آشنائی با عناصر یک شبکه محلی

سخاروش - با این که هر شبکه محلی دارای ویژگی ها و خصایص منحصربفرد مختص به خود می باشد که به نوعی آن را از سایر شبکه ها متمایز می نماید ، ولی در زمان پیاده سازی و اجرای یک شبکه محلی ، اکثر آنان از استانداردها و عناصر شبکه ای مشابه ای استفاده می نمایند . شبکه های WAN نیز دارای وضعیتی مشابه شبکه های محلی بوده و امروزه در این نوع شبکه ها از مجموعه ای گسترده از اتصالات (از Dial-up تا broadband) استفاده می گردد که بر پهنای باند ، قیمت و تجهیزات مورد نیاز به منظور برپاسازی این نوع شبکه ها تاثیر می گذارد .
در ادامه به برخی از مهمترین ویژگی ها و عناصر شبکه ای استفاده شده در شبکه های محلی اشاره می گردد :

رسانه های انتقال داده در شبکه های کامپیوتری ، ستون فقرات یک شبکه را تشکیل می دهند . هر شبکه کامپیوتری می تواند با استفاده از رسانه های انتقال داده متفاوتی ایجاد گردد . وظیفه رسانه های انتقال داده ، حمل اطلاعات در یک شبکه محلی می باشد . شبکه های محلی بدون کابل از اتمسفر به عنوان رسانه انتقال داده استفاده می نمایند . رسانه های انتقال داده عناصر لایه یک و یا فیزیکی شبکه های محلی می باشند .

هر رسانه انتقال داده دارای مزایا و محدودیت های مختص به خود می باشد . طول کابل ، قیمت و نحوه نصب از مهمترین ویژگی های رسانه های انتقال داده می باشند .

اترنت ، متداولترین تکنولوژی استفاده شده در شبکه های محلی می باشد که اولین مرتبه با همکاری سه شرکت دیجیتال ، اینتل و زیراکس و با نام DIX ارائه گردید . در ادامه و در سال 1983 موسسه IEEE با استفاده از DIX ، استاندارد 802.3 IEEE را مطرح نمود . در ادامه استانداردهای متعددی توسط کمیته های تخصصی IEEE ارائه گردید .

قبل از انتخاب یک مدل خاص اترنت برای پیاده سازی شبکه ، می بایست کانکتورهای مورد نیاز برای هر نمونه پیاده سازی را بررسی نمود . در این رابطه لازم است سطح کارآئی مورد نیاز در شبکه نیز بررسی گردد .

مشخصه های کابل و کانکتورهای مورد نیاز برای پیاده سازی هر یک از نمونه های اترنت ، متاثر از استانداردهای ارائه شده توسط انجمن های صنایع الکترونیک و مخابرات (EIA/TIA) می باشد .

با توجه به لایه فیزیکی مربوطه ، از اتصالات متفاوتی در شبکه های اترنت استفاده می گردد . کانکتور RJ-45 (برگرفته از registered jack) متداولترین نمونه در این زمینه است .

برای اتصال دستگاه های شبکه ای از کابل ها ی متفاوتی استفاده می گردد . مثلا" برای اتصال سوئیچ به روتر ، سوئیچ به کامپیوتر ، هاب به کامپیوتر از کابل های straight-through و برای اتصال سوئیچ به سوئیچ ، سوئیچ به هاب ، هاب به هاب ، روتر به روتر ، کامپیوتر به کامپیوتر و روتر به کامپیوتر از کابل های crossover استفاده می گردد .

Repeater ، یک سیگنال را دریافت و با تولید مجدد آن ، امکان ارسال آن را در مسافت های طولانی تر قبل از تضعیف سیگنال فراهم می نماید . در زمان توسعه سگمنت های یک شبکه محلی، می بایست از استانداردهای موجود در این زمینه استفاده نمود . مثلا" نمی توان بیش از چهار repeater را بین کامپیوترهای میزبان در یک شبکه استفاده نمود .

