تفاوت Post و Get :

تقریبا می‌توانند همه کارهای یکدیگر را انجام دهند ولی بهتر است که Post زمانی بکار برود که ما در حال فرستادن چیزی به دیتابیس هستیم . مثل لاگین کردن که ما پسورد و یوزرنیم را می‌فرستیم. و از get برای گرفتن دیتا از دیتابیس استفاده شود.

تفاوت دیگری که در کلاس گفته نشد. وقتی ما از متد Getاستفاده می‌کنیم، در URLسایت دیتایی که فرستاده ایم دیده می‌شوند:

https://123.com/mypage.php?username=123&password=123

اما برای Postبه این شکل نیست و Urlبه همان شکل

https://123.com/mypage.php

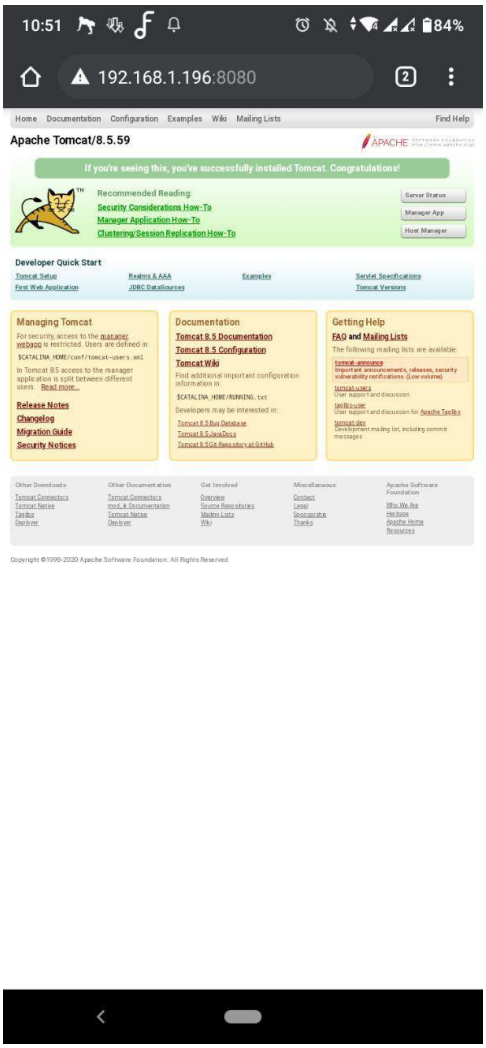
باقی می‌ماند!

Postداده ها را به صورت یک پکیج جداگانه می‌فرستد و از لحاظ امنیتی مناسب تر است.

برای استفاده از Bookmarkها بهتر است از Getاستفاده شود چون Url ایجاد شده توسط آن متفاوت است در صورتی که برای post هیچ تفاوتی بین url اصلی و پس از تائید کردن فرم وجود ندارد.

در متود postبهتر می‌توان داده های متنی و فایل ها را ارسال کرد.

تصوير TOMCAT :



:1-3

Private IP:

ایپی خصوصی فقط به شبکه داخلی که وصل هستید مختص هستش و بیش تر برای ارتباط درون شبکه ای استفاده می‌شود. هر کسی که به اینترنت وصل می‌شود یک آیپی خصوصی و یک آیپی پابلیک دارد. آیپی پابلیک برای وصل شدن به شبکه بیرونی (اینترنت) هست و توسط ISP کنترل می‌شود. آیپی خصوصی را می‌توان از طریق Ipconfig مشاهده کرد اما ایپی پابلیک را باید از طریق اینترنت و یا استفاده از سرویس گوگل پیدا کرد. رنج ایپی های خصوصی

10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, 192.168.0.0 – 192.168.255.255

و بقیه آیپی ها پابلیک هستند.

آیپی های پابلیک همگی یکتا هستند.در صورتی که همان طور که گفته شد آیپی های خصوصی یکتا نیستند و در همه نتورک ها یکسان هستند.

