

Branch Office Infrastructure Solution

Architecture Guide

Version 3.0

Published: February 2008

Revised: September 2008

For the latest information, please see
microsoft.com/**BranchOffice**

Copyright © 2008 Microsoft Corporation. All rights reserved. Complying with the applicable copyright laws is your responsibility. By using or providing feedback on this documentation, you agree to the license agreement below.

If you are using this documentation solely for non-commercial purposes internally within YOUR company or organization, then this documentation is licensed to you under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/2.5/ or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS". Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation. Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Active Directory Domain Services, Internet Security and Acceleration Server, Office Visio 2007, System Center Configuration Manager 2007, Virtual Server 2005, Windows Server 2003, Windows Server 2008, Windows Server 2008 Hyper-V , Windows SharePoint Service, and windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback. You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

[Branch Infrastructure Architecture 1](#_Toc209810514)

[Goals and Objectives 1](#_Toc209810515)

[Audience 1](#_Toc209810516)

[Branch Office Logical Design 2](#_Toc209810517)

[Branch Services Design 2](#_Toc209810518)

[Base Services 2](#_Toc209810519)

[Extended Services 3](#_Toc209810520)

[Branch Infrastructure Environment 4](#_Toc209810521)

[Service Placement Approaches 5](#_Toc209810522)

[Centralized 6](#_Toc209810523)

[Distributed 7](#_Toc209810524)

[Hybrid 8](#_Toc209810525)

[Service Placement Considerations 10](#_Toc209810526)

[Service Provisioning 12](#_Toc209810527)

[Appliance Form Factor 12](#_Toc209810528)

[General Purpose Server Form Factor 13](#_Toc209810529)

[Operating System Configuration 14](#_Toc209810530)

[Single Operating System per Server 14](#_Toc209810531)

[Multiple Operating Systems per Server 14](#_Toc209810532)

[Branch Infrastructure Physical Design 15](#_Toc209810533)

[Physical Network Structure 17](#_Toc209810534)

[WAN Connections 18](#_Toc209810535)

[Link Characteristics 18](#_Toc209810536)

[Network Link Scenarios 20](#_Toc209810537)

[Network Segmentation in the Branch Site 21](#_Toc209810538)

[Other Network Design Considerations 21](#_Toc209810539)

[Security Considerations 22](#_Toc209810540)

[Management Considerations 23](#_Toc209810541)

[Summary 24](#_Toc209810542)

[Additional Resources 25](#_Toc209810543)

[Feedback 25](#_Toc209810544)

# Branch Infrastructure Architecture

For many years, designing IT infrastructures to support branch sites has been a challenging task. The complexities introduced by the limitations in available network latency, bandwidth, performance issues, and geographic separation, have a significant impact on an organization’s ability to implement an appropriate single IT solution for all of its sites. As wide area network (WAN) bandwidth and performance grows, client and server technologies are also introduced (or enhanced) to support branch operations better, and the situation continues to improve. However, there will always be a fundamental difference in the design for a geographically distributed IT infrastructure and the design for a single site, because branch sites introduce a number of significant constraints that modify the options that are available to solution designers.

This guide updates the architecture approach that was taken in Chapter 2 of the “Branch Office Infrastructure Solution for Microsoft Windows Server 2003 Release 2” guide, and specifically deals with the changes that were introduced by the Windows® Vista® operating system and the Windows Server® 2008 operating system. Although the fundamental architectural principles in this guide remain very similar, the technologies and capabilities have moved on. This guide provides the necessary updates to ensure your branch infrastructure designs take advantage of the latest technical approaches.

## Goals and Objectives

This guide introduces a method of designing a service-based branch infrastructure design. The branch environment is typically part of a larger network that supports an organization's main sites and data centers. However, branch sites introduce a number of significant constraints that modify the options that are available to solution designers. This guide explains how to look at the specific requirements of the branch office within the larger context of an organization's IT services.

## Audience

The primary audience for this guide is the experienced Infrastructure Architect or IT professional who is responsible for designing one or more of the services that are included in a branch infrastructure. A branch infrastructure consists of many services and applications, so a single individual may not have all of the skill sets that are required to design a branch infrastructure solution.

Instead, the design process usually requires a design team. Together, the design team members must have a good working knowledge of all of the core technologies that are required in a branch infrastructure design, including the following:

* The Windows Server and client operating system platforms
* N-Tier client/server architecture
* Limited bandwidth networking and connectivity environments
* Service operations and business requirements
* Reliability, availability, security, performance, compatibility, and other hardware and software management concepts
* The infrastructure services and technologies that are described in this solution Software distribution and update management services and products
* Backup and recovery techniques and tools
* Automation tools
* Virtual machine concepts and processes

# Branch Office Logical Design

Before going into the physical designs for branch sites, it is important to understand that a number of logical approaches ultimately govern your physical design. You should consider the logical approaches to the designs for each service in your architecture. This section looks at the logical structure and taxonomy of providing services that function at the required level in a remotely distributed environment.

## Branch Services Design

An extensive range of services is required in an organization's infrastructure. The key to a successful branch infrastructure design is to determine which of these services are required in the branch site and how they should be placed to meet the requirements of the branch users.

To help manage the scope of your design process, you may find it helpful to categorize the services that are provided to the branch sites. The previous version of this guide focused on two basic tiers of services, *core* and *extended*. The primary purpose of the categorization is to help you to identify and standardize on the services that form the minimum service requirements for all of the branch sites in your organization. If you can standardize on these services you will make a significant step towards simplifying the complexities of a branch infrastructure.

With the introduction of the Server Core Edition of Windows Server 2008, Microsoft has updated the terminology to help reduce the possibility of confusion between services that provide *core branch site services* and services that are available on the Server Core edition of Windows Server 2008.

This guide refers to two categories of services: *base* and *extended.*

### Base Services

Base services provide the fundamental infrastructure services that support the IT infrastructure of an organization and other specialized extended services support business functions or revenue generating activities. Base service, in this context, does not imply an inferior service; base services simply provide the most basic functionality to the branch infrastructure. In the Branch Office Infrastructure Solution (BOIS), the following services are identified as basic:

* **Directory services**. The authentication service for BOIS is Active Directory® Domain Services. AD DS in Windows Server 2008 includes improvements to help you deploy AD DS more simply and securely. For example, AD DS includes a new type of domain controller called a read-only domain controller (RODC). RODCs provide a way for you to deploy domain controllers in scenarios in which physical security cannot be guaranteed, such as branch sites.
* **DHCP services**. Dynamic Host Configuration Protocol (DHCP) provides the TCP/IP address allocation service to the network. Windows Server 2008-based DHCP servers can automatically provide client computers and devices with TCP/IPv4 and IPv6 based IP addresses.
* **Name resolution services**. Domain Name System (DNS) is the primary address resolution service for the TCP/IP protocol and the Windows platform. The Windows Internet Name Service (WINS) design process has also been documented, because this may be required to support the legacy NetBIOS naming service.
* **File services**. These services provide technologies that help manage storage, enable file replication, manage shared folders, and ensure fast file searching. You can use Windows Server 2008 to provide Distributed file system (DFS) Replication services that can replicate data between DFS Namespaces and sites in the branch environment.
* **Print services**. These services provide the printing and printer features for the branch design. You can use the Print Management snap-in to monitor print queues and receive notifications when print queues stop processing print jobs. It also enables you to migrate print servers and deploy printer connections by using Group Policy.
* **Base client services**. These services provide a minimum level of client computer-based services. These services can include technologies such as Windows Vista Folder Redirection and Offline Files, malware defense settings and tools to help protect the client from malware, and client-based remote control services.
* **Base management services**. These services provide a minimum acceptable management service for the branch sites. The services selected for the BOIS are update services, monitoring services, and backup and recovery services.

