

بسمه تعالی



آزمایشگاه شبکه

دانشکده برق و کامپیوتر

دانشگاه صنعتی اصفهان

زمستان ۱۴۰۱

دکتر حیدرپور، دکتر فانیان

پیش گزارش آشنایی با مقدمات شبکه، پروتکل ها و wireshark

فهرست:

شبکه چیست؟

مدل Open System Interconnection (OSI)

تعریف پروتکل

مدل لایه TCP / IP

IP پروتکل

کلاس‌های مختلف IP نسخه‌ی ۴

gateway

آدرس‌های خاص

MAC Address

TCP پروتکل

UDP پروتکل

ICMP پروتکل

ARP پروتکل

DNS پروتکل

DHCP پروتکل

SAN پروتکل

NAS پروتکل

اشتراک‌گذاری فایل در شبکه

تجهيزات شبکه و حدود عملکرد آنها

دستورات خط فرمان

- ipconfig
- netsh
- netstat
- nslookup
- arp
- whois
- traceroute & tracepath
- ping

وایرشارک

- قسمت اول
- قسمت دوم
- قسمت سوم
- قسمت چهارم
- قسمت پنجم

شبکه چیست؟

شبکه دو یا چند کامپیوتر است که برای به اشتراک گذاشتن منابع خود (مثل چاپگر و CD-ROM)، رد و بدل کردن فایل‌ها و یا ارتباط با یکدیگر متصل شده‌اند. در واقع شبکه با اتصال کامپیوترها به روش‌های گوناگون شرایطی را فراهم می‌آورد که برای انتقال هزینه‌ها کاهش یافته و سرعت و ریسک انتقال نیز پایین بیاید. مزایای استفاده از شبکه عبارتند از:

- اشتراک منابع
- کاهش هزینه‌ها
- افزایش کارایی سیستم
- حذف محدودیت‌های جغرافیایی در تبادل داده‌ها

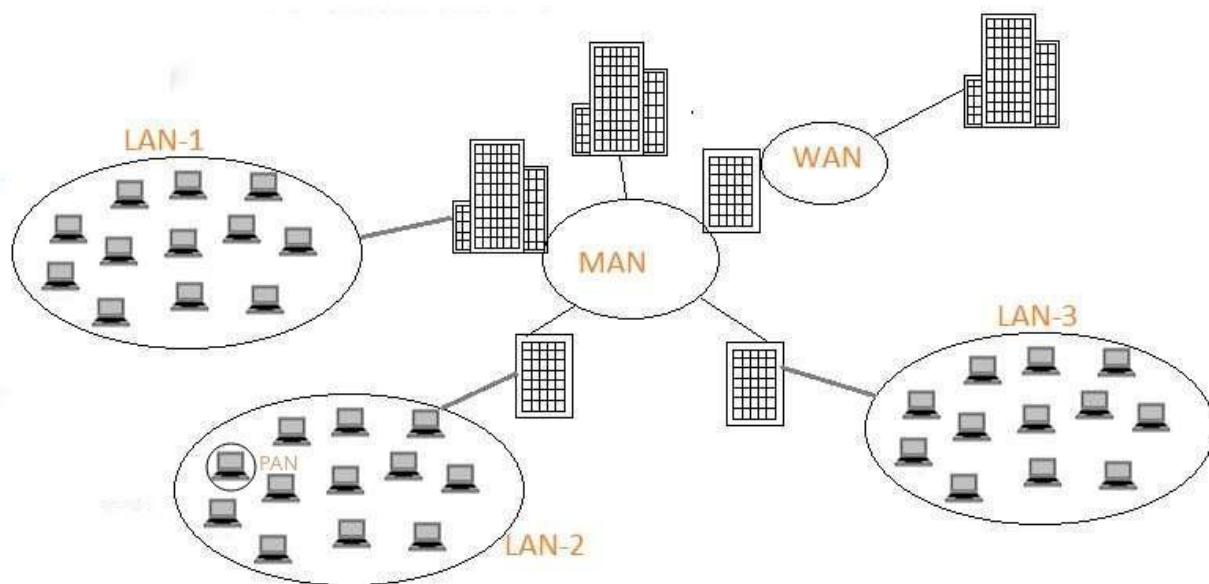
اجزای اصلی موجود در شبکه

- کامپیوتر سرویس گیرنده که از خدمات موجود در شبکه استفاده می‌کند.
- کامپیوتر سرویس دهنده که خدمات متفاوت را در اختیار دیگر کامپیوترها قرار می‌دهد.
- تمامی موارد ارتباط دهنده بین کامپیوترها شامل کابل، کانکتور و تجهیزات ارتباط می‌باشد.
- شامل تمام منابع موجود در شبکه مانند مانیتور، اسکنر، صفحه کلید، چاپگر و ... می‌باشد.
- به کلیه منابعی گفته می‌شود که کامپیوتر سرویس دهنده در اختیار کامپیوتر سرویس گیرنده قرار می‌دهد، برای مثال چاپگر، اسکنر و ...

انواع شبکه

➤ از نظر گستردگی و موقعیت فیزیکی یا جغرافیایی

- Local area network :LAN
- Metropolitan area network :MAN
- Wide area network :WAN (برای مثال اینترنت یک WAN است)
- Storage area network :SAN
- Personal area network :PAN
- Campus area network: CAN



نمونه‌ای از شبکه‌های PAN, LAN, MAN, WAN

دقت فرمایید که شبکه‌های دیگری نیز وجود دارند و در قسمت بالا تنها به اشاری تعدادی از آنها پرداخته شده است.

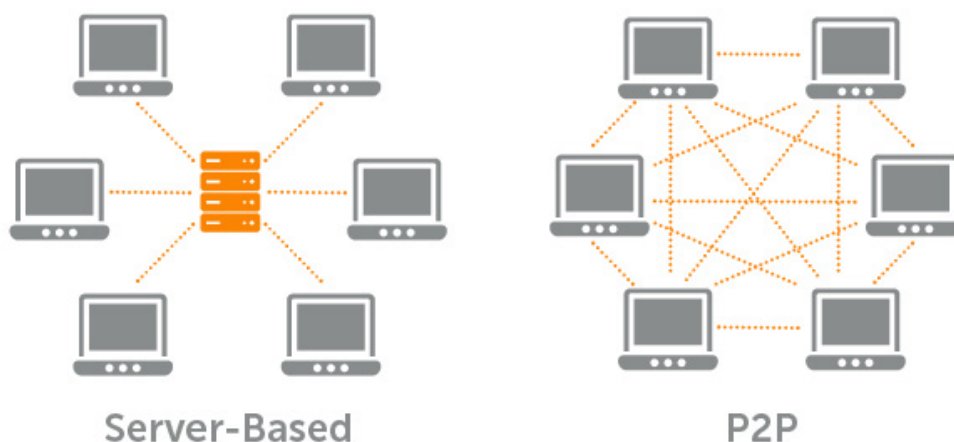
➤ از نظر مدل سرویس‌دهی

○ شبکه‌های نظیر به نظیر (peer to peer)

در این شبکه ایستگاه ویژه‌ای جهت نگهداری فایل‌های اشتراکی و سیستم‌عامل شبکه وجود ندارد. هر ایستگاه می‌تواند به منابع سایر ایستگاه‌های شبکه دسترسی پیدا کند.

○ شبکه‌های مبتنی بر سرویس‌دهنده (Server Based)

در این مدل شبکه، یک کامپیوتر به عنوان سرویس‌دهنده کلیه فایل‌ها و نرم‌افزارهای اشتراکی نظیر پردازنده‌ها، کامپایلرها، بانک‌های اطلاعاتی و سیستم‌عامل شبکه را در خود نگهداری می‌کند. یک کاربر به سرویس‌دهنده متصل شده و فایل‌ها و اطلاعات خود را برمی‌دارد.



مقایسه p2p و server-based [OBJ:OBJ]

➤ از نظر تکنولوژی انتقال داده

○ Broadcast

یک کانال مخابراتی مشترک بین همه کامپیوترهای شبکه وجود دارد که ارسال پیام در قالب بسته‌های کوچکی توسط هر کامپیوتر صورت می‌گیرد؛ آدرس مقصد بخشی از پیام است و بسته توسط همه کامپیوترها دریافت و در صورت تعلق به خود، بسته پردازش می‌شود و در غیر این صورت نیز نادیده گرفته می‌شود. در این شبکه هر کامپیوتر آدرس یکتا دارد.

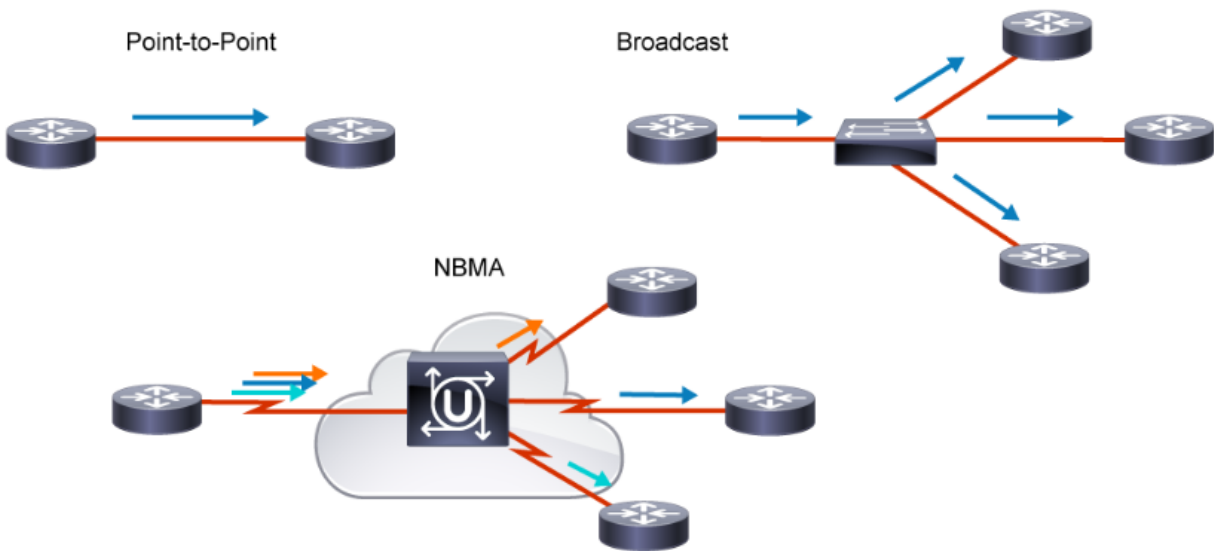
○ Point to Point

بین دو ماشین در شبکه، یک کانال فیزیکی و مستقیم وجود دارد و هیچ ماشین دیگری به آن کانال متصل نخواهد بود.

