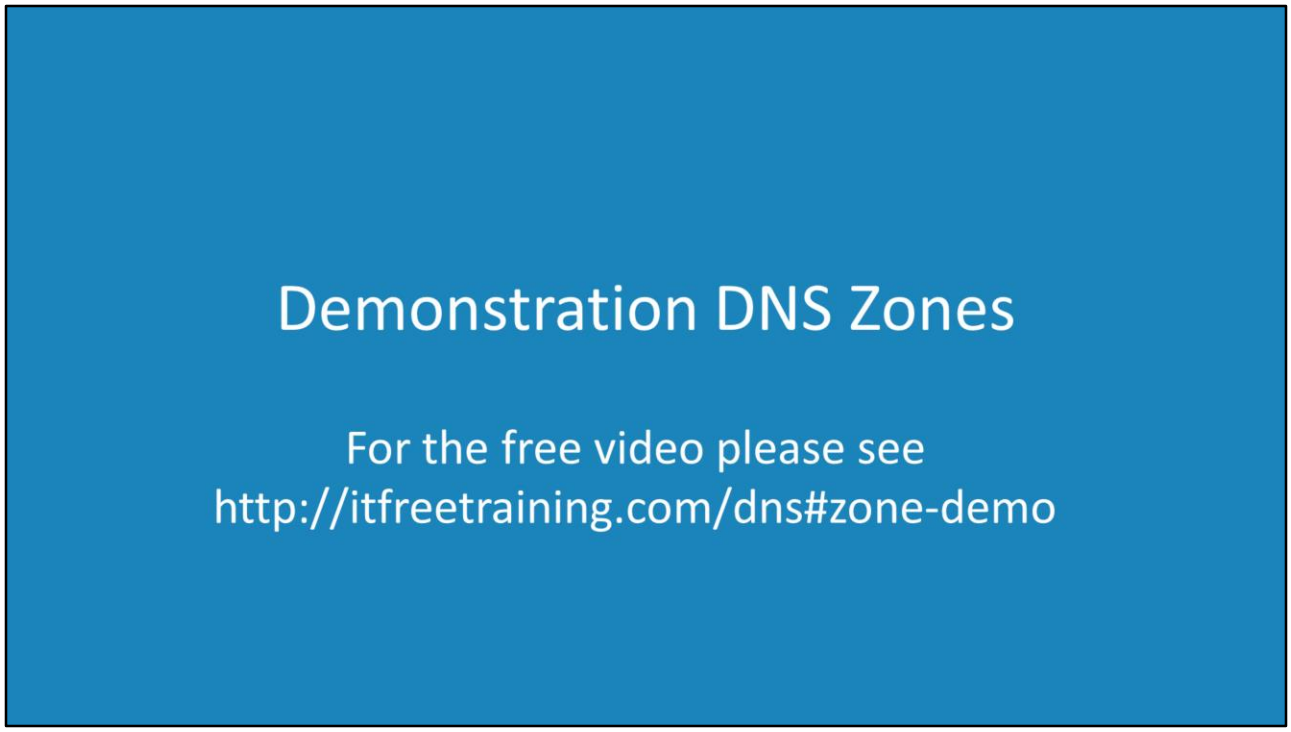
