Principled Technologies®

TEST REPORT
OCTOBER 2009

A feature and performance analysis of the Intel vPro technology-based Dell Latitude E6400 notebook system running Windows 7

Executive summary

Dell Inc. (Dell) commissioned Principled Technologies (PT) to analyze the features and performance of the Intel® vPro™ technology-based Dell™ Latitude™ E6400 notebook system with Intel® Core™ 2 Duo Mobile Processor P8700 running Microsoft Windows® 7 Ultimate (Windows 7).

To do so, we tested this system and several comparison systems. Appendix A provides detailed system configuration information.

Intel vPro technology is a set of features on notebook and desktop PCs. There are three main hardware features of vPro:

- Core 2 Duo/Quad or Centrino 2 processor
- Integrated components
- Hardware-based management technology (Intel AMT 4.0)

Our testing focused on the following Intel vPro technology features: Windows Virtual PC RC (Windows XP Mode), BranchCache, DirectAccess, and Remote upgrade.

KEY FINDINGS

- SYSmark 2007 Preview performance for Virtual XP Mode on the Dell Latitude E6400 was 27 percent better than Windows XP Professional SP3 on the previous-generation Dell Latitude D610 notebook system. (See Figure 1.)
- Using BranchCache, the second client in our environment was able to execute the tasks at a time savings of over 85 percent over the first client (3 minutes 20 seconds faster). (See Figure 2.)
- DirectAccess provides a constant, reliable, and secure connection to a worker's network resources, and makes that connection 78 percent faster than a conventional VPN. (See Figure 3.)
- Using Intel AMT lets IT departments save the cost of travel or shipping to and from branch offices by centralizing the management of PCs. Once configured, the remote upgrade process completed up to 22 percent faster than the manual upgrade process. (See Figure 4.)

Windows XP Mode for Windows 7 allows you to run your Windows XP productivity applications directly from a Windows 7-based PC. However, you must have a notebook with Intel Virtualization Technology to run a Windows XP virtual machine in Windows 7. In our testing, we used the SYSmark 2007 Preview v1.06 benchmark to compare the Windows XP virtual machine's performance on the current Dell Latitude E6400 with Windows XP performance on a previous-generation Dell notebook system, the Dell Latitude D610.

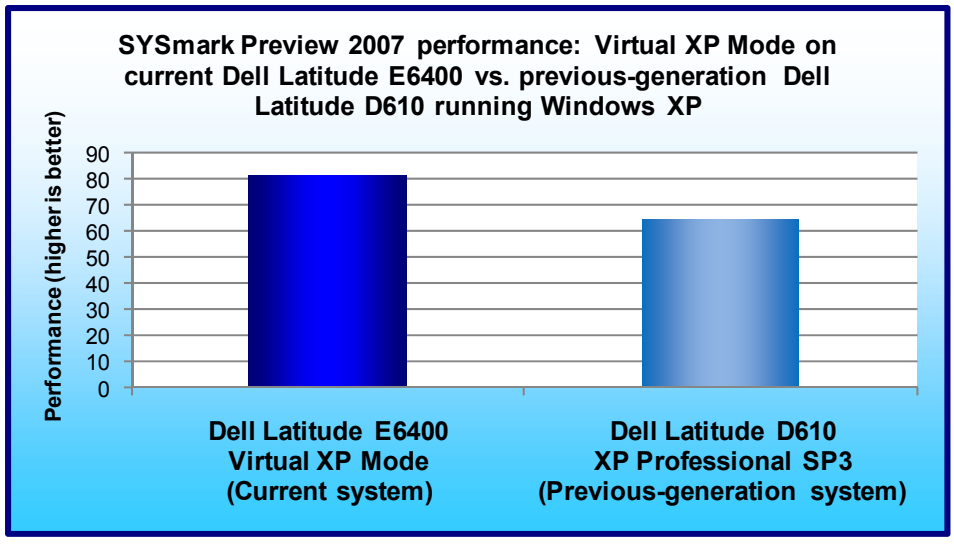

Figure 1: SYSmark 2007 Preview productivity results for our test systems. Higher numbers are better.

As Figure 1 shows, the SYSmark 2007 Preview performance for Virtual XP Mode on the Dell Latitude E6400 was 27 percent better than Windows XP Professional SP3 on the previous-generation Dell Latitude D610 notebook system.[1]

1 See Principled Technologies report, "A performance comparison of current and previous generation Dell Latitude notebook systems" (http://www.principledtechnologies.com/clients/reports/Dell/Latitude_1009.pdf).

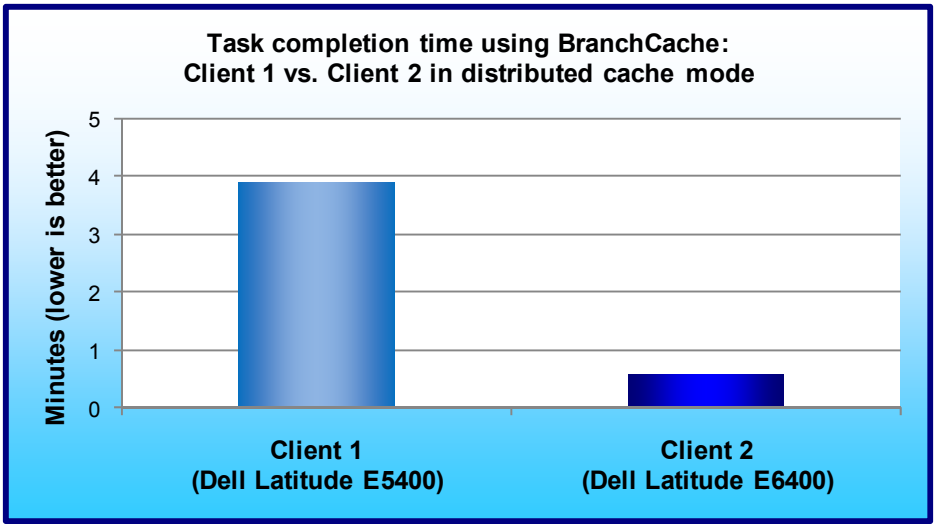

Figure 2: Task completion time using BranchCache – the sum of the averages for all tasks. Lower numbers, reflecting shorter times, are better.

BranchCache enables content from file and Web servers on a wide area network (WAN) to be cached on computers at a local branch office. BranchCache can improve application response time and reduce WAN traffic. We tested the application responsiveness for two current Dell Latitude notebook system clients in a BranchCache distributed mode environment. After the first client has executed a set of common tasks, such as file copies and file opens, BranchCache allows the second client to complete the same tasks considerably faster.

As Figure 2 shows, the second client in our environment was able to execute the tasks at a time savings of over 85 percent over the first client (3 minutes 20 seconds faster). More complete results are in the Test results section and Appendix B.

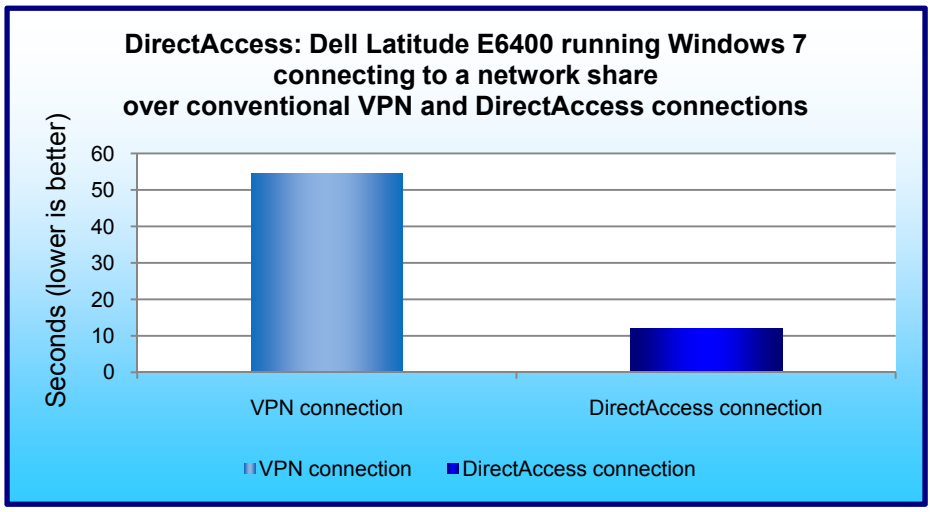

Figure 3: Time taken to connect to a network share – connection made over a conventional VPN versus connection made using DirectAccess. Lower numbers, reflecting shorter times, are better.

DirectAccess gives mobile users seamless access to corporate intranet resources wherever they travel, as well as at home, without needing to use a VPN. This transparent connection, which is active whenever the user is connected to the Internet, can enhance the work experience and increase productivity. We configured our vPro-based notebook to connect to a DirectAccess server, and tested the transparency of that connection, as described in the Connect E6400 to the Corpnet subnet section of the Test Methodology section below.

As Figure 3 shows, when configured with a DirectAccess connection, around 12 seconds passed from the point we logged into the notebook to the point we connected to the intranet resources. However, this connection happened completely in the background, without any thought or intervention from the user. The manual process of connecting to our test network and accessing our shared files over a conventional VPN, on the other hand, took almost 54 seconds to complete, 78 percent longer than the DirectAccess connection.

Intel AMT is part of the Intel Management Engine, which is another feature of Intel's vPro technology. Intel AMT consists of a set of remote management features that allows remote power up, power down, reboot, access to the

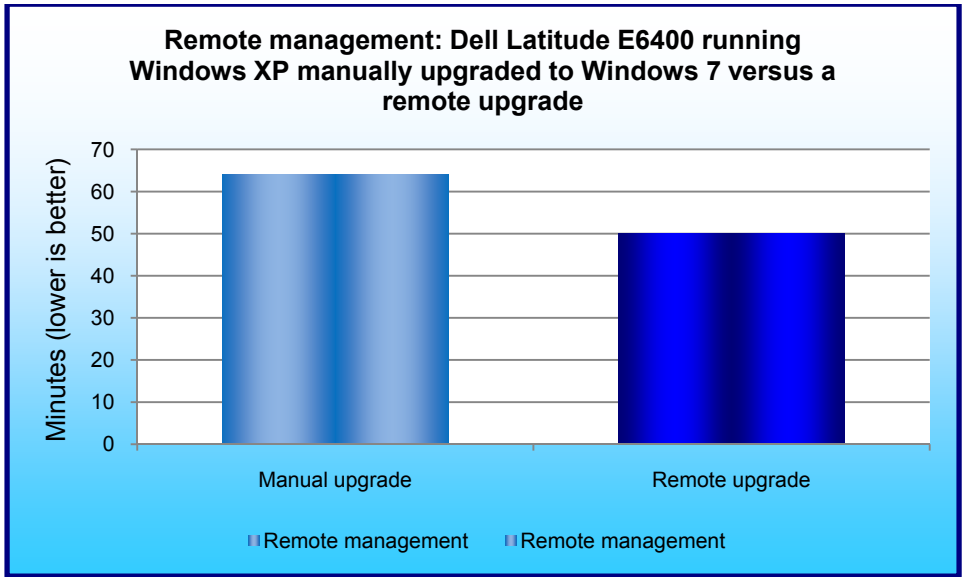

Figure 4: Task completion time using BranchCache – the sum of the averages for all tasks. Lower numbers, reflecting shorter times, are better.

BIOS, and access to system information. In our testing, we configured System Center Configuration Manager 2007 SP2 (SCCM) on one of our member servers, and performed a remote upgrade of our vPro technology-based Dell Latitude E6400 from Windows XP SP3 to Windows 7 Ultimate. In the process, we demonstrated the potential ease with which a centralized IT department can migrate its workforce from a Windows XP-based shop to Windows 7. Using Intel vPro technology, SCCM manages PCs without requiring the IT department to either (1) send an IT administrator to the branch office or (2) incur the cost of shipping systems to the centralized IT department to perform the migration. As Firgure 4 shows, a manual upgrade from Microsoft Windows XP Professional to Windows 7 Ultimate, including Microsoft Office 2007 with Service Pack 2, required 1 hour and 4 minutes on our test system, whereas the remote upgrade took 50 minutes, 22 percent less time than the manual upgrade.

Workload

SYSmark 2007 Preview v1.06

SYSmark 2007 Preview is a performance metric BAPCo created to measure system performance.