○ NBMA

NBMA یا Non-Broadcast Multi-Access نوعی توپولوژی شبکه است که برای مدیریت جریان داده‌ها در یک شبکه استفاده می‌شود. در یک شبکه NBMA، هر گره دارای یک آدرس منحصر به فرد است و داده‌ها فقط به گره خاصی که آدرس داده شده است ارسال می‌شود، نه به تمام گره‌های شبکه. این برخلاف یک شبکه‌ی broadcast است که در آن داده‌ها به تمام گره‌های شبکه ارسال می‌شود. شبکه‌های NBMA معمولاً در شبکه‌های بزرگ مانند شبکه‌های

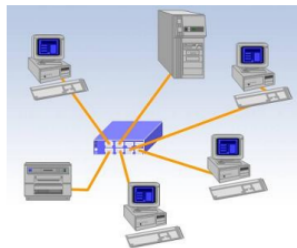
WAN استفاده می‌شوند. نمونه‌هایی از این شبکه‌ها عبارتند از ATM، Frame Relay و MPLS.



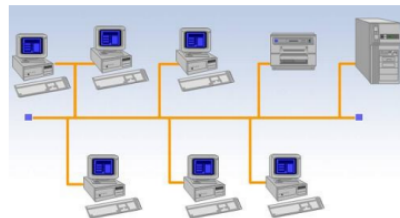
مقایسه Broadcast و Point to Point و NBMA

➤ انواع توپولوژی (روش اتصال فیزیکی کامپیوترها) در شبکه LAN

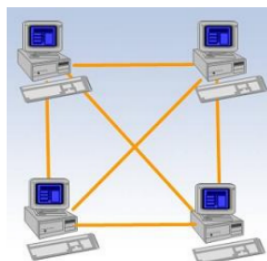
۲. روش ستاره ای یا متمرکز (star)



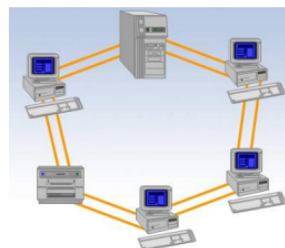
۱. خطی یا سری (bus)



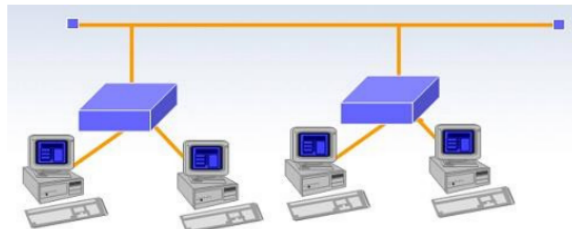
۴. روش پوششی (mesh)



۳. روش حلقه ای (ring)



۵. روش ترکیبی (hybrid) (به عنوان نمونه خطی - ستاره ای)

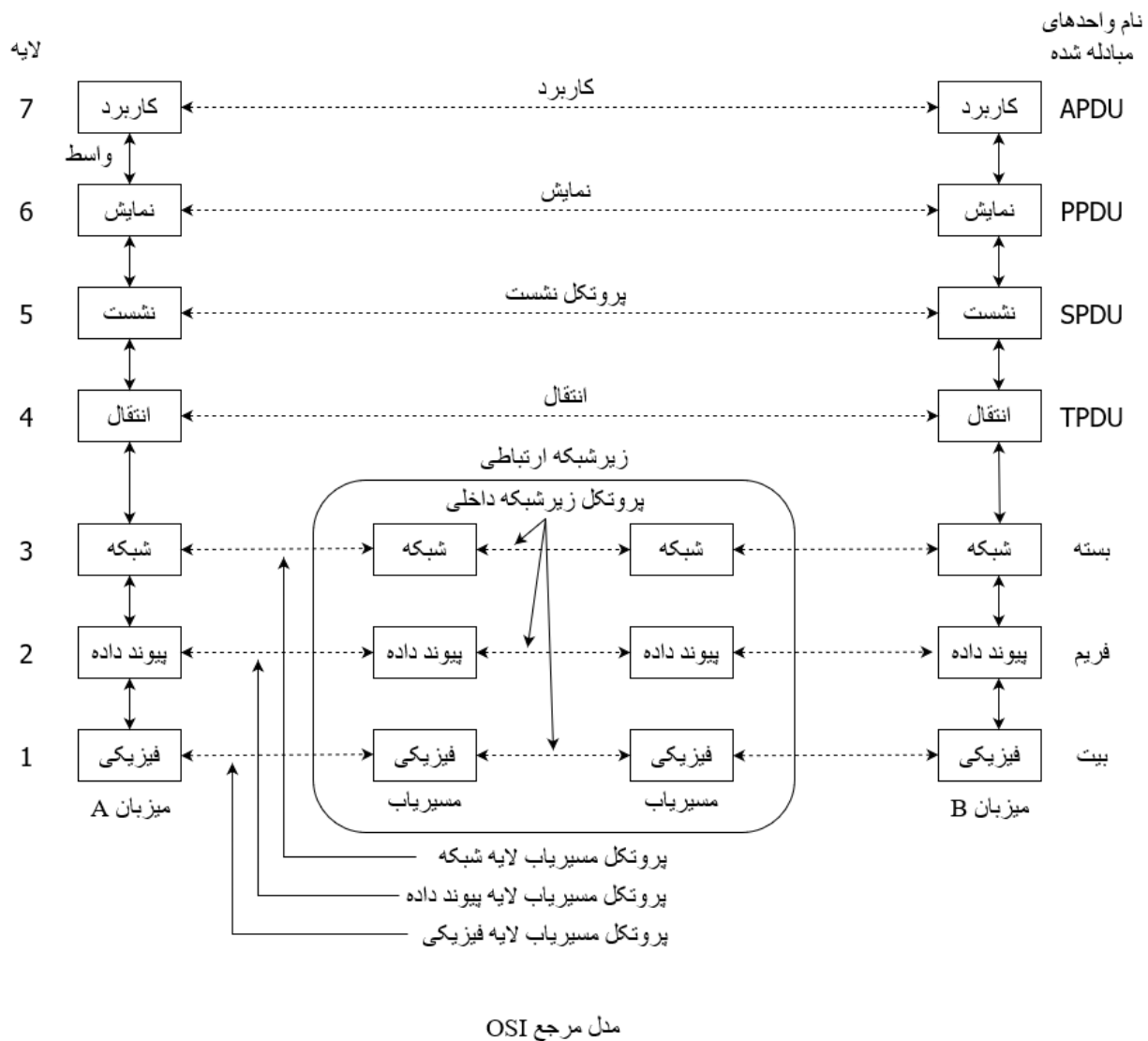


مدل Open System Interconnection (OSI)

مدل OSI یک مدل مفهومی مرجع است که ارتباطات بین اجزاء موجود در شبکه را استاندارد سازی و مشخص می کند. این مدل، بستری فراهم می کند که چگونگی ارسال، دریافت و تفسیر اطلاعات رد و بدل شده بین اجزاء مختلف شبکه را دیکته می کند.

مدل OSI ارتباطات شبکه ای را در ۷ لایه تقسیم بندی می کند و با گذر داده ها از هر لایه، پردازش های متفاوتی روی داده انجام شده و ممکن است اطلاعاتی که برای ارتباطات بعدی لازم است نیز به داده افزوده شود. این ۷ لایه عبارتند از:

۱. لایه فیزیکی: وظیفه ی انتقال بیت های خام را از طریق کانال ارتباطی بر عهده دارد.
۲. لایه پیوند داده ها: با شکستن داده های ورودی به بسته های کوچک (فریم)، خط فیزیکی پر خطا را به خط ارتباطی عاری از خطا برای لایه ی شبکه تبدیل می کند.
۳. لایه شبکه: عملکرد زیر شبکه را کنترل می کند. از مسائل مطرح در این لایه آدرس دهی و مسیریابی بسته ها (packet) می باشد. آدرس دهی در این لایه به صورت logical است.
۴. لایه انتقال: این لایه جریان ارتباط و انتقال داده روی شبکه را کنترل و مدیریت می کند. دو پروتکل اصلی استفاده شده در این لایه پروتکل های TCP و UDP هستند که در ادامه معرفی می شوند.
۵. لایه نشست: لایه نشست مسئول ایجاد ارتباط و ساخت یک جلسه بین سیستم یا نرم افزار مبدا و سیستم یا نرم افزار مقصد را به عهده دارد. بعد از برقرار یک ارتباط بین مبدا و مقصد، همگام سازی و آماده سازی بین دو انتهای ارتباط توسط این لایه انجام می شود تا شرایط برای ارسال داده ها فراهم شود. برخی از وظایف این لایه عبارتند از احراز هویت طرفین ارتباط، بررسی اعتبار پیام ها و اتمام جلسه.
۶. لایه ارائه: این لایه اطلاعات مختلفی که برنامه های کاربردی تولید می کنند را به فرم استاندارد تبدیل می کند و به عنوان مترجمی برای لایه کاربرد عمل می کند. از جمله اعمالی که این لایه روی داده ها انجام می دهد می توان به فرمت بندی اعداد نمایی، فشردن سازی و رمزنگاری اشاره کرد.
۷. لایه کاربرد: در این لایه، قواعد مربوط به چگونگی تعامل کاربر با داده های ارسالی به شبکه یا دریافتی از آن مشخص می شود. همچنین توصیف و تبدیل داده ها به مفاهیمی قابل درک برای برنامه های کاربردی در این لایه انجام می شود.



تعریف پروتکل:

- مجموعه‌ای از قوانین است که دو دستگاه برای انتقال موفق داده، از آن‌ها پیروی می‌کنند، برخی از مواردی که یک پروتکل آن‌ها را مشخص می‌کند عبارتند از:
- نحوه تشخیص خطا و تصحیح خطاهای احتمالی که حین تبادل داده ممکن است اتفاق بیفتد.
- روش متراکم سازی داده‌ها
- 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 داده‌ها
- طول هر فریم داده

تاکنون انواع مختلفی از پروتکل‌ها برای استفاده‌های مختلف طراحی شده‌اند و هر کدام دارای معایب و مزایایی هستند. برخی از پروتکل‌ها ساده، برخی با قابلیت اطمینان بیشتر و برخی دارای سرعت بالاتری هستند. برخی از پروتکل‌های متداول عبارتند از: TCP/IP، UDP، FTP، PPP و ... توضیحات کامل در مورد عملکرد هر پروتکل در متن‌های با نام RFC توسط IETF انتشار می‌یابد (مثلاً RFC شماره ۷۹۱ اطلاعات جامعی را در مورد پروتکل IP ارائه می‌کند).

مدل لایه TCP / IP:

پروتکلی استاندارد برای ارتباط کامپیوترهای موجود در یک شبکه اینترنت است. از این پروتکل، به منظور ارتباط در شبکه‌های بزرگ استفاده می‌شود. برقراری ارتباط از طریق پروتکل‌های متعددی که در چهار لایه‌ی مجزا سازماندهی شده‌اند، میسر می‌گردد.

در زمان ایجاد یک ارتباط، ممکن است در یک لحظه تعداد زیادی از برنامه‌ها، با یکدیگر ارتباط برقرار نمایند؛ این پروتکل دارای قابلیت تفکیک و تمایز یک برنامه‌ی موجود بر روی یک کامپیوتر با سایر برنامه‌ها بوده و پس از دریافت داده‌ها از یک برنامه، آنها را برای برنامه متناظر موجود بر روی کامپیوتر دیگر ارسال می‌نماید. نحوه ارسال داده توسط پروتکل از محلی به محل دیگر، با فرآیند ارسال یک نامه از شهری به شهری دیگر قابل مدل‌سازی است.

