آموزش CCNA

۱ فصل اول: مفاهیم شبکه و بررسی اجمالی لایه پیوند داده‌ها

در این فصل به مروری بر مفاهیم شبکه می پردازیم در مورد مدل OSI و لایه های آن، مدل TCP/IP و همچنین مفاهیم شبکه های محلی از جمله کابل کشی و سویچینگ آن صحبت می کنیم.

۱-۱ مدل OSI و مدل TCP/IP

به دلیل نبود حافظه اشتراکی در شبکه های کامپیوتری، تمام ارتباطات براساس تبادل پیام‌ها از طریق شبکه ارتباطی برقرار می‌شود زمانی که فرآیند الف درون یک ماشین می‌خواهد با فرآیند ب درون ماشینی دیگر ارتباط برقرار کند، ابتدا در فضای آدرس خودش یک پیام می‌سازد و سپس یک فراخوانی سیستم انجام می‌دهد تا سیستم عامل، بسته پیام را ارسال کند. البته بین دو فرآیند باید توافقاتی بر سر معنی بیت‌های ارسالی وجود داشته باشد. برای انجام بهتر این توافقات در سطوح مختلف سازمان جهانی استاندارد (ISO)[1] یک مدل مرجع با نام مدل ارتباطات سیستم باز (OSI)[2] ارائه کرده است. یک سیستم باز سیستمی است که بتواند تحت استانداردها و قواعدی که ساختار داده‌ها را مشخص می‌کند با هر سیستم باز دیگری ارتباط برقرار کند. این قواعد به پروتکل[3] معروف است.

1. International standard Organization

2. Open system interconnecion

3. Protocol

یک تقسیم‌بندی کلی در پروتکل‌ها وجود دارد. پروتکل‌های اتصال‌گرا[1] که در آن پیش از تبادل اطلاعات، مبدأ و مقصد بین خود یک مسیر برپا می‌کنند و ممکن است در مورد پروتکل‌ها نیز با هم توافق کنند و پس از تبادل اطلاعات مسیر را قطع می‌کنند. تلفن یک ارتباط اتصال‌گرا است. دسته دیگر پروتکل‌ها، بدون اتصال[2] هستند، که برای تبادل اطلاعات هیچ عملیات اولیه لازم نیست و فرستنده بسته اطلاعاتی خود را هر گاه حاضر شد به روی شبکه می‌فرستد. مانند انداختن یک نامه در صندوق پست.

در مدل OSI ارتباطات به هفت سطح یا لایه تقسیم شده است.

هر لایه با بخش مشخصی از عملیات ارتباطی سروکار دارد. بسته اطلاعاتی که در هر لایه می‌رسد با انجام عملیاتی به لایه زیرین ارسال می‌شود. مانند اینکه هر لایه یک سرآیند[3] به بسته اضافه می‌کند. و در سمت مقصد نیز هر لایه سرآیند مربوط را حذف می‌کند. اعمال لازم را انجام می‌دهد و بسته را به لایه بالایی می‌فرستد. به دلیل اینکه هر لایه برای خود پروتکل یا پروتکل‌هایی دارد به این مدل لایه‌ای پشته پروتکلی[4] نیز گفته می‌شود.

معمولا لایه های این مدل از پایین به بالا شماره‌گذاری می‌شوند. یکی از دلایل آن اینست که معمولا اشکال زدایی از شبکه از پایین به بالا انجام می پذیرد. سه لایه پایین دارای پروتکل‌های سطح پایین هستند.لایه‌ها از پایین به این شرح هستند.

---

4. Connection oriented

5. Connectionless

6. header

7. Protocol stack

۱ – لایه فیزیکی[۱] : روی ارسال و دریافت صفر ویک‌ها تأکید دارد و استانداردهای آن را مانند سطح ولتاژ، سرعت انتقال و ... در اختیار دارد. و به معنی بیت‌ها کاری ندارد.

۲ – لایه پیوند داده‌ها: داده‌ها را در قالب یک سری قاب[۲] ارسال می‌کند که در هر قاب قابلیت تشخیص خطا نیز وجود دارد.

۳ – لایه شبکه[۳]: وظیفه اصلی این لایه مسیریابی است که در شبکه‌های محلی مطرح نیست. پر استفاده ترین پروتکل این لایه در حال حاضر IP[۴] است. که یک پروتکل بدون اتصال می‌باشد. در مقابل پروتکلی با نام کانال مجازی[۵] وجود دارد که در شبکه‌های ATM استفاده می‌شود که پروتکلی اتصال‌گرا است.

۴ – لایه انتقال[۶]: این لایه آخرین لایه از لایه‌های زیر بنایی شبکه است.

این لایه اطلاعات لایه‌های بالاتر را به قسمت‌های مناسبی تقسیم می‌کند و آن‌ها را به لایه‌های پایین‌تر می‌فرستد.

