

فصل اول - آشنایی با مفاهیم شبکه و اجزای آن (۳ نمره)

۱. مزایای استفاده از یک شبکه رایانه ای را بنویسید.

اشتراک منابع نرم افزاری و سخت افزاری، ارتباط بر خط ، مدیریت و پشتیبانی متمرکز ، صرفه جویی در زمان و هزینه

۲. اجزای یک شبکه رایانه ای را نام ببرید و توضیح دهید.

رایانه سرویس دهنده (Server): رایانه ای که به درخواست رایانه های سرویس گیرنده پاسخ می دهد و منابع را با آنها به اشتراک می گذارد و مدیریت سرویس گیرنده ها را نیز بر عهده دارد.

رایانه سرویس گیرنده (Client): رایانه ای که درخواست استفاده از منابع موجود در شبکه را دارد (رایانه های Workstation یا ایستگاه کاری) محیط انتقال: کانال ارتباطی که می تواند سیمی یا بی سیم باشد

سیستم عامل شبکه: کنترل و مدیریت فعالیت های رایانه های شبکه را به منظور دستیابی به منابع مشترک و تبادل اطلاعات بر عهده دارد.

پروتکل (Protocol): مجموعه قوانینی که که با رعایت آنها سرویس دهی در شبکه برقرار می شود.

۳. شبکه های رایانه ای از نظر ابعاد و گستردگی فیزیکی به چند دسته تقسیم می شوند؟

شبکه های محلی (LAN): پایه شبکه های دیگر و کوچکترین فرم شبکه است. از دو تا چندصد رایانه با فاصله کم تشکیل می شود.

مثل شبکه رایانه ای یک برج ۵۰ طبقه با بیش از ۵۰۰ گره فعال

شبکه دانشگاهی (CAN): از چند شبکه محلی مجاور هم تشکیل شده و معمولاً در محیط دانشگاهی یا محیط پادگان نظامی یا کارخانه های بزرگ مورد استفاده قرار می گیرد. به آن شبکه پردیس نیز می گویند.

شبکه شهری (MAN): از چند شبکه محلی غیر مجاور در سطح یک شهر تشکیل شده مثلاً اگر بخواهیم سه منطقه آموزش و پرورش یک شهر را به هم متصل کنیم نوع شبکه ایجاد شده، از نوع شبکه شهری است.

شبکه گسترده (وسیع WAN): بزرگترین نوع شبکه به لحاظ وسعت بوده و معمولاً فضایی بزرگتر از یک شهر را در برمی گیرد. WAN می

تواند از ترکیب دو رایانه با فاصله دور تشکیل شود که از طریق خطوط تلفن با هم ارتباط دارند و یا این که از ترکیب دو یا چند شبکه LAN با فاصله دور و یا ترکیبی از چند شبکه MAN به وجود آمده باشد و به لحاظ وسعت جغرافیایی محدودیتی ندارد. کانال ارتباطی در این شبکه ها اغلب امواج مایکرو ویو یا ماهواره و خطوط مخابرات است.

مثلاً شبکه اینترنت بزرگترین شبکه گسترده WAN است. یا شبکه بین شعب بانک های کشور، یک شبکه گسترده یا WAN است.

۴. در تقسیم بندی شبکه های رایانه ای از نظر گستردگی فیزیکی، سیستم بانکی شتاب به کدام دسته تعلق دارد؟ WAN

۵. شبکه های رایانه ای از نظر مدل سرویس دهی به چند دسته تقسیم می شوند؟

الف) شبکه مبتنی بر سرویس دهنده (Server Base): در یک شبکه SB ساده یک رایانه فقط نقش سرویس دهنده را داشته و ما بقی سیستم های شبکه در نقش سرویس گیرنده ظاهر می شوند و در شبکه های بزرگتر تعدادی از سیستم ها فقط نقش سرویس دهنده را دارند و سایر سیستم ها نقش سرویس گیرنده را دارند.

سیستم عامل های SB ، از انواع خاصی می باشند مانند Novell و ویندوزهای سرور میکروسافت.

ب) شبکه نظریه نظیر (Peer to Peer): هر رایانه به طور همزمان هم سرویس دهنده و هم سرویس گیرنده است و کاربران هر رایانه می توانند داده های خود را در شبکه به اشتراک بگذارند.

به شبکه های PtP گروه کاری (Workgroup) میگویند یعنی گروه کوچکی از افراد حدود ۱۰ رایانه یا کمتر که تشکیل شبکه PtP را میدهند.

۶. مزایا و معایب شبکه های SB را بنویسید.

مزایا:

بالا بودن امنیت در شبکه است چون یک مدیر، سیاست های کلی را تعیین می کند و برای کلیه کاربران شبکه اعمال می کند.

می توان هزاران کاربر یا سرویس گیرنده داشت. به طوریکه سرویس گیرنده ها نیازی به داشتن سخت افزار قوی به لحاظ RAM و CPU ندارند.

شبکه SB برای استفاده در شبکه های متوسط و بزرگ مناسب است

معایب:

نصب، پیکربندی و مدیریت سیستم عامل های شبکه SB پیچیده بوده و نیاز به متخصص دارد. یکی از معایب بزرگ شبکه SB این است که چنانچه سرویس دهنده دچار مشکل شود، سرویس دهی در کل شبکه دچار اختلال می شود.

۷. مزایا و معایب شبکه های PtP را بنویسید.

مزایا: به نسبت شبکه ساده ای است.

به لحاظ راه اندازی، هزینه کمتری نسبت به شبکه SB خواهد داشت.

از بیشتر سیستم عامل های موجود می توان در شبکه PtP استفاده کرد و به نرم افزار خاصی برای کار با شبکه نیاز ندارند. هر کاربر مدیر خودش است، چون مدیریت متمرکز وجود ندارد چنانچه مشکلی برای یکی از رایانه ها به وجود آید کل شبکه دچار اختلال نمیشود.

معایب:

امکان رشد در آن خیلی محدود است.

۸. شبکه اینترنت از نظر سرویس دهی به کدام دسته شبکه های رایانه ای تعلق دارد؟ شبکه نظیر به نظیر (Peer to Peer)

۹. شبکه های بی سیم از نظر ابعاد و گستردگی به چند دسته تقسیم می شوند؟

WWANs: شبکه WAN به صورت بی سیم است که به وسیله سیستم ماهواره ای یا آنتن هایی که در جاهای مختلف نصب شده ارتباط را برقرار می کند. به عنوان مثال سیستم ارتباطی تلفن های همراه بر مبنای WWANs است.

WMANs: ساختار شبیه WWANs دارد با این تفاوت که وسعت سرویس دهی آن فقط در سطح شهرها است. می تواند به عنوان پشتوانه برای شبکه های سیم مسی یا فیبر نوری مورد استفاده قرار گیرند. از امواج رادیویی و نور مادون قرمز برای انتقال اطلاعات استفاده می کنند.

WLANs: برای استفاده در محیط های کوچک مانند شرکت ها یا فضای باز دانشکده ها یا اماکن عمومی با وسعت کم (مانند فرودگاه) است. بیشتر به صورت موقتی در ادارات و شرکت ها یا محل هایی که نصب سیم مسی سخت است استفاده می شود. در جاهایی که کاربران محل مشخص و ثابتی ندارند و می خواهند به همه اطلاعات دسترسی داشته باشند و یا از رایانه کیفی یا جیبی استفاده می کنند بسیار مناسب است.

WGAN: مانند شبکه تلفن جهانی کنونی عمل می کند و کاربران می توانند در حالی که بین کشورها مسافرت می کنند متصل به شبکه باقی بمانند. از مزایای این شبکه دارا بودن پهنای باند کافی برای دسترسی به اینترنت است.

WPANs: با این فناوری کاربران به صورت AD HOC با یکدیگر ارتباط برقرار می کنند. AD HOC استاندارد است که ارتباط بی سیم بین رایانه و تجهیزات جانبی، مانند رایانه جیبی PDAs یا تلفن همراه و رایانه کیفی را تا فضایی حدود ۱۰ متر برقرار می کند.

۱۰. انواع فناوری های WPANs کدامند؟

مادون قرمز (Infra red): از امواج مادون قرمز برای انتقال اطلاعات استفاده می شود. هر دو دستگاه فرستنده و گیرنده مجهز به این فناوری باید در دید مستقیم یکدیگر و بدون مانع باشند مانند کنترل تلویزیون. بیشتر در ساخت صفحه کلید و ماوس استفاده می شود. در شبکه کامپیوتری مادون قرمز حداکثر فاصله رایانه ها یا وسایل جانبی ۵ متر است.

بلوتوث: از امواج رادیویی استفاده می کند و می تواند اطلاعات را تا مسافت ۱۰۰ متر انتقال دهد. امواج رادیویی می تواند از موانع عبور کند. برای ارتباط بین تلفن همراه، رایانه جیبی، چاپگر و ... در فاصله های کم استفاده می شود.

۱۱. کاربردهای بلوتوث را بنویسید.

هدست بلوتوث (Headset): این دستگاه به راحتی قادر است با رایانه یا تلفن همراهی که روی آن تنظیم شده ارتباط صوتی برقرار کند.

چاپ (Printing): بعضی از چاپگرها مجهز به این فناوری هستند.

پل ارتباطی/اینترنت (Internet Bridge): اگر تلفن همراه مجهز به بلوتوث باشد از طریق سرویس Dial Up Networking (DUN) می توان با اینترنت ارتباط برقرار کرد سپس رایانه ای که از طریق بلوتوث به تلفن همراه متصل است می تواند بدون اتصال مودم از اینترنت استفاده کند.

تبادل اطلاعات (File exchange): در این روش تبادل اطلاعات به صورت نظیر به نظیر انجام می شود. وقتی بلوتوث رایانه فعال شود به طور خودکار شروع به شناسایی سایر دستگاه های نزدیک به خود میکند و بعد از صدور مجوز از طرف ارسال کننده اقدام به ارسال اطلاعات میکند.

۱۲. WLANs به چند صورت مختلف مورد استفاده قرار می گیرند؟

حالت اول: رایانه های مجهز به کارت شبکه بی سیم به دستگاه اکسس پوینت متصل می شوند و دستگاه اکسس پوینت پل ارتباطی بین رایانه های بی سیم و شبکه داخلی موجود خواهد بود. در این حالت کلیه رایانه های بی سیم علاوه بر ارتباط با هم به شبکه داخلی هم متصل هستند.

حالت دوم: رایانه های مجهز به کارت شبکه بی سیم به صورت نظیر به نظیر به یکدیگر متصل می شوند و در این حالت ارتباط با شبکه داخلی وجود ندارد (به دلیل عدم استفاده از اکسس پوینت).

۱۳. سرویس های رایج در شبکه های رایانه ای را نام ببرید. اشتراک منابع-تبادل پیغام-مدیریت از راه دور

فصل دوم - سیستم های انتقال اطلاعات (۱ نمره)

۱. مد انتقال را تعریف کنید.

تعداد بیت هایی که به طور همزمان از طریق کانال ارتباطی ارسال می شوند را مد انتقال می نامند.

۲. انواع مد انتقال کدامند؟

پشت سرهم (Serial): در ارسال سریال، بیت ها به صورت تک به تک و پشت سر هم انتقال می یابند. برای کنترل بیت ها، ابتدا و انتهای بیت ها با یک سری علامت به نام های بیت شروع و بیت پایان مشخص می شود.

موازی (Parallel): تعدادی از بیت ها (n بیت) به صورت همزمان و با هم و به صورت گروهی از طریق تعدادی کانال (n کانال) ارسال می شوند.

