فصل هشتم

پشتیبانی دسترسی از راه‌دور

مباحث این فصل در دو قسمت "مقدماتی" و "حرفه‌ای‌تر شوید" ارائه شده است. در ابتـدای هـر فصل به بررسی مطالب ساده‌تری پرداخته شده که در استاندارد 70-687 وجود دارد و در قسـمت "حرفه‌ای‌تر شوید" مباحث تخصصی‌تری مربوط به پشتیبانی از نصب ویندوز ۸٫۱ که در استاندارد 70-688 وجود دارد پرداخته شده است. لذا توصیه می‌شود ابتدا قسمت مباحث ابتدایی را مطالعه کرده و در صورتی‌که به مطالب تسلط پیدا کردید قسمت "حرفه‌ای‌تر شوید" را مطالعه نمایید.

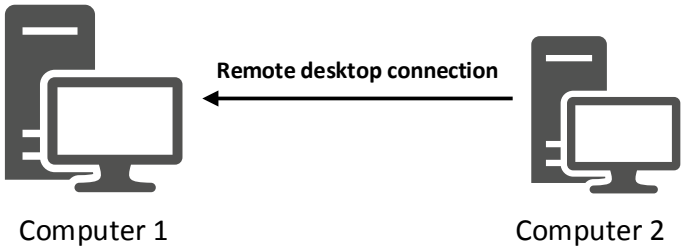
پروتکل Remote Desktop یا RDP

این پروتکل امکان دسترسی از راه‌دور کاربران به دسکتاپ و برنامه‌های کاربردی درون آن را فراهم می‌سازد. در واقع شما می‌توانید از راه‌دور به سرورهای درون سازمان Remote Desktop بزنید و با برنامه‌های کاربردی درون آن کار کنید. در کتاب ویندوز سرور۲۰۱۲ به‌صورت کامل با Remote Desktop آشنا خواهیدشد. دراین‌جا فقط با فعال‌سازی و اتصال Remote Desktop ساده آشنا خواهید شد. برای آشنایی با تنظیمات Remote Desktop تمرین ۸- ۱ را انجام دهید.

تمرین ۸- ۱

عنوان: پیکربندی Remote Desktop و نحوه‌ی اتصال به آن

شرح : در این تمرین Remote Desktop را برروی کامپیوتر۱ فعال کرده و از طریق کامپیوتر۲ به دسکتاپ کامپیوتر۱ متصل خواهیم شد.



مراحل تمرین:

گام۱ فعال‌سازی Remote Desktop برروی کامپیوتر۱

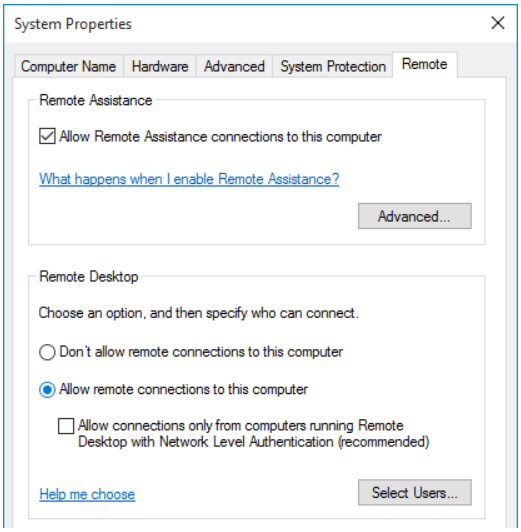
گام۲ اتصال از کامپیوتر۲ به کامپیوتر۱ ازطریق Remote Desktop

گام۱ فعال‌سازی Remote Desktop برروی کامپیوتر۱

۱. برروی This PC راست‌کلیک کرده و گزینه Properties را انتخاب کنید.

۲. از قسمت سمت چپ برروی Remote setting کلیک کنید.

۳. در پنجره باز شده مطابق با شکل ۸- ۱گزینه Allow remote connection to this computer را انتخاب و برروی دکمه OK کلیک کنید.

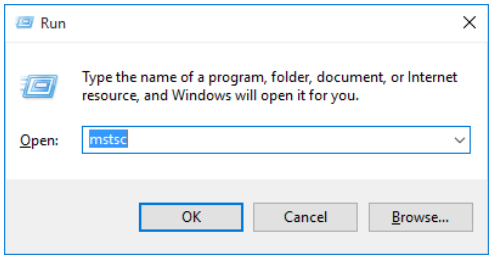


شکل ۸– ۱

گام۲ اتصال از کامپیوتر۲ به کامپیوتر۱ از طریق Remote Desktop

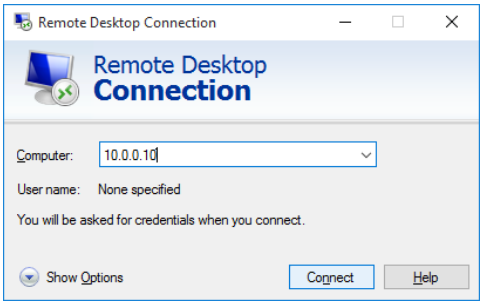
۱. وارد کامپیوتر ۲ شوید.ابتدا مطمئن شوید که کامپیوتر ۱ را Ping می‌کنید.