در اینجا نیز مجدداً رخداد خطا چک می‌شود. مهمترین پروتکل‌های این لایه TCP[۱] و UDP[۲] هستند اولی اتصال گرا و دومی بدون اتصال است. یک

---

8. Physical layer

9. Frame

۳. Network layer

۴. Internet protocol

۵. virtual channel

۶. Transport layer

پروتکل دیگر که مورد استفاده قرار می‌گیرد RTP[۳] است که پروتکلی مخصوص ارسال داده‌های فوری و زمان حال هستند (مانند صوت و تصویر) که گارانتی برای ارسال کامل بسته‌ها را انجام نمی‌دهد اما روی ارسال داده کنترل و نظارت دارد.

سه لایه باقیمانده حاوی پروتکل‌های سطح بالا هستند.

۵- لایه جلسه[۴]: لایه جلسه در حقیقت مدل پیشرفته لایه انتقال است. اعمالی نظیر کنترل گفتگو و امکانات همزمانی و نگهداری اطلاعات در مورد ارسال اطلاعات و امکان قراردادن نقاط بررسی[۵] در مسیرهای طولانی است. که در صورت خراب شدن ارسال از آخرین نقطه بررسی ادامه دهد. بسیاری از برنامه‌های کاربردی به این لایه علاقه ندارند و آن را پشتیبانی نمی‌کنند.

۶- لایه ارائه[۶]: لایه ارائه روی کدها و استانداردهای ارائه اطلاعات توافق می‌کند تا فرستنده و گیرنده بر سر معنی داده‌های ارسالی توافق داشته باشند.

۷- لایه کاربرد[۱]: مجموعه‌ای از برنامه‌های کاربردی شبکه حل پست الکترونیکی FTP[۲] و HTTP[۳] و ...

---

۱. Transmission Control protocol

۲. Universal datagram protocol

۳. Realtime transport protocol

۴. Session Layer

۵. Check point

۶. Presentation layer

در سه لایه سطح بالا داده‌ها ساختاری یکپارچه برای داده‌ها وجود دارد. برای مثال در این سه لایه با یک فایل به شکل یک عنصر واحد برخورد می‌شود. اما در لایه‌های پایین‌تر، داده ها به قطعات کوچکتری تقسیم می‌گردند تا انتقال آن‌ها در شبکه آسان‌تر باشد. در هر لایه به این قطعات داده یک نام اطلاق می‌گردد. در لایه فیزیکی، داده ها در سطح بیت هستند. اما بخش‌های داده در لایه انتقال، قطعه[۴]، در لایه شبکه، بسته[۵] و در لایه پیوند داده‌ها، قاب[۶] نامیده می‌شوند.به واحد اندازه‌گیری داده در هر لایه اصطلاحا PDU گفته می‌شود. در این لایه‌ها داده ای که از لایه بالاتر دریافت می‌شود، اصطلاحا کپسوله[۷] می‌گردد. به این معنی که داده ها در یک بسته جدید قرار می گیرد و به ابتدا و در برخی موارد انتهایش داده‌هایی اضافه می‌گردد. مانند یک بسته پستی که در بسته بزرگتری قرار می‌گیرد و ارسال می‌شود. به داده‌های ابتدایی سرآیند[۸] و به داده‌هایی که در انتها اضافه می‌گردد، پی‌آیند[۹] گفته می‌شود.به عبارت دیگر هر لایه از محتوای داخلی لایه بالاتر اطلاع ندارد و تنها وظیفه ارسال آن را بر عهده دارد.

---

۱. Application loyer

۲. File Transfer Protocol

۳. HyperText Transfer Protocol

۴.Segment

۵. Packet

۶. Frame

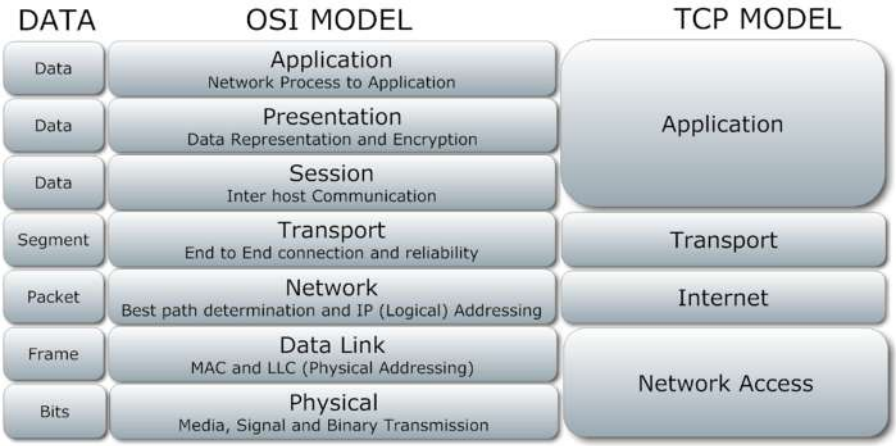
۷.Encapsulate

۸.Header

۹.Trailer

TCP/IP در ابتدا مدلی برای شبکه نظامی وزارت دفاع ایالات متحده آمریکا بود. پس از اینکه این مدل از حالت نظامی خارج شد، تبدیل به پشته پروتکلی مورد استفاده در Unix گردید و بعدها توسط مایکرسافت نیز مورد استفاده قرار گرفت.