هاب در واقع repeater های چند پورته می باشند . در اغلب موارد تفاوت بین دو دستگاه فوق ، تعداد پورت های ارائه شده توسط هر یک از آنان است . با این که یک repeater معمولا" دارای صرفا" دو پورت می باشد ، یک هاب می تواند دارای چهار تا بیست و چهار پورت باشد . در شبکه های Ethernet 10BAST-T و یا Ethernet 100BASE-T استفاده از هاب بسیار متداول است . با استفاده از هاب ، توپولوژی شبکه از bus خطی که در آن هر دستگاه مستقیما" به ستون فقرات شبکه متصل می گردد ، به یک مدل ستاره و یا star تبدیل می شود . داده دریافتی بر روی یک پورت هاب برای سایر پورت های متصل شده به یک سگمنت شبکه ای مشابه نیز ارسال می گردد . (بجزء پورتی که داده را ارسال نموده است) . به موازات افزایش دستگاه های متصل شده به یک هاب ، احتمال بروز تصادم و یا Collision افزایش می یابد . یک تصادم زمانی بروز می نماید که دو و یا بیش از دو ایستگاه در یک لحظه اقدام به ارسال داده در شبکه نمایند . در صورت بروز یک تصادم ، تمامی داده ها از بین خواهد رفت . هر دستگاه متصل شده به یک سگمنت مشابه شبکه ، عضوی از یک collision domain می باشند .

در برخی موارد لازم است که یک شبکه بزرگ محلی به سگمنت های کوچکتر و قابل مدیریتی تقسیم گردد. هدف از انجام این کار کاهش ترافیک و افزایش حوزه جغرافیائی یک شبکه است . از دستگاه های شبکه ای متفاوتی به منظور اتصال سگمنت های متفاوت یک شبکه به یکدیگر استفاده می گردد . Bridge ، سوئیچ ، روتر و gateway نمونه هائی در این زمینه می باشند . سوئیچ و Bridge در لایه Data Link مدل مرجع OSI کار می کنند . وظیفه Bridge ، اتخاذ تصمیم هوشمندانه در خصوص ارسال یک سیگنال به سگمنت بعدی شبکه است . پس از دریافت یک فریم توسط Bridge ، آدرس MAC مقصد فریم در جدول Bridge بررسی تا مشخص گردد که آیا ضرورتی به فیلترینگ فریم وجود دارد و یا می بایست فریم به سمت یک سگمنت دیگر هدایت گردد .
فرآیند تصمیم گیری با توجه به مجموعه قوانین زیر انجام می شود :
□ در صورتی که دستگاه مقصد بر روی سگمنت مشابه باشد ، Bridge فریم دریافتی را بلاک و آن را برای سایر سگمنت ها ارسال نمی نماید . به فرآیند فوق، فیلترینگ می گویند .
□ در صورتی که دستگاه مقصد بر روی یک سگمنت دیگر باشد ، Bridge آن را به سگمنت مورد نظر فوروارد می نماید .
□ در صورتی که آدرس مقصد برای Bridge ناشناخته باشد ، Bridge فریم را برای تمامی سگمنت های موجود در شبکه بجزء سگمنتی که فریم را از آن دریافت نموده است ، فوروارد می نماید . به فرآیند فوق flooding می گویند. استفاده مناسب از

Bridge ، افزایش کارآئی یک شبکه را به دنبال خواهد داشت .

از سوئیچ در برخی موارد به عنوان یک bridge چند پورته نام برده می شود . با این که یک Bridge معمولی ممکن است دارای صرفا" دو پورت باشد که دو سگمنت شبکه را به یکدیگر متصل می نماید ، سوئیچ می تواند دارای چندین پورت باشد. همانند bridge ، سوئیچ ها دارای دانش و آگاهی لازم در خصوص بسته های اطلاعاتی دریافتی از دستگاه های متفاوت موجود در شبکه می باشند و دانش خود را نیز متناسب با شرایط موجود ارتقاء می دهند(یادگیری) . سوئیچ ها از اطلاعات فوق به منظور ایجاد جداول موسوم به جداول فورواردینگ استفاده نموده تا در ادامه قادر به تعیین مقصد داده ارسالی توسط یک کامپیوتر برای کامپیوتر دیگر موجود بر روی شبکه باشند .

با این که سوئیچ و Bridge دارای شباهت هائی با یکدیگر می باشند ، ولی سوئیچ ها دستگاه هائی بمراتب پیشرفته تر و حرفه ای تر نسبت به Bridge می باشند . همانگونه که اشاره گردید ، معیار اتخاذ تصمیم Bridge برای فورواردینگ یک فریم ، آدرس MAC یک فریم است . سوئیچ دارای چندین پورت است که سگمنت های متفاوت شبکه به آنان متصل می گردند . سوئیچ ها با توجه به تاثیر محسوس آنان در افزایش کارآئی شبکه از طریق بهبود سرعت و پهنای باند ، به یکی از متداولترین دستگاه های ارتباطی شبکه تبدیل شده اند .