The services identified here represent a collection of services that provide a minimum acceptable level for the features of a branch infrastructure environment. You can review and modify this service listing at any time to meet the needs of your organization.

### Extended Services

Typically, base services do not provide specific customer or end-user services; however, extended services do provide these services. The list of extended services varies greatly from organization to organization. Examples of common extended services include:

* **Application services**. These services provide line-of-business applications for the organization. There are a number of technologies that you can use to support an application in a branch office environment, including support for a distributed client base as part of the application's original design requirements.
* **Web caching**. This service aims to optimize the Internet access experience for branch office users and to provide an additional layer of protection by using proxy services in the design.
* **Messaging services**. This is the provision of e-mail services for an organization and includes both the internal e-mail and gateway services to the Internet.
* **Collaboration services**. Web-based collaborations services such as Windows SharePoint® Services provide this extended service.
* **Extended management services**. With the addition of a specialized management solution, such as Microsoft® System Center Configuration Manager 2007, you can improve on the basic management functionality and include assessment, deployment, and update management for your branch applications, servers, clients, and devices.
* **Extended monitoring services**. This is the provision of a specialized monitoring solution, such as Microsoft® System Center Operations Manager 2007. Using a solution like this you can greatly enhance your ability to improve upon basic branch management functionality and include assessment, deployment, and update management for your branch applications, servers, clients, and devices.
* **Branch network access services**. This is a collection of technologies such as Network Access Protection, Server and Domain Isolation and Rights Management Services. These services are especially relevant in cases of branch site as their distributed nature can pose a higher risk compared to central hub sites.

You can extend this list to cover the wide range of other services that you want to provide to your organization. These and other key services have been selected as part of the BOIS scope to help you to deal with common services in a typical environment. For the most up-to-date list of extended services that are available for the BOIS, please see http://[www.microsoft.com/branchoffice](http://www.microsoft.com/branchoffice).

When you have identified the services that are required for your organization, it is usually very beneficial to create a visual representation of those services that will help you to communicate those services to other people in your organization. For example, the Microsoft Office Visio® 2007 stencil templates that are provided with these guides provide a visual representation of the services that are illustrated in Figure 1.



Figure 1. Branch logical services view

This figure shows the services without any representation of the underlying physical instantiation of the design. This is a key level of abstraction that needs to be understood, because a service may be illustrated as a single computer but may well be provided by a number of computers in the final design. At this stage, the requirements of the overall design are not necessarily understood enough to determine the physical requirements of the solution. Only after you have considered the design of all of the services can you construct a complete physical network diagram to document the design plan.

## Branch Infrastructure Environment

The branch infrastructure environment includes the branch sites themselves, any regional sites that they may connect through, and, where applicable, a central site that is associated with the branch sites. Because the goals of the business and many other organization-specific factors determine an organization's environment, no single definition of an environment fits in all organizations, although the goals for this environment are usually consistent with the following statement:

*“Provide a secure, fault tolerant, high performance IT infrastructure to all geographic areas of the organization for as little cost a possible.”*

This is an excellent mission statement to keep in mind for your designs, but there are a number of technical and non-technical constraints that affect your ability to deliver a design that meets this statement. The key to successful branch infrastructure design to identify these constraints and their effect and then communicate them to the relevant parties *before* the design is agreed or implemented. This is especially true in larger environments that are unlikely to support a single common approach in all of the branch sites. For these organizations, the final design must provide various levels of performance and fault tolerance for the end users and support staff across the environment.

When you attempt to map particular service designs for each branch site you often find that various sites and services require different approaches. For example, a centralized information Web portal typically lends itself to a centralized design, however the performance of a WAN can often make a centralized file service impractical for the branch users, especially if they are working with large files. For this reason, you must approach each service design on a case-by-case basis and determine if the specific characteristics of the service and the requirements of the users at the branch site support the preferred approach.

For large or complex organizations, a number of decisions have to be made based on business needs to determine the most appropriate branch office infrastructure. The decision tree below, shown in figure 2 below, depicts the criteria that need to be considered to deploy the most appropriate infrastructure.



Figure 2. High level branch design stages

Like most elements of branch design, there are many variations on these scenarios including hybrid. However, the three branch scenarios that are presented in this guide provide a good starting point for classifying the common technology approaches that can be used to provide the required services to your branch infrastructure.

## Service Placement Approaches

The placement of individual services in a branch infrastructure environment presents an almost infinite number of possibilities for branch office architectures. However, most architectures can be represented by the following three approaches, which reflect the entire spectrum of possibilities:

* **Centralized**. All services located in a central site. This approach is at one end of the spectrum, representing the most centralized solution.
* **Distributed**. All services located in the branch office. This approach is at the other end of the spectrum, representing the least centralized solution.
* **Hybrid**. Services in the central site and a subset of services accelerated over the WAN by providing a local copy or other caching mechanism in the branch site. This approach is in the middle of the spectrum and represents a partially centralized solution.

Although the design details may vary, you will probably find that your branch office infrastructure reflects a combination of the characteristics of these three approaches.

### Centralized

Centralized branch offices, sometimes referred to as *micro-branches* or *satellite offices*, do not host services locally because the central site provides all of the branch site services and support. This is appropriate only for branch offices that can tolerate the performance and availability constraints that are introduced by the WAN connection, which is not a common scenario. The following lists outline the advantages and disadvantages of satellite branch offices as they relate to the primary design considerations.

The advantages of using this approach include:

* Deployment is cost effective because no servers are placed directly in the branch site. This can be offset by the costs of deploying services in the central site, the increased costs of the WAN, and the performance degradation due to WAN latency.
* Total cost of ownership (TCO) can be much lower for monitoring and managing server-based services. This is because it is easier to manage the reduced number of components, which are in close proximity to the people who administer them, and the skill sets required to manage the services are generally more focused on individual technologies.
* It is typically easier to secure a centralized system than a distributed system because there is a reduction in the exposed surface area and potential entry points.
* It is easier to establish high availability and backup and recovery support for a centralized environment because clustering, replication, and other technologies and techniques are commonly deployed in a centralized environment and because it is easier to manage availability locally rather than remotely.
* Service delivery is more efficient and effective because of the following considerations:
* The economy of scale that is possible by using a small group of skilled resources to provision services
* The structured processes that are used to ensure quality and cost control for service provisioning
* The standardized tools that are used to support automation and proactive monitoring

The disadvantages of using this approach include:

* Management of client (user) computers may present a significant challenge. All client computers must be dealt with from the central site; no branch site appliance or server remains to act as distribution point for software and updates, or as a collection point for management services. Some technologies support using a client computer to distribute software and updates to other client computers in the branch office, but such technologies have the same challenges as remote management of other services. Removing servers and server support does not totally remove the need for support in the branch because typically desktop and application support is still required.
* Removing branch servers does not remove the need for network servers in the branch. For example services like name resolution (DNS or WINS), authentication and printing are often more effective when delivered at the branch site.
* It may be necessary to increase the capacity for the branch network connection. Although the costs for network connections are decreasing in many areas of the world, it can be very expensive to obtain the required capacity and scale, especially in specific geographic regions. Latency becomes an increasingly bigger issue if a large number of transactions must take place over the WAN and it may not be possible to reduce this latency because it is inherent in the WAN link technology itself.
* The branch is completely dependent on the network link for access to data and services. The potential downtime can be offset by using an alternative network link (preferably through the use of another provider, to make sure that the network link is not aggregated at any point between the branch office and the central location). But the cost of this can be prohibitive. Performance is totally dependent on the network link, even though some optimization of productivity over the wire is possible; the technologies that are required to do this most effectively are still emerging.
* Timely support of the branch can be a challenge across geographic boundaries and time zones. If support is provided only from the hub site, and branch offices span multiple time zones, the hub site must be staffed to provide support during business hours for all branch sites. This can mean that the saving of the branch support staff is offset by an additional requirement at the hub site.
* Remote service management for branch sites requires remote access, monitoring, and automated software delivery mechanisms that work across the WAN.