این پشته پروتکلی از چهار لایه تشکیل شده. لایه اول که لایه دسترسی به شبکه[۱]نام گرفته است، معادل لایه‌های فیزیکی و پیوند داده ها از مدل OSI می‌باشد. لایه دوم لایه اینترنت نام دارد که معادل لایه شبکه است. لایه سوم، لایه انتقال است و در نهایت لایه های جلسه، ارائه و کاربرد از مدل OSI ادغام شده اند و به عنوان لایه چهارم یعنی لایه کاربرد در TCP/IP به کار می‌روند.



شکل ۱-۱ لایه های مدل OSI و TCP/IP[14]

۱. Network Access

۱-۲ انواع توپولوژی‌های شبکه

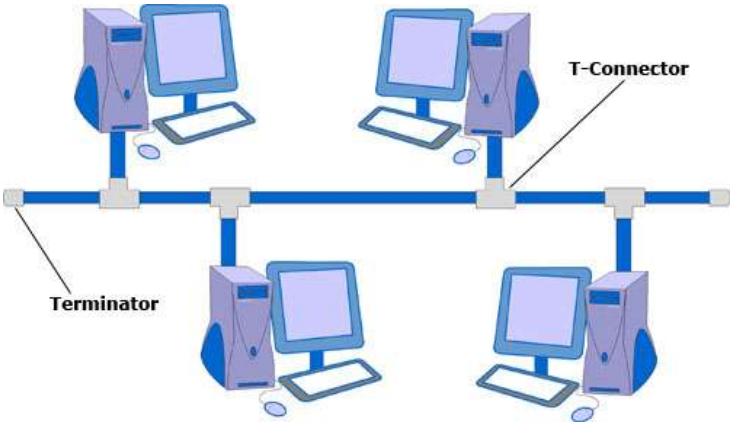
شبکه های محلی[۱] از پرکاربردترین انواع شبکه های کامپیوتری هستند که در محدوده‌ای مانند یک اتاق، ساختمان یا شرکت نصب می‌گردد. اصولابرای اتصال کامپیوترها به یک شبکه بایستی یک رسانه انتقال داده وجود داشته باشد. این رسانه می تواند کابل مسی، فیبر نوری یا امواج بی‌سیم باشند. برای اینکه کامپیوتر بتواند به این رسانه متصل شود و عملیات تبدیل صفر و یک با سیگنال‌های قابل انتقال در رسانه انجام گیرد (و بالعکس) به سخت افزاری تحت عنوانکنترل‌گر واسط شبکه[۲]یا به اختصار (NIC) نیاز داریم. هر NIC یک محل برای ارتباط با رسانه ارتباطی است. مثال‌هایی از NIC را می‌توان نام برد. مانند مودم، کارت شبکه کامپیوتر و پورت های سوییچ.

یکی ازاولین مواردی که باید برای راه‌اندازی یک شبکه محلی مشخص شود، چگونگی قرار گیری و اتصال کامپیوترهای درون شبکه به هم یا اصطلاحا توپولوژی است.مهم‌ترین توپولوژی‌های مورد استفاده به شرح زیر است:

توپولوژی گذرگاه (BUS): یک مسیر ارتباطی مشترک تحت عنوان گذرگاه در این توپولوژی وجود دارد که همه کامپیوترها به آن متصل می‌شوند. مانند یک خیابان که درب همه خانه‌ها به آن باز می‌شود و همه اعضای این خانه‌ها از طریق این مسیر مشترک با هم ارتباط برقرار می کنند.

۱. Local Area Network(LAN)

۲. Network Interface Controler

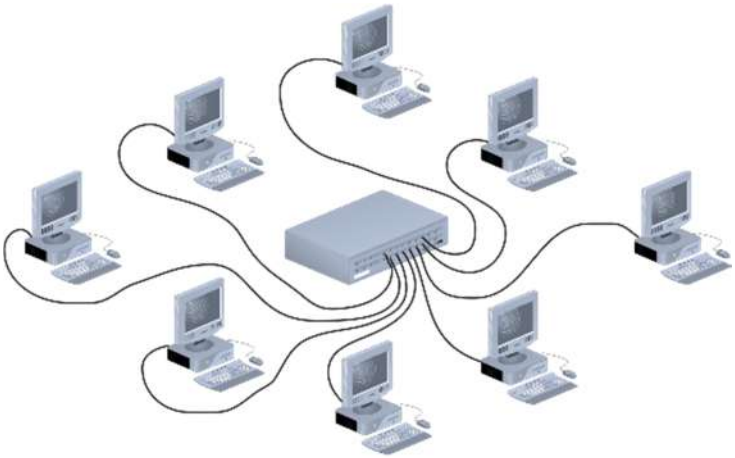


شکل ۱-۲ توپولوژی گذرگاه [10]

هر NIC توسط قطعه‌ای به نام T-Connector به گذرگاه مشترک متصل می‌گردد. در هر دو انتهای گذرگاه نیز قطعه‌ای به نام Terminator وجود دارد که در واقع یک مقاومت به همراه یک خازن است که باعث می شود جریان الکتریکی به شکل درست در سیم مسی در جریان باشد. مشخص است که هر کامپیوتر که بسته های داده را روی گذرگاه مشترک ارسال می کند. این بسته به همه کامپیوترها می رسد و هر کامپیوتر آدرس مقصد بسته را بررسی می‌کند و در صورتی که متعلق به خود بود آن را می‌خواند. این مساله باعث می‌شود که تعداد کامپیوترهای درون یک شبکه با توپولوژی گذرگاه هر چه بیشتر شود، ترافیک هم به صورت تصاعدی بالا رود. ضمنا یک مشکل مهم در توپولوژی گذرگاه این است که اگر بخشی از این گذرگاه قطع گردد، کل شبکه از کار می‌افتد.

