۱. **لایه های OSI را نام برده و هر یک را به اختصار توضیح فرمایید؟**

لایه فیزیکی:Physical layer

اولین لایه مدل OSI بوده و در پایین ترین سطح این مدل است. در این لایه نحوه اتصال دو ایستگاه به یکدیگر از طریق کابل و توپولوژی های شبکه و سرعت آنها توضیح داده می شود.

لایه پیوند داده ها:Data link layer

دومین لایه از مدل OSIمی باشد که وظیفه این لایه آن است که با استفاده از مکانیزم ها کشف و کنترل خطا، داده را روی یک کانال بدلیل وجود نویز، بدون خطا به مقصد برساند.

لایه شبکه:Network layer

سومین لایه از مدل OSIمی باشد که وظیفه مسیریابی و یافتن آدرس های مبدا و مقصد برای انتقال داده را به عهده دارد.

پیچیده ترین لایه مدل OSI است چون عمل مسیریابی در آن انجام می شود.

لایه انتقال:Transport layer

چهارمین لایه از مدل OSIمی باشد که همانطور که از نامش پیداست وظیفه آن انتقال اطلاعات است.

این لایه داده را از لایه بالاتر یعنی session گرفته و به قطعاتی با اندازه مناسب تقسیم کرده، اطلاعات مبدا و مقصد از قبیل شماره پورت به پاکت اضافه می کند و به لایه شبکه تحویل می دهد.

لایه نشست:Session layer

پنجمین لایه از مدل OSIمی باشد در این لایه مانند لایه انتقال ارسال اطلاعات است اما خدمات پیشرفته ای نیز ارائه می کند در این لایه ارتباط بین دو ایستگاه با یک توافق آغاز می شود (Authentication , Authorization , login) و ادامه می یابد تا طی روالی هماهنگ پایان یابد.

لایه نشست:Presentation layer

ششمین لایه از مدل OSIمی باشد در این لایه داده ها به روش استاندارد کد گذاری و قالب بندی می شوند.

برای اینکه کامپیوترهای با کدها و قالب بندی مختلف بتوانند داده ارسال کنند باید با استفاده از یک کدگذاری و قالب بندی استاندارد تبادل اطلاعات نمایند که برای سیستم عامل های مختلف قابل فهم باشد.

لایه نشست:Application layer

هفتمین لایه از مدل OSIو همچنین بزرگترین لایه از این مدل می باشد. این لایه نقطه ورودی است برای دستیابی به مدل OSIاست. تمام برنامه های شبکه در این لایه قرار دارند و ارتباط بین برنامه های روی شبکه در این لایه فراهم می گردد.

در این لایه خدمات سودمندی از قبیل ارسال فایل، کنترل یک کامپیوتر از راه دور و.... ارائه می گردد.

۲. **وظایف لایه پیوند داده‌ها (Data Link) چیست؟ توضیح دهید که این لایه چگونه خطاها را مدیریت می‌کند؟**

لایه پیوند داده ها:Data link layer

دومین لایه از مدل OSIمی باشد که وظیفه این لایه آن است که با استفاده از مکانیزم ها کشف و کنترل خطا، داده را روی یک کانال بدلیل وجود نویز، بدون خطا به مقصد برساند.

در زمان انتقال اطلاعات ممکن است فریم خراب یا گم شود این وظیفه لایه پیوند داده هاست که در مقصد فریم را بررسی و خطایابی نماید

وظیفه دیگر این لایه اطلاعات ارسالی از لایه بالاتر را به واحد های استاندارد و مجاز تبدیل کرده و افزودن فیلد های اطلاعاتی خاص (مثل آدرس مبدا، آدرس مقصد، کدهای کشف خطا و ...) یک فریم را تشکیل داده و برای لایه بعدی آماده می کند.

این لایه خود از دو زیر لایه به نام های LLCوMAC تشکیل شده است . هر کدام از این زیر لایه ها وظایفی را به عهده دارند

زیر لایهLLC

فریم بندی و شماره گذاری فریم ها و ارسال

دریافت فریم ها در کامپیوتر مقصد و بازسازی آن

فرستادن Acknowledge به فرستنده در صورت دریافت صحیح اطلاعات برای هر فریم

در صورت عدم ارسال Acknowledge از سوی گیرنده برای یک فریم آن فریم دوباره توسط فرستنده ارسال خواهد شد

زیر لایهMAC

این زیر لایه کنترل دسترسی رسانه نحوه و روش دسترسی یک ایستگاه به شبکه را بیان می دارد که دو نمونه از آن عبارتند از:

Token Pasing

CSMA/CD(carrier sense multiple access / collision detection)

روشToken Pasing

جلوگیر از تصادم یاcollision

حرکت یک بسته خالی از اطلاعات درون شبکه(Token)

کامپیوتر برای ارسال اطلاعات منتظر Token می ماند

اقدام به ارسال اطلاعات پس از رسیدن Token به کامپیوتر

باقی ماندن Token تا پایان ارسال کامل اطلاعات نزد کامپیوتر

عدم ارسال اطلاعات توسط کامپیوتر های دیگر

ارسال Acknowledge پس از پایان ارسال اطلاعات توسط کامپیوتر دریافت کننده به کامپیوتر مبدا

ایجاد یک Token توسط کامپیوتر مبدا و آزاد کردن آن در شبکه

روشCSMA/CD

در این روش اگر دو کامپیوتر همزمان اقدام به ارسال اطلاعات کنند تصادم رخ می دهد برای جلوگیری از این تصادم هر دو کامپیوتر ارسال را رها کرده و مدت زمانی به صورت تصادفی صبر کرده و سپس مجددا اقدام به ارسال اطلاعات می کنند.

۳. **در لایه فیزیکی(Physical) ، کدام فناوری‌ها و ابزارها برای انتقال داده استفاده می‌شوند؟ مثال بزنید.**

لایه انتقال:Transport layer

چهارمین لایه از مدل OSIمی باشد که همانطور که از نامش پیداست وظیفه آن انتقال اطلاعات است.

این لایه داده را از لایه بالاتر یعنی session گرفته و به قطعاتی با اندازه مناسب تقسیم کرده، اطلاعات مبدا و مقصد از قبیل شماره پورت به پاکت اضافه می کند و به لایه شبکه تحویل می دهد.

لایه انتقال:Transport layer

چهارمین لایه از مدل OSIمی باشد که همانطور که از نامش پیداست وظیفه آن انتقال اطلاعات است.

این لایه داده را از لایه بالاتر یعنی session گرفته و به قطعاتی با اندازه مناسب تقسیم کرده، اطلاعات مبدا و مقصد از قبیل شماره پورت به پاکت اضافه می کند و به لایه شبکه تحویل می دهد.

٤. **در مقایسه بین لایه انتقال (Transport) و لایه شبکه(Network) ، هرکدام چه مسئولیت‌هایی دارند؟ با ذکر مثال توضیح دهید.**

لایه شبکه:Network layer

سومین لایه از مدل OSIمی باشد که وظیفه مسیریابی و یافتن آدرس های مبدا و مقصد برای انتقال داده را به عهده دارد.

پیچیده ترین لایه مدل OSI است چون عمل مسیریابی در آن انجام می شود.

این لایه ترافیک شبکه را نیز کنترل کرده و با انتخاب مسیر جدید برای داده از بروز ترافیک جلوگیری می کند.

پروتکل IP که از مهمترین پروتکل های شبکه است در این لایه قرار دارد که وظیفه آن آدرس دهی می باشد.

لایه فیزیکی:Physical layer

اولین لایه مدل OSI بوده و در پایین ترین سطح این مدل است. در این لایه نحوه اتصال دو ایستگاه به یکدیگر از طریق کابل و توپولوژی های شبکه و سرعت آنها توضیح داده می شود.

این لایه مسئول تبدیل اطلاعات از بیت به سیگنال های الکتریکی می باشد. در واقع اگر بخواهیم موقعیت این لایه را نشان دهیم لبه کارت شبکه ما یعنی مابین کارت شبکه و رسانه انتقال (کابل و...) همان لایه فیزیکی می شود.

پارامترهایی که باید در این لایه مورد نظر باشند عبارتند از:

ماهیت فیزیکی خط انتقال(مسی، فیبر نوری، مایکروبو و(....

چگونگی نمایش بیت ها در قالب سیگنال متناسب با کانال

ظرفیت کانال فیزیکی و نرخ ارسال(bit rate)

مسائل مکانیکی و الکتریکی مانند نوع کابل، باند فرکانسی و نوع رابط کابل (کانکتور(

۵. **تفاوت‌های اصلی پروتکل‌های TCP و UDP را توضیح دهید و بگویید کدام یک برای پخش ویدئو مناسب‌تر است و چرا؟**

اتصال گراconnection oriented : در این پروتکل ابتدا ارتباط برقرار می شود بعد داده ارسال می گردد(TCP)

بدون اتصال connection less : در این پروتکل نیازی به برقراری ارتباط قبل از ارسال داده نیست(UDP)

TCP(Transmission Control Protocol)

این پروتکل یک پروتکل اتصال گرا (Connection Oriented) می باشد بدین معنی که ابتدا ارتباط برقرار شده و سپس داده ارسال می شود و این پروتکل نیز به بسته اطلاعاتی تحت عنوان هدر (Header) اضافه می کند.

در این پروتکل ایجاد یک ارتباط TCP معروف به دست تکانی سه مرحله ای (three way handshake) می باشد.

در این پروتکل صحت دریافت داده ها مشخص می گردد و دارای امنیت بیشتری نسبت به UDP می باشد.

UDP(User Datagram Protocol)

این پروتکل یک پروتکل بدون اتصال (connection less) می باشد یعنی برای ارسال اطلاعات ابتدا ارتباط برقرار نمی شود سپس اطلاعات ارسال شود. از این پروتکل زمانی استفاده می شود که صحت داده ها در سمت دریافت کننده مهم نبوده و سرعت از اهمیت بیشتری برخوردار باشد

امینت در این پروتکل کمتر از TCP می باشد ولی سرعت آن بیشتر است.

۶. **پروتکل‌های ICMP و ARP چه تفاوت‌هایی دارند و چگونه در شبکه‌ها استفاده می‌شوند؟**

پروتکل ICMP (Internet Control Message Protocol)

این پروتکل در کنار پروتکل IP برای بررسی انواع خطا و ارسال پیام برای مبدا بسته در هنگام بروز اشکالات ناخواسته استفاده می شود. در واقع ICMP یک سیستم گزارش خطاست

چون ICMP خود درون یک بسته IP جاسازی می شود بنابراین فیلد پروتکل در سرآیند بسته IP باید باشماره مشخصه پروتکل ICMP تنظیم شود.

