات و خدمات اکتیو و پسیو شبکه کامل کننده و مکمل یکدیگر میباشند.

تجهیزات پسیو شبکه چیست؟

مهم‌ترین بخش راه اندازی شبکه، تجهیزات مستقر در زیرساخت است. پسیو (Passive) به معنای غیرفعال است و به تجهیزاتی اشاره دارد که تاثیری روی انتقال داده‌ها ندارند. پسیو به خدمات نصب و راه اندازی تجهیزات شبکه که وارد مرحله پیکربندی نمی‌شوند گفته می‌شود.

تجهیزات پسیو شبکه های کامپیوتری تجهیزاتی هستند که بدون جریان برق کار می‌کنند و نیازی به جریان الکتریسیته ندارند. تجهیزات پسیو شبکه فاقد برنامه‌ریزی هستند و به لحاظ اندازه قابل تغییر نبوده و ثابت هستند. منظور از ثابت و غیر قابل تغییر بودن این است که هنگامی که یکی از ملزومات پسیو شبکه مثل رک را خریداری می‌کنید، امکان تغییر اندازه آن وجود ندارد.

تجهیزات پسیو در تعامل با تجهیزات اکتیو قابل استفاده هستند، زیرا مادامی که تجهیزات اکتیو آماده نباشند، هیچ‌گونه اطلاعاتی انتقال نمی‌یابد و در واقع شبکه قابل استفاده نیست. اولین قدم در عملیات پسیو شبکه، طراحی استاندارد، پیاده‌سازی نقشه طراحی و به‌کارگیری تجهیزات با کیفیت است.

تجهیزات پسیو شبکه چیست ؟

از جمله اصلیترین تجهیزات پسیو شبکه میتوان به موارد ذیل اشاره کرد:

- کابلهای شبکه
- پچ کورد شبکه
- داکت / ترانک
- پچ پنل
- سوکت های دیواری
- کیستون شبکه
- فیس پلیت
- رک شبکه

تفاوت بین تجهیزات پسیو و اکتیو چیست؟

خدمات اکتیو و پسیو در تکمیل یکدیگر معرفی شده و هیچ‌کدام نسبت به دیگری ارجحیت ندارند. طوری که برقراری ارتباط کامل میان شبکه بدون اتصال مناسب میان اجزا ممکن نیست. تقسیم‌بندی اکتیو و پسیو کاملا ذهنی و برای درک و ارتباط بهتر کارشناسان شبکه است.

تفاوت تجهیزات پسیو و اکتیو شبکه در یک کلام به امکان تغییر داده‌های قابل انتقال مربوط است. در اکتیو نتورک تجهیزات و خدمات داده‌های شبکه را تغییر می‌دهند، اما در پسیو نتورک هیچ فعالیتی، چه مستقیم چه غیرمستقیم، روی داده‌های قابل انتقال تاثیر نمی‌گذارد. پسیوکار بیشتر با کابل‌کشی و اکتیوکار با نصب نرم افزار شبکه سروکار دارد. تجهیزات شبکه اکتیو انرژی تولید می‌کنند، جریان را کنترل می‌کنند و به منبع خارجی نیاز دارند؛ در حالی که در شبکه پسیو تجهیزات انرژی مصرف می‌کنند، قدرت کنترل جریان را ندارند و هیچ‌گونه منبع خارجی نمی‌خواهند.

شبکه اکتیو و پسیو چیست؟

شبکه پسیو نوعی شبکه کامپیوتری است که در آن هر گره روی یک عملکرد یا فرآیند از پیش تعریف شده کار می‌کند. شبکه پسیو هیچ کد یا دستورالعمل تخصصی را در هیچ گره‌ای اجرا نمی‌کند و رفتار خود را به صورت پویا تغییر نمی‌دهد. به‌طور معمول، این رفتار مربوط به هر گره روتر شبکه است. شبکه پسیو یکی از متداول‌ترین نوع شبکه‌بندی تجهیزات است. البته این امر مستلزم آن است که کل زیرساخت‌های شبکه قبل از بهره برداری از پیش تعیین و تنظیم شوند.

شبکه اکتیو، شبکه‌ای است که انواع مختلفی از تجهیزات الکترونیکی در آن‌ها وجود دارد. این دستگاه‌ها ممکن است در سمت کاربر نهایی، در مرکز شبکه برای پشتیبانی از پروتکل اترنت به منظور بهبود سرعت بارگذاری و بارگیری بسته‌های اطلاعاتی باشند.

