

# ویندوز 10

پشتیبانی از نصب ویندوز ۱۰



این PDF به صورت تصویری و مرحله به مرحله توضیح داده شده است.

[www.NetworkBooks.ir](http://www.NetworkBooks.ir)  
[www.TejaratServer.ir](http://www.TejaratServer.ir)



برگرفته از پروژه های عملی شرکت



# فصل اول

## پشتیبانی از نصب ویندوز 10

---

---

مباحث این فصل در دو قسمت "مقدماتی" و "حرفه‌ای‌تر شوید" ارائه شده است. در ابتدای هر فصل به بررسی مطالب ساده‌تری پرداخته شده و در قسمت "حرفه‌ای‌تر شوید" مباحث تخصصی‌تری مربوط به نظارت و پشتیبانی از ویندوز 10 منابع را مورد بررسی قرار داده ایم لذا توصیه می‌شود ابتدا قسمت مباحث ابتدایی را مطالعه کرده و در صورتی که به مطالب تسلط پیدا کردید قسمت "حرفه‌ای‌تر شوید" را مطالعه نمایید.

ویندوز 10 یکی از نسخه‌های سیستم‌عامل شرکت مایکروسافت بوده که برای کاربران تولید شده است. همان‌گونه که می‌دانید مایکروسافت تمامی سیستم‌عامل‌های خود را در نسخه‌های متفاوتی تولید می‌کند و تفاوت این سیستم‌عامل‌ها در میزان امکاناتی است که به کاربر داده می‌شود.

### انواع نسخه‌های Windows 10

ویندوز 10 در 4 نسخه منتشر شده است که در ادامه مورد بررسی قرار گرفته است. **Windows Home**: این نوع ویندوز برای استفاده از کاربران خانگی طراحی شده است و قابل استفاده در PC و تبلت است. این نوع نسخه بسیار شبیه نسخه windows 8.1 Home است. **Windows 10 Professional (Windows 10 Pro)**: از این نسخه معمولاً در سازمان‌هایی با ابعاد کوچک تا متوسط مورد استفاده قرار می‌گیرد. از جمله خصوصیات که این نسخه از سیستم‌عامل نسبت به نسخه‌های قبلی دارد شامل موارد زیر می‌باشد:

- پشتیبانی از Bit Locker و Bit Locker To Go (در فصل 5 با این قابلیت آشنا خواهید شد)
- امکان استفاده از Remote Desktop
- پشتیبانی از مجازی‌سازی سمت Client (Client Hyper-V)
- و ...

**Windows 10 Enterprise**: این نسخه کامل‌ترین نسخه ویندوز بوده و تمام قابلیت‌ها در این نسخه پیاده شده است. این نسخه برای استفاده سازمانی و IT مورد استفاده قرار می‌گیرد.  معماری ARM: نوعی از معماری پردازنده‌های کامپیوتری بوده که تنها دستورالعمل‌های 32 بیتی را پردازش کرده و مهم‌ترین دلیل استفاده از این نوع پردازنده، مصرف بسیار پایین انرژی است. این موضوع باعث استفاده گسترده آن‌ها در ابزارهای پرتابل مانند تلفن هوشمند یا تبلت شده است.

**Windows 10 Education**: این نسخه تمام قابلیت‌های ویندوز 10 نسخه Enterprise را دارد و این نسخه برای استفاده در مدرسه، دانشگاه و ... طراحی شده است.

برای مشاهده تفاوت بین نسخه‌های ویندوز 10 با جزئیات بیشتر می‌توانید جدول 1-1 را مورد بررسی قرار دهید.

Features	Desktop			
	Home	Pro	Enterprise	Education
Architecture	IA-32, x86-64			
Availability	OEM, Retail	OEM, Retail, Volume licensing	Volume licensing, OEM	Volume licensing
N Edition Available	Yes	Yes	Yes	Yes
Maximum physical memory (RAM)	4 GB on 32-bit 128 GB on 64-bit	4 GB on 32-bit 2048 GB on 64-bit		
Continuum	Yes	Yes	Yes	Yes
Cortana	Yes	Yes	Yes, except LTSB	Yes
Hardware device encryption	Yes	Yes	Yes	Yes
Microsoft Edge	Yes	Yes	Yes, except LTSB	Yes
Microsoft account	Yes	Yes	Yes	Yes
Mobile device management	Yes	Yes	Yes	Yes
Side-loading of line of business apps	Yes	Yes	Yes	Yes
Virtual desktops	Yes	Yes	Yes	Yes
Windows Hello	Yes	Yes	Yes	Yes
Windows Spotlight	Yes	Yes	Yes	Yes
Assigned Access 8.1	No	Yes	Yes	Yes
BitLocker and EFS	No	Yes	Yes	Yes
Business Store	No	Yes	Yes	Yes
Current Branch for Business (CBB)	No	Yes	Yes	Yes
Joining a domain and Group	No	Yes	Yes	Yes
Enterprise data protection	No	Yes	Yes	Yes

Enterprise Mode Internet Explorer (EMIE)	No	Yes	Yes	Yes
Hyper-V	No	64-bit SKUs only	64-bit SKUs only	64-bit SKUs only
Joining a Microsoft Azure Active Directory	No	Yes	Yes	Yes
Private catalog	No	Yes	Yes	Yes
Windows Update for Business	No	Yes	Yes	Yes
Remote Desktop	Client only	Client and host	Client and host	Client and host
Remote App	Client only	Client only	Client and host	Client and host
AppLocker	No	No	Yes	Yes
BranchCache	No	No	Yes	Yes
Credential Guard (Pass the hash mitigations)	No	No	Yes	Yes
Device Guard	No	No	Yes	Yes
DirectAccess	No	No	Yes	Yes
Start screen control with Group Policy	No	No	Yes	Yes
User experience control and lockdown	No	No	Yes	Yes
Windows To Go	No	No	Yes	Yes
Long Term Servicing Branch (LTSB)	No	No	Yes	No
In-place upgrade to Enterprise edition	No	Yes	N/A	No
In-place upgrade to Education edition	Yes	Yes	No	N/A
Update to newer builds	Yes	Yes	Yes	Yes

جدول 1-1

### سخت افزار مورد نیاز

یکی از موارد مهم قبل از اقدام به نصب سیستم عامل توجه به قدرت سخت افزار فعلی می باشد. در جدول 1-2 حداقل سخت افزارهای مورد نیاز جهت نصب ویندوز 10 بیان شده است. توجه داشته باشید که ویندوز 10 نیز همانند سایر محصولات دارای دو نسخه 32 و 64 بیتی است. بررسی تفاوت این دو معماری 32 و 64 بیتی در حوصله این کتاب نبوده و در کتاب Network+ این موضوع بررسی خواهد شد.

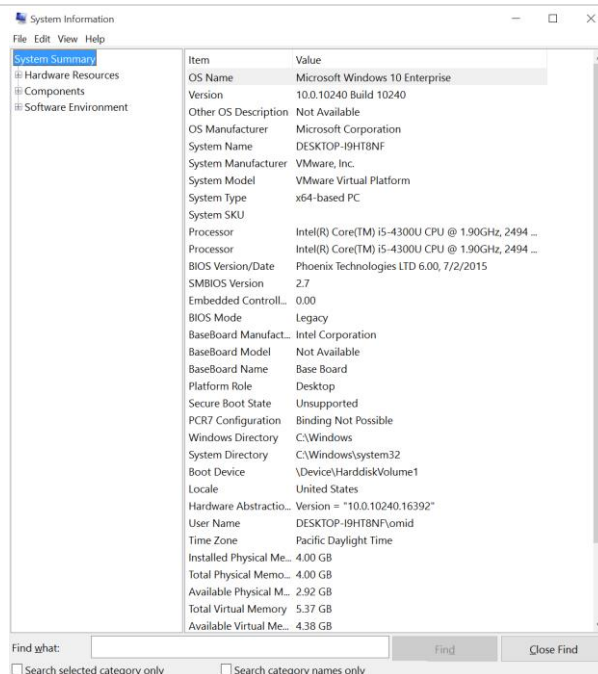
	32-bit (x86)	64-bit (x64)
Processor speed	1 gigahertz (GHz) or faster	1 GHz or faster
System memory (RAM)	1 GB	2 GB
Available hard disk space	16 GB	20 GB
Graphics adapter	DirectX 9 graphics adapter with WDDM driver	DirectX 9 graphics adapter with WDDM driver
Secure Boot	Unified Extensible Firmware Interface (UEFI)-based BIOS	UEFI-based BIOS

جدول 1-2

### بررسی سخت‌افزار سیستم جهت نصب ویندوز 10

تا به این‌جای کار از حداقل نیازهای سخت‌افزاری به منظور نصب ویندوز 10 آگاه شده‌اید، در ادامه باید بتوانید از سخت‌افزار فعلی خود گزارشاتی را تهیه نمایید و بررسی کنید که آیا می‌توان ویندوز 10 را نصب کرد یا خیر. برای پاسخ به این سوال تنها کافی است تا عبارت msinfo32 را در Run اجرا کنید.

پس از اجرای دستور فوق پنجره‌ای مانند شکل 1-1 ظاهر خواهد شد که می‌توان در این پنجره مشخصات سیستم فعلی را مشاهده نمود.



شکل 1-1

## انواع حالت‌های نصب ویندوز

مایکروسافت به منظور نصب و راه‌اندازی ویندوز 10 دو روش در نظر گرفته است که شامل:

1. نصب از ابتدا (**Clean Installation**): در این حالت یک ویندوز کاملاً خام و بدون هیچ برنامه‌ای نصب خواهد شد که در ادامه باید برنامه‌های موردنیاز خود را بر روی آن نصب کنید.
  2. بروزرسانی (**Upgrade**): با استفاده از این حالت ویندوز فعلی که بر روی سیستم موجود می‌باشد به ویندوز 10 به‌روز رسانی خواهد شد. توجه داشته باشید که در این حالت نرم‌افزارهای موجود بر روی ویندوز قبلی در ویندوز 10 نیز حفظ خواهد شد.
- توجه داشته باشید که نمی‌توان ویندوز 32 بیتی را به ویندوز 64 بیتی بروزرسانی کرد. به عنوان مثال نمی‌توان از ویندوز 8 که 32 بیتی می‌باشد عملیات بروزرسانی به ویندوز 10 از نوع 64 بیتی را انجام داد.

یکی از موارد مهمی که ممکن است همواره ذهن کاربران را درگیر کند این است که چه زمانی باید از Clean Installation و چه زمانی باید از Upgrade استفاده کرد.

به‌صورت کلی نصب ویندوز در حالت Clean Installation توصیه می‌شود چراکه در این حالت می‌توان از عدم انتقال ویروس و نرم‌افزارهای مخرب اطمینان حاصل کرد. توجه به این نکته

ضروری است که همیشه نمی توان نصب ویندوز را در حالت Clean Installation انجام داد چرا که ممکن است یکی از شرایط زیر حاکم باشد:

- یکسری اطلاعات خیلی مهم و ضروری بر روی ویندوز قبلی خود داشته باشید.
  - یکسری نرم افزاری خاص که دارای License های قانونی هستند بر روی ویندوز قدیمی خود داشته باشید.
  - کاربر نیاز داشته باشد تا تمامی تنظیمات ویندوز قدیمی از جمله: تنظیمات شبکه، برنامه ها، تنظیمات ویندوز، آپدیت های انجام شده و ... را حفظ نماید.
- با وجود تمامی موارد ذکر شده همیشه این امکان وجود ندارد که با استفاده از گزینه Upgrade بتوان تمامی اطلاعات را به ویندوز 10 منتقل کرد چراکه این انتقال شدیداً به ویندوز قدیمی شما بستگی دارد. در باتوجه به ویندوز قبلی خود مواردی که پس از انجام عملیات Upgrade در ویندوز 10 باقی خواهند ماند نشان داده شده است.

Upgrading from	What you can keep
Windows 8	Windows Store apps, desktop applications, personal files, Windows settings
Windows 7	Applications, personal files, Windows settings
Windows Vista SP 1	Personal files, Windows settings
Windows XP SP3	Personal files

جدول 1-3

## نصب ویندوز 10

در این قسمت قصد داریم تا ویندوز 10 را به صورت گام به گام و در حالت Clean Installation نصب کنیم. فرآیند نصب در ویندوز 10 بسیار ساده و آسان می باشد که برای این کار کافی است تا تمرین 1-1 انجام دهید.

### تمرین 1-1

عنوان: نصب ویندوز 10

شرح: در این تمرین قصد بر آن است تا ویندوز 10 را در حالت Clean Installation نصب کنیم.

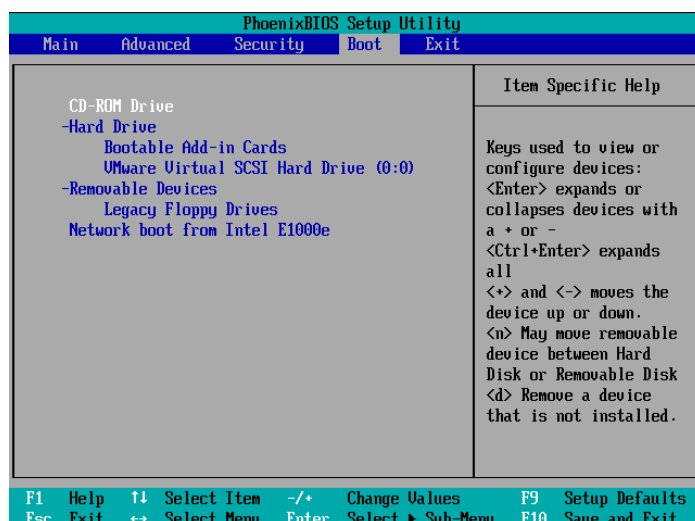
تجهیزات و پیش نیازها:

- DVD نصب ویندوز 10



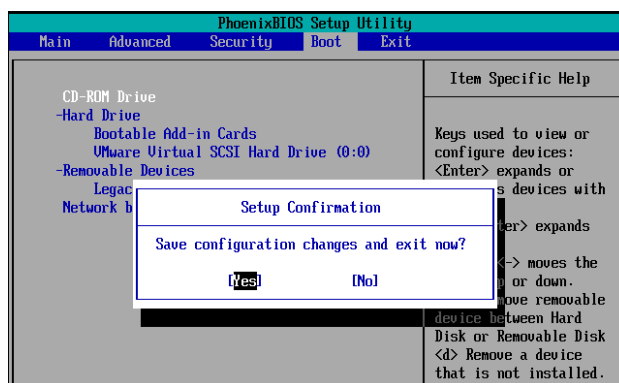
• حداقل سخت‌افزار لازم جهت نصب  
مراحل تمرین:

1. ابتدا رسانه نصب ویندوز 10 را در درایو DVD قرار دهید.
2. در ادامه باید وارد تنظیمات BIOS سیستم شده و مشخص کنید که عملیات بوت سیستم باید از DVD نصب ویندوز 10 صورت پذیرد. برای این منظور کافی است تا پس از روشن کردن سیستم دکمه Delete را فشار دهید. صفحه‌ای مطابق با شکل 1-2 نمایان خواهد شد. در ادامه باید وارد سربرگ Boot شده و ترتیب بوت شدن سیستم خود را مشخص نمایید (توجه داشته باشید که ممکن است صفحه مربوط به BIOS در سیستم‌های مختلف مانند شکل 1-2 نباشد).



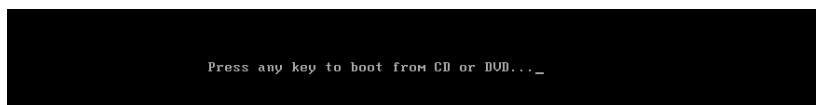
شکل 1-2

3. پس از انجام تغییرات، کلید F10 را فشار دهید و سپس گزینه Yes را انتخاب کنید تا تغییرات اعمال شده و سیستم Restart شود.



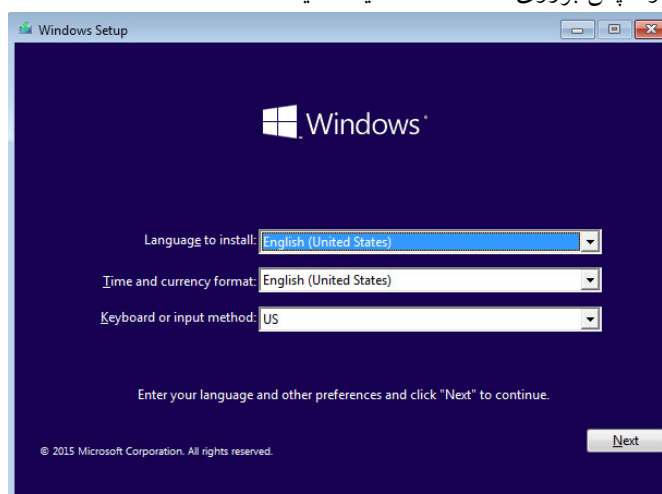
شکل 1-3

4. پس از مشاهده پیام شکل 1-4 با فشردن هر دکمه از صفحه کلید وارد مراحل نصب ویندوز شوید.



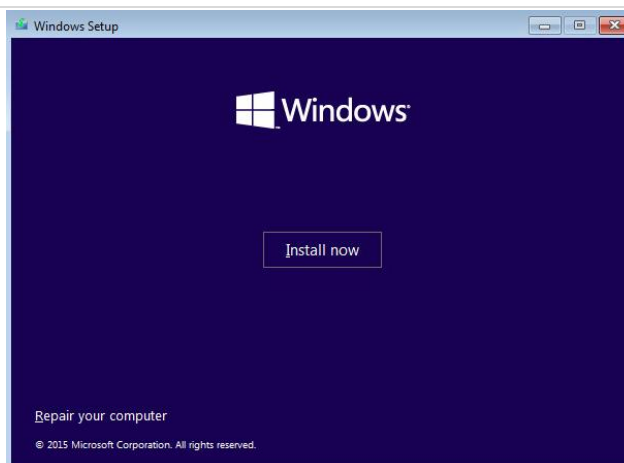
شکل 1-4

5. در ادامه باید گزینه‌های مربوط به زبان، تنظیمات مربوط به زمان و زبان صفحه کلید را مشخص کرده و سپس بر روی دکمه Next کلیک کنید.



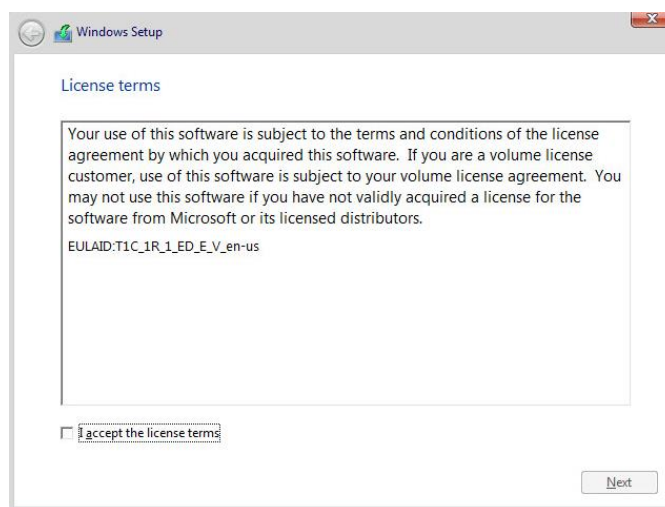
شکل 1-5

6. در ادامه بر روی دکمه Install Now کلیک کنید.



شکل 1-6

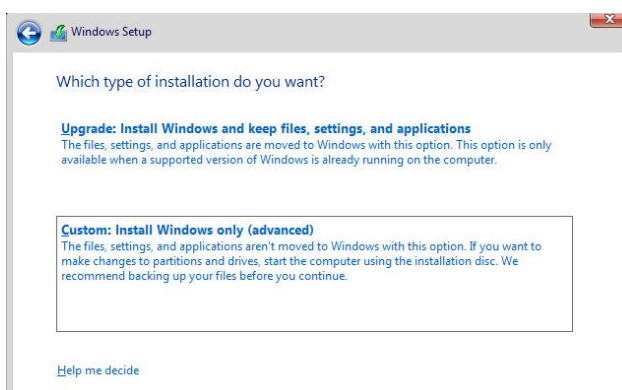
7. در پنجره License Terms گزینه I accept the license terms را زده و بر روی دکمه Next کلیک کنید.



شکل 1-7

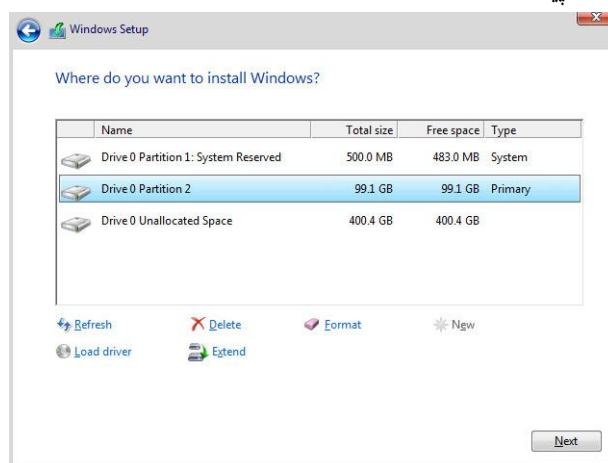
8. در پنجره دو گزینه وجود دارد که شامل:

- Upgrade: Install Windows and Keep files, Settings and Application: استفاده از این گزینه باعث می‌شود تا بتوان ویندوز قبلی را به ویندوز 10 بروزرسانی کرد.
  - Custom: Install Windows only (Advanced): استفاده از این گزینه باعث می‌شود تا بتوان ویندوز 10 را در حالت clean نصب کرد.
- با انتخاب گزینه Custom: Install Windows only (Advanced) مراحل نصب را ادامه دهید.



شکل 8-1

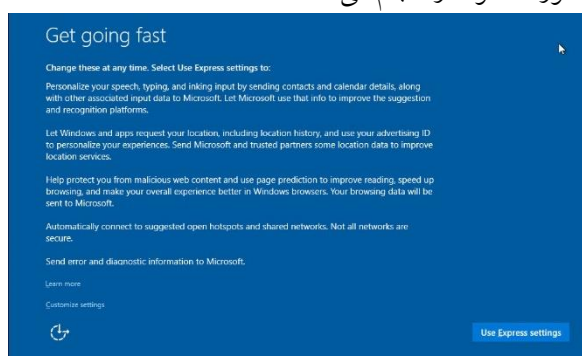
9. در پنجره **Where do you want to install windows** لیستی از پارتیشن‌های موجود بر روی هارد نشان داده می‌شود که برای نصب ویندوز باید یکی از آن‌ها را انتخاب کنید. پارتیشن موردنظر را انتخاب کرده و سپس بر روی **Format** کلیک کنید تا تمام اطلاعات از پارتیشن حذف شده و آماده نصب شود. پس از انجام مرحله **Format** بر روی دکمه **Next** کلیک کرده تا مراحل نصب ادامه پیدا کند.



شکل 9-1

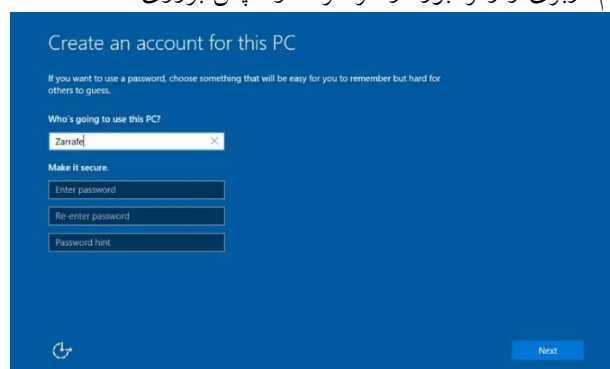
10. بعد از انتخاب پارتیشن موردنظر و کلیک کردن بر روی دکمه **Next** مراحل نصب ویندوز شروع شده و مابقی کارها به صورت خودکار انجام می‌پذیرد.  
 توجه داشته باشید که ممکن است در طول مراحل نصب چندبار سیستم **Restart** شود.  
 11. پس از این که مراحل نصب ویندوز به پایان رسید، پنجره‌ای مطابق با نمایان خواهد شد که

در این پنجره بر روی Use Express Setting کلیک کنید با انتخاب این دکمه ویندوز یک سری تنظیمات اولیه را به صورت خودکار انجام می دهد.



شکل 1-10

12. در مرحله بعد باید تنظیمات مربوط به Username و Password را انجام دهید. مقادیر مناسب را برای نام کاربری و رمز عبور در نظر گرفته و سپس بر روی دکمه Next کلیک کنید.



شکل 1-11

پس از انجام این مراحل ویندوز 10 نصب شده و می توانید از آن استفاده کنید.

**عنوان:** بروزرسانی از ویندوز قدیمی به ویندوز 10

**شرح:** در این تمرین قصد برآن است تا ویندوز قدیمی را به ویندوز 10 بروزرسانی کنیم.

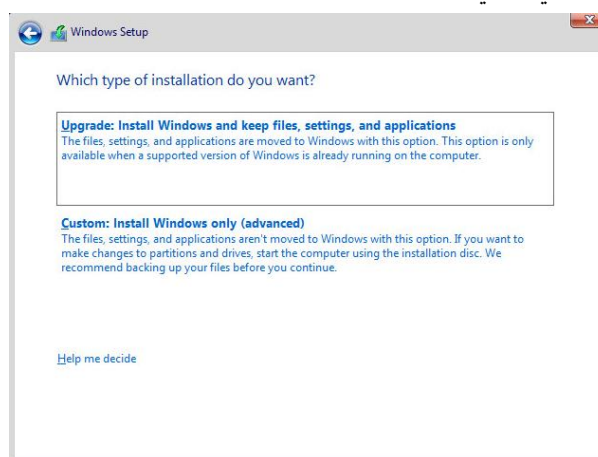
**تجهیزات و پیش نیازها:**

- DVD نصب ویندوز 10
- حداقل سخت افزار لازم جهت نصب

**مراحل تمرین:**

تمامی مراحل موجود در تمرین 1-1 را انجام دهید اما توجه داشته باشید که در مرحله 8 باید گزینه Upgrade: Install Windows and Keep files, Settings and Application را انتخاب کرده

و سپس بروی Next کلیک کنید.



شکل 1-12

## آشنایی با سیستم های Multiboot یا بوت چندگانه

سیستم multiboot یا بوت چندگانه، به سیستمی گفته می شود که دارای حداقل دو سیستم عامل باشد. در این نوع سیستم، هر سیستم عامل به صورت یک واحد مجزا و جداگانه عمل می کند. از سیستم های multiboot معمولاً برای تست نرم افزارها بروی سیستم عامل های مختلف مورد استفاده قرار می گیرد. عملکرد سیستم Multiboot تقریباً همانند VHD است. راه اندازی سیستم Multiboot بسیار ساده است و برای کسانی که آشنایی با VHD ندارند، می تواند یک گزینه خوب محسوب شود.

برای راه‌اندازی یک سیستم Multiboot نیاز به فضای کافی برای نصب یک سیستم‌عامل دیگر دارید. اگر فضای لازم را در اختیار دارید می‌توانید یک پارتیشن را Shrink کرده و با فضای Shrink شده یک پارتیشن جدید ساخته. در این قسمت ما فرض می‌گیریم که شما یک پارتیشن آماده ایجاد کرده و می‌خواهید یک سیستم‌عامل دیگر در کنار سیستم‌عامل موجود در کامپیوترتان نصب کنید.

شما می‌توانید به راحتی چندین سیستم‌عامل بر روی کامپیوتر خود داشته باشید. برای این کار کافی است تمرین 1-3 را انجام دهید.

### تمرین 1-3

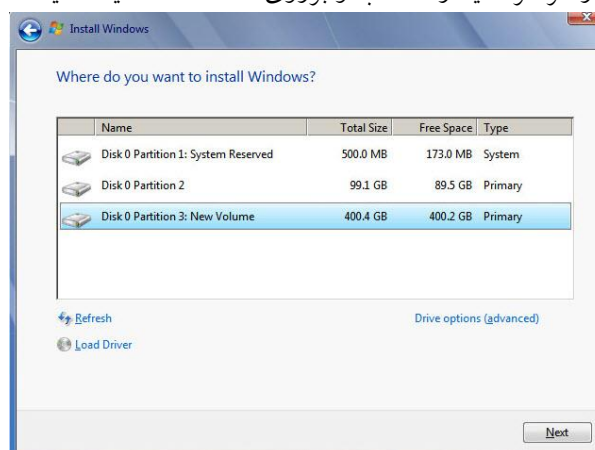
عنوان: ایجاد یک سیستم Multiboot

تجهیزات و پیش‌نیازها:

- کامپیوتر دارای یک سیستم‌عامل
- پارتیشنی با فضای خالی برای نصب سیستم‌عامل دوم

مراحل تمرین:

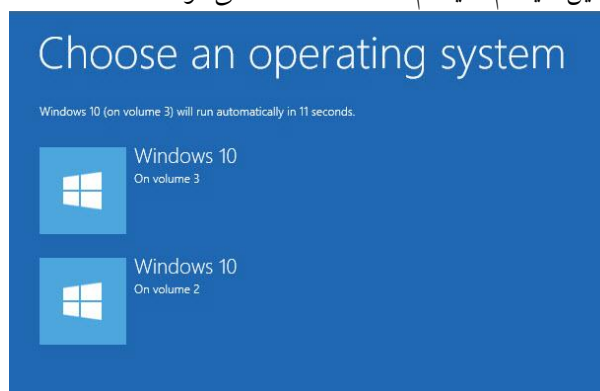
1. کامپیوتر خود را از روی DVD-ROM بوت کنید تا وارد مراحل نصب ویندوز شود.
2. مراحل نصب را طی کرده تا به مرحله ایجاد پارتیشن برسید. در اینجا پارتیشنی که برای نصب سیستم‌عامل دوم در نظر گرفته‌اید را انتخاب و بر روی دکمه Next کلیک کنید.



شکل 1-13

3. پس از این‌که نصب سیستم‌عامل به پایان رسید، در هنگام بوت شدن کامپیوتر پنجره‌ای مانند شکل 1-14 مشاهده خواهید کرد که می‌توانید سیستم‌عامل موردنظر خود را انتخاب کرده و

وارد آن شوید. به این سیستم، سیستم Multiboot گفته می‌شود.

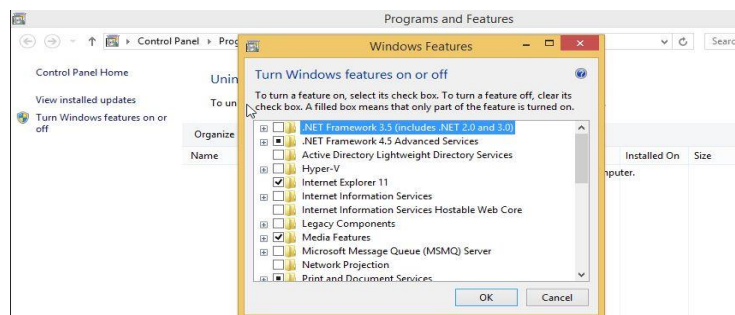


شکل 1-14

## نصب ویژگی‌های اضافی

به صورت کلی هنگامی که ویندوز 10 نصب می‌شود، تمامی ویژگی‌ها و قابلیت‌های سیستم عامل بر روی آن فعال نیست. این دسته از ویژگی‌ها و قابلیت‌ها اجباری نبوده و سیستم عامل در حالت عادی بدون وجود آن‌ها می‌تواند به نیازهای کاربر پاسخ دهد. نمونه‌های بارز از این قابلیت‌ها شامل TFTP، Net framework، Telnet و ... می‌باشد.

به منظور فعال‌سازی این ویژگی‌ها در ویندوز باید وارد مسیر **Programs ← Control Panel ← Programs and Features** شده و در سمت چپ بر روی لینک **Turn Windows features on or off** کلیک کنید تا با پنجره‌ای مطابق با شکل 1-15 روبرو شوید.



شکل 1-15

در این پنجره می‌توانید آن دسته از ویژگی‌هایی که مورد نیاز شما می‌باشد را انتخاب کرده و در



نهایت بر روی دکمه OK کلیک کنید تا مراحل نصب شروع شود.

### پیکربندی محل ذخیره پروفایل کاربران

یکی از موارد مهم در هنگام استفاده از شبکه، ذخیره‌سازی اطلاعات به‌صورت جامع و متمرکز می‌باشد به نحوی که اگر برای کامپیوترهای کلاینت اتفاقی رخ دهد، داده‌ها از بین نرود. مزیت انجام این کار امنیت بیشتر در حفظ اطلاعات می‌باشد چراکه اطلاعات کاربران در سرورهای ذخیره‌ساز و قدرتمندی قرار خواهد گرفت و تضمین لازم برای حفظ اطلاعات فراهم می‌شود. عملیات ذخیره‌سازی داده‌ها در شبکه‌های بزرگ نیازمند محیط Domain است تا کاربران به آن متصل شده و فایل‌های خود را در File Server ذخیره کنند. در شبکه‌های کوچک و با استفاده از ویندوز 10 نیز می‌توان این عملیات را انجام داد و اطلاعات مربوط به پوشه‌های Desktop، Downloads، Pictures و ... که در پوشه Documents قرار دارند را در محلی دیگر از جمله: پوشه‌ای دیگر در درایو C، درایوی دیگر در همان کامپیوتر و یا یک پوشه به اشتراک گذاشته شده در سطح شبکه تغییر داد

# پشتیبانی ویندوز 10

پشتیبانی از نرم افزارها




پشتیبانی ویندوز 10  
Windows 10

موسسه تخصصی رایانه

این PDF به صورت تصویری و مرحله به مرحله توضیح داده شده است.

[www.NetworkBooks.ir](http://www.NetworkBooks.ir)  
[www.TejaratServer.ir](http://www.TejaratServer.ir)

برگرفته از پروژه های عملی شرکت



# فصل دوم

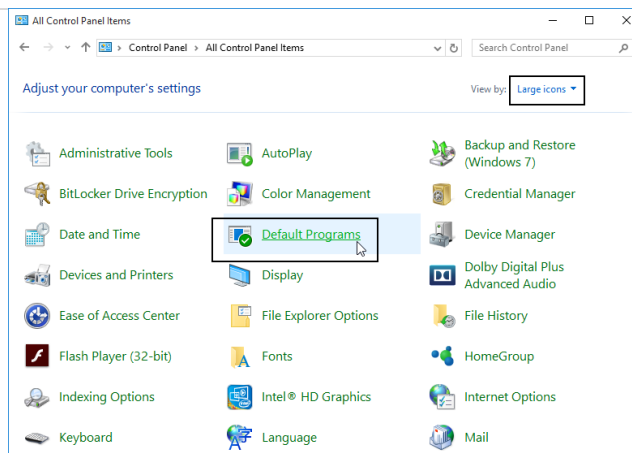
## پشتیبانی از نرم افزار ها

مباحث این فصل در دو قسمت "مقدماتی" و "حرفه‌ای‌تر شوید" ارائه شده است. در ابتدای هر فصل به بررسی مطالب ساده‌تری پرداخته شده و در قسمت "حرفه‌ای‌تر شوید" مباحث تخصصی‌تری مربوط به پشتیبانی از نرم افزار ها در ویندوز 10 را مورد بررسی قرار داده ایم لذا توصیه می‌شود ابتدا قسمت مباحث ابتدایی را مطالعه کرده و در صورتی که به مطالب تسلط پیدا کردید قسمت "حرفه‌ای‌تر شوید" را مطالعه نمایید.

### پیکربندی تنظیمات نرم افزارهای پیش فرض

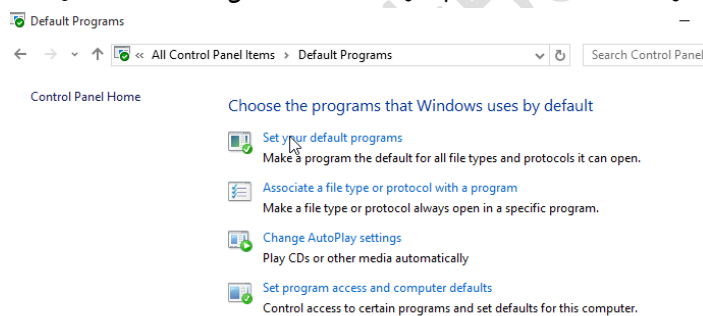
زمانی که کاربر برنامه‌های مختلف از جمله نرم افزار مرورگر وب، مشاهده عکس، مشاهده فایل-های متنی و ... را در ویندوز نصب می‌کند ممکن است که برای انجام یک کار خاص (مانند مشاهده صفحات وب) چندین برنامه موجود باشد. به عنوان مثال برای مشاهده یک صفحه اینترنتی به طور پیش فرض نرم افزار Internet Explorer 11 در ویندوز وجود دارد اما ممکن است نرم افزار-های جانبی دیگری از جمله Google Chrome, Mozilla Firefox و ... بر روی سیستم نصب شده باشد، بنابراین در چنین شرایطی می‌توان تنظیماتی انجام داد تا ویندوز به صورت پیش فرض از یکی از این نرم افزارها برای مشاهده صفحات وب استفاده کند.