### Distributed

A distributed branch is highly self-sufficient, with little or no dependence on a hub site because the branch office provides most, if not all, of the services and support. Distributed branch offices are common in the following situations:

* The IT organization is distributed and each branch office is generally managed locally.
* The branch office requires local deployment and management due to one or both of the following reasons:
* Services cannot be implemented in the central site and run over the WAN without unacceptable degradation of performance or availability.
* Services in the branch office cannot be managed over the WAN from the central network because of lack of bandwidth.

Note   The need for a local branch server and the need to manage it locally are separate considerations. The distributed branch office described in this section links the two concepts because it is intended to represent the most distributed scenario (where both the server and support are in the branch office).

The following list describes the advantages of a distributed branch design:

* The branch users have no dependencies on centralized services for the day-to-day business functionality that they require, so the reliability of the network link to a hub site is not a significant issue.
* Because all of the services are provided locally, everything is available at LAN speeds.
* Communications with the hub site and other parts of the organization typically do not require heavy bandwidth, so the cost of the network link is generally lower.
* A branch office that is autonomous from a technical perspective and is locally managed provides the following advantages:
* Consolidation of services within a branch office is facilitated by the fact that a single person is usually responsible for administration of everything in the de-centralized environment, so cross-group security and administration problems generally do not exist.
* Service delivery resources are co-located with the business, so service is generally responsive and aligned to the local requirements of the business.

The following list describes the disadvantages of distributed branch offices:

* It is the most expensive option because all services must be self-sufficient and available locally.
* It is more likely to require local support personnel, which requires the availability of specific skills that can be difficult and costly to maintain at an appropriate level.
* If the branch office is not physically or logically as secure as the hub (because of local management, high risk of data theft or tampering, or other factors), there may be an increased exposure to the security of any corporate data that resides in the branch office. This increases the risk of data loss from the branch site.
* For any service that is not managed by a central IT organization, it may be a challenge to ensure that corporate requirements and standards are followed. Branch offices may evolve in different directions, which may make it difficult in the long-term to move to more centralized purchasing and IT structures, as well as more standardized technologies and processes.
* There is a significant chance of independent developments that are not coordinated across branch offices or with the hub site, which can be difficult and expensive to reconcile.
* It may be expensive to maintain reliability and availability because of the capital expenditures that are required to deploy hardware and software to provide redundancy. Such systems are often underused because it is not possible to obtain the economy of scale that is possible in a central site.
* Scalability for local systems requires careful planning. The cost of implementing scalable systems at branch offices can be very high and local systems may be deployed in a more reactive manner than systems in centralized sites, so they are generally not designed for scalability. Local systems often start with a single server that is later renamed and reconfigured to support growth, as opposed to central sites, which generally build in scalability technologies (such as Storage Area Networks and load balancing).
* Often, the service delivery infrastructure is not documented and only a single support person knows how it is implemented. A branch office can become dependent on the specialized skill set of one individual and this person can prevent the implementation of standards, centralized policies, and tools if he perceives those things as a threat to himself. A lack of structured processes can make it difficult to implement standards and to ensure that the required changes are made to protect the environment.
* Typically, each site deploys some solutions that may not be compatible with the central site or does not support automation, which can make it difficult to gather data for measurement and reporting purposes. This can severely affect the ability of a business to meet regulatory, government, or other compliance requirements.
* Best practices are not always shared across sites, which can complicate administration and result in higher maintenance costs.
* It can be difficult, if not impossible, to integrate branch functions that do not follow strict change management procedures with centrally managed standardized and controlled functions.
* It can be very difficult to provide enterprise-wide backup and recovery support because of the large number of specialized functionality, unique processes, and independent administrators.

### Hybrid

The hybrid approach provides some decentralized services and support in the branch, however, most services and support are provided by the hub site. For services located at the hub site, local access is often provided through the use of caching and WAN acceleration techniques. Hybrid branch offices are common in organizations that have centralized environments where the application architecture and the capacity of the WAN connection between the hub site and branch can support the centralization of some services. But other services that are not designed for use over a WAN cannot be run remotely because of bandwidth and latency issues.

The following list describes the advantages of the hybrid approach:

* If the branch site infrastructure fails, a level of service is still available across the WAN. If the WAN fails, a level of services is still available for the branch site from the branch–based infrastructure.
* Monitoring and management processes can be standardized across the organization because they are carried out centrally, which can improve cost effectiveness and security.
* Services provided at the branch site provide optimal performance between the branch office and central site, with less dependence on the quality of the network.
* Replication of data to the branch can reduce the impact of problems with WAN availability. For instance, the replication of both read and write data to and from the branch (such as that which DFS Replication provides) makes data available locally even if the WAN is unavailable. Caching and use of services, such as print services that use only non-persistent data, also provide good local availability for centralized services. Although some centralized services are not available when WAN connectivity is unavailable, critical applications deployed in the central site should all have two-way caching to ensure ongoing availability.
* Services are more scalable, partly because the combined demand for services in the central site makes more effective use of hardware and software on fewer instances. This is also the case because service consolidation is not limited to services from a single site. Consolidation makes it more cost effective to deploy and maintain services, including backup and recovery support.
* Many of the service delivery advantages of centralization can be realized and local support resources are generally available for client-side support and occasional server-support functions.
* Processes support quick response to local business needs, while still working within the centralized service management structure.
* The branch office can generally make use of the automation tools that are deployed at the hub site, with the added value of having a local resource to help to ensure quality.

The following list describes the disadvantages of using the hybrid approach:

* Not all services are currently designed to enable acceleration. This is especially a problem for applications that require encryption. However you can design a solution that would run the services locally or introduce trusted intermediaries that handle encryption.
* Acceleration of services requires capital outlay and management of the branch devices, although co-location of services on the same device can minimize these expenses.
* Using a single server to host end-user services and the infrastructure services they depend on can be a challenge. Some of the primary challenges include providing appropriate isolation, maintaining offline business support, and satisfying domain administrator security requirements.
* As with distributed branch sites, potential security risks in the hybrid branch office can also mean increased security risks to corporate data in the branch site. However these can now be mitigated by technologies such as Bit Locker Driver Encryption on any Windows Server 2008 branch servers.
* Not all services are designed for transparent failover. Manual failover procedures can be complicated and time consuming, require training to implement.
* Appropriate delegation of authority for managing branch services can be a challenge to implement in the context of a corporate security policy, especially for services that require autonomy.
* Maintaining service delivery quality requires the coordination of branch office and central site processes, especially for the service desk, incident and problem management, change configuration, and release management.
* Service delivery interactions between branch and central sites needs to be carefully monitored to provide consistency in end user experience.