۳. سرعت ارسال اطلاعات در کدام یک از روش های سری یا موازی بیشتر است؟ موازی

۴. سیگنال چیست؟

مفهومی را که به انتقال اطلاعات از نقطه ای به نقطه دیگر و همچنین یک سری از پالس ها در رایانه اشاره می کند، سیگنال می نامند. امواج رادیویی و ویدیویی نمونه ای از این سیگنال ها هستند.

۵. انواع سیگنال را نام ببرید.

سیگنال آنالوگ: شبیه یک موج هستند که در زمان های مختلف مقادیر مختلفی دارند. صدای شخصی که در حال صحبت کردن است، نمونه ای از یک سیگنال آنالوگ است؛ به این صورت که صدا به صورت ممتد تولید شده و بلندی صدا دائماً در حال تغییر است.

سیگنال دیجیتال: فقط دو حالت دارد یعنی ارزش عددی سیگنال دیجیتال صفر یا یک است و در واحدهای زمانی مختلف فقط دو ارزش عددی متفاوت داریم.

۶. نویز چیست؟

نویز عامل مخربی است که شکل سیگنال ها را تغییر می دهد و باعث بروز اختلال می شود.

۷. چه عواملی باعث به وجود آمدن نویز می شوند؟

حرارت: حرارت باعث می شود الکترون ها در جهات نامشخص شروع به حرکت نمایند؛ این حرکت گاهی با سیگنال ها هم جهت شده و اندازه و شکل آنها را که همان الگوی سیگنال هاست، تغییر می دهد و این به معنی ایجاد نویز است.

تلفات: نویزهای القایی نویزهایی هستند که موتورهای مکانیکی مثل موتور ماشین یا وسایل الکتریکی تولید می کنند، این وسایل شبیه یک آنتن فرستنده عمل می کنند و می توانند نویز را ارسال کنند و کابل شبکه، شبیه یک آنتن گیرنده نویزهای ارسال شده را دریافت می کند. هم شنوایی: به اثرگذاری میدان مغناطیسی یک کابل از کابل مجاور آن هم شنوایی گفته می شود. نویزهایی که کابل های برق فشار قوی یا رعد و برق ایجاد می کنند، از انواع نویزهای هم شنوایی محسوب می شوند.

۸. اثر نویز بر روی کدام یک از سیگنال های آنالوگ یا دیجیتال بیشتر است؟ سیگنال آنالوگ چون حتی کمی تغییرات فرکانس،

شکل سیگنال را در آن لحظه تغییر می دهد.

۹. سرعت انتقال اطلاعات را تعریف کنید.

مقدار اطلاعاتی که در واحد زمان به وسیله تجهیزات شبکه ارسال می شود. واحد اندازه گیری آن بیت بر ثانیه (bps) است.

۱۰. سرعت انتقال اطلاعات با پهنای باند و نویز چه ارتباطی دارد؟

سرعت انتقال اطلاعات با پهنای باند ارتباط مستقیم دارد، هرچه پهنای باند بیشتر شود سرعت انتقال اطلاعات نیز بیشتر می شود. از طرفی سرعت انتقال با نویز نسبت معکوس دارد و نویز در این زمینه عامل محدودکننده ای است. پهنای باند، ظرفیت انتقال یک رسانه یا کابل است. در صورتی که سرعت انتقال، سرعت ارسال اطلاعات در واحد زمان است.

فصل سوم - پیکربندی شبکه و روش های دسترسی به خط انتقال (۲/۵ نمره)

۱. توپولوژی (هم بندی یا پیکربندی) را تعریف کنید.

اجزای یک شبکه را میتوان به روشهای مختلف طبق یک نقشه مشخص به هم متصل کرد. به این طرح و نقشه اتصال، پیکربندی شبکه میگویند. هم بندی دارای دو حالت فیزیکی و منطقی است، در حالت فیزیکی چگونگی اتصال ظاهری اجزای شبکه مشخص می شود که به وسیله کابل به هم متصل می شوند و حالت منطقی آن، نحوه تبادل اطلاعات و چگونگی دسترسی رایانه ها به محیط انتقال را مشخص می کند.

۲. انواع هم بندی را نام ببرید.

هم بندی خطی (BUS)، هم بندی مشبک (Mesh)، هم بندی ستاره ای (Star)، هم بندی حلقوی (Ring)

۳. هم بندی خطی (BUS) چگونه است؟

جنبه ظاهری یا فیزیکی: تمام سیستم ها با یک قطعه کابل به یکدیگر متصل شده اند. جنبه منطقی: زمانی که یک رایانه اطلاعات را ارسال می کند به تمام رایانه ها ارسال می شود و رایانه ای که دارای آدرس مشخص است اطلاعات را دریافت کرده و سایر رایانه ها اطلاعات را به خط اصلی بر می گردانند.

۴. کار ترمیناتور در هم بندی خطی چیست؟

در کابل شبکه خطی، سیگنال ها پس از رسیدن به انتهای خط (فضای باز) دوباره به خط اصلی برمی گردند و باعث تداخل و مختل شدن کل شبکه می شوند، به همین دلیل باید در ابتدا و انتهای خط شبکه از ترمیناتور استفاده شود. ترمیناتور حاوی یک مقاومت الکتریکی است که وابسته به کابل و ... است که در نوع خاصی از شبکه ها ۵۰ اهم است.

۵. مزایا و معایب هم بندی خطی را بنویسید.

مزایا: ساده ترین نوع هم بندی - ارزان ترین نوع هم بندی - کابل کمتری مصرف می شود - افزایش یا کاهش سیستم ها به راحتی انجام می شود
معایب: سرعت پایین تر نسبت به بقیه هم بندی ها دارد
عیب یابی شبکه مشکل و زمان بر است، تکنولوژی قدیمی است

اگر یکی از ترمیناتورها قطع یا خراب شود، ارتباط تمامی اجزای شبکه قطع می شود و شبکه از کار می افتد
در صورت قطع شدن یک قسمت از کابل اصلی، ارتباط تمام اجزای شبکه قطع می شود و شبکه از کار می افتد.

۶. هم بندی مشبک (Mesh) چگونه است؟

تمام رایانه های شبکه دو به دو با یک کابل مستقل به هم متصل می باشند که این حالت ایده آل است و به آن مش کامل می گویند. به طوری که تعداد رایانه های متصل در شبکه n باشد $n-1$ کابل به هر رایانه متصل می شود. (اگر یکی از اتصالات برقرار نباشد به آن مش ناقص میگویند).

۷. مزایا و معایب هم بندی مشبک را بنویسید.

مزایا: اگر یکی از ارتباط ها قطع شود از مسیر دیگری ارتباط برقرار می شود - مطمئن ترین و پایدارترین نوع ارتباط را دارا است.
معایب: به دلیل استفاده زیاد کارت شبکه و کابل، پیچیده ترین و گران ترین نوع هم بندی است.

۸. هم بندی ستاره ای (Star) چگونه است؟

جنبه ظاهری: تمام رایانه های شبکه توسط یک کابل مستقل به یک نقطه مرکزی به نام Hub Switch متصل می شوند.
اگر از Hub معمولی استفاده شود، سیگنالها به تمام رایانه های متصل به هاب ارسال می شوند ولی اگر از سوئیچ استفاده شود، سیگنالها فقط به رایانه مقصد ارسال می گردند.

جنبه منطقی: سیگنال ها از رایانه فرستنده به سوئیچ ارسال می شود سپس سوئیچ آنها را به سایر رایانه های شبکه ارسال می کند.

۹. مزایا و معایب هم بندی ستاره ای را بنویسید.

مزایا:

- ✓ قطع شدن یک کابل به طور معمول بر روی بقیه شبکه تأثیری نمی گذارد مگر این که مربوط به سرویس دهنده باشد (در SB)
- ✓ در صورت استفاده از سوئیچ، سیگنال ها فقط به رایانه مقصد ارسال می شوند نه تمام رایانه ها، که باعث کاهش حجم ترافیک می شود.
- ✓ در صورت استفاده از سوئیچ، امکان تبادل اطلاعات دو به دو به صورت هم زمان وجود خواهد داشت.
- ✓ هزینه نگهداری و رفع عیب آن نسبت به هم بندی خطی پایین تر است.

معایب:

- ✓ مصرف کابل و هزینه پیاده سازی آن از هم بندی خطی بیشتر است.
 - ✓ اگر به هر دلیلی دستگاه مرکزی از کار بیفتد، کل شبکه از کار می افتد.
۱۰. در هم بندی ستاره ای اگر نقطه مرکزی از کار بیفتد کل شبکه از کار باز می ایستد. برای رفع این مشکل چه کارهایی میتوان انجام داد؟

- ✓ معمولاً هاب را از نظر فیزیکی در یک تابلوی مخصوص معروف به Rack نصب کرده و Rack را در یک مکان مطمئن و با شرایط محیطی مناسب قرار می دهند .
- ✓ در شبکه هایی که ضریب حساسیت آن ها بیشتر است، ترکیبی از دو یا چند سوئیچ را درهم بندی Mesh قرار داده و بدین ترتیب اگر یکی از سوئیچ ها از کار بیفتد، سوئیچ های دیگر بلافاصله وارد عمل شده و ترافیک از طریق آنها به عبور خود ادامه میدهد (تحمل خطا)

۱۱. هم بندی حلقوی (Ring) چگونه است؟

- هر رایانه به صورت منطقی (نه فیزیکی) به رایانه مجاور خود متصل است و آخرین رایانه هم به اولین رایانه متصل است و رایانه ها تشکیل یک حلقه را می دهند .
- در عمل برای اتصال حلقه ای رایانه ها از یک دستگاه مرکزی به نام MAU (واحد دسترسی چندگانه) استفاده می شود و تمام رایانه ها با یک کابل به MAU متصل می شوند (مانند هم بندی ستاره ای)
- شبکه های طراحی شده با هم بندی حلقه ای را شبکه Token Ring یا Token Passing نیز می گویند، زیرا انتقال اطلاعات در این شبکه ها بر اساس گردش یک بسته مخصوص به نام Token است.

۱۲. انواع هم بندی حلقوی را نام ببرید.

- هم بندی حلقوی یک طرفه: Token ها فقط در یک جهت حرکت می کنند.
- هم بندی حلقوی دو طرفه: Token ها در هر دو جهت حرکت می کنند. در واقع نوع ناقص هم بندی Mesh است.

۱۳. برای اتصال دو شبکه حلقوی با هم چه کار باید کرد؟

- باید RO (Ring out) سوئیچ اول را به RI (Ring In) سوئیچ دوم متصل کرده و همچنین RO سوئیچ دوم را به RI سوئیچ اول وصل کنیم.
۱۴. مزایا و معایب هم بندی حلقوی را بنویسید.

مزایا:

- نحوه گردش اطلاعات دارای اولویت بندی و زمان بندی است تا تداخل به وجود نیاید.
- برای شبکه های با ترافیک بالا مناسب است، چون تداخل وجود ندارد.

معایب:

- ✓ اگر عیبی در MAU بوجود بیاید، کل شبکه از کار خواهد افتاد.
- ✓ افزودن یا کاستن رایانه ها در شبکه به سادگی ممکن نیست
- ✓ مصرف کابل و هزینه پیاده سازی آن نسبت به هم بندی خطی بیشتر است.
- ✓ مانند هم بندی خطی اگر قسمتی از حلقه قطع شود، کل شبکه از کار می افتد چون اطلاعات قادر به گردش کامل نخواهند بود.

۱۵. در کدام یک از انواع هم بندی، با قطع شدن قسمتی از کابل، کل شبکه از کار می افتد؟ هم بندی خطی و هم بندی حلقوی

۱۶. تفاوت MAU و هاب در چیست؟

MAU در شبکه حلقوی استفاده می شود و انتقال اطلاعات درون آن نیز به صورت حلقوی است اما هاب در شبکه ستاره ای استفاده می شود و اطلاعات را به صورت Broadcast انتقال می دهد.

