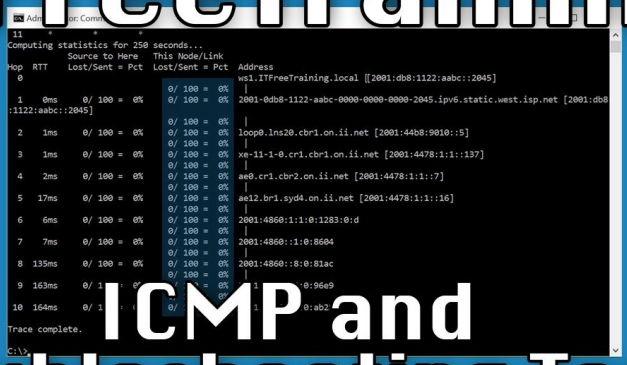
ITFreeTraining

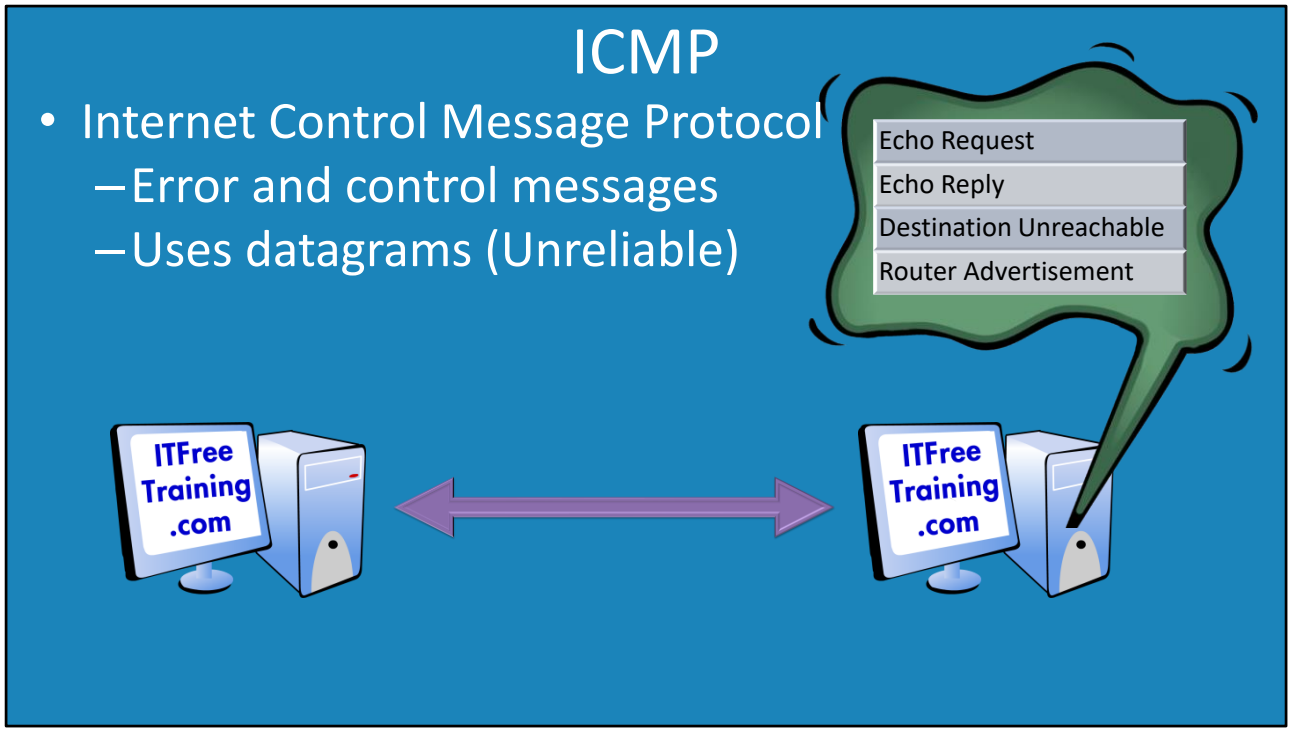


ICMP and Troubleshooting Tools

For the free video please see
http://itfreetraining.com/ipv6/icmpv6

ICMP is used as the internet protocol for control and troubleshooting. This video will look at how the ICMP protocol works in IPv6 and also a number of command line tools that utilize ICMP. These tools are invaluable to the administrator in troubleshooting and supporting their network.

Copyright 2018 © http://ITFreeTraining.com

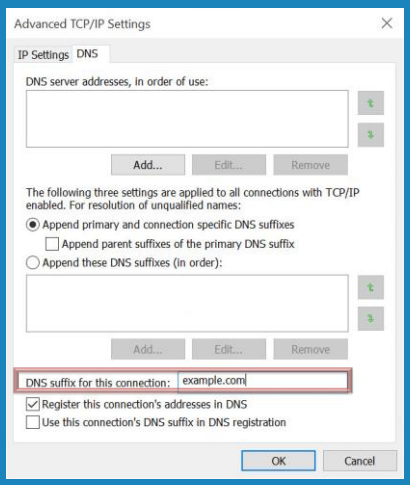


00:14 Internet Control Message Protocol or ICMP provides error and control information that is used by the internet protocol. ICMP uses datagrams to send messages on the network. Datagrams are unreliable. This means, ICMP is not checked to see if it arrives at the destination. For example, just like sending a letter in the post, you cannot be sure if the message reaches the destination. ICMP is routable on the internet and used for such tasks as testing if a node is responsive on the network. If the node is not reachable, ICMP is used to find where the problem is. In IPv6 router advertisements are sent with ICMP. A lot of troubleshooting tools use ICMP.

Copyright 2018 © http://ITFreeTraining.com

IPConfig

- Displays network configuration of that computer



01:00 The IPConfig command does not use any ICMP message. It instead, reads the network configuration of the computer and displays it to the administrator. IPConfig is a great command for the administrator to quickly find out the network configuration of the computer. This command is normally run at the start of the troubleshooting process to find out the basic information about the computer like the IP Address and DNS servers.

Each network adapter in the computer will be displayed in a separate section. The following configuration may be displayed.
Connection specific DNS suffix: An administrator is able to configure a DNS suffix for each network adapter. This is configured in the advanced TCP/IP settings. If no connection specific DNS suffix is configured, the domain suffix will be used.
IPv6 Address: This is the IPv6 address being used by the network adapter.
Link-local IPv6 Address: This IP Address is assigned automatically to the adapter. It is used for communication on the local network. For example, neighbor discovery uses this address. At the end of the address is a % followed by a number. This is the zone index number. It is used to identify the adapter.
Default gateway: This is the IP Address that traffic will be sent to for remote networks. In this case example, the address used in the link local address of the router. Either a unicast or link local address can be used. This comes down to administrator preference.

