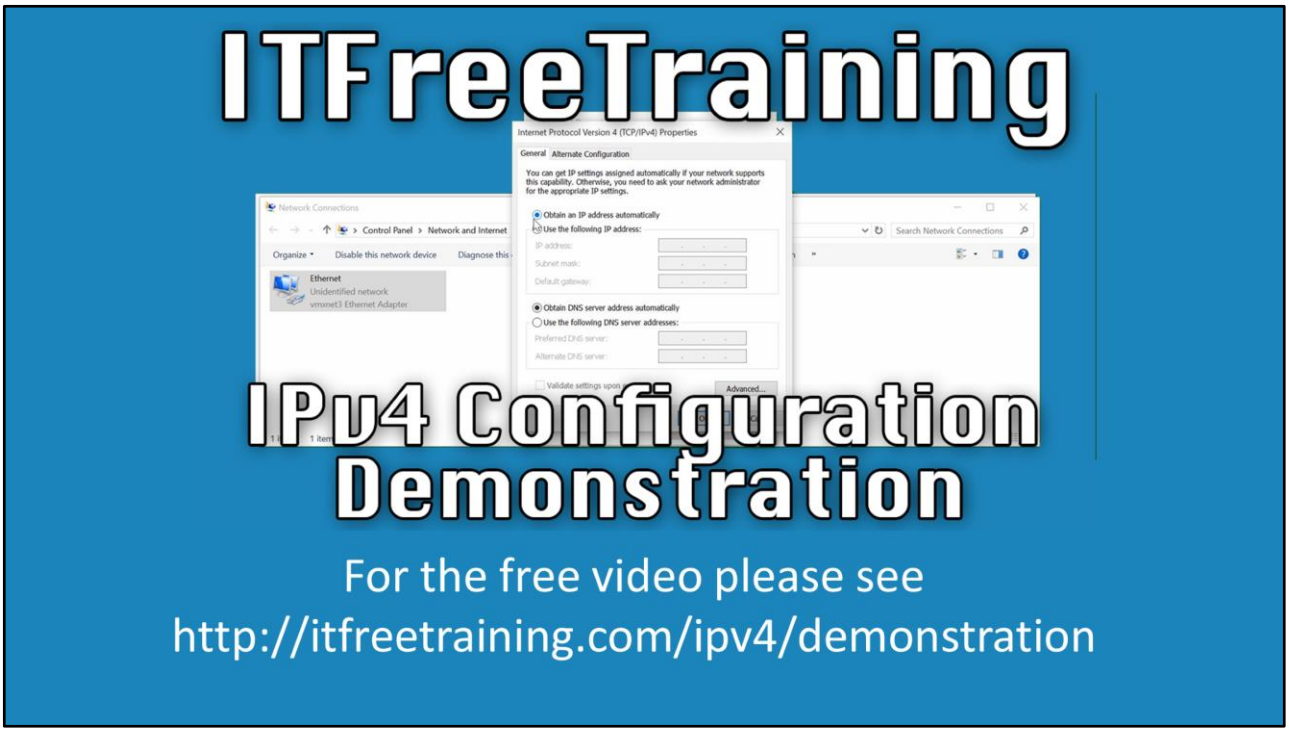
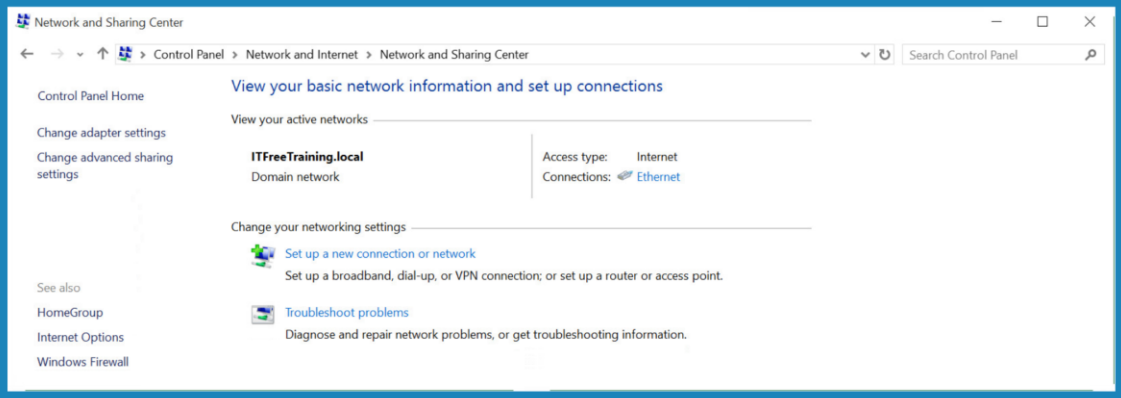


IPv4 Configuration Demonstration
In this video from ITFreeTraining, I will look at how to setup and control the IPv4 protocol as well as quickly touching upon how to configure the IPv6 protocol, since some of the configuration is very similar. However, in the IPv6 course, I go into a lot more detail about IPv6. Understanding how to configure these protocols and what options you have available to you is a valuable skill for an administrator to successfully configure and setup networks.

Access the rest of the course: http://ITFreeTraining.com/ipv4
Download the PDF handout:
http://ITFreeTraining.com/handouts/ipv4/demonstration.pdf

Network and Sharing Center

- Central area for management and configuration
- Show maps of current network



Network and Sharing Center

0:27 – To configure networking on Windows, first open the control panel.

0:35 – From the control panel, select the option “Network and Internet”.

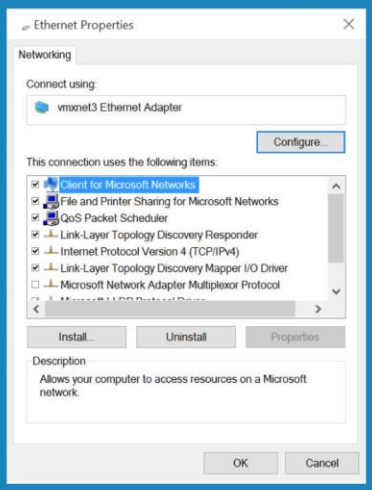
0:40 – From “Network and Internet” select the option “Network and Sharing Center”. The “Network and Sharing Center” provides a central area for management and configuration of networking in Windows. It provides a quick way to access wizards to configure networking, for example creating a VPN or a new connection as well as a map of the local network. “Network and Sharing Center” shows which networks the computer is connected to. This includes physical network cards and also connections via devices like VPNs.