۱۷. انواع هم بندی ها را از لحاظ مصرف کابل، سرعت، هزینه، عیب یابی و اشکال زدایی مقایسه کنید.

مصرف کابل: مشبک < ستاره ای < حلقوی < خطی

سرعت: مشبک < ستاره ای < حلقوی < خطی

هزینه: مشبک < حلقوی < ستاره ای < خطی

اشکال زدایی: ستاره ای < مشبک < حلقوی < خطی

۱۸. مفهوم روش دسترسی به خط انتقال چیست؟

به مجموعه قوانینی که تعیین می کنند داده ها چگونه در کابل شبکه قرار گیرند و یا این که داده ها چگونه از کابل شبکه دریافت شوند روش دسترسی می گویند. روش های دسترسی؛ از دسترسی همزمان رایانه ها به کابل شبکه جلوگیری می کنند.

۱۹. انواع روش های رایج برای دسترسی به خط انتقال را نام ببرید.

الف) روش دسترسی چندگانه تشخیص حامل با تشخیص برخورد (CSMA/CD)

ب) روش عبور نشانه (Token Passing)

ج) روش اولویت تقاضا

۲۰. روش CSMA/CD را توضیح دهید.

هر رایانه کابل شبکه را برای ترافیک چک می کند یعنی فقط وقتی که رایانه تشخیص دهد یا حس کند (Sense) کابل آزاد است و ترافیکی روی شبکه وجود ندارد داده را روی کابل ارسال می کند و تا زمانی که داده به مقصد نرسد رایانه دیگری نمی تواند روی کابل داده ارسال کند.

۲۱. پدیده برخورد یا Collision چیست؟

در روش دسترسی CSMA/CD اگر دو یا چند رایانه دقیقاً به طور همزمان روی کابل شبکه داده ارسال کنند برخورد به وجود می آید و وقتی چنین اتفاقی بیفتد، دو رایانه درگیر برای یک دوره زمانی تصادفی، انتقال را متوقف می سازند و سپس سعی در ارسال مجدد می نمایند.

۲۲. پدیده برخورد یا Collision در کدام یک از انواع هم بندی روی می دهد؟ چرا؟

در هم بندی خطی به دلیل وجود کابل مشترک

۲۳. چرا روش دسترسی CSMA/CD دارای پایین ترین سطح محبوبیت بین روش های دسترسی دیگر است؟

هر چقدر تعداد رایانه ها بیشتر شود ترافیک شبکه نیز بیشتر خواهد شد. در نتیجه برای اجتناب از برخورد، شبکه کند می شود. قابلیت تشخیص برخورد پارامتر مهمی در محدودیت فاصله در CSMA/CD است.

۲۴. روش عبور نشانه (Token Passing) را توضیح دهید.

در عبور نشانه، بسته خاصی به نام نشانه (Token) به صورت حلقوی از طریق کابل از یک رایانه به رایانه دیگر گردش می کند. وقتی رایانه ای بخواهد داده ها را در طول شبکه ارسال کند باید منتظر نشانه (Token) آزاد بماند. وقتی نشانه آزاد تشخیص داده شد، رایانه می تواند داده ها را انتقال دهد. مادامی که نشانه توسط یک رایانه مورد استفاده قرار می گیرد، سایر رایانه ها نمی توانند داده ای را منتقل کنند چون در این روش در هر لحظه فقط یک رایانه می تواند از نشانه استفاده کند.

۲۵. مزیت روش عبور نشانه بر روش دسترسی CSMA/CD چیست؟

در این روش رقابت و برخورد وجود ندارد و هیچ زمانی برای ارسال مجدد داده صرف نمی شود و ترافیکی هم بر روی شبکه به وجود نمی آید.

۲۶. ویژگی های روش اولویت تقاضا را بنویسید.

✓ از روش های جدید دسترسی به خط انتقال است.

✓ در این روش کنترل دسترسی شبکه از ایستگاه کاری به هاب انتقال می یابد .

✓ در هم بندی ستاره ای استفاده میشود.

✓ ارتباط بین رایانه فرستنده با هاب و هاب با رایانه مقصد برقرار است.

✓ راندمان بیشتری نسبت به روش CSMA/CD دارد.

✓ در این روش از چهار زوج سیم استفاده می شود که باعث می شود رایانه ها همزمان هم ارسال و هم دریافت داده داشته باشند.

۲۷. سرعت کدام یک از روش های دسترسی به خط بیشتر است؟ دلیل آن را بنویسید.

در روش اولویت تقاضا از چهار زوج سیم استفاده می شود که باعث می شود رایانه ها به طور همزمان هم ارسال و هم دریافت داده داشته باشند.

۲۸. چه عواملی در سرعت دسترسی به خط مؤثر است؟

جنس کابل، روش دسترسی به خط انتقال

فصل چهارم - محیط های انتقال و اجزای آن (۱/۵ نمره)

۱. محیط انتقال را تعریف کنید و انواع آن را نام ببرید.

به هر رسانه ای که بتواند اطلاعات را به گردش درآورده و هدایت کند اصطلاحاً محیط انتقال می گوئیم. - دو دسته : سیمی و بی سیم

۲. تفاوت محیط های انتقال بی سیم و با سیم چیست؟

در انتقال بی سیم از فضای مادی به عنوان محیط انتقال استفاده می شود اما در محیط انتقال سیمی از کابل مسی یا فیبر نوری استفاده می شود.

۳. انواع محیط انتقال بی سیم (Wireless) را نام ببرید.

اشعه مادون قرمز (Infra red)، نور لیزر (Laser)، امواج رادیویی (Radio waves)

۴. سه فناوری مادون قرمز در شبکه های محلی را بنویسید.

SIR IrDA2: مادون قرمز با سرعت کم (سرعت انتقال ۱۱۵ کیلوبیت بر ثانیه)

MIR IrDA: مادون قرمز با سرعت متوسط (سرعت انتقال ۱/۱۵ مگابیت بر ثانیه)

FIR IrDA: مادون قرمز با سرعت بالا (سرعت انتقال ۴ مگابیت بر ثانیه)

۵. اشعه مادون قرمز در فاصله بیشتری انتشار می یابد یا پرتو لیزر؟ نور لیزر

۶. مزیت امواج رادیویی نسبت به مادون قرمز و لیزر چیست؟

یکی از مزایای استفاده از امواج رادیویی برای انتقال داده، توانایی عبور امواج رادیویی از موانع فیزیکی است (البته مقداری از پهنای باند کاهش می یابد). استفاده از امواج رادیویی در فرکانس های مختلف بیشترین کاربرد را در بین شبکه های بی سیم دارد.

۷. انواع محیط انتقال سیمی (کابلی Wired) کدامند؟

الف) کابل مسی : که از یک یا چند رشته سیم مسی برای انتقال سیگنال های الکتریکی استفاده می شود.

ب) کابل فیبر نوری : از چند رشته تار نازک از جنس ترکیبات مخصوص مانند پلاستیک فشرده یا سیلیس که ضریب شکستی نزدیک به ضریب شکست شیشه دارند، استفاده می شود.

فیبر نوری یکی از محیط های انتقال داده با سرعت بالا است. یک تار فیبر نوری معادل ۹۰۰ زوج سیم مسی قدرت انتقال اطلاعات را دارد.

فیبر نوری داده های دیجیتال (پالس های الکتریکی) را به صورت پالس های نور هدایت می کند پس در دو انتهای فیبر نوری مبدل های پالس الکتریکی به نور و بالعکس وجود دارد.

۸. در محیط انتقال سیمی (کابلی Wired) از چه نوع کابل هایی استفاده می شود؟

الف) کابل هم محور (Coaxial) مانند کابل آنتن تلویزیون رنگی

ب) کابل زوج به هم تابیده (Twisted Pair) مانند سیم تلفن

ج) کابل فیبر نوری

۹. کابل هم محور Coaxial از چه بخش هایی تشکیل شده است؟

الف) مغز مسی: وظیفه آن هدایت سیگنال الکتریکی است که می تواند تک رشته ای یا چند رشته ای باشد.

ب) عایق داخلی: عایق بین مغز مسی و محافظ سیمی (توری) است.

ج) محافظ توری (بافته شده) سیمی: که از سیگنال های انتقالی در مقابل نویز حفاظت می کند.

د) عایق بیرونی

۱۰. کابل کواکسیال در چه نوع هم بندی استفاده می شود؟ هم بندی خطی

۱۱. علت تابیده بودن سیم ها به هم در کابل زوج به هم تابیده چیست؟

کابل TP در ساده ترین شکل از یک زوج سیم مسی شبیه سیم تلفن تشکیل شده اند، اما کابل هایی که در شبکه رایانه ها مورد استفاده قرار می

گیرند شامل چهار زوج سیم می باشند. علت تابیده بودن سیم ها به هم آن است که اولاً میدان مغناطیسی در اطراف خود بر اثر القاء به وجود

نیاورند و ثانیاً اثرات نویز القاء شده روی خود را تا اندازه های خنثی نمایند. هر زوج برای یک کانال ارتباطی مخابراتی مورد استفاده قرار می گیرد

۱۲. کابل TP در چه نوع هم بندی استفاده می شود؟ ستاره ای و حلقوی

۱۳. مزایا و معایب کابل TP را بنویسید.

مزایا:

✓ کابل TP نسبت به Coaxial ارزانتر است.

✓ کابل TP توانایی انتقال بالاتری نسبت به Coaxial دارد.

معایب:

✓ نویز اثر بیشتری روی TP دارد.

✓ مشکل همشنوایی (Cross Talk) در TP وجود دارد.

✓ کابل TP نسبت به Coaxial مقاومت کمتری در مقابل میرایی سیگنال ها دارد.

۱۴. انواع کابل TP (بر اساس نوع محافظ) کدامند؟

الف) بدون محافظ UTP (Unshielded)

ب) محافظ دار STP (Shielded) که شامل انواع زیر است:

- اگر محافظ کابل TP از جنس فویل آلومینیوم باشد به آن FTP می گویند.

- اگر هر زوج سیم به طور جداگانه محافظ (فویل آلومینیوم یا سیم بافته شده) داشته و مجموعه آنها نیز محافظ داشته باشند، به آن نوع کابل

SSTP می گویند که به دو صورت SFTP، FFTP وجود دارند.

۱۵. انواع کابل TP (بر اساس حداکثر سرعت و نوع کاربرد) چگونه تقسیم بندی می شوند؟

به چند دسته یا Category تقسیم می شوند که به صورت عدد Cat مانند Cat 5 نمایش داده می شوند.

۱۶. کابل فیبر نوری از چه بخشهایی تشکیل شده است؟

الف) هسته (Core): هسته نازک شیشه ای در مرکز فیبر که سیگنال های نوری در آن حرکت می کنند.

ب) روکش (Cladding): بخش خارجی فیبر بوده که دورتادور هسته را احاطه کرده و باعث برگشت نور منعکس شده به هسته می گردد.

ج) بافر رویه (Buffer Coating): روکش پلاستیکی رنگی که هم باعث حفاظت فیبر می شود و هم باعث تشخیص فیبر در سر دیگر کابل برای

اتصال سوکت ها می شود.

د) الیاف قوی (Strengthening fibers): برای بالا بردن قدرت کشش کابل فیبر نوری

ه) روکش بیرونی کابل (Cable Jacket): روکش پلاستیکی است

۱۷. چرا برای اتصال کابل فیبر نوری به کارت شبکه از دو تار فیبر نوری استفاده می شود؟

از آنجا که تار فیبر نوری انتقال داده را در یک جهت انجام می دهد، به همین منظور یک تار برای ارسال و یک تار برای دریافت استفاده میشود.