کار دیگر ICMP حمل درخواست های گوناگون برای دریافت اطلاعات به سیستم های دیگر و برگرداندن جواب های حاوی آن اطلاعات است PING .هم یک ابزار کمکی در این پروتکل است که با زدن این دستور به همراه IP مقصد در محیط CMD تعداد ۴ پاکت ارسال می کند و مشخص کننده برقراری ارتباط بین دستگاه مبدا و مقصد می باشد.

ARP (Address Resolution Protocol)

کار پروتکل ARP تبدیل آدرس IP به MAC بوده و با ارسال بسته های Broadcast در سطح شبکه، آدرس های MAC ماشین های داخل شبکه را شناسایی می کند. هنگامی که یک ماشین نیاز به برقراری ارتباط با دیگران داشته باشد، به جدول ARPمراجعه می کند. اگر آدرس MAC در این جدول پیدا نشد، پروتکل ARP یک بسته Broadcast را برای شناسایی آن درون شبکه پخش می کند.

در واقع در جدول ARP برای هر IP آدرس MAC آن مشخص شده است.

۷. **DNSچگونه کار می‌کند و چرا استفاده از آن برای کاربران ضروری است؟**

DNS(domain name system)

سیستم های TCP/IP از این پروتکل برای تحلیل نام میزبانها به آدرس IP مورد نیاز برای تبادل اطلاعات استفاده می کنند. پورت مربوط به آن ۵۳ است.

۸. **توضیح دهید که پروتکل HTTP چگونه با HTTPS تفاوت دارد و چه مکانیزم‌هایی برای امنیت بیشتر در HTTPS استفاده می‌شود؟**

HTTP(hyper text transfer protocol)

پروتکلی است که سرویس دهنده و سرویس گیرنده وب از آن برای تبادل پیغام ها و همچنین دیدن صفحات وب در سمت سرویس گیرنده استفاده می کنند. زمانی که شما یک صفحه وب را مشاهده می کنید، در واقع از این پروتکل استفاده کرده اید. پورت مربوط به آن ۸۰ است.

HTTPS

یک پروتکل مطمئن برای تبادل اطلاعات در وب می باشد که S پایان آن نشان دهنده SSL بوده که برای انجام سرویس های احراز هویت و رمزنگاری استفاده می شود. پورت مربوط به آن ۴۴۳ است.

۹. **پروتکل DHCP چیست و چگونه به طور خودکار آدرس IP تخصیص می‌دهد؟ مراحل را توضیح دهید.**

DHCP(dynamic host configuration protocol)

از این پروتکل برای دادن IP به صورت اتوماتیک استفاده می شود. پورت مربوط به آن ۶۸ و ۶۷ است.

DHCP(dynamic host configuration protocol)

از این پروتکل برای دادن IP به صورت اتوماتیک استفاده می شود.

هنگامی که سرور DHCP بالا بوده و به سوییچ متصل است و کاربر هم به سوییچ متصل شده و حالت تنظیم IP خود را در حالت اتوماتیک قرار دهد، یک بسته Broadcast توسط کاربر در شبکه با عنوان DHCP Discover پخش می شود. این بسته بدین معنی است که کاربر به دنبال سرور DHCP می گردد. هنگامی که این بسته به سرور DHCP رسید، سرور آن را تحویل گرفته و یک بسته Unicast به عنوان DHCP Offer به سمت کاربر ارسال می کند. این بسته بدین معنی است که سرور DHCP خود را به کاربر معرفی می کند. کاربر پس از دریافت این بسته، یک بسته Broadcast به عنوان DHCP Requestرا در سطح شبکه پخش خواهد کرد که بیانگر آمادگی برای گرفتن IP اتوماتیک است. در این زمان سرور DHCP پس از دریافت بسته DHCP Request یک بسته Unicast با عنوان DHCP Ack را به سمت کاربر ارسال می کند که این بسته حاوی اطلاعات مربوط به IP اتوماتیک برای کاربر است.

۱۰. **تفاوت آدرس‌های عمومی (Public) و خصوصی (Private) در شبکه چیست و در چه شرایطی از هرکدام استفاده می‌شود؟**

Public & private IP

Public IPبه آدرس IP گفته می شود که جنبه عمومی داشته و در اینترنت معتبر می باشد.

Private IP به آدرس IP گفته می شود که در شبکه های محلی مورد استفاده قرار می گیرد.

۱۱. **تفاوت بین پورت‌های Well-Known و Dynamic را توضیح دهید. هر کدام در چه شرایطی استفاده می‌شوند؟**

پورت‌های شناخته شده

پورت‌های شناخته شده از بازه ۰ تا ۱۰۲۳ هستند این پورت‌ها برای خدمات عمومی و اختصاصی استفاده می‌شوند از پروتکل‌ها و خدماتی مانند HTTP (پورت ۸۰)، FTP (پورت ۲۱)، DNS (پورت ۵۳)، SSH (پورت ۲۲) و غیره استفاده می‌شود.....

پورت‌های ثبت شده

پورت های ثبت شده از بازه ۱۰۲۴ تا ۴۹۱۵۱ هستند این پورت ها توسط برنامه ها یا خدماتی که خیلی رایج نیستند استفاده می شوند اما توسط آنها برنامه ها یا خدماتی که نیاز به پورت خاص خود دارند استفاده می شود سازمان ها می توانند از IANA (مرکز ثبت شماره اینترنت) درخواست هر شماره پورت خاصی در این بازه را بکنند.

پورت‌های دینامیک

پورت‌های داینامیک از بازه ۴۹۱۵۲ تا ۶۵۵۳۵ هستند این پورت‌ها همچنین به عنوان پورتِ موقت یا خصوصی شناخته می شوند از این پورت ها برای ارتباطاتی که موقتی یا کوتاه مدت هستند استفاده می شود این پورت ها ثبت شده یا اختصاصی نیستند و میتوانند توسط هر فرایند استفاده شوند.

۱۲. **چگونه فایروال می‌تواند بر اساس شماره پورت‌ها امنیت شبکه را تأمین کند؟ مثال بزنید.**

نگاهی دقیق بر نحوه کار فایروال

نحوه کار فایروال مانند یک سرباز وظیفه‌شناس است و مرزی محکم بین شبکه داخلی شما و دنیای اینترنت ایجاد می‌کند. در پاسخ به اینکه وظیفه فایروال چیست، می‌توان گفت وظیفه اصلی آن، بازرسی دقیق تمام بسته‌های اطلاعاتی است که قصد ورود یا خروج از شبکه شما را دارند. بسته‌های اطلاعاتی، مانند قطعات کوچکی از یک پازل هستند که برای انتقال اطلاعات در اینترنت استفاده می‌شوند.

فایروال فقط به ترافیکی خوش‌آمد می‌گوید که از قبل ورود آن هماهنگ شده باشد. **به‌عبارتی عملکرد فایروال به‌گونه‌ای است که پس از بررسی دقیق این بسته‌ها، با کمک مجموعه‌ای از قوانین از پیش تنظیم‌شده، بسته‌های بی‌خطر را از مخرب تشخیص می‌دهد.** این قوانین مانند دستورالعمل‌های یک مرزبان هوشیار، فایروال را در تصمیم‌گیری‌هایش راهنمایی می‌کنند.

عملکرد فایروال بر اساس چند نکته مهم در داده‌ها تعیین می‌شوند. مانند اینکه ترافیک از کجا آمده است؟ به کجا می‌رود و چه محتوایی دارد. برای مثال، تصویر زیر نشان می‌دهد چطور فایروال اجازه ورود به ترافیک مجاز را در شبکه خصوصی کاربر می‌دهد:

علاوه‌براین، فایروال امکان بازسازی بسته‌های اطلاعاتی را هم دارد. یعنی می‌تواند آن‌ها را براساس قوانین خود تغییر دهد و به پروتکل‌های شبکه بگوید هر بسته را به کجا ارسال کنند. این ویژگی به فایروال اجازه می‌دهد ترافیک شبکه را به شکل هوشمندانه‌تری مدیریت کند و امنیت شبکه را بیش از پیش ارتقا دهد.

در پاسخ به این سوال که فایروال جلوی کدام حملات را می‌گیرد، باید گفت فایروال‌ها با استفاده از الگوریتم‌های مختلف، ترافیک ورودی و خروجی را بررسی می‌کنند و اگر ترافیک مطابق با قوانین تعریف‌شده در فایروال نباشد، آن را مسدود می‌کنند. این قوانین براساس آدرس IP، پورت، پروتکل، نوع ترافیک و سایر عوامل تعریف می‌شوند و جلوی حملاتی مانند حملات DoS و DDoS را می‌گیرند.

۱۳. **پورت ۲۲ به چه پروتکلی تعلق دارد و کاربرد آن چیست؟ توضیح دهید چگونه می‌توان از آن برای مدیریت سرورها استفاده کرد؟**

SSH چیست؟ یک توضیح مختصر و مفید

SSH (Secure Shell) پروتکل استانداردی برای ارتباط بین دو کامپیوتر در شبکه‌ی اینترنت است و با توجه به اینکه تمامی اطلاعات در این مسیر به‌صورت رمزنگاری شده ردوبدل می‌شود، این پروتکل به‌عنوان یکی از ایمن‌ترین سیستم‌های ارتباطی در شبکه‌ی اینترنت محسوب می شود. همین موضوع باعث شده است SSH به یکی از مهم‌ترین و ایمن‌ترین پروتکل‌ها برای ارتباط دو کامپیوتر در شبکه‌ی اینترنت از سال ۱۹۹۵ تا کنون تبدیل شود.

۴. پورت SSH چیست؟

پروتکل SSH از پورت شماره ۲۲ استفاده می‌کند.

۵. کلید SSH چیست؟

کلید SSH اعتبارنامه‌ای برای دسترسی پروتکل شبکه (Secure Shell) SSH است. این پروتکل ایمن از احراز هویت رمزگذاری‌شده برای ارتباط از راه دور و بین ماشین‌ها در شبکه باز ناامن بهره می‌برد. SSH به‌منظور انتقال فایل از راه دور و مدیریت شبکه و دسترسی از راه دور به سیستم‌عامل استفاده می‌شود.

۶. OpenSSH چه کاربردهایی دارد؟

OpenSSH یک دیمون سرور را فراهم می‌کند و از ابزارهای کلاینت برای تسهیل عملیات کنترل از راه دور ایمن و رمزگذاری‌شده و انتقال فایل استفاده می‌کند و به‌طور مؤثر جایگزین ابزارهای قدیمی می‌شود.