SYSmark 2007 Preview determines its overall rating from the mean result from four workload scenarios: e-learning, office productivity, video creation, and 3D modeling. SYSmark 2007 Preview records the time the system takes to complete each individual operation in each scenario.

SYSmark 2007 Preview consists of the following applications and corresponding tasks: Adobe® After® Effects 7 (e-learning), Adobe® Illustrator® CS2 (video creation), Adobe® Photoshop® CS2 (video creation), AutoDesk® 3ds Max® 8 (3D modeling), Macromedia® Flash 8 (e-learning), Microsoft® Excel 2003 (office productivity), Microsoft® Outlook 2003 (office productivity), Microsoft® PowerPoint 2003 (office productivity), Microsoft® Word 2003 (office productivity), Microsoft® Project 2003 (office productivity), Microsoft® Windows Media™ Encoder 9 series (video creation), Sony® Vegas 7 (video creation), SketchUp 5 (3D modeling), and WinZip® 10.0 (office productivity).

To learn more, visit http://www.bapco.com/support/sysmark2007preview/Help/Help.html.

Test results

BranchCache application responsiveness

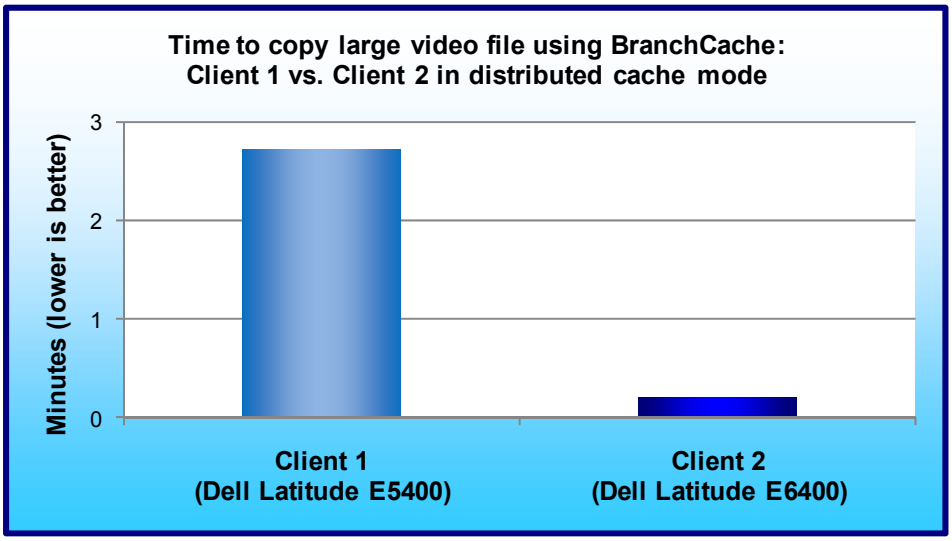

Figure 5: Time to copy large video file using BranchCache. Lower numbers, reflecting shorter times, are better.

Figure 5 shows the time to copy a large video file for two current Dell Latitude notebook system clients in a BranchCache distributed mode environment. The second client in our environment (Dell Latitude E6400) performed the task at a time savings of almost 93 percent over the first client (Dell Latitude E5400)—2.5 minutes faster.

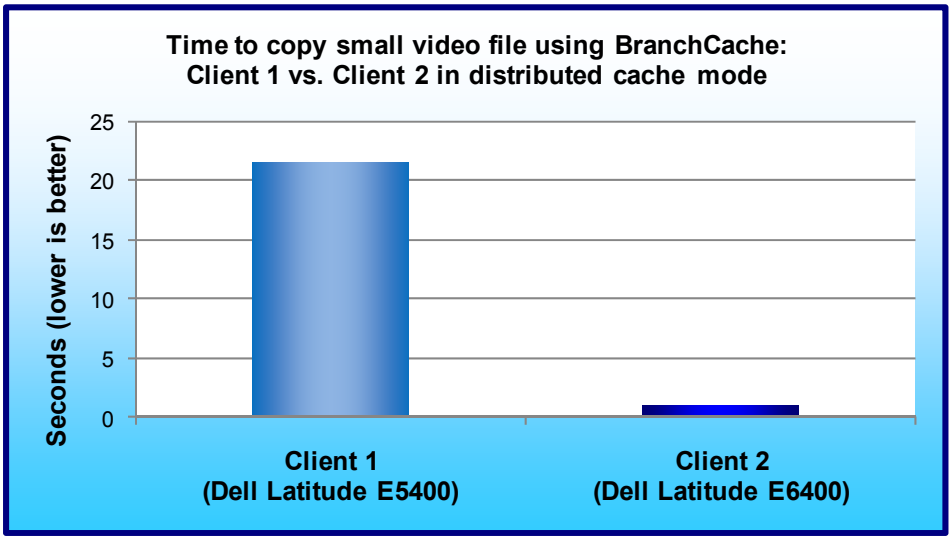

Figure 6: Time to copy small video file using BranchCache. Lower numbers, reflecting shorter times, are better.

Figure 6 shows the time to copy a small video file for two current Dell Latitude notebook system clients in a BranchCache distributed mode environment. The second client in our environment (Dell Latitude E6400) performed the task at a time savings of over 95 percent over the first client (Dell Latitude E5400)—over 20 seconds faster.

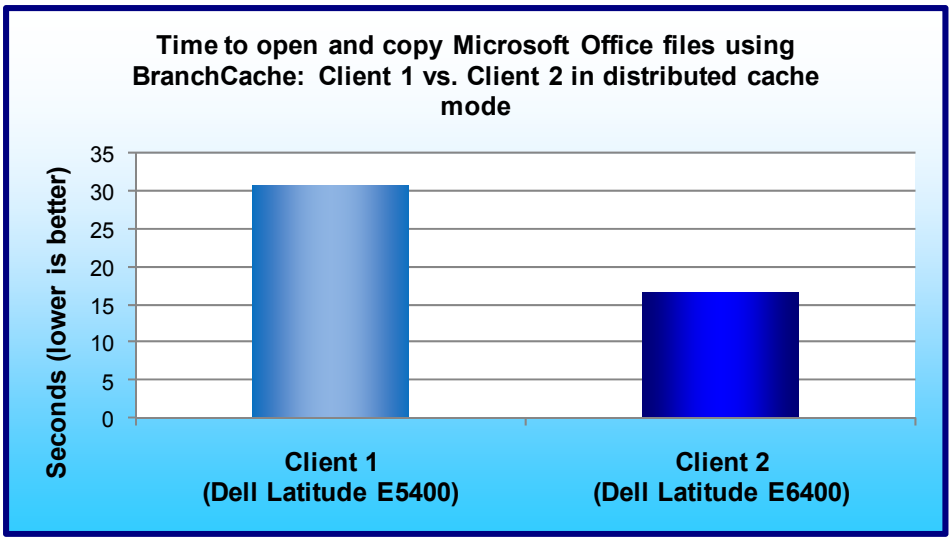

Figure 7 shows the time to open and copy Microsoft Office files for two current Dell Latitude notebook system clients in a BranchCache distributed mode environment. The second client in our environment (Dell Latitude E6400) performed the task at a time savings of over 45 percent over the first client (Dell Latitude E5400)—almost 14 seconds faster.

Figure 7: Time to open and copy Microsoft Office files using BranchCache. Lower numbers, reflecting shorter times, are better.

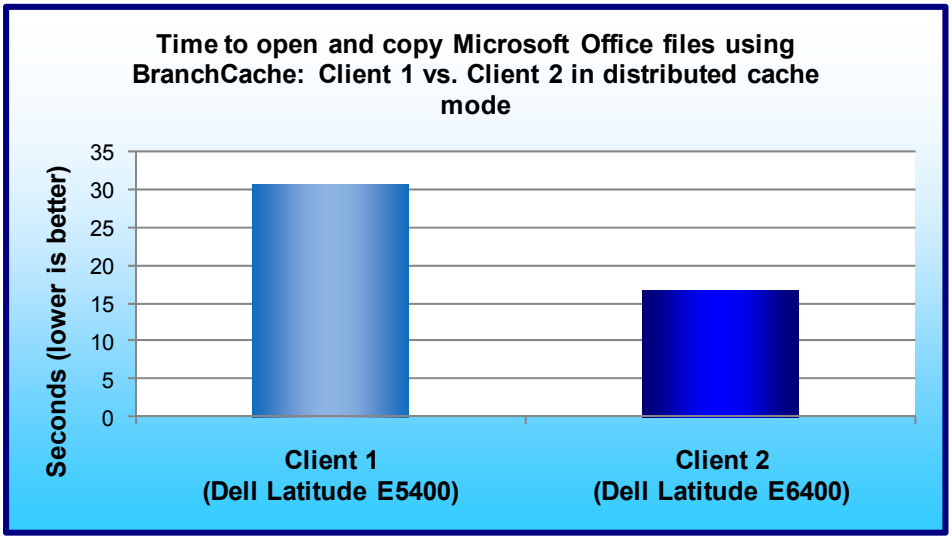

Figure 8 shows the time to open and copy PDF documents for two current Dell Latitude notebook system clients in a BranchCache distributed mode environment. The second client in our environment (Dell Latitude E6400) performed the task at a time savings of over 83 percent over the first client (Dell Latitude E5400)—over 8 seconds faster.

Figure 8: Time to open and copy PDF documents using BranchCache. Lower numbers, reflecting shorter times, are better.

Test methodology

In this section, we provide the methodology for three sets of tests: SYSmark 2007 Preview v.1.06, system responsiveness, and application responsiveness. For the application responsiveness and system responsiveness tests, we ran each test three times, taking the median of the three runs.

Measuring performance with BAPCo SYSmark 2007 Preview v1.06

Setting up the test

Prior to installing SYSmark 2007 Preview, we installed both Virtual PC RC and Virtual XP Mode. We installed all applicable Windows updates in Virtual XP Mode. We allocated the maximum amount of memory to Virtual XP Mode before installing and running SYSmark 2007 Preview.

1. Disable the User Account Control.
    a. Click Start→Control Panel.
    b. At the User Accounts and Family Safety settings screen, click Add or remove user account.
    c. At the User Account Control screen, click Continue.

d. Click Go to the main User Accounts page.
e. At the Make changes to your user account screen, click Turn User Account Control on or off.
f. At the User Account Control screen, click Continue.
g. Uncheck Use User Account Control to help protect your computer, and click OK.
h. At the You must restart your computer to apply these changes screen, click Restart Now.

2. Purchase and install SYSmark 2007 Preview v1.05 from https://www.bapcostore.com/store/product.php?productid=16165&cat=251&page=1.
3. At the Welcome to InstallShield Wizard screen, click Next.
4. At the License Agreement screen, select I accept the terms in the License Agreement, and click Next.
5. At the Choose Destination Location screen, click Next.
6. At the Ready to Install the Program screen, click Install.
7. When the installation is complete, click Finish.

Running the test

1. Launch SYSmark 2007 Preview by double-clicking the desktop icon.
2. Click Run.
3. Select Official Run, choose 3 Iterations, check the box beside run conditioning run, and enter a name for that run.
4. When the benchmark completes and the main SYSmark 2007 Preview menu appears, click Save FDR to create a report.
5. Record the results for each iteration.

Configuring the network infrastructure for the BranchCache, DirectAccess, and remote upgrade testing

Configuring the domain controller

The domain controller is a server running Windows Server 2008 R2 Enterprise Edition. This server is configured as a domain controller with Active Directory and acts as the DNS and DHCP server for the intranet subnet. It also serves as an enterprise root CA for the domain.

Installing the operating system

Install Windows Server 2008 R2 Enterprise Edition as a standalone server.

1. Start the installation of Windows Server 2008 R2.
2. Follow the instructions to complete the installation, specifying Windows Server 2008 R2 Enterprise Edition and a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect the network adapter to the Corpnet subnet.

Configuring TCP/IP on the domain controller

Configure the TCP/IP protocol with a static IP address of 10.0.0.1 and the subnet mask of 255.255.255.0.