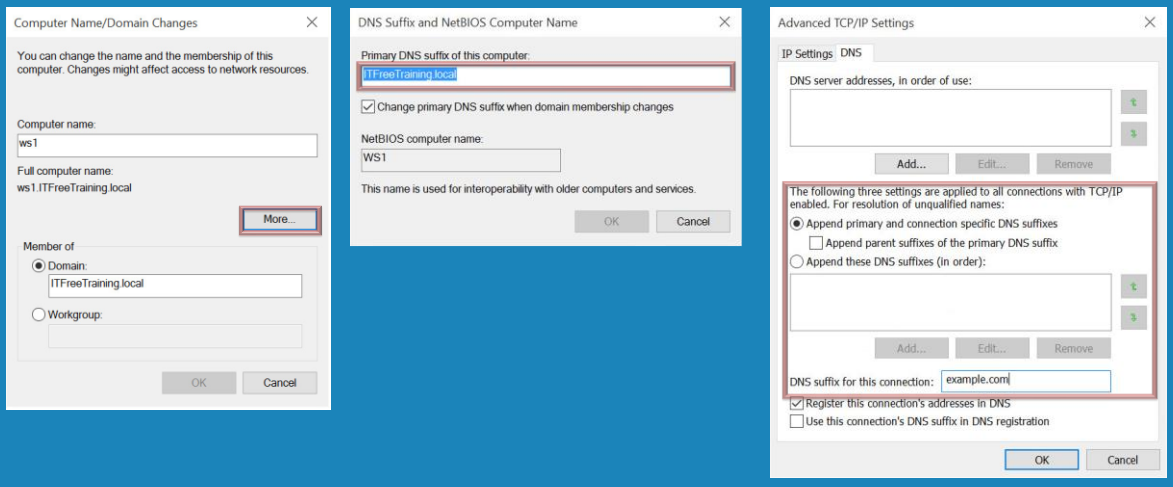
By default, there is a network adapter called ISATAP. This will be listed as disconnected unless the administrator configures it and it is able to establish a connection. ISATAP is a transition protocol that allows IPv6 networks to communicate with each other when they are separated by an IPv4 network.

There will also be a section called Teredo. Teredo is a transition technology that allows IPv4 only computers to communicate on the IPv6 internet. It is enabled by default, but does require some configuration before it will start working.

Copyright 2018 © http://ITFreeTraining.com

IPConfig /all

- Displays additional network configuration



04:10 To obtain more detailed network information about the computer and network adapters, the administrator can add the slash all switch. This will display a lot more information, so to prevent the information from scrolling up the screen "| More" can be added to the end. This will pause the output when the screen is full.

At the top of the output, is information about the computer. This will include the following:
Host Name: This is the name given to the computer.
Primary DNS Suffix: This is the default DNS suffix. When the user attempts to resolve a single label name, this DNS suffix is added to the DNS suffix if no others have been configured. This DNS suffix is configured by pressing the more button found in the properties of the computer. By default, this is configured to the same DNS name as the domain. It is recommended that it is left on this setting.
Node Type: This setting determines how names will be resolved when a WINS server is on the network. DNS is the primary resolving system used by Windows since Windows 2000. By default, Hybrid is used which will contact a WINS server if one is configured and perform a broadcast. It is recommend to leave this setting on the default.
IP Routing Enabled: This settings determines if the computer will route traffic between network cards if configured. By default this is switched off for security reasons. This setting is available on both client and server operating systems.
WINS Proxy Enabled: This setting is used to transfer WINS requests from one network to another. This is used when the original client does not have the ability to send the request directly to the other network. Nowadays, all devices use the internet protocol so can contact a WINS server directly and WINS is not used on most networks, so it is unlikely the administrator

Copyright 2018 © http://ITFreeTraining.com

will need to configure this option.
DNS Suffix Search List: When a single label name is attempted to be resolved, for example WS1, all the entries in the DNS suffix list will be appended and tested. In this example, only ws1.itfreetraining.local will be tested. More can be added in the advanced TCP/IP Settings. For example, you could put entries in for ITFreeTraining.local and HighCostTraining.local and both will be tested when a single label is attempted to be resolved like WS1. That is, ws1.ITFreeTraining.local and ws1.HighCostTraining.local.

Each network adapter will have its own section. Some of the configuration items listed may be:
Description: This is configured by the manufacturer when the adapter is installed. This can be changed by the administrator.
Physical Address: This is the MAC address of the network adapter or equivalent.
DHCP Enabled: If the computer is configured to automatically obtain network configuration this option will be set to 'yes'. If the computer has a static defined IP Addresses this will be configured to 'no'.
Autoconfiguration Enabled: With IPv4, the computer will automatically configure an IP Address in the range 169.254.1.0 to 169.254.254.255 when it cannot contact a DHCP server. This can be switched off. In IPv6, autoconfiguration will configure a link-local address starting with fe80. This cannot be switched off for IPv6 as this is required for basic IPv6 functions like neighbor discovery.
IPv6 Address: This is the current IPv6 address that will be used by the network adapter. An IPv6 address has three states; tentative, preferred and deprecated. An IPv6 address is tentative for a fraction of a second while the network is checked for duplicates. It then becomes preferred and can be used. When it reaches the end of it life it will become deprecated and can still be used, however new connections should not be made using this address.
Lease Obtained: This is the time and date when the lease was obtained.
Lease Expires: This is the time and date when the lease will expire.
Link-local IPv6 address: This is the IPv6 address that is used on the local network only. This will always start with fe80 and is used for basic IPv6 services like neighbor discovery.
DHCPv6 IAID: IAID stands for Identity Association Identifier. This is used to identify a group of related IPv6 addresses. For example, one computer may have multiple network cards that share the same IAID.
DHCPv6 Client DUID: This is a unique number generated by the client. There are a number of different ways the client can generate this number. For example, based on the MAC address, time or assigned by the vendor. There are advantages to each. For example, based on the vendor means the network card can be changed and the DUID does not change. This means a reservation on a DHCP server does not have to change when a network card is being replaced.

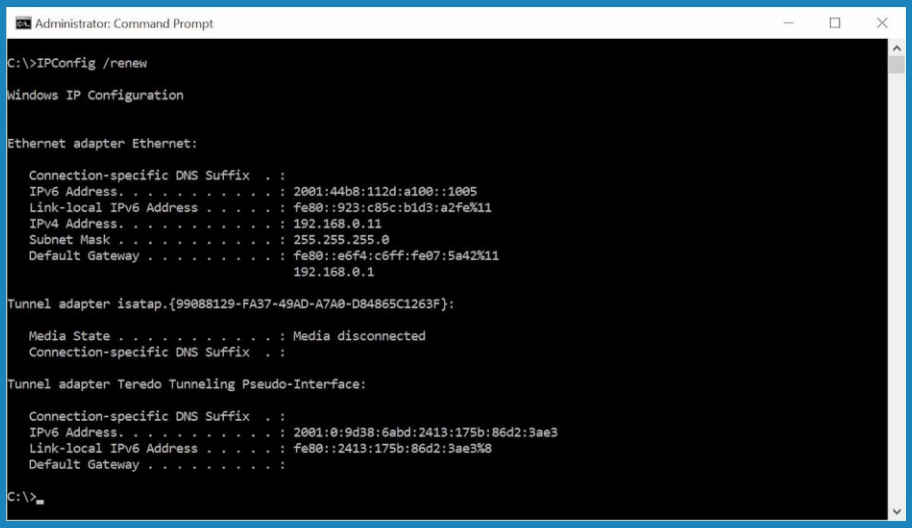
Copyright 2018 © http://ITFreeTraining.com

NetBIOS over Tcpip: This is a legacy option that allows the older NetBIOS standard to travel over TCP/IP. Unless the administrator has good reason to, this option should be left enabled.