۱۸. انواع فیبرهای نوری را نام ببرید.

فیبرهای تک حالت (Mode Single) یا SM: برای ارسال یک سیگنال در هر فیبر استفاده می شود. یک هسته کوچک دارند و برای فواصل بیشتر از ۱۰ کیلومتر استفاده می شوند.

فیبرهای چندحالت (Mode Multi) یا MM: برای ارسال چندین سیگنال در یک فیبر استفاده می شود. هسته بزرگتر دارند و تا فاصله ۱۰ کیلومتر از آن ها استفاده می شود.

۱۹. مزایای فیبر نوری را بنویسید.

- ✓ امکان استفاده در فواصل طولانی تر.
- ✓ نرخ انتقال بیشتر (پهنای باند فیبر نوری به منظور ارسال اطلاعات به مراتب بیشتر از سیم مسی است).
- ✓ عدم نویزپذیری نسبت به میدانهای مغناطیسی.
- ✓ امنیت بیشتر به دلیل عدم امکان انشعاب گرفتن در بین مسیر بدون داشتن امکانات پیشرفته و تخصصی.
- ✓ تضعیف ناچیز (تضعیف سیگنال در فیبر نوری به مراتب کمتر از سیم مسی است).
- ✓ عدم اتصالی در فیبر نوری، بر خلاف سیم های مسی که با از بین رفتن روکش سیم امکان اتصالی وجود دارد.

۲۰. کاربرد کابل Straight و Cross چیست؟

Crossover	Straight
اتصال مستقیم دو رایانه با هم	اتصال رایانه به هاب یا سویچ
اتصال سویچ به سویچ	اتصال رایانه به پریز شبکه یا پانل
اتصال هاب به هاب	اتصال روتر به سویچ یا هاب
اتصال هاب به سویچ	
اتصال روتر به سویچ	
اتصال روتر به روتر	

۲۱. زوج سیم های استفاده شده در استاندارد T568A و T568B کدام است؟

در استاندارد T568B - که در ایران و آمریکا استفاده می شود- شماره پین های فرد همواره سفید با یک نوار رنگی هستند. اما در استاندارد T568A - که در اروپا و کانادا استفاده می شود- اتصالات سبز و نارنجی برعکس شده، بنابراین زوج های یک و دو بر روی چهار پین وسط قرار می گیرند.

شماره پین	رنگ	زوج
یک	سفید/ سبز	سوم
دو	سبز	سوم
سه	سفید / نارنجی	دوم
چهار	آبی	یک
پنج	سفید /آبی	یک
شش	نارنجی	دوم
هفت	سفید/قهوه ای	چهارم
هشت	قهوه ای	چهارم

T568A

شماره پین	رنگ	زوج
یک	سفید/ نارنجی	دوم
دو	نارنجی	دوم
سه	سفید / سبز	سوم
چهار	آبی	یک
پنج	سفید /آبی	یک
شش	سبز	سوم
هفت	سفید/قهوه ای	چهارم
هشت	قهوه ای	چهارم

T568B

۲۲. چند مورد از سخت افزارهای مورد نیاز در شبکه های فیبر نوری را نام ببرید.

پیچ پنل فیبر نوری، پیچ کورد فیبر نوری، کانکتورهای فیبر نوری، آداپتور فیبر نوری، دستگاه فیوژن برای اتصال فیبرنوری

۲۳. وظایف کارت شبکه کدامند؟

- ✓ آماده سازی داده از رایانه برای انتقال به کابل شبکه.
- ✓ ارسال داده به رایانه های دیگر در شبکه.
- ✓ کنترل جاری شدن داده ها بین رایانه و سیستم کابل کشی.
- ✓ دریافت داده از کابل شبکه و تبدیل آنها به داده های قابل پردازش برای پردازنده مرکزی رایانه.

انواع محیط های انتقال سیمی یا کابلی را از لحاظ سرعت، امنیت، هزینه، مسافت و نویز بررسی کنید.

سرعت: فیبر نوری < TP < Coaxial

امنیت: فیبر نوری < TP < Coaxial

هزینه: فیبر نوری < Coaxial < TP

مسافت: فیبر نوری < TP < Coaxial

عدم نویز پذیری: فیبر نوری < Coaxial < TP

۲۴. حداقل فاصله بین کابل شبکه و کابل برق باید چقدر باشد؟ ۵ تا ۳۰ سانتیمتر

۲۵. عوامل مؤثر در تعیین نوع کابل را نام ببرید.

نوع توپولوژی شبکه، سنگینی ترافیک شبکه، طول کابل، بودجه تعیین شده برای کابل کشی، نیازهای ایمنی شبکه، نوع کابل های موجود در بازار، بررسی توسعه پذیر بودن شبکه، فاصله نودها با هاب و سوئیچ و سرور

۲۶. آیا می توان در کابل کشی یک شبکه از همه انواع کابل (مانند Cat5 , Fiber , Cat6 و ...) استفاده کرد؟ سرعت و

راندمان شبکه در این حالت چگونه است؟

بله مثلاً می توان برای Backbone ها از Fiber Optic استفاده کرد و برای اتصالات کلاینت ها Cat5 را به کار برد.

۲۷. برای اتصال چند سوئیچ یا هاب از چه نوع کابلی باید استفاده گردد؟ کابل های Crossover

فصل ششم - آشنایی با پروتکل TCP/ IP و سرویس های آن (۳/۵ نمره)

۱. پروتکل چیست؟ انواع رایج آن را نام ببرید.

پروتکل مجموعه قوانین نرم افزاری است که رعایت آنها باعث بهره برداری از امکانات سخت افزاری و برقراری سرویس در شبکه می شود.

۲. نقش پروتکل در رایانه ارسال کننده داده چیست؟

✓ شکستن داده ها به بخش های کوچکتر، به نام بسته (packet)

✓ اضافه کردن اطلاعات آدرس مقصد به بسته

✓ آماده سازی داده ها برای انتقال از طریق کارت شبکه بر روی کابل شبکه.

۳. نقش پروتکل در رایانه دریافت کننده داده چیست؟

✓ دریافت بسته های داده از کابل شبکه

✓ ایجاد نواری از بسته های ارسالی از رایانه فرستنده

✓ کپی کردن بسته ها به بافر برای دوباره اسمبل کردن به عنوان داده

✓ پذیرش داده ها به شکل برنامه قابل استفاده

توجه اگر پروتکل های استفاده شده در رایانه های فرستنده و گیرنده با هم متفاوت باشند امکان دریافت درست داده ها در رایانه گیرنده وجود نخواهد داشت و یا این که بسته های دریافتی در رایانه گیرنده قابل استفاده نخواهد بود.

۴. پروتکل TCP/IP چیست؟

TCP/IP مجموعه کاملی از پروتکل های تعریف شده برای استفاده در شبکه های خصوصی و اینترنت است، ولی نام آن در واقع ترکیبی از دو پروتکل کنترل انتقال TCP و پروتکل اینترنت IP است.

۵. مهم ترین خصوصیات پروتکل TCP/IP چیست؟

✓ قابل استفاده در انواع شبکه ها

✓ پشتیبانی به وسیله انواع سیستم عامل ها

✓ مورد استفاده به عنوان پروتکل اصلی اینترنت

- ✓ قابلیت مسیر یابی
- ✓ حق انتخاب در انتقال اطلاعات به صورت اتصال گرا (TCP) و بدون اتصال (UDP)
- ✓ ارسال گروهی
- ✓ پیکربندی پیچیده

۶. درباره ویژگی قابلیت مسیریابی پروتکل TCP/IP توضیح دهید.

در TCP/IP الگوریتم های متنوع مسیریابی برای انتخاب مسیر بهینه از میان روترها (مسیریاب ها) تعبیه شده و به همین خاطر یکی از مهم ترین پروتکل ها برای استفاده در شبکه های WAN به شمار می رود .
هم بندی غالب شبکه های WAN از نوع Mesh است و در نقاط مرزی مابین شبکه ها از Router استفاده می شود پس پروتکل مورد استفاده باید دارای قابلیت مسیریابی (Routing) باشد.

۷. سرویس های رایج در پروتکل TCP/IP را نام ببرید.

- | | |
|----------------------------|---|
| ✓ FTP (انتقال فایل) | ✓ Telnet (شبیه ساز ترمینال متنی) |
| ✓ HTTP (کار با صفحات وب) | ✓ RDP (شبیه ساز ترمینال گرافیکی) |
| ✓ SMTP (ارسال ایمیل) | ✓ SNMP (مدیریت یکپارچه شبکه) |
| ✓ POP3 (دریافت ایمیل) | ✓ SNTP (یا NTP یکسان کردن زمان بین سرویس گیرنده و سرویس دهنده) |

۸. درباره سرویس FTP توضیح دهید.

سرویسی که انتقال پرونده را بین ماشینهای مختلف با سخت افزارهای متنوع و سیستم عاملهای گوناگون امکان پذیر می سازد.
FTP از دو قسمت تشکیل شده:

الف) FTP Client : مثل IE (Internet Explorer)

ب) FTP Server : مثل IIS که بسته ای است شامل چندین سرویس که یکی از آن ها FTP Server است.

کاربر با اجرای نرم افزار FTP Client به FTP Server متصل شده و با توجه به مجوزهای امنیتی می تواند پرونده های مورد نیاز را از سرویس دهنده دریافت کرده یا آن ها را روی سرویس دهنده ذخیره کند.

۹. چه دستوراتی در محیط FTP رایج است؟

بعضی از دستورات شامل موارد زیر است:

- | | |
|---|--|
| asci: انتقال فایل های اسکی | Bell : پس از اتمام Download صدای بوق می آید. |
| Binary : انتقال فایل های باینری | Pwd: دیدن مسیردایرکتوری |
| Cd : تغییر دایرکتوری در remote machine | help: دیدن لیست دستورات ftp |
| get: کپی کردن فایل از remote machine به local machine | Close : بدون خارج شدن از برنامه FTP به اتصال پایان میدهد |

۱۰. درباره سرویس HTTP توضیح دهید.

برای دستیابی به اطلاعات است . از دو بخش تشکیل شده:

الف : HTTP Client : همان Web Browser یا Web Client است. (مثل IE, Netscape, Fire Fox)

ب : HTTP Server : همان Web Server است.

کاربر نرم افزار HTTP Client مانند Fire Fox را اجرا کرده و درخواست دسترسی به اطلاعات یا حتی اجرای برنامه را به سرویس دهنده ارسال می دهد. سرویس دهنده درخواست را بررسی و پس از آماده کردن پاسخ، آن را در قالب Web Page برای سرویس گیرنده می فرستد. سرویس گیرنده این صفحات را دریافت کرده و با قالب مناسب به کاربر نشان می دهد. زبان صفحات وب اکثراً HTML یا XML است.

۱۱. درباره سرویس POP3 و SMTP توضیح دهید.

هر دو سرویس برای EMail استفاده می شوند .

برای تهیه، ارسال، دریافت و خواندن نامه از نرم افزار Mail Client (مثل Outlook Microsoft و Express Outlook) استفاده می شود. پس از اجرای Mail Client و پیکربندی آن، کاربر می تواند نامه را تایپ کرده، عکس یا پرونده های دیگری را به آن پیوست کرده و پس از تعیین گیرنده و موضوع نامه آن را ارسال کند. محتوای نامه همراه ضامائم پیوست، با پروتکل SMTP به سمت Mail Server ارسال می شود. Mail Server پس از دریافت نامه آدرس گیرنده را بررسی می کند و اگر گیرنده شخصی خارج از حوزه پستی خودش باشد آن را با SMTP به Mail Server حوزه گیرنده تحویل می دهد و Mail Server گیرنده، نامه را در صندوق پستی شخص گیرنده ذخیره می کند. شخص گیرنده به Mail Server حوزه خود متصل شده و با پروتکل POP3 نامه هایش را از سرویس دهنده دریافت کرده و در صندوق پستی محلی واقع در رایانه خودش منتقل می کند.