۲. حال در Run کلمه mstsc را وارد کرده و برروی دکمه Ok کلیک کنید.



شکل ۸– ۲

۳. در پنجره باز شده آدرس IP کامپیوتر۱ را وارد کرده و برروی دکمه Connect کلیک کنید.

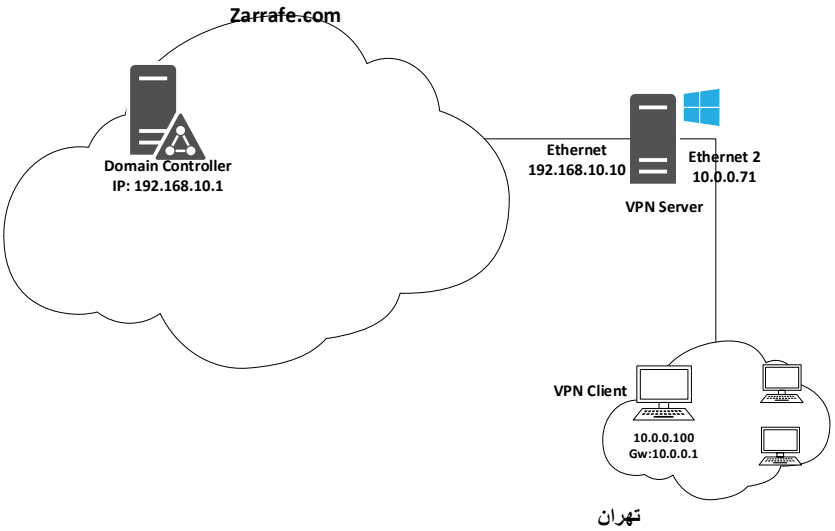


شکل ۸– ۳

۴. در پنجره ظاهر شده برروی دکمه yes کلیک کنید.
۵. در پنجره ظاهر شده نام‌کاربری و رمزعبور کامپیوتر ۱ را وارد کرده. پس از مدتی دسکتاپ کامپیوتر ۱ را مشاهده خواهید کرد.

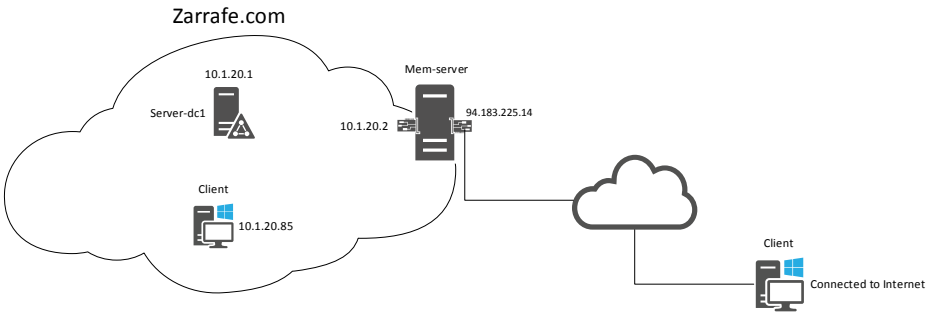
شبکه‌خصوصی‌مجازی یا Virtual Private Network

یکی از موارد مهم و قابل توجه در استفاده از شبکه‌ها، قابلیت اتصال از راه‌دور می‌باشد. به نحوی که کاربران بتوانند کارهایشان را بدون وجود محدودیت جغرافیایی انجام دهند. این امر با پیاده-سازی یک ارتباط امن و خصوصی (یا VPN) اتفاق افتاده و یک استاندارد را تشکیل می‌دهد. از آن‌جایی که VPN یک استاندارد بوده پس درنتیجه محدودیتی به پلتفرم نداشته و برروی تمامی دستگاه‌ها قابل استفاده می‌باشد. یکی از مواردی که همواره مدنظر است برقراری امنیت این ارتباط می‌باشد و برای این منظور راه‌کارهای زیادی ارائه داده‌شده‌است. در ادامه قصد داریم تا انواع پروتکل‌های VPN و نحوه امن‌کردن این‌دسته از ارتباطات را مورد بررسی قرار دهیم.
برای راه اندازی VPN نیاز به یک سرور VPN و پیکربندی کلاینت‌های VPN می‌باشد.
در شکل ۸- ۴ شبکه سازمان زرافه وجود دارد. به‌وسیله راه اندازی VPN این امکان فراهم می-شود تا کاربران بتوانند از منزل به سرویس‌های درون شبکه محلی دسترسی داشته‌باشند و دورکاری انجام دهند. برای این منظور یک سرور VPN درلبه سازمان قرار داده می‌شود. این سرور از یک سمت به شبکه محلی و از سمت دیگر به شبکه اینترنت متصل است و برروی آن تنظیمات سرور VPN انجام شده است.
کارمندان از بیرون‌سازمان با ایجاد یک اتصال VPN می‌توانند به سرور VPN متصل شوند. پس از اتصال سیستم کلاینت یک IP از محدوده شبکه LAN محلی به خود اختصاص داده این نکته قابل توجه است که در واقع کارمندان در شبکه ای بیرون از سازمان قرار دارند اما از لحاظ منطقی مثل اینکه کلاینت در شبکه محلی قرار دارد.
همچنین پس از برقراری VPN یک تونل منطقی بین کلاینت و سرور VPN ایجاد می‌شود و کلیه ترافیک‌ها از طریق این تونل رد و بدل می‌شوند و افراد عمومی به ترافیک های درون این تونل دسترسی نخواهند داشت.
همچنین ازطلاعات درون این تونل می‌توانند رمزگذاری بشوند یا نشوند. در ادامه به بررسی پروتکل های VPN و چگونگی عملکرد و پیاده‌سازی آن‌ها خواهیم پرداخت.



