# PXE BOOT AND SYSTEM CENTER 2012 CONFIGURATION MANAGER

Luke Ramsdale

SUPPORT ESCALATION ENGINEER, MICROSOFT CORPORATION

# CONTENTS

## INTRODUCTION TO PXE BOOT AND CONFIGURATION MANAGER

PXE boot in System Center 2012 Configuration Manager (ConfigMgr 2012) enables administrators to easily access the Windows Preinstallation Environment (WinPE) across the network via the Preboot Execution Environment (PXE). PXE is an industry standard created by Intel that provides pre boot services within the devices firmware which enables devices to download network boot programs to client computers.

System Center 2012 Configuration Manger relies on the Windows server role Windows Deployment Services (WDS) via the WDS PXE provider. In Configuration Manager 2012 the SMS PXE provider (SMSPXE) registers with the WDS service and supplies the logic for the PXE client requests.

PXE boot issues are one of the biggest call generators for the Configuration Manager Global Business Support (GBS) team which is in part due to the reliance on and interdependencies with networking protocols such as DHCP and TFTP.

This article is an update of this article which contains detailed descriptions of PXE issues that occur in Configuration Manger 2007. It also attempts to provide some deeper insights into the PXE booting process.

Note that there is also a wizard driven Guided Walkthrough available that uses much of the same information to walk you through troubleshooting some of the more common PXE related issues in the following Microsoft Knowledge Base article:

3012951 - *GUIDED WALKTHROUGH FOR TROUBLESHOOTING PXE BOOT ISSUES IN SYSTEM CENTER 2012 CONFIGURATION MANAGER* (http://support.microsoft.com/kb/3012951)

## KB ARTICLES

Before beginning any troubleshooting on the PXE Service Point, review the following KB articles to see if any of the issues described in the following KB articles could be causing problems (this is not an exhaustive list):

**Cumulative Update 2 for System Center 2012 R2 Configuration Manager**
http://support.microsoft.com/kb/2970177

**Cumulative Update 4 for System Center 2012 Configuration Manager Service Pack 1**
http://support.microsoft.com/kb/2922875

**Windows 7 client deployment over IPv6 PXE network boot does not work.**
http://support.microsoft.com/kb/2803741

**WDS does not start on a PXE enabled remote Distribution Point in System Center 2012 Configuration Manager**
http://support.microsoft.com/kb/2712387

**The Windows Deployment Service cannot be started on a computer that has more than 20 logical processors and that is running Windows Server 2008 R2 or Windows Server 2008**
http://support.microsoft.com/kb/2121690

**The DNS Server service binds to all ports in the Windows Deployment Services port range on a server that is running Windows Server 2008 R2 or Windows Server 2008**
http://support.microsoft.com/kb/977512

**Error message when Windows Deployment Service clients cannot obtain the boot image from a Windows Server 2008 R2-based WDS server: "PXE-E78: Could not locate boot server"**
http://support.microsoft.com/kb/979720

**Boot program fails when you try to install Windows by using a WDS server that is running Windows Server 2008 R2**
http://support.microsoft.com/kb/2649909

**The WDS server may not start, and an error is logged in the System log when you start the WDS server**
http://support.microsoft.com/kb/954410

**You cannot start a UEFI-based computer by using a Windows Server 2008 R2-based server that has WDS deployed**
http://support.microsoft.com/kb/2757588

**"Timeout occurred" error message when you try to download a file from a Windows Server 2008 R2-based Windows Deployment Services server by using the TFTP protocol**
http://support.microsoft.com/kb/2517669

**Error message when Windows Deployment Service clients cannot obtain the boot image from a Windows Server 2008 R2-based WDS server: "PXE-E78: Could not locate boot server"**
http://support.microsoft.com/kb/979720

**Operating system deployment over a network using WDS fails in Windows Server 2008 and in Windows Server 2008 R2**
http://support.microsoft.com/kb/975710

## UEFI SUPPORT IN WDS

In order to make full use of WDS and UEFI ensure you install the PXE enabled DP on a Windows Server 2012 site system so that IA32 is supported.

Support for x64 UEFI boot does exist in WDS when installed on Windows server 2008, more information can be found here.

## SETTING UP IP HELPERS

If the DHCP server, the client PC, and the ConfigMgr 2012 server running Windows Deployment Services (WDS) and the PXE enabled DP are all on the same subnet or VLANs then IP helpers are not a requirement.

Otherwise, if either the DHCP server, the client PC, or the ConfigMgr 2012 server running WDS and the PXE enabled DP are on separate subnets or VLANs, which is usually the case in most environments, the first step to take before trying to install and configure the PXE Service Point and WDS is to set up IP Helpers on the routers. This process varies and is dependent on the router hardware manufacturer but the general overview is outlined at the below TechNet article:

Configuring Your Router to Forward Broadcasts

http://technet.microsoft.com/en-us/library/cc732351(WS.10).aspx#Updating

For further information on how to properly configure IP Helpers on the routers, please contact the hardware manufacturer of the router.

IP Helpers are necessary because the PXE request generated by the client PC is a broadcast that does not travel outside of the local subnet or VLANs. It only stays within the local subnet or VLANs. If the DHCP server and/or the WDS/PXE enabled DP are not on the same subnet or VLANs as the client PC, they will not see or hear the PXE request broadcast from the client PC. The servers will therefore not respond to the PXE request. To have the PXE request broadcast traverse between subnets or VLANs, the PXE request broadcast needs to be forwarded by the router to DHCP and WDS/PXE Service Point servers so that they can properly respond to the client PC's PXE request.

An alternative to using IP Helpers is setting DHCP Options on the DHCP server, specifically DHCP Options 60 (PXE Client), 66 (Boot Server Host Name), and 67 (Boot file Name). However, DHCP Options can be problematic and may not work reliably or consistently. Furthermore the use of DHCP Options to control PXE requests in Configuration Manager 2012 is not supported by Microsoft. Therefore the recommended and supported method of PXE booting client PCs that are on a different subnet than the DHCP or WDS/PXE Service Point servers is the use of IP Helpers.

For additional information regarding DHCP Options not being recommended or supported please see the below articles:

Using DHCP Options 60, 66, and 67

http://technet.microsoft.com/en-us/library/cc732351(WS.10).aspx#Using

PXE client computers do not start when you configure the Dynamic Host Configuration Protocol server to use options 60, 66, 67

http://support.microsoft.com/kb/259670

The only exception where a DHCP Option needs to be used is when DHCP and WDS reside on the same server. In this instance, DHCP Option 60, and only DHCP Option 60, needs to be set. DHCP Options 66 and 67 should still NOT be set in this scenario. For more information, please see the below section "Co-hosting DHCP and WDS on the Same Server".

It is IMPERATIVE that before continuing that it has been verified that the routers have IP Helpers configured AND that the DHCP server does NOT have DHCP Options 60, 66, or 67 configured. Not meeting both of these criteria will cause the PXE Service Point not to work correctly. When checking DHCP options, make sure to check options at both the server and scope levels.

In certain instances, configuring DHCP Options 60, 66, and 67 may make it appear that the PXE boot process is proceeding further along than before these options were configured, but in most cases it proceeds further down an incorrect path and ends up failing.

## CO-HOSTING DHCP AND WDS ON THE SAME SERVER

One consideration when setting up a ConfigMgr PXE enabled DP is if WDS and DHCP are going to reside on the same or different servers. Best practice is to host the WDS and DHCP services on two separate servers, but there should be no issues in hosting both services on one server.

However when WDS and DHCP are co-hosted on the same server, WDS needs a special configuration to listen on a specific port. This configuration is outlined in the following TechNet article under the section Windows Deployment Services (WDS) and DHCP --> PXE Service Point Configuration Item --> DHCP considerations.

Planning for PXE Initiated Operating System Deployments

http://technet.microsoft.com/en-us/library/hh397405.aspx

According to the above article, the following two actions need to take place when WDS and DHCP are co-hosted on the same server:

1. The value UseDHCPPorts needs to be set to 0 on the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WDSServer\Providers\WDSPXE

2. The WDS command:

WDSUTIL /Set-Server /UseDHCPPorts:No /DHCPOption60:Yes

The one problem with the above recommendations is that in order to run the WDSUTIL command, WDS has to be first configured. This goes against the best practice of NOT configuring WDS when installing a ConfigMgr PXE enabled DP. However, the two options being specified via the WDSUTIL command, UseDHCPPorts and DHCPOption60, can be configured using alternate methods that do not require the WDSUTIL command, and therefore do not require WDS to be configured:

1. The UseDHCPPorts WDSUTIL switch is actually the equivalent of setting the registry key value:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WDSServer\Providers\WDSPXE!UseDHCPPorts

to 0 as described in #1 above.

Therefore using the UseDHCPPorts WDSUTIL switch is duplicated and not needed as long as the registry key has been manually set as described in the above above TechNet article. Please note that if WDS has not been installed, this registry key may not be present and therefore cannot be set until after WDS has been installed.

2. The WDSUTIL DHCPOption60 switch is actually a setting that sets an option on the DHCP service, not the WDS service. Therefore instead of using WDSUTIL to set a DHCP option, an equivalent DHCP command can be used to set the same option. This approach allows the required DHCP setting to be set without configuring WDS and before WDS is even installed. This approach can be achieved via the netsh command as described in the following MSDN article:

Configuring DHCP for Remote Boot Services

http://msdn.microsoft.com/en-us/library/dd128762(WinEmbedded.51).aspx

To summarize and shorten the netsh commands described in the above article, close any DHCP consoles that are open and then run following two commands from an elevated command prompt:

netsh dhcp server \\<DHCP_server_machine_name> add optiondef 60 PXEClient String 0 comment=PXE support

netsh dhcp server \\<DHCP_server_machine_name> set optionvalue 60 STRING PXEClient

where <DHCP_server_machine_name> is the name of the DHCP/WDS server (without the brackets <>).