1. In Initial Configuration Tasks, click Configure networking.
2. In Network Connections, right-click Local Area Connection, and click Properties.
3. Click Internet Protocol Version 4 (TCP/IPv4), and click Properties.
4. Select Use the following IP address, type `10.0.0.1` next to IP address, and type `255.255.255.0` next to Subnet mask.
5. Click Advanced, and click the DNS tab.
6. In DNS suffix for this connection, type `corp.catawba.com` click OK twice, and click Close.
7. Close the Network Connections window.
8. In Initial Configuration Tasks, click Provide computer name and domain.
9. In System Properties, click Change. In Computer name, type `DC1` click OK twice, and click Close. When the application prompts you to restart the computer, click Restart Now.
10. After restarting, log in using the local administrator account.
11. In Initial Configuration Tasks, click Do not show this window at logon, and click Close.

Configuring the server as a domain controller and DNS server

Configure the server as a domain controller and DNS server for the corp.catawba.com domain.

1. In the console tree of Server Manager, click Roles. In the details pane, click Add Roles, and click Next.
2. On the Select Server Roles page, click Active Directory Domain Services, click Add Required Features, click Next twice, and click Install. When installation is complete, click Close.
3. To start the Active Directory Installation Wizard, click Start, type `dcpromo`, and press Enter.
4. In the Active Directory Installation Wizard dialog box, click Next twice.
5. On the Choose a Deployment Configuration page, click Create a new domain in a new forest, and click Next.
6. On the Name the Forest Root Domain page, type `corp.catawba.com` and click Next.
7. On the Set Forest Functional Level page, in Forest Functional Level, click Windows Server 2008 R2, and click Next.
8. On the Additional Domain Controller Options page, click Next, click Yes to continue, and click Next.
9. On the Directory Services Restore Mode Administrator Password page, type a strong password twice, and click Next.
10. On the Summary page, click Next.
11. Wait while the wizard completes the configuration of Active Directory and DNS services, and click Finish.
12. When the application prompts you to restart the computer, click Restart Now.
13. After the computer restarts, log into the CORP domain using the Administrator account.

Installing and configuring DHCP on the domain controller

Configure DC1 as a DHCP server so that the test client can automatically configure itself when connecting to the Corpnet subnet.

1. In the console tree of Server Manager, click Roles.
2. In the details pane, under Roles Summary, click Add roles, and click Next.
3. On the Select Server Roles page, click DHCP Server, and click Next twice.
4. On the Select Network Connection Bindings page, verify that 10.0.0.1 is selected, and click Next.
5. On the Specify IPv4 DNS Server Settings page, verify that corp.catawba.com is listed under Parent domain.
6. Type `10.0.0.1` under Preferred DNS server IP address, and click Validate. Verify that the result returned is Valid, and click Next.
7. On the Specify WINS Server Settings page, accept the default setting of WINS is not required on this network, and click Next.
8. On the Add or Edit DHCP Scopes page, click Add.
9. In the Add Scope dialog box, type `Corpnet` next to Scope Name. Next to Starting IP Address, type `10.0.0.100` next to Ending IP Address, type `10.0.0.150`, next to Subnet Mask, type `255.255.255.0` Click OK, and click Next.
10. On the Configure DHCPv6 Stateless Mode page, select Disable DHCPv6 stateless mode for this server, and click Next.
11. On the Authorize DHCP Server page, select Use current credentials. Verify that CORP\Administrator is displayed next to User Name, and click Next.
12. On the Confirm Installation Selections page, click Install.
13. Verify the installation was successful, and click Close.

Creating DNS A records on the domain controller

Create DNS Address (A) records for the names crl.catawba.com and nls.corp.catawba.com.

1. Click Start, point to Administrative Tools, and click DNS.
2. In the console tree of DNS Manager, open DC1.
3. Right-click Forward Lookup Zones, click New Zone, and click Next.
4. On the Zone Type page, click Next.
5. On the Active Directory Zone Replication page, click Next.
6. On the Zone Name page, type `catawba.com` and click Next.
7. On the Dynamic Update page, click Allow both nonsecure and secure dynamic updates, click Next, and click Finish.
8. In the console tree, right-click catawba.com, and click New Host (A or AAAA).

9. In Name, type `crl` In IP address, type `10.0.0.2` Click Add Host, click OK, and click Done.
10. In the console tree, open corp.catawba.com.
11. Right-click corp.catawba.com, and click New Host (A or AAAA).
12. In Name, type `nls` In IP address, type `10.0.0.3` Click Add Host, click OK, and click Done.
13. Close the DNS Manager console.

Installing an enterprise root CA on the domain controller

Protected communication across the Internet between DirectAccess clients and servers requires computer certificates for IPsec-based authentication. In this step, install an enterprise root CA on DC1 to provide computer certificates for domain member computers.

1. In the console tree of Server Manager, click Roles.
2. Under Roles Summary, click Add roles, and click Next.
3. On the Select Server Roles page, click Active Directory Certificate Services, and click Next twice.
4. On the Role Services page, click Next.
5. On the Setup Type page, click Enterprise, and click Next.
6. On the CA Type page, click Root CA, and click Next.
7. On the Private Key page, click Create a new private key, and click Next.
8. On the Cryptography page, click Next.
9. On the CA Name page, click Next.
10. On the Validity Period page, click Next.
11. On the Certificate Database page, click Next.
12. On the Confirm Installation Selections page, click Install.
13. On the Results page, click Close.

Creating a user account in Active Directory

Create a user account in Active Directory that you will use when logging into CORP domain member computers.

1. Click Start, point to Administrative Tools, and click Active Directory Users and Computers.
2. In the console tree, open corp.catawba.com, right-click Users, point to New, and click User.
3. In the New Object - User dialog box, next to Full name, type `User1` for User, and in User logon name, type `User1`
4. Click Next.
5. In Password, type the password that you want to use for this account, and in Confirm password, type the password again.
6. Clear the User must change password at next logon check box, and select the Password never expires check box.
7. Click Next, and click Finish.
8. In the console tree, click Users.
9. In the details pane, double-click Domain Admins.
10. In the Domain Admins Properties dialog box, click the Members tab, and click Add.
11. Under Enter the object names to select (examples), type `User1` and click OK twice.
12. Leave the Active Directory Users and Computers console open for the following procedure.

Creating a security group for DirectAccess client computers

Create a security group that you will use to apply DirectAccess client computer settings to the member computers. The E6400 computer account will be part of this security group after joining the domain.

1. In the Active Directory Users and Computers console tree, right-click Users, point to New, and click Group.
2. In the New Object - Group dialog box, under Group name, type `DA_Clients`
3. Under Group scope, choose Global, under Group type, choose Security, and click OK.
4. Close the Active Directory Users and Computers console.

Creating and enabling a custom certificate template

Create a certificate template so that requesting computers can specify the subject name and subject alternative name of a certificate.

1. Click Start, type `mmc` and press Enter.

2. Click File, and click Add/Remove Snap-in.
3. In the list of snap-in, click Certificate Templates, click Add, and click OK.
4. In the console tree, open Certificates Templates.
5. In the contents pane, right-click the Web Server template, and click Duplicate Template.
6. Click Windows Server 2008 Enterprise, and click OK.
7. In Template display name, type `Web Server 2008`
8. Click the Security tab.
9. Click Authenticated Users, and select Enroll in the Allow column.
10. Click Add, type `Domain Computers` and click OK.
11. Click Domain Computers, and select Enroll in the Allow column.
12. Click the Request Handling tab.
13. Select Allow private key to be exported.
14. Click OK.
15. Close the MMC window without saving changes.
16. Click Start, point to Administrative Tools, and click Certification Authority.
17. In the console tree, expand corp-DC1-CA, right-click Certificate Templates, point to New, and click Certificate Template To Issue.
18. In the list of certificate templates, click Web Server 2008, and click OK.
19. Close the Certification Authority console.

Creating and enabling firewall rules for ICMPv4 and ICMPv6 traffic

Configure Windows Firewall with Advanced Security rules that allow inbound and outbound ICMPv4 and ICMPv6 Echo Request messages. These messages need to be sent and received to provide connectivity for Teredo-based DirectAccess clients.

1. Click Start, click Administrative Tools, and click Group Policy Management.
2. In the console tree, open Forest: Catawba.com\Domains\corp.catawba.com.
3. In the console tree, right-click Default Domain Policy, and click Edit.
4. In the console tree of the Group Policy Management Editor, open Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security.
5. In the console tree, right-click Inbound Rules, and click New Rule.
6. On the Rule Type page, click Custom, and click Next.
7. On the Program page, click Next.
8. On the Protocols and Ports page, for Protocol type, click ICMPv4, and click Customize.
9. In the Customize ICMP Settings dialog box, click Specific ICMP types, select Echo Request, and click OK.
10. Click Next.
11. On the Scope page, click Next.
12. On the Action page, click Next.
13. On the Profile page, click Next.
14. On the Name page, for Name, type `Inbound ICMPv4 Echo Requests` and click Finish.
15. In the console tree, right-click Inbound Rules, and click New Rule.
16. On the Rule Type page, click Custom, and click Next.
17. On the Program page, click Next.
18. On the Protocols and Ports page, for Protocol type, click ICMPv6, and click Customize.
19. In the Customize ICMP Settings dialog box, click Specific ICMP types, select Echo Request, and click OK.
20. Click Next.
21. On the Scope page, click Next.
22. On the Action page, click Next.
23. On the Profile page, click Next.
24. On the Name page, for Name, type `Inbound ICMPv6 Echo Requests` and click Finish.
25. In the console tree, right-click Outbound Rules, and click New Rule.
26. On the Rule Type page, click Custom, and click Next.
27. On the Program page, click Next.

28. On the Protocols and Ports page, for Protocol type, click ICMPv4, and click Customize.
29. In the Customize ICMP Settings dialog box, click Specific ICMP types, select Echo Request, and click OK.
30. Click Next.
31. On the Scope page, click Next.
32. On the Action page, click Allow the connection, and click Next.
33. On the Profile page, click Next.
34. On the Name page, for Name, type `Outbound ICMPv4 Echo Requests` and click Finish.
35. In the console tree, right-click Outbound Rules, and click New Rule.
36. On the Rule Type page, click Custom, and click Next.
37. On the Program page, click Next.
38. On the Protocols and Ports page, for Protocol type, click ICMPv6, and click Customize.
39. In the Customize ICMP Settings dialog box, click Specific ICMP types, select Echo Request, and click OK.
40. Click Next.
41. On the Scope page, click Next.
42. On the Action page, click Allow the connection, and click Next.
43. On the Profile page, click Next.
44. On the Name page, for Name, type `Outbound ICMPv6 Echo Requests` and click Finish.
45. Close the Group Policy Management Editor and Group Policy Management consoles.

Removing ISATAP from the DNS global block list

Configure the DNS Server service to remove the ISATAP name from its default global block list.

1. Click Start, click All Programs, click Accessories, right-click Command Prompt, and click Run as administrator.
2. In the Command Prompt window, type `dnscmd /config /globalqueryblocklist wpad` and press Enter.
3. Close the Command Prompt window.

Configuring CRL distribution settings

Configure the enterprise root CA with additional CRL distribution settings so that DirectAccess clients can check the CRL of certificates when connected to any of the test lab subnets.

1. Click Start, point to Administrative Tools, and click Certification Authority.
2. In the console tree, right-click corp-DC1-CA, and click Properties.
3. Click the Extensions tab, and click Add.
4. In Location, type `http://crl.catawba.com/crld/`
5. In Variable, click <CAName>, and click Insert.
6. In Variable, click <CRLNameSuffix>, and click Insert.
7. In Variable, click <DeltaCRLAllowed>, and click Insert.
8. In Location, type `.crl` at the end of the Location string, and click OK.
9. Select Include in CRLs. Clients use this to find Delta CRL locations and Include in the CDP extension of issued certificates, and click OK.
10. Click Add.
11. In Location, type `\\da1\crldist$\`
12. In Variable, click <CAName>, and click Insert.
13. In Variable, click <CRLNameSuffix>, and click Insert.
14. In Variable, click <DeltaCRLAllowed>, and click Insert.
15. In Location, type `.crl` at the end of the string, and click OK.
16. Select Publish CRLs to this location and Publish Delta CRLs to this location, and click OK.
17. Click Yes to restart Active Directory Certificate Services.
18. Close the Certification Authority console

Enabling computer certificate auto-enrollment

Configure the root CA so that Group Policy issues computer certificates automatically.

