بسم الله الرحمن الرحیم

مجموعه مقالات اینترنتی

موضوع:

آموزش شبکه های کامپیوتری

LEARNING NETWORK

گرد آورنده :

داوود خرسند

D_KHORSAND

Email:

DKHX2000@yahoo.com

DKHX2000@Gmail.com

AUTUMN 2005

پائیز ۸۴

DHCP و نحوه کار آن

اکثر کاربران اینترنت با واژه IP آشنايي دارند.IP یک عدد ۳۲ بيتي است که به صورت ۸ بیت ۸ بیت با یک نقطه از یکدیگر مجزا میشوند و هر یک از آنها معرف یک کامپیوتر در اینترنت است. به عبارت دیگر آدرس هر کامپیوتر در اینترنت با IP مشخص میشود. آیا تا به حال از خود سئوال کرده اید که فرایند تعیین IP براي سیستم شما در یک شبکه یا اینترنت چیست؟

DHCP Service :

DHCP مخفف عبارت Dynamic Host Configuration Protocol است که با نصب این سرویس بر روي یک Server میتوانیم در ان یک Range IP تعریف نموده و از ان بخواهیم تا به Client هایي که IP انها به صورت اتوماتیک تنظیم شده است IP اختصاص دهد.(تمامي کاربران اینترنت به صورت اتوماتیک IP دریافت میکنند.)

چگونگي کارکرد یک DHCP:

زمانیکه یک کاربر کامپیوتر خود را راه اندازي مي کند سیستم عامل آن بعد از بالا آمدن در خواستIP میکند. بعد از آن ٤ مرحله انجام میگیرد:

DHCP Discover-١

در این مرحله Client درخواست خود را جهت دریافتIP در شبکه Broadcast میکند. به آدرس ۲۵۵,۲۵۵,۲۵۵,۲۵۵ ارسال میکند و IP خود او نیز ۰,۰,۰,۰ در نظر میگیرد.

DHCP Offer-٢

در این مرحله تمام DHCP Server هائیکه Broadcast انجام شده در مرحله اول را دریافت میکنند از Range IP تعریف شده بر روي خود یک IP انتخاب نموده و به همراه مدت زماني که قرار است آنIP را در اختیار Client قرار دهد و آنرا به شکل زیر ارسال میکند.

Source IP=IP of DHCP Server
Destination MAC Address=Client Destination IP=255.255.255.255

DHCP Request-٣

Client درخواست کننده پس از دریافت DHCP Offer ها اولین DHCP Offer را انتخاب نموده و آنرا توسط یک Packet در شبکه Broadcast میکند و در آن Packet آدرسDHCP Server که Offer او قبول شده است مشخص مینماید.

DHCP Ack,DHCP Nack -٤

پس از آنکه Client به DHCP Server که Offer اوقبول شده DHCP Request را فرستاد در صورتیکه هنوز IP که Offer شده در Range او وجود داشته باشد و توسط Admin حذف نشده باشد Server DHCP تایید خود را مبني بر اختصاص IP به Client اعلام میکند. ولي اگر IP توسط Admin از Range مربوطه حذف شده باشد DHCP به Client درخواست کننده پیغامDHCP Nack را ارسال میکند و Client مجبور میشود که تمام مراحل را دوباره طي کند.

اگر DHCP در شبکه موجود نباشد:
Client پس از ارسال DHCP Discover یک ثانیه منتظر جواب مي ایستد اگر جوابي دریافت نکرد ۳بار دیگر به فاصله زماني ۹ و ۱۳ و ١٦ ثانیه دوباره Broadcast میکند اگر باز هم جوابي نگرفت هر ٥ دقیقه یک بار به کار خود ادامه میدهد.

APIPA (Automatic Private IP Addressing) :
Client هاي ۹۸ و ۲۰۰۰ اگر DHCP را پیدا نکنند به هر دلیلي به صورت اتوماتیک از رنج x.y.١٦٩,٢٥٤ یک IP انتخاب میکنند. در ضمن قبل از استفاده از آن آنرا Broadcast میکنند تا احیانا Client دیگري در حال استفاده از آن IP نباشد. با این حال هر ٥ دقیقه یک بار به تلاش خود مبني بر گرفتن IP از DHCP ادامه میدهد.

دستور ipconfig:

با استفاده از این دستور که در Command Prompt اجرا میشود میتوان تنظیمات IP را مشاهده کنیم.براي گرفتن IP از DHCP باید دستور IPCONFIG/RENEW را درCMD وارد کنیم و براي ازاد کردن IP دستور IPCONFIG/RELEASE را در همان CMD وارد میکنیم.

IP reservation:

در صورت نیاز میتوان براي کامپیوتر ها و مخصوصا Network Printer ها IP رزرو نمود تا هر بار که آنها درخواست IP نمودند آن IP هاي رزرو شده به آنها اختصاص داده شود براي این کار دانستنMAC Address کارت شبکه مورد نیاز است.

Lease Time:

به مدت زماني که یک IP به یک Client اختصاص داده میشود Lease Time میگویند که به صورت پیش فرض ۸ روز است.

فایروال ها : یک ضرورت اجتناب ناپذیر در دنیای امنیت اطلاعات

امنیت اطلاعات و ایمن سازی کامپیوترها به یک ضرورت غیرقابل انکار در عصر اطلاعات تبدیل شده است. پرداختن به مقوله امنیت اطلاعات با زبانی ساده بیش از هر زمان دیگر احساس می شود، چراکه هر یک از عوامل انسانی و غیرانسانی دارای جایگاه تعریف شده ای در نظام مهندسی امنیت اطلاعات می باشند. آشنائی اصولی و منطقی با این نظام مهندسی و آگاهی از عناصر موجود در این ساختار به همراه شناخت علمی نسبت به مسئولیت هر یک از عناصر فوق، امری لازم و حیاتی است.

فایروال ها ، یکی از عناصر اساسی در نظام مهندسی امنیت اطلاعات می باشند که استفاده از آنان به یک ضرورت اجتناب ناپذیر در دنیای امنیت اطلاعات و کامپیوتر تبدیل شده است . بسیاری از افرادی که جدیدا" قدم در عرصه گسترده امنیت اطلاعات می گذارند ، دارای نگرانی و یا سوالات مفهومی خاصی در ارتباط با فایروال ها و جایگاه استفاده از آنان در جهت ایمن سازی شبکه های کامپیوتری می باشند .

در این مطلب قصد داریم به برخی از مفاهیم و نکات مهم و اساسی در خصوص فایروال ها اشاره ای داشته باشیم تا از این رهگذر بتوانیم دانش لازم به منظور بکارگیری و مدیریت بهینه فایروال ها را بدست آوریم .

NAT (برگرفته از Translation Network Address)

اولین و در عین حال مهم ترین وظیفه یک فایروال ، جداسازی شبکه داخلی یک سازمان از اینترنت است . یکی از فنآوری های موجود که ما را در جهت نیل به خواسته فوق کمک می نماید ، جداول NAT می باشند (NAT ، همچنین کمک لازم در جهت حل معضل کمبود آدرس های IP را ارائه می نماید) . مهمترین ایده مطرح شده توسط NAT ، عدم دستیابی به اکثر کامپیوترهای موجود در یک شبکه خصوصی از طریق اینترنت است . یکی از روش های نیل به خواسته فوق ، استفاده از آدرس های IP غیرمعتبر (Invalid) می باشد .

در اکثر موارد بکارگیری NAT ، صرفا" آدرس IP معتبر (Valid) به فایروال نسبت داده می شود و تمامی کامپیوترهائی که مسئولیت حفاظت از آنان به فایروال واگذار شده است ، از آدرس های IP که صرفا" بر روی شبکه داخلی معتبر می باشد ، استفاده می نمایند . با تبعیت از چنین رویکردی ، زمانی که یک کامپیوتر موجود در شبکه داخلی نیازمند برقراری ارتباط با دنیای خارج است ، اقدام به ارسال درخواست خود برای فایروال می نماید . در ادامه فایروال به نمایندگی از کامپیوتر متقاضی ، درخواست مورد نظر را ارسال می نماید . در زمان مراجعت درخواست ارسالی ، پاسخ مربوطه به فایروال رسیده و در نهایت ، فایروال آن را برای کامپیوتر موجود در شبکه داخلی ارسال می نماید .

فرض کنید ، کاربری قصد داشته باشد که یک وب سایت خاص را از طریق کامپیوتر موجود بر روی یک شبکه داخلی ملاقات نماید .پس از درج آدرس وب سایت مورد نظر در بخش آدرس برنامه مرورگر ، درخواست وی به یک درخواست HTTP ترجمه شده و برای فایروال ارسال می گردد . در ادامه ، فایروال از آدرس IP مختص به خود در ارتباط با درخواست HTTP و به نمایندگی از کاربر ارسال کننده درخواست ، استفاده می نماید . پس از پاسخ به درخواست ، پاسخ مربوطه برای فایروال ارسال شده و در نهایت فایروال آن را برای کاربر مربوطه ارسال می نماید .

فیلترینگ پورت ها

فیلترینگ پورت ها از جمله مهمترین عملیاتی است که توسط فایروال ها انجام می شود و شاید به همین دلیل باشد که اکثر مردم بر

این اعتقاد هستند که فایروال ها صرفا" به همین دلیل خاص طراحی و پیاده سازی شده اند و اغلب ، آنان را به عنوان ابزاری در جهت فیلترینگ پورت ها تصور می نمایند . همانگونه که می دانید ، مبادلات اطلاعات مبتنی بر پروتکل TCP/IP با استفاده و محوریت پورت ها انجام می گردد . در این رابطه ٦٥،٥٣٥ پورت TCP و به همین اندازه پورت UDP جداگانه وجود دارد که می توان از آنان به منظور مبادله اطلاعات استفاده نمود .

به منظور آشنائی با جایگاه پورت ها و نقش آنان در مبادله اطلاعات در پروتکل TCP/IP ، می توان آنان را نظیر ایستگاه های رادیوئی تصور نمود . فرض کنید TCP به عنوان موج FM و UDP به عنوان موج AM باشد . در چنین وضعیتی ، می توان یک پورت در پروتکل TCP/IP را همانند یک ایستگاه رادیوئی تصور نمود . همانگونه که یک ایستگاه رادیوئی با اهداف خاصی طراحی شده است ، پورت های TCP و UDP نیز چنین وضعیتی را داشته و با اهداف خاصی طراحی شده اند . یکی از مهمترین دلایل ضرورت استفاده از فایروال ها و فیلترینگ پورت ها ، استفاده غیرمتعارف از پورت ها به منظور نیل به اهدافی دیگر است . مثلا" پورت ٢١ مربوط به پروتکل TCP بطور سنتی به منظور FTP استفاده می گردد و مهاجمان می توانند از پورت فوق و با استفاده از برنامه هائی نظیر Telnet سوء استفاده نمایند (با این که پورت فوق به منظور استفاده توسط برنامه Telnet طراحی نشده است) .

پویش پورت ها و آگاهی از پورت های باز ، از جمله روش های متداولی است که توسط مهاجمان و به منظور یافتن یک نقطه ورود مناسب به یک سیستم و یا شبکه کامپیوتری ، مورد استفاده قرار می گیرد . مهاجمان پس از آگاهی از پورت های باز ، با بکارگیری برنامه هائی نظیر Telnet زمینه ورود غیر مجاز به یک سیستم را برای خود فراهم می نمایند .

وضعیت فوق و تهدیدات امنیتی مرتبط با آن ، ضرورت فیلترینگ پورت ها را به خوبی نشان می دهد . با فیلترینگ پورت ها ، این اطمینان ایجاد خواهد شد که هیچ چیزی نمی تواند از طریق یک پورت باز ارسال گردد مگر پروتکل هائی که توسط مدیریت شبکه به آنان اجازه داده شده است . مثلا" در صورتی که فیلترینگ پورت بر روی پورت ٢١ مربوط به پروتکل TCP اعمال گردد ، صرفا" به مبادلات اطلاعات مبتنی بر FTP اجازه داده خواهد شد که از این پورت استفاده نمایند و مبادله اطلاعات به کمک سایر پروتکل ها و بکارگیری پورت فوق ، امکان پذیر نخواهد بود .

محدوده عملیاتی فیلترینگ پورت ها می تواند از موارد اشاره شده نیز تجاوز نموده و در سطح هدر یک بسته اطلاعاتی و حتی محتویات آن نیز تعمیم یابد . در چنین مواردی ، هدر بسته اطلاعاتی بررسی و با مشاهده اطلاعاتی نظیر آدرس مبداء ، مقصد ، شماره پورت و سایر موارد دیگر در رابطه با آن اتخاذ تصمیم می گردد . مشکل موجود در این رابطه به وجود اطلاعات جعلی و یا نادرست در هدر بسته های اطلاعاتی برمی گردد . مثلا" فرستنده می تواند آدرس های IP و سایر اطلاعات ذخیره شده در هدر بسته های اطلاعاتی را جعل نماید . به منظور غلبه بر مشکل فوق ، نوع دیگری از فیلترینگ که برخی فایروال ها به آن stateful packet inspections و یا فیلترینگ پویای بسته های اطلاعاتی می گویند ، ایجاد شده است . در مدل فوق ، در مقابل بررسی هدر بسته های اطلاعاتی ، محتویات آنان مورد بازبینی قرار می گیرد . بدیهی است با آگاهی از این موضوع که چه چیزی در بسته اطلاعاتی موجود است ، فایروال ها بهتر می توانند در رابطه با ارسال و یا عدم ارسال آن برای یک شبکه داخلی تصمیم گیری نمایند

ناحیه غیرنظامی (Demilitarized Zone)

نواحی غیرنظامی (DMZ) ، یکی دیگر از ویژگی های ارائه شده توسط اکثر فایروال ها می باشد . DMZ ، ناحیه ای است که تحت قلمرو حفاظتی فایروال قرار نمی گیرد . فایروال های مختلف ، نواحی DMZ را با روش های متفاوتی پیاده سازی می نمایند . مثلا" برخی از فایروال ها ، صرفا" شما را ملزم به معرفی آدرس IP ماشینی می نمایند که قصد استقرار آن در ناحیه DMZ وجود دارد .برخی از فایروال ها دارای یک پورت شبکه ای اختصاصی می باشند که می توان از آن برای هر نوع دستگاه شبکه ای که قصد استقرار آن در ناحیه DMZ وجود دارد ، استفاده گردد .

پیشنهاد می گردد ، حتی المقدور از نواحی DMZ استفاده نگردد ، چراکه ماشین های موجود در این نواحی از امکانات حفاظتی و امنیتی فایروال استفاده نخواهند کرد و تنها گزینه موجود در این رابطه امکانات ارائه شده توسط سیستم عامل نصب شده بر روی ماشین و سایر توصیه هائی است که با رعایت و بکارگیری آنان ، وضعیت امنیتی سیستم بهتر می گردد .

در صورتی که برای ایجاد یک ناحیه DMZ دلایل موجه و قانع کننده ای وجود دارد ، می بایست با دقت و برنامه ریزی صحیح توام با رعایت مسائل امنیتی اقدام به انجام چنین کاری گردد. در صورتی که ماشین مستقر در ناحیه DMZ دارای یک اتصال به شبکه داخلی نیز باشد ، مهاجمان با تمرکز بر روی ماشین فوق می توانند نقطه مناسبی برای ورود به شبکه را پیدا نمایند . پیشنهاد می گردد به عنوان یک قانون و اصل مهم ، ماشین های موجود در ناحیه DMZ دارای اتصالاتی به غیر از پورت DMZ فایروال نباشند .

فورواردینگ پورت ها

در بخش قبل به نحوه عملکرد فیلترینگ پورت ها به منظور بلاک نمودن استفاده از یک پروتکل بجزء یک آدرس IP خاص، اشاره گردید . فورواردینگ پورت نیز بر اساس همین مفاهیم مطرح و در سازمان هائی که در ارتباط با NAT می باشند ، کارساز خواهد بود .

برای آشنائی با مفهوم فورواردینگ پورت ها ، یک مثال نمونه را بررسی می نمائیم .

فرض کنید ، سازمانی دارای یک سرویس دهنده وب است که از آدرس IP: 192.168.0.12 (یک آدرس معتبر نمی باشد ولی فرض کنید که چنین واقعیتی وجود ندارد) استفاده می نماید و می بایست امکان دستیابی عمومی به آن فراهم گردد . در صورتی که سرویس دهنده وب فوق تنها سرویس دهنده موجود در سازمان است که می بایست امکان دستیابی عمومی به آن فراهم گردد ، می بایست یک قانون فیلترینگ بسته های اطلاعاتی در سطح فایروال تعریف گردد که تمامی درخواست های HTTP بر روی پورت ۸۰ و به مقصد هر آدرس موجود در شبکه بجزء آدرس IP:192.168.0.12 ، بلاک گردد . پس از تعریف قانون فوق ، در صورتی که کاربری یک درخواست HTTP را برای آدرس های دیگری ارسال نماید ، با پیامی مبنی بر این که وب سایت درخواستی وجود ندارد ، مواجه خواهد شد .

در مثال فوق ، این فرض نادرست را کردیم که امکان دستیابی عمومی به آدرس IP:192.168.0.12 وجود دارد . آدرس فوق صرفا" بر روی یک شبکه خصوصی معتبر بوده و امکان دستیابی آن از طریق اینترنت وجود نخواهد داشت . بدیهی است در چنین وضعیتی می بایست آدرس سرویس دهنده وب خصوصی خود را با یک آدرس عمومی جایگزین نمائید . (با این که یک گزینه مطلوب در این رابطه نمی باشد) . برخی از مراکز ارائه دهنده خدمات اینترنت (ISP) ، صرفا" امکان استفاده از یک آدرس IP عمومی را در اختیار شما قرار داده و بدیهی است که در چنین مواردی ما دارای گزینه های متعددی برای اختصاص این آدرس نخواهیم بود و می بایست آن را به فایروال اختصاص داد .

یکی از موارد استفاده سنتی از NAT به مواردی نظیر آنچه اشاره گردید ، بر می گردد . سازمان فرضی دارای صرفا" یک آدرس IP معتبر است و آن را به فایروال نسبت داده و از NAT به منظور تسهیل در مبادله اطلاعات بین ماشین های موجود در شبکه داخلی و اینترنت استفاده می نماید . در چنین مواردی یک مشکل همچنان باقی می ماند . NAT به منظور بلاک نمودن ترافیک تمامی ارتباطات ورودی بجزء آنانی که درخواست آنان از طرف یکی از ماشین های موجود در شبکه داخلی ارسال شده است ، طراحی شده است و ما همچنان دارای یک سرویس دهنده وب می باشیم که می خواهیم امکان دستیابی عمومی به آن را نیز فراهم نمائیم .

به منظور حل مشکل فوق می توان از فورواردینگ پورت استفاده نمود . در واقع فورواردینگ پورت ، قانونی است که به فایروال می گوید در صورتی که درخواست های خاصی بر روی یک پورت خاص برای وی ارسال شده باشد ، می بایست درخواست مربوطه را برای یک ماشین طراحی شده بدین منظور بر روی شبکه داخلی، ارجاع نماید . در مثال اشاره شده ، ما قصد داریم امکان دستیابی عمومی به سرویس دهنده وب را فراهم نمائیم . بدین منظور می بایست یک قانون فورواردینگ پورت بدین منظور تعریف که به فایروال اعلام نماید هر درخواست HTTP بر روی پروتکل TCP و پورت ۸۰ را به آدرس IP:192.168.0.12 تغییر مسیر داده و برای آن ارسال نماید. پس از تعریف قانون فوق ، شخصی که قصد دستیابی به وب سایت سازمان شما را داشته باشد ، پس از فعال نمودن برنامه مرورگر ، اقدام به درج آدرس سایت سازمان شما دربخش مربوطه می نماید. مرورگر کاربر مورد نظر به منظور آگاهی از آدرس domain سایت سازمان شما ، اقدام به ارسال یک درخواست DNS می نماید تا از این طریق نسبت به آدرس IP نسبت داده شده به domain آگاهی لازم را پیدا نماید . بدیهی است آدرسی که پیدا خواهد شد و به عنوان مرجع در اختیار مرورگر قرار خواهد گرفت، همان آدرس IPعمومی است که شما آن را به فایروال نسبت داده اید . مرورگر در ادامه ، درخواست HTTP را برای آدرس IP عمومی شما ارسال می نماید که در حقیقت این درخواست برای فایروال ارسال می گردد . فایروال درخواست را دریافت و آن را برای سرویس دهنده وب ارسال می نماید (فورواردینگ) .

انواع حملات در شبکه های کامپیوتری (بخش اول)

امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری از جمله موضوعاتی است که این روزها در کانون توجه تمامی سازمان ها و موسسات قرار گرفته شده است . در یک شبکه کامپیوتری به منظور ارائه خدمات به کاربران ، سرویس ها و پروتکل های متعددی نصب و پیکربندی می گردد. برخی از سرویس ها دارای استعداد لازم برای انواع حملات بوده و لازم است در مرحله اول و در زمان نصب و پیکربندی آنان ، دقت لازم در خصوص رعایت مسائل ایمنی انجام و در مرحله دوم سعی گردد که از نصب سرویس ها و پروتکل های غیرضروری ، اجتناب گردد . در این مقاله قصد داریم از این زاویه به مقوله امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری پرداخته و در ادامه با انواع حملاتی که امروزه متوجه شبکه های کامپیوتری است ، بیشتر آشنا شویم . قطعا" شناسائی سرویس های غیرضروری و انواع حملاتی که مهاجمان با استفاده از آنان شبکه های کامپیوتری را هدف قرار می دهند ، زمینه برپاسازی و نگهداری شبکه های کامپیوتری ایمن و مطمئن را بهتر فراهم می نماید .

مقدمه

حملات در یک شبکه کامپیوتری حاصل پیوند سه عنصر مهم سرویس ها ی فعال ، پروتکل های استفاده شده و پورت های باز می باشد . یکی از مهمترین وظایف کارشناسان فن آوری اطلاعات ، اطمینان از ایمن بودن شبکه و مقاوم بودن آن در مقابل حملات است (مسئولیتی بسیار خطیر و سنگین) . در زمان ارائه سرویس دهندگان ، مجموعه ای از سرویس ها و پروتکل ها به صورت پیش فرض فعال و تعدادی دیگر نیز غیر فعال شده اند.این موضوع ارتباط مستقیمی با سیاست های یک سیستم عامل و نوع نگرش آنان به مقوله امنیت دارد. در زمان نقد امنیتی سیستم های عامل ، پرداختن به موضوع فوق یکی از محورهائی است که کارشناسان امنیت اطلاعات با حساسیتی بالا آنان را دنبال می نمایند.

اولین مرحله در خصوص ایمن سازی یک محیط شبکه ، تدوین ، پیاده سازی و رعایت یک سیاست امنیتی است که محور اصلی برنامه ریزی در خصوص ایمن سازی شبکه را شامل می شود . هر نوع برنامه ریزی در این رابطه مستلزم توجه به موارد زیر است :

- بررسی نقش هر سرویس دهنده به همراه پیکربندی انجام شده در جهت انجام وظایف مربوطه در شبکه
- انطباق سرویس ها ، پروتکل ها و برنامه های نصب شده با خواسته ها ی یک سازمان
- بررسی تغییرات لازم در خصوص هر یک از سرویس دهندگان فعلی (افزودن و یا حذف سرویس ها و پروتکل های غیرضروری ، تنظیم دقیق امنیتی سرویس ها و پروتکل های فعال) .

تعلل و یا نادیده گرفتن فاز برنامه ریزی می تواند زمینه بروز یک فاجعه عظیم اطلاعاتی را در یک سازمان به دنبال داشته باشد . متاسفانه در اکثر موارد توجه جدی به مقوله برنامه ریزی و تدوین یک سیاست امنیتی نمی گردد . فراموش نکنیم که فن آوری ها به سرعت و به صورت مستمر در حال تغییر بوده و می بایست متناسب با فن آوری های جدید ، تغییرات لازم با هدف افزایش ضریب مقاومت سرویس دهندگان و کاهش نقاط آسیب پذیر آنان با جدیت دنبال شود . نشستن پشت یک سرویس دهنده و پیکربندی آن بدون وجود یک برنامه مدون و مشخص ، امری بسیار خطرناک بوده که بستر لازم برای بسیاری از حملاتی که در آینده اتفاق خواهند افتاد را فراهم می نماید . هر سیستم عامل دارای مجموعه ای از سرویس ها ، پروتکل ها و ابزارهای خاص خود بوده و نمی توان بدون وجود یک برنامه مشخص و پویا به تمامی ابعاد آنان توجه و از پتانسیل های آنان در جهت افزایش کارائی و ایمن سازی شبکه استفاده نمود. پس از تدوین یک برنامه مشخص در ارتباط با سرویس دهندگان ، می بایست در فواصل زمانی خاصی ، برنامه های تدوین یافته مورد بازنگری قرار گرفته و تغییرات لازم در آنان با توجه به شرایط موجود و فن آوری های جدید ارائه شده ، اعمال گردد . فراموش نکنیم که حتی راه حل های انتخاب شده فعلی که دارای عملکردی موفقیت آمیز می باشند ، ممکن است در آینده و با توجه به شرایط پیش آمده قادر به ارائه عملکردی صحیح ، نباشند .

وظیفه یک سرویس دهنده

پس از شناسائی جایگاه و نقش هر سرویس دهنده در شبکه می توان در ارتباط با سرویس ها و پروتکل های مورد نیاز آن به منظور انجام وظایف مربوطه ، تصمیم گیری نمود . برخی از سرویس دهندگان به همراه وظیفه آنان در یک شبکه کامپیوتری به شرح زیر می باشد :

Logon Server : این نوع سرویس دهندگان مسئولیت شناسائی و تائید کاربران در زمان ورود به شبکه را برعهده دارند . سرویس دهندگان فوق می توانند عملیات خود را به عنوان بخشی در کنار سایر سرویس دهندگان نیز انجام دهند .

Network Services Server : این نوع از سرویس دهندگان مسئولیت میزبان نمودن سرویس های مورد نیاز شبکه را برعهده دارند . این سرویس ها عبارتند از :

- DHCP Dynamic Host Configuration (Protocol)
- DNS (Domain Name System)
- WINS Windows Internet Name (Service)
- SNMP (Simple Network Management Protocol)

Application Server : این نوع از سرویس دهندگان مسئولیت میزبان نمودن برنامه ها ی کاربردی نظیر بسته نرم افزاری Accounting و سایر نرم افزارهای مورد نیاز در سازمان را برعهده دارند .

File Server : از این نوع سرویس دهندگان به منظور دستیابی به فایل ها و دایرکتوری ها ی کاربران ، استفاده می گردد .

Print Server : از این نوع سرویس دهندگان به منظور دستیابی به چاپگرهای اشتراک گذاشته شده در شبکه ، استفاده می شود .

Web Server : این نوع سرویس دهندگان مسئولیت میزبان نمودن برنامه های وب و وب سایت های داخلی و یا خارجی را برعهده دارند .

FTP Server : این نوع سرویس دهندگان مسئولیت ذخیره سازی فایل ها برای انجام عملیات Downloading و Uploading را برعهده دارند. سرویس دهندگان فوق می توانند به صورت داخلی و یا خارجی استفاده گردند .

Email Server : این نوع سرویس دهندگان مسئولیت ارائه سرویس پست الکترونیکی را برعهده داشته و می توان از آنان به منظور میزبان نمودن فولدرهای عمومی و برنامه های Gropuware ، نیز استفاده نمود.

News/Usenet (NNTP) Server : این نوع سرویس دهندگان به عنوان یک سرویس دهنده newsgroup بوده و کاربران می توانند اقدام به ارسال و دریافت پیام هائی بر روی آنان نمایند .

به منظور شناسائی سرویس ها و پروتکل های مورد نیاز بر روی هر یک از سرویس دهندگان ، می بایست در ابتدا به این سوال پاسخ داده شود که نحوه دستیابی به هر یک از آنان به چه صورت است ؟ : شبکه داخلی ، شبکه جهانی و یا هر دو مورد . پاسخ به سوال فوق زمینه نصب و پیکربندی سرویس ها و پروتکل های ضروری و حذف و غیر فعال نمودن سرویس ها و پروتکل های غیرضروری در ارتباط با هر یک از سرویس دهندگان موجود در یک شبکه کامپیوتری را فراهم می نماید .