The above two commands set up and enable DHCP Option 60 on a DHCP server. Normally DHCP Option 60 is not set up by default on a DHCP server. The first command sets up DHCP Option 60 but does not actually enable it. The second command actually enables DHCP Option 60.

If after running the above two commands an option named "Unknown" is displayed in the DHCP console instead of "060 PXE Client", reboot the server. After the reboot the option should display correctly. This usually happens if a DHCP console was open when the above two commands were run.

If DHCP is ever moved to another server and removed from the server hosting WDS, the above actions need to be reversed. To reverse the above actions take the following two actions on the WDS server:

Set the value of the following registry key value:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WDSServer\Providers\WDSPXE!UseDHCPPorts

This can be done by running the following command from an elevated command prompt:

REG ADD "HKLM\SYSTEM\CurrentControlSet\services\WDSServer\Providers\WDSPXE" /v UseDHCPPorts /t REG_DWORD /d 1 /f

2.From an elevated command prompt, run the following two commands to remove DHCP Option 60:

netsh dhcp server \\<DHCP_server_machine_name> delete optionvalue 60

netsh dhcp server \\<DHCP_server_machine_name> delete optiondef 60 PXEClient

where <DHCP_server_machine_name> is the name of the DHCP/WDS server (without the brackets <>).

In the above two commands, the first command disables DHCP Option 60, while the second one removes DHCP Option 60 completely. For this reason only the first command is truly needed. However if DHCP Option 60 needs to be removed completely, make sure to run BOTH commands in the above order. Only running the second command will leave an option named "Unknown" on the DHCP server.

## INSTALLATION & CONFIGURATION

### PREREQUISITES & REQUIREMENTS FOR A PXE ENABLED DP

For more information on supported configurations please refer to:
http://technet.microsoft.com/en-us/library/gg682077.aspx

- An existing distribution point installed on a supported site system.
- Windows Deployment Services (WDS)

For Windows Server 2008, Windows Server 2008 R2 and Windows server 2012 WDS is installed and configured automatically when you configure a distribution point to support PXE or Multicast.

For Windows Server 2003, you must install WDS manually via the Add Remove Windows Components in the Add/Remove Control Panel. Do not manually configure WDS.

- A functioning DHCP server.
- If the client machine is located on a different subnet/VLAN to the PXE enabled DP then you will need to enable IP helpers on the switch or router separating these network segments (please refer to the setting up IP helpers section above).

### INSTALLATION & CONFIGURATION

How to install a Site System Role in Configuration Manager:
http://technet.microsoft.com/en-us/library/5c669a3c-404f-4a5d-88f0-bc40443ebaae#BKMK_HowtoInstallSiteSystems

How to Deploy Operating Systems by Using PXE in Configuration Manager
http://technet.microsoft.com/en-us/library/gg712266.aspx#BKMK_CreatePXEDistributionPoint

## HOW IT WORKS

We will now look at the processes involved in the installation of the SMSPXE provider. In all instances in this document we are using System Center 2012 Configuration Manager R2 CU2 and a remote site system installed on Windows Server 2012 with the DP role installed.

### PXE SERVICE POINT INSTALLATION

Installation is initiated by ticking the “Enable PXE support for clients” on the PXE tab of the distribution point properties. When the PXE support is enabled, an instance of SMS_SCI_SysResUse class is created.

**SMSProv.log:**

| | | | |
|---|---|---|---|
| PutInstanceAsync SMS_SCI_SysResUse | SMS Provider | 04/09/2014 11:30:13 | 1552 (0x0610) |
| CExtProviderClassObject::DoPutInstanceInstance | SMS Provider | 04/09/2014 11:30:13 | 1552 (0x0610) |
| INFO: 'RemoteDp.sc.local' is a valid FQDN. | SMS Provider | 04/09/2014 11:30:13 | 1552 (0x0610) |

**TIP:**

In the WMI namespace Root\SMS\Site_RR2 (where RR2 is the site code of the site) the SMS_SCI_SYSResUSe class contains all the site systems roles on the primary site server. You can run the following query in WBEMTEST to identify all the DPs on that site server:

SELECT * FROM SMS_SCI_SysResUse WHERE rolename like 'SMS Distribution Point'

Changing the properties of these roles via the SDK will alter the site control file and configure the DP. The ISPXE property name is a member of the props property and is set to 1 when the DP is PXE enabled.

The SMS database monitor component detects the change to the DPNotificaiton and DistributionPoints table and drops files in the distmgr.box:

**Smsdbmon.log:**

```
RCV: UPDATE on SiteControl for SiteControl_AddUpd_HMAN [RR2  ][19604]
RCV: UPDATE on SiteControl for SiteControl_AddUpd_SiteCtrl [RR2  ][19605]
SND: Dropped C:\Program Files\Microsoft Configuration Manager\inboxes\hman.box\RR2.SCU  [19604]
SND: Dropped C:\Program Files\Microsoft Configuration Manager\inboxes\sitectrl.box\RR2.CT0  [19605]
RCV: UPDATE on Sites for Sites_Interop_Update_HMAN [RR2  ][19606]
SND: Dropped C:\Program Files\Microsoft Configuration Manager\inboxes\hman.box\RR2.ITC  [19606]
RCV: UPDATE on DistributionPoints for DP_Properties_Upd [15  ][19607]
RCV: INSERT on PkgNotification for PkgNotify_Add [RR200002  ][19608]
RCV: INSERT on PkgNotification for PkgNotify_Add [RR200003  ][19609]
RCV: INSERT on DPNotification for DPNotify_ADD [15  ][19610]
RCV: UPDATE on SiteControlNotification for SiteCtrlNot_Add_DDM [RR2  ][19611]
SND: Dropped C:\Program Files\Microsoft Configuration Manager\inboxes\distmgr.box\15.NOT  [19607]
SND: Dropped C:\Program Files\Microsoft Configuration Manager\inboxes\distmgr.box\RR200002.PKN  [19608]
SND: Dropped C:\Program Files\Microsoft Configuration Manager\inboxes\distmgr.box\RR200003.PKN  [19609]
SND: Dropped C:\Program Files\Microsoft Configuration Manager\inboxes\distmgr.box\15.DPN  [19610]
Site Control Notification.
```

The distribution manager component on the primary site server then initiates the configuration of the remote DP:

**Distmgr.log:**

| | | | |
|---|---|---|---|
| ConfigureDP | SMS_DISTRIBUTION_MANAGER | 04/09/2014 11:30:26 | 3776 (0x0EC0) |
| IISPortsList in the SCF is "80". | SMS_DISTRIBUTION_MANAGER | 04/09/2014 11:30:26 | 3776 (0x0EC0) |
| IISSSLPortsList in the SCF is "443". | SMS_DISTRIBUTION_MANAGER | 04/09/2014 11:30:26 | 3776 (0x0EC0) |
| IISWebSiteName in the SCF is "". | SMS_DISTRIBUTION_MANAGER | 04/09/2014 11:30:26 | 3776 (0x0EC0) |
| IISSSLState in the SCF is 448. | SMS_DISTRIBUTION_MANAGER | 04/09/2014 11:30:26 | 3776 (0x0EC0) |
| DP registry settings have been successfully updated on RemoteDp.sc.local | | | |
| | SMS_DISTRIBUTION_MANAGER | 04/09/2014 11:30:26 | 3776 (0x0EC0) |
| ConfigurePXE | SMS_DISTRIBUTION_MANAGER | 04/09/2014 11:30:26 | 3776 (0x0EC0) |

In the SMS DP provider log on the remote DP we can see the following information about the PXE install, initially the PxeInstalled reg key is not found:

**Smsdpprov.log**

[66C][Thu 09/04/2014 11:30:28]:CcmInstallPXE
[66C][Thu 09/04/2014 11:30:28]:RegQueryValueExW failed for Software\Microsoft\SMS\DP, PxeInstalled
[66C][Thu 09/04/2014 11:30:28]:RegReadDWord failed; 0x80070002

The Visual C++ redistributable is installed:

**Smsdpprov.log**

[66C][Thu 09/04/2014 11:30:28]:Running: C:\SMS_DP$\sms\bin\vcredist_x64.exe /q /log "C:\SMS_DP$\sms\bin\vcredist.log"
[66C][Thu 09/04/2014 11:30:28]:Waiting for the completion of: C:\SMS_DP$\sms\bin\vcredist_x64.exe /q /log "C:\SMS_DP$\sms\bin\vcredist.log"
[66C][Thu 09/04/2014 11:30:39]:Run completed for: C:\SMS_DP$\sms\bin\vcredist_x64.exe /q /log "C:\SMS_DP$\sms\bin\vcredist.log"

WDS is installed:

**Smsdpprov.log**

[66C][Thu 09/04/2014 11:30:39]:Created the DP mutex key for WDS.
[66C][Thu 09/04/2014 11:30:39]:Failed to open WDS service.
[66C][Thu 09/04/2014 11:30:39]:WDS is NOT INSTALLED
[66C][Thu 09/04/2014 11:30:39]:Installing WDS.
[66C][Thu 09/04/2014 11:30:39]:Running: ServerManagerCmd.exe -i WDS -a
[66C][Thu 09/04/2014 11:30:39]:Failed (2) to run: ServerManagerCmd.exe -i WDS -a
[66C][Thu 09/04/2014 11:30:39]:Running: PowerShell.exe -Command Import-Module ServerManager; Get-WindowsFeature WDS; Add-WindowsFeature WDS
[66C][Thu 09/04/2014 11:30:39]:Waiting for the completion of: PowerShell.exe -Command Import-Module ServerManager; Get-WindowsFeature WDS; Add-WindowsFeature WDS
[66C][Thu 09/04/2014 11:31:35]:Run completed for: PowerShell.exe -Command Import-Module ServerManager; Get-WindowsFeature WDS; Add-WindowsFeature WDS
[66C][Thu 09/04/2014 11:31:35]:Successfully installed WDS.

