سوالات احتمالی مصاحبه تخصصی

معرفی دستورPing

دستور Ping یا Packet Internet Group از ساده ترین و کاربردی ترین ابزارهای خطایابی قابل دسترس TCP/IP است.این کامند برای تست اتصال یک دستگاه یا سیستم به سیستم های دیگر و تایید فعال بودن سیستم مقصد استفاده می شود.همچنین برای بررسی برقراری ارتباط با یک host در شبکه نیز از این کامند استفاده می شود.

1. -a : تبدیل آدرس IP به نام آن
2. -f : با نوشتن این عبارت ،از قطعه قطعه کردن بسته های ارسالی توسط روترها و getway ها ، جلوگیری می شود.
3. -i : تعیین مقدار یا ظرفیت داده های ارسالی در یک packet ،این مقدار به صورت پیش فرض 32 بایت است و حداکثر تا 65500 بایت می تواند ظرفیت داشته باشد.
4. - n count : تعیین تعداد درخواستهای ارسالی که به صورت پیش فرض 4 است.

معرفی دستور Tracert

Tracert کامندی است که تنها برای انجام یک وظیفه ی اساسی طراحی شده است و آن نیز تعیین مسیری است که بسته های داده برای رسیدن به مقصد طی می کنند.این دستور با دستور ping متفاوت است.درواقع ping به شما می گوید که آدرسی که آن را ping کرده اید فعال یا run است یا خیر و برقراری ارتباط را بررسی می کند اما tracert تک تک روترهایی را که بسته های داده در مسیر با آن برخورد خواهند داشت را برای کاربر نشان می دهد.در واقع زمانی که بسته های داده به مقصد نمی رسند و یا زمان پاسخ دستور ping زمانی نامعقول و طولانی باشد از این دستور استفاده می کنیم.لازم به ذکر است که این کامند هم همانطور که پیشتر ذکر کردم، همانند کامند ping از پروتکل ICMP استفاده می کند.

1. -d : این سوئیچ مانع از تبدیل IP ها به hostname ها می شود.بدون استفاده از این سوئیچ برنامه همچنان کار می کند منتها با تبدیل IP مربوط به هر هاب به hostname آن که این عمل سرعت انجام پروسه را پایین می آورد.
2. -h : با استفاده از این سوئیچ می توان حداکثر تعداد هاب های یک روتر را تعیین کرد.به صورت پیش فرض تعداد هاب هایی که بسته ها برای رسیدن به remote host رد می کنند 30 عدد می باشد.اما در برخی موارد که لازم است این تعداد محدود شوند می توان از این سوئیچ استفاده کرد.
3. -w : مدت زمانی را (براساس میلی ثانیه) که طول می کشد تا یک برنامه منتظر پاسخ بماند را تعیین می کند. در مواقعی که مشکل پهنای باند داریم ، کم یا زیاد کردن این مدت زمان می تواند به ما کمک کند.
4. -j : بدن استفاده از این سوئیچ،بسته ها از مسیری که به صورت پیش فرض برایشان در نظر گرفته شده عبور می کنند.زمانی که از این سوئیچ استفاده می کنید، tarcertهمان مسیری را که برایش تعریف شده دنبال می کند و به کامپیوتر شما برمیگردد.به این option که Loose Source Rooting Option می گویند و کامند آن به صورت زیر اجرا می شود.

معرفی دستور NSLookup

NSLookup یک ابزار مفید برای خطایابی ، تست و رفع اشکال مشکلات مربوط به DNSاست.زمانی که از این کامند استفاهده می کنیم ،نام host و IP آدرس DNS سیستم نشان داده می شود.درصورتی که DNS ، failشود یا اطلاعات نادرست ارائه دهد،سرعت برقراری ارتباط در شبکه کاهش می یابد و client ها دچار مشکل می شوند.

در حالت noninteractive ، تنها یک دستور NSLookup تایپ نمی شود.بلکه گزینه های دیگری نیز در ادامه ی آن تایپ می شود.مثلا اگر برای حل مشکل خود به دنبال یک IP بخصوص می باشید،می توانید پس از تایپ NSlookup ،نام سایتی که به دنبال IPآن هستید را تایپ کنید یا باالعکس یعنی اگر IP را دارید و به دنبال نام سایت هستید نیز می توانید از این حالت استفاده کنید.در جدول زیر،کامندهای دستور NSLookupرا ارائه شده است.در پایان به صورت مختصر تعدادی از سوئیچ های این کامند را بررسی می کنم .

1. Ls : این سوئیچ اطلاعات را برای DNS domain به صورت لیست در می آورد.
2. Server : سرور DNS را تبدیل به سرور به خصوصی که کاربر می خواهد می کند .
3. Ser po[rt] : پورتی که توسط DNS استفاده می شود را تغییر می دهد.
4. Set ret[ry] :تعداد ورودی ها را مشخص می کند.
5. Set ty[pe] :نوع اطلاعاتی که بررسی می شود را تغییر می دهد.