سرویس های حیاتی و موردنیاز

هر سیستم عامل به منظور ارائه خدمات و انجام عملیات مربوطه ، نیازمند استفاده از سرویس های متفاوتی است . در حالت ایده آل ، عملیات نصب و پیکربندی یک سرویس دهنده می بایست صرفا" شامل سرویس ها و پروتکل های ضروری و مورد نیاز به منظور انجام وظایف هر سرویس دهنده باشد. معمولا" تولید کنندگان سیستم های عامل در مستندات مربوطه به این سرویس ها اشاره می نمایند. استفاده از مستندات و پیروی از روش های استاندارد ارائه شده برای پیکربندی و آماده سازی سرویس دهندگان ،زمینه نصب و پیکربندی مطمئن با رعایت مسائل ایمنی را بهتر فراهم می نماید .

زمانی که کامپیوتری در اختیار شما گذاشته می شود ، معمولا" بر روی آن نرم افزارهای متعددی نصب و پیکربندی های خاصی نیز در ارتباط با آن اعمال شده است . یکی از مطمئن ترین روش ها به منظور آگاهی از این موضوع که سیستم فوق انتظارات شما را متناسب با برنامه تدوین شده ، تامین می نماید ، انجام یک نصب Clean با استفاده از سیاست ها و لیست ها ی از قبل مشخص شده است . بدین ترتیب در صورت بروز اشکال می توان به سرعت از این امر آگاهی و هر مشکل را در محدوده خاص خود بررسی و برای آن راه حلی انتخاب نمود. (شعاع عملیات نصب و پیکربندی را به تدریج افزایش دهیم) .

مشخص نمودن پروتکل های مورد نیاز

برخی از مدیران شبکه عادت دارند که پروتکل های غیرضروری را نیز بر روی سیستم نصب نمایند ، یکی از علل این موضوع ، عدم آشنائی دقیق آنان با نقش و عملکرد هریک از پروتکل ها در شبکه بوده و در برخی موارد نیز بر این اعتقاد هستند که شاید این پروتکل ها در آینده مورد نیاز خواهد بود. پروتکل ها همانند سرویس ها ، تا زمانی که به وجود آنان نیاز نمی باشد ، نمی بایست نصب گردند . با بررسی یک محیط شبکه با سوالات متعددی در خصوص پروتکل های مورد نیاز برخورد نموده که پاسخ به آنان امکان شناسائی و نصب پروتکل های مورد نیاز را فراهم نماید .

- به چه نوع پروتکل و یا پروتکل هائی برای ارتباط سرویس گیرندگان (Desktop) با سرویس دهندگان ، نیاز می باشد ؟
- به چه نوع پروتکل و یا پروتکل هائی برای ارتباط سرویس دهنده با سرویس دهنده ، نیاز می باشد ؟
- به چه نوع پروتکل و یا پروتکل هائی برای ارتباط سرویس گیرندگان (Desktop) از راه دور با سرویس دهندگان ، نیاز می باشد ؟

- آیا پروتکل و یا پروتکل های انتخاب شده ما را ملزم به نصب سرویس های اضافه ای می نمایند ؟
- آیا پروتکل های انتخاب شده دارای مسائل امنیتی خاصی بوده که می بایست مورد توجه و بررسی قرار گیرد ؟

در تعداد زیادی از شبکه های کامپیوتری ،از چندین سیستم عامل نظیر ویندوز ، یونیکس و یا لینوکس ، استفاده می گردد . در چنین مواردی می توان از پروتکل TCP/IP به عنوان فصل مشترک بین آنان استفاده نمود. در ادامه می بایست در خصوص فرآیند اختصاص آدرس های IP تصیم گیری نمود (به صورت ایستا و یا پویا و به کمک DHCP) . در صورتی که تصمیم گرفته شود که فرآیند اختصاص آدرس های IP به صورت پویا و به کمک DHCP ، انجام شود، به یک سرویس اضافه و با نام DHCP نیاز خواهیم داشت . با این که استفاده از DHCP مدیریت شبکه را آسانتر می نماید ولی از لحاظ امنیتی دارای درجه پائین تری نسبت به اختصاص ایستای آدرس های IP ، می باشد چراکه کاربران ناشناس و گمنام می توانند پس از اتصال به شبکه ، بلافاصله از منبع صادرکننده آدرس های IP ، یک آدرس IP را دریافت و به عنوان یک سرویس گیرنده در شبکه ایفای وظیفه نمایند. این وضعیت در ارتباط با شبکه های بدون کابل غیرایمن نیز صدق می نماید. مثلا" یک فرد می تواند با استقرار در پارکینگ یک ساختمان و به کمک یک Laptop به شبکه شما با استفاده از یک اتصال بدون کابل ، متصل گردد. پروتکل TCP/IP ، برای "معادل سازی نام به آدرس " از یک سرویس دهنده DNS نیز استفاده می نماید . در شبکه های ترکیبی شامل چندین سیستم عامل نظیر ویندوز و یونیکس و با توجه به این که ویندوز NT 4.0 و یا ۲۰۰۰ شده است ، علاوه بر DNS به سرویس WINS نیز نیاز می باشد . همزمان با انتخاب پروتکل ها و سرویس های مورد نیاز آنان ، می بایست بررسی لازم در خصوص چالش های امنیتی هر یک از آنان نیز بررسی و اطلاعات مربوطه مستند گردند(مستندسازی ، ارج نهادن به زمان خود و دیگران است) . راه حل انتخابی ، می بایست کاهش تهدیدات مرتبط با هر یک از سرویس ها و پروتکل ها را در یک شبکه به دنبال داشته باشد .

مزایای غیرفعال نمودن پروتکل ها و سرویس های غیرضروری

استفاده عملیاتی از یک سرویس دهنده بدون بررسی دقیق سرویس ها ، پروتکل ها و پیکربندی متناظر با هر یک از آنان زمینه بروز تهدیدات و حملات را در یک شبکه به دنبال خواهد داشت . فراموش نکنیم که مهاجمان همواره قربانیان خود را از بین سرویس دهندگانی که به درستی پیکربندی نشده اند ، انتخاب می نمایند. بنابراین می بایست به سرعت در خصوص سرویس هائی که قصد غیرفعال نمودن آنان را داریم ، تصمیم گیری شود . قطعا" نصب سرویس ها و یا پروتکل هائی که قصد استفاده از آنان وجود ندارد ، امری منطقی و قابل قبول نخواهد بود. در صورتی که این نوع از سرویس ها نصب و به درستی پیکربندی نگردند ، مهاجمان می توانند با استفاده از آنان ، آسیب های جدی را متوجه شبکه نمایند . تهدید فوق می تواند از درون شبکه و یا خارج از شبکه متوجه یک شبکه کامپیوتری گردد . بر اساس برخی آمارهای منتشر شده ، اغلب آسیب ها و تهدیدات در شبکه یک سازمان توسط کارکنان کنجکا و و یا ناراضی صورت می پذیرد تا از طریق مهاجمان خارج از شبکه .

بخاطر داشته باشید که ایمن سازی شبکه های کامپیوتری مستلزم اختصاص زمان لازم و کافی برای برنامه ریزی است . سازمان ها و موسسات علاقه مندند به موازات عرضه فن آوری های جدید ، به سرعت از آنان استفاده نموده تا بتوانند از مزایای آنان در جهت اهداف سازمانی خود استفاده نمایند. تعداد و تنوع گزینه های انتخابی در خصوص پیکربندی هر سیستم عامل ، به سرعت رشد می نماید . امروزه وجود توانائی لازم در جهت شناسائی و پیاده سازی سرویس ها و پروتکل های مورد نیاز در یک شبکه خود به یک مهارت ارزشمند تبدیل شده است. بنابراین لازم است کارشناسان فن آوری اطلاعات که مسئولیت شغلی آنان در ارتباط با شبکه و ایمن سازی اطلاعات است ، به صورت مستمر و با اعتقاد به اصل بسیار مهم " اشتراک دانش و تجارب " ، خود را بهنگام نمایند. اعتقاد عملی به اصل فوق ، زمینه کاهش حملات و تهدیدات را در هر شبکه کامپیوتری به دنبال خواهد داشت .

حملات (Attacks)

با توجه به ماهیت ناشناس بودن کاربران شبکه های کامپیوتری ، خصوصا" اینترنت ،امروزه شاهد افزایش حملات بر روی تمامی انواع سرویس دهندگان می باشیم . علت بروز چنین حملاتی می تواند از یک کنجکاوی ساده شروع و تا اهداف مخرب و ویرانگر ادامه یابد.

برای پیشگیری ، شناسائی ، برخورد سریع و توقف حملات ، می بایست در مرحله اول قادر به تشخیص و شناسائی زمان و موقعیت بروز یک تهاجم باشیم . به عبارت دیگر چگونه از بروز یک حمله و یا تهاجم در شبکه خود آگاه می شویم ؟ چگونه با آن برخورد نموده و در سریعترین زمان ممکن آن را متوقف نموده تا میزان صدمات و آسیب به منابع اطلاعاتی سازمان به حداقل مقدار خود برسد ؟ شناسائی نوع حملات و نحوه پیاده سازی یک سیستم حفاظتی مطمئن در مقابل آنان یکی از وظایف مهم کارشناسان امنیت اطلاعات و شبکه های کامپیوتری است .شناخت دشمن و آگاهی از روش های تهاجم وی ، احتمال موفقیت ما را در رویاروئی با آنان افزایش خواهد داد. بنابراین لازم است با انواع حملات و تهاجماتی که تاکنون متوجه شبکه های کامپیوتری شده است ،

بیشتر آشنا شده و از این رهگذر تجاربی ارزشمند را کسب تا در آینده بتوانیم به نحو مطلوب از آنان استفاده نمائیم . جدول زیر برخی از حملات متداول را نشان می دهد :

انواع حملات

Denial of Service (DoS) & Distributed Denial of Service (DDoS)	
Back Door	Spoofing
Man in the Middle	Replay
TCP/IP Hijacking	Weak Keys
Mathematical	Password Guessing
Brute Force	Dictionary
Birthday	Software Exploitation
Malicious Code	Viruses
Virus Hoaxes	Trojan Horses
Logic Bombs	Worms
Social Engineering	Auditing
System Scanning	

پایگاه داده های پیشرفته

تعریف علمی و تئوریکی که از پایگاه داد ها در دنیای نرم افزار ارائه گردیده است عبارت است از : مجموعه ای از داده های بهم مرتبط که طبق یك ساختار مشترك ، تحت کنترل متمرکز و با حداقل افزونگی به صورت اشتراکی و همزمان قابل استفاده باشند .
اما امروز وقتی صحبت از فناوری های نوین در عرصه پایگاه داده ها و نرم افزار های مرتبط با آن به میان می آید، محیطی به مراتب قدرتمند تر و انعطاف پذیر تر از تعریف فوق به ذهن می آید که برای مدیران ، طراحان و برنامه نویسان پایگاه داده ها نوید لذت بخش توسعه و تولید سریع (RAD)محیطهای مبتنی بر بانك های اطلاعاتی را بهمراه دارد .
در سالهای اخیر متولیان و تصمیم گیران بسته های بانك های اطلاعاتی با توجه به شرایط حاکم بر دنیای امروز از قبیل رشد روز افزون داده ها و اطلاعات ، وسعت ، گستردگی حیطه کاربری و ..... استانداردهای متنوع دیگری را برای اینگونه محصولات تدوین نموده اند که در ذیل به برخی از آنها اشاره می گردد .

Platform Independency:

این مقوله مربوط به مفهوم قابلیت نصب و راه اندازی بسته بانك اطلاعاتی بر روی سیستم عامل های مختلف (انعاف پذیری در نصب) است . یك پایگاه داده پیشرفته لزوما وابسته به سیستم عامل خاص و یا احتمالا بستر سخت افزاری ویژه ای نیست و از این طریق قابلیت انعطاف پذیری و اطمینان بالایی را برای کاربران خود فراهم می آورد .

Locking & Concurrency:

برای اطمینان از صحت داده ها و جلوگیری از تاخیرها و انتظارات طولانی در محیط های پر کار پایگاه داده ها ، از این تکنولوژی جهت مدیریت بهینه فرآیندها و داده های بانك اطلاعاتی استفاده می شود .

Long Term Transaction Handling:

در یك محیط پایگاه داده بعضا تراکنش (Transaction) یا تراکنش هایی در سیستم به صورت معلق (Suspend) بوجود می آیند (بدین معنی که پس از ارسال آنها دستور همانند دستور Commit مبنی بر تائید آنها صادر نمی گردد) که این امر باعث بروز ترافیك در صف مربوط به تراکنش ها و توقف نسبی آنها می شود. یك پایگاه داده مناسب باید بتواند این امر را بخوبی کنترل و مدیریت نماید .

Memory Utilization Support:

کنترل در نحوه تخصیص و واکشی حافظه ، تنظیم و به طور کلی مدیریت حافظه دیگر امتیازی است که در یك پایگاه داده پیشرفته

وجود دارد .

Encoding & Decoding Data:

یك پایگاه داده پیشرفته امنیت بالایی برای داده ها و کاربران خود فراهم می آورد . از جمله این موارد می توان به توانایی به رمز در آوردن داده های ذخیره شده در بانك اطلاعاتی اشاره نمود.

Block Level Recovery :

در یك بانك اطلاعاتی پیرشفته ، در صورت بروز خرابی در بانك ، شما مجبور به بازیابی تمام فایل ها (Full Recovery) نیستید . یعنی می توان فقط بلاك های معیوب را بازیابی نمود و فرآیندی را بر روی سایر داده ها انجام نداد .

64 Bit Proccessing:

این واژه به مفهوم پردازش در مدل ٦٤ بیتی است که سرعت و کارآیی بالتری را نسبت به سایر مدل ها بهمراه دارد .

Multimedia & Large Object Support:

مدیریت و کنترل در نحوه خیره و بازیابی داده های بزرگ کاراکتری ، باینری ، صوتی و تصویری در تمامی پایگاه داده های پیشرفته وجود دارد .

Standby Database:

Satandbyیك پشتیبان از پایگاه داده اولیه است که بر روی یك سرور ثانویه قرار می گیرد و تمام تغییرات پایگاه داده با یك تکنولوژی خاص بر روی آن درج می گردد و به صورت Standby در موارد بروز خطا و نارسایی در بانك ، فعال گردیده و مورد استفاده کاربران قرار می گیرد .

Cluster Support:در یك پایگاه داده توزیع یافته (Distributed Database) در صورت سنگین شدن پردازشهای یك سرور و یا ازدیاد تراکنش در طرف یك یا چند سرور خاص ، باید امکان انتقال فرآیندها به سوی سرورهای دیگر وجود داشته باشد . این مهم در پایگاه داده های مدرن امروزی همچون Oracle وجود دارد .

ANSI/SQL 92 Standard Compatible:

رعایت موارد مندرج در استاندارد ANSI / SQL 92از ملزومات و پیش نیازهای یك پایگاه داده پیشرفته است که در آن تمامی موارد مورد لزوم برای بانك های اطلاعاتی امروزی لحاظ گردیده است .

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 که بر پهنای باند ، قیمت و 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 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 محلی می باشندیا فیزیکی شبکه های

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 ۱۹۸۳ موسسه IEEE با استفاده از DIX ، استاندارد IEEE 802.3 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 باشد می انجمن های صنایع الکترونیک و مخابرات(EIA/TIA)

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 repeaterرا 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 starتبدیل 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 Bridgeدر 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 ، Bridgeفریم 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 ، Bridgeآن را به سگمنت مورد نظر فوروارد می نماید.

□در صورتی که آدرس مقصد برای Bridge ناشناخته باشد ، Bridgeفریم 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 RARPرا 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 ۲۵۰۰ از یک کانکتور AUIاستفاده 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 Aمی 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 .

هر آنچه که باید در مورد MP3 PLAYER بدانیم

اشاره :

در اين مقاله خواندني سعي شده است به‌طور كلي معايب و مزاياي يك MP3 Player بررسي شود تا در نهايت با جمع‌بندي خودتان بتوانيد براي خريد يا عدم خريد آن‌ها تصميم بگيريد.

مقدمه:

مي‌توان MP3 Player ها را جزء يكي از بزرگ‌ترين ابداعات صنعت ساخت وسايل پخش موسيقي قابل حمل، به‌حساب آورد. آن‌ها نسبت به مدل‌هاي قديمي‌تر خود مثل واكمن يا CD-Man بسيار كوچك‌تر و نيرومندترند و با قابليت‌هاي بسيار زيادي كه دارند اصلاً با آن‌ها قابل مقايسه نيستند.

دريافت مستقيم فايل موسيقي از اينترنت، اجراي ميكس دلخواه روي آهنگ، ضبط صداي محيط و يا صداي خودتان، گوش كردن به راديو و ضبط همزمان برنامه‌ها يا آهنگ‌هاي راديو، افزايش مقدار حافظه و ... بخشي از امكانات فوق‌العاده‌اي است كه امروزه MP3 Player در اختيار شما گذاشته‌است.

در اين مقاله سعي شده است به‌طور كلي معايب و مزاياي يك MP3 Player معرفي شود تا در نهايت با جمع‌بندي خودتان بتوانيد براي خريد يا عدم خريد آن‌ها تصميم بگيريد.

براي خريد يك MP3 Player بايد فاكتورهاي متعددي را در نظر بگيريد. در اينجا مهمترين آن‌ها در پنج دسته تقسيم‌بندي شده است كه به ترتيب به بررسي آن‌ها مي‌پردازيم.

۱ – خوب يا بد؛ مسئله اين است!

بهتر است قبل از خريد هر چيزي از مزايا و معايب آن به خوبي مطلع شويم تا بعداً دچار مشكل نشويم. به جرأت مي‌توات گفت: بزرگ‌ترين و شايد اصلي‌ترين امتياز MP3 Player نسبت به ساير دستگاه‌هاي پخش موسيقي قابل حمل، ذخيره كردن تعداد زيادي فايل موسيقي دلخواه در فضايي كوچك باشد. به عبارت ديگر شما با استفاده از MP3 Player مي‌توانيد همواره مجموعه‌اي از آهنگ‌هاي دلخواه خود را همراه داشته باشيد و هر وقت كه از يكي از آن‌ها خسته شديد مي‌توانيد به راحتي آن را پاك كنيد و با آهنگي ديگر تعويض كنيد و اين‌كار را بارها بدون افت كيفيت پخش انجام دهيد. اين مزيت، شما را از حمل ده‌ها نوار كاست يا CD به

همراه خود بي‌نياز مي‌كند. ضمناً يادآور مي‌شويم كه روي CDها تنها يك بار مي‌توانيد آهنگ‌هاي دلخواه خود را كپي كنيد و نوار كاست هم بعد از چند بار ضبط، دچار افت كيفيت زيادي مي‌شود، ولي اين اتفاقات در MP3 نخواهد افتاد.

از امكانات ديگر MP3 Player مي‌توان به امكان برنامه‌ريزي پخش اشاره كرد. كساني كه از يك يا دو آهنگ خاص بيشتر لذت مي‌برند مي‌توانند دستگاه را به‌گونه‌اي برنامه‌ريزي كنند كه ابتدا آن چند آهنگ و سپس ساير آهنگ‌ها را پخش كند. تنظيم زمان پخش، طن صدا و حالت پخش (POP، Classic و Rock و ...)، انجام ميكس‌هاي گوناگون، پخش راديو FM و ضبط مستقيم از آن، داشتن ورودي Line-in براي ضبط آهنگ از دستگاه‌هاي پخش ديگر، قابليت ارتقاي حافظه و نمايشگر و ... از ديگر امتيازات يك MP3 Player خوب است كه در هنگام خريد بايد به آن‌ها توجه كنيد.
از بارزترين معايب اين دستگاه‌ها، قيمت بالاي آن‌هاست. اگر براي شما ذخيره يك ساعت موسيقي كافي است، مشكل زيادي در تهيه هزينه آن نخواهيد داشت، اما اگر اصرار داريد كه در هر جا و مكاني، هر موسيقي‌اي را كه دوست داريد، بشنويد، شايد به يك شغل خوب يا يك عموي پولدار احتياج پيدا كنيد!
البته همان‌طور كه گفتيم بعضي از MP3 Player ها مي‌توانند از كارت حافظه نيز پشتيباني كنند كه اگر هم‌اكنون در خريد MP3 Player با حافظه بالا مشكل داريد، مي‌توانيد متناسب با بودجه خود يكي از آن‌ها را تهيه كنيد و بعداً به حافظه آن‌ها اضافه كنيد.

۲ – انواع مختلف، بهاي مختلف

MP3 Player را مي‌توان به سه دسته كلي تقسيم كرد: مدل‌هاي خانگي، شخصي و ماشيني (براي اتومبيل).
MP3 Player خانگي معمولاً ظاهري شبيه DVD دارد و مي‌تواند فايل‌هاي MP3 را از روي CD پخش كنند. با توجه به امكانات متعدد اين نوع از MP3 Player و توجه بر اين نكته كه شما چقدر به استفاده از همه امكانات اصرار داريد، قيمت آن‌ها متغير است و به چند صدهزار تومان هم مي‌رسد.

آن نوع ازMP3 Player كه در اتومبيل‌ها مورد استفاده واقع مي‌شود، درست مثل پخش اتومبيل در جلوي داشبورد قرار مي‌گيرد. انواع ديگري از آن‌ها درست مثل نوع خانگي خود هستند و برخي ديگر به شما اجازه مي‌دهند آهنگ‌هاي MP3 را روي بلندگوهاي اتومبيل بشنويد. (البته امروز با استفاده از دستگاهي جديد به نام Airwave، مي‌توانيد آهنگ‌هاي يك MP3 Player شخصي را روي باندهاي اتومبيل بشنويد). اين نوع MP3 Player ها نسبتا گران هستند.

بالاخره سومين و آخرين نوع آن‌ها كه در اين مقاله قرار است بيشتر درباره آن‌ها بدانيم، انواع شخصي MP3 است كه خيلي كوچك و سبك هستند كه باعث مي‌شود به راحتي در جيب يا دست قابل حمل باشند. قيمت اين محصولات از ۴۰-۵۰ هزار تومان تا ۵۰۰ هزارتومان متغير است. ادامه اين مقاله بر MP3 Player شخصي متمركز است.

۳ – ويژگي‌هاي اصلي

وزن و اندازه: براي بسياري از مردم داشتن وزني سبك، دليل خوبي براي خريد است و خيلي وقتشان را صرف آن مي‌كنند. همچنين اغلب مردم دوست دارند كوچك‌ترين نوع را تهيه كنند.

يك تجربه: اگر دستان بزرگي داريد يا انگشتان شما چاق است، از خريد يكMP3 Player كه كليدهاي ريز و كوچكي دارد، حتماً صرف‌نظر كنيد. زيرا اين ويژگي شما سبب مي‌شود نتوانيد به درستي كليدها را فشار دهيد و بعد فكر مي‌كنيد كه MP3 Player شما خراب است و ... . پس حتماً در هنگام خريد مدلي را تهيه كنيد كه با دستان شما سازگار باشد.

فرمت پخش: هم‌اكنون از بين فايل‌هاي فشرده موسيقي مي‌توان به فايل‌هاي ديگري غير از MP3 نيز اشاره كرد. كه MP3 Player مي‌تواند آن‌ها را پخش كند. مثلاً فرمت WMA متعلق به شركت مايكروسافت است يا Real Network از فرمت G2 يا RM استفاده مي‌كنند كه امروزه گسترش زيادي پيدا كرده‌اند. خيلي ازMP3 Playerها مي‌توانند هر سه فرمت را پخش كنند و بعضي ديگر هيچ فرمت ديگري غير از MP3را تشخيص نمي‌دهند. حتي برخي ديگر مي‌توانند براي پخش فرمت‌هاي آينده (مثل MP4) بروز شوند. اين‌كه MP3 Player شما تنها بتواند فايل‌هاي.MP3 را پخش كند نشانه ضعف آن نيست. چون اصلاً براي پخش آن‌ها ساخته شده است، ولي اگر از فرمت‌هاي ديگر نيز پشتيباني كند، يك امتياز براي شما محسوب خواهد شد.

حافظه و نوع آن: بيشتر MP3 Player از يك حافظه داخلي استفاده مي‌كنند. كه معمولاً بين ۵ تا64 MB متغير است. يك MP3 Player با حافظه ۶۴ MB به طور متوسط مي‌تواند در حدود يك ساعت موسيقي را در خود ذخيره كند. برخي ديگر از MP3 Playerها از كارت‌هاي حافظه استفاده مي‌كنند و برخي ديگر كه به آن‌ها گسترش‌پذير نيز مي‌گويند، از هر دو قابليت بهره‌برداري مي‌نمايند.

كارت‌هاي حافظه نيز انواع مختلفي دارند. مثل:MMC ((Multi Media Card، Smart Media، Compact Flash وMemory Stick (براي محصولات شركت سوني). MP3 Player گران‌تر، از يك هارددیسك استفاده مي‌كنند. البته با اين‌كه در يك هارددیسك مي‌توان صدها هزار فايل موسيقي ذخيره كرد، بايد به قيمت بالاي آن و لزوم احتياط در جابه‌جايي آن (براي پرهيز از ضربه خوردن و صدمه ديدن) نيز توجه كرد.

نوع باتري و عمر آن: معمولاً MP3 Player مي‌توانند از دو نوع باتري استفاده كند. يا يك باتري دروني قابل شارژ يا باتري‌هاي قلمي معمولي (قابل شارژ و غيرقابل شارژ) اگر از MP3 Playerاي كه باتري قلمي مصرف مي‌كنند استفاده مي‌كنيد، بدانيد كه در برخي مدل‌ها بايد نوع باتري خود (قابل شارژ يا غيرقابل شارژ) را انتخاب كنيد و بعد از MP3 Player استفاده كنيد. با اين نوع باتري‌ها تا ۳۵ ساعت (بسته به نوع باتري) مي‌توانيد موسيقي گوش كنيد.
نوع ديگري نيز از MP3 Player باتري‌هاي ليتيم توكار يا NiMH قابل شارژ استفاده مي‌كنند كه با يك شارژر كه در بسته خود MP3 Player است شارژ مي‌شود. اين نوع MP3 Player با هر بار شارژ، ۸ تا ۱۰ ساعت كار مي‌كنند.
روي سايت www.batteries.com مي‌توانيد اطلاعات جامع و كاملي درباره بيش از ۳۵۰۰ مدل باتري NiMH و آلكالاين كه در بيشتر MP3 Playerها از آن‌ها استفاده مي‌شود، به دست مي‌آوريد.

صفحه نمايشگر: MP3 Player شما بايد داراي صفحه نمايش باشد تا گزارش دقيقي از نام آهنگ، وضعيت صدا، و نوع پخش، مقدار باقي مانده شارژ، ترتيب پخش، و ... را به شما ارائه دهد. همچنين بايد حتماً قابليت ديد در شب را نيز داشته باشد تا در تاريكي هم بتوانيد از صفحه نمايش استفاده كنيد.

نقل و انتقال: براي آن‌كه بتوانيد روي MP3 Player خود آهنگ كپي كنيد، بايد آن را به رايانه خود متصل كنيد. بالاترين بازده سرعت در اتصالات:
Firewire (IEEE-1394) يا در USB 2.0 قابل دسترسي است. پس بهتر است MP3 Player شما يكي از اين دو را پشتيباني كند.

نرم‌افزار: معمولاً همراه با MP3 Player يك CD نيز به شما ارائه مي‌شود كه نرم‌افزارهايي متعددي براي استفاده ازMP3 روي آن‌ها وجود دارد، نرم‌افزارهائي كه استفاده از آن‌ها باعث مي‌شود لذت بيشتري در كار با MP3 Player خود ببريد. ضمناً از اينترنت نيز مي‌توانيد نرم‌افزارهاي گوناگوني را دريافت كنيد. براي نمونه به سايت نرم‌افزار Jukebox MusicMatch مراجعه كنيد.

سازگاري: اگر شما بهترين MP3 Player را با بهترين نرم‌افزارها و زيباترين شكل بخريد تا زماني كه با رايانه شما سازگاري نداشته باشد، به هيچ دردي نمي‌خورد. بنابراين مطمئن باشيد كه رايانه شما از لحاظ اتصالات، درگاه‌ها و نصب نرم‌افزارهاي موردنياز، حتماً با MP3 Player انتخابي شما سازگار باشد.

۴ – ويژگي‌هاي پيشرفته

راديو FM: برخي از MP3 Player درون خود يك تيونر راديو هم دارند كه هر زمان كه از شنيدن موسيقي خسته شديد، مي‌توانيد راديو گوش كنيد. مدل‌هاي جديدتر به صورت مستقيم از راديو صدا را ضبط مي‌كنند و معمولاً مي‌توانند ۲۰ تا ۳۰ ايستگاه را در حافظه خود ذخيره كنند. البته در هنگام حركت ممكن است كمي هم صداي خش‌خش بشنويد كه به اين علت است كه تيونر آن‌ها معمولاً خيلي قوي نيست و ضمناً آنتن هم ندارند.

