اصطلاحات کامپیوتری

در این بخش با تمامی کلمات و اصطلاحات کامپیوتری به زبان فارسی و توضیحات فراوان آشنا خواهید .

Half-duplex :

بعضی از مودمها دارای سوئیچی هستند که به شما اجازه انتخاب بین Half-duplex و Full-duplex را میدهد. انتخاب درست برای این سوئیچ بستگی به برنامه ای دارد که از مودم برای انتقال داده استفاده میکند. در حالت Half-duplex هر کاراکتر انتقال داده شده بلافاصله بر روی صفحه نمایش شما ظاهر می شود (به همین دلیل به این حالت Local Echo هم گفته می شود). در حالت Full-duplex داده منتقل شده تا زمانی که توسط طرف مقابل دریافت نشده و به شما باز گشت نداده شده است، به نمایش در نمی آید .(Remote Echo) اگر شما برنامه ای ارتباطی را اجرا می کنید و در آن

هر کاراکتر دوبار ظاهر می شود احتمالا مودم شما بجای اینکه در حالت Half-duplex باشد در حالت Full-duplex است، در نتیجه هر کاراکتر دو بار اکو می شود یک بار Local Echo و بار دیگر Remote Echo.

DRM؛

مخفف Digital Rights Management می باشد و سیستمی است برای حفاظت از حق کپی رایت داده های موجود در اینترنت و سایر رسانه های دیجیتال توسط فعال نمودن توزیع مطمئن داده ها و یا غیرفعال نمودن توزیع غیرقانونی داده ها. مثلا یک DRM سیستم از مالکیت معنوی دارنده اثر توسط Encrypting حفاظت می کند بنابراین داده فقط توسط کاربران مجاز قابل استفاده خواهد بود. روش دیگر علامت گذاری محتوا توسط Digital Watermark یا روشهای مشابه، برای جلوگیری از توزیع آزادانه اطلاعات است.

LCP :

مخفف Link Control Protocol می باشد. این پروتکل بخشی از پروتکل PPPاست.در ارتباطات ppp) مثل ارتباط شما باISP تان از طریق خط تلفن) هم دستگاه فرستنده و هم دستگاه گیرنده ی پیام، بسته های LCP را برای تصمیم گیری در مورد چگونگی انتقال بسته های داده می فرستند. یک بسته ی LCP هویت شما را هنگام برقراری ارتباط با ISP بررسی می کند و سپس در مورد پذیرش یا رد درخواست اتصال شما تصمیم می گیرد. این بسته همچنین سایز قابل قبول بسته های داده تبادلی بین طرفین را مشخص می کند. همچنین بدنبال مشکل در پیکربندی ارتباطی می گردد و در صورت وجود مشکل به ارتباط خاتمه می دهد. انتقال داده در شبکه، تا زمانی که LCP هویت شما را تائید نکرده باشد ممکن نخواهد بود.

Dongle :

وسیله ایست که برای کنترل دسترسی به برنامه ای خاص، به کامپیوتر متصل

می شود. این وسیله موثرترین ابزار برای محافظت از نرم افزار در برابر کپی است. در کامپیوترهای PC این وسیله به پورت موازی و در کامپیوترهای MAC به پورت ADB متصل می شود. تمامی اطلاعات ورودی و خروجی پورت از Dongle عبور می کنند ولی Dongle مانع عبور آنها نمی شود و می توان از پورت، همانند زمانی که هیچ وسیله ای به آن متصل نیست استفاده کرد. چندین Dongle را می توان به یک پورت متصل کرد.