توپولوژی ستاره (Star): در این توپولوژی همه ماشین‌ها به یک دستگاه مرکزی متصل می‌شوند. به این ترتیب ممکن است در مجموع کابل بیشتری

استفاده شود. اما اگر یکی از کابل های بین یک ماشین و دستگاه مرکزی قطع گردد، در بقیه شبکه ارتباط قطع نمی‌گردد. به همین دلیل امروزه خیلی کم پیش میاید که شبکه‌ای ببینیم که با توپولوژی گذرگاه بسته شده باشد. در عوض در بسیاری از شبکه‌های محلی از توپولوژی ستاره استفاده می‌گردد.



شکل ۱-۳ توپولوژی ستاره [11]

دستگاه مرکزی مورد استفاده در این توپولوژی می تواند از نوع Hub باشد. درون این دستگاه یک نوع گذرگاه مشترک وجود دارد. به عبارت دیگر هر پیامی که از یک پورت آن وارد شود از تمامی پورتهای دیگر خارج خواهد شد. بنابر این در زمان استفاده از Hub در توپولوژی ستاره‌ای، مانند توپولوژی گذرگاه بسته ارسالی از یک ماشین به همه ماشین های درون آن شبکه می‌رسد. به عبارت دیگر یک شبکه با توپولوژی ستاره‌ای که از Hub استفاده می‌کند، از نظر منطقی یک گذرگاه (BUS) است.

اگر به جای Hub از دستگاه دیگری به نام سوییچ[۱] استفاده شود، این امکان به وجود می‌آید که بسته ارسالی به جای اینکه به همه کامپیوترها ارسال شود، تنها به سمت مقصد هدایت گردد. به همین دلیل در حال حاضر بیشتر به جای Hub از سوییچ استفاده می‌گردد. در این مورد چگونگی عملکرد سوییچ در ادامه بیشتر صحبت خواهیم کرد.

اگر تعداد ماشین‌ها بیش از تعداد پورت‌های سوییچ باشد، بایستی از دو یا چند سوییچ استفاده کنیم. با اتصال چند سوییچ (یا Hub) به هم توپولوژی ستاره‌ای گسترش یافته[۲] تشکیل می‌گردد. معمولا هر سوییچ یک یا دو پورت دارد که به Uplink موسوم است. این پورت‌ها معمولا نسبت به پورتهای دیگر سوییچ سرعت بالاتری دارند.برای اتصال سوییچها به هم معمولا از این Uplinkها استفاده می‌شود. برای اتصال سوییچ‌ها به هم دو روش وجود دارد. روش اول این است که پورت Uplink هر سوییچ را به یک پورت(در صورت امکان Uplink) سوییچ بعدی زده شود. در این حالت سوییچ‌ها به شکل سری به هم متصل می‌شوند. این روش این مشکل اساسی را دارد که اگر در بین راه یکی از کابل‌های ارتباطی بین سوییچ‌ها قطع شود یا یکی از سوییچ‌ها از سرویس خارج گردد. کل شبکه به دو قسمت تقسیم می‌شود و امکان ارتباط بسیاری از ماشین‌ها با هم از بین می‌رود.

راه دوم این است که از پورت Uplink تمامی سوییچ‌ها به یک سوییچ مرکزی یک کابل، متصل شود. این سوییچ مرکزی که به آن سوییچ هسته[۳]

۱.Switch

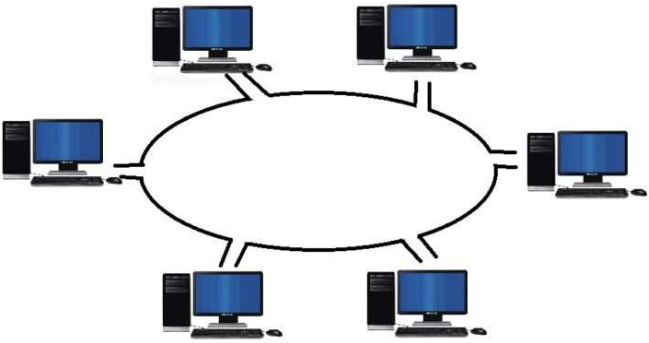
۲.Expanded Star

۳.Core Switch

گفته می‌شود، معمولا از سرعت بالاتری نسبت به سوییچ‌های دیگر در شبکه برخوردار است. به سوییچ هسته و مجموعه اتصالات از سوییچ‌های غیر هسته به آن، ستون فقرات[۴] شبکه گفته می‌شود.