ضبط صدا: با بهره‌گيري از يك ميكروفون صداي داخلي، MP3 Player مي‌توانند با كيفيت قابل قبولي صداي محيط را ضبط كنند. خيلي از آن‌ها تنظيماتي دارند كه قبل ازضبط مي‌توان نوع ديجيتايز شدن آن‌ها (مثلا PCM)، نوع ضبط كانال (Stereo يا Mono) و ... را مشخص كرد.

اعلام مقدار باقي مانده باتري: خوب است بدانيد كه چقدر از باتري مصرف كرده‌ايد و چقدر ديگر موجودي داريد و كي بايد باتري را عوض يا باتري آن را شارژ كنيد.

كنترلرهاي اكولاريزر: اين توانمندي‌ها قابليت‌هايي است كه براساس آن مي‌توان اكولايزر پخش را تغيير داد تا متناسب با نوع آهنگ به كيفيتي بالاتر برسيم.

پخش اتفاقي: براي آن‌كه از پخش ترتيبي موسيقي‌ها خسته نشويد، اين ويژگي آهنگ‌ها را به‌طور اتفاقي پخش مي‌كنند.

ادامه پخش به صورت خودكار: اين ويژگي اين امكان را فراهم مي‌كند كه ادامه‌هاي آهنگ‌هاي خود را از جايي كه قبلاً MP3 Player را خاموش كرده‌ايد، گوش كنيد.

حمل با خيالي آسوده: برخي از شركت‌ها كيف‌هايي را همراه MP3 Player ارائه مي‌دهند كه مي‌توان آن‌ها به كمربند بست و آن را داخل كيف گذاشت. برخي ديگر دستبندي مي‌دهند كه MP3 Player به راحتي در آن قرار مي‌گيرد و با امنيت كامل مي‌توان آن را حمل كرد. برخي ديگر هم بندهاي گردني ارائه مي‌دهند كه مي‌توان را مثل گردنبندي آويزان كرد تا راحت‌تر قابل دسترسي باشند.

ضد آب بودن: بهتر است اين خاصيت هم در MP3 Player وجود داشته باشد تا اگر خواستيد در استخر هم موسيقي گوش كنيد، مانعي نداشته باشيد! :)

۵ – ضمائم

اغلب ابزارهاي موردنياز يك MP3 Player همراه با آن‌ها ارائه مي‌شود، ولي بدانيد حداقل مواردي را كه بايد هنگام خريد به شما ارائه كنند، يك هدفون و يك آداپتور AC و كابل‌هاي اتصال خواهد بود. ساير موارد مثل كنترل از راه دور و كارت حافظه و ... بسته به نوع مدل ارائه خواهد شد.
در آخر هم توجه شما را به اين نكته جلب مي‌كنيم كه قبل از خريد قطعي، از گارانتي آن نيز اطلاع پيدا كنيد. شركت ارائه دهنده گارانتي را بشناسيد و از معتبر بودن آن اطمينان حاصل كنيد. سعي كنيد محصولي را تهيه كنيد كه بالاترين زمان گارانتي را داشته باشند.
روي برگ گارانتي را نيز با دقت بخوانيد و تاريخ شروع آن را، كه معمولاً به ميلادي است، حتماً در نظر بگيريد و مراقب باشيد كه خيلي از زمان آن نگذشته باشد. روي برگ گارانتي، بايد شماره سريال وجود داشته باشد. حتماً آن را با سريال روي دستگاه يا جعبه آن تطبيق دهيد. تا بعداً دچار مشكل نشويد.

نكاتي كه در اينجا مطرح شد، مهمترين مواردي است كه بايد در هنگام خريد MP3 Player به آن‌ها توجه كرد. بايد به خيلي از مسائل توجه نمود، تا بتوان يك پخش‌كننده MP3 خوب و مناسب خريد و از كار با آن لذت برد.

پورتال چیست؟

پورتال چیست؟

نام پورتال ها را زیاد شنیده ایم، اما شاید برای برخی از ما این سئوال پیش آمده باشد که واقعا یک پورتال چیست؟ چه ویژگیها و خصوصیاتی دارد؟ و چه تفاوتی با یک وب سایت دارد؟ ترجمه کلمه Portal به فارسی در فرهنگهای لغت "*دریچه*"، "*درگاه*" و "*مدخل*" ذکر شده اما کلمه پورتال در تکنولوژی اطلاعات معنی متفاوتی دارد. اگر بخواهیم ساده بگوییم، *پورتال صفحه وب واسطی است که امکان دسترسی آسان را به هر چیزی که کاربر ، برای انجام وظیفه یا خواسته اش نیاز دارد – بدون توجه به اینکه محل فیزیکی آن کجاست، فراهم می کند.* به بیان دیگر پورتال *"درگاهی"* است به دنیایی مجازی که کاربر می تواند از طریق امکانات فراهم شده در آن، تمامی نیازهای خود را براورده کند. نیازهایی مانند جستجو و یا خرید(مثلا یک کتاب)، دسترسی به حساب بانکی، افزایش و کاهش اعتبار یک حساب اعتباری و یا به روز رسانی اطلاعات سخت افزاری از محل کار، پورتال همه چیز را از طریق درگاهی واحد برای کاربر خود فراهم می سازد.

ویژگیهای اصلی یک پورتال عبارت اند از:

تجمع اطلاعات

هدف دار بودن اطلاعات

دردسترس بودن اطلاعات

دریچه ورود منحصر به فر

یک پورتال نیز مانند یک کامپیوتر خانگی، اطلاعات و خدمات گوناگونی را در یک صفحه وب واحد و به صورتی سازگار و خوش ترکیب در دسترس می گذارد. گاهی به این صفحه web top هم گفته می شود. پورتال می تواند نقطه شروع یا صفحه اولیه مشخصی داشته باشد که کاربران در زمان اتصال به وب آن را مشاهده کنند. اگر چه بر خلاف صفحه کامپیوتر، پورتال می تواند از طریق مجموعه وسیع دستگاههایی که قابلیت اتصال به وب در آنها پیش بینی شده (از جمله تلفن های موبایل) مورد استفاده قرار گیرد.

هر چند شباهت ظاهری فراوانی میان یک وب سایت و یک پورتال وجود دارد به گونه ای که در نگاه اول تفاوت محسوسی میان آن دو مشاهده نمی شود اما این دو کاملا از یکدیگر متفاوت اند.سوال اینجاست که به طور مشخص تفاوت آن دو در چیست؟ در پاسخ به این سوال باید گفت ویژگیهای زیر در یک پورتال آن را از یک وب سایت متمایز می کند:

۱-درگاه ورود منفردی که از طریق آن می توان به مجموعه منابع مرتبط با پورتال دست یافت.

۲-نمایش هدفدار اطلاعات با استفاده از تجربیات کاربر.

۳-دسترسی تقسیم بندی شده به انواع داده و اطلاعات گروه بندی شده.

۴-در اختیار گذاشتن امکان ارتباط و همکاری میان تمامی کاربران و استفاده کنندگان پورتال.

۵-امکان پیوستن به نرم افزارها و سیستم های نرم افزاری که گردش کاری مشخص و تعریف شده ای دارند.

تاریخچه خلاصه پورتال

اگر در دنیای کامپیوتر به عقب بازگردیم، زمانی را خواهیم یافت که در آن سیستم های نرم افزاری به گونه ای متحول شدند که دیگر لازم نبود برای کار با یک برنامه، برنامه های دیگر بسته شوند، یعنی می توانستیم همزمان از چند برنامه کاربردی استفاده کنیم بدون آنکه با مشکلی مواجه شویم.امکانی که قبل از آن وجود نداشت. تاریخچه پورتال ها از همان زمان آغاز شد و نسلهای تکامل یافته آنها یکی پس از دیگری پا به عرصه دنیای اطلاعات گذاشتند.

نسل اول پورتال ها :

اولین پورتال ها، که از آنها تحت عنوان نسل اول نام برده می شود، بر فراهم نمودن محتویات ایستا، مستندات و همچنین خوراکهای اطلاعاتی زنده در صفحات وب مبتنی بودند. مثالهای نمونه این نسل سایت های yahoo یا Excite است. این پورتالها در محیطی به هم پیوسته، اهداف مشابهی را دنبال کرده و صفحه واسط مشخص و منحصر به فردی را برای دستیابی به مجموعه اطلاعات توزیع شده در سراسر شرکت یا سازمان خود، در اختیار کاربر می گذاشتند. این اطلاعات معمولا شامل اخبار شرکت، شرایط و فرم های استخدام، اطلاعاتی مربوط به کارکنان و چگونگی ارتباط با آنها، مستندات رسمی و سیاست های اعلام شده شرکت و همچنین لینک های ارتباطی مفید بود.

نسل دوم پورتال ها :

نسل دوم پورتال ها بر اطلاعات مشخص تر و نرم افزارها متمرکز بودند. در اساس شباهت زیادی به خصوص در زمینه فراهم آوردن اطلاعات با نسل اول داشتند با این همه تفاوت مهمی نیز وجود داشت: این پورتالهای امکان همکاری کاربران را در محیطی به هم پیوسته فراهم می کردند و همین امکان، نقطه تمایز آنها با نسل پیشین محسوب می شد.

پورتال های نسل دوم قابلیت همکاری متقابل را در ادارات مجازی برای تیم های کاری و به منظور انجام وظایفشان فراهم می ساختند. نسل دوم پورتال ها سرویس های متعددی داشتند که از جمله آنها می توان به سرویس های مدیریت محتوی (سازمان دهی و مدیریت اطلاعات مرتبط) و سرویس های همکاری (که به کاربران امکان می داد با یکدیگر گپ زده و برای یکدیگر ایمیل فرستاده و قرار ملاقات تنظیم کنند) اشاره کرد. در این پورتال ها قابلیت تعریف گروه های کاربری نیزفراهم آمده بود. به بیان دیگر این پورتال ها سازو کار همکاری داخلی را در یک سازمان فراهم می ساختند.

نسل سوم پورتال ها :

نسل سوم با هدف ایجاد فضای مجازی تجارت الکترونیک (E-Business) بوجود آمد. پورتال های نسل سوم به عنوان واسط ارتباطی کارمندان، تهیه کنندگان، تولید کنندگان و مشتریان قلمداد می شوند. ویژگی فوق العاده این پورتالها امکان مرتبط شدن نرم افزارهای مستقر در سرورهای مختلف است. به بیان دیگر، این پورتال ها نقطه به هم پیوستن محتویات و برنامه های کاربردی مستقر در

سرورهای مختلف بطور همزمان و با استفاده از همکاری سرویسهای خدماتی آنان اند. به علاوه امکان دسترسی به محتویات و امکانات سیستمهای مختلف را از طریق ابزارها و تجهیزات متنوع، بسته به نیاز کاربر امکان پذیر می کنند. این گروه پورتال ها مجموعه قابل توجه و ارزشمندی از اطلاعات، مستندات، امکانات و قابلیتهای نرم افزارهای مرتبط را از طریق درگاه واحدی برای کاربر فراهم می کنند.

به علاوه، این پورتالها به صورتی خودکار و بر اساس نقش کاربران هدفمند شده و ویژگیهایی خاص آنها می یابند. به بیان دیگر، نحوه نمایش، محتوی و امکانات در دسترس، بسته به نقش تعریف شده برای کاربر به گونه ای منحصر به فرد و خاص وی در اختیار او قرار می گیرد. کلید توسعه آینده این نسل از پورتال ها،ایجاد چهارچوب های کاری باز (از قبل تعریف نشده) برای سرویس های عمومی خواهد بود.

انواع پورتال ها

یک سازمان مجموعه متنوعی از کاربران دارد که از جمله آنها می توان به مشتریان، شرکا، کارمندان اشاره کرد. همه این کاربران علاقه مندند از اطلاعات و خدمات آن سازمان استفاده کنند. کاملا آشکار است که هر کدام از آنها نیازهای خاص و اغلب متفاوتی دارد. برای پاسخگویی به این تنوع، انواع مختلف پورتال ایجاد شده و مورد استفاده قرار می گیرد. به طور کلی بر حسب چگونگی پاسخگویی به نیازهای کاربران، پورتال ها را می توان در چهار گروه زیر دسته بندی کرد:

Business to Customer Portal (B2C)

این نوع از پورتال با سیستمهای CRM ۱[1] مرتبط بوده و دسترسی مستقیم مصرف کننده را به مجموعه وسیعی از اطلاعات و خدمات فراهم می کند – برای مثال، اطلاعاتی مانند "راهنمای استفاده از محصولات" و "وضعیت سفارش مشتری " در خرید های خود و همچنین امکانات ارتباطی کاربر با بخش پشتیبانی مشتریان در این پورتال ها پیش بینی می شود. مانند هر پورتال دیگری، یک پورتال B2C معمولا در قد و قواره ای ارائه می شود که نیازهای مشتریان خود را پاسخ دهد.

Business to Business Portal (B2B)

نوع دیگر پورتال در زنجیره مدیریت منابع شکل می یابد۲[2]. در این نوع پورتال اطلاعات لازم برای تولید کنندگان،تهیه کنندگان، نمایندگی ها و همچنین توزیع کنندگان، به گونه ای مناسب و دسته بندی شده جمع آوری و در اختیار آنان قرار می گیرد. نمونه عمومی پورتال B2B - برای مثال، یک شریک تجاری را قادر می کند تا به بخشهایی از اطلاعات و امکانات مانند سفارش خرید و صدور فاکتور دسترسی داشته و از امکانات این بخشها استفاده کند. به هم پیوستن برنامه های کاربردی یکی از پیشنیازهای لازم برای یکپارچه سازی محیط های تجاری در بستری واحد و ایجاد محیط مجازی لازم برای کسب و کار است. محیطی که در آن امکان تهیه کالا یا خدمات، صدور صورت حساب خرید و فروش، دسترسی به اطلاعات تولید و دیگر امکانات مرتبط با نیازها فراهم می اید.

B2E

این پورتال ها که اغلب با عنوان پورتال های اینترانتی شناخته می شوند معمولا به منظور تجمیع، انتشار و به اشتراک گذاری اطلاعات و خدمات به پرسنل یک سازمان ایجاد می شوند. B2E ها به دو دسته اصلی تقسیم می شوند:

- پورتالهای کارکنان که امکان دسترسی به محتویات به هم پیوسته ای مانند اخبار شرکت، اطلاعات سخت افزاری و نرم افزاری، موتور جستجو و منابع فنی و گزارشها را در اختیار می گذارد. اطلاعات این نوع پورتال معمولا در دسترس همه کارکنان یک سازمان قرار می گیرد. این پورتال کارکنان و شاغلین یک سازمان را قادر می کند تا از طریق گپ و گروههای گفتگو با یکدیگر در تماس بوده و با یکدیگر همکاری کنند. عموما، این پورتال ها امکاناتی نظیر ثبت نام در یک کلاس و یا یک اردو را نیز در اختیار کاربر خود قرار می دهند. به علاوه کاربران این پورتال معمولا می توانند اطلاعات شخصی خود مانند نام و کلمه عبور را تغییر دهند.
- Knowledge worker portal که با یک یا مجموعه اهداف مشخص مثلا فروش یک محصول ایجاد می گردد. این پورتال ها مجموعه ای از محتویات را به منظور پشتیبانی از فرآیند یا فرآیندهای مشخصی در اختیار می گذارند. برای مثال یک برنامه تکنسین خودکار ممکن است نیازمند منابعی از برنامه های کاربردی دیگر مثلا برنامه های تعمیر و نگهداری باشد تا بتواند اطلاعات لازم در زمینه تاریخچه بازبینی و تعمیر، زمان بندی تجهیز و یا قطعات و لوازم مورد نیاز برای تعمیر آن را کسب کند.

پورتال های عمومی (Mega Or Public Portal)

این پورتال ها با عنوان پورتال های اینترنتی شناخته می شوند و مهمترین ویژگی آنها فراوانی مخاطبانشان است. این نوع از پورتال ها نیز در دو گروه دسته بندی می شوند:

پورتال های عمومی که تمامی کاربران اینترنت را مخاطب قرار می دهند (برای مثال Yahoo، Excite، Google و مانند آن)

پورتال های خاص (صنعتی، بازرگانی، خدماتی) که به آنها پورتال های عمودی نیز گفته شده و مخاطبان محدود و مشخصی دارند (مانند پورتال های بانکها، سازمانهای دولتی، وزارتخانه ها و ...)

باید توجه داشت که یک پورتال می تواند از پیوند انواع پورتال های دیگر ایجاد شود. به علاوه همانطور که یک سازمان کاربران متنوعی دارد، می تواند (و گاهی نیز لازم است) که پورتال های مختلفی برای پشتیبانی از نیازهای آنان داشته باشد.

جنبه های کارکردی یک پورتال

اگر چه پورتال ها در انواع و اندازه های متنوعی ساخته می شوند اما ویژگیهای محدود و مشخصی هسته اصلی آنها شناخته می شود:

- هر پورتال اطلاعات و خدمات را یکجا و در یک محل جمع آوری می کند.
- هر پورتال می تواند در اندازه لازم برای شخص و یا گروه سازمان دراید.
- هر پورتال در هر زمان و از هر مکانی قابل دسترس است.

یک پورتال مجموعه اطلاعات و خدمات را یکجا و در یک محل جمع آوری می کند

هدف اصلی فراهم آوردن امکان دسترسی آسان به هرچیزی (اطلاعات و خدمات) است که یک کاربر برای انجام وظایف و مسئولیتهایش به آن احتیاج دارد، صرف نظر از اینکه منبع آن کجا باشد.

اطلاعاتی که یک پورتال فراهم می کند

- **داده های ساخت یافته**. داده هایی که به صورتی سازمان یافته اند که امکان جستجوی آسان آنها وجود داشته باشد (اغلب به صورت سلسله مراتب و بر اساس کلمات کلیدی). فهرست الفبایی کتابهای یک کتابخانه مثال خوبی از داده های ساخت یافته است. داده های ساخت یافته اغلب شامل، گزارشها، تحلیلها، پرس و جوهای مشخص و دیگر انواع دانش مرتبط با کسب و کار است.
- **داده های بدو ن ساختار**، که جستجو در آنها معمولا دشوار بوده و خارج از یک بانک اطلاعاتی قرار دارند. از این نوع داده می توان متن ها، صوت، تصویر و یا گرافیک و اشکالی مانند مستندات Office ، memos ، ایمیل، قرارهای ملاقات را مثال زد.
- **اطلاعات خاص** ۳ [3]،که شامل محتویات قابل خرید و فروش (مثل انواع اخبار، گزارشها، اطلاعات مربوط به سهام، کاریکاتورها و محتویات بی اهمیت) بوده و مخصوصا به منظور استفاده در فرایندهای تولیدی دیگر تهیه و در اختیار قرار می گیرند.

خدماتی که به وسیله یک پورتال فراهم می شود

- **همکاری**، (با عنوان خدمات ارتباطی نیز شناخته می شود) و به کاربران اجازه می دهد تا با یکدیگر گپ بزنند، در بحثهای گروهی مشارکت داشته باشند، مطالب خود را در اختیار دیگران قرار دهند و...

  مدیریت محتوی که انواع جستجو ها، رهگیریها را مدیریت کرده و همچنین قابلیتهای خاصی را به منظور استخراج داده ها در اختیار می گذارد.
- **خدمات شخصی** (با عنوان خدمات تراکنشی نیز نام برده می شود) که کاربران را قادر می سازد تا با دیگر سیستمها (مثلا سیستمهای فروشنده و یا نماینده یک محصول) مستقیم و بدون واسطه مرتبط باشند. معمولا این قابلیت به کاربر امکان می دهد تا برای مثال فعالیتهای زیر را انجام دهد:
  - محصولات یک سازمان را خریداری کند
  - ملاقاتهای خود را زمان بندی کند
  - حساب خود را مشاهده یا تراز کند
  - در کلاس مورد علاقه خود ثبت نام کند

هر پورتال می تواند در اندازه لازم برای شخص و یا گروه سازمان دراید.

یکی از ویژگیهای جالب یک پورتال شکل و عملکرد متفاوت آن برای اشخاص مختلف است. یکی از روشهایی که به این منظور استفاده می شود، متناسب سازی و تغییر شکل و قابلیتهای پورتال بر حسب خواسته ها یا تجارب شخص یا گروه استفاده کننده از آن است. به همین دلیل است که کاربران متفاوت شکل متفاوتی از یک پورتال مشاهده کرده و اطلاعات و خدمات متفاوتی در اختیار ایشان قرار می گیرد:

@امکان تغییر بر حسب خواسته ها بر حسب تجارب شخص یا گروه عموما personalize نامیده می شود و به این معنی است که در پورتال امکان انتخاب نحوه نمایش محتوی پیش بینی شده است. اغلب این انتخاب بصورت خودکار و بر اساس نقش کاربر (مثلا پست سازمانی وی) انجام می شود. برای مثال وقتی کارمند فروش به سیستم وارد می شود، به صورت خودکار فهرستی از جدیدترین محصولات برای وی به نمایش در می آید. با این همه در بعضی از پورتال ها انتخاب محتوی نمایش داده شده به کاربر محول می شود تا در زمان ورود به پورتال خود آن را انتخاب کند.

@تغییر و Customize شدن یک پورتال شامل انتخاب چگونگی شکل ظاهری آن (مثلا رنگ و چیدمان صفحه)،مدل مرورگر و محل نمایش محتویات روی صفحه است. یک پورتال می تواند حتی برچسب و عنوان تجاری مشخصی داشته و ظاهر متفاوتی را برای انواع کاربرانش به نمایش گذارد.

این دو ویژگی به پورتال امکان می دهد تا مجموعه مشخص و تعریف شده ای از کاربران (مثلا مشتریان، شرکا و یا کارکنان) را هدف قرار دهد. بعضی از پورتال ها حتی می توانند برای هر کاربر مشخص، شکل و شمایل متفاوتی از خود نشان دهند.

یک پورتال در هر زمان و از هرمکانی همیشه در دسترس است

از آنجا که پورتال ها برای استفاده در محیط وب ساخته می شوند، در هر زمان و از هر مکانی با استفاده از یک مرورگر استاندارد وب در دسترس اند. انواع تجهیزات مبتنی بر وب نیز از جمله تلفنهای موبایل، دسترسی به پورتال ها را به غایت آسان و مفید کرده اند.

اشاره :

شبکه‌اي کاربران خواهان دسترسي و استفاده از سرويس‌هايي شبکه‌اي را با تعدادي کلاينت و چندين سرور در نظر بگيريد. در چنين انتظار تبادل و سرور را در نظر بگيريد که کاربران FTP سطح شبکه فراهم شده است. به عنوان مثال يك هستند که توسط سرورها در که هويت کاربران براي سرور شناخته شود و درخواست‌هايي که دريافت فايل از آن را دارند. غالباً در چنين محيط‌هايي نياز داريم اينترنت يك سرور ارسال مي‌شود توسط آن سرور اعتبارسنجي شوند، ضمناً در شبکه‌هاي بزرگ مانند جهت استفاده از سرويس‌هاي مي‌بايستي هويت کاربري که به سيستم کلاينت لازم است که سرور نيز هويت خود را براي کلاينت اثبات کند. توجه کنيد که که هويت خود سيستم کلاينت را نشان (IP پارامترهايي (به عنوان مثال آدرس درخواستي را ارسال کرده شناخته شود و به متعددي به وجود آمدند که پروتکل نمي‌توانيم اعتماد کنيم. براي رفع چنين مشکلاتي، مکانيزم‌ها يا پروتکل‌هاي امنيتي مي‌دهند .کربروس يکي از آن‌ها مي‌باشد

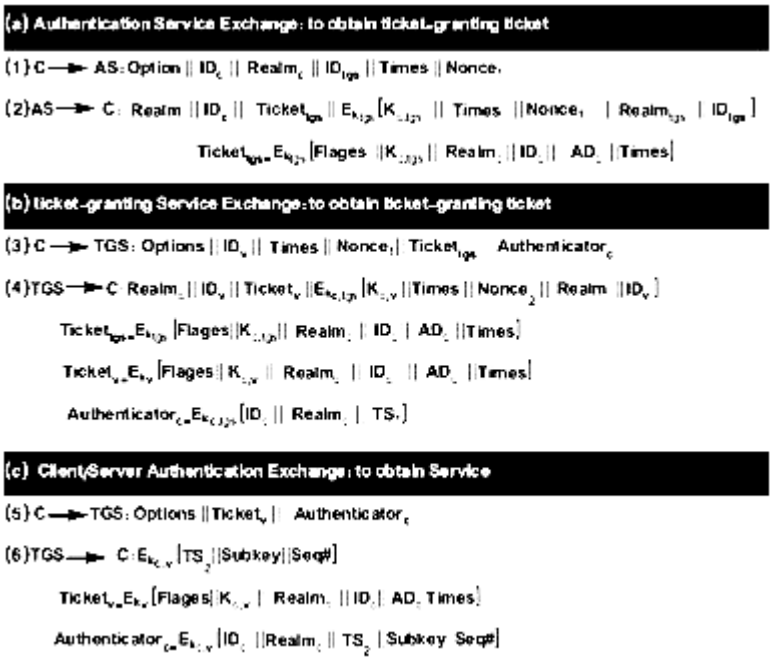
همان‌گونه که در قسمت قبلي اين مقاله در شماره ۴۶ اشاره شد، براي برقراري امنيت در شبکه‌ها چندين پروتکل امنيتي ساخته شده‌اند که يکي از آن‌ها کربروس مي‌باشد. در قسمت اول با مفاهيم اوليه پروتکل تشخيص هويت و نحوه کارکرد کربروس آشنا شديد و نسخه ۴ اين پروتکل مورد بررسي قرار گرفت. در اين قسمت نسخه‌هاي جديدتر کربروس را به تفضيل بررسي مي‌کنيم.

نسخه ۵ کربروس

در نسخه ۵ بیشتر مشکلات نسخه‌هاي قبلي حل شده است به طوري که الگوريتم رمز مورد استفاده و پروتکل آدرس‌دهي لايه شبکه با استفاده از Flagهايي در پيام‌ها مشخص مي‌شوند و لذا به راحتي قابل تغييرند. طول عمر بليط هم به صورت صريح به شکل زمان تولد و مرگ بليط در پيام‌ها بيان مي‌شود. البته غير از رفع مشکلات نسخه ۴، قابليت‌هاي خاصي نيز در اين نسخه اضافه شده است. گفت‌وگوي کربروس نسخه ۵ به صورت جدول ۲ مي‌باشد.

همان‌طور که مشاهده مي‌کنيد باز هم گفت‌وگوها در سه مرحله انجام مي‌شود و هدف گفت‌وگوهاي هر مرحله هم همان است که در نسخه ۴ گفته شد. فقط داده‌هاي خاصي در پيام‌ها اضافه شده که اين داده‌ها به شرح زير هستند:

Times: کلاينت، اين داده را ارسال مي‌کند تا درخواست کند که از خصوصيات زماني خاصي (time setting) توسط سرور استفاده شود (مثلاً زمان شروع و فرمت زمان)



Nonce: در دو پيام اول و سوم، کلاينت يک مقدار تصادفي به نام Nonce را توليد کرده و به سرور تشخيص هويت در پيام اول و به TGS در پيام دوم ارسال مي‌کند و سپس انتظار دارد که در پاسخ‌هايي که دريافت مي‌کند همان Nonce قرار داده شده باشد، البته به صورت رمز شده. به اين ترتيب گام ديگري جهت جلوگيري از حمله تکرار و اطمينان از تازه بودن داده‌هاي دريافتي بر مي‌دارد.

Options: در اين داده، کلاينت درخواست مي‌کند که بليط ويژگي‌هاي خاصي را داشته باشد.

Flags: ويژگي‌هاي خواسته شده در داده Options توسط کلاينت، در فيلد Flag بليط نگهداري مي‌شود. به عبارت ديگر flags خصوصيات و حالات خاصي را که يک بليط مي‌تواند داشته باشد نشان مي‌دهد. به عنوان مثال يکي از مقاديري که flags مي‌تواند داشته باشد RENEWABLE است. بليطي که در فيلد flags آن، اين قابليت set شده باشد يعني TGS، در صورتي که عمر بليط تمام شود مي‌تواند با دادن اين بليط به AS بليط جديدي را دريافت کند و کلاينت درگير دريافت بليط مجدد ازAS ، نشود. توجه کنيد که در غير اين‌صورت لازم است کلاينت، مرحله اول گفت‌وگوي کربروس را انجام دهد و بليط ديگري را دريافت کند.

