فصلنامه علمی گروه کامپیوتر
دانشگاه شهید چمران کرمان

مبانی

شبکه‌های کامپیوتری

شماره ۱ | دوره اول | تابستان ۱۴۰۵

- مفاهیم پایه شبکه
- مدل‌های OSI و TCP/IP
- آدرس‌دهی IP و زیرشبکه‌بندی
- تجهیزات و رسانه‌های شبکه
- پروتکل‌های پرکاربرد
- مبانی امنیت شبکه
- کاربردهای عملی و عیب‌یابی

دانشگاه شهید چمران کرمان
انجمن علمی گروه کامپیوتر

فصلنامهٔ علمی گروه کامپیوتر
شمارهٔ ۱ — تابستان ۱۴۰۵

مبانی شبکه‌های کامپیوتری

ناشر: نشر بایت

شمارهٔ ۱

فهرست مطالب

فصل ۱۳: کلاینت-سرور یا همتابه‌همتا؟

فصل ۱۴: آدرس فیزیکی و پروتکل ARP

فصل ۱۵: مسیریابی و سوییچینگ

فصل ۱۶: NAT و اشتراک‌گذاری آدرس اینترنت

فصل ۱۷: عیب‌یابی مقدماتی شبکه

پیوست: واژه‌نامهٔ مختصر

پیوست: منابع

شناسنامه

دربارهٔ این شماره

این شمارهٔ فصلنامه به‌طور کامل به مبانی اولیهٔ شبکه‌های کامپیوتری اختصاص یافته و برای دانشجویانی نوشته شده که تازه با درس شبکه آشنا می‌شوند. هدف، ارائهٔ تصویری روشن و کاربردی از مفاهیم پایه پیش از ورود به مباحث تخصصی‌تر است.

مورد	توضیح
عنوان فصلنامه	مبانی شبکه‌های کامپیوتری
صاحب امتیاز	انجمن علمی گروه کامپیوتر، دانشگاه شهید چمران کرمان
استاد مشاور	امیر ایرانمنش
مدیر مسئول نشریه	امیر حسین شهریار پناه
سردبیر	احسان دهقان اناری
شماره و دوره	شمارهٔ ۱، دورهٔ اول
تاریخ انتشار	تابستان ۱۴۰۵
موضوع این شماره	مفاهیم پایهٔ شبکه‌های کامپیوتری
ناشر	نشر بایت

پیش‌گفتار

سخن استاد مشاور

امیر ایرانمنش

استاد مشاور

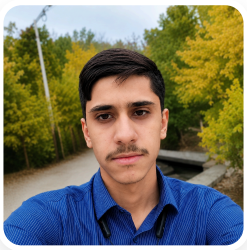
دنیای فناوری اطلاعات و شبکه‌های کامپیوتری هر روز با سرعت بیشتری در حال پیشرفت است و یادگیری مفاهیم پایه‌ای این حوزه برای دانشجویان و علاقه‌مندان اهمیت زیادی دارد. هدف از تهیه این فصلنامه، ارائه مطالبی کاربردی و قابل فهم برای آشنایی بیشتر با مباحث شبکه و ایجاد انگیزه برای یادگیری عمیق‌تر این حوزه است.

امیدوارم مطالب این شماره بتواند برای شما مفید باشد و مسیر یادگیری را برایتان هموارتر کند. از شما دانشجویان عزیز نیز دعوت می‌کنم با مطالعه، پژوهش و به اشتراک گذاشتن تجربیات خود، در رشد و پویایی فضای علمی دانشگاه نقش مؤثری داشته باشید.

برای همه شما آرزوی موفقیت، پیشرفت و آینده‌ای روشن دارم.

پیش‌گفتار

سخن مدیر مسئول نشریه



امیر حسین شهریار پناه

مدیر مسئول نشریه

سلام و احترام

انجمن‌های علمی دانشجویی فرصتی ارزشمند برای یادگیری، تجربه‌اندوزی و فعالیت‌های گروهی هستند. انتشار این فصلنامه نیز حاصل تلاش و همکاری دانشجویانی است که با علاقه و انگیزه، دانش و تجربیات خود را در قالب مطالب آموزشی و علمی در اختیار دیگران قرار داده‌اند.

امیدوارم این نشریه بتواند برای دانشجویان مفید و الهام‌بخش باشد و زمینه‌ای برای افزایش دانش، تبادل ایده‌ها و آشنایی بیشتر با دنیای فناوری اطلاعات و شبکه‌های کامپیوتری فراهم کند. از همه دانشجویانی که در تهیه این شماره مشارکت داشته‌اند صمیمانه تشکر می‌کنم و امیدوارم در شماره‌های آینده نیز شاهد حضور و همکاری پررنگ‌تر شما عزیزان باشیم.

با آرزوی موفقیت و پیشرفت برای تمامی دانشجویان عزیز.

پیش‌گفتار

سخن سردبیر

شبکه‌های کامپیوتری بخش مهمی از زیرساخت فناوری امروز را تشکیل می‌دهند؛ زیرساختی که بسیاری از خدمات و ابزارهایی که روزانه از آن‌ها استفاده می‌کنیم بر پایه آن شکل گرفته‌اند. با وجود نقش پررنگ شبکه در زندگی و کسب‌وکار، بسیاری از مفاهیم و سازوکارهای آن برای کاربران عادی پنهان باقی می‌ماند.

ایده این شماره از فصلنامه، پرداختن به همین مفاهیم پایه و کاربردی است؛ موضوعاتی که درک آن‌ها می‌تواند دید بهتری نسبت به نحوه عملکرد فناوری‌های اطراف ما ایجاد کند. تلاش شده است مطالب با زبانی روان و در عین حال علمی ارائه شوند تا برای دانشجویان و علاقه‌مندان به حوزه فناوری اطلاعات قابل استفاده باشند.

این فصلنامه حاصل همکاری اعضای انجمن علمی و دانشجویانی است که بخشی از زمان و آموخته‌های خود را برای تهیه و تدوین آن اختصاص داده‌اند. امیدوارم مطالب این شماره بتواند برای مخاطبان مفید باشد و زمینه‌ای برای آشنایی بیشتر با دنیای شبکه و فناوری اطلاعات فراهم کند.