1:11 – To configure the networking on one of the network adapters on this computer, select the option on the left “Change adapter settings”. This will show all the connections that are currently physically installed or configured. For example, a VPN connection may use a special network adapter in order to operate. In this case, the physical network adapter will appear and also the VPN connection will appear.

1:36 – To configure the network adapter, right click the adapter and then select the option “Properties”.

Network Adapter Properties

- Contains clients, services and protocols



Network Adapter Properties

1:43 – The network adapter properties contains clients, services, and protocols.

1:51 – At the top, is “Client for Microsoft Networks”. This allows the computer to access resources on a Microsoft network. For example, access a Microsoft network share. It is also possible to add additional clients, for example add a client for Novell networks.

2:08 – Below this is services. The first service is “File and Printer Sharing for Microsoft Networks”. This, as the name suggests, allows this computer to perform file and printer sharing to be used by other computers on the network. If the administrator wanted to disable file and printer sharing, it would be a simple matter to untick this service. If the service is unchecked, this will effectively render all file and printer sharing as disabled on that system. Usually the administrator would disable file sharing through the control panel as unchecking the service here will also disable administrator shares.

2:45 – The next service is Quality of Service (QoS) Packet Scheduler. The default setting reserves 20% of the bandwidth for services like Windows Update and license renewal. It is possible to alter this percentage through using Group Policy. If you uncheck this option, no bandwidth will be reserved meaning that 100 percent of the bandwidth can be utilized for software running on the computer. However, if the computer is transferring a lot of data for extended periods of time, it can potentially prevent updates and other Windows features and functions from working.

3:18 – At the bottom are the protocols. The first protocol is “Link-Layer Topology

Discovery Responder" otherwise known as LLTD. This is a technology developed by Microsoft that enables data to be obtained from computers on the network that then can be used to create a map *of* the network. This service responds back to LLTD requests. This means that other computers on the network can send requests to this computer and it will respond back. For example, using LLTD will allow other computers to identify what operating system is being run. Having the protocol appear here, however, does not mean that it will respond to LLTD requests. If LLTD were to be disabled, it would not reply to LLTD requests. Unchecking the protocol will ensure that the computer will *never* respond to LLTD requests even if it is enabled in the operating system.

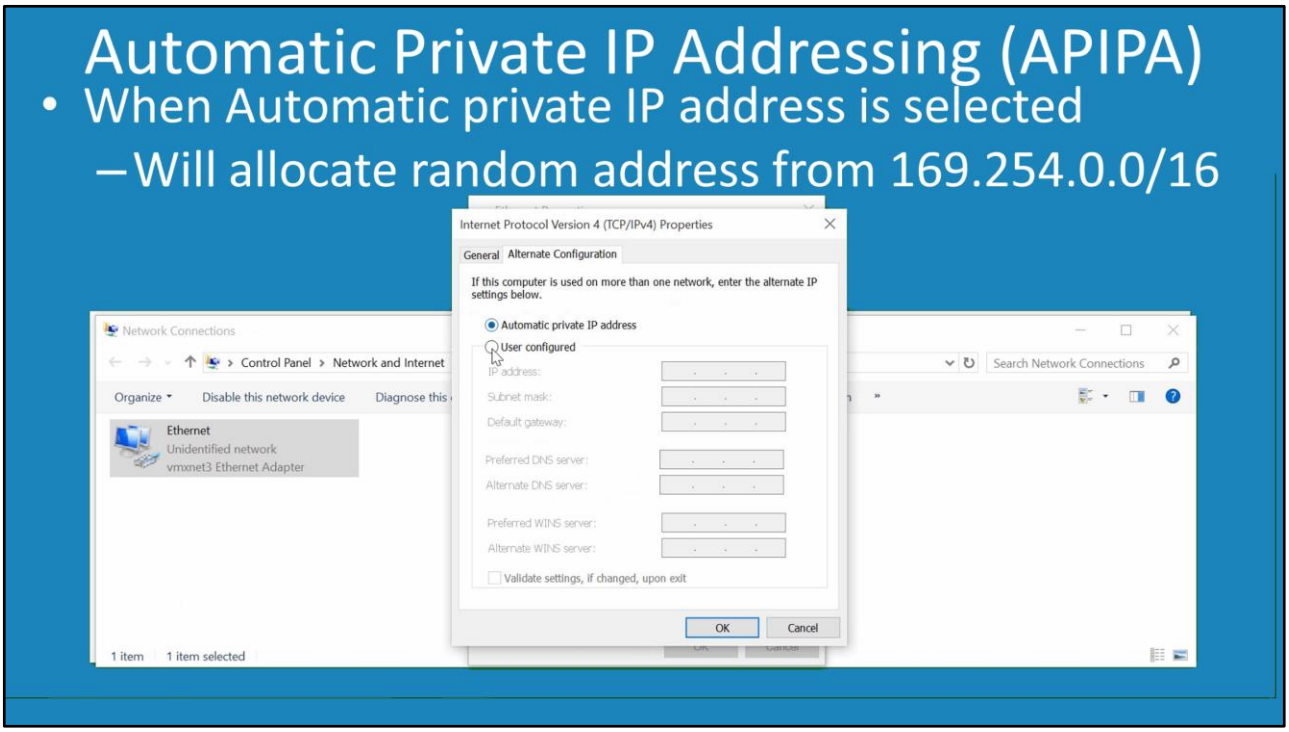
4:17 – The next protocol that I will look at is the "Link-Layer Topology Discovery Mapper I/O Driver". This protocol controls the sending of LLTD messages. This sends data about this computer using LLTD on the network so that other computers can use LLTD to build a network map.

4:36 – After this, you will see the protocol "Microsoft Network Adapter Multiplexor Protocol". This should be unchecked by default, unless you are using NIC teaming in which case this will be checked and all other items will be unchecked. NIC teaming is when multiple network cards are used in conjunction to create the one network adapter. This protocol is used by the NIC team to communicate with each physical network card.

5:04 – The next protocol is "Microsoft LLDP Protocol Driver". This is similar to LLTD in that it enables devices to transmit and communicate information to each other which can be utilized to develop a network map. The difference is that this protocol is a vendor neutral protocol. LLTD is a Microsoft specific protocol. I will next select the protocol Internet Protocol Version 4. This is where the administrator will configure IPv4.