معرفی دستورARP

همانطور که می دانید کارت شبکه یک آدرس سخت افزاری دارد که بر روی آن حک شده است.زمانیکه یک سیستم با سیستم دیگری می خواهد ارتباط برقرار کند،باید IPمربوط به host سیستمی که می خواهد با آن ارتباط برقرار کند را بداند.این روالی است که ما با آن آشنا هستیم اما در پشت پرده اتفاق دیگری می افتد.در واقع سیستم باید برای دریافت و ارسال داده از آدرس سخت افزاری یا MAC Addressاستفاده کند.حال سوالی که پیش می آید این است که یک سیستم از کجا آدرس MAC سیستم های دیگری را که می خواهد از طریق شبکه با آنها ارتباط برقرار کند را پیدا کند.پاسخ چیزی جز ARP نمی باشد.در واقع ARP یا Address Resolution Protocolبرای تبدیل آدرس های منطقی TCP/IP به آدرس های فیزیکی MAC طراحی شده است.حال این پروسه،یعنی تبدیل آدرس منطقی (از لایه ی 3 به آدرس MAC در لایه ی 2) از طریق ارسال broadcasting در داخل شبکه انجام می شود.بدین صورت که کامپیوتر ارسال کننده در داخل شبکه فریاد میزند که " این آدرس IP متعلق به چی کسی است؟من آدرس MAC تورا نیاز دارم ! ". این broadcast به داخل شبکه فرستاده می شود و همه ی host ها ، broadcastهای data را دریافت می کنند .سپس host ی که آدرس IP ارسال شده متعلق به او می باشد در پاسخ ، آدرس MAC خود را می فرستد.در نهایت این پروسه با در اختیار قرار دادن آدرس MACبه کامپیوتری که برای ارسال داده های خود نیازمند آن آدرس بود کامل می شود.

معرفی دستورIpconfig

Ipconfig یکی دیگر از دستورات کاربردی شبکه در سیستم عمل ویندوز است که برای نمایش اطلاعات مربوط به پروتکل TCP/IPاستفاده می شود.این دستور همانند دیگر دستورات شبکه در command prompt اجرا می شود.با استفاده از این دستور شما می توانید تنظیمات دیگری که مربوط به IP می باشند را مشاهده کنید مثل اینکه از کدام سرور DNS استفاده می کنید.با این دستور می توانید MAC addressیا همان آدرس فیزیکی مربوط به کارت شبکه ی خود را نیز مشاهده کنید.اگر پیش از یک کارت شبکه دارید،این دستور اطلاعات مربوط به هر کارت شبکه را به طور جداگانه نمایش می دهد.

DNS Server :

یک server است که hostnameها و آدرس IP آنها را در خود ذخیره دارد . بجاي داشتن server هاي دستي InterNIC همة ISP هاي اين سياره از يک DNS Server بهره مي جويند.

زمانيکه شما در يک hostname تايپ مي کنيد و به مودم (modem) خود مي گوييد که به آن وصل شود ، کامپيوتر شما عملي (action) به نام (DNS LOOKUP) جستجوي DNSانجام مي دهد . بعبارت ديگر کامپيوتر شما از DNS Server درون ISP سرويس دهندة اينترنت آدرس IP مناسب را براي hostname تايپ شده توسط شما درخواست مي کند .

اگر DNS Server درون ISP شما پاسخ را نداند آنرا از یک DNS Server سطح بالاتر دریافت خواهد کرد . و همینطور اگر DNS Server سطح بالاتر جوابي نداشته باشد باز هم به سراغ DNS Server سطح بالاتر خواهد رفت و در نهایت به بالاترین مرحله یعني InterNIC خواهد رسید.

سرور DNS جهت برقراری ارتباط از Port 53 پرتکل های UDP و TCP استفاده می نماید

مفهوم FQDN :

نام دامنه جامع الشرایط یا FQDN یک نام دامنه یا میزبان کامل برای یک رایانه روی شبکهٔ اینترنت است. این نام از دو قسمت تشکیل شده است:

1. Hostname : نام میزبان
2. Domain Name : نام دامنه

مثلاً FQDN یک سرور ایمیل فرضی می‌تواند mymail.cisco-Classes.ir باشد Hostname .در اینجا mymail است و این نام میزبان متعلق به دامنهٔ Cisco-Classes.ir می‌باشد. در این مثال ir یک دامنهٔ سطح بالا یا TLD می‌باشد که دقیقاً مثل ریشهٔ یک درایو روی رایانهٔ شماست.

به همین ترتیب یک نشانی وب می‌تواند FQDN ای مثل www.Cisco-Classes.ir داشته باشد. که این نام می‌تواند، FQDN سرور وب سایت وبنولوزی باشد. در اینجا www نام هاست یا Hostname است و Cisco-Classes.ir نام دامنه محسوب شده که جمعاً www.Cisco-Classes.ir یک FQDN محسوب می‌شود.

زمانی که می‌خواهید به یک سرور متصل شوید، حالا فرقی نمی‌کند که به کدام سرویس آن سرور می‌خواهید متصل شوید، با داشتن Hostname به تنهایی نمی‌توانید این کار را انجام دهید. اما با داشتن FQDN که Hostname قسمتی از آن است، به راحتی می‌توانید با یافتن IP آن سرور به سرور متصل شوید.

از آنجایی که روی اینترنت دو تا سرور یا رایانه می‌توانند Hostname یکسان داشته باشند، اما قادر به داشتن Domain Name یکسان نیستند، پس FQDN یا نام دامنهٔ جامع الشرایط هر سرور فرق می‌کند. پس از نظر اتصال به سرور مشکلی به وجود نخواهد آمد.

اکتیودایرکتوری یا Active Directory :

اکتیودایرکتوری در واقع یک سرویس است که در شبکه امکان ذخیره سازی اطلاعات و استفاده از آن برای کاربران مجاز و مدیران شبکه بر اساس فرآیندی به نام Loginرا ارائه می دهد. این سرویس توسط شرکتی به نام مایکروسافت ارائه داده شده است. تمامی اشیائی که در شبکه وجود دارند بصورت یکپارچه و در قالب یک محل واحد توسط سرویس اکتیودایرکتوری قابل مشاهده هستند. با استفاده از اکتیودایرکتوری ما می توانیم ساختار سلسله مراتبی شبکه را نیز ببینیم . اکتیودایرکتوری می تواند وظایف بسیار زیادی را انجام دهد که برخی از آنها شامل ارائه اطلاعات در خصوص سخت افزارهای متصل شده به شبکه ، پرینترها ، سرویس ها و ایمیل ها ، وب سرور ها و بسیاری دیگر از نرم افزارهایی است که در شبکه مشغول به فعالیت هستند ، می شود. اگر بخواهیم بصورت کلی وظایف اکتیودایرکتوری را تشریح کنیم به شکل زیر می شود :

- نگهداری متمرکز اشیاء شبکه یا Network Objects : هر چیزی که به شبکه متصل شود به عنوان یک شیء در شبکه شناخته می شود.این اشیاء می توانند شامل پرینتر ، نرم افزارهای امنیتی ، گروه ها ، کاربرها و بسیاری دیگر از همین قبیل موارد باشند.برای شناسایی هر یک از این اشیاء در اکتیودایرکتوری مکانیزمی به نام Security Identifier یاSID در نظر گرفته شده است.