شکل ۸– ۴

مثال دیگر از استفاده VPN زمانی است که شما بخواهید کارمندان از منزلشان یا در هنگام ماموریت از طریق اینترنت که یک بستر عمومی است به صورت ایمن به شبکه داخلی متصل شوند برای این منظور نیز VPN استفاده خواهد شد. در شکل ۸– ۴ قابل مشاهده است که کلاینت از درون اینترنت به سرور VPN که در لبه شبکه محلی وجود دارد متصل شده است بنابراین یک تونل بین کلاینت و سرور VPN ایجاد می‌شود که اصطلاحاً به آن شبکه خصوصی‌مجازی گفته می‌شود.



شکل ۸– ۵

مثال دیگر از استفاده VPN زمانی است که شما از VPN به عنوان فیلترشکن استفاده می‌کنید. در آن زمان یک شبکه خارج‌از ایران وجو دارد و فیلتر نمی‌باشد، شما از شبکه ای درون ایران یک اتصالVPN به شبکه خارج از ایران می‌زنید یک تونل بین شما و سرور VPN آن شبکه ایجاد می‌شود؛ و کامپیوتر شما یک آدرس IP از محدوده شبکه خارج از ایران می‌گیرد مثل این‌که شما از شبکه خارج از ایران به اینترنت متصل هستید.

پروتکل‌های VPN

پروتکل‌هایی که در ویندوز ۸,۱ برای استفاده از VPN مورد استفاده قرار می‌گیرد دامنه وسیعی دارد. در ادامه تمامی پروتکل‌هایی که برای VPN مورد استفاده قرار می‌گیرند را بررسی خواهیم کرد.

زمانی که از VPN استفاده می‌کنید به سه دسته از پروتکل‌های زیر باید توجه کنید:

- پروتکل‌های VPN
- پروتکل‌های احراز هویت
- پروتکل‌های رمزنگاری

پروتکل PPP

از این پروتکل زمانی استفاده می‌شود که نیاز به برقراری ارتباط بین دو سیستم با استفاده از لینک سریال باشد. یکی از نمونه‌های بارز برای استفاده از این پروتکل زمانی است که کاربر با استفاده از اتصال Dial-up ارتباطی را برقرار می‌کند. این ارتباط یک ارتباط لایه ۲ بوده و می‌تواند پروتکل TCP/IP را در فریم‌های لایه ۲ کپسوله کند.

پروتکل PPTP

یک پروتکل لایه ۲ بوده که در آن فریم‌های PPP در پکت‌های IP کپسوله شده است. این پروتکل نسبت به PPP بهتر عمل می‌کند،چراکه بسته‌ها در هنگام انتقال داده‌ها با استفاده از یکی از پروتکل‌هایMS-CHAP v1 و MS-CHAP v2، EAP و PEAP کپسوله شده و سپس ارسال می‌شوند.

پروتکل L2TP

این پروتکل که برای برقراری ارتباط VPN مورد استفاده قرار می‌گیرد به منظور برقراری امنیت در ارتباط از تکنولوژی IPsec استفاده می‌کند. این تکنولوژی از الگوریتم DES یا 3DES استفاده کرده و بسته‌ها را رمزنگاری می‌کند. این پروتکل در ویندوزهای XP به بالا پشتیبانی می‌شوند.

پروتکل SSTP

این پروتکل ترافیک‌های PPP و یا L2TP را از طریق یک درگاه امن (SSL) ارسال می‌کند و امنیت را با بکارگیری کلیدهای خصوصی و عمومی تامین می‌کند. این نمونه از VPN در ویندوزهای ۷ به بالا پشتیبانی می‌شود.