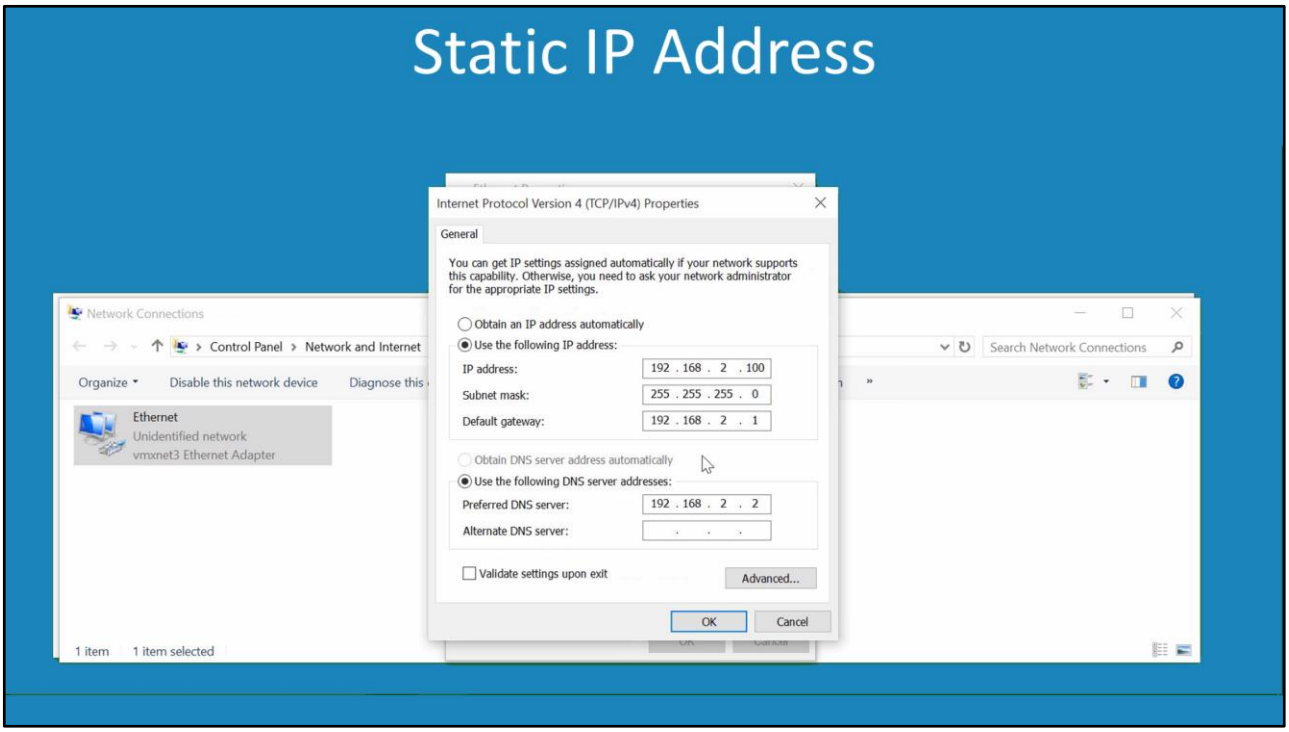
5:35 – Make sure "Internet Protocol Version 4 (TCP/IPv4)" is selected and press the Properties button. By default, the setting "Obtain an IP address automatically" will be selected. When this setting is selected, Windows will always attempt to contact a Dynamic Host Configuration Protocol (DHCP) server in order to obtain an IP Address.

5:50 – Below this, notice the option "Obtain DNS server address automatically". When this is selected, Windows will attempt to obtain the IP Address of a DNS server or servers from a DHCP server. On most networks, a DHCP server will be running which allocates IP Addresses to clients. On a home network, the network device that is used to connect to the internet will in most cases be configured as a DHCP server. If the computer is plugged into a network that does not have a DHCP server configured, the administrator may want to configure network settings that will be used in this case. If I select the tab, "Alternate Configuration", this is where the settings are configured that are used when Windows cannot contact a DHCP server.



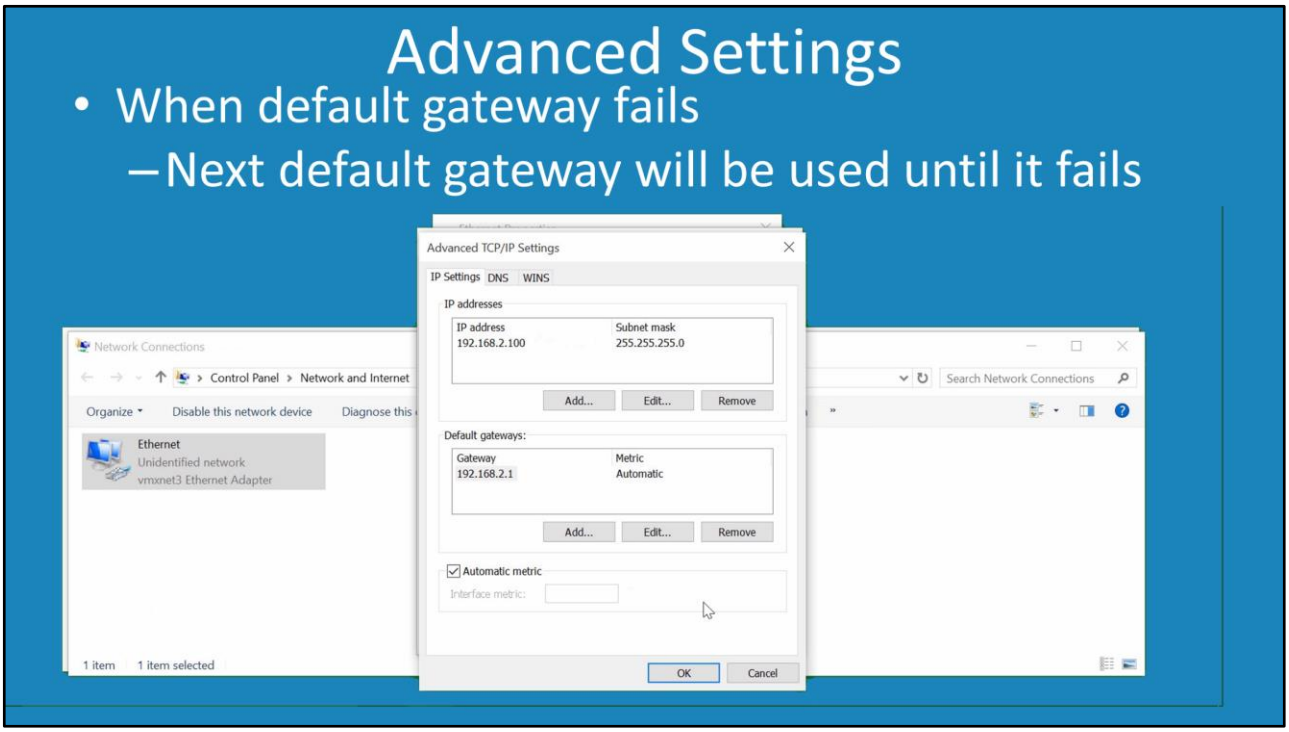
Automatic Private IP Addressing (APIPA)