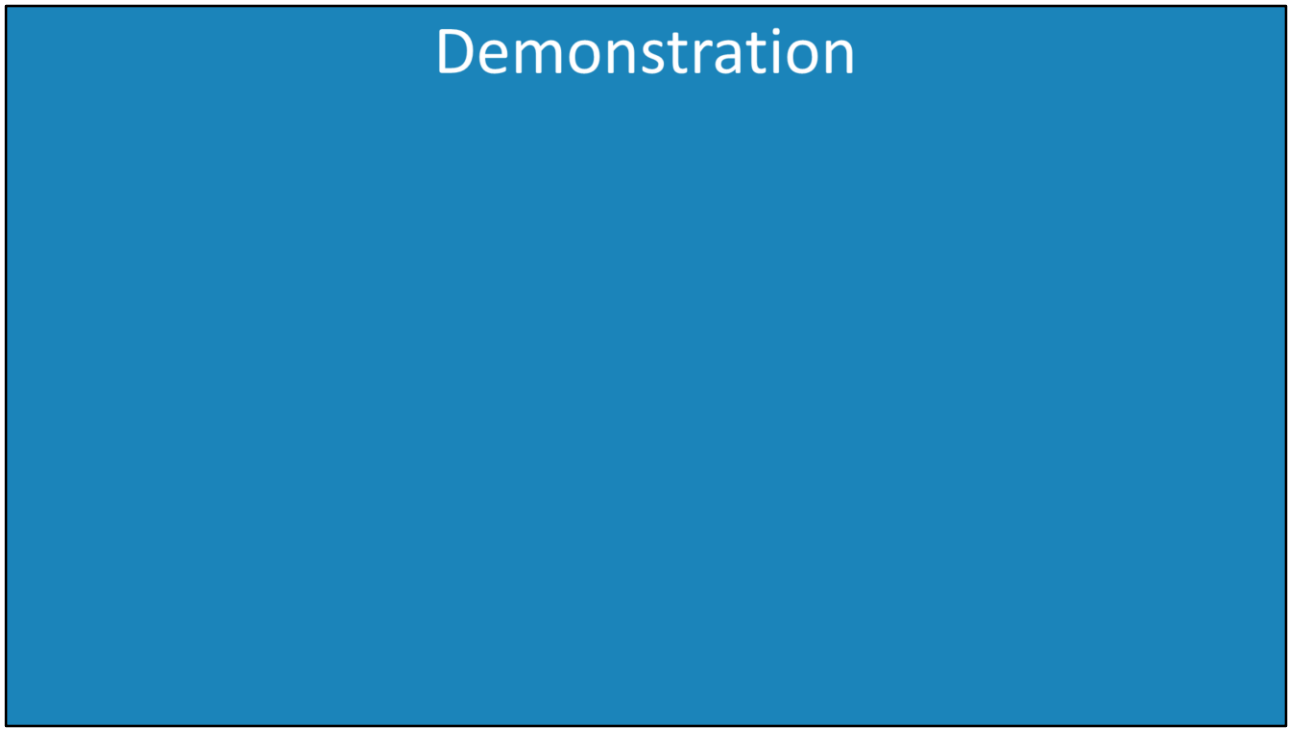