۱۵. **مزایای افزونگی (Redundancy) در طراحی شبکه چیست؟ با ذکر مثال توضیح دهید.**

افزونگی یا Redundancy چیست؟

افزونگی مفهومی است که در بسیاری از حوزه‌ها کاربرد دارد، اما در دنیای فناوری اطلاعات و شبکه‌ها کاربرد آن بیشتر و خاص‌تر است. در این حوزه، Redundancy به معنای ایجاد نسخه های اضافی از اجزا یا سیستم‌ها است تا در صورت بروز مشکلات یا خرابی‌ها، عملکرد سیستم بدون وقفه ادامه یابد.

این فرایند باعث می‌شود که سیستم‌ها در برابر اختلالات مختلف مقاوم‌تر شوند و از آسیب‌های احتمالی جلوگیری کنند. به عبارت دیگر، Redundancy به معنای اطمینان از تداوم کار بدون هیچ‌گونه اختلال و دسترسی به خدمات است.

اگر بخواهیم فقط در یک مورد بگوییم که مزیت Redundancy در شبکه چیست، باید به افزایش امنیت و پایداری سیستم‌های قرار گرفته در شبکه اشاره کنیم. در سیستم‌های ریداندنت، چندین نسخه از هر عنصر حیاتی یا بخش حساس وجود دارد که این موضوع به کاهش ریسک خرابی و از دست دادن اطلاعات کمک می‌کند. به‌علاوه، افزونگی نه تنها به حفظ عملکرد و امنیت کمک می‌کند، بلکه بهبود سرعت و کارایی سیستم‌ها را نیز به همراه دارد.

۱۶. چگونه می‌توان یک شبکه را به گونه‌ای طراحی کرد که از Single Point of Failure جلوگیری کند؟

تعریف نقطه تکی شکست یا خرابی (SPOF)

نقطه تکی شکست یک ریسک احتمالی محسوب می‌شود که توسط خطایی در طراحی، پیاده‌سازی، یا تنظیم یک مدار یا سیستم به وجود آمده است. به عبارتی دیگر، SPOF یک خطا یا اختلال در عملکرد بوده که می‌تواند به از کار افتادن یک سیستم یا شبکه منجر شود. وجود نقطه تکی خرابی در یک دیتاسنتر یا هر نوع محیط آی‌تی محور دیگر، با توجه موقعیت نقطه و بخش‌های وابسته به آن، ممکن است در ظرفیت کاری یا حتی فعالیت کل دیتاسنتر اختلال ایجاد نماید.

یک سرور متمرکز، بهترین مثال از نقطه تکی شکست

یک دیتاسنتر را در نظر بگیرید که در آن یک سرور به تنهایی یک اپلیکیشن را اجرا می‌کند. در این حالت، سخت افزار این سرور یک نقطه تکی شکست برای دسترسی به اپلیکیشن مذکور است؛ یعنی اگر سخت افزار سرور با مشکل مواجه شود، اپلیکیشن متوقف یا از دسترس خارج خواهد شد. در چنین حالتی، کاربران امکان استفاده از اپلیکیشن را نخواهند داشت و احتمال از دست رفتن داده‌های مهم هم وجود دارد.

تنها سوئیچ شبکه، نمونه‌ای دیگر از نقطه تکی شکست

در یک نمونه دیگر از SPOF، تعدادی از سرورها صرفا از طریق یک سوئیچ شبکه (Network Switch) به یکدیگر متصل شده‌اند. در نتیجه اگر مشکلی برای سوئیچ به وجود بیاید یا حتی اگر از منبع تغذیه خود جدا شود، سرورهای متصل به آن هم از سایر سرورهای شبکه جدا خواهند شد. در این حالت، سوئیچ شبکه یک نقطه تکی شکست است و از کار افتادن آن می‌تواند دسترسی به سرورهای زیادی مختل کند.

برای مقابله با چنین سناریویی، سوئیچ‌ها و ارتباطات اضافی مورد استفاده قرار می‌گیرند تا سرورهای یک شبکه راه‌های ارتباطی جایگزین داشته باشند و اگر مشکلی برای سوئیچ اصلی پیش آمد، فعالیت‌شان بدون اختلال ادامه پیدا کند.

جلوگیری از به وجود آمدن سینگل پوینت آف فیلیر

سازنده هر دیتاسنتر وظیفه شناسایی و برطرف کردن هر نقطه تکی شکست را بر عهده دارد. با این حال، بر طرف کردن SPOF هم هزینه‌های قابل توجهی به همراه دارد و قیمت سرورها، کابل‌ها و سوئیچ‌های اضافی می‌تواند به رقم بالایی برسد. بنابراین سازنده باید اهمیت هر بخش و هزینه مورد نیاز برای برطرف کردن نقاط تکی خرابی آن را مورد در نظر بگیرد و سپس مواردی که ارزش هزینه کردن را دارند، برطرف نماید.

۱۷. **تفاوت بین Redundant Hardware و Redundant Links را توضیح دهید و مثال بزنید.**

میزبانی Redundant چیست و چرا سرور شما به آن نیاز دارد؟

سرورهای میزبانی Redundant با ارائه نسخه‌های موازی و تجهیزات اضافی، تضمین می‌کنند که سایت یا اپلیکیشن شما در صورت بروز هرگونه اختلال، همچنان در دسترس باقی بماند. با این نوع میزبانی، حتی اگر یکی از سرورها یا بخش‌های سخت‌افزاری دچار مشکل شود، بلافاصله نسخه های اضافی فعال می شوند و از وقفه در دسترسی به خدمات جلوگیری می‌کنند.

با انتخاب میزبانی Redundant، چه به‌صورت سرور اضافی و چه به‌صورت سرور تکراری (Replicate Server) می‌توانید از پایداری و تداوم عملکرد سرویس‌های خود اطمینان داشته باشید. این موضوع به‌خصوص برای کسب‌وکارهایی که به‌صورت آنلاین فعالیت دارند و حتی کوتاه‌ترین قطعی می‌تواند منجر به از دست رفتن مشتری و درآمد شود، بسیار حیاتی است. به همین دلیل، استفاده از این نوع میزبانی موجب جلب رضایت مشتری و تقویت اعتماد آن‌ها به سرویس شما می‌شود.

علاوه بر این، استفاده از میزبانی Redundant می‌تواند به بهینه‌سازی عملکرد سرور نیز کمک کند. با توزیع متوازن بار بین سرورهای متعدد، سرورهای شما می‌توانند درخواست‌های بیشتری را بدون افت سرعت پاسخ دهند. به این ترتیب، کاربران تجربه سریع‌تر و بهتری از وب‌سایت یا سرویس آنلاین شما خواهند داشت که در بلندمدت منجر به رشد و توسعه کسب‌وکار شما می‌شود.

۱۸. **توضیح دهید که چگونه استک کردن سوئیچ‌ها می‌تواند مدیریت شبکه را ساده‌تر کند.**

استک کردن سوییچ‌ها به شما این امکان را می‌دهد که یک شبکه بزرگ‌تر را به صورت سلسله مراتبی سازماندهی کنید. این کار باعث می‌شود:

- **مقیاس‌پذیری:** به راحتی می‌توانید با افزودن سوییچ‌های بیشتر، ظرفیت شبکه خود را افزایش دهید.
- **مدیریت متمرکز:** با استفاده از پروتکل‌هایی مانند Layer 3، می‌توانید ترافیک بین شبکه‌های مختلف را به طور متمرکز مدیریت کنید.
- **بهبود عملکرد:** با تقسیم شبکه به بخش‌های کوچکتر، می‌توانید ازدحام ترافیک را کاهش دهید و عملکرد کلی شبکه را بهبود بخشید.
- **قابلیت اطمینان:** در صورت خرابی یک سوییچ، بقیه شبکه همچنان به کار خود ادامه می‌دهند.

به طور خلاصه، استک کردن سوییچ‌ها باعث می‌شود مدیریت شبکه پیچیده‌تر به نظر نرسد و به شما انعطاف‌پذیری بیشتری در گسترش و نگهداری آن بدهد.

استک کردن سوییچ‌ها مدیریت شبکه را به چند طریق ساده‌تر می‌کند:

1. **تقسیم‌بندی منطقی شبکه:** می‌توانید شبکه‌تان را به زیرشبکه‌های مجزا تقسیم کنید (مانند VLANها) تا ترافیک را از یکدیگر جدا نگه دارید. این کار امنیت و عملکرد را بهبود می‌بخشد.
2. **مدیریت متمرکز سیاست‌ها:** می‌توانید سیاست‌های امنیتی و QoS را در سطح استک اعمال کنید، نه در هر سوییچ به صورت جداگانه.
3. **تشخیص و عیب‌یابی آسان‌تر:** با تقسیم شبکه، مشکل یابی و ردیابی ترافیک ساده‌تر می‌شود. می‌توانید به سرعت محل مشکل را پیدا کنید.
4. **توزیع بارکاری:** با توزیع ترافیک بین سوییچ‌های مختلف، از بارگذاری بیش از حد یک سوییچ جلوگیری می‌کنید.
5. **اتوماسیون:** بسیاری از سوییچ‌های استک شده قابلیت اتوماسیون را دارند که کارها را ساده تر می‌کند.

به طور کلی، استک کردن سوییچ‌ها به شما کنترل بیشتری بر شبکه می‌دهد و مدیریت آن را کارآمدتر می‌کند.

۱۹. معایب احتمالی استک کردن سوئیچ‌ها چیست و چگونه می‌توان این معایب را کاهش داد؟

معایب احتمالی استک کردن سوییچ‌ها و راهکارهای کاهش آنها:

- **پیچیدگی اولیه:** راه‌اندازی و پیکربندی استک می‌تواند پیچیده باشد.
- **کاهش:** از راهنماها و مستندات سازنده استفاده کنید. از قابلیت‌های خودکار پیکربندی (مانند StackWise) استفاده کنید.
- **نقطه شکست واحد (Single Point of Failure):** اگر یکی از سوییچ‌های استک خراب شود، ممکن است کل استک تحت تاثیر قرار گیرد.
- **کاهش:** از سوییچ‌های دارای قابلیت Redundancy استفاده کنید (مانند StackWise Virtual).
- **هزینه:** سوییچ‌های استک شده معمولاً گران‌تر از سوییچ‌های جداگانه هستند.
- **کاهش:** بر اساس نیازهای واقعی خود، تعداد سوییچ‌ها را به درستی تخمین بزنید.
- **محدودیت در قابلیت‌های خاص:** برخی از قابلیت‌ها ممکن است در استک‌ها محدود باشند.
- **کاهش:** قبل از خرید، بررسی کنید که آیا قابلیت‌های مورد نیاز شما در استک پشتیبانی می‌شوند.
- **مشکلات سازگاری:** مطمئن شوید که سوییچ‌های مختلف از یک سازنده و مدل سازگار هستند.
- **کاهش:** فقط از سوییچ‌های یک سازنده و مدل استفاده کنید.

