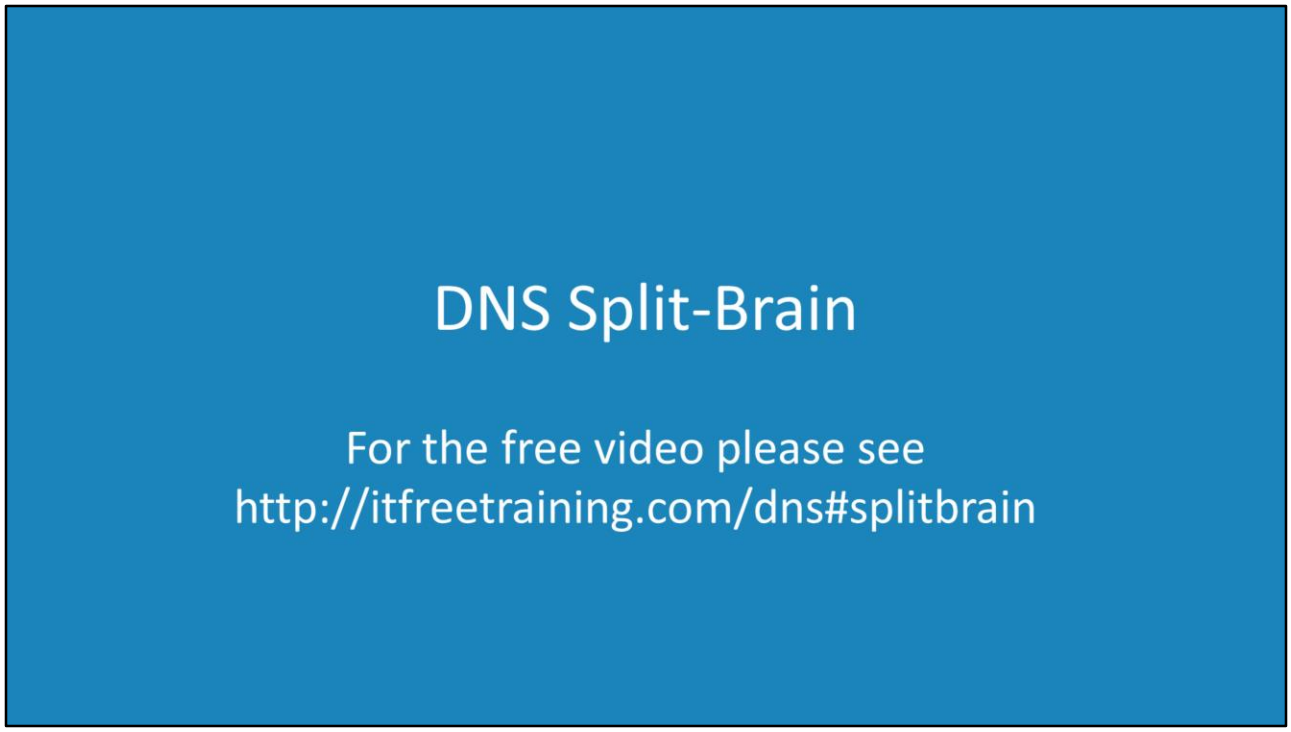
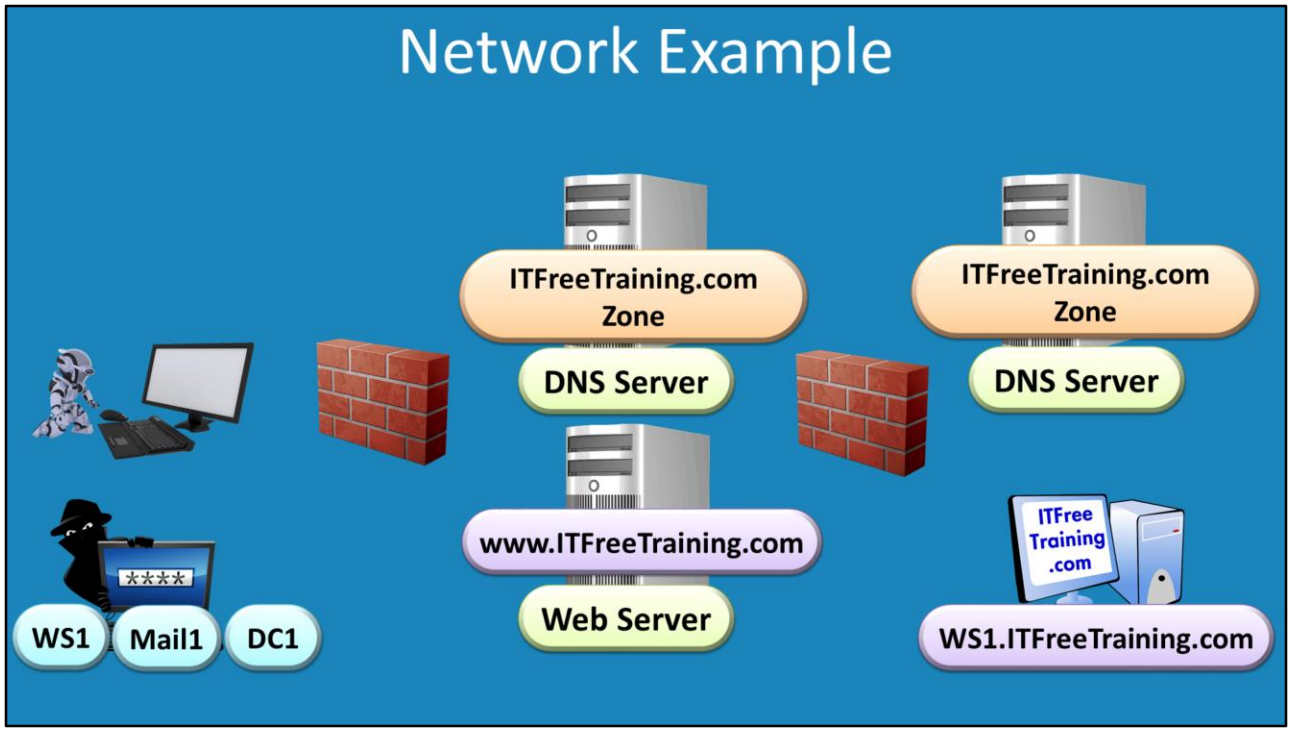
