

مدل TCP/IP آشنائی با مدل TCP/IP لایه‌ها و پروتکل‌ها

مدل TCP/IP پیش از مدل OSI توسعه پیدا کرده است. مدل TCP/IP دارای معماری دقیقاً شبیه به معماری مدل OSI نیست.

مدل TCP/IP متشکل از پنج لایه به شرح زیر است:

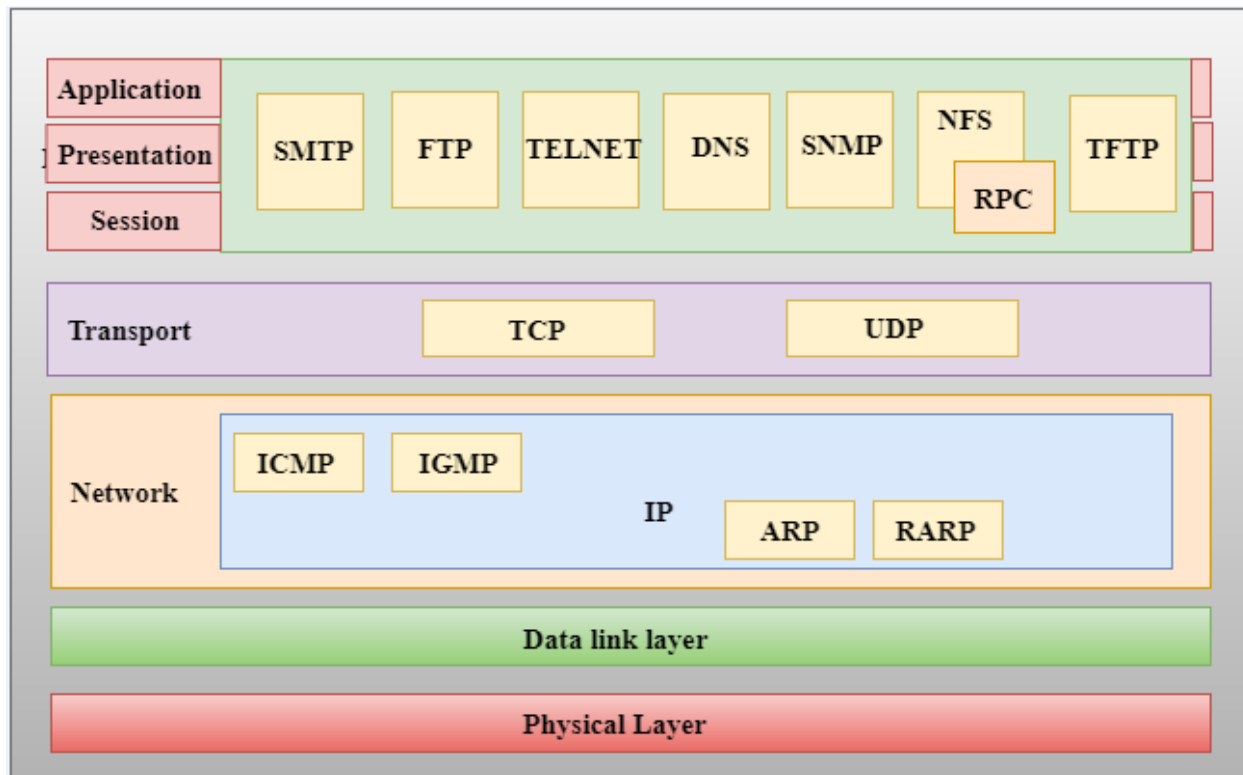
- لایه اپلیکیشن (Application Layer) ؛
- لایه انتقال (Transport Layer) ؛
- لایه شبکه (Network Layer) ؛
- لایه دیتالینک (Data Link Layer) ؛
- لایه فیزیکی (Physical Layer) ؛

چهار لایه ابتدائی (از پائین) استانداردهای فیزیکی لازم برای انجام کار، رابط کاربری شبکه، شبکه‌بندی داخلی و عملکردهای انتقالی را مطابق با چهار لایه ابتدائی مدل OSI پوشش می‌دهند. این چهار لایه در مدل TCP/IP به وسیله یک لایه منفرد که به نام «لایه اپلیکیشن (Application Layer)» نامیده می‌شود نامیده می‌شوند.

