**پروتکل SMB چیست و چگونه کار می کند؟**

SMB مخفف کلمه ی Server Message Block می باشد. این نوع پروتکل به کامپیوترهای موجود در شبکه این امکان را می دهد تا فایل ها را در یک شبکه یا دامین به اشتراک بگذارند. این موضوع مانند این است که کاربر از هارد لوکال استفاده کند.این پروتکل به کاربر یا برنامه ها اجازه دسترسی به فایل های موجود در سرور ریموت و سایر منابع را می دهد.پروتکل SMB یک پروتکل ارتباطی مبتنی بر سرور – کلاینت و پاسخ – درخواست است که برای اشتراک گذاری دسترسی به فایل‌ها، پورت های سریال و سایر منابع موجود در شبکه از آن استفاده می کنند.برای مثال کامپیوتری که به شبکه ی ویندوزی متصل است می تواند با پرینتری که به یک کامپیوتر دیگر در شبکه وصل است، پرینت بگیرد.  البته این روش زمانی قابل استفاده است که هر دو سیستم از پروتکل SMB استفاده کرده باشند.همان طور که گفته شد پروتکل SMB را با عنوان پروتکل پاسخ – درخواست نیز می شناسند. این یعنی این پروتکل چندین پیام را بین کلاینت و **[سرور](https://meftah.com/products/server)** منتقل می کند تا سیستم بتواند ارتباط را برقرار کند.

کلاینت ها می توانند فایل های که روی ریموت سرور موجود هستند را باز کند، بخواند، ایجاد، منتقل و به روز رسانی کند. به علاوه می تواند به عنوان یک پروتکل انتقالی برای IPC نیز کار کند.IPC این قابلیت را دارد تا چندین کاربر بتوانند به صورت همزمان درخواست خود را ارسال کنند.پروتکل های SMB برای اولین بار توسط IBM طراحی و عرضه شدند. این پروتکل ها در کامپیوترهای ویندوزی قابل استفاده بوده و به علاوه با استفاده از نرم افزاری به نام Samba در پلتفرم های دیگر مانند یونیکس و مک نیز قابل استفاده هستند.بنابراین تمامی کامپیوترها با هر نوع سیستم عاملی می توانند فایل ها و پرینترها در شبکه به اشتراک بگذارند.بنابراین می توان گفت که در دفتری که شبکه ی ویندوز داشته و گرافیست آن از مک و متخصص آی تی آن از سیستم یونیکس استفاده می کند هیچ گونه مشکلی نخواهد داشت. به طور کلی کلاینت ها و سرورها ممکن است از هر نوعی از SMBها استفاده کنند.

SMB موجب می شود تا ترافیک بالایی در شبکه ایجاد شود و برای حل این مشکل می توانید از DSN و یا WINS استفاده کنید، البته این نوع روش ها رایج نیستند.

## **پروتکل SMB چگونه کار می کند؟**

پروتکل SMB در لایه ی هفتم مدل OSI یعنی لایه اپلیکیشن جای دارد بنابراین پروتکل های سطح پایینی برای انتقال دارد. پروتکل های لایه ی انتقال معمولا از این نوع پروتکل استفاده می کنند.امروزه برای TCP/ IP هایی که برای ارتباط دستگاه ها از SMB پشتیبانی نمی کنند باید روی پروتکل های انتقال از NetBIOS استفاده شود.همان طور که می دانید پروتکل SMB یک پروتکل سرور کلاینی بوده و مجموعه ای از بسته های داده می باشد که هر کدام از این بسته ها شا مل درخواست است که کلاینت می فرستد و یا پاسخی که به سرور می فرستد. این بسته های صورت های مختلفی دارند.یکی از این بسته ها، بسته Session می باشد که این بسته اتصالی را به وجود آورده و قطع کرده تا از این طریق منابع سرور بتوانند به اشتراک گذاشته شوند.

بسته های دیگر بسته دسترسی فایل هستند که فایل های روی سرور ریموت را دستکاری کرده و قابل دسترسی می کنند.

بسته دیگر بسته ی پیغام عمومی است، این بسته داده ها را برای صف های پرینت ارسال کرده و همچنین داده های وضعیت صف پرینت را فراهم می کند.

بعضی از بسته های پیغام ها گروه بندی می شوند و این بسته ها در یک انتقال ارسال می شوند. این موضوع باعث می شود تا زمان تاخیر کمتر شده  پهنای باند نیز بیشتر شود. این فرایند Packet Batching نام دارد.

## **امنیت SMB**

مباحث امنیتی تعبیه شده در پروتکل SMB دارای دو سطح است که کاربر و اشتراک گذاری هستند. اشتراک گذاری  فایل یا پرینتری که کلاینت ها می‌توانند به آن دسترسی یابند.