احسان دهقان اناری

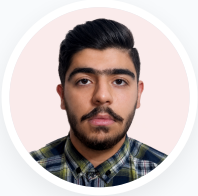
سردبیر

معرفی

تیم نویسندگان

احسان دهقان اناری

دانشجوی کاردانی فناوری اطلاعات



امیر محمد شیخ پور

دانشجوی کاردانی فناوری اطلاعات

محمد امین اعرابی نژاد

دانشجوی کاردانی فناوری اطلاعات

محمد مهدی امیری

دانشجوی کاردانی فناوری اطلاعات

عرفان میرزارحمانی

دانشجوی کاردانی فناوری اطلاعات

حسین گوهری

دانشجوی کاردانی فناوری اطلاعات

فصل ۱

نویسنده: **محمد مهدی امیری**

مقدمه و اهمیت شبکهٔ کامپیوتری

شبکهٔ کامپیوتری (Computer Network) به مجموعه‌ای از دو یا چند دستگاه گفته می‌شود که از طریق یک رسانهٔ ارتباطی به یکدیگر متصل شده‌اند تا بتوانند داده، منابع سخت‌افزاری و سرویس‌ها را با یکدیگر به اشتراک بگذارند. این تعریف ساده، پایه و اساس تقریباً تمام فناوری‌های ارتباطی امروزی از اینترنت خانگی گرفته تا مراکز دادهٔ عظیم شرکت‌های بزرگ فناوری است.

چرا به شبکه نیاز داریم؟

- اشتراک‌گذاری منابع: چاپگر، فضای ذخیره‌سازی یا اتصال اینترنت می‌تواند بین چند کاربر مشترک باشد.
- ارتباطات: ایمیل، پیام‌رسان‌ها و تماس تصویری همگی بر پایهٔ شبکه کار می‌کنند.
- دسترسی به داده از راه دور: کارمندان می‌توانند به فایل‌های سازمان از هر مکانی دسترسی داشته باشند.
- مقیاس‌پذیری کسب‌وکار: سرویس‌های ابری امکان رشد سریع زیرساخت را بدون خرید سخت‌افزار جدید فراهم می‌کنند.
- هم‌افزایی محاسباتی: چند کامپیوتر می‌توانند با اتصال به هم، توان پردازشی خود را برای انجام یک وظیفهٔ سنگین (مانند رندر ویدئو یا محاسبات علمی) ترکیب کنند.

اجزای اصلی یک شبکهٔ ساده

- گره یا Node: هر دستگاهی که به شبکه متصل است (کامپیوتر، گوشی، چاپگر).
- رسانهٔ انتقال: کابل، فیبر نوری یا امواج رادیویی که داده از طریق آن جابه‌جا می‌شود.
- پروتکل: مجموعه قوانینی که نحوهٔ ارسال و دریافت داده را مشخص می‌کند.
- تجهیزات شبکه: دستگاه‌هایی مانند سوییچ و روتر که مسیر داده را مدیریت می‌کنند.
- آدرس شبکه: شناسه‌ای یکتا (مانند آدرس IP) که هر دستگاه را در شبکه قابل‌شناسایی می‌کند.

کاربرد شبکه در صنایع مختلف

اهمیت شبکه محدود به دنیای فناوری اطلاعات نیست؛ تقریباً هر صنعتی امروزه به‌نوعی به زیرساخت شبکه وابسته است.

- بانکداری: انتقال آنی تراکنش‌ها بین شعب و دستگاه‌های خودپرداز از طریق شبکه‌های امن.
- سلامت: پروندهٔ الکترونیک بیمار و اتصال تجهیزات پزشکی هوشمند به شبکهٔ بیمارستان.
- آموزش: کلاس‌های آنلاین، سامانه‌های مدیریت یادگیری و کتابخانه‌های دیجیتال.
- صنعت و تولید: اینترنت اشیای صنعتی (IIoT) برای پایش خط تولید در زمان واقعی.
- حمل‌ونقل: سامانه‌های ردیابی ناوگان، چراغ‌های راهنمایی هوشمند و خودروهای متصل.

نکته

حتی ساده‌ترین کار روزمره مانند باز کردن یک صفحهٔ وب، در پشت‌صحنه شامل ده‌ها تبادل پیام میان دستگاه‌های مختلف شبکه است که در کسری از ثانیه انجام می‌شود.

فصل ۲

تاریخچهٔ مختصر شبکه‌های کامپیوتری

نویسنده: **محمد مهدی امیری**

شناخت مسیر تکاملی شبکه کمک می‌کند مفاهیم امروزی را بهتر درک کنیم؛ چراکه بسیاری از تصمیم‌های طراحی فعلی، پاسخی به محدودیت‌های گذشته بوده‌اند.

دهه	رویداد کلیدی
دههٔ ۱۹۵۰ میلادی	نخستین آزمایش‌های ارتباط بین کامپیوترها از طریق خطوط تلفن، پیش‌زمینه‌ای برای شبکه‌های آینده.
دههٔ ۱۹۶۰ میلادی	آغاز پروژهٔ ARPANET توسط وزارت دفاع آمریکا به‌عنوان نخستین شبکهٔ سوییچینگ بسته‌ای.
دههٔ ۱۹۷۰ میلادی	معرفی پروتکل‌های اولیهٔ TCP و IP برای ارتباط بین شبکه‌های ناهمگون و ابداع اترنت در آزمایشگاه زیراکس.
دههٔ ۸۰ میلادی	گسترش شبکه‌های محلی (LAN) با فناوری اترنت، پیدایش DNS و استانداردسازی پروتکل‌های شبکه.
دههٔ ۹۰ میلادی	همه‌گیرشدن اینترنت عمومی، ظهور وب جهان‌گستر و نخستین مرورگرهای گرافیکی.
دههٔ ۲۰۰۰ به بعد	گسترش شبکه‌های بی‌سیم، موبایل، رایانش ابری، شبکه‌های اجتماعی و اینترنت اشیا.

دهه	رویداد کلیدی
دهه ۲۰۱۰ به بعد	ظهور شبکه‌های نرم‌افزار محور (SDN)، اینترنت پرسرعت 5G و گسترش امنیت شبکه به‌عنوان اولویت اول سازمان‌ها.

نکته

مفهوم سوییچینگ بسته‌ای (Packet Switching) که در دههٔ ۶۰ میلادی مطرح شد، هنوز هم اساس ارسال داده در اینترنت امروزی است؛ به این معنا که داده پیش از ارسال به بسته‌های کوچک‌تر تقسیم می‌شود.