Copyright 2018 © http://ITFreeTraining.com

IPConfig /Renew

- Renews current lease with DHCP server

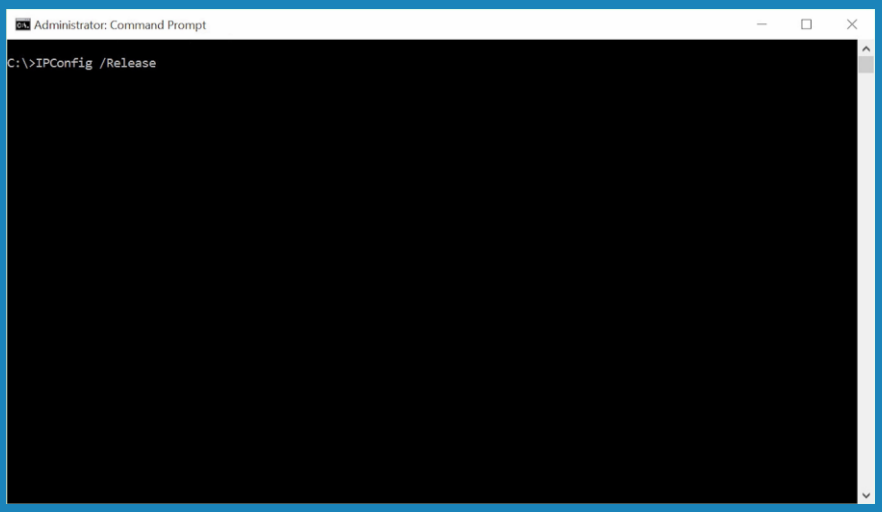


11:00 The Renew switch will force Windows to renew it lease with the DHCP server. If Windows does not have a current lease, it will force Window to attempt to get one. If the administrator makes changes to the DHCP server, for example changing a DNS server, the Renew command will force Windows to renew the lease and thus get the changes. Renewing the lease also resets the lease time back to zero.

Copyright 2018 © http://ITFreeTraining.com

IPConfig /Release

- Contacts the DHCP and releases the current config

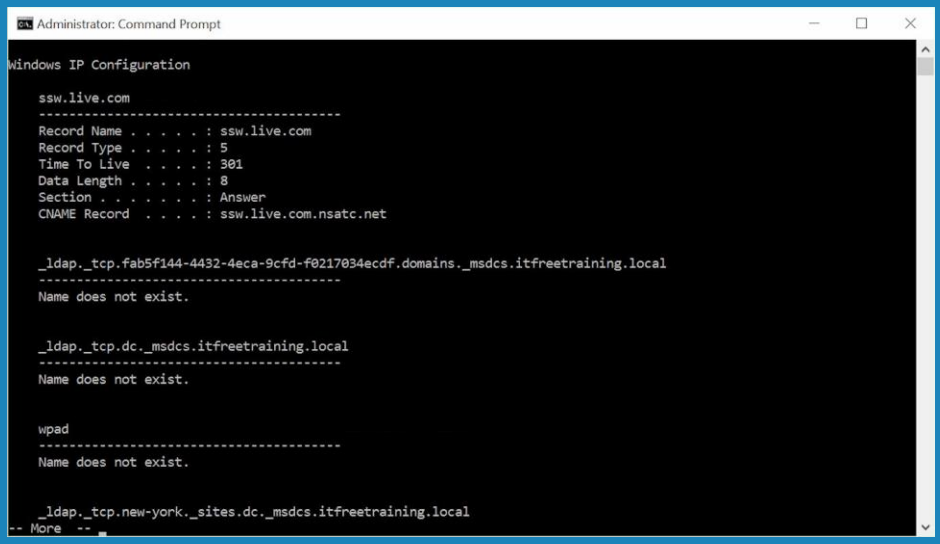


11:30 The Release switch will attempt to contact the DHCP server and give up the lease it currently has. In some cases, the computer may have changed networks or the DHCP server is down. If the DHCP server is not contactable, the command will time out and the configuration will be released. In older versions of Windows, it was not uncommon for the release command to have to be run when changing networks. Newer versions of Window are much better at detecting that the computer has changed from one network to another and automatically contact the DHCP server on that network to obtain a lease for that network.

Copyright 2018 © http://ITFreeTraining.com

IPConfig /DisplayDNS

- Display DNS cache on local computer

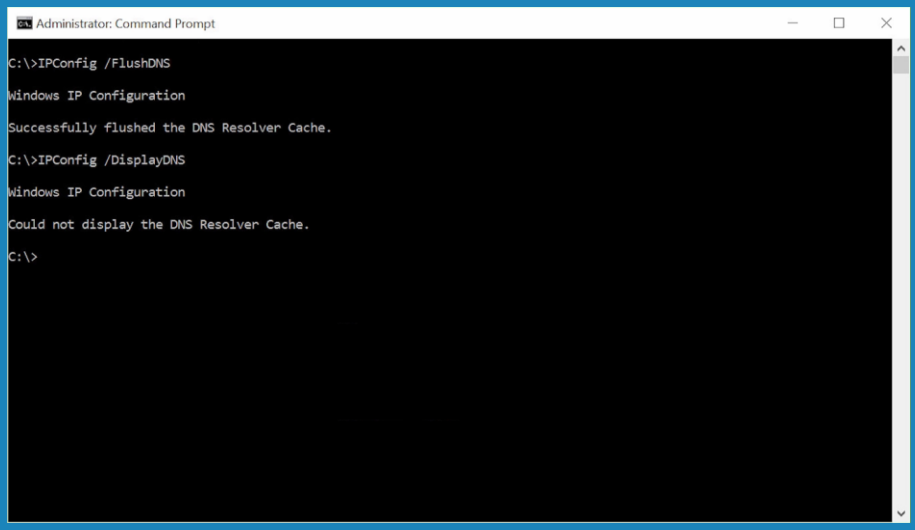


12:20 The DisplayDNS switch will list all the current DNS records in the local DNS cache. For example, if a web page has recently been visited, the DNS record for that web site will be present in the local DNS cache. Also present will be the DNS records that are required for Active Directory, for example, the LDAP records.