برقراری ارتباط با فعال شدن یک برنامه بر روی کامپیوتر مبدا آغاز می‌گردد. برنامه فوق، داده‌های مورد نظر جهت ارسال را به گونه‌ای آماده و فرمت‌بندی می‌نماید که برای کامپیوتر مقصد قابل خواندن و استفاده باشد (مشابه نوشتن نامه با زبانی که دریافت کننده قادر به مطالعه‌ی آن باشد). در ادامه آدرس کامپیوتر مقصد، به داده‌های مربوطه اضافه می‌گردد (مشابه آدرس گیرنده که بر روی یک نامه مشخص می‌گردد). پس از انجام عملیات فوق، داده به همراه اطلاعات اضافی (درخواستی برای تایید در مقصد)، در طول شبکه به حرکت درآمده تا به مقصد مورد نظر برسد. عملیات فوق ارتباطی به محیط انتقال شبکه به منظور انتقال اطلاعات نداشته و تحقق عملیات فوق با رویکردی مستقل نسبت به محیط انتقال، انجام خواهد شد.

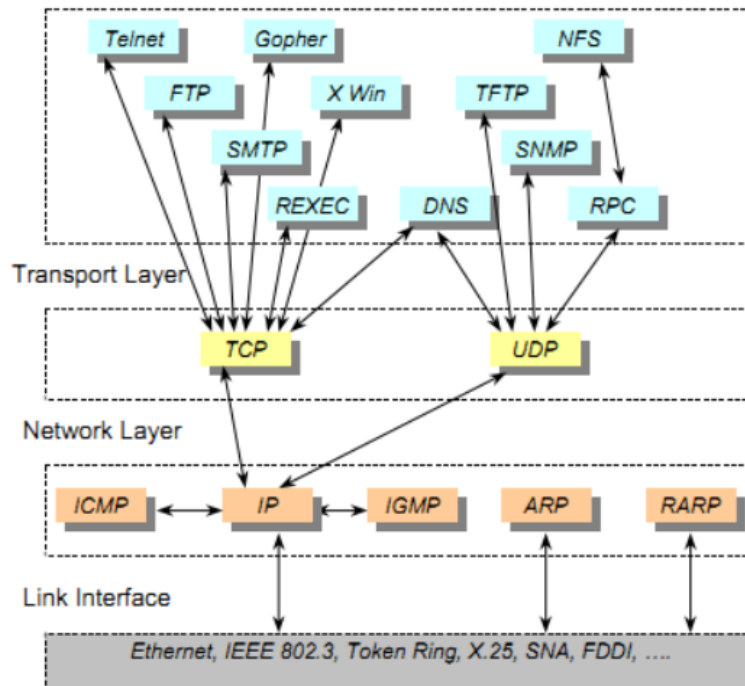
OSI vs

TCP/IP



مقایسه لایه‌ها در مدل مرجع OSI با مدل TCP / IP

Application Layer

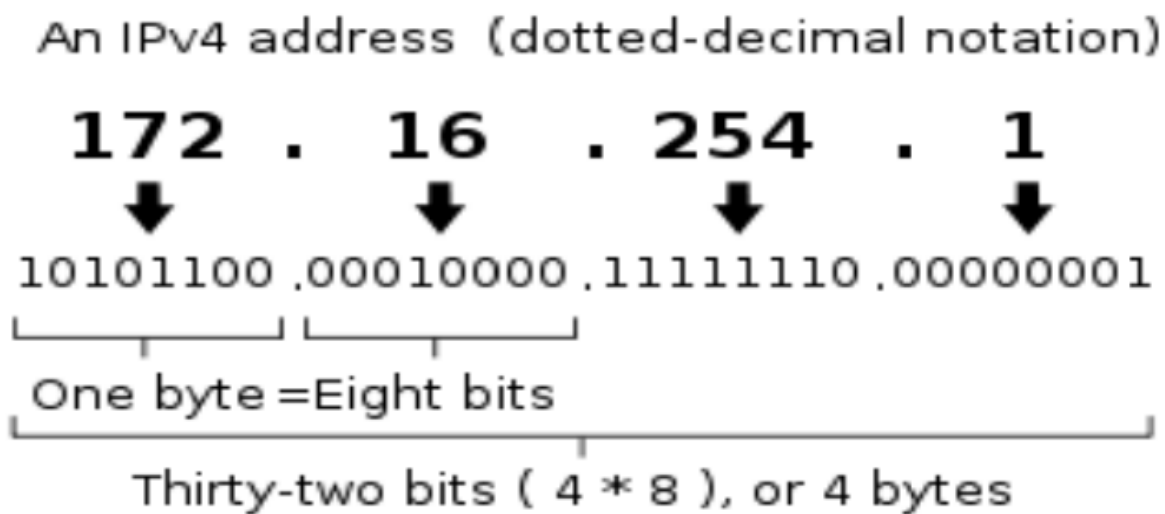


پروتکل‌های لایه‌های متفاوت شبکه

پروتکل IP:

یکی از پروتکل‌های مهم موجود در لایه اینترنت که مسئولیت آدرس‌دهی logical را بر عهده دارد، IP می‌باشد. IP شامل دو مدل IPv4 و IPv6 است.

آی‌پی ورژن ۴ استاندارد مورد استفاده برای انتقال داده‌ها از طریق اینترنت است. اولین بار در اوایل دهه ۱۹۸۰ به کار گرفته شد و از آن زمان تا کنون مورد استفاده گسترده قرار گرفته است. ساختار IPv4 مطابق تصویر زیر است:



ساختار IP و رزرن ۴

همانطور که در تصویر بالا مشخص است، IPv4 شامل ۴ فیلد می‌باشد که عددی بین ۰ تا ۲۵۵ (یعنی ۸ بیت) می‌باشد که هر بخش با یک نقطه از بخش دیگر جدا شده است. از آنجایی که این ورژن آی‌پی ۳۲ بیتی است انتظار می‌رود نهایتاً به 2^{32} دستگاه را بتواند پشتیبانی کند که منطبقاً این تعداد از تمام دستگاه‌های مورد نیاز با دسترسی به اینترنت خیلی بیشتر است.

ویژگی‌های اصلی IPv4 عبارتند از:

طول آدرسی‌ها ۳۲ بیتی هستند که تعداد محدودی از آدرس‌های IP منحصربه‌فرد را امکان‌پذیر می‌کند. این منجر به ایجاد فناوری ترجمه آدرس شبکه (NAT) شده است که برای حفظ آدرس‌های IPv4 با نداشت چندین آدرس خصوصی به یک آدرس عمومی واحد استفاده می‌شود.

لازم به ذکر است IPv4 دارای هیچ ویژگی امنیتی داخلی نیست (No Built-in Security) و آن را در برابر حملات آسیب‌پذیر می‌سازد. همچنین هدر (Header) آن پیچیده است (Complex Header) که منجر به افزایش سربار و کاهش کارایی می‌شود. علیرغم محدودیت‌های آن، IPv4 امروزه به طور گسترده مورد استفاده قرار می‌گیرد و دلیل آن بخاطر سختی زیرساخت شبکه به صورت یک‌باره است؛ اما به دلیل تعداد محدود آدرس‌های IPv4، پذیرش IPv6 برای اطمینان از رشد مداوم اینترنت ضروری شده است.

آی‌پی ورژن ۶ آخرین نسخه پروتکل اینترنت (IP) است که استاندارد مورد استفاده برای انتقال داده‌ها از طریق اینترنت است. به عنوان ارتقاء IPv4 طراحی شده است که از روزهای اولیه اینترنت استفاده می‌شد و اکنون آدرس‌های آن تمام شده است؛ طول آدرس‌های IPv6 برابر ۱۲۸ بیت است و فضای آدرس بسیار بزرگتری را ارائه می‌دهند. این اجازه می‌دهد تا تعداد بسیار بیشتری از آدرس‌های IP منحصر به فرد داشته باشیم که با توجه به افزایش تعداد دستگاه‌های متصل به اینترنت، مهم است.

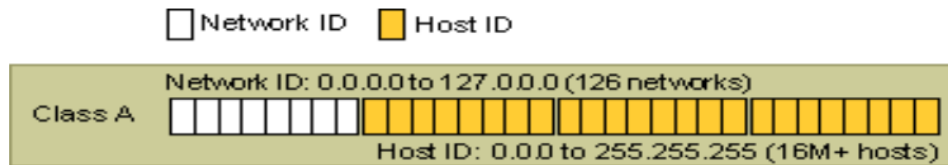
در مقایسه با IPv4، شامل ویژگی‌های امنیتی داخلی است، مانند پشتیبانی از IPsec، که راهی امن برای انتقال داده‌ها از طریق اینترنت فراهم می‌کند. همچنین هدر IPv6 ساده‌تر و کارآمدتر از هدر IPv4 است که منجر به بهبود سرعت پردازش و کاهش سربار می‌شود. علی‌رغم این پیشرفت‌ها، انتقال از IPv4 به IPv6 ادامه دارد و به دلیل حجم زیادی از زیرساخت‌ها و دستگاه‌های موجود که از IPv4 استفاده می‌کنند، کند بوده است. با این حال، همانطور که آدرس‌های IPv4 همچنان در حال اتمام هستند، پذیرش IPv6 به طور فزاینده‌ای ضروری می‌باشد.

کلاس‌های مختلف IP نسخه‌ی ۴:

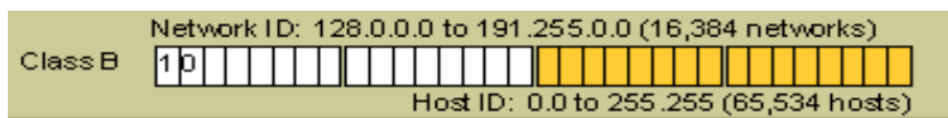
سه کلاس پایه‌ای مختلف نشانی‌دهی IP، برای شبکه‌های بزرگ، متوسط و کوچک وجود دارد. کلاس A برای شبکه‌های بزرگ، کلاس B برای شبکه‌های متوسط و کلاس C برای شبکه‌های کوچک است. علاوه بر این سه کلاس، کلاس D نیز برای پخش چندگانه، ارسال اطلاعات به گروهی از رایانه‌ها مورد استفاده قرار می‌گیرد. همچنین کلاس E نیز وجود دارد که برای کارهای جستجو مورد استفاده قرار می‌گیرد.

Subnet mask	CIDR	پایان	شروع	طول بر حسب بیت	کلاس
۲۵۵,۰,۰,۰	/۸	۱۲۷,۲۵۵,۲۵۵,۲۵۵	۰,۰,۰,۰	۰	Class A
۲۵۵,۲۵۵,۰,۰	/۱۶	۱۹۱,۲۵۵,۲۵۵,۲۵۵	۱۲۸,۰,۰,۰	۱۰	Class B
۲۵۵,۲۵۵,۲۵۵,۰	/۲۴	۲۲۳,۲۵۵,۲۵۵,۲۵۵	۱۹۲,۰,۰,۰	۱۱۰	Class C
Not defined	/۴	۲۳۹,۲۵۵,۲۵۵,۲۵۵	۲۲۴,۰,۰,۰	۱۱۱۰	Class D(multicast)
Not defined	/۴	۲۵۵,۲۵۵,۲۵۵,۲۵۵	۲۴۰,۰,۰,۰	۱۱۱۱	Class E(reserved)

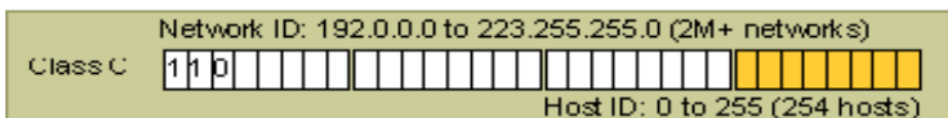
- در کلاس A آدرس‌های IP با عددی بین ۱ تا ۱۲۶ شروع می‌شوند و آدرس میزبان در سه جزء آخر قرار می‌گیرد.