### Service Placement Considerations

Each organization has priorities that dictate which requirements are most significant and, thus, which ones have the most impact on the design of the branch infrastructure solution. For instance, a military organization might prioritize security and design a security-centric solution, a retailer might structure a solution for reliability and performance, and an insurance company might be most interested in a solution based predominantly on TCO. As part of your early analysis efforts during the Envisioning Phase of your project, you should have identified technical, business, and other requirements and limitations that affect the placement of services.

You need this information to effectively evaluate the options and tradeoffs for each branch site service, both the general design considerations covered in this section and the service-specific design considerations that the following list outlines:

* **IT organization**. Central sites and branch offices generally have very different IT organizations in place to deploy and support the IT infrastructure and services deployed there. It is important to understand the differences between these two types of IT organizations and the types of potential tradeoffs that are required to determine where to locate services, such as the following:
* The skill sets needed to manage each service and where these skills need to be available (centrally or in a specific branch site)
* Any changes required in the structure or nature of the IT organization to meet both short-term and long-term goals related to branch site services
* **Political considerations**. The nature and number of an organization's political considerations can affect service placement. For each service, you should determine if any political factors prevent services from being centralized or located at the branch offices. Such political factors can have related security considerations (for example, for protection of sensitive data, as covered later in this section). But ownership, perceived and real needs for autonomy or isolation, and other political issues can also limit where a service is located. For example, individual groups can each have specific administration requirements that are not met if the service is centralized or is co-located on the same server as other services.
* **Legal and regulatory considerations**. Depending on the geographic and industry affiliations of an organization, legal restrictions or requirements for regulatory compliance can either restrict or facilitate streamlining of branch site services. Some of the restrictions that can have an impact include the following:
* Country or other laws that govern national, international, or any cross-boundary operations
* Union regulations that restrict movement or responsibilities of personnel
* Industry-specific restrictions on the use of hardware or software
* **Security**. The branch office sites can introduce a number of security risks that you must consider. For more information about security considerations, see the Security Considerations section later in this guide.
* **Availability and reliability**. Availability and reliability can pose significant challenges to the centralization of branch site services and to the consolidation of services. The two most significant factors are:
* **Centralization of services**. A centralized environment generally offers more sophisticated clustering and other failover and recovery services, well-defined service levels and commitments, immediate access to hardware parts and software, and extended hours of support that are not typical in a branch office. However, the simple fact that each transaction between the branch office and the central office requires data to travel across a WAN introduces the potential for loss of connectivity, especially if the WAN link is not reliable.
* **Consolidation and co-hosting services on a branch server**. A server that is running multiple services represents a single point of failure that can have significant impact. If one service or device driver fails, or if the branch site server operating system fails, all of the services that are running on the server become unavailable. Although local hosting of services removes the dependency on WAN availability and can make services more readily available, the expense of deploying redundant servers and services and establishing off-site recovery support can be prohibitive and prevent local establishment of appropriate recovery methods.

Implementation of redundancy and clustering is generally driven by the availability requirements for services, especially those required by specific line-of-business (LOB) applications. The most common options for services located in the branch office are the following:

* **Non-redundant servers in the branch**. This is the least expensive and least fail-safe option, but local disk mirroring can provide some failover protection from disk failures. Appropriate hardware service contracts can help to minimize downtime. Use of Windows Server 2008 and the latest hardware can provide high reliability with minimal cost.
* **Branch site service redundancy**. To provide redundancy for a branch server, you can either use a second server in the branch or add redundancy at the hub site for specific services (with backup handled over the WAN). Most distributed services do not require service clustering. Some services, such as file services, include a data store that can be replicated to another location for redundancy. To avoid replication conflicts and loss of modifications, such data stores should be accessed in only one place at a time. Using centralized redundancy for local servers in the branch office (such as providing backup print queues) can be fairly inexpensive due to the economy of scale that occurs when the central site provides redundancy for multiple locations. Redundancy always increases management overhead but provides better availability for the end user.
* **Single server for local services, with local redundancy and Windows clustering for services***.* This requires Windows Server 2008, Enterprise Edition or Windows Server 2008, Datacenter Edition but is still a cost-effective method. Windows provides automated management capabilities, although deployment and management are still more complex than providing centralized redundancy and clustering in the hub site.
* **Backup and recovery**. Effective implementation of backup and restore support requires definition and implementation of well-defined processes and procedures. Because backup and restore procedures generally require physical intervention (such as changing tapes), they can be difficult to manage remotely. Backup to or restoration from a centralized location requires significant WAN capacity, so lack of sufficient capacity on the WAN link can cause failure of the backup or restore operation, or can interfere with the availability of other services. For more information about backup and recovery, see the BOIS Base Management Services guide at http://www.microsoft.com/branchoffice.
* **Performance and capacity**. Design considerations for performance and capacity can involve complex tradeoffs between functionality and speed. The nature of central sites (including the tendency to be more standardized and conservative in their pursuit of technology) generally results in their not running the latest hardware and software. However, the types of technologies are probably more sophisticated than those available in the typical branch site (such as having more load balancing and other services). The technologies and sophistication, combined with the restrictions of WAN connectivity, can significantly affect user productivity and the user experience in general. Although local services typically provide the best performance and user experience, other factors involved with providing local access, such as cost and management overhead, may outweigh performance impacts if established SLAs can be met with centralized services.
* **Scalability**. The central site infrastructure is generally highly scalable, more cost-effective to expand, and more efficient to update because the entire infrastructure is designed for scalability. This type of infrastructure also tends to use resources more efficiently and provide better economies of scale for all services. Branch offices generally offer little scalability because new components are typically added as required, and scalability is not designed into the infrastructure. To accommodate future growth and minimize the need for site visits and replacements of centrally managed branch site servers, the servers typically have considerably more capacity than is initially required. Because capacity generally becomes less expensive over time, providing extra capacity before it is needed means the capacity costs more per unit than it would later.
* **Cost**. The cost of streamlining the branch office infrastructure is a calculation of the difference between the cost of continuing with the current solution and the cost of deploying a new one. Most of the costs are related to all of the factors covered previously in this section, but there are also ancillary costs and cost-related factors that you should consider. Additionally, centralization or co-location of services can make it difficult for customers (consumers of the services, especially owners of specific services) to know how the money allocated for IT support is being spent and what they are getting in return. Individual ownership of branch site services and servers provides greater transparency, which produces a more definitive link between the budget and what customers receive. The result can be loosely defined agreements instead of formal SLAs.

## Service Provisioning

After you have determined the requirements for the placement of services at the branch offices, the next logical step is to determine the preferred method of provisioning those services. As with service placement in a branch infrastructure, there are an almost infinite number of possibilities for branch office service provisioning. However, most can be represented by two basic approaches:

* **Appliance-based branch office services**. The designer determines that the services that are required at the branch office can be provided by some form of specialized branch office appliance.
* **General purpose server-based branch offices services**. The designer can standardize on a common general server platform, such as Windows Server 2008 to provide the branch office services.

Although the design details may vary, you will probably find that your branch office infrastructure solutions reflect a combination of the characteristics of these two approaches.

### Appliance Form Factor

Over recent years, a great deal of development has gone into creating network appliances to provide services that would attempt to create a *branch-office-in-a-box*. The basic premise behind the development of these appliances is that they can be shipped to the branch office, plugged in, turned on, and then work, all with minimal configuration.