This video will look at how to create primary, secondary, stub zones, and reverse look up zones using Microsoft DNS server. The video also looks at how to replicate changes between different zones. By the end of video you will be able to create the correct zone for your replication needs inside your company and also to external companies.

Copyright 2013 © http://ITFreeTraining.com



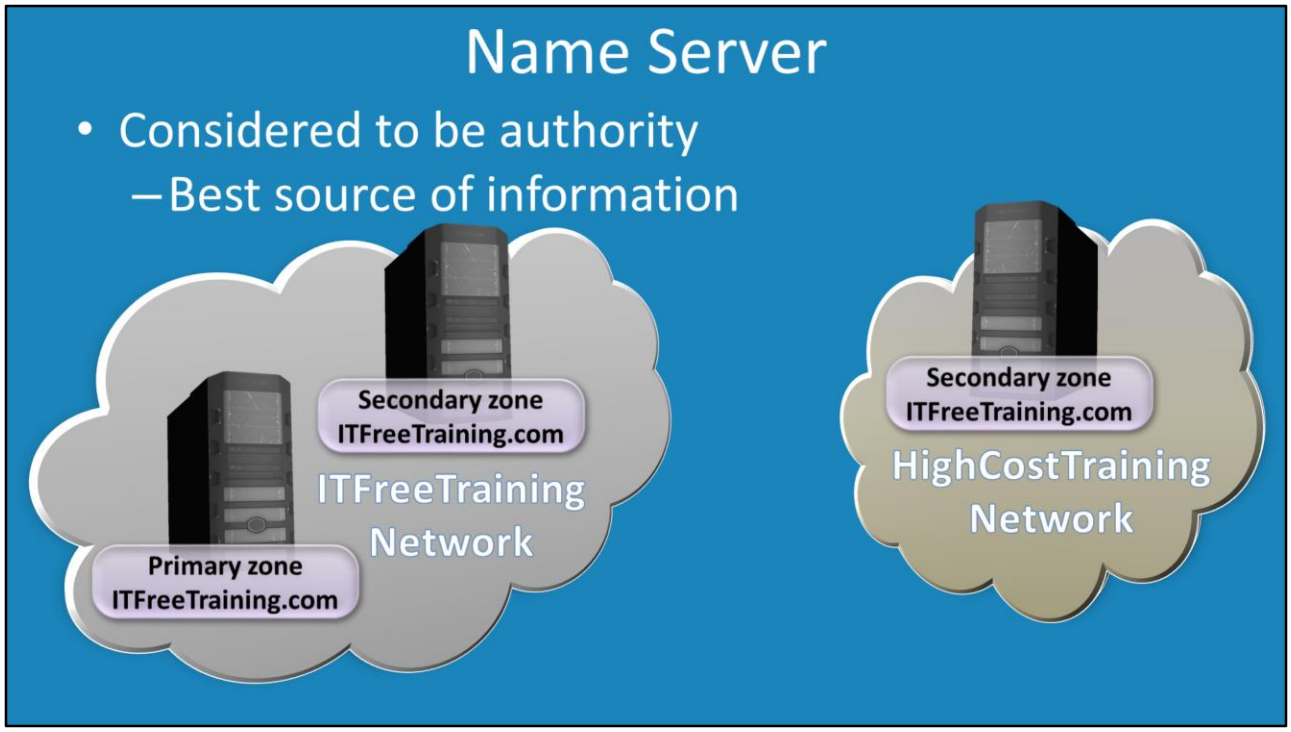
Demonstration
This video uses Remote Server Administration Tools (RSAT) on Windows 8. To install, see the following link. http://itfreetraining.com/tools

To open DNS Manager, open charms by moving the mouse to the top right hand corner of the screen and then perform a search for dnsmgmt.msc
If you receive a prompt for the server, enter the name of the server that is running DNS. In this case, DNS is running on the Domain Controller NYDC1.
When you expand down through DNS Manager, there is a section called Forward Lookup Zones. This section will contain all zones except for reverse look up zones. In this case, a domain exists so the zone ITFreeTraining.local has automatically been created and DNS records have been added to it. To find out more information about a particular zone, right click the zone and select properties.
In the properties of the zone, at the top is section called type. This will tell you if the zone is Active Directory Integrated, Primary, Secondary or Stub zone. If you want to change the type of zone, press the button “change” next to it.
On the change zone type “dialog”, if you un-tick the option “Store the zone in Active Directory (available only if DNS server is a domain controller)”, this will remove the zone from Active Directory and store it in a text file. If the zone file is stored in Active Directory, it will be available from any Domain Controller in the domain that has DNS installed on it. It may also be available to other Domain Controllers with DNS installed on them if the replication for the DNS zone is configured for forest wide replication.