1. Click Start, click Administrative Tools, and click Group Policy Management.

2. In the console tree, open Forest: corp.catawba.com\Domains\corp.catawba.com.
3. In the console tree, right-click Default Domain Policy, and click Edit.
4. In the console tree of the Group Policy Management Editor, open Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies.
5. In the details pane, right-click Automatic Certificate Request Settings, point to New, and click Automatic Certificate Request.
6. In the Automatic Certificate Request Wizard, click Next.
7. On the Certificate Template page, click Computer, click Next, and click Finish.
8. Close the Group Policy Management Editor and Group Policy Management consoles.

Configuring the DirectAccess server

The DirectAccess server is a member server running Windows Server 2008 R2 configured with Internet Information Services (IIS).

Installing the operating system on the DirectAccess server

Install Windows Server 2008 R2 as a standalone server.

1. Start the installation of Windows Server 2008 R2.
2. Follow the instructions to complete the installation, specifying a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect one network adapter to the Corpnet subnet and the other to the Internet subnet.

Configuring TCP/IP properties on the DirectAccess server

Configure the TCP/IP protocol with static IP addresses on both interfaces.

1. In Initial Configuration Tasks, click Configure networking.
2. In Network Connections, right-click the network connection that is connected to the Corpnet subnet, and click Rename.
3. Type `Corpnet` and press Enter.
4. Right-click Corpnet, and click Properties.
5. Click Internet Protocol Version 4 (TCP/IPv4), and click Properties.
6. Select Use the following IP address. In IP address, type `10.0.0.2` In Subnet mask, type `255.255.255.0`
7. Select Use the following DNS server addresses. In Preferred DNS server, type `10.0.0.1`
8. Click Advanced, and then click the DNS tab.
9. In DNS suffix for this connection, type `corp.catawba.com` click OK twice, and click Close.
10. In the Network Connections window, right-click the network connection that is connected to the Internet subnet, and click Rename.
11. Type `Internet` and press Enter.
12. Right-click Internet, and click Properties.
13. Click Internet Protocol Version 4 (TCP/IPv4), and click Properties.
14. Select Use the following IP address. In IP address, type `131.107.0.2` In Subnet mask, type `255.255.255.0`
15. Click Advanced. On the IP Settings tab, click Add for IP Addresses.
16. In IP address, type `131.107.0.3` In Subnet mask, type `255.255.255.0` and click Add.
17. Click the DNS tab.
18. In DNS suffix for this connection, type `isp.example.com` and click OK three times.
19. Close the Network Connections window.
20. To check network communication between DA1 and DC1, click Start, click All Programs, click Accessories, and click Command Prompt.
21. In the Command Prompt window, type `ping dc1.corp.catawba.com`
22. Verify that there are four responses from 10.0.0.1.
23. Close the Command Prompt window.

Note: You need to configure two consecutive public IPv4 addresses on the DirectAccess server's Internet interface so that Teredo-based DirectAccess clients can detect the type of NAT that they are located behind (cone vs. symmetric).

Joining the DirectAccess server to the CORP domain

1. In Initial Configuration Tasks, click Provide Computer Name and Domain.
2. In the System Properties dialog box, on the Computer Name tab, click Change.
3. In Computer Name, type `DA1`. In Member of, click Domain, and type `corp.catawba.com`
4. Click OK.
5. When the application prompts you for a user name and password, type `User1` and its password, and click OK.
6. When you see a dialog box welcoming you to the corp.catawba.com domain, click OK.
7. When the application prompts you that you must restart the computer, click OK.
8. On the System Properties dialog box, click Close.
9. When the application prompts you to restart the computer, click Restart Now.
10. After the computer has restarted, click Switch User, click Other User, and log onto the CORP domain with the User1 account.
11. In Initial Configuration Tasks, click Do not show this window at logon, and click Close.

Installing the Web Server (IIS) role on the DirectAccess server

Install the Web Server (IIS) role to make the DirectAccess server a Web server. The DirectAccess server will host an external CRL so that remote DirectAccess clients can access a Web-based CRL distribution point for IP-HTTPS-based connections.

1. In the console tree of Server Manager, click Roles. In the details pane, click Add Roles, and click Next.
2. On the Select Server Roles page, click Web Server (IIS)**,** and click Next three times.
3. Click Install.
4. Verify that all installations were successful, and click Close.
5. Leave the Server Manager window open.

Creating a Web-based CRL distribution point

Create a Web-based CRL distribution point for DirectAccess clients.

1. Click Start, point to Administrative Tools, and click Internet Information Services (IIS) Manager.
2. In the console tree, open DA1, and Sites.
3. Right-click Default Web Site, and click Add virtual directory.
4. In Alias, type `CRLD`
5. In Physical path, click the ellipsis (…).
6. Click the drive on which Windows Server 2008 R2 is located, and click Make New Folder.
7. Type `CRLDist` press Enter, and click OK twice.
8. In the contents pane, double-click Directory Browsing.
9. In the Actions pane, click Enable.
10. In the console tree, click the CRLD folder.
11. In the contents pane, double-click Configuration Editor.
12. In Section, open system.webServer\security\authentication\requestFiltering.
13. In the contents pane, double-click allowDoubleEscaping to change it from False to True.
14. In the Actions pane, click Apply.
15. Close the Internet Information Services (IIS) Manager window.

Configuring permissions on the CRL distribution point file share

Configure the permissions on the CRLDist file share so that the Domain Controller (DC1) can write the CRL files.

1. Click Start, and click Computer.
2. Double-click the drive on which Windows Server 2008 R2 is located.
3. In the details pane, right-click the CRLDist folder, and click Properties.
4. Click the Sharing tab, and click Advanced Sharing.
5. Select Share this folder.
6. In Share name, add `$` to the end of the CRLDist name to hide the share, and click Permissions.
7. Click Add, and click Object Types.
8. Select Computers, and click OK.
9. In Enter the object names to select, type `DC1` and click OK.

10. In Group or user names, click the DC1 computer. In Permissions for DC1, click Full Control, and click OK twice.
11. Click the Security tab, and click Edit.
12. Click Add, and click Object Types.
13. Select Computers, and click OK.
14. In Enter the object names to select, type `DC1` and click OK.
15. In Group or user names, click the DC1 computer. In Permissions for DC1, click Full Control, click OK, and click Close.
16. Close the Local Disk window.

Publishing the CRL on the DirectAccess server (DA1)

Publish the CRL from the Domain Controller (DC1) and check for CRL files on the DirectAccess server (DA1).

1. On DC1, click Start, point to Administrative Tools, and click Certification Authority.
2. In the console tree, double-click corp-DC1-CA, right-click Revoked Certificates, point to All Tasks, and click Publish.
3. If the application prompts you to do so, click New CRL, and click OK.
4. Click Start, type `\\da1\crldist$` and press Enter.
5. In the crldist$ window, you should see two CRL files: corp-DC1-CA and corp-DC1-CA+.
6. Close the crldist$ window and the Certification Authority console.

Obtaining an additional certificate on the DirectAccess server (DA1)

Obtain an additional certificate for DA1 with a customized subject and alternative name for IP-HTTPS connectivity.

1. On DA1, click Start, type `mmc` and press Enter. Click Yes at the User Account Control prompt.
2. Click File, and click Add/Remove Snap-ins.
3. Click Certificates, click Add, click Computer account, click Next, select Local computer, click Finish, and click OK.
4. In the console tree of the Certificates snap-in, open Certificates (Local Computer)\Personal\Certificates.
5. Right-click Certificates, point to All Tasks, and click Request New Certificate.
6. Click Next twice.
7. On the Request Certificates page, click Web Server 2008, and click More information is required to enroll for this certificate.
8. On the Subject tab of the Certificate Properties dialog box, in Subject name, for Type, select Common Name.
9. In Value, type `da1.catawba.com` and click Add.
10. In Alternative name, for Type, select DNS.
11. In Value, type `da1.catawba.com` and click Add.
12. Click OK, click Enroll, and click Finish.
13. In the Details pane of the Certificates snap-in, verify that a new certificate with the name da1.catawba.com was enrolled with Intended Purposes of Server Authentication.
14. Right-click the certificate, and click Properties.
15. In Friendly Name, type `IP-HTTPS Certificate` and click OK.
16. Close the console window. If the application prompts you to save settings, click No.

Configuring the file server

The file server is a member server running Windows Server 2008 R2, and is configured with IIS.

Installing the operating system on the file server

1. Start the installation of Windows Server 2008 R2.
2. Follow the instructions to complete the installation, specifying a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect the network adapter to the Corpnet subnet.

Configuring TCP/IP properties on the file server

1. In Initial Configuration Tasks, click Configure networking.

2. In the Network Connections window, right-click Local Area Connection, and click Properties.
3. Click Internet Protocol Version 4 (TCP/IPv4), and click Properties.
4. Select Use the following IP address. In IP address, type `10.0.0.3` In Subnet mask, type `255.255.255.0`
5. Select Use the following DNS server addresses. In Preferred DNS server, type `10.0.0.1`
6. Click Advanced, and click the DNS tab. In DNS suffix for this connection, type `corp.catawba.com` click OK twice, and click Close.
7. Close the Network Connections window and leave the Initial Configuration Tasks window open.
8. To check name resolution and network communication between APP1 and DC1, click Start, click All Programs, click Accessories, and click Command Prompt.
9. In the Command Prompt window, type `ping dc1.corp.catawba.com`
10. Verify that there are four replies from 10.0.0.1.
11. Close the Command Prompt window.

Joining the file server to the CORP domain

1. In Initial Configuration Tasks, click Provide Computer Name and Domain.
2. In the System Properties dialog box, on the Computer Name tab, click Change.
3. In Computer Name, type `APP1` In Member of, click Domain, and type `corp.catawba.com`
4. Click OK.
5. When the application prompts you for a user name and password, type `User1` and its password, and click OK.
6. When you see a dialog box welcoming you to the corp.catawba.com domain, click OK.
7. When the application prompts you that you must restart the computer, click OK.
8. On the System Properties dialog box, click Close.
9. When the application prompts you to restart the computer, click Restart Now.
10. After the computer restarts, click Switch User, and click Other User and log onto the CORP domain with the User1 account.
11. In Initial Configuration Tasks, click Do not show this window at logon, and click Close.

Obtaining an additional certificate on the file server

Obtain an additional certificate with a customized subject and alternative name for network location.

1. Click Start, type `mmc` and press Enter.
2. Click File, and click Add/Remove Snap-in.
3. Click Certificates, click Add, select Computer account, click Next, select Local computer, click Finish, and click OK.
4. In the console tree of the Certificates snap-in, open Certificates (Local Computer)\Personal\Certificates.
5. Right-click Certificates, point to All Tasks, and click Request New Certificate.
6. Click Next twice.
7. On the Request Certificates page, click Web Server 2008, and click More information is required to enroll for this certificate.
8. On the Subject tab of the Certificate Properties dialog box, in Subject name, for Type, select Common Name.
9. In Value, type `nls.corp.catawba.com` and click Add.
10. In Alternative name, for Type, select DNS.
11. In Value, type `nls.corp.catawba.com` and click Add.
12. Click OK, click Enroll, and click Finish.
13. In the details pane of the Certificates snap-in, verify that a new certificate with the name nls.corp.catawba.com was enrolled with Intended Purposes of Server Authentication.
14. Close the console window. If the application prompts you to save settings, click No.

Installing the Web Server (IIS) role on the file server

Install the Web Server (IIS) role to make the file server a Web server.

1. In the console tree of Server Manager, click Roles. In the details pane, click Add Roles, and click Next.
2. On the Select Server Roles page, select the Web Server (IIS) check box, and click Next three times.
3. Click Install.

4. Verify that all installations were successful, and click Close.

Configuring the HTTPS security binding on the file server

Configure the HTTPS security binding so that the file server can act as the network location server.

1. Click Start, point to Administrative Tools, and click Internet Information Services (IIS) Manager.
2. In the console tree of Internet Information Services (IIS) Manager, open APP1/Sites, and click Default Web site.
3. In the Actions pane, click Bindings.
4. In the Site Bindings dialog box, click Add.
5. In the Add Site Binding dialog box, in the Type list, click https. In SSL Certificate, click the certificate with the name nls.corp.catawba.com. Click OK, and click Close.
6. Close the Internet Information Services (IIS) Manager console.

Creating a shared folder on the file server

Create a shared folder and a text file within the folder.