- در کلاس B آدرس‌های IP با عددی میان ۱۲۸ تا ۱۹۱ شروع می‌شوند و با عددی توسط موسسه اختصاص دهنده IP تعیین می‌شود، ادامه می‌یابند. دو جزء آخر متغیر هستند.



- در کلاس C آدرس‌های IP با عددی بین ۱۹۲ تا ۲۲۳ شروع می‌شوند و با دو عددی که توسط موسسه اختصاص دهنده IP تعیین می‌گردد، ادامه می‌یابند. جزء آخر متغیر خواهد بود.



- اکثر تجهیزات شبکه IP آدرس‌های کلاس E را مسیریابی نمی‌کنند و برای شبکه‌ی تست است.

:gateway

gateway یک دستگاه شبکه است که به عنوان یک واسطه بین دو یا چند شبکه عمل می‌کند و داده‌ها را بین آنها ارسال می‌کند. gateway مسئول مسیریابی داده بین شبکه‌های مختلف و تبدیل پروتکل‌ها در صورت نیاز است. یک gateway می‌تواند در انواع مختلفی من جمله روتر، فایروال، VPN، مودم، توزیع کننده‌ی بار (load balancer) و ... ظاهر شود.

همچنین gateway می‌تواند به عنوان یک دستگاه مستقل یا به عنوان یک جزء نرم‌افزاری در حال اجرا بر روی رایانه پیاده‌سازی شود.

در لینوکس می‌توان با استفاده از دستور "ip route show" و یا "netstat -r" ملاحظه فرمود. همچنین در ویندوز هم می‌توان با دستور "route print" و یا دستور ipconfig به آدرس gateway رسید.

آدرس‌های خاص:

- آدرس **255.255.255.255**: اگر بخواهیم به صورت باینری بگوییم، تمام ارقام این آدرس برابر ۱ خواهد بود. این IP برای انتشار پیام به شبکه محلی است، به این معنی که توسط هر میزبان IP در شبکه محلی قابل رویت است یا به عبارتی دیگر برای ارسال پیام‌های فراگیر برای تمام ماشین‌های میزبان بر روی شبکه محلی، که ماشین فرستنده در آن شبکه قرار دارد به کار می‌رود.
- آدرس **0.0.0.0**: هر ماشین میزبان که آدرس IP خود را نداند، این آدرس را بعنوان آدرس خود فرض می‌کند. مثل اینکه برای کسی نامه بفرستید ولی آدرس خود را بعنوان نویسنده ننوشته باشید، در نتیجه گیرنده نمی‌تواند پاسخی بدهد.
- حالتی که تمام بیت‌های ID شبکه صفر (تمام بایت‌های آن ۰) باشد ولی ID میزبان معتبر باشد: این آدرس وقتی به کار می‌رود که آدرس میزبان، آدرس مربوط به شبکه خودش را نداند. مثال: 0.0.123.54 برای کلاس B.
- حالتی که IP با یک یا چند بایت با مقدار ۲۵۵ شروع شود: هیچ شبکه‌ای نمی‌تواند یک ID به صورتی داشته باشد که با یک یا چند بایت با مقدار ۲۵۵ شروع شود. این گونه آدرس‌ها برای الگوهای زیر شبکه (Subnet Mask) استفاده شده‌اند. مثال: 255.255.0.0

:MAC Address

MAC Address یک آدرس فیزیکی است. این آدرس در زمان تولید دستگاهی که قابلیت اتصال به شبکه را دارد، توسط کارخانه تولید کننده به آن تخصیص داده می‌شود به صورتی که این آدرس یکتا باشد. بنابراین به کمک مک آدرس می‌توان به صورت یکتا یک دستگاه متصل به شبکه را مشخص کرد.

یک سیستم کامپیوتری می‌تواند چندین اینترفیس قابل اتصال به شبکه داشته باشد، مثلاً یک کارت شبکه و یک اینترفیس اتصال بی‌سیم (Wi-Fi). این دو اینترفیس یک مک آدرس متمایز از هم دارند بنابراین توجه به این نکته ضروری است که به کمک مک آدرس اینترفیس‌ها به صورت یکتا مشخص می‌شوند و نه سیستم‌های کامپیوتری.

طول مک آدرس ۴۸ بیت است که معمولاً به فرمت XX-XX-XX-XX-XX-XX به صورت ۱۲ رقم در مبنای ۱۶ نمایش داده می‌شود. برای به دست آوردن مک آدرس تمام اینترفیس‌های سیستم می‌توان از دستور "getmac" در Command Prompt استفاده کرد.

پروتکل TCP:

TCP به این منظور طراحی شد تا یک دنباله از بایت‌ها را به صورت مطمئن و عاری از خطا بین دو نقطه‌ی پایانی از شبکه‌ای که نامطمئن و مستعد خطاست، منتقل نماید.

در شکل زیر ساختار یک قطعه‌ی TCP را مشاهده می‌کنید. فیلدهای پورت مبدا و پورت مقصد نقاط انتهایی دو طرف یک اتصال را مشخص می‌نمایند. ترتیب قطعه‌ی داده و اعلام وصول داده‌ها با فیلدهای sequence number و acknowledgment number مشخص می‌شوند.

TCP Header																																
Bit offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Source port																Destination port															
32	Sequence number																															
64	Acknowledgment number (if ACK set)																															
96	Data offset			Reserved			N S	C W R	E C E	U R G	A C K	P S H	R S T	S Y N	F I N	Window Size																
128	Checksum																Urgent pointer (if URG set)															
160	Options (if Data Offset > 5)																							padding								
...	...																															

در ادامه توضیح پرچم‌های تک بیتی ECE, CWR, NS, FIN, SYN, PST, PSH, ACK, Urg داده می‌شود:

بیت NS(ECN): برای محافظت در برابر پنهان کاری عمدی یا تصادفی بسته‌های TCP فرستنده استفاده می‌شود. با جلوگیری از بهره‌برداری ECN برای بدست آوردن سهم ناعادلانه از پهنای باند، باعث بهبود کنترل ازدحام می‌شود. کاربر صحیح ECN نیازمند همکاری گیرنده در فرستادن سیگنال پاسخ Congestion Experienced به فرستنده است اما این پروتکل مکانیزمی برای الزام این همکاری ندارد.

بیت ECE(ECN Echo): اگر بیت SYN، فعال شده باشد، این بیت نشان دهنده‌ی این است که بسته TCP قابلیت ECN دارد. اگر بیت SYN، صفر باشد این بیت نشان می‌دهد که بسته‌ای دارای پرچم set شده‌ی Congestion Experienced در سرآیند بسته‌ی IP بوده، در طول مبادله اطلاعات، دریافت شده است.

بیت CWR(Congestion Window Reduced): توسط فرستنده برای نشان دادن دریافت یک segment که پرچم ECE آن set شده و به مکانیزم کنترل ازدحام جواب داده، set می‌شود.

بیت URG: در صورتی که این بیت ۱ باشد معینی می‌شود که در فیلد Urgent Pointer مقدار معتبری قرار دارد و بایستی مورد پردازش قرار بگیرد.

بیت ACK: اگر این بیت ۱ باشد، به این معنا است که در فیلد Acknowledgement Number عدد معتبری قرار دارد. بیت‌های ACK و SYN نقش دیگری نیز دارند که در ادامه به آن اشاره خواهد شد.

بیت PSH: اگر این بیت ۱ باشد، از گیرنده تقاضا می‌شود که داده‌های موجود را بافر (buffer) نکرده و در اسرع وقت تحویل داده شود.

بیت RST: اگر این بیت ۱ باشد، به این معنی است که این ارتباط به صورت یک طرفه خاتمه یافته است.
بیت SYN: این بیت نقش اساسی در ارتباط یک بسته TCP بازی می‌کند. برقراری ارتباط یک طرفه TCP از روند زیر تبعیت می‌کند:

- شروع کننده ارتباط یک بسته TCP بودن هیچ داده‌ای و با تنظیم بیت‌های $SYN=1$ و $ACK=0$ تقاضای یک ارتباط جدید می‌کند.

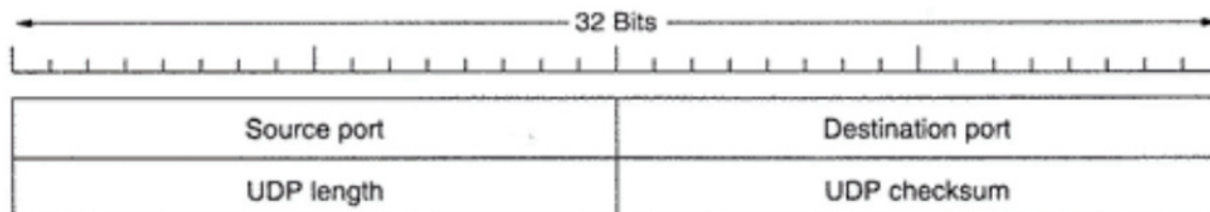
- در صورتی که طرف مقابل تمایل به برقراری ارتباط داشته باشد، برای طرف مقابل یک بسته با قرار دادن بیت‌های $SYN=1$ و $ACK=1$ می‌فرستد. بنابراین، تمایل خود را برای برقراری ارتباط به طرف مقابل اعلام می‌کند.

بیت FIN: اگر یکی از طرفین هیچ داده دیگری برای فرستادن نداشته باشد، این بیت را در آخرین بسته برابر با ۱ قرار می‌دهد و ارتباط را یک طرفه قطع می‌کند. باید توجه داشت که ارتباط هنوز به طور کامل قطع نشده است و باید طرف مقابل نیز در آخرین بسته خود این فیلد را برابر با ۱ قرار داده تا ارتباط کامل قطع شود.

پروتکل UDP:

UDP یا User Datagram Protocol یک پروتکل بدون اتصال در لایه انتقال است. UDP اطلاعات را از طریق پروتکل IP منتقل می‌کند، اما به دلیل اینکه از Sequence Number و سیستمی مانند Three Way Handshake که در پروتکل TCP استفاده می‌شود پشتیبانی نمی‌کند، پروتکل چندان قابل اطمینانی نیست. به این معنی که درستی تحویل پیام‌ها در این پروتکل مورد بررسی قرار نمی‌گیرد اما تضمین می‌کند که حداکثر تلاش خود را برای تحویل اطلاعات انجام دهد. بنابراین، این پروتکل رسیدن اطلاعات را در مقصد بررسی نمی‌کند و لذا نرخ ارسال آن به مراتب بالاتر از پروتکل TCP می‌باشد.