عملکردهای مدل TCP/IP

مدل TCP/IP از یک ساختار سلسله مراتبی استفاده می‌کند که سبب می‌شود ماژول‌های تعاملی ایجاد شود، این ماژول‌ها هر کدام وظیفه مستقل و مشخصی را در شبکه انجام می‌دهند.

ساختار سلسله مراتبی به معنای آن است که لایه‌های بالایی به وسیله دو و یا چند پروتکل سطح پایین تر از خود حمایت و پشتیبانی می‌شود.



پروتکل‌های هر کدام از لایه‌ها در مدل TCP/IP

لایه دسترسی شبکه در مدل TCP/IP (Network Access Layer)

لایه دسترسی شبکه پائین‌ترین لایه در مدل TCP/IP است. یک لایه شبکه ترکیبی از لایه‌های فیزیکی (Physical Layer) و لایه دیتالینک (Data link layer) است که در مدل مرجع OSI تعریف شده بود.

لایه شبکه تعیین‌کننده نحوه ارسال فیزیکی داده‌ها به سمت شبکه است. وظیفه اصلی این لایه آن است که داده‌ها را میان دو دیوایس در یک شبکه انتقال دهد.

عملکردهائی که در این لایه انجام می‌شود، به وسیله دیتاگرام IP در درون فریم‌های (Frame) به وسیله شبکه و الگوی IP آدرس‌ها در آدرس‌های فیزیکی کپسوله‌سازی (Encapsulating) می‌شود.

پروتکل‌های استفاده شده به وسیله این لایه شامل Ethernet، Token Ring، FDDI، X.25 و Frame relay می‌شوند.

لایه اینترنت در مدل TCP/IP (Internet Layer)

لایه اینترنت دومین لایه در مدل TCP/IP است. لایه اینترنت همچنین به عنوان لایه شبکه (Network Layer) شناخته می‌شوند.

اصلی‌ترین وظیفه لایه اینترنت آن است که پکت‌های داده را از هر شبکه‌ای ارسال کند و در عین حال پکت‌هایی که به مقصد او ارسال می‌شوند را از شبکه دریافت نمایند.

پروتکل‌هایی که در لایه شبکه مورد استفاده قرار می‌گیرند شامل موارد زیر هستند:

پروتکل IP

پروتکل IP بخش مهم و چشمگیری از کل مجموعه TCP/IP را شامل می‌شود. اساسی‌ترین موارد مرتبط به این پروتکل را در بخش زیر بررسی می‌کنیم.

اساسی‌ترین مسئولیت‌های پروتکل IP در لایه شبکه:

▪ آدرس دهی بر مبنای IP (IP Addressing): این پروتکل آدرس میزبان‌های پیاده‌سازی شده منطقی را به شکل IP آدرس‌ها می‌داند. آدرس‌ها به وسیله اینترنت و لایه‌ها بالاتر برای تعریف دیوایس‌ها بر روی شبکه و ایجاد مسیرهای ارتباطی میان آن استفاده می‌شود.

▪ ارتباطات هاست به هاست: (Host to Host) پروتکل IP تعیین کننده مسیرهایی است که داده‌ها از طریق آن‌ها انتقال پیدا می‌کنند.

▪ فرمت دهی و کپسوله‌سازی داده‌ها: (Data Encapsulation and Formatting) یک پروتکل IP می‌تواند داده‌ها را از پروتکل‌های لایه انتقال (Transport Layer) بپذیرد. یک پروتکل IP مطمئن می‌شود که داده‌های ارسالی و دریافتی به شکل مطمئنی هستند. این پروتکل داده‌ها را در درون IP «دیتاگرام» کپسوله‌سازی می‌کند.

▪ بخش‌بندی و مونتاژ کردن پیام: (Fragmentation and Reassembly) محدودیت اندازه IP دیتاگرام‌ها که به وسیله پروتکل‌های لایه دیتالینک اعمال می‌شود به عنوان «حداکثر واحد قابل ارسال (MTU)» (Maximum Transmission Unit) نامیده می‌شود. اگر اندازه IP دیتاگرام‌ها بزرگتر از واحد MTU باشد، در آن صورت پروتکل IP دیتاگرام را به واحدهای کوچکتر می‌شکند و آن‌ها می‌توانند به راحتی بر روی شبکه محلی جابجا شوند. بخش‌بندی کردن (Fragmentation) می‌تواند به وسیله ارسال کننده یا یک روتر میانجی انجام شود. در طرف دریافت کننده، تمام بخش‌های ارسالی به همدیگر مونتاژ می‌شوند تا اصل پیام به دست آید.