1. Click Start, and click Computer.
2. Double-click the drive on which Windows Server 2008 R2 is installed.
3. Click New Folder, type `Files` and press Enter. Leave the Local Disk window open.
4. Click Start, click All Programs, click Accessories, right-click Notepad, and click Run as administrator.
5. In the Untitled – Notepad window, type `This is a shared file`
6. Click File, click Save, double-click Computer, double-click the drive on which Windows Server 2008 R2 is installed, and double-click the Files folder.
7. In File name, type `Example.txt` and click Save. Close the Notepad window.
8. In the Local Disk window, right-click the Files folder, point to Share with, and click Specific people.
9. Click Share, and click Done.
10. Close the Local Disk window.

Configuring INET1

INET1 will run Windows Server 2008 R2 and it will host the Web Server (IIS), DNS, and DHCP server roles.

Installing the operating system on INET1

1. Start the installation of Windows Server 2008 R2.
2. Follow the instructions to complete the installation, specifying a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect the network adapter of INET1 to the Internet subnet.

Configuring TCP/IP properties on INET1

1. In Initial Configuration Tasks, click Configure networking.
2. In the Network Connections window, right-click Local Area Connection, and click Properties.
3. Click Internet Protocol Version 4 (TCP/IPv4), and click Properties.
4. Select Use the following IP address. In IP address, type `131.107.0.1` In Subnet mask, type `255.255.255.0`
5. Click Advanced, and click the DNS tab.
6. In DNS suffix for this connection, type `isp.example.com` and click OK.
7. Click OK, and click Close to close the Local Area Connection Properties dialog box.
8. Close the Network Connections window.
9. To check network communication between INET1 and DA1, click Start, click All Programs, click Accessories, and click Command Prompt.
10. In the Command Prompt window, type `ping 131.107.0.2`
11. Verify that there are four responses from 131.107.0.2.
12. Close the Command Prompt window.
13. Click Start, right-click Network, and click Properties.
14. In the Network and Sharing Center window, click Change advanced sharing settings.
15. In the Advanced sharing settings window, click Turn on file and printer sharing, and click Save changes.
16. Close the Network and Sharing Center window.

Renaming the computer

1. In Initial Configuration Tasks, click Provide Computer Name and Domain.
2. In the System Properties dialog box, on the Computer Name tab, click Change.
3. In Computer Name, type `INET1`
4. Click OK.
5. When the application prompts you that you must restart the computer, click OK.
6. On the System Properties dialog box, click Close.
7. When the application prompts you to restart the computer, click Restart Now.
8. After the computer has restarted, log on with the local Administrator account.
9. In Initial Configuration Tasks, click Do not show this window at logon, and click Close.

Installing the Web Server (IIS) and DNS server roles

Next, install role services for INET1, which will act as an Internet Web and DNS server for computers that are connected to the Internet subnet.

1. In Server Manager, under Roles Summary, click Add Roles, and click Next.
2. On the Select Server Roles page, select the Web Server (IIS) and DNS Server check boxes, and click Next.
3. Click Next twice to accept the default Web server settings, and click Install.
4. Verify that all installations were successful, and click Close.

Configuring NAT1

NAT1 will run Windows 7, and it will act as a NAT between the Internet and Homenet subnets. NAT1 configuration consists of the following steps:

Note: You must install two network adapters in NAT1.

Installing the operating system on NAT1

1. Connect one network adapter to the Internet subnet and the other network adapter to the Homenet subnet.
2. Start the installation of Windows 7.
3. When the application prompts you for a user name, type `User1` When the application prompts you for a computer name, type `NAT1`
4. When the application prompts you for a password, type a strong password twice.
5. When the application prompts you for protection settings, click Use recommended settings.
6. When the application prompts you for your computer's current location, click Public.

Configuring Network Connections properties

Next, configure the names of the adapters in the Network Connections folder for the subnets to which they are connected.

1. Click Start, and click Control Panel.
2. Under Network and Internet, click View status and tasks, and click Change adapter settings.
3. In the Network Connections window, right-click the network connection that is connected to the Homenet subnet, and click Rename.
4. Type `Homenet` and press Enter.
5. In the Network Connections window, right-click the network connection that is connected to the Internet subnet, and click Rename.
6. Type `Internet` and press Enter.
7. Leave the Network Connections window open for the next procedure.
8. Click Start, click All Programs, click Accessories, right-click Command Prompt, and click Run as administrator.
9. To check network communication between NAT1 and INET1, in the Command Prompt window, type `ping inet1.isp.example.com` and press Enter.
10. Verify that there are four responses from 131.107.0.1.

11. In the Command Prompt window, type `netsh interface 6to4 set state state=disabled` and press Enter.
12. Close the Command Prompt window.

Configuring Internet connection sharing

1. In the Network Connections window, right-click Internet, and click Properties.
2. Click the Sharing tab, select Allow other network users to connect through this computer's Internet connection, and click OK.

Configuring the Dell Latitude E6400

The Dell Latitude E6400 is running Windows 7 Ultimate and you will use it to demonstrate how DirectAccess works for remote computers.

Installing the operating system on E6400

1. Connect the Dell Latitude E6400 to the Corpnet subnet.
2. Start the installation of Windows 7 Ultimate.
3. When the application prompts you for a user name, type `User1` When the application prompts you for a computer name, type `E6400`
4. When the application prompts you for a password, type a strong password twice.
5. When the application prompts you for protection settings, click Use recommended settings.
6. When the application prompts you for your computer's current location, click Work.

User Account Control

When you configure the Windows 7 operating system, you are required to click Continue in the User Account Control (UAC) dialog box for some tasks. Several of the configuration tasks require UAC approval. When the application prompts you to do, always click Continue to authorize these changes.

Joining the Dell Latitude E6400 to the CORP domain

1. Click Start, right-click Computer, and click Properties.
2. Under Computer name, domain, and workgroup settings, click Change settings.
3. In the System Properties dialog box, click Change.
4. In the Computer Name/Domain Changes dialog box, click Domain, type `corp.catawba.com` and click OK.
5. When the application prompts you for a user name and password, type the user name and password for the User1 domain account, and click OK.
6. When you see a dialog box that welcomes you to the corp.catawba.com domain, click OK.
7. When you see a dialog box that prompts you to restart the computer, click OK.
8. In the System Properties dialog box, click Close.
9. In the dialog box that prompts you to restart the computer, do not click anything, and proceed to the following procedure.

Adding the Dell Latitude E6400 to the DA_Clients security group

Add the Dell Latitude E6400 to the DA_Clients security group so that it can receive DirectAccess client settings through Group Policy.

1. On DC1, click Start, point to Administrative Tools, and click Active Directory Users and Computers.
2. In the console tree, open corp.catawba.com, and Users.
3. In the Details pane, double-click DA_Clients.
4. In the DA_Clients Properties dialog box, click the Members tab, and click Add.
5. In the Select Users, Contacts, Computers, or Groups dialog box, click Object Types, click Computers, and click OK.
6. Under Enter the object names to select (examples), type `E6400` and click OK.
7. Verify that E6400 appears below Members, and click OK.
8. Close the Active Directory Users and Computers console.
9. On the the Dell Latitude E6400, in the dialog box that prompts you to restart the computer, click Restart Now.

10. After the Dell Latitude E6400 restarts, click Switch User, click Other User, and log onto the CORP domain with the User1 account.

Verifying the computer certificate on the Dell Latitude E6400

Verify that a computer certificate has been installed on the Dell Latitude E6400.

1. On the Dell Latitude E6400, click Start, type `mmc` and press Enter.
2. Click File, and click Add/Remove Snap-in.
3. Click Certificates, click Add, select Computer account, click Next, select Local computer, click Finish, and click OK.
4. In the console tree, open Certificates (Local Computer)\Personal\Certificates.
5. In the details pane, verify that a certificate was enrolled with Intended Purposes of Client Authentication and Server Authentication. This certificate will be used for authentication with DA1.
6. Close the console window. When the application prompts you to save settings, click No.

Testing access to intranet resources

Verify that the Dell Latitude E6400 can access intranet Web and file share resources on APP1.

1. From the taskbar, click the Internet Explorer® icon.
2. In the Welcome to Internet Explorer 8 window, click Next. In the Turn on Suggested Sites window, click No, don't turn on, and click Next. In the Choose your settings dialog box, click Use express settings, and click Finish.
3. In the Toolbar, click Tools, and click Internet Options. For Home page, click Use blank, and click OK.
4. In the Address bar, type `http://app1.corp.catawba.com/` and press Enter. You should see the default IIS 7 Web page for APP1.
5. Leave the Internet Explorer window open.
6. Click Start, type `\\app1\Files`,and press Enter.
7. You should see a folder window with the contents of the Files shared folder.
8. In the Files shared folder window, double-click the Example.txt file. You should see the contents of the Example.txt file.
9. Close the example.txt - Notepad and the Files shared folder windows.

Testing access to the network location server

Verify that E6400 can access the intranet network location server.

1. From the taskbar, click the Internet Explorer icon.
2. In the Address bar, type `https://nls.corp.catawba.com/` and press Enter. You should see the default IIS 7 Web page.
3. Close Internet Explorer.

Testing access to intranet resources from the Internet subnet

Connect E6400 to the Internet subnet and demonstrate that the Web and file share resources on APP1 are not accessible from the Internet.

1. Unplug the Ethernet cable of E6400 from the switch for the Corpnet subnet, and plug it into the switch for the Internet subnet.
2. From the taskbar, click the Internet Explorer icon.
3. In the Address bar, type `http://app1.corp.catawba.com/` and then press Enter. You should see the Internet Explorer cannot display the webpage message.
4. Close the Internet Explorer window.
5. Click Start, type `\\app1\Files` and press Enter.
6. You should see the Windows cannot access \\app1\files message. Click Cancel.
7. Unplug the Ethernet cable of E6400 from the switch for the Internet subnet and plug it into the switch for the Corpnet subnet.

Configuring DirectAccess

Use the following procedures to configure DirectAccess and verify the resulting intranet configuration:

Installing the DirectAccess feature on DA1

Before you can run the DirectAccess Setup Wizard, you must install the DirectAccess feature on DA1.

1. If needed, log onto DA1 with the User1 user account and password.
2. If needed, click Start, point to Administrative Tools, and click Server Manager.
3. In the main window, under Features Summary, click Add features
4. On the Select Features page, select DirectAccess Management Console.
5. In the Add Features Wizard window, click Add Required Features.
6. On the Select Features page, click Next.
7. On the Confirm Installation Selections page, click Install.
8. On the Installation Results page, click Close.

Running the DirectAccess Setup wizard on DA1

Run the DirectAccess Setup Wizard to configure DA1 and the Group Policy settings for DirectAccess clients.