IKEV2

این پروتکل امن‌ترین نوع از VPN بوده و از لحاظ ساختاری شبیه به L2TP عمل می‌کند اما با این تفاوت‌که کلیدها و مجوزهای مورد استفاده برای رمزنگاری‌داده به‌صورت پویا توسط پروتکل تامین می‌گردد. این پروتکل از ویندوز 7 به بالا پشتیبانی می‌شود.

پروتکل‌های احرازهویت (Authentication) و رمزگذاری

در هنگام استفاده از VPN چندین روش برای احرازهویت کاربران وجود دارد تا بتوان با استفاده از آن‌ها امنیت لازم را برای برقراری ارتباط امن کاربران فراهم نمود. در ادامه به چندین پروتکل اشاره خواهیم کرد.

PAP: این پروتکل دارای کمترین سطح امنیتی است و در هنگام انجام عملیات احرازهویت رمزهای‌عبور به صورت متن عادی (Plain Text) ارسال می‌شوند. برای همین منظور این پروتکل در حالت عادی استفاده نمی‌شود و تنها زمانی مورد استفاده قرار می‌گیرد که نیاز به انجام عملیات خطایابی باشد.

CHAP: این پروتکل در هنگام احرازهویت کاربران رمزهای‌عبور را به‌صورت متن عادی در شبکه ارسال نمی‌کند. در این پروتکل از روش دست‌تکانی سه طرفه استفاده می‌شود به این شکل که:

- ابتدا سرور یک متن‌چالش (به نام Challenge را) به سمت کلاینت ارسال می‌کند.
- کلاینت از رمزعبور خود (و یا کلیدی که بین سرور و کلاینت مشترک می‌باشد) استفاده کرده و متن‌چالش (یا همان Challenge) را رمز و سپس به سمت سرور ارسال می‌کند.
- سرور متن‌چالش دریافتی را با رمزعبور مربوط به کلاینت بازگشایی می‌کند و درصورتی‌که متن‌چالش برای سرور قابل قبول بود (به این شرط که متن‌چالش ارسال شده و دریافت شده از کاربر باید یکسان باشد) کاربر عملیات احرازهویت را با موفقیت به پایان می‌رساند.

MS-CHAP v2: این پروتکل توسط شرکت مایکروسافت و براساس CHAP ایجاد شده است و از لحاظ عملکردی بسیار شبیه به CHAP است.

EAP-MS-CHAP v2: این پروتکل با استفاده از الگوریتم EAP احرازهویت را انجام می دهد. EAP ارائه دهنده قوی‌ترین و انعطاف پذیرترین خصوصیات امنیتی می‌باشد.

با استفاده از این روش می‌توانیم بر سر روش‌های احرازهویت پیشرفته‌تر از رمزعبور بحث کنیم. روش‌هایی هم‌چون Certificate و SmartCardRemote Desktop هـا. ایـن روش بـه عنـوان روش پیش‌فرض برای ارتباطات بر روی کامپیوترهای مبتنی بر ویندوز ۸ در نظرگرفته شده است.

حال که با مفاهیم مربوط به پروتکل‌های VPN و پروتکل‌های ایمن‌سازی اتصال آشنا شـدید بهتـر است تا با نحوه ایجاد و پیاده‌سازی کانکشن در ویندوز ۸,۱ آشنا شوید.

به‌منظور ساخت کانکشن VPN در ویندوز ۸,۱ بایستی تمرین ۸-۲ را دنبال نما**یید**.

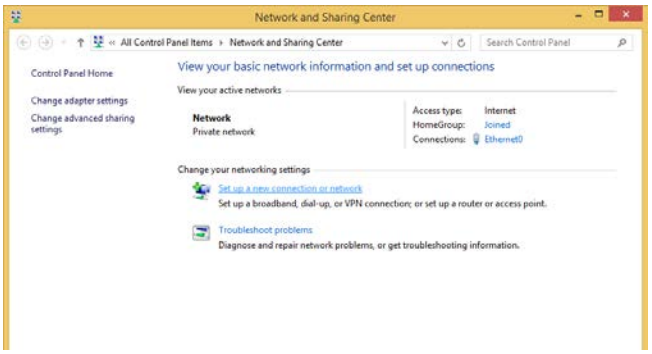
تمرین ۸- ۲

عنوان: ساخت کانکشن VPN در ویندوز ۸,۱

مراحل تمرین:

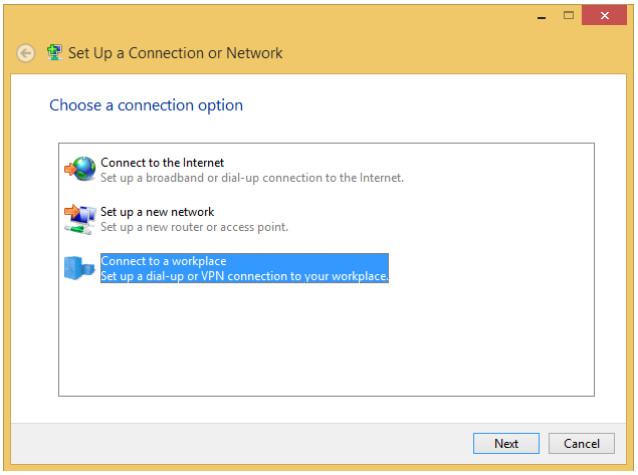
۱. ابتدا وارد Control Panel و سپس Network and Sharing Center را اجرا نمایید.

