

Microsoft

Exam 70-687

Configuring Windows 8.1

Version: 12.0

[Total Questions: 266]

Topic 1, Volume A**Question No : 1 - (Topic 1)**

A company has 100 client computers that run Windows 8.1.

You need to assign static IPv6 addresses to the client computers.

Which Windows Powershellcmdlet should you run?

- A. Set-NetTCPSetting
- B. Set-NetIPInterface
- C. Set-NetIPv6Protocol
- D. set-NetIPAddress

Answer: D

Explanation:

<http://technet.microsoft.com/en-us/library/hh826151.aspx>

Set-NetIPAddress

The Set-NetIPAddress cmdlet modifies IP address configuration properties of an existing IP address.

To create an IPv4 address or IPv6 address, use the New-NetIPAddress cmdlet.

Question No : 2 - (Topic 1)

A company has an Active Directory Domain Services (AD DS) domain. All client computers run Windows 8.1.

Portable client computers no longer connect to the corporate wireless network.

You need to ensure that when the corporate wireless network is available, the computers always connect to it automatically.

Which two actions would achieve the goal? (Each correct answer presents a complete solution. Choose two.)

- A. Create a Group Policy object (GPO) to configure a wireless network policy. Link the GPO to the organizational unit that contains the computers.
- B. Configure the corporate wireless network as an unmetered network.
- C. Configure the corporate wireless network as a preferred network.
- D. Manually connect to the corporate wireless network and select the option to connect automatically to that network.

Answer: C,D

Explanation: Answer:

Configure the corporate wireless network as a preferred network.

Manually connect to the corporate wireless network and select the option to connect automatically to that network.

<http://blogs.technet.com/b/canitpro/archive/2014/03/05/windows-8-1-tips-manage-wireless-network-profiles.aspx>

Windows 8.1 tips: Managing Wireless Network Profiles

And finally, if you wanted to change the preferred order for your machine to connect to specific wireless network, you could move a network up in the priority list by using the command: `set profileorder name=goose interface="Wi-Fi" priority=1`

```
netsh wlan>set profileorder name=goose interface="Wi-Fi" priority=1
Priority order of profile "goose" is updated successfully.
```

<http://www.eightforums.com/tutorials/20152-wireless-networks-priority-change-windows-8-a.html>

How to Change Connection Priority of Wireless Networks in Windows 8 and 8.1

Windows usually connects to networks in this priority order:

- ✍ Ethernet
- ✍ WiFi (wireless)
- ✍ Mobile broadband

When you connect to a new WiFi network, it's added to the list, and Windows will connect to that network while it's in range. If you connect to another WiFi network while in range of the first network, Windows will prefer the second network over the first one.

Mobile broadband networks are treated differently. If you manually connect to a mobile

broadband network when there is a WiFi network in range, the mobile broadband network is preferred just for that session. The next time you're in range of both networks, the WiFi network is preferred. This is because mobile broadband networks typically are metered.

If you want to force your PC to prefer a mobile broadband network over WiFi, tap or click the WiFi network in the list of networks, and then click Disconnect. Windows won't automatically connect to that WiFi network.

Question No : 3 - (Topic 1)

A company has client computers that run Windows 8.1. The corporate network is configured for IPv4 and IPv6.

You need to disable Media Sensing for IPv6 on the client computers without affecting IPv4 communications.

What should you do on each client computer?

- A. Run the Disable-NetAdapterBinding Windows PowerShell cmdlet.
- B. Run the Disable-NetAdapter Windows PowerShell cmdlet.
- C. Run the Set-NetIPv6Protocol Windows PowerShell cmdlet.
- D. Run the Set-NetIPv4Protocol Windows PowerShell cmdlet.

Answer: C

Explanation: <http://technet.microsoft.com/en-us/library/hh826144.aspx>
Set-NetIPv6Protocol

Set-NetIPv6Protocol -DhcpMediaSense<DhcpMediaSense>

Specifies a value for Media Sense. The cmdlet modifies the value for this setting.

Media Sense provides a mechanism for the network adapter to notify the protocol stack of media connect and disconnect events. These events trigger the DHCP client to take an action, such as attempting to renew a DHCP lease or removing routes that are related to a disconnected network. When Media Sense is enabled, the network parameters on the laptop of a roaming user are automatically and transparently updated without requiring a restart when the user moves from one location to another. The acceptable values for this parameter are:

- Enabled
- Disabled

The default value is Enabled.

Further information:

Disable-NetAdapterBinding

The Disable-NetAdapterBinding cmdlet disables a binding to a network adapter. Running this cmdlet causes loss of network connectivity depending on the binding that is disabled.

Note: Disabling some adapter bindings can automatically enable other network adapter bindings.