USB :

مخفف Bus Universal Serial می باشد که یک استاندارد Bus خارجی است که نرخ انتقال داده در آن به ۱۲ Mbpsمی رسد. هر USB پورت می تواند برای اتصال ۱۲۷ وسیله جانبی، مثل موس، مودم، کیبورد، دوربین دیجیتالی و ... مورد استفاده قرار گیرد (برای این کار به یک USB Hub احتیاج دارید .(از Hot Plugging و Plug And Play پشتیبانی می کند. این فناوری در سال ۱۹۹۶ عرضه شد؛ در آن زمان تولید کنندگان کمی

این پورت را در محصولاتشان عرضه می کردند ولی در سال 1998 و با محصول پر فروش iMac این فناوری عمومی شد و امروزه این فناوری تا حدی گسترده شده که تمامی MotherBoard های جدید دارای USB پورت هستند. هم اکنون دو نوع USB پورت وجود دارد USB 1.1 و USB 2.0که اختلاف آنها در سرعت تبادل اطلاعات با کامپیوتر است. اینطور انتظار میرود که USB کم کم جای پورتهای سری و موازی را بگیرد. در اینصورت وسایلی مانند مانیتور، پرینتر، کیبورد و موس را باید به USB پورت MotherBoardمتصل کنید.

Virus :

به برنامه یا قطعه ای کد گفته می شود که پس از اجرا در سیستم کپی هایی از خودش را به فایلهای مورد نظر اضافه کرده و آنها را آلوده می کند و بسته به نوع آن اعمال مختلفی را از ظاهر شدن پیغامی خاص در صفحه تا رساندن آسیبهای بسیار جدی به سیستم انجام می دهد. ویروسها این قابلیت را دارند که خود را تکثیر کنند. حتی ویروس ساده ای که اقدام به تولید کپی

از خود در سیستم میکند می تواند خطر آفرین باشد چون برای این کار از منابع سیستم بهره می گیرد و ممکن یاعث ایجاد وقفه در سیستم شود.

ویروسهای خطرناکتر قابلیت انتشار در شبکه ها و عبور از سیستمهای امنیتی را دارند Micro Virus ها نوع خاصی از ویروسها هستند که به جای آلوده کردن فایلهای اجرایی یا بوت سکتور Document های Word را آلوده می کنند.

Worm :

کرم را می توان نوع خاصی از ویروس دانست که برای انتشار از طریق شبکه طراحی شده اند. کرمها معمولا از طریق ایمیل یا برنامه های اشتراک گذاری فایلها (p2p) منتشر می شوند. کرمها ضمن آلوده کردن کامپیوتری که در آن قرار دارد از طریق Contact های موجود در آن برای تمامی آنها ارسال می شود و با عناوین فریبنده گیرنده را به گشودن فایل الحاقی ترغیب می کند. کرمها بدلیل ارسال به کاربران بسیار زیاد در زمان کم، ترافیک شبکه را بسیار بالا برده و باعث کند شدن فعالیت Mail Server ها می شود.

Dropper :

همچنین با نامهای Virus Dropper و Dropper Program شناخته می شود.

برنامه ای است که پس از اجرا یک ویروس اسب تروا یا یک کرم را درون کامپوتر شما بارگذاری می کند .خود یک ویروس نیست و خواص ویروس نظیر تکثیر شدن را ندارد. شاید بیشتر بتوان آنرا شبیه اسب تروا دانست که حاوی کدهای مخرب است و توسط برنامه های ویروس یاب قابل شناسایی نیست خوشبختانه استفاده از Dropper ها غیر متداول است وگرنه مطمئنا مشکلات بزرگی را باعث می شدند.