6:37 – By default, the option "Automatic private IP address" will be selected. When this is selected, and when Windows cannot obtain an IP Address from a DHCP server, a random IP Address will be used. This will start with 169.254. The idea is that if multiple computers are connected to the same network that does not have a DHCP server, the computers will be able to communicate with each other. However, this IP Address is not routable on other networks or the Internet. If the administrator wants to configure their own fallback IP settings, the option "User configured" can be selected and then the details can be configured below this. This is useful to the administrators when they have a computer that connects up to a network that does not have a DHCP server and they want to use their own configuration when this occurs. However, the computer at other times will connect to networks that do have DHCP servers, so static configuration in this case would not make sense.



Static IP Address

7:40 – On the General tab an IP Address can be configured. To do this, select the option “Use the following IP address” and enter in an IP Address, subnet mask and default gateway. When an IP Address is configured like this it is referred to as a static IP Address. Below this, the option “Use the following DNS server addresses” will automatically be selected. For this, enter in an IP Address for a DNS server. On most networks there will be two DNS servers. In this case I will only enter in the one, or at least only one for the moment. This is all the basic configuration that is needed to communicate on the network and have traffic routed through to the Internet. In some cases, more configurations may be required. To configure more settings, I will press the Advanced button.



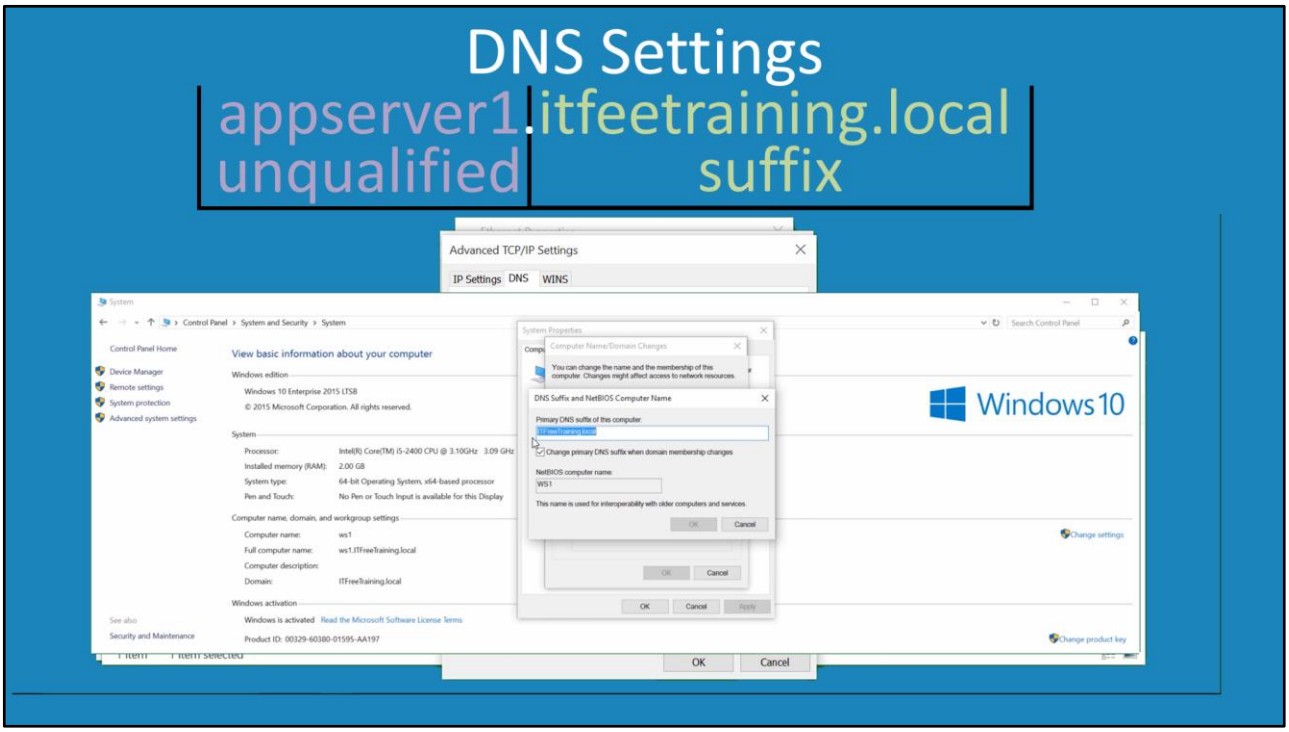
Advanced Settings

8:40 – At the top, notice the section “IP addresses”. In some cases, the computer may need to be assigned multiple IP Addresses.

8:50 – To assign a second IP Address to this computer, press the Add button. This will allow a second IP Address and subnet mask to be entered in.

9:00 – Once the IP Address is entered in, press the Add button, and the second IP Address will be added. When multiple IP Addresses are assigned to the same computer like this, it is referred to as multihoming. An example of when this may be used is with servers. For example, a particular service may be being moved from an old server to a new server. The older server is shut down but the clients are still attempting to access it via the older IP Address. The solution is to give the new server the IP Address of the old server. It can now respond to requests on the old server’s IP Address and the IP Address the new server has. When all the clients are using the new server’s IP Address, the old IP Address can be removed. This concept also applies to the section below for default gateways.

9:50 – In this example, a second default gateway will be added. Additional gateways work differently from additional IP Addresses. Windows will use the one default gateway until it detects it’s not working. When this occurs, it will switch to the next default gateway. Windows will keep using the working gateway until it fails. So if the first default gateway becomes available again, Windows will not switch back to it.