Subkey: کليد ديگري مي‌باشد که کلاينت انتخاب کرده و در هر نشست به سرور ارسال مي‌کند تا ارتباطات اين نشست با اين کليد رمز شود. البته اين فيلد اختياري است و در صورتي که کلاينت آن را ارسال نکند، از همان کليد به اشتراک گذاشته شده در پيام ۳ و ۴ يعني kc,v استفاده مي‌شود.

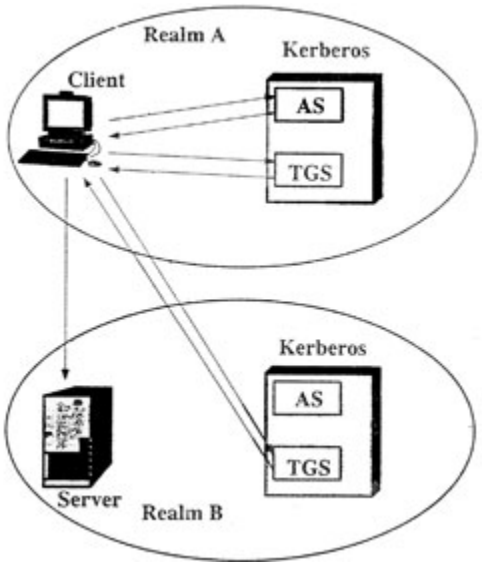
Seq: شماره ترتيب پکت‌ها مي‌باشد. کلاينت درAuthenticator شماره آغازي را به سرور ارسال مي‌کند و سرور در هر بسته‌اي که به کلاينت ارسال مي‌کند يک رقم به اين شماره اضافه مي‌کند. استفاده از اين فيلد جهت اطمينان از اصالت پيام‌ها مي‌باشد. به اين صورت که در هر بسته مي‌بايستي يک واحد به seq اضافه شده باشد و در صورتي که seq مقدار مورد انتظار را نداشته باشد کلاينت آن را بسته معتبر نمي‌داند.

Realm: به مجموعه يک AS و TGS و سرورهاي مربوطه و کلاينت‌هايي که از AS استفاده مي‌کنند يک قلمرو کربروس

(realm kerberos) مي‌گويند. در پيام اول، كلاينت در داده Realmc مشخص مي‌كند كه TGS موردنظر او در چه قلمرويي قرار دارد. در بليط‌ها، Realm مشخص كننده قلمرويي است كه بليط در آن اعتبار دارد. در داخل Authenticator هم كلاينت مشخص مي‌كند كه خود او جزء كدام قلمرو است.

براي درك بيشتر به شكل ۱ توجه كنيد كه در آن كلاينت موجود در قلمرو A مي‌خواهد از سروري در قلمرو B استفاده كند. لذا از TGS مربوط به قلمرو خود (A) درخواست بليط استفاده از TGS قلمرو B را مي‌كند و سپس از TGS قلمرو B بليط استفاده از سرور را مي‌گيرد.

همان‌طور كه قبلاً نيز اشاره شد، طراحان كربروس اين پروتكل را براي محيط خاصي طراحي نكرده‌اند و لذا اين پروتكل توسط شركت‌هاي مختلف به صورت‌هاي گوناگوني پياده‌سازي شده است. آنچه كه تا اين‌جا شرح داده شد استاندارد اصلي كربروس (RFC 1510) بود، در ادامه چگونگي پياده‌سازي كربروس در ويندوز ۲۰۰۰ را بررسي مي‌كنيم.



كربروس در ويندوز ۲۰۰۰

يكي از مفاهيمي كه در دنياي امنيت مطرح مي‌شود اين است كه زير ساخت‌هاي امنيتي تا جايي كه امكان دارد از ديد كاربر نهايي پنهان يا شفاف (transparent) باشد. به عبارت ديگر، كاربر نهايي جز در مواقع لزوم، درگير مسايل امنيتي شبكه نشود (درگير نشدن كاربر نهايي با مسايل امنيتي امتياز بزرگي است ولي متأسفانه در اغلب موارد برنامه‌نويسان (developers) هم به صورت كاربر نهايي با مسايل امنيتي برخورد مي‌كنند و هم در سطح حرفه‌اي از (۱) SSPI استفاده مي‌كنند حال اين‌كه SSPI واسطي است براي درگير نشدن با جزييات زيرساخت‌هاي امنيتي!) مايكروسافت اين امر را در سيستم‌هاي خود كاملاً رعايت كرده است به طوري كه شايد تعجب كنيد اگر بشنويد كه وقتي يك Domain ويندوز ۲۰۰۰ راه‌اندازي مي‌كنيد در واقع يك قلمرو كربروس هم ايجاد كرده‌ايد كه شامل Controller Domain و كلاينت‌هاي متصل به آن مي‌باشد، به عبارت ديگر Domain و قلمرو كربروس به يك مفهوم مي‌باشند و در دنياي مايكروسافت به قلمرو كربروس نام Domain اطلاق مي‌شود. در يك قلمرو كربروس، دو سرور وجود داشتند كه يكي سرور تشخيص هويت (AS) و ديگري سرور اعطاكننده بليط (LTGS) بود. مايكروسافت اين دو سرور را در يك سرور قرار داده كه همان Domain Controller شبكه است. يعني Domain Controller وظيفه تشخيص هويت و صدور بليط TGT (مانند AS) و نيز صدور بليط براي استفاده از سرورهاي موجود در شبكه (مانند TGS) را به عهده دارد. اگر تاكنون به ساختار ويندوز ۲۰۰۰ توجه كرده باشيد متوجه شده‌ايد كه زيرساخت و سرويس‌هاي امنيتي ويندوز۲۰۰۰ در نقطه خاصي از ساختار سيستم‌عامل قرار ندارد و در كل ساختار اين سيستم‌عامل پراكنده شده‌اند كه كربروس هم از اين قاعده مستثني نيست. لذا درك چگونگي كاركرد كربروس شايد كمي پيچيده به نظر برسد. در ادامه به صورت جزيي‌تر ساختار كربروس در ويندوز ۲۰۰۰ را بررسي مي‌كنيم.

در كلاينت‌هايي كه عضو Domain ويندوز۲۰۰۰ هستند كتابخانه‌اي به نام Kerberos.dll وجود دارد كه دو مجموعه از توابع را ارايه مي‌كند:

۱- توابع لازم جهت ساختن پيام‌هايي كه سيستم كلاينت در پروتكل كربروس ارسال مي‌كند استفاده مي‌شود.

۲- توابعي كه پاسخ‌هاي سرور را گرفته و اصالت پاسخ را بررسي كرده و نيز قسمت‌هاي لازم مانند بليط را از پاسخ دريافتي جدا مي‌كنند.

(كتابخانه‌ها يا dllها، برنامه‌هايي هستند كه مانند ساير برنامه‌ها نوشته مي‌شوند ولي معمولاً داراي فرم و ديالوگ نيستند و خودشان به تنهايي كاري انجام نمي‌دهند، بلكه لازم است برنامه ديگري نوشته شود كه از توابع داخل اين كتابخانه‌ها استفاده كند). با استفاده از اين كتابخانه سيستم كلاينت وقتي مي‌خواهد پيام اولي را كه در ساختار پروتكل كربروس توضيح داده شد ارسال كند، يكي از توابع كتابخانه kerberos.dll را فراخواني مي‌كند و اطلاعات لازم براي ساختن پيام اول را (نام DC، نام كاربر، كلمه عبور، nonce) در اختيار اين تابع قرار مي‌دهد و اين تابع پيام را ساخته و به كلاينت مي‌دهد تا به سمت سرور ارسال كند. همچنين هنگام دريافت پاسخ سرور، بسته پاسخ را در اختيار يكي ديگر از توابع اين كتابخانه قرار مي‌دهد تا صحت بسته دريافتي را كنترل كند و بليط را از بقيه داده‌ها جدا كند. كتابخانه‌اي هم با نام kdcsvs.dll Kerberos key (distribution Center service) روي سرور وجود دارد كه

كاري مشابه Kerberos.dll به عهده دارد با اين تفاوت كه توابع لازم جهت دريافت بسته‌هاي ارسالي از كلاينت و بررسي اصالت بسته و ساختن پاسخ مناسب در جواب به درخواست كلاينت را در خود دارد.
همان‌طور كه گفته شد، كتابخانه‌ها به تنهايي قابل استفاده نيستند و لازم است برنامه ديگري از توابع كتابخانه استفاده كند. كتابخانه‌هاي سمت سرور و كلاينت كربروس نيز توسط برنامه ديگري فراخواني شده و مورد استفاده قرار مي‌گيرند. برنامه‌اي كه از كتابخانه‌ها استفاده مي‌كند خود يك برنامه دو بخشي است. (فرض كنيد دو فايل .exe كه از توابع همديگر استفاده مي‌كنند) يك بخش از اين برنامه srm Security (reference monitor) نام دارد كه جزء قسمت Executive ويندوز ۲۰۰۰ است (قسمت Executive ويندوز ۲۰۰۰ شامل برنامه‌ها و ماژول‌هاي سيستمي است كه داراي حقوق ويژه‌اي جهت دسترسي به تمام منابع سخت‌افزاري و نرم‌افزاري سيستم مي‌باشند) قسمت دوم اين برنامه lsass.exe (local security authority subsystem) نام دارد كه جزء قسمت Usermode ويندوز ۲۰۰۰ مي‌باشد كه با حق دسترسي كمتري نسبت به srm اجرا مي‌شود و شما مي‌توانيد آن را در task manager مشاهده كنيد. توجه داشته باشيد كه srm و lsass فقط جهت پياده‌سازي پروتكل كربروس در ويندوز ۲۰۰۰ قرار نگرفته‌اند بلكه اين دو برنامه لايه‌اي را فراهم مي‌كنند كه ويندوز۲۰۰۰ بتواند بدون هيچ‌گونه تنظيمات اضافي، در صورتي كه لازم باشد از پروتكل‌هاي ديگري (كتابخانه‌هاي امنيتي ديگري كه در سيستم وجود دارد) جهت تشخيص هويت استفاده كند. LSASS داراي دو سرويس با نام‌هاي winlogon و netlogon است كه توسط آن‌ها اطلاعات هويتي كاربر را مي‌گيرد. WINLOGON سرويسي است كه فرم welcome و پس از فشردن Alt+Ctrl+Del فرم درخواست نام كاربري و كلمه عبور و نام Domain را نشان مي‌دهد.

حال كه ساختار كلي كربروس را متوجه شديد قدم به قدم سناريويي كه ويندوز ۲۰۰۰ در هر بار ورود به Domain اجرا مي‌كند را دنبال مي‌كنيم:

- winlogon پس از دريافت Alt+Ctrl+Del فرم ورود به ويندوز (Domain) را نشان مي‌دهد.

- نام كاربري، كلمه عبور، نام Domain را وارد مي‌كنيد و دكمه OK را كليك مي‌كنيد.

- winlogon اطلاعات وارد شده توسط شما را گرفته و به lsass مي‌دهد. LSASS با استفاده از توابع موجود در كتابخانه kerberos.dll كلمه عبور وارد شده را با توابع درهم‌سازي (MD ۵) از حالت عادي خارج مي‌كند و متن عادي كلمه عبور به سرعت از بين مي‌رود.

- چنانچه شما نام Domain را وارد نكرده باشيد روال تشخيص هويت توسط winlogon ادامه پيدا مي‌كند، ولي در اين‌جا فرض مي‌كنيم كه مي‌خواهيم وارد Domain شويم، لذا ادامه روال تشخيص هويت به netlogon منتقل مي‌شود. netlogon با استفاده از كتابخانه كربروس درخواست كلاينت را مي‌سازد. اين درخواست شامل: آدرس IP كلاينت، نام DC موردنظر، logon ID name و يك عدد تصادفي به نام nonce كه با استفاده از مقداري كه در مرحله قبل با اعمال توابع درهم‌سازي روي كلمه عبور كاربر توسط winlogon به دست آمده بود رمز شده است. كلاينت انتظار دارد سرور بتواند آن را (nonce) از رمز خارج كرده و مجدداً به كلاينت ارسال كند. البته باز هم به شكل رمز شده، و لذا هويت سرور به كلاينت اثبات مي‌شود. ضمناً سرور هم انتظار دارد كه با استفاده از كليد خصوصي كلاينت كه در Active Directory نگهداري مي‌شود، بتواند آن را از رمز خارج كند. Active Directory يك بانك اطلاعاتي (DB) براي نگهداري موجوديت‌هاي يك شبكه مي‌باشد.

- netlogon پس از ساختن پيام با استفاده از DNS موجود در شبكه IP آدرس كامپيوتر Domain controller را به دست مي‌آورد و پيام ساخته شده را ارسال مي‌كند و سپس منتظر پاسخ مي‌شود.

- سرويس netlogon موجود روي سرور، درخواست بليط tgt كلاينت را مي‌گيرد و آن را به lsass مي‌دهد. lsass با استفاده از كتابخانه kdcsvc.dll موجود روي سرور نام كاربر را در Active Directory جستجو مي‌كند، چنانچه نام پيدا شود با استفاده از كلمه عبور آن كاربر كه در Directory Active ثبت شده‌nonce را از رمز خارج مي‌كند و در ادامه پس از تشخيص اصالت پيام، DC در پاسخ به درخواست كلاينت، داده‌هاي زير را به آن ارسال مي‌كند.

۱- فلگر مشخص‌كننده نوع پيام (بليطTGT)

۲- داده‌هايي كه با استفاده از كليد كلاينت رمز شده كه شامل:

۱- كليد نشست، تاريخ انقضاي كليد، تاريخ تشخيص هويت، زمان شروع و پايان استفاده از بليط، نام Domain كه بليط در آن معتبر

است و nonce مي‌باشد.
۳- بليط TGT (كه توسط كليدي كه در اختيارDC و سرورهاي موجود در شبكه member servers مي‌باشد، رمز شده است

- سرويس كربروس سمت كلاينت، پيام را دريافت كرده و پس از بررسي‌هاي لازم و تشخيص اصالت پيام، شما وارد Domain مي‌شويد.

نتيجه اين روال تشخيص هويت، ورود شما به Domain و به دست آوردن بليط TGT مي‌باشد و در هر بار كه وارد Domain ويندوز۲۰۰۰ مي‌شويد اين روال طي مي‌شود.
بديهي است وقتي شما مي‌خواهيد به سروري كه در Domain قرار دارد دسترسي پيدا كنيد و از منابع آن استفاده كنيد، روالي كه در پروتكل كربروس شرح داده شده با استفاده ازlsass و كتابخانه‌هاي كربروس طي مي‌شود (پيام‌هاي ۳ و ۴ با DC و ۵ و ۶ با سرور موردنظر تبادل مي‌شوند) كه در اين‌جا به شرح مجدد آن‌ها نمي‌پردازيم.
پروتكل كربروس پروتكل پيش‌فرض تشخيص هويت در ويندوز ۲۰۰۰ مي‌باشد و براي استفاده از آن هيچ‌گونه تنظيماتي را نياز نداريم. با اين وجود در قسمت سياست‌هاي امنيتي (Domain Policy console) قسمتي با نام Policy Kerberos وجود دارد كه از طريق آن مي‌توانيد برخي از مشخصات بليطها و به‌طور كلي پروتكل را تغيير دهيد. به عنوان مثال طول مدت عمر بليط، proxiable بودن بليط كه مشخص مي‌كند سيستمي به نمايندگي از صاحب اصلي بليط، بليط را استفاده مي‌كند (كلاينت A به سرور B دسترسي پيدا مي‌كند و در حين استفاده از B حالتي پيش مي‌آيد كه B براي پاسخ به A لازم است از سرور C استفاده كند در چنين حالتي B از بليط A استفاده كرده و به C وصل مي‌شود) و برخي ديگر از مشخصات بليطها كه قابليت تنظيم دارند. توجه داشته باشيد كه اين تنظيمات به صورت پيش‌فرض تماماً مقاديري كه در استاندارد RFC۱۵۱۰ كربروس آمده است نيستند و مايكروسافت با توجه به پياده‌سازي خود، آن‌ها را تنظيم كرده است. همچنين ملاحظه كرديد كه در بسياري از موارد ديگر هم پياده‌سازي مايكروسافت با استاندارد ارايه شده متفاوت است از جمله يكي ديگر از اين تفاوت‌هاي مهم اين است كه در استاندارد ارايه شده از پروتكل udp استفاده مي‌شود ولي در ويندوز ۲۰۰۰ ازtcp استفاده مي‌گردد.

تخصص شبكه و مدركCCNP

اشاره :

در شماره‌هاي گذشته ماهنامه شبكه، مطالبي در مورد مدارك مخصوص مهندسي شبكه همانند +Network و CCNA به چاپ رسيده است. مدرك +Network مربوط به آشنايي اصولي و پايه‌اي با مفاهيم اساسي شبكه است و مدرك CCNA مربوط به برپايي و پيكربندي شبكه‌هاي مبتني بر تجهيزات سيسكو كه كمتر از يكصد كلاينت در شبكه دارند. در اين شماره قصد داريم مدرك مقطع بالاتر شركت سيسكو براي شبكه‌هاي بزرگتر را معرفي كنيم. لازم به يادآوري است كه منابع مورداستفاده اين مقاله، سايت شركت سيسكو، مجلات الكترونيكي مربوط به كسب مدرك و راهنماي موسسه آموزشي كاريار ارقام مي‌باشد.

معرفي

CCNP يك مدرك رده بالاي مهندسي شبكه است. افرادي كه صاحب مدرك مذكور شوند قادر خواهند بود شبكه‌هاي بزرگ كامپيوتري كه بين صد تا بيش از پانصد كامپيوتر دارند، را نصب، پيكربندي و عيب‌يابي نمايند. اين نوع شبكه‌ها كه عموماً در كارخانجات صنعتي بزرگ مراكز عظيم تجاري و همچنين سازمان‌هاي بزرگ مستقر هستند، برخلاف شبكه‌هاي محلي كوچك و شبكه‌هاي دفتري، به

دليل نوع استفاده، تعداد كاربران زياد و نقشي كه در پيشبرد اهداف نهايي آن سازمان ايفا مي‌كنند، از حساسيت و اهميت حياتي برخوردارند. لذا افرادي كه با كسب مدرك CCNP پا به عرصه پرداختن به اين‌گونه شبكه‌ها مي‌گذارند نسبت به دارندگان مدارك ديگري چون CCNA، اهداف بزرگتر و به دنبال آن مشكلات و دردسرهاي بيشتري را پيش‌رو دارند. در عوض، اين افراد از لحاظ موقعيت شغلي در رده‌هاي بالاتر، از لحاظ حساسيت نقشي كه به عهده دارند داراي مسؤوليت خطيرتر، و از لحاظ درآمد، وضعيتي مطلوبتر از ساير دست‌اندركاران طراحي و نصب شبكه دارند.
به‌طور كلي CCNP مدركي است كه چيزي را جهت دستيابي داوطلب به فناوري روز شبكه‌هاي بزرگ كم نمي‌گذارد. مباحث متعددي كه در اين دوره مطرح مي‌شود به صورت همه جانبه، هر نوع فناوري در زمينه شبكه‌هاي مذكور را مورد بررسي قرار مي‌دهد و در اين راه هر مسأله مهمي مثل امنيت، كيفيت سرويس (QoS)، شبكه‌هاي مجازي (VPN) و تكنولوژي باندپهن را به تفصيل مطرح مي‌نمايد.

پيش‌نياز

داوطلبان كسب مدرك CCNP بايد اولين قاعده هرم تحصيلي شركت سيسكو يعني مدرك CCNA را كه مربوط به شبكه‌هاي محلي كوچك مي‌شود گذرانده باشند. به طور كلي و بدون در نظر گرفتن هدف كسب مدرك، اشخاصي كه مايلند در دوره‌هاي آموزشي CCNP شركت نمايند بايد با مفاهيم اساسي و مهمي چون موارد زير آشنايي قبلي داشته باشند:
ISL، Route Redistribution، IP، X.25، OSPF، IPX، DDR، VLSM، IGRP، PSTN، Relay Frame، Async Routing، VLAN، ISDN ، Apple talk، FDDI،Ethernet و ۱۰. ۸۰۲.

اهداف

شخصي كه به دريافت مدرك CCNP نايل مي‌شود از لحاظ رده شغلي در ميان تمام شغل‌هايي كه مربوط به مهندسي شبكه و خصوصاً نصب راه‌اندازي شبكه با استفاده از تجهيزات سيسكو مي‌شود، در رده دوم يعني پس از مدرك CCIE كه مربوط به مشاوران حرفه‌اي سيسكو است قرار مي‌گيرد. اين بدين معني است كه شخص دارندهCCNP مي‌تواند اولاً فاصله مقام خود را با ارشدترين سطح كارشناسي شبكه به يك قدم برساند. كارشناس شبكه با ارتقاي مدرك خود از CCNA به CCNP نه تنها تسلط خود بر مباحث مربوط به شبكه‌هاي LAN و Dial up را افزايش مي‌دهد بلكه از محدوده شبكه‌هاي محلي با كاربرد كوچك خارج شده و توانايي خود را در راه‌اندازي شبكه‌هاي WAN تثبيت مي‌كند.
براي كسب مدرك CCNP شركت در ۴ دوره آموزشي و گذراندن موفقيت‌آميز آزمون‌هاي هر كدام از آن‌ها الزامي است. اين دوره عبارتند از:

۱- ساخت شبكه‌هاي عادي سيسكو (BSCI)

در اين دوره، نحوه اتصال و استفاده از روترهاي سيسكو در شبكه‌هاي LAN و WAN براي سايت‌هاي متوسط تا بزرگ آموزش داده مي‌شود. در اين دوره مباحث جامعي در زمينه پروتكل‌هاي EIGRP، BGP، EGP،OSPF و ISIS مطرح شده و داوطلبان با دو نوع پروتكل مسيريابي به نام‌هاي Distance Vector و Link State آشنا شوند. با اتمام اين دوره، داوطلب مي‌تواند سرويس‌هاي IOS مناسب يك روتر سيسكو را انتخاب و راه‌اندازي نمايد.

۲- ساخت شبكه‌هاي چند لايه سيسكو (BCMSN)

در اين دوره، نحوه ايجاد يك فضاي شبكه براساس فناوري سوئيچينگ چندلايه در سرعت‌هاي بالاي اترنت به مديران شبكه‌ها آموزش داده مي‌شود. اين دوره شامل مفاهيم مسيريابي و سوئيچينگ و فناوري‌هاي لايه دو و سه است. داوطلبان پس از طي اين دوره قادر خواهند بود يك فضاي سوئيچينگ چند لايه را برپا ساخته و به كنترل ترافيك شبكه با استفاده از سيستم‌هاي احراز هويت لايه‌هاي مختلف بپردازند.

۳- ساخت شبكه‌هاي راه‌دور (BCRAN)

در اين دوره، داوطلب چگونگي پيكربندي و عيب‌يابي شبكه‌هايي كه در جاهاي ديگر ايجاد شده و از طريق تكنولوژي راه‌دور (Remote) به سايت مركزي دسترسي دارند را فرا مي‌گيرد. همچنين حالت عكس اين عمل يعني دسترسي راه‌دور به سايت مركزي با مصرف كمترين پهناي‌باند نيز در اين دوره مورد بحث قرار مي‌گيرد. به طور كلي در BCRAN توجه ويژه‌اي به شبكه‌هاي WAN به عمل آمده و نحوه پيكربندي تجهيزات سيسكو و برقراري ارتباط بهينه بين سايت مركزي و ساير شعبات و مسايل مربوط به كيفيت سرويس (QOS) در يك شبكه WAN تشريح مي‌شود.

اين دوره به خصوص براي مديران شبكه‌ها كه مسؤول اجرا و عيب‌يابي Backbone يك شبكه WAN هستند از اهميت خاصي برخوردار است.

۴- پشتيباني و رفع عيب شبكه (CIT)

در اين دوره، داوطلب چگونگي عيب‌يابي كامپيوترهاي سرويس گيرنده يا سرويس‌دهنده كه تحت پروتكل‌هاي مختلف به هم متصل گشته‌اند و از سوئيچ‌ها و روترهاي سيسكو استفاده مي‌كنند را فرا مي‌گيرد. بنابراين با گذراندن دوره مذكور، مي‌توان به تحليل و شناسايي مشكلات در محيط‌هاي Fast Ethrnet، VLAN، Frame Relay، ISDN BRI و ... پرداخت و مشكلات پيچيده مربوط به سوئيچ‌ها و روترهاي سيسكو را حل كرد.

وضعيت درآمد

طبق آمار مجله Certification، ميانگين درآمد دارندگان مدرك CCNP در سال ۲۰۰۳ برابر ۶۴ هزار دلار در سال بوده است كه در مقايسه با مدرك بنيادين و سطح مبتدي شبكه يعني +Network با ۳۸ هزار دلار در سال و مدرك سيسكو سطح متوسط شبكه يعني CCNA با ۴۸ هزاردلار در سال، از فاصله جالب توجهي برخوردار است. در اين آمار، مدرك مهندسي شبكه مايكروسافت درآمدي در حدود ۴۳ هزاردلار در سال را از آن خود كرده است كه اين مسأله به نوعي بيانگر دشواري مراحل يادگيري و سطح بالاي مدرك CCNP است. همچنين طبق آمار ديگري كه از طرف موسسه آموزشي Cert City صورت گرفته است، دارندگان مدرك CCNP با حداقل ۱۲ درصد افزايش حقوق يعني بيش از ۶ هزار دلار نسبت به وضعيت قبلي خود با مدرك CCNA مواجه گشته‌اند.

همچنين آماري كه مجله TCPMag ارايه مي‌دهد حاكي از كاهش ۷ درصدي تعداد دارندگان اين مدرك نسبت به سال قبل ۲۰۰۲ است. اما در همين مورد سايت Cert Mag اعلام كرده است كه ميانگين درآمد دارندگان مدرك CCNP برابر ۶۹ هزاردلار در سال بوده است كه نسبت به مدرك CCNA از يك افزايش ۱۰ هزاردلاري در سال حكايت مي‌كند

راهنماي ساخت سي دي هاي AUTO RUN

اشاره

خود را به كاربر معرفي مي‌كنند، بدون هاي تجاري و تبليغاتي به محض اين‌كه در درايو قرار مي‌گيرند، به سرعتDVD ها ياCD بيشتر ها هنگامي جذاب‌تر مي‌شود كه با يك صفحهDVD ها ياCD ارايه اطلاعات در اين آن‌كه كاربر به چيزي دست زده باشد. اين نوع ما مي‌خواهيم با معرفي يك نرم‌افزار، ، يك موزيك مهيج و يا حتي يك فيلم كوتاه همراه شود. در اين مقالهFlash يك انيميشن ،splash .هايي كه مي‌خواهيد رايت كنيد بهره ببريدCD فوق در كاري كنيم تا شما بتوانيد به راحتي از امكانات

در حالت معمول اگر شما يك فايل انيميشن يا يك موسيقي را روي CD رايت كنيد و آن را درون درايو قرار دهيد اتفاق خاصي نمي‌افتد. چون در سيستم‌عامل‌ها به طور معمول قابليت autorun يا خودراه‌انداز وجود ندارد. (اگر چه در ويندوز XP راه‌هاي زيادي براي اين‌كار وجود دارد).

براي اين‌كه ما يك autorun CD داشته باشيم، علاوه بر اطلاعات موردنظرمان بايد فايل‌هاي ديگري نظير فايل autorun.inf را نيز روي CD قرار دهيم. نوع اين فايل txt بوده و خودتان نيز مي‌توانيد آن را ايجاد كنيد. اما آسان‌ترين راه، استفاده از برنامه‌اي است كه اين‌كار را به راحتي براي شما انجام مي‌دهد. يكي از برنامه‌هايي كه در اين كار به شما كمك فراواني مي‌كند، برنامه‌اي است تحت عنوان Autorun wizard v ۰,۲ كه نسخه آزمايشي آن از روي نشاني

http://www.rjlsoftware.com/software/utility/autorun/order.shtml قابل دريافت است. البته اين برنامه صفحه splash (همان صفحه ظاهر شونده اوليه) خود را به Autorun CD شما مي‌افزايد و همچنين هزينه خريد آن در حدود بيست دلار است.

براي ساختن CD خودراه‌انداز قبل از هر كاري لازم است در آن قسمتي از هارددیسك كه اطلاعات موردنظر شما براي رايت CD وجود

دارد، پوشه‌اي ايجاد كنيد كه بعداً در برنامه Autorun wizard مورد استفاده قرار بگيرد سپس بايد برنامه را اجرا كنيد و تمام كارهايي كه CD شما از لحظه قرار گرفتن در درايو بايد انجام دهد را در آن معرفي مي‌كنيد. سپس CD خودرا رايت كنيد.