در ویندوز 10 Default Programs ابزاری است که با استفاده از آن می‌توان مشخص کرد که در هنگام بازکردن یک فایل خاص (با پسوند مشخص)، از چه برنامه‌ای استفاده شود. برای دسترسی به ابزار Default Programs ابتدا وارد Control Panel شده و سپس بر روی Default Programs دوبار کلیک کنید (برای این که Default Programs را به راحتی پیدا کنید، نحوه نمایش را از حالت Category به Large icon تغییر دهید).



شکل 2-1

بعد از اجرای ابزار Default Programs پنجره‌ای مطابق با شکل 2-2 نمایان خواهد شد.



شکل 2-2

همان‌گونه که در شکل 2-2 قابل مشاهده است، چهار گزینه وجود دارد که شامل:

- **Set your default Programs:** با انتخاب این گزینه می‌توان نرم‌افزار پیش‌فرض را برای اجرا انواع فایل‌ها و پروتکل‌ها مشخص کرد.
- **Associate a file type or protocol with a Program:** با استفاده از این گزینه می‌توان مشخص کرد که فایل‌های خاص توسط چه نرم‌افزاری اجرا شوند. توجه داشته باشید این گزینه زمانی کاربرد دارد که برای یک پسوند خاص چندین نرم‌افزار موجود باشد.
- **Change auto play settings:** با استفاده از این گزینه می‌توان مشخص کرد زمانی که کاربر CD یا DVD را درون درایو قرار می‌دهد چه عملی انجام شود. زمانی که این گزینه تنظیم شود دیگر نیازی نیست تا کاربر مشخص کند که در هنگام ورود دیسک چه عملیاتی انجام شود.

**Set program access and computer defaults**: این گزینه برای کنترل دسترسی یک نرم افزار خاص که توسط کاربر مورد استفاده قرار می گیرد است. به عنوان مثال مشخص کنید که کاربر به چه نرم افزارهایی از طریق Desktop یا محل های دیگر دسترسی دارد. در ادامه قصد داریم تا با این چهار گزینه بیشتر آشنا شده و تنظیمات هر کدام را انجام دهیم.

### تمرین 2-1

عنوان: تنظیم برنامه Internet Explorer به عنوان نرم افزار پیش فرض برای مشاهده صفحات وب

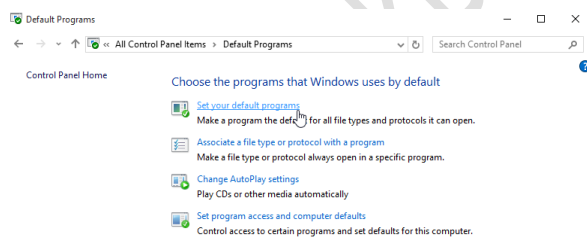
تجهیزات و پیش نیازها:

• ویندوز 10

مراحل تمرین:

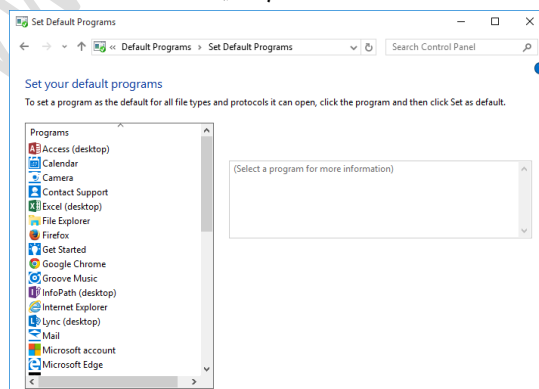
1. Control Panel را باز کرده و سپس بروی Default Programs دوبار کلیک کنید.

2. در پنجره باز شده بروی Set your Default Programs کلیک کنید.



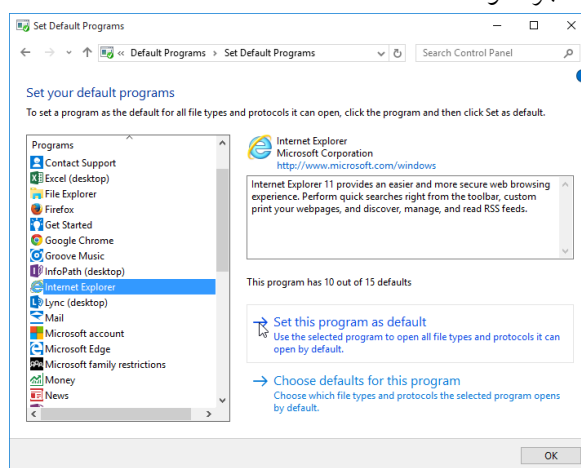
شکل 2-3

3. در پنجره باز شده Internet Explorer را انتخاب کنید.



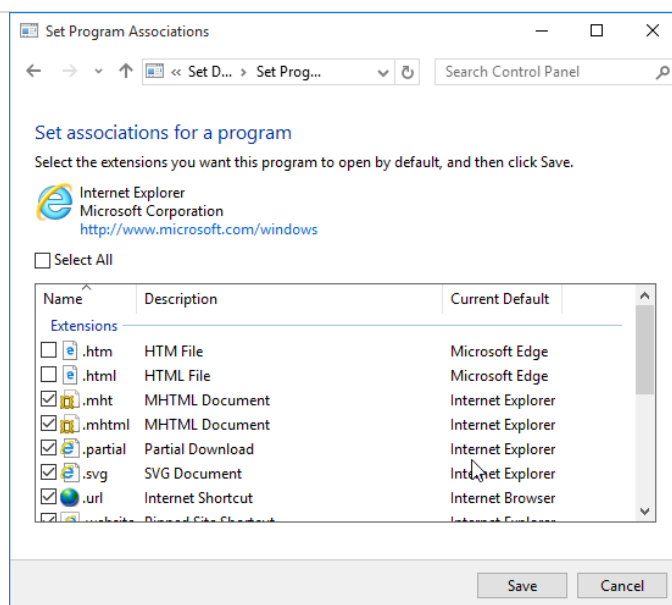
شکل 2-4

4. با انتخاب گزینه Set this Program as the Default تمامی فایل‌های سازگار با این نرم‌افزار از Internet Explorer اجرا خواهند شد.



شکل 2-5

5. با انتخاب گزینه Choose Defaults for this Program می‌توان به صورت جزئی‌تر مشخص کرد که کدام دسته از فایل‌ها توسط Internet Explorer اجرا شوند. با کلیک بر روی این گزینه پنجره‌ای مطابق با شکل 2-6 نمایان خواهد شد. همان‌گونه که در قابل مشاهده است می‌توان تمامی فایل‌ها و پروتکل‌هایی که قابل اجرا با IE هستند را مشاهده کرد. گزینه‌های مورد نظر را انتخاب کرده و بر روی دکمه Save کلیک کنید.



شکل 2-6

## تمرین 2-2

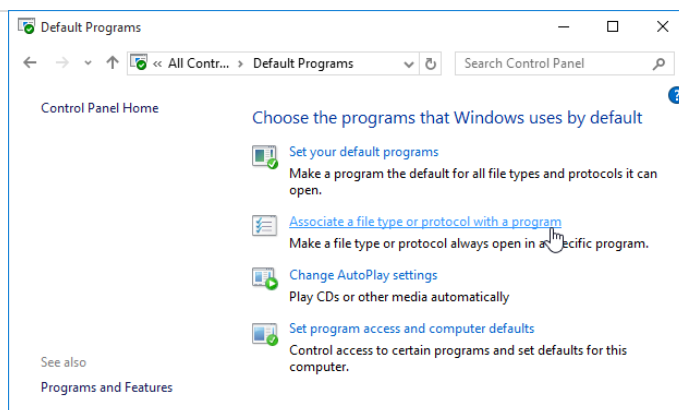
عنوان: تعیین برنامه‌ای مشخص جهت اجرای فایل‌های خاص

مراحل تمرین:

1. Control Panel را باز کرده و سپس بروی Default Programs دوبار کلیک کنید.

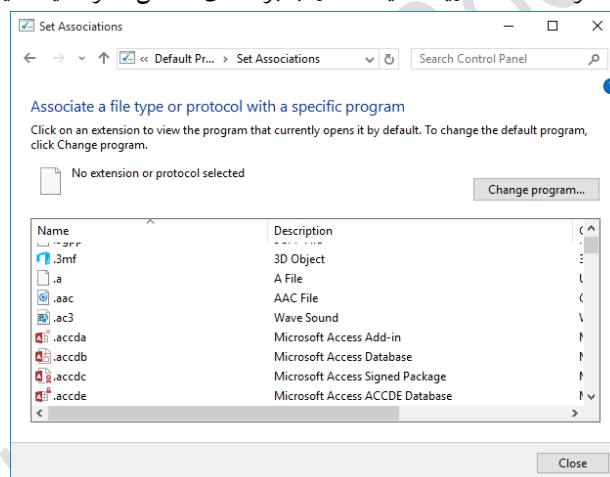
2. در پنجره Default Programs بروی Associate a File type or Protocol with a Program کلیک کنید.





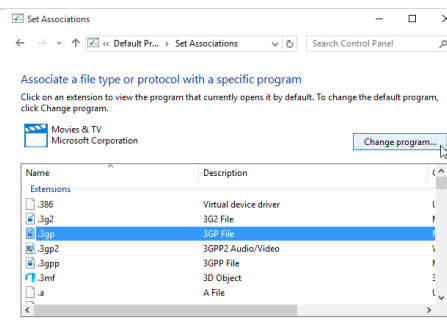
شکل 2-7

3. در پنجره ظاهر شده لیستی از انواع مختلف فایل با پسوندهای متفاوت قابل مشاهده می‌باشد. بر روی فایل موردنظر که قصد دارید همیشه آنرا با برنامه‌ای خاص اجرا کنید کلیک کنید.



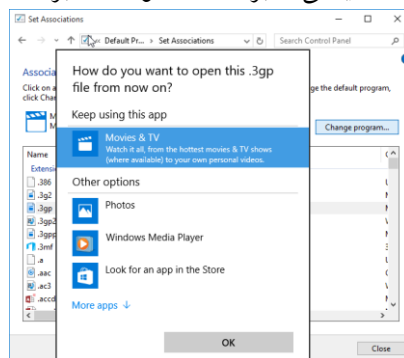
شکل 2-8

4. در ادامه بر روی دکمه Change Program کلیک کنید.



شکل 2-9

5. یک لیست باز شده که در آن لیستی از برنامه‌ها وجود دارد. برنامه مورد نظر را انتخاب کنید.



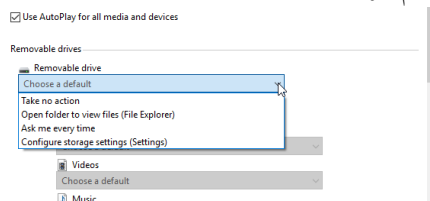
شکل 2-10

### تمرین 2-3

عنوان: تغییر برنامه پیش فرض در هنگام وارد کردن DVD

مراحل تمرین:

1. Control Panel را باز کرده و سپس بروی Default Programs دوبار کلیک کنید.
2. در پنجره Default Programs بروی Change AutoPlay Settings کلیک کنید تا پنجره‌ای مطابق با شکل 2-11 ظاهر شود. در این پنجره می‌توان تنظیمات مربوط به اجرای خودکار CD، DVD، Flash و ... را تنظیم کرد.

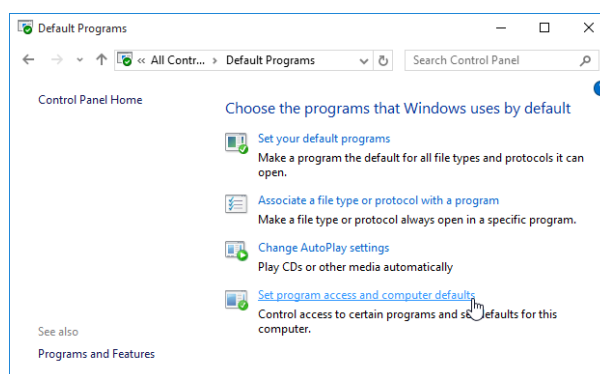


شکل 2-11

3. گزینه مدنظر را انتخاب کرده و در ادامه بر روی Save کلیک کنید.

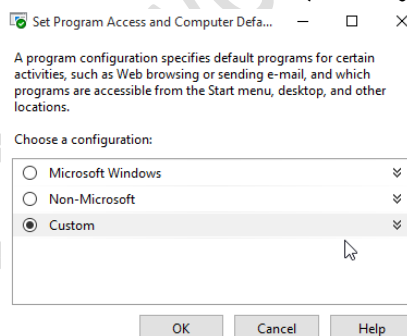
برای تعیین دسترسی نرم افزارهای پیش فرض مراحل زیر را دنبال کنید :

1. در پنجره Default Programs بر روی Set Program Access and Computer Defaults کلیک کنید .



شکل 2-12

2. یکی از گزینه های زیر را انتخاب کنید .

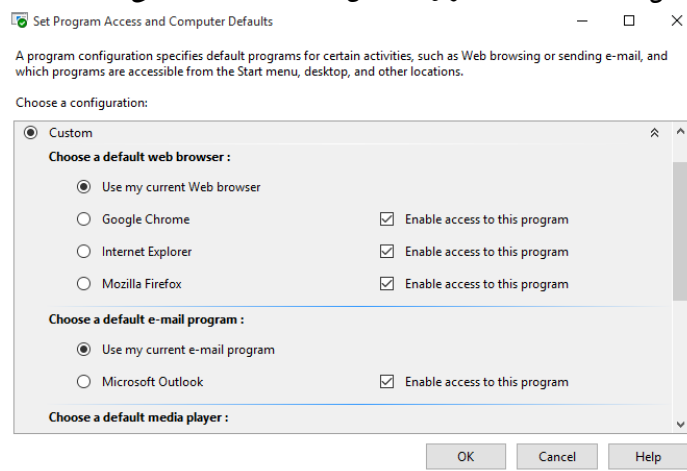


شکل 2-13

**Microsoft Windows** : در صورت انتخاب این گزینه تمام نرم افزارهای مبتنی بر مایکروسافت به عنوان نرم افزار پیش فرض انتخاب می شوند. به عنوان مثال در صورت وجود نرم افزار Outlook این نرم افزار به عنوان نرم افزار پیش فرض برای مدیریت ایمیل انتخاب خواهد شد.

**Non-Microsoft Windows** : با انتخاب این گزینه تمام دسترسی ها از نرم افزارهای مبتنی بر مایکروسافت سلب خواهد شد، همچون Internet Explorer, Windows Media Player, Microsoft Outlook, ...

**Custom**: با استفاده از این گزینه می‌توانید تمامی موارد گفته شده را به صورت دلخواه تنظیم کنید. که در شکل 2-14 تنظیمات مربوط به این قسمت را مشاهده می‌کنید.



شکل 2-14

## نصب و تعمیر نرم افزارها

در ویندوز 10 راه‌های متفاوتی برای نصب و تعمیر نرم افزارهایی که دچار مشکل شده‌اند وجود دارد. در حالت معمولی به منظور نصب نرم افزار کافی است تا فایل نصب آن را اجرا کنید اما در ویندوز 10 می‌توان با استفاده از دستورات متنی عملیات نصب نرم افزار را انجام دهید. یکی دیگر از قابلیت‌هایی که در ویندوز 10 وجود دارد امکان بررسی سازگاری نرم افزارهای مختلف با ویندوز می‌باشد.

1. استفاده از دستور MSIExec به منظور نصب نرم افزار
2. استفاده از ACT به منظور بررسی سازگاری نرم افزار با ویندوز 10

### دستور MSIExec

همان‌گونه که گفته شد با استفاده از این دستور می‌توان عملیات نصب نرم افزارهای متفاوت را انجام داد و علاوه بر این موضوع می‌توان عملیات‌های دیگر از جمله تعمیر نرم افزارها را نیز انجام داد. به منظور استفاده از MSIExec می‌بایست از محیط دستوری CMD استفاده کنید. شکل کلی دستور msiexec به شکل زیر است:

```
msiexec /i {Package | Product Code}
```

این دستور دارای پارامترهای زیادی می‌باشد که در اینجا سوئیچ /i نشان‌دهنده آن سوئیچ نصب

نرم افزار است.

**Package**: مشخص کننده نام و مسیر مربوط به نرم افزاری است که قصد نصب آنرا دارید.

**Product Code**: عددی منحصر به فرد برای Windows installer است.

در جدول 1-2 پارامترهای دستور `msiexec` نشان داده شده است.

Parameter	Additional commands	What it does
/a		Applies the administrative installation option.
/f	Below are the additional commands you can use with /f and may be used as so: <code>msiexec /fpecms Example.msi</code>	Enables the use of various repair parameters and is used as so: <code>msiexec /f [p][o][e][d][c][u][m][s][v](Package   ProductCode)</code>
	P	Reinstalls only if file is missing.
	O	Reinstalls if file is missing or if an older version is installed.
	E	Reinstalls if file is missing or an equal or older version is installed.
	D	Reinstalls if file is missing or a different version is installed.
	C	Reinstalls if file is missing or the stored checksum does not match the calculated value.
	A	Forces all files to be reinstalled.
	U	Rewrites all required user-specific registry entries.
	m	Rewrites all required computer-specific registry entries.
	s	Overwrites all existing shortcuts.
	v	Runs from source and recaches the local package.
/x		Uninstalls a product.
/j	Below are commands you can use with /j and may be used as so: <code>msiexec /j [(u   m)] Package</code>	Advertises a product.
	U	Advertises a product to the current user.
	M	Advertises a product to all users of the computer.
/p		Applies an update.

جدول 1-2

## تمرین 2-4

**عنوان:** آشنایی با نحوه استفاده از دستور `MSIExec`

**شرح:** در این تمرین قصد داریم تا با استفاده از دستور `MSIExec` فایل نصب نرم افزار

`xmlnotepad` را بروی ویندوز 10 به نحوی نصب کنیم که کاربر از مراحل نصب آگاه نشود.

**تجهیزات و پیش نیازها:**

• ویندوز 10

• وجود فایل `Setup` نرم افزار `xmlnotepad`

مراحل تمرین:

1. ابتدا محیط Command Prompt را باز کنید.

2. دستور زیر را وارد کرده و سپس دکمه Enter را فشار دهید.

`Msiexec /I c:\xmlnotepad.msi /passive`

Administrator: Command Prompt

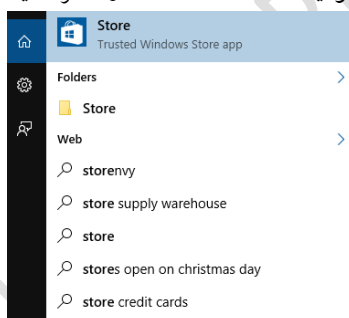
C:\Users\Zarrafe>msiexec /i c:\xmlnotepad.msi /passive

شکل 2-15

3. بعد از گذشت چند ثانیه برنامه نصب شده و می توانید از آن استفاده نمایید.

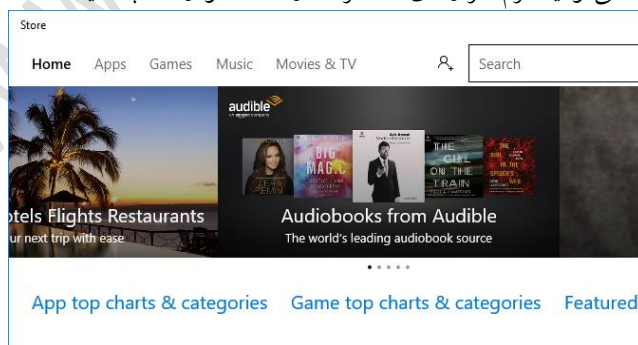
## مدیریت برنامه های Windows Store

کلمه store را جستجو کنید تا بتوانید Windows Store را اجرا کنید.



شکل 2-16

در پنجره باز شده می توانید نرم افزارهای مدنظرتان را جستجو و نصب کنید.



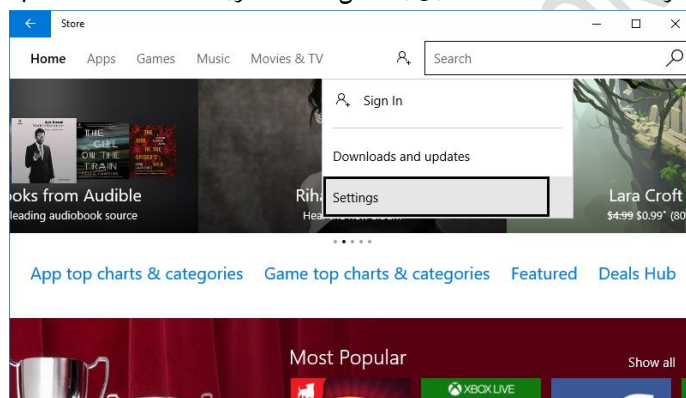
شکل 2-17

به صورت پیش فرض تمام برنامه‌ها از طریق Windows Store نصب می‌شوند این قابلیت را دارند تا به صورت خودکار عملیات بروزرسانی خودشان را انجام دهند. از این رو ممکن است تا حجم زیادی از پهنای باند اینترنت صرف بروزرسانی نرم‌افزارهای Windows Store گردد. به منظور محدود و یا غیرفعال کردن این عملیات بروزرسانی تمرین زیر را انجام دهید.

## تمرین 2-5

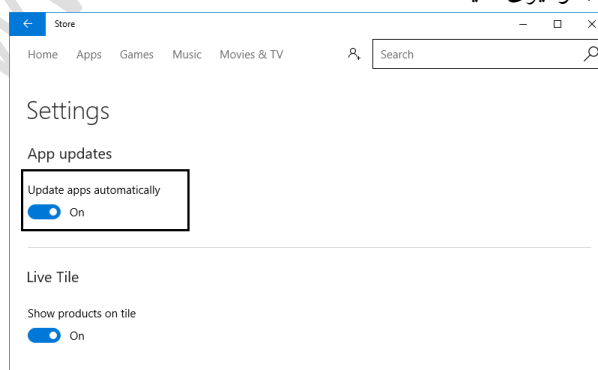
عنوان: غیرفعال‌سازی عملیات بروزرسانی در Windows Store  
مراحل تمرین:

1. از منوی استارت Store را جستجو و اجرا کنید.
2. در پنجره Windows Store مطابق با شکل 2-18 گزینه Settings را انتخاب نمایید.



شکل 2-18

3. در این پنجره می‌توانید خاموش کردن گزینه `update app automatically` از به روز رسانی برنامه‌ها جلوگیری کنید.



شکل 2-19

## کنترل دسترسی به نرم افزارها و سخت افزارها

کنترل دسترسی به نرم افزار و یا سخت افزارها یکی از موارد مهم در ویندوز 10 می باشد. به عنوان مثال می توان مشخص کرد که کاربر اجازه اجرای یک سری نرم افزار را داشته باشد یا خیر و یا این که کاربر از چه سخت افزارهایی می توانند استفاده کند. برای این منظور چندین روش مختلف با قابلیت های متفاوت ارائه شده است که شامل:

- محدود کردن نرم افزارها با استفاده از App Locker
- محدود کردن نرم افزارها با استفاده از Software Restriction Policies
- مدیریت نصب و دسترسی Removable Device ها

### محدود کردن نرم افزار با استفاده از App Locker

محدودسازی دسترسی کاربران امری است که در بسیاری از سازمان ها و ادارات مورد توجه قرار می گیرد. با استفاده از App Locker و بدون نیاز به نرم افزارهای جانبی می توان محدودیت ها و دسترسی ها را به راحتی ایجاد کنید.

App locker برای محدود کردن دسترسی ها 4 قانون کلی را ارائه می دهد که شامل:

1. قانون فایل های اجرایی (Executable Rules) که شامل فایل هایی با پسوند .exe و .com است.
  2. قانون پکیج های نصب (Windows Installer Rules) که شامل فایل هایی با پسوند .mst, .msi و .msp است.
  3. قانون اسکریپت های اجرایی (Script Rules) که شامل فایل هایی با پسوند .ps2, .bat, .js, .cmd و .vbs است.
  4. قانون فایل های نصبی (Package app Rules) و در ویندوز 10 آمده است) که فایل هایی با پسوند .appx است.
- توجه داشته باشید که App locker تنها قادر به محدودسازی فایل های اجرایی می باشد.



# پشتیبانی ویندوز 10

پشتیبانی از پیکربندی  
سخت افزارها و درایورها



این PDF به صورت تصویری و مرحله به مرحله توضیح داده شده است.

[www.NetworkBooks.ir](http://www.NetworkBooks.ir)

[www.TejaratServer.ir](http://www.TejaratServer.ir)



برگرفته از پروژه های عملی شرکت



# فصل سوم

پشتیبانی از پیکربندی سخت‌افزارها و درایورها

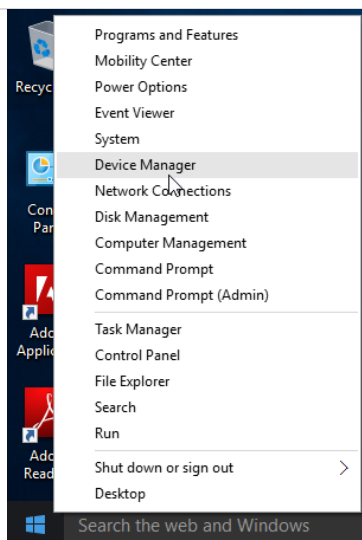


### سیستم نصب و مدیریت سخت افزارها و درایورها

یکی از موارد مهم و اساسی بعد از نصب ویندوز، نصب درایورهای مربوط به دستگاه‌های سخت-افزاری (مانند کارت گرافیک، پرینتر، اسکنر و ...) می‌باشد. نصب درایورها از اهمیت ویژه‌ای برخوردار است چراکه ویندوز زمانی می‌تواند از نهایت قدرت سخت‌افزار استفاده کند که درایور مربوط به سخت‌افزار به درستی در ویندوز شناسایی شده باشد. در گذشته نصب اکثر دستگاه‌ها توسط یک دیسک جداگانه که درایور بر روی آن قرار داشت صورت می‌پذیرفت اما امروزه ویندوز این قابلیت را دارد که بتواند درایورهای مربوط به سخت‌افزار را تشخیص داده و نصب کند. گاهی اوقات نیز مشکلاتی در نصب درایورها پیش می‌آید که ممکن است این مشکل ناشی از عدم-سازگاری درایور با ویندوز 10 و یا ناشی از Certificate های نامعتبر می‌باشد. یکی از اصلی‌ترین بخش‌های ویندوز Device Manager بوده که با استفاده از آن می‌توان به مدیریت درایورهای مربوط به سخت‌افزارها پرداخت.

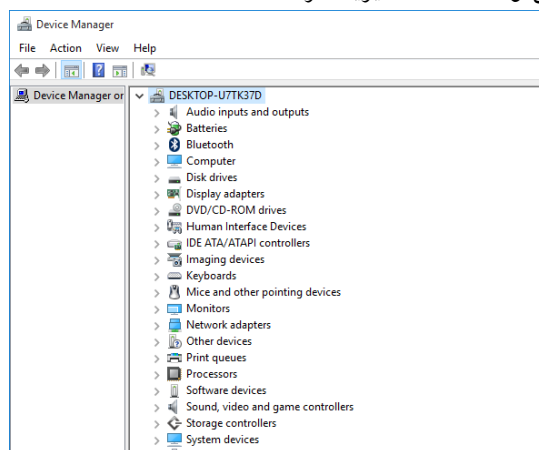
### نصب و مدیریت درایورها به کمک Device Manager

ابزار Device Manager برای نمایش، نصب، حذف، فعال و غیرفعال کردن درایور دستگاه‌های سخت‌افزاری استفاده می‌شود. به منظور اجرای Device Manager کافی است تا بر روی Start راست کلیک کرده و گزینه Device Manager را انتخاب کنید.



شکل 3-1

پنجره‌ای مطابق با شکل 3-2 نمایان خواهد شد که لیستی از تمام سخت‌افزارها و وضعیت آنها قابل مشاهده است و می‌توان آنها را مدیریت کرد.



شکل 3-2

### بررسی گزینه‌های موجود در منو اصلی ابزار Device Manager

ابزار Device Manager همانند سایر برنامه‌ها دارای یک منو بوده و همان‌گونه که در شکل 3-2 قابل مشاهده است در آن گزینه‌های File، Action، View و Help قرار دارد.

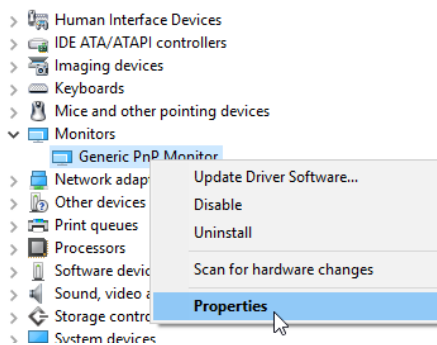
**منو File:** از منوی File گزینه option را انتخاب کنید. تغییراتی را که در کنسول هر Device ایجاد می کنید در Profile آن دستگاه ذخیره می کند که می توانید با زدن Delete Files آن ها را پاک کنید. **منو Action:** از این منو به منظور دسترسی به فرمان های مختلف استفاده می شود که شامل: بروزرسانی درایور، فعال و غیرفعال کردن درایور، حذف درایور، بررسی تغییرات سخت افزاری و اضافه کردن سخت افزار جدید می باشد.

**منو View:** با استفاده از این منو می توان نحوه نمایش دسته بندی های دستگاه ها را در Device Manager تغییر دهید.

**منو Help:** از این منو می توان برای دستیابی به راهنما استفاده کرد.

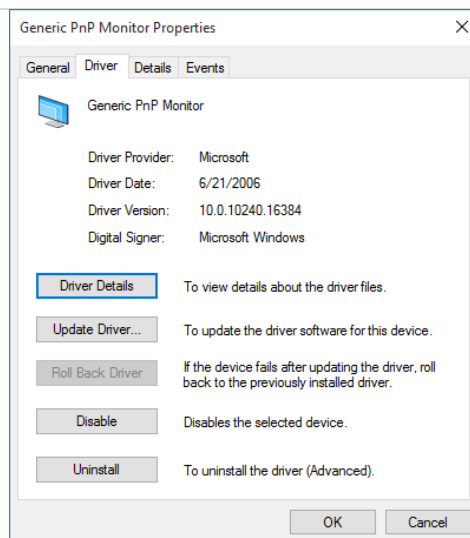
### لیست دستگاه های موجود در Device Manager

در صفحه اصلی Device Manager لیستی از تمام دستگاه های متصل شده به سیستم را مشاهده می کنید که در این لیست دسته بندی های متفاوتی از دستگاه ها ایجاد شده است. به عنوان مثال لیستی از هارد دیسک های موجود در دسته Hard Drives قرار می گیرند. به منظور دستیابی به اطلاعات بیشتر در مورد یک دستگاه کافی است تا بر روی آن راست کلیک کرده و سپس گزینه Properties را انتخاب نمایید.



شکل 3-3

بعد از انتخاب گزینه Properties پنجره ای مطابق با شکل 3-4 نمایش داده خواهد شد که در آن 4 سربرگ از جمله General، درایور، Details و Events وجود دارد.



شکل 3-4

**سربرگ General:** در این سربرگ اطلاعاتی از جمله نوع دستگاه، کارخانه تولیدکننده و وضعیت فعلی دستگاه را نشان می‌دهد.

**سربرگ Driver:** در این سربرگ یکسری جزئیات در مورد درایور نشان داده شده است و می‌توان آن را بروزرسانی، غیرفعال و حذف نمایید.

**سربرگ Details:** در این سربرگ دو قسمت **Property** و **Value** وجود دارد که با انتخاب گزینه‌های موجود در **Property** می‌توان جزئیات بیشتری در مورد دستگاه را مورد بررسی قرار دهید.

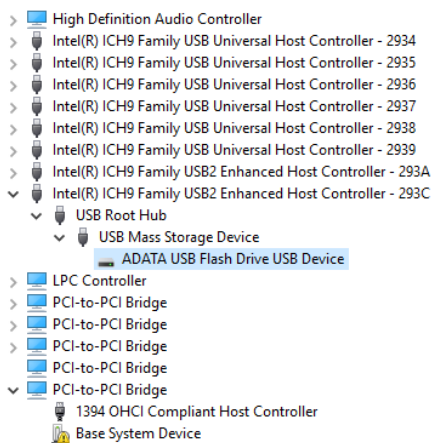
**سربرگ Events:** در این سربرگ می‌توان رخدادهای صورت گرفته برای دستگاه را مورد بررسی قرار دهید.

### بررسی حالت‌های مختلف نمایش دستگاه‌ها در Device Manager

گاهی اوقات لازم است تا نحوه نمایش لیست دستگاه‌ها در پنجره **Device Manager** را تغییر داد. به‌عنوان مثال مشخص کرد که چه دستگاه‌هایی به چه پورتی متصل شده‌اند و یا اینکه چه دستگاه‌هایی از چه نوع حافظه‌ای استفاده می‌کنند. برای این منظور در **Device Manager** چهار حالت مختلف برای نمایش دستگاه‌ها وجود دارد که از منوی **View** در دسترس بوده و شامل موارد زیر می‌باشد:

**Devices By Connection:** زمانی از این گزینه استفاده می‌شود که نیاز باشد تا بررسی کنید چه دستگاهی از طریق چه درگاهی به سیستم متصل شده است.

به عنوان مثال به شکل 3-5 دقت کنید:



شکل 3-5

در شکل 3-5 مشخص است که حافظه USB Flash به یکی از درگاه‌های USB از سیستم متصل شده است که سریال آن 293C می‌باشد.

**Devices By Type:** این حالت از نمایش، حالت پیش فرض بوده و تمامی دستگاه‌ها را متناسب با ماهیت‌شان دسته‌بندی می‌شوند. به عنوان مثال تمامی هارددیسک‌ها را در یک دسته نمایش می‌دهند.

**Resources By Type:** با استفاده از این گزینه می‌توان تمام منابع اختصاص داده شده به دستگاه‌ها را مورد بررسی قرار داد. این منابع شامل: دسترسی به حافظه مستقیم (DMA)، ورودی/خروجی (IO)، درخواست وقفه (IRQ)، آدرس‌های حافظه و ... می‌باشد.

**Resources By Connection:** با استفاده از این گزینه می‌توان تمام منابع اختصاص داده شده به دستگاه‌ها را با توجه به نوع اتصالشان به سیستم مورد بررسی قرار داد.

در تمرین 3-1 قصد داریم تا شما را با یک نمونه بارز از کاربردهای Device Manager در عیب‌یابی درایورها آشنا کنیم.

### تمرین 3-1

**عنوان:** بررسی تداخل درایورهای نصب‌شده بر روی سیستم

**شرح:** گاهی اوقات پیش می‌آید که در هنگام نصب درایورها کارکرد سیستم دچار نقص شده و با مشکل مواجه شده است. سعی داریم تا با استفاده از ابزار Device Manager این مشکل را پیدا کنیم.

تجهیزات و پیش‌نیازها:

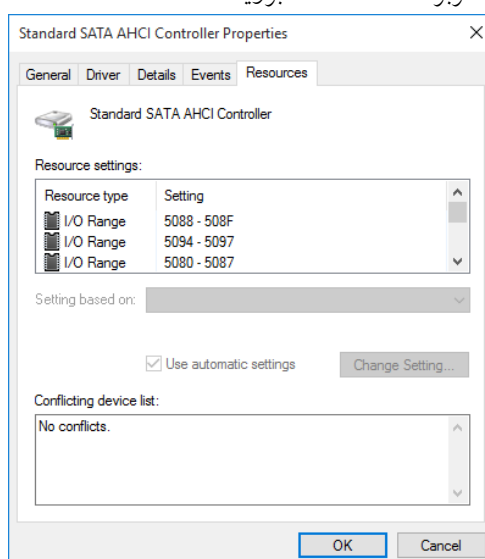
• ویندوز 10

مراحل تمرین:

ابزار Device Manager را اجرا کنید.

از منوی View یکی از گزینه‌های Resources By Type و یا Resources By Connection را انتخاب کنید.

1. بر روی دستگاهی که فکر می‌کنید درایورهایش مشکل دارد دوبار کلیک کنید.
2. در پنجره باز شده به سربرگ Resources بروید.