Many organizations have attempted this approach with varying degrees of success.

The following list describes the advantages of the appliance-based services approach:

* Branch office appliances offer a relatively simple initial configuration and short startup times.
* Most branch office appliances hold little or no unique end-user data, which typically makes the process of appliance site backup very simple or not required.
* For small office appliances, the initial purchase cost is often significantly less than server-based services.

The following list describes the disadvantages of the appliance-based services approach:

* Service support can be limited on some branch appliances. If your organization determines a requirement for a branch-based service that cannot be provided by the appliance other solutions will be required.
* The configuration and management of the appliance often require product specific administrators. This requires additional staff training as well as appliance specific support and operations procedures.

The capabilities of the appliance-based solutions are evolving all the time. Solutions can now be scaled to include virtualized services that are provided from an appliance-based form factor. While these enhanced capabilities enable the appliance to provide a more flexible solution at the branch site, the same basic advantages and disadvantages still apply.

### General Purpose Server Form Factor

Server-based services are provided by a general purpose server that is flexible in its capabilities and can be configured to provide a wide variety of services to the branch office at varying levels of performance, scalability, and reliability.

The following list describes the advantages of the server-based services approach:

* By standardizing on a server-based approach, organizations can create a common server platform across all of their branch offices. This standardization enables support staff and processes to be standardized.
* A server-based solution offers a much wider variety of the services that can be hosted at the branch offices, so a common platform and support structure can be established across the branch office infrastructure.
* As an organization’s requirements change, the server-based approach provides a far more flexible platform to support changes in service requirements at each site. Server hardware can also be repurposed elsewhere in the organization if a branch office is merged with another office.

The following list describes the disadvantages of the server-based services approach:

* For small branch offices, the initial purchase cost is often higher than a simple appliance-based solution.
* The additional flexibility of the server-based solution introduces an additional level of complexity. Although this complexity can be managed through the use of technologies such as Group Policy, deployment images, and virtualization, there is still some additional setup overhead typically associated with this approach.
* The more advanced services of a server-based solution typically require the maintenance of branch office-based end-user data. There is usually a requirement for additional backup and recovery procedures to ensure this branch data is protected in the event of a branch office disaster.

Windows Server 2008–based server solutions can be highly configured and customized by using scripts and Group Policy. With the addition of Server Core and Hyper-V, it is now possible to create a highly customized branch office server that also has the ability to be managed as part of an organization’s standard management platform and can also be reconfigured if the needs of the branch office change.

## Operating System Configuration

Windows Server 2008 includes Windows Server Hyper-V, a powerful virtualization technology that has strong management and security features. Hyper-V provides an excellent platform for a virtualized solution in branch offices, which can help organizations to reduce costs, and increase agility and system availability for branch office-based servers.

By using this enhanced functionality, you can now maintain multiple instances of fully functional server operating systems on a single branch office-based physical server.

### Single Operating System per Server

A single functional operating system is installed and configured on one piece of server hardware. The following list describes the advantages of the single operating system per server approach:

* The risks and scope of effect that is associated with hardware failure can be mitigated by spreading services and applications across different server hardware platforms.
* Hardware requirements are reduced when a server hardware platform only supports a single server OS instance.
* Server performance is generally better when server hardware is dedicated to a single server OS instance.

The following list describes the disadvantages of the single operating system per server approach:

* Can be costly to devote an entire server hardware platform to a single operating system instance, if branch locations require a substantial degree of local services and applications.
* Reduces agility because a new server hardware platform must be purchased and configured to deploy a new server instance if needed.
* Requires additional space and infrastructure, such as environmental controls, to support that extra hardware and branch sites may have limited space and server hardware.
* Increases administrative overhead to support the additional hardware, apply firmware, troubleshoot hardware issues, and resolve potential driver issues.
* Increases the costs of additional hardware that is associated with maintenance contracts, infrastructure costs, and space requirements.

### Multiple Operating Systems per Server

The traditional method of working with server hardware has always been to allocate a single operating system to the hardware. Affordable, reliable, and robust server virtualization technologies make the option to maintain multiple operating systems on the same physical hardware an attractive option for many organizations.

The following list describes the advantages of multiple operating systems per server approach:

* The use of server virtualization can reduce the costs that are associated with hardware purchases and maintenance, if the required hardware purchases needed to support virtualization do not cost more than additional single server instances would.
* Server virtualization increases agility because deploying an additional virtual server is much faster than deploying a new physical server instance and virtual networks are much more flexible than physical networks.
* It is possible to use multiple Windows Server 2008 instances to improve security without a significant effect on cost through virtualization.
* Administrative overhead and support costs can be reduced by using server virtualization because this reduces the number of hardware platforms deployed at branch locations.
* Server backup and restore performance can be improved by using server virtualization because each server hard drive instance exists as a single file on the host server, so, when backing up the host server, the backup process can backup several servers at the same time.
* Application incompatibilities and other server software failures can be easily restored by copying virtual hard drive images to backup storage before changes are made and then using these images as restore points.

The following list describes the disadvantages of the multiple operating systems per server approach:

* The risks and scope of impact that is associated with hardware failure can be increased when hosting more than one operating system instance on a single server hardware platform.
* Hardware requirements to support server virtualization can be more demanding than those that support single server instances, so costs per server may be higher even though total server purchase costs may be reduced.
* The performance of virtualized servers may be less robust than that of a single server instance running on a devoted single server hardware platform, in some cases.

If the branch office service requirements are significant enough, it is possible to design a branch site solution in both scale-up and scale-out configurations.

# Branch Infrastructure Physical Design

The design of the physical branch infrastructure has a significant impact on the design of other services and components. The performance and availability of the network determine whether a service can appropriately support user requirements for accessing services over a WAN. There is no single right or wrong choice for where to locate servers and services, and no single solution will fit every organization or every branch site. The characteristics and requirements of each organization and site should determine branch infrastructure placement. Although management and other philosophies in an organization (such as mandates to consolidate services and support) may set the initial direction for the design of the branch infrastructures, the most appropriate solution for each site must meet the functional and business requirements in a realistic manner. The solution must also make provision for the technical, process, and personnel considerations that are related to those requirements. The types of design considerations that are not specific to a single site server and that should be applied to all servers include the following:

* Branch server placement considerations, including the general implications of server placement on security, people, and processes, as well as on the organization itself.
* Current server hardware standards across the organization.
* Hardware performance and power requirements.
* Server hardware vendor agreements and warranties.
* Remote manageability capabilities of the server hardware.
* Physical security characteristics of the branch sites.

The branch-site infrastructure design should focus on how to optimize the use of hardware, software, and support (including the use of personnel resources) in each branch office. Regardless of which design you use, you should plan to minimize the differences between branch infrastructures wherever possible. If you can create a common branch-site standard, or at least a small number of tightly controlled standards, you will significantly reduce your ongoing support and management costs.