توپولوژی حلقه (Ring)

توپولوژی حلقه مانند توپولوژی گذرگاه اکنون تنها در موارد خاص استفاده می شود. از نظر ساختار مانند یک گذرگاه است که ابتدا و انتهایش به هم متصل شده و تشکیل یک حلقه را داده است.



شکل ۱-۴ توپولوژی حلقه[12]

یک سطح ولتاژ ثابت است که به آن اصطلاحا Token گفته می‌شود. هر کامپیوتر این ولتاژ را دریافت کند، اگر در آن لحظه داده‌ای برای ارسال نداشته باشد آن ولتاژ را عینا به خروجی منتقل می‌کند. اصطلاحا Token را به ماشین بعدی پاس می‌دهد. اما اگر داده‌ای برای ارسال داشته باشد. به

[۴].Backbone

جای Token، داده خود را ارسال می کند.اصطلاحا Token را حبس می‌کنند. در پایان رسال داده ها، دوباره سطح ولتاژ ارسالی را به ولتاژ Token باز می‌گردانند تا Token به ماشین بعدی برود.

مزیت این توپولوژی این است که در هر حالت تنها یک ماشین در حال نوشتن است. اما در دو توپولوژی قبل این امکان وجود دارد که دو ماشین، همزمان آغاز با ارسال داده کنند و حالت برخورد[۵] رخ دهد و هر دو داده خراب شوند. در مورد مقابله با حالت برخورد در ادامه صحبت خواهیم نمود.

روش حلقه در پیاده‌سازی مشکلاتی مانند گذرگاه دارد که باعث شده کماکان پرطرفدارترین توپولوژی بین طراحان و اجراکنندگان شبکه‌های محلی همان روش ستاره‌ای باشد.

۱-۳ کابل‌های مورد استفاده در شبکه‌های محلی

در شبکه های محلی معمولا برای رسانه ارتباطی از کابل‌های مختلف استفاده می‌شود.

کابل مورد استفاده در توپولوژی گذرگاه، کابلی مسی از نوع "Coaxial" است. دو نوع کابل Coaxial وجود دارد:

نوع اول به Thinnet یا 10Base2 معروف است. از نظر ظاهری قابل انعطاف و نسبتا نازک است (مانند کابل آنتن تصویری) حداکثر ارسال داده‌ای که تضمین می‌کند، ۱۰ مگابیت بر ثانیه است. به شرطی که طول کابل از

۵. Collision

۲۰۰ متر بیشتر نشود. در صورت افزایش طول بیش از ۲۰۰ متر نرخ ارسال داده به تدریج کم خواهد شد.

نوع دوم به Thicknet یا 10Base5 معروف است. از نظر ظاهری ضخیم‌تر است و به انعطاف کمی دارد. پس کار با آن سخت‌تر است. اما نرخ ارسال ۱۰ مگابیت بر ثانیه را تا مسافت ۵۰۰ متر تضمین می‌کند.

شکل ۱-۵ کابل‌های Coaxial[13]

اما در توپولوژی حلقه و ستاره‌ای معمولا از کابل‌های به هم تابیده یا به اختصار TP[۶] استفاده می‌شود. در این کابل‌ها زوج سیم‌های به هم تابیده استفاده می‌شود. این نوع تابیدن زوج‌ها به هم علاوه بر اینکه سیمهارا قویتر

۶.Twisted Pair

می‌کند جلوی نفوذ امواج پارازیتی خارجی را تا حد زیادی می‌گیرد. اصطلاحا جلوی القای بار جانبی گرفته می‌شود. این کابل‌ها معمولا در سه نوع اصلی تولید می‌شوند. کابل UTP[۷] و کابل STP[۸] و کابل FTP[۹]. کابل UTP تنها رشته‌های به هم تابیده است که توسط یک روکش پلاستیکی پوشیده شده. کابل STP روی کابلهای به هم تابیده، رشته های فلزی قرار دارد که کار نویزگیری بیشتر و محافظت سیم‌ها در برابر شکستگی و قطع شدگی را بر عهده دارند. در کابل FTP روی هر سیم به هم تابیده یک لایه فویل قرار دارد که علاوه بر نویزگیری، مقاومت دربرابر آتش را بالا می‌برد. طراح شبکه بنا به وضعیت و مکان قرارگیری، یکی از انواع گفته شده را انتخاب می‌کند.

شکل ۱-۶ کابلهای TP[13]

۷.Unshielded Twisted Pair

۸.Shielded Twisted Pair

۹.FoiledTwisted Pair

شکل ۱-۷ سوکت‌های مهم متصل به کابل‌های TP (RJ-11 و RJ-45) [13]

اما کابل‌ها از نظر میزان عبور داده و تعداد زوج سیم‌ها به چند دسته (Category) یا به اختصار Cat تقسیم می‌شوند.