### **احراز هویت سطح کاربر**

کلاینتی که قصد دارد به اشتراک گذاری روی سرور دسترسی داشته باشد باید دارای نام کاربری و رمز عبور باشد. پس از اتمام احراز هویت کاربر می تواند به منابع دسترسی داشته باشد.این سطح امنیتی موجب می شود تا ادمین ها بتوانند کاربران و گروه های مجاز به دسترسی را تعیین کنند.

### **احراز هویت سطح Share**

دسترسی به share توسط پسوردی که مخصوص آن است قابل کنترل است. برخلاف سطح قبلی در این سطح شما نیازی به احراز هویت و وارد کردن نام و پسورد ندارید.در این دو سطح امنیتی رمز عبور قبل از این که ارسال شود رمز نگاری می شود. پروتکل SMB از دو نوع رمز گذاری به نام NTLM و LAN Manager استفاده می کند.

### **Dialect های پروتکل SMB**

Dialectها مجموعه ای از بسته ها در غالب پیغام هستند که نسخه ای از پروتکل را تعریف می کنند. پروتکل CIFS یکی از این Dialectها از نوع SBM می باشد.  این دو نوع پروتکل روی VMS و همچنین نسخه های یونیکس و سایر سیستم عامل ها قابل دسترسی هستند.کلاینت های ویندوزی معمولا قابلیت پشتیبانی  از 6 دیالکت و بیشتر SMB را دارند. این کلاینت ها بر این که بتوانند ارتباط را با سرور برقرار کنند از SMB استفاده می کنند.شما باید دیالکتی را انتخاب کنید که بالاترین سطح کارایی را داشته باشد و هم کلاینت و سرور از آن پشتیبانی کنند. این فرآیند negotiating the dialect نام دارد.استفاده از پروتکل های smb موجب می شود تا قابلیت ها بهبود یافته، امنیت و کارایی نیز افزایش پیدا کند. در ادامه چند دیالکت مهم را بررسی می کنیم.

(SMB 1.0 (1984: ایجاد شده توسط آی بی ام برای به اشتراک گذاری فایل در DOS. قفل اپورتونیستی (OpLock) را به عنوان یک مکانیزم ذخیره سازی برای مشتری طراحی کرده تا ترافیک شبکه را کاهش دهد.

(CIFS (1996: زبان SMB توسعه یافته مایکروسافت که در ویندوز ۹۵ عرضه شده است. پشتیبانی از اندازه فایل های بزرگتر، انتقال مستقیم بر روی TCP / IP و لینک های نمادین و لینک های سخت افزوده شده است.

(SMB 2.0 (2006: با ویندوز ویستا و ویندوز سرور ۲۰۰۸ منتشر شده است. برای بهبود عملکرد، مقیاس پذیری و انعطاف پذیری افزایش یافته و پشتیبانی از شتاب WAN افزوده شده است.

(SMB 2.1 (2010: با ویندوز سرور ۲۰۰۸ R2 و ویندوز ۷ معرفی شده است. مدل لیزینگ مشتری oplock جایگزین OpLock برای افزایش ذخیره و بهبود عملکرد است. به روز رسانی های دیگر شامل پشتیبانی از حداکثر انتقال حداکثر (MTU) و بهبود بهره وری انرژی است که مشتریان را با فایل های باز از یک سرور SMB به حالت sleep فعال می کند.

(SMB 3.0 (2012: در ویندوز ۸ و ویندوز سرور ۲۰۱۲ عرضه شده است. برای بهبود در دسترس بودن، عملکرد، تهیه نسخه پشتیبان، امنیت و مدیریت، چندین نسخه قابل ارتقا وجود دارد. قابل توجه ویژگی های جدید شامل SMB Multichannel، SMB مستقیم، شکستن شفاف دسترسی مشتری پشتیبانی از VSS از راه دور، رمزگذاری SMB و بیشتر.

(SMB 3.02 (2014:در ویندوز ۸٫۱ و ویندوز سرور ۲۰۱۲ R2 معرفی شده است. شامل به روز رسانی عملکرد و توانایی به طور کامل غیر فعال کردن پشتیبانی CIFS / SMB 1.0، از جمله: حذف باینری مربوط.

(SMB 3.1.1 (2015: با ویندوز ۱۰ و ویندوز سرور ۲۰۱۶ منتشر شده است. پشتیبانی از رمزنگاری پیشرفته، یکپارچگی قبل از شناسایی برای جلوگیری از حملات در یک سو مردانه و شمشیر گویش خوشه ای، از سوی دیگر به روز رسانی ها اضافه شده است. در سال ۲۰۱۷ حملات WannaCry و Petya ransomware یک آسیب پذیری در SMB 1.0 را برای بارگیری نرم افزارهای مخرب بر روی مشتریان آسیب پذیر و گسترش آن در بین شبکه ها مورد استفاده قرار دادند. مایکروسافت پس از آن یک پچ را منتشر کرد، اما متخصصان توصیه کرده اند که کاربران و مدیران گام دیگری برای غیر فعال کردن SMB 1.0 / CIFS در تمام سیستم ها داشته باشند.