ما از طریق اینترنت نمی‌توانیم به آیپی های خصوصی دسترسی داشته باشیم. امروز Natاین اجازه را به ما می‌دهد که به چند آیپی خصوصی همگی یک آیپی پابلیک منحصر به فرد داده شود. آیپی های پابلیک توسط ISP و IANAکنترل و مدیریت می‌شوند در صورتی که آیپی های خصوصی به همان روتر اختصاص دارد و مدیریت آنها دست روتر است.

آیپی های پابلیک پولی هستند اما آیپی های خصوصی با استفاده از یک روتر به ما داده می‌شوند و لازم نیست پول پرداخت شود.

چون این آیپی ها در V4ها خود ظرفیت امروزی را جوابگو نبودند و این ضعف توسط IPV6 در حال از بین رفتن است که حتی از لحاظ امینتی هم سطح بالاتری دارد.

:2-3

NAT SERVER:

میبایست توسط یک آدرس منحصر به فرد به یکدیگر شناسایی شوند. این آدرس منحصر به یک شماره 32 بیتی می باشد و ترکیب این 32 بیت برای بیش از 4 میلیارد آدرس، به عنوان آدرس IP شناخته می شود.

جهت برطرف شدن این مشکل، یک راه حل موقت به نام Network Address Translation NAT معرفی شد .به دو نوع آدرسIP ، عمومی و خصوصی متصل می گردد.

تا زمانیکه آدرس های خصوصی در شبکه ی داخلی باقی بمانند و وارد اینترنت نشوند، می توانند مورد استفاده ی کاربران قرار گیرند

NATاین امکان را فراهم می کند تا کاربر از آدرس IP خصوصی (private IP)در شبکه داخلی استفاده کند، این نوع از اختصاص آی پی خصوصی معمولا از طریق DHCP انجام می شود.

هنگامی که میزبان شبکه ی داخلی نیاز به برقراری ارتباط با شبکه عمومی (اینترنت) داشته باشد، این همان جایی است که آدرس عمومی به کار گرفته می شود. این آدرس معمولا از یک ISP خریداری شده و قابل رویت هم است.

آدرس IP عمومی (Public IP)منحصر به فرد خواهد بود و هیچ کس دیگری از این آدرس استفاده نخواهد کرد.

هنگامی که میزبان شبکه داخلی با یک آدرس آی پی داخلی نیاز به برقراری ارتباط با خارج از شبکه خصوصی خود را پیدا می کند، از آدرس ip عمومی در دروازه شبکه برای شناسایی خود به سایر نقاط جهان استفاده می کند و این ترجمه ip خصوصی به IP عمومی توسط NAT انجام می گیرد.

به عنوان مثال یک رایانه با Address IP داخلی 192.168.1.10 درخواست ارتباط با یک وب سرور در جایی از اینترنت را دارد، NATآدرس 192.168.1.10 را به آدرس عمومی ترجمه و به عنوان مثال 1.1.1.1 را نشان می دهد.

به طوری که آدرس داخلی در هنگام ارتباط با دنیای بیرون به عنوان آدرس عمومی شناخته می شود. زمانی که وب سرور در اینترنت به این رایانه داخلی پاسخ دهد، باید پاسخ خود را به آدرس منحصر به فرد و قابل رویت در اینترنت یا همان آی پی آدرس عمومی ارسال کند.

درنتیجه نمی توان از آی پی آدرس اصلی 192.168.1.10 استفاده کرد چرا که این ip آدرس خصوصی است و از شبکه های خارجی قابل رویت نمی باشد و می بایست جهت دریافت پاسخ از وب سرور از آدرس عمومی 1.1.1.1 استفاده شود.

