

# [Term paper on managing a merger](https://assignbuster.com/term-paper-on-managing-a-merger/)

[Business](https://assignbuster.com/essay-subjects/business/), [Company](https://assignbuster.com/essay-subjects/business/company/)

## Key considerations behind establishing trust relationships between the two domains

Trust between domains refers to the relationship between domains that enables a domain controller in one domain to authenticate the users in another domain (Gibson, 2001). All domain trust relationships have two domains: the trusted domain and the trusting domain. The types of trust include Forest, Realm, External, and Shortcut (Gibson, 2001). For the purposes of this paper on Quality Corporation (Quality. ad) and Crescent Inc. (Crescent. ad), these considerations regard the Forest Type domains. There are several considerations in the establishment of trust relationships between domains.
The first is the characterization of the trust into one of these four categories; one-way, transitive, two-way and non-transitive. The one-way trust is a single trust relationship in which domain A trusts domain B the authentication requests are passed on from the trusting to the trusted domain (Hoffmann & Beaumont, 2005). It is worth noting that each time someone creates a new child domain, another two-way transitive trust relationship is created. Gibson (2001) defines a transitive trust as one whereby the trust relationship that is extended to one domain is automatically extended to any other domain that is trusted to the parent domain. The new transitive relationship operates between the child domain and the parent domain. As such, the transitive relationships flow upward from the main tree thereby creating transitive trusts between all the domains in the principal domain tree.
The administrators of the two domains also need to consider the Name Resolution. The administrators need to resolve the names across the two forests and they need to set up the Domain Name System (DNS) to resolve the names (Shinder, 2001; Gibson, 2001). The three commonest ways to do this are; using Stub Zones, Conditional Forwarders, and Secondary Zone Transfers (Microsoft. com, 2014). The Conditional Forwarders are much easier to configure and troubleshoot as compared to the Zone Transfers. The administrators using the Conditional Forwarder need to know the Internet Protocol (IP) address of the target DNS and the domain name of the domain housing the DNS server to which the configuration is being done (Microsoft. com, 2014).
Using the Conditional Forwarders may not be efficient because the changes in the authoritative childe server result in changes for the parent server, which must be configured manually using new IP addresses that are generated during the change process (Goldman & Skamarock, 2007). Secondary servers are efficient because they maintain a list of the authoritative DNS servers to be used by the secondary copy of the zone. In addition, the list is updated as DNS servers get added and removed from the target domain. However, it is more complicated to configure and the administrator can expose the IP address to unwarranted parties (Goldman & Skamarock, 2007).
The other consideration is the setting up of one-way incoming forest domain for one side of a two-way trust. First, one needs to open Active Directory Domains (AD domain) and Trusts. The AD domains are grouped into tree structures. The AD domains can have multiple child or dependent domains, which can have their own child domains. Moreover, the authentication within the AD domains works through transitive trust relationship. Using the AD domains, one can identify the DNS name. In this case, the company names (Quality AD. and Crescent AD) can be the public domain name and they can serve as the DNS names (microsoft. com, 2014). The sub-domain and the alternate names can also be the same as the DNS name.

## The other key considerations are the security considerations. These considerations focus on

- Security settings for the Interforest Trusts
- The potential threats to the established Interforest Trusts
- The interaction between the Securing trusts and the other Window Technologies
- The requirements for minimum administrative credentials for all securing trusts
Administrators can use two types of security enhancement to secure the settings for the Interforest Trusts. These are; Security Identifier (SID) filtering and Selective Authentication. SID forest filtering involves prevention of malicious users who have administrative credentials from controlling a trusting (Gibson, 2001). Selective authentication on the other hand involves lessening the attack surface through the restriction of the quantity requests that can pass through an Interforest Trust.
In considering the potential threats to Interforest Trusts, the administrators can consider the attacks from malicious users in trusted forests and the threats posed by malicious users in a rival organization. Selective authentication can be used to address these potential threats from an external party.
Thirdly, the system expectations such as the Active Directory Federation Services (AD FS) should be weighed for adherence to security issues against other window technologies. Goldman and Skamarock, (2007)assert that all the technologies that go into the combined systems the merged company must be supportive and collaborative of each other in the enhancement of security for the entire system supporting the Core Network Services.