Copyright 2018 © http://ITFreeTraining.com

IPConfig /FlushDNS

- Clears the local DNS cache on the computer

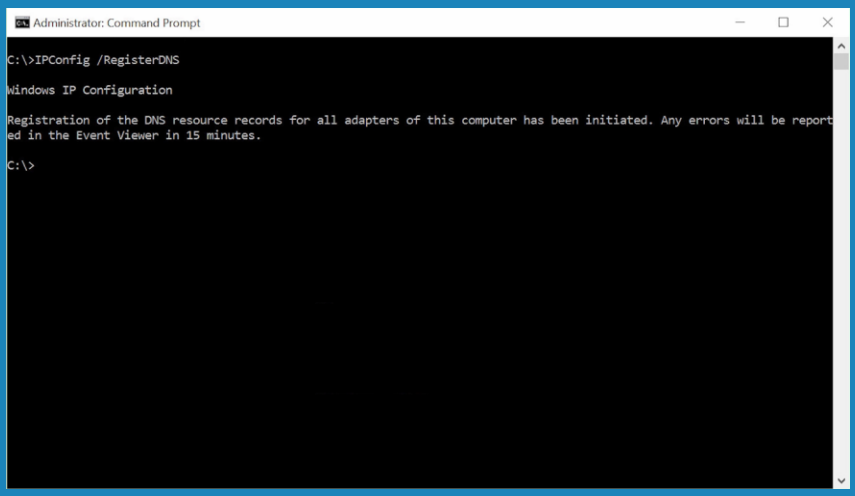


13:15 The switch FlushDNS will clear the local DNS cache on the computer. This is useful when a change is made on the network to a DNS record. The Windows computer will continue to use the local cache copy of the DNS record until it expires. FlushDNS will clear the local cache. This forces the computer to contact the DNS server and obtain updated DNS records.

Copyright 2018 © http://ITFreeTraining.com

IPConfig /RegisterDNS

- Forces computer to register IP Address in DNS
- Requires DNS server to support dynamic updates

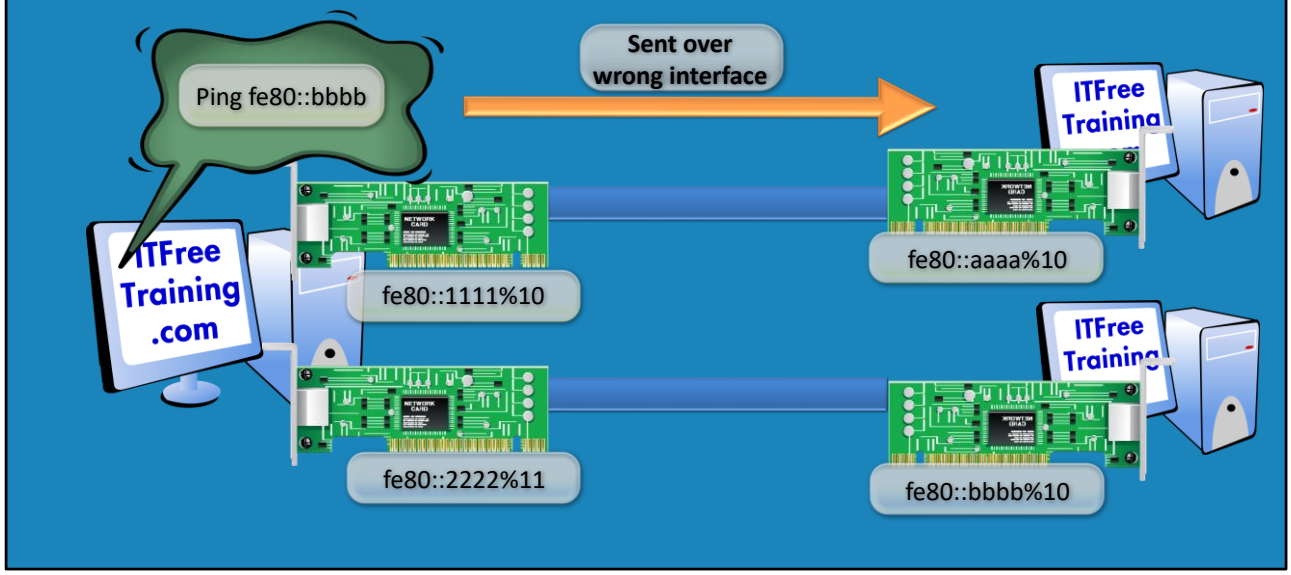


13:40 When dynamic DNS is used, this allows a Windows computer to contact a DNS server and register its DNS name and IP Address. After this has happened, the IP Address of the computer may change. When this happens, the DNS server will still have the old DNS record until it expires. The switch RegisterDNS forces the Windows client to register its DNS name on the DNS server. If the DNS server is configured for dynamic DNS, the old DNS record if present will be updated, or a new DNS record will be created. When the command is run, Windows will not give an indication if the command was successful. In order to determine if the command was successful, check the Event Viewer or the Windows DNS Server.

Copyright 2018 © http://ITFreeTraining.com

Ping with Zone ID

- Adding %11 (Zone ID) will use that interface

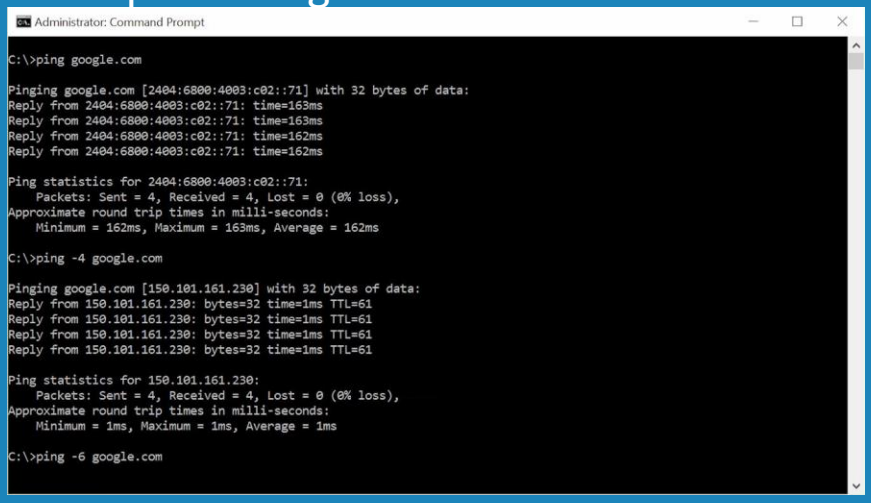


14:10 The ping command will send a message to another node on the network. If the other node is online and configured to respond, it will send a message back to the first node. The ping command is used in basic troubleshooting. In IPv6, a device may have many network adapters, and each adapter will have its own link-local address. When sending a ping to another link-local address, Windows may not know which network adapter to send the ping command to. If this is the case, Windows allows the zone ID to be added to the end of the command. The zone ID will force Windows to use that particular network adapter.