Copyright 2013 © http://ITFreeTraining.com

If a zone is changed so it not stored in Active Directory, dynamic updates will be changed to none. Secure dynamic updates are only available for Active Directory Integrated zones. If you have a non- Active Directory Integrated zone, it can only support secure updates if non-secure updates are allowed as well.
To connect to another Windows DNS server, right click DNS at the top and select the option “Connect to DNS Server” and then enter in the name of the computer that you want to connect to.
To create a new zone, right click on Forward Lookup Zones and select the option “new zone” to launch the new zone wizard. From the wizard, select the zone that you want, these can be primary zone, secondary zone, or stub zone. If the option “Store the zone in Active Directory (available on only if DNS server is a writeable domain controller” is grayed out, DNS is not installed on a server that is a Domain Controller. If you are creating a new secondary zone, the wizard will ask for the name of the DNS zone and then ask for an IP Address of a master zone. This can be any DNS server that has a copy of the DNS zone and does not matter if it is Active Directory Integrated, Primary or Secondary. If you receive an error message stating “Validation error, please try again later” it is most likely that the other DNS server has not been configured to replicate zone data.
To configure a zone to allow zone transfers, right click the zone and select properties. From here, select the tab “zone transfers”. In order to allow other DNS servers to transfer zone data from that zone, the option “Allow zone transfers” needs to be ticked. By default this option is not ticked. There are 3 different options available. These are, “To any server”, “only to servers listed on the Name Servers tab” and “Only to the following server”. If you select the option “to any server”, this will allow zone transfers to anyone who asks for it. This can be used by a hacker to gain information about the network, called foot printing. If your DNS server is behind a firewall, this may be an acceptable security risk. If the option “Only to servers listed on the Name Server tab” is selected, then only DNS servers that are listed on the Name Server Tab in the properties for that zone will be allowed to receive zone transfers. If you want to use this option, you need to ensure that the DNS server that you want to receive zone transfers is listed on the Name Servers tab. If it is not, you can add it manually.

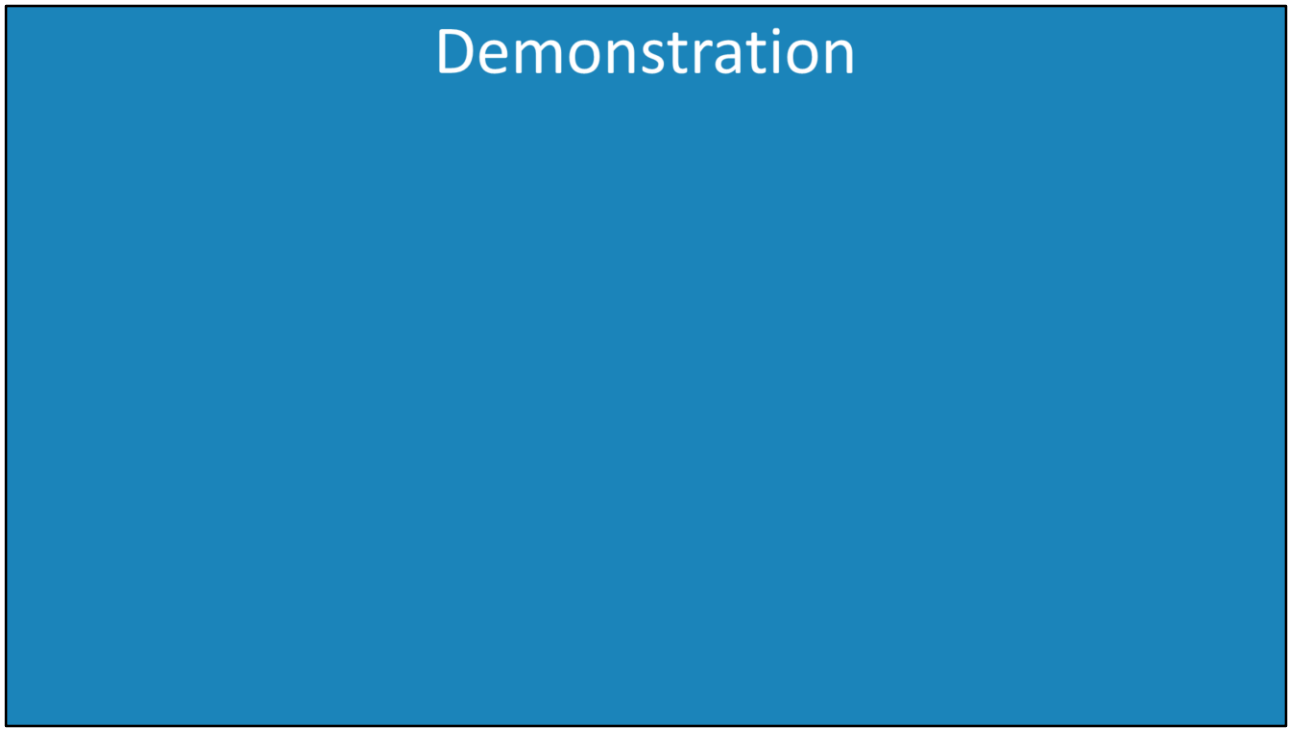
Copyright 2013 © http://ITFreeTraining.com