روند تکامل شبکه نشان می‌دهد که هر نسل از فناوری، پاسخی به یک نیاز واقعی بوده است: از نیاز نظامی به ارتباط مقاوم در برابر خرابی، تا نیاز امروزی به اتصال میلیاردها دستگاه هوشمند به یکدیگر.

فصل ۳

انواع شبکه بر اساس گسترهٔ جغرافیایی

نویسنده: **محمد مهدی امیری**

شبکه‌ها معمولاً بر اساس وسعت پوششی که ارائه می‌دهند دسته‌بندی می‌شوند. این دسته‌بندی به مهندسان کمک می‌کند فناوری و تجهیزات مناسب را انتخاب کنند.

نوع شبکه	گستره	مثال کاربردی
PAN	چند متر	اتصال هدفون بلوتوث به گوشی
LAN	یک ساختمان یا اتاق	شبکهٔ داخلی یک دانشگاه یا شرکت
CAN	چند ساختمان نزدیک به هم	اتصال دانشکده‌های مختلف یک دانشگاه به هم
MAN	یک شهر	شبکهٔ ارتباطی بین چند شعبهٔ یک بانک در یک شهر
WAN	کشور یا قاره	اینترنت جهانی و شبکهٔ بین دفاتر بین‌المللی یک شرکت

در عمل، بسیاری از سازمان‌ها ترکیبی از این انواع را به‌طور هم‌زمان استفاده می‌کنند: شبکهٔ داخلی هر شعبه یک LAN است، ارتباط میان شعب یک شهر از طریق MAN برقرار می‌شود و اتصال به دفتر مرکزی در شهری دیگر از طریق WAN انجام می‌گیرد.

نکته

مرز بین این دسته‌بندی‌ها همیشه دقیق نیست؛ برخی شبکه‌های دانشگاهی بزرگ می‌توانند هم‌زمان ویژگی‌های CAN و MAN داشته باشند.

فصل ۴

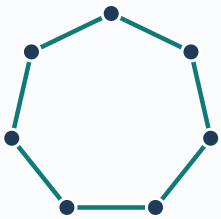
توپولوژی‌های شبکه

نویسنده: **امیر محمد شیخ پور**

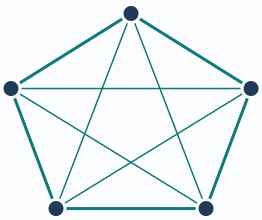
توپولوژی به آرایش فیزیکی یا منطقی اتصال دستگاه‌ها در یک شبکه گفته می‌شود. انتخاب توپولوژی مناسب بر هزینه، قابلیت اطمینان و سادگی عیب‌یابی شبکه اثر مستقیم دارد.

Star

Bus



Ring



Mesh

توپولوژی	مزیت اصلی	عیب اصلی
Star	عیب‌یابی و مدیریت آسان	وابستگی به سلامت سوییچ مرکزی
Bus	کابل‌کشی کم و ارزان	قطعی کابل اصلی = قطعی کل شبکه

توپولوژی	مزیت اصلی	عیب اصلی
Ring	کنترل دسترسی منظم به رسانه	خرابی یک گره می‌تواند حلقه را مختل کند
Mesh	مقاومت بالا در برابر خرابی	هزینه و پیچیدگی بالای کابل‌کشی

توپولوژی ترکیبی (Hybrid)

در بسیاری از سازمان‌های بزرگ، به‌جای استفاده از یک توپولوژی خالص، ترکیبی از چند توپولوژی به‌کار می‌رود؛ برای مثال ممکن است هر طبقهٔ ساختمان به‌صورت ستاره‌ای سیم‌کشی شده باشد، اما اتصال میان طبقات از الگوی مش پیروی کند. این رویکرد، انعطاف‌پذیری طراحی را افزایش می‌دهد.

توپولوژی مناسب را چگونه انتخاب کنیم؟

در عمل، اکثر شبکه‌های محلی امروزی از توپولوژی ستاره‌ای فیزیکی استفاده می‌کنند، حتی اگر از نظر منطقی رفتار دیگری داشته باشند. دلیل اصلی، سادگیِ افزودن یا حذف یک دستگاه بدون اختلال در بقیهٔ شبکه است.

> **نکته**
>
> توپولوژی مش معمولاً در بخش‌های حیاتیِ شبکه‌های سازمانی بزرگ یا در شبکه‌های بی‌سیم مش خانگی به‌کار می‌رود که قطعی هیچ نقطه‌ای مجاز نیست.

فصل ۵

مدل مرجع OSI

نویسنده: **احسان دهقان اناری**

مدل OSI (Open Systems Interconnection) یک چارچوب هفت‌لایه است که نحوهٔ ارتباط دو دستگاه در شبکه را به‌صورت مفهومی توضیح می‌دهد. هر لایه وظیفهٔ مشخصی دارد و فقط با لایه‌های مجاور خود در تعامل است.

#	نام لایه	وظیفهٔ کلیدی
۷	Application	ارتباط مستقیم با نرم‌افزارهای کاربر مانند مرورگر و ایمیل
۶	Presentation	تبدیل قالب داده، رمزنگاری و فشرده‌سازی
۵	Session	برقراری، مدیریت و پایان‌دادن به نشست ارتباطی
۴	Transport	تضمین رسیدن داده و کنترل جریان (TCP و UDP)
۳	Network	مسیریابی بسته‌ها بین شبکه‌های مختلف (آدرس‌دهی IP)
۲	Data Link	انتقال قاب‌ها در یک پیوند فیزیکی و آدرس‌دهی MAC
۱	Physical	انتقال بیت‌های خام از طریق کابل یا امواج رادیویی

نکتهٔ یادگیری

برای به‌خاطرسپردن ترتیب لایه‌ها از بالا به پایین، عبارت رایج «All People Seem To Need Data Processing» در منابع انگلیسی استفاده می‌شود.

مثال کاربردی: مسیر یک پیام از لایه‌های OSI

فرض کنید یک پیام کوتاه را در یک برنامهٔ پیام‌رسان تایپ می‌کنید و دکمهٔ ارسال را می‌زنید. داده در مسیر خروجی از لایهٔ کاربرد شروع شده و به‌ترتیب از لایه‌های پایین‌تر عبور می‌کند؛ در هر لایه سرآیند (Header) مخصوص همان لایه به داده افزوده می‌شود. این فرایند را کپسوله‌سازی (Encapsulation) می‌نامند.