TFTP read filters are configured:

**Smsdpprov.log**

```
[66C][Thu 09/04/2014 11:31:35]:Setting TFTP config key as:
System\CurrentControlSet\Services\WDSSERVER\Providers\WDSTFTP
[66C][Thu 09/04/2014 11:31:35]:Configuring TFTP read filters
[66C][Thu 09/04/2014 11:31:35]:SetupComplete is set to 0
```

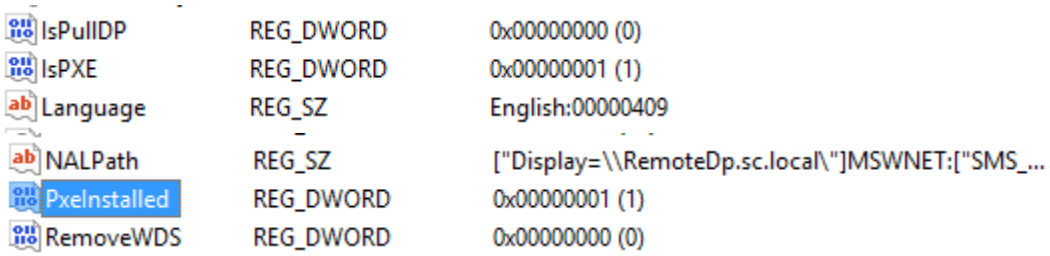
The REMINST share is created and WDS is configured:

**Smsdpprov.log**

```
[66C][Thu 09/04/2014 11:31:35]:RegQueryValueExW failed for Software\Microsoft\Windows\CurrentVersion\Setup, REMINST
[66C][Thu 09/04/2014 11:31:35]:RegReadDWord failed; 0x80070002
[66C][Thu 09/04/2014 11:31:35]:REMINST not set in WDS
[66C][Thu 09/04/2014 11:31:35]:WDS is NOT Configured
[66C][Thu 09/04/2014 11:31:35]:Share (REMINST) does not exist. (NetNameNotFound) (0x00000906)
[66C][Thu 09/04/2014 11:31:35]:GetFileSharePath failed; 0x80070906
[66C][Thu 09/04/2014 11:31:35]:REMINST share does not exist. Need to create it.
[66C][Thu 09/04/2014 11:31:35]:Enumerating drives A through Z for the NTFS drive with the most free space.

[66C][Thu 09/04/2014 11:31:37]:Drive 'C:\' is the best drive for the SMS installation directory.
[66C][Thu 09/04/2014 11:31:37]:Creating REMINST share to point to: C:\RemoteInstall
[66C][Thu 09/04/2014 11:31:37]:Succesfully created share REMINST
[66C][Thu 09/04/2014 11:31:37]:Removing existing PXE related directories
[66C][Thu 09/04/2014 11:31:37]:Registering WDS provider: SourceDir: C:\SMS_DP$\sms\bin
[66C][Thu 09/04/2014 11:31:37]:Registering WDS provider: ProviderPath: C:\SMS_DP$\sms\bin\smspxe.dll
[66C][Thu 09/04/2014 11:31:37]:DoPxeProviderRegister
[66C][Thu 09/04/2014 11:31:37]:PxeLoadWdsPxe
[66C][Thu 09/04/2014 11:31:37]:Loading wdspxe.dll from C:\Windows\system32\wdspxe.dll
[66C][Thu 09/04/2014 11:31:37]:wdspxe.dll is loaded
[66C][Thu 09/04/2014 11:31:37]:PxeProviderRegister has suceeded (0x00000000)
[66C][Thu 09/04/2014 11:31:37]:Disabling WDS/RIS functionality
[66C][Thu 09/04/2014 11:31:39]:WDSServer status is 1
[66C][Thu 09/04/2014 11:31:39]:WDSServer is NOT STARTED
[66C][Thu 09/04/2014 11:31:39]:Running: WDSUTIL.exe /Initialize-Server /REMINST:"C:\RemoteInstall"
[66C][Thu 09/04/2014 11:31:39]:Waiting for the completion of: WDSUTIL.exe /Initialize-Server /REMINST:"C:\RemoteInstall"
[66C][Thu 09/04/2014 11:31:50]:Run completed for: WDSUTIL.exe /Initialize-Server /REMINST:"C:\RemoteInstall"
[66C][Thu 09/04/2014 11:31:50]:CcmInstallPXE: Deleting the DP mutex key for WDS.
[66C][Thu 09/04/2014 11:31:50]:Installed PXE
[66C][Thu 09/04/2014 11:32:03]:CcmInstallPXE
[66C][Thu 09/04/2014 11:32:03]:PXE provider is already installed.
[66C][Thu 09/04/2014 11:32:03]:Installed PXE
```

On the remote DP we can now see the following added in HKLM\Software\Microsoft\SMS\DP:




PxeInstalled and IsPXE are set to 1.

If we look at the remote DP's file system there is a new log in C:\SMS_DP$\sms\logs:

SMSPXE.log

**SMSPXE.log**

Machine is running Windows Longhorn. (NTVersion=0X602, ServicePack=0)
Cannot read the registry value of MACIgnoreListFile (00000000)
MAC Ignore List Filename in registry is empty
Begin validation of Certificate [Thumbprint B64B9DAF9BFB76A99DC050C21E33B3489643D111] issued to 'e728f6ce-29a6-4ac3-974e-ba3dc855d9a4'
Completed validation of Certificate [Thumbprint B64B9DAF9BFB76A99DC050C21E33B3489643D111] issued to 'e728f6ce-29a6-4ac3-974e-ba3dc855d9a4'

The distribution point should now be PXE enabled and ready to accept incoming requests.

## ADDING BOOT IMAGES TO PXE ENABLED DP

When a new PXE enabled DP has been configured there are a couple of additional steps to complete. You must distribute the x86 and x64 boot image to the newly PXE enabled DP.

To do this navigate to Software Library > Operating Systems > Boot Images > Boot Image (x86) > right click and select distribute content > Add the Boot Image to the PXE enabled DP.

Repeat this process for the Boot Image (x64).

Once this has been completed distribution manager will start processing the request and initiate the distribution to the remote DP:

**DistMgr.log**

Found notification for package 'RR200004'
Used 0 out of 30 allowed processing threads.
Starting package processing thread, thread ID = 0x152C (5420)
Start adding package to server ["Display=\\RemoteDp.sc.local\"]MSWNET:["SMS_SITE=RR2"]\\RemoteDp.sc.local\...
Attempting to add or update a package on a distribution point.
Successfully made a network connection to \\RemoteDp.sc.local\ADMIN$.
CreateSignatureShare, connecting to DP
Signature share exists on distribution point path \\RemoteDp.sc.local\SMSSIG$
Share SMSPKGC$ exists on distribution point \\RemoteDp.sc.local\SMSPKGC$

Checking configuration of IIS virtual directories on DP
["Display=\\RemoteDp.sc.local\"]MSWNET:["SMS_SITE=RR2"]\\RemoteDp.sc.local\
Creating, reading or updating IIS registry key for a distribution point.
Virtual Directory SMS_DP_SMSSIG$ for the physical path C:\SMSSIG$ already exists.
Created package transfer job to send package RR200004 to distribution point
["Display=\\RemoteDp.sc.local\"]MSWNET:["SMS_SITE=RR2"]\\RemoteDp.sc.local\.
StoredPkgVersion (9) of package RR200004. StoredPkgVersion in database is 9.
SourceVersion (9) of package RR200004. SourceVersion in database is 9.

Package transfer manager (this DP is remote) then initiates the sending of the content:

**PkgXferMgr.log**

DeleteJobNotificationFiles deleted 1 *.PKN file(s) this cycle.
Found send request with ID: 105, Package: RR200004, Version:9, Priority: 2, Destination: REMOTEDP.SC.LOCAL, DPPriority: 200
Created sending thread (Thread ID = 0x1140)
Sending thread starting for Job: 105, package: RR200004, Version: 9, Priority: 2, server: REMOTEDP.SC.LOCAL, DPPriority: 200
Sending legacy content RR200004.9 for package RR200004
Finished sending SWD package RR200004 version 9 to distribution point REMOTEDP.SC.LOCAL
Sent status to the distribution manager for pkg RR200004, version 9, status 3 and distribution point
["Display=\\RemoteDp.sc.local\"]MSWNET:["SMS_SITE=RR2"]\\RemoteDp.sc.local\
StateTable::CState::Handle - (8210:1 2014-09-10 13:19:12.087+00:00) >> (8203:3 2013-11-26 15:43:48.108+00:00)
Successfully send state change notification 7F6041B0-3EE2-427F-AB72-B89610A6331C
Sending thread complete

SMS distribution point provider then deploys the WIM to the remote install directory:

**Smsdpprov.log**

[468][Wed 09/10/2014 14:09:59]:A DP usage gathering task has been registered successfully
[99C][Wed 09/10/2014 14:19:07]:Content 'RR200004.9' for package 'RR200004' has been added to content library successfully
[99C][Wed 09/10/2014 14:19:07]:Expanding
C:\SCCMContentLib\FileLib\E8A1\E8A136A1348B4CFE97334D0F65934845F2B4675D0B7D925AB830378F4ECF39B9 from
package RR200004
[99C][Wed 09/10/2014 14:19:07]:Finding Wimgapi.Dll
[99C][Wed 09/10/2014 14:19:07]:Found C:\Windows\system32\wimgapi.dll
[99C][Wed 09/10/2014 14:19:07]:Expanding RR200004 to C:\RemoteInstall\SMSImages

SMSPXE discovers the new image:

**SMSPXE.log**

Found new image RR200004
PXE::CBootImageManager::QueryWIMInfo
Loaded C:\Windows\system32\wimgapi.dll
Opening image file C:\RemoteInstall\SMSImages\RR200004\boot.RR200004.wim
Found Image file: C:\RemoteInstall\SMSImages\RR200004\boot.RR200004.wim
PackageID: RR200004
ProductName: Microsoft® Windows® Operating System
Architecture: 0
Description: Microsoft Windows PE (x86)
Version:
Creator:

```
SystemDir: WINDOWS
Closing image file C:\RemoteInstall\SMSImages\RR200004\boot.RR200004.wim
PXE::CBootImageManager::InstallBootFilesForImage
Temporary path to copy extract files from: C:\RemoteInstall\SMSTempBootFiles\RR200004.
```

**TIP:**

Ensure that these boot images have been configured to deploy from the PXE enabled DP. Right click the boot image > properties > Data Source > Check “Deploy this boot image from the PXE-enabled distribution point.”

## PXE BOOT PROCESS

The example boot process described here involves three machines, the DHCP server, the PXE enabled DP and the client (x64 BIOS) machine. All are located on the same subnet.

### AQUIRING TCP/IP PARAMETERS AND TFTP BOOT SERVER

Once a device is powered on and completes the POST it will begin the PXE boot process (usually prompted via the boot selection menu).

1. The first thing the PXE firmware will do is send a **DHCPDISCOVER** (a UDP packet) broadcast to get TCP/IP details and will include a list of parameter requests, here is an example network trace of a the parameter list from the DHCPDISCOVER packet:

```
⊞ Option: (53) DHCP Message Type (Discover)
⊟ Option: (55) Parameter Request List
    Length: 24
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (2) Time Offset
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (5) Name Server
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (11) Resource Location Server
    Parameter Request List Item: (12) Host Name
    Parameter Request List Item: (13) Boot File Size
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (16) Swap Server
    Parameter Request List Item: (17) Root Path
    Parameter Request List Item: (18) Extensions Path
    Parameter Request List Item: (43) Vendor-Specific Information
    Parameter Request List Item: (54) DHCP Server Identifier
    Parameter Request List Item: (60) Vendor class identifier
    Parameter Request List Item: (67) Bootfile name
    Parameter Request List Item: (128) DOCSIS full security server IP [TODO]
    Parameter Request List Item: (129) PXE - undefined (vendor specific)
    Parameter Request List Item: (130) PXE - undefined (vendor specific)
    Parameter Request List Item: (131) PXE - undefined (vendor specific)
    Parameter Request List Item: (132) PXE - undefined (vendor specific)
    Parameter Request List Item: (133) PXE - undefined (vendor specific)
    Parameter Request List Item: (134) PXE - undefined (vendor specific)
    Parameter Request List Item: (135) PXE - undefined (vendor specific)
```

The PXE client identifies the vendor and machine specific information in order to request the location and file name of the appropriate boot image file.

2. The DHCP server and the PXE enabled DP then sends a **DHCPOFFER** to the client containing all the relevant TCP/IP parameters.

   In this case the DHCP offer below doesn't contain the server name or boot file information because this is the offer from the DHCP server rather than the PXE enabled DP.

```
Dhcp: Reply, MsgType = OFFER, TransactionID = 0x5E3CD04C
    OpCode: Reply, 2(0x02)
    Hardwaretype: Ethernet
    HardwareAddressLength: 6 (0x6)
    HopCount: 0 (0x0)
    TransactionID: 1581043788 (0x5E3CD04C)
    Seconds: 0 (0x0)
  + Flags: 0 (0x0)
    ClientIP: 0.0.0.0
    YourIP: 10.238.0.3
    ServerIP: 10.238.0.14
    RelayAgentIP: 0.0.0.0
  + ClientHardwareAddress: 00-15-5D-3C-D0-4C
    ServerHostName:
    BootFileName:
    MagicCookie: 99.130.83.99
  + MessageType: OFFER - Type 53
  + SubnetMask: 255.255.0.0 - Type 1
  + RenewTimeValue: Subnet Mask: 4 day(s),0 hour(s) 0 minute(s) 0 second(s) - Type 58
  + RebindingTimeValue: Subnet Mask: 7 day(s),0 hour(s) 0 minute(s) 0 second(s) - Type 59
  + IPAddressLeaseTime: Subnet Mask: 8 day(s),0 hour(s) 0 minute(s) 0 second(s) - Type 51
  + ServerIdentifier: 10.238.0.14 - Type 54
  + Router: 10.238.0.29 - Type 3
  + DomainNameServer: 10.238.0.14 - Type 6
  + DomainName: SC.LOCAL - Type 15
  + End:
    Padding: Binary Large Object (3 Bytes)
```

3. The client then replies with a **DHCPREQUEST** once the client selects a DHCPOFFER. This contains the IP address from the offer that is selected.

4. The DHCP server responds to the DHCPREQUEST with a **DHCPACK** which contains the same details as the DHCPOFFER, the server host name and the boot file name are not provided here:

```
Bootstrap Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x5e3cd04c
    Seconds elapsed: 0
  + Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 10.238.0.3 (10.238.0.3)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 00:15:5d:3c:d0:4c (00:15:5d:3c:d0:4c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  + Option: (53) DHCP Message Type (ACK)
  + Option: (58) Renewal Time Value
  + Option: (59) Rebinding Time Value
  + Option: (51) IP Address Lease Time
  + Option: (54) DHCP Server Identifier
  + Option: (1) Subnet Mask
  + Option: (3) Router
  + Option: (6) Domain Name Server
  + Option: (15) Domain Name
  + Option: (255) End
    Padding
```

5. At this point we still don't have the boot file information, however now the client has an IP address, the PXE client sends a new DHCPREQUEST to the PXE enabled DP after also receiving a DHCPOFFER from the earlier DHCPDISCOVER broadcast.

6. The PXE enabled DP sends a DHCPACK which contains the BootFileName location, the WDS network boot program (NBP).

```
Dhcp: Reply, MsgType = ACK, TransactionID = 0x5E3CD04C
    OpCode: Reply, 2(0x02)
    Hardwaretype: Ethernet
    HardwareAddressLength: 6 (0x6)
    HopCount: 0 (0x0)
    TransactionID: 1581043788 (0x5E3CD04C)
    Seconds: 4 (0x4)
  + Flags: 0 (0x0)
    ClientIP: 10.238.0.3
    YourIP: 0.0.0.0
    ServerIP: 10.238.0.2
    RelayAgentIP: 0.0.0.0
  + ClientHardwareAddress: 00-15-5D-3C-D0-4C
    ServerHostName:
    BootFileName: smsboot\x86\wdsnbp.com
    MagicCookie: 99.130.83.99
  + MessageType: ACK - Type 53
  + ServerIdentifier: 10.238.0.2 - Type 54
  + Generaloption: UUID/GUID based Client Identifier - Type 97
  + DHCPEOptionsVendorClassIdentifier:
  + DHCPEOptionsContinueOption:
  + End:
```

## DOWNLOADING THE BOOT FILES

7. Once the DHCP conversation has completed the client will start the TFTP session with a read request:

```
+ Ipv4: Src = 10.238.0.3, Dest = 10.238.0.2, Next Protocol = UDP, Packet ID = 3, Total IP Length = 67
+ Udp: SrcPort = 2070, DstPort = TFTP, Trivial File Transfer Protocol(69), Length = 47
- Tftp:  Read Request - File: smsboot\x86\wdsnbp.com, Transfer Mode: octet tsize: 0
    OpCode: Read Request (1)
  - RRQ: File: smsboot\x86\wdsnbp.com, Transfer Mode: octet tsize: 0
      Filename: smsboot\x86\wdsnbp.com
      Mode: octet
    - Option: tsize: 0
        Option: tsize
        Value: 0
```

The server responds with the tsize and then the blksize. The client will then transfer the file from the server in blocks of data. The size of these blocks is the blksize and in this case it is set to 1456 bytes. The blksize is configurable on Windows 2008 and up (see http://support.microsoft.com/kb/975710 for more details).