۲۰. چگونه می‌توان سوئیچ‌های استک‌شده را مدیریت کرد و آیا نیاز به نرم‌افزار خاصی دارند؟

مدیریت سوئیچ‌های استک شده معمولاً از طریق یک رابط واحد انجام می‌شود. این کار معمولاً از طریق یکی از روش‌های زیر امکان‌پذیر است:

- **رابط خط فرمان (CLI):** می‌توانید از طریق CLI به هر یک از سوییچ‌ها در استک دسترسی داشته باشید و آنها را به صورت جداگانه یا به عنوان یک واحد مدیریت کنید.
- **رابط وب:** بسیاری از سوییچ‌های استک شده دارای رابط وب هستند که امکان مدیریت و نظارت بر استک را فراهم می‌کند.
- **رابط مدیریت اختصاصی:** برخی از سازندگان سوییچ، نرم‌افزار اختصاصی برای مدیریت استک‌ها ارائه می‌دهند.

نیاز به نرم‌افزار خاص:

بله، اگرچه می‌توان استک را از طریق CLI یا رابط وب مدیریت کرد، اما استفاده از نرم‌افزار مدیریت اختصاصی می‌تواند کار را بسیار ساده‌تر و کارآمدتر کند. این نرم‌افزارها امکاناتی مانند:

- **پیکربندی متمرکز:** پیکربندی همه سوییچ‌های استک را به صورت همزمان انجام دهید.
- **نظارت بر وضعیت:** وضعیت کلی استک، وضعیت هر سوییچ، و ترافیک را نظارت کنید.
- **تشخیص و عیب‌یابی:** به سرعت مشکلات را شناسایی و عیب‌یابی کنید.
- **مدیریت سیاست‌ها:** سیاست‌های امنیتی و QoS را در سطح استک اعمال کنید.

سازمان‌هایی که شبکه‌های بزرگ و پیچیده‌ای دارند، معمولاً از نرم‌افزارهای مدیریت اختصاصی برای استک‌های خود استفاده می‌کنند.

۲۱. تفاوت بین استک کردن فیزیکی و مجازی چیست و کدام یک برای شبکه‌های بزرگ مناسب‌تر است؟

استک کردن فیزیکی (Physical Stacking):

- در این روش، سوییچ‌ها به صورت فیزیکی به هم متصل می‌شوند (معمولاً با کابل‌های خاص) و یک واحد واحد به نظر می‌رسند.
- منابع (CPU، حافظه، پهنای باند) به اشتراک گذاشته می‌شوند.
- ساده‌تر است، اما انعطاف‌پذیری کمتری دارد.
- **مناسب برای:** شبکه‌های کوچک تا متوسط که نیازمند انعطاف‌پذیری زیادی نیستند.

استک کردن مجازی (Virtual Stacking):

- سوییچ‌ها از طریق یک پروتکل (مانند StackWise Virtual) به هم متصل می‌شوند و منابع خود را به صورت مجازی به اشتراک می‌گذارند.
- سوییچ‌ها به عنوان دستگاه‌های جداگانه عمل می‌کنند، اما به عنوان یک واحد مدیریت می‌شوند.
- انعطاف‌پذیری بیشتری دارد و امکان افزودن یا حذف سوییچ‌ها را بدون نیاز به تغییرات فیزیکی فراهم می‌کند.
- **مناسب برای:** شبکه‌های بزرگ و پیچیده که نیازمند انعطاف‌پذیری بالا و مقیاس‌پذیری هستند.

کدام یک برای شبکه‌های بزرگ مناسب‌تر است؟

استک کردن مجازی (Virtual Stacking) به طور کلی برای شبکه‌های بزرگ مناسب‌تر است. این روش انعطاف‌پذیری و مقیاس‌پذیری بیشتری را ارائه می‌دهد و امکان مدیریت آسان‌تر را فراهم می‌کند. همچنین، در صورت بروز مشکل در یکی از سوییچ‌ها، کل شبکه تحت تأثیر قرار نمی‌گیرد.

۲۲. نحوه عملکرد پروتکل Spanning Tree در جلوگیری از حلقه‌ها در سوئیچ‌های استک‌شده را توضیح دهید.

پروتکل Spanning Tree Protocol (STP) از ایجاد حلقه‌های ترافیکی در شبکه‌های مبتنی بر Ethernet جلوگیری می‌کند، و این موضوع برای سوئیچ‌های استک شده نیز بسیار مهم است. در اینجا نحوه عملکرد STP در این زمینه توضیح داده شده است:

1. **انتخاب Root Bridge:** STP ابتدا یک Root Bridge را در شبکه انتخاب می‌کند. Root Bridge سوئیچی است که نزدیک‌ترین مسیر به یک پلین‌افیس (PDU) دارد.
2. **انتخاب Designated Bridge:** هر سوئیچ غیر-Root Bridge، یک Designated Bridge (DB) در میان خود انتخاب می‌کند. DB سوئیچی است که بهترین مسیر به Root Bridge را دارد.
3. **مسیرهای بلاک شده:** STP مسیرهای پشتیبان (backup paths) را مسدود می‌کند تا از ایجاد حلقه‌ها جلوگیری کند. این کار با بلاک کردن پورت‌های خاصی انجام می‌شود.
4. **پورت‌ها در حالت‌های مختلف:** پورت‌های STP می‌توانند در حالت‌های مختلفی قرار بگیرند:

- **Blocking:** پورت مسدود شده و ترافیکی از آن عبور نمی‌کند.
- **Listening:** پورت در حال دریافت BPDU (Bridge Protocol Data Unit) است.
- **Learning:** پورت در حال یادگیری آدرس‌های MAC است.
- **Forwarding:** پورت ترافیک را عبور می‌دهد.

در سوئیچ‌های استک شده:

- STP در استک، یک Root Bridge واحد را انتخاب می‌کند.
- پورت‌های استک‌شده به عنوان یک واحد در نظر گرفته می‌شوند و در نتیجه، STP اطمینان حاصل می‌کند که هیچ حلقه ترافیکی در کل استک ایجاد نشود.
- STP ترافیک را فقط از طریق یک مسیر واحد در استک ارسال می‌کند، حتی اگر چندین مسیر پشتیبان وجود داشته باشد.

به طور خلاصه، STP با شناسایی و مسدود کردن مسیرهای پشتیبان، از ایجاد حلقه‌های ترافیکی در شبکه‌های استک شده جلوگیری می‌کند و به حفظ پایداری شبکه کمک می‌کند.

۲۳. توضیح دهید که چگونه لایه‌های مختلف OSI با هم کار می‌کنند تا یک ایمیل از فرستنده به گیرنده ارسال شود؟

1. **لایه فیزیکی (Physical Layer):**

- اطلاعات دیجیتال (0 و 1) به سیگنال‌های الکتریکی، نوری یا رادیویی تبدیل می‌شوند.
- این سیگنال‌ها از طریق کابل‌های شبکه (مانند کابل اترنت) یا بی‌سیم منتقل می‌شوند.

2. **لایه پیوند داده (Data Link Layer):**

- داده‌ها به فریم‌هایی تقسیم می‌شوند.
- آدرس‌های MAC (Media Access Control) برای شناسایی دستگاه‌های شبکه استفاده می‌شوند.
- بررسی خطا انجام می‌شود.

3. **لایه شبکه (Network Layer):**

- هر فریم به یک بسته (packet) تبدیل می‌شود.
- آدرس‌های IP (Internet Protocol) برای شناسایی دستگاه‌ها در شبکه استفاده می‌شوند.
- مسیر بهینه برای ارسال بسته تعیین می‌شود (مثلاً از طریق روترها).

4. **لایه انتقال (Transport Layer):**

- بسته به TCP یا UDP، داده‌ها به قطعات کوچکتر تقسیم می‌شوند (TCP) یا به صورت یک بلوک داده ارسال می‌شوند (UDP).
- TCP تضمین تحویل داده‌ها را با استفاده از آدرس‌های پورت و بررسی خطا ارائه می‌دهد.
- UDP سریعتر است اما تضمین تحویل داده‌ها را ندارد.

5. **لایه جلسه (Session Layer):**

- یک اتصال بین فرستنده و گیرنده ایجاد و مدیریت می‌شود.
- اطلاعات مربوط به جلسه تبادل می‌شود.

6. **لایه ارائه (Presentation Layer):**

- داده‌ها رمزگذاری و فشرده می‌شوند.
- فرمت داده‌ها (مانند ASCII یا UTF-8) تنظیم می‌شود.

7. **لایه کاربرد (Application Layer):**

- این لایه با برنامه‌های کاربردی (مانند کلاینت ایمیل) تعامل دارد.
- پروتکل SMTP (Simple Mail Transfer Protocol) برای ارسال ایمیل، و POP3 یا IMAP برای دریافت ایمیل استفاده می‌شوند.
- برنامه ایمیل (مانند Outlook یا Gmail) از این لایه برای ارسال و دریافت ایمیل استفاده می‌کند.

خلاصه فرآیند:

1. شما ایمیل را در برنامه ایمیل خود می‌نویسید (لایه کاربرد).
2. برنامه ایمیل، اطلاعات را به پروتکل SMTP تحویل می‌دهد (لایه کاربرد).
3. SMTP اطلاعات را به TCP تحویل می‌دهد (لایه انتقال).
4. TCP اطلاعات را به IP تحویل می‌دهد (لایه شبکه).
5. IP اطلاعات را به فریم تبدیل می‌کند (لایه پیوند داده).
6. فریم از طریق شبکه منتقل می‌شود (لایه فیزیکی).
7. در سمت گیرنده، فرآیند معکوس انجام می‌شود تا ایمیل به برنامه ایمیل گیرنده تحویل داده شود.

این فرآیند به صورت خودکار و نامرئی برای کاربر انجام می‌شود، اما درک نحوه همکاری لایه‌های مختلف OSI به ما کمک می‌کند تا بفهمیم چگونه ارتباطات در شبکه‌های کامپیوتری انجام می‌شوند.

۲۴. چگونه می‌توان با استفاده از VLAN امنیت شبکه را افزایش داد؟ توضیح دهید.