Spyware :

نام دیگر آن Ad-Aware است Spyware .به هر برنامه ای که به جمع آوری اطلاعات شخصی افراد هنگام اتصال به اینترنت می پردازد اطلاق می شودSpyware .ها معمولا جزئی پنهانی درون برنامه های رایگان و یا برنامه هایی با مدت استفاده محدود (Freeware Or Shareware) هستند که می

توان آنها را از اینترنت دانلود کردSpyware .ها پس از نصب به Monitor

کردن فعالیتهای شما در اینترنت می پردازند و اطلاعات کسب شده را در

پس زمینه ارتباط اینترنتی شما برای نویسندگانش می فرستدSpyware .ها

قابلیت جمع آوری اطلاعات در مورد آدرسهای ایمیل، شماره کارتهای

اعتباری و حتی پسوردهای شما را دارند Spyware .را می توان شبیه اسب

تروا دانست چون در هر دو مورد شما هنگام نصب یک برنامه این برنامه ها

را نیز ناخواسته در سیستمتان نصب می کنید. یکی از روشهای معمول قربانی

شدن نصب برنامه هایی است که برای تبادل فایل ها در اینترنت وجود دارد

(این برنامه ها peer-to-peer نامیده می شوند نظیر .(Kaaza نکته

دردناکتر در موردSpyware ها اینست که این برنامه ها چون برای فعالیت

از منابع سیستم شما استفاده می کنند ممکن است باعث ناپایداری سیستم و

یا حتی Crash بشود. همچنین این برنامه ها از پهنای باند اتصال اینترنتی شما

می کاهند.(بدلیل استفاده از اتصال اینترنتی برای ارسال اطلاعات به سرقت

رفته)

چونSpyware ها برنامه های اجرایی مستقلی هستند قابلیت های دیگری از جمله Monitor کردن کلید های فشرده شده کیبورد، گشتن بدنبال فایل یا برنامه ای خاص در سیستم، نصب Spyware های دیگر خواندن Cookie ها و تغییر صفحه وب پیش فرض را دارند Licensing Agreement.ها که قبل از نصب اکثر برنامه ها باید با مفاد آن موافقت کنید ممکن است در مورد نصب Spyware توسط برنامه مورد نظر به شما هشدار دهد (البته در جایی که کمترین احتمال دیده شدن را دارد) ولی از آنجا که هیچکس تمایلی به خواندن متن طولانی Licensing Agreement را نداردSpyware ها را با موافقت خودتان در سیستم نصب می کنید.

Trojan Horse :

برنامه ایست مخرب که ظاهرعادی و بی آزاری دارد. این برنامه پس از اجرا در کامپیوتر هدف، اختیار کامل آنرا بدست نفوذ گران می دهد و به آنها اجازه انجام هر کاری را در سیستم مورد حمله می دهد. اسب تروا

قابلیت تکثیر خود را ندارد ولی می تواند حامل ویروس یا کرم باشد. یک اسب تروا از دو قسمت تشکیل شده است: یک قسمت که باید توسط طعمه دانلود و اجرا شود که معمولا حجم کمی دارد (زیر (100 kb مثلا برنامه ای که ادعا می کند کشنده فلان ویروس است ممکن است خود یک اسب تروا باشد، و قسمت دوم اسب تروا که روی کامپوتر مهاجم قرار دارد و پس از اجرای جزءِ دیگر برنامه روی کامپیوتر قربانی و دریافت آدرس IP قربانی توسط مهاجم این دو قسمت برنامه با هم ارتباط برقرار کرده و مهاجم قادر خواهد بود در کامپیوتر قربانی مانند کامپیوتر خود Expelor کند و به حذف اضافه و تغییر هر چیز مورد علاقه اش بپردازد. همانطور که اشاره شد طعمه یک اسب تروا شدن به این آسانی ها نیست زیراخود فرد باید مرتکب این اشتباه بشود. البته بعضی سایتها این کار را برای شما انجام می دهند! که این مشکل هم با نصب یک فایروال مناسب حل شدنی است. به حملاتی از این دست Back Door می گویند چون شبیه زمانی است که شخصی از در پشتی منزل وارد شود و بدون اطلاع شما و در حضور خودتان

به شما آسیب برساند.

عبارت اسب تروا یا Trojan Horse برگرفته از یکی از داستانهای کتاب ایلیاد

هومر نویسنده یونان باستان است که در آن مهاجمان اسب بزرگ چوبی را

به نشانه صلح و آشتی (البته با تعدادی جنگجو در درون آن) به درون شهر

محاصره شده تروا می فرستند و ...!