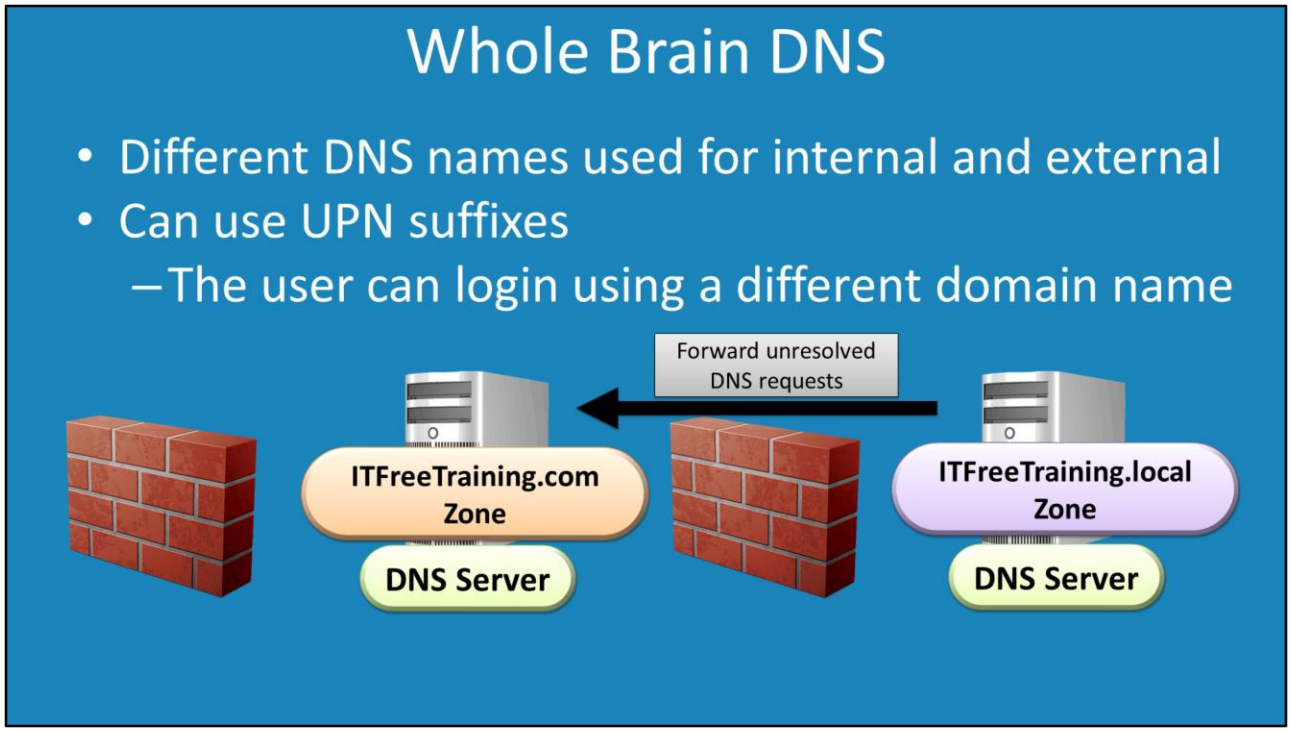