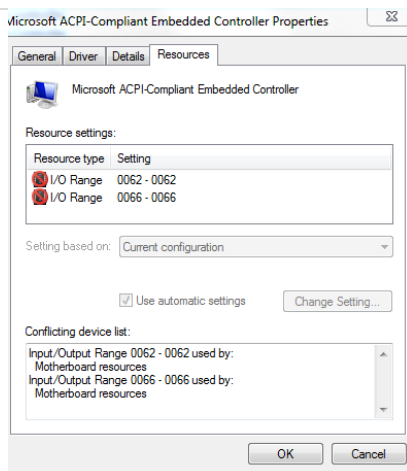


شکل 3-6

3. در صورتی که سخت‌افزار موردنظر با سخت‌افزار دیگری تداخل داشته باشد در قسمت Conflicting Device List نمایش داده خواهد شد.

به‌عنوان مثال در شکل 3-6 هیچ‌گونه تناقضی بین درایورها وجود ندارد اما در شکل 3-7 قابل مشاهده است که کدام دستگاه‌ها با یکدیگر دارای تناقض هستند.





شکل 3-7

### نصب و حذف درایورها

در ویندوز اکثر درایورها به صورت خودکار نصب خواهند شد اما در بعضی مواقع یکسری از آن‌ها شناسایی نشده و نصب نخواهند شد، بنابراین باید از روش‌های دیگری جهت نصب آن‌ها اقدام کرد.

- استفاده از **Action Center**: در واقع Action Center ابزاری است که با استفاده از آن می‌توان مشکلات فعلی در درایورها را بررسی کرده و به صورت خودکار راه‌حلی مناسب را ارائه می‌کند.
- **دانلود درایور**: یکی دیگر از روش‌های نصب درایور، مراجعه به سایت سازنده دستگاه و دانلود فایل‌های مورد نیاز است.

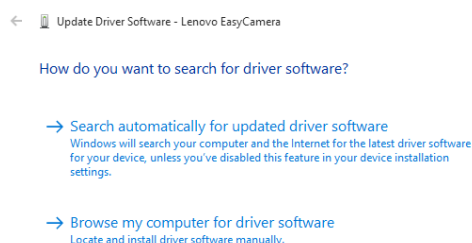
توجه داشته باشید که ویندوز به صورت خودکار در هنگام به‌روزرسانی فایل‌های اصلی سیستم-عامل (با استفاده از ابزار Windows Update)، درایورها را نیز دانلود و نصب خواهد کرد. این موضوع زمانی صحت خواهد داشت که نوع اتصال سیستم به اینترنت در حالت Metered Connection نباشد. در غیر این صورت (اگر اتصال به اینترنت از نوع Metered Connection باشد) عملیات دانلود به صورت خودکار انجام نخواهند شد.

### بروزرسانی درایورهای نصب شده

توجه داشته باشید که با استفاده از ابزار Device Manager می‌توان عملیات بروزرسانی درایورها را نیز انجام داد. بروزرسانی درایورها از این جهت حائز اهمیت می‌باشد که ممکن است درایورهای نصب شده به درستی عمل نکرده و نیاز است تا آن‌ها را بروزرسانی کنید. برای این

منظور کافی است تا ابتدا Device Manager را اجرا کرده و سپس بروی سخت‌افزار موردنظر راست‌کلیک کرده و گزینه Update Driver Software را انتخاب کنید. در پنجره باز شده دو گزینه وجود دارد که شامل:

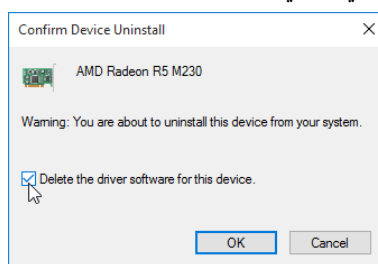
- **Search automatically for updated driver software**: استفاده از این گزینه باعث می‌شود تا به صورت آنلاین آخرین نسخه درایور دانلود و نصب شود.
- **Browse my computer for driver software**: استفاده از این گزینه باعث می‌شود تا بتوان درایورهای از قبل دانلود شده را نصب کنید.



شکل 3-8

## حذف درایورها با استفاده از Device Manager

به منظور حذف یک درایور کافی است تا بروی سخت‌افزار موردنظر راست‌کلیک کرده و گزینه Uninstall را انتخاب کنید. در پنجره باز شده گزینه Delete the driver software for this device را انتخاب کرده و بروی OK کلیک کنید.



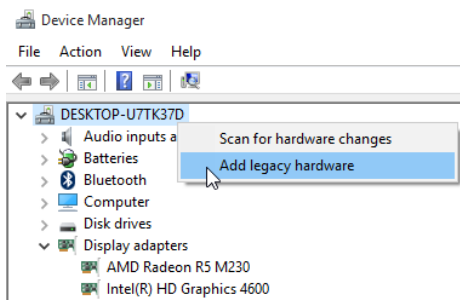
شکل 3-9

## نصب درایورها برای دستگاه‌های قدیمی

دستگاه‌هایی که از اینترنت سرچ استفاده نکرده و قدیمی هستند به‌عنوان دستگاه‌های Legacy شناخته شده و برای نصب آن‌ها باید مراحل زیر را طی کنید.

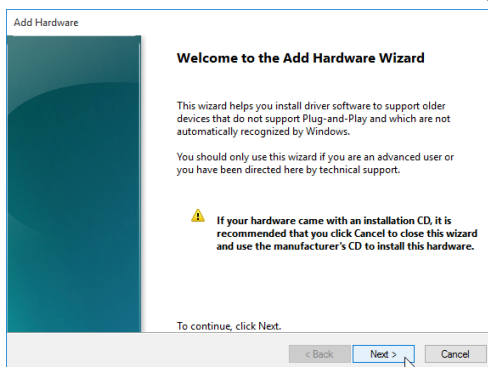
1. ابتدا ابزار Device Manager را اجرا کرده و سپس از منوی Action گزینه

Add Legacy Hardware را انتخاب کنید.



شکل 3-10

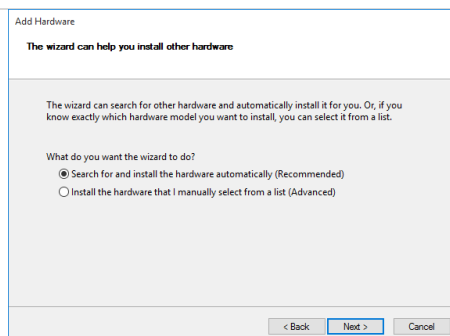
2. در پنجره باز شده بر روی دکمه Next کلیک کنید.



شکل 3-11

3. در ادامه دو گزینه وجود دارد که شامل:

- **Search for and install the hardware automatically (Recommended)**: با انتخاب این گزینه سیستم به صورت خودکار شروع به جستجوی دستگاه‌ها کرده و آنرا نصب می‌کند.
- **Install the hardware that I manually select from a list**: انتخاب این گزینه باعث می‌شود تا بتوانید یک لیست از کل سخت‌افزارها را مشاهده کرده و موارد موردنظر را نصب کنید.

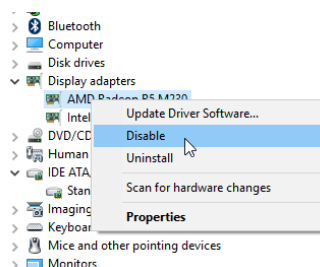


شکل 3-12

### غیرفعال کردن درایور و بازگشت به حالت قبل

گاهی اوقات لازم است تا یک یا چند سخت افزار را غیرفعال کرد، توجه داشته باشید که انجام این کار با حذف سخت افزار کاملاً متفاوت می باشد. هنگامی که سخت افزار غیرفعال می شود، ویندوز تلاشی در فعال سازی مجدد آن نداشته اما زمانی که یک درایور حذف می شود، ویندوز در راه اندازی مجدد (Restart) تمامی سخت افزارهای ناشناخته را بررسی کرده و سعی می کند تا آنها را نصب کند.

برای غیرفعال سازی یک Device کافی است بر روی آن راست کلیک کرده و گزینه Disable را انتخاب کنید.



شکل 3-13

☑ یکی از دلایل اصلی غیرفعال سازی درایور زمانی است که نیاز به بررسی تداخل های به وجود آمده در سیستم باشد. به عنوان مثال درایورای که در عملکرد سیستم اختلال ایجاد کرده است را می توان به صورت موقت غیرفعال کرده تا از صحت این موضوع اطمینان حاصل نمایید.

گاهی اوقات با انجام به روزرسانی های درایور ممکن است تا مشکلات جدیدی (از جمله بروز تداخل درایور جدید با سایر درایورهای موجود) به وجود آید که این موارد را می توان با بازگشت به حالت قبل (Rollback) برطرف کرد. توجه داشته باشید که گزینه Rollback زمانی فعال خواهد شد که درایور جدیدی بر روی درایور قدیمی نصب شده باشد.

## پیکربندی دستگاه‌ها

بعد از این که نصب درایورها به پایان رسید شما قادر خواهید بود تا تنظیمات مربوط به دستگاه‌ها را انجام دهید. برای این منظور راه‌های متفاوتی وجود دارد که در اینجا به دو روش رایج‌تر خواهیم پرداخت.

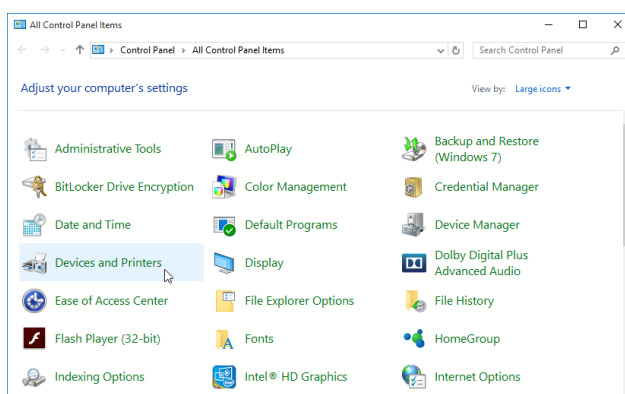
1. روش اول استفاده از Devices and Printers

2. روش دوم استفاده از Device Stage

## استفاده از Devices and Printers

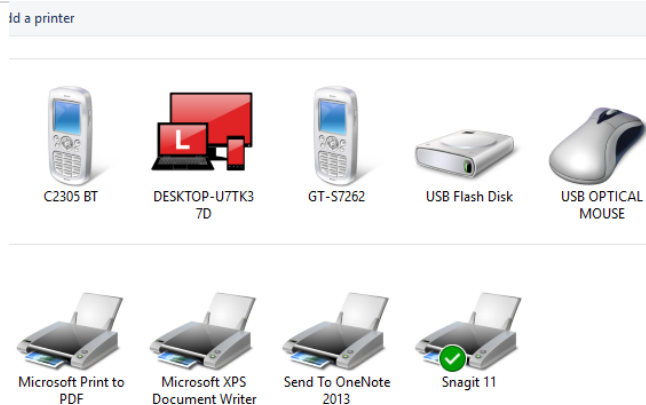
برای دسترسی به Devices and Printers مراحل زیر را انجام دهید.

1. ابتدا وارد Control Panel شده و سپس بروی Devices and Printers دوبار کلیک کنید.



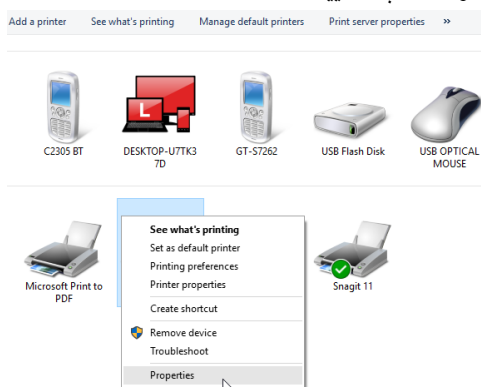
شکل 3-14

2. در پنجره باز شده تمامی دستگاه‌هایی که نصب شده‌اند نمایش داده می‌شوند.



شکل 3-15

3. به منظور تغییر تنظیمات دستگاه‌ها کافی است تا بر روی دستگاه موردنظر راست کلیک کرده و سپس گزینه Properties را انتخاب نمایید.



شکل 3-16

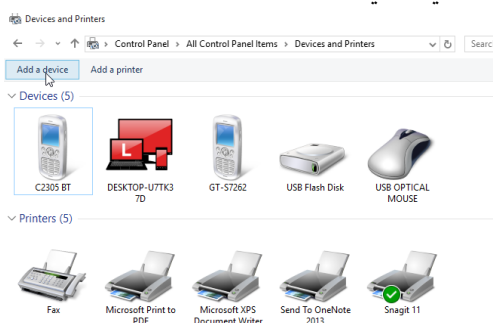
4. با توجه به دستگاهی که انتخاب کرده‌اید، در پنجره Properties سربرگ‌های متفاوتی را مشاهده خواهید کرد که می‌توانید تنظیمات موردنظر خود را انجام دهید. این روش یکی از ساده‌ترین و سریع‌ترین روش‌ها به منظور دسترسی به تنظیمات و اعمال تغییرات لازم بر روی دستگاه‌ها می‌باشد.

### اضافه کردن دستگاه جدید از طریق Devices and Printers

یکی دیگر از کاربردهای برنامه Devices and Printers اضافه کردن دستگاه‌های جدید به ویندوز می‌باشد (منظور همان نصب درایور است). برای این منظور کافی است تا مراحل زیر را انجام دهید:

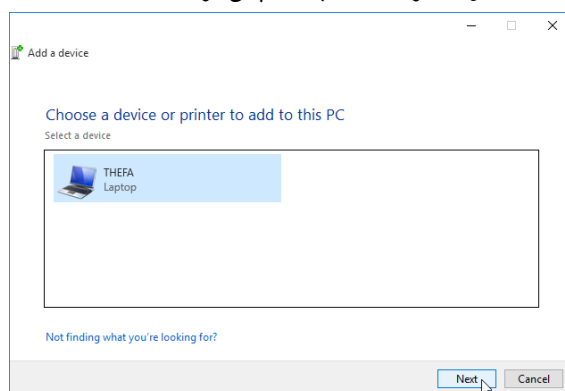
1. ابتدا از طریق Control Panel ابزار Devices and Printers را اجرا کنید.

2. بروی Add a device کلیک کنید.



شکل 3-17

3. با انتخاب این گزینه تمامی دستگاه‌هایی که توسط ویندوز کشف می‌شوند را لیست کرده و در ادامه کافی است تا دستگاه موردنظر را انتخاب و سپس بروی Next کلیک کنید.



شکل 3-18

4. در ادامه مراحل نصب دستگاه به اتمام خواهد رسید و می‌توانید دستگاه جدید را در لیست Devices and Printers مشاهده نمایید.

### بررسی امنیتی درایورهای نصب شده

یکی از موارد مهم در هنگام تهیه درایور بررسی اصالت آن می‌باشد چرا که گاهی اوقات ممکن است درایورهای نصب شده دارای برنامه‌های مخرب و یا ویروس باشند. به منظور بررسی امنیت و اطمینان از صحت درایورهای نصب شده کافی است تا مراحل زیر را انجام دهید:

1. Command Prompt را در حالت Administrator اجرا کنید (برروی Command Prompt

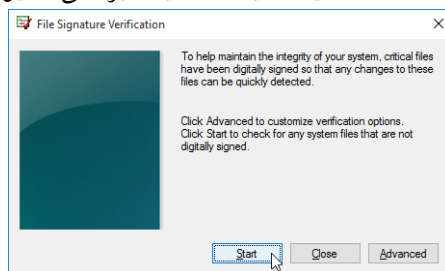
راست کلیک کرده و گزینه Run as Administrator را انتخاب نمایید).  
 2. در پنجره cmd عبارت sigverif را تایپ کرده و کلید Enter را فشار دهید.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>sigverif_
```

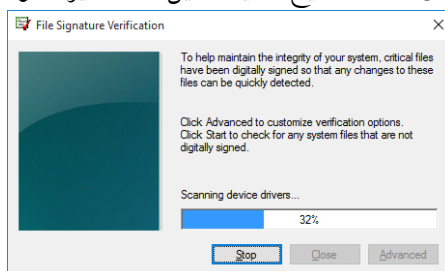
شکل 3-19

3. در این پنجره بروی دکمه Start کلیک کنید تا عملیات بررسی درایورها شروع شود.



شکل 3-20

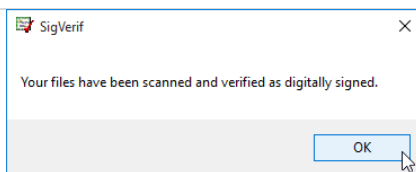
4. بعد از بررسی درایورهای دستگاه نتایج در یک فایل log ذخیره خواهد شد.



شکل 3-21

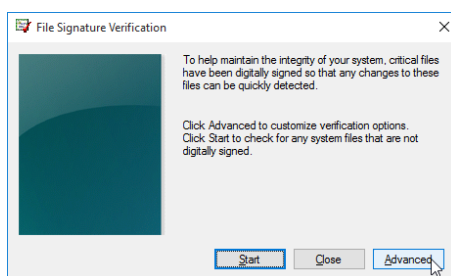
5. با مشاهده پیغامی مانند شکل 3-22 بروی OK کلیک کنید.





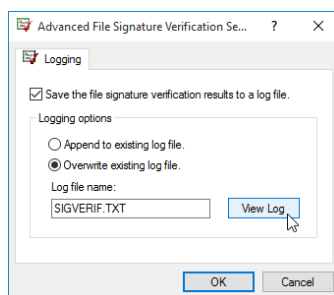
شکل 3-22

6. در پنجره File Signature Verification بر روی دکمه Advanced کلیک کنید.



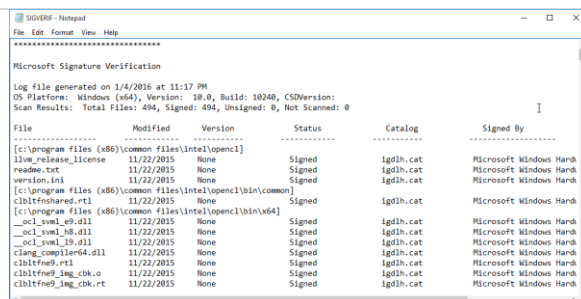
شکل 3-23

7. در پنجره باز شده بر روی دکمه View Log کلیک کنید.



شکل 3-24

8. در پنجره باز شده می‌توانید جزئیات بیشتری از درایورها کسب کنید.



شکل 3-25

پس از اتمام بررسی اگر که درایوری به صورت Unassigned پیدا شود، سخت‌افزار و دستگاه مرتبط با این درایور به شما نشان داده خواهد شد و با توجه به نتایج به دست آمده می‌توانید به حل مشکلات بپردازید.

توجه داشته باشید که درایور بعضی از دستگاه‌ها به صورت Unassigned توسط شرکت سازنده نصب می‌شوند اما آن دسته از درایورهایی که توسط کاربر دست‌کاری می‌شوند توسط ویندوز تشخیص داده شده و اعلان می‌گردند.

در زمان نصب درایورهای جدید ممکن است که ویندوز تعدادی از آن‌ها را از نوع Unassigned تشخیص دهد و با یکی از سه پیغام زیر مواجه شوید که در ادامه مورد بررسی قرار گرفته است.

### سیاست‌های نصب درایور با استفاده از Policy Editor

یکی از مواردی که همواره مدنظر است عدم وجود امکان نصب درایور توسط کاربران عادی می‌باشد. یکی از دلایل اصلی این موضوع این است که کاربران عادی باید تنها قادر به نصب درایورهایی باشند که از قبل توسط مدیر تست شده و مشکلی نداشته باشند. برای کنترل و مدیریت بهتر چنین مواردی می‌توان از Local Group Policy Editor استفاده کنید که در تمرین 3-2 با نحوه کار این کنسول آشنا خواهید شد.

### تمرین 3-2

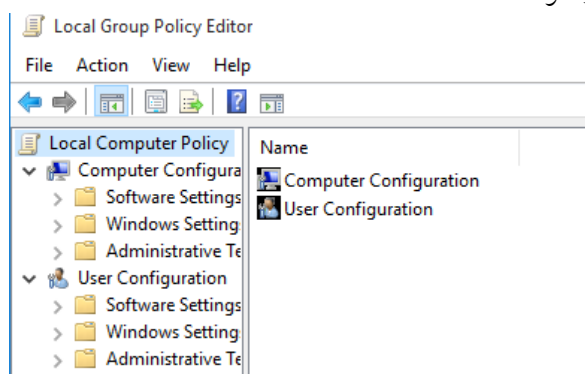
عنوان: استفاده از Group Policy و پیکربندی ویندوز جهت اجازه کاربران جهت نصب درایور بر روی سیستم.

تجهیزات و پیش‌نیازها:

• ویندوز 10

مراحل تمرین:

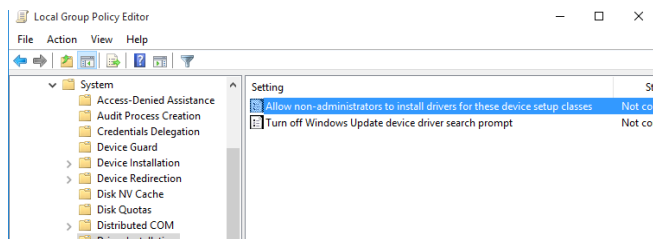
1. در Run عبارت gpedit.msc را تایپ کرده و بر روی دکمه OK کلیک کنید تا کنسول Group Policy باز شود.



شکل 3-26

2. در پنجره باز شده مسیر زیر را طی کنید.

Computer Configuration → Administrative Templates → System → Driver-Installation

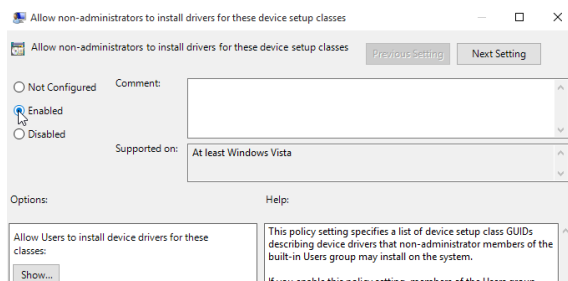


شکل 3-27

3. در ادامه بر روی Allow Non-Administrators To Install Drivers For These Device

Setup Classes دوبار کلیک کنید تا پنجره‌ای مطابق با شکل 3-28 باز شود.

4. با انتخاب گزینه Enable می‌توان به کاربران عادی نیز اجازه بروزرسانی درایورها را اعطاء نمود.



شکل 3-28

# پشتیبانی ویندوز 10

پشتیبانی از تنظیمات شبکه



این PDF به صورت تصویری و مرحله به مرحله توضیح داده شده است.

[www.NetworkBooks.ir](http://www.NetworkBooks.ir)  
[www.TejaratServer.ir](http://www.TejaratServer.ir)



برگرفته از پروژه های عملی شرکت



# فصل چهارم

## پشتیبانی از تنظیمات شبکه

مباحث این فصل در دو قسمت "مقدماتی" و "حرفه‌ای‌تر شوید" ارائه شده است. در ابتدای هر فصل به بررسی مطالب ساده‌تری پرداخته شده و در قسمت "حرفه‌ای‌تر شوید" مباحث تخصصی‌تری مربوط به پشتیبانی از تنظیمات شبکه را مورد بررسی قرار داده ایم لذا توصیه می‌شود ابتدا قسمت مباحث ابتدایی را مطالعه کرده و در صورتی که به مطالب تسلط پیدا کردید قسمت "حرفه‌ای‌تر شوید" را مطالعه نمایید.

## آشنایی با آدرس‌دهی IP

آدرس‌دهی لایه 3 در پشته پروتکل TCP/IP از نوع IP است. آدرس IP یک عدد 32 بیتی است و هر کلاینتی که بخواهد به شبکه متصل شود باید از آن استفاده کند. در آن واحد هر آدرس IP در جهان مختص به یک کلاینت بوده و به صورت انحصاری مورد استفاده قرار می‌گیرد. آدرس‌های IP به چهار قسمت 8 بیتی (4 بایت) تقسیم می‌شوند و هر قسمت با استفاده از نقطه مجزا می‌شوند.

از آنجایی که هر بیت 2 حالت (0 یا 1) می‌تواند داشته باشد، پس در نتیجه با استفاده از 32 بیت می‌توان  $2^{32}$  حالت مختلف را ایجاد کرد که هر حالت معادل با یک عدد است. حالت‌های مختلفی که می‌توان با 32 بیت ایجاد کرد برابر با  $2^{32} = 4.294.967.296$  خواهد بود.

### نحوه نمایش آدرس‌های IP

جهت نمایش آدرس‌های IP می‌توان از دو حالت استفاده کرد.

1. **حالت دهدهی (Decimal):** این حالت، مرسوم‌ترین روش جهت نمایش آدرس‌های IP بوده و قسمت‌های مختلف از آدرس به صورت دهدهی نمایش داده می‌شود.

**IP Address:** 129 . 43 . 204 . 242

2. **حالت دودویی (Binary):** در این حالت هر یک از 4 قسمت را به صورت دودویی نشان می‌دهند.

**IP Address:** 10000001 . 00101011 . 11001100 . 11110010

از آنجایی که هر دو روش گفته شده دارای اهمیت بالا در نمایش آدرس‌های IP است. پس در نتیجه به بررسی نحوه تبدیل عدد مبنای 2 به مبنای 10 و بالعکس می‌پردازیم.

### تبدیل عدد مبنای 2 به مبنای 10

برای تبدیل عدد مبنای 2 به 10 در ابتدا کافی است تا عدد دودویی خود را بنویسید و پس در بالای هر عدد ارزش مکانی بیت‌ها را مشخص کنید. به مثال 1 زیر توجه کنید:

**مثال 1:**

می‌خواهیم عدد دودویی 10000001 را به مبنای 10 تبدیل کنیم.

**گام 1** نوشتن عدد مبنای 2 و تعیین ارزش مکانی برای هر بیت

7	6	5	4	3	2	1	0	ارزش مکانی هر بیت
1	0	0	0	0	0	0	1	عدد مبنای دو

**گام 2** عدد 2 را به توان ارزش مکانی هر بیت برسانید.

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$	ارزش مکانی 2
1	0	0	0	0	0	0	1	عدد مبنای 2

**گام 3** نتیجه عدد نوشته شده در قسمت ارزش مکانی را حساب کرده و معادل آن را بنویسید.

128	64	32	16	8	4	2	1	نتیجه عدد به توان رسیده
1	0	0	0	0	0	0	1	عدد مبنای 2

**گام 4** حال باتوجه به عددهای مبنای 2، آن دسته از اعدادی که برابر با 1 است را جدا کرده و نتیجه عدد به توان رسیده را با یکدیگر جمع کنید.

128	64	32	16	8	4	2	1	نتیجه عدد به توان رسیده
1	0	0	0	0	0	0	1	عدد مبنای 2

نتیجه نهایی برابر با  $1+128$  است پس در نتیجه عدد دودویی 10000001 برابر با 129 خواهد بود.

حال که با روال کار آشنا شدید می توانید جهت تسریع در تبدیل اعداد مبنای 2 به مبنای 10 گام های 1، 2 و 3 را یکباره انجام دهید و در مرحله بعد محاسبات مربوط به گام 4 را تکمیل نمایید.

## مثال 2:

عدد (10001001) در مبنای 2 را به مبنای 10 تبدیل کنید.

**گام 1** از راست به چپ معادل هر عدد 2 را به توان ارزش مکانی هر بیت بنویسید.

128	64	32	16	8	4	2	1	معادل عدد مبنای 2 در مبنای 10
1	0	0	0	1	0	0	1	عدد دودویی

**گام 2** اعداد دودویی که برابر با 1 هستند را جدا کرده و معادل دهدهی آن را بنویسید.

128	64	32	16	8	4	2	1	معادل عدد مبنای 2 در مبنای 10
1	0	0	0	1	0	0	1	عدد دودویی

نتیجه نهایی برابر با  $1+8+128$  است پس در نتیجه عدد دودویی 10001001 برابر با 137 خواهد بود.

## تمرین 4-1

1. معادل هریک از اعداد دودویی زیر را در مبنای 10 محاسبه کنید.

- 11000000.01010000.11000010.11000001
- 00010001.10000101.11000011.00110010
- 10010100.10000101.11001011.01010100

حل این تمرین را به شما واگذار می‌کنیم.

2. مشکلات مربوط به آدرس‌های IP زیر را بررسی کنید.

1. 116.117.049.132
2. 131.132.7.1045
3. 151.195.251020
4. 24.32.10110000.30

حل تمرین:

1. در هنگام نوشتن آدرس IP در مبنای 10 نمی‌توان 0 را قبل از اعداد گذاشت: 049
2. آدرس‌های IP ورژن 4 نمی‌توانند بیشتر از چهار قسمت داشته باشند.
3. حداکثر عددی که می‌توان در هر قسمت 8 بیتی ایجاد کرد 255 است.
4. در هنگام نمایش آدرس IP نمی‌توان ترکیبی از اعداد دودویی و دهدهی استفاده کرد.

## تبدیل عدد مبنای 10 به مبنای 2

جهت انجام این کار کافی است تا مراحل زیر را انجام دهید.

در ادامه می‌خواهیم عدد 116 را به مبنای 2 تبدیل کنیم.

**گام 1** ابتدا عدد 2 را از سمت راست به چپ به توان عددهای 0 تا 7 برسانید.

عدد  $116_{10} \leftarrow ( ? )_2$

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$	اعداد توان 2
?	?	?	?	?	?	?	?	معادل بیتی

**گام 2** حال معادل اعداد توان 2 را محاسبه کنید.

128	64	32	16	8	4	2	1	اعداد توان 2
								معادل بیتی

**گام 3** در این گام باید تمام اعدادی که در ساخت 116 مشارکت دارند را پیدا کرده و معادل

بیتی آن‌ها را برابر با 1 و سایر اعدادی که مشارکت ندارند را برابر با صفر قرار دهید. برای این



منظور عدد 116 را باید از سمت چپ‌ترین عدد توان 2 که همان 128 است، کم کنید. از آنجایی که نمی‌توان عدد 116 را از 128 کم کرد می‌توان نتیجه گرفت که 128 در ساخت عدد 116 مشارکت نداشته و در قسمت معادل بیتی باید مقدار صفر را برای آن در نظر بگیرید. حال 116 را باید از عدد توان 2 بعدی (که همان 64 است) کم کنید و مقدار 1 در قسمت معادل بیتی در نظر بگیرید. در ادامه حاصل تفریق را باید از عدد توان 2 بعدی (که همان 32 است) کم کنید و همین روال را تا انتها طی کنید.

برای درک بهتر این گام به قسمت‌های زیر دقت کنید.

**قسمت اول:** عدد 116 را از 128 کم کنید. از آنجایی که این عمل امکان‌پذیر نیست عدد صفر را در قسمت معادل بیتی قرار دهید.

128	64	32	16	8	4	2	1	اعداد توان 2
-128								
116								
0								معادل بیتی

**قسمت دوم:** عدد 116 را از عدد 64 کم کنید (64-116) و عدد 1 را در قسمت معادل بیتی قرار دهید.

128	64	32	16	8	4	2	1	اعداد توان 2
-128	-64							
116	116							
0	1							معادل بیتی

**قسمت سوم:** مابقی عدد کم شده از قسمت دوم را از عدد 32 کم کنید (32-52) و عدد 1 را در قسمت معادل بیتی قرار دهید.

128	64	32	16	8	4	2	1	اعداد توان 2
-128	-64	52-32						
116	116							
0	1	1						معادل بیتی

**قسمت چهارم:** باقی‌مانده حاصل تفریق از قسمت سوم را از 16 کم کنید (16-20) و عدد 1 را در قسمت معادل بیتی بنویسید.

128	64	32	16	8	4	2	1	اعداد توان 2
-----	----	----	----	---	---	---	---	-----------------

-128	-64	<del>52-32</del>	20-16					
116	116							
0	1	1	1					معادل بیتی

قسمت پنجم: باقی مانده حاصل تفریق از قسمت چهارم را از 8 کم کنید (4-8). همان گونه که قابل مشاهده است نمی توان عدد 8 را از 4 کم کنید. پس در نتیجه معادل بیتی را برابر با صفر قرار دهید.

128	64	32	16	8	4	2	1	اعداد توان 2
-128	-64	<del>52-32</del>	<del>20-16</del>	4-8				
116	116							
0	1	1	1	0				معادل بیتی

قسمت ششم: باقی مانده حاصل کسر از قسمت پنجم را از 4 کسر کنید (4-4) و عدد 1 را در قسمت معادل بیتی بنویسید.

128	64	32	16	8	4	2	1	اعداد توان 2
-128	-64	<del>52-32</del>	<del>20-16</del>	4-8	4-4			
116	116							
0	1	1	1	0	1			معادل بیتی

قسمت هفتم: از آنجایی که باقی مانده در قسمت پنجم برابر با صفر شده است، پس بنابراین سایر قسمت های بیتی باید برابر با صفر قرار گیرند.

128	64	32	16	8	4	2	1	اعداد توان 2
-128	-64	<del>52-32</del>	<del>20-16</del>	4-8	4-4	0	0	
116	116							
0	1	1	1	0	1	0	0	معادل بیتی

حال که با روال کلی آشنا شدید می توانید گام 1 و 2 را همزمان انجام داده و گام 3 را در مرحله ای جداگانه محاسبه نمایید.

### مثال 3:

عدد 190 را به معادل دودویی تبدیل کنید.

گام 1 اعداد توان 2 را از 0 تا 7 بنویسید.

128	64	32	16	8	4	2	1	اعداد توان 2
								معادل بیتی

گام 2 معادل بیتی را برای عدد 190 از سمت چپ به راست حساب کنید.

128	64	32	16	8	4	2	1	اعداد توان 2
-128	62-64	62-32	30-16	14-8	6-4	2-2		
190								
1	0	1	1	1	1	1	0	معادل بیتی

## انواع آدرس دهی

همان طور که قبلاً اشاره شد آدرس های IP عددی 32 بیتی است که با استفاده از آن می توان عددی بسیار بزرگ را ایجاد کرد. حال برای این که بتوان این فضای آدرس دهی را مدیریت کرد دو روش آدرس دهی Classfull و Classless وجود دارد که در ادامه به آن ها می پردازیم.

### آدرس دهی Classfull

در حالت Classfull کل فضای آدرس دهی IP به یک سری محدوده بانام کلاس شکسته شده و به هر کلاس یک رنج از آدرس ها اختصاص داده شده است. قبل از این که به بررسی این کلاس ها بپردازیم بهتر است تا چند نکته را مورد بررسی قرار دهیم. هر آدرس IP از دو قسمت تشکیل شده است:

1. آدرس شبکه
2. آدرس کلاینت

### آدرس شبکه

از آنجایی که در شبکه TCP/IP شبکه‌های زیادی وجود دارد و هر شبکه دارای تعدادی کلاینت است، پس در نتیجه باید به هر شبکه یک آدرس اختصاص داد از این رو هر آدرس IP دارای یک بخش به نام آدرس شبکه است و کلاینت‌هایی که دارای آدرس شبکه یکسان باشند در عضویت یک شبکه قرار خواهند گرفت. مثال عینی از این نوع آدرس را می‌توان به شماره تلفن‌های مخابراتی نسبت داد. آن دسته از مشترکین که در یک شهر قرار دارند دارای کد یکسانی هستند به عنوان مثال کد شهر شیراز 071 است، حال تمامی مشترکین که ابتدای شماره خود 071 داشته باشند مطمئناً شهروند شیرازی هستند.

### آدرس کلاینت

درواقع آدرس کلاینت بخش دوم از اجزاء تشکیل دهنده IP است. هر کلاینت که در یک شبکه قرار می‌گیرد باید آدرس منحصر به فرد در همان شبکه داشته باشد تا بتواند با سایر کلاینت‌ها به تبادل داده بپردازد. در مثال شماره تلفن‌های مخابراتی این قسمت مشابه شماره مشترک می‌باشد، به عنوان مثال 32321199.

با توجه به مطالب گفته شده، در سطح اینترنت تعداد شبکه‌های زیادی وجود دارد که ممکن است در هر کدام از آن‌ها کلاینت‌های زیادی قرار داشته باشد. برای این که بتوان محدوده آدرس شبکه و کامپیوتر را مشخص کرد از Subnet Mask استفاده می‌شود. در حقیقت Subnet Mask همانند آدرس IP یک عدد 32 بیتی بوده که متشکل از یک‌ها و صفرهای پیوسته است. توجه داشته باشید که Subnet Mask از سمت چپ به راست باید دارای یک‌های پیوسته باشد. در ادامه مثال‌هایی از Subnet Mask را مشاهده می‌کنید.

Subnet Mask:	11111111	.	11111111	.	11111111	.	00000000
	معادل دودویی						

Subnet Mask:	255	.	255	.	255	.	0
	معادل ده‌دهی						

در صورتی که آدرس‌های Subnet Mask دارای پیوستگی در یک‌ها و صفرها نباشد معتبر نبوده و استفاده از آن‌ها مجاز نیست.

Subnet Mask	11111111	.	11110111	.	11110010	.	00000000
	معادل دودویی						

Subnet Mask	255	.	247	.	242	.	0
	معادل ده‌دهی						

در واقع آدرس‌های IP بدون وجود Subnet Mask معنی ندارد چرا که نمی‌توان قسمت مربوط به

آدرس شبکه و آدرس کلاینت را تشخیص داد. در حقیقت با توجه به یک‌های Subnet Mask می‌توان قسمت مربوط به آدرس شبکه و با توجه به صفرهای Subnet Mask می‌توان قسمت مربوط به آدرس کلاینت را در آدرس IP تشخیص داد. برای درک بهتر این موضوع بهتر است تا به مثال 4: توجه کنید.

**مثال 4:**

یک آدرس IP براساس مشخصات زیر وجود دارد

**IP:** 192.1610.1

**Subnet Mask:** 255.255.255.0

آدرس شبکه و آدرس کامپیوتر در IP مشخص شده را با توجه به Subnet Mask مشخص کنید.

**گام 1** ابتدا معادل دودویی (بیتی) آدرس IP و Subnet Mask را بنویسید.

192	.	168	.	1	.	1	آدرس IP دهدهی
11000000	.	10101000	.	00000001	.	00000001	معادل دودویی
<hr/>							
255	.	255	.	255	.	0	آدرس Subnet Mask دهدهی
11111111	.	11111111	.	11111111	.	00000000	معادل دودویی

**گام 2** معادل دودویی آدرس IP و Subnet Mask را با یکدیگر And کنید.

<b>IP</b>	11000000	.	10101000	.	00000001	.	00000001
<b>Subnet Mask</b>	11111111	.	11111111	.	11111111	.	00000000
<b>نتیجه عملیات And</b>	11000000	.	10101000	.	00000001	.	00000000

**گام 3** حال با به دست آوردن نتیجه عملیات دودویی باید آن را به معادل دهدهی تبدیل کنید.

<b>نتیجه عملیات And</b>	11000000	.	10101000	.	00000001	.	00000000
<b>معادل دهدهی</b>	192	.	168	.	1	.	0

عدد به دست آمده برابر با آدرس شبکه خواهد بود.

**گام 4** به دست آوردن آدرس کلاینت

برای به دست آوردن آدرس کلاینت باید گام‌های 2 و 3 را انجام دهید با این تفاوت که در گام 2 به جای انجام عملیات And باید از Or استفاده کنید.

حال عملیات Or را بر روی معادل بیتی IP و Subnet Mask را انجام دهید.

<b>IP:</b>	11000000	.	10101000	.	00000001	.	00000001
<b>Subnet Mask:</b>	11111111	.	11111111	.	11111111	.	00000000

نتیجه عملیات Or      11111111 . 11111111 . 11111111 . 00000001

**گام 5** حال با به دست آوردن نتیجه عملیات دودویی باید آن را به معادل دهدهی تبدیل کنید.

نتیجه عملیات And      11111111 . 11111111 . 11111111 . 00000001

معادل دهدهی      255 . 255 . 255 . 1

آن قسمت از عدد که برابر با 255 نباشد نشان دهنده آدرس کلاینت است.

با توجه به عملیات انجام شده می توان آدرس های شبکه و کلاینت را به کمک Subnet Mask به دست آورد.

آدرس IP	
آدرس شبکه	آدرس کلاینت
192 . 168 . 1 .	1

Subnet Mask را می توان به شیوه های مختلفی نشان داد که شامل:

1. نمایش دودویی

2. نمایش دهدهی

3. نمایش CIDR

**نمایش دودویی:** در نمایش دودویی باید Subnet Mask را به صورت ترکیبی از یک ها و صفرهای پیوسته نشان دهید.

11111111.11111111.11111111.00000000

**نمایش دهدهی:** در این حالت از نمایش، مقدار Subnet Mask را باید به صورت دهدهی بنویسید.

IP: 192 . 168 . 1 . 1

Subnet: 255 . 255 . 255 . 0

**نمایش CIDR:** در حالت CIDR تعداد یک های موجود در قسمت های باینری با استفاده از علامت / در کنار آدرس IP نشان داده می شود.

192.1610.1/24

در زیر می توانید مثالی از نحوه نمایش سه حالت گفته شده را ببینید.

IP: 192 . 168 . 1 . 1

Subnet Mask: 11111111 . 11111111 . 11111111 . 00000000

Subnet Mask: 255 . 255 . 255 . 0

Subnet Mask: /24 مجموع بیت های 1 برابر با 24 است.

CIDR به دلیل سادگی و گویا بودن در شیوه نمایش، بیشتر مورد استفاده قرار می گیرد.

IP →	172	·	16	·	20	·	1	
Subnet Mask:	255	·	255	·	0	·	0	⇒
								<b>IP+Subnet</b> <b>Mask=172.16.20.1/16</b>

### کلاس‌های آدرس IP

کلاس‌هایی که در آدرس‌دهی Classfull مورد استفاده قرار می‌گیرند شامل کلاس‌های A، B، C، D و E است. در شکل 1-4 می‌توان کل فضای اختصاص داده آدرس و میزان آدرس‌های IP اختصاص داده شده به هر کلاس را مشاهده نمود.



شکل 1-4

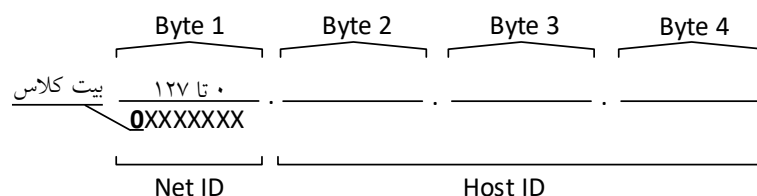
### محدوده آدرس‌های IP

هرکدام از کلاس‌های گفته شده دارای محدوده مختص به خود هستند که برای تشخیص این محدوده کافی است تا به «بیت کلاس» دقت کنید. بیت کلاس در هر کلاس متفاوت است که در ادامه در هر کلاس تعداد بیت‌ها و مقدار آن‌ها را مشخص کرده‌ایم.

#### کلاس A

آدرس‌هایی که بایت اول آن‌ها در محدوده 0 تا 127 باشد جزء کلاس A محسوب شده و Subnet Mask مربوط به این کلاس برابر با 255.0.0.0 است. این Subnet Mask نشان‌دهنده این

است که بایت اول از IP مربوط به آدرس شبکه و مابقی بایت‌ها مربوط به آدرس کلاینت است.



شکل 2-4

همان‌گونه که در شکل 2-4 مشخص شده است اولین بیت برابر با صفر بوده که این بیت مربوط به «بیت کلاس» است، بیت کلاس در کلاس A به صورت ثابت برابر صفر است و هفت بیت به قسمت Net ID و 24 بیت به قسمت Host ID اختصاص داده شده است. پس در نتیجه در این کلاس  $2^7 = 128$  رنج از آدرس‌های متفاوت را می‌توان ایجاد کرد که در هر رنج  $2^{24}$  کلاینت می‌تواند آدرس‌دهی شود.



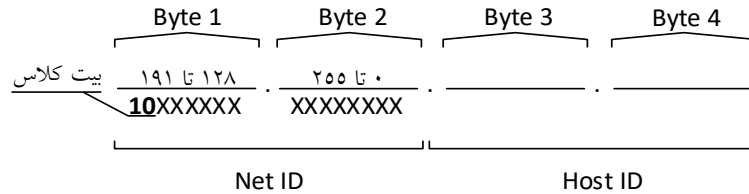
شکل 3-4

اولین و آخرین رنج یعنی صفر و 127 قابل استفاده نیستند و برای آدرس‌های خاص در نظر گرفته شده‌اند.

### کلاس B

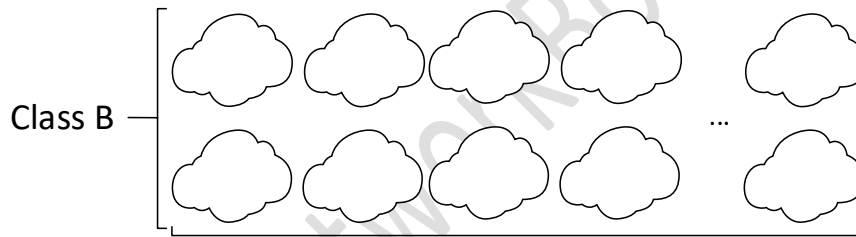
آدرس‌هایی که بایت اول آن‌ها در محدوده 128 تا 191 باشند جزء کلاس B حساب شده و Subnet Mask مربوط به این کلاس برابر با 255.255.0.0 است. با توجه به Subnet Mask می‌توان متوجه شد که دو بایت اول نشان‌دهنده آدرس شبکه و دو بایت دوم نشان‌دهنده آدرس کلاینت است.





شکل 4-4

همانگونه که مشخص شده است دو بیت اول مربوط به «بیت کلاس» است و 14 بیت به قسمت Net ID و 16 بیت به قسمت Host ID اختصاص داده شده است. پس در نتیجه در این کلاس  $2^{14} = 16.384$  رنج از آدرس های متفاوت را می توان ایجاد کرد که در هر رنج  $2^{16}$  کلاینت می تواند آدرس دهی شود.

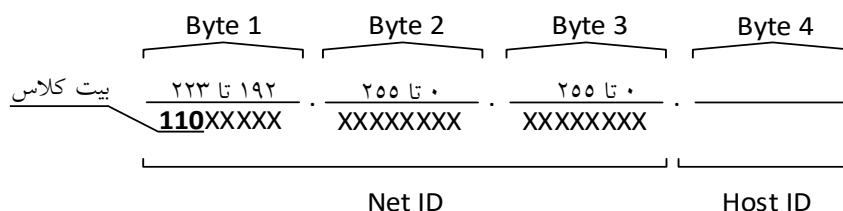


تعداد شبکه ها برابر با ۱۶۳۸۴ عدد خواهد بود

شکل 4-5

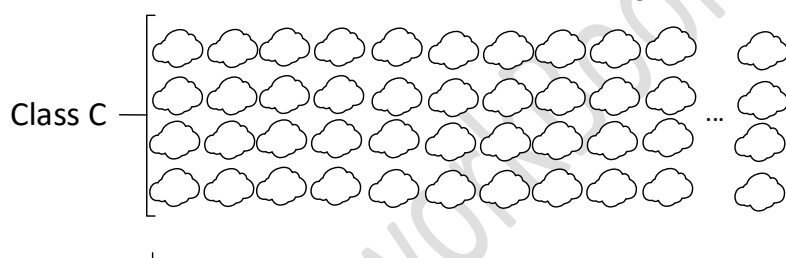
### کلاس C

آدرس هایی که بایت اول آن ها در محدوده 192 تا 223 باشند جزء کلاس C حساب شده و Subnet Mask مربوط به این کلاس برابر با 255.255.255.0 است. با توجه به Subnet Mask می توان متوجه شد که سه بایت اول نشان دهنده آدرس شبکه و بایت آخر نشان دهنده آدرس کلاینت است.



شکل 6-4

همان‌گونه که در شکل 6-4 مشخص شده است سه‌بیت اول مربوط به «بیت کلاس» است و 21 بیت به قسمت Net ID و 8 بیت به قسمت Host ID اختصاص داده شده است. پس در نتیجه در این کلاس  $2^{21} = 2,097,152$  رنج از آدرس‌های متفاوت را می‌توان ایجاد کرد که در هر رنج  $2^8$  کلاینت می‌تواند آدرس‌دهی شود.



تعداد شبکه‌ها برابر با  $2,097,152$  عدد خواهد بود

شکل 7-4

### کلاس D

هدف از ایجاد این کلاس فراهم آوردن قابلیت Multicast بوده و هر آدرس از این کلاس را می‌توان به یک گروه اختصاص داد. در هر گروه ممکن است چندین کلاینت وجود داشته باشد پس در نتیجه کلاینت‌ها علاوه بر داشتن آدرس IP از کلاس A، B یا C، دارای یک آدرس IP دیگر از رنج D بوده که نشان‌گر عضویت کلاینت در گروه است. در کلاس D تنها یک رنج از آدرس IP وجود دارد که از  $224.0.0.0$  شروع شده و به  $239.255.255.255$  ختم می‌شود.

### کلاس E

در کلاس E یک رنج از آدرس IP وجود دارد که از  $240.0.0.0$  شروع شده و به  $255.255.255.255$  ختم می‌شود. آدرس‌های موجود در این کلاس رزرو شده بوده و در حالت

عادی نمی‌توان از آن‌ها استفاده کرد.

### بررسی محدوده‌های آدرس IP

در هر رنج از آدرس IP اولین و آخرین آدرس به صورت رزرو شده بوده و نمی‌توان از آن‌ها برای آدرس‌دهی به کلاینت استفاده کرد. اولین آدرس از هر رنج مربوط به آدرس شبکه و آخرین آدرس مربوط به آدرس Broadcast است. در مثال 5: با نحوه تعیین آدرس‌های یک رنج آشنا خواهید شد.

آدرس شبکه: آدرسی است که از آن برای اشاره به یک شبکه استفاده می‌شود و یکی از استفاده‌های آن در جدول مسیریابی روتر می‌باشد.

آدرس Broadcast: زمانی که یک کامپیوتر بخواهد بسته‌ای را به تمام کامپیوترهای درون شبکه خود ارسال کند از این آدرس استفاده می‌کند.

#### مثال 5:

محدوده آدرس‌های کلاینت مربوط به آدرس 192.16100.0/24 را مشخص کنید.

جواب: از آنجایی که بایت اول این آدرس برابر با 192 است می‌توان متوجه شد که کلاس این آدرس C است، پس در نتیجه سه بایت اول مربوط به قسمت شبکه بوده و بایت آخر مربوط به کلاینت است. آدرس شبکه باید به صورت ثابت نوشته شود و شما باید تمام حالت‌های آدرس کامپیوتر را در زیر لیست کنید.

#### 192.16100.0/24

192.16100.0	اولین آدرس (آدرس شبکه) ←
192.16100.1	اولین آدرسی که به کلاینت اختصاص داده می‌شود ←
192.16100.2	
.	
.	
192.16100.254	آخرین آدرسی که به کلاینت اختصاص داده می‌شود ←
192.16100.255	آخرین آدرس (آدرس Broadcast) ←

#### مثال 6:

کلاینتی دارای یک آدرس IP برابر با 192.1610.100/24 است. موارد زیر را مشخص کنید.

1. کلاس آدرس
2. آدرس شبکه
3. اولین آدرسی که به کلاینت اختصاص می‌شود

4. آخرین آدرسی که به کلاینت اختصاص داده می‌شود

5. آدرس Broadcast

جواب: باتوجه به بایت اول از آدرس IP که برابر با 192 است می‌توان متوجه شد که این آدرس در کلاس C قرار دارد. محدوده آدرس‌های کلاینت را بنویسید.

192.1610.0

اولین آدرس (آدرس شبکه)

192.1610.1

اولین آدرسی که به کلاینت اختصاص داده می‌شود

.

192.1610.254

آخرین آدرسی که به کلاینت اختصاص داده می‌شود

192.1610.255

آخرین آدرس (آدرس Broadcast)

### انواع آدرس‌های IP

دامنه و هدف عملیاتی آدرس‌های IP براساس محدوده و نوع کار متفاوت است. به‌طورکلی آدرس‌های IP به دو صورت Private (خصوصی) یا Public (عمومی) مورد استفاده قرار می‌گیرند. آدرس Public به‌صورت عمومی بوده و از هر نقطه‌ای از جهان که دسترسی به اینترنت امکان‌پذیر باشد، می‌توان به آن‌ها متصل شد. این نوع از آدرس‌ها به‌صورت ماهانه و یا سالیانه دارای هزینه‌ای مشخص هستند.

آدرس‌های Private در شبکه‌های خصوصی و محیط‌های آزمایشگاهی استفاده شده و دسترسی به این آدرس‌ها از نوع محلی است. به این معنی که آدرس‌های IP از نوع خصوصی تنها در شبکه‌ای که درحال استفاده است معتبر بوده و قابل دسترس می‌باشد. این آدرس‌ها در اینترنت قابل مشاهده و دسترسی نمی‌باشد.

به‌صورت کلی تمامی آدرس‌های موجود در اینترنت از نوع Public بوده به جزء چند رنج مشخص که در جدول 4-1 می‌توانید این محدوده‌ها را مشاهده نمایید.

محدوده آدرس‌های Private		
تا	از	
10.255.255.255/8	10.0.0.0/8	کلاس A
172.31.255.255/16	172.16.0.0/16	کلاس B
192.168.255.255/24	192.1610.0/24	کلاس C

باتوجه به محدوده‌های مشخص شده در جدول 4-1 موارد زیر قابل برداشت است:

- در کلاس A تنها یک رنج مشخص شده است که در آن می‌توان  $2^{24}$  آدرس را به کلاینت‌ها اختصاص داد.
- در کلاس B تعداد 16 رنج مشخص شده است که در هرکدام از آن‌ها می‌توان  $2^{16}$  آدرس را به کلاینت‌ها اختصاص داد.
- در کلاس C تعداد 255 رنج مشخص شده است که در هرکدام از آن‌ها می‌توان  $2^8$  آدرس را به کلاینت‌ها اختصاص داد.

در هنگام انتخاب کلاس برای شبکه باید به حداکثر تعداد کلاینت‌ها توجه کنید و کلاسی را انتخاب کنید که کمترین هدر رفت داشته باشد. به مثال 7: توجه کنید.

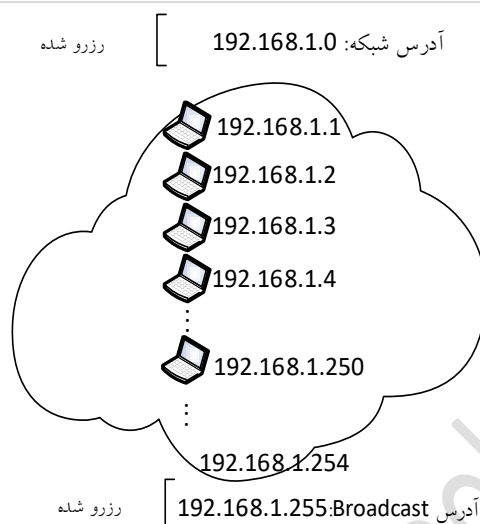
#### مثال 7:

الف) در شرکت زرافه 250 سیستم وجود دارد و نیاز است تا به سیستم‌ها آدرس IP از یک کلاس اختصاص دهیم، حال یک راه‌کار برای انتخاب کلاس ارائه دهید.

جواب: باتوجه به این‌که تعداد سیستم‌های موجود در شرکت 250 عدد است پس در نتیجه استفاده از کلاس C می‌تواند تعداد آدرس‌های موردنیاز برای کلاینت‌ها فراهم کند. چراکه آدرس‌های کلاس C حداکثر 256 آدرس را در اختیار شما قرار می‌دهد و باتوجه به 2 آدرس رزرو شده، 254 آدرس در دسترس است.

از آنجایی که شبکه مربوط به شرکت زرافه یک شبکه محلی است، پس در نتیجه باید آدرس‌های خصوصی را به شبکه اختصاص دهید.

Class → C  
IP Address → 192.1610.0/24

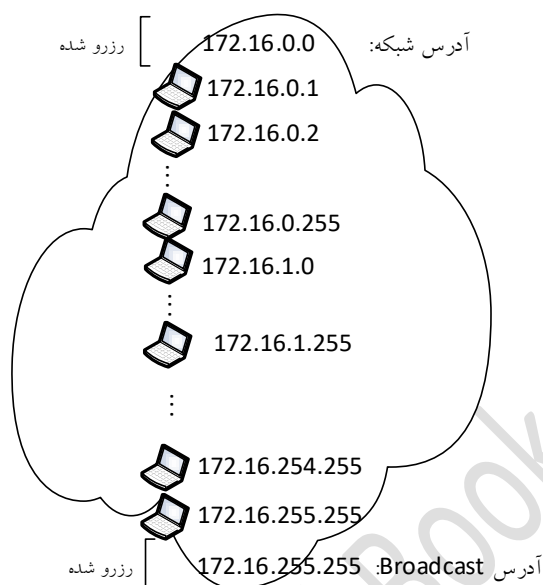


شکل 8-4

- محدوده آدرس استفاده شده: 192.168.0.0
  - تعداد آدرس های موجود در این رنج: 256 عدد
  - تعداد آدرس های رزرو شده: 2 عدد
  - تعداد آدرس های قابل استفاده برای کلاینت ها: 254 عدد
  - تعداد آدرس های مورد نیاز: 250 عدد
  - تعداد هدر رفت آدرس: 4 عدد که از آدرس 251 تا 254 است.
- ب) سازمانی به نام X وجود دارد که در حدود 400 سیستم خریداری کرده است و نیاز دارد تا تمامی سیستم ها در یک شبکه از نوع خصوصی قرار دهد.
- جواب:** در واقع اینجا کلاسی از آدرس IP نیاز است تا بتوان با استفاده از آن حداقل 400 کلاینت را آدرس دهی کرد. همان گونه که می دانید کلاس C حداکثر 254 سیستم را تحت پوشش قرار می دهد پس در نتیجه نمی توان 400 سیستم را با استفاده از کلاس C آدرس دهی کرد، از این رو می بایست از کلاس B استفاده کرد. حال از کلاس B یک رنج از آدرس های خصوصی را به سازمان اختصاص می دهیم.

Class → B

IP Address → 172.16.0.0/16



شکل 9-4

- محدوده آدرس استفاده شده: 172.16.0.0
- تعداد آدرس‌های موجود در این رنج: 65536 عدد
- تعداد آدرس‌های رزرو شده: 2 عدد
- تعداد آدرس‌های قابل استفاده برای کلاینت‌ها: 65534 عدد
- تعداد آدرس‌های مورد نیاز: 400 عدد
- تعداد هدر رفت آدرس: 65134 عدد

نکته‌ای که در این تمرین قابل توجه است میزان هدر رفته‌ای آدرس IP است. در هنگام استفاده از کلاس B می‌توان در حدود 65.536 آدرس IP در هر رنج داشته باشید اما در این تمرین تنها از 400 آدرس استفاده شده و مابقی بلااستفاده است. این موضوع یکی از اصلی‌ترین معایب آدرس‌های Classfull است و جهت رفع این مشکل از روش دیگری به نام Classless استفاده شده است که در ادامه به شرح آن خواهیم پرداخت.

### برخی از آدرس‌های خاص

- آدرس IP تمام صفر و Subnet Mask تمام صفر مانند IP: 0.0.0.0 و SubnetMask:0.0.0.0 در جدول مسیریابی نشان‌دهنده Default Route است.

- **آدرس شبکه 127:** از این آدرس به عنوان Loopback استفاده می‌شود. برای تست استفاده می‌شود.
- **قسمت آدرس کامپیوتر تمام صفر:** مانند 192.1610.0 که این آدرس به عنوان آدرس شبکه شناخته می‌شود.
- **قسمت آدرس شبکه تمام یک:** مانند 192.1610.255 که این آدرس به عنوان آدرس Broad Cast شناخته می‌شود. اگر کامپیوتری بخواهد بسته‌ای را ارسال کند که تمام کامپیوترهای درون یک شبکه آنرا دریافت کنند باید از آدرس Broad Cast به عنوان آدرس مقصد استفاده کند.
- **آدرس 169.254.X.Y با Subnet Mask 255.255.0.0:** اگر آدرس IP مربوط به کلاینت مایکروسافت را روی حالت اتوماتیک بگذارید و در صورتی که سرور DHCP در شبکه وجود نداشته باشد، کلاینت از این محدوده IP می‌گیرد. به این محدوده APIPA می‌گویند. آدرس APIPA یا Automatic Private IP Addressing در اینترنت مسیریابی نخواهند شد.

## آدرس دهی IPv6

آدرس IPv4 قادر است تا در حدود 4.3 میلیارد آدرس یکتا را فراهم کند که محدوده بزرگی به نظر می‌رسد، اما با رشد اینترنت در آینده‌ای نزدیک این آدرس‌ها جوابگوی تعداد کاربران نخواهد بود، پس در نتیجه نیاز به یک محدوده که آدرس‌های بیشتری را دربرگیرد حس می‌شود. به همین دلیل آدرس IPv6 به وجود آمد که محدوده فوق‌العاده بزرگی را نسبت به IPv4 فراهم می‌کند.

با رشد اینترنت کلیه وسایل منزل مانند پرده، میکروفر، یخچال و... نیاز به آدرس IP دارند تا بتوانند عضوی از اینترنت بشوند. آدرس IPv6 این امکان را فراهم می‌کند تا به تک تک سلول‌های موجود بر روی کره زمین آدرس یکتا اختصاص دهید. IPv6 از 128 بیت برای آدرس دهی استفاده می‌کند.

## مزایای IPv6

1. فراهم‌آوری کیفیت سرویس یا QOS در IPv6
  2. محدوده وسیع برای آدرس دهی که معادل  $2^{128}$  فضای آدرس است.
  3. ساختار مسیریابی ساده‌تر
  4. عدم نیاز به وجود سرور DHCP
- در صورت وجود یک زیرشبکه، هر کلاینت با استفاده از آدرس MAC مربوط به خود یک



آدرس را ایجاد می‌کند که Link Local نامیده می‌شود.

▪ در صورت وجود چند زیر شبکه و روتر بین آن‌ها، تمامی کلاینت‌ها با استفاده از آدرسی که روتر به آن‌ها می‌دهد و آدرس Mac خود یک آدرس منحصر به فرد تولید می‌کند.

5. امنیت بیشتر

6. عدم نیاز به NetBIOS و ARP

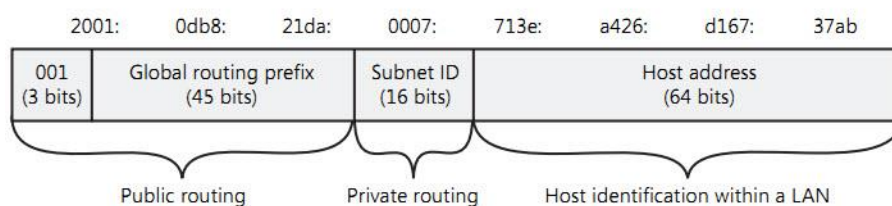
## انواع IPv6

### Global Address

مشابه آدرس‌های عمومی (Public) در IPv4 است.

ساختار یک GA را در شکل 10-4 می‌بینید:

2001:db8:21da:7:713e:a426:d167:37ab



شکل 10-4

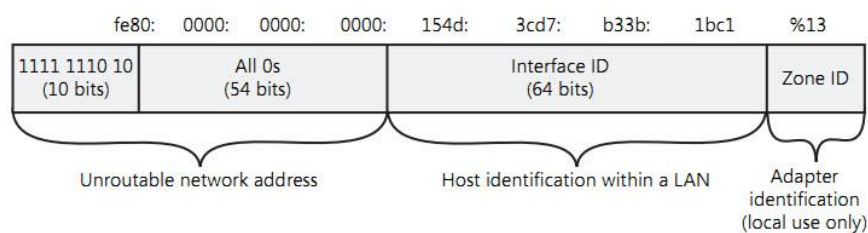
1. مسیریابی عمومی - **Public Routing**: 48 بیت اول برای مسیریابی عمومی و جهانی استفاده می‌شود.  
سه بیت اول به‌طور ثابت 001 بوده که نشان‌دهنده آدرس GA است و 45 بیت بعدی توسط IANA به ISP و یا شرکت اختصاص داده می‌شود.
2. مسیریابی خصوصی - **Private Routing**: 16 بیت بعد به‌عنوان شماره زیر شبکه یا Subnet ID است که در واقع ISP آن را به مشتریان خود اختصاص می‌دهد.
3. شناسه میزبان - **Host identification**: 64 بیت آخر مربوط به کلاینت‌ها بوده که هر کلاینت با استفاده از آدرس Mac خود آن را تولید می‌کند.

### (LLA) Link-Local Address

مشابه APIPA (محدوده 169.254.0.0) بوده و در واقع همان آدرس خصوصی یا Private است. کلاینت‌هایی که در شبکه محلی از این آدرس‌ها استفاده می‌کنند قابل مسیریابی نبوده و در اینترنت

مورد استفاده قرار نمی‌گیرند. در ادامه ساختار LLA را مشاهده می‌کنید.

fe80::154d:3cd7:b33b:1bc1%13



شکل 11-4

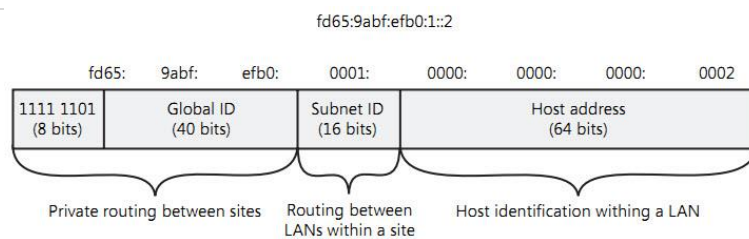
آدرس شبکه (Unroutable Net Address): 48 بیت اول به‌عنوان آدرس شبکه در نظر گرفته می‌شود که همیشه با fe80 شروع خواهد شد و 10 بیت اول آن ثابت است و 54 بیت بعدی همه صفر است.

شناسه میزبان - Host identification: هر کلاینت با استفاده از آدرس Mac خود این قسمت را ایجاد کرده که طول آن 64 بیت است.

شناسه کارت شبکه یا Adapter Identification: با همان شناسه ناحیه (Zone ID) که این قسمت را با علامت % در انتهای هر آدرس محلی می‌بینید. اگر یک کلاینت وجود داشته باشد که دارای دو کارت شبکه بوده و به دو شبکه متفاوت متصل باشد با استفاده از این قسمت متوجه خواهد شد که بسته را باید از کدام کارت شبکه خود خارج کند.

### (ULA) Unique Local Address

شبهه آدرس‌های خصوصی در IPv4 بوده که این آدرس‌ها در شبکه Private قابل مسیریابی می‌باشند، اما در شبکه Public قابل مسیریابی نخواهند بود. با استفاده از این آدرس‌ها می‌توان یک شبکه اینترنت بسیار بزرگ را ایجاد کنید.



شکل 12-4

مسیریابی خصوصی بین سایت (Private Routing Between Sites): با FD شروع شده و در واقع هشت بیت اول نشان‌دهنده آدرس ULA است و در صورت نیاز FC00 هم می‌تواند باشد. 40 بیت بعدی یک شناسه سراسری یا Global ID است که به صورت تصادفی توسط سایت ساخته می‌شود.

مسیریابی بین زیرشبکه‌های درون یک سایت (Routing Between LANs within a Site): این 16 بیت نشان‌دهنده آدرس زیرشبکه است.

شناسه میزبان Host identification: هر کلاینت با استفاده از آدرس Mac خود این قسمت را تولید می‌کند.

نکته: آدرس Loopback یا همان 127.0.0.1 در IPv6 برابر ::1 است.

برای دیدن تنظیمات IPv6 می‌توان از دستور زیر استفاده کرد:

```
Administrator: Command Prompt

C:\Windows\system32\ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . :

Wireless LAN adapter Local Area Connection* 13:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . . :
    Link-local IPv6 Address . . . . . : fe80::29f1:d244:54cb:a54e%16
    IPv4 Address. . . . . : 192.168.1.103
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::c66e:1fff:fed3:db09%16
    192.168.1.1
```

شکل 13-4

# پشتیبانی ویندوز 10

پشتیبانی از به اشتراک گذاری منابع



این PDF به صورت تصویری و مرحله به مرحله توضیح داده شده است.

[www.NetworkBooks.ir](http://www.NetworkBooks.ir)

[www.TejaratServer.ir](http://www.TejaratServer.ir)



برگرفته از پروژه های عملی شرکت



# فصل پنجم

## پشتیبانی از به اشتراک گذاری منابع

مباحث این فصل در دو قسمت "مقدماتی" و "حرفه‌ای تر شوید" ارائه شده است. در ابتدای هر فصل به بررسی مطالب ساده‌تری پرداخته شده و در قسمت "حرفه‌ای تر شوید" مباحث تخصصی‌تری مربوط به پشتیبانی از به اشتراک گذاری منابع را مورد بررسی قرار داده‌ایم لذا توصیه می‌شود ابتدا قسمت مباحث ابتدایی را مطالعه کرده و در صورتی که به مطالب تسلط پیدا کردید قسمت "حرفه‌ای تر شوید" را مطالعه نمایید.

## مقدمه

به اشتراک گذاری منابع (مانند فایل، دستگاه و ...) یکی از موارد مهم و ضروری در بسترهای شبکه تلقی می‌شود. به اشتراک گذاری منابع نیز باید در یک چهارچوب خاص صورت پذیرد به نحوی که باعث به وجود آمدن مشکلات امنیتی نشود چرا که تمام کاربران نباید به همه منابع اشتراکی دسترسی داشته باشند (تمام دسترسی‌ها باید با مجوز لازم صورت گیرد). در این فصل قصد داریم تا با نحوه تنظیم دسترسی‌ها و مجوزهای لازم به منابع اشتراک گذاشته شده بپردازیم.

### پیکربندی منابع به اشتراک گذاشته شده

در ویندوز 10 برای اشتراک گذاری فایل‌ها و پوشه‌ها راه‌ها و روش‌های زیادی وجود دارد که هر کدام دارای ویژگی‌های خاصی است. به صورت خلاصه در ویندوز 10 می‌توان با استفاده از Home group، SkyDrive و ... عملیات به اشتراک گذاری را انجام داد.

در ادامه سعی داریم تا از طریق روش‌های زیر عملیات اشتراک گذاری منابع را انجام دهیم:

- اشتراک گذاری با استفاده از Home group
- اشتراک گذاری با استفاده از Folder Sharing
- اشتراک گذاری با استفاده از Public Folder Sharing

### پیکربندی تنظیمات Home Group

استفاده از Home Group یکی از آسان‌ترین روش‌های به اشتراک گذاری اسناد، چاپگرها، پوشه‌ها و دیگر منابع بر روی شبکه محلی می‌باشد. توجه داشته باشید که در این حالت به صورت پیش-فرض تنها مجوز خواندن برای فایل‌های به اشتراک گذاشته شده در نظر گرفته می‌شود اما می‌توان با انجام تغییراتی در تنظیمات Home Group مجوز خواندن/نوشتن را فعال کرد. در ادامه با نحوه پیاده‌سازی Home Group در قالب تمرین 5-1 آشنا خواهید شد.

## تمرین 5-1

## عنوان: ساختن Home Group

شرح: در این تمرین قصد داریم تا با استفاده دو ویندوز 10 و از طریق Home Group یک‌سری فایل را به اشتراک گذاشته و از این فایل‌ها در شبکه استفاده کنیم.

## تجهیزات و پیش‌نیازها:

- وجود دو ویندوز 10 که در یک شبکه قرار دارند.
- از درستی تنظیمات IP و اتصال فیزیکی کامپیوترها اطمینان حاصل کنید.

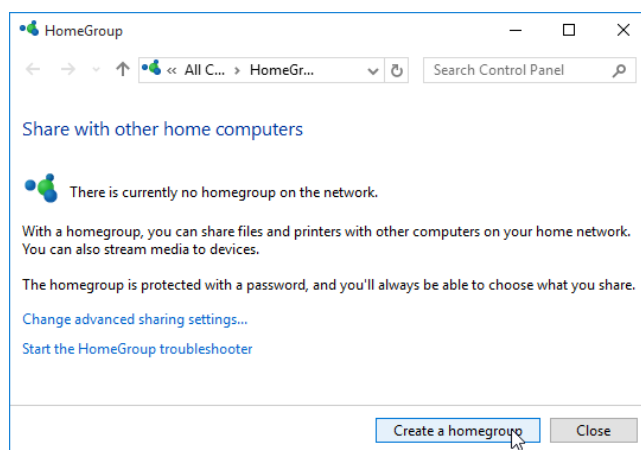
## مراحل تمرین:

- گام 1 راه‌اندازی Home Group با استفاده از ویندوز 10
- گام 2 متصل شدن به Home Group با استفاده از ویندوزی دیگر
- گام 3 دسترسی به فایل‌ها از طریق Home Group

## گام 1 راه‌اندازی Home Group با استفاده از ویندوز 10

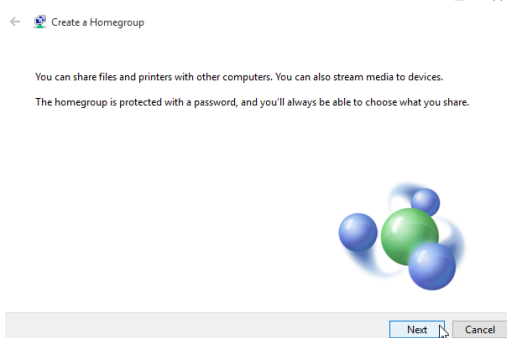
برای ساخت Home Group مراحل زیر را دنبال نمایید:

1. وارد Control Panel شده و سپس عبارت Home Group را جستجو کنید تا با پنجره‌ای مطابق با شکل 1-5 مواجه شوید. در ادامه بر روی دکمه Create a home group کلیک کرده تا مراحل ایجاد Home group شروع شود.



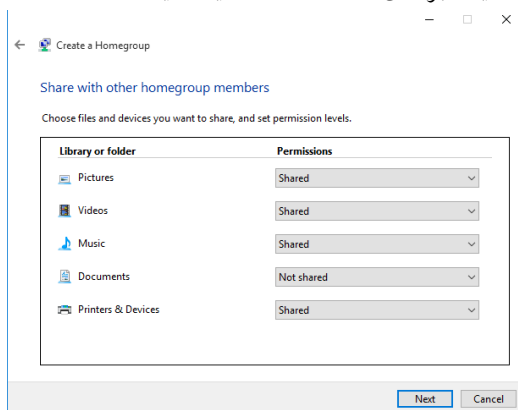
شکل 1-5

2. در پنجره‌ی ظاهر شده بر روی گزینه Next کلیک کنید.



شکل 2-5

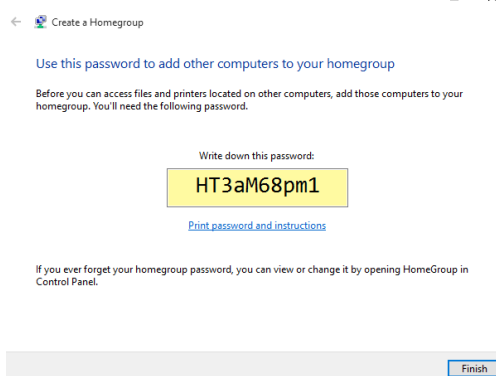
3. در ادامه باید مشخص کنید که چه مواردی به صورت پیش فرض در Home group به اشتراک گذاشته شود. مطابق با نیاز، هر کدام از موارد لازم را در حالت Shared قرار دهید تا در شبکه به اشتراک گذاشته شود. با کلیک بر روی دکمه Next عملیات ایجاد Home group انجام خواهد شد.



شکل 3-5

4. پس از این که مراحل ایجاد Home Group به پایان رسید، پنجره‌ای مانند شکل 4-5 نمایش داده می‌شود که حاوی یک رمز عبور می‌باشد. توجه داشته باشید که این رمز عبور باید در اختیار کسانی قرار گیرد که قصد دارید به Home group بپیوندند.



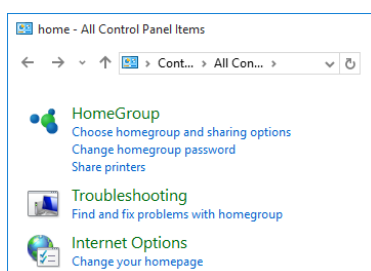


شکل 4-5

## گام 2 اتصال به Home Group با استفاده از ویندوزی دیگر

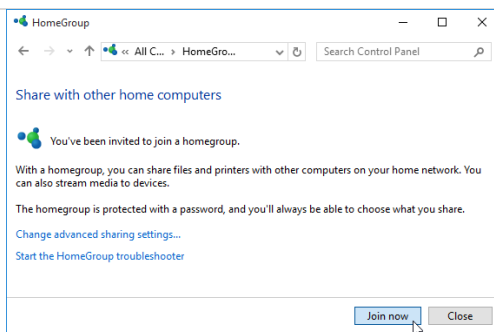
در ادامه باید با استفاده از یک ویندوز دیگر به Homegroup ملحق شد تا بتوان اشتراک‌گذاری منابع را انجام داد. برای این منظور مراحل زیر را انجام دهید.

1. وارد Control Panel شده و سپس عبارت Home group را جستجو کنید و سپس بر روی Home Group کلیک کنید.



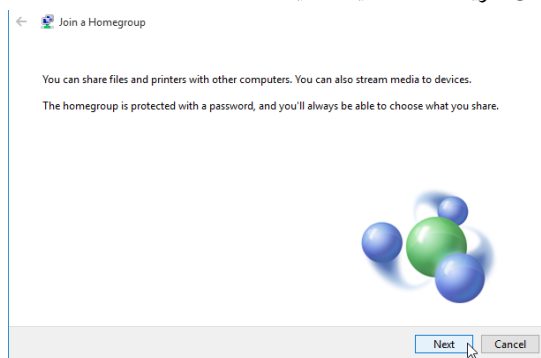
شکل 5-5

2. در پنجره ظاهر شده بر روی Join now کلیک کنید تا بتوانید سیستم را به شبکه Home group ملحق کنید.



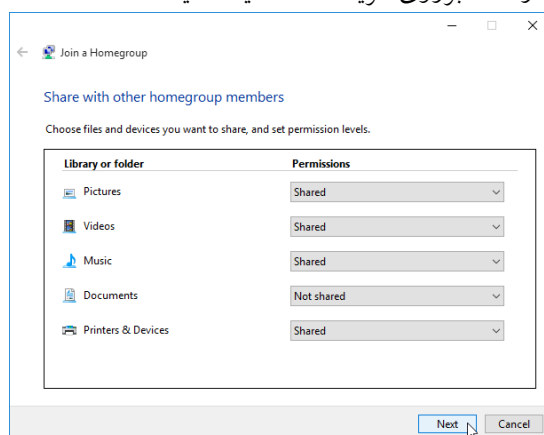
شکل 5-6

3. در این پنجره بر روی گزینه Next کلیک کنید.



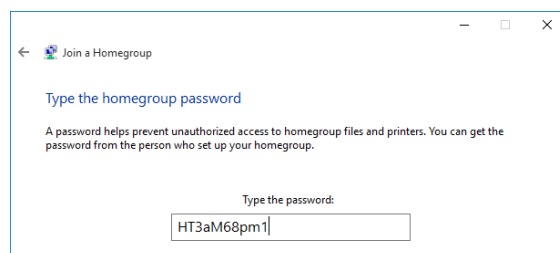
شکل 5-7

4. در این مرحله مشخص کنید که چه مواردی به صورت پیش فرض در Home group به اشتراک گذاشته شود. مطابق با نیاز، هر کدام از موارد لازم را در حالت Shared قرار دهید تا در شبکه به اشتراک گذاشته شود. در ادامه بر روی گزینه Next کلیک کنید.



شکل 5-8

5. رمز عبور مربوط به Home group را وارد کنید و در انتها بر روی Next کلیک کنید تا مراحل اتصال برقرار گردد.

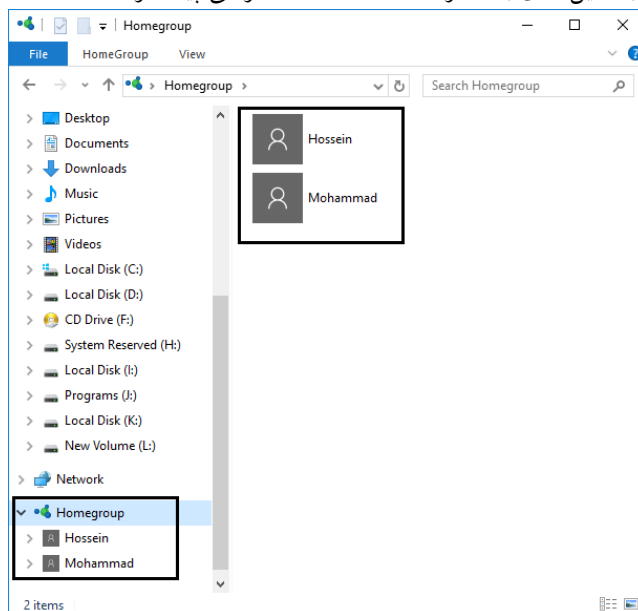


شکل 5-9

گاهی اوقات لازم است تا مجوزهای اختصاص داده شده به منابع اشتراکی دارای سطح دسترسی - های متفاوتی باشد، از این رو باید به افراد مورد نظر سطح دسترسی های متفاوتی اختصاص دهید.

### گام 3 دسترسی به فایل ها از طریق Home Group

در هر یک از کامپیوتر ها می توانید با اجرای This PC و سپس کلیک بر روی Home Group لیست کامپیوتر های درون Home Group ایجاد شده را مشاهده کنید. و با دبل کلیک بر روی هر کامپیوتر می توان به فایل های به اشتراک گذاشته شده دسترسی پیدا کرد.



شکل 5-10

**عنوان:** تغییر سطح مجوزهای دسترسی در Homegroup

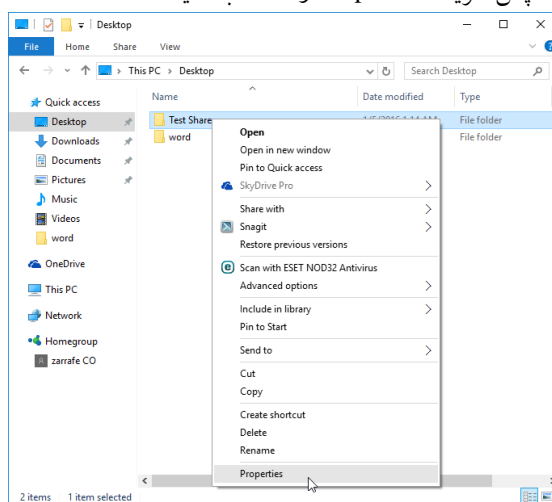
**شرح:** در این تمرین قصد داریم تا برای پوشه‌های اشتراک گذاشته شده مجوز خواندن و نوشتن را در نظر بگیریم (به صورت پیش فرض مجوزهای اختصاص داده شده در Homegroup از نوع فقط خواندنی می‌باشد).

**تجهیزات و پیش‌نیازها:**

- قبل از انجام این تمرین باید تمرین 5-1 را انجام دهید.

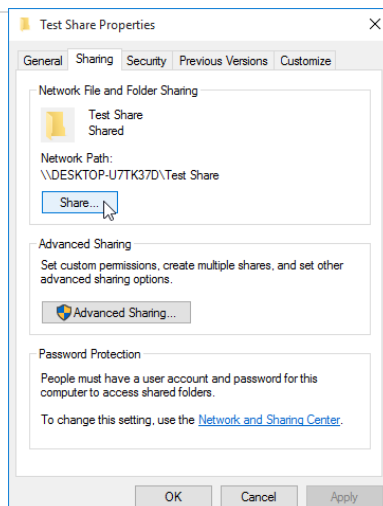
**مراحل تمرین:**

1. در ابتدا File Explorer را باز کرده و سپس بروی پوشه‌ای که قبلاً به اشتراک گذاشته‌اید راست کلیک کرده و سپس گزینه Properties را انتخاب کنید.



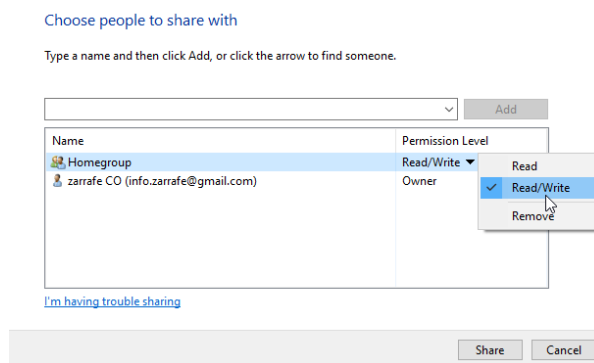
شکل 11-5

2. در پنجره باز شده به سربرگ Sharing رفته و بروی دکمه Share... کلیک کنید.



شکل 12-5

3. در ادامه گزینه Homegroup را Add کرده و از ستون Permission Level گزینه Read/Write را انتخاب کنید.



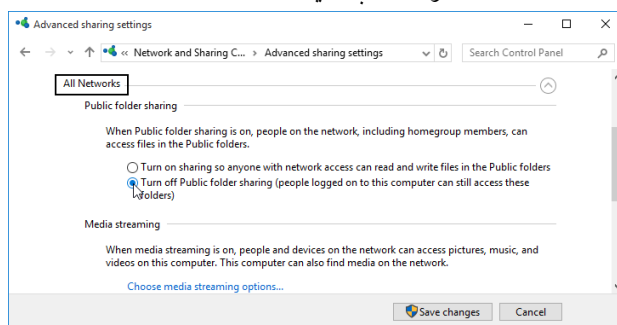
شکل 13-5

4. با انجام این کار به پوشه موردنظر مجوز خواندن و نوشتن را در هنگام استفاده از Home group اختصاص خواهید داد و تمامی افرادی که در Homegroup قرار دارند می‌توانند در این پوشه عملیات خواندن و نوشتن را انجام دهند.

**پوشه‌های عمومی**

پوشه‌های عمومی یا Public Folder یکی دیگر از راه‌های به اشتراک گذاری داده‌ها می‌باشد چراکه این دسته از پوشه‌ها به صورت پیش فرض به اشتراک گذاشته شده است و تمامی کاربرانی که به شبکه دسترسی دارند می‌توانند به این پوشه‌های دسترسی داشته باشند. مسیری که می‌توان این پوشه‌ها را مشاهده کنید در C:\Users\Public می‌باشد. ممکن است گاهی اوقات لازم باشد تا از اشتراک گذاری این پوشه‌ها در شبکه جلوگیری کنید که برای این کار کافی است تا مراحل زیر را انجام دهید:

1. از Control Panel وارد Network & Sharing Center شوید.
2. در پنجره Network & Sharing Center و از قسمت سمت چپ بر روی لینک Change Advanced Sharing Setting کلیک کنید.
3. در پنجره‌ی باز شده از قسمت پروفایل All Networks گزینه Turn off Public folder Sharing را انتخاب کنید.



شکل 5-14

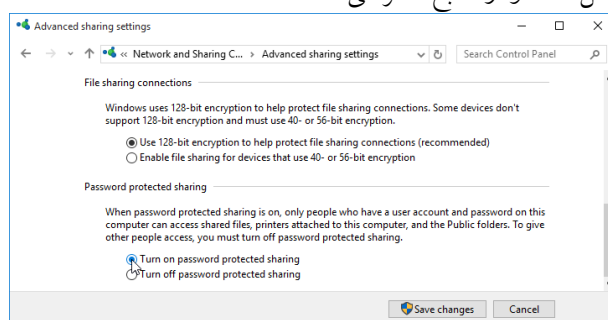
4. در نهایت بر روی دکمه Save changes کلیک کنید تا تنظیمات ذخیره شود.

### تنظیمات مربوط به رمز عبور در زمان دسترسی به فایل اشتراکی

یکی دیگر از گزینه‌های مهمی که می‌توان در پنجره Advanced Sharing Settings پیدا کرد، Password protected sharing می‌باشد. با استفاده از این گزینه می‌توان مشخص کرد که مجوز اتصال به سیستم جهت دسترسی به منابع تنها در اختیار افرادی قرار خواهد گرفت که بر روی سیستم دارای حساب کاربری باشند. برای بررسی این تنظیمات در پنجره Network and Sharing Center بر روی لینک Change Advanced Sharing setting کلیک کنید. سپس در پنجره ظاهر شده در قسمت Password Protection Sharing دو انتخاب وجود دارد که شامل:

**Turn on password protected sharing:** با انتخاب این گزینه افرادی می‌توانند از منابع اشتراکی در سطح شبکه در سیستم استفاده کنند که دارای رمز عبور باشند.

**Turn off password protected sharing:** با انتخاب این گزینه می‌توان مشخص کرد که تمام افراد به سیستم متصل شده و از منابع اشتراکی استفاده کنند.



شکل 5-15

## اشتراک گذاری در حالت پیشرفته

یکی دیگر از روش‌های اشتراک گذاری منابع استفاده از حالت پیشرفته در سربرگ Sharing می‌باشد. مزیتی که در این روش وجود دارد قابلیت انجام تنظیمات بیشتر و اعمال مجوزهایی با جزئیات بیشتر می‌باشد. برای آشنایی بیشتر با این روش تمرین 3-5 را انجام دهید.

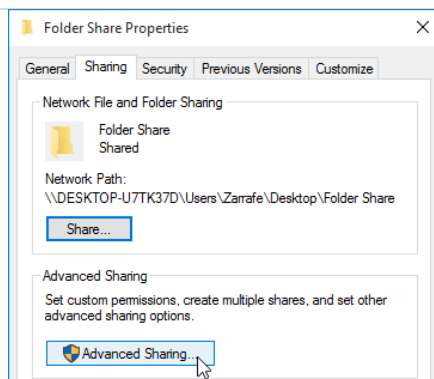
### تمرین 3-5

**عنوان:** به اشتراک گذاری منابع با حالت پیشرفته

**شرح:** در این تمرین قصد داریم تا پوشه‌ای را با استفاده از حالت پیشرفته برای تمام افراد موجود در شبکه به اشتراک بگذاریم.

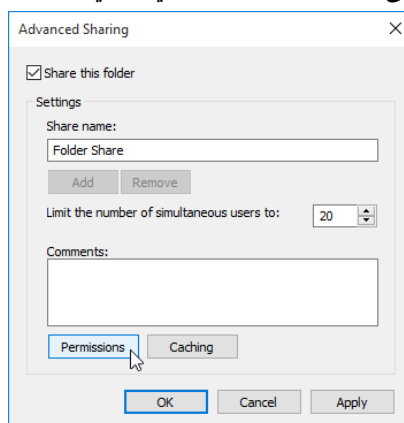
**مراحل تمرین:**

1. بر روی پوشه مورد نظر راست کلیک کرده و سپس گزینه Properties را انتخاب کنید.
2. به سربرگ Sharing رفته و سپس بر روی گزینه Advanced Sharing کلیک کنید.



شکل 5-16

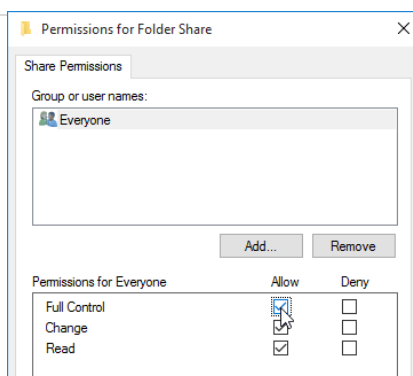
3. در این قسمت گزینه **Share this folder** را انتخاب کنید و به دلخواه می‌توانید نامی متفاوت را برای پوشه در سطح شبکه در نظر بگیرید که برای این مورد در قسمت **Share name** نامی برای پوشه وارد کنید. سپس بر روی دکمه **Permissions** کلیک کنید.



شکل 5-17

4. در قسمت بالا **Everyone** را انتخاب کرده و مطابق با شکل 5-18 تنظیمات را انجام دهید. حال بر روی دکمه **OK** کلیک کنید.

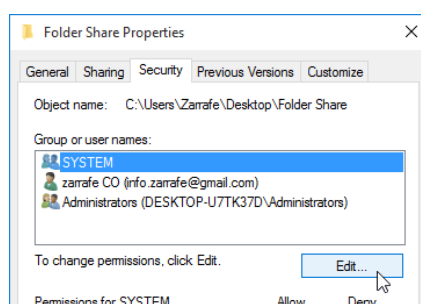




شکل 5-18

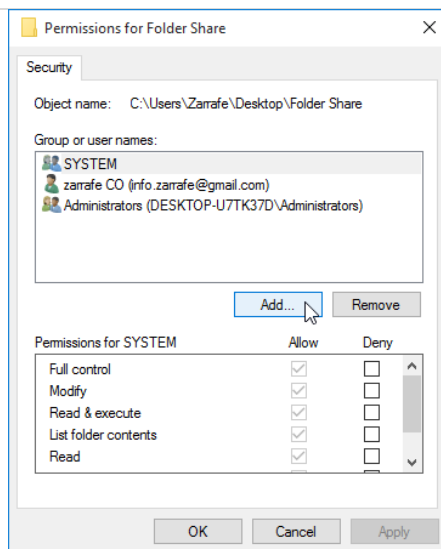
☑ تا به این جای کار پوشه مورد نظر در شبکه به اشتراک گذاشته شده است و کاربران تنها قادر به مشاهده‌ی این موارد به اشتراک گذاشته شده می‌باشند و نمی‌توانند از اطلاعات درون پوشه‌ها استفاده کنند، چرا که باید مجوزهای سطح دیسک (NTFS) نیز تعیین شود.

5. در پنجره‌ی Properties مربوط به پوشه مورد نظر به سربرگ Security رفته و سپس بر روی دکمه Edit کلیک کنید.



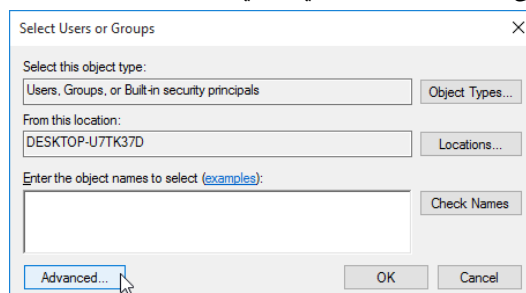
شکل 5-19

6. در پنجره‌ی باز شده بر روی دکمه Add... کلیک کنید.



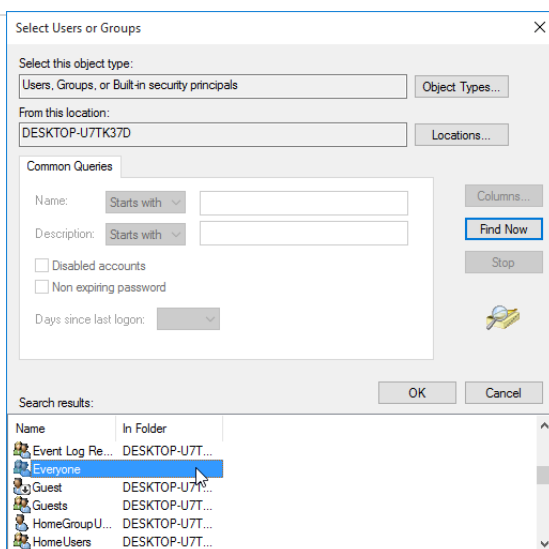
شکل 20-5

7. در این پنجره بر روی دکمه Advanced کلیک کنید.



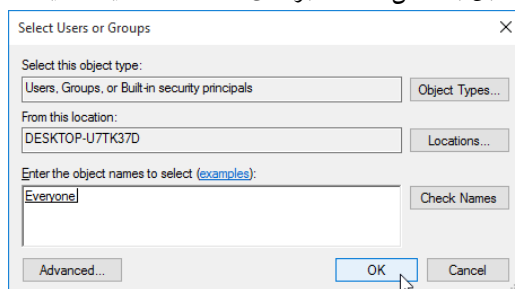
شکل 21-5

8. در این پنجره بر روی Find Now کلیک کنید سپس در لیست Everyone را انتخاب کرده و بر روی دکمه OK کلیک کنید.



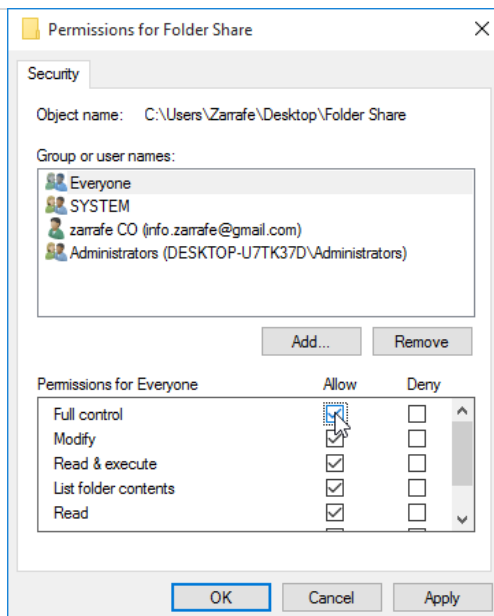
شکل 5-22

9. در پنجره باز شده مطابق با شکل 5-23 بر روی دکمه OK کلیک کنید.



شکل 5-23

10. در قسمت بالایی، Everyone را انتخاب کرده و مطابق با شکل 5-24 تمام گزینه‌ها را انتخاب کرده و بر روی دکمه OK کلیک کنید.



شکل 5-24

در شکل 5-24 و در قسمت Permissions for Everyone لیستی از مجوزها وجود دارد که بعضی از آنها شامل:

**Read:** این مجوز اجازه می‌دهد تا کاربران تنها مجوز خواندن پوشه‌ها را داشته باشند و نتوانند تغییراتی را در آن اعمال نمایند.

**Change:** این مجوز علاوه بر مواردی که در مجوز Read بیان شد این اجازه را فراهم می‌کند تا کاربران بتوانند تغییراتی در محتویات و مشخصات داده‌ها انجام دهند.

**Full Control:** این گزینه تمامی مجوزهای پوشه را به کاربران می‌دهد.

11. حال تمامی کاربران شبکه می‌توانند به این پوشه دسترسی کامل داشته باشند.

### اشتراک گذاری منابع با استفاده از کنسول MMC

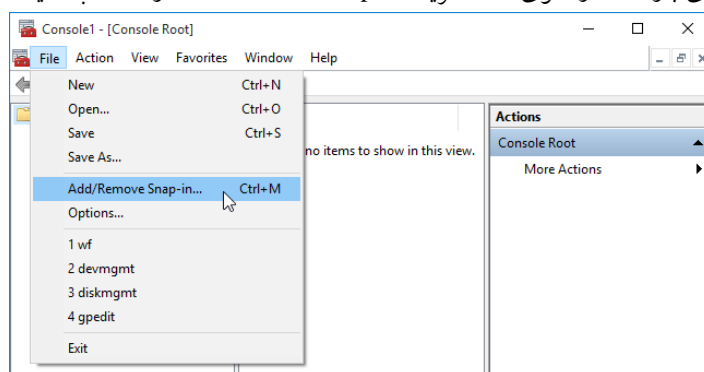
همان‌گونه که تا به اینجا متوجه شدید راه‌ها و روش‌های زیادی برای به اشتراک گذاری منابع وجود دارد که یکی دیگر از این روش‌ها استفاده از کنسول مدیریتی MMC می‌باشد. این کنسول یک محیط ساده و در عین حال منسجمی دارد که در آن می‌توان کل پوشه‌های به اشتراک گذاشته شده را مشاهده و مدیریت کرد.

به منظور آشنایی با این کنسول بهتر است تا کار با آن را در قالب تمرین 5-4 مورد بررسی قرار دهیم.

## تمرین 4-5

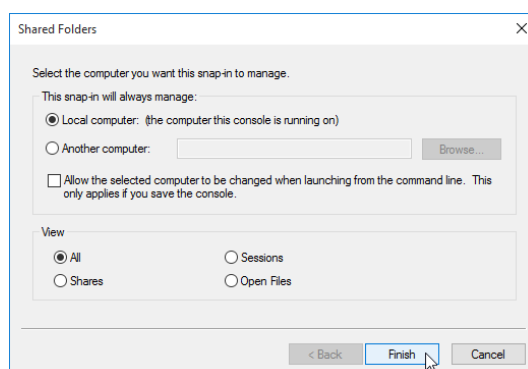
**عنوان:** به اشتراک گذاری پوشه با استفاده از کنسول MMC در ویندوز 10  
**شرح:** در این تمرین قصد داریم تا پوشه‌ای با نام Folder\_Share را برای تمامی کاربران شبکه به اشتراک بگذاریم به نحوی که کاربران تنها اجازه خواندن از این پوشه را داشته باشند.  
**مراحل تمرین:**

1. در عبارت Run MMC را تایپ کنید و بر روی گزینه OK کلیک کنید.
2. در پنجره‌ی باز شده از منوی File گزینه Add/Remove Snap in را انتخاب کنید.



شکل 5-25

3. در پنجره‌ی باز شده از قسمت سمت چپ گزینه Share Folder را انتخاب کرده و با استفاده از دکمه Add به قسمت سمت راست منتقل کنید در صفحه باز شده مطابق شکل 5-26 بر روی Finish کلیک کنید.

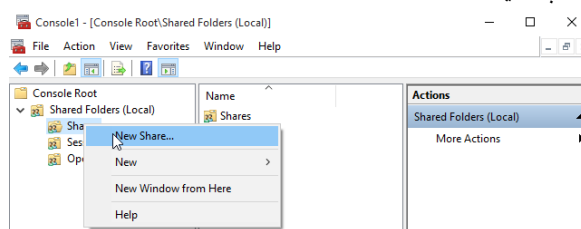


شکل 5-26

4. بعد از اضافه کردن Shared Folders در زیرشاخه آن سه گزینه وجود دارد که شامل: Shares: در این قسمت می‌توان کل پوشه‌های به اشتراک گذاشته شده را مشاهده کرد.

**Sessions:** در این قسمت می توان متوجه شد که چه افرادی به سیستم شما متصل می باشند.  
**Open Files:** در این قسمت می توان متوجه شد که چه افرادی در حال استفاده از چه منابعی هستند.

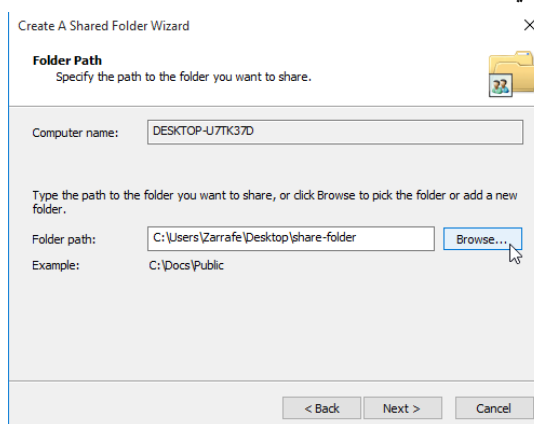
5. در ادامه برای اشتراک گذاری پوشه، بر روی Shares راست کلیک کرده و سپس گزینه New Share را انتخاب کنید.



شکل 5-27

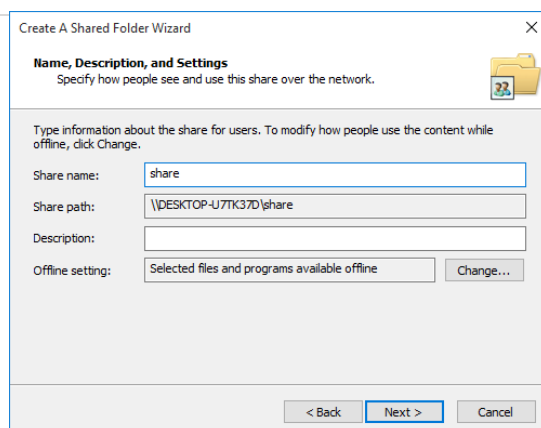
6. در این پنجره بر روی دکمه Next کلیک کنید.

7. در ادامه باید با استفاده از دکمه Browse... مسیر پوشه مورد نظر را مشخص کنید و سپس بر روی Next کلیک کنید.



شکل 5-28

8. در قسمت Share name نامی برای پوشه اشتراکی در نظر گرفته و سپس بر روی Next کلیک کنید.



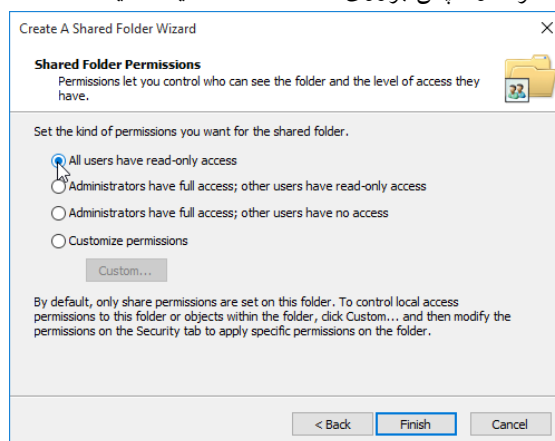
شکل 5-29

9. در پنجره‌ی Shared Folder Permissions می‌توان مجوزهای موردنظر را برای پوشه در سطح شبکه مشخص کنید. در این پنجره سه حالت وجود دارد:

- در این حالت تمامی کاربران مجوز کامل به پوشه دارند.
- با انتخاب این حالت تمامی مدیران دسترسی کامل به پوشه را دارند و سایر کاربران تنها مجوز خواندن از پوشه را دارند.
- در این حالت تمامی مدیران دسترسی کامل به پوشه را دارند و سایر کاربران مجوز دسترسی ندارند.

• در این حالت می‌توانید مجوزهای دسترسی مطابق با نیاز خود تعریف کنید.

گزینه اول را انتخاب کرده و سپس بروی دکمه Finish کلیک کنید.

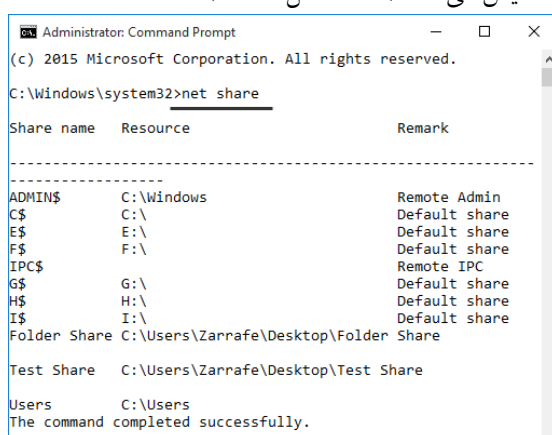


شکل 5-30

10. در انتها بروی دکمه Finish کلیک کنید.

## اشتراک گذاری با استفاده از Command Line (CMD)

استفاده از دستورات در محیط Command Prompt برای اشتراک گذاری پوشه‌ها به عنوان یکی از روش‌های معمول در بین کاربران حرفه‌ای می‌باشد. Net share دستوری که مختص کار با پوشه‌های اشتراکی در سطح شبکه می‌باشد. در صورتی که دستور Net share را به تنهایی اجرا کنید، اطلاعات تمامی پوشه‌های اشتراکی که در سیستم وجود دارد را نمایش می‌دهد (مانند شکل 5-31)



```

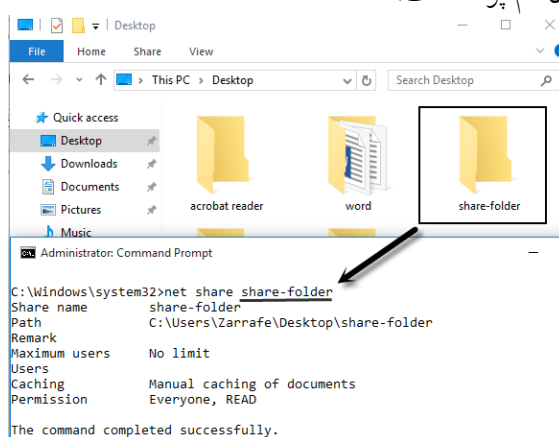
Administrator: Command Prompt
(c) 2015 Microsoft Corporation. All rights reserved.
C:\Windows\system32>net share

Share name      Resource                Remark
-----
ADMIN$          C:\Windows              Remote Admin
C$              C:\                      Default share
E$              E:\                      Default share
F$              F:\                      Default share
IPC$            G:\                      Remote IPC
G$              G:\                      Default share
H$              H:\                      Default share
I$              I:\                      Default share
Folder Share    C:\Users\Zarrafe\Desktop\Folder Share
Test Share      C:\Users\Zarrafe\Desktop\Test Share
Users           C:\Users
The command completed successfully.

```

شکل 5-31

در صورتی که بخواهید اطلاعات جزئی‌تری از پوشه به اشتراک گذاشته را مشاهده کنید کافی است تا نام پوشه را همراه با دستور Net Share استفاده کنید مانند [ShareFolderName] net share که در اینجا Share همان نام پوشه است.



```

Administrator: Command Prompt
C:\Windows\system32>net share share-folder

Share name      share-folder
Path            C:\Users\Zarrafe\Desktop\share-folder
Remark
Maximum users   No limit
Users
Caching         Manual caching of documents
Permission      Everyone, READ
The command completed successfully.

```

شکل 5-32



همان‌گونه که گفته شد با استفاده از دستور Net share می‌توان پوشه‌هایی را به اشتراک گذاشت. برای آشنایی بیشتر با نحوه‌ی عملکرد این دستور مراحل زیر را انجام دهید. با استفاده از محیط دستوری، پوشه‌ای بانام C\_Share که در مسیر C:\ قرار دارد را، با نام Test\_Share به اشتراک بگذارید.

1. محیط Command Prompt را از منوی Start اجرا نمایید.

2. با استفاده از دستور زیر سعی کنید تا پوشه را به اشتراک بگذارید.