- لایهٔ Application: متن پیام آماده و به فرمت مشخص برنامه تبدیل می‌شود.
- لایهٔ Transport: پیام به بخش‌های کوچک‌تر تقسیم و شمارهٔ پورت مقصد افزوده می‌شود.
- لایهٔ Network: آدرس IP مبدأ و مقصد به هر بخش داده اضافه می‌شود.
- لایهٔ Data Link: آدرس MAC دستگاه بعدی در مسیر افزوده و قاب آماده می‌شود.
- لایهٔ Physical: قاب به‌صورت بیت‌های خام روی رسانهٔ انتقال ارسال می‌شود.

در سمت گیرنده، همین فرایند در جهت معکوس و با نام کپسوله‌گشایی (Decapsulation) انجام می‌شود تا پیام اصلی بازسازی شود.

فصل ۶

مدل TCP/IP

نویسنده: **احسان دهقان اناری**


مدل TCP/IP نسخهٔ عملی‌تر و ساده‌شدهٔ مدل OSI است که مبنای واقعی اینترنت امروزی قرار گرفته و از چهار لایه تشکیل شده است.

لایهٔ TCP/IP	معادل در OSI	مثال پروتکل
Application	کاربرد، نمایش، نشست	HTTP, FTP, DNS
Transport	انتقال	TCP, UDP
Internet	شبکه	IP, ICMP
Network Access	پیوند داده، فیزیکی	Ethernet, Wi-Fi

برخلاف مدل OSI که بیشتر جنبهٔ آموزشی و مرجع دارد، مدل TCP/IP همان چیزی است که در تجهیزات واقعی شبکه پیاده‌سازی شده است.

نام‌گذاری واحد داده در هر لایه

در هر لایه از مدل TCP/IP، واحد داده نامی متفاوت دارد که آشنایی با آن هنگام مطالعهٔ متون تخصصی ضروری است.

لایه	نام واحد داده (PDU)
Application	داده (Data)
Transport	قطعه (Segment) در TCP یا دیتاگرام (Datagram) در UDP

لایه	نام واحد داده (PDU)
Network	بسته (Packet)
Network Access	قاب (Frame)

فصل ۷

آدرس‌دهی IP

نویسنده: **امیر محمد شیخ پور**

نسخهٔ چهارم پروتکل اینترنت (IPv4)

هر آدرس IPv4 از ۳۲ بیت تشکیل شده که معمولاً به‌صورت چهار عدد ده‌دهی جدا شده با نقطه نمایش داده می‌شود، مانند 192.168.1.10. این آدرس‌ها به دو بخش شبکه و میزبان تقسیم می‌شوند.

کلاس	محدودهٔ اکتت اول	کاربرد رایج
کلاس A	۱ تا ۱۲۶	شبکه‌های بسیار بزرگ
کلاس B	۱۲۸ تا ۱۹۱	شبکه‌های متوسط، مانند دانشگاه‌ها
کلاس C	۱۹۲ تا ۲۲۳	شبکه‌های کوچک، مانند شرکت‌ها و منازل

آدرس‌های خصوصی رایج مانند بازهٔ 10.0.0.0 تا 10.255.255.255 یا 192.168.0.0 تا 192.168.255.255 در شبکه‌های داخلی استفاده می‌شوند و در اینترنت عمومی قابل مسیریابی نیستند.

زیرشبکه‌سازی به زبان ساده

زیرشبکه‌سازی (Subnetting) یعنی تقسیم یک شبکهٔ بزرگ به چند شبکهٔ کوچک‌تر با استفاده از قرض‌گرفتن بیت از بخش میزبان آدرس. این کار مدیریت شبکه را ساده‌تر و مصرف آدرس را بهینه‌تر می‌کند.

برای مثال، شبکهٔ 192.168.1.0/24 دارای ۲۵۶ آدرس است. اگر همین شبکه را با ماسک /26 تقسیم کنیم، به چهار زیرشبکهٔ ۶۴ آدرسی تبدیل می‌شود که هرکدام می‌تواند به یک بخش سازمانی مانند آموزش، مالی یا فناوری اطلاعات اختصاص یابد.

کلاس	ماسک زیرشبکهٔ پیش‌فرض	نماد CIDR
کلاس A	255.0.0.0	/8
کلاس B	255.255.0.0	/16
کلاس C	255.255.255.0	/24

نسخهٔ ششم پروتکل اینترنت (IPv6)

با توجه به اتمام تدریجی آدرس‌های IPv4، نسخهٔ IPv6 با طول ۱۲۸ بیت طراحی شد تا فضای آدرس‌دهی به‌مراتب بزرگ‌تری فراهم کند. این آدرس‌ها به‌صورت هشت گروه شانزده‌تایی و با جداکنندهٔ دونقطه نمایش داده می‌شوند، مانند 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

> **نکته**
>
> برخلاف تصور رایج، IPv6 جایگزین اجباری IPv4 نیست؛ در حال حاضر بسیاری از شبکه‌ها هر دو نسخه را به‌صورت هم‌زمان (Dual Stack) پشتیبانی می‌کنند.

فصل ۸

تجهیزات شبکه

نویسنده: **محمد امین اعرابی نژاد**

تجهیز	لایهٔ کاری اصلی	وظیفه
Hub	Physical	تکرار سیگنال به همهٔ پورت‌ها بدون هوشمندی؛ امروزه کمتر استفاده می‌شود
Switch	Data Link	هدایت هوشمند داده تنها به پورت مقصد بر اساس آدرس MAC
Router	Network	مسیریابی بسته‌ها بین شبکه‌های مختلف بر اساس آدرس IP
Access Point	Data Link	ایجاد دسترسی بی‌سیم و اتصال آن به شبکهٔ سیمی
Modem	Physical	تبدیل سیگنال دیجیتال به آنالوگ و برعکس برای اتصال به اینترنت
Firewall	Multilayer	کنترل و فیلترکردن ترافیک ورودی و خروجی برای امنیت شبکه

انتخاب تجهیز مناسب معمولاً به اندازهٔ شبکه، بودجه و نیاز به هوشمندی در مدیریت ترافیک بستگی دارد. برای یک خانه یا دفتر کوچک، یک روتر خانگی معمولاً هر سه وظیفهٔ مودم، روتر و اکسس‌پوینت را هم‌زمان انجام می‌دهد؛ اما در شبکه‌های سازمانی بزرگ، هر یک از این نقش‌ها به دستگاه‌های تخصصی جداگانه سپرده می‌شود.