۱۲. نام پروتکلی که ارسال ایمیل را انجام می دهد چیست؟ POP3 و SMTP

۱۳. درباره سرویس Telnet توضیح دهید.

ترمینال وسیله ای است که برای ارسال و دریافت اطلاعات استفاده می شود اما هیچ گونه پردازشی روی اطلاعات در آن صورت نمی گیرد مثلاً یک Keyboard و یک Monitor؛ و پردازش اطلاعات در سیستم مرکزی (Central System) انجام می شود. Telnet یک سرویس Terminal Emulator است که اطلاعات را به صورت Text نشان می دهد. Telnet هم از دو بخش تشکیل شده:

الف) Telnet Client: که روی رایانه شخصی اجرا می شود و آن را تبدیل به ترمینال می کند.

ب) Telnet Server یا Telnet Daemon (telnetd): که روی Central System اجرا شده و اطلاعات را از ترمینال Telnet سرویس گیرنده دریافت و پس از پردازش به وسیله سیستم مرکزی، برای ترمینال کلاینت می فرستد.

۱۴. تفاوت عمده و اساسی ترمینال با یک رایانه PC چیست؟

ترمینال وسیله ای است که برای ارسال و دریافت اطلاعات استفاده می شود اما هیچ گونه پردازشی روی اطلاعات در آن صورت نمی گیرد و پردازش اطلاعات در سیستم مرکزی (Central System) انجام می شود اما در PC پردازش نیز صورت می گیرد.

۱۵. کدام سرویس TCP/IP از ترمینال استفاده می کند؟ برای اتصال به سیستم مرکزی به چه چیزهایی نیاز دارد؟

Telnet - Telnet Client و Telnet Server

۱۶. درباره سرویس RDP توضیح دهید.

مانند Telnet ولی گرافیکی است و رایانه شخصی را تبدیل به یک ترمینال گرافیکی می کند. از دو بخش تشکیل شده:

الف) RDP Client (Terminal Client): در مایکروسافت، همان برنامه Remote-Desktop است.

ب) RDP Server (Terminal Server): در مایکروسافت، همان سرویس Remote-Desktop است.

۱۷. درباره سرویس SNMP توضیح دهید.

سرویس مدیریت شبکه یکپارچه در شبکه های متوسط و بزرگ است.

از دو بخش تشکیل شده:

الف) SNMP Agent: مسئول جمع آوری اطلاعات بوده و باید روی همه سیستم ها، تک به تک فعال شود.

ب) SNMP Viewer (SNMP Manager): اطلاعات جمع آوری شده توسط Agent ها در کل شبکه را گردآوری و تجزیه و تحلیل میکند.

۱۸. درباره سرویس NTP (NTP) توضیح دهید.

زمان را بین سرویس گیرنده و سرویس دهنده یکسان (Synchronize) می کند. از دو بخش تشکیل شده:

الف) NTP Client (Time Client)

ب) NTP Server (Time Server)

NTP Client در زمان های مشخص با NTP Server ارتباط برقرار کرده و ساعت خود را با ساعت سرویس دهنده تنظیم می کند.

۱۹. Host چیست؟ خصوصیات اصلی هر Host را نام ببرید.

هر سیستمی در شبکه که از TCP/IP برای ارتباط استفاده کند، Host نام دارد.

دو مشخصه Host عبارتند از:

الف) نام: Host Name (TCP/IP Name)

ب) آدرس: Host Address (IP Address)

۲۰. دو قالب برای نامگذاری سیستم ها (Host Name) در شبکه وجود دارد. آن ها را نام ببرید و برای هر کدام مثال بزنید.

✓ اسم مستعار Alias یا Unqualified : مانند Client80 و Narges

✓ FQDN (Fully Qualified Domain Name) : مانند sina.sharif.ac.ir و www.yahoo.com

۲۱. تفاوت قالب اول نامگذاری (Alias) با قالب دوم (FQDN) چیست؟

قالب دوم کامل تر است. معمولاً اسامی قالب اول در محدوده داخلی شبکه ها استفاده شده، نیازی به ثبت ندارند اما اسامی قالب دوم ثبت می شوند. در این صورت چه در محدوده داخلی و چه افراد خارج از شبکه داخلی می توانند از آن ها برای مراجعه به Host استفاده کنند.

۲۲. یک اسم در قالب دوم (FQDN) معمولاً از چه قسمت هایی تشکیل می شود؟

الف) نام یا سرویسی که Host ارائه می دهد یا نقشی که Host بازی می کند. مثل: Web Server : www و Mail server : mail

ب) نام شرکت، سازمان، مجموعه یا شخصی که Host بدان تعلق دارد (Company Name) مثل: microsoft, IRIB, Bank

ج) حوزه فعالیت میزبان (Activities) مثل: com, net, org, gov, mil, edu, ac, info, int, biz, tv, ws, ...

د) وابستگی منطقه ای و محلی اعم از فرهنگی، اجتماعی، ... یا زبان استفاده شده در سایت. (Locality) مثل: Iran : ir و Canada : ca

نکته : FQDN هر چه قدر هم که ناقص باشد، اجزای آن باید از چپ به راست ترتیب یاد شده راعایت کنند و نباید آن ها را جابه جا کرد.

۲۳. در یک FQDN ، Domain Name و Service Name به کدام قسمت ها گفته می شود؟

اگر بخش ابتدایی سمت چپ Service Name است (مانند www) و به مجموع بقیه قسمت ها Domain گفته می شود که شامل نام

شرکت، حوزه فعالیت و کشور می شود.

۲۴. Domain های edu, net, com, ac, gov, prof, inf, org در چه حوزه هایی مورد استفاده قرار می گیرند.

edu: مخفف Education برای مقاصد آموزشی

gov: مخفف Government مربوط به نهاد های دولتی

net: مخفف network به معنی شبکه

com: مخفف Commercial به معنی تجاری

inf: مخفف Information به معنی اطلاعات برای اطلاع رسانی

ac: مخفف Academic برای دانشگاه ها و آموزش عالی

org: مخفف organizations به معنی سازمان و تشکیلات

۲۵. کار SubDomain چیست؟

به زیر مجموعه های یک Domain اصطلاحاً SubDomain می گویند .

معمولاً از SubDomain برای نشان دادن شرکت ها، زیرگروه ها یا ساختارهای فرعی در یک مجموعه بزرگ استفاده می شود.

۲۶. تفاوت Computer Name با Full Computer Name چیست؟

الف) Computer Name (NetBIOS Name): اسم حداکثر ۱۵ کاراکتری است که هنگام نصب OS به رایانه داده می شود که باید در محدوده شبکه داخلی منحصر به فرد بوده و تکراری نباشد .

ب) Full Computer Name (TCP/IP Name): همان Host Name در پروتکل TCP/IP است. ممکن است قالب اول یا دوم باشد.

به صورت پیش فرض در رایانه هایی که عضو Work Group باشند TCP/IP Name دقیقاً برابر با NetBIOS Name است از طرفی چون

NetBIOS Name ساده و تک قسمتی است، TCP/IP Name هم به صورت تک قسمتی برابر با آن می شود یعنی در قالب اول است.

اگر رایانه به عضویت Domain در Active Directory درآید آنگاه TCP/IP Name در قالب دوم می شود.

۲۷. در پروتکل TCP/IP چند نوع آدرس برای IP وجود دارد؟ IPv4 و IPv6

۲۸. TCP/IP نسخه ۶ چیست و چه تفاوتی با نسخه ۴ دارد؟

IPv4، ۳۲ بیتی است و به دسیمال تبدیل شده اما IPv6، ۱۲۸ بیتی است و به هگزادسیمال تبدیل می شود. افزایش فضای آدرس دهی، امنیت بالاتر، پیکربندی خودکار، پشتیبانی قوی و ... از مزایای IPv6 است.

۲۹. استانداردهای اینترنت برای انواع آدرس های IPv4 را نام ببرید.

الف) *Unicast*: برای یک رابط شبکه در یک زیر شبکه اختصاص می یابد (یک مخاطب) برای ارتباط یک به یک استفاده می شود.
ب) *Multicast*: به یک یا چند رابط شبکه واقع در زیر شبکه های مختلف اختصاص می یابد (چند مخاطب) و برای ارتباط یک به چند استفاده می شود.

ج) *Broadcast*: به تمام رابط های شبکه در یک زیر شبکه اختصاص داده می شود (برای تمام مخاطب های یک زیر شبکه) و برای ارتباط یک به همه در یک زیر شبکه مورد استفاده قرار می گیرد.

۳۰. هر آدرس IPv4 دارای دو بخش است. آن ها را نام ببرید.

- ✓ پیشوند زیر شبکه (شناسه شبکه یا آدرس شبکه Network ID): تمام گره های شبکه در یک زیر شبکه باید دارای Subnet prefix یکسانی بوده و پیشوند زیر شبکه باید در کل شبکه های TCP/IP منحصر به فرد باشد
- ✓ ID میزبان (آدرس میزبان Host ID): برای شناسایی گره ها در زیر شبکه به کار میرود و باید در یک زیر شبکه منحصر به فرد باشد.

۳۱. قالب کلی IP Address چگونه است؟

IP Address در مجموع یک عدد ۳۲ بیتی یا ۴ بایتی است که به فرم W.X.Y.Z تنظیم می شود. به طوری که ممکن است از ۴ بایت ممکن یک تا ۳ بایت برای پیشوند زیر شبکه و یا یک تا ۳ بایت برای ID میزبان در نظر گرفته شود.
آدرس های IPv4 در شبکه به وسیله رایانه ها به صورت رشته ای از بیت ها دیده می شود که به صورت ۴ گروه ۸ تایی می باشند از بیت ها، به عنوان مثال 130.1.16.1 به صورت 0000010 00000001 00010000 00000001 دیده می شود.

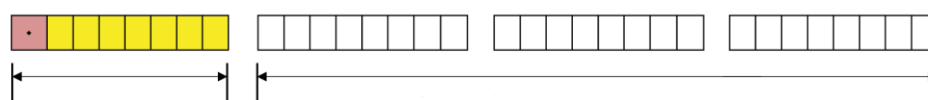
۳۲. کلاس های آدرس در IPv4 را نام ببرید.

کلاس های IPv4 میزان بیت یا بایت اختصاص یافته به پیشوند زیر شبکه و Host ID و تعداد شبکه ها و تعداد میزبان ها را تعیین می کنند. پنج نوع کلاس نام های کلاس A، B، C، D و E داریم.
کلاس A، B و C برای Unicast است.
کلاس D برای Multicast رزرو شده است.
کلاس E نیز برای کارهای آزمایشگاهی رزرو شده است.

۳۳. در مورد کلاس A توضیح دهید.

Network.host.host.host

قالب:



مناسب برای شبکه های: دارای میزبان خیلی زیاد

تعداد بیت زیر شبکه: ۸ بیت (۱ بایت)

تعداد بیت میزبان: ۲۴ بیت (۳ بایت)

تعداد میزبان: تا ۱۶۷۷۷۲۱۴-۲ تا ۲۲۴ میزبان را پشتیبانی می کند. (به جای هر host می توان از اعداد ۱ تا ۲۵۴ را استفاده کرد. در واقع اعداد اختصاص یافته به هر host در قالب کلی ۲^۸ یعنی از ۰ تا ۲۵۵ است ولی اعداد ۰ و ۲۵۵ در شرایط خاصی استفاده می شود).