UDP داده‌ها را در قالب قطعاتی ارسال می‌کند که در ابتدای آن‌ها ۸ بایت سرآیند و سپس داده‌های لایه‌ی کاربرد قرار می‌گیرند. این سرآیند در شکل زیر نشان داده شده است. دو فیلد شماره‌ی پورت به منظور شناسایی نقاط پایانی (پرونده‌های نهایی) در ماشین‌های مبدا و مقصد به کار می‌آید.



پروتکل ICMP:

این پروتکل امکانات لازم در خصوص اشکال‌زدائی و گزارش خطا در رابطه با بسته‌های اطلاعاتی غیر قابل توزیع را فراهم می‌نماید. با استفاده از ICMP، کامپیوترها و روترها (router) که از IP به منظور ارتباطات استفاده می‌نمایند، قادر به گزارش خطا و مبادله اطلاعاتی محدود در رابطه وضعیت بوجود آمده می‌باشند. مثلاً در صورتی که IP قادر به توزیع یک بسته اطلاعاتی به مقصد مورد نظر نباشد، ICMP یک پیام مبتنی بر غیر قابل دسترس بودن را برای کامپیوتر مبدا ارسال می‌دارد. با اینکه پروتکل IP به منظور انتقال داده بین روترهای متعدد استفاده می‌گردد، ولی ICMP به نمایندگی از TCP/IP مسئول ارائه گزارش خطا و یا پیام‌های کنترلی است. تلاش ICMP در جهت این نیست که پروتکل IP را به عنوان یک پروتکل مطمئن مطرح نماید چراکه پیام‌های ICMP دارای هیچ‌گونه محتویاتی مبتنی بر اعلام وصول پیام Acknowledgment بسته اطلاعاتی نمی‌باشند بلکه صرفاً سعی در گزارش خطا و ارائه فیدبک‌های لازم در رابطه با تحقق یک وضعیت خاص را می‌نماید. این پروتکل مسئول انجام کارهای زیر است:

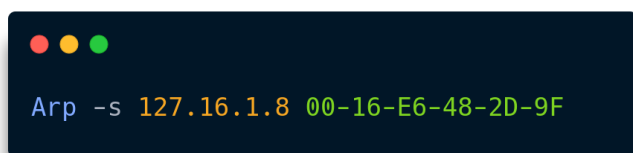
- Echo Request و Echo Replay برای کنترل امکان ارتباط با یک دستگاه مرتبط با شبکه مبتنی بر IP
- Source quench message برای اطلاع دادن buffer overflow به کامپیوتر ارسال کننده اطلاعات
- Destination Unreachable که نمایش دهنده عدم امکان ارتباط با مقصد مورد نظر می‌باشد

- یک سیستم می‌تواند از این پروتکل برای امتحان اینکه آیا سیستم دیگر فعال است یا خیر با فرستادن ping استفاده کند. اگر سیستم ping شده فعال باشد به فرستادن پیام پاسخ واکنش نشان می‌دهد.

پروتکل ARP:

از این پروتکل به منظور تبدیل آدرس‌های IP به آدرس‌های فیزیکی (MAC Address) استفاده می‌شود. در واقع به این کار name resolve می‌گویند. روش کار این پروتکل به این صورت است که آدرس هر میزبان به عنوان یک عضو در شبکه در جدولی به نام ARP یا حافظه ARP نگهداری می‌شود. جدول ARP رابط بین آدرس‌های فیزیکی و آدرس‌های IP در یک شبکه است. زمانی که یک میزبان بر روی شبکه قصد فرستادن یک پیام به میزبان دیگری روی شبکه دارد، میزبان اول آدرس فیزیکی مقصد را از روی جدول ARP معین می‌کند. اگر آدرس مقصد در جدول موجود نباشد، فرستنده یا مرجع یک پخش (broadcast) روی شبکه می‌فرستد. این درخواست حاوی آدرس IP نامشخص می‌باشد. تمام میزبان‌ها در شبکه درخواست ARP را دریافت می‌کنند و میزبانی که آدرس IP نامشخص متعلق به آن است، آدرس فیزیکی خود را به مرجع یا میزبان اول می‌فرستد. جدول ARP ارتباط جدید را به عنوان یک آدرس جدید در خود نگهداری می‌کند.

برای استفاده از پروتکل ARP از دستور ARP در Command Prompt استفاده می‌کنیم. به عنوان مثال دستور arp -a لیست آدرس‌های فیزیکی را به همراه آدرس IP آن‌ها نشان می‌دهد. از دستورات دیگر می‌توان به arp -s را نام برد که به صورت استاتیک یک درایه به جدول ARP اضافه می‌کند. نحوه‌ی استفاده از آن در مثال زیر آمده است:



```
Arp -s 127.16.1.8 00-16-E6-48-2D-9F
```

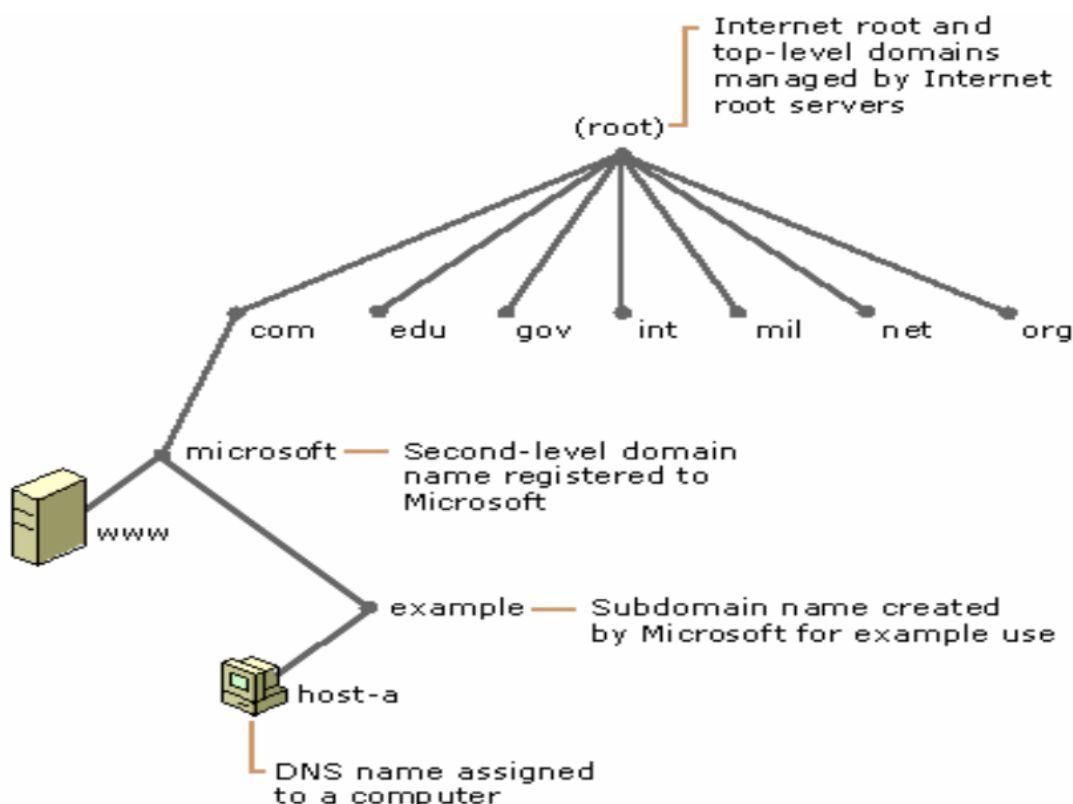
برای مشاهده‌ی دیگر فرمت‌های این دستور از help در Command Prompt یا man در terminal استفاده کنید.

پروتکل DNS:

DNS یک پایگاه سلسله مراتبی است که در جهان به طور گسترده برای ذخیره سازی انواع مختلفی از اطلاعات شامل آدرس های IP، نام حوزه ها و اطلاعات سرویس دهنده پست الکترونیک مورد استفاده قرار می گیرد. روش کار DNS به طور خلاصه این چنین است: برای تبدیل یک نام به آدرس IP، برنامه یک تابع کتابخانه ای به نام تبدیل کننده (resolver) را فراخوانی می کند و نام مورد نظر را به صورت پارامتر به آن می دهد. تبدیل کننده یک بسته ی UDP را به سرویس دهنده ی DNS محلی می فرستد، که این DNS آدرس IP معادل نام خواسته شده را یافته و به تبدیل کننده بر می گرداند. که آن هم به نوبه ی خود، آدرس برنامه را به فراخوان کننده تحویل می دهد. برنامه هم پس از به دست آوردن آدرس IP کامپیوتر مقصد، می تواند با آن ارتباط TCP برقرار کرده یا بسته های UDP به آن بفرستد.

همانطور که در شکل زیر مشاهده می کنید، در بالای سلسله مراتب این درخت ریشه سرورهای DNS وجود دارد. این درخت شامل اطلاعات در مورد سرورهای DNS در سطوح پایین تر سلسله مراتب می باشد. سطوح پایین تر سلسله مراتب DNS شامل سرورهای DNS برای نام حوزه های [org]، [com] و [net] می باشد.

برای استفاده از پروتکل DNS از دستور nslookup استفاده می کنیم که در دستور کار با نحوه استفاده از آن آشنا خواهید شد.



پروتکل DHCP:

DHCP یا همان Dynamic Host Configuration Protocol یک پروتکل شبکه است که تخصیص آدرس‌های IP و سایر پارامترهای پیکربندی شبکه را به دستگاه‌های شبکه مانند رایانه‌ها، تلفن‌های هوشمند و چاپگرها به طور خودکار انجام می‌دهد. هدف DHCP این است که با حذف نیاز به پیکربندی دستی آدرس‌های IP و سایر تنظیمات در هر دستگاه، مدیریت شبکه‌های بزرگ را آسان کند.

نحوه‌ی کارکرد DHCP به صورت زیر است:

- دستگاهی مانند رایانه یک پیام broadcast را ارسال می‌کند که یک آدرس IP و سایر اطلاعات پیکربندی شبکه را درخواست می‌کند.
- یک سرور DHCP درخواست را دریافت می‌کند و یک آدرس IP از مجموعه‌ای از آدرس‌های موجود به همراه سایر اطلاعات پیکربندی شبکه، مانند default gateway، subnet mask و آدرس‌های سرور DNS به دستگاه اختصاص می‌دهد.
- سرور DHCP پاسخی را به دستگاه ارسال می‌کند که شامل آدرس IP اختصاص داده شده و سایر اطلاعات پیکربندی شبکه است.
- دستگاه از آدرس IP اختصاص داده شده و سایر اطلاعات پیکربندی شبکه برای پیکربندی خود برای استفاده در شبکه استفاده می‌کند.
- سرور DHCP آدرس‌های IP را که به دستگاه‌ها اختصاص داده است را ردیابی می‌کند و مجموعه آدرس‌های IP موجود را مدیریت می‌کند. وقتی دستگاهی دیگر از آدرس IP استفاده نمی‌کند، سرور DHCP آن آدرس را برای استفاده مجدد در دسترس قرار می‌دهد.