Split-Brain DNS is when the same DNS name is used for internal and external clients. This video looks at the problems associated with Split-Brain and how it may be configured to get around these problems. The choice of Split-Brain or the alterative whole brain approach is up to the individual administrator to decide which approach is best for the network that they support.



Network Example

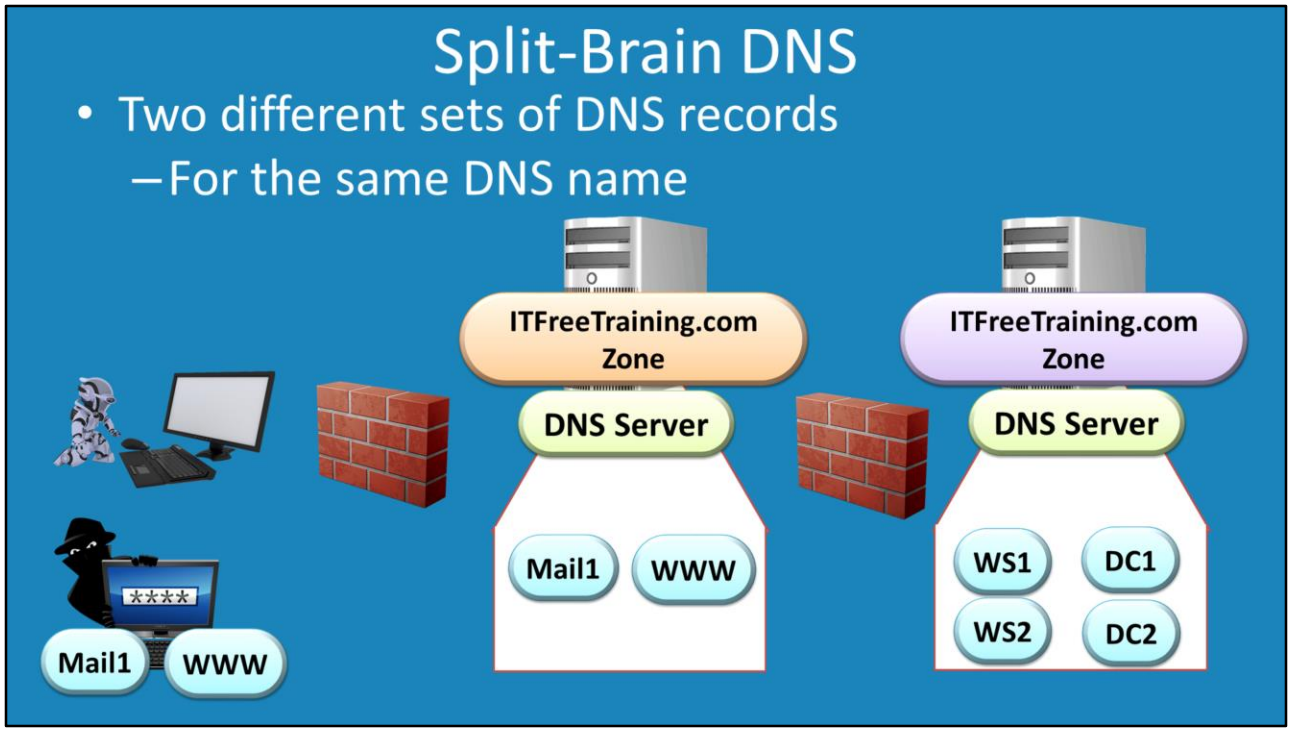
If you use the same DNS name for the internal network and the external network, the simplest way to implement this would be to use the same zone data on the internal and external network. The problem with this approach is twofold. Firstly this means that the internal DNS records are now exposed to the internet and a hacker may get this information. Using this information, the hacker can foot print the network and gain a good understanding of how many clients and what types of services you have on the network. The second problem is that internal clients may use different IP addresses to access resources than external clients. For example, the company web site may have an external IP Address but the routing on the network does not correctly route internal clients to the web page. In order for this to occur, the internal clients must use an internal IP Address. The DNS server will not know which IP Address to respond with.