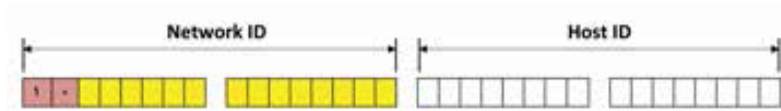
تعداد شبکه: تا ۱۲۶ = ۲-۲^۷ را پشتیبانی می کند. (بیت اول شبکه ثابت است پس ۲^۷ می شود).

مقدار W: ۱-۱۲۶ (اولین بیت سمت چپ همیشه باید صفر باشد پس ما ۷ بیت داریم که می توانند ۱ باشند بنابراین ۲^۷-۱ یعنی ۱۲۷ شبکه خواهیم داشت اما چون عدد ۱۲۷ برای Loop back ذخیره شده فقط می توانیم از ۱ تا ۱۲۶ را برای کلاس A استفاده کنیم).

۳۴. در مورد کلاس B توضیح دهید.

Network.Network.host.host

قالب:



مناسب برای شبکه های: متوسط تا بزرگ

تعداد بیت زیرشبکه: ۱۶ بیت (۲ بایت)

تعداد بیت میزبان: ۱۶ بیت (۲ بایت)

تعداد میزبان: تا $2^{16} - 2 = 65534$ میزبان را پشتیبانی می کند. (تمام صفر و تمام یک استفاده نمی شود)

تعداد شبکه: تا $2^{14} = 16384$ را پشتیبانی می کند. (بیت اول و دوم شبکه ثابت است پس 2^{14} می شود).

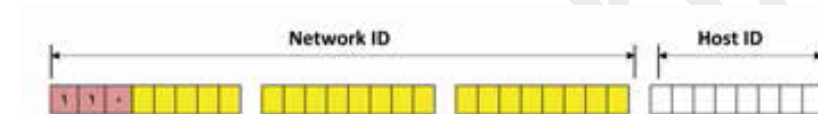
مقدار w: ۱۹۱-۱۲۸ (اولین بیت سمت چپ در Network ID همیشه ۱ و دومین بیت همیشه ۰ است یعنی بایت اول در حالت حداکثری برابر

۱۰۱۱۱۱۱ است (یعنی عدد ۱۹۱) پس اولین بایت یا همان w می تواند اعداد ۱۲۸ تا ۱۹۱ باشد).

۳۵. در مورد کلاس C توضیح دهید.

Network.Network.Network.host

قالب:



مناسب برای شبکه های: کوچک

تعداد بیت زیرشبکه: ۲۴ بیت (۳ بایت)

تعداد بیت میزبان: ۸ بیت (۱ بایت)

تعداد میزبان: تا $2^8 - 2 = 254$ میزبان را پشتیبانی می کند. (تمام صفر و تمام یک استفاده نمی شود)

تعداد شبکه: تا $2^{21} = 2097152$ را پشتیبانی می کند.

مقدار w: ۱۹۲-۲۲۳ (اولین و دومین بیت سمت چپ در Network ID همیشه ۱ و سومین بیت همیشه ۰ است یعنی بایت اول در حالت

حداکثری برابر ۱۱۰۱۱۱۱۱ است (یعنی عدد ۲۲۳) پس اولین بایت یا همان w می تواند اعداد ۱۹۲ تا ۲۲۳ باشد).

جدول ۱-۶ خلاصه کلاس های Unicast

نام کلاس	مقدار w	بخش شبکه	بخش میزبان	آدرس های شبکه	آدرس های میزبان
A	۱-۱۲۶	w	x y z	۱۲۶	۱۶۲۷۷۲۱۴
B	۱۲۸-۱۹۱	w x	y z	۱۶۳۸۴	۶۵۵۳۴
C	۱۹۲-۲۲۳	w x y	z	۲ ۹۷۱۵۲	۲۵۴

۳۶. شماره شبکه یا Network Number (NN) چیست؟

اگر تمام بیت های Host ID برابر ۰ باشد، به آن IP آدرس، NN می گویند. از شماره شبکه یا NN نمی توان برای یک گره استفاده کرد.

۳۷. Broadcast Address (BA) چیست؟

اگر اعداد مربوط به Host ID برابر ۲۵۵ باشد عدد حاصله BA نامیده می شود.

IPv4 آدرس های Broadcast را برای ارسال بسته های اطلاعاتی از یک منبع به تمام سیستم های موجود در همان شبکه استفاده می کند.

اگر کاربری فرمان ارسال اطلاعات را برای 130.25.10.7 صادر کند فقط یک Host یا Node که دارای این آدرس است اطلاعات را دریافت (پردازش) خواهد کرد که اصطلاحاً Unicast گفته می شود ولی اگر فرمان برای 130.25.255.255 صادر شود ، تمام گره های متصل به شبکه های با آدرس شبکه Network ID 130.25 را دریافت و پردازش خواهد کرد . که اصطلاحاً Broadcast نامیده می شود.

۳۸. در مورد کلاس D توضیح دهید.

کلاس D برای Multicast رزرو شده است . IPv4 از آدرس چندپخشی (Multicast) برای ارائه بسته های اطلاعاتی از یک منبع به چند مقصد استفاده می کند.

بیت اول در کلاس D به صورت ۱۱۱۰ است یعنی بایت اول در حالت حداکثری برابر ۱۱۱۰۱۱۱۱ است. (یعنی عدد ۲۳۹) پس در کلاس D اولین بایت یا همان W می تواند اعداد ۲۲۴ تا ۲۳۹ باشد یعنی کلاس D از رنج 224.0.0.0 تا 239.255.255.255 است.

۳۹. در مورد کلاس E توضیح دهید.

برای کارهای آزمایشگاهی (تحقیقاتی) رزرو شده است ۴ بیت اول به صورت ۱۱۱۱ است یعنی بایت اول در حالت حداقلی برابر ۱۱۱۱۰۰۰۰ است (یعنی عدد ۲۴۰) و حداکثر مقدار برابر ۱۱۱۱۱۱۱۱ است (یعنی عدد ۲۴۰) پس اولین بایت یا همان W می تواند اعداد ۲۴۰ تا ۲۵۵ باشد.

۴۰. آدرس های ویژه در IPv4 کدامند؟

✓ آدرس IPv4 نامشخص (0.0.0.0): فقط برای آدرس منبع ، زمانی که گره با IPv4 پیکربندی نشده باشد و با استفاده از سرویس DHCP بخواند IPv4 خود را به دست آورد مورد استفاده قرار می گیرد.

✓ آدرس Loop back: یک گره را برای ارسال بسته ها به خودش فعال می کند.

۴۱. ماسک زیر شبکه (Subnet Mask) چیست؟

ماسک زیر شبکه برای نشان دادن شناسه مربوط به شبکه و همچنین شناسه مربوط به میزبان است. که بیت های هر بخش آن یا همه صفر و یا همه ۱ هستند (یعنی اعداد ۰ و ۲۵۵)

برای تعیین شناسه شبکه ، به ازای هر بخش آدرس شبکه ؛ عدد ۲۵۵ قرار می گیرد و به ازای هر بخش میزبان عدد صفر جایگزین می شود. عدد ۲۵۵ به مفهوم ثابت بودن آدرس IP در یک زیر شبکه و عدد ۰ به مفهوم عدد متغیر ۱ تا ۲۵۴ است.

با استفاده از ماسک زیر شبکه می توان کلاس شبکه را تعیین کرد.

مثال: اگر آدرس یک گره برابر عدد 192.168.1.1 باشد ، Subnet Mask آن به صورت 255.255.255.0 و آدرس IP ، کلاس C است.

۴۲. از کجا بدانیم که NetID آزاد و استفاده نشده کدام است؟

IANA (www.IANA.org) متولی این کار است و مسئولیت تخصیص فضای آدرس ها را به عهده دارد و برای انتخاب NetID به آن مراجعه می کنند. البته برای منطقه اروپا کار را به www.ripe.net تفویض کرده و چون در ایران معمولاً از آدرس های اروپایی استفاده میشود ما به ripe مراجعه و فرم درخواست IP را تکمیل می کنیم و پس از طی تشریفات یک NetID منحصر به فرد در اختیار ما قرار داده می شود.

۴۳. برای آدرس دهی گره های یک شبکه از کدام کلاس استفاده کنیم؟

مرحله اول: تعیین کلاس با توجه به حداکثر تعداد Host.

مرحله دوم: اخذ شماره شبکه معتبر (Valid Network Number یا Valid IP Address)

مرحله سوم: تعیین آدرس اولین Host تا آخرین Host.

مرحله چهارم: تعیین Broadcast Address.

۴۴. تفاوت Valid IP و Invalid IP در چیست؟

IP معتبر (Valid IP): هر IP که ما بتوانیم بر روی NIC و یا کارت شبکه خود تنظیم کنیم.

IP نامعتبر (Invalid IP): شامل IP هایی که در رنج IP های قرار دادی در شبکه قرار نگیرد، مثل ۱۹۲،۱۶۸،۱،۲۵۵

و یا IP هایی مانند Net ID Address، Loopback IP Address، Host ID Address، Broadcast آدرسها که ما نمی توانیم آنها را به هیچ کارت شبکه ای اختصاص دهیم.

۴۵. سگمنت (Segment) چیست؟

Segment به بخشی از شبکه که سیستم های آن دارای یک Network ID هستند اشاره می کند. گاهی هم به بخشی از شبکه که بین تجهیزات شبکه ای مثل دو روتر یا دو سوئیچ قرار دارد گفته می شود.

فصل هفتم - امنیت در شبکه (۱/۵ نمره)

۱. دیواره آتش (Firewall) چیست؟

از مهمترین روش های پیاده سازی امنیت شبکه است که تا حد زیادی از دسترسی غیرمجاز دنیای بیرون به منابع داخلی شبکه جلوگیری میکند. دیواره آتش می تواند یک دستگاه سخت افزاری و یا یک برنامه نرم افزاری و یا ترکیبی از هر دو باشد که اطلاعات ورودی از اینترنت یا شبکه به سیستم را بررسی می کند و به برخی از درخواست ها اجازه ورود به شبکه داده شده و به برخی دیگر اجازه ورود داده نمی شود.

۲. منظور از دیواره آتش داخلی و خارجی چیست؟

به دیواره آتش نرم افزاری، دیواره آتش داخلی و به دیواره آتش سخت افزاری، دیواره آتش خارجی می گویند. دیواره آتش سخت افزاری معمولاً در شبکه های بزرگ مورد استفاده قرار می گیرد. دیواره آتش سخت افزاری در بین شبکه شما و یک شبکه دیگر در سازمان دیگر و یا اینترنت قرار گرفته و سطوح امنیتی را برای شما فراهم می کند. دیواره آتش نرم افزاری نیز برای برقراری لایه امنیتی استفاده می شوند.

۳. با دیواره آتش می توان چه نوع محافظت هایی انجام داد؟

- ✓ دیواره های آتش بخش های مربوط به آدرس مبدأ و مقصد و شماره پورت مبدأ و مقصد شبکه های ورودی را مورد بررسی قرار می دهند پس:
- ✓ دیواره آتش از دسترسی هکرها و برنامه های مخرب (مانند کرم ها) به رایانه شما از طریق شبکه یا اینترنت جلوگیری می کند
- ✓ یک دیواره آتش همچنین می تواند از ارسال برنامه های مخرب از طریق رایانه شما به شبکه نیز جلوگیری کند
- ✓ از طریق دیواره آتش می توان با انجام تنظیمات مربوطه از اجرای یک برنامه خاص جلوگیری کرد.
- ✓ یکی از ویژگی های دیواره آتش شبکه، مدیریت متمرکز است که با استفاده از آن می توان تمام کاربران شبکه را مورد حفاظت قرار داد.
- ✓ علاوه بر حفاظت دسترسی از خارج، میتوان برای محدود کردن دسترسی اعضای شبکه به خارج از شبکه نیز پیکربندی لازم را انجام داد.