Copyright 2018 © http://ITFreeTraining.com

Ping

- By default will send the request 4 times
- Return trip time is given in milliseconds



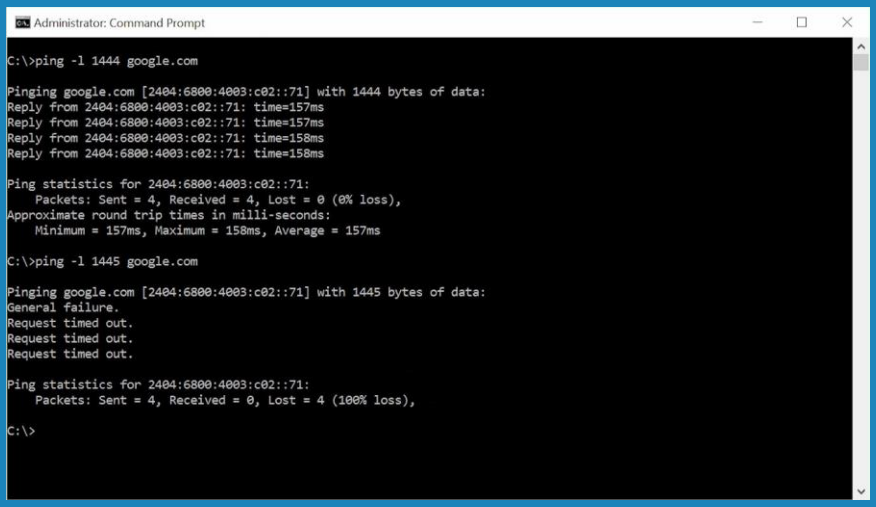
15:40 When the ping command is used with a DNS name, Windows will automatically contact a DNS server and obtain the IP Address of that DNS name. Windows will then ping that IP Address four times. If Windows receives a response back, the round trip in milliseconds is reported. This is useful in troubleshooting to determine if a node is online and the time a message may take to travel over the network.

The ping command supports the use of -4 and -6. When these are used, this forces the ping command to use either the IPv4 protocol or the IPv6 protocol. If they are not specified, Windows will try the IPv6 protocol first and then try the IPv4 protocol. A lot of Windows commands support the -4 and -6 switches.

Copyright 2018 © http://ITFreeTraining.com

Ping -l

- Specific the packet size

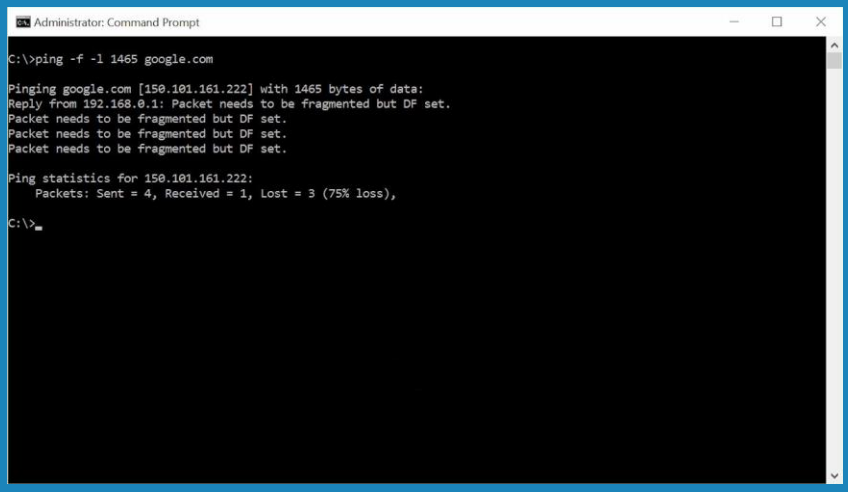


16:40 The -l switch configures what size packet the ping command will use. This is useful in troubleshooting, for example if a router between two points only supports a certain size packet. The internet protocol will divide a large packet into parts when this occurs. In most cases this does not present a problem. However, with applications like VPN, the VPN will think that the packet has been tampered with and will drop the packet. When this occurs, the source location may need to reduce its packet size.

Copyright 2018 © http://ITFreeTraining.com

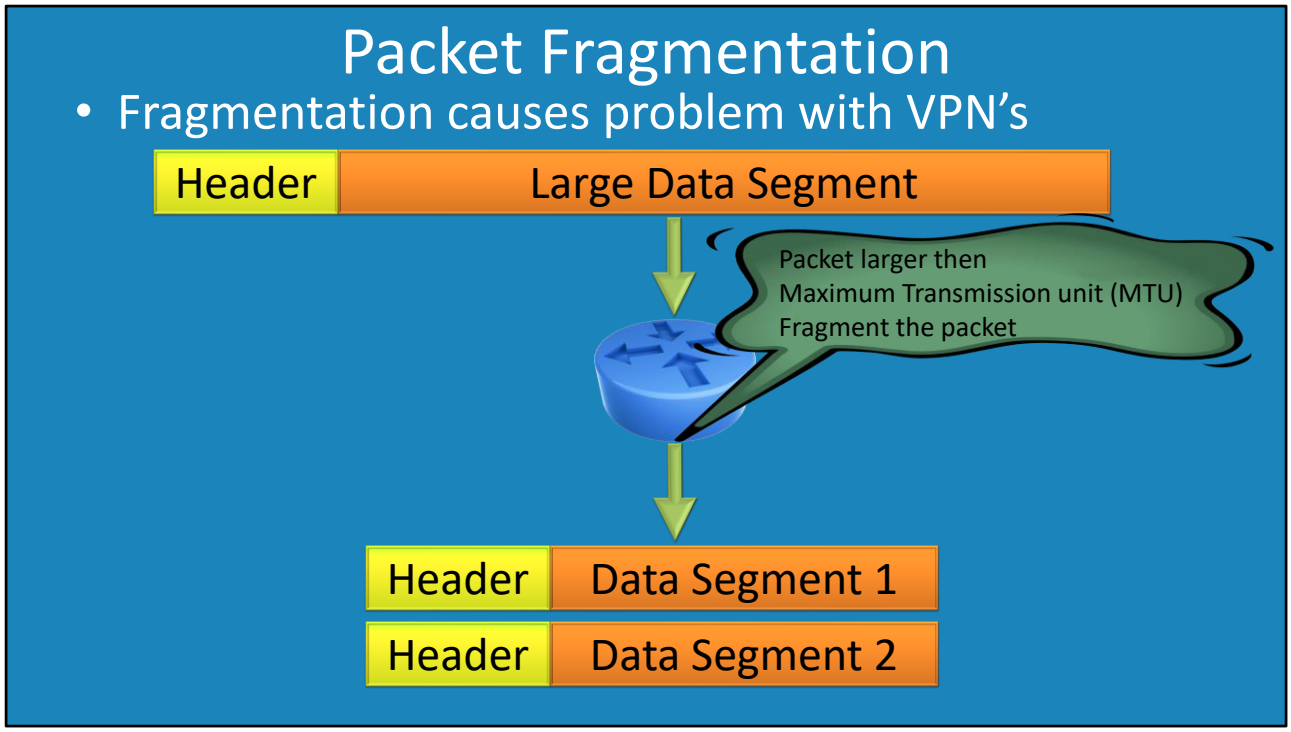
Ping -f

- Prevents packet from being fragmented
- Supported on IPv4 only



17:10 The -f switch prevents a packet from being fragmented. This occurs when the packet goes through a router that has a lower packet size then the original packet. Adding the f switch will report back that a router needs to fragment the packet, but has not been able to.