از مزایای کلیدی DHCP این است که نیاز به پیکربندی دستی تنظیمات شبکه را از بین می‌برد که می‌تواند زمان بر و مستعد خطا باشد. DHCP همچنین مدیریت شبکه‌های بزرگ را با ارائه یک روش متمرکز برای مدیریت آدرس‌های IP و سایر اطلاعات پیکربندی شبکه آسان می‌کند. علاوه بر این، DHCP می‌تواند به صورت پویا آدرس‌های IP را در صورت نیاز به دستگاه‌ها تخصیص دهد، که می‌تواند در محیط‌هایی که دستگاه‌ها اغلب از شبکه اضافه و حذف می‌شوند، مفید باشد.

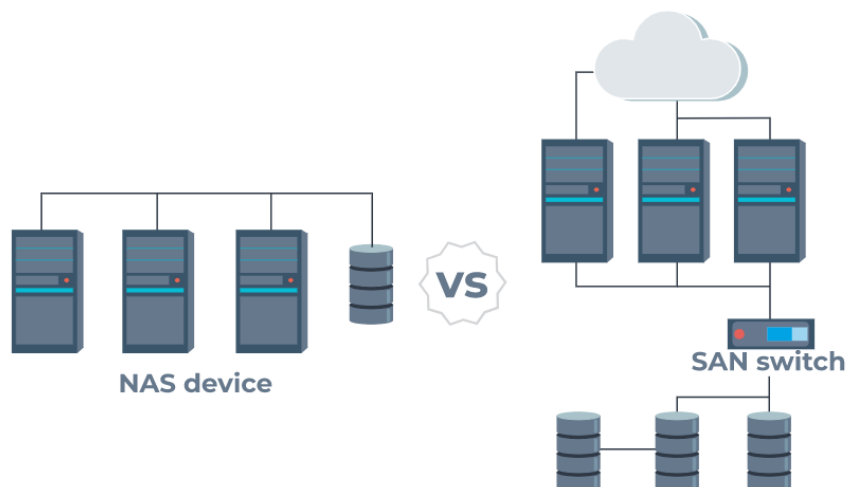
پروتکل SAN

SAN مخفف Storage Area Network است. SAN یک شبکه اختصاصی پرسرعت است که دسترسی در سطح بلوک به فضای ذخیره‌سازی را فراهم می‌کند. هدف اصلی SAN ارائه مدیریت ذخیره‌سازی متمرکز و خودکار و بهینه‌سازی استفاده از ذخیره‌سازی داده‌ها است.

SAN متشکل از چندین دستگاه ذخیره‌سازی، سوئیچ‌ها و سیستم‌های میزبان است که توسط یک شبکه پرسرعت متصل شده‌اند. دستگاه‌های ذخیره‌سازی ممکن است شامل disk arrays, tape libraries و سایر دستگاه‌های ذخیره‌سازی باشند. میزبان از طریق یک پروتکل SAN مانند کانال فیبر، iSCSI یا FCoE به منابع ذخیره‌سازی دسترسی دارند. SAN توابع Data transfer و همین‌طور Device management، احراز هویت (برای امنیت) و همچنین پشتیبان‌گیری (برای حفاظت از داده) را در اختیار میزبان قرار می‌دهد.

پروتکل NAS

NAS مخفف Network Attached Storage است. یک دستگاه ذخیره‌سازی متصل به شبکه (NAS) یک سرور ذخیره‌سازی اطلاعات رایانه‌ای در سطح فایل مستقل است که به یک شبکه رایانه‌ای متصل است و دسترسی به داده‌ها را برای گروه ناهمگنی از مشتریان فراهم می‌کند. دقت فرمایید که دسترسی در NAS بر اساس فایل است ولی در SAN بر اساس دیسک بلاک است؛ لذا دستگاه‌های NAS از اتصال استاندارد اینترنت استفاده می‌کنند و می‌توان با استفاده از انواع پروتکل‌های سطح فایل مانند SMB/CIFS (مورد استفاده در سیستم‌های مبتنی بر ویندوز)، NFS (مورد استفاده در سیستم‌های مبتنی بر لینوکس) و FTP به آنها دسترسی داشت. دستگاه‌های NAS معمولاً در مشاغل کوچک تا متوسط، دفاتر خانگی و دفاتر شعب راه دور برای ارائه ذخیره‌سازی متمرکز داده‌ها و پشتیبان‌گیری، و همچنین برای به اشتراک‌گذاری فایل‌ها و داده‌ها بین چندین کاربر و مشتریان استفاده می‌شوند.



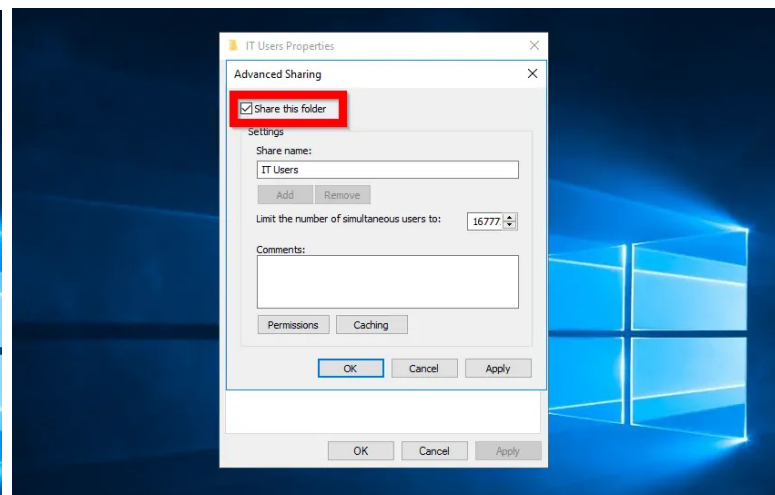
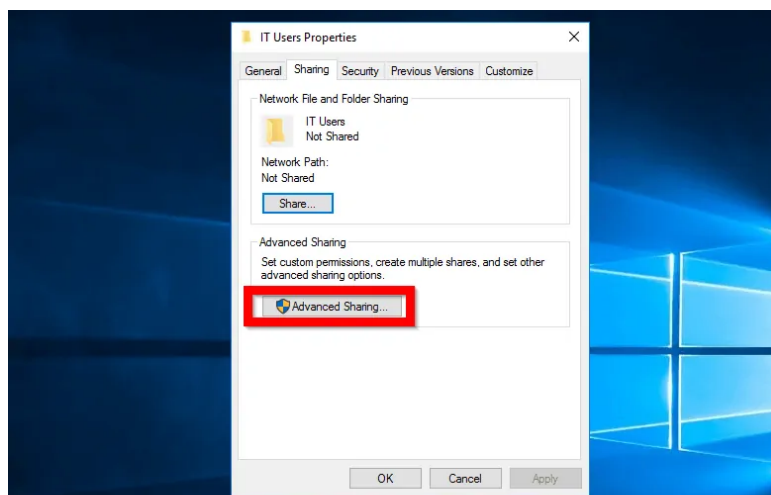
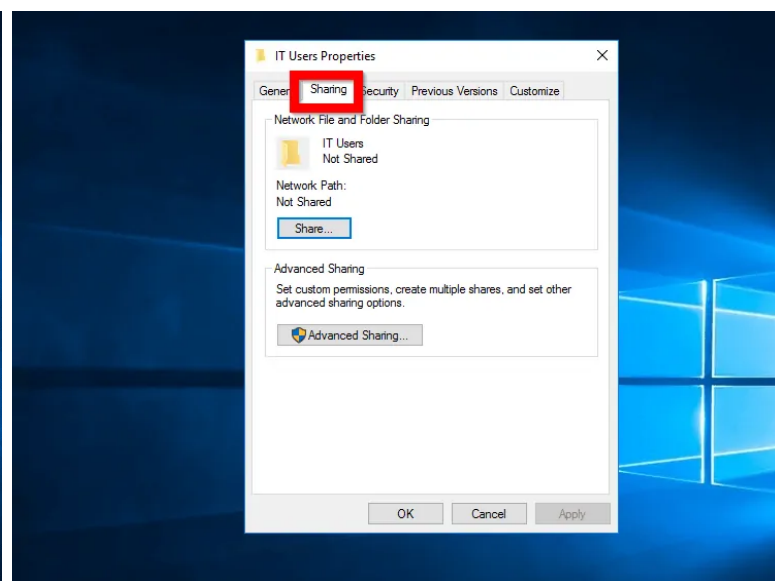
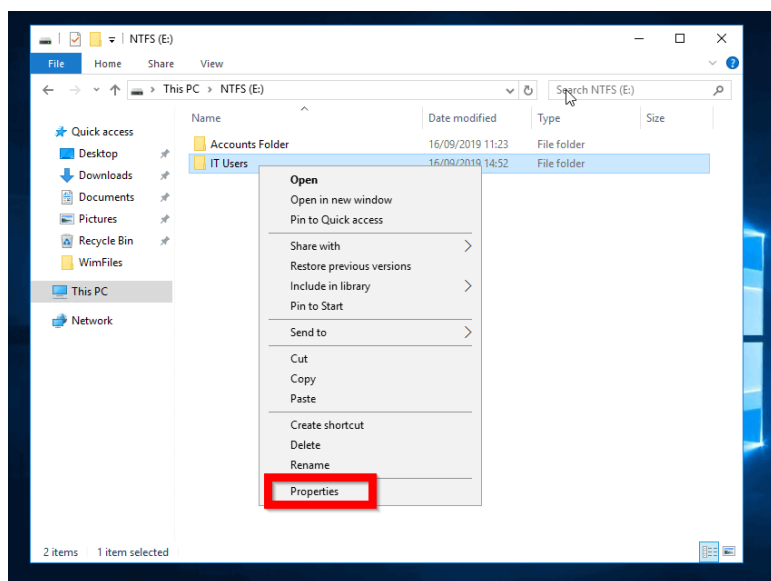
همانطور که در تصویر بالا ملاحظه می‌فرمایید، NAS تنها چند دیسک را از طریق شبکه به اشتراک می‌گذارد اما SAN یک پروتکل ذخیره‌سازی برایمان فراهم می‌کند که این کار باعث می‌شود یک انتزاع ایجاد نموده و به واسطه‌ی این عمل امنیت بالا رفته، بازدهی می‌تواند بهتر باشد و همینطور بحث‌های مرتبط با مقیاس‌پذیری و دسترسی‌پذیری را بهتر کنترل کند.