1. Click Start, point to Administrative Tools, and click DirectAccess Management.
2. In the console tree, click Setup. In the details pane, click Configure for step 1.
3. On the DirectAccess Client Setup page, click Add.
4. In the Select Group dialog box, type `DA_Clients` click OK, and click Finish.
5. Click Configure for Step 2.
6. On the Connectivity page, for Interface connected to the Internet, select Internet. For Interface connected to the internal network, select Corpnet. Click Next.
7. On the Certificate Components page, for Select the root certificate to which remote client certificates must chain, click Browse. In the list of certificates, click the corp-DC1-CA root certificate, and click OK.
8. For Select the certificate that will be used to secure remote client connectivity over HTTPS, click Browse. In the list of certificates, click the certificate named IP-HTTPS Certificate, and click OK. Click Finish.
9. Click Configure for Step 3.
10. On the Location page, click Network Location server is run on a highly available server, type `https://nls.corp.catawba.com/` click Validate, and click Next.
11. On the DNS and Domain Controller page, note the entry for the name corp.catawba.com with the IPv6 address 2002:836b:2:1:0:5efe:10.0.0.1. This IPv6 address is assigned to DC1 and is composed of a 6to4 network prefix (2002:836b:2:1::/64) and an ISATAP-based interface identifier (::0:5efe:10.0.0.1). Click Next.
12. On the Management page, click Finish.
13. Click Configure for Step 4. On the DirectAccess Application Server Setup page, click Finish.
14. Click Save, and click Finish.
15. In the DirectAccess Review dialog box, click Apply. In the DirectAccess Policy Configuration message box, click OK. Click Start, point to Administrative Tools, and click DirectAccess Management.
16. In the console tree, click Setup. In the details pane, click Configure for step 1.
17. On the DirectAccess Client Setup page, click Add.
18. In the Select Group dialog box, type `DA_Clients` click OK, and click Finish.
19. Click Configure for Step 2.
20. On the Connectivity page, for Interface connected to the Internet, select Internet. For Interface connected to the internal network, select Corpnet. Click Next.
21. On the Certificate Components page, for Select the root certificate to which remote client certificates must chain, click Browse. In the list of certificates, click the corp-DC1-CA root certificate, and click OK.
22. For Select the certificate that will be used to secure remote client connectivity over HTTPS, click Browse. In the list of certificates, click the certificate named IP-HTTPS Certificate, and click OK. Click Finish.
23. Click Configure for Step 3.
24. On the Location page, click Network Location server is run on a highly available server, type `https://nls.corp.catawba.com/` click Validate, and click Next.
25. On the DNS and Domain Controller page, note the entry for the name corp.catawba.com with the IPv6 address 2002:836b:2:1:0:5efe:10.0.0.1. This IPv6 address is assigned to DC1 and is composed of a 6to4

network prefix (2002:836b:2:1::/64) and an ISATAP-based interface identifier (::0:5efe:10.0.0.1). Click Next.
26. On the Management page, click Finish.
27. Click Configure for step 4. On the DirectAccess Application Server Setup page, click Finish.
28. Click Save, and click Finish.
29. In the DirectAccess Review dialog box, click Apply. In the DirectAccess Policy Configuration message box, click OK.

Updating IPv6 settings on APP1

Force APP1 to refresh its IPv6 settings so that it can immediately configure itself as an ISATAP host.

1. On APP1, click Start, click All Programs, click Accessories, right-click Command Prompt, and click Run as administrator.
2. From the Command Prompt window, type `sc control iphlpsvc paramchange` and press Enter.
3. Close the Command Prompt window.

Updating IPv6 settings on DC1

Force DC1 to refresh its IPv6 settings so that it can immediately configure itself as an ISATAP host.

1. On DC1, click Start, click All Programs, click Accessories, right-click Command Prompt, and click Run as administrator.
2. From the Command Prompt window, type `sc control iphlpsvc paramchange` and press Enter.
3. Close the Command Prompt window.

Updating Group Policy and IPv6 settings on E6400

Force E6400 to update its Group Policy settings so that it is configured as a DirectAccess client, and immediately update its IPv6 settings so that it can configure itself as an ISATAP host.

1. On E6400, click Start, click All Programs, click Accessories, right-click Command Prompt, and click Run as administrator.
2. From the Command Prompt window, type `gpupdate` and press Enter.
3. From the Command Prompt window, type `sc control iphlpsvc paramchange`,and press Enter.
4. Leave the Command Prompt window open for the next procedure.

Verifying ISATAP-based connectivity

Verify that E6400 can connect to DC1 and APP1 by using IPv6 and ISATAP-based addresses.

1. On E6400, from the Command Prompt window, type `ipconfig /flushdns` and press Enter.
2. From the Command Prompt window, type `ping 2002:836b:2:1::5efe:10.0.0.1` and press Enter. This is the ISATAP-based address of DC1. You should see four successful replies.
3. From the Command Prompt window, type `ping 2002:836b:2:1::5efe:10.0.0.3` and press Enter. This is the ISATAP-based address of APP1. You should see four successful replies.
4. From the Command Prompt window, type `ping dc1.corp.catawba.com` and press Enter. You should see the name dc1.corp.catawba.com resolved to the IPv6 address 2002:836b:2:1::5efe:10.0.0.1 and four successful replies.
5. From the Command Prompt window, type `ping app1.corp.catawba.com` and press Enter. You should see the name app1.corp.catawba.com resolved to the IPv6 address 2002:836b:2:1::5efe:10.0.0.3 and four successful replies.
6. Leave the Command Prompt window open for the next procedure.

Verifying DirectAccess functionality for E6400 when connected to the Internet subnet

The following procedures verify DirectAccess functionality for E6400 when it is connected to the Internet subnet:

Connecting E6400 to the Internet subnet

This procedure simulates the roaming of E6400 from an intranet (the Corpnet subnet) to the Internet (the Internet subnet).

1. Unplug the Ethernet cable of E6400 from the switch for the Corpnet subnet, for Windows 7 Ultimate wait 15 seconds, and then plug it into the switch for the Internet subnet. Wait until the network icon in the notification area of the desktop displays a yellow caution sign.

2. To verify that the proper IPv4 address has been configured, from the Command Prompt window, type `ipconfig` and press Enter.
3. In the display of the Ipconfig.exe tool, verify that the interface named Local Area Connection has an IPv4 address that begins with 131.107.
4. Leave the Command Prompt window open for the next procedure.

Verifying connectivity to Internet resources

Verify that E6400 can use Internet DNS servers and access Internet resources.

1. From the Command Prompt window, type `ping inet1.isp.example.com` and press Enter.
2. You should see the name inet1.isp.example.com resolved to the IPv4 address 131.107.0.1 and four successful replies.
3. From the taskbar, click the Internet Explorer icon.
4. In the Address bar, type `http://inet1.isp.example.com/` and press Enter. You should see the default IIS 7 Web page for INET1.
5. Leave the Internet Explorer window open for the next procedure.

Verifying intranet access to Web and shared folder resources on APP1

Verify that E6400 can access intranet resources as if it was connected to the Corpnet subnet.

1. From the Command Prompt window, type `ping app1` and press Enter.
2. You should see the name app1.corp.catawba.com resolved to the IPv6 address 2001:836b:2:1:0:5efe:10.0.0.3 and four successful replies.
3. In Internet Explorer, in the Address bar, type `http://app1.corp.catawba.com/`,press Enter, and press b. You should see the default IIS 7 Web page for APP1.
4. Close Internet Explorer.
5. Click Start, type `\\app1\files` and press Enter. You should see a folder window with the contents of the Files shared folder.
6. In the Files shared folder window, double-click the Example.txt file.
7. Close the example.txt - Notepad window and the Files shared folder window.

Examining the E6400 IPv6 configuration

1. From the Command Prompt window, type `ipconfig` and press Enter.
2. From the display of the Ipconfig.exe tool, notice that an interface named Tunnel adapter 6TO4 Adapter has an IPv6 address that begins with 2002:836b:. This is a 6to4 address based on an IPv4 address that begins with 131.107. Notice that this tunnel interface has a default gateway of 2002:836b:2::836b:2, which corresponds to the 6to4 address of DA1 (131.107.0.2 in colon-hexadecimal notation is 836b:2). E6400 uses 6to4 and this default gateway to tunnel IPv6 traffic to DA1.

Verifying DirectAccess functionality for the E6400 when connected to the Homenet subnet

Connecting E6400 to the Homenet subnet

This procedure simulates the roaming of E6400 from the Internet (the Internet subnet) to a home network that is connected to the Internet (the Homenet subnet).

1. Unplug the Ethernet cable of E6400 from the switch for the Internet subnet, for Windows 7 Ultimate, wait 15 seconds, and plug it into the switch for the Homenet subnet. Wait until the network icon in the notification area of the desktop displays a yellow caution sign.
2. To verify that the proper IPv4 address has been configured, from the Command Prompt window, type `ipconfig` and press Enter.
3. In the display of the Ipconfig.exe tool, verify that the interface named Local Area Connection has an IPv4 address starting with 192.168.137.
4. Leave the Command Prompt window open for the next procedure.

Verifying connectivity to Internet resources

Verify that E6400 can use Internet DNS servers and access Internet resources.

1. From the Command Prompt window, type `ping inet1.isp.example.com` and press Enter.

2. You should see the name inet1.isp.example.com resolved to the IPv4 address 131.107.0.1 and four successful replies.
3. In the task bar, click the Internet Explorer icon.
4. In the Address bar, type `http://inet1.isp.example.com/` press Enter, and press F5. You should see the default IIS 7 Web page for INET1.
5. Leave the Internet Explorer window open for the next procedure.

Verifying intranet access to Web and shared folder resources on APP1

Verify that E6400 can access intranet resources as if it was connected to the Corpnet subnet.

1. In the Address bar of Internet Explorer, type `http://app1.corp.catawba.com/` and press Enter. You should see the default IIS 7 Web page for APP1.
2. Close Internet Explorer.
3. Click Start, type `\\app1\files` and press Enter.
4. You should see a folder window with the contents of the Files shared folder.
5. In the Files shared folder window, double-click the Example.txt file.
6. Close the example.txt - Notepad window and the Files shared folder window.

Examining the E6400 IPv6 configuration

Examine the IPv6 configuration of E6400.

1. From the Command Prompt window, type `ipconfig` and press Enter.
2. From the display of the Ipconfig.exe tool, notice that an interface has an IPv6 address that starts with 2001: This is a Teredo address assigned by DA1. When E6400 is behind a NAT that does not support 6to4 router functionality, E6400 uses Teredo to tunnel IPv6 traffic to DA1.
3. Leave the Command Prompt window open for the next procedure.

Disabling Teredo connectivity on E6400

This procedure simulates the roaming of E6400 from a home network to a private network with a Web proxy or firewall that does not forward Teredo traffic. In this environment, E6400 uses the IP-HTTPS protocol to connect to the DirectAccess server.

1. From the Command Prompt window, type `netsh interface teredo set state disabled` and press Enter.
2. Unplug the Ethernet cable of E6400 from the switch for the Homenet subnet, for Windows 7 Ultimate, wait 15 seconds, and plug it back into the switch for the Homenet subnet. Wait until the network icon in the notification area of the desktop displays a yellow caution sign.
3. From the Command Prompt window, type `ipconfig` and press Enter.
4. In the display of the Ipconfig.exe tool, verify that there is an interface named IPHTTPSinterface with an IPv6 address that starts with 2002:836b:2:2. This is an address DA1 assigns to the IP-HTTPS interface. When E6400 is behind a Web proxy or firewall that does not forward Teredo traffic, E6400 uses IP-HTTPS to tunnel IPv6 traffic to DA1.
5. Leave the Command Prompt window open for the next procedure.

Verifying intranet access to Web and file share resources on APP1

Verify that E6400 can access intranet resources as if it was connected to the Corpnet subnet.

1. In the Address bar, type `http://app1.corp.catawba.com/` press Enter, and press F5. You should see the default IIS 7 Web page for APP1.
2. Close Internet Explorer.
3. Click Start, type `\\app1\files` and press Enter.
4. You should see a folder window with the contents of the Files shared folder.
5. In the Files shared folder window, double-click the Example.txt file.
6. Close the example.txt - Notepad window and the Files shared folder window.

Enabling Teredo connectivity on E6400

In this procedure, you enable Teredo connectivity on E6400.

1. From the Command Prompt window, type `netsh interface teredo set state enterpriseclient` and press Enter.

2. From the Command Prompt window, type `ipconfig` and press Enter.
3. In the display of the Ipconfig.exe tool, verify that an interface has an IPv6 address that starts with 2001:.

Running the DirectAccess test

Connect E6400 to the Corpnet subnet to test intranet connectivity for the last time.

1. Unplug the Ethernet cable of E6400 from the switch for the Homenet subnet, and plug it into the switch for the Corpnet subnet.
2. For Windows 7 Ultimate, restart E6400.
3. Simultaneously log onto E6400 by using the User1 account and start the timer.
4. Browse to the network share.
5. Stop the timer when the shared resources appear in Windows Explorer.

Running the VPN test

1. For Windows 7 Ultimate, restart E6400.
2. Open Network and Sharing Center to monitor network connections.
3. Simultaneously select the network icon from the systray and start the timer.
4. Select VPN from the list of network connection options, and click the Connect button.
5. Open Windows Explorer when the VPN Connection appears in Network and Sharing Center.
6. Browse to the network share
7. Stop the timer when the shared resources appear in Windows Explorer.

BranchCache application responsiveness tests

Setting up the host file server to use BranchCache

We installed the BranchCache for Network Files role service of the File Services server role. We used the Group Policy Management Console to enable BranchCache for selected shares on the server.

Setting up the clients

We set up the two Dell Latitude notebook system clients in distributed cache mode, using the following command in an elevated command prompt: netsh branchcache set service mode=DISTRIBUTED.