Copyright 2018 © http://ITFreeTraining.com

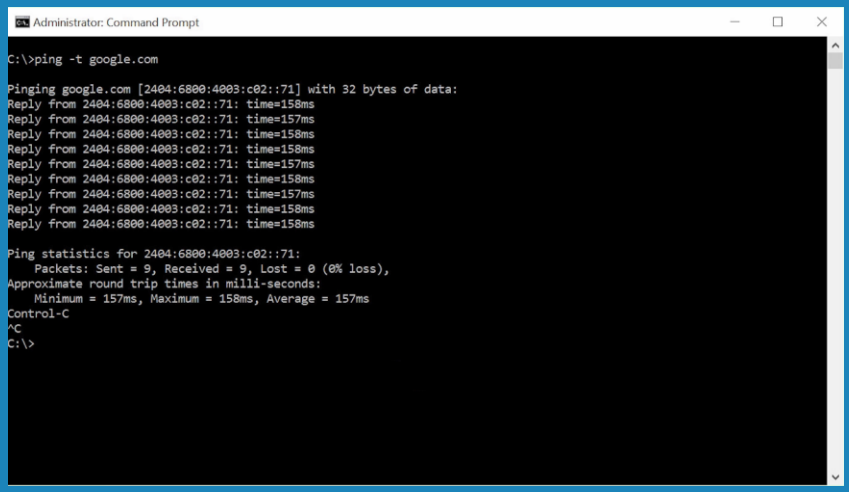


17:35 This is the process of dividing a packet up into smaller parts. For example, if a packet is sent on the network that is 2000 bytes in size and reaches a router that support 1500 byte packets, the packet will be divided into two. Having two 1000 byte packets is smaller than the maximum packet size of 1500 the router supports. When the two packets arrive at the destination, they will be put back together in sequence. Packet fragmentation in most cases does not cause any problems. However, in security sensitive applications like VPNs this can cause problems. This is because the VPN support thinks that packet has been tampered with when it is divided into smaller parts and is dropped.

Copyright 2018 © http://ITFreeTraining.com

Ping -t

- Sends unlimited number of pings
- Until CTRL-BREAK or CTRL-C is pressed

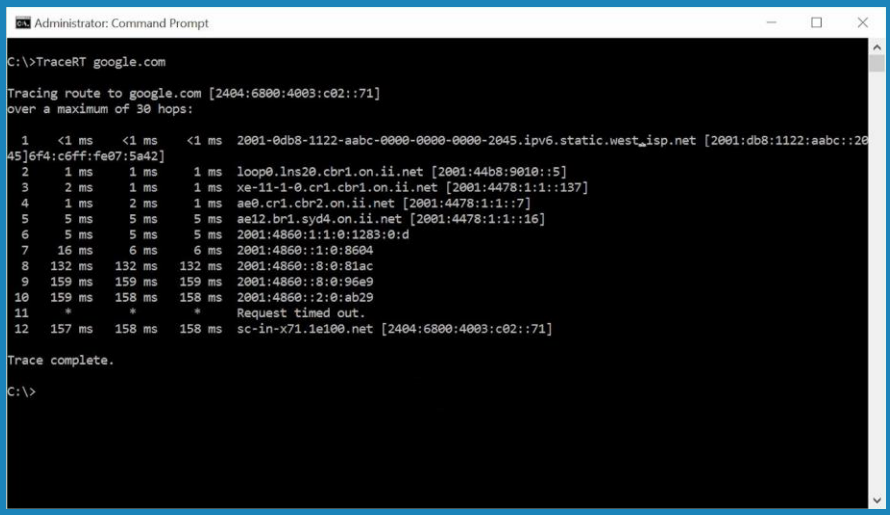


18:35 The -t switch will keep sending pings until ctrl-break or ctrl-c is pressed. Normally the ping command will send four pings and then stop. The -t switch is useful when performing processes like rebooting servers. By pinging the server, this will tell the administrator when the server has finished the reboot and has started back up.