```
net share Test_Share=C:\C_Share
```

Administrator: Command Prompt

```
C:\>net share Test_Share=c:\C_Share
Test_Share was shared successfully.
```

شکل 33-5

3. با استفاده از دستور Net Share مطمئن شوید که پوشه به درستی اشتراک گذاشته شده است.

Administrator: Command Prompt

```
C:\>net share

Share name      Resource                Remark
-----
ADMIN$          C:\Windows              Remote Admin
C$              C:\                     Default share
E$              E:\                     Default share
F$              F:\                     Default share
IPC$            C:\                    Remote IPC
G$              G:\                     Default share
H$              H:\                     Default share
I$              I:\                     Default share
Folder Share   C:\Users\Zarrafe\Desktop\Folder Share
share-folder   C:\Users\Zarrafe\Desktop\share-folder
Test Share     C:\Users\Zarrafe\Desktop\Test Share
Test_Share     c:\C_Share
Users          C:\Users
The command completed successfully.
```

شکل 34-5

در کنار استفاده از دستور net share می‌توانید از سوئیچ‌های زیر استفاده کنید:

- **/users: number**: این سوئیچ حداکثر تعداد کاربرانی که می‌توانند همزمان به منابع اشتراکی دسترسی داشته باشند را تعیین می‌کند. به‌عنوان مثال در دستور زیر مشخص شده است که حداکثر 20 کاربر می‌توانند از پوشه Test\_Share به‌صورت همزمان استفاده کنند.

```
Net share Test_Share /users: 20
```

• **/unlimited**: این سوئیچ مشخص می‌کند که تمامی کاربران شبکه می‌توانند همزمان از منابع به اشتراک گذاشته شده استفاده کنند. به‌عنوان مثال در دستور زیر مشخص شده است که بی‌نهایت کاربر می‌توانند از پوشه Test\_Share به صورت همزمان استفاده کنند.

```
Net share Test_Share /unlimited
```

• **/cache:automatic**: این سوئیچ قابلیت Offline File را به‌صورت خودکار برای پوشه‌های به اشتراک گذاشته شده فعال می‌کند.

• **/cache>manual**: این سوئیچ مشخص می‌کند که کاربران باید به‌صورت دستی پوشه‌های به اشتراک گذاشته را Cache کنند.

• **/cache:no**: این سوئیچ اجازه استفاده از قابلیت Offline File را نمی‌دهد.

• **/Delete**: با استفاده از این سوئیچ می‌توان پوشه‌ها را از حالت اشتراک گذاشته شده خارج کرد.

• **/net help**: این سوئیچ راهنمایی جامع درباره‌ی تمامی سوئیچ‌ها را در اختیار شما قرار می‌دهد.

توجه داشته باشید که با اضافه‌کردن علامت \$ در انتهای نام اشتراکی پوشه، می‌توان پوشه‌ها را به‌صورت مخفی به اشتراک گذاشت (مانند شکل 5-35).

```
Administrator: Command Prompt
C:\>net share Test_Share$c=c:\C_Share
Test_Share$ was shared successfully.
```

شکل 5-35

## اشتراک گذاری پوشه با استفاده از Windows PowerShell

استفاده از Windows PowerShell همانند محیط Command Prompt مبتنی بر دستور بوده با این تفاوت که محیط PowerShell امکانات و قابلیت‌های بیشتری را در اختیار کاربران قرار می‌دهد. در مراحل زیر قصد داریم تا با استفاده از محیط PowerShell اقدام به اشتراک گذاری پوشه در سطح شبکه کنیم.

با استفاده از PowerShell پوشه‌ای به‌نام P\_Share را که در درایو C:\ قرار دارد، به نام New\_Share به اشتراک می‌گذاریم.

1. در Run عبارت powershell.exe را وارد کرده و محیط PowerShell اجرا گردد.

2. در خط فرمان دستور `new-smbshare` را وارد کرده و سپس بر روی دکمه Enter کلیک کنید.

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> new-smbshare

cmdlet New-SmbShare at command pipeline position 1
Supply values for the following parameters:
Path: _
  
```

شکل 5-36

3. در ادامه باید مسیر پوشه موردنظر را وارد کنید.

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> new-smbshare

cmdlet New-SmbShare at command pipeline position 1
Supply values for the following parameters:
Path: c:\p_share
Name: _
  
```

شکل 5-37

4. در انتها با وارد کردن نامی برای پوشه اشتراکی مراحل به اشتراک گذاری پوشه انجام می شود.

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> new-smbshare

cmdlet New-SmbShare at command pipeline position 1
Supply values for the following parameters:
Path: c:\p_share
Name: New_Share

Name      ScopeName Path      Description
-----
New_Share *      c:\p_share
  
```

شکل 5-38

5. با استفاده از دستور `Get-SmbShare` مطمئن شوید که مراحل به اشتراک گذاری پوشه به درستی انجام شده باشد.

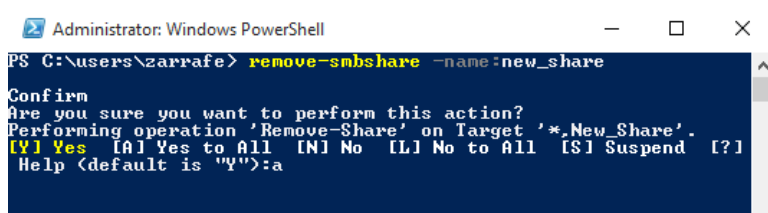
```

Administrator: Windows PowerShell
PS C:\users\zarrafe> get-smbshare

Name      ScopeName Path      Description
-----
ADMIN$    *      C:\Windows
C$        *      C:\
E$        *      E:\
F$        *      F:\
Folder Share *      C:\Users\Zarrafe\Desktop\Folder Share
G$        *      G:\
H$        *      H:\
I$        *      I:\
IPC$      *
New_Share *      c:\p_share
share-folder *      C:\Users\Zarrafe\Desktop\share-folder
Test Share *      C:\Users\Zarrafe\Desktop\Test Share
Test_Share *      c:\C_Share
Test_Share$ *      c:\C_Share
Users     *      C:\Users
  
```

شکل 5-39

با استفاده از دستور Remove-SmbShare می‌توان پوشه را از حالت اشتراک گذاشته شده خارج کرد.

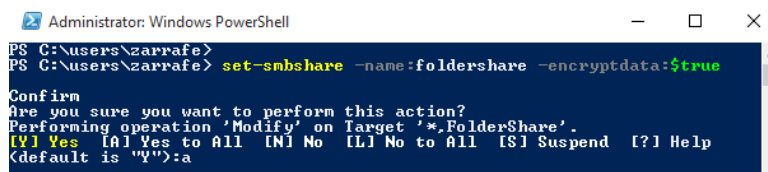


```

Administrator: Windows PowerShell
PS C:\users\zarrafe> remove-smbshare -name:new_share
Confirm
Are you sure you want to perform this action?
Performing operation 'Remove-Share' on Target '*,New_Share'.
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):a
  
```

شکل 40-5

با استفاده از دستور set-smbshare می‌توان مشخصات منابع به اشتراک گذاشته شده را تغییر داد. به‌عنوان مثال در شکل 41-5 پوشه Folder Share در حالت رمزگذاری شده (Encrypt) قرار می‌گیرد.



```

Administrator: Windows PowerShell
PS C:\users\zarrafe>
PS C:\users\zarrafe> set-smbshare -name:foldershare -encryptdata:$true
Confirm
Are you sure you want to perform this action?
Performing operation 'Modify' on Target '*,FolderShare'.
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):a
  
```

شکل 41-5

# پشتیبانی ویندوز 10

پشتیبانی از مدیریت دیسک



این PDF به صورت تصویری و مرحله به مرحله توضیح داده شده است.

[www.NetworkBooks.ir](http://www.NetworkBooks.ir)  
[www.TejaratServer.ir](http://www.TejaratServer.ir)



برگرفته از پروژه های عملی شرکت



## فصل ششم

### پشتیبانی از مدیریت دیسک

مباحث این فصل در دو قسمت "مقدماتی" و "حرفه‌ای‌تر شوید" ارائه شده است. در ابتدای هر فصل به بررسی مطالب ساده‌تری پرداخته شده و در قسمت "حرفه‌ای‌تر شوید" مباحث تخصصی‌تری مربوط به پشتیبانی از مدیریت دیسک را مورد بررسی قرار داده ایم لذا توصیه می‌شود ابتدا قسمت مباحث ابتدایی را مطالعه کرده و در صورتی که به مطالب تسلط پیدا کردید قسمت "حرفه‌ای‌تر شوید" را مطالعه نمایید.

## مدیریت دیسک

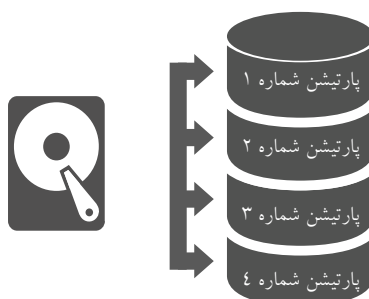
در این قسمت به بررسی مباحث درمورد ساختار دیسک، پارتیشن و فایل سیستم‌ها خواهیم پرداخت.

### آشنایی با نوع دیسک (Disk Type)

در ابتدا بهتر است تا قبل از پرداختن به نحوه پارتیشن‌بندی دیسک، با انواع دیسک‌ها آشنا شوید. به صورت کلی دیسک‌ها را می‌توان به دو دسته دیسک‌های Basic و Dynamic تبدیل کرد. دیسک‌های Basic به دلیل داشتن مدیریت آسان بیشتر مورد استقبال قرار گرفتند و در حالت عادی سیستم‌عامل‌ها از این نوع دیسک‌ها استفاده می‌کنند. دیسک‌های Basic می‌توانند با استفاده از روش‌های MBR و GPT پارتیشن‌بندی شوند، که در ادامه با MBR و GPT آشنا خواهید شد.

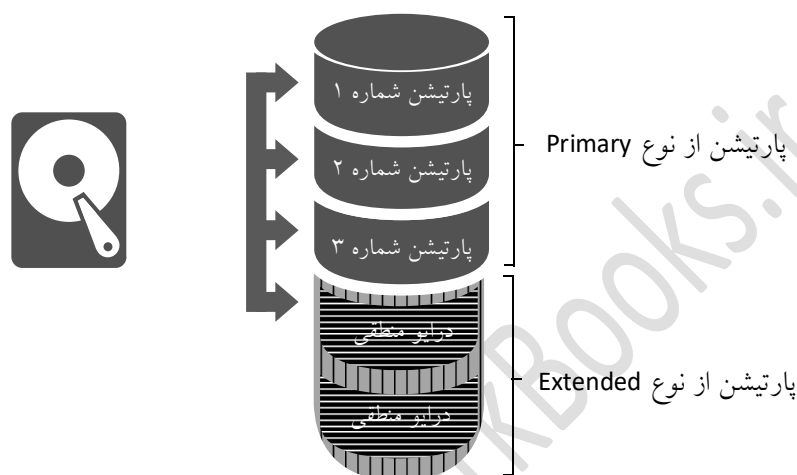
### آشنایی با MBR

به صورت پیش‌فرض تمامی سخت‌افزارهایی که سیستم‌عامل ویندوز بر روی آن‌ها نصب و اجرا می‌شود از دیسکی استفاده خواهد شد که نحوه پارتیشن‌بندی‌اش از نوع MBR باشد. در واقع زمانی که از MBR استفاده می‌شود، محل قرارگیری پارتیشن‌ها بر روی دیسک توسط یک جدول نگهداری می‌شود. در حالت عادی حداکثر تعداد پارتیشن‌هایی که می‌توان بر روی یک دیسک از نوع MBR ایجاد کرد برابر با 4 پارتیشن خواهد بود. توجه داشته باشید که تمامی 4 پارتیشن از نوع Primary ایجاد خواهد شد.



شکل 6-1

☑ پارتیشن Primary پارتیشنی است که سیستم عامل ویندوز می تواند بر روی آن نصب شود. همان گونه که قابل مشاهده است تنها می توان 4 پارتیشن از نوع Primary را بر روی دیسک ایجاد کرد. اما حالتی وجود دارد که با حذف یکی از پارتیشن های Primary و ایجاد یک پارتیشن از نوع Extended، می توان چندین درایو منطقی ایجاد کرد.

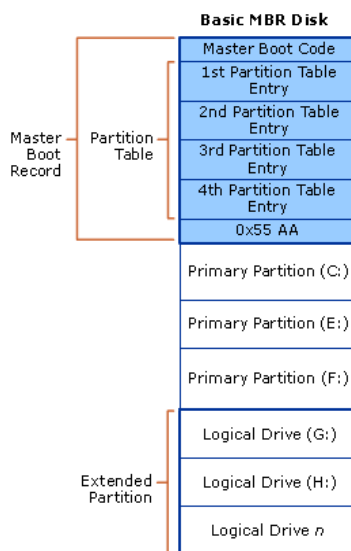


شکل 2-6

توجه داشته باشید که سیستم عامل و MBR حتماً می بایستی در پارتیشنی قرار گیرند که از نوع Primary باشد اما سایر درایوها می توانند از نوع منطقی در پارتیشن Extended باشند. MBR در واقع مشخص کننده پارتیشن ها و ساختار دیسک بوده و محل قرارگیری پارتیشن های Primary و Extended را مشخص می کند.

با توجه به شکل 3-6 در جدول MBR چهار اشاره گر وجود دارد که سه تای آن ها به پارتیشن های Primary اشاره کرده (C, E و F) و یکی از آن ها به پارتیشن Extended اشاره می کند. توجه داشته باشید که پارتیشن Extended در اینجا شامل 3 درایو از نوع Logical است (و پارتیشن Extended می تواند شامل n پارتیشن Logical باشد).





شکل 3-6

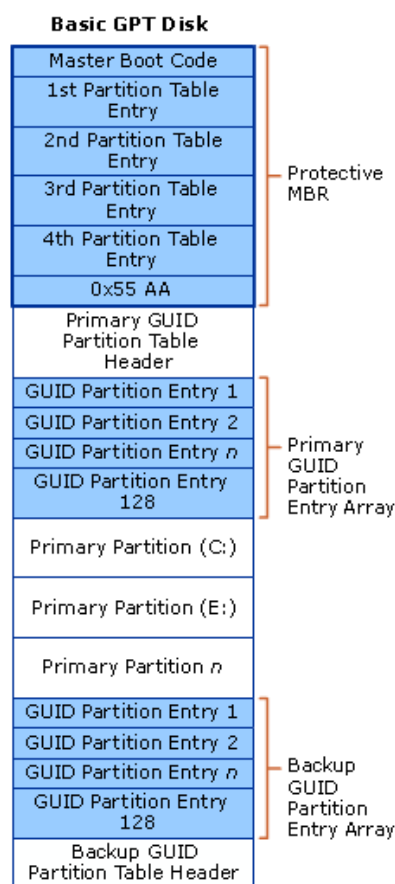
### آشنایی با GPT

کامپیوترهای اولیه دارای دیسک‌هایی با ظرفیت محدود و اندک بودند. هر دیسک شامل یک سری Sector بود که با دسته‌بندی این سکتورها، درایوها و یا پارتیشن‌هایی ایجاد می‌شد. با پیشرفت در نحوه ساخت و تولید دیسک، فضای ذخیره‌سازی شدیداً افزایش پیدا کرد تا جایی که دیگر نمی‌شد از MBR به‌منظور مدیریت فضای درایوها و یا پارتیشن‌ها استفاده کرد. از این‌رو یک شیوه دیگر برای مدیریت فضای دیسک استفاده شد که GPT نام دارد. همان‌گونه که قبلاً گفته شد در دیسک‌های MBR تنها می‌توان چهار پارتیشن از نوع Primary ایجاد کرد اما این درحالی است که با استفاده از GPT می‌توان تا 128 پارتیشن از نوع Primary ایجاد کرد.

**دیسک‌های GPT دارای مشخصه‌های زیر هستند:**

- امکان ایجاد پارتیشن‌هایی با حجم بزرگتر از 2 ترابایت
- وجود CRC به‌منظور محافظت از جدول پارتیشن‌ها برای افزایش قابلیت اطمینان

در شکل 4-6 ساختار کلی از دیسک GPT نمایش داده شده است. در ادامه این ساختار مورد بررسی قرار داده شده است.



شکل 4-6

**Protective MBR**: یکی از موارد مهمی که باید به آن توجه کرد قابلیت پشتیبانی از تکنولوژی‌های قدیمی است. در GPT به منظور برقراری سازگاری با دیسک‌های MBR، بخشی با نام Protective MBR در نظر گرفته شده است، چراکه ممکن است برخی از نرم‌افزارهای قدیمی مدیریت دیسک مانند F-Disk و NT Disk Administrator که قادر به تشخیص درایوهای GPT نیستند، ساختار دیسک GPT را به هم ریخته و باعث از بین رفتن اطلاعات شوند. با استفاده از

Protective MBR این نرم‌افزارها نخواهند توانست ساختار دیسک‌های GPT را به هم بریزند چراکه دیسک را به‌عنوان یک حافظه پر و یا ناشناخته تلقی خواهند کرد.

**Primary GUID Partition Table Header:** درواقع این فیلد نشان‌دهنده آغازجدول GTP است و اطلاعاتی از جمله طول سرآیند اصلی (Primary) و پشتیبان (Backup) مشخص شده است؛ همچنین CRC مربوط به سرآیند و پارتیشن‌ها در این فیلد قرار دارد.

**Primary GUID partition Entry Array:** درواقع نشان‌دهنده محل شروع هرپارتیشن بر روی دیسک است.

**Backup GUID partition Entry Array:** نسخه پشتیبان از محل قرارگیری پارتیشن‌ها بر روی دیسک است.

**Backup GUID Partition Table Header:** نسخه پشتیبان از سرآیند اصلی است.

اموری که می‌توان با دیسک‌های Basic انجام داد شامل:

- ایجاد و حذف پارتیشن‌ها
- ایجاد و حذف درایوهای منطقی
- فرمت کردن پارتیشن‌ها و تعیین آن به‌عنوان پارتیشن Active

دیسک‌های Dynamic یک‌سری ویژگی‌های بیشتر و بهتری را در اختیار شما قرار می‌دهند که دیسک‌های Basic از انجام آن‌ها عاجز هستند. به‌عنوان مثال می‌توان با استفاده از دیسک‌های Dynamic قابلیت‌هایی مانند Span، Strip و یا RAID را پیاده‌سازی کرد که در همین فصل به این مباحث پرداخته خواهد شد. دیسک‌های Dynamic همانند دیسک‌های Basic می‌توانند از روش-های MBR و GPT به‌منظور پارتیشن‌بندی فضای دیسک استفاده کنند. از مزایای مهم این دیسک‌ها مدیریت متمرکز داده‌ها است به نحوی که داده‌ها می‌توانند بر روی چند دیسک پراکنده شده و مدیریت شوند.

یکی دیگر از قابلیت‌های دیسک Dynamic گسترش فضای درایوها بدون محدودیت است به این معنی که می‌توان فضای یک درایو را در بین چند هارددیسک پخش کرد اما این درحالی است که دیسک‌های Basic فضای یک پارتیشن در صورتی قابل گسترش است که فضای پیوسته در هارد-دیسک فعلی وجود داشته باشد.

☑ در دیسک‌های Basic از شیوه MBR استفاده می‌شود و از پارتیشن Primary به‌منظور میزبانی ویندوز و پارتیشن Extended برای مدیریت درایوهای منطقی (Logical Drives) استفاده می‌شود.

☑ در دیسک‌های Basic که از نوع MBR هستند می‌توان 4 پارتیشن از نوع Primary و یا سه پارتیشن از نوع Primary و یک پارتیشن از نوع Extended تعریف کرد و اما در هنگامی که از GPT استفاده می‌شود می‌توان تا 128 درایو تعریف کرد.

☑ بر روی پارتیشن Extended که در درایوهای Basic تعریف می‌شود، می‌توان درایوهای منطقی تعریف کرد.

به درایوهایی که بر روی دیسک‌های Basic ایجاد می‌شود پارتیشن (Partition) گفته شده و به درایوهایی که بر روی دیسک‌های Dynamic ایجاد می‌شود Volume گفته می‌شود اما در متن کتاب برای سهولت تماماً از واژه پارتیشن استفاده شده است.

### آشنایی با Partition Style

به روشی که سیستم عامل برای سازمان‌دهی پارتیشن‌ها بر روی دیسک استفاده می‌کند Partition Style (نحوه پارتیشن‌بندی دیسک) گفته می‌شود.

Partition Style یا Partition Schema مربوط به زیرساخت اصلی دیسک بوده و مشخص می‌کند که پارتیشن‌بندی باید به چه صورت انجام پذیرد. در ویندوز دو نوع پارتیشن را می‌توان تولید و استفاده کرد که این پارتیشن‌ها شامل MBR و GPT است. هر کدام از روش‌های گفته شده دارای مزایا و معایب خاص خود بوده که در ادامه با موارد جزئی‌تر آشنا خواهید شد. توجه داشته باشید ویندوز در حالت پیش فرض به دیسکی نیاز دارد که پارتیشن موجود در آن از نوع MBR باشد.

## بررسی File System

**تعریف سیستم فایل - File System:** سیستم فایل ابزاری است برای سازمان‌دهی، نگهداری و بازیابی داده‌ها و همچنین مدیریت فضای سخت‌افزاری که داده‌ها بر روی آن قرار گرفته‌اند. به کمک فرمت‌های فایل سیستم، می‌توان نحوه ذخیره داده‌ها در رسانه ذخیره‌سازی را تعریف کنیم. فایل سیستم داده‌ها را به بهترین نحو ممکن سازمان‌دهی می‌کند و آن‌ها را با ویژگی‌های خاص سخت‌افزاری و نحوه ذخیره‌سازی بر روی دیسک تطبیق می‌دهد. ویندوز 8 از فایل سیستم NTFS و FAT32 پشتیبانی می‌کند اما در ویندوز سرور فایل سیستم Refs نیز وجود دارد که دارای ویژگی‌های بیشتری می‌باشد.

در هنگام برنامه‌ریزی جهت پیکربندی فضای ذخیره‌سازی سازمان File System از دو جهت برای سیستم عامل دارای اهمیت است: اول این که File System می‌تواند نهایت سطح امنیت برای تمامی اطلاعاتی که در خودسرور ذخیره شده‌اند را فراهم آورد و دوم این که موظف به ردیابی تمامی

داده‌های خود است.

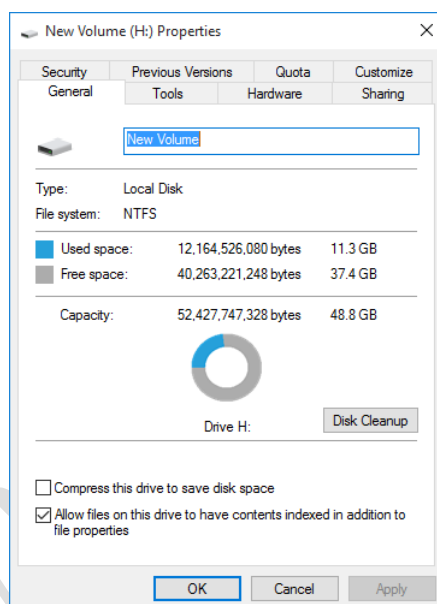
منظور از ردیابی داده، ثبت اطلاعات مربوط به داده‌های ذخیره‌شده در رسانه‌های ذخیره‌سازی است و در صورت بروز هرگونه تغییر در داده‌ها، اطلاعات مربوط به کاربری که باعث بروز تغییرات شده است را ذخیره و نگهداری کند.

ویندوز سرور 2012 از دو فایل سیستم پشتیبانی می‌کند:

Windows NT File System (NTFS)

Resilient File System (ReFS)

برای مشاهده فایل سیستم روی یکی از درایوها راست‌کلیک کرده و سپس گزینه Properties را انتخاب کنید.



شکل 5-6

## فایل سیستم ReFS

این نوع فایل سیستم تنها در ویندوز سرور 2012 به بعد موجود می‌باشد، در این کتاب تنها به بررسی ویژگی‌های این نوع فایل سیستم پرداخته ایم. ReFS برای به حداکثر رساندن دسترسی پذیری داده به‌وجود آمده است. با استفاده از ReFS در صورتی که ویندوز با مشکل مواجه شود، سیستم می‌تواند به عملیات خود ادامه دهد.

ReFS با استفاده از جامعیت داده یا Data Integrity، داده‌ها را در هنگام بروز خطا محافظت می‌کند.

## ویژگی‌های ReFS

- **دسترسی پذیری (Availability):** استراتژی نجات در ReFS باعث می‌شود تا در صورت بروز مشکل برای برخی از داده‌های هارددیسک، اطلاعات سالم از خراب جدا شود و مورد استفاده قرار گیرند.
- **مقیاس پذیری (Scalability):** ReFS می‌تواند از درایوهای (Volume‌هایی) با اندازه <sup>78</sup>2<sup>78</sup> بایت پشتیبانی کند که یکی از مزایای مهم این File System است.
- **Robust Disk Updating:** ReFS از یک سیستم بروزرسانی Disk با نام Allocate-on-Write Transactional Mode استفاده می‌کند. این مدل به جلوگیری بسیاری از مشکلات در نوشتن داده‌ها کمک می‌کند. چراکه ReFS در هنگام نوشتن داده‌ها در چندین مکان به صورت اتوماتیک اطلاعات جداول را بروزرسانی می‌کند.
- **Data Integrity:** ReFS از Check-Sum برای بررسی و صحت داده‌های ذخیره‌شده استفاده می‌کند.
- **Application Compatibility:** ReFS از بسیاری از ویژگی‌های NTFS و Win 32 API پشتیبانی می‌کند. به همین دلیل ReFS با بسیاری از برنامه‌های ویندوز سازگاری دارد.

## ویژگی‌های NTFS

- **Disk Quotas:** از این قابلیت جهت تخصیص فضا به کاربران سطح شبکه برای استفاده از هارددیسک استفاده می‌شود. می‌توان یک درایو را به اشتراک گذاشت و به هرکاربر اندازه مشخصی از آن درایو را اختصاص داد.
- **File System Encryption:** یکی از مشکلات اساسی که در سطح شبکه وجود دارد این است که مدیران اجازه دسترسی کامل به فایل‌های ذخیره‌شده بر روی سرور را دارند و این موضوع ممکن است از نظر حفظ حریم خصوصی اطلاعات کاربران، عیب بزرگی باشد. به همین دلیل در هنگام ذخیره کردن داده‌های کاربران، از رمزنگاری استفاده‌شده تا مدیران نتوانند از این داده‌ها سوءاستفاده کنند.
- **Dynamic Volumes:** با استفاده از این Volume‌ها می‌توان به راحتی در نحوه پیکربندی درایوها تغییراتی را بدون نیاز به Offline کردن هارددیسک انجام داد و یا در هنگام پیاده‌سازی RAID نیازی به Reboot کردن سرور نیست. این نوع پارتیشن‌ها در ReFS نیز وجود دارند.
- **Mounted Drive:** با استفاده از این ویژگی می‌توانید یک هارددیسک را به یک پوشه NTFS نگاشت کنید که این موضوع قدرت مدیریتی بالاتر و بهینه‌تر را ارائه می‌دهد.

- **Remote Storage:** با استفاده از این قابلیت می‌توان فایل‌هایی را که به‌ندرت استفاده می‌شوند را به یک درایو ذخیره‌ساز جانبی مانند Tape منتقل کرد که این عملیات جابه‌جایی به‌صورت خودکار صورت می‌پذیرد و باعث استفاده بهینه در حافظه خواهد شد.
- **Self-Healing NTFS:** این ویژگی باعث می‌شود تا در صورت بروز مشکلی در سطح دیسک بدون نیاز به Offline کردن هارددیسک بتوان مشکل را برطرف کرد.
- **Security:** در NTFS علاوه بر قابلیت تعیین سطح دسترسی بر روی پوشه می‌توان بر روی فایل‌ها نیز مجوز دسترسی اعمال کرد. این موضوع در ReFS نیز صدق می‌کند. با توجه به موارد گفته‌شده استفاده از NTFS امری اجتناب‌ناپذیر است، اما باید توجه داشته باشید که جهت نصب AD درایو شما باید حتماً از نوع NTFS باشد. در صورتی که می‌خواهید یک پارتیشن را از FAT یا FAT32 به NTFS تبدیل کنید، می‌توانید از دستور Convert استفاده کنید. مانند دستور زیر که پارتیشن C: را از FAT به NTFS تبدیل می‌کند.