Running the tests

We completed eight sets of application responsiveness tests: opening video files, copying video files, opening Word documents, copying Word documents, opening PowerPoint decks, copying PowerPoint decks, opening PDF documents, and copying PDF documents. Note: We ran each test on the first client one time, recording the first timed run. We ran each test on the second client six times, recording the last three timed runs.

Opening video files

1. Navigate to the network share on the host server.
2. Select the large video file.
3. Simultaneously select Play from the toolbar and start the timer.
4. Stop the timer when the first frame begins to play.
5. Select the small video file.
6. Simultaneously select Play from the toolbar and start the timer.
7. Stop the timer when the first frame begins to play.

Copying video files

1. Navigate to the network share on the host server.
2. Select the large video file.
3. Right-click and select Copy.
4. Right-click the desktop.
5. Simultaneously select Paste and start the timer.
6. Stop the timer when the copy operation is complete, as indicated by the disappearance of the copy status bar.
7. Select the small video file.
8. Right-click and select Copy.

9. Simultaneously select Paste and start the timer.
10. Stop the timer when the copy operation is complete, as indicated by the disappearance of the copy status bar.

Opening Word documents

1. Navigate to the network share on the host server.
2. Select the 3MB Word document.
3. Simultaneously select Open from the toolbar and start the timer.
4. Stop the timer when the document appears.
5. Select the 2MB Word document.
6. Simultaneously select Open from the toolbar and start the timer.
7. Stop the timer when the document appears.
8. Select the 80KB Word document.
9. Simultaneously select Open from the toolbar and start the timer.
10. Stop the timer when the document appears.

Copying Word documents

1. Navigate to the network share on the host server.
2. Select the 3MB Word document.
3. Right-click and select Copy.
4. Right-click the desktop.
5. Simultaneously select Paste and start the timer.
6. Stop the timer when the copy operation is complete, as indicated by the disappearance of the copy status bar.
7. Select the 2MB Word document.
8. Right-click and select Copy.
9. Right-click the desktop.
10. Simultaneously select Paste and start the timer.
11. Stop the timer when the copy operation is complete, as indicated by the disappearance of the copy status bar.
12. Select the 80KB Word document.
13. Right-click and select Copy.
14. Right-click the desktop.
15. Simultaneously select Paste and start the timer.
16. Stop the timer when the copy operation is complete, as indicated by the disappearance of the copy status bar.

Opening PowerPoint decks

1. Navigate to the network share on the host server.
2. Select the PowerPoint deck.
3. Simultaneously click Open from the toolbar and start the timer.
4. Stop the timer when the first slide appears.

Copying PowerPoint decks

1. Navigate to the network share on the host server.
2. Select the PowerPoint deck.
3. Right-click and select Copy.
4. Right-click the desktop.
5. Simultaneously select Paste and start the timer.
6. Stop the timer when the copy operation is complete, as indicated by the disappearance of the copy status bar.

Opening PDF documents

1. Navigate to the network share on the host server.
2. Select the PDF document.
3. Simultaneously click Open from the toolbar and start the timer.

4. Stop the timer when the PDF document appears.

Copying PDF documents

1. Navigate to the network share on the host server.
2. Select the PDF document.
3. Right-click and select Copy.
4. Right-click the desktop.
5. Simultaneously select Paste and start the timer.
6. Stop the timer when the copy operation is complete, as indicated by the disappearance of the copy status bar.

Remote upgrade test

To perform the remote upgrade from Microsoft Windows XP to Microsoft Windows 7 Ultimate, we installed and configured Microsoft System Center Configuration Manager 2007 SP2 on one of our member servers.

Running the Microsoft System Center Configuration Manager 2007 prerequisite checker

1. Insert the DVD.
2. When the menu appears, click Run the prerequisite checker.
3. Enter the name of the SQL server in the primary site field, leaving the instance name blank.
4. Resolve any problem(s) listed in the Installation Prerequisite Check dialog box, and re-run the prerequisite checker until all issues are resolved.

Installing Microsoft System Center Configuration Manager 2007

1. Insert the DVD.
2. When the menu appears, click Configuration Manager 2007 to install.
3. Review the Welcome screen, and click Next.
4. Select Install a Configuration Manager site server, and click Next.
5. Accept the license, and click Next.
6. Select Custom settings, and click Next.
7. Select No, I do not want to participate right now at the Customer Experience Improvement Program Configuration screen, and click Next.
8. Enter the product key, and click Next.
9. Accept the default installation destination folder, and click Next.
10. Enter the Site code and Site name at the Site Settings dialog box, and click Next.
11. Select Configuration Manager Mixed Mode at the Site Mode dialog box, and click Next.
12. Select all options available at the Client Agent Selection dialog box, and click Next.
13. Enter the SQL Server name and Configuration Manager database name, and click Next.
14. Specify the SMS provider settings, and click Next.
    Specify the Management point, and click Next.
15. Choose the TCP port settings, and click Next.
16. Check for updates and download newer versions, and click Next.
17. Create a local folder to store these updates if necessary, and click Next.
18. Download updates.
19. Once done, click OK to review the settings summary, and click Next to start the final prerequisite check.
20. After the final prerequisite check completes, click Begin Install.
21. Launch the configuration manager at the completion of the installation.

Adding SCCM server computer account to SMS groups

1. Start Active Directory users and computers, and sure that Advanced Features are enabled.
2. Select the Users option from the left pane, and in the right pane, scroll down to the SMS groups.

   Note: If you DO NOT see the SMS groups listed, do the following:
   - Log into Active Directory Users and Computers on the domain controller.
   - Enable advanced view.
   - Right-click Users, and choose New, Group:

    - make a new 'domain local' security group you call `SMS_SiteSystemToSiteServerConnection_WIN`
    - make a new domain local security group you call `SMS_SiteToSiteConnection_WIN`
  - Change WIN to your site code

3. Double-click SMS_SiteSystemToSiteServerConnection_WIN, and click the Members tab.
4. Click the Add button.
5. Click the Object Types button in the Select Users, Contacts, Computers, or Groups dialog box that opens.
6. Select Computers from the list of object types.
7. Click OK**,** followed by Advanced, and Find now**,** and scroll down until you see the server onto which you installed SCCM. Select it.
8. Click OK**,** click OK again, and click Apply to complete this action.
9. Double-click SMS_SiteToSiteConnection_Win.
10. Repeat steps 4 through 8.

Setting site boundaries and verifying that site name is configured for Active Directory

1. Launch the SCCM Configuration Manager Console console, expand Site settings, right-click the Boundaries node, and select New Boundary from the context menu.

   Note: You'll need to know the AD site name. By default, the AD site name is Default-First-Site-Name. You can change that in Active Directory sites and services if the site name is the same in both Active Directory and SCCM site boundaries

2. Select Active Directory site from the Type drop-down menu.
3. Click the Browse button, and select the Active Directory site name you configured earlier in AD sites and services.
4. Click the OK button to complete.
5. Click OK again to view the SCCM Site boundary set up in Configuration Manager Console.

Setting and configuring the site system roles

1. Launch Active Directory Users and Computers, and create the following two new Domain Users.
   - SMSadmin
   - SMSread
2. Launch the SCCM Configuration Manager Console.
3. Expand Site Settings and Site Systems, and click the SCCM Server name.
4. Right-click your server name, and choose New Roles.
5. Accept the defaults, and click Next.
6. Select Server Locator point, State Migration point, Reporting point, and Software update point from the list.
7. Click the red exclamation mark to input a path to store the SMP data, and click Next.
8. Accept the default report folder for the Reporting Point, and click Next.
9. At the Software Update Point dialog box, put a checkmark in Use this server as the active software update point, leaving the Sync source settings at the default settings, and click Next.
10. Accept the Synchronization source and schedule, and click Next.
11. At the Update classifications dialog box, choose the following: Critical Updates, Definition Updates, Security Updates, Service Packs, Update Rollups, and Updates. Click Next.
12. At the Products to update dialog box, choose Office, SQL, and Windows. Click Next.
13. Set English as the Language preference, and click Next.
14. Review the summary, and click Finish.
15. Click Close when the Site Role Wizard completes.

Configuring the Distribution Point (DP) and the Management Point (MP)

1. Launch the SCCM Configuration Manager Console, and highlight the SCCM server listed under site systems.

2. Double-click the Configuration Manager Console distribution point, and place a checkmark in the Allow clients to transfer content from this distribution point using BITS, HTTP, and HTTPS check box. Click OK.
3. Double-click the Configuration Manager Console Management Point to open its properties, put a check mark in the Allow devices to use this management point check box, and click Apply.

Making sure the System Management container in Active Directory has the correct permissions for SCCM

1. Start up the Active Directory Users and Computers console.
2. Make sure that Advanced Features are enabled under the View option.
3. Select System from the left pane, and scroll down to the System Management Container.
4. Right-click System Management Container, choose properties, and select the Security tab.
5. Verify the SCCM server account is listed in the Group or user names; if it is not there, add it by clicking on Add.
6. Click Object Types.
7. Select computers from the Object Types dialog box.
8. Click the OK button, the Advanced button to expand the view, and the Find Now button.
9. Highlight the server, and click the OK, button.
10. Click OK again to add it to the Security tab.
11. Click the Advanced button.
12. Highlight the server, and click the Edit button.
13. In the Permission Entry for System Management dialog that launches, click the drop-down menu called Apply onto: and select This object and all descendant objects.
14. Select Full Control for the Allow permissions, and select Apply these permissions to objects and /or containers within this container only. Click OK when you are finished.

Publishing this site in Active Directory Domain Services

1. In Configuration Manager, do the following:
    - Highlight your SCCM Site.
    - Right-click, choose properties, Advanced.
    - Select Publish this site in active directory domain services

Configuring Client Agents

1. Open the SCCM administrator console, and expand the site Management/site name/site settings.
2. Select Client Agents, and double-click Hardware Inventory Client Agent.
3. Click the Enable hardware inventory on clients check box if needed, and set the inventory schedule to 7 days.
4. Click Apply, and click OK.
5. Double-click Software Inventory Client Agent.
6. Click the Enable software inventory on clients check box if needed, and set the inventory schedule to 7 days.
7. Select the Inventory Collection tab, and delete the default scan listed.
8. Click the yellow star, and add files of type *.exe.
9. Click on Set…, and select the All client hard disks radio button.
10. Click Apply, and Click OK.
11. Double-click Advertised Programs Client Agent.
12. Click the Enable software distribution to clients check box if needed, and select New program notification icon opens Add or Remove Programs.
13. Select the Notification tab.
14. Click the Display a notification message check box.
15. Click Apply, and click OK.
16. Double-click Desired Configuration Management Agent.
17. Under the Simple schedule radio button, set the schedule to 7 days.
18. Click Apply, and click OK.
19. Double-click Remote Tools Client Agent.

20. Select the Users cannot change policy or notification settings in the Remote Control Control Panel check box.
21. Under the Remote Assistance tab, click the check box for both Configure unsolicited Remote Assistance settings and Configure solicited Remote Assistance Settings.
22. Under Remote Assistance settings, select Full Control for Level of access allowed.
23. Click Apply, and click OK.

Client Installation Methods

1. In the left pane of the SCCM administrator console, select Client Installation Methods.
2. Double-click Client Push Installation.
3. Click the Enable Client Push Installation to assigned resources check box.
4. Click the Workstations check box.
5. Click the Server check box.
6. Click the Domain controllers check box.
7. Click the Enable Client Push Installation to site systems check box.
8. Under the Accounts tab, click the yellow star and set the account to Administrator or a new user account, if desired.
9. Select the Client tab, and set the Installation Properties string to `SMSSITECODE=CON`
10. Click Apply, and click OK.

Configuring Discovery Methods

1. In the left pane of the SCCM administrator console, select Discovery Methods.
2. Select Heartbeat Discovery Properties.
3. Click the Enable Heartbeat Discovery check box, and set the schedule to 1 hour.
4. Click Apply, and click OK.
5. Select Active Directory System Group Discovery Properties.
6. Select Active Directory System Discovery Properties.
7. Click the Enable Active Directory System Discovery check box, and set the schedule to 1 hour.
8. Under the Polling Schedule tab, click the Run discovery as soon as possible check box.
9. Click the Schedule button, and set the Recurrence pattern to recur every 1 hour.
10. Under the Active Directory attribute tab, click the yellow star to add an Active Director container.
11. In the New Active Directory Container window, select the Local domain radio button.
12. Click OK, and when the Select New Container window appears, click OK again.
13. Click Apply, and click OK.