امروزه انواع مختلفی از شبکه‌های مسی پسیو وجود دارد. شبکه‌ای که تقریباً همه با آن آشنا هستیم، شبکه تلویزیون کابلی خانگی (CATV) است. در شبکه catv مسی، ارائه‌دهنده خدمات کابلی، سیگنال را از طریق کابل کواکسیال به خانه مشترکان تحویل می‌دهد. در ابتدایی‌ترین حالت، کابل وارد خانه و به یک تلویزیون می‌رسد. برای خانه‌هایی که چند تلویزیون دارند، سیگنال باید میان تلویزیون‌ها تقسیم شود. تقسیم معمولاً با یک دستگاه ارزان قیمت انجام می‌شود که معمولاً به آن تقسیم‌کننده می‌گویند. اسپلیتر نیازی به برق ندارد. معمولاً یک ورودی واحد دارد و ممکن است دو، سه، چهار یا بیشتر خروجی داشته باشد.

یکی از مشکلات این نوع شبکه پسیو از دست دادن قدرت سیگنال است. وقتی سیگنال ارائه‌دهنده کابل تقسیم می‌شود و به چند تلویزیون منتقل می‌شود، قدرت سیگنال هر تلویزیون کاهش می‌یابد. افزودن بیش از حد تلویزیون‌ها می‌تواند قدرت سیگنال را کاهش دهد.

در چنین شرایطی کاربران مجبور هستند از شبکه اکتیو catv استفاده کنند. شبکه اکتیو مسی نیز انواع مختلفی دارد. همان‌گونه که در مثال قبل به آن اشاره کردیم در مدل یک شبکه پسیو catv خانگی، وقتی تعداد تجهیزات زیاد می‌شود و قدرت سیگنال کاهش پیدا می‌کند کاربران به سراغ شبکه اکتیو می‌روند. در این حالت یک کابل وارد خانه می‌شود و به آمپلی‌فایر (تقویت‌کننده) هدایت می‌شود. تقویت‌کننده، سیگنال کابل را تقویت و سپس تقسیم می‌کند. قدرت سیگنال در هر خروجی آمپلی‌فایر تقریباً با قدرت سیگنال کابل ورودی یکسان است.

بدین ترتیب مشکل قدرت سیگنال در شبکه پسیو حل می‌شود، اما پیچیدگی را افزایش می‌دهد. علاوه بر این، اگر آمپلی‌فایر توزیع‌کننده خراب شود، همه تجهیزات سیگنال‌های خود را از دست می‌دهند. شبکه اکتیو و پسیو هر کدام مزایای خود را دارند.

تفاوت شبکه اکتیو و پسیو

نوع شبکه در بررسی تفاوت شبکه اکتیو و پسیو نقش مهمی دارد. شبکه اکتیو مسی یکی از انواع اصلی است که دسته‌بندی‌های مختلفی دارد. تفاوتی که میان شبکه اکتیو مسی و پسیو مسی وجود دارد این است که برخی تجهیزات، همچون آمپلی‌فایر به منظور تقویت سیگنال‌های آسیب دیده استفاده می‌شود و این اطمینان را می‌دهد که سیگنال‌ها می‌توانند تا مسافت‌های طولانی منتقل شود.

ساختار شبکه‌های اکتیو مسی پیچیده‌تر از شبکه‌های پسیو است و بدون استفاده از تجهیزات اکتیو غیر قابل استفاده است. شبکه پسیو نوری یکی دیگر از انواع پسیو شبکه‌ها است و شباهت زیادی با شبکه پسیو مسی دارد، با این تفاوت که در این شبکه‌ها، به جای کابل‌های شبکه مثل کواکسیال از کابل‌های نوری استفاده می‌شود. در این نوع شبکه، کوپلر نقش کلیدی دارد و وظیفه آن، توزیع و جفت سیگنال‌های نوری است. البته در شبکه‌های پسیو نوری می‌توان از اسپلیتر نوری برای توزیع سیگنال‌های نوری استفاده کرد.

نحوه نظارت بر شبکه جنبه دیگری از تفاوت شبکه اکتیو و پسیو را مشخص می‌کند. مانیتورینگ شبکه اکتیو synthetic monitoring نام دارد. در روش مذکور ترافیک آزمایشی به شبکه تزریق می‌شود تا خطاها یا مشکلات درون شبکه شناسایی شوند. این روش در یافتن و گزارش داده‌های بلادرنگ مثل از دست دادن بسته، جیتر (jitter) ، زمان پاسخ پروتکل‌های http و https و غیره کمک می‌کند.

فرایند نظارت پسیو شبکه شامل ثبت و تجزیه و تحلیل ترافیک واقعی کاربران برای درک روندهای استفاده از شبکه است. در این حالت ابزار نظارتی می‌تواند به ردیابی این موضوع بپردازد که کدام عناصر شبکه پهنای باند موجود را مصرف می‌کنند. در این روش به جای تزریق داده‌های آزمایشی برای تجزیه و تحلیل ترافیک از داده‌های واقعی کاربران استفاده می‌شوند.