▪ مسیریابی: (Routing) هنگامی که IP دیتاگرام بر روی یک شبکه مانند LAN شبکه محلی، MAN (شبکه شهری) یا WAN (شبکه گسترده) ارسال می‌شود، آن به عنوان یک «تحویل مستقیم (Direct

»Delivery) شناخته می‌شود. هنگامی که منبع و مقصد بروری شبکه دور دست باشند، در آن صورت IP

دیتاگرام‌ها به صورت غیر مستقیم (Indirectly) ارسال می‌شوند. این کار می‌تواند به وسیله مسیره‌ی IP

دیتاگرام‌ها از طریق چند دستگاه مانند روتر (Router) انجام شود.

پروتکل ARP

پروتکل ARP برگرفته از سرنام عبارت «Address Resolution Protocol» است. در واقع یک

پروتکل لایه شبکه است که برای یافتن مسیرهای و آدرس‌های فیزیکی IP آدرس‌ها به کار می‌رود.

دو دلیل اصلی که سبب می‌شود از پروتکل ARP استفاده شود به شرح زیر است:

- درخواست ARP: در زمانی که فرستنده می‌خواهد آدرس فیزیکی یک دیوایس را بر روی شبکه بداند، آن

درخواست ARP خودش را بر روی شبکه منتشر می‌کند.

- پاسخ ARP: هر دیوایس متصل به شبکه که درخواست ARP را دریافت کند، آن را پذیرش می‌کند، اما تنها

در زمانی به آن پاسخ می‌دهد که IP آدرس پیام آن مشابه با IP آدرس خودش باشد، سپس این دیوایس دریافت

کننده اقدام به پاسخ دهی به درخواست ARP ارسال شده می‌کند. در حین فرایند پذیرش آدرس فیزیکی به

قسمت کش حافظه و سرواره دیتاگرام اضافه می‌شود.

پروتکل ICMP

ICMP برگرفته از سرنام عبارت «Internet Control Message Protocol» یا «پروتکل پیام کنترل اینترنت» است. این پروتکل در واقع مکانیسمی است که به وسیله‌هاست‌ها یا روترها برای ارسال اعلام‌ها (Notifications) به سمت ارسال کننده پیام، با توجه به مسئله‌هایی که در دیتاگرام پیام دریافتی ایجاد شده است به کار می‌رود.

یک دیتاگرام می‌توانم از یک روتر به دیگر سفر کنند تا در نهایت به مقصد مورد نظر خودش برسد. اگر یک روتر قادر نباشد داده‌ها را به دلایلی مانند شرایط غیر معمول برای مثال قطع شدن لینک ارتباطی، آتش سوزی بر روی دیوایس و یا از کار افتادن شبکه، از خود عبور دهد، در آن صورت پروتکل ICMP به کار می‌رود تا ارسال کننده را نسبت به عدم تحویل دیتاگرام آگاه سازد.

یک پروتکل ICMP اساساً دارای دو عبارت کلی است:

▪ ICMP Test (آزمون): در شرایط تست ICMP از یک سری از آزمایش‌ها استفاده می‌شود تا از امکان تحویل دیتاگرام به مقصد مطمئن شویم.

▪ ICMP Reply (پاسخ): در شرایط پاسخ ICMP از یک سری از چکاب‌ها استفاده می‌شود تا مطمئن شویم که آیا دیوایس مورد نظر به ما پاسخگو است یا خیر.

اصلی ترین وظیفه پروتکل ICMP آن است که مسئله‌های موجود را «گزارش» دهد، نه آنکه نسبت به درست کردن آن‌ها اقدام نماید. مسئولیت درست کردن پیام‌ها بر عهده ارسال کننده می‌باشد.

ICMP می‌تواند پیام‌ها را تنها به منبع ارسال کند، و آن‌ها را تحویل هیچ روتر میانی در مسیر نمی‌دهد، زیرا دیتاگرام‌ها آدرس‌های منبع و مقصد را حمل می‌کنند و روترهای در مسیر تنها وظیفه انتقال پیام را بر عهده دارند.