- شناسایی Schema : شناسایی هر یک از Object های موجود در شبکه با استفاده از الگویی انجام می شود که در اکتیودایرکتوری تعریف شده است و در اصطلاح فنی به این شناسایی characterization schema گفته می شود. همچنین در اکتیودایرکتوری این اطلاعات موجود در یک شیء است که تعریف کننده نقش شیء در ساختار شبکه است.

- سلسله مراتب یا Hierarchy : اکتیودایرکتوری از یک ساختار سلسله مراتبی تبعیت می کند که بر اساس پروتکل DNS ایجاد می شود . از این ساختار سلسله مراتبی یا موروثی برای شناسایی محل اشیاء در این سلسله مراتب استفاده می شود. بصورت کلی سه سطح در این سلسله مراتب وجود دارد سطوح forest وTree و Domain از این جمله اند. بالاترین سطح از این سطوح سطح Forest است که مدیران شبکه از طریق آن می توانند تمامی اشیاء موجود در کل مجموعه اکتیودایرکتوری را مشاهده و تجزیه و تحلیل کنند. سطح دوم Tree است که خود تشکیل شده از چندین Domain است.

DHCP Server :

DHCP یا Dynamic Host Configuration Protocol مکانیزمی استاندارد است که جهت کاهش پیچیدگی مدیریت آدرس دهی در شبکه طراحی شده است.در بیان خیلی ساده از DHCP میتوان گفت،کلیه کلاینتها جهت ورود به شبکه نیازمند IP هستند DHCP در بر دارنده مجموعه ای IP است که آنها را جهت ارائه دادن به کلاینتهای شبکه مدیریت و نگهداری میکند.مسئولیتهایی مانند اینکه کلیه سیستم ها در بدو ورود به شبکه و ارائه درخواست بتوانند سریع و بدون تاخیر IP دریافت، در شبکه دو سیستم دارای IP یکسان نباشند،سیستم هایی که مدتهاست خاموش و بلا استفاده اند IP خود را در شبکه مشغول نگه نداشته باشد،مدیریت IP هابر اساس کارت شبکه های موجود در شبکه باشد یا بر اساس موارد دیگر و .... از مسئولیتهای این سرویس مهم می باشد .این سرویس به همراه سرویس DNS از جمله سرویس های مهم در شبکه محسوب میشوند که دوشادوش همدیگر سبب ایجاد نظم موجود در شبکه از نظر آدرس دهی میشوند.

سرور DHCP جهت برقراری ارتباط در سمت server از شماره پورت 67 و در سمت client از پورت 68 استفاده میکند . پروتکل هایی که در ارتباط با DHCP کار میکنند شامل IP, BOOTP, UDP, TCP, RARP میباشند

Exchange Server :

اکسچنج سرور یا Exchange Server یکی از سری محصولات محبوب و معروف از سرورهای مایکروسافت است که در شبکه های بزرگ استفاده میشود .

کاربرد اصلی این محصول در اصل استفاده به عنوان یک ایمیل سرور یا همون پست الکترونیک است ، سرویس پست الکترونيك يا سرويس دهنده ايميل در واقع يك نرم افزار كاربرديست كه ايميل ها را از سرويس گيرنده هاي ايميل (Client) و يا سرورهاي پست الكترونيك (Mail Server) ديگر دريافت كرده و بعد آنها را به دست گيرندگان مي رساند. اين سرور پست الكترونيك معمولا شامل فضاي ذخيره سازي پيام ها ، مجموعه اي از قوانين قابل تعريف ، ليستي از كاربران و مجموعه اي از ماژول هاي ارتباطي ميباشد.

پروتکل ICMP

پروتکل icmp یا internet control message protocol جهت خطایابی در کامپیوتر ها ، روتر ها و host ها، بررسی وجود سیگنال و به طور کلی بررسی وضعیت ارتباطی بین روتر و سرور ها مورد استفاده قرار می گیرد.

پروتکل icmp امکانات لازم در خصوص اشکال زدایی ، گزارش خطاها و همچنین مبادله ی اطلاعات محدود در بستر یک شبکه را ارائه می دهد.با توجه به اینکه icmpصرفا مسئول ارائه ی پیغام های کنترلی و گزارش خطاها و نهایتا ارائه ی فیدبک های لازم در جهت تحقق یک وضعیت خاص است ، حاوی هیچ گونه اطلاعاتی مبنی بر اعلام وصول بسته های اطلاعاتی (acknowledgment) نمی باشد.