Migrating from Windows XP SP3 to Windows 7 Ultimate manually using Windows Easy Transfer

1. Insert the Windows 7 Ultimate DVD into the DVD drive.
2. Start the timer, and using Windows Explorer, browse to the DVD drive on your computer, and double-click migsetup.exe in the Support\Migwiz directory to launch the Windows Easy Transfer program.
3. Select the option for An external hard disk or USB flash drive, and select Next.
4. Select This is my old computer. Windows Easy Transfer scans the computer.
5. When scanning completes, customize your profile, and add/remove folders and files you want to include in the Shared Items list.
6. Click Next, and enter your password
7. Click Save and locate USB drive or Network location for saving Windows Easy Transfer files.
8. Start Windows 7 Setup by browsing to the root folder of the DVD in Windows Explorer and double clicking setup.exe.
9. Click Custom to perform an upgrade to your existing Windows installation.
10. Select the partition of Windows XP, and click Next.
11. Boot into your Windows 7 at the completion of installation.
12. Select Start→All Programs→Accessories→System Tools→Windows Easy Transfer.
13. Select An external hard disk or USB flash drive.
14. Select This is my new computer.
15. Select Yes, open the file.

16. Browse to the location in which you saved the Easy Transfer file in Step 7. Select the file, and select Open.
17. Select Transfer to transfer all files and settings, or select custom settings and files by clicking Customize.
18. Select Close after Windows Easy Transfer completes moving your files.
19. Install Windows 7 drivers, if available, from Dell's web site.
20. Run Windows Updates, and install all updates through 10/22/2009
21. Insert Office 2007 Enterprise Edition DVD.
22. Select Setup from the Autoplay dialog box.
23. Click the Install button,
24. When the Office 2007 installation completes, install Service Pack 2.
25. Stop the timer.

Appendix A – Detailed system configuration information

Figure 9 presents detailed system configuration for the two current Dell Latitude notebooks.

Dell Latitude notebook systems	Dell Latitude E6400	Dell Latitude E5400
General		
Processor and OS kernel: (physical, core, logical) / (UP, MP)	1P,1C,2L / MP	1P,1C,2L / MP
System power management policy Windows 7	Dell Mobile Battery Methodology	Dell Mobile Battery Methodology
Processor power-saving option	EIST	EIST
System dimensions (length x width x height)	13.25" x 9.6" x 1.25"	13.4" x 9.6" x 1.6"
System weight	5 lbs. 2 oz.	5 lbs. 10 oz.
CPU		
Vendor	Intel	Intel
Name	Core 2 Duo	Core 2 Duo
Model number	P8700	T7250
Stepping	R0	M0
Socket type and number of pins	Socket P (478)	Socket P (478)
Core frequency (GHz)	2.53	2.00
Front-side bus frequency (MHz)	1,066	800
L1 cache	32 KB + 32 KB (per core)	32 KB + 32 KB (per core)
L2 cache (MB)	3	2
Platform		
Vendor	Dell	Dell
Motherboard model number	0W620R	0D695C
Motherboard chipset	Intel GM45	Intel GM45
Motherboard revision number	07	07
System/motherboard serial number	JBCWTK1	6NJ1VK1
BIOS name and version	Dell A15 (07/31/2009)	Dell A13 (08/11/2009)
BIOS settings	Default	Default
Memory module(s)		
Vendor and model number	Nanya NT1GT64UH8D0FN-AD	Nanya NT1GT64UH8D0FN-AD
Type	PC2-6400	PC2-6400
Speed (MHz)	800	800
Speed running in the system (MHz)	800	800
Timing/Latency (tCL-tRCD-tRP-tRASmin)	6-6-6-18	6-6-6-18
Size (MB)	2,048	2,048
Number of memory module(s)	2	2
Channel (single/dual)	Dual	Dual
Hard disk		
Vendor and model number	Seagate ST980313AS	Seagate ST9120312AS
Size (GB)	80	120
Buffer size (MB)	8	8
RPM	5,400	5,400
Type	SATA 3.0 Gb/s	SATA 3.0 Gb/s
Controller	Intel 82801IM (ICH9-M)	Intel 82801IM (ICH9-M)
Driver Windows XP	Intel 8.8.0.1009 (02/11/2009)	Intel 8.8.0.1009 (02/11/2009)
Driver Windows Vista	Intel 8.8.0.1009 (02/11/2009)	Intel 8.8.0.1009 (02/11/2009)

Dell Latitude notebook systems	Dell Latitude E6400	Dell Latitude E5400
Driver Windows 7	Intel 8.9.2.1002 (08/07/2009)	Intel 8.9.2.1002 (08/07/2009)
Operating system		
Name	Microsoft Windows 7 Ultimate	Microsoft Windows 7 Ultimate
Build number	7600	7600
Service pack	NA	NA
File system	NTFS	NTFS
Kernel	ACPI x86-based PC	ACPI x86-based PC
Language	English	English
Microsoft DirectX version	11	11
Graphics		
Vendor and model number	Mobile Intel GMA 4500MHD	Mobile Intel GMA X4500HD
Type	Integrated	Integrated
Chipset	Mobile Intel 4 Series Express Chipset	Mobile Intel 4 Series Express Chipset
BIOS version	1659.0	1659.0
Total available graphics memory (MB)	743	776
Dedicated video memory (MB)	32	32
System video memory (MB)	32	96
Shared system memory (MB)	679	648
Driver Windows XP	Intel 6.14.10.5082 (06/25/2009)	1,024 x 768 x 32 bit
Driver Windows Vista	Intel 7.15.10.1861 (07/31/2009)	Intel 6.14.10.5082 (06/25/2009)
Driver Windows 7	Intel 8.15.10.1855 (07/28/2009)	Intel 7.15.10.1861 (07/31/2009)
Driver Windows XP	Intel 6.14.10.5082 (06/25/2009)	Intel 8.15.10.1855 (07/28/2009)
Sound card/subsystem		
Vendor and model number	IDT High Definition Audio CODEC, Intel High Definition Audio HDMI	IDT High Definition Audio CODEC, Intel High Definition Audio HDMI
Driver Windows XP	IDT 5.10.5607.0 (09/05/2007), Intel 5.10.1.1048 (12/05/2008)	IDT 5.10.5607.0 (09/05/2007), Intel 5.10.1.1048 (12/05/2008)
Driver Windows Vista	Microsoft 6.0.6002.18005 (06/21/2006), Intel 6.10.1.2077 (07/10/2009)	Microsoft 6.0.6002.18005 (06/21/2006), Intel 6.10.1.2077 (07/10/2009)
Driver Windows 7	Microsoft 6.1.7600.16385 (07/13/2009), Intel 6.10.1.2073 (05/26/2009)	Microsoft 6.1.7600.16385 (07/13/2009), Intel 6.10.1.2073 (05/26/2009)
Ethernet		
Vendor and model number	Intel 82567LM Gigabit	Broadcom NetXtreme 57xx Gigabit
Driver Windows XP	Intel 9.50.14.2 (04/04/2008)	Broadcom 11.7.2.0 (11/26/2008)
Driver Windows Vista	Intel 9.50.14.2 (04/04/2008)	Broadcom 11.7.2.0 (10/22/2008)
Driver Windows 7	Intel 10.0.6.0 (06/12/2009)	Microsoft 10.100.4.0 (04/26/2009)
Wireless		
Vendor and model number	Intel 5100 AGN	Dell Wireless 1397 WLAN Mini-Card
Driver Windows 7	Intel 12.4.1.11 (05/14/2009)	Broadcom 5.30.21.0 (07/07/2009)

Dell Latitude notebook systems	Dell Latitude E6400	Dell Latitude E5400
Bluetooth		
Vendor and model number	NA	NA
Driver Windows 7	NA	NA
Modem		
Vendor and model number	NA	NA
Driver Windows 7	NA	NA
Optical drive(s)		
Vendor and model number	Matshita UJ862A	LG GT10N
Type	DVD-RW	DVD-RW
Interface	SATA	SATA
Dual/Single layer	Dual	Dual
USB ports		
Number	4	4
Type	USB 2.0	USB 2.0
Other	Media card reader	Media card reader
IEEE 1394 ports		
Number	1 (4-pin)	1 (4-pin)
Monitor		
LCD type	WXGA	WXGA
Screen size	14.1"	14.1"
Refresh rate (Hz)	60	60
Power Adapter		
Type	Dell DA90PE1-00 90W	Dell DA90PE1-00 90W
Battery life		
Type	Dell PT434 lithium-ion	Dell KM742 lithium-ion
Size (length x width x height)	8.25" x 2" x .80"	8.10" x 2" x .75"
Rated capacity	5050 mAh / 11.1V (56Wh)	5050 mAh / 11.1V (56Wh)
Weight (oz)	11	11

Figure 9. Detailed system configuration for the two current Dell Latitude notebooks.

Appendix B – Detailed BranchCache application responsiveness results

Figure 10 presents the detailed test results for the systems.

Previous generation desktop systems	Client 1 – Dell Latitude E5400	Client 2 – Dell Latitude E6400
Operating system	**Windows 7 Ultimate**	**Windows 7 Ultimate**
Application responsiveness		
Test case 1: Opening video files		
Large video file begins playing - median	00:05.15	00:01.19
Small video file begins playing - median	00:01.78	00:01.34
Test case 2: Copying video files		
Large video file copy complete - median	02:43.63	00:11.84
Small video file copy complete - median	00:21.44	00:00.98
Test case 3: Opening Word documents		
3MB Word document appears - median	00:07.07	00:05.01
2MB Word document appears - median	00:08.79	00:06.21
80KB Word document appears - median	00:03.88	00:01.84
Test case 4: Copying Word documents		
3MB Word document copy complete - median	00:02.67	00:00.65
2MB Word document copy complete - median	00:01.22	00:00.65
80KB Word document copy complete - median	00:01.09	00:00.58
Test case 5: Opening PowerPoint decks		
First PowerPoint slide appears - median	00:05.15	00:01.19
Test case 6: Copying PowerPoint decks		
PowerPoint deck copy complete - median	00:00.79	00:00.61
Test case 7: Opening PDF documents		
PDF document appears - median	00:08.61	00:01.11
Test case 8: Copying PDF documents		
PDF copy complete - median	00:01.23	00:00.56

Figure 10: Detailed test results for the two current Dell Latitude notebook system clients in BranchCache distributed cache mode.

Appendix C – Detailed VPN connection results

Figure 11 presents the detailed test results for the systems.

Test system	Dell Latitude E6400
Connecting via a VPN	
Connecting to a network share – Run 1	00:54.44
Connecting to a network share – Run 2	00:54.78
Connecting to a network share – Run 3	00:52.64

Figure 11: Detailed test results for the Dell Latitude E6400notebook system connecting to a test network using a conventional VPN connection.

About Principled Technologies

We provide industry-leading technology assessment and fact-based marketing services. We bring to every assignment extensive experience with and expertise in all aspects of technology testing and analysis, from researching new technologies, to developing new methodologies, to testing with existing and new tools.
When the assessment is complete, we know how to present the results to a broad range of target audiences. We provide our clients with the materials they need, from market-focused data to use in their own collateral to custom sales aids, such as test reports, performance assessments, and white papers. Every document reflects the results of our trusted independent analysis.

We provide customized services that focus on our clients' individual requirements. Whether the technology involves hardware, software, Web sites, or services, we offer the experience, expertise, and tools to help you assess how it will fare against its competition, its performance, whether it's ready to go to market, and its quality and reliability.

Our founders, Mark L. Van Name and Bill Catchings, have worked together in technology assessment for over 20 years. As journalists, they published over a thousand articles on a wide array of technology subjects. They created and led the Ziff-Davis Benchmark Operation, which developed such industry-standard benchmarks as Ziff Davis Media's Winstone and WebBench. They founded and led eTesting Labs, and after the acquisition of that company by Lionbridge Technologies were the head and CTO of VeriTest.

Principled Technologies, Inc.
1007 Slater Road, Suite 250
Durham, NC 27703
www.principledtechnologies.com
info@principledtechnologies.com