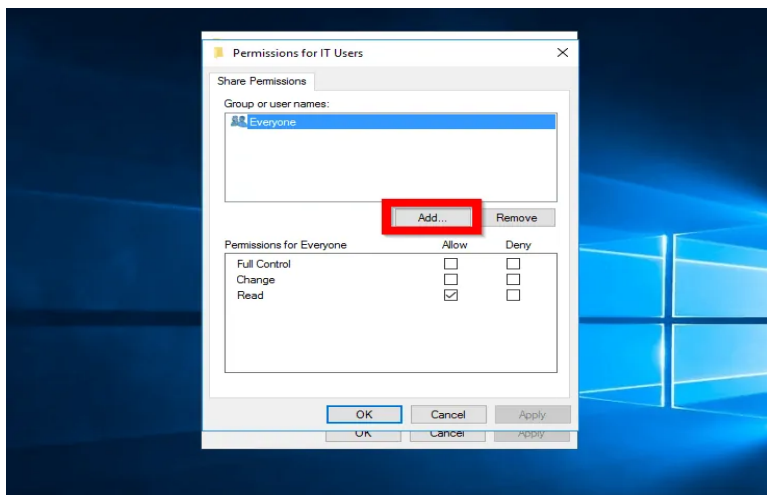
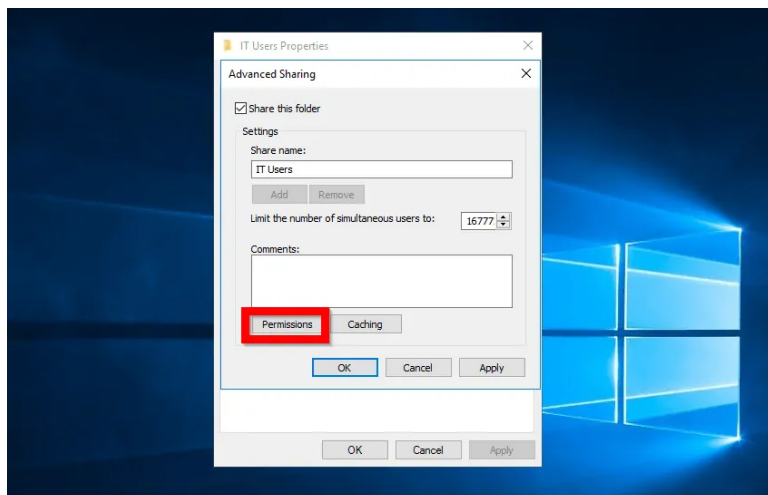
اشتراک‌گذاری فایل در شبکه

در لینوکس پروتکل NFS یا همان Network File System وجود دارد که در NAS نیز مورد استفاده قرار می‌گیرد. با این پروتکل می‌توان فایل‌ها را به اشتراک گذاشت.

همچنین سرویس SAMBA یک برنامه است که با استفاده از پروتکل‌های SMB و CIFS کمک می‌کند تا بتوانیم فایل و پوشه‌ها را در لینوکس به اشتراک بگذاریم.

در ویندوز نیز با راست کلیک بر روی یک پوشه و رفتن به قسمت properties و سپس انتخاب Sharing و لحاظ کردن تنظیمات لازمه در قسمت Advanced Sharing در همین بخش، می‌توان سطح دسترسی اشتراک‌گذاری پوشه و همچنین یوزرهای مورد دسترس را مشخص نمود.





تجهیزات شبکه و حدود عملکرد آنها:

- Hub:** در این دستگاه که در حد لایه Physical عمل می کند، سیگنال ها پس از دریافت بدون هیچگونه تحلیلی، خروجی را سریعاً ارسال می کند. این دستگاه به عنوان یک واسط برای ارتباط بین دستگاه ها هر سیگنال را پس از دریافت به تمام پورت ها غیر از پورت مبدا ارسال می کند. روش عملکرد Hub همواره به صورت Half Duplex می باشد.
- Switch:** در این دستگاه علاوه بر دریافت و ارسال سیگنال کارهای دیگری نیز انجام می شود. در حقیقت حدود عملیاتی که در switch انجام می شوند لایه Datalink می باشد. یعنی سوئیچ در دو لایه پایینی OSI کار می کند. Switch سیگنال ها را دریافت کرده و پس از دریافت آن ها یک Frame به صورت کامل، ابتدا اقدام به کنترل CRC و سپس آدرس مبدا و مقصد (MAC Address) آن می نماید. با کنترل آدرس مبدا، شماره پورت و MAC Address مربوط به کامپیوتر ارسال کننده در جدول Filter/Forward ثبت می گردد و اطلاعات صرفاً به همان پورتی که مقصد به آن متصل است ارسال می شود. در صورت وجود نداشتن آدرس کامپیوتر مقصد در جدول مذکور، Frame دریافت شده توسط switch به تمام پورت ها ارسال شده یا اصطلاحاً Flood می شود. ضمناً در صورتی که یک Frame از نوع Broadcast به switch برسد، به تمام پورت ها فلود می شود.
- Bridge:** این دستگاه به switch شباهت دارد و از نظر لایه های کاری نیز در دو لایه پایینی کار می کند. تمام موارد کاری آن شبیه switch است با این تفاوت که تعداد پورت های آن معمولاً دو تا و در برخی موارد چهارتا می باشد و برای اتصال شبکه های Bus به یکدیگر طراحی شده اند.

- **Router**: این دستگاه یک لایه بالاتر از switch کار می کند. در حقیقت این دستگاه در سه لایه پایینی از OSI کار می کند و از آدرس های logical برای تشخیص مسیر ارسال Frame استفاده می کند. بر خلاف switch که در صورت دریافت Frame از نوع broadcast آن را Flood می کند، Router اجازه عبور آن را نمی دهد.

دستورات خط فرمان

● Ipconfig

برای نشان دادن اطلاعات IP مورد استفاده قرار می گیرد؛ این دستور در ویندوز استفاده می شود و معادل لینوکسی آن ifconfig و یا دستور ip می باشد.

- ipconfig/all جزئیات بیشتری مانند DNS Server ها را نیز نشان می دهد.
 - ipconfig/renew برای تجدید آدرس IP یک کارت شبکه ی مشخص استفاده می شود
- برای مشاهده ی دیگر آپشن های این دستور می توانید از HELP خط فرمان استفاده کنید.

● netsh

این دستور به شما اجازه می دهد تا به صورت محلی (Local) و یا از راه دور (remote) تنظیمات شبکه ی کامپیوتری که netsh را اجرا می کند، تغییر و یا نمایش دهید.

netsh همچنین از طریق اسکریپت نویسی (scripting) این اجازه را به شما می دهد تا گروهی از دستورات را به حالت Batch برای کامپیوترهای مشخصی اجرا نمایید. همچنین این امکان را در اختیار شما قرار می دهد تا تنظیمات را در قالب یک فایل متنی به منظور پیکربندی سیستم های دیگر ذخیره کنید. به عنوان مثال دستور زیر کارت شبکه ای به نام local area connection را با آدرس IP معادل 192.168.0.100 و subnet mask معادل 255.255.255.0 و همچنین default gateway معادل 192.168.0.1 پیکربندی می کند.

```
netsh interface ip set address name="Local Area Connection" static 192.168.0.100 255.255.255.0 192.168.0.1
```

با استفاده از دستور زیر می توان از DHCP، یک IP جدید گرفت.



```
netsh interface ip set address "Local Area Connection" dhcp
```

برای تنظیم DNS Server به صورت static از دستور زیر استفاده می‌کنیم:



```
netsh interface ip set dns name="Local Area Connection"  
source=static addr=192.168.0.2 register=none
```

همچنین اگر بخواهیم DNS Server را به صورت Dynamic از دستور زیر استفاده می‌کنیم:



```
netsh interface ip set dns name="Local Area Connection" source=dhcp
```

برای اطلاعات بیشتر و آشنایی با کاربردهای بیشتر این دستور می‌توانید از لینک زیر بهره ببرید.

<https://www.cyberithub.com/31-most-useful-netsh-command-examples-in-windows>

لازم به ذکر است این دستور به مدیران شبکه اجازه می‌دهد تنظیمات مختلف شبکه از جمله پیکربندی شبکه، عیب‌یابی و تسک‌های مربوط به امنیت را مدیریت کنند. دستور netsh را می‌توان برای پیکربندی تنظیمات اجزای مختلف شبکه، از جمله آدرس‌های IP، سرورهای DNS، سرورهای WINS، مسیریابی و دسترسی از راه دور استفاده کرد. تنها نکته‌ی باقی مانده آن است که این دستور تنها برای سیستم‌عامل ویندوز می‌باشد و برخی از کارهای یاد شده را در لینوکس می‌توان با دستور iptable انجام داد. برای اطلاعات بیشتر می‌توانید لینک زیر را مطالعه فرمایید.

<https://phoenixnap.com/kb/iptables-tutorial-linux-firewall>

• netstat

این دستور اتصالات شبکه (network connections) ورودی و خروجی و جداول مسیریابی و... را نشان می‌دهد. از دستور netstat -a برای مشاهده‌ی connection ها و پورت‌های TCP و UDP در حال شنود استفاده می‌شود.

همچنین از netstat -r برای مشاهده جدول مسیریابی استفاده می‌شود.

می‌توان از "netstat -p protocol" نیز برای مشاهده‌ی connection ها با پروتکل خاص استفاده می‌شوند، استفاده کرد.

• nslookup

به کمک دستور nslookup می‌توان رکوردها و ازجمله آدرس IP مربوط به DNS یک دامنه یا به صورت برعکس دامنه مربوط به یک IP را به دست آورد ("Reverse DNS Lookup"). این دستور دو مد کاری interactive و non-interactive دارد.

با استفاده از دستور به فرم "nslookup google.com" در حالت non-interactive هستیم و در نتیجه‌ی اجرای این دستور، آدرس IP دامنه google.com به عنوان خروجی تولید می‌شود. اگر دستور nslookup را به تنهایی در Command Prompt اجرا کنیم وارد حالت تعاملی می‌شویم که در این حالت می‌توان در یک حالت رفت و برگشتی برای دامنه های مختلف با وارد کردن آدرس دامنه IP آدرس آن را دریافت کرد.

برای انجام Reverse DNS Lookup نیز کافی است به جای آدرس دامنه مورد نظر، آدرس IP مورد نظر را وارد کنیم: "nslookup 8.8.8.8".

• arp

دستور arp یک ابزار خط فرمان در ویندوز و لینوکس است که کش ARP یا همان Address Resolution Protocol را نمایش داده و امکان تغییر آن را می‌دهد. ARP پروتکلی است که یک آدرس IP را به یک آدرس فیزیکی (MAC) در شبکه نگاشت می‌کند.

حافظه کش ARP برای ذخیره نگاشت‌های ARP که اخیراً جستجو شده‌اند برای دسترسی سریع‌تر استفاده می‌شود. دستور arp را می‌توان برای مشاهده محتویات کش ARP و همچنین برای افزودن، حذف یا تغییر ورودی‌های کش استفاده کرد.

در قسمت زیر چند نمونه از استفاده‌ی این دستور در دو سیستم‌عامل لینوکس و ویندوز را مثال خواهیم زد.

○ نمایش کش ARP فعلی:

```
arp -a #in windows  
arp -n #in linux
```

○ افزودن ARP static:

```
arp -s <ip-address> <mac-address> #in windows  
arp -s <ip-address> <mac-address> <interface> #in linux
```

○ حذف یک رکورد ARP:

```
arp -d <ip-address> #in both OS
```

برای اطلاعات بیشتر می‌توانید HELP یا man این دستور را متناظر با سیستم‌عامل مورد استفاده‌ی خود ملاحظه فرمایید.

• whois:

whois پروتکلی است که یک رابط برای ذخیره سازی و به دست آوردن اطلاعات مربوط به یک دامنه را فراهم می کند. به کمک کلاینت whois می‌توان اطلاعاتی که برای یک دامنه در سرورهای

whois ذخیره شده است را به دست آورد. دستور whois را میتوان برای یک IP آدرس یا یک دامنه به کار برد. مثال: "whois 8.8.8.8".

از جمله اطلاعاتی که در خروجی whois نمایش داده میشود، سرورهای DNS دامنه مورد است که یکی از کاربردهای مهم دستور whois به دست آوردن آدرس و لیست این سرورها میباشد.