DNS Settings

10:15 – Select the DNS tab. At the top, the DNS servers can be configured. Currently there is only one configured. It was possible to configure two on the previous screen; however, on this screen the administrator is free to configure more than two if they wish.

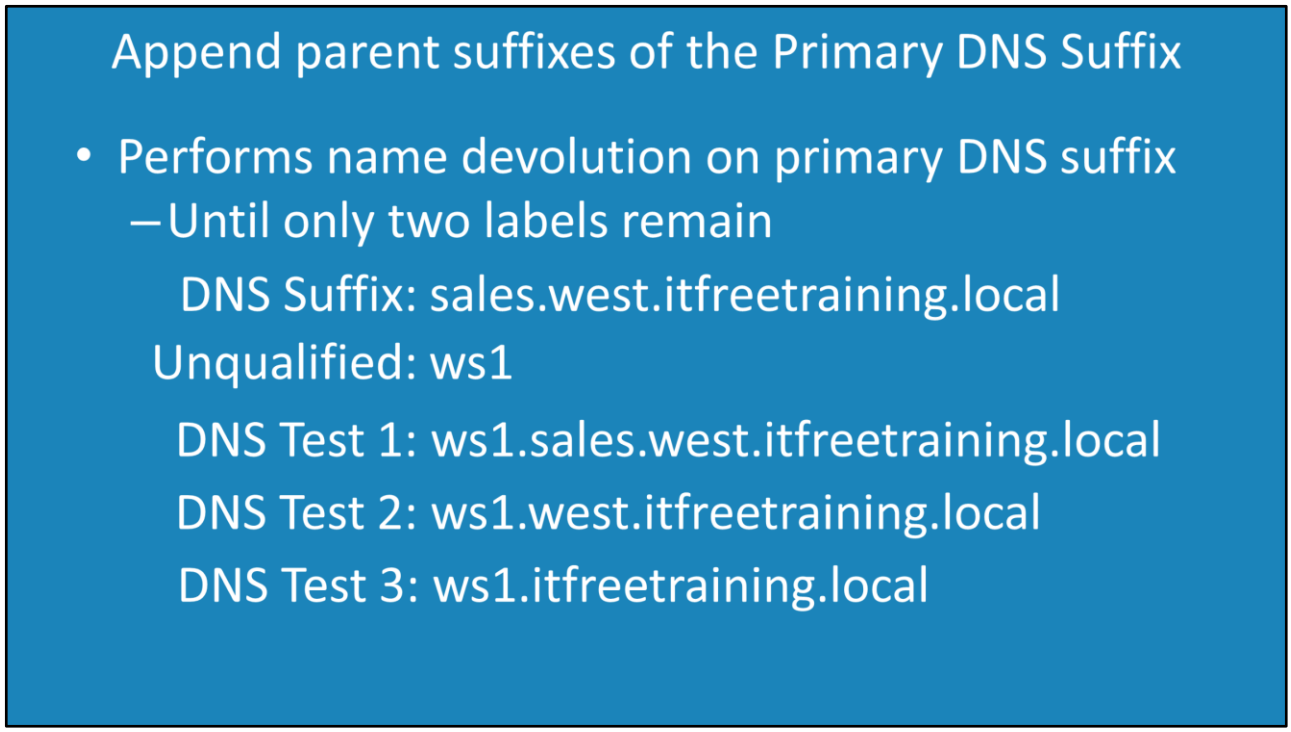
10:32 – Press the Add button to add a second DNS server. For most networks, two DNS servers are enough; on some networks three DNS servers are used. Keep in mind that when resolving names, each DNS server will need to be contacted. Having too many DNS servers can cause delays on unresolvable names since Windows will wait for each DNS server to be contacted and state that the name could not be resolved.

11:03 – Under DNS servers are the settings that can be configured for how unqualified names are handled. To understand what an unqualified name is, consider the following example. The unqualified name in this example would be the left-hand side, AppServer1. An unqualified domain name cannot be resolved by DNS, so a suffix must be added.

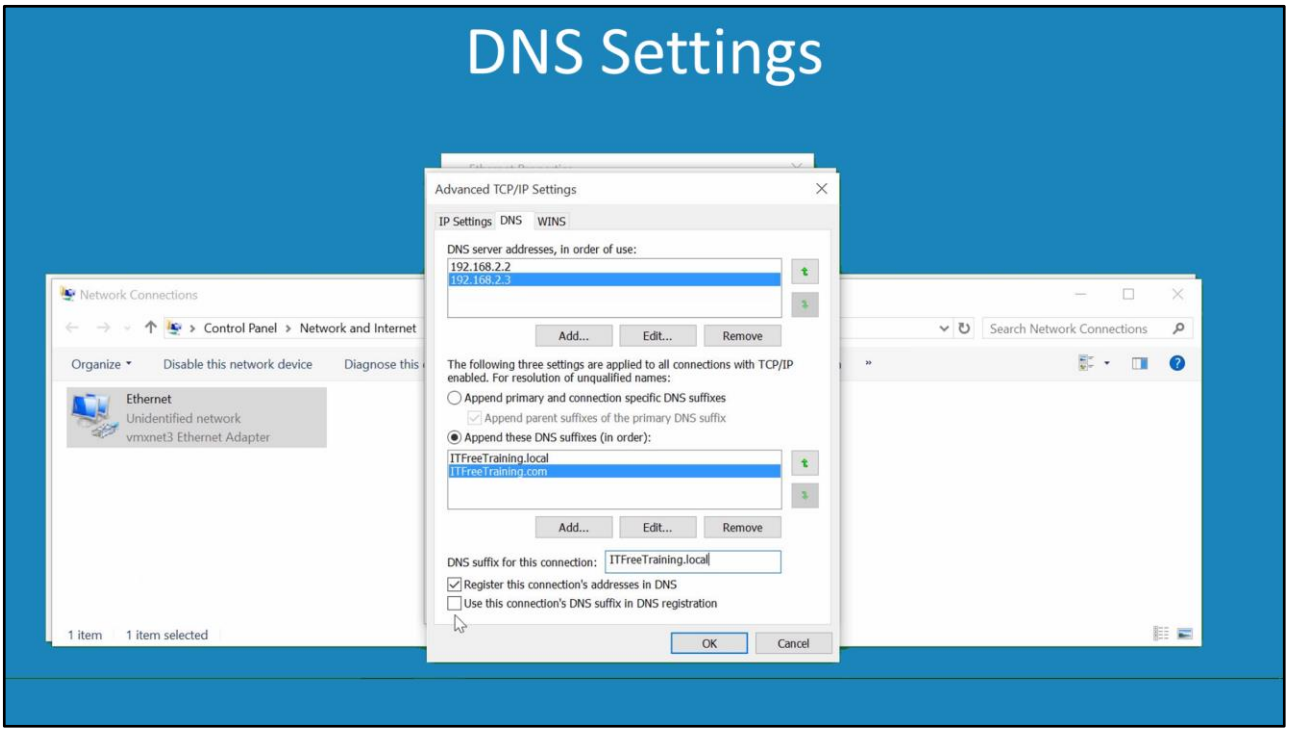
11:27 – To show this better, I will open a command prompt. When a ping is performed to an unqualified domain name, AppServer1, notice that this is resolved to an address. On closer inspection, notice that the suffix ITFreeTraining.local was added to the unqualified name. This was found by the DNS server and the IP Address returned. So the unqualified name had a suffix added to become a fully qualified domain name which the DNS server could resolve.