دسته بندی	نام استاندارد	سرعت	تعداد زوج	نوع سوکت
Cat-1	-	64 Kb/s	۱	RJ-11
Cat-2	-	64 Kb/s	۴	RJ-45
Cat-3	10BaseT	10Mb/s	۴	RJ-45
Cat-4	-	16 Mb/s	۴	RJ-45
Cat-5	100BaseT	100 Mb/s	۴	RJ-45
Cat-5e	1GBaseT	1 Gb/s	۴	RJ-45
Cat-6	1GBaseT	1 Gb/s	۴	RJ-

				45
Cat-6A	10GBaseT	10 Gb/s	۴	RJ-45

جدول ۱-۱ دسته بندی سیم‌های به هم تابیده

در حال حاضر معمولا از کابل‌های Cat-5 به بعد در راه‌اندازی شبکه‌ها استفاده می‌گردد.

اما در برخی موارد به جای کابل مسی از فیبر نوری برای ارتباط استفاده می‌شود. فیبر نوری دارای مزایایی و معایبی نسبت به کابل مسی است.

در فیبر نوری به دلیل استفاده از سیگنال نوری، می توانیم داده را در مسافت بیشتری ارسال کنیم. ضمنا این سیگنالهای نوری دربرابر نویز و پارازیت تاثیر نمی‌پذیرند. از همه مهمتر، امنیت عبور داده از فیبر نوری بالا است. روی کابل‌های مسی می‌توان به وسیله گیره‌های جاسوسی که به آنها اصطلاحا Spy Vampire گفته می‌شود. از میانه سیم یک مسیر گرفت و داده ها را علاوه بر مقصد اصلی دریافت کرد. به این کار در مقوله امنیت داده Sniff کردن گفته می‌شود. اما چنین کاری در فیبرهای نوری ممکن نیست.

اما استفاده از فیبر نوری گران و دارای محدودیت است. اولا فیبرها دارای انعطاف محدود هستند و نباید در طول مسیر زیاد از حد خم یا تا شوند. ضمنا اتصالاتی که به این فیبر متصل می‌شود به راحتی کابل مسی نیست. در کابل مسی به راحتی و با یک آچار مخصوص سوکت‌ها را متصل می‌کنیم. اما در فیبر نوری، اتصالات توسط دستگاهی به نام فیوژن متصل می‌گردند. این دستگاه توسط روشی به نام جوش فیوژن،

اتصالات را به نحوی به فیبر نوری جوش می‌دهد و یک ساختار یکپارچه می‌سازد.

فیبرهای نوری در دو مد تکی[۱۰] و چندگانه[۱۱] وجود دارند. در مد تکی، یک سیگنال نوری توسط منبع نوری لیزری تولید می‌شود و برای ارسال سیگنال در مسیرهای طولانی طراحی شده. در این مد از فیبرهای نوری تا مسافت ۷۰ کیاومتر استفاده شده است. در صورتی‌که از فیبر نوری تکی در مسافت خیلی کوتاه استفاده گردد، ممکن است انرژی بالای لیزر باعث سوختگی ماژول‌های مورد استفاده گردد.

در مد چندگانه معمولا به جای لیزر از LED استفاده می شود و چند سیگنال همزمان ارسال می‌گردند که با توجه به فرکانس‌های مختلف و با استفاده از شکست نور قابل ترکیب و تفکیک هستند. این نوع فیبر برای مسافت‌های کوتاه و در حد داخل یک مجموعه استفاده می‌شود.

سرعت انتقال داده در فیبر نوری تا میزان 10 Gb/s است.

۱-۴ برخورد (Collision) و مقابله با آن

در بخش توضیح توپولوژی‌های شبکه گفتیم که اگر دو ماشین در یک شبکه همزمان داده را روی رسانه مشترک ارسال نمایند، برخورد رخ می‌دهد و داده با خطا مواجه خواهد شد.

یکی از راه‌ها برای رخ ندادن برخورد استفاده از یک توپولوژی بدون برخورد[۱۲] مانند توپولوژی حلقه است. اما در صورت استفاده از توپولوژی گذرگاه یا ستاره‌ای، امکان بروز برخورد وجود دارد. بنابر این باید این

---

۱۰. Single-Mode

۱۱. Multi-Mode

۱۲. Collision Free

برخورد تشخیص داده و در مقابل آن تمهدات لازم اندیشیده شود. یکی از روش‌های استاندارد موجود که برای این حالت، مورد استفاده قرار می‌گیرد، CSMA/CD[۱۳] است.

در این روش هر ماشین که بخواهد روی رسانه اشتراکی داده‌ای ارسال کنم ابتدا به رسانه گوش می‌کند که ببیند آیا در حال حاضر روی رسانه داده‌ای در حال انتقال است یا خیر. به این مرحله Listening گفته می‌شود. پس از اینکه فرستنده تشخیص داد که رسانه آزاد است، داده مورد نظر را ارسال می‌کند. مساله زمانی رخ می‌دهد که دو فرستنده همزمان، رسانه را آزاد تشخیص دهند و با فاصله زمانی ناچیز شروع به ارسال داده نمایند. در این حالت است که برخورد رخ می‌دهد. بنابر این هر فرستنده در طول زمان ارسال داده وارد فاز تشخیص برخورد خواهد شد. به عبارت دیگر همزمان با ارسال داده به رسانه آن را بررسی می‌کند که آیا همان داده از روی رسانه خوانده می‌شود یا خیر. این عمل توسط پایه LoopBack انجام می‌شود. این پایه در زمان ارسال داده، همزمان رسانه انتقال را می‌خواند و داده را به درون کارت شبکه باز می‌گرداند. اگر دو یا چند فرستنده با هم روی رسانه داده ارسال کنند، هر کدام از آنها داده‌ای متفاوت با داده خود می بینند. در این حالت هر فرستنده‌ای که متوجه برخورد شود، ارسال داده خود را قطع می کند. ضمنا برای اینکه مطمئن شود اعضای دیگر شبکه که ممکن است گیرنده داده باشند، حتما از نامعتبر بودن داده با خبر شده اند، یک سیگنال خبری به نام سیگنال مخدوش[۱۴]ارسال می‌کند. این سیگنال