The following list summarizes the main options for branch site infrastructure classes:

* **Server-less.** Provides a bare minimum of branch hardware, usually just the basic network routing and network infrastructure. All other servers are provided from a centralized location. Some branch servers may be provided directly from the branch client computers, for example, local physically attached printers.
* **Branch Office Box**. Uses some form of appliance or networking device to provide a set of local services to the site. This form factor is often marketed as a “Branch Office Box” or “Branch in a Box” product. Typically these appliances provide a focused sub-set of an organization’s services to the branch site, often using WAN acceleration techniques to optimize the use of the available bandwidth between the sites.
* **Virtualized Branch Office Box**. In recent years the lines between an appliance and a server have become more blurred. As the appliance operating systems have become more complex and the services they offer have become more diverse. Recent generations of branch office boxes have now started offering virtualization capabilities. By using this hardware is it possible to create virtual machines that manage the more complex services at the branch site. This option can provide challenges to the organization’s management infrastructure and branch site performance, as well as increase the impact of the hardware failure.
* **Single server**. Provides a single physical server with a single instance of an installed operating system. This option can be very cost effective due to the low overhead for hardware, software, and management required. This option can, however, present challenges to the administrative model, security, local server configuration and standards, and performance, as well as increase the impact of server hardware failure.
* **Multiple server.** If the service requirements for performance, availability, or security isolation are beyond the capabilities of a single physical server, additional servers can be added to the infrastructure. This option has significant cost implications both initially for purchase costs and subsequently for ongoing support and operations.
* **Single virtualized**. By using Microsoft Virtual Server 2005 R2 and Microsoft Windows Server 2008 Hyper-V, you can run isolated instances of an operating system as guests on a host operating system. Each virtual machine requires its own operating system and management services, such as the update services, backup, and antivirus services. Hyper-V is Microsoft’s recommended branch virtualization platform because it provides enhanced functionality in areas such as scalability, high performance, reliability, security, flexibility, and manageability. Hyper-V provides scalability and high performance by supporting features like guest multi-processing support and 64-bit guest and host support; reliability and security through its hypervisor architecture; and flexibility and manageability by supporting features like quick migration of virtual machines from one physical host to another.
* **Multiple virtualized**. With this option, the services are on dedicated virtual machines, which can then be allocated to multiple host servers. There are usually three basic reasons for this:
* **Security**. If one or more virtual machines have elevated security requirements or attack vectors, (for example if one for the virtual machines was for a domain controller and the other was for a public facing Web server), good security practices dictate that these virtual machines should be physically isolated from each other.
* **Performance**. Each virtual machine draws from the available pool of resources; these resources are provided by the virtual server host server hardware. If the aggregated resource requirement is beyond the capabilities of the available server hardware, additional servers may be required.
* **Availability**. By using Windows Server 2008 Hyper-V you can setup clusters of physical host servers to provide high availability for the virtual machines that are hosted on those servers. This technique is known as a *host cluster* to differentiate it from a cluster of virtual machines on a single virtual server host computer, which is typically referred to as a *guest cluster*.

This option is not cost effective compared with the other options, but it can provide good scalability and simple management of the servers. A hardware partition provides the advantage of having only one hardware platform to monitor and manage, while still enabling computer-level management of resources.

The option that you choose for each service determines the number of branch servers that are required. Use the information in this guide, along with the information in the other guides in the Branch Office Infrastructure Solution series, to determine the most appropriate options for each branch service that is required in the branch office.

## Physical Network Structure

The design of the physical network infrastructure has a significant impact on the design of other services and components. The performance and availability of the network determine whether a service can appropriately support user requirements for accessing services over a WAN.

The first stage of the physical network design is to determine the most appropriate WAN structure for connecting the branch offices of an organization. The two most common network structures for WANs are the following:

* **Single-hub network**. The hub site connects directly to multiple branch sites. This is a common WAN structure for organizations that have multiple branch offices, but the branch offices must have almost identical business functions and operate within the borders of a single country or smaller region. Figure 3 shows a sample network structure with one hub site.



Figure 3. Single-hub network

The single-hub network generally requires only a single network connection for the branch office, unless branch offices must connect to each other, or unless a separate Internet connection is required.

* **Multi-hub network**. Generally provides at least three tiers of network connections. This is a common structure for larger or international organizations that have many branch offices with diverse business functions. This WAN structure commonly has one central hub site for corporate headquarters and one hub site per geographic region (for example, a separate hub for the Americas, Europe, and Asia Pacific). Branch offices in each region connect directly to the regional hub site.

Figure 4 shows a sample network structure with one central hub site and two regional hub sites.



Figure 4. Multi-hub network

The multi-hub network is more complex because there are potentially more layers in the network. For instance, if branch sites require any services from the central hub site, they must generally go through the regional hub site to connect to the central hub site. With this structure, branch sites are dependent on the availability, capacity, and performance of the link between the branch site and the regional hub site, as well as the link between the regional hub site and the central hub site. The multi-hub network may be further extended, if branch sites are connected to other branch sites, so you must determine the services that must be available in second-tier sites. Options for the second-tier sites include the following:

* Have the same set of services available locally as the first-tier branch site
* Have more services available locally (because of insufficient network availability, capacity, or performance)
* Have fewer services available locally and rely on the services that are provided by the hub site

## WAN Connections

The next stage of design is to assess the design considerations for the WAN connection of the branch site to the central site, including any changes that are required to provide access for any services that are to be centralized. The network link that connects the branch site to the hub site is a critical component of any WAN. The WAN link can significantly affect the availability of any services that require access over the WAN.

### Link Characteristics

The links that provide WAN connectivity between hub sites are usually relatively high-capacity, high-availability private links. The WAN link to the branch site can vary considerably, based on several factors (especially link costs and the branch site requirements). The following list outlines the link characteristics that have the most significant impact on network performance and availability and how each can affect the centralization of branch site services:

* **Link type**. This is a primary determinant of network speed, support for network loads, and network availability. Link type includes whether the connection is persistent (such as a leased line) or on-demand (such as dial-up and Integrated Services Digital Network (ISDN)), as well as the protocols that it uses (such as virtual private networking (VPN), Frame Relay, or satellite). On-demand connections limit the availability of the network and may incur a charge every time the connection is established. The quality of the telecommunications infrastructure in specific geographic locations may affect even persistent connections, so they are not always connected. Some services can be forced into the branch site because the availability requirements of services that depend on the service in question exceed what can possibly be delivered by the network link. This could be because of network load generated by interdependent services or the connectivity requirements of the service itself. For instance, although the ongoing traffic patterns of a service might not place a significant load on the WAN, a delay in establishing an initial connection over dial-up or satellite link could cause a service to timeout or fail.
* **Link bandwidth**. This is the theoretical maximum speed of the link, but the real speed is limited by network latency.
* **Link latency**. This is the time that it takes a network packet to get from one place to another, which constrains the minimum time (amount of delay) required for a transaction (round trip). Depending on the requirements and behavior of the application-level protocols, perceived performance can be seriously affected by latency, regardless of the bandwidth of the network link. Services and applications that work in a “windowed” manner, such as file transfers, can have multiple outstanding packets before requiring acknowledgments and are generally not significantly affected by latency. Alternatively, “ping pong” services and applications that require a response to each request before transmitting another request (such as Terminal Services or two-tier and three-tier applications) are generally latency sensitive. For example, bulk transfer of data, such as a file copy, may perform well because of its streaming nature, but browsing a folder structure on a branch share may be considerably slower because Windows Explorer needs to transfer new data every time the user browses to another folder. This is compounded by the amount of data that is transferred to provide the richness of the Windows Explorer window.
* **Link capacity**. This is the theoretical amount of aggregate data that can be pushed through a network link. It is closely tied to link speed.
* **Link utilization**. This is expressed as a percentage of total capacity for the link. Utilization includes all network traffic (such as the background transactions required to monitor and manage the network and services), other individual services and applications that use the network, and specific functions that depend on the network (such as security cameras, security systems, and VoIP). Utilization generally varies over the course of a day, week, month, and year. Many organizations target utilization to 60–80 percent.