Protocol :

فرمتی از پیش تعریف شده برای برقراری ارتباط بین دو کامپیوتر.بعبارت

دیگر مجموعه ای از قوانین که دو دستگاه برای انتقال موفق داده، از آنها

پیروی می کنند. برخی از مواردی که یک پروتوکل آنها را مشخص می کند

عبارتند از:

-نحوه تشخیص خطا و تصحیح خطاهای احتمالی که حین تبادل داده ممکن

است اتفاق بیفتد.

-روش متراکم سازی داده ها

-چگونگی اعلان پایان یک فریم داده توسط فرستنده

-چگونگی اعلان دریافت یک فریم داده توسط گیرنده و نحوه ادامه ارسال

داده در صورت عدم موفقیت گیرنده، در دریافت صحیح داده ها

-طول هر فریم داده

-و .....

تا کنون انواع مختلفی از پروتوکلها برای استفاده های مختلف طراحی شده

اند و هر کدام دارای معایب و مزایایی هستند برخی از پروتوکلها ساده،

برخی با قابلیت اطمینان بیشتر و برخی دارای سرعت بالاتر هستند.

برخی از پروتوکلهای متداول عبارتند از PPP ، FTP ، UDP ، TCP/IP :و

... توضیحات کامل در مورد عملکرد هر پروتوکل در متنهایی با نام RFC

توسط IETF انتشار می یابند (مثلا RFC شماره ۷۹۱ ، اطلاعات جامعی را

در مورد پروتوکل IP ارائه می کند) .

IP :

مخفف . Internet Protcol این پروتوکل فرمت بسته های داده Ip)

(Datagramو نحوه آدرس دهی در آنها را مشخص می کند. این پروتوکل بدلیل نقایصی که دارد با پروتوکل TCP همراه شده و ارسال و دریافت داده را میسر می سازد.

این پروتوکل را می توان شبیه سیستم پست معمولی دانست چون در آن بین فرستنده و گیرنده ارتباطی برقرار نمی شود و فرستنده اطلاعی از دریافت و یا عدم دریافت پیام توسط گیرنده ندارد و دیگر اینکه بسته های ارسالی الزاما با همان ترتیبی که فرستاده شده اند توسط گیرنده دریافت نخواهند شد. لذا برای رفع این نواقص از پروتوکل TCP کمک گرفته می شود که باعث برقراری یک ارتباط مجازی بین فرستنده و گیرنده می شود.

این دو پروتوکل با یکدیگر مدل TCP/IP را تشکیل می دهند که اساس کار اینترنت بر پایه این مدل است. هم اکنون) IPV4 ورژن شماره ٤ پروتوکل (Ipدر اینترنت مورد استفاده قرار می گیرد ولی با توجه به رشد سریع اینترنت و محدودیت آدرس دهی در این ورژن، IPV6 در آینده مورد استفاده قرار خواهد گرفت.

TCP :

مخفف . Transmission Control Protocol در این پروتوکل قبل از ارسال

داده ها، بین فرستنده و گیرنده یک ارتباط مجازی ایجاد می گردد .TCP به

هر بسته داده یک شماره سریال اختصاص می دهد در مقصد این شماره

سریالها بررسی می شود تا از دریافت تمامی بسته ها و ترتیب درست آنها

اطمینان حاصل شود. مقصد پس از دریافت هر بسته شماره بسته بعدی را به

مبدا اعلام می کند. مبدا در صورتی که پاسخ مناسبی از مقصد در مدت

زمان معینی دریافت نکند، بسته قبلی را مجددا ارسال خواهد کرد. بدین

ترتیب بسته ها با اطمینان کامل (از دریافت در مقصد) در اینترنت منتقل

می شوند.