Whole Brain DNS

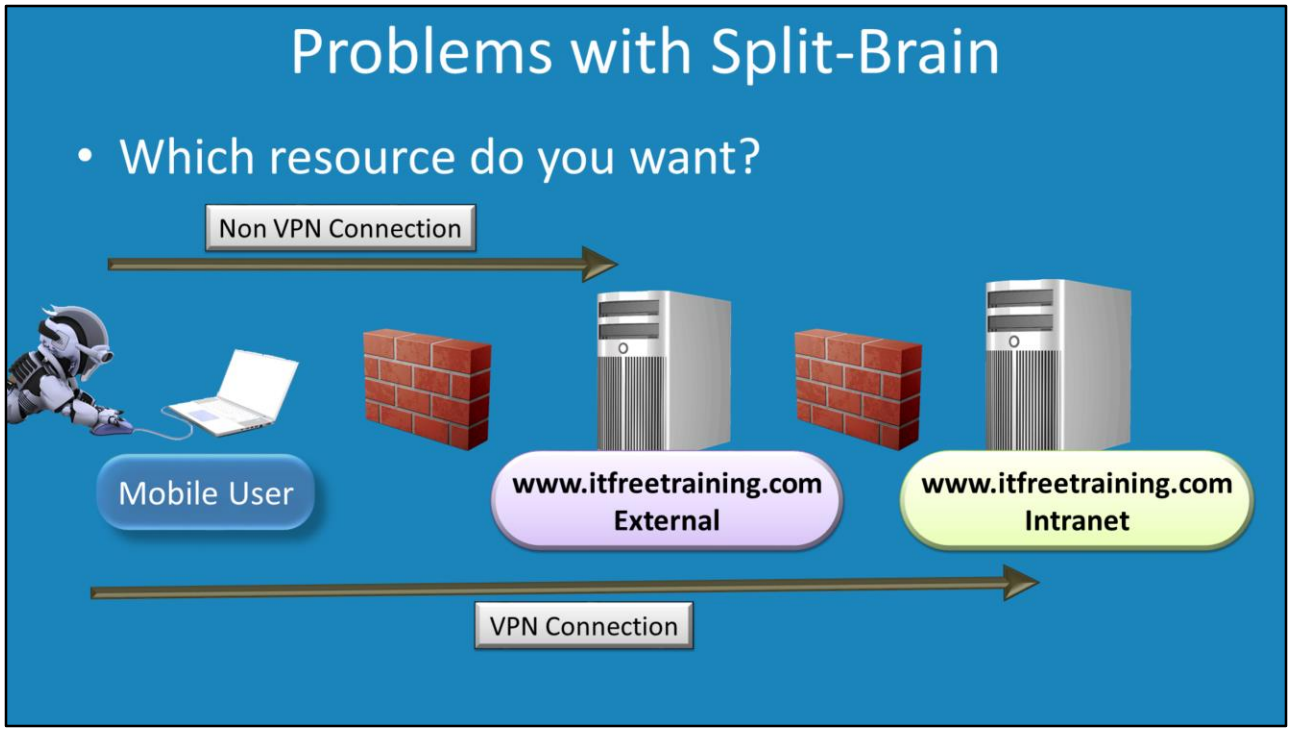
The whole brain approach is when different domain names are used for the internal and external network. A common approach is to use .local for internal networks and .com for external networks. Using this approach it is quite easy to understand and set up for the administrator. It does however make it a little more complex for the user and thus you are making a trade off from a simple network to look after to one that is more complicated for the end user to use. Using the whole brain approach means that if a hacker were to gain access to the DNS records in the .com namespace, these DNS records are publicity available anyway so this is not really a security concern. The .local records are used on the internal network and thus a lot harder for a hacker to gain access to these.

If the internal DNS server cannot resolve a DNS request, for example it is asked for the IP Address of google.com, this DNS request can be forwarded to the other DNS server which can resolve it. This adds additional security to the network meaning that the internal DNS server does not have to communicate directly with the internet.