● traceroute & tracepath

ابزارهای شبکه‌ای که برای نمایش مسیر طی شده توسط بسته‌ها از مبدا به مقصد استفاده میشوند. از این ابزارها برای تشخیص مشکلات شبکه و عیب یابی مشکلات اتصال استفاده میشود.

traceroute در اکثر سیستم عامل‌های مبتنی بر یونیکس از جمله لینوکس در دسترس است و tracepath ابزاری معادل در سیستم های لینوکس است. tracert نیز ابزاری معادل در ویندوز است. در قسمت زیر مثالی از هر دو سیستم عامل آورده‌ایم.

```
$ traceroute www.google.com
```

```
traceroute to www.google.com (216.58.204.174), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  1.755 ms  1.732 ms  1.636 ms
 2  10.0.0.1 (10.0.0.1)  5.155 ms  4.968 ms  5.406 ms
 3  * * *
 4  216.239.48.10 (216.239.48.10)  17.925 ms  19.688 ms  19.854 ms
 5  * * *
 6  209.85.244.121 (209.85.244.121)  22.851 ms  22.939 ms  23.113 ms
 7  72.14.237.45 (72.14.237.45)  26.307 ms  26.501 ms  26.728 ms
 8  216.58.204.174 (216.58.204.174)  26.955 ms  27.045 ms  27.122 ms
```

```
C:\> tracert www.google.com
```

```
Tracing route to www.google.com [216.58.204.174]
over a maximum of 30 hops:
 0  <1 ms  <1 ms  <1 ms  router.local [192.168.1.1]
 1  16 ms  17 ms  16 ms  10.0.0.1
 2  *      *      *      Request timed out.
 3  21 ms  20 ms  20 ms  216.239.48.10
 4  *      *      *      Request timed out.
 5  22 ms  21 ms  22 ms  209.85.244.121
 6  25 ms  26 ms  25 ms  72.14.237.45
 7  26 ms  27 ms  25 ms  216.58.204.174
 8  26 ms  27 ms  26 ms  www.google.com [216.58.204.174]

Trace complete.
```

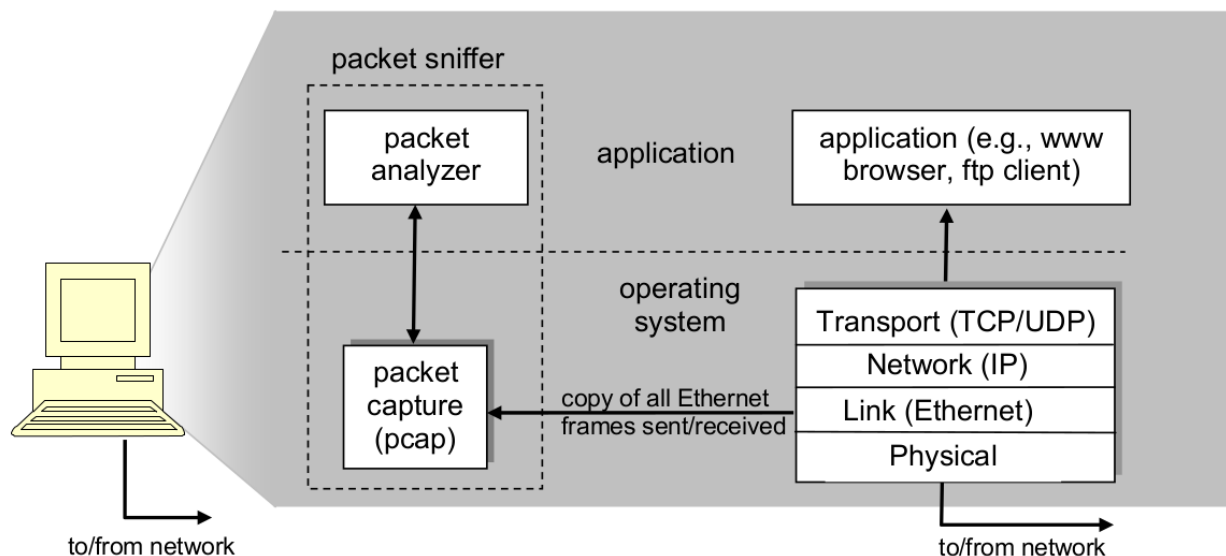
• ping

دستور ping یک ابزار تشخیص (diagnostic) شبکه است که برای در دسترس بودن یک دستگاه شبکه و اندازه‌گیری زمان رفت و برگشت بسته‌ها برای ارسال آن‌ها از دستگاه مبدأ به دستگاه هدف و برگشت آن‌ها استفاده می‌شود. دستور ping با ارسال بسته‌های echo request پروتکل ICMP به دستگاه مورد نظر و منتظر پاسخ در قالب بسته‌های ICMP echo reply کار می‌کند.

دستور ping نتایجی من جمله تعداد بسته‌های دریافتی و زمان رفت و برگشت (RTT) را برای هر بسته نمایش می‌دهد. نتایج ping می‌تواند اطلاعاتی در مورد عملکرد شبکه ارائه دهد و به شناسایی علت مشکلات شبکه کمک کند.

وایرشارک (wireshark)

نرم‌افزار وایرشارک (wireshark) یک ابزار برای مشاهده و تحلیل بسته‌های دریافتی و یا ارسالی از هر یک از رابط‌های شبکه ماشین است که بر روی آن نصب می‌شود. به اینگونه ابزارها به اصطلاح packet sniffer می‌گویند (sniff به معنای بو کشیدن است و از آنجایی که در وایرشارک یک کپی از هر بسته ارسالی و یا دریافتی برای نمایش و تحلیل به وایرشارک ارسال می‌شود به آن «بو کننده بسته» و یا همان packet sniffer می‌گویند). تصویر زیر مبنای عمل کرد وایرشارک را نشان می‌دهد.



نحوه کار wireshark

همانطور که در تصویر بالا مشخص است، یک کپی از تمام بسته‌هایی که از رابط‌های مختلف شبکه، که به ماشین متصل هستند می‌توانند برای مازول packet capture وایرشارک ارسال شوند و در ادامه توسط مازول packet analyzer نمایش و تحلیل شوند.

پس از دریافت (توسط لینک <http://www.wireshark.org/download.html>)، نصب و اجرای وایرشارک اولین صفحه‌ای که در این نرم‌افزار دیده می‌شود به کاربر اجازه می‌دهد که یکی از رابط‌های شبکه (interface) که قصد مشاهده بسته‌های دریافتی و یا ارسالی از آن را دارد انتخاب کند. پس از انتخاب یک رابط شبکه صفحه اصلی نرم‌افزار وایرشارک باز می‌شود که در آن تمام بسته‌هایی که از آن رابط دریافت و یا ارسال می‌شوند نمایش داده می‌شود. تصویر زیر نمای کلی این صفحه و قسمت‌های مختلف آن را نشان می‌دهد.

The screenshot displays the Wireshark network protocol analyzer interface. It is divided into several main sections:

- Command menus:** Located at the top, including File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help.
- display filter:** A bar below the menus with the text "Apply a display filter ... <Ctrl-F>".
- listing of captured packets:** A table showing a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Length/Info. The table lists various protocols including ARP, TCP, and TLSv1.2.
- details of selected packet header:** A section below the packet list showing the hierarchical structure of the selected packet (Frame 327). It includes details for Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Transport Layer Security.
- Packet Content in hexadecimal and ASCII:** A section at the bottom showing the raw data of the selected packet in hexadecimal and ASCII format.

At the bottom of the window, the status bar indicates "Packets: 338 - Displayed: 338 (100.0%) - Dropped: 0 (0.0%) Profile: Default".

بخش‌های مختلف برنامه وایرشارک

این صفحه شامل ۵ قسمت است.

قسمت اول:

در قسمت بالایی منوهای هستند که مهمترین آن‌ها منوهای File و Capture هستند. منوی فایل به شما اجازه ذخیره بسته‌های اخذ شده توسط وایرشارک و یا باز کردن فایل‌هایی که شامل بسته‌های از قبل اخذ شده هستند را می‌دهد (فایل‌ها به فرمت pcap ذخیره می‌شوند). منوی Capture اجازه شروع و یا پایان اخذ بسته‌های دریافتی و یا ارسالی از روی رابط شبکه را می‌دهد.

قسمت دوم:

در قسمت فیلتر می‌توان مشخص کرد که از بین بسته‌ها کدامیک در قسمت سوم (لیست بسته‌ها) نمایش داده شود. مثلاً با نوشتن tcp در قسمت فیلتر، تنها بسته‌های tcp لیست می‌شوند. برای مثال اگر در این قسمت عبارت "ip.addr == your_IP_address" را وارد نمایید تنها بسته‌هایی که یا فرستنده و یا گیرنده‌ی آن‌ها ip ماشین شما است را نمایش خواهد داد.

قسمت سوم:

در قسمت لیست بسته‌ها، بسته‌های دریافتی و ارسالی از رابط شبکه پس از فیلتر شدن توسط مشخصاتی که در نوار فیلتر بیان شده‌اند نمایش داده می‌شود. اطلاعاتی مانند زمان دریافت و یا ارسال، آدرس IP مبدا و مقصد و ... هم در مورد هر بسته نمایش داده می‌شود و اطلاعات جزئی‌تر در مورد هر بسته با انتخاب آن در قسمت چهارم نمایش داده می‌شود (شاید برای شما سوال پیش بیاید که مگر ممکن است بسته‌ای که فرستنده یا گیرنده‌ی آن ماشین ما نباشد، به دست کارت شبکه‌ی ما برسد؟ پاسخ آن است که بله ممکن است؛ در این باره تحقیق بفرمایید).

قسمت چهارم:

در قسمت جزئیات بسته، محتوای هر بسته‌ای که در لیست بسته‌ها (قسمت سوم) انتخاب شود نمایش داده می‌شود. محتوای سرآیند بسته‌ها به صورت پروتکل به پروتکل بسته‌بندی می‌شوند و با انتخاب هر پروتکل، اطلاعات آن نمایش داده می‌شود و در عین نمایش بیتی فیلدهای مختلف آن پروتکل، نام آن فیلد برای راحتی کار کاربران انسانی توسط وایرشارک نمایش داده می‌شود.

قسمت پنجم:

نهایتاً در پایین صفحه تمام محتوای بسته به دو صورت هگزادسیمال (hexadecimal) و اسکی (Ascii) نمایش داده می‌شود.

بهترین راه برای آموختن هر نرم‌افزار کار کردن با آن است :) بنابراین هر چه زودتر وایرشارک را بر روی ماشین خود نصب کنید و با سرکشی به قسمت‌های مختلف با قابلیت‌های مختلف وایرشارک آشنا شوید. در تجربه شیرین آشنایی خود با وایرشارک می‌توانید از مطالبی که در مستندات آنلاین وایرشارک که در لینک زیر موجود است نیز بهره ببرید:

[/https://www.wireshark.org/docs](https://www.wireshark.org/docs)

در پایان شایان ذکر است که معادل ترمینالی وایرشارک تحت عنوان tcpdump و tshark نیز در سیستم‌های لینوکس در دسترس هستند که می‌توانید در مورد آنها نیز تحقیق نمایید.

بهترین باشید :)