Here we can see the end of the DHCP conversation and the start of the TFTP transfer:

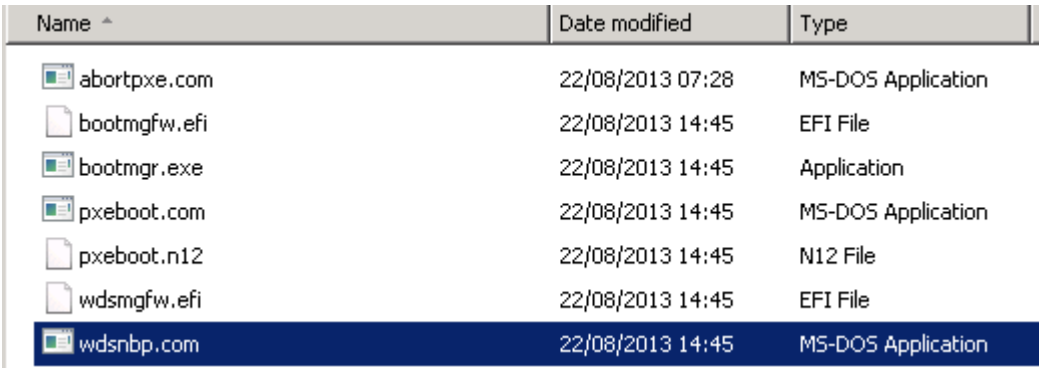
| | | | |
|---|---|---|---|
| 10.238.0.2 | 10.238.0.3 | DHCP | DHCP:Reply, MsgType = ACK, TransactionID = 0x5E3CD04C |
| 10.238.0.3 | 10.238.0.2 | TFTP | TFTP: Read Request - File: smsboot\x86\wdsnbp.com, Transfer Mode: octet tsize: 0 |
| 10.238.0.2 | 10.238.0.3 | TFTP | TFTP: Option Acknowledgement - tsize: 30832 |
| 10.238.0.3 | 10.238.0.2 | TFTP | TFTP: Error - ErrorCode: 0, ErrorMessage: TFTP Aborted |
| 10.238.0.3 | 10.238.0.2 | TFTP | TFTP: Read Request - File: smsboot\x86\wdsnbp.com, Transfer Mode: octet blksize: 1456 |
| 10.238.0.2 | 10.238.0.3 | TFTP | TFTP: Option Acknowledgement - blksize: 1456 |
| 10.238.0.3 | 10.238.0.2 | TFTP | TFTP: Acknowledgement - Block Number: 0 |
| 10.238.0.2 | 10.238.0.3 | TFTP | TFTP: Data - Block Number: 1 |
| 10.238.0.3 | 10.238.0.2 | TFTP | TFTP: Acknowledgement - Block Number: 1 |
| 10.238.0.2 | 10.238.0.3 | TFTP | TFTP: Data - Block Number: 2 |
| 10.238.0.3 | 10.238.0.2 | TFTP | TFTP: Acknowledgement - Block Number: 2 |
| 10.238.0.2 | 10.238.0.3 | TFTP | TFTP: Data - Block Number: 3 |
| 10.238.0.3 | 10.238.0.2 | TFTP | TFTP: Acknowledgement - Block Number: 3 |
| 10.238.0.2 | 10.238.0.3 | TFTP | TFTP: Data - Block Number: 4 |
| 10.238.0.3 | 10.238.0.2 | TFTP | TFTP: Acknowledgement - Block Number: 4 |
| 10.238.0.2 | 10.238.0.3 | TFTP | TFTP: Data - Block Number: 5 |
| 10.238.0.3 | 10.238.0.2 | TFTP | TFTP: Acknowledgement - Block Number: 5 |

When the WDS network boot program (NBP) has been transferred to the machine it will be executed. In this case it starts by downloading the **wdsnbp.com**. The NBP dictates whether the client can boot from the network, whether the client must press F12 to initiate the boot and which boot image the client will receive.

NBPs are both architecture and firmware specific (BIOS or UEFI). On BIOS computers the NBP is a 16-bit real-mode application, therefore, it is possible to use the same NBP for both x86-based and x64-based operating systems.

In this case (x64 BIOS machine) the NBP is physical located in the following directory on the PXE enabled DP:

\\remotedp\c$\RemoteInstall\SMSBoot\x64




These files perform the following functions:

**PXEboot.com – x86 and x64 BIOS**

Requires the end-user to press the F12 key for PXE boot to continue. (This is the default NBP.)

**PXEboot.n12 – x86 and x64 BIOS**

Immediately begins PXE boot (does not require pressing F12 on the client).

**AbortPXE.com – x86 and x64 BIOS**

Allows the device to immediately begin booting by using the next boot device specified in the BIOS. This allows for devices that should not be booting using PXE to immediately begin their secondary boot process without waiting for a timeout.

**Bootmgfw.efi – x64 UEFI and IA64 UEFI**

The EFI version of PXEboot.com or PXEboot.n12 (in EFI, the choice of whether or not to PXE boot is handled within the EFI shell, and not by the NBP). Bootmgfw.efi is equivalent to combining the functionality in PXEboot.com, PXEboot.n12, abortpxe.com, and bootmgr.exe.

**wdsnbp.com – x86 and x64 BIOS**

A special NBP developed for use by Windows Deployment Services that serves the following general purposes:

- Architecture detection
- Pending devices scenarios

**Wdsmgfw.efi – x64 UEFI and IA64 UEFI**

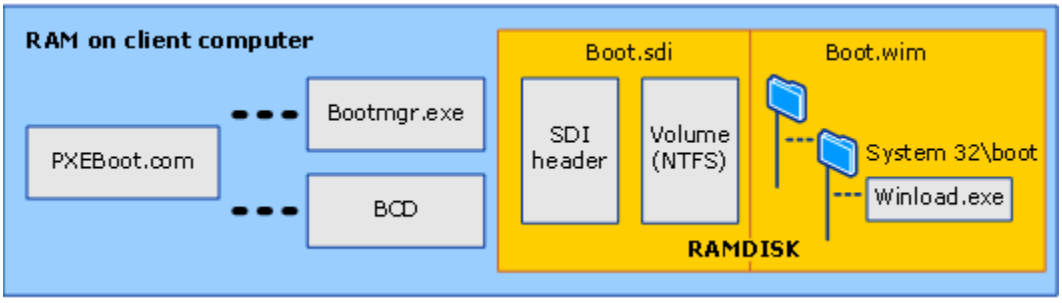
A special NBP developed for use by Windows Deployment Services that serves the following general purposes:

- Handles prompting the user to press a key to continue PXE boot
- Pending devices scenarios

8. The NBP downloads the operating system loader and the boot files via TFTP which include the following:

smsboot\x64\pxeboot.com
smsboot\x64\bootmgr.exe
\SMSBoot\Fonts\wgl4_boot.ttf
\SMSBoot\boot.sdi
\SMSImages\RR200004\boot.RR200004.wim

9. The RAMDISK is created using these files and the WinPE WIM file in memory.



## SMSPXE.LOG

The most important log for understanding where the boot process has failed is the SMSPXE.log. This is located on the site system which hosts the PXE enabled DP.

In this case SMSPXE.log is located in C:\SMS_DP$\sms\logs because the DP is installed on a remote site system.

When a machine first attempts to PXE boot the DHCPDISCOVER will be detected in the SMSPXE.log:

**SMSPXE.log**

[010.238.000.002:67] Recv From:[000.000.000.000:68] Len:548 7deae0d0

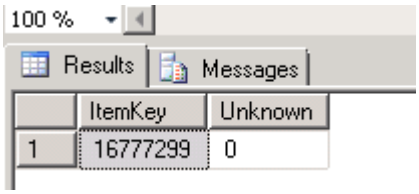
The first thing that the SMSPXE provider will do is query the Configuration Manager database to see whether the machine exists. This is important because it needs to understand whether the machine is an unknown computer or currently exists as a client.

It does this by running a number of stored procedures in SQL which are prefixed with “NBS”. In this case it initially executes NBS_LookupPXEDevice with the following parameters:

```
exec NBS_LookupPXEDevice N'32E5B71A-B626-4A4B-902E-7F94AD38B5B3',N'00:15:5D:3C:D0:4C'
```

NBS_LookupPXEDevice checks the database tables to see whether an existing record exists with the MAC address or SMBIOS GUID, these are the parameters for this stored procedure as you can see above.

If I run this in SQL I see the following results:




This returns an Itemkey of a known machine. You will then see the following logged in the SMSPXE.log, notice the same ItemKey is printed in the log that was returned from the stored procedure and it confirms the device is known.

**SMSPXE.log**

Client lookup reply: <ClientIDReply><Identification Unknown="0" ItemKey="16777299" ServerName=""><Machine><ClientID/><NetbiosName/></Machine></Identification></ClientIDReply>
MP_LookupDevice succeeded: 16777299 1 16777299 1 0
00:15:5D:3C:D0:4C, 32E5B71A-B626-4A4B-902E-7F94AD38B5B3: device is in the database.