Split-Brain DNS

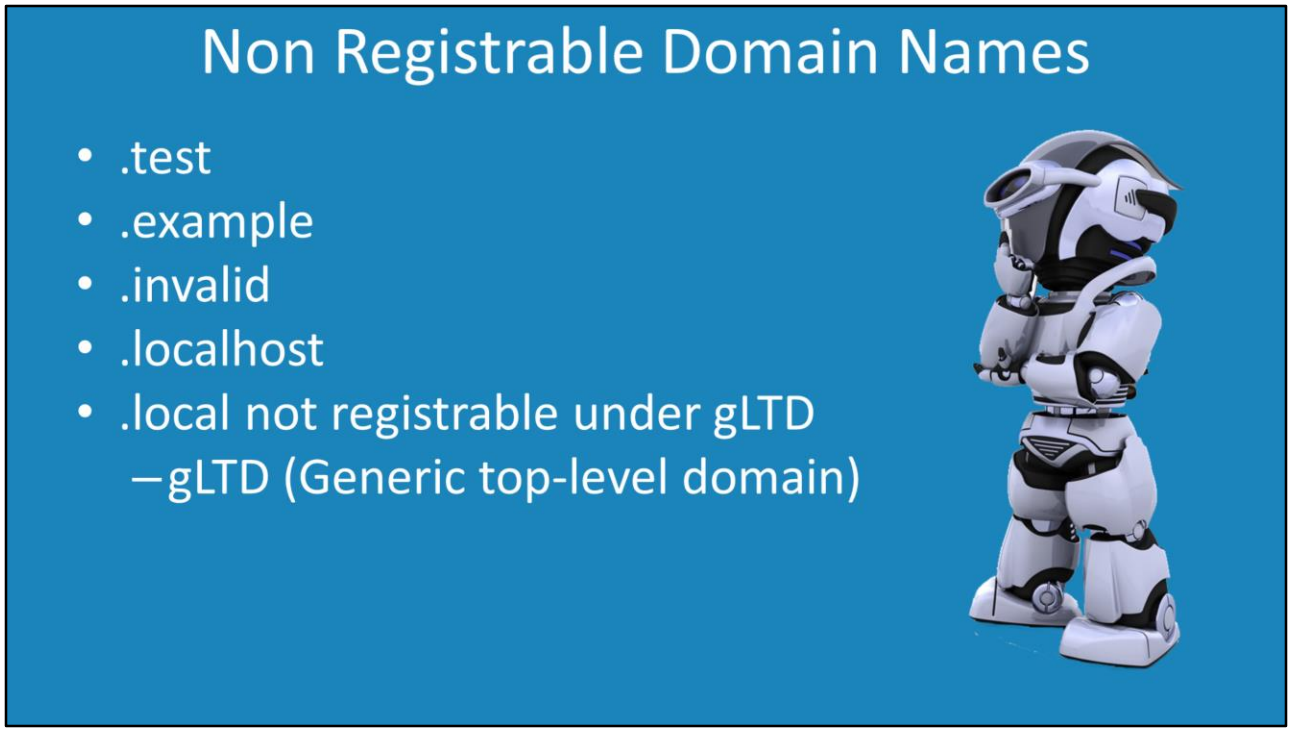
The best way to implement split-brain is to have two different zone files for the same DNS name. The internal DNS server would hold its own set of DNS records while the external DNS server would hold a different set. This means that if an attacker was to gain access to the external DNS server, they would only be able to gain access to DNS records that are publicity available.



Problem with Split-Brain

The problem with Split Brain is that depending on how a user accesses the network will determine which resources they will be directed to. The most common example is when the user connects via a VPN connection. When connected via a VPN connect the user will be accessing the network just like they were in the office. If you have resources with the same name, like web server or mail servers, the user may be directed to the wrong service. This can become more complicated when you have companies with different offices and divisions around the world. Making sure the user is directed correctly can become quite difficult.

When a user connects using a service like DirectAccess, DirectAccess has the ability to configure rules which will direct the user to resources based on their connection. Although this is possible, it does make it more difficult for the administrator as the rules need to be configured.



Non Registrable Domain Names
There are a number of domain names ending in the following that will never be able to be registered. These are .test, .example, .invalid and .localhost. Under gLTD (Generic top-level domain) it is possible to register domain names ending in keywords like .apple, .xbox etc. In order to get one of these domain names, a company must put in an application and have it approved. This is a long process and a company must show just cause and meet a number of requirements in order to get the top level domain. It is nowhere as simple as registering a domain name. If a company attempted to register the top level domain name .local this would be declined. This means that you are safe to use domain names ending in .local even though it is not listed as a non registrable domain name.

See http://YouTube.com/ITFreeTraining or http://itfreetraining.com for our always free training videos. This is only one video from the many free courses available on YouTube.

References
"MCTS 70-640 Configuring Windows Server 2008 Active Directory Second edition" pg 449-451
"Split-Brain DNS" http://technet.microsoft.com/en-us/library/ee382323(v=ws.10).aspx
"Footprinting" http://en.wikipedia.org/wiki/Footprinting
"gTLD Applicant Guidebook Version 2012-06-04
"http://newgtlds.icann.org/en/applicants/agb/guidebook-full-04jun12-en.pdf 2-9 to 2-10