: POP3

POP3 یک پروتکل استاندارد ایمیل می باشد که برای دریافت ایمیلها از یک سرور راه دور به یک ایمیل کلاینت لوکال مورد استفاده قرار می گیرد. در واقع با استفاده ازPOP3 ، امکان دانلود پیامها از میل سرور به email client مهیا میگردد و شما میتوانید به پیامهای خود حتی به صورت آفلاین و لوکال بر روی سیستم خود دسترسی داشته باشید البته دقت کنید که اگر از طریق POP3به حساب کاربری ایمیل خود متصل شوید، ضمن دانلود پیامها بر روی سیستم شما، تمامی آنها از روی سرور حذف می شوند. با توجّه به این موضوع، اگر صرفاً با یک email clientهمچون Outlook یا Thunderbirdو یا سایر نرم افزارهای مربوطه به حساب کاربری ایمیل خود متصل می شوید و در صورتی که صرفاً از این طریق قصد دارید پیامهای موجود در صندوق پیامهای دریافتی خود را مشاهده کنید، پروتکل POP3 بسیار کار راه انداز، سریع و خوب میباشد. این پروتکل بصورتی ساده طراحی شده که پیامهای قابل دانلود را پس از دانلود توسطemail client ، از روی سرور کاملاً پاک میکند. این موضوع بدین معنی است که بعد از این، دسترسی به پیامها از روی سیستمی دیگر و یا از طریقی به غیر از استفاده از email clientاولیه، امکان پذیر نیست POP3 .به صورت پیشفرض، برای کار خود از دو پورت زیر استفاده میکند :

- **پورت 110** که به صورت پیش فرض و رمز نگاری نشده میباشد.
- **پورت 995** که به صورت رمز نگاری شده و برای برقراری ارتباطات امن POP3 مورد استفاده قرار میگیرد

: IMAP

IMAP مشابه با پروتکلPOP3 ، یکی از پروتکلهای استاندارد ایمیل می باشد که به منظور دسترسی به ایمیلها در یک سرور راه دور از طریق ایمیل کلاینتهای لوکال مورد استفاده قرار می گیرد. هر دو پروتکل IMAP و POP3 در حال حاضر تقریباً توسط تمامی وب سرورها وemail client ها پشتیبانی و قابلیت استفاده دارند .IMAP نیز ویژگی دانلود پیام از میل سرور به email client را برای شما مهیا میسازد، اما بر خلاف POP3 به گونه ای طراحی شده است که پیامها را پس از دانلود از روی میل سرور حذف نمیکند و همچنان بر روی میل سرور پیامها در دسترس قرار خواهند داشت و این بدین معنی است که شما همواره از طریق سیستمهای مختلف و یا سایرemail client ها امکان دسترسی و خواندن پیامها را خواهید داشت. این موضوع بالاخص زمانی که شما دارای چندین سیستم میباشید مثلاً در محلّ کار و منزل و یا از طریق گوشی میخواهید به ایمیلهای خود دسترسی داشته باشید و یا اگر پیامهای خود را از طریق چندین نرم افزار email client دنبال میکنید؛ بسیار حائز اهمیت است و بدین منظور می بایست از پروتکل IMAP استفاده کنید. اما در عوض نسبت به POP3 از فضای دیسک و منابع پردازشی بیشتری هم استفاده میکند چون تمامی پیامها در سرور یا همان INBOX یا (MailBox) ذخیره شده اند. IMAP به صورت پیشفرض، برای کار خود از دو پورت زیر استفاده میکند :

- **پورت 143** که به صورت پیش فرض و رمز نگاری نشده میباشد.
- **پورت 993** که به صورت رمز نگاری شده و برای برقراری ارتباطات امن IMAP مورد استفاده قرار میگیرد

: SMTP

پروتكل SMTP مخفف SIMPLE MAIL TRANSFER PROTOCOL بوده كه از اين پروتكل براي ارسال پيام‌هاي الكترونيكي E-mailاستفاده مي‌شود.

پروتکل SMTP به دلیل محدودیت‌هایی در نگهداری نامه‌ها، معمولا با پروتکل‌های POP3یا یا IMAP استفاده می‌شود که برای کاربران امکان ذخیره نامه‌ها را روی یک سرور یا دانلود آنها را از سرور فراهم می‌کند.

SMTP به صورت پیشفرض، برای کار خود از سه پورت زیر استفاده میکند :

- **پورت 25** که به صورت پیش فرض و رمز نگاری نشده میباشد.
- **پورت 465** که به صورت رمز نگاری شده و برای ارسال پیامهای امن SMTP مورد استفاده قرار میگیرد
- **پورت 2525** زمانی که توسطISP ، پورت 25 سرور بسته شده باشد، پورت 2525معمولاً در سرورها باز میباشد و شما میتوانید از این طریق به صورت رمز نگاری نشده با SMTP پیام خود را ارسال کنید.

مفهوم Virtualization :

این تکنیک با ایجاد چندین ماشین مجازی بر روی یک سخت افزار امکان استفاده بهینه از سخت افزار و سهولت در نگهداری را فراهم نموده و راندمان و مهیا بودن منابع و کاربردها را به طرز چشم گیری بالا می برد. در حال حاضر مجازی سازی جزء لاینفک راه اندازی مراکز داده حساس است و بدون آن، ایجاد مرکز داده شامل خرید و نصب سخت افزارهای زیاد، اتلاف سرمایه گذاری و عدم استفاده از امکانات مهیا شده خواهد بود. در روش قدیمی به ازاء هر کاربرد یا سرویس مورد نیاز سازمان، یک سرور سخت افزاری اختصاص داده می شد. در این مدل منابع داخلی سرور به طور موثر مورد استفاده قرار نگرفته و نگهداری سخت افزارهای متعدد مدیران فنی را با مشکلات مختلف درگیر می کند.
با مجازی سازی چندین کاربرد بر روی یک سخت افزار پیاده سازی می شوند. یک مرکز داده اتوماتیک و مکانیزه، ساخته شده بر پایه مجازی سازی، به تغییرات سریعتر پاسخ داده و با ایجاد قابلیت انعطاف فنی و اجرایی تاثیر گذار ی بیشتری در بازار دارد.
زیرساخت های مجازی شده، منابع و کاربردها (حتی سرورها) را در هر جا و هر زمان که لازم باشد مهیا می کند و مشتریان مراکز داده مجازی شده، از طریق تلفیق منابع و در قالب سیستم های با قابلیت مهیا بودن بالا و با زیرساخت مجازی سازی شده، در هزینه های کلی خود 50 - 70 % صرفه جویی می کنند به عبارت دیگر : استفاده از یک نرم افزار خاص براي جداسازي منابع فيزيكي یک کامپیوتر در قالب کامپیوترهای مجازی (Machine Virtual) را مجازی سازی گویند .سیستم عامل میزبان (Host)، اولین سیستم عامل است و مستقیما روی سخت‌افزار فیزیکی نصب می‌شود. مجازی سازی به وسیله نرم‌افزاری که روی این سیستم عامل نصب می‌شود و کار می‌کند، انجام می‌گیرد. سیستم‌عامل‌های میهمان (Guest)، تحت نرم‌افزار مجازی سازی و روی (VM) Virtual Machine های اختصاصی خودشان اجرا می‌شوند. سیستم عامل‌های میهمان از طریق لایه مجازی سازی به‌منابع ماشین فیزیکی (کامپیوتر اصلی) دسترسی دارند. برای استفاده از مجازی سازی راهکارهای مختلفی وجود دارد که میتوان با توجه به نیاز سازمان (و یا کاربر) هر یک را در جای خودش پیاده کرد. شرکت هایی نظیر VMWare و Microsoft و ... در خصوص مجازی سازی راه کارها و نرم افزارهای مناسبی را ارائه کرده اند.
در کل با استفاده از مجازی سازی میتوان به راحتی از سیستم عامل ها (به همراه تمامی سرویس ها و برنامه هایشان) به صورت مقطعی (Snapshot) و یا به صورت کلی (Clone و Export) نسخه پشتیبان تهیه کرد. برخی از مزایای Virtualization عبارتند از:

1. کاهش هزینه ها (شامل هزینه های مالی - زمان - و ... در کل TCO (آیتم 1733) را کاهش می دهد)
2. افزایش امنیت (مجازی سازی با جدا کردن سیستم عامل هایی که سرویس های مختلفی ارائه میکنند به افزایش امنیت و Fault Tolerance (تحمل خطا) کمک می نماید)

نکته : در خصوص استفاده از مجازی سازی به علت این که خیلی از سرور ها و سرویس ها روی یک سرور فیزیکی قرار میگیرند باید به مورد بک آپ گیری منظم از Virtual Machine ها و همچنین سرور قیزیکی بک آپ نیز توجه خاصی داشت (چرا که در صورت نداشتن سرور بک آپ با از کار افتادن سرور فیزیکی (Host) سازمان تمامی سرویس هایی که سیستم عامل آنها به صورت Virtual Machine بوده است از دسترس خارج خواهند شد)

3. آسان تر شدن جابجایی سرور ها و بک آپ گیری و مدیریت آنها

مفهوم RAID :

به مجموعه ای از هاردها که با الگوریتم ها و روش های خاصی یک دیتا را ذخیره می کنند. هدف از ساخت و ایجادRAID را میتوان به شرح زیر مطرح کرد :

1. امنیت دیتا یا همان تحمل خطا (Fault tolerance)
2. افزایش سرعت Read/Write و در نتیجه افزایشPerformance

انواع RAID :

معرفی RAID 0 :

این نوع با نام striped volumeهم شناخته می شود . در اینجا حد اقل نیاز به دو عدد دیسک داریم . اگر تعداد دیسک ها را n در نظر بگیریم در این روش وقتی دیتایی به دست RAID Controller میرسد آن را به n قسمت تقسیم می کند و هر قسمت را داخل یک دیسک ذخیره می کند.

مزایا : سرعت بسیار بالایی دارد این RAID به Crazy raid معروف است.

معایب : اصلا تحمل خطا ندارد یعنی این که اگر یک دیسک Fail شود کل دیتا ناقص میشود.

کاربرد : در جایی که به سرعت بالا نیاز داریم و مانایی دیتا برایمان اهمیتی ندارد مثلا در Cache server ها و در محیط تست و لابراتور های آموزشی.

معرفی RAID 5 :

برای جبران معایب صفر و یک ساخته شد. مکانیسم عملکرد به این صورت است که کنترلر دیتا را به N-1 قسمت تقسیم میکند و هر قسمت را روی یک دیسک مینویسد وروی دیسک باقیمانده Parity مربوط به آن n قسمت را مینویسد : Parity.یک فرمول به دست آمده از بخش های دیتا است که سایزش اندازه دیگر بخش هاست.مثال: با 3 دیسک رید 5 راه اندازی کرده ایم بلاک A به n-1 قسمت که میشود 2 قسمت تقسیم میشود که میدهد A1 , A2 حالا A1 روی دیسک اول و A2 روی دیسک دوم و Parity(A1A2) روی دیسک سوم ذخیره میشود با تلفیق A1 با Parity به A2 و با تلفیق A2 با Parity به A1 میرسیم. کنترلر برای ذخیره این قسمت ها روی دیسک به صورت چرخشی عمل می کند یعنی Parity را به ترتیب هر بار روی یک دیسک می نویسد.تحمل خطا در این روش یک دیسک است.یعنی اگر دو دیسک همزمان از بین بروند دیتا را از دست میدهیم. اگر یک دیسک از بین برود دو حالت پیش می آید یا اینکه Parity بوده که خب مشکلی برای دیتا ایجاد نمی شود یا اینکه یک قسمت از دیتا بوده که باز با تلفیق سایر قسمت ها با Parityکنترل به آن قسمت می رسد و Recovery انجام میدهد.

کاربرد: رید 5 کاربرد عمومی دارد مثلا برایFile server , Web server

معرفی RAID 6 :

مشابه رید 5 می باشد منتها دوبار Parity دارد. در روش چون دوتا Parity داریم دیتا به n-2 قسمت تقسیم می شود.در این رید نیاز به حداقل 4 دیسک داریم.نحوه ایجاد : Parity یک بار برای قسمت های دیتا Parity محاسبه می کند و یک بار هم برای مجموع Parity قبلی و دیتا Parity محاسبه می کند .چون دو تا Parity داریم تحمل خطا به دو دیسک افزایش می یابد.