12:00 – Go back to the advanced settings, the settings at the bottom section

determine how a suffix will be added to an unqualified domain name. The top option is “Append primary and connection specific DNS suffixes”. The primary suffix is stored in the system properties. Open the control panel, select “Network and Internet” and then select “System”. This will show the basic information for the system.
12:33 – To see the primary suffix for the computer, next select “Change settings” under “Computer name, domain and workgroup settings”. This will show the System Properties.
12:42 – Next I will press the button “Change” and the press the button “More”. Notice at the top under “Primary DNS suffix of the computer” the DNS suffix ITfreeTraining.local. This is the primary suffix for the computer. By default, this is configured to the domain DNS suffix. This can be changed, but it is generally a good idea to keep them the same whenever possible. I will now go back to the DNS settings. So, you can see where the primary suffix comes from; however, it also mentions a connection suffix. This is configured further down in the “DNS suffix for this connection”. If you want to enter in a custom suffix for that connection, you are free to do this. So essentially when an unqualified domain name is being attempted to be resolved, the primary suffix and the connection suffix will be tried assuming a connection suffix has been configured.
13:44 – The checkbox below this, “Append parent suffixes of the primary DNS suffix” does not do anything given this example, so let’s look at an example where it *would* do something.



Append parent suffixes of the Primary DNS Suffix
13:57 – When this checkbox is checked, name devolution is performed on the primary DNS suffix until only two labels remain. So what does this mean? If in the following example this DNS suffix was configured, when an attempt is made to resolve an unqualified DNS name, the following will happen. First the complete DNS suffix is added to the DNS name and tested. The next step is to remove the left most label and test again. So in this example the sales label is removed and the test performed against the remaining suffix. If the name cannot be resolved, the next step is to remove another label and attempt to resolve the DNS name a third time. The tests stop here because the suffix has been reduced down to two labels -- the label ITFreeTraining and the label local. Since only two labels remain from the original DNS suffix, if the DNS name cannot now be resolved it will be reported back that the name is unresolvable. This option is very useful when you have a forest with subdomains. Having the option checked will ensure a computer in a child domain will test the parent domain when attempting to resolve unqualified names.

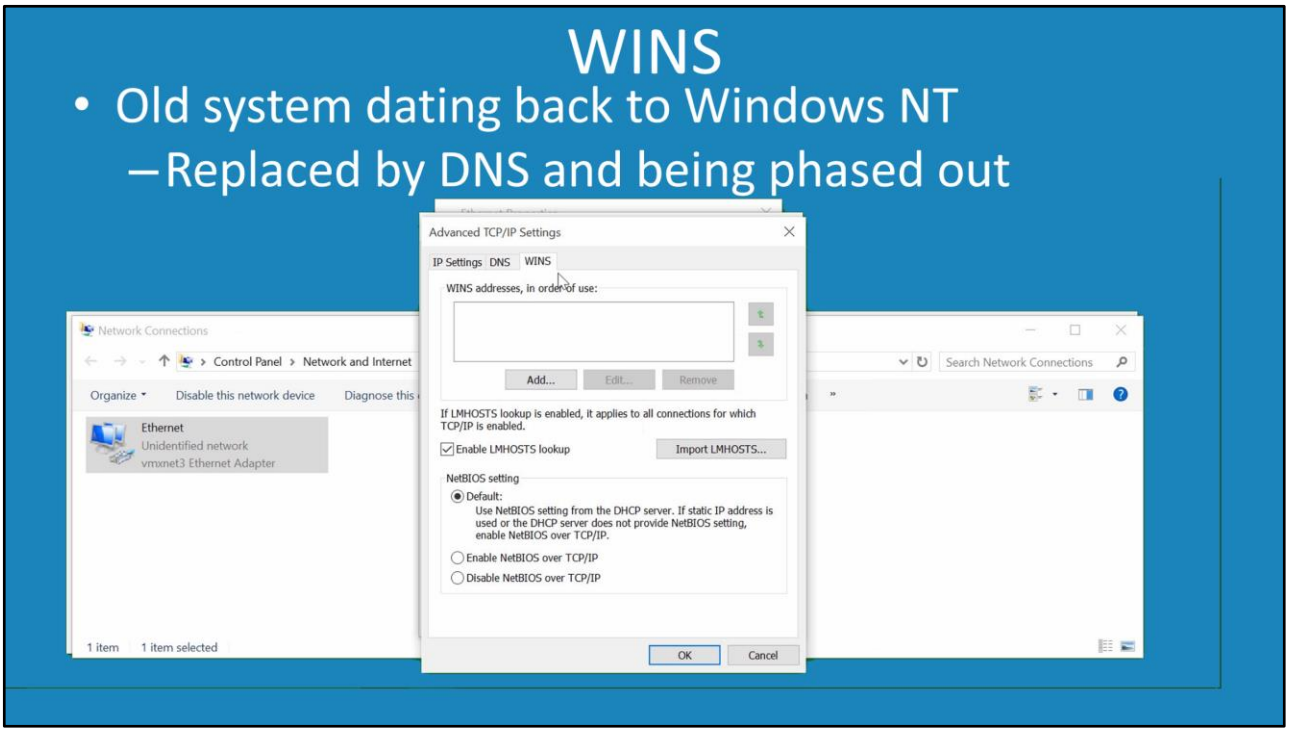


DNS Settings

15:14 – The next option in DNS settings is “Append these DNS suffixes (in order)”. When this option is selected, the DNS suffixes listed below this will be tested in order. By default, there are none present. If I press the Add button, I can add the DNS suffix ITFreeTraining.local.