۴. آیا وجود دیواره آتش در یک شبکه ضروری است؟ چرا؟

بله چون دیواره آتش از دسترسی غیرمجاز دنیای بیرون به منابع داخلی شبکه جلوگیری می کند.

۵. دیواره آتش به لحاظ سطح استفاده به چند دسته تقسیم می شود؟

- الف) دیواره آتش شخصی یا رومیزی (Desktop or personal firewalls): برای حفاظت از یک میزبان و رایانه متصل به اینترنت بکار میرود.
- ب) دیواره آتش شبکه یا سروری (Network firewalls): برای محافظت از شبکه در برابر حملات طراحی شده است و بالاترین سطح حفاظت را در اختیار کاربران سازمانی قرار می دهد.

۶. آیا می توان از دیواره آتش به جای ضدویروس استفاده کرد؟ چرا؟

دیواره آتش یک سطح حفاظتی را ارائه می کند ولی هرگز عدم تهاجم به سیستم شما را تضمین نمی کند. همچنین دیواره آتش برای مقابله با خطرات شناخته شده طراحی شده است. یک دیواره آتش نمی تواند شبکه و منابع آن را از خرابکاران داخلی محافظت کند. یک دیواره آتش معمولاً نمی تواند از ورود ویروس ها جلوگیری کند چون به جزئیات داده ها توجهی ندارند.

۷. وظایف دیواره آتش را بیان کنید.

مدیریت و کنترل ترافیک شبکه: که به عنوان اولین و اساسی ترین وظیفه دیواره آتش است.

ثبت و گزارش وقایع: مدیر شبکه می تواند با کمک اطلاعات ثبت شده به کنترل ترافیک ایجاد شده توسط کاربران مجاز بپردازد. در یک روال ثبت مناسب، مدیر می تواند به راحتی به بخش های مهم از اطلاعات ثبت شده دسترسی پیدا کند. همچنین یک دیواره آتش خوب باید بتواند علاوه بر ثبت وقایع، در شرایط بحرانی، مدیر شبکه را از وقایع مطلع کند و برای وی اخطار بفرستد.

۸. بهتر است تنظیمات پیش فرض برای دیوار آتش چگونه باشد؟

✓ دیوار آتش فعال باشد.

✓ دیوار آتش برای تمام نقاط شبکه فعال باشد (منزل یا محل کار، مکان عمومی، و یا دامنه).

✓ دیوار آتش برای تمام اتصالات شبکه فعال باشد.

✓ تمام اتصالات ورودی غیرضروری مسدود شوند

۹. کار زبان Exceptions در پنجره Firewall چیست؟

با استفاده از این زبان می توان برای بعضی از برنامه های کاربردی استثناء قائل شد و یا بعضی از درگاه ها را برای تبادل اطلاعات باز گذاشت.

۱۰. چه برنامه های دیوار آتش رایجی وجود دارد؟

Symantec و Zone Alarm, Trend Micro's PC cillin

فصل هشتم - سیستم عامل های شبکه ای (۲/۵ نمره)

۱. ویژگی های مهم سیستم عامل های سرویس دهنده را نام ببرید.

✓ امنیت (Security)

✓ چند وظیفه ای (Multitasking)

✓ پشتیبانی از چندین پردازنده (Multi Processor Support)

✓ قابلیت اطمینان و پایداری (Reliable & Stable)

✓ تحمل خطا (Fault Tolerance)

✓ نرم افزار تهیه نسخه پشتیبان (Backup Utilities)

✓ ابزارهای مدیریتی (Simple & Unified Administrative Tools)

✓ پشتیبانی (Support)

۲. امنیت در سیستم عامل های شبکه ای در چه حوزه هایی بررسی می شود؟

الف (امنیت در حوزه دسترسی به دیسک و فایل سیستم

ب (امنیت در حوزه عملیاتی که کاربرد عام دارند مانند:

✓ تغییر ساعت سیستم

✓ نصب نرم افزار، سخت افزار و انجام تنظیمات

✓ اجرای برنامه ها و تغییر در پارامترهای مربوطه

ج (امنیت در حوزه شبکه و اطلاعات تبادل)

د (امنیت در ورود به سیستم

۳. تفاوت چند وظیفه ای (Multitasking) و چند برنامه ای (Multi programming) را بنویسید.

✓ چند وظیفه ای: توانایی اجرای همزمان چندین برنامه با هم است. سیستم عاملهای خانواده ویندوز چند وظیفه ای هستند. در چند

وظیفه ای یک فرایند می تواند به بخشها یا نچهایی تقسیم شود که می توانند به صورت همزمان اجراء شوند.

✓ سیستم عامل چند برنامه ای، برای جلوگیری از تلف شدن وقت پردازشگر میتواند اجرای چند برنامه را به طور همزمان بر عهده بگیرند.

یعنی در هر لحظه چند برنامه در داخل حافظه موجود هستند به هر کدام از این برنامه ها در مرحله اجرای خاص خود قرار دارند. این

برنامه ها به صورت قسمت قسمت مطابق با احتیاجات ورودی و خروجی خود پردازش میشوند.

۴. تحمل خطا (Fault Tolerance) چیست؟

عدم تأخیر در ارائه سرویس و قدرت تحمل در هنگام بروز مشکل و خطاهای عمدتاً سخت افزاری است .

نکته اصلی در FT این است که هنگام بروز خطا اولاً زمان قطع شدن سرویس بسیار کوتاه بوده، ثانياً عملیات جایگزینی بدون عوامل انسانی و به طور خودکار صورت می گیرد. سپس مسئول سیستم در فرصت مناسب می تواند اشکال ها را بررسی و رفع کند.

۵. System Data و User Data را تعریف کنید.

اطلاعات را در حالت کلی می توان به دو دسته تقسیم کرد:

الف) User Data : اطلاعاتی که کاربر به صورت مستقیم از اهمیت آن آگاهی دارد، مانند انواع پرونده ها یا حتی برنامه های کاربردی که تهیه و نصب کرده است.

ب) System Data : اطلاعاتی که کاربر به طور مستقیم با آن سروکار ندارد بلکه برای سیستم عامل مهم است.

۶. قابلیت های ابزارهای خاص تهیه پشتیبان (مانند NTBackup) چیست؟

الف) به کمک ابزارهایی مانند NTBackup به راحتی از اطلاعات سیستمی نسخه پشتیبان تهیه می شود.

ب) از پرونده هایی که در حال استفاده هستند می توان به راحتی نسخه پشتیبان تهیه کرد.

ج) سیاست های تهیه پشتیبان تنوع بیشتری دارد.

د) می توان انجام عملیات را به طور خودکار در موعد دلخواه زمانبندی کرد.

ه) می توانند از مجوزهای امنیتی (لیست دسترسی افراد به پرونده ها که به اختصار ACL خوانده می شود) نیز پشتیبان گرفته و بازایی کنند.

۷. انواع سیستم عامل های شبکه را نام ببرید.

شرکت مایکروسافت به طور کلی در مورد سیستم عامل، دو دسته محصول ارائه کرده است:

✓ سیستم عامل هایی برای نصب و کاربرد در سرویس گیرنده. (Client Operating Systems): مثل Windows 7

✓ سیستم عامل هایی برای نصب و کاربرد در سرویس دهنده. (Server Operating Systems): مثل Windows 2008 server

۸. حداقل سخت افزار لازم برای نصب سیستم عامل Windows 2008 server چیست؟

✓ پردازنده با سرعت ۲ GHz بالاتر استفاده شود.

✓ حافظه اصلی RAM حداقل ۵۱۲ MB و توصیه می شود که ۲ GB یا بیشتر باشد.

✓ فضای خالی دیسک سخت حداقل ۱۰ گیگابایت ولی بهتر است از ۴۰ گیگابایت بیشتر باشد.

فصل سیزدهم - DNS و روش های تبدیل اسم به (۲ نمره)

۱. کاربرد سرویس DNS در شبکه را توضیح دهید.

سرویس Domain Name System یا سیستم نام دامنه عمل تطبیق نام با آدرس IP را انجام می دهد (در حقیقت DNS، یک سیستم پایگاه داده ای است که نام FQDN را به آدرس IP ترجمه می کند)

۲. انواع اسامی دامنه DNS را نام ببرید.

اسامی در DNS از ساختار درختی سلسله مراتبی به نام فضای نام دامنه (Domain Namespace) تشکیل شده و از ۵ مجموعه استفاده میشود:

الف) دامنه ریشه (Root Domain): در بالاترین محل ساختار درختی و به صورت یک نقطه "." است یعنی تمام اسامی اینترنتی به یک نقطه ختم می شوند. البته در موقع معمولاً در معرفی یک آدرس اینترنتی آن را نمی نویسند، ولی باید توجه داشته باشید که این نقطه بخشی از نام

آدرس اینترنتی است (برخلاف نقطه های دیگر آدرس که به عنوان جداکننده استفاده می شود). مثل: www.sanjesh.org.

ب) TLD (Top Level Domain): دومین بخش از ساختار درختی آدرس و تعیین کننده حوزه فعالیت است و به دو بخش تجزیه می شود:

✓ gTLD (Generic TLD): حوزه عمومی فعالیت و تعیین کننده نوع سازمان و شامل پسوندهایی نظیر .org، .ac، .net، .edu

، .com و ... است.

✓ ccTLD (Country Code): از یک استاندارد دو حرفی برای تعیین کشور (حوزه جغرافیایی) استفاده می شود مانند .jp، .uk، .us

، .ir و ... که به ترتیب مشخص کننده کشورهای ایران، تایوان، عراق، ژاپن، انگلیس و آمریکا و ... است.

گاهی gTLD و ccTLD به صورت ترکیبی استفاده قرار می شوند که ابتدا gTLD و سپس ccTLD قرار می گیرد. (gTLD.ccTLD) به عنوان نمونه دیگر برای مدارس و سازمان های وابسته به آن در کشور ما، از sch.ir استفاده می شود.

(ج) SLD (Secondary Level Domain): دومین سطح دامنه که به صورت منحصر به فرد بوده و می توان آن را به ثبت رساند.

(د) زیر دامنه (Sub Domain): که به شرکت های مربوطه واگذار می شود (در واقع به SLD واگذار می شود)

برای مثال شرکت Microsoft می تواند زیر دامنه Support را ایجاد نماید و کنترل نام زیر دامنه بر عهده شرکت Microsoft خواهد بود.

(ه) نام میزبان (Host Name): مانند برگ درخت در ساختار درختی است که برای شناسایی یک منبع خاص استفاده می شود.

۱۴. فرم کلی اسامی اینترنتی (FQDN) چگونه است؟ Host.subdomain.SLD.TLD.

۱۵. مفهوم هر یک از اجزای آدرس اینترنتی <http://www.tvoccd.sch.ir> را بنویسید.

sch.ir : TLD است که sch = gTLD و ir = ccTLD

tvoccd همان SLD است و www همان Host Name است.

۱۶. اجزای DNS را نام ببرید.