آدرس های عمومی(public)

آدرس های عمومی توسط سازمان ICANN صادر میشود و شامل شناسه های شبکه (Network IDs)کلاس بندی شده (دسته بندی قدیمی) و پیشوندهای آدرسی بر پایه روش (CIDR) روش مدرن می باشد. در مورد پیشوندهای آدرسی بر اساس روش مدرن CIDR، مقداراکتت اول در بازه های 1 تا 126 و 128 تا 223 میباشند .البته در این بین پیشوندهای آدرسی از جنس آدرس خصوصی (private) بصورت استثنا وجود دارند که در بخش آدرس های خصوصی به بیان آن ها می پردازیم .
هنگامی که آدرس های عمومی تخصیص داده شد، مسیرها به روترهای اینترنتی اضافه میشوند؛ بنابراین ترافیک به آدرسی که با معادل آدرس عمومی آن تطبیق دارد ارسال میشود .

آدرس های خصوصی(Private)

هر اینترفیسی به آدرسی احتیاج دارد تا در کل شبکه خاص و منحصربفرد باشد .اگر این شبکه اینترنت باشد، هر اینترفیس در یک زیر شبکه متصل به اینترنت به ادرسی احتیاج دارد که در کل اینترنت خاص و منحصربفرد باشد. همگام با رشد اینترنت، نیاز شرکت های متصل به اینترنت برای تخصیص آدرس IP به اینترفیس های موجود در اینترانت خود نیز بیشتر میشود. این موج از نیاز به اینترنت با رشد روز افزون خود ظرفیت تخصیص آدرس های عمومی را بخطر انداخته است .
با تحلیل آدرس های مورد نیاز شرکت ها، طراحان اینترنت به این نتیجه رسیده اند که در بسیاری از شرکت ها، بسیاری از هاست ها نیازی به ارتباط مستقیم به اینترنت ندارند. این دسته از سیستم ها که به مجموعه خاصی از سرویس های اینترنتی مثل دسترسی وب و ایمیل غالبا نیاز دارند، نوعا از طریق Gateway های موجود در لایه Application مثل سرورهای پروکسی و سرورهای ایمیل، سرویس های اینترنت خود را دریافت میکنند. پس به این نتیجه میرسیم که بسیاری از شرکت ها به بازه محدودی از آدرس های اینترنتی برای سرورهای پروکسی، سرورهای ایمیل، روترها، فایروال ها و سیستم های Nat کننده ارتباطات که مستقیما به اینترنت متصل هستند، نیاز دارند .
اما برای آدرس دهی هاست های موجود در شرکت که به دسترسی مستقیم به اینترنت نیازی ندارند، آدرس هایی نیاز هست که با آدرس های عمومی تخصیص یافته در اینترنت یکسان نباشند. برای حل مشکل آدرس دهی، طراحان اینترنتی بخشی از فضای آدرس دهی IPv4 را رزرو کرده اند و نام این محدوده از آدرس ها را فضای آدرس های خصوصی نامگذاری کرده اند. یک آدرس IPv4 در فضای آدرس خصوصی به هیچ عنوان تحت نام یک آدرس عمومی به دیوایسی در اینترنت اختصاص داده نمیشود .ادرس های IPv4 ای که در محدوده آدرس خصوصی قرار دارند به آدرس های خصوصی معروف هستند. به علت ان که آدرس های عمومی و خصوصی با یکدیگر همپوشانی ندارند، آدرس های خصوصی هر با آدرس های عمومی یکی نخواهند شد .
فضای آدرس خصوصی در RFC 1918 با پیشوندهای آدرسی زیر تعریف شده است :

- 10.0.0.0/8 (10.0.0.1 تا 10.255.255.254)
- 172.16.0.0/12 (172.16.0.1 تا 172.31.255.254)
- 192.168.0.0/16 (192.168.0.1 تا 192.168.255.254)

مفهوم NAT :

NAT مانند یک منشی است که درون یک شرکت بزرگ مشغول کار است. این بدان معنی است که منشی شما تمام تماس ها را به شما وصل نمی کند ، مگر اینکه خودتان به آن جواب دهید و از برقراری ارتباط راضی باشید. و کسانی که برای تماس با شما درخواستی را به منشی فرستاده اند نیز ، درخواستشان تا بیکار نشدن شما تعلیق می شود و به محض اینکه توانایی پاسخگویی به ارباب رجوع را پیدا کردید ، می توانید به منشی بگویید که ارباب رجوعی را که تعلیق کرده بودی را آزاد کن و بگذار با من تماس داشته باشد .

کاربران همیشه برای ارتباط با شرکت ، شماره های اصلی را می گیرند که به غیر از انجام این کار هم کار دیگری نمی توانند انجام دهند. یعنی زمانی که با یک شرکتی تماس می گیرید ، در واقع با منشی آن شرکت تماس گرفته اید . و منشی آنجا متناظر با تقاضای شما و انتظار برقراری تماستان با شخص مورد نظرتان ، تماس شما را به شخص مورد نظرتان هدایت می کند که البته همچنان که قبلا گفتیم ، شخص مورد نظر باید توانایی مکالمه به تماس گیرنده را داشته باشد .

این امر نیز برای شبکه های کامپیوتری نیز توسط Cisco گسترش یافت . به این گونه که Network Address Translation یا همان NAT توسط دستگاه هایی مانند Router، Firewall یا کامپیوتر هایی که بین شبکه داخلی و شبکه جهانی قرار می گیرند نیز استفاده می شد NAT . حالت های مختلفی دارد و همچنین می تواند به روشهای مختلفی نیز کار کند که عبارتند از:

Static NAT :

در این روش یک آدرس Private را تبدیل به یک آدرس Public می کند یا به عبارتی یک دستگاه از شبکه داخلی به یک IP از شبکه خارجی تبدیل می شود.