Disable-NetAdapter

The Disable-NetAdapter cmdlet disables a network adapter. A network adapter must be enabled to connect to a network. This cmdlet causes loss of network connectivity of the specified network adapter. Note: Do not disable the network adapter being used to manage a remote computer. By default the user will be prompted to confirm the network adapter should be disabled

Set-NetIPv4Protocol



Is not a valid cmdlet.

Question No : 4 DRAG DROP - (Topic 1)

A company has an Active Directory Domain Services (AD DS) domain. All client computers run Windows 8.1. Two computers named COMPUTER1 and COMPUTER2 are connected to one network switch and joined to the domain. Windows Firewall is turned off on both computers.

You are planning a remote management solution.

You have the following requirements:

-  Ensure that COMPUTER2 can run remote commands on COMPUTER1.
-  Test the solution by successfully running a command from COMPUTER2 that

executes on COMPUTER1.

You need to select the commands to run on COMPUTER1 and COMPUTER2 to meet the remote management requirements.

Which commands should you run? (To answer, drag the appropriate command or commands to the correct location or locations in the answer area. Commands may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.)

Click here to enter text.

wecutil -s COMPUTER1 ipconfig

wininit /s COMPUTER1 ipconfig

winrm quickconfig

winrs quickconfig

winrs -r:COMPUTER1 ipconfig

On this computer	Run this command
COMPUTER1	
COMPUTER2	

Answer:

Click here to enter text.

wecutil -s COMPUTER1 ipconfig

wininit /s COMPUTER1 ipconfig

winrm quickconfig

winrs quickconfig

winrs -r:COMPUTER1 ipconfig

On this computer	Run this command
COMPUTER1	winrm quickconfig
COMPUTER2	winrs -r:COMPUTER1 ipconfig

Question No : 5 - (Topic 1)

A company has 100 client computers that run Windows 8.1. The client computers are members of a workgroup.

A custom application requires a Windows Firewall exception on each client computer.

You need to configure the exception on the client computers without affecting existing firewall settings.

Which Windows PowerShell cmdlet should you run on each client computer?

- A. New-NetFirewallRule
- B. Set-NetFirewallSetting
- C. Set-NetFirewallRule
- D. Set-NetFirewallProfile
- E. New-NetIPSecMainModeRule

Answer: A

Explanation:

<http://technet.microsoft.com/en-us/library/jj554908.aspx>

New-NetFirewallRule

The New-NetFirewallRule cmdlet creates an inbound or outbound firewall rule and adds the rule to the target computer.

Further information:

Set-NetFirewallSetting

The Set-NetFirewallSetting cmdlet configures properties that apply to the firewall and IPsec settings, regardless of which network profile is currently in use. This cmdlet allows the administrator to specify global firewall behavior.

Set-NetFirewallRule

The Set-NetFirewallRule cmdlet modifies existing firewall rule properties.

Set-NetFirewallProfile

The Set-NetFirewallProfile cmdlet configures options for the profiles, including domain, public, and private, that are global, or associated with the input rules.

New-NetIPSecMainModeRule

The New-NetIPsecMainModeRule cmdlet creates an IPsec main mode rule.

A main mode rule contains a set of local and remote end points to determine the peers to which it applies. When an application on the local computer attempts to communicate with one of these specified remote hosts, the computer attempts to establish a security association (SA) with the remote server.

Question No : 6 - (Topic 1)

A company has an Active Directory Domain Services (AD DS) domain. All client computers run Windows 8.1. Portable client computers connect to the corporate wireless network.

You have the following requirements:

- ✍ Prevent users from configuring a wireless network by using settings from a USB flash drive.
- ✍ Do not affect the use of other USB devices.

You need to create a Group Policy object (GPO) to meet the requirements.

Which GPO should you create?

- A.** A GPO that disables the Allow only USB root hub connected Enhanced Storage Features policy setting.
- B.** A GPO that enables wireless policy processing.
- C.** A GPO that prohibits connections to mobile broadband networks when roaming.
- D.** A GPO that configures Windows Connect Now settings.

Answer: D

Explanation:

<http://windows.microsoft.com/en-US/windows-vista/What-is-Windows-Connect-Now>
Computer Configuration\Policies\Administrative Templates\Network\Windows Connect Now Turn Off Ability To Configure Using A USB Flash Drive setting:

Prevents Windows from being able to store a Windows Connect Now configuration to a UFD. Because the Windows Connect Now information stored on a UFD contains information that can allow computers to access your protected wireless network, you might choose to disable this setting to improve the security of your wireless networks.