The next step involves running NBS_GetPXEBootAction with a number of parameters (the ItemKey, the UnknownItemKey, the SMBIOS GUID, the MAC address and the DP name:

```
exec NBS_GetPXEBootAction N'16777299',N'2046820352',N'32E5B71A-B626-4A4B-902E-
7F94AD38B5B3',N'00:15:5D:3C:D0:4C',N'RemoteDp.sc.local'
```

This returns a list of task sequence offers that are available to that machine, here is the result of running that stored procedure in SQL:

| OfferID | OfferIDTime | PkgID | PackageVersion | PackagePath | BootImageID | Mandatory | Known |
|---|---|---|---|---|---|---|---|
| RR220028 | 2014-09-03 16:15:00.000 | RR2000CE | | http://RemoteDp.sc.local/SMS_DP_SMSPKG$/RR200004 | RR200004 | 0 | 1 |
| RR220028 | 2014-09-03 16:15:00.000 | RR2000CE | | \\REMOTEDP.SC.LOCAL\SMSPKGC$\RR200004\ | RR200004 | 0 | 1 |
| RR220026 | 2014-08-20 09:09:00.000 | RR200127 | | http://RemoteDp.sc.local/SMS_DP_SMSPKG$/RR200004 | RR200004 | 0 | 1 |
| RR220026 | 2014-08-20 09:09:00.000 | RR200127 | | \\REMOTEDP.SC.LOCAL\SMSPKGC$\RR200004\ | RR200004 | 0 | 1 |
| RR220014 | 2014-04-24 11:25:00.000 | RR2000D5 | | http://RemoteDp.sc.local/SMS_DP_SMSPKG$/RR200004 | RR200004 | 0 | 1 |
| RR220014 | 2014-04-24 11:25:00.000 | RR2000D5 | | \\REMOTEDP.SC.LOCAL\SMSPKGC$\RR200004\ | RR200004 | 0 | 1 |
| RR22000E | 2014-02-10 11:10:00.000 | RR200024 | | http://RemoteDp.sc.local/SMS_DP_SMSPKG$/RR200004 | RR200004 | 0 | 1 |
| RR22000E | 2014-02-10 11:10:00.000 | RR200024 | | \\REMOTEDP.SC.LOCAL\SMSPKGC$\RR200004\ | RR200004 | 0 | 1 |
| RR22000D | 2014-01-29 15:26:00.000 | RR200012 | | http://RemoteDp.sc.local/SMS_DP_SMSPKG$/RR200004 | RR200004 | 0 | 1 |
| RR22000D | 2014-01-29 15:26:00.000 | RR200012 | | \\REMOTEDP.SC.LOCAL\SMSPKGC$\RR200004\ | RR200004 | 0 | 1 |

**TIP:**

If a PXE enabled DP is configured on a secondary site the NBS stored procedures are actually just linked to the parent primary site database and run from there. If you look in SQL on the secondary site the primary site is a linked server. The tables required to run these are not present on a secondary site.

Here is the first offer listed in the SMSPXE.log:

**SMSPXE.log**

Client lookup reply: <ClientIDReply><Identification Unknown="0" ItemKey="16777299" ServerName=""><Machine><ClientID/><NetbiosName/></Machine></Identification></ClientIDReply>

Client Identity: GUID:4e3afb04-fd6a-4e97-a7ff-22baa381a813
00:15:5D:3C:D0:4C, 32E5B71A-B626-4A4B-902E-7F94AD38B5B3: SMSID=GUID:4e3afb04-fd6a-4e97-a7ff-22baa381a813
OfferID=RR220028, PackageID=RR2000CE, PackageVersion=, BootImageID=RR200004,
PackagePath=http://RemoteDp.sc.local/SMS_DP_SMSPKG$/RR200004, Mandatory=0
00:15:5D:3C:D0:4C, 32E5B71A-B626-4A4B-902E-7F94AD38B5B3: found optional advertisement RR220028

Once the PXE Provider has a list of offers it chooses the first in the list and provides this data as the boot action reply.

**SMSPXE.log**

Client boot action reply: <ClientIDReply><Identification Unknown="0" ItemKey="16777299" ServerName=""><Machine><ClientID>GUID:4e3afb04-fd6a-4e97-a7ff-22baa381a813</ClientID><NetbiosName/></Machine></Identification><PXEBootAction LastPXEAdvertisementID="" LastPXEAdvertisementTime="" OfferID="RR220028" OfferIDTime="03/09/2014 16:15:00" PkgID="RR2000CE" PackageVersion="" PackagePath="http://RemoteDp.sc.local/SMS_DP_SMSPKG$/RR200004" BootImageID="RR200004" Mandatory="0"/></ClientIDReply>

00:15:5D:3C:D0:4C, 32E5B71A-B626-4A4B-902E-7F94AD38B5B3: SMSID=GUID:4e3afb04-fd6a-4e97-a7ff-22baa381a813
OfferID=RR220028, PackageID=RR2000CE, PackageVersion=, BootImageID=RR200004,
PackagePath=http://RemoteDp.sc.local/SMS_DP_SMSPKG$/RR200004, Mandatory=0
00:15:5D:3C:D0:4C, 32E5B71A-B626-4A4B-902E-7F94AD38B5B3: found optional advertisement RR220028
Looking for bootImage RR200004

**00:15:5D:3C:D0:4C, 32E5B71A-B626-4A4B-902E-7F94AD38B5B3: found optional advertisement RR220028**
**Looking for bootImage RR200004**

The final lines logged confirms that the PXE provider has found an optional advertisement for the machine and that it is looking for the appropriate boot image.

At this point the PXE client initiates the TFTP download of the network boot program and the boot files as described above.

## WINPE BOOT

Once WinPE has booted the TS boot shell is initiated from the SMS folder that is included in the WinPE image (this folder is injected into the boot WIM when it is imported into Configuration Manager). You can see this process logged from the SMSTS.log which is located in the X:\Windows\Temp\SMSTS\smsts.log

**TIP:**

To access this log in WinPE enable the command prompt on the boot image. Right click the boot image > properties > Customization > check “Enable command support (testing only). You can then access the command prompt by pressing F8 in WinPE.

Here is the initial TS boot shell process:

**SMSTS.log**

```
==============================[ TSBootShell.exe ]==============================
Succeeded loading resource DLL 'X:\sms\bin\i386\1033\TSRES.DLL'
Debug shell is enabled
Waiting for PNP initialization...
RAM Disk Boot Path: NET(0)\SMSIMAGES\RR200004\BOOT.RR200004.WIM
Booted from network (PXE)
Network(PXE) path: X:\sms\data\
Found config path X:\sms\data\
This is not a fixed non usb disk
Booting from removable media, not restoring bootloaders on hard drive
X:\sms\data\WinPE does not exist.
X:\_SmsTsWinPE\WinPE does not exist.
Executing command line: wpeinit.exe -winpe
The command completed successfully.
Starting DNS client service.
Executing command line: X:\sms\bin\i386\TsmBootstrap.exe /env:WinPE /configpath:X:\sms\data\
The command completed successfully.
```

Followed by the task sequence manager boot strap:

**SMSTS.log**

```
 ==============================[ TSMBootStrap.exe ]==============================
Command line: X:\sms\bin\i386\TsmBootstrap.exe /env:WinPE /configpath:X:\sms\data\
Succeeded loading resource DLL 'X:\sms\bin\i386\1033\TSRES.DLL'
Succeeded loading resource DLL 'X:\sms\bin\i386\TSRESNLC.DLL'
Current OS version is 6.2.9200.0
Adding SMS bin folder "X:\sms\bin\i386" to the system environment PATH
PXE Boot with Root = X:\
Executing from PXE in WinPE
Loading TsPxe.dll from X:\sms\bin\i386\TsPxe.dll
```

Once TSPXE is loaded it downloads the TS variables using TFTP:

**SMSTS.log**

```
TsPxe.dll loaded
Device has PXE booted
Variable Path: \SMSTemp\2014.09.05.18.20.31.0001.{0C616323-A027-41B0-A215-057AF4F1E361}.boot.var
Succesfully added firewall rule for Tftp
Executing: X:\sms\bin\i386\smstftp.exe -i 10.238.0.2 get \SMSTemp\2014.09.05.18.20.31.0001.{0C616323-A027-41B0-A215-
057AF4F1E361}.boot.var X:\sms\data\variables.dat
Executing command line: "X:\sms\bin\i386\smstftp.exe" -i 10.238.0.2 get \SMSTemp\2014.09.05.18.20.31.0001.{0C616323-
A027-41B0-A215-057AF4F1E361}.boot.var X:\sms\data\variables.dat
Process completed with exit code 0
Succesfully removed firewall rule for Tftp
Successfully downloaded pxe variable file.

Loading Media Variables from "X:\sms\data\variables.dat"
Loading Media Variables from "X:\sms\data\variables.dat"
Found network adapter "Intel 21140-Based PCI Fast Ethernet Adapter (Emulated)" with IP Address 10.238.0.3.
Loading Media Variables from "X:\sms\data\variables.dat"
Loading variables from the Task Sequencing Removable Media.
Loading Media Variables from "X:\sms\data\variables.dat"
Succeeded loading resource DLL 'X:\sms\bin\i386\1033\TSRES.DLL'

Setting SMSTSMP TS environment variable
Setting _SMSMediaGuid TS environment variable
Setting _SMSTSBootMediaPackageID TS environment variable
Setting _SMSTSHTTPPort TS environment variable
Setting _SMSTSHTTPSPort TS environment variable
Setting _SMSTSIISSSLState TS environment variable
Setting _SMSTSLaunchMode TS environment variable
Setting _SMSTSMediaPFX TS environment variable
Setting _SMSTSPublicRootKey TS environment variable
Setting _SMSTSRootCACerts TS environment variable
Setting _SMSTSSiteCode TS environment variable
Setting _SMSTSSiteSigningCertificate TS environment variable
Setting _SMSTSUseFirstCert TS environment variable
Setting _SMSTSx64UnknownMachineGUID TS environment variable
Setting _SMSTSx86UnknownMachineGUID TS environment variable
```

At this point TSPXE locates the management point (MP) and downloads policy before presenting the user interface for the user to select the optional task sequence:

**SMSTS.log**

```
site=RR2,RR2, MP=http://ConfigMgrR2.SC.LOCAL, ports: http=80,https=443
   certificates are received from MP.
CLibSMSMessageWinHttpTransport::Send: URL: ConfigMgrR2.SC.LOCAL:80  CCM_POST /ccm_system/request
Request was successful.
Downloading policy from http://ConfigMgrR2.SC.LOCAL.
Retrieving Policy Assignments:
   Processing Policy Assignment {7898f153-a6de-43e9-98c3-ca5cc61483b0}.
   Processing Policy Assignment {fba19677-0e9b-490d-b601-07e247979bd4}.
   Processing Policy Assignment {6306ca4c-e7ed-4cf5-8419-af9b1695a909}.
   Processing Policy Assignment {05a027ff-e9cf-4fa1-8bd8-4565481061e2}.
  Processing Policy Assignment {b3c991f6-9f83-43c3-875c-f60c4492d278}.
  …
 Successfully read 152 policy assignments.
```