HTTP :

مخفف . Hypertext Transfer Protocol این پروتوکل در وب مورد

استفاده قرار می گیرد. در این پروتوکل نحوه فرمت و چگونگی انتقال داده

ها مشخص می شود همچنین HTTP وظیفه وب سرور و مرورگر وب را

در مواجهه با هر دستور مشخص می کند. مثلا وقتی شما آدرس یک سایت را در مرورگر وب خود وارد می کنید یک دستور HTTP به وب سروری که صفحه مورد نظر شما در آن قرار دارد، فرستاده می شود و باعث می شود تا صفحه مورد نظر برای شما ارسال شود.

HTTPیک پروتوکل Stateless نامیده می شود زیرا هر دستور در آن بطور مستقل و بدون توجه به دستورات قبل و بعد از آن اجرا می شود. به همین دلیل است که ایجاد وب سایتهایی که متناسب با ورودی کاربر عکس العمل مناسب را انجام دهند، مشکل است. البته این نقیصه HTTP توسط برخی تکنیکها نظیر Cookie , JavaScript , Java , Activex برطرف شده است.

FTP :

مخفف . File Transfer Protocol از این پروتوکل در اینترنت برای تبادل فایلها استفاده می شود. عملکرد FTP نظیر عملکرد پروتوکل HTTP برای

دریافت یک صفحه وب از یک سرور یا SMTP برای انتقال نامه های

الکترونیکی در اینترنت است. این سه پروتوکل از پروتوکلهای تابعه TCP/IP

بشمار می آیند. از FTP غالبا برای دریافت فایل از یک سرور و یا ارسال

فایل به آن استفاده می شود (مثل ارسال صفحات وب ساخته شده از کاربر

به سرور).

Bridge :

وسیله ایست که دو Lan مختلف یا دو سگمنت از یک Lan را که از پروتوکل

ارتباطی یکسانی استفاده می کنند، به یکدیگر متصل می سازد. Bridge

توانایی کنترل ترافیک، فیلتر کردن بسته های داده و ... را دارد. توسط

Bridgeمی توان یک Lan با تعداد ایستگاههای کاری زیاد را به سگمنت های

کوچکتری تقسیم کرد که در نتیجه هر سگمنت مانند یک شبکه مستقل عمل

کرده و برقراری ارتباط ایستگاهها راحتتر انجام می شود. هرگاه دو ایستگاه

بطور همزمان اقدام به ارسال بسته های داده در شبکه کنند، تصادم

(collision)رخ می دهد که مانع ارسال صحیح داده می شود و هر چه

تعداد ایستگاهها بیشتر باشد، احتمال رخ دادن تصادم نیز بیشتر می گردد .

Bridgeبا تقسیم شبکه به چندین سگمنت از احتمال رخ دادن تصادم می کاهد. همچنین اگر پیامی از یک ایستگاه برای ایستگاهی دیگر در همان سگمنت ارسال شود Bridge مانع انتشار پیام در سگمنت های دیگر شده و بار ترافیک سایر سگمنت ها را سنگین نمی کند.

Repeater :

ساده ترین جزءِ ارتباطی در شبکه ، Lan که سیگنالهای ارتباطی در کابلها را تقویت یا دوباره سازی می کند Repeater ،می باشد. سیگنالهای ارتباطی در طول مسیر کابلها بر اثر عواملی مانند نویز و غیره دچار تغییر شکل و یا میرایی (ضعیف شدن تدریجی) می شوند. یک Repeater آنالوگ می تواند سیگنالهای دریافتی را تقویت نماید، در حالیکه Repeater دیجیتال توانایی بازسازی سیگنالهای دریافتی با کیفیتی نزدیک به کیفیت اصلی را داراست. با استفاده از Repeater ها می توان طول کابلهای داده را افزایش داد و در

نتیجه ایستگاههای کاری که در فاصله دورتری (البته تا حد معینی از فاصله) از یکدیگر واقعند را نیز می توان بهم متصل کرد که در نهایت باعث گسترش فیزیکی شبکه می شود.