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>convert c: /fs:ntfs_
```

شکل 6-6

## بررسی تنظیمات فعلی دیسک‌ها

از آنجایی که سرورها دارای چندین هارددیسک هستند، نیاز است تا تمامی تنظیمات دیسک‌ها مورد بررسی قرار داد. ویندوز سرور 2012 با استفاده از کنسول مدیریتی Disk Management محیطی را در اختیار شما قرار داده تا بتوان تنظیمات مربوط به دیسک‌ها را انجام داد.

# پشتیبانی از ویندوز 10

نظارت و پشتیبانی از ویندوز ۱۰



این PDF به صورت تصویری و مرحله به مرحله توضیح داده شده است.

[www.NetworkBooks.ir](http://www.NetworkBooks.ir)  
[www.TejaratServer.ir](http://www.TejaratServer.ir)



برگرفته از پروژه های عملی شرکت





# فصل هفتم

## نظارت و پشتیبانی از ویندوز 10

مباحث این فصل در دو قسمت "مقدماتی" و "حرفه‌ای‌تر شوید" ارائه شده است. در ابتدای هر فصل به بررسی مطالب ساده‌تری پرداخته شده و در قسمت "حرفه‌ای‌تر شوید" مباحث تخصصی‌تری مربوط به نظارت و پشتیبانی از ویندوز 10 منابع را مورد بررسی قرار داده‌ایم لذا توصیه می‌شود ابتدا قسمت مباحث ابتدایی را مطالعه کرده و در صورتی که به مطالب تسلط پیدا کردید قسمت "حرفه‌ای‌تر شوید" را مطالعه نمایید.

## مقدمه

یکی از مهم‌ترین وظایف تیم IT اطمینان از صحت عملکرد کلاینت‌ها، امنیت در عملکرد، درستی نصب درایورها با توجه به نسخه سیستم‌عامل و کارکرد صحیح سخت‌افزار مربوط به کامپیوترها می‌باشد. این موضوع (خرابی‌های نرم‌افزاری، نصب و بروزرسانی سیستم‌عامل، نصب درایورها و نرم‌افزارها) یکی از پردردسرتین و دغدغه‌های اصلی مدیران IT می‌باشد.

از این رو برای این‌که خرابی‌های نرم‌افزاری و همچنین مشکلات امنیتی شبکه را به حداقل برسانیم حتما باید سیستم‌عامل‌ها، آنتی‌ویروس‌ها و نرم‌افزارهای بروزی را برای کلاینت‌های شبکه فراهم آورد. در رابطه با سرورها اهمیت این موضوع بسیار بیشتر بوده تا حدی که توصیه می‌شود تا هیچ‌گاه اقدام به پیاده‌سازی و پیکربندی سرویسی بر روی یک سرور که سیستم‌عامل‌اش بروز نمی‌باشد نکنید، چرا که این امکان وجود دارد تا با مشکلات زیادی روبرو شوید. توجه داشته باشید که مشکلات امنیتی سرورهای شبکه را به مراتب خیلی بیشتر مورد تهدید قرار می‌دهند، پس بنابراین هرگز از بروزرسانی سیستم‌عامل‌های سرور امتناع نکنید.

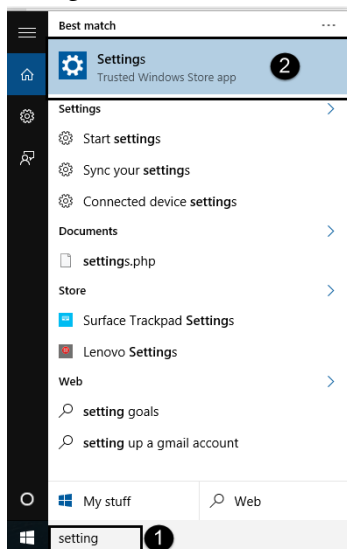
سایتی که در آن به‌روزرسانی کلیه سیستم‌عامل‌های مایکروسافت را می‌توان یافت Windows Update نام دارد.

حتی اگر که در این سایت آپدیت خاصی مد نظرتان باشد، به راحتی می‌توان به صورت دستی آن را در سایت جستجو و دریافت کرد. فایل‌های بروزرسانی معمولا به صورت KBxxxxxxx نامگذاری می‌شوند (مانند KB25884370).

در انواع نسخه مختلف سیستم‌عامل‌های ویندوز نرم‌افزاری به نام Windows Update وجود دارد و بسته به نسخه سیستم‌عامل فایل‌های مربوط به بروزرسانی ویندوز را از سایت مایکروسافت برای شما لیست می‌کند و در صورت تایید شما آن‌ها را دانلود و اعمال می‌کند.

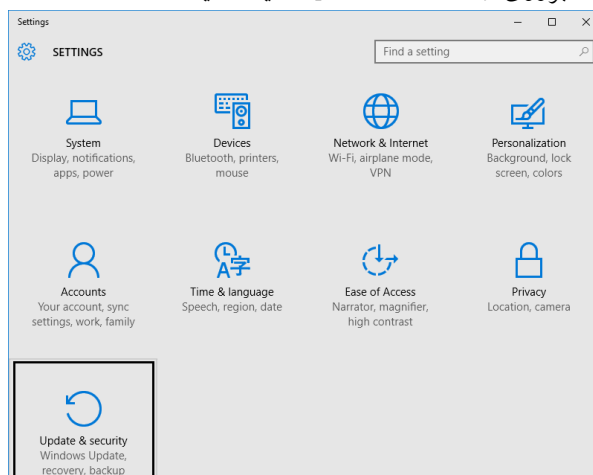
## کار با نرم‌افزار Windows Update

1. در منوی استارت Setting را جستجو کرده و مطابق شکل 7-1 Setting را اجرا کنید.



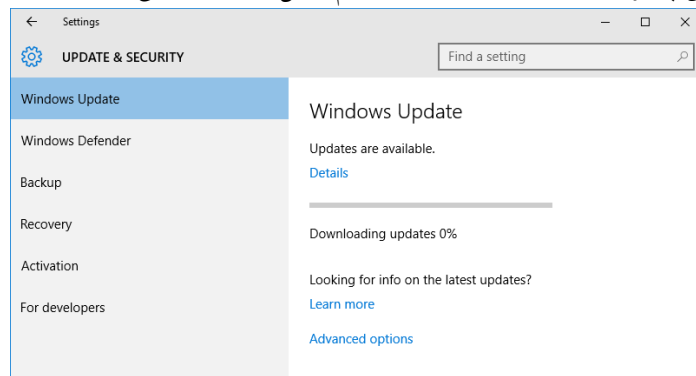
شکل 7-1

2. در پنجره باز شده بر روی Update and Security کلیک کنید.



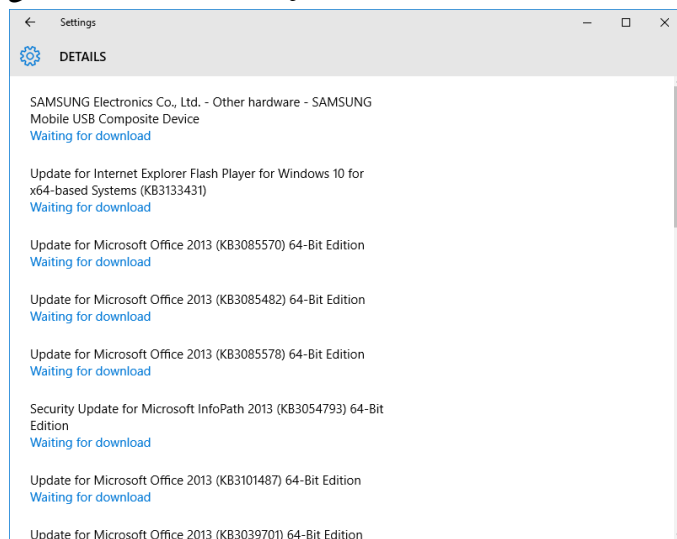
شکل 7-2

3. در این پنجره وضعیت update های سیستم عامل را مشاهده می کنید.



شکل 7-3

4. با کلیک بر روی لینک Detail می توان وضعیت Update ها را مشاهده کرد. همانطور که در شکل 4-7 مشاهده می کنید لیست Update ها و توضیحات در مورد آن ها، همچنین وضعیت آن ها را مشاهده می کنید. در اینجا همه update ها در انتظار دانلود (waiting for download) می باشند.

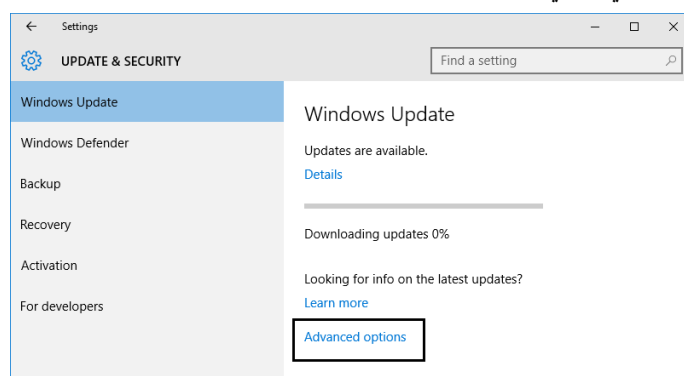


شکل 4-7

برای این که مشخص کرد که به روزرسانی به چه نحوی باید صورت بپذیرد و یا این که در چه زمانی باید فایل های مورد نیاز دانلود شود، باید در قالب یک سری استراتژی این موارد را پیاده سازی کرد که در ادامه به بررسی استراتژی های بروز رسانی خواهیم پرداخت.

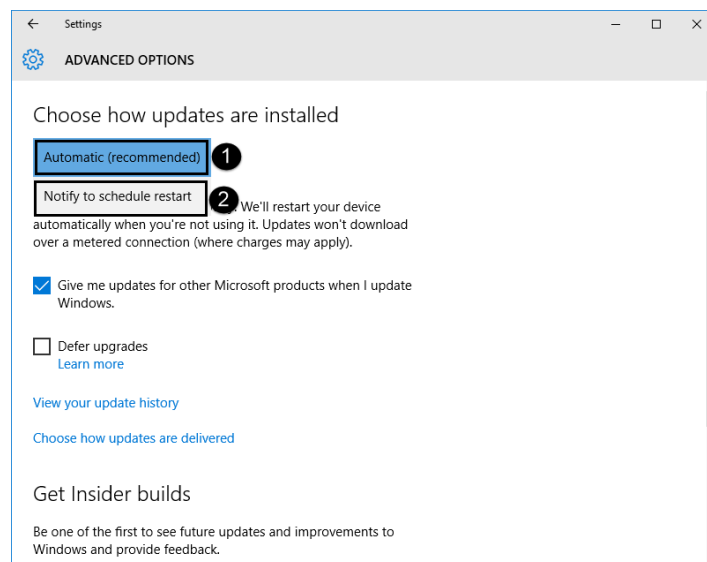
### مشخص کردن استراتژی‌های بروزرسانی

استراتژی آپدیت یعنی فایل‌های آپدیت‌ها چه زمانی باید دانلود و آپدیت‌ها چه زمانی باید نصب شوند. برای مشخص کردن استراتژی آپدیت وارد پنجره Update and Security شوید و بر روی لینک Advanced options کلیک کنید.



شکل 5-7

در پنجره باز شده و از لیست کشویی (مانند شکل 6-7) باید یکی از گزینه‌های موجود را انتخاب کنید.



شکل 6-7

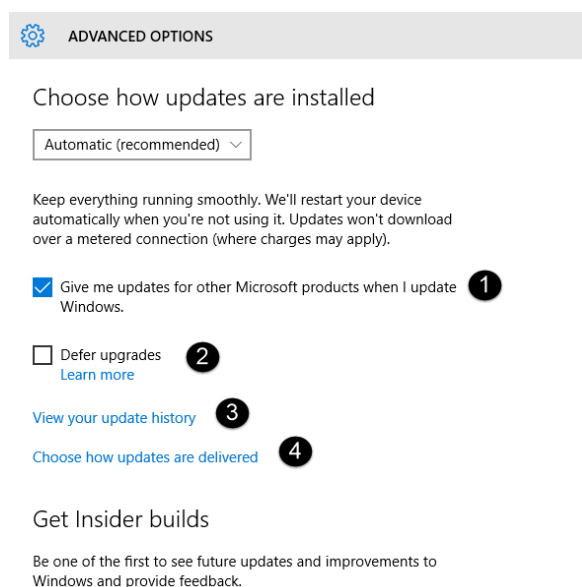
**1 Automatic:** با انتخاب این گزینه تمامی بروزرسانی‌های مربوط به سیستم‌عامل بدون دخالت کاربر دانلود می‌شود و نصب خواهد شد.

**2 Notify and Schedule restart**: برای نصب و ریستارت شده آپدیت ها از کاربر سوال

پرسیده می شود.

دیگر گزینه های صفحه Change setting

در پنجره Advanced Options چندین گزینه دیگر وجود دارد که در ادامه به بررسی آنها خواهیم پرداخت.



شکل 7-7

1 همان گونه که می دانید مایکروسافت نرم افزارهای زیادی را ارائه کرده است و برای هر کدام از این نرم افزارها یک سری بروزرسانی برای آنها در دسترس قرار خواهد گرفت. نرم افزار Microsoft Office یکی از نمونه های بارز از این گونه بروزرسانی است. با انتخاب این گزینه در زمان بروزرسانی سیستم عامل، دانلود بروزرسانی این نرم افزارها نیز به کاربر پیشنهاد خواهد شد.

2 زمانی که این گزینه را فعال نمایید ویژگی های جدید ویندوز تا چندین ماه نصب و دانلود نمیشود. این نوع به روزرسانی بر روی بروزرسانی های امنیتی تأثیری ندارد.

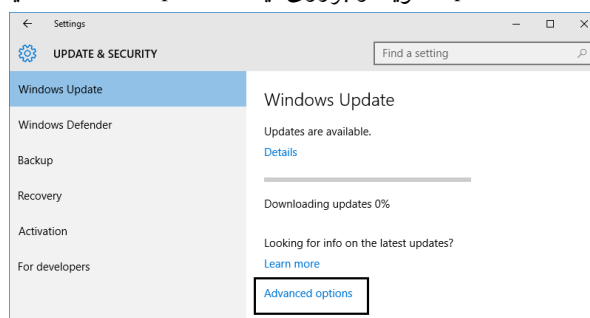
3 بوسیله این گزینه وضعیت Update های اخیر را مشاهده کنید و در صورت نیاز Update ها را حذف کنید.

4 از این قسمت می‌توان تنظیماتی انجام داد که این کامپیوتر Update های خود را در اختیار کامپیوتر های دیگر درون شبکه قرار دهد و یا آپدیت ها را از کامپیوترهای درون شبکه محلی دریافت کند. بدین صورت سرعت به‌روزرسانی کلاینت‌ها افزایش می‌یابد.

## بازگردانی کردن به‌روزرسانی‌ها

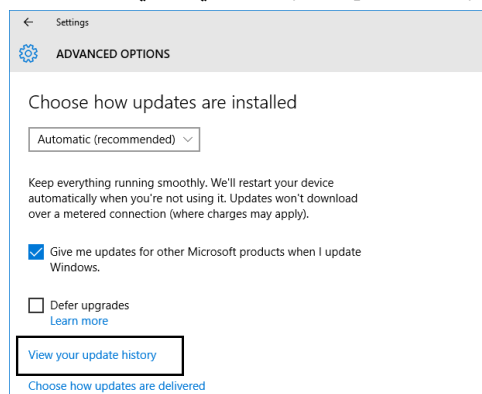
در صورتی که پس از به‌روزرسانی سیستم شما دچار مشکل شد می‌توانید به‌روزرسانی‌هایی که انجام داده‌اید را به‌حالت قبل بازگردانید برای انجام این کار مراحل زیر را دنبال کنید:

1. وارد پنجره Update and Security شوید و بر روی لینک Advanced options کلیک کنید.



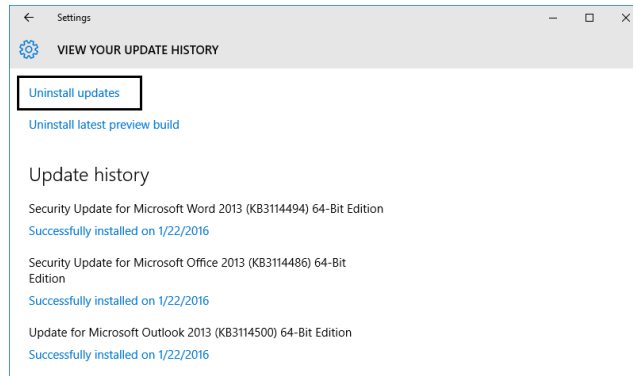
شکل 7-8

2. در این صفحه بر روی View your update history کلیک کنید.



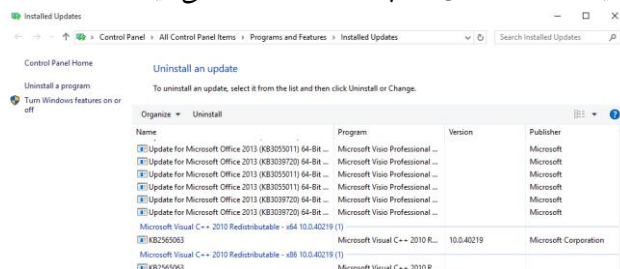
شکل 7-9

3. در این صفحه بروی Uninstall Update کلیک کنید.



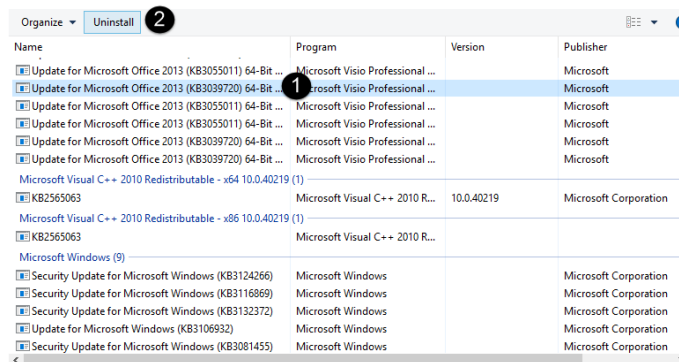
شکل 7-10

4. در این قسمت لیست Update های نصب شده را مشاهده می کنید.



شکل 7-11

5. از لیست Update مورد نظر را انتخاب و در منوی بالایی بروی دکمه Uninstall کلیک کنید تا Update حذف شود.



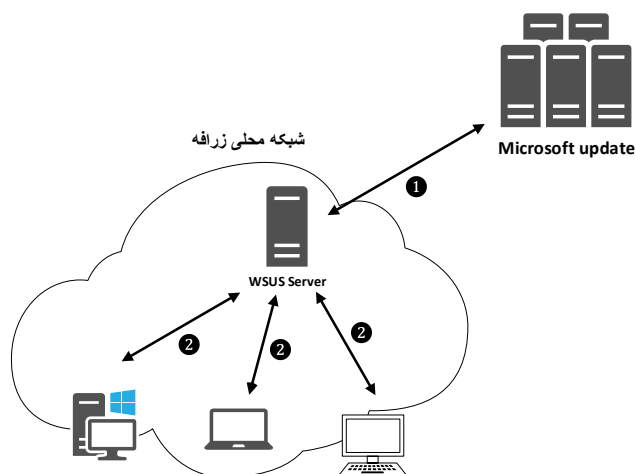
شکل 7-12



## سرویس (Windows Service Update Services) WSUS

برای درک بهتر از عملکرد سرویس WSUS به این مثال توجه کنید و فرض کنید که سازمانی در ابعاد بزرگ وجود دارد و در حدود 10.000 کامپیوتر دارد. سازمان با یک لینک به اینترنت متصل شده است تا بتواند سرویس های خود را به بیرون ارائه دهد و همچنین کاربران داخلی بتوانند از اینترنت استفاده کنند. حال در نظر بگیرید اگر هر 10.000 کامپیوتر برای بروزرسانی سیستم عامل - شان بخواهند به سایت مایکروسافت متصل شوند و فایل های بروزرسانی را دانلود کنند بر روی خط اتصال به اینترنت یک گلوگاه به وجود می آید و کل پهنای باند به منظور بروزرسانی سیستم عامل ها هدر خواهد رفت و در نتیجه کارهای دیگر سازمان مختل می شود. به عنوان مثال فرض کنید که تمام کامپیوترها دارای ویندوز 10 باشند و اگر کل فایل های بروزرسانی مربوط به ویندوز 10 در حدود 50 مگابایت باشد، هر 10.000 کامپیوتر یک فایل 50 مگابایتی تکراری را از سایت مایکروسافت دانلود می کنند که این موضوع بهینه نیست.

برای رفع این مشکل مایکروسافت سرویس WSUS را ارائه داده است. در شکل 7-13 چگونگی عملکرد این سرویس را مشاهده می کنید.



شکل 7-13

باتوجه به شکل 7-13 در گام اول (1) سرور WSUS که در شبکه داخلی وجود دارد با سایت مایکروسافت ارتباط برقرار کرده و کلیه فایل های بروزرسانی مربوط به تمام نسخه سیستم عامل های مایکروسافت (از جمله ویندوز XP، 7، 8، 2003، 2008، 2012 و ...) را دانلود می کند. سپس در گام دوم (2) تمامی کلاینت ها باید به نحوی تنظیم شوند که تمام فایل های بروزرسانی را از سرور WSUS دریافت کنند. این موضوع هم باعث افزایش سرعت و هم باعث بهینگی در استفاده از حجم

و پهنای باند اینترنت خواهد شد.

در ادامه امکاناتی که سرویس WSUS در اختیار شما قرار می‌دهد و شرایط کافی برای نصب آن را مورد بررسی قرار خواهیم داد.

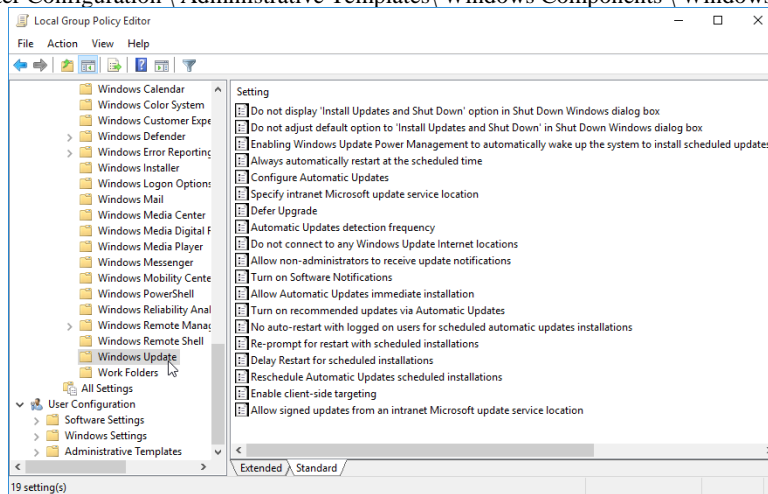
## تنظیمات پیشرفته Windows Update

در صورتی که نیاز به تنظیمات بیشتری برای مدیریت بروزرسانی‌ها دارید می‌توانید از ابزار کارآمد Group Policy استفاده کنید تا امکانات بیشتر و پیشرفته‌تری را در این امر در اختیار شما بگذارد. برای انجام این تنظیمات مراحل زیر را دنبال کنید:

1. در Run عبارت gpedit.msc را تایپ کنید تا Local Group Policy Editor باز شود.

2. مسیر زیر را دنبال کنید.

Computer Configuration \ Administrative Templates \ Windows Components \ Windows Update



شکل 7-14

همان‌طور که مشاهده می‌کنید در این بخش policyهای زیادی دیده می‌شود که هر کدام از آنها تنظیمات ویژه‌ای را در بحث بروزرسانی انجام خواهند داد. در ادامه برخی از Policyها را مورد بررسی قرار داده‌ایم.

### : Do Not Display “Install Updates And Shut Down” Option ...

با فعال کردن این گزینه در زمان خاموش کردن سیستم بروزرسانی‌ها حتی اگر آماده نصب هم

باشند نشان داده نخواهد شد .

#### **: Enabling Windows Update Power Management ...**

در هنگام فعال بودن این گزینه در صورتی که بروزرسانی زمان بندی شده باشد و ویندوز در حالت Hibernate باشد، سیستم به طور خودکار روشن می شود تا بروزرسانی انجام شود.

#### **: Always Automatically Restart At The Scheduled Time**

با فعال کردن این گزینه بعد از هر بروزرسانی مهم، سیستم به صورت اتوماتیک راه اندازی مجدد می شود .

#### **: Configure Automatic Updates**

این گزینه مشخص می کند که بروزرسانی خودکار چگونه صورت گیرد . در صورتی که این گزینه فعال شود و گزینه Auto download and installation settings انتخاب گردد بروزرسانی ها به صورت خودکار دانلود و نصب می شوند.

#### **: Automatic Updates Detection Frequency**

با فعال کردن این گزینه می توان مشخص کرد که ویندوز چه زمانی را برای بررسی بروزرسانی های جدید اختصاص دهد .

#### **: Do Not Connect To Any Windows Update Internet Locations**

با فعال کردن این گزینه هیچکدام از کلاینت ها نمی توانند بروزرسانی های جدید را دریافت کنند.

#### **: Allow Non-Administrators To Receive Update Notifications**

با فعال کردن این گزینه کاربران عادی نیز می توانند اعلان های مربوط به بروزرسانی را دریافت

#### **: Turn On Software Notifications**

کنند با فعال کردن این گزینه زمانی که بروزرسانی برای یک نرم افزار وجود داشته باشد با یک پیغام آن را اعلان می کند .

#### **: Allow Automatic Updates Immediate Installation**

با فعال کردن این گزینه زمانی که بروزرسانی دانلود شده و کاملاً آماده می باشد به صورت خودکار سریعاً نصب می شود .

#### **: Turn On Recommended Updates Via Automatic Updates**

با فعال بودن این گزینه Important Updates و Recommended Updates ها به صورت خودکار نصب می شوند.

#### **: No Auto-Restart With Logged On Users For Scheduled Automatic Updates Installations**

در صورتی که این گزینه فعال شود Restart خودکار سیستم در طول بروزرسانی انجام نمی شود و

در آخر به کاربر اعلان می کند تا سیستم را Restart کند اما در صورتی که غیرفعال باشد به کاربر پیغام می دهد و پس از گذشت 5 دقیقه سیستم به صورت خودکار Restart می شود.

#### **: Allow Signed Updates From An Intranet Microsoft Update Service Location**

با فعال کردن این گزینه بروزرسانی خودکار را از شرکت های غیرمایکروسافتی قبول می کند در صورتی که Certificateها معتبر باشد.

## نظارت بر عملکرد سیستم

بعد از این که تمامی تنظیمات سیستم انجام شد حال نوبت به نظارت کردن بر سیستم می رسد تا مطمئن شویم که سیستم به صورت کارآمدی وظایف خود را انجام می دهد، همانند مثال های قبل در این جا نیز ابزارهایی وجود دارد که به ما برای نیل به این هدف کمک خواهد کرد.

### Task Manager

به کمک Task Manager می توانید پردازش هایی که از منابع سیستم استفاده می کنند را مدیریت کنید . کاربردهای Task Manager برای کاربر از شامل : بستن پردازش هایی که سیستم را دچار مشکل کرده اند، بستن برنامه هایی که نیاز به اجرای خودکار آنها نیست ، نمایش کاربرانی که از سیستم استفاده می کنند و ...

Task Manager 7 سربرگ دارد که در ادامه با این سربرگ ها آشنا خواهید شد . برای دسترسی به Task Manager 3 راه وجود دارد . که عبارتند از:

1- فشردن کلیدهای Alt+Ctrl+Delete و انتخاب گزینه Task Manager

2- فشردن کلیدهای Ctrl+Shift+Esc

3- راست کلیک روی Task bar و انتخاب گزینه Task Manager

### بررسی سربرگ های مختلف Task Manager

#### سربرگ Processes

در این سربرگ کلیه پردازش های فعلی را مشاهده می کنید که شامل دو دسته پردازش وجود دارند:

#### قسمت Apps

پردازش های ایجاد شده توسط کاربر باشند در این قسمت مشاهده می شوند. به ازاء هر برنامه در

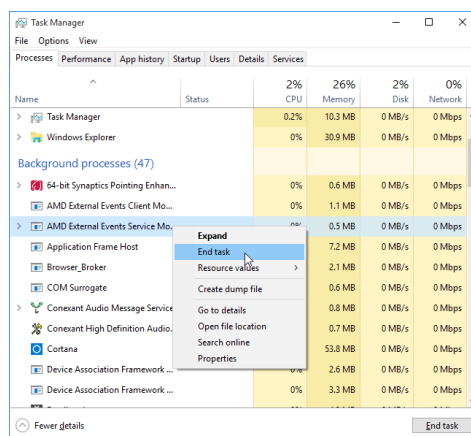
حال اجرا می‌تواند یک یا چندین پردازش در این قسمت ایجاد شود.

### Back ground processes

کاربر به صورت مستقیم در ایجاد این پردازش‌ها نقشی نخواهند داشت. معمولاً این پردازش‌ها توسط سیستم عامل یا برنامه‌های سیستمی ایجاد می‌شوند.

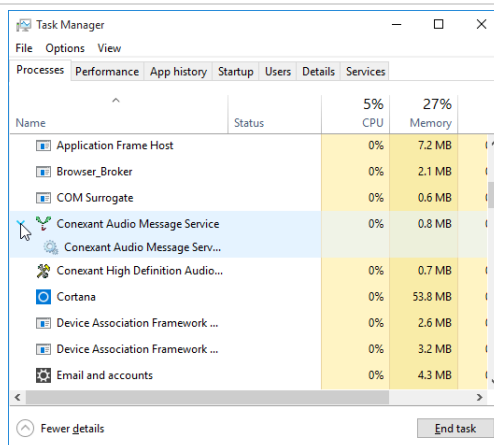
### چگونگی بستن پردازش‌ها (End Task)

برای بستن هر یک از پردازش‌ها کافی است بر روی آن راست کلیک کرده و گزینه End Task را انتخاب کنید.



شکل 7-15

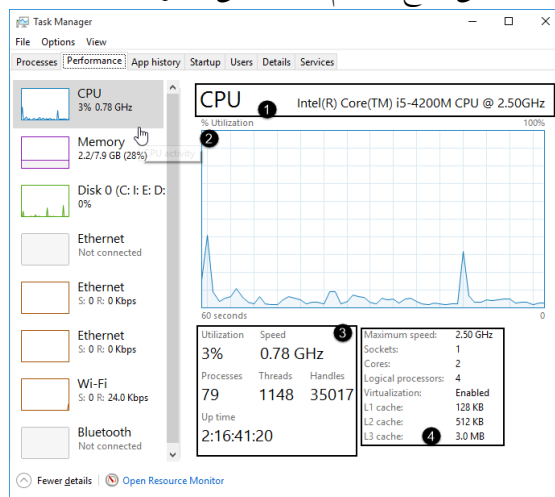
با کلیک کردن بر روی دکمه جهت‌دار هر پردازش، لیست پردازش‌های در ارتباط با آن را مشاهده کنید (مانند شکل 7-16).



شکل 7-16

### سربرگ Performance

در این سربرگ وضعیت کارایی منابع سیستم و اطلاعاتی درمورد آنها را مشاهده خواهید کرد.



شکل 7-17

در سمت چپ بر روی گزینه‌ی CPU کلیک کنید تا در قسمت سمت راست اطلاعات مربوط به CPU را مشاهده کنید.

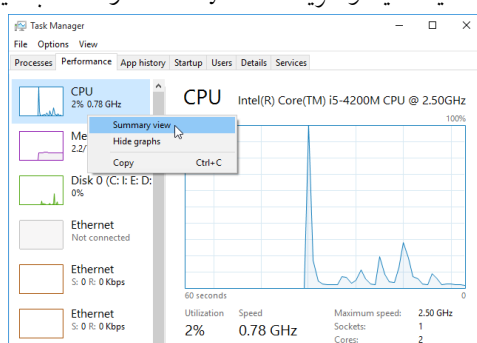
1 نام و مدل CPU را مشاهده می‌کنید.

2 نمودار مربوط به CPU Utilization را مشاهده می‌کنید که درصد کارکرد و مشغول بودن CPU را نشان می‌دهد.

3 اطلاعات مربوط به Utilization یا کارکرد، سرعت (Speed)، تعداد پردازش‌ها (Process)، تعداد Threadها و اطلاعات دیگری را مشاهده می‌کنید.

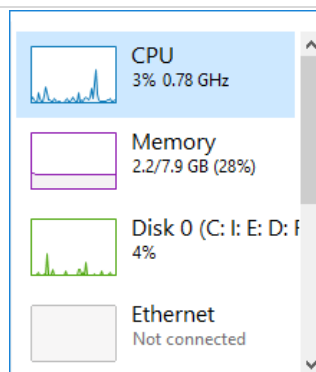
4 در این قسمت اطلاعات در مورد سرعت CPU، تعداد CPU، تعداد هسته‌های CPU، تعداد پردازنده‌های منطقی یا هسته‌های منطقی، مقدار Cache level یک، دو و سه و همچنین اطلاعاتی در مورد این که CPU از تکنولوژی مجازی‌سازی پشتیبانی می‌کند یا خیر را مشاهده می‌کنید.

برای این که بتوانید در هنگام کار این اطلاعات را نیز زیرنظر داشته‌باشید بر روی یکی از گزینه‌ها در پنل سمت چپ، راست کلیک کنید و گزینه Summary View را انتخاب کنید.



شکل 7-18

پس از کلیک بر روی Summary View پنجره‌ی مورد نظر به شکل 7-19 در خواهد آمد که در این حالت می‌تواند هنگام کار به شما کمک کند.



شکل 7-19

### سربرگ App history

همانند سربرگ Processes در این جا نیز ممکن است بعضی از نرم افزارها ساختاری درختی را دنبال کنند . همانند Mail, Calendar, and People که شامل زیر مجموعه های زیر است :

Name	CPU time	Network	Metered network	Tile updates
Camera	0:00:00	0 MB	0 MB	0 MB
Contact Support	0:00:00	0 MB	0 MB	0 MB
Cortana	0:04:32	11.8 MB	0 MB	0 MB
Get Office	0:00:01	0.1 MB	0 MB	0 MB
Get Skype	0:00:00	0 MB	0 MB	0 MB
Get Started	0:00:00	0 MB	0 MB	0 MB
Groove Music	0:00:00	0 MB	0 MB	0 MB
Mail and Calendar (2)	0:00:01	0 MB	0 MB	0 MB
Calendar				
Mail				
Maps	0:00:00	0 MB	0 MB	0 MB
Microsoft Edge	0:02:18	2.0 MB	0 MB	0 MB
Microsoft Solitaire Collec...	0:00:00	0 MB	0 MB	0 MB
Money	0:00:00	0.1 MB	0 MB	0.1 MB

شکل 7-20



# پشتیبانی ویندوز 10

پشتیبانی دسترسی از راه دور



این PDF به صورت تصویری و مرحله به مرحله توضیح داده شده است.

[www.NetworkBooks.ir](http://www.NetworkBooks.ir)

[www.TejaratServer.ir](http://www.TejaratServer.ir)



برگرفته از پروژه های عملی شرکت



# فصل هشتم

## پشتیبانی دسترسی از راه دور

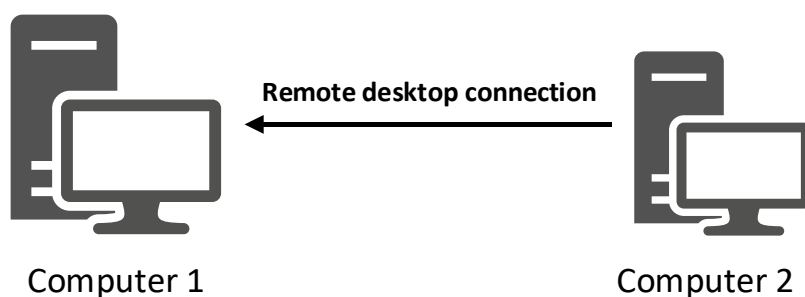
مباحث این فصل در دو قسمت "مقدماتی" و "حرفه‌ای‌تر شوید" ارائه شده است. در ابتدای هر فصل به بررسی مطالب ساده‌تری پرداخته شده و در قسمت "حرفه‌ای‌تر شوید" مباحث تخصصی‌تری مربوط به نظارت و پشتیبانی دسترسی راه دور مورد بررسی قرار داده شده لذا توصیه می‌شود ابتدا قسمت مباحث ابتدایی را مطالعه کرده و در صورتی که به مطالب تسلط پیدا کردید قسمت "حرفه‌ای‌تر شوید" را مطالعه نمایید.

### پروتکل Remote Desktop یا RDP

این پروتکل امکان دسترسی از راه دور کاربران به دسکتاپ و برنامه‌های کاربردی درون آن را فراهم می‌سازد. در واقع شما می‌توانید از راه دور به سرورهای درون سازمان Remote Desktop بزنید و با برنامه‌های کاربردی درون آن کار کنید. در کتاب ویندوز سرور 2012 به صورت کامل با Remote Desktop آشنا خواهید شد. در این جا فقط با فعال‌سازی و اتصال Remote Desktop ساده آشنا خواهید شد. برای آشنایی با تنظیمات Remote Desktop تمرین 8-1 را انجام دهید.