لایه انتقال در مدل TCP/IP (Transport Layer)

لایه انتقال مسئول ایجاد ایمن‌سازی (Reliability)، کنترل جریان (Flow Control) و درست کردن پیام‌هایی هستند که بر روی شبکه ارسال می‌گردند.

دو پروتکل در لایه انتقال استفاده می‌شوند که شامل پروتکل User Datagram و پروتکل Transmission Control می‌گردد.

پروتکل User Datagram (User Datagram Protocol)

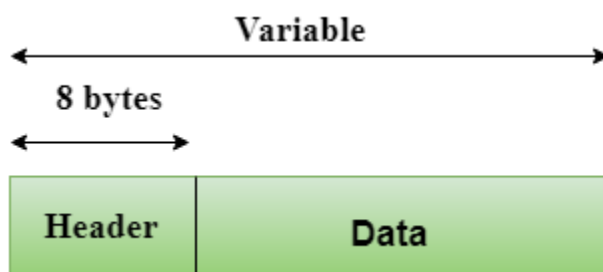
این پروتکل سرویس‌های بدون ارتباط (Connectionless service) و تحویل سر به سر (End to End delivery) را میسر می‌کند.

پروتکل UDP یک پروتکل غیر قابل اعتماد است. این پروتکل می‌تواند خطاها را کشف کند، اما نمی‌تواند به ما بگوید که چه خطاهایی در حال وقوع است.

پروتکل UDP خطاها را کشف می‌کند و پروتکل ICMP گزارشی از خطاها را به سمت فرستنده ارسال می‌کند که در آن نشان می‌دهد که دیتاگرام کاربر دچار آسیب و نقصان شده است.

پروتکل UDP شامل فیلدهای اطلاعاتی زیر است:

- آدرس پورت منبع: آدرس پورت منبع آدرس برنامه کاربردی است که پیام در آن ساخته شده است.
- آدرس پورت مقصد: آدرس پورت مقصد شامل آدرس برنامه کاربردی است که پیام را دریافت می کند.
- طول کلی پیام: آن تعریف کننده تعداد کلی بیت های دیتاگرام کاربر در هر بایت است.
- چک سام (Checksum): چک سام یک فیلم شانزده بیتی است که برای تعیین خطا از آن استفاده می شود.
- پروتکل UDP نمی تواند بگوید که کدامیک از بسته ها گم شده است. پروتکل UDP تنها حاوی بیت های چک سام است؛ آن نمی تواند ID دیتاگرام های معیوب را در خود نگه دارد.



اضافه کردن سرواره به فریم داده در پروتکل UDP

Header Format

Source port address 16 bits	Destination port address 16 bits
Total length 16 bits	Checksum 16 bits

فرمت سرواره ها در پروتکل UDP در مدل TCP/IP

پروتکل کنترل انتقال (TCP) (Transmission Control Protocol)

این پروتکل خدمات کامل لایه انتقال را برای نرم افزارهای کاربردی مهیا می کند. آن می تواند یک مدار مجازی میان ارسال کننده و دریافت کننده ایجاد کند و در زمانی که قصد ارسال پیام وجود دارد آن را فعال سازد.

TCP یک پروتکل قابل اعتماد است که از آن برای تشخیص خطاها و انتقال دیتاگرام فریم ها استفاده می شود. به همین خاطر، این پروتکل، مطمئن می شود که تمام بخش های یک پیام به وسیله دریافت کننده دریافت شده است و یک تائید را قبل از ارسال بقیه پیام دریافت شده است، و پس از دریافت این تائید دریافت، نسبت به از بین بردن مسیر مجازی اقدام می کند.

در سمت ارسال کننده TCP پیام را به واحدهای کوچکتری که به عنوان سگمنت (Segment) شناخته می شوند تقسیم می کند. هر کدام از سگمنت ها دارای یک شماره متوالی هستند که برای دوباره چینی فریم ها و ساختن پیام اصلی به کار گرفته می شوند.

در سمت دریافت کننده، پروتکل TCP اقدام به جمع آوری تمام سگمنت ها می کند و بار دیگر بر اساس شماره متوالی که به آن ها نسبت داده شده است، این سگمنت ها را مرتب می کند تا پیام اصلی بازسازی شود.