استفاده از (Virtual Local Area Network) VLAN یکی از روش‌های موثر برای افزایش امنیت شبکه است. VLANها به شما امکان می‌دهند یک شبکه فیزیکی را به چند شبکه منطقی تقسیم کنید. در اینجا نحوه افزایش امنیت شبکه با استفاده از VLANها توضیح داده شده است:

1. جداسازی ترافیک:

- با تقسیم شبکه به VLANها، می‌توانید ترافیک را بین گروه‌های مختلف کاربران یا دستگاه‌ها جدا کنید.
- این کار از دسترسی غیرمجاز به منابع شبکه جلوگیری می‌کند. برای مثال، می‌توانید VLAN جداگانه‌ای برای سرورها، ایستگاه‌های کاری و دستگاه‌های مهمان ایجاد کنید.

2. کنترل دسترسی:

- می‌توانید سیاست‌های امنیتی مختلفی را برای هر VLAN اعمال کنید.
- این کار به شما امکان می‌دهد دسترسی به منابع خاص را محدود کنید و از دسترسی غیرمجاز جلوگیری کنید.

3. کاهش سطح حمله:

- اگر یک VLAN آلوده شود، آسیب به VLANهای دیگر محدود می‌شود.
- این کار به جلوگیری از گسترش بدافزار و حملات سایبری کمک می‌کند.

4. بهبود نظارت و عیب‌یابی:

- با تقسیم شبکه به VLANها، می‌توانید ترافیک را به راحتی نظارت و ردیابی کنید.
- این کار به شما کمک می‌کند تا مشکلات امنیتی را به سرعت شناسایی و رفع کنید.

5. استفاده از Segmentation برای کاربران حساس:

- می‌توانید یک VLAN جداگانه برای کاربران با اطلاعات حساس (مانند حساب‌های بانکی یا اطلاعات پزشکی) ایجاد کنید.
- این کار به محافظت از این اطلاعات در برابر دسترسی غیرمجاز کمک می‌کند.

6. اعمال سیاست های امنیتی متناسب با هرگروه:

- می توانید سیاست های امنیتی متفاوتی را برای هر VLAN اعمال کنید. مثلا یک VLAN می تواند دسترسی به اینترنت را محدود کند و یا فقط به برخی از وب سایت ها اجازه دسترسی دهد.

به طور خلاصه:

VLANها با تقسیم شبکه به شبکه‌های منطقی، به شما امکان می‌دهند کنترل دسترسی را بهبود بخشید، ترافیک را جدا کنید و سطح حمله را کاهش دهید. این کار به افزایش امنیت شبکه و محافظت از اطلاعات حساس کمک می‌کند.

۲۵. **چگونه می‌توان از حملات Man-in-the-Middle در یک شبکه جلوگیری کرد؟ توضیح دهید.**

1. استفاده از رمزنگاری قوی (Encryption)

- **HTTPS** (TLS/SSL): اطمینان حاصل کنید که تمام وب‌سایت‌ها با HTTPS ارتباط برقرار می‌کنند.
- **VPN** (Virtual Private Network): ارتباطات بین کاربر و سرور را از طریق یک لایه رمزنگاری امن انجام می‌دهد.
- **SSH** برای دسترسی امن به دستگاه‌ها.

2. اعمال احراز هویت قوی (Authentication)

- **احراز هویت دو عاملی (FA2)**: برای اطمینان از هویت کاربر.
- **استفاده از گواهی‌های دیجیتال** (Digital Certificates) در سرویس‌های امن.

3. پیکربندی شبکه امن

- **استفاده از DHCP Snooping**: جلوگیری از ایجاد سرور DHCP غیرمجاز.
- **Dynamic ARP Inspection (DAI)**: جلوگیری از حملات ARP Spoofing.
- **Port Security**: محدود کردن تعداد دستگاه‌های متصل به پورت.

4. پیشگیری از سوئیچینگ مجازی (MAC Spoofing)

- استفاده از **X802.1** برای احراز هویت دستگاه‌ها قبل از اتصال به شبکه.
- **Sticky MAC Address**: ذخیره MAC دستگاه‌های مجاز در سوئیچ.

5. نرم‌افزارهای امنیتی

- **Firewall** و **IDS/IPS** برای تشخیص و جلوگیری از ترافیک مشکوک.
- **Antivirus** و **Anti-malware** برای جلوگیری از نصب نرم‌افزارهای مخرب.

6. آموزش کاربران

- آموزش کاربران درباره خطرات اتصال به شبکه‌های نامطمئن (مثلاً Wi-Fi عمومی).
- اجتناب از کلیک روی لینک‌های مشکوک.

7. استفاده از سرویس‌های امن

- **DNS over HTTPS (DoH)** یا **DNS over TLS (DoT)** برای جلوگیری از حملات DNS Spoofing.

- **نتیجه:**
- حملات MitM را می‌توان با **ترکیب رمزنگاری، احراز هویت، پیکربندی شبکه امن و آموزش کاربران** به طور مؤثر جلوگیری کرد.

۲۶. پروتکل SNMP چیست و چگونه در مدیریت شبکه استفاده می‌شود؟ مثال بزنید.

SNMP (Simple Network Management Protocol) یک پروتکل استاندارد برای مدیریت دستگاه‌های شبکه است.

عملکرد:

SNMP به شما اجازه می‌دهد پارامترهای دستگاه‌های شبکه (مانند روترها، سوئیچ‌ها، چاپگرها و غیره) را نظارت، پیکربندی و مدیریت کنید.

نحوه کار:

- **Agent:** نرم‌افزاری روی دستگاه شبکه که اطلاعات را جمع‌آوری می‌کند.
- **Manager:** نرم‌افزاری روی کامپیوتر مدیریت شبکه که درخواست اطلاعات را ارسال می‌کند.
- **MIB (Management Information Base):** پایگاه داده‌ای که اطلاعات مربوط به دستگاه را تعریف می‌کند.

کاربردها:

- **نظارت بر وضعیت دستگاه:** بررسی CPU، حافظه، ترافیک شبکه و غیره.
- **تشخیص خطا:** دریافت هشدار در صورت بروز مشکل.
- **پیکربندی دستگاه:** تغییر تنظیمات دستگاه از راه دور.
- **جمع‌آوری آمار:** جمع‌آوری اطلاعات ترافیکی و عملکردی برای تحلیل.

به طور خلاصه، SNMP ابزاری قدرتمند برای مدیریت و نظارت بر شبکه‌های بزرگ است.

۲۷. چگونه Load Balancing می‌تواند عملکرد شبکه را بهبود ببخشد؟ مزایای آن چیست؟

Load balancing عملکرد شبکه را به شکل زیر بهبود می‌دهد:

1. توزیع بار بین چندین سرور

- دریافت ترافیک را بین چندین سرور تقسیم می‌کند تا هیچ سروری بیش از حد بار نگیرد.
- از اشباع سرورها جلوگیری می‌کند.

2. افزایش دسترس‌پذیری (Availability)

- اگر یک سرور خراب شود، ترافیک به سرورهای دیگر منتقل می‌شود.
- توقف سرویس کاهش می‌یابد.

3. افزایش سرعت پاسخگویی

- کاربران به سرورهای کم‌بار متصل می‌شوند.
- زمان پاسخگویی (latency) کاهش می‌یابد.

4. مقابله با ترافیک بالا

- در زمان اوج ترافیک (مثلاً در فروش های ویژه)، بار را به سرورهای اضافی منتقل می‌کند.
- عملکرد پایدار حفظ می‌شود.

5. قابلیت ارتقا (Scalability)

- با افزودن سرورهای بیشتر، ظرفیت شبکه را افزایش می‌دهد.
- بدون توقف سرویس.

6. بهبود امنیت

- می‌توان از سرورهای امن‌تر در برابر حملات (مثلاً DDoS) استفاده کرد.
- ترافیک را بر اساس قوانین امنیتی توزیع می‌کند.

نتیجه:

Load balancing عملکرد شبکه را سریع‌تر، پایدارتر و قابل اطمینان‌تر می‌کند و تجربه کاربری را بهبود می‌بخشد.

۲۸. با ذکر یک مثال توضیح دهید که چگونه روترها و سوئیچ‌ها در یک شبکه بزرگ با هم کار می‌کنند؟

در یک شبکه بزرگ، **روترها** و **سوئیچ‌ها** با هم ترکیبی از عملکرد لایه‌های مختلف شبکه ایجاد می‌کنند:

مثال: شبکه یک شرکت با چند طبقه

- **سوئیچ‌ها** در هر طبقه (مثلاً اتاق کار، بخش فناوری اطلاعات) دستگاه‌های را به یکدیگر متصل می‌کنند.
  - مثال: دستگاه‌های کارمند در طبقه اول از طریق یک سوئیچ به شبکه متصل می‌شوند.
  - سوئیچ فقط ترافیک را در **لایه 2 (فیزیکی و داده‌های لینک)** جهت‌دهی می‌کند (بر اساس MAC Address).
- **روترها** در مرکز شبکه قرار دارند و اتصال بین شبکه‌های مختلف (مثلاً طبقات یا شعبه‌های مجزا) را ایجاد می‌کنند.
  - مثال: روتر از طریق IP Address ترافیک بین طبقه اول و دوم (یا اینترنت) جهت‌دهی می‌کند.
  - روتر در **لایه 3 (شبکه)** کار می‌کند و مسیرهای مربوطه را تعیین می‌کند.

کارکرد همکاری:

1. کارمند در طبقه اول (با IP: 192.168.1.10) می‌خواهد به سرور اینترنت دسترسی پیدا کند.
2. ترافیک از طریق **سوئیچ** به روتر می‌رود (چون IP سرور خارج از شبکه داخلی است).
3. روتر، مسیر را بر اساس **آدرس IP** تعیین می‌کند و ترافیک را به اینترنت ارسال می‌کند.
4. پاسخ از اینترنت از طریق روتر و سوئیچ به کارمند باز می‌گردد.

نتیجه:

- **سوئیچ**: ارتباط داخلی سریع در یک شبکه محلی.
- **روتر**: ارتباط بین شبکه‌های مختلف (مثلاً داخلی و خارجی).

همکاری این دو دستگاه امکان ارتباط سریع و کارآمد در شبکه بزرگ را فراهم می‌کند.

۲۹. چگونه می‌توان از ابزارهای مانیتورینگ شبکه برای شناسایی مشکلات استفاده کرد؟ مثال بزنید.

از ابزارهای مانیتورینگ شبکه برای شناسایی مشکلات به شرح زیر استفاده می‌شود:

1. نظارت بر ترافیک شبکه

- تشخیص افزایش ناگهانی ترافیک (مثلاً حملات DDoS).
- شناسایی دستگاه‌های مصرف‌کننده بیش از حد باندویث.

2. بررسی وضعیت دستگاه‌ها

- تشخیص خرابی یا عدم پاسخ دادن سرورها، روترها یا سوئیچ‌ها.
- ارسال هشدار در صورت افت عملکرد.