Router :

وسیله ایست که وظیفه انتقال بسته های داده بین شبکه های مختلف را بر عهده دارد. یک روتر حداقل به دو شبکه WAN ، LAN و یا یک LAN و ISPمتصل است. روتر اصطلاحا Protocol Independent است؛ یعنی انتقال بسته های داده بین دو شبکه که از پروتوکلهای مختلف در ارتباطات داخلی خود استفاده می کنند، را نیز به درستی انجام می دهد. روترها در GATEWAY ، یعنی محل ارتباط دو شبکه قرار دارند.

در Header هر بسته داده، مشخصات ایستگاه گیرنده آن مشخص شده است. روتر پس از خواندن آدرس گیرنده، بر اساس جدول مسیریابی و الگوریتم های مسیریابی و با توجه به بار ترافیک شبکه، بسته را از کوتاهترین

و کم ترافیک ترین مسیر به مقصد می رساند. روترها برای تشخیص مسیر مناسب، توسط پروتوکلهایی نظیر ICMP با یکدیگر ارتباط برقرار می کنند.

دو نوع روتر داریم؛ روتر Static که جدول مسیریابی آن توسط مدیر شبکه مقدار دهی می شود و روتر Dynamic که جدول مسیریابی را خودش تنظیم می کند و بطور اتوماتیک آنرا Update می نماید. همچنین این روتر اطلاعات خود را با مسیریاب بعدی مبادله می کند.

Gateway :

Gateway؛ یک عضو در شبکه می باشد که به مثابه یک ورودی به شبکه ای دیگر است . طبق این تعریف ISP شما که باعث برقراری ارتباط شما با اینترنت می شود یک Gateway است Gateway .می تواند سخت افزاری یا نرم افزاری باشد و وظیفه اصلی آن تبدیل پروتوکل ها به یکدیگر است.

مثلا اگر شما در یک LAN از پروتوکلی خاص استفاده می کنید، برای اتصال به اینترنت احتیاج به Gateway دارید تا این پروتوکل را به پروتوکل مورد

استفاده در اینترنت تبدیل کند Gateway .همچنین به عنوان یک Proxy

Serverیا Firewall عمل می کند.

Hub :

وسیله ایست دارای چندین پورت که از آن برای اتصال ایستگاههای کاری

موجود در یک) LAN اعم از کامپیوتر، پرینتر و...) به یکدیگر استفاده می

شود. می توان عملکرد آنرا شبیه یک Repeater چند پورته (Multi Port)

دانست. هر ایستگاه توسط کابلی به یکی از پورتهای موجود در هاب متصل

می شود و به این طریق اطلاعات ارسالی از یک ایستگاه برای سایر ایستگاهها

قابل دسترسی خواهد بود. یک Passive Hub اطلاعات ارسالی از یک ایستگاه

را فقط به یک ایستگاه دیگر ارسال می کند) و نه سایر ایستگاهها) و در مقابل

Active Hub ،اطلاعات ورودی را روی همه پورتها کپی می کند و بدین

ترتیب اطلاعات برای همه ایستگاهها ارسال می شود. استفاده از هاب عمل

حذف و اضافه کردن ایستگاهها به شبکه را بدلیل عدم نیاز به پیکربندی

مجددف، آسانتر می سازد.

Port :

-1مجرایی است سخت افزاری برای ورود و خروج اطلاعات به کامپیوتر.

سوکت های موجود در پشت کیس کامپیوتر که وسایل جانبی به آنها متصل

می شوند، نمونه ای از پورتها به شمار می روند. دونوع پورت وجود دارد:

سریال و موازی.