## Consolidating Core Network services

The merger of two companies requires the respective IT teams to build combined infrastructure and consolidate networks that are secure, reliable, and cost effective. The teams need to develop flexible and open IP Address Management (IPAM) solution that can map all the networks connected to the system. A solution by BlueCat Solutions called the DNS/DHCP Server (Domain Name System (DNS)/Dynamic Host Configuration Protocol (DHCP) maps all network connections into a single view (microsoft. com, 2014). This can enable deep understanding of business issues. The system can allow administrators to address security concerns. In case there are divestitures, one can separate and segment networks easily and address any concerns (microsoft. com, 2014). The system also allows for scalability without the need for re-architecture and there are no obstacles in business growth.
This system operates on the merging of the DNS and the DHCP aspects of the network. The DHCP is a networking protocol that has been standardized for use on IP networks (microsoft. com, 2014). It distributes network configuration parameters dynamically. The distributed parameters include IP addresses for services and interfaces. When using the DHCP, computers in a system request for and get automatic assignation of IP addresses and other networking parameters from a DHCP server (Gibson, 2001). This eliminates the requirement of an administrator to configure the settings manually.
The integration of the DNS and DHCP is an effective way to consolidate the network services of Crescent Inc and Quality Ad. The two combined systems associate the Transmission Control protocol (TCP) and the IP address that had been assigned by a DHCP to a client together with its Fully Qualified Domain Name (FQDN) (microsoft. com, 2014). The mapping of a domain name to an IP address requires a change in the address or the name must be updated on the DNS. Since DHCP, protocol does not update the DNS automatically, in case of change of IP address by a DHCP server, then servers running on Windows Server 2008 and 2012 can register with DNS in order to allow for cooperation between the two. All of the following three reasons can trigger a dynamic update; removal, addition, or modification of IP addresses in the Transmission Control Protocol (TCP) properties that have been configured for any of the installed network connections (microsoft. com, 2014). Secondly, when there is change in the IP lease or a renewal of any of the installed network connections with the DHCP server. Thirdly is when there is a command that manually refreshes or restarts the client name registration in the DNS such as the registerdns/ipconfig command (microsoft. com, 2014).
The DHCP and the DNS remain updated when they are synchronized. However, using the two together on may present problems when the systems are using static and old DNS servers that are unable to interact dynamically when the DHCP configurations change. Administrators can avoid these incidences if they upgrade the old and static DNS servers with those that can support DNS dynamic updates (Goldman & Skamarock, 2007). The administrator can also assign IP addresses to reservations that have infinite lease duration for the DHCP clients who use DNS and do not support Net BIOS (Basic Input/Output System).
In case the DHCP and the DNS core services fail, the business stops, because websites become inaccessible, and all network-dependent applications including CRM (customer relationship management), ERP (Enterprise Resource Planning) and Voice Over IP (VOIP) fail to function and their users are not able to find cloud services or virtual machines. The BlueCat DNS/DHCP server ensures business connectivity and resolves these issues by consolidating Core Networking Services effectively (microsoft. com, 2014).
The solution offers a comprehensive view of all network connections and devices to the consolidation. In addition, it also allows for the identification of policy gaps that can expose the network to risks (microsoft. com, 2014). The overall system enables for the migration of the DHCP, IPAM, and DNS systems to single system of record. It also reduces the network expenditures through the consolidation of operations, facilities, and resources (microsoft. com, 2014). In all, the solution enables for the central management of all devices that are connected to a given network.