3. تشخیص مشکلات پایه‌ای

- شناسایی اتصالات قطع شده یا تأخیر بالا (latency).
- بررسی پکت‌های از دست رفته (packet loss).

4. تحلیل عملکرد سرورها

- نظارت بر CPU، حافظه و دیسک سرورها.
- تشخیص بار بالای سرور و نیاز به ارتقا.

5. شناخت منابع مصرف‌کننده بیش از حد

- شناسایی اپلیکیشن‌های یا کاربرانی که ترافیک زیادی می‌سازند.
- اعمال محدودیت دسترسی در صورت نیاز.

6. گزارش‌های تحلیلی

- ارائه گزارش‌های روزانه/هفتگی برای شناسایی روندهای مشکل‌ساز.
- پیش‌بینی مشکلات قبل از وقوع.

7. هشدارهای اتوماتیک

- فعال‌سازی هشدار در صورت بروز خطا (مثلاً پکت از دست رفته بیش از حد).
- ارسال اطلاعات به تیم فنی برای اقدام سریع.

نتیجه:

ابزارهای مانیتورینگ شبکه با ارائه داده‌های واقعی و هشدارهای زمانی، به شناسایی و رفع سریع مشکلات کمک می‌کنند و عملکرد شبکه را پایدار نگه می‌دارند.

SNMP (Simple Network Management Protocol) یک پروتکل استاندارد برای مدیریت دستگاه‌های شبکه است.

عملکرد:

SNMP به شما اجازه می‌دهد پارامترهای دستگاه‌های شبکه (مانند روترها، سوئیچ‌ها، چاپگرها و غیره) را نظارت، پیکربندی و مدیریت کنید.

نحوه کار:

- **Agent:** نرم‌افزاری روی دستگاه شبکه که اطلاعات را جمع‌آوری می‌کند.
- **Manager:** نرم‌افزاری روی کامپیوتر مدیریت شبکه که درخواست اطلاعات را ارسال می‌کند.
- **MIB (Management Information Base):** پایگاه داده‌ای که اطلاعات مربوط به دستگاه را تعریف می‌کند.

کاربردها:

- **نظارت بر وضعیت دستگاه:** بررسی CPU، حافظه، ترافیک شبکه و غیره.
- **تشخیص خطا:** دریافت هشدار در صورت بروز مشکل.
- **پیکربندی دستگاه:** تغییر تنظیمات دستگاه از راه دور.
- **جمع‌آوری آمار:** جمع‌آوری اطلاعات ترافیکی و عملکردی برای تحلیل.

به طور خلاصه، SNMP ابزاری قدرتمند برای مدیریت و نظارت بر شبکه‌های بزرگ است.

۳۰. چگونه می‌توان با ترکیب مفاهیم VLAN و Redundancy یک شبکه امن و پایدار طراحی کرد؟ توضیح دهید.

با ترکیب **VLAN** و **Redundancy**، می‌توان یک شبکه امن و پایدار طراحی کرد:

---

1. VLAN: جداسازی و امنیت

- **جداسازی ترافیک**: شبکه را به گروه‌های منطقی (VLAN) تقسیم کنید (مثلاً: اداری، فنی، مهمان).
- **محدودیت دسترسی**: اجازه دسترسی به منابع فقط برای گروه‌های مجاز.
- **کاهش سطح حمله**: اگر یک VLAN آلوده شود، انتقال به دیگر VLANها محدود می‌شود.

---

2. Redundancy: پایداری و دسترس‌پذیری

- **سوئیچ‌های استک شده یا مجازی**: از دو سوئیچ به عنوان پشتیبان استفاده کنید.
- **روترهای مسیردهی دوگانه**: از مسیرهای جایگزین برای اتصال اینترنت یا بین VLANها.
- **پورت‌های مکمل (Port Trunking)**: از لینک‌های چندگانه برای انتقال داده استفاده کنید.

---

3. ترکیب هر دو: امنیت + پایداری

- **VLAN در شبکه‌های متعدد**: هر VLAN در یک سوئیچ مستقل یا استک قرار دارد.
- **سرویس‌دهی مداوم**: اگر یک سوئیچ خراب شود، VLANهای مربوطه از طریق سوئیچ دیگر ادامه می‌یابند.
- **مسیردهی امن**: از مسیرهای پشتیبان برای انتقال ترافیک بین VLANها استفاده کنید.

مثال:

- یک شرکت دارای VLAN اداری و فنی است.
- دو سوئیچ استک شده دارند (پشتیبانی).
- اگر سوئیچ اصلی خراب شود، VLANها به سوئیچ دوم منتقل می‌شوند.
- ترافیک داخل VLANها ایمن می‌ماند و دسترسی به اینترنت از طریق روترهای مسیردهی دوگانه ادامه دارد.

نتیجه:

ترکیب VLAN (امنیت) و Redundancy (پایداری) منجر به شبکه‌ای می‌شود که **امن، پایدار و قابل اطمینان** است.

۳۱. کابل‌های شبکه از انواع مختلفی مانندUTP ، STPو FTP تشکیل شده‌اند. این کابل‌ها چه تفاوت‌هایی با یکدیگر دارند و در چه شرایطی باید از هر کدام استفاده کرد؟

تفاوت کابل‌های شبکه: UTP، STP، FTP

نوع کابل	ویژگی	مزیت	کاربرد	نیاز به شرایط
UTP (Unshielded Twisted Pair)	بدون محافظت از شرایط محیطی	ارزان، سبک، نصب آسان	شبکه‌های داخلی (مثلاً دفتر کار)	محیط‌های بدون تداخل الکترومغناطیسی
STP (Shielded Twisted Pair)	دارای لایه محافظ فلزی (Shield)	مقاومت بالا در برابر تداخل	محیط‌های صنعتی، نزدیک به تجهیزات قدرت	تداخل زیاد (مثلاً نزدیک کابل برق)
FTP (Foil Twisted Pair)	لایه محافظ فلزی فقط روی جفت‌های کابل	امنیت بیشتر نسبت به UTP	شبکه‌های حساس به تداخل	نیاز به حفاظت متوسط

نکات کلیدی:

- **UTP**: انتخاب اصلی برای بیشتر موارد (مثلاً 80% شبکه‌های اداری).
- **STP**: در محیط‌های پر تداخل (مثلاً کارخانه، پایگاه نظامی).
- **FTP**: میانه بین UTP و STP، مناسب برای شبکه‌های کوچک با تداخل متوسط.

نتیجه:

انتخاب کابل بستگی به **محیط**، **تداخل الکترومغناطیسی** و **نیاز امنیت** دارد.

- **UTP** برای بیشتر موارد مناسب است.
- **STP** برای محیط‌های صنعتی.
- **FTP** گزینه میانی است.

۳۲. چرا در برخی شرایط از کابل فیبر نوری به جای کابل‌های مسی استفاده می‌شود؟ تفاوت‌ها و مزایای کابل‌های فیبر نوری را توضیح دهید.

در برخی موارد، **کابل فیبر نوری** به جای **کابل مسی** استفاده می‌شود به دلیل مزایای قابل توجه آن در **سرعت**، **فاصله**، **امنیت** و **مقاومت**.

تفاوت‌های کابل فیبر نوری و مسی

ویژگی	کابل مسی (UTP/STP)	کابل فیبر نوری
نوع سیگنال	الکتریکی	نوری (پالس نور)
سرعت انتقال	تا 10 Gbps (در کابل‌های جدید)	تا 100 Gbps یا بیشتر
فاصله انتقال	تا 100 متر (در Ethernet)	تا 10 کیلومتر (یا بیشتر با تقویت‌کننده)
مقاومت در برابر تداخل	پایین (معرض تداخل الکترومغناطیسی)	بسیار بالا (غیرحساس به تداخل)
امنیت	قابل نفوذ (نیاز به رمزنگاری)	بسیار امن (نیاز به قطع فیزیکی برای نفوذ)
وزن و سایز	سنگین‌تر و ضخیم‌تر	سبک و نازک
هزینه	پایین‌تر	بالاتر (نیاز به تجهیزات خاص)

مزایای فیبر نوری

1. **سرعت بسیار بالا**: مناسب برای داده‌های حجیم (مثلاً فیلم، ابر، ارتباطات بین دانشگاه‌ها).
2. **فاصله طولانی**: بدون کاهش کیفیت تا 10 کیلومتر (در مسیرهای مسی این فاصله محدود است).
3. **مقاومت در برابر تداخل**: نیازی به ایزولاسیون الکترومغناطیسی نیست.
4. **امنیت بالا**: نیاز به قطع فیزیکی برای نفوذ دارد (شیار نمی‌شود).
5. **وزن کم و نصب آسان**: در فضاهای محدود یا طولانی مسیر مناسب است.

کاربردهای فیبر نوری

- ارتباطات بین شهری/بین‌المللی
- شبکه‌های داده بزرگ (Data Centers)
- ارتباطات بین ساختمان‌ها
- شبکه‌های حساس (مثلاً بیمارستان، نظامی)

جمع‌بندی

فیبر نوری در مواردی که نیاز به **سرعت بالا**، **فاصله طولانی** و **امنیت** است، ترجیح داده می‌شود.

کابل مسی همچنان برای **شبکه‌های داخلی کوچک** و **اقتصادی** مناسب است.

۳۳. مفهوم Port Security چیست و چرا در شبکه‌های مدرن مورد استفاده قرار می‌گیرد؟ توضیح دهید که این قابلیت چگونه به بهبود امنیت شبکه کمک می‌کند.

مفهوم Port Security (امنیت پورت)

Port Security یک ویژگی در سوئیچ‌های لایه 2 است که **محدودیت دسترسی به پورت‌های شبکه** را از طریق **محدود کردن تعداد دستگاه‌های متصل** و **محدود کردن آدرس‌های MAC** انجام می‌دهد.

- **چرا در شبکه‌های مدرن مورد استفاده قرار می‌گیرد؟**
  - جلوگیری از **اتصال غیرمجاز** به شبکه (مثلاً اتصال دستگاه ناشناس).
  - جلوگیری از **حملات مانند MAC Flooding** یا **ARP Spoofing**.
  - حفاظت از **منابع شبکه** در برابر تهدیدات داخلی.