۲. برروی لینک Set up a new connection or network کلیک کنید.



شکل ۸- ۶

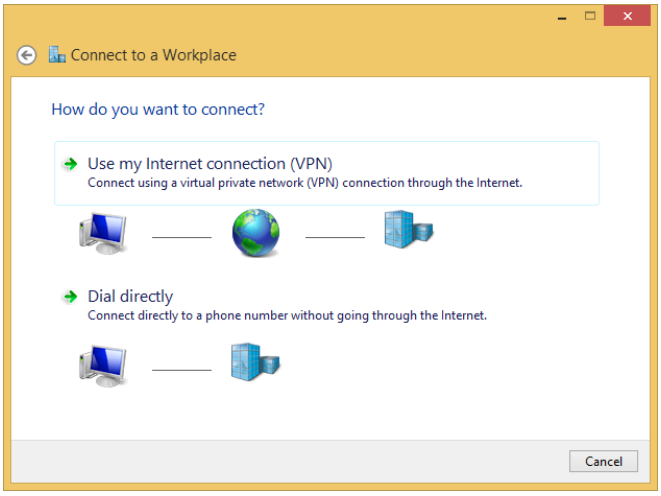
۳. در ادامه گزینه Connect to a workplace را انتخاب و سپس برروی Next کلیک کنید.



شکل ۸–۷

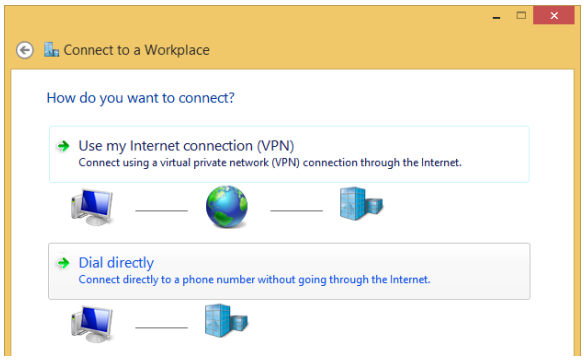
۴. در پنجره Connect to a Workplace دو گزینه قابل انتخاب است که شامل:

- Use my Ineternet connection: برقراری ارتباط VPN با استفاده از اینترنت
- Dial directly: برقراری ارتباط VPN با شماره‌گیری یک تلفن



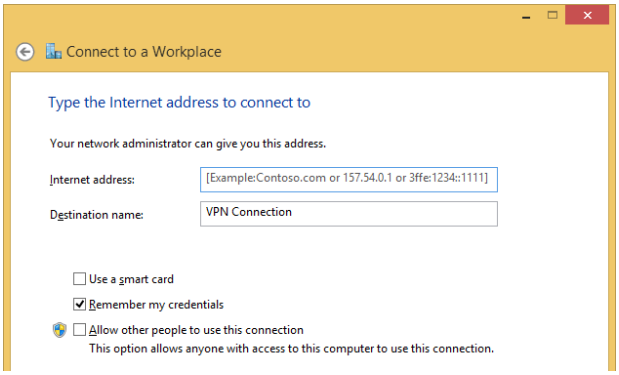
شکل ۸–۸

۵. با انتخاب گزینه Use my Internet connection مراحل ایجاد کانکشن را ادامه دهید.



شکل ۸- ۹

۶. در ادامه باید آدرس IP مربوط به سرور VPN و یک نام برای کانکشن وارد نمایید و در انتها برروی Create کلیک کنید.



شکل ۸- ۱۰

با انجام مراحل بالا کانکشن VPN ایجاد شده و اتصال به سرور انجام می‌پذیرد. به‌منظور قطع و برقراری اتصال مجدد به VPN کافی است تا برروی آیکن شبکه در کنار ساعت کلیک کنید و از منوی باز شده برروی نام VPN کلیک کنید و گزینه Connect یا Disconnect را انتخاب کنید.

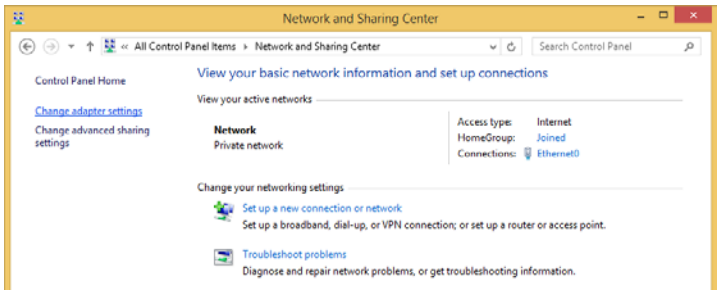
شکل ۸- ۱۱

تغییر مشخصات مربوط به کانکشن‌ها

بعد از ایجاد کانکشن VPN می‌توانید تنظیمات مربوط به آن را بررسی کـرده و درصـورت نیـاز تغییرات مورد نیاز را اعمال نمایید.