Dynamic NAT :

در این روش یک(pool) رنج از آدرس های Public را به یک رنج از Private IP شبکه داخلی اختصاص می دهیم. در این حالت تعدادIP های داخلی و خارجی باید برابر باشد.

(PAT) Overloaded NAT :

این روش مشابه Dynamic NAT می باشد با این تفاوت که به تعداد دستگاه هایی که می خواهند از اینترنت استفاده کنند نیاز به IP نداریم و تعداد می تواند کمتر و یا حتی یک عدد باشد ، در این روش با استفاده از پورت های یکIP می توانیم چندین هزار IP Invalid را به بیرون از شبکه داخلی هدایت کنیم

کاربردهای اصلیNAT :

- Source NAT: امکان ایجاد ارتباط یک دستگاه که دارای Private IP است را به اینترنت فراهم می کند.
- Destination NAT : امکان ایجاد ارتباط به یک دستگاه که دارای Private IP است را از اینترنت فراهم می کند.

Routing Protocol های Distance-Vector :

پروتکل های Distance Vector از معیار Hop Count یا تعداد روترهای مسیر برای Metric در Routing Table های خود استفاده می کنند. الگوریتم مورد استفاده در اینگونه از پروتکل ها بسیار ساده است و Routing Table با محاسبات ساده ریاضی ایجاد می شود. پروتکل های Distance Vector معمولا برای شبکه های کوچکی که کمتر از 16 عدد Routerدر آنها وجود دارد مورد استفاده قرار می گیرند در واقع این نوع پروتکل ها با کم کردن تعداد Router های مسیر از به وجود آمدن Loop در شبکه یا بهتر بگوییم Routing Loop در شبکه جلوگیری می کنند. این پروتکل ها در وهله های زمانی معین Routing Table های خود را با یکدیگر یکسان سازی می کنند ، یکی از مشکلات الگوریتم های Distance Vectorدر این است که کلیه اطلاعات موجود در Routing Table را حتی با کوچکترین تغییر برای سایر روترهای مجموعه ارسال می کنند و Incremental Update را در واقع پشتیبانی نمی کردند که در نسخه های جدید الگوریتم های Distance Vectorاین مشکل حل شد. الگوریتم های مسیریابی مثل RIPv1 و IGRP از این نوع Routing protocol ها هستند.

Routing Protocolهای Link-State :

در پروتکل های Routing ای که بصورت Link State کار می کنند تفاوت محسوسی با حالت Distanced Vector وجود دارد.الگوریتم های مورد استفاده در این نوع پروتکل ها نسبت به Distanced Vectorها کاملا متفاوت عمل می کند و دارای پیچیدگی های خاص خود می باشد ، در این الگوریتم ها از فاکتورهایی مثل Hop Count ، فاصله ، سرعت لینک و ترافیک بصورت همزمان برای تعیین بهترین مسیر و بهترین cost برای انجام عملیات Routing استفاده می شود.آنها از الگوریتمی به نام Dijkstra برای تعیین پایینترین cost برای Route ها استفاده می کنند. روترهایی که از پروتکل های Link State استفاده می کنند فقط زمانی Routing Table های همدیگر را یکسان سازی می کنند که چیز جدیدی به Routing Table یکی از Router ها اضافه شده باشد. به همین دلیل هم کمترین ترافیک را در هنگام یکسان سازی Routing Table با همدیگر ایجاد می کنند. الگوریتم های مسیریابی مثل OSPF و IS-ISاز این نوع پروتکل های Link State هستند.

Routing Protocolهای Hybrid :

همانطور که از نام این نوع پروتکل Routing نیز پیداست این نوع پروتکل ترکیبی از پروتکل های Distance Vector و Link State است و در واقع مزایای هر یک از این نوع پروتکل ها را در خود جای داده است.زمانیکه صحبت از قدرت پردازشی روترها می شود از قابلیت های Distance Vector ها و زمانیکه صحبت از تبادل Routing Table ها در شبکه می باشد از قابلیت های Link State ها استفاده می کند. امروزه تقریبا همه شبکه های بزرگ در دنیا از پروتکل های Hybrid استفاده می کنند ، الگوریتم مسیریابی مثل EIGRP از انواع پروتکل های Hybrid Routing هستند.

پروتکل RIP :

پروتکل Routing Information Protocol یا RIP یکی از قدیمی ترین پروتکل های مسیریابی Distance Vector است که از پارامتر Hop Countبه عنوان Metricاستفاده می کند .برای اینکه بتواند از به وجود آمدن Loopدر فرآیند روتینگ جلوگیری کند محدودیت تعداد Hopهای مجاز از مبدا به مقصد را به عنوان مکانیزم جلوگیری از Loop قرار داده است. حداکثر تعداد Hopهای مجاز در RIP عدد 15 است . این محدودیت تعداد Hopباعث محدود شدن اندازه شبکه هایی می شود که RIP از آنها پشتیبانی می کند ، یعنی RIP را نمی توان در شبکه هایی که بیش از 15 عدد Hopیا روتر دارند استفاده کرد . Hop Count مقدار 16 به معنی فاصله بی نهایت برای RIP در نظر گرفته می شود به زبانی دیگر یعنی Route مورد نظر از نظر RIP غیر قابل دسترسی در نظر گرفته می شود .با استفاده از مکانیزمهای Split Horizon، Route Poisoningو HoldDown از انتشار اطلاعات Routing اشتباه و پخش شدن چنین اطلاعاتی جلوگیری می کند.