لایه اپلیکیشن مدل (TCP/IP (Application Layer)

لایه اپلیکیشن بالاترین لایه در مدل TCP/IP است. آن مسئول اجرای پروتکل های سطح بالا و ارائه پیام به کاربر می باشد. این لایه به کاربر اجازه می دهد که با اپلیکیشن ها کاربردی شبکه کار کند.

هنگامی که یک پروتکل لایه اپلیکیشن می‌خواهد با لایه دیگر اپلیکیشن در تماس باشد، آن داده‌های مورد نظرش را به لایه انتقال (Transport Layer) ارسال می‌کند.

در لایه اپلیکیشن ممکن است فعالیت‌های سردرگم کننده‌ای رخ دهد. هر اپلیکیشنی نمی‌تواند در درون لایه اپلیکیشن قرار گیرد، تنها مواردی می‌توانند در این لایه قرار گیرند که می‌توانند با سیستم در ارتباط باشند. برای مثال، ویرایشگر نوشته مانند نرم‌افزار MS Office Word نمی‌تواند با در لایه اپلیکیشن باشد، در حالی مرورگری که از پروتکل HTTP برای تعامل با شبکه استفاده می‌کند می‌تواند در لایه اپلیکیشن قرار گیرد و با بهره‌گیری از پروتکل HTTP با لایه‌های پائین دست در تعامل قرار گیرد.

پروتکل‌های اصلی که در لایه اپلیکیشن استفاده می‌شوند به شرح زیر هستند:

▪ HTTP: این پروتکل برگرفته از سرنام عبارت «Hypertext Transfer Protocol» است. این پروتکل

به ما اجازه دسترسی به داده‌هایی که بر روی شبکه جهانی وب قرار دارد را می‌دهد. آن می‌تواند داده‌ها را در فرم نوشته‌های ساده (Plain Text)، فایل‌های صوتی، و فایل‌های ویدئویی انتقال دهد. آن به عنوان یک پروتکل انتقال فرانوخته شناخته می‌شود که می‌تواند به صورت بسیار کارآمدی در محیط‌هایی که از فرانوخته (Hypertext) استفاده می‌کنند کار کنند و پیام‌ها و پرونده‌ها را از یک دیوایس به دیگری انتقال دهد.

▪ SNMP: این پروتکل برگرفته از سرنام عبارت «Simple Network Management Protocol»

است. این پروتکل در واقع بیشتر یک فریمورک است که برای مدیریت کردن دیوایس‌های بر روی اینترنت با استفاده از مجموعه پروتکل‌های TCP/IP به کار می‌رود.

▪ SMTP: این پروتکل برگرفته از سرنام عبارت «Simple Mail Transfer Protocol» است. پروتکل

TCP/IP از این پروتکل برای ارسال نامه‌های الکترونیکی در روی شبکه استفاده می‌کند. این پروتکل برای

ارسال داده‌ها به شکل ایمیل به آدرس‌های ایمیل مشخص شده) نه IP آدرس‌ها (استفاده می‌شود.

▪ DNS: این پروتکل برگرفته از سرنام عبارت «Domain Name System» است. همیشه یک IP آدرس

منحصر به فرد برای ارتباط دیوایس و یاهاست به شبکه جهانی اینترنت معرفی می‌شود. با این حال برای بسیاری

از افراد به خاطر سپردن این IP آدرس‌ها کار مشکلی است، برای همین به جای IP آدرس‌ها از «نام آدرس»

استفاده می‌شود. به همین خاطر سیستم‌هایی وجود دارند که نام‌ها را در برابر IP آدرس‌ها الگو می‌کنند به این

سیستم‌ها DNS گفته می‌شود. در واقع آن‌ها جدول‌های اطلاعاتی هستند که هر نام آدرس را در برابر یک IP

آدرس قرار می‌دهند.

▪ TELNET: این عبارت مخفف عبارت «Terminal Network» است. از این پروتکل برای ایجاد ارتباط

میان کامپیوتر محلی و کامپیوترهای راه دور استفاده می‌شود به نحوی که ترمینال رایانه محلی بتواند به ترمینال

رایانه یا دیوایس دور دست متصل شود.

FTP: این پروتکل برگرفته از سر نام عبارت «File Transfer Protocol» است FTP. یک پروتکل اینترنتی

استاندارد است که برای انتقال فایل‌ها از یک کامپیوتر به کامپیوتر دیگر استفاده می‌شود.

Website: <https://itbaz.net/6682/tcp-ip-model/>