Copyright 2018 © http://ITFreeTraining.com

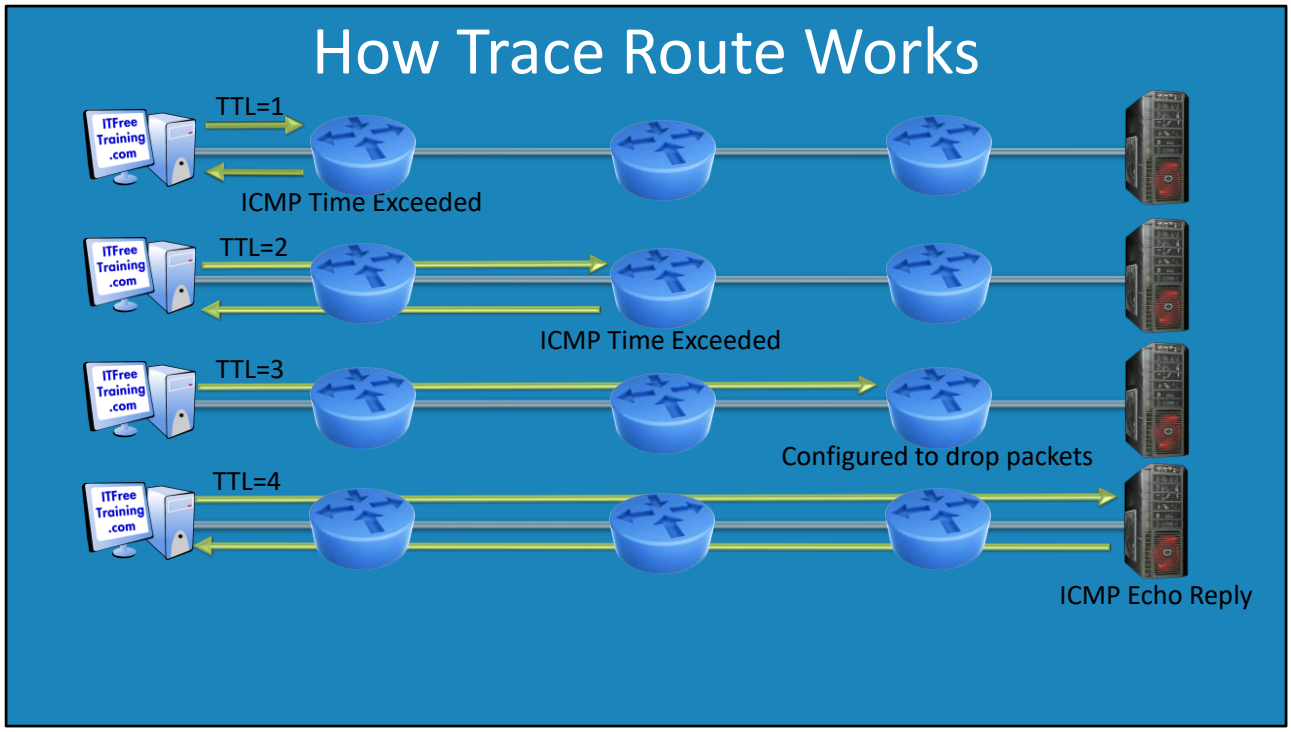
TraceRT

- Traces route to destination



19:00 Trace route tells the administrator which routers or hops the packets travel through to reach the destination. By default, trace route will perform a reverse look up of the IP Address at each hop. This will give the administrator the DNS name and thus give them an idea where the hop may be. Just like the ping command, four round trip values are given for the time taken to each hop and back. If no response is received from a hop, the round-trip value will be given as an asterisk.

Copyright 2018 © http://ITFreeTraining.com

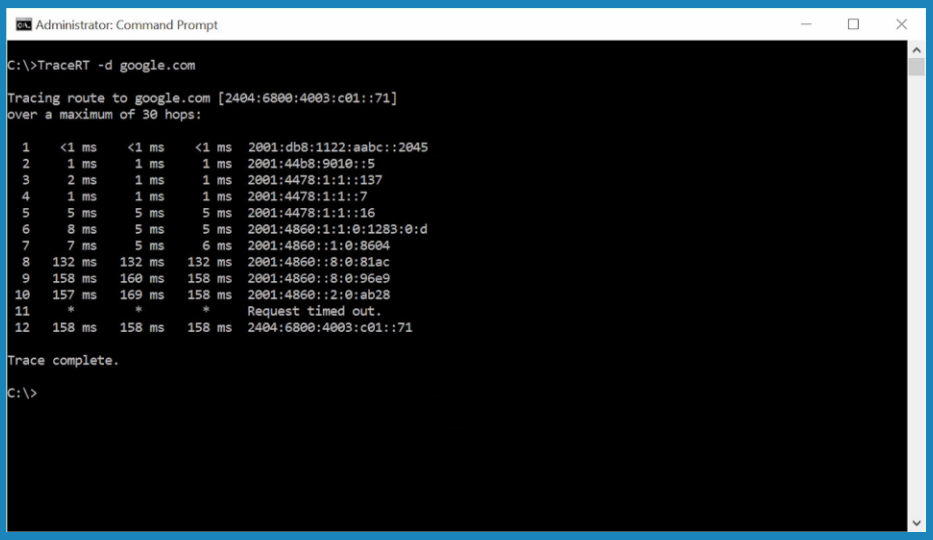


20:30 Trace route works by sending ping requests to the destination. Just like the ping command, three pings are sent. The first group of four requests has the TTL or Time To Live field in the packet set to one. The TTL field determines how many times a packet can be routed on the network before it is dropped. Without a TTL field, a packet could be caught in a routing loop and travel in circles forever. When the TTL field reaches zero, the router will send an ICMP time exceeded message. This is how Windows knows the IP Address of each hop. In some cases, a router or a firewall may be configured to not send the ICMP time exceed message back. When this occurs, trace route will display all asterisks in the time columns. Keep in mind as well, asterisks may be displayed in all columns with high congestion where the packet is getting lost on the return trip.

Copyright 2018 © http://ITFreeTraining.com

TraceRT -d

- Does not resolve IP addresses to DNS names

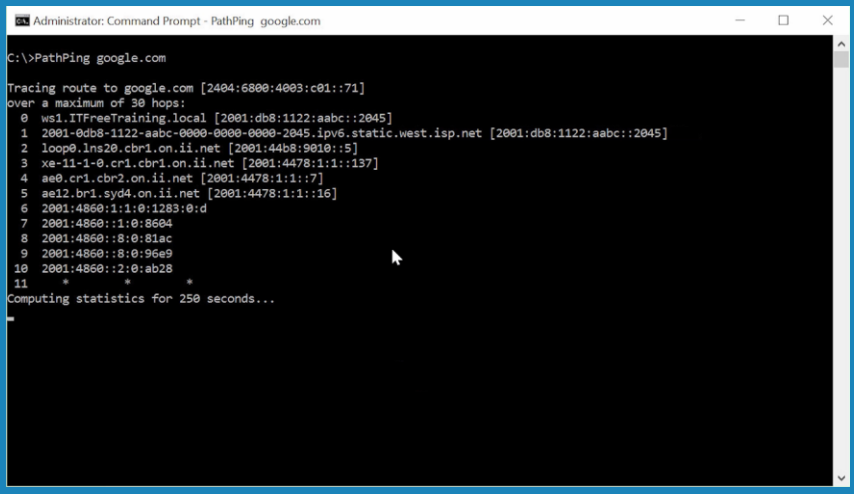


22:45 If you run TraceRT with the -d switch, TraceRT will not attempt to resolve IP Addresses back to DNS names. This makes TraceRT run faster, however it does not give the administrator any information about where the hop is other than the IP Address.

Copyright 2018 © http://ITFreeTraining.com

PathPing

- Combines Ping and trace route showing packet lost
- Helps finds where network problems may be

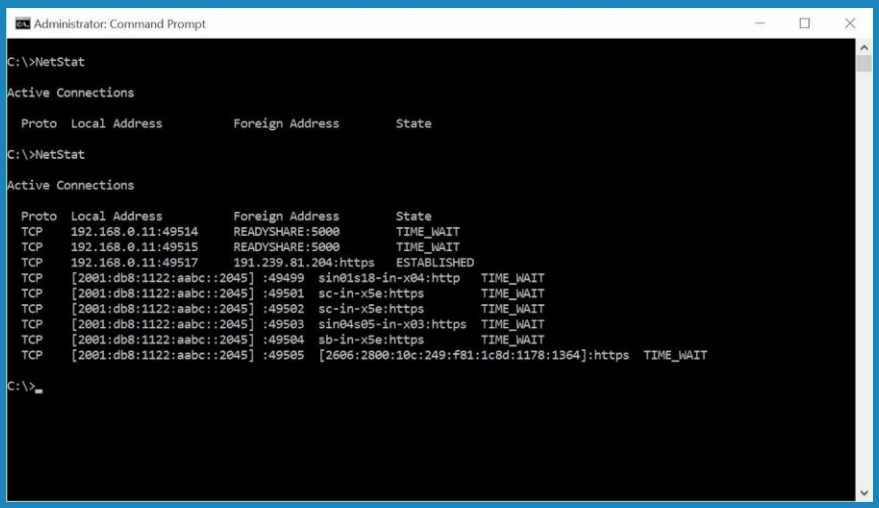


24:30 The PathPing command combines ping and TraceRT together. The command first works out the path from the client to the destination. When this is complete, a number of pings are performed over a random period of time. The number of pings lost is recorded as well as the round trip. This gives the administrator an indication of where congestion on the network may be. This is particularly useful when there are intermittent problems on the network.