-2در شبکه های مبتنی بر TCP/IP و) UDP منظور شبکه هایی است که در

ارتباطات خود از این دو پروتوکل استفاده می کنند) به نقطه پایانی یک

ارتباط منطقی، پورت اطلاق می شود. این نوع پورتها در نرم افزارها برای

ارتباطات شبکه‌ای استفاده می شوند و بر خلاف تعریف اول، این پورتها مکانی

فیزیکی و قابل رویت را اشغال نمی کنند و مفاهیمی انتزاعی اند.

-3تبدیل یک نرم افزار قابل اجرا در یک پلتفرم به نرم افزار قابل اجرا در

پلتفرم دیگر. مثلا تبدیل یک نرم افزار قابل اجرا در Windows به نرم افزاری قابل اجرا در Macintosh.

Parallel Port :

پورت موازی یکی از پورتهای موجود در پشت کیس کامپیوتر است که دارای ۲۵ پین (و نوع کانکتور(Female می باشد و برای اتصال وسایل جانبی نظیر پرینتر مورد استفاده قرار می گیرد. این پورت توانایی انتقال 8 بیت داده را بطور همزمان دارا می باشد و برای اتصال به این پورت از کانکتور ۲۵ پینی نوع DB-25 استفاده می شود. سرعت انتقال داده در آن ۸ برابر پورت سریال می باشد. انتقال اطلاعات توسط این پورت در فواصل بیشتر از ۶ متر قابلیت اعتماد کمتری دارد. نام دیگر این پورت LPT است.

Serial Port :

این پورت توانایی انتقال یک بیت داده در هر لحظه را دارد. برای اتصال وسایلی نظیر Mouse و Modem به کامپیوتر استفاده می شود. اکثر

پورتهای سریال از کانکتورهای نوع RS-232C یا RS-422 استفاده می کنند.

نام دیگر این پورت Communications Port یا به اختصار COM port است

که با نامهای COM1، COM2 و مانند آن شناخته می شوند.

Firewire :

این پورت سریال توانایی انتقال داده تا سرعت ٤٠٠ Mbsدر ١٣٩٤ (aو تا

800 Mbpsدر ١٣٩٤ (bرا دارا می باشد. نام دیگر این استاندارد

IEEE1394میباشد. این پورت توسط Apple ابداع و به کار گرفته شد و با

نام Firewire معرفی گردید ولی سایر شرکتها محصولات مبتنی بر

استاندارد IEEE 1394 خود را با نامهای دیگری از جمله I.LINK یا LYNX

بکار می برند. هر پورت ١٣٩٤ توانایی اتصال به ۶۳ وسیله خارجی دیگر را

دارد. علاوه بر سرعت بالا، این پورت از انتقال موازی داده بهره می برد در

نتیجه این پورت را به پورتی ایده آل برای دستگاههایی که احتیاج به انتقال

حجم زیادی از داده و real-time نیاز دارند (نظیر دوربین های دیجیتال

حرفه ای VCR ،ها ، دوربین های فیلمبرداری معمولی و (TV تبدیل می کند.

اگرچه این پورت انعطاف پذیری و سرعت بالایی دارد ولی قیمت آن نیز قابل توجه است. سرعت انتقال داده در این پورت از پورت SUB بسیار بیشتر است (حدودا ۳۰ برابر). این پورت مانند USB از Plug-And-Play و Hot-Pluggingپشتیبانی می کند. همچنین برق مورد نیاز دستگاههای متصل را تامین می کند.

Null Modem :

نوعی کابل که برای اتصال دو کامپیوتر به یکدیگر مورد استفاده قرار می گیرد. این کابل به پورت سریال دو دستگاه متصل شده و عمل انتقال داده را بدون نیاز به مودم انجام می دهد Null Modem .بخصوص برای کامپیوتر های پورتابل مناسب است چون بوسیله آن عمل انتقال داده با سایر کامپیوترها به آسانی و بدون نیاز به وسیله ارتباطی دیگری انجام می پذیرد.