- **چگونه به امنیت شبکه کمک می‌کند؟**
  1. **محدودیت تعداد دستگاه‌ها**
     - می‌توانید مشخص کنید که چند دستگاه می‌توانند به یک پورت متصل شوند (مثلاً فقط 1 دستگاه).
     - جلوگیری از اتصال چند دستگاه از طریق هکر یا هکرینگ.
  2. **محدودیت آدرس MAC**
     - فقط دستگاه‌هایی که آدرس MAC آن‌ها در لیست مجاز باشد، می‌توانند وارد شوند.
     - از اتصال دستگاه‌های ناشناس جلوگیری می‌کند.
  3. **اقدامات امنیتی در صورت نقض**
     - **Shutdown**: پورت را غیرفعال می‌کند.
     - **Restrict**: ترافیک غیرمجاز را می‌سوزاند و اخطار می‌دهد.
     - **Protect**: ترافیک غیرمجاز را نادیده می‌گیرد.

- **مثال کاربردی**
  - در یک دفتر کار، یک پورت سوئیچ فقط برای یک کامپیوتر مجاز است.
  - اگر کسی دستگاه دیگری به آن پورت وصل کند، پورت خودکار غیرفعال می‌شود.

- **جمع‌بندی**

Port Security یک لایه امنیتی ساده اما مؤثر است که در **شبکه‌های مدرن** برای جلوگیری از دسترسی غیرمجاز، تهدیدات داخلی و حفاظت از پورت‌ها استفاده می‌شود.

۳۴. چگونه می‌توان **Port Security** را در یک سوئیچ شبکه فعال کرد؟ مراحل پیاده‌سازی را با ذکر دستورات (برای سوئیچ‌های سیسکو) توضیح دهید.

1. ورود به حالت کنترل پورت

bash ویرایش با Canvas

```
Switch(config)# interface fa0/1
```

(در اینجا `fa0/1` نام پورت مورد نظر است)

2. فعال‌سازی Port Security

bash ویرایش با Canvas

```
Switch(config-if)# switchport port-security
```

3. محدودیت تعداد دستگاه‌های متصل (مثلاً 1 دستگاه)

bash ویرایش با Canvas

```
Switch(config-if)# switchport port-security maximum 1
```

4. اضافه کردن آدرس MAC مجاز (اختیاری)

bash ویرایش با Canvas

```
Switch(config-if)# switchport port-security mac-address 0001.0002.0003
```

5. تنظیم رفتار در صورت نقض (مثلاً غیرفعال کردن پورت)

bash ویرایش با Canvas

```
Switch(config-if)# switchport port-secur violation shutdown
```

6. فعال‌سازی مکانیزم یادداشت MAC خودکار (sticky)

bash ویرایش با Canvas

```
Switch(config-if)# switchport port-security mac-address sticky
```

7. ذخیره تنظیمات

bash ویرایش با Canvas

```
Switch# write memory
```

🔹 توضیحات کلیدی

- `maximum 1` : فقط یک دستگاه مجاز است.
- `violation shutdown` : در صورت اتصال دستگاه غیرمجاز، پورت غیرفعال می‌شود.
- `sticky` : سیستم خودکار آدرس MAC دستگاه مجاز را یاد می‌گیرد.

🔹 مثال کامل

bash ویرایش با Canvas

```
Switch(config)# interface fa0/1
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security violation shutdown
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# exit
Switch# write memory
```

🔹 نکته

پس از فعال‌سازی، اگر دستگاهی غیرمجاز به پورت وصل شود، پورت به حالت **err-disabled** می‌رود.

برای بازگرداندن:

bash ویرایش با Canvas

```
Switch# shutdown
Switch# no shutdown
```

۳۵. سه نوع رفتار (Violation Modes) در Port Security را توضیح دهید. هر کدام از این رفتارها در چه شرایطی استفاده می‌شوند؟

رفتارهای Violation Mode در Port Security

در Port Security، سه حالت Violation Mode وجود دارد که تعیین می‌کنند در صورت نقض قوانین (مانند اتصال دستگاه غیرمجاز)، سوئیچ چه واکنشی نشان دهد:

1. **Restrict (محدود کردن)**
   - **عملکرد:** ترافیک دستگاهی که نقض کرده (یعنی آدرس MAC آن در لیست مجاز نیست) را می‌سوزاند (drop) و یک پیام هشدار (log) ثبت می‌کند. پورت همچنان فعال می‌ماند و به ارسال و دریافت ترافیک ادامه می‌دهد.
   - **شرایط استفاده:**
     - وقتی می‌خواهید از اتصال دستگاه‌های غیرمجاز جلوگیری کنید، اما می‌خواهید پورت همچنان برای تست یا عیب‌یابی فعال بماند.
     - وقتی می‌خواهید هشداری دریافت کنید و به صورت دستی اقدام کنید.
   - **مثال:** اتصال یک دستگاه ناشناس به پورت، ترافیک آن سوسو می‌خورد و یک پیام در لاگ سوئیچ ثبت می‌شود.
2. **Shutdown (غیرفعال کردن)**
   - **عملکرد:** پورت را به طور کامل غیرفعال می‌کند. اتصال دستگاه قطع می‌شود و پورت دیگر ترافیکی را ارسال یا دریافت نمی‌کند.
   - **شرایط استفاده:**
     - وقتی امنیت شبکه اولویت دارد و اتصال دستگاه‌های غیرمجاز به هیچ وجه قابل قبول نیست.
     - برای جلوگیری از حملات و آسیب‌های احتمالی.
   - **مثال:** اتصال یک دستگاه غیرمجاز به پورت، پورت به طور خودکار غیرفعال شده و دستگاه دیگر نمی‌تواند به شبکه متصل شود.
3. **Protect (محافظت)**
   - **عملکرد:** ترافیک دستگاهی که نقض کرده را نادیده می‌گیرد (ignore). هیچ هشداری ثبت نمی‌شود و پورت به کار خود ادامه می‌دهد. این حالت توصیه نمی‌شود.
   - **شرایط استفاده:**
     - این حالت معمولاً استفاده نمی‌شود و خطرناک است، زیرا دستگاه‌های غیرمجاز می‌توانند به شبکه نفوذ کنند بدون اینکه هیچ هشداری دریافت شود.
   - **مثال:** اتصال یک دستگاه غیرمجاز به پورت، ترافیک آن نادیده گرفته می‌شود و پورت به کار خود ادامه می‌دهد، اما این کار امنیت شبکه را به خطر می‌اندازد.

۳۶. تفاوت بین Port Security Dynamic و Static چیست؟ هر کدام چه مزایا و معایبی دارند؟

ویژگی	Static MAC	Dynamic MAC
تعریف	آدرس MAC دستگاه به صورت دستی و ثابت در پورت ثبت می‌شود.	سیستم خودکار آدرس MAC دستگاه‌های مجاز را یاد می‌گیرد و ذخیره می‌کند.
نحوه اضافه شدن	دستی توسط مدیر (با دستور `switchport port-security mac-address <mac>`)	خودکار (با دستور `switchport port-security mac-address sticky`)
انعطاف‌پذیری	پایین (نیاز به دستی اضافه کردن هر دستگاه)	بالا (خودکار یاد می‌گیرد)
امنیت	بالا (آدرس‌ها ثابت و کنترل شده)	متوسط (می‌تواند در صورت نقض تغییر کند)
نیاز به نگهداری	بالا (مدیر باید دستگاه‌های جدید را اضافه کند)	پایین (خودکار انجام می‌شود)

مزایا و معایب

Static MAC ✅

- **مزایا:**
  - امنیت بالا (آدرس‌ها ثابت و قابل اطمینان).
  - مناسب برای دستگاه‌های ثابت (مثلاً چاپگر، سرور).
- **معایب:**
  - نیاز به دستی اضافه کردن هر دستگاه جدید.
  - اگر دستگاه جایگزین شود، نیاز به دستی اصلاح می‌شود.

Dynamic MAC (Sticky) ✅

- **مزایا:**
  - خودکار یاد می‌گیرد و نیاز به دستی اضافه کردن ندارد.
  - مناسب برای دستگاه‌های متغیر (مثلاً لپ‌تاپ کاربران).
- **معایب:**
  - امنیت کمتر (می‌تواند دستگاه غیرمجاز یاد شود).
  - اگر دستگاهی نقض کند، ممکن است آدرس آن در لیست مجاز قرار گیرد.

🔹 **کاربرد مناسب**

- **Static MAC**: دستگاه‌های ثابت (سرور، چاپگر، دوربین).
- **Dynamic (Sticky)**: دستگاه‌های متغیر (کاربران، لپ‌تاپ).

🔹 **جمع‌بندی**

- **Static**: امنیت بالا، نیاز به نگهداری.
- **Dynamic (Sticky)**: راحتی، مناسب دستگاه‌های متغیر.

۳۷. فرض کنید در یک شبکه، پورت یک سوئیچ با پیام Error-Disabled مواجه شده است. چگونه می‌توانید علت این مشکل را شناسایی و آن را برطرف کنید؟ مراحل را با جزییات بیان کنید.

اگر یک پورت سوئیچ سیسکو با پیام "error disabled" مواجه شود، این وضعیت معمولاً ناشی از **Port Security Violation** است. برای شناسایی و رفع مشکل:

🔹 **1. شناسایی علت**

- **دستور:**

bash — ویرایش با Canvas

```
show interfaces status
```

- پورتی که `err-disabled` است را پیدا کنید.
- **دستور:**

bash — ویرایش با Canvas

```
show interfaces <port> status
```

- جزئیات بیشتر (مثلاً `Port Security , err-disabled`).
- **دستور:**

bash — ویرایش با Canvas

```
show logging
```

- لاگ‌ها را بررسی کنید تا ببینید چه خطا (مثلاً `security violation`) رخ داده است.

🔹 2. رفع مشکل

✅ حالت 1: رفع خودکار (اگر `errdisable recovery` فعال باشد)

- فعال کردن ترمینال:

```bash
errdisable recovery cause psecure-violation
errdisable recovery interval 30
```

- پورت پس از 30 ثانیه خودکار فعال می‌شود.

✅ حالت 2: رفع دستی

- **غیرفعال کردن پورت:**

```bash
shutdown
```

- **فعال کردن مجدد:**

```bash
no shutdown
```

- اگر مشکل ادامه داشت، از `errdisable recovery` استفاده کنید.

🔹 3. جلوگیری از تکرار

- بررسی **Violation Mode**:

```bash
show running-config interface <port>
```

- اگر `shutdown` است، به `restrict` یا `protect` تغییر دهید.
- **حذف MAC غیرمجاز:**

```bash
clear port-security sticky interface <port>
```

🔹 جمع‌بندی

- **علت اصلی:** Violation در Port Security.
- **راه حل:** `no shutdown` → `show logging` → فعال کردن `errdisable recovery`.
- **پیشگیری:** تنظیم `restrict` و فعال کردن `errdisable recovery`.