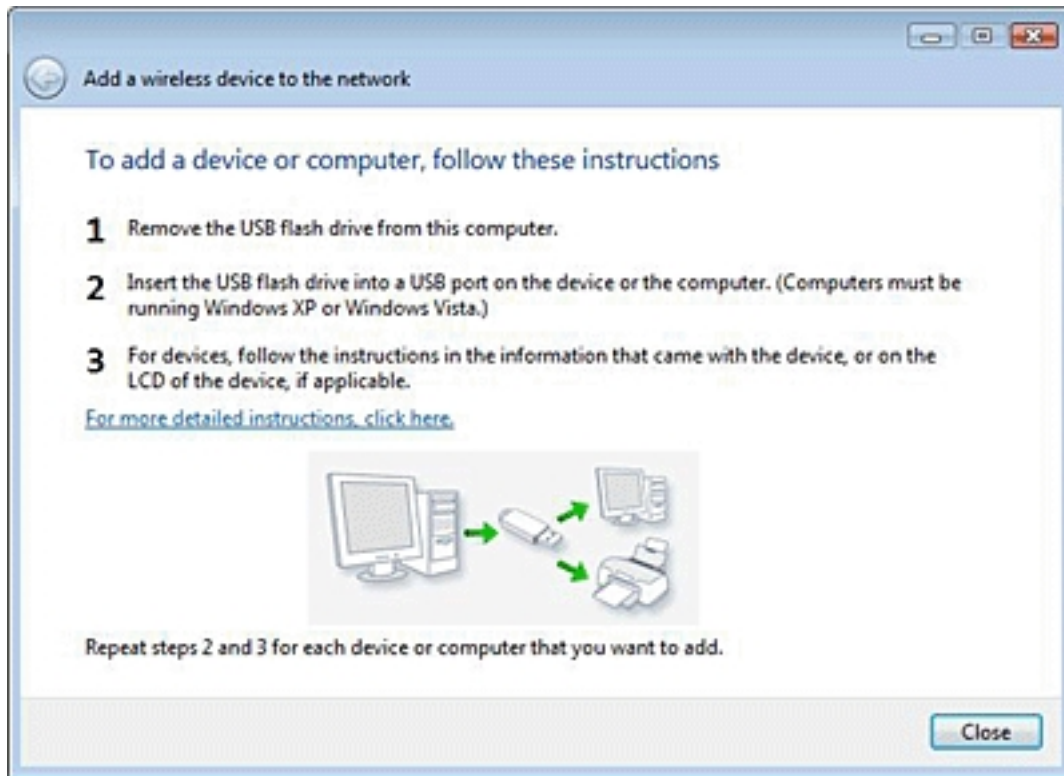
<http://sourcedaddy.com/windows-7/windows-connect-now-in-windows-7.html>

<http://windows.microsoft.com/en-US/windows-vista/What-is-Windows-Connect-Now>
What is Windows Connect Now?

Microsoft Windows Connect Now (WCN) is a technology designed to address the need for a simple and more secure way to configure network devices and computers. In addition to easier device configuration, you can use WCN to save wireless network settings to a USB flash drive and then plug that drive into devices (such as routers) and computers so you can quickly and easily add them to a network.

http://support.epson.ru/products/manuals/101846/html_z/setpn_4.htm

Using WCN (Windows Connect Now)



Question No : 7 - (Topic 1)

A company has client computers that run Windows 8.1.

The client computers are connected to a corporate private network.

Users are currently unable to connect from their home computers to their work computers by using Remote Desktop.

You need to ensure that users can remotely connect to their office computers by using Remote Desktop. Users must not be able to access any other corporate network resource from their home computers.

Which setting should you configure on the home computers?

- A. Virtual Private Network connection
- B. Remote Desktop local resources
- C. DirectAccess connection
- D. Remote Desktop Gateway IP address

Answer: A

Explanation:

DirectAccess is for Windows Server 2008/2012/Win 7 Ultimate/Enterprise/Win 8 Enterprise only RD Gateway setup is only for servers

Create VPN through manage networks. File --> Allow incoming connections. Connect through internet and create VPN which will allow one computer at a time to view the hosts resources, and only the hosts resources unlike standard VPNs.

Question No : 8 - (Topic 1)

A company has an Active Directory Domain Services (AD DS) domain. All client computers run Windows 8.1. Client computers use Windows BitLocker Drive Encryption with a Trusted Platform Module (TPM) chip.

You need to create a Group Policy object (GPO) that will secure the TPM owner information.

Which policy setting should you configure?

- A. Enable the Turn on TPM backup to Active Directory Domain Services policy setting.
- B. Enable the Configure the level of TPM usage authorization information available to the registry policy setting.
- C. Set the Configure the level of TPM owner authorization information available to operating system policy setting to Full.
- D. Enable the Configure TPM platform validation profile policy setting.

Answer: A

Explanation:

<http://technet.microsoft.com/en-us/library/jj679889.aspx>

Trusted Platform Module Services Group Policy Settings

If you enable this policy setting, TPM owner information will be automatically and silently backed up to AD DS when you use Windows to set or change a TPM owner password.