راهنماي گام به گام

استفاده از برنامهAutorun Wizard

- 1در جايي كه اطلاعات موردنظر شما براي رايت روي CD وجود دارد پوشه‌اي ايجاد كنيد و نام آن را CD Base يا هر نام ديگري كه در حافظه‌تان مي‌ماند بگذاريد و فايل Autorun.zip را در اين پوشه باز كنيد .

- 2فايل Config.exe را اجرا كنيد .با اين كار wizard برنامه آغاز به كار مي‌كند. به زبانه Base folderبرويد و آدرس پوشه موردنظرتان را كه فايل‌هاي مربوط به Autorun بايد در آنجا ساخته شوند را وارد كنيد. بدون تعيين اين آدرس نمي‌توانيد وارد مراحل بعدي شويد .

- 3زبانه بعدي Auto Lunch نام دارد .تمام اتفاقاتي كه قرار است وقتي CD را در درايو مي‌گذاريم، بيفتند را در اين‌جا به برنامه معرفي مي‌كنيم. اتفاقاتي مثل باز شدن ويندوز اكسپلورر يا مثلاً اجرا شدن چند فايل و ... مثلاً فايل‌هاي موردنظرتان براي اجرا شدن را انتخاب كنيد. در آخر روي Lunch file و بعد روي Configure كليك كنيد و آدرس فايل‌هايي را كه مي‌خواهيد استفاده شوند به برنامه بدهيد.

- 4روي Icon كليك كنيد. اگر آيكون خاصي را براي CD موردنظر داريد آدرس فايل .ICO را به برنامه بدهيد .همچنين اگر صفحه splash

را نيز مي‌خواهيد روي CD داشته باشيد آدرس تصوير آن را به برنامه بدهيد.

- 5روي زبانه options شما مي‌توانيد يك برچسب (label) مشخص و البته يك فايل صوتي .wav را به CD خود ضميمه كنيد. روي زبانه Test روي كليد Test را كليك كنيد. اگر از نتيجه كار راضي هستيد آن را save كنيد و Autorun wizard را ببنديد .

- 6برنامه رايت CD را باز كنيد و همه فايل‌هاي موجود در فولدر CD Base يا هر نام ديگري كه انتخاب كرده بوديد) را روي CD رايت كنيد. در اين فولدر به غير از فايل‌هاي موردنظرتان، بايد فايل‌هاي autorun.inf و autorun.dat و autorun.exe نيز وجود داشته باشند.

نگاهي به امكانات نسخه SQL Server 2005جديد

Isolation Level Snapshot

يكي از روش‌هايي كه به انواع متدهاي قفل كردن رديف‌هاي يك جدول بانك‌اطلاعاتي در نسخه جديد اضافه شده است، شيوه تصويربرداري از ركورد است. در روش‌هاي قبلي، اگر يك يا چند ركورد بانك اطلاعاتي توسط دستور BeginTrans كه شروع يك فرآيند را مشخص مي‌كند در شرف تغيير يا حذف قرار مي‌گرفتند، تا مادامي كه فرآيند مذكور توسط دستور Commit Trans تأييد يا توسط RollBack منتفي نشود، از هيچ جا و برنامه‌اي نمي‌توان ركوردهاي مذكور را حتي با دستور ساده SELECT خواند. اما در روش جديد قفل‌گذاري، در صورت بروز چنين رويدادي ساير كاربران مي‌توانند همواره آخرين ارزش ركوردهاي مذكور را با اين فرض كه هنوز هيچ تغييري در آن‌ها ايجاد نشده است بخوانند و مورد استفاده قرار دهند.

باز هم دات‌نت

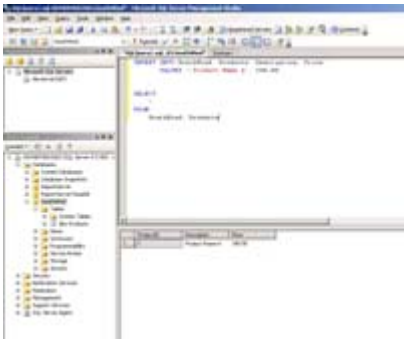
با نسخه جديد SQL Server، برنامه‌نويسان بانك‌هاي اطلاعاتي قادرند از امكانات و قابليت‌هاي موجود در پلتفرم دات‌نت و كليه توابع و كلاس‌هاي ساخته شده در آن بهره‌مند شوند. يكي از ابتدايي‌ترين و در عين حال اساسي‌ترين اين قابليت‌ها، امكان استفاده از دو زبان مهم و كاربرپسند دات‌نت يعني ويژوال بيسيك و سي‌شارپ در پياده‌سازي اجزاي مختلف يك بانك‌اطلاعاتي است. اين عامل

نه‌تنها باعث مي‌شود كه برنامه‌نويسان براي نوشتن ماژول‌هايي مثل تريگرها، روال‌ها (Stored Procedures) در توابع به جاي استفاده از زبان استاندارد و در عين حال پيچيده T-SQL ، بتوانند از زبان‌هاي محيط دات‌نت با تمام ساختارها، دستورات، كلاس‌ها، آرايه‌ها، و خلاصه تمام ويژگي‌هاي يك زبان شي گرا استفاده كنند، بلكه اين همكاري نزديك بين موتور برنامه‌نويسي دات‌نت يعني CLR (كه مسؤول تبديل كدهاي نوشته شده دات‌نت به زبان سيستم‌عامل است) و موتور بانك اطلاعاتي SQLServer باعث شده تا به غير از تنوع زبان‌هاي برنامه‌نويسي قابل استفاده درSQLServer، تغيير قابل توجهي نيز در كارايي ماژول‌هاي مذكور پيش آيد. در واقع موضوع از اين قرار است كه اصولاً كدهاي نوشته شده به زبان‌هاي دات‌نت، ابتدا توسط كامپايلر به زبان (IL) ترجمه مي‌شوند. سپس CLR اين كد مياني را به كد قابل فهم سيستم‌عامل تبديل و آماده اجرا مي‌نمايد. اين كار سبب مي‌شود تا كدهاي نهايي به دليل اين‌كه بسيار به سيستم‌عامل نزديك مي‌باشد سريع‌تر از كدهاي TSQL (كه فقط توسط موتور بانك اطلاعاتي قابل اجرا هستند) اجرا شوند و در زمان اجرا از كارايي بيشتري برخوردار باشند. البته اين مسأله بدين معني نيست كه استفاده از زبان‌هاي دات‌نت هميشه بر زبان‌هاي SQL ارجحيت دارد، بلكه منظور آن است كه در برخي موارد ممكن است آن قدر منطق و الگوريتم يك ماژول پيچيده باشد كه برنامه‌نويس استفاده از زبان‌هاي دات‌نت را به دليل آسان‌تر بودن ساختار و دستورات آن به زبان SQL ترجيح دهد. بنابراين زماني كه بيشترعمليات يك ماژول مربوط به خواندن و نوشتن اطلاعات باشد بهتر است از همان دستورات استاندارد SQL يعني SELECT ، UPDATE،DELETE وINSERT استفاده كرده و بي‌جهت منابع سيستم را صرف تعريف متغيرها و كلاس‌هاي دات‌نت ننمايد. اما در ماژول‌هايي كه بيشتر عملياتشان شامل پردازش اطلاعات مثل انجام عمليات‌هاي رياضي يا مقايسه اطلاعات با يكديگر است بهتر است تا هم از امكانات برنامه‌نويسي و هم از سرعت و كارايي بالاي دات‌نت در اين زمينه بهره برد و ماژول‌هاي مذكور را با زبان‌هاي دات‌نت پياده‌سازي كرد.

ADO .NET وارد مي‌شود

طبق يك سنت نه‌چندان قديمي برنامه‌نويسي در محيط ويندوز، برنامه‌نويسان SQLServer، بانك اطلاعاتي موردنظرشان را برروي سرور و برنامه كاربردي نوشته شده با زباني مثل ويژوال بيسيك را بر روي كلاينت‌ها قرار مي‌دهند. سپس از طريق اين برنامه كاربردي و با استفاده از اشيايي از جنس ADO داده‌هاي موردنياز خود را از سمت سرور دريافت كرده و يا به آن ارسال مي‌كنند. اكنون اين ارتباط به لطف نسخه جديد SQLServer و همچنين محيط دات‌نت، با امكانات جديدADO.NET بسيار كامل‌تر از قبل شده است.
اين ارتباط جديد با استفاده از مكانيسمي به نام اعلان (Notification) به يك ارتباط دوطرفه فعال تبديل شده به طوري كه ADO.NET قادر است پيغام‌هايي را از سمت پايگاه داده به سمت كلاينت ارسال كند. به عنوان مثال فرض كنيد كه شما با استفاده ازADO تعدادي از ركوردهاي يك جدول بانك اطلاعاتي را انتخاب كرده و مشغول كار برروي آن‌ها هستيد. در همين هنگام كاربر ديگري از طريق كلاينت و ADO خود، ركوردي در محدوده ركوردهاي مورد انتخاب شما را تغيير مي‌دهد يا حذف مي‌كند. در اين وقت موتور پايگاه داده با ارسال پيغامي به ADO شما، اين مسأله را با استفاده از فراخواني يك رخداد (Event) شي ADO به اطلاعتان مي‌رساند.
علاوه براين قابليت جديد، فناوري جديد ديگري هم با استفاده ازADO.NET به نسخه جديد SQLServer اضافه شده و آن امكان چند پرس‌وجوي همزمان توسط يك شي ADO است. در اين شيوه اگر يك شي ADO با استفاده از دستور SELECT مشغول خواندن تعدادي از ركوردهاي يك جدول بانك اطلاعاتي باشد، مي‌تواند بدون اين‌كه منتظر به پايان رسيدن اين عمليات شود، تعداد ديگري از ركوردهاي يك جدول ديگر بانك اطلاعاتي را بخواند. اين قابليت جديد با نام Multiple Active Result Set (MARS) كه قبلاً فقط در كرسرهاي سمت سرور (server side) و آن هم نه با كارايي بالا وجود داشت اكنون در كرسرهاي سمت راست كلاينت هم وجود دارد و تفاوت عمده آن با شكل قديمي هم علاوه بر مورد مذكور، امكان ايجاد چند كرسر در يك شي ADO به صورت همزمان است.
SQLServer نسخه ۲۰۰۵ به خوبي از تمام اين ويژگي‌ها، پشتيباني مي‌كند.

تكنولوژي XML



اكنون كه XML به يك استاندارد ارتباطي بين سكوهاي مختلف تبديل شده است، نسخه جديد SQLServer هم از توجه كافي به آن و ايجاد يك انقلاب در ساده‌تر استفاده كردن از آن طفره نرفته است. در نسخه ۲۰۰۰ كاربران قادر بودند تا با استفاده از دستور FOR XML نتيجه يك پرس‌وجوي SELECT از يك بانك اطلاعاتي را به درون يك فايل XML بريزند يا مثلاً با دستور OPEN XML مي‌توانستند يك فايل XML را باز كرده و شروع به خواندن دستورات درون آن نمايند.
از آن‌جا كه در نسخه جديد SQLServer توجه خاصي به اين استاندارد و زبان ارتباطي شده است، يك نوع داده جديد (Data type) به انواع داده‌هاي قبلي و استاندارد SQL مثل int، char و امثال آن اضافه شده است.

اين نوع داده جديد كه XML نام دارد و داراي خصوصيات يك نوع داده موجود در يك محيط شيگرا است، داراي متدهاي پيشرفتهاي چون () ()Value،nodes() ، ()query،exist و ()modify بوده و قادر است انواع پردازشهاي قابل انجام برروي اسناد XML را به راحتي انجام دهد. عمليات جستجو، تغيير، حذف و درج مقادير موردنظر در داخل يك فايل XML را ميتوان با استفاده از متدهاي مذكور و صرفاً با چند خط برنامهنويسي انجام داد. همچنين در اين نسخه برخلاف نسخه ۲۰۰۰، با استفاده از دستور FOR XML ميتوان يك شيء از جنس XML را بدون ارسال آن به كلاينت، برروي سرور ساخته و از آن نگهداري كرد. با اين كار ميتوان جداولي را كه مرتباً مورد رجوع كاربران قرار ميگيرند هراز گاهي در قالب XML به داخل حافظه آورد و كاربران مذكور به جاي رجوع به جداول اصلي در هارددیسك، با استفاده از دستورات ويژه جستجو درXML ، متغير مذكور را در حافظه سرور مورد جستجو قرار دهند و بدينوسيله يك نوع عمل Cache كردن را جهت افزايش سرعت دسترسي به اطلاعات تكراري شبيهسازي كنند. در اين حالت، كاربران به جاي استفاده از دستورSELECT استاندارد ميتوانند از OPEN XML كه در نسخه ۲۰۰۵ قادر است متغيرهاي جديد از نوع XML را بخواند استفاده كرده و به سرعت به اطلاعات موردنياز خود دسترسي پيدا كنند. اين قابليت جديد آنقدر در سريعتر كردن جستجو در برنامههاي تحت وب مهم و مؤثر است كه جاي هيچ مشكلي را در استفاده از آن باقي نميگذارد.

سرويس اعلان (Notification)

همانطور كه گفتيم سيستم اعلان درSQLServer قادر است پيغامهايي را طي زمانهاي مشخص به سمت كاربران بفرستد. مثلاً تصور كنيد كه تعدادي كاربر در حال اتصال به يك بانك حاوي اطلاعات مربوط به ارزش سهام در بورس هستند. از آنجايي كه ممكن است قيمت سهام هر شركت يا مؤسسه براي تعدادي از كاربران از اهميت زيادي برخوردار باشد، ميتوان اين سيستم را طوري تنظيم كرد تا هرگاه ارزش سهام خاصي كه موردنظر هر كاربر است تغيير كرد، به صورت اتوماتيك به وي اعلام شود. كاربر هم ميتواند اين تغييرات را برروي برنامه كاربردي خود، تلفن همراه (در قالب SMS،Windows Messenger) و يا ايميل بهصورت مرتب دريافت و مشاهده كند.

سرويس گزارشگيري

سرويس جديد توليد گزارشهاي متنوع در نسخه ۲۰۰۵ به يكي از جالبترين و پركاربردترين قابليتهاي اين نسخه تبديل شده است، وجود يك موتور گزارشگر قوي در سمت سرور و يك ابزار مناسب ساخت گزارش با واسط كاربر عالي، باعث شده تا برنامهنويسان بتوانند گزارشهاي موردنظر خود را با كارايي و سرعت مناسب در سمت سرور بسازند به طوري كه اين گزارشهاي سمت سرور توسط هر برنامه كاربردي سمت كلاينت در هر پلتفرمي با همان امكانات اتصال به SQLServer قابل مشاهده است.

بهبودهاي ايجاد شده در زبان

در SQLServer ۲۰۰۵ تغييرات بسيار مثبتي در زبان SQL T ايجاد شده است. اين تغييرات در زمينههاي مختلف مثل مديريت خطاها، جستجوهاي بازگشتي (Recursive Query) و حتي در بدنه موتور پايگاه دادهها انجام شده و كارايي كلي ذخيره و يا خواندن اطلاعات را به نحو مطلوبي افزايش داده است. به عنوان مثال دردستورات

TSQL، دو اپراتور جديد ديده ميشود، كه PIVOT وUNPIVOT نام دارند. اين دو اپراتور كه در قسمت FROM يك پرسوجو مورد استفاده قرار ميگيرند ميتوانند نتيجه يك جستجوي انجام شده توسط دستور SELECT را به جاي برگرداندن در قالب رديفها يا ركوردهاي پشتسرهم، به صورت ستونهاي مختلف يك يا چند ركورد برگردانند. در اين روش يكي از ستونهاي (فيلدهاي) يك جستجو به عنوان محور معرفي شده و بقيه ستونها براساس آن به صورت افقي طبقهبندي ميشوند. به يك مثال توجه كنيد:

SELECT CUSTOMER ID, order No

CustomerID FROM orders PIVOT

1	**25**	**1120**	**4400**	

2	**350**			
3	**443**	**1780**		
4	**555**	**1980**	**2222**	**8989**

نتيجه جستجوي فوق چيزي شبيه جدول بالا خواهد بود

همان‌طور كه مشاهده مي‌كنيد با استفاده از اپراتور مذكور، نتيجه پرس‌وجوي انجام شده به اين صورت كه هر رديف به يك شماره مشتري و چندين شماره سفارش مربوطه به آن مشتري در قالب ستون‌هاي مختلف است، در مي‌آيد. اين همان چيزي است كه سال‌ها درSQLServer وجود نداشت و ابزارهاي مختلف گزارش‌سازي مثل CrystalReport آن را با نام Cross Tab به كاربران خود ارايه مي‌دادند. در همين رابطه اپراتورUNPIVOT هم عمل عكس اپراتور مذكور را انجام مي‌دهد.
اپراتور ديگري كه مي‌تواند نقش مهمي را در دستورات SQL بازي كند APPLY نام دارد كه در قسمت FROM يك دستور SQL به كار مي‌رود. با استفاده از اين دستور مي‌توان خروجي يك تابع (Function) را با يك يا چند جدول ديگر تركيب (Join) كرد همان‌طور كه مي‌دانيد در SQLServer ۲۰۰۵ توابع مي‌توانند يك يا چند رديف يك جدول اطلاعاتي را برگردانند كه اين خروجي مي‌تواند با يك جدول ديگر با استفاده از اپراتور مذكور تركيب شود.

مديريت خطا

در نسخه‌هاي قديمي SQLServer براي كشف و مديريت خطا از سيستم Error Handling استفاده مي‌شد. اين شيوه كشف خطا كه در زباني مثل ويژوال بيسيك ٦ هم مورد استفاده قرار مي‌گرفت با استفاده از دستور GOTO مي‌توانست كنترل و خط اجراي روال را از يك محل به محل ديگر و در واقع از محل بروز خطا به محل مديريت و آشكار كردن (Raise) آن ببرد و بدين‌وسيله پيغام خطايي را به كار نشان دهد. نسخه جديد SQLServer با تأثير از پلتفرم دات‌نت، از دستورات ويژه كشف و مديريت خطا با عنوان Exception Handling استفاده مي‌كند. اين روش با استفاده از دستورات جديد TRY/CATCH شيوه بهتري از مديريت خطا را به اجرا مي‌گذارد. در اين روش برخلاف روش قبل، تمام خطاهاي اتفاق‌افتادني مثل خطاهاي مربوط به تبديل داده‌ها به يكديگر (DataConversion) به خوبي مديريت شده و از بروز خطاهايي كه منجر به اتمام ناقص عمليات يك روال يا تريگر مي‌شود جلوگيري به عمل مي‌آيد.

افزايش ترافيك وب‌سايت پنج روش رايگان براي

محمود بشاش - وقتي براي اولين بار وارد دنياي بازاريابي اينترنتي شدم، فكر كردم مي‌توانم وب‌سايت تازه تأسيسم را به تعدادكمي موتور جستجو معرفي كرده، سپس منتظر هجوم مراجعين بمانم. منتظر معجزه‌اي بودم تا افراد را وادار كند به وب‌سايت من مراجعه كرده، كالا بخرند و دوباره باز گردند.
اما، چه خيال باطلي! ... تازه فهميدم اين كار به زمان بيشتري نياز دارد.از آن زمان به بعد به كارآيي عجيب وغريب و خارق العاده

بازاريابي اينترنتي پي برده‌ام.
در اين جا پنج روش رايگان افزايش ترافيك وب سايت را براي شما بازگو مي‌كنم.
مطمئن باشيد تمام اين روش ها كاملا رايگان بوده،با صرف كمي وقت به سودمندبودن آنها پي مي‌بريد.

۱- نوشتن مقالات

نوشتن وانتشار مقاله با موضوع مرتبط با سايت شما دست كم دو فايده‌ي اساسي دارد:
- افرادي كه مجذوب اين مقاله شده‌اند، آن را خوانده، براي جستجوي مطالب بيشتر،روي URL شما كليك مي‌كنند.به اين ترتيب يك مراجع هدف دار داريد.از اين جهت از كلمه‌ي جهت دار استفاده مي‌كنم كه اين خواننده مي‌خواهد، مطالب بيشتري در مورد موضوع مقاله‌ي قبلي پيدا كند.
- با هر بار انتشار اين مقاله ،لينك‌هاي شما نيز منتشر مي‌شود.همراه بودن ليست لينك‌ها و URLبا مقالات ، تعداد لينك‌هاي برگشتي سايت شمارا زياد كرده، به نوبه‌ي خود رتبه‌ي شما را در موتور جستجوي مربوطه افزايش مي‌دهد.

۲-شبكه‌ي تالار گفتگو

تالارهاي گفتگوي فراواني درباره‌ي هر موضوعي كه فكرش را بكنيد، به شكل برخط(OnLine) وجود دارد. دربيشتر اعلان‌هاي گفتگو، پوسترهايي براي ضميمه كردن امضا و همين طور اطلاعات ديگر مانند نام، URL و حتي گاهي تبليغات، در نظر گرفته شده‌است. با مراجعه‌ي منظم به اين تالارهاي گفتگو، شركت در بحث‌ها، مطرح‌كردن پرسش و پاسخ به پرسش‌ها، مي‌توانيد ضمن ايجاد رابطه‌ي توأم با اعتماد با ساير اعضا ، به طور رايگان به تبليغ سايت خود بپردازيد. فقط سعي كنيد براي تالارهاي گفتگو مفيد بوده، به قوانين آن احترام گذاشته، هيچ‌گاه هرزنامه نفرستيد.

۳- لينك‌هاي دوطرفه

اين لينك‌ها دو فايده براي شما دارد:
اول اين كه با تبادل هرچه بيشتر لينك‌ها ، احتمال اين كه افراد، لينك شما را در سايت‌هاي ديگر ديده و به سايت شما مراجعه كنند، بيش‌تر مي‌شود.
نكته‌ي ديگر اين‌كه، موقعيت شما در موتورهاي جستجو به كل تغيير مي‌كند به طور خلاصه لينك‌هاي بيش‌تر از سايت‌هاي ديگر، مساوي است با رتبه‌ي بالاتر در موتورهاي جستجو.
در اين جا چند "بايد" و"نبايد" را در مورد تبادل لينك ذكر مي‌كنم:
- لينك خودرا به سايت‌هايي بفرستيد كه مورد علاقه‌ي مراجعين شما هستند.
- به صفحاتي با هزاران لينك،كه دايركتوري‌هاي لينك نامنظمي دارند، لينك نفرستيد.چون نه براي ايجاد ترافيك سايت سودمند است ونه براي رتبه‌ي شما در موتورهاي جستجو.
- با سايت‌هايي لينك، مبادله كنيدكه در صفحه‌ي اصلي شان، دايركتوري لينك به طور صريح ذكر شده باشد.
- از صفحات، با لينك‌هاي‌انبوه ياFFA استفاده نكنيد.احتمال بالا بردن ترافيك سايت، از اين طريق، بعيدبه نظر مي‌رسدو حتي ممكن است موتورهاي جستجو شما را جريمه كنند.
- از دايركتوري‌هاي لينك، براي پيداكردن شركاي مناسب تبادل لينك، استفاده كنيد.سايت-Link-http:/www.homebiz-direct.com Exchange-Resources.html سايت مناسبي براي جستجوي دايركتوري‌هاي مشهور تبادل لينك است.
همواره كارهاي‌تان را طبق اصولي مشخص انجام دهيد.مي‌توانيداز نرم افزارهاي تبادل لينك يا صفحه‌ي گسترده براي پي‌گيري لينك‌هاي درخواستي و حفظ جزييات ارتباط با ساير سايت‌ها استفاده كنيد.

٤- امضاي ايميل

اين روشي بسيار ساده ، اما تقريبا فراموش شده براي افزايش مراجعين به سايت است.
ما تقريبا هرروز، ايميل‌هاي زيادي مي‌فرستيم، اما اغلب فقط اسم خودرا در آن نوشته،گاه حتي چيزي نمي‌نويسيم. چرا ايميل‌هاي‌تان را با امضايي حاوي اسم و مطالب اندكي درباره‌ي وب سايت‌تان به همراه URL تمام نمي‌كنيد؟
باوركنيد بدون زياده روي مي‌توان در چهار خط، تمام مطالب لازم را بيان كرد. حتماً از افزايش خارق العاده‌ي مراجعين به سايت، پس از اين كار، متعجب خواهيد شد. باورش سخت است، اما كنجكاوي، دريافت كنندگان ايميل‌ها را وادار مي‌كند روي لينك شما كليك كنند.

۵- تبادل ترافيك

اين روش ازآسان‌ترين راه‌هاي جذب مخاطب به سايت است. مثلاً، مي‌توانيد مزيت‌هاي رايگان براي وب گردي تعيين كنيد.
نقطه‌ي ضعف اين روش اين است كه افرادي كه از طريق مبادله‌ي ترافيك به سايت شما مراجعه مي‌كنند، به اندازه مراجعين از روش‌هاي قبلي هدف‌مند نيستند، زيرا اين افراد به يك دليل در اين تبادل ترافيك شركت مي‌كنند و آن به دست آوردن اعتبار بيش‌تر در كم‌ترين زمان ممكن است. اكنون زمان آن فرا رسيده كه شما وارد عمل شويد، چگونه مي‌توانيد فردي را كه فقط بيست ثانيه يا كم‌تر در صفحه‌ي وب شما توقف مي‌كند، تحت تأثير قرار دهيد.
- مخاطبين خود را بشناسيد. زماني را به مبادله‌ي تبليغات اختصاص داده، در عين حال به نوع صفحات وبي كه تبليغ مي‌كنيد، توجه كنيد. اطمينان حاصل كنيد كه تبليغات شما به شكلي هدف‌مند، افراد را جذب مي‌كند.
- سعي كنيد، تبليغاتي تنظيم كنيد كه خواندن آنها حداكثر چند ثانيه وقت بگيرد. تهيه‌ي تبليغات طولاني وقت‌گير، هنر چنداني نمي‌خواهد. مطمئن باشيد افراد از خواندن آنها خسته شده، بدون توجه به مطالب، روي دكمه‌ي "Next" كليك مي‌كنند.
به طور منظم، زماني را به مطالعه اين پنج روش مولد ترافيك، اختصاص دهيد. خواهيد ديد در يك چشم به هم زدن سايت شما در مسير پيشرفتي هدفمند گام برمي‌دارد.

مرزهاي سرعت عبور از ADSL2 - ADSL2+

اشاره :

شركت‌هاي مخابرات منطقه‌اي را به قولي صاحبان بزرگترين معادن مس دنيا مي‌دانند و اين كنايه‌اي است از حجم عظيم سيم‌هاي مسي كه بين اين مراكز مخابراتي و محل سكونت يا محل كار مشتركين تلفن نصب گرديده‌اند. استفاده بهينه از اين سرمايه، در دستور كار اين شركت‌ها قرار دارد و چند سالي است كه فناوري مودم‌هاي ديجيتال (DSL) به عنوان راه‌حلي هوشمندانه جهت انتقال ديتاي پرسرعت برروي اين سيم‌ها مطرح گرديده است. در اين ميان، مودم‌هاي خانواده ADSL به لحاظ وسعتِ به‌كارگيري در كاربردهاي خانگي، رتبه اول فروش را به خود اختصاص داده‌اند. در مقاله فناوري ADSL (ماهنامه شبكه شماره ٤١) مباني اين مودم‌ها تشريح گرديده است و در اين نوشتار سعي داريم شما را با جديدترين گونه‌هاي آنها آشنا نماييم.

در ژانويه ۲۰۰۳ سازمان ITU (سازمان بين‌المللي استانداردهاي مخابراتي) پس از فروش حدود پانزده ميليون مودمADSL در سطح جهان، مشخصات جديدي را براي اين استاندارد منتشر نمود. سري مودم‌هاي ADSL موفقترين رده ADSL را در جهان به خود اختصاص مي‌دهند و ITU سعي فراواني جهت توسعه آن دارد.