Zone, Name Server, Name Resolution, Resource Records

۱۷. Zone (از اجزای DNS) را تعریف کنید.

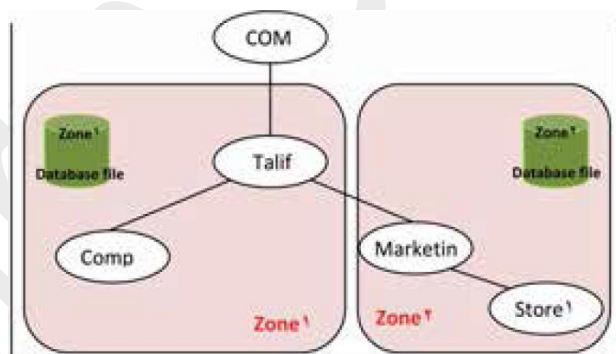
Zone فضای نام دامنه را به چند بخش تقسیم می کند تا مدیریت آنها راحت تر شود. Zone شامل رکوردهای منابع برای اسامی یک منطقه خاص است.

هر Zone شامل یک بانک اطلاعاتی مخصوص به خود است که تمامی اطلاعات مربوط به زیر دامنه های خود را در آن نگهداری می کند.

باید توجه داشت که Zone معادل Domain نیست بلکه از یک یا چند Domain مجاور هم تشکیل شده است.

۱۸. با یک مثال وظیفه Zone را نشان دهید.

قلمروی Talif.com به دو Zone تقسیم شده است. این Zone ها به یک مدیر اجازه می دهند قلمروی Talif و Comp را مدیریت کند و به مدیر دیگر، مدیریت قلمرو marketing و Storel را واگذار می کند.



۱۹. Name Server را تعریف کنید.

به کامپیوتری گفته می شود که سرویس DNS بر روی آن نصب شده و داده های مربوط به یک یا چندین Zone را در خود نگهداری می کند.

در واقع Name Server دارای یک فایل بانک اطلاعاتی اصلی است که به بانک اطلاعاتی Zone ها اشاره دارد.

۲۰. Name Resolution را تعریف کنید.

فرآیندی است که توسط Name Server جهت پیدا کردن کامپیوتر در یک دامنه، با تبدیل اسم به IP و یا بالعکس، انجام می گیرد.

۲۱. انواع درخواستها در DNS را نام ببرید.

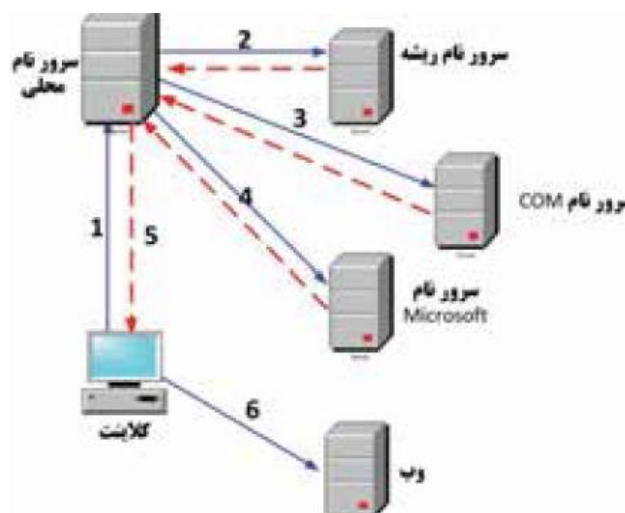
Forward Lookup Query: درخواست های Forward، نام را به IP تبدیل می کنند.

Reverse lookup Query: درخواست های Reverse، IP را به نام تبدیل می کنند.

معمولاً ابزارهای عیب یابی مانند دستور NSlookup از این سرویس برای برگشت گزارش به Client استفاده می کنند.

۲۲. با یک مثال مراحل درخواست های Forward را تحلیل کنید.

- ۱ کلاینت درخواست forward برای `www.microsoft.com` را به سرور محلی خود ارسال می کند.
- ۲ سرور محلی، درخواست را با بانک اطلاعاتی خود مقایسه می کند در صورتی که این درخواست قبلاً ثبت شده باشد و IP آن را یک بار جستجو کرده باشد، IP را به کلاینت بازمی گرداند اما اگر قبلاً این آدرس درخواست نشده باشد برای شناسایی قلمروی Top level آن، درخواست را برای سرور ریشه (Root Server) ارسال می کند. بعد از بازگشت مشخص می کند قلمروی آن `.com` * است.
- ۳ سرور محلی، درخواست را به سرور `com` می فرستد. آدرس تحلیل و در پاسخ `Second level`، `microsoft` را برمی گرداند.
- ۴ سرور محلی این بار درخواست را به سرور `microsoft` ارسال می کند. با توجه به این که این آدرس در سرور `microsoft` ثبت گردیده، این سرور IP آن را برای سرور محلی برمی گرداند.
- ۵ سرور محلی، IP را به کلاینت می فرستد.
- ۶ کلاینت IP را دریافت کرده و در اختیار مرورگر خود قرار می دهد تا کاربر توسط آن به سایت مورد درخواست خود دسترسی پیدا کند.



۲۳. وقتی سرویس دهنده Local, IP درخواست شده سرویس گیرنده را پیدا کرد چرا اسم و IP را در Cache کپی می کند؟

وقتی Name Server فرآیند جست و جو را انجام می دهد برای گرفتن پاسخ به چندین پرس و جو نیاز دارد به همین دلیل برای کاهش بار ترافیک شبکه، نتایج آنها را Cache می کند. این نتایج برای مدت زمان معینی با عنوان TTL (Time To live) نگهداری می شوند.

۲۴. انواع Resource Records (در DNS) را نام ببرید.

بانک اطلاعاتی Zone، اطلاعات خود را به صورت رکورد ذخیره می کند. این رکوردها به صورت های متفاوتی، اطلاعاتی را نگه داری می کنند که مهمترین آنها عبارتند از:

- ✓ رکورد `(A or AAAA) Host`: رکورد نوع A بیشترین نوع رکوردی است که در DNS و برای اختصاص نام دامنه یک کامپیوتر به آدرس IPv4 استفاده می شود. (AAAA برای تعریف رکورد برای کامپیوتر دارای آدرس IPv6 به کار می رود).
- ✓ رکورد Alias `(CNAME)`: به شما امکان می دهد که چندین نام را برای یک کامپیوتر خاص استفاده کنید. برای مثال سرورهای معروفی که به نام `www` نام گذاری شده اند اغلب از نوع CNAME هستند.
- ✓ رکورد PTR `(Pointer)`: رکورد نوع PTR در بخش Reverse برای اختصاص IP به نام دامنه یک کامپیوتر به کار می رود.
- ✓ رکورد `(Service location) SRV`: برای پیدا کردن محل یک سرویس مشخص در دامنه مورد استفاده قرار می گیرد. برنامه های کاربردی مثل AD، توسط این نوع رکورد آدرس سرورهای مرتبط با خود را پیدا می کنند.
- ✓ رکورد: NS از این رکورد برای معرفی Name Server استفاده می شود. این رکورد قابل ایجاد به صورت دستی نیست.

۲۵. فرمائی بنویسید که به وسیله آن بتوان IP یک Host با نام `http://www.tvoccd.sch.ir` به دست آورد.

✓ استفاده از فرمان Ping : `ping www.tvoccd.sch.ir`

✓ استفاده از فرمان nslookup : `nslookup www.tvoccd.sch.ir`

فصل پانزدهم - DHCP Server مقدماتی (۲/۵ نمره)

۱. کاربرد DHCP Server چیست؟

سرویس DHCP پروتکلی است که اجازه می دهد به صورت متمرکز پیکربندی آدرس IP و دیگر تنظیمات TCP/IP میزبان های شبکه به صورت خودکار و پویا انجام شده و کاربران شبکه را از پیکربندی دستی آدرس های IP بی نیاز می کند .
با استفاده از DHCP شما آدرس IP را به یک یا چند میزبان شبکه برای مدت زمانی خاص اجاره می دهید.

۲. مزایای DHCP در ویندوز 2008 سرور را بنویسید.

- ✓ قابل پیکربندی است، یعنی با استفاده از DHCP مشکل تداخل IP ها (IP Conflict) به وجود نمی آید.
- ✓ کاهش زمان مدیریت پیکربندی و امکان تنظیم مجدد آدرس های IP
- ✓ استفاده مجدد از آدرس های IP پس از اتمام زمان مشخص شده
- ✓ کلاینت ها برای استفاده از تنظیمات جدید DHCP سرور نیازی به راه اندازی دوباره ندارند.
- ✓ علاوه بر آدرس Unicast از آدرس Multicast نیز پشتیبانی می کند.

۳. معایب استفاده از DHCP را بنویسید.

- ✓ مشکل امنیتی (رایانه غیر مجاز هم می تواند از سرور درخواست IP داشته باشد).
- ✓ در صورت خرابی سرویس DHCP تخصیص آدرس IP به کلاینت ها با شکست مواجه خواهد شد.
- ✓ افزایش ترافیک شبکه به خاطر ارتباط کلاینت با سرویس دهنده DHCP اتفاق خواهد افتاد.

۴. عملکرد DHCP را در چهار مرحله تشریح کنید.

وقتی که یک کاربر رایانه خود را راه اندازی می کند سیستم عامل آن بعد از بالا آمدن در خواست IP می کند و آن را از سرویس دهنده DHCP دریافت می کند . به طوری که این درخواست و دریافت به ترتیب در طی چهار مرحله تکمیل می شود:

الف) *DHCP Discover*: در این مرحله کلاینت پیام DHCP Discover خود را جهت دریافت IP در شبکه Broadcast می کند .
در این حالت آدرس IP کلاینت به صورت 0.0.0.0 خواهد بود.

ب) *DHCP Offer* (پیشنهاد IP/از طرف سرور DHCP): در این مرحله تمام سرویس دهنده های DHCP از محدوده آدرس IP تعریف شده بر روی خود یک IP انتخاب کرده و به همراه مدت زمانی که قرار است آن IP را در اختیار کلاینت قرار دهد، ارسال می کند.

ج) *DHCP Request* (درخواست برای تایید IP پیشنهادی): کلاینت درخواست کننده پس از دریافت IP های پیشنهادی، اولین IP پیشنهادی را انتخاب کرده و آن را توسط یک Packet در شبکه Broadcast می کند و در آن Packet آدرس سرویس دهنده DHCP را که پیشنهاد او قبول شده است مشخص می نماید.

د) *تأیید درخواست IP با پیام DHCP Ack*: در صورتی که هنوز IP که پیشنهاد شده در محدوده یا رنج IP های سرویس دهنده DHCP وجود داشته باشد و توسط Admin حذف نشده باشد DHCP Server تأیید خود را مبنی بر اختصاص IP به سرویس گیرنده با پیام DHCP ack اعلام می کند .

ولی اگر IP توسط Admin از محدوده مربوطه حذف شده باشد سرویس دهنده DHCP به کلاینت درخواست کننده پیام DHCP Nack را ارسال می کند و Client مجبور می شود که تمام مراحل را دوباره طی کند.

۵. چگونه می توان یک IP خصوصی را برای یک سرویس گیرنده رزرو کرد؟

در Scope (محدوده آدرس دهی DHCP) با گزینه Reservations میتوان آدرس مشخصی را برای کلاینت به طور دائمی اختصاص داد.

۶. چگونه می توان از روی سرویس دهنده IP و Mac Address یک سرویس گیرنده را پیدا کرد؟

عمل دریافت تنظیمات IP از سرور DHCP توسط سرویسی به نام DHCP انجام می گیرد. این سرویس باید بر روی سرویس گیرنده ها فعال باشد . این سرویس به طور پیش فرض در حالت Started قرار دارد و جهت دسترسی به آن می توان از کنسول سرویس ها Services.msc استفاده کرد.