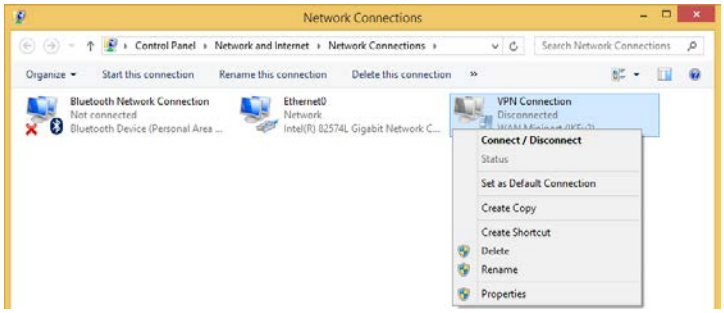
برای دسترسی به تنظیمات VPN کافی است تا مراحل زیر را انجام دهید:

۱. ابتدا از Control Panel برنامه Network and Sharing Center را اجرا کرده و سپس از منـوی سمت چپ برروی لینک Change adapter settings کلیک کنید.



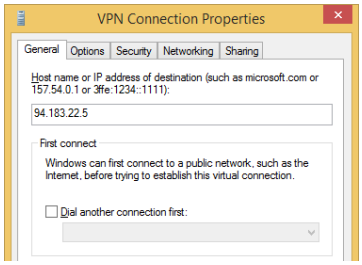
شکل ۸– ۱۲

۲. در پنجره ظاهر شده برروی VPN مورد نظر راست‌کلیک کرده و سپس گزینه Properties را انتخاب کنید.



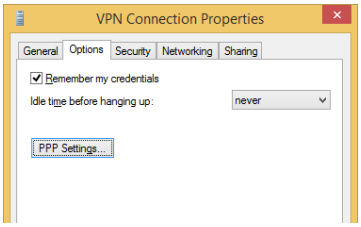
شکل ۸– ۱۳

۳. در پنجره باز شده چندین سربرگ وجود دارد که در شکل ۸– ۱۴ قابل مشاهده است.



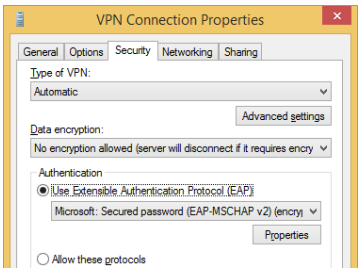
شکل ۸– ۱۴

- در سربرگ General می‌توانید Host name و یا آدرس IP مربوط به سرور را تغییر دهید.
- در سربرگ Option می‌توانید تنظیمات مربوط به اتصال PPP و به یاد سپاری موارد امنیتی را مورد بررسی قرار دهید.



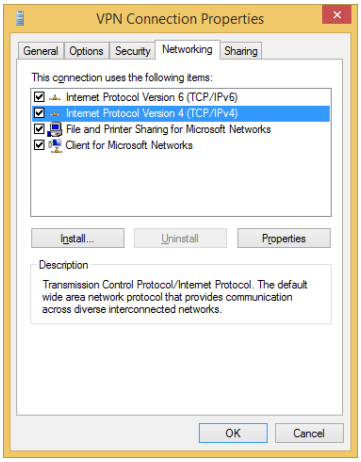
شکل ۸- ۱۵

- در سربرگ Security می‌توان نوع پروتکل VPN (مانند PPTP، L2TP، SSTP و IKEv2) و همچنین پروتکل رمزنگاری داده‌ها در VPN (مانند none، required، maximum strength) و همچنین پروتکل احرازهویت (مانند PAP، CHAP، MS-CHAP و ...) را تغییردهید.



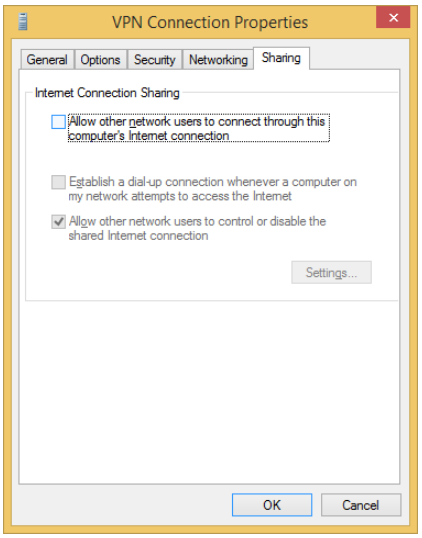
شکل ۸- ۱۶

- در سربرگ Networking می‌توان تنظیمات TCP/IP مربوط به کانکشن VPN را مشاهده کرده و در صورت نیاز تغییراتی را اعمال کنید.