15:39 – Once added, I will next add the DNS suffix ITFreeTraining.com. This allows the administrator to customize which DNS suffixes will be used. This is particularly useful after domain migrations or when changes occur on the network. For example, the DNS name for the company may change but some services are listed under the old name. When this occurs, the old DNS suffixes can be listed with the new DNS suffix while the old services are being migrated.

16:14 – The next option down is “DNS suffix for this connection”. In this case I will enter in this value of ITFreeTraining.local. This option does two things. If the option “Append primary and connection specific DNS suffixes” is checked, this will test the primary suffix and the connection suffix which was just entered in. In this case, it has been made the same as the primary suffix; however, this could be a different value. For example, if this network connection was connected to a different network the administrator may want to use a different suffix. For example, if the server had two network cards – one connected to ITFreeTraining.local and the other connected to East.ITFreeTraining.local. In this case the administrator may want to use the East suffix for one of the network connections. The second reason this option becomes important is with the checkbox “Register this connection’s addresses in DNS”. If this option is checked, Windows will attempt to use dynamic DNS to create a DNS record on the DNS server. By default, the primary suffix will be used. However, if the checkbox below this, “Use this connection’s DNS suffix in DNS registration” is checked, the DNS suffix for the connection will be used when the DNS record is registered.

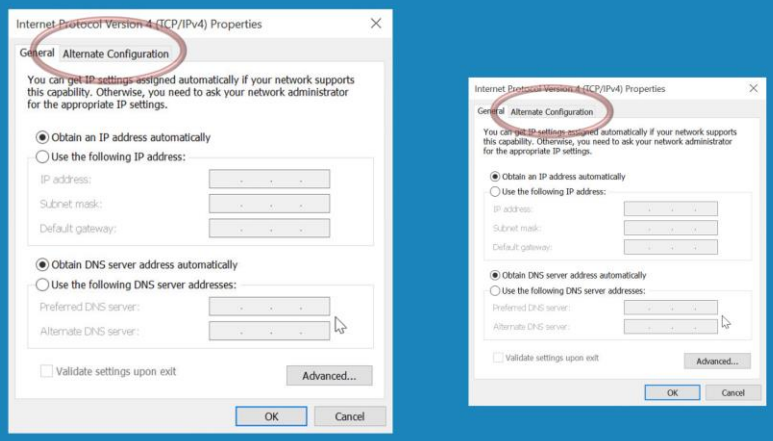


WINS

17:39 –Select the WINS tab. WINS is an old Microsoft name resolution system dating back to Windows NT days. It was the primary name resolution system used by Windows before DNS replaced it. Nowadays WINS has been deprecated and reduced to a feature rather than a role in Windows Server. I would not be surprised if in future editions of Windows it was removed completely. WINS will not be covered in much detail in this course as it is unlikely that you will be asked any questions on it in the exam. I will now go back to the properties of the network adapter. I will next select Internet Protocol Version 6 and open its properties. This course is on IPv4 and we do have another course on IPv6, but the settings work much the same so it is worth having a quick look.