سپس NAT از بایگانی خود برای ترجمه بسته های دریافت شده از وب سرور استفاده می کند و متوجه می شود آدرسی که به 1.1.1.1 منتهی شده است مربوط به آدرس شبکه داخلی 192.168.1.10 می باشد و دستگاهی که اطلاعات را درخواست کرده، پاسخ خود را دریافت می نماید.

دو مورد از مزیت های : NAT

1)صرفه جویی در : IP تمامی رایانه ها به آدرس عمومی نیاز ندارند.

2) امنیت : تنها آدرس عمومی دیده می شود و سایر IP ها پشت یک ip عمومی قرار خواهند گرفت در نتیجه رایانه های خصوصی از شبکه ی خارجی پنهان می مانند.

(3-3

آیپی دهی اتوماتیک:

آیپی دهی استاتیک:

آیپی دهی استاتیک Static یا به صورت دستی می باشد . در این روش شما به عنوان مدیر شبکه به صورت دستی آی پی مورد نظر را در سیستم مورد نظر تایپ کرده و به صورت کاملا دستی آن را پیکربندی می کنید .این روش جز در جاهایی که تعداد کمی کامپیوتر وجود دارد , توصیه نمی شود.

آیپی دهی دینامیک:

آیپی دهی دینامیک شیوه بهتر آیپی دهی می باشد .در این روش دستگاهی تحت عنوان DHCP) Dynamic Host Configuration Protocol)در شبکه قرار می گیرد که وظیفه آی پی دهی به صورت خودکار به کامپیوتر های شبکه را برعهده می گیرد . در اینجا نمی خواهیم به شرح این دستگاه بپردازیم ولی برای درک بهتر فرض کنیم که ما در شبکه خود یک سرور DHCP داریم که یک رنج آی پی به او تعلق می گیرد و کلاینت ها به صورت دینامیک به سرور DHCP می گویند که من به یک آی پی نیاز دارم و DHCPیک آی پی از رنج در نظر گرفته شده را به او می دهد.

این روش معمولترین روش آی پی دهی به کلاینت ها در شبکه می باشد . شما به عنوان مدیر شبکه یک سرور DHCP را پیکربندی می کنید و یک رنج آی پی خاص برای او تعریف می کنید و کلاینت ها به نیاز خود می رسند .

در زمانی که DHCPتعریف نشده باشد یا فاصله ارتباط با روتر زیاد باشد:

سیستم عامل , با استفاده از روش APIPA شروع به آی پی دهی به کامپیوتر های درون شبکه میکند .APIPA مخفف کلمه Automatic Private IP Addressing می باشد که در این روش با استفاده از رنج آی پی 169.254.0.0 که به این منظور رزرو شده است سیستم ها آی پی دریافت می کنند

(4

TCP VS UDP:

هر دوی این پروتکل ها یک کار انجام میدهند وآن ارسال داده و پکت ها بر روی بستر شبکه به مقصد میباشد با این تفاوت که وقتی شما اطلاعات خود را بر مبنای پروتکل TCP ارسال میکنید از زمان ارسال تا رسیدن اطلاعات به مقصد صحت ارسال ان بررسی خواهد شد تا اطلاعات بصورت کامل و سالم به دست گیرنده رسیده باشد ولی در پروتکل UDP اینطور نیست پروتکل صرفا وظیفه

ارسال را بعهده داشته و دیگر برایش مهم نیست که این اطلاعات به دست گیرنده رسیده یا نه و یا اگر رسیده سالم رسیده یا ناقص.