## Integrating both AD forests and elimination of duplication of service

Prior to Quality Corporation (Quality . ad) and Crescent Inc. (Crescent. ad) getting into a merger, each of the two companies had its own fully functional networking systems. Each had their primary DHCP, DNS and Domain Controller servers and several secondary servers located in other cities away from the headquarters. As such, the integration of both networks should avoid duplicating the services previously rendered by each company. Instead, the companies should merge to create synergy in the delivery of services. Already a plan has been laid out to consolidate the core issues of the DNS and the DHCP, and to ensure a smooth transition in the assignation of IP addresses and the changes that come with the changes. Since both companies are running server 2012 as the domain controllers and it has advanced capabilities and capacities, it should be able to accommodate the consolidated core services.
Crescent Inc has developed several enhancements for the widgets that Quality Corporation produces. Shinder (2001) observes that widgets being softwares to be used for the web bear limited functionality. Once they are installed within a web, an end user can execute the applications. The widgets simply occupy a portion of the webpage and find useful information from other websites. Since Crescent has produced enhancements that Quality Corporation produces and both companies are set to merge, then the best way to ensure efficient consolidation of the web services is through the Active Directory Federation Services (AD FS).
The AD FS ought to set up in the servers currently being used by Quality Corporation in the server 2012 operating system. According to Hofman and Beaumont (2005) windows server 2012 has efficient IP management roles and has a deeper support of cloud computing services. In addition, server 2012 has excellent deduplication or the elimination of duplicate and redundant information. The server does this by supporting the specialized data compression and elimination of duplicate copies on New technology File Systems (NTFS) volumes (microsoft. com, 2014). The elimination of duplication provides more storage for data in the hard drives. In addition, windows server 2012 has the IIS 8, which gives the administrator the options of logging into additional custom fields from the response or the request headers or from server variables (microsoft. com, 2014). This feature gives windows server 2012 centralized certificate management. It allows for better provision of identify information, is resistant to forgery and retains all security aspects of digital certificates.
The Federation Services creates a highly extensible, secure identity and internet-scalable solution that can operate across multiple platforms that use windows as well as non-windows environments (microsoft. com, 2014). Since the Flexible Single Master Operation (FMSO) roles are located on Server01, which is located at the Quality HQ, then the AD FS needs to be installed and operated from the Quality Corporation server. For the Crescent. ad domain, the FSMO roles are located on RWDC01, which is located at the Crescent HQ and, therefore, these ones serve as the user accounts that will need authentication and approval of their credentials prior to them accessing information contained in the Quality servers. Moreover, the Quality. ad has several servers that are configured as Certificate Authorities while the Crescent. ad domain has a single Certificate Authority. This gives the Quality. ad domain more security rights and ability to host the AD FS and become the central server in the merger of the two networks.
In essence, AD FS being an identity access solution shall offer browser-based clients with seamless access to several protected internet applications. This will happen through the applications and the accounts that are located in the two organizations and networks. In the current scenario, the engineering documents are located in the ServerDocs at the Austin office thereby presenting a challenge in the consolidation of Core Network Services by the Quality Inc engineering team. The web server that hosts the ServerDocs is under Quality Corporation’s management and the user accounts in Crescent’s network will be required to provide secondary credentials when they attempt to access the application. The AD FS retains the authenticity of the certificates that preserve the security of each of the networking systems for both Quality Corporation and Crescent Inc.
The above scenario is solved by setting up AD FS in Quality’s server so that it can offer credentials to Crescent and making the most appropriate authorization decision in the process. One can install the AD FS after installing the windows server 2012 by going to the list of tasks and clicking on “ add roles” then the “ Active Directory Federation Services”. The Microsoft Management Console (MMC) manages the AD FS server roles (Hofman & Beaumont, 2005).
The AD FS runs four main server roles. Firstly, the AD FS runs federation service in this case the federation servers installed at Quality Corporation head quarters at Austin, route authentication requests from user accounts from Crescent Inc. Secondly, the federated servers can run the role of Federation Service Proxy (FSP). This role operates in the perimeter network, the screened subset, or the demilitarized zone (Microsoft. com, 2014). Here, the FSP uses the WS-Federation Passive Requestor Profile (WS-F PRP) protocols in the collection of user credential information from relevant browser clients. It then sends the user credential information to the federation service (Microsoft. com, 2014). Thirdly, the AD FS can play the role of Claims-Aware Agent. This role enables for the querying of the AD FS using the claims-aware application present in various web servers. The querying entails security token claims after which the Ad FS can make personalized application and authorization decisions. Fourthly, the AD FS can play the role service of Windows token-based agent. This application uses windows-based authorization mechanisms to support conversations emanating from AD FS security token to an impersonation level (Microsoft. com, 2014).
The AD FS makes the secondary accounts and the credentials thereof unnecessary by providing trust relationships that can be used to project each user’s access rights and digital identity to trusted partners. A federated environment allows each of the organizations to continue managing its identities although the two can also project and accept identities from other organizations in a secure manner.

## References

Active Directory Federation Services Overview. (n. d.). Active Directory Federation Services Overview. Retrieved June 13, 2014, from http://technet. microsoft. com/en-us/library/cc772593(v= ws. 10). aspx
Gibson, D. (2011). Microsoft Windows networking essentials. Hoboken, NJ: Wiley Pub..
Goldworm, B., & Skamarock, A. (2007). Blade servers and virtualization transforming enterprise computing while cutting costs. Indianapolis, Ind.: Wiley Technology Pub..
Hofmann, M., & Beaumont, L. R. (2005). Content networking: architecture, protocols, and practice. Amsterdam: Morgan Kaufmann.
Integrating DHCP with DNS. (n. d.). Integrating DHCP with DNS. Retrieved June 13, 2014, from http://technet. microsoft. com/en-us/library/cc771732. aspx
Shinder, D. L. (2001). Computer networking essentials. Indianapolis, IN: Cisco Press.