---

۱۳. Carrier Sense Multiple Access with Collision Detection

۱۴. Jam Signal

داده معمولا متفاوت با داده‌هایی می گردد که هر کدام از فرستنده‌ها ارسال کردند و یک ساختار ۳۲ بیتی مشخص است. پس از آن فرستنده بسته داده مخدوش شده را پس از یک مدت زمان تصادفی، مجددا ارسال می‌نماید.

یکی از راه‌هایی که در یک ارتباط نقطه به نقطه[۱۵] بین دو ماشین، باعث جلوگیری از برخورد می گردد، استفاده از ارتباط نیمه‌دوطرفه[۱۶] به جای تمام‌دوطرفه[۱۷] است. در ارتباط نیمه دو طرفه. هر طرف این ارتباط در یک لحظه می‌تواند فرستنده یا گیرنده باشد. به عبارت دیگر همزمان نمی‌توان هم فرستاد و هم دریافت نمود. بنابر این هیچ‌گاه حالتی رخ نمی‌دهد که هر دو طرف ارتباط فرستنده باشند و در نتیجه برخورد رخ نمی دهد. در روش نیمه دو طرفه، گیرنده به مسیر ارتباطی گوش می کند. تا زمانی که داده ارسال شود، داده را دریافت می‌نماید. زمانی که فرستنده پایان ارسال را اعلام کند، جای فرستنده و گیرنده عوض می‌شود و این روال ادامه دارد. به همین دلیل تاخیر نسبت به روش تمام دوطرفه، بیشتر است. هر چند که سرعت انتقال داده تفاوتی نداشته باشد. در حال حاضر ارتباطات بی‌سیم معمول به صورت نیمه دو طرفه برقرار می گردد.

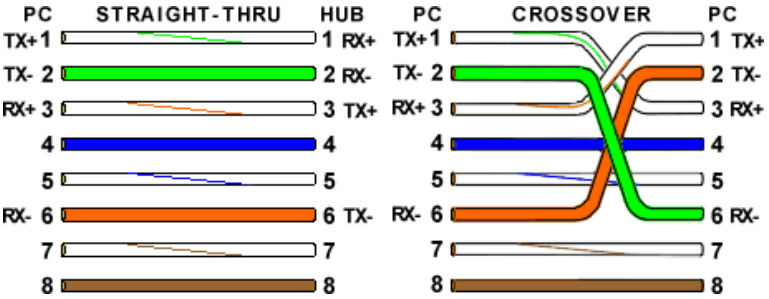
در ارتباط دو ماشین با کابل هم می توان ارتباط نیمه دو طرفه و تمام دو طرفه داشت. در حالت تمام دو طرفه، هر دو بایستی بتوانند همزمان داده ارسال و دریافت کند و برخورد رخ ندهد. به همین دلیل پایه ارسال

۱۵.Point to Point

۱۶.Half Duplex

۱۷.Full Duplex

و دریافت هم NIC مشخص است و در ارتباط تمام دوطرفه بین دو ماشین کابل ارتباطی طوری ساخته می‌شود که پایه ارسال هر طرف به پایه دریافت طرف مقابل متصل شده باشد. به چنین کابلی، کابل متقاطع[۱۸] گفته می‌شود. اما اگر ماشین‌ها به یک عنصر مرکزی مانند Hub متصل شده باشند، این عنصر وظیفه دارد داده های دریافتی از پایه ارسال یک ماشین را به پایه دریافت سایر ماشین‌ها برساند. پس در این حال به کابل مستقیم[۱۹] نیاز داریم.



شکل ۱-۸ کابل مستقیم و متقاطع [15]

توجه بفرمایید که معمولا در شماره گذاری کابل‌ها از این روش استفاده می‌شود که سوکت را طوری می گیریم که پین‌های فلزیش رو به بالا باشند. حال سیمی که به اولین پین از سمت چپ متصل می‌گردد، شماره ۱ محسوب می‌شود.

یک تکنولوژی در برخی کارتهای شبکه وجود دارد به نام Auto-MDIX[۲۰]که در آن، اگر در زمان ارسال مکررا برخورد روی دهد، جای

۱۸.Crossover

۱۹.Straight

۲۰.Auto-Media Dependent Interface X

پایه‌های ارسال و دریافت را عوض می‌کند. اگر دو ماشینی که می‌خواهند ارتباط نقطه به نقطه داشته باشند، از کارت‌های شبکه با این تکنولوژی استفاده نمایند، دیگر اجباری به استفاده از کابل متقاطع نیست و با کابل مستقیم هم قادر به برقراری ارتباط خواهند بود. به این کارت‌های شبکه گاهی MDIX Support هم گفته می‌شود.