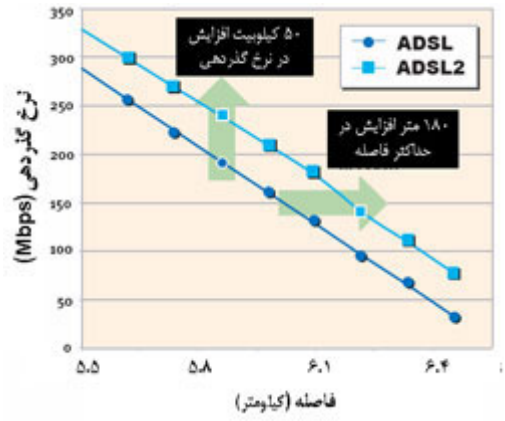
نوع مودم	استاندارد	تاريخ معرفي
ADSL	G.992.1 G.992.2	1999
ADSL2 +ADSL2	G.992.3 G.992.4 G.992.5	2002 2003
RE-ADSL2	G.992.3 Reach Extended	2003

استانداردهاي جديد با نامهاي ADSL2 و +ADSL ٢ به بازار معرفي شده‌اند. (ITU-G.992.5) براي اولين بار موفق‌شد نرخ گذردهي در جهت دريافت (downstream) را به ٢٤ مگابيت در ثانيه برساند و گونه‌اي از ADSL ٢ كه در اكتبر ٢٠٠٣ معرفي شد، حداكثر مسافت قابل دسترسي را به بيش از ٦ كيلومتر رساند. افزايش كارآيي در استانداردهاي فوق در واقع انعكاسي از نياز استفاده‌كنندگان و فراهم‌كنندگان خدمات ADSL درارتباط با افزايش نرخ گذردهي و مسافت قابل‌استفاده مي‌باشد. سرعت بالاي اين گروه از مودمهاي DSL، به فراهم‌كنندگان خدمات، امكان ارائه خدماتي همچون ويدئوي OnLine را مي‌دهد.

با وجود ارتقاء صورت گرفته، مودمهاي جديد به طور كامل با مودمهاي نسل پيشين خود سازگار مي‌باشند. به اين ترتيب فراهم‌كنندگان خدمات نيازي به جايگزيني سيستمهاي موجود خود ندارند و امكان توسعه تدريجي را مي‌يابند. **جدول ١** خلاصه‌اي از استانداردهاي اوليه و جديد ADSL را نشان مي‌دهد.

بهبود كارآيي

ADSL2 به شكلي طراحي شده كه در خطوط مخابراتي و با وجود تداخلات ناشي از مكالمات تلفني به نرخ گذردهي و مسافت بيشتري دست يابد. بهبود در تكنيك مدولاسيون، كاهش سرباره، بهره‌وري بيشتر در مكانيسم كدينگ، بهبود فرايند آماده‌سازي مودم، ارتقاء الگوريتمهاي پردازش سيگنال و كاهش در نسبت لازم براي سيگنال به نويز (SNR) برخي از تغييرات انجام گرفته جهت دستيابي به اهداف فوق مي باشند.



ميزان افزايش كارايي در مودم هاي ADSL2

كاهش اتلاف در پهناي باند

در مودمهاي معمولي ADSL، سرباره‌هاي ارتباطي از يك مقدار ثابت برخوردار مي‌باشند و در مجموع Mbps٣٢ از ظرفيت گذردهي را به خود اختصاص مي‌دهند. اين مقدار سرباره در مسافت‌هاي طولاني كه ظرفيت گذردهي تا Kbps١٢٨ كاهش مي‌يابد، به معني اتلاف ٢٥ درصدي خواهد بود. در مقابل در مودمهاي جديد، مقدار سرباره متناسب با نوع كاربرد و شرايط خط ارتباطي از Kbps٤ تا Kbps٣٢ انتخاب مي‌گردد كه تا ٨ برابر كاهش اتلاف را نشان مي‌دهد.

به طور همزمان، به كارگيري تكنيك كدينگ Reed-Solomon در مودمهاي جديد، بهره‌وري كدينگ را افزايش داده است و به كاهش پديده انعكاس در انتهاي خطوط و همچنين كاهش تداخل ناشي از امواج راديويي AM كمك مي‌كند.

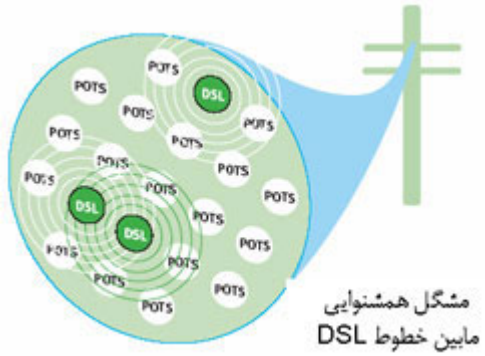
افزايش كارآيي كدينگ و كاهش اتلاف به افزايش نرخ گذردهي در مودمهاي ADSL ٢ نسبت به انواع پيشين منجر گرديده است.

افزايش نرخ گذردهي در مسافت‌هاي بالاي ۵ كيلومتر در حد Kbps۵۰ مي‌باشد و افزايش مسافت در حد ۱۸۰ متر مي‌باشد كه در مجموع فضاي قابل پوشش را تا ٦درصد افزايش مي‌دهد.

ساير ويژگي‌ها

- **تشخيص خودكار:** تشخيص خودكار كارآيي در مودم ADSL ۲ به مراتب بهتر از سلف خود انجام مي‌گيرد، به اين ترتيب كه مودم‌هاي هر دو طرف ارتباط قادر به اندازه‌گيري ميزان نويز، شدت تضعيف و نسبت سيگنال به نويز مي‌باشند. اطلاعات فوق در اختيار نرم‌افزار مديريت شبكه قرار مي‌گيرد تا در انجام فرايند نصب و خدمات پس از نصب شركت‌هاي فراهم‌كننده خدمات به كارگرفته شود.
- **شروع سريع:** آغاز به كار در ADSL ۲ بسيار سريعتر از گونه‌هاي پيشين و در مدت ۳ ثانيه انجام مي‌گيرد، درصورتي‌كه همين زمان در مورد مودم‌هاي ADSL در حدود ۱۰ ثانيه است.
- **ديتاي اختصاصي:** يك گزينه اختياري در ADSL ۲ وجود دارد كه استفاده از پهناي باند تلفني (POTS) را براي ارسال ديتا در جهت ارسال (Upstream) امكانپذير مي‌كند. اين گزينه براي مكان‌هايي كه داراي دو يا چند خط تلفن مي‌باشند و نيازي به استفاده از قابليت تلفني ADSL ۲ ندارند، مفيد خواهد بود.

بهبود در مديريت توان الكتريكي



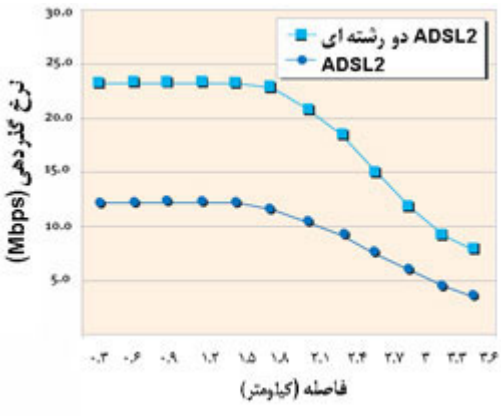
نسل اول مودم‌هاي ADSL در تمام مدت با حداكثر توان مصرفي كار مي‌كنند كه اتلاف انرژي و افزايش حرارت از نتايج آن است. در مقابل ADSL ۲ مانند يك كامپيوتر شخصي قادر است به حالت آماده‌باش(Stand by) درآيد و مصرف توان را به حداقل برساند. در اين حالت، مودم علاوه بر صرفه‌جويي در مصرف انرژي، حرارت كمتري نيز توليد مي‌كند كه به كارگيري آن را در ايستگاه‌هاي مركزي آسانتر مي‌سازد. مديريت توان در مودم‌هاي ADSL ۲ داراي دو سطح عملياتي L ۲ و L ۳ مي‌باشد. انتخاب اينكه مودم در كدام حالت (عادي يا آماده‌باش) كاركند، با توجه به نرخ ترافيك عبوري يا بدون فعاليت‌ماندن مودم براي يك مدت مشخص تعيين مي‌گردد.

براي مثال زماني كه فايلي بزرگ از روي اينترنت بارگذاري مي‌گردد، ADSL ۲ در حالت توان كامل قرار مي‌گيرد تا گذردهي را به حداكثر برساند. اما با كاهش ترافيك (براي مثال در زماني كه يك صفحه وب معمولي مطالعه مي‌شود) مودم به حالت L ۲ فرو مي‌رود و توان مصرفي را كاهش مي‌دهد. البته مودم همواره آماده است تا به سرعت به حالت عادي بازگردد و تمام اين تغييرات بدون درگير شدن برنامه‌هاي كاربردي و بدون از دست رفتن حتي يك بيت از اطلاعات انجام مي‌گيرد. درصورتي‌كه مودمي براي مدتي خاص بدون هر گونه ترافيكي باقي بماند، مي‌تواند به پايين‌ترين حالت مصرف انرژي يعني L ۳ برود. در اين حالت حدود ۳ ثانيه براي بازگشت مجدد به وضعيت عادي زمان لازم است.

تطبيق نرخ انتقال

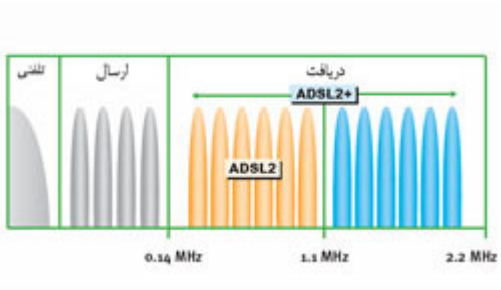
خطوط تلفن معمولاً در قالب كابل‌هاي چندرشته‌اي (با حداقل ۲۵ رشته‌سيم) به كار گرفته مي‌شوند. يكي از آثار فيزيكي به كارگيري كابل‌هاي چندرشته‌اي، امكان القاي الكترومغناطيسي علائم الكتريكي يك رشته سيم در ديگري است كه به همشنوايي (Crosstalk) موسوم است. همشنوايي به همراه رطوبت، تغيير درجه حرارت و تداخلات ناشي از راديوهاي AM، از مهمترين عوامل كاهش كارآيي در خطوط ADSL محسوب مي‌گردند.

ADSL2 به كمك يكي از قابليت‌هاي خود موسوم به <تطبيق پيوسته نرخ انتقال> بدون ايجاد تداخل در فرايند ارائه خدمات، شرايط كانال ارتباطي را تشخيص داده و نرخ انتقال را با شرايط فوق هماهنگ مي‌كند. براي مثال شروع به كار فرستنده يك ايستگاه راديويي محلي مي‌تواند شرايط جديدي را براي خطوط مخابراتي آن منطقه ايجاد كند كه در اين صورت ۲ ADSL بدون آنكه كاربر را متوجه سازد، نرخ انتقال خود را با شرايط فوق تطبيق مي‌دهد.



افزايش نرخ گذر با استفاده از ADSL2 دو رشته اي

ADSL2 چندتايي (Bounded ADSL2)

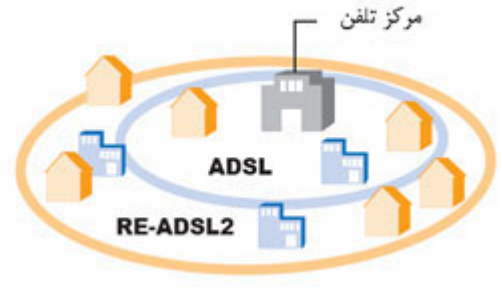


فراهم كنندگان خدمات طيف گسترده‌اي از مشتريان را پوشش مي‌دهند و بديهي است كه با نيازها و خواسته‌هاي متفاوتي روبرو باشند، مشتريان تجاري معمولا خواستار نرخ گذردهي بالاتر از مقادير استاندارد مي‌باشند. خوشبختانه ۲ ADSL اين قابليت را دارد كه با به كارگيري همزمان چند رشته سيم به نرخ بالاتري دست يابد. تكنيك به كار گرفته شده اقتباسي از تكنيك مالتي پلكس وارونه در شبكه‌هاي ATM مي‌باشد. در اين تكنيك اطلاعات در مبداء به قطعاتي تقسيم مي‌شوند كه هر يك برروي يكي از كانال‌هاي موجود ارسال مي‌گردد، در گيرنده فرايند عكس انجام مي‌پذيرد و با سرهم كردن قطعات فوق، اطلاعات اوليه بازسازي مي‌شود.

طيف فركانسي مودم هايADSL

روش‌هاي انتقال همزمان صدا بر روي ADSL2

يكي از ويژگي‌هاي مودم‌هاي ADSL، تقسيم طيف فركانسي يك خط تلفن به دو بخش مستقل با مشخصات متمايز مي‌باشد كه اين دو بخش به مكالمات تلفني (POTS) و تبادل ديتا اختصاص دارند. به اين ترتيب دارندگان مودم‌هاي ADSL قادر به استفاده همزمان از خط تلفن خود خواهند بود، بدون آنكه اختلالي در فرايند ارسال و دريافت ديتا ايجاد كنند.



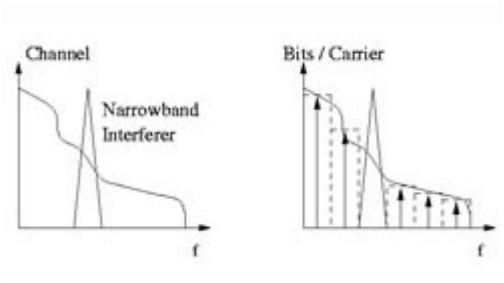
مودم‌هاي ADSL2، علاوه بر اين، امكان برقراري ارتباطات صوتي از طريق تكنيكي موسوم به <صداي كانالیزه شده بر روي> (CVoDSL DSL) را فراهم مي‌كند. CVoDSL يك كانال به پهناي ٦٤ كيلو هرتز را از داخل پهناي باند مربوط به ۲ ADSL جدا مي‌كند و به صورت يك خط معمولي تلفني به كار مي‌گيرد. تكنيك فوق از نوآوري‌هاي ۲ ADSL مي‌باشد و به‌طور كلي با تكنيك‌هاي معمول انتقال صوت برروي مودم‌هاي DSL (مانند VoIP يا VoATM) كه مبتني‌بر تبديل صوت به ترافيك بسته‌اي ديتا مي‌باشند، متمايز است.

با استفاده از تكنيك CVoDSL صوت به صورت دست نخورده و بدون تبديل باقي مي‌ماند و سرويس‌دهنده قادر خواهد بود تا ٤ خط تلفني را بر روي يك خط ۲ ADSL ايجاد كند.

توسعه فضاي تحت پوشش در ADSL2

گسترش يافته

تكنيك انتقال در مودم‌هاي ADSL



تكنيك انتقال مورد استفاده در مودم هايADSL ، تكنيك (Discrete Multition) DMT مي‌باشد .DMT فضاي فركانسي كانال را به تعدادي ريزكانال با عرض باند ٤ KHZبراي هريك تقسيم مي‌كند. تعداد اين زيركانال‌ها كه اصطلاحاً تن (Tone) ناميده مي‌شوند، براي استانداردهاي سري ADSL2 به ٥١٢ عدد بالغ مي‌گردد. به طور معمول تن‌هاي ۱

الي ٥ خاص ارتباطات تلفني مي‌باشند. از تن ٦ الي ٣١ و يا ٦٤ براي ارسال ديتا استفاده مي‌شود و باقي تن‌ها به دريافت ديتا اختصاص دارند. يكي از قابليت‌هاي ADSL به‌كارگيري انعطاف‌پذير تن‌ها متناسب با كاربرد و شرايط كانال مي‌باشد.

ADSL2+

سير پيشرفت مودم‌هاي ADSL با معرفي (G.299.5) +ADSL2 باز هم كامل‌تر گرديد. در +ADSL2 افزايش دو برابري پهناي باند از ١/١ مگاهرتز به ٢/٢مگاهرتز، در مسافت‌هاي كمتر از ١٥٠٠ متر، نرخ دريافت را تا دو برابر افزايش مي‌دهد. طيف فركانسي بزرگتر، همچنين +٢ ADSL را نسبت به معضل همشنوايي مقاومتر مي‌كند.

ضمائم استاندارد

كاربردها و شرايط خاص، مشخصات ويژه‌اي را طلب مي‌كند كه در استانداردهاي اصلي ADSL وجود ندارد. ضمائم به منظور پوشش‌دادن به اين شرايط خاص ايجاد گرديده‌اند. به طور كلي هر ضميمه از بخشي از پهناي باند ADSL براي كاربردي خاص استفاده مي‌كند و بسياري از ضمائم اوليه ADSL براي استانداردهاي نسل جديد ٢ ADSL و +٢ ADSL نيز كاربرد دارند.

ضميمه A: متداولترين گونه ADSL مي‌باشد كه در آمريكاي شمالي، اروپا و آسيا كاربرد دارد. در اين ضميمه، بخش پايين پهناي باند براي ارتباطات عادي تلفني و بخش‌هاي بعدي به ترتيب براي ارسال و دريافت ديتا مورد استفاده قرار مي‌گيرد.
ضميمه B: شبيه به گونه A مي‌باشد، با اين تفاوت كه براي خطوط تلفن ISDN كاربرد دارد. تلفن ISDN نسبت به تلفن عادي از پهناي باند بيشتري استفاده مي‌كند. ضميمه B به طور گسترده‌اي در كشور آلمان به كار گرفته شده‌است.
ضميمه C: خاص سيستم مخابرات تلفني كشور ژاپن طرح شده است كه در واقع گونه خاصي از استاندارد ISDN

مي‌باشد.
ضميمه I: نسخه جديدي از ضميمه C مي باشد كه نرخ گذردهي را

درسمت دريافت تا دو برابر افزايش مي‌دهد.
ضميمه J: اين گونه به صورت كاملاً ديجيتالي كار مي‌كند و فضاي اختصاص يافته به ارتباطات تلفني را براي افزايش نرخ گذردهي ديتا به كار مي‌گيرد.
ضميمه L: يكي از جديدترين ضمائم استاندارد ٢ ADSL مي‌باشد كه در بازار با نام ٢ ADSL <گسترش‌يافته (RE-ADSL2)> شناخته مي‌شود. RE-ADSL2 با افزايش توان ارسال علائم، بر تضعيف حاصل از خطوط طولاني غلبه مي‌كند. نتيجه حاصل، افزايش ٣٧ درصدي در فضاي قابل پوشش مي باشد. البته توان اضافي
RE-ADSL در فواصل كوتاهتر نيز به افزايش نرخ گذردهي نسبت به استاندارد پايه ADSL كمك مي‌كند.

پیش‌بینی‌ها

از آنجایی‌که ارتقاء استاندارد ADSL به سطح ۲ ADSL و +ADSL2 در ITU ناشی از خواست فراهم‌کنندگان خدمات و استفاده‌کنندگان این فناوری بوده است، بدیهی است که کلیه پیش‌بینی‌ها انتظار تکرار موفقیت ADSL را در انواع جدید آن نیز دارند.

ویندوز "Longhorn" چیست؟

مایکروسافت اکنون در حال تولید نسخه جدید ویندوز با کدی به نام "Longhorn" می‌باشد. "Longhorn" به منظور ایجاد پایه و اساسی برای ابداع یك صنعت جدید طراحی شده است که در نهایت شرکت‌های بازرگانی را قادر به استفاده از تکنولوژی به نحو احسن و رویارویی با موانع کمتری می‌سازد. و همچنین به مشتریان امکان می‌دهد تا مزایای بیشمار و گسترده این تکنولوژی را بهتر بشناسند.

"Longhorn" به پیشرفت و بهینه‌سازی موارد مهم ذیل کمك می‌کند:

* تمرکز دقیق و جدی روی اصول بنیادی و اساسی سیستم عامل از جمله افزایش سطح قابلیت اطمینان، عملکرد و کارآیی و سهولت استفاده.

* کمك هر چه بیشتر به کاربران کامپیوتر به منظور عملکرد هوشیارانه و کسب تجربیات جدید و جالب بدست کاربران خانگی.

* پلاتفرم توسعه دهنده نسل بعدی که توسعه دهندگان را در ایجاد برنامه‌های کاربردی موفق یاری می‌دهد.

ما در حال حاضر از نزدیك با مشتریان خود گفتگو کرده و نظرات آنها را می‌شنویم. چه شما از یك کامپیوتر در خانه یا در محل کار استفاده کنید یا عضوی از گروه توسعه دهندگان ویندوز باشید، "Longhorn" مطمئنا ابتکارات عمل بی نظیر و بی‌سابقه‌ای را در اختیار شما می‌گذارد که در واقع دنیای کاربران ویندوز را به دوران و دهه دیجیتال رهنمون می‌سازد.

مایکروسافت تاریخ دقیق دستیابی گسترده به سیستم عامل کلاینت ویندوز "Longhorn" را به ۲۰۰٦ تغییر و اعلام نموده است. تکنولوژی‌های توسعه دهنده ویندوز WinFX نیز برای ویندوز Windows Server 2003 و XP در دسترس خواهد بود.

ردموند، واشنگتن، ۲۷ آگوست سال ۲۰۰٤: شرکت مایکروسافت اعلام کرده است که امکان دسترسی گسترده به سیستم عامل کلاینت (سرویس گیرنده) ویندوز با کد "Longhorn" در سال ۲۰۰٦ فراهم خواهد شد و عناصر مهم این پلاتفرم توسعه دهنده ویندوز WinFX در "Longhorn" برای ویندوز XP و Windows Server 2003 نیز در دسترس خواهد بود.

"Longhorn" قابلیت بهره وری کاربر را افزایش داده و قابلیت‌های مهم جدیدی را برای توسعه دهندگان نرم‌افزار به ارمغان می‌آورد و همچنین میزان اهمیت، کاربرد و قابلیت اطمینان آنرا بالا می‌برد.

بیل گیتس، رئیس بخش نرم‌افزار شرکت مایکروسافت گفت، دستیابی مشتریان به "Longhorn" در سال ۲۰۰٦ پیشرفت‌های مهمی را در زمینه‌های کارآیی، ایمنی و قابلیت اطمینان ببار آورده و به ایجاد هر چه سریعتر برنامه‌های کاربردی جدید و مناسب بدست توسعه دهندگان صنعت کمك می‌کند.

مایکروسافت پس از عرضه "Longhorn" یك سیستم فرعی ذخیره‌سازی ویندوز را با کدی به نام "WinFX" در اختیار مشتری قرار می‌دهد. این سیستم ذخیره‌سازی جدید یك سازمان داده و قابلیت‌های مدیریت پیشرفته‌ای را فراهم می‌سازد که با در دسترس قرار گرفتن کلاینت "Longhorn" در ابتدا بصورت بتا (آزمایشی) مورد استفاده قرار می‌گیرد.

Jim Allchin، معاون گروه پلاتفرم‌های شرکت مایکروسافت گفت، مشتریان ما به طور واضح بیان کرده‌اند که خواهان افزایش هر چه بیشتر میزان تولید و بهره‌وری و همینطور کاربرد آسانتر و قابلیت اطمینان و امنیت روزافزون هستند، همچون سایر ابتکارات عملی که اکنون آنها را بکار می‌بندیم. جهت برخورداری مشتریان از این ویژگی‌ها باید چندین معامله را انجام دهیم. مصرف‌کنندگان و OEMها (سازندگان تجهیزات اصلی) نیز بدنبال این ویژگی‌ها در چهارچوب زمانی مناسبی هستند. دید بلند مدت ما به پلاتفرم ویندوز نیز همینطور باقی خواهد ماند.

Jeff Truax، مدیر IT شرکت Frontier Airlines گفت: مطالبی که مایکروسافت اکنون اعلام می‌دارد امکان دستیابی "Longhorn" را سریعتر می‌سازد. به نظر می‌رسد که با پیشرفت قدرت تولید و بهره‌وری و همچنین امنیت بیشتر و تمرکز روی نکات و اصول اساسی، بتوان مزایا و بهره بیشتری در تجارت کسب نمود.

در جلسه‌ای که با حضور صدها توسعه دهنده برتر شرکت‌های سراسر دنیا انجام شد، مایکروسافت اعلام نمود که تکنولوژی‌های توسعه دهنده ویندوز WinFX از جمله سیستم فرعی جدید عرضه شده با کد "Avalon" و سیستم فرعی جدید برقراری ارتباط با کد Indigo در سال ۲۰۰۶ برای ویندوز XP و Windows Server 2003 مایکروسافت در دسترس خواهند بود، که در نهایت زمینه مناسب برای توسعه دهندگان را جهت نوشتن برنامه‌هایی که روی صدها میلیون کامپیوتر قابل اجرا خواهند بود فراهم کرده و گسترش می‌دهد ودر نتیجه تجربیات کاربران این سیستم عامل‌ها نیز بالا می‌رود.

Scott Borduim مقام ارشد این تکنولوژی در شرکت Autodesk گفت، Avalon و Indigo هر دو به ما امکان می‌دهند تا برنامه‌های کاربردی دلخواه خود و مشتریان کنترل کننده چرخه حیات آنها را ایجاد نماییم. در دسترس بودن Avalon و "Longhorn" برای ویندوز XP همچون "Longhorn" به ما امکان می‌دهد تا این تکنولوژی‌ها را سریعتر کشف نموده و مورد بهره‌برداری قرار دهیم.

Leslie House، معاون Vivendi Universal Games Knowledge Adventure Studio گفت، ظهور هسته پلاتفرم جدید WinFX در ویندوز XP و ویندوز ۲۰۰۳ به برنامه‌های کاربردی WinFX امکان می‌دهد تا پایگاه‌های نصب شده گسترده‌تری را در برگرفته و پلاتفرم بهتر و جذابتری را برای نرم‌افزار آموزشی ما ایجاد نماید.

"Avalon" يك سيستم فرعی گرافيكی است كه سازندگان را قادر به ايجاد برنامه‌هايی می‌سازد كه ميزان تجربيات كاربران را بالا می‌برد.

"Indigo" نيز روش جديدی برای ايجاد و اجرای سيستم‌های مرتبطی است كه بر اساس معماری مبتنی بر سرويس‌های وب ساخته شده است. پشتيبان سرويس‌های وب پيشرفته در "Indigo" پيام‌های قابل تبادل مطمئن‌تر و ايمن‌تر و همچنين قابليت عمل گسترده‌تر در چند محيط را فراهم می‌سازد.

بيانات كنونی فقط به سيستم عامل كلاينت "Longhorn" مربوط می‌شود. قابليت دستيابی به سيستم عامل سرور ويندوز "Longhorn" نيز تا سال ۲۰۰۷ ادامه خواهد يافت

را روي اينترنت قرار دهيد؟ چگونه مي توانيد سايت خود

اشاره :

هنگامي كه طراحي و ساخت سايت خود را با مهارت به پايان برديد، زمان آن فرا مي‌رسد كه بگذاريد مردم نيز آن را ببينند. در اين مقاله مي‌بينيد كه چگونه مي‌توانيد سايت خود را به سادگي و بدون مشكلات و ايرادات بي‌دليل بر روي اينترنت قرار دهيد. زماني كه موعد انتشار سايتتان بر روي اينترنت فرا مي‌رسد احتمالاً بيشتر وقتتان را صرف محتواي صفحات خواهيد كرد تا نحوه دسترسي آن به صورت آن‌لاين. اما همين نحوه انتشار و اصول آن است كه تفاوت يك سايت حرفه‌اي را از يك سايت غيرحرفه‌اي نشان مي‌دهد.

نحوه كنار هم قرار دادن فايل‌ها و صفحات و اتصالات بين آن‌ها مي‌تواند تأثير زيادي بر كارايي يك سايت داشته باشد. به طوري‌كه اگر لينك‌هاي بين صفحات را به صورتي غير كارا ايجاد كنيد، مرورگر اينترنت مجبور مي‌شود براي گرفتن هر صفحه، دو بار درخواست ارسال نمايد.
هميشه سعي كنيد صفحات وب خود را به ساده‌ترين روشي كه مي‌توانيد بر روي سرويس‌دهنده قرار دهيد، و موقع اتمام كار و انتقال فايل‌ها به سرويس‌دهنده از ايجاد تغييراتي كه باعث از كار افتادن كل سايت مي‌گردد اجتناب كنيد. سعي كنيد سايت خود را به نحوي بسازيد كه همه بازديدكنندگان بتوانند آن را به همان صورتي كه ساخته‌ايد و با همان قابليت‌ها و ويژگي‌ها ببينند.
به خاطر داشته باشيد كه مجبور نيستيد فضاي وب مورد نياز سايت خود را از ISP خود دريافت كنيد. به علاوه فضاهاي مجاني نيز به ندرت تمامي ابزارهاي لازم را در بردارند. به خصوص اگر يك سايت جذاب و پر بازديدكننده ايجاد كرده و براي استقرار آن از چنين فضاهاي مجاني استفاده كرده باشيد، مي‌توانند به سادگي شما را در لحظه نياز تنها بگذارند. به هر حال اگر واقعاً قصد انتشار سايت خود را داريد يا صرفاً در حال بررسي گزينه‌هاي مختلف هستيد، ساخت صفحات وب به صورتي كارا و قابل حمل، نتيجه بيشتري خواهد داشت.