Name Server

A name server record points to a DNS server that is considered to be an authoritative for that zone. This means that the DNS server holds an up to date DNS records. This does not mean that the DNS zone has to be a primary zone. A DNS server can hold a secondary zone and still be considered authoritative. The point to remember is that the DNS zone needs to be up to date. In this example, a secondary zone is found in the ITFreeTraining network and the HighCostTraining network. It would make sense to make the DNS server in the ITFreeTraining an authoritative DNS server. This is because the DNS server on the internal ITFreeTraining network will always be keep up to date. In the case of the DNS server in the HighCost Training network, this DNS server may not be always up to date as changes on the HighCost Training network may affect the ability of the DNS server to obtain updates. Since the HighCostTraining network is an external network and can be supported by different IT people, there is no guarantee that this DNS server will always be up to date as changes on the High Cost Training network may prevent this from happening.

Copyright 2013 © http://ITFreeTraining.com



Demonstration

To add a new Name Server, on the Name Servers tab press the button add and then enter in the name of the server that you want to add. If you press the resolve button, Windows will attempt to resolve the hostname given. You may receive the error message stating that “The server with this IP address is not authoritative for the required zone.” This is normal since the DNS server has not been added as yet, it is not yet an authoritative DNS server.

Given enough time the DNS zone file will replicate itself. If you want to start the process manually. Right click the zone and select the option “Transfer from Master”. At any time, you can press the F5 key to force a refresh of the data shown on the screen.

In the properties of any zone there is a tab called “Start of Authority (SOA)”. This tab shows the replication information for the zone. At the top is the serial number. Each time a change is made to the zone, this number is increased by one. A secondary zone on another server only needs to compare this number with the DNS server that it is replicating with to determine if it has the latest version of the DNS zone data. In the middle of the tab is the settings “Refresh Interval” and “Retry Interval”. The refresh interval determines when the second DNS server will check for updates on the other DNS server. If it cannot contact this server, the retry interval will determine how long it will wait until it tries again.

If the DNS zone data is stored in a text file, you can read this text file in the folder c:\Windows\system32\dns

Copyright 2013 © http://ITFreeTraining.com

To create a stub zone, right click forward look up zone and select new zone. For the new zone wizard, select the option stub zone.
If you decide to store the zone in Active Directory, the wizard will ask how the zone file is to be replicated in Active Directory. You can choose between the domain, forest and windows 2000 compatibility options if you are using Windows Server 2000 servers on your network.
Like a secondary zone, you need to enter in a DNS name for the zone and also a DNS server where requests for this DNS name can be forwarded to. You may get an error saying “Validation error, please try again later”. This can occur if security has not been configured on that DNS server to allow this DNS server access. Since a stub zone only accesses the SOA and NS servers which are generally available to the public anyway, it is generally safe to ignore this message.
A reverse look up zone is not required for day to day activity. They are generally used for troubleshooting. To create one, right click on reverse look up zone and select new zone. The new zone wizard is much the same as when creating a forward look up zone. This includes the replication scope option if the zone is being stored in Active Directory and dynamic update options.
When creating a reverse lookup zone you have the option to create a reverse lookup zone for IPv4 or IPv6. For IPv4 addresses, you can enter a long or short address as you wish. The wizard will automatically create the required subnet mask depending on the value that you enter. If you enter in an IPv6 address, you will need to add the number of bits used in the network prefix to the address in order for it to work.

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
“Name server” https://en.wikipedia.org/wiki/Name_server

Copyright 2013 © http://ITFreeTraining.com