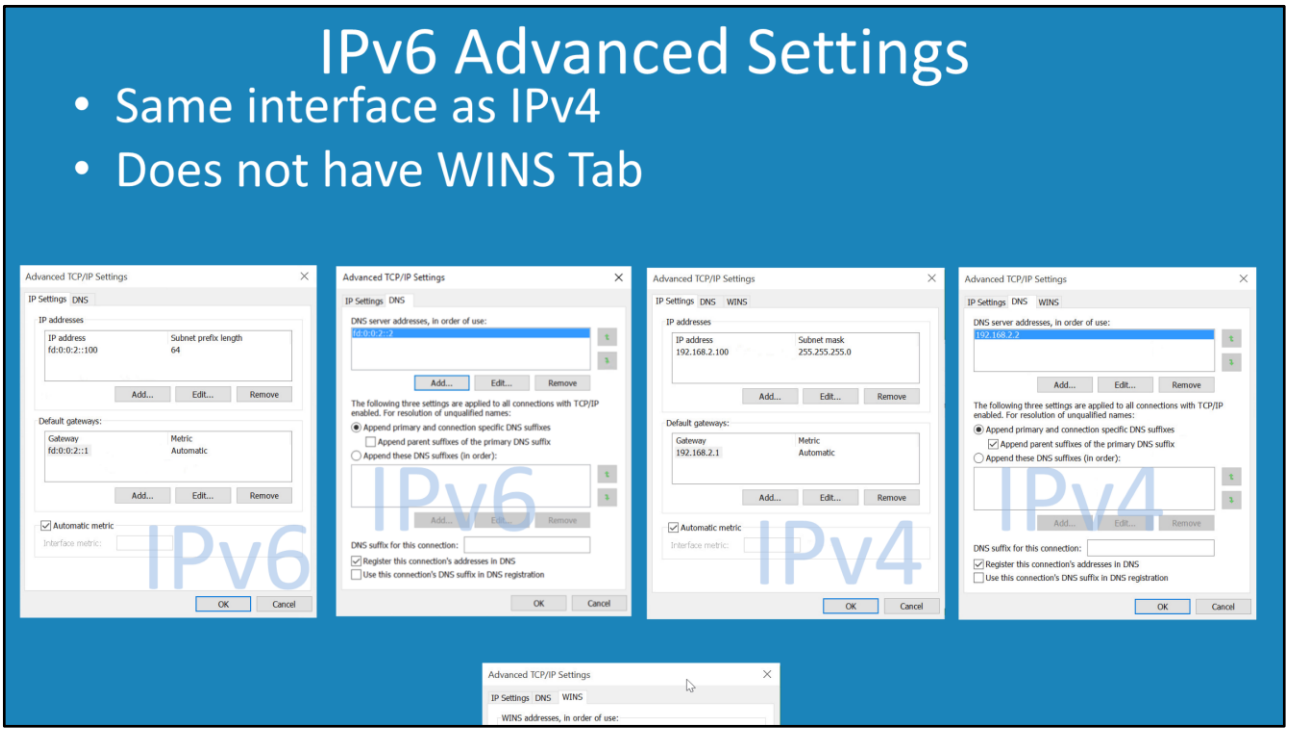
IPv6

- Does not contain alternative configuration



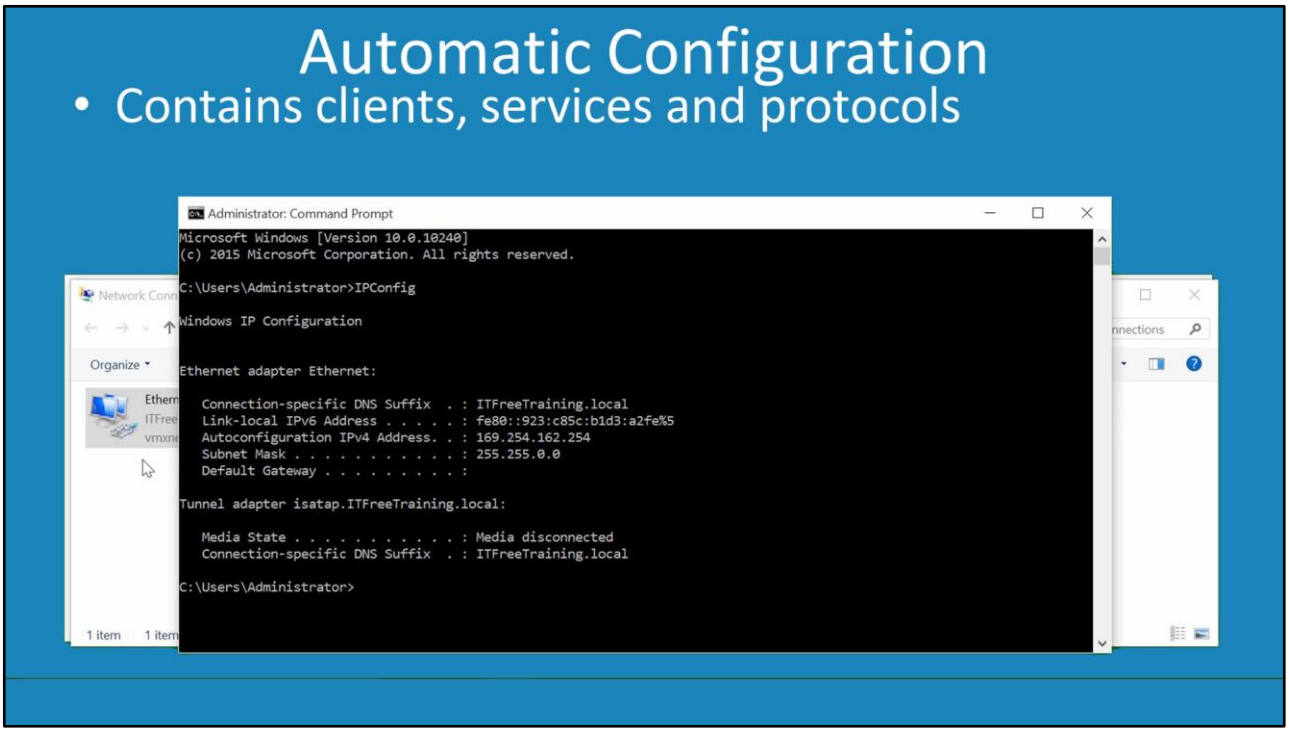
IPv6

18:32 – The first thing to notice on the IPv6 tab is the “Alternate Configuration” tab is missing. This is available in IPv4 and allows the administrator to configure an alternative configuration when it cannot be obtained via DHCP. IPv6 offers improvements via auto configuration so alternative configuration is not required. Just like IPv4, the configuration can be dynamically or statically configured. I will now enter in a static IP Address and other details like DNS servers. Notice the process is the same as IPv4. The only difference is that IPv6 addresses are used rather than IPv4.



IPv6 Advanced Settings

19:15 – Press the Advanced button, you will notice the interface is the same as the IPv4 interface. The only difference is that IPv6 addresses are used. So essentially there is no real difference. Select the DNS tab, notice that the interface is the same as the IPv4 interface. Also, notice that the settings for the DNS suffix have been used. The DNS suffix settings are shared between IPv4 and IPv6 settings. The last thing to notice is that the WINS tab is not present. WINS was designed for IPv4 and does not support IPv6 so it will not be present. I will now go back to the general settings and will configure it to obtain an IP Address and DNS servers automatically. I will also select the IPv4 protocol, open the properties and configure it so it also obtains its configuration automatically.



Automatic Configuration

20:14 – Once done, I will exit out of the adapter settings. There is no DHCP server on this network, so the adapter will need to automatically assign settings itself. To have a look at what gets assigned, I will right click on the start menu and select the option to open a command prompt. To see the configuration assigned to this computer, run the command IPConfig. Notice that an IPv6 IP address has been automatically assigned. In the IPv6 course I will go into this in a lot more detail. On the next line down, notice the IPv4 address that has been assigned. This has been assigned using APIPA. This IP Address will allow this computer to communicate with other computers on the same network that have an APIPA address. That covers it for the basic configuration of the Internet Protocol on Windows computers. I hope you have found this video useful and hope to see you in other videos from us (in particular our course on IPv6). Until the next video, I would like to thank you for watching.

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

"Installing and Configuring Windows Server 2012 R2 Exam Ref 70-410" pages 203-205
"Client for Microsoft Networks" https://technet.microsoft.com/en-us/library/cc757950(v=ws.10).aspx

"Link Layer Topology Discovery"
https://en.wikipedia.org/wiki/Link_Layer_Topology_Discovery
"IPv4 and IPv6 Advanced DNS Tab" https://technet.microsoft.com/en-us/library/cc754143.aspx?f=255&MSPPError=-2147217396
"Configuring Query Settings" https://technet.microsoft.com/en-us/library/cc959339.aspx?f=255&MSPPError=-2147217396

Credits
Trainer: Austin Mason http://ITFreeTraining.com
Voice Talent: HP Lewis http://hplewis.com
Companion Document: Phillip Guld https://philguld.com
Video Production: Kevin Luttman http://www.KevinLuttman.com
Quality Assurance: Brett Batson http://www.pbb-proofreading.uk