FTP دو مرحله‌اي

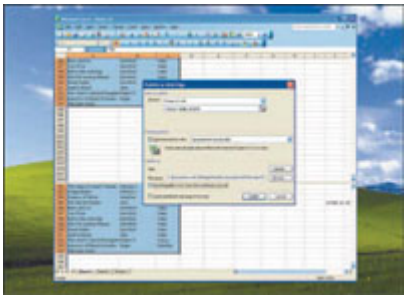
بسياري از نرم‌افزارهاي طراحي و ويرايش صفحات وب، قادر به انتقال و بارگذاري آن‌ها بر روي سرويس‌دهنده نيز مي‌باشند (كه به اين كار انتشار سايت يا Publish كردن سايت گفته مي‌شود). اين بدين معني است كه تغييراتي كه به سايت خود مي‌دهيد به سرعت به سايت بارگذاري شده بر روي سرويس‌دهنده انتقال داده شده و اعمال مي‌شود. اگر ترجيح مي دهيد همه چيز را دو بار كنترل كنيد، نرم‌افزار طراحي وب خود را به گونه‌اي تنظيم كنيد كه به جاي انتقال و انتشار مستقيم صفحات به سرويس‌دهنده راه دور، آن‌ها را به صورت محلي بر روي هارددیسك منتشر كند و پيش از اين كه آن‌ها را توسط FTP به سرويس‌دهنده راه دور انتقال دهيد، آن‌ها را در مرورگر اينترنت خود مشاهده و كنترل كنيد كه آيا همه چيز درست است يا خير. سعي كنيد پوشه سايت منتشرشده را در ريشه درايو قرار دهيد تا براي بارگذاري آن‌ها بر روي سرويس‌دهنده، مجبور نباشيد در درختواره پوشه‌هاي درايو خود به دنبال آن بگرديد.

FTP متني و دودويي

هنگامي كه صفحات HTML (يا CSS و فايل‌هاي اسكريپتي) را توسط FTP به سرويس‌دهنده انتقال مي‌دهيد به خاطر داشته باشيد كه اين انتقال در مد يا حالت متن انجام شود تا كاراكترهاي انتهاي خطوط و تعيين‌كننده خطوط جديد در اين فايل‌ها به صورت صحيح فرستاده شده و ساختار اين فايل‌ها به صورت درست منتقل شود. در غير اين صورت متن داخل فايل‌ها به خطوطي بسيار كوتاه يا بسيار بلند تبديل مي‌گردد. در حالت انتقال فايل‌ها در مد متن، سه استاندارد مختلف براي انتقال كاراكترهاي سر سطر وجود دارد. استاندارد مناسب را انتخاب كنيد. همچنين مراقب كاراكترهاي اضافي نرم‌افزارهاي واژه پرداز باشيد. از سوي ديگر، فايل‌هاي گرافيكي، تصاوير، فايل‌هاي صوتي و اجرايي و به عبارت ديگر هر چيزي كه نمي‌توانيد آن را در Notepad باز كنيد بايد در مد يا حالت دودويي يا باينري منتقل شوند. اگر نوع انتقال را براي هر قالب فايل بر اساس پسوند آن‌ها از قبل براي نرم‌افزار FTP مشخص كنيد نيازي نخواهيد داشت مد انتقال را هر بار به صورت دستي تغيير دهيد.

ديواره آتش

اگر سايتتان را از كامپيوتر محل كار روزآمد كرده و به سرويس‌دهنده راه دور منتقل مي‌كنيد، احتمالاً كامپيوتر مزبور داراي يك ديواره آتش مي‌باشد كه نقل و انتقالات فايل‌ها را بين كامپيوتر شما و اينترنت زير نظر دارد و جلوي دسترسي‌هاي غير مجاز را مي‌گيرد. حال چه اين دسترسي از بيرون به كامپيوتر شما صورت گرفته باشد و چه از درون كامپيوتر شما به دنياي بيرون صورت گرفته باشد (كه ارتباط نرم‌افزار FTP شما با سرويس‌دهنده راه دور از ديد فايروال نيز در زمره مورد دوم قرار مي گيرد.) لذا اگر نرم‌افزار FTP شما قادر به برقراري ارتباط با سرويس‌دهنده راه دور نمي‌باشد يكي از دلايل آن مي‌تواند اين قضيه باشد. در اين صورت به منظور ارتباط با سرويس‌دهنده راه دور و انتقال فايل‌ها مجبور خواهيد بود براي عبور از ديواره آتش، در حالت غيرفعال كار كنيد. اين حالت را در تنظيمات اتصال خود مشخص كنيد تا مجبور نباشيد هر بار آن را تغيير دهيد.



در نرم‌افزار Excel با فعال نمودن قابليت ذخيره خودكار فايل صفحه گسترده به صورت يك صفحه وب نيازي نخواهيد داشت خودتان هر بار به طور دستي اين كار را انجام دهيد و مي‌توانيد در وقتتان صرفه‌جويي كنيد .

انتشار خودكار

تنها نرم‌افزارهاي طراحي وب قادر به ايجاد فايل‌هاي HTML نيستند. شما به عنوان نمونه مي‌توانيد در نرم‌افزار Excel نيز فايل جداول خود را به صورت HTML تبديل كنيد. تنها كافي است خانه‌هاي مورد نظر خود را انتخاب كرده و گزينهSave As Web Page<File را انتخاب كنيد و در پنجره ظاهر شده، دكمه راديويي ذخيره تمام خانه‌ها يا خانه‌هاي انتخاب شده را تنظيم كنيد. با انتخاب گزينه interactivity Add صفحه‌اي با كنترل‌هاي پايه‌اي اكسل ايجاد خواهد شد. پس از آن، دكمه Publish را كليك كنيد. در همين پنجره در صورتي كه مايل باشيد مي‌توانيد گزينهAutoRepublish everythime this workbook is saved را علامت بزنيد كه با اين كار، نيازي نخواهيد داشت به هنگام ذخيره فايل خود، هر بار اين مسير را تكرار كنيد و نرم‌افزار اكسل هنگامي كه شما فايل خود را ذخيره مي كنيد، به طور خودكار فايل HTML آن را نيز ايجاد مي‌كند.

كشيدن و انداختن

شما مي‌توانيد براي انتقال فايل‌هاي سايت خود به سرويس‌دهنده، به جاي يك نرم‌افزار FTP جداگانه، از مرورگر اينترنت نيز استفاده كنيد. براي اين كار كافي است آدرس ftp سرويس‌دهنده راه دور را در نوار آدرس مرورگر تايپ كرده و كليد Enter را بزنيد. پس از آن يك پنجره in Log ظاهر مي‌شود كه مي‌توانيد نام كاربري و كلمه عبور خود را وارد كنيد. پس از آن، پوشه‌هاي سايت شما بر روي سرويس‌دهنده راه دور ظاهر مي‌شود. درست به همان شكلي كه پوشه‌هاي يكي از درايوهاي محلي كامپيوتر خودتان ديده مي‌شود. مي‌توانيد هر فايل يا پوشه‌اي را كه مايل باشيد تغيير نام دهيد يا آن‌ها را حذف كنيد و حتي مي‌توانيد درست مانند كشيدن و انداختن از پنجره يك درايو در كامپيوتر خود به پنجره درايوي ديگر، فايل‌ها را از پوشه سايت در حال طراحي در كامپيوتر خود، بر داشته و آن را در داخل پنجره مرورگر بيندازيد. مرورگر خودش فايل‌ها را به سرويس‌دهنده انتقال خواهد داد. ارتباط شما با سرويس‌دهنده راه دور تا زماني كه پنجره‌هاي مرورگري كه به سرويس‌دهنده راه دور به صورت FTP متصل شده‌اند باز است برقرار مي‌ماند و پس از بستن همه اين پنجره‌ها، مرورگر، ارتباط را خاتمه مي دهد (ارتباط FTP ايجاد شده با

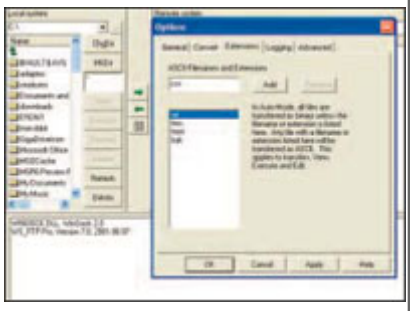
اين نشاني مانند يك آدرس پست الكترونيك عادي به نظر مي‌رسد و عمل مي‌كند اماSpammer ها براي به‌دست آوردن آن دچار مشكل خواهند شد، چرا كه اين آدرس پست الكترونيك، در حقيقت يك تصوير است كه با تكه‌اي كد Javascriptهمراه شده است .

سرويس‌دهنده راه دور و نه ارتباط با اينترنت).

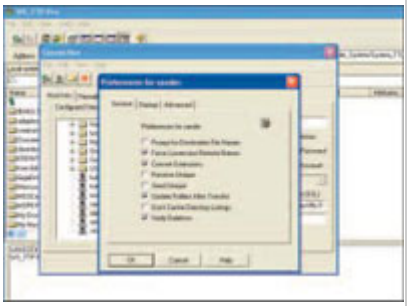
راهنماي قدم به قدم

FTPرا خودكار كنيد

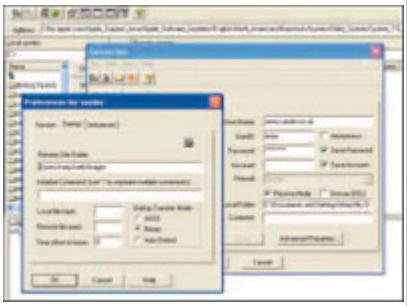
براي اتصال FTP تنظيمات كاملي را مشخص سازيد تا فايل‌هاي شما در محلي درست بر روي سرويس‌دهنده FTP قرار گرفته و با نامي درست منتقل شوند.



1پس از اين كه يك اتصال براي سايت خود ايجاد كرديد، پوشه مبدا، يعني محلي كه فايل‌ها و صفحات سايت شما بر روي كامپيوتر شما قرار دارد را مشخص كنيد. بر روي دكمه Advanced Properties كليك كنيد و در برگه Startup ، پوشه مقصد، يعني پوشه‌اي كه فايل‌ها و صفحات، پس از انتقال به سرويس‌دهنده در آن قرار خواهند گرفت را تعيين كنيد. مد يا حالت انتقال فايل‌ها را بر روي Auto Detect قرار دهيد، مگر اين كه به مشكل برخورد نماييد.



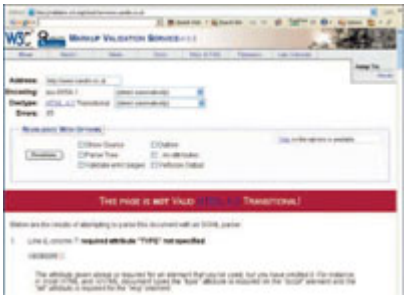
2هر سرويس‌دهنده‌اي با سرويس‌دهنده ديگر متفاوت است. لذا براي به دست آوردن يك نتيجه به خصوص، بايد گزينه‌هاي مختلفي را تنظيم نماييد. در زبانه Sessionمي‌توانيد تعيين كنيد كه آيا نام‌ها تماماً با حروف كوچك ارسال شوند يا خير و يا پسوندها در هر جلسه اتصال و انتقال فايل‌ها تبديل شوند يا خير. براي اين كار گزينه Tools > Options > Convert را انتخاب كنيد.



3به جاي انتخاب مد انتقال متن يا ASCII و دودويي به صورت مستقل و جداگانه براي هر فايل، از منوي Tools زير منوي Optionsو در آن، گزينه Extensions را انتخاب كنيد و تمامي پسوندهايي را كه قرار است در حالت متني يا دودويي انتقال يابند، تعيين‌كنيد. نرم‌افزار WS FTP Proفايل‌هاي در حال انتقال را نيز به طور خودكار براي شما مرتب مي‌كند.

استفاده از وبلاگ‌ها

استفاده از يك سايت سرويس‌دهنده وبلاگ روش بسيار آساني براي روزآمد كردن سايت است. چرا كه مي‌توانيد از ابزارهاي از قبل آماده شده توسط سرويس‌دهنده وبلاگ براي اين كار استفاده كنيد و متن جديد خود را به صفحه وب خود اضافه كنيد. و فرقي هم نمي‌كند كه از كجا و چگونه مطلب خود را براي سرويس‌دهنده پست كنيد. از طريق يك صفحه وب، از طريق پست الكترونيك در يك كافي‌نت يا از طريق سرويس ارسال پيام كوتاه موسوم به SMS در تلفن‌هاي همراه. سيستم موجود در سرويس‌دهنده وبلاگ پيام شما را گرفته و آن را به طور خودكار به صفحه وب شما اضافه مي‌كند. لذا مي‌توانيد سايتتان را از هر كجاي دنيا كه بخواهيد، بروز نماييد و مطالب جديد را به آن اضافه نماييد. براي اطلاع از نحوه به كارگيري مطالبي كه براي سايت خود پست نموده‌ايد، سري به اين نشاني بزنيد.



اطمينان حاصل كنيد كه كد HTML صفحه وب شما به خوبي نوشته شده است. بسياري از نرم‌افزارهاي ويرايشگر صفحات وب، هنگام طراحي صفحات وب، كدهاي HTML اضافي و به‌دردنخور در داخل آن‌ها قرار مي‌دهند كه باعث كند شدن روند بارگذاري صفحه در مرورگر مي‌گردد.

كنترل كنيد و باز هم كنترل كنيد

پس از اين كه تمامي صفحات سايت خود را به صورت دستي كنترل كرديد، اين كار را از طريق سرويس كنترل اعتباري كه به همين منظور و به صورت مجاني در سايت كنسرسيوم جهاني وب (W3C) قرار داده شده است نيز انجام دهيد. سايت W3C پس از بررسي سايت شما، اعلام مي‌كند كه آيا سايت داراي استانداردهاي مناسب يك سايت خوب مي‌باشد يا خير.

سايتتان را به‌صورت قابل دسترس براي همه افراد طراحي كنيد.

با به‌كارگيري نكاتي كه در سايت كنسرسيوم جهاني وب و در اين بخش قرار داده شده است صفحات سايت خود را به گونه‌اي بسازيد كه همه بازديدكنندگان، از جمله افراد داراي ناتوانايي‌هاي جسمي و معلول نيز بتوانند از آن استفاده كنند.

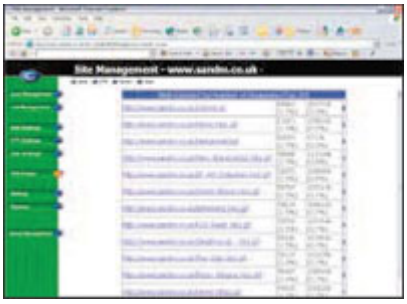
رنگ‌هايي را كه در سايتتان به كار برده‌ايد بررسي كنيد.

تعداد بسيار بسيار زيادي از مردم دچار كوررنگي هستند. اگر مي‌خواهيد ببينيد صفحاتي كه با مهارت و صرف وقت زياد، طراحي كرده‌ايد از ديد چنين افرادي چگونه به نظر مي‌رسد، صفحات خود را از طريق اين سايت بارگذاري كنيد و يا نكاتي را كه در آزمايشگاه رنگ‌ها ذكر شده است مطالعه كنيد تا از بازه رنگ‌هايي كه افراد داراي كوررنگي قادر به تشخيص آن‌ها هستند اطلاع پيدا كنيد.

اگر داراي مشكل كوررنگي هستيد ببينيد رنگ‌ها چگونه به نظر مي‌رسند و تأثير آن‌ها را بر صفحات سايت خود ببينيد.

از امتيازات ويژه‌اي كه سرويس‌دهنده در مورد زبان‌هاي برنامه‌نويسي تحت سرويس‌دهنده در اختيارتان قرار مي‌دهد اطلاع حاصل كنيد.

اگر قصد داريد اسكريپت‌هايي را كه به يك زبان تحت سرويس‌دهنده (مانند ASP) نوشته‌ايد بر روي سايت خود قرار دهيد، اطلاع حاصل كنيد كه آيا سرويس‌دهنده شما، زباني را كه شما با آن برنامه‌نويسي نموده‌ايد، پشتيباني مي‌كند يا خير (به عنوان مثال Perl يك زبان مشترك است كه تقريباً همه سرويس‌دهنده‌ها آن را پشتيباني مي‌كنند) و پيگيري كنيد كه چه مواردي را لازم است رعايت كنيد تا كدهايي كه نوشته‌ايد، واقعاً بر روي سرويس‌دهنده كار كند. اگر سرويس‌دهنده شما يك سرويس‌دهنده يونيكس باشد ممكن است قادر باشيد به آن telnet نماييد و از فرمان CHMOD استفاده نماييد. بيشتر شركت‌هاي فراهم كننده اينترنت اجازه نمي‌دهند كه خودتان چنين كاري را انجام بدهيد و لذا مجبوريد از خود آن‌ها در اين مورد بپرسيد كه سرويس‌دهنده، چه زبان يا زبان‌هايي را پشتيباني مي‌كند. اگر چنين است احتمالاً ممكن است محدوديت‌هاي ديگري هم در مورد اسكريپت‌هايي كه مي‌توانيد در سايتتان استفاده كنيد وجود داشته باشد. سعي كنيد پيش از اين كه يك اسكريپت پيچيده را بنويسيد در اين مورد كسب اطلاع كنيد.



گزارش‌هاي آماري سايتتان را با دقت دنبال كنيد و ببينيد چه كساني مراجعه مي‌كنند و قصدشان از بازديد سايت شما چه بوده است.

اندازه مناسبي را انتخاب كنيد

شما نمي‌توانيد انتظار داشته باشيد كه همه بازديدكنندگان سايت شما وضوح صفحه نمايش يكسان براي مشاهده آن استفاده نمايند يا همه، به هنگام بازديد از سايت شما، پنجره مرورگر خود را در حالت حداكثر اندازه آن مورد استفاده قرار داده باشند. از اين رو سايت خود را در دقت‌هاي مختلف صفحه نمايش بررسي كرده و ظاهر آن را ببينيد. اگر نرم‌افزار طراحي سايت شما قادر به پيش نمايش صفحات در دقت‌هاي مختلف صفحه نمايش نيست، از ميله جستجوي سريع شركت DQSD كه آدرس سايت آن www.dqsd.net مي‌باشد استفاده نماييد. اين ميله، پس از نصب در ميله وظايف ويندوز قرار مي‌گيرد و علاوه بر مهيا نمودن امكان جستجو از طريق Google براي شما و چندين سايت به درد بخور ديگر، مي‌تواند يك سايت را در پنجره مرورگري با اندازه‌اي مشخص باز نمايد. به طوري كه مثلاً چنانچه قصد جستجو به دنبال چيزي را از طريقGoogle داشته باشيد، ديگر نيازي نداريد خودتان يك پنجرهExplorer Inetrnet باز كرده، سايت Google را بياوريد و در جعبه متن جستجو، نام چيزي را كه به دنبال آن بگرديد تايپ كرده و كليد Enter يا دكمه Search را بزنيد. ميله جستجوي سريع DQSD خودش همه اين كارها را براي شما انجام مي‌دهد. براي مشاهده يك سايت مانند http://www.mysite.com در يك وضوح به خصوص نظير X600۸۰۰ نيز كافي است در جعبه متن ميله DQSD بنويسيد " http://www.mysite.com winres 600X800 " پس از آن، اين ميله يك پنجره مرورگر با اندازه مشخص شده باز كرده و سايت درخواستي شما را در آن نشان مي‌دهد.

تنظيمات ميزباني وب

شما مجبور نيستيد ميزباني سايت وب خود را به فراهم كننده اتصال به اينترنت خود بسپاريد. در زير، نكاتي ذكر مي‌شود كه مي‌توانيد آن‌ها را هنگام انتخاب يك ميزبان در نظر داشته باشيد.

بازي Frontpage

Frontpage Extensionsمجموعه‌اي است كه شما را قادر مي‌سازد قابليت‌هايي را به سايتتان اضافه كنيد بدون آن كه لازم باشد خودتان كدي براي استفاده از آن قابليت‌ها بنويسيد، مانند دفاتر يادبود يا Guest book ، فرم‌هاي پرس‌وجو، ابزارهاي جستجو، پيمايش سايت و گالري‌هاي عكس .ببينيد

آیا میزبان شما Frontpage Extensions را پشتیباني مي‌كند يا خير. در غير اين صورت نمي‌توانيد از اين ابزارها استفاده كنيد. اگر سايت وب شما بر روي يك سرويس‌دهنده ويندوز قرار دارد مي‌توانيد در نرم‌افزار Frontpage از منوي File گزينه Open Web را انتخاب كرده و آدرس URLسايت خود را در پنجره ظاهر شده به عنوان نام سايت وب و نيز آدرس FTP سايت خود را به همراه نام كاربري و كلمه عبور آن وارد كنيد تا به سايت خود متصل شويد و به طور زنده با سايت خود، كار كنيد. در اين حالت هر تغييري كه به صفحات خود مي‌دهيد مستقيماً به سايت شما اعمال مي‌شود.

بيت‌هاي پهناي باند

به سايت‌هايي كه قول پهناي باند نامحدود را مي‌دهند هرگز اعتماد نكنيد. چرا كه پهناي باند بالاخره يك مرز و محدوديتي دارد. ممكن است ما از اين مرز اطلاع نداشته باشيم، اما بالاخره اين مرز وجود دارد. چنين سايت‌هايي مي‌توانند از شما پول اضافي مطالبه كنند و يا اگر سايت شما از محبوبيت بالايي برخوردار است آن را بدون اطلاع شما معلق كنند. بر اساس يك حساب سر انگشتي شما براي هر بيست‌هزار بازديد به پانصد مگا بيت پهناي باند نياز خواهيد داشت. بيشتر مردم نيز تنها يك صفحه از سايت شما را بازديد نمي‌كنند و احتمالاً به جاهاي مختلف آن سر مي‌زنند.

پشتيبان‌گيري را جدي بگيريد

سايت شما پشتيبان‌گيري نخواهد شد مگر آن كه شما صريحاً چنين چيزي را درخواست كنيد. همواره يك نسخه پشتيبان از سايت را در محل امني قرار دهيد، به خصوص اگر سايت شما يك سايت مبتني بر پايگاه داده است كه چيزي بيش از صفحات HTML اي كه براي آن نوشته‌ايد را در خود دارد.

كدام پايگاه داده

اگر قصد داريد از پايگاه داده كوچكي براي سايت خود استفاده كنيد، ببينيد آيا ميزبان شما پايگاه داده اكسس يا ODBCرا پشتيباني مي‌كند يا خير. براي سيستم‌هاي پيچيده‌تر، پشتيباني از پايگاه‌داده‌هاي MySqlيا SQL Server و يا ASP.NET را بررسي كنيد اما درباره` مهارت‌هاي برنامه‌نويسي خود منطقي و واقع‌گرايانه برخورد كنيد و چيزي را فراي توان خود انتخاب نكنيد.

گزارش‌هاي آماري

ببينيد چگونه مي‌توانيد دريابيد چه تعداد بازديد كننده به سايت شما مراجعه مي‌كنند، كدام صفحات را بيشتر سر مي‌زنند، از كجاها مي‌آيند و به دنبال چه چيزهايي مي‌گردند.

فايل‌هاي پيش‌فرض به كار ببريد

بيشتر سرويس‌دهنده‌گان وب هنگام درخواست مشاهده يك سايت يا فولدري سايت، به طور پيش‌فرض محل درخواست را به دنبال صفحاتي با نام‌هاي index ،default يا welcome با پسوند. htm . يا html جستجو مي‌كنند و در صورت موجود بودن يكي از اين فايل‌ها، آن را به مرورگر ارسال مي‌كنند. لذا نيازي نيست براي تبليغ سايت خود به ديگران بگوييد صفحه index.html را در سايت شما به از يك شده شما مثلاً آدرسhttp://www.mysite.com/index.html ببينند و مي‌توانيد به ديگران يك آدرس وب شسته رفته و تر و تميز به صورتhttp://www.mysite.com بدهيد. اما سعي كنيد در هر يك از پوشه‌هاي سايت خود، يك فايل پيش‌فرض با يكي از نام‌هاي ياد شده در بالا قرار دهيد. چرا كه برخي از سرويس‌دهنده‌ها، هنگامي كه درخواستي را براي مشاهده محتويات يك پوشه دريافت كرده و هيچ يك از فايل‌هاي پيش فرض را در آن پيدا نكردند، به جاي آن، ليست كل فايل‌هاي داخل آن پوشه را نشان مي‌دهند.

صفحاتتان را به صفحه پيش فرض لينك نكنيد

به جاي لينك نمودن يك صفحه به صفحه‌اي با نام پيش فرضي چون index.htm ، سعي كنيد صفحه مورد نظر را به پوشه‌اي كه صفحه پيش فرض در آن قرار دارد لينك كنيد. چرا كه بيشتر مرورگرها تشخيص نمي‌دهند كهwww.mysite.com/books وwww.mysite.com/books/index.htm در حقيقت معادل هم هستند، لذا ممكن است بازديدكنندگان سايت شما لينك‌هايي را كه قبلاً ديده‌اند با رنگي درست مشاهده نكنند (توجه كنيد كه مرورگرها، در يك صفحه وب، لينك‌هايي را كه قبلاً مشاهده كرده‌ايد به رنگي ديگر نشان مي‌دهند تا بدين طريق متوجه شويد كه كدام لينك‌ها را از آن صفحه، مشاهده كرده‌ايد). براي يك لينك، يك آدرس را به كار ببريد و در همه جاهاي ديگر نيز همان را مورد استفاده قرار دهيد. اين كار باعث مي‌شود كه در صورت نياز به انجام تغيير، اين كار سريعتر انجام شود. اگر هنگام كنترل نمودن صفحاتي كه طراحي كرده‌ايد، استفاده از لينك به پوشه، در كامپيوتر شما جواب نمي‌دهد و به جاي آن ليستي از محتواي پوشه مورد نظر به شما نشان داده مي‌شود، فقط بر روي صفحه پيش فرض در آن پوشه كليك كنيد.

براي فايل‌هاي سايت خود ساختاري سلسله مراتبي ترتيب دهيد

طبيعتاً جالب نخواهد بود اگر تمام صفحات و فايل‌هاي سايت خود را در ريشه سايت قرار دهيد. اگر براي فايل‌ها و صفحات سايت خود ساختاري را در نظر بگيريد، مديريت آن‌ها راحت‌تر انجام مي‌شود. بدين ترتيب به هنگام حل يك مشكل در بخشي به خصوص از سايت، تنها با فايل‌هاي درگير در همان مشكل سر و كار خواهيد داشت و اگر اين قسمت، قسمتي است كه عموماً آن را بروز رساني مي‌كنيد، حذف فايل‌هاي قديمي از آن به آساني انجام خواهد شد. شما همچنين مي‌توانيد فايل‌ها را براساس نوع آن‌ها دسته‌بندي كنيد. مثلاً فايل‌هاي گرافيكي را در يك پوشه، فايل‌هاي صوتي را در يك پوشه و كدهاي اسكريپت را در يك پوشه مجزا قرار دهيد. سعي كنيد حتماً پيش از آغاز كار سايت، اين ساختار را مشخص كنيد. چرا كه اگر ساختاري را به صورت موقت ايجاد كرده و به طراحي سايت بپردازيد و بعد تصميم بگيريد تغييري در اين ساختار ايجاد نماييد، بايد كليه لينك‌هاي مربوط به ساختار قبلي را در كل صفحات سايت تغيير دهيد. با اين كار، حتي مدخل‌هاي موتور جستجو (در سايت شما يا موتورهاي جستجوي ديگر) نيز از اعتبار خواهد افتاد و به هنگام جستجو، ممكن است آدرس صفحه‌اي را بدهند كه ديگر وجود ندارد يا به جاي ديگري منتقل شده است.

از علامت تقسيم (/:slash) استفاده كنيد.