انواع نسخه های : RIP

- Version 1
- Version 2
- RIPng (RIP next generation)

ویژگی های RIP version 1 :

- یک پروتکل Classful است و از VLSM پشتیبانی نمی کند
- دارای امکان Authentication (احراز هویت) نیست
- Advertisementها را به صورت Broadcast ارسال می کند

ویژگی های RIP version 2 :

- در سال 1993 ارائه شد .
- یک پروتکل Classless است و از VLSM پشتیبانی می کند
- امکان Authentication (احراز هویت) را دارد
- Advertisementها را به جای Broadcast به صورت multicast به آدرس 224.0.0.9 ارسال می کند

ویژگی های RIPng :

- پشتیبانی ازIPv6
- از پروتکل UDP با شماره پورت 521 استفاده می کند.

پروتکل OSPF :

پروتکل مسیریابی Open Shortest Path First که به اختصار OSPFنامیده می شود یک پروتکل مسیریابی Link state است که می تواند ترافیک های مربوط به پروتکل IP را مدیریت کند OSPF .نسخه های مختلفی دارد که در حال حاضر از نسخه 2 آن بیشتر استفاده می شود OSPF.بر خلاف برخی پروتکل ها که بصورت انحصاری توسط شرکت ها ارائه می شوند یک پروتکل کاملا جامع و بدون وابستگی به هیچ برند خاصی است ، تقریبا همه روترهایی که در دنیا وجود دارند از پروتکل OSPF پشتیبانی می کنند .پروتکل مسیریابی Open Shortest Path First یا OSPFاز الگوریتم Shortest Path First یا SPF که توسط Dijkstra طراحی شده است برای جلوگیری از بوجود آمدن Routing Loopدر توپولوژی شبکه ها استفاده می کند و به نوع یک شبکه Loop Free ایجاد می کند OSPF .فرآیند Convergenceسریعی دارد و از طرفی قابلیت Incremental Updateرا نیز با استفاده از Link State Advertisement یا LSAفراهم می کند OSPF .یک پروتکل Classless است و به شما این اجازه را می دهد که برای طراحی یک ساختار سلسله مراتبی شبکه از VLSMو Route Summarization براحتی استفاده کنید.

ویژگی هایOSPF :

- IP Sub netting
- Authentication
- Fast Converges
- Partial Update
- Summarization
- Multicast
- IP Protocol 89
- Administrative Distance 110

جدول های OSPF :

- Topology Table
- Neighbor Table

پروتکل ERGRP :

Enhanced Interior Gateway Routing Protocol یا EIGRP یک پروتکل مسیریابی Distance Vector توسعه داده شده است که جزو ساخته های شرکت سیسکو می باشد EIGRP . بر اساس و پایه پروتکل مسیریابی IGRP پیاده سازی شده است و تا حدود زیادی پیاده سازی و تنظیمات آن شبیه به IGRP می باشد EIGRP .را به عنوان یک پروتکل مسیریابی ترکیبی یا Hybrid هم می شناسند و ای به خاطر این است که ویژگی هایی این پروتکل ترکیبی از پروتکل های مسیریابی Distance Vector و Link State است. هم IGRP و هم EIGRP قابلیت ایجاد کردن Load Balancing با استفاده از شش مسیر ارتباطی را دارند و مکانیزم محاسبه متریک یا Metricدر آنها شبیه به هم است. سرعت Convergenceدر پروتکل مسیریابی EIGRP به نسبت IGRP بالاتر است و با توجه به اینکه از Incremental Update پشتیبانی می کند ترافیک و Load کمتری را ایجاد می کند. از دیگر امکانات مهمی که در EIGRP وجود دارد می توان به وجود توپولوژی Routing Loop Free ، پشتیبانی از VLSM، امکان استفاده از Route Summarization ، پشتیبانی از Multicast و Incremental Update و همچنین پشتیبانی از چندین Routed Protocol مختلف از قبیل IP ، IPXو Apple Talk اشاره کرد EIGRP .از الگوریتمی به نام Uses Diffuses Update Algorithm که به اختصار DUAL نامیده می شود

ویژگی هایEIGRP

- تبادل سریع اطلاعات بین روترها
- پشتبانی از VLSM
- ارسال فقط تغییرات جدول مسیریابی بجای کل جدول مسیریابی
- پشتیبانی از شبکه های براساس IP ، IPX، AppleTalk
- استفاده از شماره پروتکل 88
- پشتیبانی از load-balancing به صورت نامتقارن
- ارسال اطلاعات روتینگ به صورت Multicast به ادرس 224.0.0.10
- پشتیبانی از مکانیزم تائید هویت
- خلاصه سازی به صورت دستی یاauto
- AD : EIGRP Summery=5 ، EIGRP Internal=90 ، EIGRP External=170

انواع پیام ها در EIGRP

- Hello : جهت شناسایی همسایه و همچنین به عنوان مکانیزم اعلام فعال بودن
- Update : ارسال اطلاعات مربوط به جدول مسیریابی
- Query : درخواست برای یک مسیر خاص
- Reply : پاسخ به درخواست مربوط به مسیر خاص
- ACK : تایید دریافتUpdate

جدول هایEIGRP

پروتکل EIGRP دارای 3 جدول زیر می باشد :

- Routing : بهترین مسیر در این جدول قرار می گیرد
- Neighbor : شامل لیست همسایه ها
- Topology : دمسیرهایی که می توانند جایگزین بهترین مسیر شوند در این جدول قرار می گیرند

نکته Best Route : (بهترین مسیر) به نام Successor عنوان می شود و با حرف S نشان داده می شود و در جدول Routing قرار می گیرد .

نکته Backup Route : (مسیر پشتیبان) به نام Feasible Successor عنوان می شود و با حروف FS نشان داده می شود و در جدول Topology قرار می گیرد .

نکته Feasible Distance : همان Metric روتر تا مقصد می باشد و با حروف FD نمایش داده می شود .

نکته Reported Distance : نشان دهنده Metric همسایه ما تا مقصد می باشد و با حروف RD نمایش داده می شود .

نکته : زمانی یک Route می تواند FS شود که RD ان Route از FD مسیر Successor کمتر باشد.