شکل ۸- ۱۷

- در سربرگ Sharing می‌توان تنظیمات مربوط به اشتراک‌گذاری کانکشن (ICS) را انجام دهید.



شکل ۸– ۱۸

فعال‌سازی VPN Reconnect

گاهی اوقات ممکن است که در هنگام استفاده از VPN ارتباط با سرور دچار مشکل‌شده و قطعی رخ دهد. از این‌رو با استفاده از VPN Reconnect می‌توان بدون این‌که نیاز به انجام کار اضافی باشد اتصال VPN را مجدداً برقرار کرد. توجه داشته باشید که VPN Reconnect را تنها می‌توان زمانی استفاده کرد که از پروتکل IKEv2 استفاده شده باشد. در ادامه قصد داریم تا این قابلیت را در ویندوز ۸٫۱ فعال کنیم.

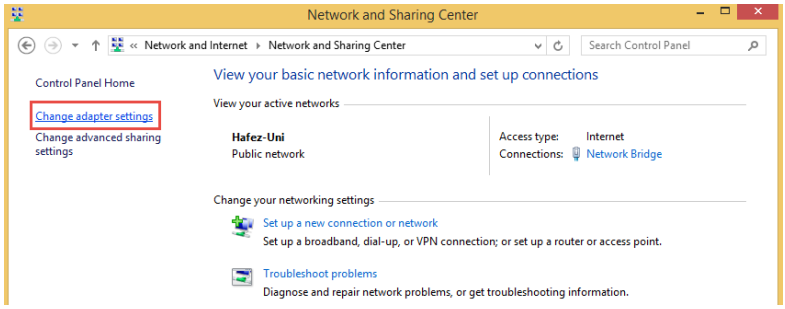
تمرین ۸– ۳

عنوان: فعال‌سازی قابلیت VPN Reconnect در ویندوز ۸٫۱

شرح: در این تمرین قصد داریم تا قابلیت VPN Reconnect را در ویندوز ۸٫۱ فعال کرده به نحوی‌که اگر اتصال VPN دچار مشکل شد بعد از گذشت ۵ دقیقه مجدداً سعی شود تا اتصال برقرار شود.

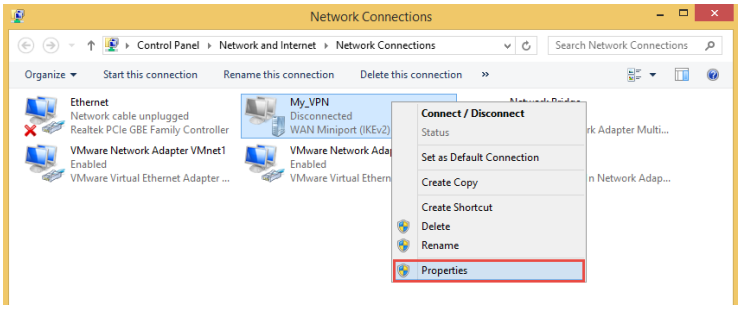
مراحل تمرین :

۱. ابتـدا Network and Sharing Center را بـاز کـرده و سـپس از منـوی سـمت چـپ گزینـه Change adapter settings را انتخاب کنید.



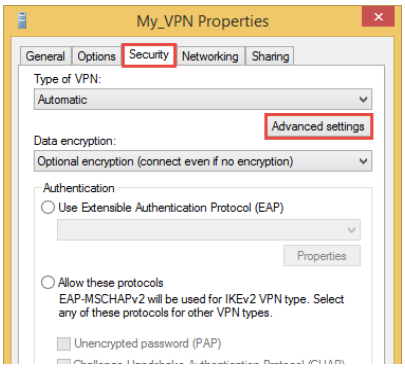
شکل ۸– ۱۹

۲. در ادامه برروی کانکشن VPN خود راست‌کلیک کرده و گزینه Properties را انتخاب کنید.



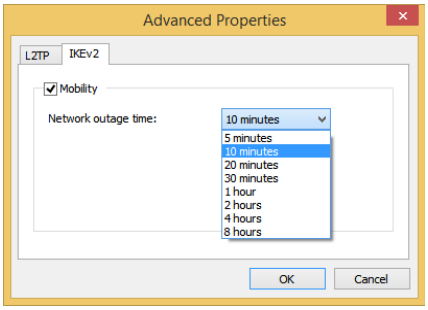
شکل ۸– ۲۰

۳. در پنجره باز شده به سربرگ Security رفتـه و سـپس بـرروی دکمـه Advanced Settings کلیک کنید.



شکل ۸– ۲۱

۴. در پنجره باز شده به سربرگ IKEV2 بروید و گزینه Mobility را انتخاب کرده و از قسمت Network outage time ،بازه زمانی‌اتصال مجدد VPN را تنظیم کنید. در این تمرین هدف ما ۱۰ دقیقه است.