۳۸. فرآیند Three-Way Handshake در پروتکل TCP را توضیح دهید. چرا این مکانیزم برای برقراری ارتباط در شبکه ضروری است؟ همچنین بیان کنید که اگر یکی از مراحل این فرآیند با مشکل مواجه شود، چه پیامدهایی برای ارتباط رخ خواهد داد.

🔹 Three-Way Handshake در TCP

هدف: برقراری ارتباط مطمئن و دوطرفه بین دو گره (مثلاً کلاینت و سرور) قبل از ارسال داده.

✅ مراحل Three-Way Handshake

1. SYN (سیگنال شروع)

- کلاینت به سرور ارسال می‌کند:

```
SYN=1, Seq=x
```

- کلاینت یک شماره ترتیب تصادفی (x) انتخاب می‌کند.

2. SYN-ACK (تأیید و ادامه)

- سرور پاسخ می‌دهد:

```
SYN=1, ACK=1, Seq=y, Ack=x+1
```

- y : شماره ترتیب سرور
- x+1 : تأیید دریافت x ازکلاینت

3. ACK (تأیید نهایی)

- کلاینت پاسخ می‌دهد:

```
ACK=1, Seq=x+1, Ack=y+1
```

- تأیید دریافت y از سرور

چرا این مکانیزم ضروری است؟

- **تأیید دوطرفه:** هر دو طرف می‌دانند که دیگری آماده است.
- **جلوگیری از ارسال داده نامعتبر:** قبل از ارسال داده، اطمینان حاصل می‌شود.
- **ایجاد ارتباط مطمئن:** از طریق تأییدهای متقابل، ارتباط قابل اعتماد می‌شود.

اگر یکی از مراحل با مشکل مواجه شود:

مراحل	پیامد
1. SYN ارسال نشود	سرور پاسخ نمی‌دهد. کلاینت **timeout** می‌شود.
2. SYN-ACK نرسد	کلاینت **retransmit** می‌کند. اگر چند بار تکرار شود، ارتباط **شکست می‌خورد**.
3. ACK نرسد	سرور نمی‌داند کلاینت آماده است. ارتباط **ناتمام می‌ماند**.

جمع‌بندی

- **ضرورت:** اطمینان از آمادگی هر دو طرف و ایجاد ارتباط مطمئن.
- **اشکال:** باعث **عدم اتصال** یا **تکرار تلاش‌های ارسال** می‌شود.
- **پیامدها:** **timeout**، **اتصال ناموفق**، یا **ارتباط ناقص**.

۳۹. تفاوت‌های بین Unicast ، Multicast و Broadcast در شبکه‌های کامپیوتری چیست؟ نحوه عملکرد هر یک را توضیح دهید و بیان کنید که در چه شرایطی از هر یک استفاده می‌شود. همچنین، مزایا و معایب هر روش را با مثال شرح دهید.

نوع	تعداد دریافت‌کنندگان	نحوه ارسال	مثال	کاربرد	مزایا	معایب
Unicast	1 دریافت‌کننده	از یک منبع به یک مقصد	ارسال ایمیل به یک کاربر	ارتباط دوطرفه (مثلاً HTTP, FTP)	امنیت بالا، کنترل دقیق	مصرف بیشتر باندwidth در ارتباطات گسترده
Multicast	چند دریافت‌کننده	از یک منبع به گروهی از مقاصد	پخش ویدیو زنده (IPTV)	پخش چندنفره (مثلاً VoIP, Video Streaming)	کاهش ترافیک، کارایی بالا	نیازبه پشتیبانی سوئیچ/ rout r
Broadcast	همه در شبکه	از یک منبع به تمامی مقاصد	پیدا کردن سرور DHCP	ارسال پیامات سیستمی (مثلاً ARP)	سادگی ارسال	ترافیک زیاد، خطر امنیتی

نحوه عملکرد

1. Unicast

- داده از یک IP منبع به یک IP مقصد ارسال می‌شود.
- مثال: دانلود فایل از یک وب‌سایت.

2. Multicast

- داده به یک **آدرس گروهی** ارسال می‌شود.
- فقط کاربران عضو گروه آن را دریافت می‌کنند.
- مثال: پخش زنده ویدیو به 100 نفر.

3. Broadcast

- داده به **همه دستگاه‌های شبکه** ارسال می‌شود.
- از آدرس `255.255.255.255` یا `192.168.1.255` استفاده می‌شود.
- مثال: درخواست DHCP از طریق ARP.

کاربرد و مثال

نوع	کاربرد	مثال
Unicast	ارتباط دوطرفه	دانلود فایل از سرور
Multicast	پخش گروهی	پخش زنده ویدیو (IPTV)
Broadcast	ارسال سیستمی	پیدا کردن سرور DHCP

جمع‌بندی

- **Unicast**: دقیق، امن، اما ناکارآمد در پخش گروهی.
- **Multicast**: کارآمد در پخش گروهی، نیاز به پشتیبانی سخت‌افزاری.
- **Broadcast**: ساده، اما خطرناک و مصرف‌کننده باندwidth.

۴۰. یک سوال محاسباتی در مورد **Subnetting** نیز در آزمون داده میشود.

🔹 محاسبه Subnetting (تقسیم شبکه)

هدف: تقسیم یک شبکه IP به زیرشبکه‌های کوچکتر برای مدیریت بهتر و کاهش ترافیک.

✅ مراحل محاسبه Subnetting

1. **تعیین کلاس IP و ماسک اولیه**
   - مثال: IP: `192.168.1.0` → کلاس C → ماسک: `255.255.255.0` (24 بیت)
2. **تعیین تعداد زیرشبکه‌ها یا دستگاه‌ها**
   - مثال: نیاز به 6 زیرشبکه → باید `n = 3 ^2` → `n ≥ 6` (می‌توان 8 زیرشبکه ایجاد کرد)
3. **محاسبه بیت‌های اضافی (subnet bits)**
   - برای 6 زیرشبکه: 3 بیت (چون `8 = 3^2`)
   - ماسک جدید: `255.255.255.224` (27 بیت)
4. **محاسبه زیرشبکه‌ها**
   - ماسک: `255.255.255.224` → `11100000` → بخش شبکه: 27 بیت
   - **گام زیرشبکه:** `256 - 224 = 32`
   - زیرشبکه‌ها:
     - `192.168.1.0/27`
     - `192.168.1.32/27`
     - `192.168.1.64/27`
     - ...
     - `192.168.1.192/27`

5. تعیین محدوده IP هر زیرشبکه

- مثال: `192.168.1.0/27`
  - **شبکه:** `192.168.1.0`
  - **محدوده:** `192.168.1.1` تا `192.168.1.30`
  - **Broadcast:** `192.168.1.31`

🔹 فرمول‌های کلیدی

توضیح	فرمول
بیت‌های مورد نیاز	`2^n ≥ تعداد زیرشبکه`
دستگاه‌های قابل استفاده (مثلاً 30 در /27)	`2^m - 2 ≥ تعداد دستگاه`
مثال: 256 - 224 = 32	`ماسک بخش انتهایی = 256 - گام`

🔹 مثال کامل

- IP: `192.168.1.0/24`
- نیاز به 6 زیرشبکه → 3 بیت
- ماسک: `255.255.255.224` (/27)
- زیرشبکه‌ها: `0, 32, 64, 96, 128, 160, 192, 224`
- هر زیرشبکه: 30 دستگاه (از 1 تا 30)

🔹 جمع‌بندی

- **هدف:** تقسیم شبکه برای کارایی و امنیت.
- **مهم‌ترین مراحل:** تعیین بیت‌های اضافی، محاسبه گام، محدوده IP.
- **نکته:** از `2^n - 2` برای دستگاه‌های قابل استفاده کنید (مگر اینکه `ip subnet-zero` فعال باشد).

https://www.aparat.com/v/kje4y72

https://www.aparat.com/v/fnu2371

https://www.aparat.com/v/jA19c

۱۴. توضیح دهید که چرا برخی از پورت‌ها در برابر حملات سایبری آسیب‌پذیر هستند.

چرا برخی پورت‌ها در برابر حملات سایبری آسیب‌پذیر هستند؟

پورت‌ها در شبکه به عنوان **درگاه‌های ارتباطی** عمل می‌کنند. برخی از آن‌ها به دلایل زیر آسیب‌پذیر هستند:

✅ **1. استفاده از پروتکل‌های قدیمی و ناامن**

- مثال: **Telnet (پورت 23)**، **FTP (پورت 21/20)**
- مشکل: داده‌ها **بدون رمزنگاری** ارسال می‌شوند ← حملات **Sniffing** و **Brute Force** امکان‌پذیر است.

✅ **2. نیاز به احراز هویت ضعیف یا عدم وجود آن**

- مثال: **RDP (پورت 3389)**
- اگر رمز عبور ساده باشد یا احراز هویت انجام نشود ← حملات **Brute Force** و **Password Spraying** انجام می‌شود.

✅ **3. نرم‌افزارهای قدیمی و با شکاف امنیتی**

- مثال: **Port 80 (HTTP)**، **Port 443 (HTTPS)**
- اگر سرور یا اپلیکیشن دارای **شکاف امنیتی** (مثل CVE-2021-44228 در Log4j) باشد ← حملات **Remote Code Execution** امکان‌پذیر است.

✅ **4. پورت‌های باز و بدون فیلترینگ**

- مثال: **پورت 22 (SSH)**، **پورت 3306 (MySQL)**
- اگر **فایروال** نباشد یا تنظیمات امنیتی نباشد ← حملات **Port Scanning** و **Exploitation** انجام می‌شود.

✅ **5. پورت‌های استاندارد (Well-Known Ports)**

- مثال: **Port 80, 443, 22, 25**
- حمله‌کنندگان از این پورت‌ها به عنوان **هدف اولیه** استفاده می‌کنند چون پرکاربرد هستند.

🔹 **چگونه از آسیب‌پذیری پورت‌ها جلوگیری کنیم؟**

1. **فیلترینگ پورت** (فایروال)
2. **استفاده از رمزنگاری** (SSL/TLS)
3. **به‌روزرسانی نرم‌افزارها**
4. **استفاده از پورت‌های غیراستاندارد** (مثلاً پورت 22 را تغییر دهید)
5. **محدود کردن دسترسی** (IP Whitelisting)
6. **استفاده از IDS/IPS** برای تشخیص حملات

- **جمع‌بندی**

پورت‌های آسیب‌پذیر معمولاً به دلیل:

- **پروتکل‌های ناامن**
- **نیاز به احراز هویت ضعیف**
- **نرم‌افزارهای قدیمی**
- **باز بودن بدون فیلترینگ**

→ امنیت شبکه را تهدید می‌کنند.

راه حل: امنیت لایه‌ای، فیلترینگ، رمزنگاری و به‌روزرسانی.