سوئیچینگ ، یک فن آوری است که کاهش ترافیک و افزایش پهنای باند در شبکه های محلی اترنت را به دنبال خواهد داشت . سوئیچ ها را بسادگی می توان جایگزین هاب نمود ، چراکه آنان از زیرساخت سیستم کابل موجود می توانند استفاده نمایند .

سوئیچ ها دارای سرعتی بمراتب بیشتر از Bridge بوده و قادر به حمایت از پتانسیل های جدیدی نظیر شبکه های VLAN می باشند .

یک سوئیچ اترنت دارای مزایای متعددی است ، مثلا" به کاربران متعددی اجازه داده می شود که به صورت موازی از طریق مدارات مجازی و سگمنت های اختصاصی شبکه در یک محیط عاری از تصادم ، با یکدیگر ارتباط برقرار نمایند . بدین ترتیب از پهنای باند موجود به صورت بهینه استفاده می گردد .

روتر مسئولیت روتینگ بسته های اطلاعاتی از مبداء به مقصد را در شبکه های محلی برعهده دارد و امکان ارتباطی را برای شبکه های WAN فراهم می نماید . در شبکه های محلی روتر شامل broadcast بوده و سرویس های ترجمه آدرس محلی نظیر ARP و RARP را ارائه می نماید و می تواند با استفاده از یک ساختار Subnetwork ، شبکه را سگمنت نماید . به منظور ارائه سرویس های فوق ، روتر می بایست به LAN و WAN متصل باشد .

وظیفه کارت شبکه (NIC) ، اتصال یک دستگاه میزبان به محیط انتقال شبکه است . کارت شبکه یک برد مدار چاپی است که درون یکی از اسلات های موجود بر روی برداصلی کامپیوتر و یا دستگاه جانبی یک کامپیوتر نصب می گردد . اندازه کارت شبکه بر روی کامپیوترهای Laptop و یا notebook به اندازه یک کارت اعتباری است .

کارت های شبکه به منزله دستگاه های لایه دوم مدل مرجع OSI می باشند ، چراکه هر کارت شبکه به همراه خود یک کد منحصربفرد را که به آن آدرس MAC می گویند ، ارائه می نماید . از آدرس فوق به منظور کنترل مبادله اطلاعات در شبکه استفاده می گردد .

هر کارت شبکه دارای کانکتورهائی است که امکان اتصال آن را به محیط انتقال فراهم می نماید . در برخی موارد ممکن است نوع کانکتور موجود بر روی یک کارت شبکه با نوع رسانه انتقال داده مطابقت ننماید . مثلا" در روترهای سیسکو مدل 2500 از یک کانکتور AUI استفاده شده است و برای اتصال به یک کابل اترنت UTP cat 5 می بایست از یک transmitter/receiver که به آنان transceiver گفته می شود ، استفاده گردد . transceiver ، مسئولیت تبدیل یک نوع سیگنال و یا کانکتور به نوع دیگری را برعهده دارد . به عنوان نمونه ، یک transceiver می تواند یک اینترفیس AUI پانزده پین را به یک RJ-45 jack متصل نماید . transceiver ، به عنوان یک دستگاه لایه یک شبکه ایفای وظیفه می نماید چراکه صرفا" با بیت ها کار می نماید و دارای اطلاعات آدرس دهی خاصی و یا پروتکل های لایه بالاتر نمی باشد .

در شبکه های LAN و یا WAN ، تعدادی کامپیوتر با یکدیگر متصل شده تا سرویس های متفاوتی را در اختیار کاربران قرار دهند . برای انجام این کار ، کامپیوترهای موجود در شبکه دارای وظایف و یا مسئولیت های مختص به خود می باشند . در شبکه های نظیر به نظیر (peer-to-peer) ، کامپیوترهای موجود در شبکه دارای وظایف و مسئولیت های معادل و مشابه می باشد(هم تراز) . هر کامپیوتر می تواند هم به عنوان یک سرویس گیرنده و هم به عنوان یک سرویس دهنده در شبکه ایفای وظیفه نماید . مثلا" کامپیوتر A می تواند درخواست یک فایل را از کامپیوتر B نماید . در این وضعیت ، کامپیوتر A به عنوان یک سرویس گیرنده ایفای وظیفه نموده و کامپیوتر B به عنوان یک سرویس دهنده رفتار می نماید . در ادامه ، کامپیوترهای A و B می توانند دارای وظایف معکوسی نسبت به وضعیت قبل باشند .