نکته

در گذشته هاب‌ها به‌طور گسترده استفاده می‌شدند، اما امروزه به دلیل هدر رفتن پهنای باند و مشکلات امنیتی، تقریباً به‌طور کامل جای خود را به سوییچ‌های هوشمند داده‌اند.

فصل ۹

رسانه‌های انتقال داده

نویسنده: **احسان دهقان اناری**

کابل‌های مسی

- کابل زوج‌به‌هم‌تابیدهٔ بدون محافظ (UTP): متداول‌ترین گزینه در شبکه‌های محلی، ارزان و آسان برای نصب.
- کابل زوج‌به‌هم‌تابیدهٔ محافظ‌دار (STP): مقاومت بیشتر در برابر نویز الکترومغناطیسی، مناسب محیط‌های صنعتی.

فیبر نوری

در فیبر نوری داده به‌صورت پالس‌های نور منتقل می‌شود. پهنای باند بسیار بالا، مسافت انتقال طولانی و مصونیت در برابر تداخل الکترومغناطیسی از مزایای اصلی آن است؛ اما هزینهٔ تجهیزات و نصب آن بیشتر از کابل مسی است.

رسانهٔ بی‌سیم

امواج رادیویی مانند Wi-Fi و بلوتوث امکان اتصال بدون کابل را فراهم می‌کنند. سهولت نصب و تحرک از مزایا، و محدودیت مسافت و حساسیت به تداخل از معایب آن به‌شمار می‌آید.

استانداردهای Wi-Fi

استاندارد Wi-Fi طی سال‌ها نسخه‌های مختلفی داشته که هرکدام سرعت و برد متفاوتی ارائه می‌دهند.

نسخهٔ استاندارد	نام رایج	حداکثر سرعت تقریبی
802.11n	Wi-Fi 4	حدود ۶۰۰ مگابیت بر ثانیه
802.11ac	Wi-Fi 5	حدود ۳.۵ گیگابیت بر ثانیه

نسخهٔ استاندارد	نام رایج	حداکثر سرعت تقریبی
802.11ax	Wi-Fi 6	حدود ۹.۶ گیگابیت بر ثانیه

مقایسهٔ کلی رسانه‌ها

رسانه	سرعت تقریبی	برد معمول	هزینهٔ نسبی
کابل مسی (UTP)	تا ۱۰ گیگابیت بر ثانیه	تا ۱۰۰ متر	کم
فیبر نوری	تا چند صد گیگابیت بر ثانیه	چند کیلومتر	زیاد
بی‌سیم (Wi-Fi)	تا حدود ۱۰ گیگابیت بر ثانیه	چند ده متر	متوسط

فصل ۱۰

نویسنده: **محمد امین اعرابی نژاد**

پروتکل‌های پرکاربرد شبکه

پروتکل	کاربرد اصلی
TCP	انتقال قابل‌اطمینان داده همراه با تضمین ترتیب و تحویل بسته‌ها
UDP	انتقال سریع بدون تضمین تحویل؛ مناسب پخش زنده و بازی آنلاین
HTTP / HTTPS	انتقال صفحات وب؛ نسخهٔ S رمزنگاری‌شده و امن است
FTP	انتقال فایل بین کامپیوترها در شبکه
DNS	تبدیل نام دامنه به آدرس IP قابل‌فهم برای دستگاه‌ها
DHCP	تخصیص خودکار آدرس IP به دستگاه‌های تازه‌وارد به شبکه

شماره‌پورت‌های استاندارد

هر پروتکل معمولاً با یک شمارهٔ پورت استاندارد شناخته می‌شود که به سیستم‌عامل کمک می‌کند بداند داده را به کدام برنامه تحویل دهد.

پروتکل	شمارهٔ پورت پیش‌فرض
HTTP	۸۰
HTTPS	۴۴۳
FTP	۲۱

پروتکل	شمارهٔ پورت پیش‌فرض
DNS	۵۳
SSH	۲۲

فصل ۱۱

مبانی امنیت شبکه

نویسنده: **امیر محمد شیخ پور**

امنیت شبکه مجموعه‌ای از سیاست‌ها و ابزارهایی است که برای محافظت از محرمانگی، صحت و در دسترس‌بودن داده در برابر تهدیدها به کار می‌رود.

- فایروال: فیلترکردن ترافیک ورودی و خروجی بر اساس مجموعه قوانین از پیش تعریف‌شده.
- رمزنگاری: تبدیل داده به شکلی غیرقابل‌خواندن برای افراد غیرمجاز در حین انتقال یا ذخیره‌سازی.
- VPN (شبکهٔ خصوصی مجازی): ایجاد تونل رمزنگاری‌شده برای ارتباط امن از طریق شبکه‌های عمومی.
- احراز هویت: تأیید هویت کاربر یا دستگاه پیش از اعطای دسترسی به منابع شبکه.

چند توصیهٔ عملی برای دانشجویان

- از اتصال به شبکه‌های Wi-Fi عمومی بدون VPN برای انتقال اطلاعات حساس خودداری کنید.
- رمز عبور تجهیزات شبکهٔ خانگی مانند مودم را از مقدار پیش‌فرض کارخانه تغییر دهید.
- به‌روزرسانی نرم‌افزار تجهیزات شبکه را به‌طور منظم انجام دهید.

آشنایی با چند تهدید رایج

نوع تهدید	توضیح کوتاه
فیشینگ	فریب کاربر برای افشای اطلاعات حساس از طریق ایمیل یا پیام جعلی
حملهٔ منع سرویس (DoS)	اشغال منابع یک سرور با حجم زیاد درخواست تا از دسترس خارج شود
بدافزار (Malware)	نرم‌افزار مخربی که بدون اطلاع کاربر روی سیستم اجرا می‌شود
استراق سمع (Sniffing)	شنود ترافیک شبکه برای دستیابی به اطلاعات ارسالی بدون رمزنگاری

فصل ۱۲

نویسنده: **عرفان میرزارحمانی**

کاربردهای عملی: سه نمونهٔ واقعی

نمونهٔ اول: شبکهٔ داخلی دانشگاه

در یک شبکهٔ دانشگاهی، معمولاً هر ساختمان یک شبکهٔ محلی (LAN) مستقل دارد که از طریق روترها و لینک‌های فیبر نوری به شبکهٔ مرکزی دانشگاه متصل می‌شود.