Finally the collection and machine variables are downloaded and the welcome page is activated:

**SMSTS.log**

```
Retrieving collection variable policy.
Found 0 collection variables.
Retrieving machine variable policy.
Downloading policy body {01000053}-{RR2}.
Response ID: {01000053}-{RR2}
Reading Policy Body.
Parsing Policy Body.
Found 0 machine variables.
Setting collection variables in the task sequencing environment.
Setting machine variables in the task sequencing environment.
Running Wizard in Interactive mode
Loading Media Variables from "X:\sms\data\variables.dat"
Activating Welcome Page.
Loading bitmap
```

# TROUBLESHOOTING

## DHCP DISCOVERY

There are a number of important points to consider before starting to troubleshoot the initial DHCP discovery stage of the PXE booting process:

- If you can't see the MAC address or the DHCPREQUEST of the device you are attempting to boot in the SMSPXE.log then there is a potential network connectivity problem between the client and the DP.
- Don't use DHCP options 60, 66 and 67, this is not supported.
- Test whether the device can boot when plugged into a switch on the same subnet as the PXE enabled DP.
- Ensure the DHCP (67 and 68), TFTP (69) and BINL (4011) ports are open between the client, DHCP server and PXE DP.

At this stage of the process there are no logs to refer to but usually, when the PXE boot process fails before WinPE has booted, a PXE error code will be revealed. Examples of these errors at this stage are:

**PXE-E51: No DHCP or proxyDHCP offers were received.**
**PXE-E52: proxyDHCP offers were received. No DHCP offers were received.**
**PXE-E53: No boot filename received.**
**PXE-E55: proxyDHCP service did not reply to request on port 4011.**
**PXE-E77 bad or missing discovery server list.**
**PXE-E78: Could not locate boot server.**

There are a number of web pages that attempt to document these error codes:

HP's - What are the PXE Error Codes?

Symantec's list of PXE error codes and their meaning.

This will help narrow down the focus of the troubleshooting but it may be necessary to capture the issue with a network monitoring tool such as Netmon or WireShark.

The network monitoring tool will need to be installed on the PXE enabled DP and a machine connected to a mirrored port on the switch.

This mirrored port would be configured to copy all the network packets from the port in use by the device attempting to PXE boot. For more details on configuring mirrored ports please refer to the manual provided by the manufacturer of the specific switch or routing device.

The usual procedure is to start the network traces on both the DP and the machine connected to the mirrored port and then attempt to boot the device via PXE.

Once this has been completed then stop the traces and save them for further analysis. Here is an example of a DHCP conversation captured from the PXE enabled DP:

| Source | Destination | Protocol Name | Description |
|---|---|---|---|
| 0.0.0.0 | 255.255.255.255 | DHCP | DHCP:Request, MsgType = DISCOVER, TransactionID = 0x5E3CD04C |
| 10.238.0.2 | 255.255.255.255 | DHCP | DHCP:Reply, MsgType = OFFER, TransactionID = 0x5E3CD04C |
| 10.238.0.14 | 255.255.255.255 | DHCP | DHCP:Reply, MsgType = OFFER, TransactionID = 0x5E3CD04C |
| 0.0.0.0 | 255.255.255.255 | DHCP | DHCP:Request, MsgType = REQUEST, TransactionID = 0x5E3CD04C |
| 10.238.0.14 | 255.255.255.255 | DHCP | DHCP:Reply, MsgType = ACK, TransactionID = 0x5E3CD04C |
| 10.238.0.3 | 10.238.0.2 | DHCP | DHCP:Request, MsgType = REQUEST, TransactionID = 0x5E3CD04C |
| 10.238.0.2 | 10.238.0.3 | DHCP | DHCP:Reply, MsgType = ACK, TransactionID = 0x5E3CD04C |

The initial DHCPDISCOVER by the PXE client followed by DHCPOFFER from the DHCP server and the PXE DP. The request from the client (0.0.0.0) is made and then acknowledged by the DHCP server (10.238.0.14).

Once the PXE client has an IP (10.238.0.3) it sends a request to the PXE DP (10.238.0.2) which acknowledges it with the network boot program details.

Steps to try:

- Capture a simultaneous network trace on the client and the DP to see if the conversation is occurring as expected.
- Ensure the DHCP services are running and available.
- Check the WDS service is running on the DP.
- Make sure there are no firewalls blocking the DHCP ports.
- Check whether they machine is able to boot on the same subnet as the DP.
- Ensure IP helpers are configured correctly if booting from a different subnet than the DP.

## TFTP TRANSFER

If the error on PXE boot refers to TFTP then you have a problem transferring the files. Examples of these errors include:

**PXE-E32: TFTP open timeout.**
**PXE-E35: TFTP read timeout.**
**PXE-E36: Error received from TFTP server.**
**PXE-E3F: TFTP packet size is invalid.**
**PXE-E3B: TFTP Error - File not Found**
**PXE-T04: Access Violation**

Monitoring the network using Netmon or Wireshark is a good plan to try and troubleshoot these errors. Here is an example of the data captured from the PXE client when a TFTP open timeout occurs:

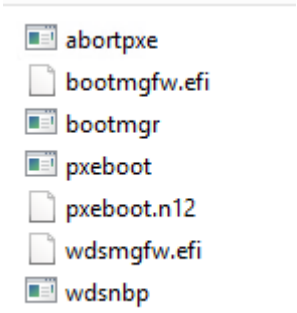
| Protocol | Length | Info |
|---|---|---|
| TFTP | 81 | Read Request, File: smsboot\x86\wdsnbp.com, Transfer type: octet, tsize\000=0\000 |
| TFTP | 60 | Option Acknowledgement, tsize\000=31124\000 |
| TFTP | 60 | Error Code, Code: Not defined, Message: TFTP Aborted |
| TFTP | 86 | Read Request, File: smsboot\x86\wdsnbp.com, Transfer type: octet, blksize\000=1456\000 |
| TFTP | 60 | Option Acknowledgement, blksize\000=1456\000 |
| TFTP | 60 | Acknowledgement, Block: 0 |
| TFTP | 1406 | Data Packet, Block: 1 |
| TFTP | 1406 | Data Packet, Block: 1 |
| TFTP | 86 | Read Request, File: smsboot\x86\wdsnbp.com, Transfer type: octet, blksize\000=1456\000 |
| TFTP | 60 | Option Acknowledgement, blksize\000=1456\000 |
| TFTP | 60 | Acknowledgement, Block: 0 |
| TFTP | 1406 | Data Packet, Block: 1 |
| TFTP | 1406 | Data Packet, Block: 1 |
| TFTP | 1406 | Data Packet, Block: 1 |
| TFTP | 1406 | Data Packet, Block: 1 |
| TFTP | 1406 | Data Packet, Block: 1 |
| TFTP | 86 | Read Request, File: smsboot\x86\wdsnbp.com, Transfer type: octet, blksize\000=1456\000 |
| TFTP | 60 | Option Acknowledgement, blksize\000=1456\000 |
| TFTP | 60 | Acknowledgement, Block: 0 |
| TFTP | 1406 | Data Packet, Block: 1 |
| TFTP | 1406 | Data Packet, Block: 1 |
| TFTP | 1406 | Data Packet, Block: 1 |
| TFTP | 1406 | Data Packet, Block: 1 |
| TFTP | 1406 | Data Packet, Block: 1 |
| TFTP | 1406 | Data Packet, Block: 1 |
| TFTP | 1406 | Data Packet, Block: 1 |
| TFTP | 1406 | Data Packet, Block: 1 |
| TFTP | 86 | Read Request, File: smsboot\x86\wdsnbp.com, Transfer type: octet, blksize\000=1456\000 |
| TFTP | 60 | Option Acknowledgement, blksize\000=1456\000 |
| TFTP | 60 | Acknowledgement, Block: 0 |

The client is sending read requests for the wdsnbp.com file but is not receiving a response, it is using the blksize 1456. Something is preventing the acknowledgment from being received by the client. Here is what it should look like:

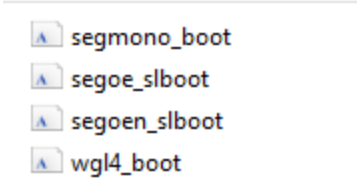
| Protocol | Length | Info |
|---|---|---|
| TFTP | 81 | Read Request, File: smsboot\x86\wdsnbp.com, Transfer type: octet, tsize\000=0\000 |
| TFTP | 56 | Option Acknowledgement, tsize\000=30832\000 |
| TFTP | 60 | Error Code, Code: Not defined, Message: TFTP Aborted |
| TFTP | 86 | Read Request, File: smsboot\x86\wdsnbp.com, Transfer type: octet, blksize\000=1456\000 |
| TFTP | 57 | Option Acknowledgement, blksize\000=1456\000 |
| TFTP | 60 | Acknowledgement, Block: 0 |
| TFTP | 1502 | Data Packet, Block: 1 |
| TFTP | 60 | Acknowledgement, Block: 1 |
| TFTP | 1502 | Data Packet, Block: 2 |
| TFTP | 60 | Acknowledgement, Block: 2 |
| TFTP | 1502 | Data Packet, Block: 3 |
| TFTP | 60 | Acknowledgement, Block: 3 |
| TFTP | 1502 | Data Packet, Block: 4 |
| TFTP | 60 | Acknowledgement, Block: 4 |
| TFTP | 1502 | Data Packet, Block: 5 |
| TFTP | 60 | Acknowledgement, Block: 5 |
| TFTP | 1502 | Data Packet, Block: 6 |
| TFTP | 60 | Acknowledgement, Block: 6 |
| TFTP | 1502 | Data Packet, Block: 7 |
| TFTP | 60 | Acknowledgement, Block: 7 |
| TFTP | 1502 | Data Packet, Block: 8 |
| TFTP | 60 | Acknowledgement, Block: 8 |
| TFTP | 1502 | Data Packet, Block: 9 |
| TFTP | 60 | Acknowledgement, Block: 9 |
| TFTP | 1502 | Data Packet, Block: 10 |
| TFTP | 60 | Acknowledgement, Block: 10 |
| TFTP | 1502 | Data Packet, Block: 11 |
| TFTP | 60 | Acknowledgement, Block: 11 |
| TFTP | 1502 | Data Packet, Block: 12 |
| TFTP | 60 | Acknowledgement, Block: 12 |
| TFTP | 1502 | Data Packet, Block: 13 |
| TFTP | 60 | Acknowledgement, Block: 13 |
| TFTP | 1502 | Data Packet, Block: 14 |