۱-۵ چگونگی عملکرد سوییچ

همانطور که گفته شد، Hub هر داده‌ای را که روی یک پورت ورودی دریافت می کند روی تمام پورت‌های دیگر تکرار می‌نماید. به عبارت دیگر از معنی داده‌ها اطلاعی ندارد. اصطلاحا گفته می‌شود که Hub دستگاهی هست که در سطح لایه ۱ کار می‌کند. اما گفته شد که در سوییچ این امکان وجود دارد که داده تنها از پورتی خارج شود که به ماشین مقصد متصل است. به عبارت دیگر سوییچ بخشی از معنی داده را متوجه می‌شود و به کمک آن می‌تواند آدرس مقصد را تشخیص دهد. به عبارت دیگر سوییچ علاوه بر لایه ۱ در سطح لایه ۲ نیز عمل می‌کند. سوییچ قاب‌ها یا همان فریم‌های داده را تشخیص می‌دهد. در سرآیند هر فریم آدرس مبدا و آدرس مقصد آن فریم وجود دارد. این آدرس که در لایه ۲ تعریف شده است، به MAC Address[۲۱]معروف است. در مورد ساختار این آدرس در ادامه، توضیح داده خواهد شد.

زمانی که یک سوییچ آغاز به کار می‌کند، هیچ اطلاعاتی از مبدأ و مقصدها ندارد. یعنی مانند Hub مجبور است هر فریمی دریافت کرد، به

Access Control

همه پورت‌های دیگرش ارسال کند. اما با دریافت یک فریم روی یک پورت، آدرس مبدا آن فریم به همراه شماره پورت را در جدولی موسوم به MAC Address Table ثبت می‌کند. با پر شدن این جدول، مشخص می‌گردد که آدرس ماشین متصل به هر پورت چیست. لذا می‌تواند با توجه به آدرس مقصد، فریم‌ها را تنها روی پورتی ارسال کند که به ماشین مقصد متصل است.این جدول معمولا در حافظه RAM دستگاه قرار دارد. به این معنی که با قطع جریان برق یا Restart کردن سوییچ، جدول پاک می‌شود. به عملیات ثبت MAC Address توسط سوییچ اصطلاحا Learning گفته می‌شود.

در سوییچ‌های سیسکو به این جدول، CAM Table[۲۲] گفته می‌شود. هر سطر از جدول در صورتی که ۳۰۰ ثانیه از آن آدرس هیچ بسته‌ای ارسال نشود، حذف می‌گردد.

استفاده از سوییچ به جای Hub علاوه بر اینکه ترافیک داده‌ها را پایین می‌آورد در امنیت و مدیریت داده تاثیر بسیار مثبتی دارد. به عنوان مثال زمانی که هر فریم ارسالی به همه ماشین‌ها می‌رسد، داده ها را در معرض دید ماشین‌هایی قرار می‌دهد که مقصد داده نیستند. ممکن است در یکی از ماشین‌ها یک نرم افزاری جاسوسی برای دسترسی غیر مجاز به داده ها قرار گرفته باشد. برای مثال نرم‌افزار تحلیل‌گر Wireshark می تواند داده‌های ورودی و خروجی از یک کارت شبکه را مشاهده و تحلیل کند. در زمانی که از توپولوژی گذرگاه استفاده می‌کنیم یا در توپولوژی ستاره‌ای هاب به کار می‌بریم، به دلیل اینکه تمامی فریم‌های منتقل شده در شبکه به هر ماشینی می‌رسد، از این

۲۲.Content addressable memory

نرم‌افزار برای sniff کردن داده‌ها هم می‌توان استفاده نمود. اما زمانی که سوییچ استفاده شود، به هر ماشین تنها فریم‌های داده‌ای می‌رسد که متعلق به اوست و داده‌های دیگر در دسترس نیست که قابل دسترسی غیر مجاز باشد.

یکی از حمله هایی که ممکن است به سوییچ شود تا کار آن را مختل کند، ارسال تعداد زیادی از آدرس های تقلبی موسوم به (Mac Fake)در زمانی کوتاه به سوییچ است. این عمل باعث پر شدن حافظه RAM تخصیص یافته به MAC Table می‌شود و سوییچ قادر به ثبت آدرس‌های واقعی نمی گردد.

در بسیاری از موارد به ویژه در مکان‌هایی که امنیت مهم‌تر است. این Mac Table به شکل دستی نوشته و به‌هنگام‌رسانی می‌شود. سپس امکان Learning به صورت خودکار غیر فعال می‌گردد. لذا حمله فوق و نظایر آن امکان نیست. اما در این حالت باید ماشین‌ها در شبکه ثابت باشند. برای نمونه اگر ماشینی به شبکه اضافه شود یا محل ماشینی تغییر یابد و به پورتی متفاوت از سوییچ وصل گردد. جدول سوییچ بایستی به صورت دستی به‌هنگام شود.