It is important to understand link capacity and utilization characteristics and to evaluate how the new solution might affect your capacity and utilization. It is also important to understand how the new solution can take advantage of the capacity that is available at specific times of the day, week, or other period.

Some of the most significant design considerations for the WAN link are the following:

* **WAN usage requirements**. The amount and type of data and transactions that branch offices typically require are primary determinants of the WAN connectivity requirements, as are the amount and type of collaboration between branch users, hub site users, or users in other branch locations.
* **WAN availability**. Failover support for the WAN link must meet branch office requirements for acceptable availability for the solution. The reliability of the WAN link affects the availability of services that are hosted in the hub site. The availability of the WAN link does not usually affect the availability of a service that is provided locally in the branch site, unless the service is dependent on one or more other services that are hosted in the hub site.
* **WAN performance**. The capacity and latency of the WAN link affects the performance of the hub site services that must be accessed over the WAN. The capacity and latency of the WAN link generally does not affect the performance of a service provided locally in the branch office unless the service uses the WAN link to transfer large amounts of data to the hub site, such as for data replication or backup. Such activity may take longer than expected or may affect the performance of other services that are dependent on the WAN.
* **Cost**. The cost of network links can vary greatly based on factors such as the type of link, country-specific or region-specific economics, and distance. It is generally feasible to provide connectivity that can meet defined user requirements, but the cost may be prohibitive. Additional costs associated with upgrading links might be offset by the savings made by removing certain services from the branch office or eliminating branch site servers entirely. In most cases, however, link costs to establish a WAN connection that has sufficient availability, capacity, and performance to enable centralization of branch site services can exceed the amount to be saved by centralizing the services. Providing network connectivity across geographic borders can be expensive (sometimes exponentially higher than connections within a single country), can cause performance and availability problems, and can present challenges in adhering to country-specific technical standards and other requirements for international communications.
* **Time zones**. Time differences between geographic regions can cause synchronization challenges, especially when changes occur, such as switching to or from daylight savings time (which is implemented at different times in different places and may not be implemented at all for some countries, states, counties, or other geographic or political entities). Time differences can also affect the availability of support staff (if an organization does not provide support 24 hours a day, seven days a week).
* **SLA requirements**. The network link must support the service delivery requirements that are defined in SLAs, and the network provider must provide the monitoring data that is required to support end-to-end service management.
* **Hub link capacity**. The hub site link capacity must be sufficient to handle network traffic for all of the branch offices combined and the management of traffic between individual branch sites must prevent potential bottlenecks when too many branch sites are placing significant loads on the link (such as might occur if all sites replicated a specific service at the same time).

### Network Link Scenarios

The diverse type and characteristics of WANs make it impossible to give specific recommendations about the WAN connection that would be most appropriate for your organization. However, based on customer data collected by various groups, it is possible to generalize three network link scenarios, one for each of the three branch infrastructure architectures that were defined previously in the Physical Network Structure section of this guide. The following list describes the characteristics of each of these scenarios and the potential applications for each:

* **High performance**. Satellite sites typically require high performance links, (at least 1.544 or 2 megabits per second, depending on location), low latency, and high availability. These sites are typically found in North America and within country borders of many Western European and other countries. This type of network link may enable organizations to centralize more services into the hub site than the other scenarios, because the reduction in management cost that results from centralizing services can outweigh the cost of providing sufficient availability. Also, the capacity and latency can be good enough that they should not negatively affect end-user productivity. In some cases, productivity may improve because of application. For instance, applications that access a store (such as a database or mainframe computer) in a hub site might benefit by being moved to application farms in a central site and by using Terminal Services to access them. The reason for the improvement is that the most intensive transactions do not occur over the WAN, and the high capacity WAN supports the reduced level of performance that users require for access to the application.
* **Medium performance**. Hybrid sites can typically use medium performance links (128–512 kilobits per second or Kbps), medium latency, and good availability. These scenarios are typically found in geographic locations that do not have the more advanced telecommunication infrastructures or in situations that require the crossing of significant geographic boundaries. The link might support centralization of services with low bandwidth requirements (such as DNS and Active Directory Domain Services, if they do not have configurations or other restrictions that prevent centralization). However, the availability of the network link might not be sufficient to ensure that the services that are left in the branch office (such as file and print services) can access any centralized services upon which they depend for name resolution, authentication, and authorization. Also, the latency of this link might not provide an acceptable user experience when using Terminal Services to access centralized applications.
* **Low performance**. Distributed sites can usually function with lower performance links (such as those less than 128 Kbps) and high latency, and are more tolerant of link unreliability. This scenario is typically found in areas of the world where the telecommunications industry is significantly under-developed or the cost of obtaining a higher performing, more available network link is cost prohibitive (such as when connecting a single branch office in a very remote location). Use of this type of link is not conducive to the centralization of services. But it simplifies the branch infrastructure design because all of the services that support the business-critical branch site functions and the services upon which they depend must be located locally in the branch site.

## Network Segmentation in the Branch Site

The next stage assesses network segmentation for the branch site and identifies the most appropriate support for the services in the new solution.

The internal network in the branch site has traditionally been a single segment network, also known as a *flat network*. This type of network provides a simple and inexpensive infrastructure with a simple IP plan. Also, if WINS or DNS name resolution becomes unavailable, fallback support is available because, by default, Windows falls back to broadcasting name resolution requests to the local IP subnet.

LAN segmentation of a branch site network can be used for segregation of computing devices in that site, such as separating servers from client computers so that the administrator can control the flow of traffic between segments and provide packet translation, filtering, firewalls, and other security measures between segments (to help protect server assets in the branch site). Segmentation also supports definition of separate rules for allowed ports and protocols, as well as packet filtering between each segment in the branch site and between the branch site and the hub site (to manage communication to and from the hub site). Although segmentation can facilitate network management, fallback of NetBIOS name resolution is not possible because the client computers and server computers are on separate segments. In addition, broadcast traffic is not typically forwarded unless the network device that is used to connect the segments locally is configured to forward broadcast traffic between the segments. If the network device fails, all communication between the segments fails.

## Other Network Design Considerations

In addition to the network link, each branch site also requires a network infrastructure that supports all of the users in the branch site and their internal connectivity requirements. Even with the goal of keeping the number of servers to a minimum, branch offices generally have separate devices (including routers and WAN access devices) for connecting the branch site to the hub site of the WAN link, as well as firewalls and proxy servers to manage network traffic. If the branch site network is segmented, the site may have additional routers. A complete design of the network infrastructure, including network servers, is out of scope for this guide, but some infrastructure components can affect how services are deployed. Additional design considerations related to the branch infrastructure and other network components include the following questions:

* **Location of centralized services**. In the case of cross-site connections (such as when a branch site must connect through a regional hub to get to services in a central hub), can the multiple links to the hub that must be traversed to consume services provide the appropriate levels of service?
* **Local Internet access**. Will Internet access be provided through a central Internet access point in the hub site, or will it be provided locally from the branch site? Is Internet access needed at all for branch sites? This design decision affects the configuration of Web caching, proxy support, and DNS name resolution.
* **Security impacts**. Will the configuration of any firewalls and proxy servers constrain performance or availability? Are there any exposures related to the use of a public network?
* **Routing limitations**. Will IP routing between branch sites pose performance or availability problems?
* **Network Address Translation (NAT)**. Is NAT required, and will it impede service operation?