نمونهٔ دوم: خانهٔ هوشمند

در یک خانهٔ هوشمند، مودم/روتر خانگی نقش مرکز شبکه را دارد. دستگاه‌هایی مانند دوربین امنیتی، لامپ هوشمند و دستیار صوتی از طریق Wi-Fi یا بلوتوث به همان روتر متصل می‌شود.

نمونهٔ سوم: سرویس‌های ابری

وقتی یک فایل را در یک سرویس ذخیره‌سازی ابری بارگذاری می‌کنید، داده از دستگاه شما عبور کرده، از طریق چندین روتر اینترنتی مسیریابی شده و در نهایت به یکی از مراکز دادهٔ آن شرکت می‌رسد. این ارتباط معمولاً با پروتکل HTTPS رمزنگاری می‌شود تا امنیت داده در طول مسیر تضمین شود.

فصل ۱۳

نویسنده: **حسین گوهری**


کلاینت-سرور یا همتابه‌همتا؟ دو مدل رایج ارتباط در شبکه

یک سوال ساده: وقتی یک ویدیو را از یوتیوب پخش می‌کنید، آن ویدیو از کجا می‌آید؟ و وقتی با یک فایل تورنت را دانلود می‌کنید، فایل از کجا می‌آید؟ جواب این دو سوال، دو مدل کاملاً متفاوت از ارتباط شبکه‌ای را نشان می‌دهد که خوب است از همین ابتدا با هردویشان آشنا باشید.

مدل کلاینت-سرور (Client-Server)

در این مدل، یک دستگاه قدرتمند به اسم سرور همیشه آماده و روشن است و منتظر می‌ماند تا دستگاه‌های دیگر (کلاینت‌ها) درخواستی برایش بفرستند. مرورگر شما وقتی یک سایت را باز می‌کند، دقیقاً همین کار را انجام می‌دهد: یک درخواست به سرور آن سایت می‌فرستد و منتظر پاسخ می‌ماند. اکثر سرویس‌هایی که هر روز استفاده می‌کنید، از ایمیل گرفته تا اینستاگرام، روی همین مدل کار می‌کنند.

- مدیریت متمرکز: چون همه‌چیز روی سرور است، به‌روزرسانی و نظارت خیلی راحت‌تر انجام می‌شود.
- امنیت بهتر: کنترل دسترسی و پشتیبان‌گیری از یک نقطهٔ مرکزی ساده‌تر است.
- وابستگی به سرور: اگر سرور از کار بیفتد، کل سرویس برای همه از دسترس خارج می‌شود.

مدل همتابه‌همتا (Peer-to-Peer یا P2P)

در این مدل خبری از سرور مرکزی نیست؛ هر دستگاه هم می‌تواند درخواست بدهد و هم می‌تواند به دیگران سرویس بدهد. دقیقاً به همین دلیل است که در دانلود تورنت، شما هم‌زمان که فایلی را دریافت می‌کنید، بخشی از آن را هم به دیگران آپلود می‌کنید.

- بدون نقطهٔ شکست مرکزی: از کار افتادن یک دستگاه، کل شبکه را از کار نمی‌اندازد.
- مقیاس‌پذیری طبیعی: هرچه کاربر بیشتری وصل شود، منابع بیشتری هم به شبکه اضافه می‌شود.
- مدیریت و امنیت سخت‌تر: چون کنترل متمرکزی وجود ندارد، نظارت بر محتوا و کیفیت سخت‌تر می‌شود.

ویژگی	کلاینت-سرور	همتابه‌همتا
مثال رایج	سایت‌ها، ایمیل، شبکه‌های اجتماعی	تورنت، برخی ارزهای دیجیتال
نقطهٔ شکست	سرور مرکزی	معمولاً وجود ندارد
هزینهٔ زیرساخت	بالا (نگهداری سرور)	پایین‌تر، پخش‌شده بین کاربران

نکته

خیلی از سرویس‌های امروزی ترکیبی از هر دو مدل هستند؛ مثلاً برخی اپ‌های پیام‌رسان از سرور برای مدیریت حساب کاربری استفاده می‌کنند، اما تماس صوتی را مستقیم و به‌صورت همتابه‌همتا بین دو گوشی برقرار می‌کنند.

فصل ۱۴

نویسنده: **عرفان میرزارحمانی**

آدرس فیزیکی دستگاه‌ها و پروتکل ARP

در فصل‌های قبل با آدرس IP آشنا شدید که مثل آدرس پستی یک دستگاه در شبکه عمل می‌کند. اما یک سوال جالب اینجا پیش می‌آید: وقتی داده در نهایت باید از یک کابل یا سیگنال بی‌سیم رد شود، سیستم از کجا می‌داند دقیقاً باید آن را به کدام دستگاه فیزیکی تحویل بدهد؟ اینجاست که آدرس MAC وارد بازی می‌شود.

آدرس MAC چیست؟

هر کارت شبکه، چه در گوشی شما باشد چه در لپ‌تاپ، از کارخانه یک شناسهٔ ۴۸ بیتی و یکتا دریافت می‌کند به اسم آدرس MAC (مثل 3C:5A:B4:12:9F:0E). این عدد برخلاف IP، معمولاً ثابت است و جابه‌جا شدن دستگاه بین شبکه‌های مختلف آن را عوض نمی‌کند؛ یک‌جور شناسنامهٔ فیزیکی برای سخت‌افزار است.

پس ARP دقیقاً چه کار می‌کند؟

فرض کنید کامپیوتر شما می‌خواهد داده‌ای را برای یک دستگاه دیگر در همان شبکهٔ محلی بفرستد و فقط آدرس IP آن را بلد است. اینجا کامپیوتر شما یک سوال بلند در کل شبکه می‌پرسد: «آدرس MAC صاحب این IP چیست؟» این کار دقیقاً همان چیزی است که پروتکل ARP (Address Resolution Protocol) انجام می‌دهد؛ یعنی پل ارتباطی بین دنیای آدرس‌های منطقی (IP) و دنیای آدرس‌های فیزیکی (MAC).