Steps to try:

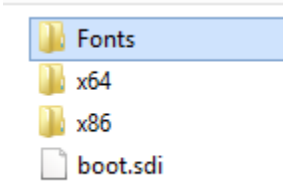
- Reduce the block size on the PXE enabled DP http://support.microsoft.com/kb/975710
- Check the WDS service is started on the DP.
- Ensure the TFTP port is open between the client and DP.
- Check the permissions on the REMINST share/folder are correct.
- Check the WDS logs for TFTP errors.
- Check that the RemoteInstall\SMSBoot\x86 and \x64 contains the following files:




The Fonts exist in SMSBoot\Fonts




And the boot.sdi exists in the RemoteInstall\SMSBoot directory




## WINPE BOOT ISSUES

**Drivers**

The most common issues that occur during this phase are driver related. On the whole the latest version of WinPE contains the vast majority of the network and mass storage drivers but there will be occasions where these need to be injected into the boot WIM.

There are a couple of important points to note here:

- Only import the drivers you need, don't just import every driver you have into the boot image.
- Only ever consider adding the NIC or mass storage drivers. It is not necessary to include other drivers.

The SMSTS.log which is located in X:\Windows\temp\SMSTS is the most useful resource to troubleshoot these issues (remember to enable the command prompt). If you don't see a line logged with a valid IP address then you probably have a driver issue:

**SMSTS.log**

Found network adapter "Intel 21140-Based PCI Fast Ethernet Adapter (Emulated)" with IP Address 10.238.0.3

To confirm this simply press F8 and perform an Ipconfig at the command line to determine whether the NIC is recognized and if it has an IP address.

**WIM Files**

Obvious but essential, make sure both x86 and x64 boot images exist on the DP. You can see the WIMs in the following directory (they will also be in the content library):

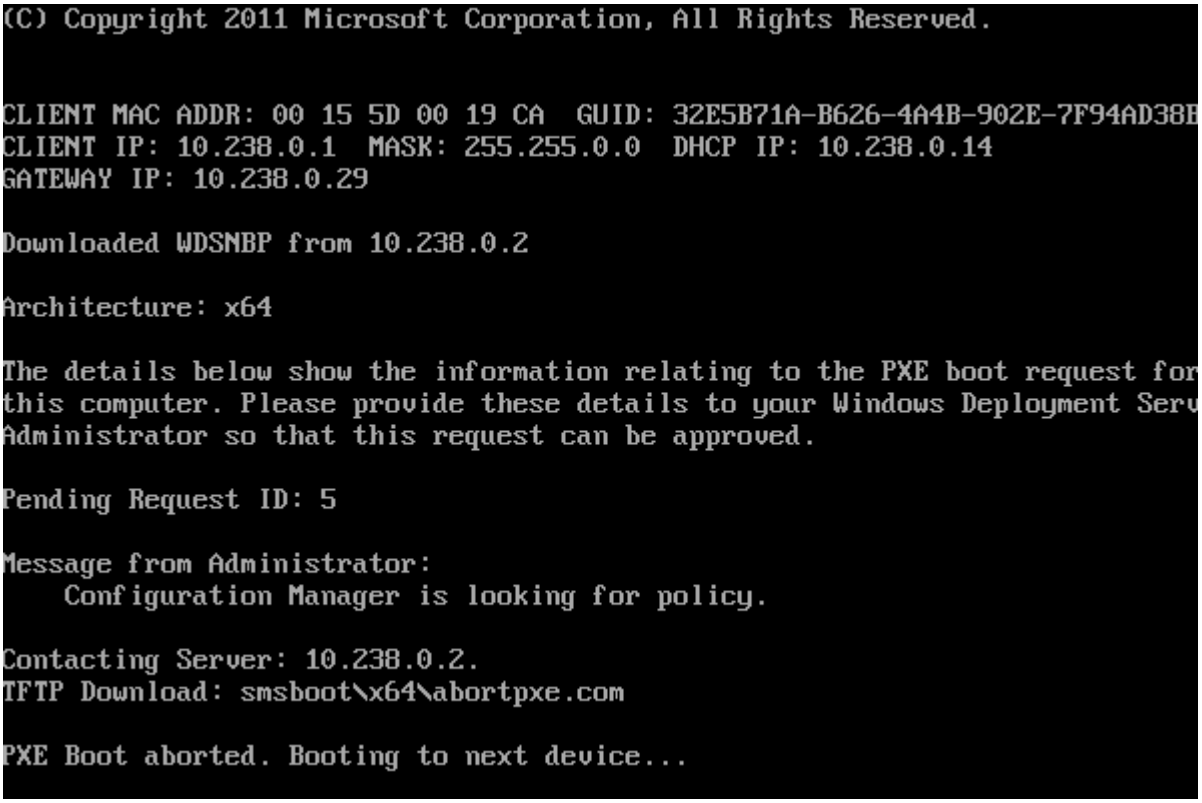
C:\RemoteInstall\SMSImages\<PackageID>

Ensure that they have been marked to "Deploy this boot image from the PXE-enabled distribution point" in the properties of the boot image.

## CONFIGMGR POLICY ISSUES

Another common issue with PXE booting is with task sequence deployments. In this example the task sequence is deployed to unknown computers but is already in the database.

The first symptom is that the PXE boot is aborted:




On further investigation we can see the following in the SMSPXE.log

**SMSPXE.log**

Client lookup reply: <ClientIDReply><Identification Unknown="0" ItemKey="16777299" ServerName=""><Machine><ClientID/><NetbiosName/></Machine></Identification></ClientIDReply>

MP_LookupDevice succeeded: 16777299 1 16777299 1 0
00:15:5D:00:19:CA, 32E5B71A-B626-4A4B-902E-7F94AD38B5B3: device is in the database.
Client boot action reply: <ClientIDReply><Identification Unknown="0" ItemKey="16777299" ServerName=""><Machine><ClientID/><NetbiosName/></Machine></Identification><PXEBootAction LastPXEAdvertisementID="" LastPXEAdvertisementTime="" OfferID="" OfferIDTime="" PkgID="" PackageVersion="" PackagePath="" BootImageID="" Mandatory=""/></ClientIDReply>
Client Identity:
00:15:5D:00:19:CA, 32E5B71A-B626-4A4B-902E-7F94AD38B5B3: SMSID= OfferID=, PackageID=, PackageVersion=, BootImageID=, PackagePath=, Mandatory=0
00:15:5D:00:19:CA, 32E5B71A-B626-4A4B-902E-7F94AD38B5B3: no advertisements found
00:15:5D:00:19:CA, 32E5B71A-B626-4A4B-902E-7F94AD38B5B3: No boot action. Aborted.
00:15:5D:00:19:CA, 32E5B71A-B626-4A4B-902E-7F94AD38B5B3: Not serviced.

When the NBS stored procedures ran they found no available policy and the boot action was aborted. The reverse can also be true, when a machine is unknown but the task sequence is deployed is to a collection of known machines.

Steps to try:

- Check the machine you are attempting to boot exists in a collection that is targeted with a task sequence deployment.
- Ensure you have checked the “Enable unknown computer support” PXE settings on the distribution point.
- If you are deploying the task sequence to unknown machines then check the machine doesn’t already exist in the database.

## LOGGING CONFIGURATIONS

### SQL LOGGING

To enable SQL logging on the site server you can alter the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Tracing\SqlEnabled

Change 0 to 1 – restarting the SMSEXEC service is not required in R2.

### ARCHIVE LOGGING

To enable archive logging you can change the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Tracing\ArchiveEnabled

Change 0 to 1

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Tracing\ArchivePath

Configure a local path, for example, C:\LogArchive

### DISTRIBUTION MANAGER VERBOSE LOGGING

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Tracing\SMS_DISTRIBUTION_MANAGER\LoggingLevel

### REMOTE DISTRIBUTION POINT VERBOSE PXE LOGGING

HKLM\SOFTWARE\Microsoft\SMS\DP\Logging\@GLOBAL\LogLevel

Change 1 to 0

### WDS LOGGING

http://support.microsoft.com/kb/936625

## FURTHER READING

**Intel detailed PXE design spec**
http://download.intel.com/design/archives/wfm/downloads/pxespec.pdf

**PXE and UEFI Performance analysis**
https://uefidk.com/sites/default/files/Intel_UEFI_PXE_Boot_Performance_Analysis.pdf