You should record this information because it can serve as the starting point for development of a complete branch site topology after completion of the design process.

# Security Considerations

To ensure appropriate security for branch offices, you must create a logical infrastructure that provides appropriate security boundaries and containment of exposures without preventing cross-organizational access. You must examine the tradeoffs that are associated with the design options for each service. Tradeoffs are generally tied to the following issues:

* The security exposures related to WAN traffic to and from the branch office.
* The security exposures related to storing data on branch site servers.
* The physical and other security characteristics of the branch office, including methods of controlling physical access to servers located in the branch office.
* The sensitivity of the business functionality (data confidentiality and other security factors related to the business and its processes).
* Security exposures related to external companies who are responsible for server maintenance, including potential security risks involved with providing administrative privileges to personnel over which the organization has no control.
* Auditing issues with audit trails that cross multiple servers, as well as multiple geographic and political boundaries, which present a significant challenge to aggregating and analyzing the data.

Centralization of services in a hub site generally means that the services are run in a secure central facility with controlled access and well-defined enforcement methods, often with a dedicated security team that is responsible for the prevention and detection of security problems. This facilitates the enforcement of security policies and helps minimize security risks. Security in branch offices is often limited by the lack of consistent security procedures and dedicated security personnel, and is at greater risk from more open physical access, sometimes with the potential for many people to have access to the physical computer. These risks can make it extremely challenging to effectively secure branch site data and other branch site resources, as well as any corporate data and resources that are shared with or replicated to the branch office.

Although placing services in a hub site introduces the potential for exposure of data traveling between the hub site and the branch office, the sophistication of technologies that are now available to encrypt network traffic can sufficiently mitigate this risk.

Other security considerations and tradeoffs exist for individual services and business requirements. A branch site design that provides appropriate security requires a detailed security plan that identifies potential security risks and outlines mitigation strategies.

# Management Considerations

Management of the branch infrastructure requires not only appropriate management of IT services, but also appropriate monitoring, maintenance, and other functions to ensure the ongoing viability of the services. Manageability is generally a reflection of the IT organization, but it is also dependent on how processes and technologies are deployed for monitoring, management, and maintenance of IT services. The most common differences between service manageability of a central site and of a branch site relate to the consistency and repeatability of the functions that provide manageability at that site.

In general, placement of services in the central site is the most cost-effective and efficient way to monitor, manage, and maintain services. However, other relevant manageability considerations exist, as described in the following list of design considerations for central and branch office placement:

* **Effectiveness**. If the management approach is centralized, well-defined, and consistent (standards-based), policies, processes, and tools usually provide very efficient and cost effective solutions. However, centralized systems can be time-consuming and expensive to implement and maintain, which can present barriers to improvements to the processes and tools. In a decentralized model, the manageability is typically more complex to monitor, manage, and service multiple branch components, especially across a limited bandwidth link. If the services are managed by local personnel in the branch office, levels of support may not be consistent. The reason for this is that a lack of standards and automated processes and tools (including lack of tracking and evaluation processes and tools) can make it difficult to measure efficiency or cost effectiveness. Branch site processes are usually more open to interpretation and innovation because strict justification of deviations from standards is not required and branch site processes can be more flexible and agile.
* **Responsiveness**. A centralized model may not be able to provide immediate assistance for problem resolution or other issues because of high numbers of support requests, which are often queued as part of a central ticketing system. Automation in central sites can facilitate responsiveness, but any changes that are required in automated support may be expensive and slow to implement (or may not be feasible unless the problem being resolved is significant enough). A distributed model may provide faster turnaround time because of the small number of systems, but it generally does not provide support 24 hours a day, seven days a week.
* **Support levels**. The central site probably offers support 24 hours a day, seven days a week because of the number and location of systems and the variety of business functions supported (and the time zones in which different functions operate). It also typically features a good replication of skills in the support group. At a branch office site, it is harder to justify support 24 hours a day, seven days a week or replication of skills. Support may be jeopardized by vacation schedules and illness.
* **Communications**. In centralized management, it is generally efficient and easy to keep everyone up-to-date because of the small size of the management group and the processes in place. After the services are distributed it can be difficult to maintain communication across branch offices and between a branch office and central site, due to the number of branch offices and the variations in processes and technologies in each branch office.
* **Optimization**. It is generally easier to optimize a centralized environment because the model is generally well understood and stable. Scalability of centralized servers facilitates optimization of hardware and software. A distributed environment can be difficult to optimize because of the more changeable nature of the branch office and the resultant lower level of experience with systems and processes. If running isolated services (on separate servers), it is difficult to optimize hardware and software usage.
* **Serviceability**. This can be easier in close proximity to the IT organization, both because of physical access to devices and the advantages of being able to manage services over a LAN. Local management in the branch site can easily service components because of physical proximity and management over a LAN. If managed from a central location, WAN performance and availability, combined with the lack of physical proximity, can challenge serviceability.
* **Backup, restore, and recovery**. A centralized solution is generally very automated and efficient. Offsite backup and recovery, especially for disaster recovery, is common. Managing this service locally can be complex, especially on consolidated servers that are running services with very different requirements.
* **Administrative model**. A centralized service is usually consistent, with well-defined IT roles that are distinct from the business management roles. A distributed model can be complex, and consolidation might present significant challenges, including the following:
* Appropriate separation of administrative roles, duties, and responsibilities if specific services require separate administrators.
* Domain administration (if domain controllers are located in the branch office and organization policies prohibit branch site administrators from being domain administrators).
* **Vendor support**. It is generally more cost-effective to put contracts in place for multiple services at a single location. In a distributed model, it can be costly to establish multiple contracts with a single or multiple vendors. Some vendors may have limited service areas that do not include all of an organization’s branch offices, which prevent the standardization of vendor contracts.

# Summary

This guide provides the foundation on which the BOIS is built, covering the critical architectural elements that determine how best to approach the design of the individual services in your implementation. The taxonomy introduced in this guide forms the fundamental terms that are used to communicate the various components of a branch office solution.

Understanding these high-level approaches influences the design of each service in the IT infrastructure. No matter what your preferred approach is, you should expect to find that a wide range of external factors may force your services to depart from your preferred approach. This is the nature of designing for branch office environments: whether you like it or not, compromise is a major component of any large organization’s branch office infrastructure. If you understand and manage these compromises, your designs will have a far greater chance of success, and if you ignore these compromises, you will risk major failures along the way.

The information provided in this guide is the starting point for the design of your Windows Server 2008–based branch office infrastructure solution. You should check the BOIS Web site often to receive additional news, guidance, and information about branch office design.

# Additional Resources

For more information about the topics and technologies described in this guide, please see the following resources:

For more information and guidance about BOIS, see:

http://[www.microsoft.com/branchoffice](http://www.microsoft.com/branchoffice)

For more information about the features that are available in Windows Server 2008, see the Windows Server 2008 TechCenter at:

[http://technet.microsoft.com/en-us/windowsserver/2008/](http://technet.microsoft.com/en-us/windowsserver/2008/default.aspx)

For more information about reduced profile server core installations, see the Server Core Installation Option for Windows Server 2008 Step-by-Step Guide at <http://go.microsoft.com/fwlink/?LinkID=105293>

For more information about server virtualization in Windows Server 2008, see the Windows Server 2008 Hyper-V TechCenter at <http://go.microsoft.com/fwlink/?LinkId=101268>

## Feedback

Please direct questions and comments about this guide to satfdbk@microsoft.com.