در شبکه های نظیر به نظیر ، هر یک از کاربران کنترل منابع خود را برعهده داشته و می توانند به منظور به اشتراک گذاشتن فایل هائی خاص با سایر کاربران ، خود راسا" تصمیم گیری نمایند . کاربران همچنین ممکن است ، به منظور دستیابی به منابع اشتراک گذاشته شده ، سایر کاربران را ملزم به درج رمز عبور نمایند . با توجه به این که تمامی تصمیمات فوق توسط هر یک از کاربران و به صورت جداگانه اتخاذ می گردد ، عملا" یک نقطه مرکزی برای کنترل و یا مدیریت شبکه وجود نخواهد داشت . در این نوع شبکه ها هر یک از کاربران مسئولیت گرفتن Backup از داده های موجود بر روی سیستم خود را برعهده داشته تا در صورت بروز مشکل بتوانند از آنان به منظور بازیافت اطلاعات استفاده نمایند . زمانی که یک کامپیوتر به عنوان یک سرویس دهنده در شبکه ایفای وظیفه می نماید ، سرعت و کارآئی آن متناسب با حجم درخواست های دریافتی کاهش خواهد یافت .

نصب و عملکرد شبکه های Peer-to-Peer ساده بوده و در این رابطه به تجهیزات اضافه ای به جزء نصب یک سیستم عامل

مناسب بر روی هر یک از کامپیوترها، نیاز نخواهد بود . با توجه به این که کاربران مسئولیت کنترل منابع خود را برعهده دارند ، به مدیریت متمرکز و اختصاصی نیاز نمی باشد .

به موازات رشد شبکه های Peer-To-Peer ، تعریف ارتباط بین کامپیوترهای موجود در شبکه و ایجاد یک هماهنگی منسجم بین آنان ، به یک مشکل اساسی در شبکه تبدیل می شود . این نوع شبکه ها تا زمانی که تعداد کامپیوترهای موجود در شبکه کمتر از ده عدد باشد ، به خوبی کار می کنند و همزمان با افزایش تعداد کامپیوترهای موجود در شبکه ، کارآئی شبکه به شدت کاهش پیدا خواهد کرد . با توجه به این که کاربران مسئولیت کنترل دستیابی به منابع موجود بر روی کامپیوترهای خود را برعهده دارند ، امنیت در این نوع شبکه ها دارای چالش های جدی مختص به خود می باشد .

در شبکه های سرویس گیرنده - سرویس دهنده ، سرویس های شبکه بر روی یک کامپیوتر اختصاصی با نام سرویس دهنده قرار گرفته و سرویس دهنده مسئول پاسخگوئی به درخواست سرویس گیرندگان می باشد . سرویس دهنده یک کامپیوتر مرکزی است که به صورت مستمر به منظور پاسخگوئی به درخواست سرویس گیرندگان برای فایل ، چاپ ، برنامه ها و سایر سرویس ها در دسترس می باشد .

سرویس دهندگان در شبکه های سرویس گیرنده - سرویس دهنده بگونه ای طراحی شده اند که بتوانند بطور همزمان به درخواست های سرویس گیرندگان متعددی پاسخ دهند . قبل از این که یک سرویس گیرنده قادر به دستیابی منابع موجود بر روی سرویس دهنده باشد ، می بایست سرویس گیرنده شناسائی و به منظور استفاده از منبع درخواستی تائید گردد . بدین منظور به هر یک از سرویس گیرندگان یک account name و رمز عبور نسبت داده می شود . بدین ترتیب بر خلاف شبکه های Peer-To-Peer ، امنیت و کنترل دستیابی متمرکز و توسط مدیران شبکه پیاده سازی و مدیریت می گردد . هزینه برپاسازی و مدیریت شبکه های سرویس گیرنده - سرویس دهنده نسبت به شبکه های Peer-to-Peer بمراتب بیشتر است و تمرکز سرویس ها در یک نقطه می تواند آسیب پذیری سیستم را افزایش داده و ارائه سرویس های online را دچار مشکل نماید . بدین منظور لازم است از راهکارهائی منطقی به منظور برخورد با مسائل غیرقابل پیش بینی و استمرار ارائه خدمات توسط سرویس دهنده استفاده گردد .

منبع: سخاروش
http://www.srco.ir