هميشه سعي كنيد در انتهايURL هايي كه به پوشه‌ها ربط داده و در صفحات سايت خود به عنوان لينك به كار مي‌بريد، يك كاراكتر (slash) "/" قرار دهيد. به عنوان مثال اگر آدرس www.mysite.com/books را بدون به كارگيري كاراكتر "/" در انتهاي آن استفاده كنيد، مرورگر شما ابتدا از سرويس‌دهنده، فايلي با نام books را درخواست مي‌كند و در صورتي كه چنين فايلي وجود نداشته باشد، سرويس‌دهنده به مرورگر اين مطلب را اطلاع مي‌دهد كه به انتهاي آدرس درخواستي، يك "/" اضافه كند و مجدداً درخواست را ارسال كند. اين به معني طولاني‌ترشدن زمان بارگذاري صفحه بوده در ضمن ممكن است و نه رنگ‌بندي لينك‌هاي ديده شده و ملاقات نشده به صورت درست انجام شود و نه لينك‌هاي نسبي در مرورگرهاي بسيار قديمي، كار خواهد كرد.

نسبي كار كنيد

ساختار دايركتوري سرويس‌دهنده وب راه دور قطعاً مشابه ساختار دايركتوري كامپيوتر شما نخواهد بود. لذا در لينك‌هاي خود هرگز از آدرس‌دهي مطلق (شامل نام درايو و مسير دقيق پوشه‌ها از ريشه تا فايل مورد لينك) استفاده نكنيد چرا كه چنين لينكي قطعاً پس از بارگذاري صفحه وب حاوي آن بر روي سايت در سرويس‌دهنده
راه دور، كار نخواهد كرد. حتي اگر هم نام يكي از پوشه‌هاي به كار رفته در يك لينك را تغيير بدهيد، بايد كل لينك‌هايي كه نام اين پوشه، در بخشي از آن‌ها به كار رفته است را در كل سايت خود تغيير بدهيد. به جاي اين كه خودتان به صورت صريح محل فايل لينك شده را طي يك آدرس‌دهي مطلق در تمامي لينك‌ها مشخص كنيد، از دستور BASE HREF براي مشخص كردن مبدا تمامي لينك‌هاي يك صفحه استفاده كنيد و همچنين از URLهاي نسبي به دايركتوري قبل و بعد در صورت نياز استفاده نماييد. رعايت چنين موردي، سايت شما را تماماً به سايتي قابل حمل مبدل خواهد ساخت.

نام‌هاي كوتاه يا بلند

اهميتي ندارد كه براي نام صفحات سايت خود از پسوند htm. استفاده مي‌كنيد يا html. چرا كه امروزه تمامي مرورگرها هر دو پسوند را مي‌شناسند و قادر به دريافت و نمايش صفحاتي با هر يك از دو پسوند ياد شده هستند. اما براي ايجاد و كنترل نمودن آسانتر لينك‌ها، تنها از يكي از اين دو پسوند استفاده كنيد. اگر نمي‌توانيد پسوند مورد نظر خود را در ابزارهاي ويرايشي خود پيدا كنيد، ممكن است نرم‌افزار FTP شما قادر باشد پسوندها را براي شما تغيير بدهد. شما مجبور نيستيد الزاماً از سيستم نام‌گذاري ۳,۸ (۸ كاراكتر براي نام و ۳ كاراكتر براي پسوند) استفاده نماييد. اما دقت كنيد كه نام‌هايي كه به كار مي‌بريد خيلي طولاني نبوده و به راحتي قابل تشخيص باشند.

مراقب حساسيت به حروف باشيد

بسياري از سرويس‌دهنده‌ها از سيستم عامل يونيكس يا لينوكس استفاده مي‌كنند كه بر خلاف سيستم‌هاي ويندوز، در آن‌ها اسامي فايل‌ها و دايركتوري‌ها از حساسيت به بزرگي و كوچكي حروف برخوردارند. به عنوان مثال اگر شما فايلي با نام GreatPhoto.jpg را بر روي سايت خود بارگذاري كنيد و در لينك به اين فايل،GREATPHOTO.jpg را به كار ببريد، لينك شما كار نخواهد كرد. سعي كنيد هميشه تمامي اسامي را با حروف كوچك استفاده كنيد تا سردرگم نشويد. برنامه ويرايشگر صفحات‌وب يا نرم‌افزار FTP بايد گزينه‌اي براي تبديل نام فايل‌ها به حروف كوچك پيش از انتقال آن‌ها به سرويس‌دهنده داشته باشد.

ايجاد كنند كه سريع‌تر توسط موتورهاي جستجو شناسايي شوند) و در كل، رتبه سايت شما را در موتورهاي جستجو بالا ببرند. اگر زندگي سايت شما به بازديدكنندگانش محتاج نمي‌بود مجبور نبوديد پولي خرج كنيد.

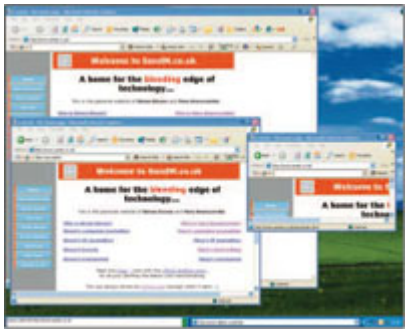
ببينيد موتورهاي جستجو در سايت‌ها به دنبال چه چيزهايي مي‌گردند و اطمينان حاصل كنيد كه شما آن چيزي را كه موتورهاي جستجو براي ثبت سايت يا صفحات سايت شما در پايگاه‌هاي داده خود نگاه مي‌كنند، در سايت يا صفحات خود و در جاي درست آن، قرار داده‌ايد. اما با اين وجود، در اين مورد خيلي خود را به دردسر نيندازيد چرا كه سايت‌هايي مانند Google مكرراً فاكتورهاي رتبه‌بندي سايت‌ها را در موتور جستجوي خود تغيير مي‌دهند. صفحات ممكن است يك بار به بالاي ليست‌هاي رتبه‌بندي صعود كنند و يك بار نيز در سطرهاي پايين قرار بگيرند. از اين رو بهتر است وقت خود را صرف بهتر نمودن سايت خود بنماييد تا به بهبود رتبه‌بندي سايت خود در موتورهاي جستجو فكر كنيد.

اطمينان حاصل كنيد كه هر صفحه از سايت شما حتماً يك عنوان مشخص داشته باشد و اين كه تگ TITLEدر كد HTMLصفحه شما، اولين جزء از قسمت HEAD و نه آخرين جزء است. براي همه تصاوير خود خصوصيت ALT را مشخص كرده و تصاوير را از طريق اين خصوصيت توضيح دهيد. نه تنها موتورهاي جستجو رتبه بهتري به صفحات شما به خاطر انجام اين كار مي‌دهند بلكه اين كار به كساني كه از يك دستگاه صفحه‌خوان براي بازديد سايت شما استفاده مي‌كنند نيز كمك مي‌كند.

موتورهاي جستجو بعضي مواقع نگاه مي‌كنند كه سايت شما در چه تاريخي براي آخرين بار بروزرساني شده است، لذا سايت خود را هميشه روزآمد نگه‌داريد و تمامي لينك‌هاي آن را از لحاظ صحت كاركرد كنترل كنيد.

تگ‌هاي META در صفحات از اهميت بسياري برخوردارند. اما آن‌ها تنها نكته‌اي نيستند كه موتورهاي جستجو به آن توجه مي‌كنند. چرا كه بسياري از افراد از اين تگها سوء استفاده مي‌كنند. در بخش META با اين فكر كه توجه افراد بيشتري را به سايتتان جلب كنيد از كلمات و تركيباتي كه ارتباطي با محتواي سايت و صفحات شما ندارند استفاده نكنيد، چرا كه با اين كار رتبه‌بندي شما پايين خواهد آمد و بازديدكنندگان شما نيز خشمگين خواهند شد زيرا درمي‌يابيد كه وعده‌هاي شما دروغين بوده است در نتيجه سايت شما را ترك كرده و هرگز باز نمي‌گردند. در اين زمينه به نكات ذكر شده در اين نشاني و نشاني www.spiderfood.net نيز توجه كنيد.

پايگاه داده خود را FTP كنيد



از ميله وظيفه (taskbar) محصول شركت DSQDبراي مشاهده سايت خود در دقت‌هاي

شما معمولاً نمي‌توانيد داده‌ها يا ركوردهاي جديد را به شيوه‌اي كه به راحتي در كامپيوتر خود به مختلف صفحه نمايش استفاده كنيد.
پايگاه داده اضافه مي‌كنيد، به طور دستي وارد پايگاه داده‌اي كه بر روي سرويس‌دهنده وب قرار دارد
وارد نماييد. اگرچه امكان انتقال ساختار پايگاه داده به سرويس‌دهنده راه دور و سپس وارد كردن داده‌ها در آن وجود دارد اما اين كار در صورت زيادبودن داده‌ها وقت‌گير است. به جاي آن سعي كنيد داده‌ها را از قبل در پايگاه داده خود مانند Access وارد كنيد و سپس فايل پايگاه داده را به سرويس‌دهنده راه دور انتقال دهيد.

آدرس پست الكترونيك خود را مخفي كنيد

اين كه دوستان و آشنايان به راحتي آدرس تماس شما را ببينند و با شما تماس بگيرند خوب است، اما قطعاً دوست نخواهيد داشت كه فرستندگان هرزنامه‌ها و Spammer ها نيز آدرس پست الكترونيك شما را از سايتتان بردارند تا هرزنامه‌ها را به سمت شما سرازير كنند. به جاي تايپ آدرس پست‌الكترونيك خود در صفحات سايت، آن را به صورت يك تصوير گرافيكي در آوريد و يك تكه كد Javascript بنويسيد كه آدرس اصلي را مخفي نگه‌مي‌دارد اما اجازه مي‌دهد هنگامي كه بازديد كنندگان بر روي آن تصوير كليك مي‌كنند، نرم‌افزار سرويس‌گيرنده پست الكترونيك آن‌ها مانندOutlook بارگذاري شود تا بتوانند به آدرسي كه نوشته‌ايد، نامه ارسال كنند. اين شيوه، جلوي بسياري از اسپمرها را مي‌گيرد. در اين صفحه چگونگي انجام اين كار توضيح داده شده و نمونه يك كد اسكريپت قرار داده شده است.

****

راه اندازي يك شبكه LAN كوچك

اگر در محیط کار یا منزل خود با بیش از یک کامپیوتر سروکار دارید احتمالا به فکر افتاده اید که آنها را به یکدیگر متصل کرده و یک شبکه کوچک کامپیوتری راه بیا ندازید .
با اتصال کامپیوتر ها به یکدیگرمیتوانید چاپگرتان را بین همه انها به اشتراک بگذارید از طریق یکی از کامپیوتر ها که به اینترنت وصل است بقیه را نیز به اینترنت متصل کنید از هر یک از کامپیوتر ها به فایل های خود از جمله عکس ها اهنگ ها و اسنادتان دسترسی پیدا کنید به بازی هایی بپردازید که نه چند بازیکن با چند کامپیوتر نیاز دارند
وبلاخره این که که خروجی وسایلی چون DVD PLAYER یا وب کم را به سایر کامپیوتر ها ارسال کنید .
در این مقاله ضمن معرفی روش های مختلف اتصال کامپیوتر ها به یکدیگر انخام تنضیمات دستی را برای بهره بردن از حد اقل مزایای یک شبکه کامپیو تری به شما نشان می دهیم .
ذکر این نکته هم لازم است که قسمت اصلی این مقاله به نصب نرم افزار اختصاص دارد اما در انتهای مطلب در خصوص ساختار شبکه و مسائل فیزیکی ان هم توضیهاتی داده ایم

روشهای اتصال :

برای اتصال کامپیوتر هایی که در فاصله ای نه چندان دور از یکدیگر قرار دارند راههای مختلفی وجود دارد که عبارتند از :
سیم کشی دیتا به صورت تو کار در حین ساخت ساختمان که امروز بسیار متداول است .
در این روش همان گونه که برای برق ساختمان از قبل نقشه می کشند و مثلا جای کلید ها و پریز ها را مشخص می کنند برای شبکه کامپیوتری هم نقشه کشی و سیم کشی می کنند .
قرار دادن سیم ها در کف اتاق و اتصال کامپیوتر هایی که در یک اتاق قرار دارند .
استفاده از فناوری بی سیم
ساتفاده از سیم کشی برق داخل ساختمان
استفاده از سیم کشی تلفن داخل ساختمان

هر یک روش ها مزایا و معایب خاص خود را دارند اما برای به اشتراک گذاشتن چاپگر فایل ها و اینتر نت باید کامپیوتر ها را به نحو صحیح و مناسبی تنظیم و آماده کنید و فرق نمی کند که کدام روش را انتخاب کرده باشید
به همین دلیل کار را از همین نقطه شروع می کنیم از آنجا که ویندوز های اکس پی و ۹۸ پر استفاده ترین ویندوز ها در منازل و دفاتر کوچک هستند نحوه اشتراک گذاری منابع در این دو ویندوز را مورد بحث قرار می دهیم هر چند مورد سایر ویندوز ها مفاهیم تغییر

نمی کند

گام های اولیه :

برای راه اندازی شبکه در منزل خود این سه کار را باید انجام دهیم :

1انتخاب فناوری مناسب شبکه که مورد نظر ما در این مقاله اترنت استاندارد است

2خرید و نصب سخت افزار مناسب این کار، که اصلی ترین آنها کارت شبکه برای هر یک از این کامپیوتر ها و یک هاب – سوییچ است

3تنظیم و آماده سازی سیستم ها به نحوی که بتوانند همدیگر را ببینند و با یکدیگر صحبت کنند

از این سه مرحله قدم سوم از همه مهم تر است .

ویندوز اکس پی قسمتی به نام NETWORK SETUP WIZARD دارد که تنظیمات شبکه را برای شما انجام می دهد .

به غیر از این متخصصان هستند که در ازای دریافت دستمزد ، شبکه شما را در محل راه می اندازند .

نام گذاری کامپیوتر ها به اشتراک گذاشتن چاپگر ها فایل ها و اتصالات اینترنتی ،اساسی ترین کارهایی هستند که این افراد برای شما انجام می دهند .

اما اگر با مشکلی مواجه بشوید یا تنظیمات کامپیوتر تان بهم بخورد ، باید بتوانید خودتان شبکه را تنظیم کنید .

کلا بد نیست مفاهیم و اصول راه اندازی یک شبکه کامپیوتری را بدانید تا به هنگام ضرورت خودتان بتوانید دست به کار شوید .

به طور کلی کار هایی که باید انجام دهید تا یک شبکه ((مرده)) را ((زنده)) کنید و به بهره برداری از ان بپر دازید ، از این قرار است :

نام گذاری کامپیوتر

دادن آدرس IP

به اشتراک گذاشتن فایل ها

به اشتراک گذاشتن چاپگر

انجام تنظیمات امنیتی

به اشتراک گذاشتن اتصال اینترنت

نام گذاری کامپیوتر :

بعد از نصب سخت افزار های مورد نیاز برای راه اندازی شبکه ، نیاز به نوبت به نصب نرم افزار های آن می رسد .

در اولین قدم باید برای تکتک کامپیوتر های موجود در شبکه خود اسمی منحصر به فرد و غیر تکراری انتخاب کنید .

علاوه بر اسم کامپیوتر اسم گروه کاری یا WORK GROUP هم مهم است . تمام کامپیوتر های یک شبکه باید عضو یک گروه کاری باشند .

ویندوز اکس پی :

برای نام گذاری کامپیوتر در ویندوز اکس پی این مراحل را دنبال کنید :

۱.پنجره control panel را باز کنید

۲.اگر حالت نمایش آیکون ها به صورت کلاسیک نیست روی لینک classic new کلیک کنید .در این حالت بر نامه system را اجرا کنید .

۳.در کادر محاوره ظاهر شده صفحه computer name را انتخاب کنید

٤.همان طور که ملا حظه می کنید کامپیوتر یک اسم کامل دارد و یک گروه کاری . روی دکمه chang کلیک کنید تا کادر محاوره بعدی ظاهر شود .

٥.در کادر اول اسمی را تایپ کنید که می خواهید به کامپیوتر تان اختصاص دهید . این اسم هر چیزی می تواند باشد ، فقط نباید تکراری باشد . مثلا اسم کامپیونر اول را pc 1 بگذارید .

٦.در کادر دوم اسمی را که می خواهید به گروه کاری خود اختصاص دهید وارد کنید .مثلا My office یا My Home یا هر چیز دیگر . حتی خود Work Group هم بد نیست .

۷. در پایان OK و دوباره OK را بزنید . اگر ویندوز خواست ری استارت کند قبول کنید .

ویندوز ۹۸

برای نام گذاری کامپیوتر در ویندوز ۹۸ این مراحل را دنبال کنید :

۱.با کلیک راست روی آیکون Network Neighborhood روی دسکتاپ گزینه ، properties را انتخاب کنید .

۲.در کادر محاوره ظاهر شده ، به صفحه identification بروید .

۳.در کادر اول ، اسم کامپیوتر و در کادر دوم اسم گروه کاری مورد نظر را بنویسید . بعد از تنظیم نام برای تک تک کامپیوتر ها و گذاشتن یک اسم برای کروه کاری تمام آنها ، کامپیوتر ها را دارای هویت کرده و در یک گروه جای داده اید . حالا نوبت به دادن آدرس IPمیرسد .

آدرس IP

آدرس IP نشانی هر کامپیوتر در شبکه است . کامپیوتر از طریق این نشانی است که یکدیگر را در شبکه پیدا می کنند .
در هر شبکه آدرس IP هر کامپیوتر باید منحصر به فرد و غیر تکراری باشد .
در باره IP و آدرس دهی از این طریق ، زیاذ میتوان صحبت کرد ، اما از آنجا که در این مقاله قصد پرداختن به تئوری را نداریم بلا فاصله دست به کار می شویم . فقط ذکر این نکته را زروری میدانیم که آدرس IP در واقع یک شماره چهار قسمتی است . هر قسمت عددی از ۰ تا ۲۵۵ است که با علامت نقطه از قسمت بعدی جدا می شود .
مثلا 192.168.0.1 یک آدرس IP است . مفهوم دیگر Subnet Mask است ، که توضیح آن هم از حوصله این مقاله خارج است . فقط این را قبول کنید که در یک شبکه کوچک ، subnet maskرا به صورت ۲۵۵,۲۵۵,۲۵۵,۰ تایین می کنیم .
در یک شبکه کوچک ، برای تمام کامپیوتر ها سه قسمت اول آدرس IP را یکسان می گیریم و فقط قسمت چهارم را برای هر کامپیوتر عدد متفاوتی را در نظر می گیریم .
مثلا در کامپیوتر اول آدرس 192.168.0.1 و برای کامپیوتر دوم آدرس ۱۹۲,۱۶۸,۰,۲ را می نویسیم و به همین ترتیب ذر بقیه کامپیوتر ها قسمت چهارم آدرس IP را عدد متفاوتی را می دهیم.

****

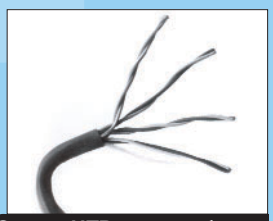
موفق و پیروز باشید

داوود خرسند

راهنمای تصویری
تجهیزات شبکه

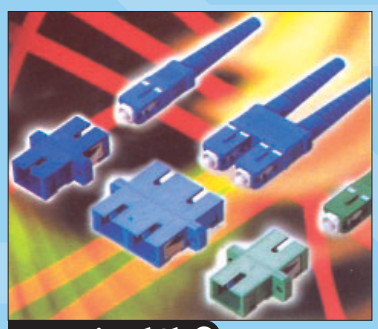
ممکن است بسیاری از خوانندگان یا علاقه‌مندان مباحث شبکه موفق نشده باشند یا موفق نشوند که نمای ظاهری بسیاری از تجهیزات شبکه را ببینند و بدانند که ادواتی که درباره آن‌ها صحبت می‌شود، از حیث ظاهر چگونه هستند. راهنمای تصویری تجهیزات شبکه در راستای پاسخگویی به همین نیاز آماده شده است. این تجهیزات را در سه گروه تجهیزات غیرفعال (Passive)، تجهیزات فعال (Active) و سایر تجهیزات آورده‌ایم.

تجهیزات غیرفعال (Passive)



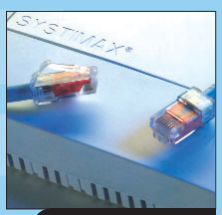
کابل‌های مسی که از چهار رشته به‌هم تابیده شده تشکیل شده‌اند را با نام UTP می‌شناسند و انواع متداول آن عبارتند از: Cat 5 ، Cat5e، Cat6 و Cat7. تفاوت عمده این استانداردها در سرعت انتقال و فرکانس کاری می‌باشد.

انواع کابل مسی UTP



قطعه‌ای برای برقراری ارتباط فیبر نوری با سایر ادوات که در انواع ST،SC یا MTRJ موجود می‌باشد.

کانکتور فیبرنوری



قطعه‌ای برای برقراری ارتباط کابل مسی با سایر ادوات

سرکابل مسی

محفظه‌ای فلزی که محل قرارگیری سوییچ‌ها، روترها، سرورها، USPها یا هر یک از ادوات شبکه می‌تواند باشد. معمولاً این رک‌ها از چهار طرف باز می‌شوند و به چرخ، درب قفل شونده شیشه‌ای و هواکش نیز مجهز هستند.

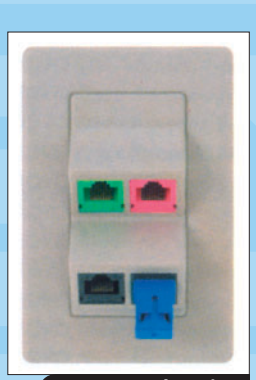
رک (Rack)

رشته‌هایی از شیشه یا پلاستیک که به جای الکترون‌ها، پرتوهای نور را عبور می‌دهد. فناوری فیبرنوری تحولی را در سرعت ارسال داده‌ها و گسترش شبکه‌ها در فواصل طولانی پدید آورد.

فیبرنوری

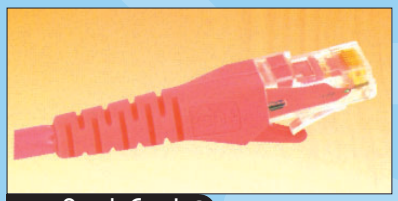
مکانیزم داخل هر پریز شبکه (برای کابل‌های مسی) که در حکم مادگی آن است.

کابل مسی Keystone



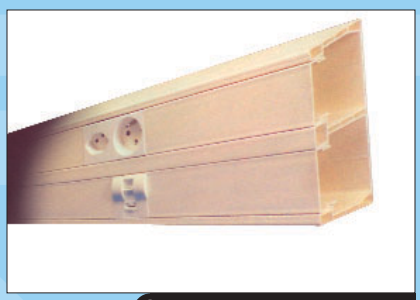
هر ایستگاه شبکه برای برقراری ارتباط با شبکه باید با استفاده از پریز اتصال فیزیکی خود را برقرار کند.

پریز دیواری مسی



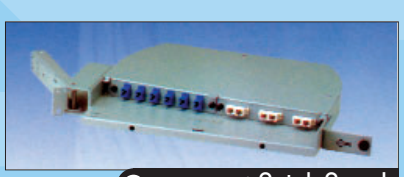
در کابل کشی ساخت یافته، برای ایجاد اتصال بین ایستگاه کاری و پریز شبکه یا اتصال تجهیزات فعال به Patch Panel داخل رک از این کابل ها استفاده می شود.

Patch Cord مسی



مسیری برای عبور کابل شبکه که در انواع فلزی یا پلاستیکی و در اندازه‌های مختلف ساخته می شود.

داکت یا کانال دیواری



محل برقراری ارتباط بین کابل های فیبرنوری و تجهیزات اکتیو در داخل رک

Patch Panel فیبرنوری

در کابل کشی ساختیافته برای برقراری ارتباط بین تجهیزات فعال با Patch Panel در داخل رک از قطعات کابلی به این شکل استفاده می شود.

Patch Cord فیبرنوری

محلی برای برقراری ارتباط بین تجهیزات اکتیو و رشته کابل های سمت کاربران در داخل یک Rack

Patch Panel برای اتصالات کابل مسی

تجهیزات فعال شبکه (Active)

سوییچ ها همان قلب تپنده شبکه های star یا ستاره‌ای هستند که وظیفه انتقال ترافیک را برعهده دارند. سوییچ ها را در انواع قابل نصب در رک یا غیرقابل نصب در رک و قابل مدیریت کردن یا غیر قابل مدیریت تقسیم بندی می کنند.

سوییچ

مسیریاب ها به عنوان ادواتی که در لایه ۳ شبکه کار می کنند، وظیفه ایجاد ارتباط بین شبکه های مختلف را برعهده دارند.

روتر(مسیریاب)

ابزاری برای تبدیل رسانه های مختلف به یکدیگر، مثلاً وقتی یک طرف ارتباط از کابل مسی و طرف دیگر از فیبرنوری استفاده می کند، یکی از این تجهیزات می تواند در میان راه قرار گیرد و ارتباط دو رسانه متفاوت را برقرار نماید.

Media Converter

قطعه‌ای در شبکه های بی سیم برای جلوگیری از آسیب های وارده به تجهیزات شبکه. به آن گاهی برق گیر نیز می گویند.

صاعقه‌گیر

کامپیوترهای سرور را می توان در انواع تیغه ای (Blade) که مناسب نصب در رک هستند تهیه نمود.

سرور تیغه ای

سرور ها در انواع مختلف، سرویس های گوناگون را به کاربران ارائه می دهند.

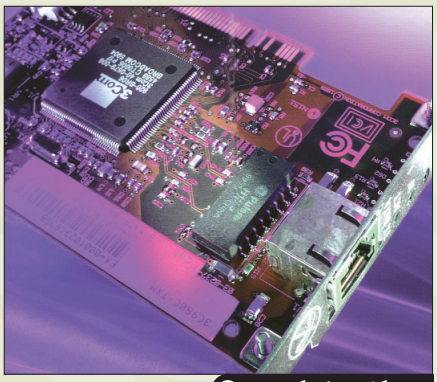
سرور

دیواره های آتش، محافظت کننده شبکه ها از حملات ویروسی، نفوذگران و کرم های آسیب رسان.

فایروال

نقطه دسترسی یا AP که مشابه سوییچ و گاهی اوقات روتر در شبکه های بی سیم عمل می کند.

Access Point (AP)



رابط فیزیکی ایستگاه های کاری با شبکه که به NIC نیز معروف هستند.

کارت شبکه

نمونه کارت شبکه ای که در شبکه های بی سیم مورد استفاده قرار می گیرد.

کارت شبکه بی‌سیم

در برخی از فناوری ها، از امواج لیزری به جای امواج رادیویی جهت ارتباط شبکه ای بی سیم استفاده می شود.

تجهیزات شبکه بی‌سیم لیزری

برای دریافت امواج رادیویی در شبکه های بی سیم که به صورت outdoor نصب می شوند به انواع متفاوتی از آنتن نیاز است .

آنتن

سایر تجهیزات و متعلقات

مودمی که برای
ارتباطات DSL
(باندپهن) استفاده می شود.

ابزار پانچ کردن کابل مسی

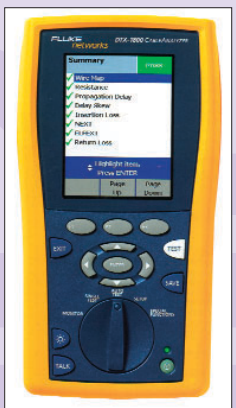
از این ابزار برای
اتصال کابل مسی و
Patch Panel
استفاده می شود.

تجهیزات ویدئو کنفرانس

ابزاری جهت برقراری
ارتباط بین نقاط دوردست
به صورت
کنفرانس ویدیویی

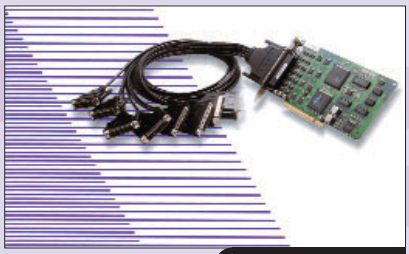
UPS

تأمین کننده برق اضطراری



تحلیلگر کابل

برای آگاهی از وضعیت شبکه و
بستر ارتباطی، یکی از
دستگاه های بسیار خوب و
کارآمد، انواع تحلیلگرهای کابل
و تحلیلگرهای شبکه می باشند.



مالتی پورت

مالتی پورت برای اتصال چندین
وسیله سریال به یکدیگر

کمربند کابل

قطعه ای پلاستیکی
برای بستن و منظم کردن
چندین رشته کابل

ابزار اتصال کانکتور فیبرنوری

از این ابزار برای
اتصال فیبرنوری و کانکتور آن
استفاده می شود.