- دستگاه یک پیام پخش‌عمومی (Broadcast) با عنوان «چه کسی این IP را دارد؟» به کل شبکه می‌فرستد.
- فقط دستگاهی که صاحب آن IP است، پاسخ می‌دهد و آدرس MAC خودش را اعلام می‌کند.
- کامپیوتر شما این جفت IP-MAC را در یک جدول موقت به اسم ARP Cache ذخیره می‌کند تا دفعهٔ بعد دوباره سوال نپرسد.

نکته

می‌توانید در ویندوز با دستور ساده‌ی arp -a همین جدول ARP سیستم خودتان را ببینید؛ لیستی از آدرس‌های IP همسایه‌های شبکه‌تان به همراه MAC هرکدام.

خلاصه اینکه هر بار داده‌ای در شبکهٔ محلی جابه‌جا می‌شود، این IP است که تعیین می‌کند «برای کجا» و این MAC است که تعیین می‌کند «دقیقاً برای کدام دستگاه»؛ و ARP همان چیزی است که این دو را به هم وصل می‌کند.

فصل ۱۵

نویسنده: **احسان دهقان اناری**

مسیریابی و سوییچینگ، خیلی ساده‌تر از چیزی که فکر می‌کنید

اسم مسیریابی و سوییچینگ معمولاً برای دانشجوهای تازه‌کار کمی ترسناک است، اما ایده‌ی پشتش شگفت‌انگیز ساده است: هر دو دربارهٔ این هستند که داده از کدام مسیر برود تا سریع‌تر و درست‌تر به مقصد برسد. فرقشان در این است که در چه مقیاسی این تصمیم را می‌گیرند.

سوییچینگ: تصمیم‌گیری داخل یک شبکهٔ محلی

سوییچ یک جدول کوچک از آدرس‌های MAC نگه می‌دارد و یاد می‌گیرد که هر دستگاه از کدام پورت به آن وصل است. وقتی داده‌ای وارد می‌شود، سوییچ فقط به همان پورت درست می‌فرستدش، نه به همهٔ پورت‌ها؛ برخلاف هاب که همه‌چیز را برای همه پخش می‌کرد.

مسیریابی: تصمیم‌گیری بین شبکه‌های مختلف

روتر یک سطح بالاتر کار می‌کند. وقتی داده باید از شبکهٔ شما خارج شود و به یک شبکهٔ کاملاً دیگر برود (مثلاً به سرور یک سایت خارجی)، این روتر است که تصمیم می‌گیرد از کدام مسیر برود. برای این کار، روتر یک جدول مسیریابی (Routing Table) دارد که در آن نوشته شده «برای رسیدن به این شبکه، از این طرف برو».

مسیریابی ایستا در برابر مسیریابی پویا

مسیرها را می‌شود به دو شکل به روتر یاد داد. یا مدیر شبکه خودش دستی می‌نویسد که هر مسیر کجا برود (مسیریابی ایستا یا Static)، یا روترها با پروتکل‌های خاصی مثل OSPF با هم صحبت می‌کنند و خودشان بهترین مسیر را کشف می‌کنند (مسیریابی پویا یا Dynamic). روش اول برای شبکه‌های کوچک و ساده مناسب است؛ روش دوم برای شبکه‌های بزرگ که مسیرها مدام تغییر می‌کنند.

ویژگی	مسیریابی ایستا	مسیریابی پویا
تنظیم	دستی توسط مدیر شبکه	خودکار بین روترها
مناسب برای	شبکه‌های کوچک و ساده	شبکه‌های بزرگ و پویا
واکنش به تغییر	نیاز به تغییر دستی دارد	خودش را تطبیق می‌دهد

نکته

یک راه ساده برای به‌خاطر سپردن تفاوت: سوییچ همسایه‌های داخل یک محله را بلد است، اما روتر بلد است بین محله‌های مختلف شهر راه پیدا کند.

فصل ۱۶

نویسنده: **امیر محمد شیخ پور**

NAT: چطور چند دستگاه با یک آدرس اینترنتی کار می‌کنند؟

یک سوال که شاید هیچ‌وقت به آن فکر نکرده باشید: در خانهٔ شما احتمالاً چند گوشی، لپ‌تاپ و شاید یک تلویزیون هوشمند هم‌زمان به اینترنت وصل‌اند. اما اگر آدرس‌های IPv4 عمومی محدودند، چطور همهٔ این دستگاه‌ها هم‌زمان اینترنت دارند؟ جواب یک کلمه است: NAT.

NAT دقیقاً چه کاری انجام می‌دهد؟

NAT مخفف Network Address Translation است. کار آن این است که آدرس‌های خصوصی داخل خانه یا شرکت شما (مثل 192.168.1.10 و 192.168.1.11) را، درست لحظه‌ای که می‌خواهند وارد اینترنت شوند، به یک آدرس عمومی مشترک (همانی که مودم یا روتر شما از ارائه‌دهندهٔ اینترنت گرفته) تبدیل می‌کند.

یعنی از دید سرورهای اینترنت، انگار همهٔ درخواست‌های خانهٔ شما از یک دستگاه واحد می‌آید؛ اما روتر شما به‌خوبی به‌خاطر دارد کدام پاسخ مال کدام دستگاه داخلی بوده و آن را به همان دستگاه برمی‌گرداند.

چرا اصلاً به NAT نیاز داریم؟

- کمبود آدرس: تعداد آدرس‌های عمومی IPv4 آن‌قدر نیست که به هر گوشی و لپ‌تاپ در دنیا یک آدرس اختصاصی بدهند.
- امنیت: چون دستگاه‌های داخل شبکهٔ شما آدرس عمومی ندارند، مستقیماً از بیرون قابل‌دسترسی و هدف حمله نیستند.
- انعطاف: می‌توانید داخل شبکهٔ خانگی یا سازمانی‌تان، آدرس‌ها را هرطور که خواستید بچینید، بدون اینکه به ساختار اینترنت جهانی ربطی داشته باشد.

نکته

نسخهٔ دقیق‌تر NAT که علاوه بر آدرس، شمارهٔ پورت را هم ترجمه می‌کند PAT نام دارد و همان چیزی است که در اکثر روترهای خانگی واقعاً اجرا می‌شود.