پروتکلTCP:

1.مبنا connection-oriented میباشد

2.از این پروتکل در جاهایی استفاده میشود که نیاز به اطمینان خاطر بالا از ارسال سالم اطلاعات میباشد

3.پروتکل های دیگر از قبیل HTTP, HTTPs, FTP, SMTP, Telnet نیز از مزایای این پروتکل بهره مند میشوند

4.بخاطر بررسی ارسال اطلاعات سرعت ارسال نسبت به UDP کمتر میباشد

5.این پروتکل سالم و کامل رسیدن اطلاعات شما به مقصد را گارانتی میکند

6.در صورت بروز خطا در ارسال اطلاعات این پروتکل اقدام به ارسال مجدد اطلاعات خواهد نمود

7.بعد از ارسال موفقیت امیز اطلاعات پیام موفقیت از طرف سیستم گیرنده دریافت خواهد شد

پروتکل :UDP

1.مبنا connection-less میباشد

2.پروتکل هایی از قبیل DNS, DHCP, TFTP, SNMP, RIP, VOIP از خدمات این پروتکل بهره می برند

3.از این پروتکل در سرور های گیم و یا سرورهای کوچک که قرار نیست کارهای مهمی انجام دهد استفاده میشود

4.هیچ گارانتی مبنی بر سالم و کامل رسیدن اطلاعات شما وجود ندارد

5.با توجه به اینکه در این پروتکل نیازی به بررسی و کنترل ارسال اطلاعات نیست سرعت ارسال از TCP بیشتر میباشد

6.در صورت بروز خطا در ارسال اطلاعات هیچ گونه ارسال مجددی وجود ندارد

7.هیچ نوع پاسخی از ماشین دریافت کننده مبنی بر دریافت موفقیت امیز اطلاعات ارسال نخواهد شد

پروتکل های ایمیل:

تعامل بین سرورها و نرم افزارهای ایمیل به وسیله پروتکل های ایمیل انجام می شود. سه پروتکل معمول مورد استفادهPOP ، IMAPو MAPI هستند که بسیاری از نرم افزارهای ایمیل تحت یکی از این سه پروتکل عمل می کنند (البته برخی آنها از بیش از یکی را به عهده دارد) ولی چرا ما باید از وجود آنها اطلاع داشته باشیم؟ مهم ترین دلیل آن انتخاب پروتکل مناسب و پیکربندی صحیح حساب ایمیل برای انجام کارهاست.

پروتکل اداره پست) یا POP که در حال حاضر نسخه ۳ آن در دسترس است (به نرم افزار ایمیل اجازه می دهد ایمیل را از یک سرور از راه دور بازیابی کند.

پروتکل دسترسی به پیغام اینترنتی) یا IMAP با نسخه کنونی ۴ (به نرم افزار موضعی ایمیل امکان دسترسی به پیغام های ایمیلی را که در یک سرور از راه دور قرار دارند فراهم می کند. یک پروتکل مرتبط به نام SMTP نیز وجود دارد که درباره آن توضیح خواهیم داد.

واسط برنامه نویسی نرم افزارهای کاربردی پیغام رسانی (MAPI) یک پروتکل مختص به مایکروسافت برای ایمیل است که می تواند به وسیله Outlook برای برقراری ارتباط با Microsoft Exchange (نرم افزار سرور ایمیل مایکروسافت) استفاده شود.

این پروتکل کارکردی بیشتر از IMAP ارائه می کند، ولی متاسفانه از آنجا که این پروتکل اختصاصی است، تنها برای تعامل های بین Outlook و Exchange کارایی دارد.

Default Port:25

کدهای HTML:

OK :200

پروسه به خوبی انجام شده است.

:401

این خطا زمانی رخ می دهد که کاربری بدون آگاهی از اطلاعات لاگین (نام کاربری و رمز عبور مربوطه) بخواهد به منبع یا صفحه ای که توسط HTTP Authentication محافظت شده دسترسی داشته باشد.

:403

به این معنی است که درخواست معتبر و بدون وجود مشکل بوده (مثلا syntax درخواست صحیح است) ولی سرور درخواست را به دلیل اینکه کاربر دسترسی های لازم به جهت استفاده از منابع مربوطه ندارد، رد می کند.

:500

خطا 500 یک خطا کلی است که نشان می‌دهد که مشکلی در سرور وجود دارد اما سرور نمی‌تواند مشکل دقیق را پیدا کند.