شکل ۸–۲۲

آشنایی با Direct Access

DirectAccess به کاربران این قابلیت را می‌دهد تا در خارج از شبکه سازمان و در یک مکان دیگر به شبکه داخلی سازمان متصل شوند. DirectAccess ساختاری متفاوت با VPN دارد و نمی‌توان آن را نوعی از VPN دانست. زمانی‌که در DirectAccess کاربران به شبکه داخلی سازمان و یا شرکت خود متصل و احرازهویت شوند، می‌توانند به منابعی هم‌چون Network share، Intranet websites، Applications، Virtual Desktops، فایل‌های شخصی و حتی پرینترها دسترسی داشته باشند. شما تا حدودی در Objective 1.2 و در بخش آشنایی با تکنولوژی‌های انتقال با مفهموم DirectAccess آشنا شدید.

در DirectAccess کاربران برای متصل شدن به شبکه داخلی سازمان نیاز به انجام هیچ‌گونه عملیاتی ندارند به این‌صورت‌که زمانی‌که کاربران به شبکه داخلی سازمان متصل نیستند و در یک مکان دیگر قرارگرفته‌اند، می‌توانند با متصل شدن به اینترنت به‌صورت کاملاً اتوماتیک به شبکه داخلی سازمان نیز متصل شوند و نیاز به هیچ‌گونه کانکشن نیست (بر خلاف VPN). همچنین در DirectAccess ادمین‌های شبکه می‌توانند کامپیوترها را به‌راحتی مدیریت کنند به‌طور مثال می‌توانند یک Group Policy را اعمال کنند و یا آپدیت‌ها را نصب کنند و کارهایی شبیه آن را انجام دهند.

بررسی حجم دانلود شده

یکی از ویژگی‌هایی که می‌توان در ویندوز ۸,۱ پیدا کرد وجود امکان بررسی حجم دانلـود شـده توسط کانکشن می‌باشد. به این معنی که با استفاده از این قابلیت می‌توانید مشخص کنیـد کـه در مدت زمان مشخص چه میزان داده تبادل شده است. استفاده از این قابلیت زمانی اهمیت پیدا می-کند که از طریق گوشی هوشمندتان ویندوز را به اینترنت متصل کرده باشید. برای استفاده از این قابلیت تنها کافی است تا مراحل زیر را انجام دهید.

تمرین ۸- ۴

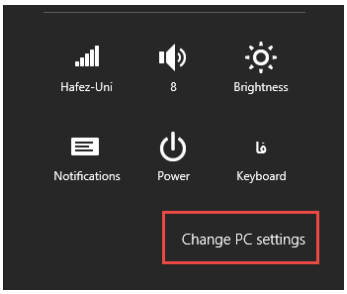
عنوان: **فعال‌سازی قابلیت تخمین میزان مصرف پهنای‌باند در ویندوز ۸,۱**

شرح: در این تمرین قصد داریم تا با استفاده از ویندوز ۸,۱ میزان پهنای باند مصرف شده را مورد بررسی قرار دهیم.

مراحل تمرین:

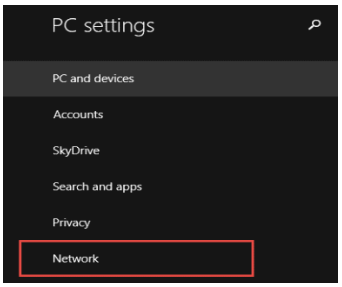
۱. از نوار سمت راست گزینه Setting را انتخاب کنید.

۲. برروی گزینه Change PC Setting کلیک کنید.



شکل ۸- ۲۳

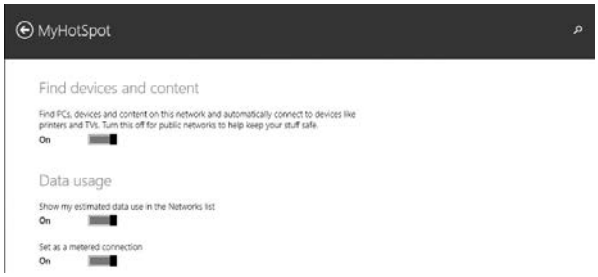
۳.از قسمت سمت چپ برروی Network کلیک کنید.



شکل ۸- ۲۴

۳. از پنجره ظاهر شده شبکه‌ای که به آن متصل هستید را انتخاب کنید.

۴. در صفحه جدید در قسمت Data usage گزینه Show my estimated data use in the network list را برابر On قرار دهید.



شکل ۸– ۲۵

به این ترتیب می‌توان با کلیک برروی نام شبکه از میزان ترافیک تبادل شده آگاه شد. برای این منظور باید برروی آیکون شبکه از کنار ساعت کلیک کرده و سپس برروی نام شبکه مورد نظر کلیک کنید.

شکل ۸– ۲۶