پس دفعهٔ بعد که دیدید همهٔ اعضای خانواده هم‌زمان دارند از یک اینترنت استفاده می‌کنند، بدانید پشت‌پرده یک NAT کوچک داخل روتر خانگی‌تان دارد بی‌وقفه کار می‌کند.

فصل ۱۷

نویسنده: **حسین گوهری**


وقتی اینترنت قطع می‌شود: چند ابزار ساده برای عیب‌یابی

همهٔ ما این تجربه را داشته‌ایم: یک‌دفعه اینترنت قطع می‌شود و اولین کاری که می‌کنیم خاموش‌وروشن‌کردن مودم است. خبر خوب این است که چند ابزار خط‌فرمانی خیلی ساده هست که می‌توانند قبل از این کار، دقیقاً نشان بدهند مشکل کجاست.

ping: زنده است یا نه؟

دستور ping ساده‌ترین و پرکاربردترین ابزار عیب‌یابی شبکه است. با نوشتن چیزی مثل ping google.com، کامپیوتر شما چند بستهٔ کوچک به آن سرور می‌فرستد و منتظر پاسخ می‌ماند. اگر پاسخ بیاید، یعنی مسیر اتصال شما تا آن سرور برقرار است؛ اگر پاسخی نیاید، مشکل یا از اتصال شماست یا از سمت مقصد.

tracert / traceroute: مسیر دقیقاً از کجا رد می‌شود؟

گاهی فقط دانستن اینکه «وصل هست یا نه» کافی نیست؛ می‌خواهید بدانید داده از چه مسیری رد می‌شود. دستور tracert (در ویندوز) یا traceroute (در لینوکس و مک) دقیقاً همین را نشان می‌دهد: لیست تمام روترهایی که بسته از میان‌شان عبور کرده تا به مقصد برسد، همراه با زمان تأخیر هر مرحله.

ipconfig / ifconfig: تنظیمات شبکهٔ خودم چیست؟

قبل از هر عیب‌یابی، خوب است بدانید تنظیمات فعلی دستگاه خودتان چیست. دستور ipconfig در ویندوز (یا ifconfig / ip addr در لینوکس) آدرس IP، ماسک زیرشبکه و دروازهٔ پیش‌فرض دستگاه شما را نشان می‌دهد؛ دقیقاً همان مفاهیمی که در فصل‌های قبل خواندید.

nslookup: آیا مشکل از DNS است؟

خیلی وقت‌ها اینترنت وصل است اما یک سایت خاص باز نمی‌شود؛ اینجا احتمالاً مشکل از سرویس نام دامنه (DNS) است. دستور nslookup به شما می‌گوید آیا نام یک دامنه اصلاً به آدرس IP ترجمه می‌شود یا نه.

دستور	چه سوالی را جواب می‌دهد؟
ping	آیا اصلاً به مقصد وصل می‌شوم؟
tracert / traceroute	داده از چه مسیری رد می‌شود؟
ipconfig / ifconfig	تنظیمات شبکهٔ خودم چیست؟
nslookup	آیا نام دامنه درست به IP تبدیل می‌شود؟

نکته

دفعهٔ بعد که اینترنت‌تان قطع شد، قبل از ریستارت‌کردن مودم، یک ping google.com بزنید؛ شاید مشکل جای دیگری باشد و با این کار زودتر پیدایش کنید.

پیوست

واژه‌نامهٔ مختصر

اصطلاح	توضیح کوتاه
Bandwidth	حداکثر ظرفیت انتقال داده در یک لینک شبکه در واحد زمان
Latency	زمان تأخیر بین ارسال و دریافت یک بستهٔ داده
Packet	واحد کوچک داده که برای انتقال در شبکه بسته‌بندی می‌شود
Node	هر دستگاه متصل به شبکه، مانند کامپیوتر یا روتر
IP Address	شناسه عددی منحصربه‌فرد برای هر دستگاه در شبکه جهت مسیریابی و ارتباط
Router	دستگاهی هوشمند برای هدایت و مسیریابی بسته‌های داده بین شبکه‌های مختلف
Switch	دستگاهی برای اتصال دستگاه‌ها در یک شبکه محلی (LAN) و انتقال هوشمند داده به مقصد
Protocol	مجموعه قوانین و استانداردهای تعیین‌شده برای تبادل بدون خطای داده در شبکه
Firewall	ابزار امنیتی سخت‌افزاری یا نرم‌افزاری برای فیلتر و کنترل ترافیک شبکه
DNS	سیستم نام دامنه که آدرس‌های متنی (مانند سایت‌ها) را به IP عددی تبدیل می‌کند

اصطلاح	توضیح کوتاه
Gateway	نقطه کلیدی یا درگاهی که یک شبکه محلی را به یک شبکه خارجی (مانند اینترنت) متصل می‌کند
Subnet	بخشی کوچک‌تر از یک شبکهٔ بزرگ‌تر که با تقسیم آدرس IP ایجاد می‌شود
Encapsulation	افزودن سرآیند مخصوص هر لایه به داده هنگام عبور در مدل OSI یا TCP/IP
Bandwidth vs Throughput	پهنای باند ظرفیت نظری کانال است، در حالی که توان عملیاتی (Throughput) نرخ واقعی انتقال داده را نشان می‌دهد

پیوست

منابع

1. ملکیان، احسان. اصول طراحی و ساختار شبکه‌های کامپیوتری. انتشارات نص.

2. حق‌شناس، فرزاد. مهندسی شبکه‌های کامپیوتری و انتقال داده. انتشارات علوم رایانه.

3. Tanenbaum, A. S., & Wetherall, D. J. Computer Networks. Pearson.

4. Forouzan, B. A. Data Communications and Networking. McGraw-Hill.

5. Comer, D. E. Computer Networks and Internets. Pearson.

6. Peterson, L. L., & Davie, B. S. Computer Networks: A Systems Approach. Morgan Kaufmann.

Scientific Quarterly of
Computer Engineering Department
Shahid Chamran University of Kerman

Fundamentals of

Computer Networks

Issue 1 | Volume 1 | Summer 2026

- Basic Network Concepts
- TCP/IP and OSI Models
- IP Addressing and Subnetting
- Network Devices and Media
- Common Network Protocols
- Network Security Fundamentals
- Practical Applications and Troubleshooting