## تمرین 8-1

عنوان: پیکربندی Remote Desktop و نحوه‌ی اتصال به آن  
 شرح: در این تمرین Remote Desktop را بر روی کامپیوتر 1 فعال کرده و از طریق کامپیوتر 2 به دسکتاپ کامپیوتر 1 متصل خواهیم شد.



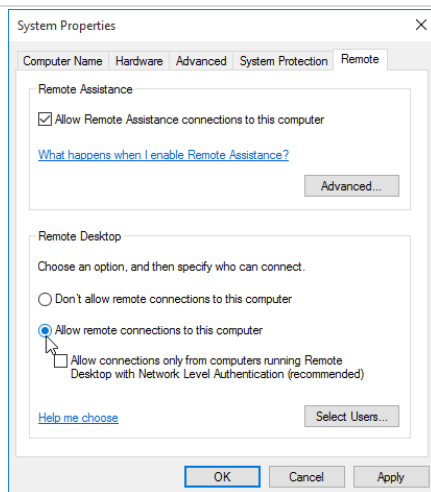
شکل 8-1

مراحل تمرین:

- گام 1** فعال‌سازی Remote Desktop بر روی کامپیوتر 1  
**گام 2** اتصال از کامپیوتر 2 به کامپیوتر 1 از طریق Remote Desktop

**گام 1 فعال‌سازی Remote Desktop بر روی کامپیوتر 1**

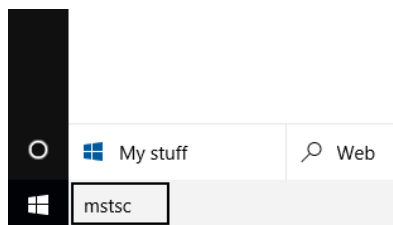
1. بر روی This PC راست‌کلیک کرده و گزینه Properties را انتخاب کنید.
2. از قسمت سمت چپ بر روی Remote Setting کلیک کنید.
3. در پنجره باز شده مطابق با شکل 8-2 گزینه Allow remote connection to this computer را انتخاب و بر روی دکمه OK کلیک کنید.



شکل 8-2

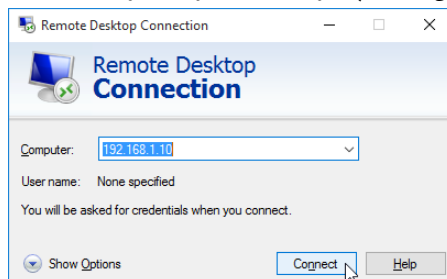
### گام 2 اتصال از کامپیوتر 2 به کامپیوتر 1 از طریق Remote Desktop

1. وارد کامپیوتر 2 شوید. ابتدا مطمئن شوید که کامپیوتر 1 را Ping می‌کنید.
2. حال در Run یا در قسمت جستجوی ویندوز کلمه mstsc را وارد کرده و بر روی دکمه Ok کلیک کنید.



شکل 8-3

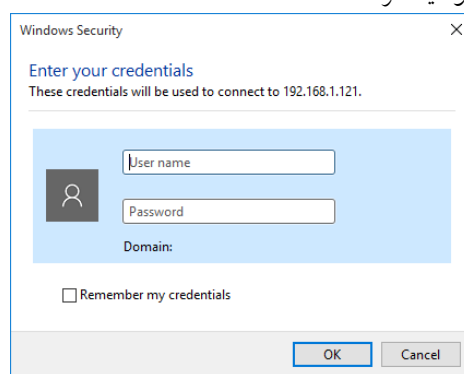
3. در پنجره باز شده آدرس IP کامپیوتر 1 را وارد کرده و بر روی دکمه Connect کلیک کنید.



شکل 8-4

4. در پنجره ظاهر شده بر روی دکمه yes کلیک کنید.

5. در پنجره ظاهر شده نام کاربری و رمز عبور کامپیوتر 1 را وارد کرده. پس از مدتی دسکتاپ کامپیوتر 1 را مشاهده خواهید کرد.



شکل 8-5

## شبکه خصوصی مجازی یا Virtual Private Network

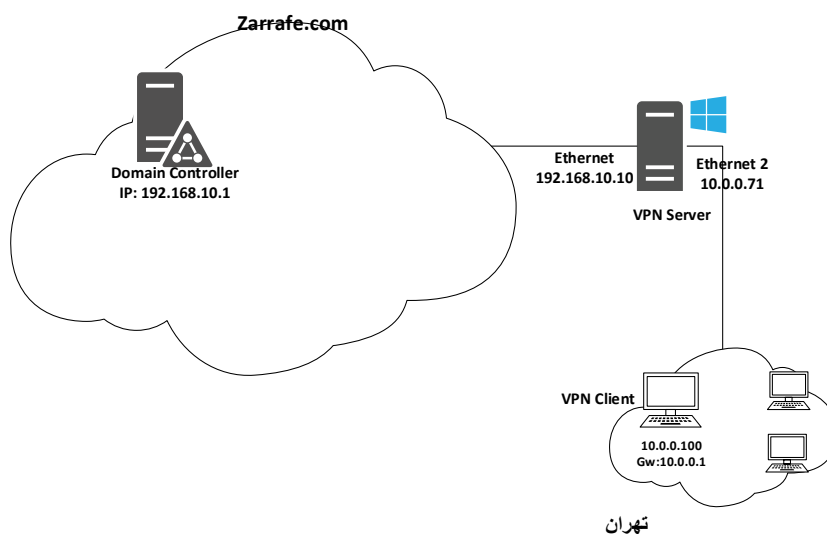
یکی از موارد مهم و قابل توجه در استفاده از شبکه‌ها، قابلیت اتصال از راه دور می‌باشد. به نحوی که کاربران بتوانند کارهایشان را بدون وجود محدودیت جغرافیایی انجام دهند. این امر با پیاده‌سازی یک ارتباط امن و خصوصی (یا VPN) اتفاق افتاده و یک استاندارد را تشکیل می‌دهد. از آنجایی که VPN یک استاندارد بوده پس در نتیجه محدودیتی به پلتفرم نداشته و بر روی تمامی دستگاه‌ها قابل استفاده می‌باشد. یکی از مواردی که همواره مدنظر است برقراری امنیت این ارتباط می‌باشد و برای این منظور راه‌کارهای زیادی ارائه داده شده‌است. در ادامه قصد داریم تا انواع پروتکل‌های VPN و نحوه امن کردن این دسته از ارتباطات را مورد بررسی قرار دهیم.

برای راه اندازی VPN نیاز به یک سرور VPN و پیکربندی کلاینت‌های VPN می‌باشد. در شکل 8-6 شبکه سازمان زرافه وجود دارد. به وسیله راه اندازی VPN این امکان فراهم می‌شود تا کاربران بتوانند از منزل به سرویس‌های درون شبکه محلی دسترسی داشته باشند و دورکاری انجام دهند. برای این منظور یک سرور VPN در لبه سازمان قرار داده می‌شود. این سرور از یک سمت به شبکه محلی و از سمت دیگر به شبکه اینترنت متصل است و بر روی آن تنظیمات سرور VPN انجام شده است.

کارمندان از بیرون سازمان 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.

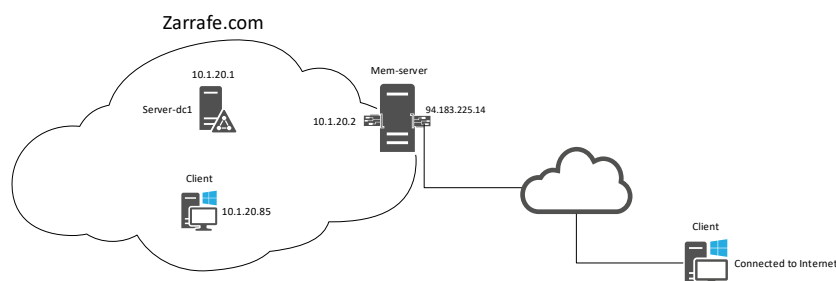
همچنین پس از برقراری VPN یک تونل منطقی بین کلاینت و سرور VPN ایجاد می‌شود و کلیه ترافیک‌ها از طریق این تونل رد و بدل می‌شوند و افراد عمومی به ترافیک‌های درون این تونل دسترسی نخواهند داشت.

همچنین از اطلاعات درون این تونل می‌توانند رمزگذاری بشوند یا نشوند. در ادامه به بررسی پروتکل‌های VPN و چگونگی عملکرد و پیاده‌سازی آن‌ها خواهیم پرداخت.



شکل 6-8

مثال دیگر از استفاده VPN زمانی است که شما بخواهید کارمندان از منزلشان یا در هنگام مأموریت 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 6-8 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 خصوصی-مجازی گفته می‌شود.



شکل 7-8

مثال دیگر از استفاده VPN زمانی است که شما از VPN به عنوان فیلترشکن استفاده می‌کنید. در آن زمان یک شبکه خارج از ایران وجود دارد و فیلتر نمی‌باشد، شما از شبکه ای درون ایران یک اتصال VPN 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 این که شما از شبکه خارج از ایران به اینترنت متصل هستید.

## پروتکل های VPN

پروتکل هایی که در ویندوز 10 برای استفاده از VPN مورد استفاده قرار می‌گیرد دامنه وسیعی دارد. در ادامه تمامی پروتکل هایی که برای VPN مورد استفاده قرار می‌گیرند را بررسی خواهیم کرد.

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

- پروتکل های VPN
- پروتکل های احراز هویت
- پروتکل های 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 نمونه های 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 2 بوده و می‌تواند پروتکل TCP/IP را در فریم های لایه 2 کپسوله کند.

### پروتکل PPTP

یک پروتکل لایه 2 بوده که در آن فریم های PPP در پکت های IP کپسوله شده است. این پروتکل نسبت به PPP بهتر عمل می‌کند، چراکه بسته ها در هنگام انتقال داده ها با استفاده از یکی از پروتکل های MS-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 بسته ها 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 7 به بالا پشتیبانی می‌شود.

### پروتکل IKE.v2

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

### پروتکل‌های احراز هویت (Authentication) و رمزگذاری

در هنگام استفاده از VPN چندین روش برای احراز هویت 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 احراز هویت رمزهای عبور 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 احراز هویت کاربران رمزهای عبور را به صورت متن عادی در شبکه ارسال نمی‌کند. در این پروتکل از روش دست‌تکانی سه طرفه استفاده می‌شود به این شکل که:

- ابتدا سرور یک متن چالش (به نام Challenge) را به سمت کلاینت ارسال می‌کند.
  - کلاینت از رمز عبور خود (و یا کلیدی که بین سرور و کلاینت مشترک می‌باشد) استفاده کرده و متن چالش (یا همان Challenge) را رمز و سپس به سمت سرور ارسال می‌کند.
  - سرور متن چالش دریافتی را با رمز عبور مربوط به کلاینت بازگشایی می‌کند و در صورتی که متن چالش برای سرور قابل قبول بود (به این شرط که متن چالش ارسال شده و دریافت شده از کاربر باید یکسان باشد) کاربر عملیات احراز هویت 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 احراز هویت را انجام می‌دهد. EAP ارائه دهنده قوی‌ترین و انعطاف پذیرترین خصوصیات امنیتی می‌باشد.



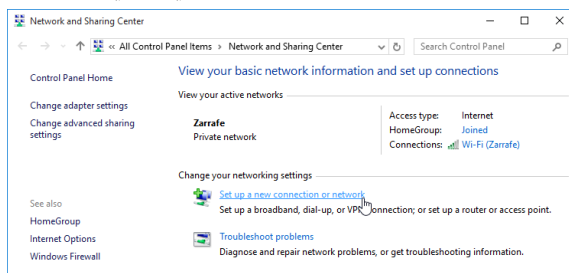
با استفاده از این روش می‌توانیم بر سر روش‌های احراز هویت پیشرفته‌تر از رمز عبور بحث کنیم. روش‌هایی هم‌چون Certificate و SmartCardRemote Desktop ها. این روش به عنوان روش پیش فرض برای ارتباطات بر روی کامپیوترهای مبتنی بر ویندوز 8 در نظر گرفته شده است. حال که با مفاهیم مربوط به پروتکل‌های VPN و پروتکل‌های ایمن‌سازی اتصال آشنا شدید بهتر است تا با نحوه ایجاد و پیاده‌سازی کانکشن در ویندوز 10 آشنا شوید. به منظور ساخت کانکشن VPN در ویندوز 10 بایستی تمرین 8-2 را دنبال نمایید.

## تمرین 8-2

عنوان: ساخت کانکشن VPN در ویندوز 10

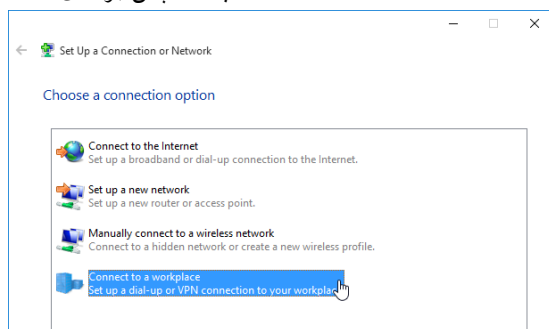
مراحل تمرین:

1. ابتدا وارد Control Panel و سپس Network and Sharing Center را اجرا نمایید.
2. بر روی لینک Set up a new connection or network کلیک کنید.



شکل 8-8

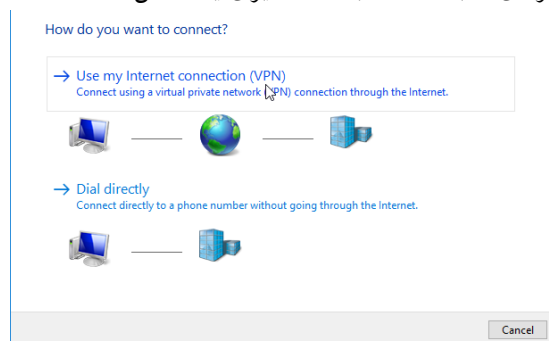
3. در ادامه گزینه Connect to a workplace را انتخاب و سپس بر روی Next کلیک کنید.



شکل 8-9

4. در پنجره Connect to a Workplace دو گزینه قابل انتخاب است که شامل:
  - Use my Internet connection: برقراری ارتباط VPN با استفاده از اینترنت

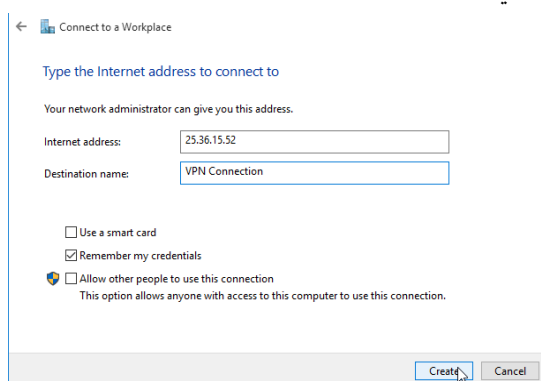
▪ Dial directly: برقراری ارتباط VPN با شماره‌گیری یک تلفن



شکل 8-10

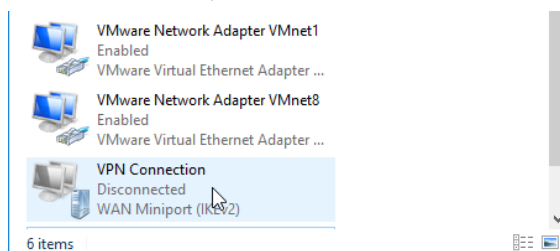
5. با انتخاب گزینه **Use my Internet connection** مراحل ایجاد کانکشن را ادامه دهید.

6. در ادامه باید آدرس IP مربوط به سرور VPN و یک نام برای کانکشن وارد نمایید و در انتها بر روی **Create** کلیک کنید.



شکل 8-11

با انجام مراحل بالا کانکشن VPN ایجاد شده و اتصال به سرور انجام می‌پذیرد. به منظور قطع و برقراری اتصال مجدد به VPN کافی است تا در **Network and Sharing Center** بر روی نام VPN کلیک کرده و گزینه **Connect** یا **Disconnect** را انتخاب کنید.



شکل 8-12

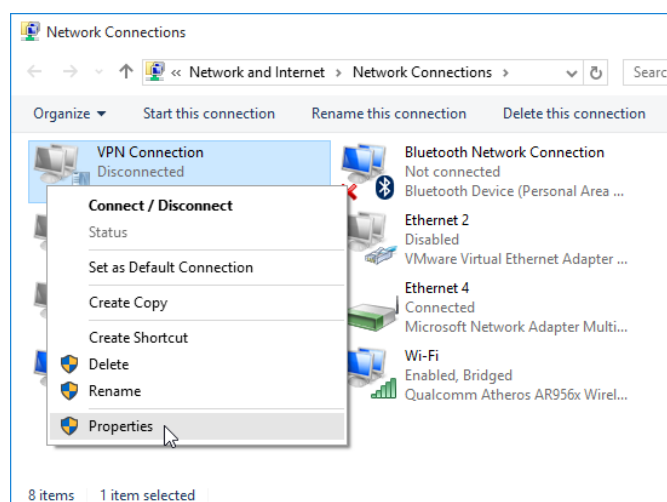
## تغییر مشخصات مربوط به کانکشن‌ها

بعد از ایجاد کانکشن VPN می‌توانید تنظیمات مربوط به آن را بررسی کرده و در صورت نیاز تغییرات مورد نیاز را اعمال نمایید.

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

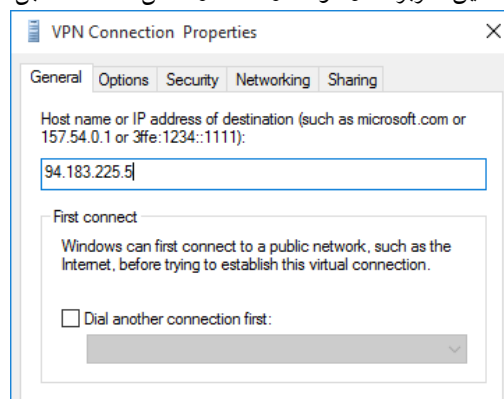
1. ابتدا از Control Panel برنامه Network and Sharing Center را اجرا کرده و سپس از منوی سمت چپ بر روی لینک Change adapter settings کلیک کنید.

2. در پنجره ظاهر شده بر روی VPN مورد نظر راست کلیک کرده و سپس گزینه Properties را انتخاب کنید.



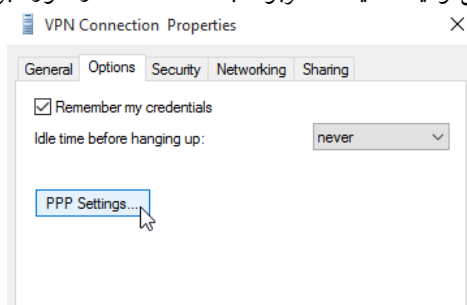
شکل 8-13

3. در پنجره باز شده چندین سربرگ وجود دارد که در شکل 8-14 قابل مشاهده است.



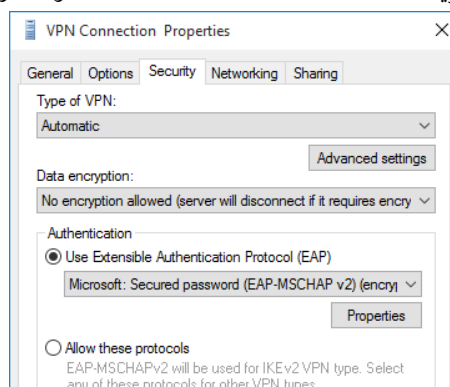
شکل 8-14

- 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 را مورد بررسی قرار دهید.



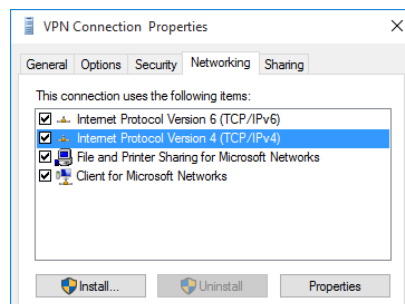
شکل 8-15

- 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 احراز هویت (مانند PAP، CHAP، MS-CHAP و ...) را تغییر دهید.



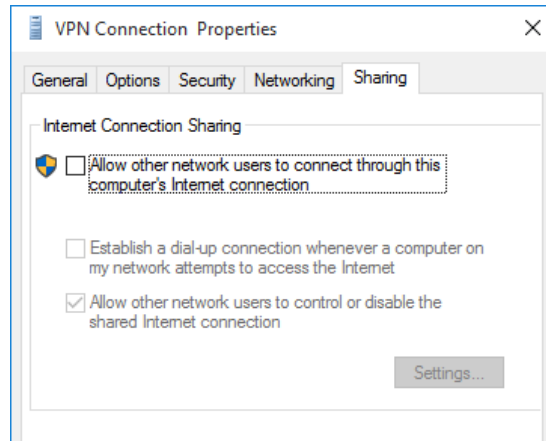
شکل 8-16

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



شکل 8-17

▪ در سربرگ Sharing می توان تنظیمات مربوط به اشتراک گذاری کانکشن (ICS) را انجام دهید.



شکل 8-18

# پشتیبانی ویندوز 10

نظارت و پشتیبانی از محیط مجازی

Hyper-V



این PDF به صورت تصویری و مرحله به مرحله توضیح داده شده است.

[www.NetworkBooks.ir](http://www.NetworkBooks.ir)

[www.TejaratServer.ir](http://www.TejaratServer.ir)



برگرفته از پروژه های عملی شرکت



# فصل نهم

نظارت و پشتیبانی از محیط مجازی (Hyper-V)

---

---

---

## پیکربندی Hyper-V

یکی دیگر از ویژگی‌های مهم در ویندوز 10 امکان نصب نرم‌افزار Hyper-V می‌باشد. امروزه با رشد و پیشرفت تکنولوژی در ساخت سخت‌افزارهای کامپیوتری، پتانسیل بالایی در اجرای پردازش‌های همروندی به وجود آمده است. از این رو با استفاده از مجازی‌سازی می‌توان از قدرت سخت‌افزار نهایت استفاده را برد. با استفاده از مجازی‌سازی می‌توانید چندین سیستم عامل را به صورت همزمان بر روی یک سخت‌افزار مشترک اجرا کنید. در ویندوز 10 قابلیت مجازی‌سازی توسط نرم‌افزار Hyper-V فراهم شده است، که این نرم‌افزار تنها بر روی نسخه‌های Professional و Enterprise قابل نصب می‌باشد.

به منظور نصب و راه‌اندازی Hyper-V نیاز به یک سری پیش‌نیاز می‌باشد که شامل:

- ویندوز 10 نسخه‌های Professional یا Enterprise با پلتفرم 64bit بیتی
- وجود پردازنده Second Level Address Translation (SLAT)
- وجود حداقل 4 گیگابایت RAM
- پشتیبانی سخت‌افزار از تکنولوژی Virtualization

## نصب Hyper-V

نرم‌افزار Hyper-V جزء سرویس‌های اصلی ویندوز 10 نمی‌باشد و به همین دلیل ابتدا باید آنرا با توجه به تمرین 9-1 نصب نمایید.

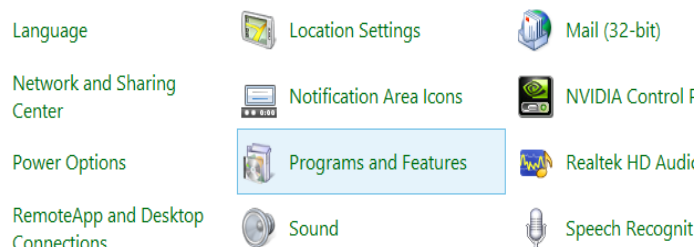
### تمرین 9-1

عنوان: نصب Hyper-v بر روی ویندوز 10

مراحل تمرین:

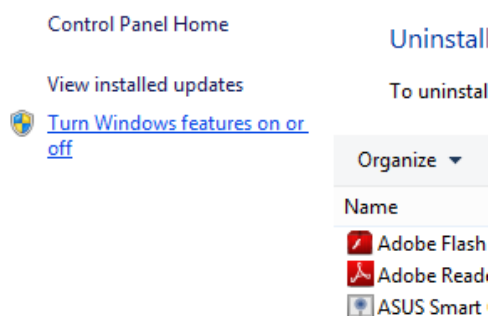
1. وارد Control Panel شوید و بر روی Programs and Features دوبار کلیک کنید.





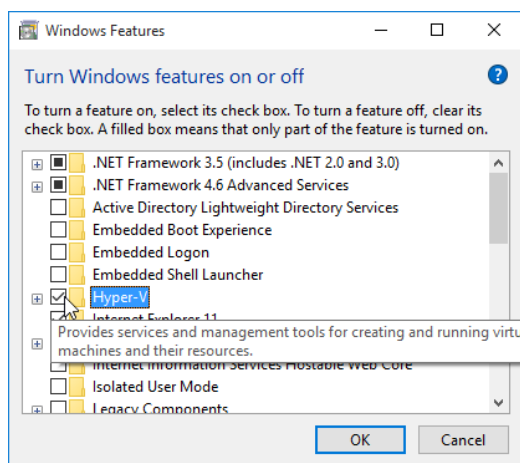
شکل 1-9

2. در پنجره باز شده بروی گزینه Turn Windows features on or off کلیک کنید.



شکل 2-9

در پنجره Windows Features همانند شکل 9-3 گزینه Hyper-V را انتخاب کرده و سپس بروی OK کلیک کنید.



شکل 3-9

3. پس از اتمام مراحل نصب، سیستم خود را Restart نمایید.  
پس از انجام مراحل بالا، نصب Hyper-V بروی سیستم به اتمام رسیده و باید مراحل پیکربندی

ماشین مجازی را شروع کنید.

## ایجاد و پیکربندی ماشین مجازی

پس از این که مراحل نصب Hyper-V به اتمام رسید باید اقدامات لازم را برای ساخت ماشین مجازی انجام دهید. برای این منظور در قالب تمرین 9-2 قصد داریم تا شما را با مراحل ساخت ماشین مجازی آشنا کنیم.

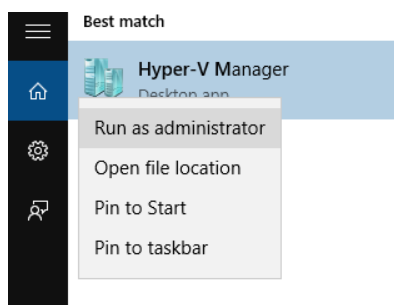
### تمرین 9-2

عنوان: ساخت ماشین مجازی

شرح: در این تمرین قصد داریم تا با استفاده از Hyper-V یک ماشین مجازی را ایجاد کنیم.

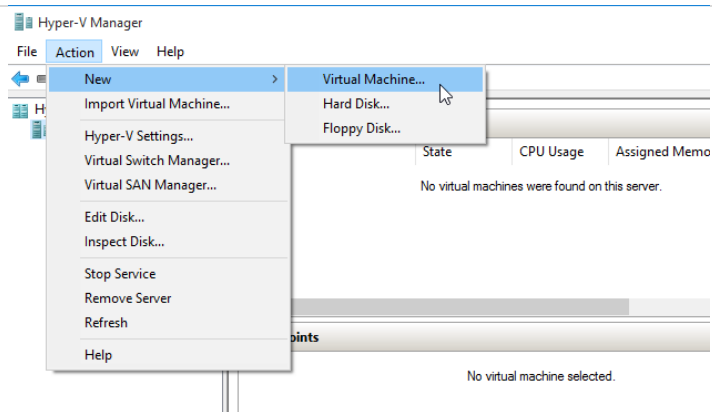
مراحل تمرین:

1. در منوی Start عبارت Hyper-V را تایپ کنید و سپس بروی Hyper-V Manager راست کلیک کرده و گزینه Run as administrator را انتخاب کنید تا کنسول مدیریتی Hyper-V نمایان شود.



شکل 4-9

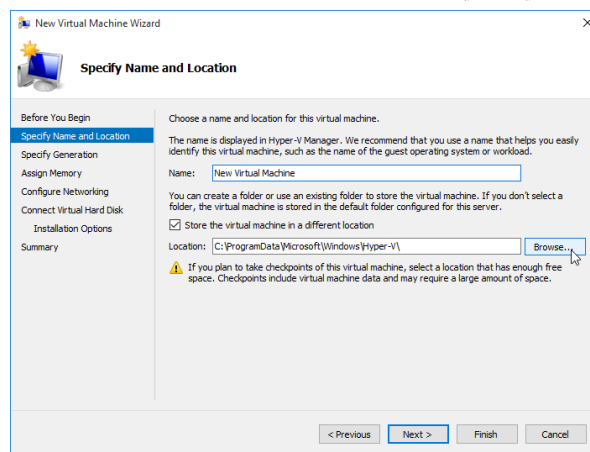
2. در پنجره‌ی باز شده از منوی Action گزینه New ← Virtual machine را انتخاب کنید.



شکل 5-9

3. بر روی گزینه Next کلیک کنید.

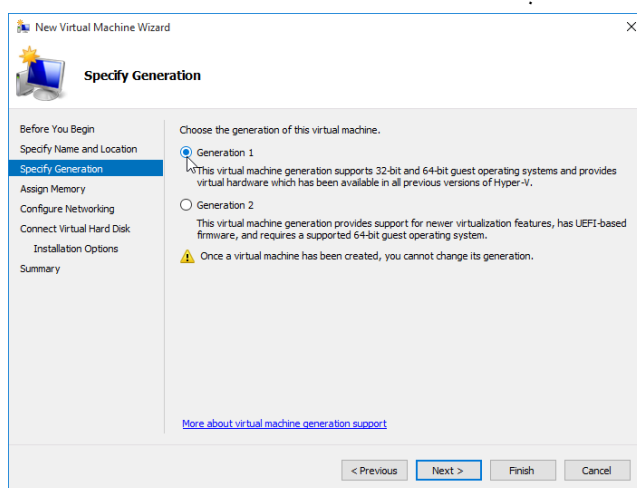
4. در این مرحله یک نام برای ماشین مجازی، و محل ذخیره شدن فایل‌های آن مشخص کنید و در ادامه بر روی Next کلیک کنید.



شکل 6-9

5. در این مرحله در صورتی که Generation 1 را انتخاب کنید بدان معناست که شما می‌خواهید از تنظیماتی که در نسل‌های قبلی Hyper-V بوده کماکان نیز استفاده کنید. ولی در صورتی که Generation 2 را انتخاب کنید به شما قابلیت‌هایی همچون PXE Boot, Secure Boot, SCSI

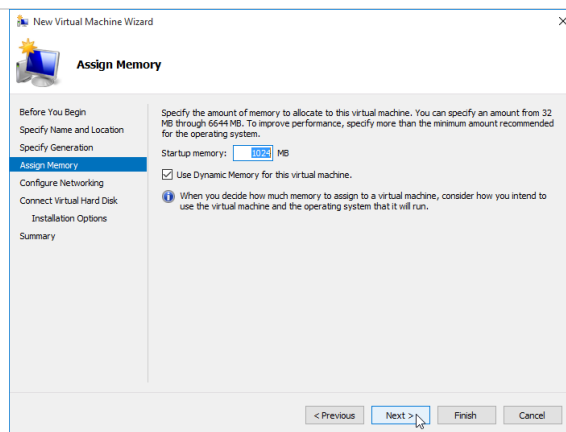
Boot را می دهد ولی به یک نکته توجه کنید که سیستم اصلی شما باید حداقل دارای ویندوز 8 و یا Windows 2012 R2 باشد.



شکل 9-7

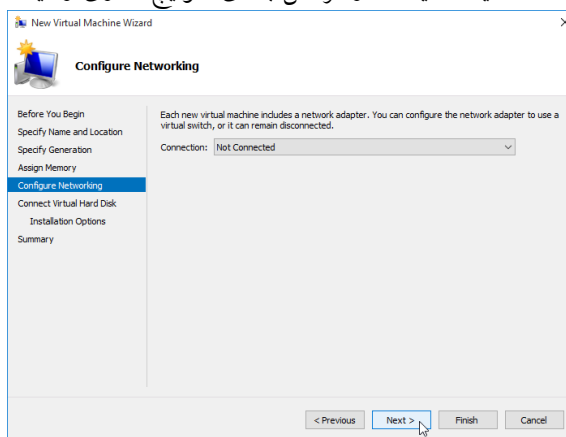
6. در این مرحله می توانید مقدار RAM را به صورت ایستا تخصیص دهید . در صورتی که می-خواهید RAM را به صورت پویا اختصاص دهید تیک گزینهی Use Dynamic Memory for this virtual Machine را بزنید.

**نکته:** در صورتی که مقدار RAM به صورت ایستا اختصاص داده شود بدین معناست که با روشن شدن ماشین مجازی همان میزان RAM به صورت یکجا به ماشین مجازی اختصاص داده می شود ولی در حالت پویا این مقدار به تدریج و با توجه به نیاز ماشین مجازی تا سقف مشخص شده افزایش پیدا می کند.



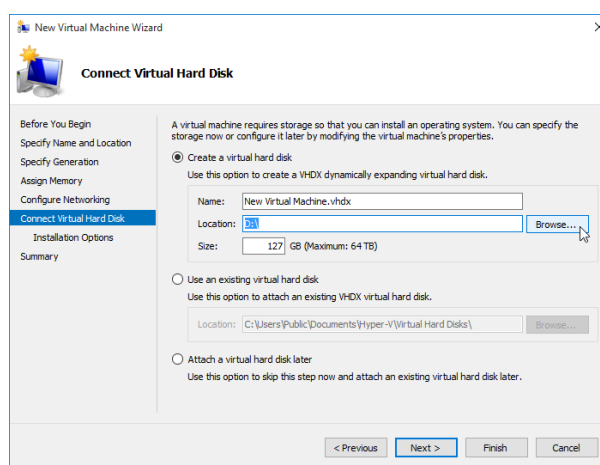
شکل 8-9

7. در این مرحله در صورتی که قبلاً سوئیچ مجازی ساخته اید، سوئیچ خود را انتخاب کنید. در غیر این صورت بر روی Next کلیک کنید تا در مراحل بعدی سوئیچ مجازی را ایجاد کنیم.



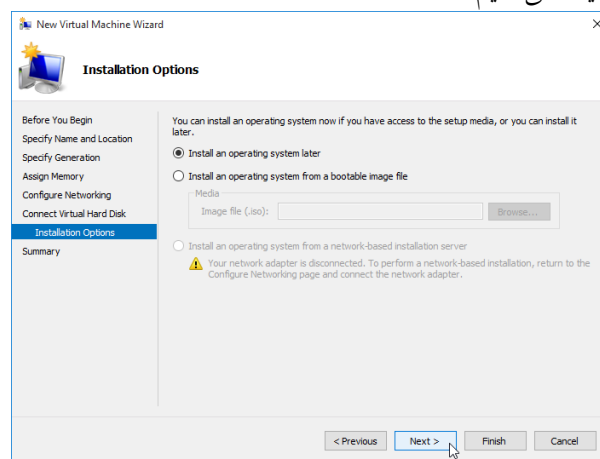
شکل 9-9

8. در این مرحله می‌بایست دیسک مجازی خود را بسازیم، در صورتی که قبلاً دیسک مجازی ساخته‌اید گزینه دوم را انتخاب کنید و مسیر آن را مشخص کنید و در صورتی که تاکنون دیسکی نساخته‌اید گزینه اول را انتخاب و نام و حجم آن را مشخص کنید و بر روی Next کلیک کنید.



شکل 10-9

9. در این مرحله می‌توان با انتخاب گزینه اول مراحل نصب ویندوز را بعداً انجام داد و یا با انتخاب گزینه دوم و معرفی یک Image از ویندوز مراحل نصب را انجام داد. ما در اینجا بر روی گزینه اول کلیک می‌کنیم.



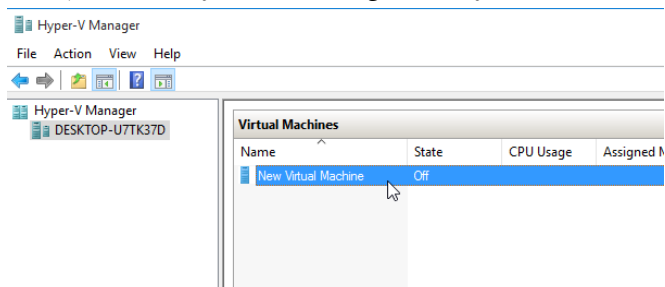
شکل 11-9

10. بر روی finish کلیک کنید تا مراحل به اتمام برسد.

## تنظیمات مربوط به ماشین مجازی

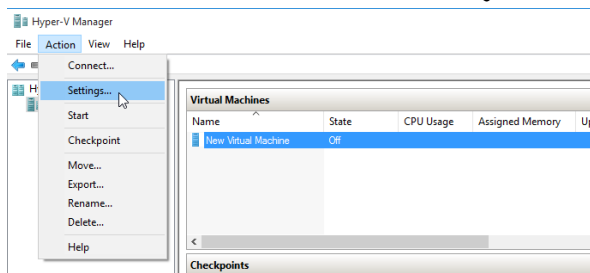
برای پیکربندی یک ماشین مجازی مراحل زیر را دنبال کنید :

1. Hyper-V Manager را باز کرده و ماشین مجازی مورد نظر خود را انتخاب کنید.



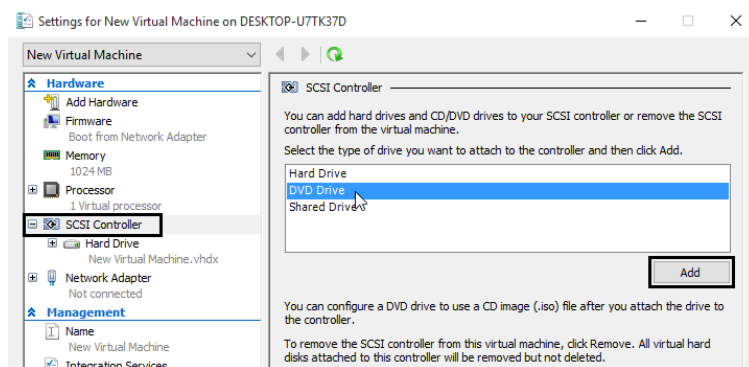
شکل 12-9

2. سپس از منوی Action بروی Settings کلیک کنید .



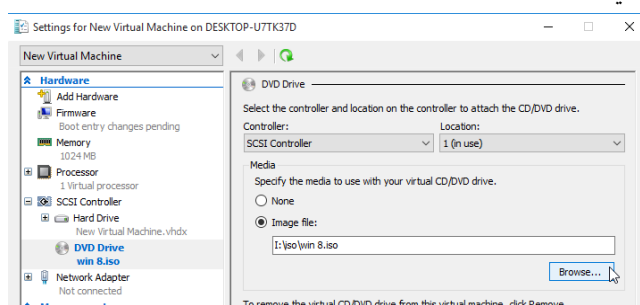
13-9

3. در این قسمت از زیرمجموعه SCSI Controller، گزینه‌ی DVD Drive را انتخاب و دکمه Add را بزنید.



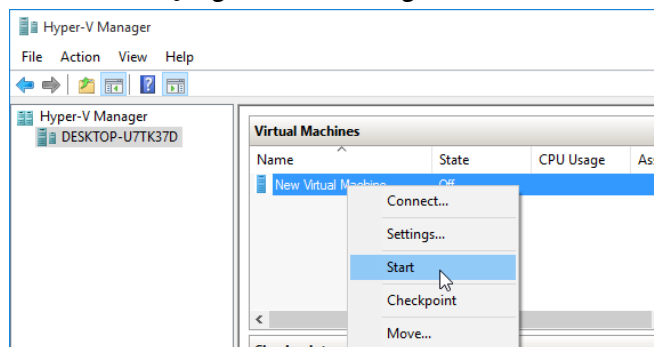
شکل 14-9

4. در این مرحله گزینه Image file را انتخاب کنید و بر روی Browse کلیک کنید و یک Image ویندوز انتخاب کنید.



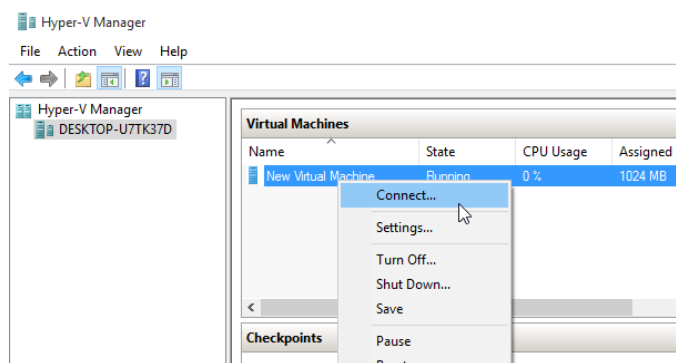
شکل 9-15

5. پس از انجام مرحله قبل در این قسمت بر روی ماشین مجازی که تازه ساخته‌اید کلیک راست کرده و بر روی Start کلیک کنید تا ماشین مجازی شما روشن شود.



شکل 9-16

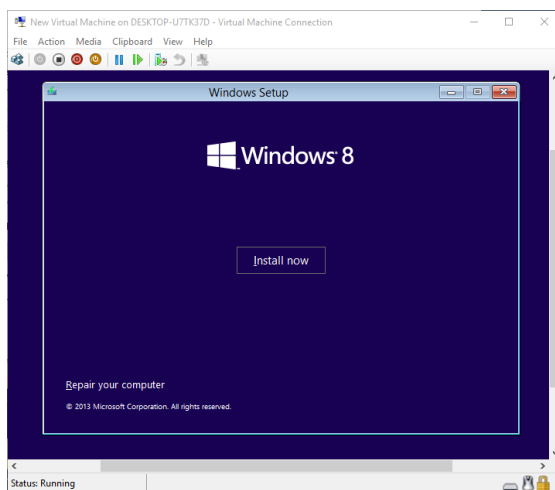
6. مجدداً راست کلیک کنید و این بار گزینه Connect را انتخاب کنید تا مانیتور ماشین مجازی خود را مشاهده کنید.



شکل 9-17



6. در این مرحله نصب ویندوز شروع خواهد شد. (در صورتی که عملیات نصب شروع نشده، از منوی Action بر روی Ctrl + Alt + Delete کلیک کنید این کار باعث می شود که سیستم راه اندازی مجدد شود)

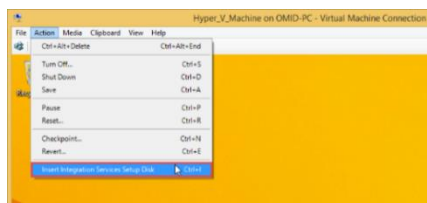


شکل 18-9

### نصب سرویس‌های تجمعی (Integration Services)

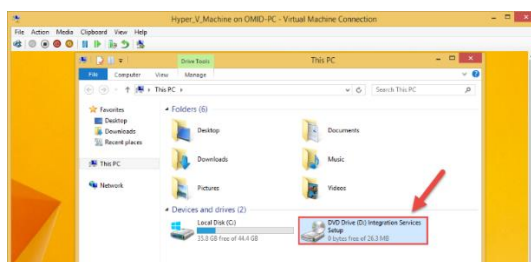
در صورتی که پس از نصب ماشین مجازی این سرویس‌ها را نصب کنید باعث می شود تا بتوانید عملکرد بهتری مابین ماشین مجازی خود و سیستم اصلی داشته باشید. برای نصب سرویس‌های تجمعی در ماشین مجازی پس از این که ماشین مجازی خود را روشن کردید بر روی ماشین مجازی راست کلیک کرده و Connect را انتخاب کنید و بعد مراحل زیر را دنبال کنید.

1. روی منوی Action کلیک کنید و گزینه Insert Integration Services Setup Disk را انتخاب کنید.



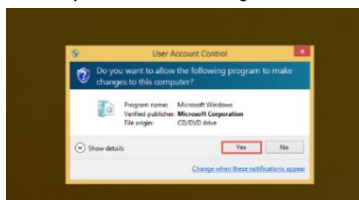
شکل 19-9

2. به File Explorer بروید و بر روی آیکون CD/Dvd ظاهر شده، کلیک کرده تا وارد مراحل نصب شوید.



شکل 9-20

3. از پنجره‌ی User Account Control گزینه Yes را انتخاب کنید.



شکل 9-21

4. اگر یک اعلان با متن *This Computer Is Already Running The Current Version Of* Integration Services اعلام شد بر روی دکمه Ok کلیک کنید .

### ساخت و مدیریت Checkpoints

Checkpointها برای ذخیره کردن حالت فعلی یک ماشین مجازی استفاده می شوند . یعنی در هر زمانی که نیاز باشد، می توان وضعیت ماشین مجازی را به زمانی که Checkpoint گرفته شده تغییر داد. همچنین checkpoint ها قابل جابه جا شدن هستند و معمولاً حجم زیادی دارند.