Copyright 2018 © http://ITFreeTraining.com

NetStat

- Show current active connection
- Add –a to show listening connections

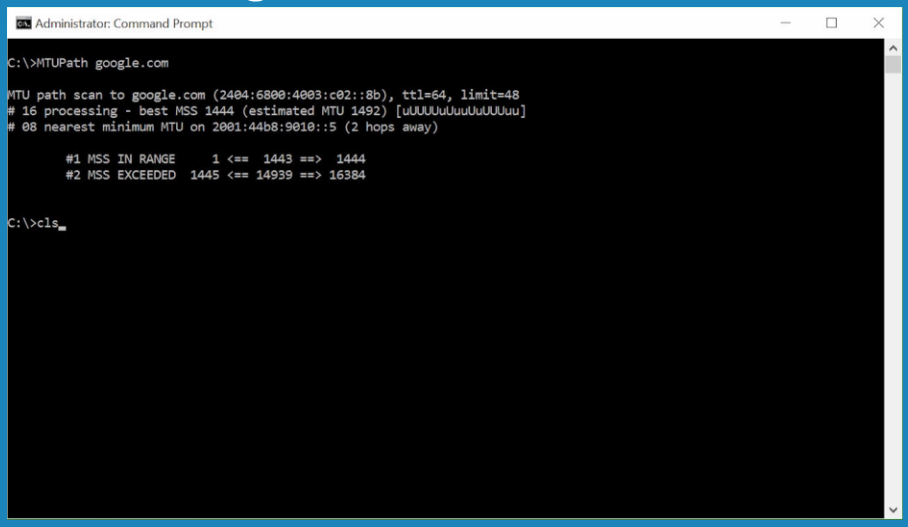


25:50 The NetStat command shows the current connection on the computer. When you open and use any application that creates a network connection, NetStat will show that connection. If you add the -a switch, this will show any ports on the computer that are open waiting for a connection.

Copyright 2018 © http://ITFreeTraining.com

MTUPath

- Works out largest MTU to a remote host

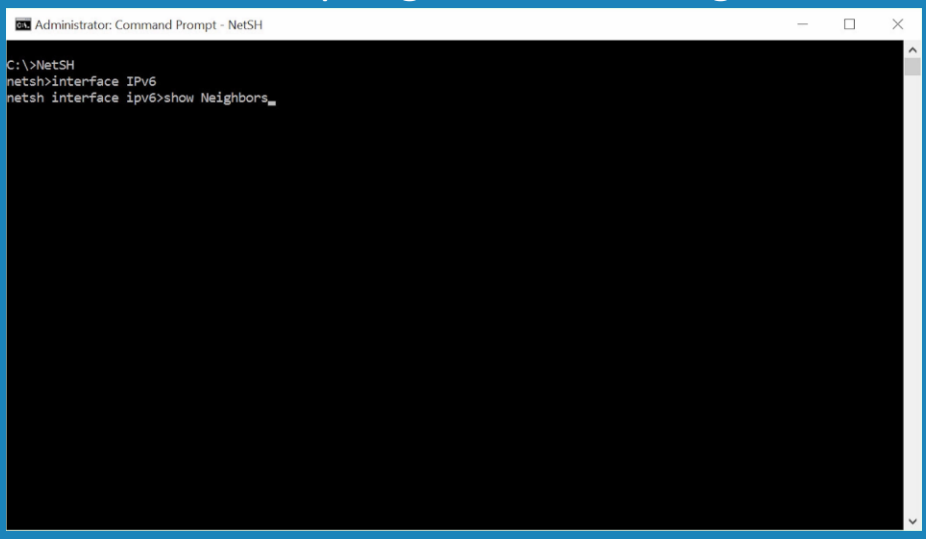


27:00 MTUPath is a free application that can be downloaded from the following location: http://www.iea-software.com/products/download.cfm. This application works out the largest maximum transmission unit (MTU) between your computer and the remote computer. The administrator can use the ping -l command to work out the maximum MTU using trial and error.

Copyright 2018 © http://ITFreeTraining.com

NetSH

- Command-line scripting network configuration tool



27:52 NetSH is a command line tool that can be used to configure networking on the local and remote computers. It can be run with or without parameters. For example you could run this from the command line:
NetSH Interface IPv6 Show Neighbors
Or you could run:
NetSH
This would give you the NetSH command prompt. From the NetSH command prompt, the command you want to run, or a part of it, can be entered in. For example you could run the following from the NetSH command prompt:
NetSH> Interface IPv6 Show Neighbors
You could also run the following:
NetSH> Interface
NetSH> IPv6
NetSH> Show Neighbors

Copyright 2018 © http://ITFreeTraining.com

Summary

- IPConfig (Displays network configuration)
- Ping (Tests network to remote node)
- TraceRT (Trace path to remote node)
- PathPing (Combines ping and trace route)
- NetStat (Show active network connections)
- MTUPath (3rd party tool)
  - Calculate max MTU to remote node
- NetSH (Command line configuration tool)

30:05 Shown below, is a quick summary of all the commands that were covered in this video.
IPConfig: Displays network configuration to the administrator. Good for getting the basic details of the network configured on the computer quickly.
Ping: Sends a message to a remote computer and waits for a response. This can be used to test the connection between two networks.
TraceRT: This command traces the route between the computer and the destination. Each step in the path, known as a 'hop' is shown.
PathPing: This combines the ping and trace route commands. First a trace is performed. After this, ping commands are sent over a random period of time. This gives the administrator an indication of where any problems on the network may be.
NetStat: NetStat shows any open connections to the computer and also any ports that have been opened on the computer and are listening.
MTUPath: This is a free download that works out the Maximum Transmission Unit (MTU) between the source computer and the remote computer.
NetSH: This is a command line configuration tool. It has a lot of options and is useful for advanced troubleshooting and configuration.

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.

Copyright 2018 © http://ITFreeTraining.com

References
"Ipconfig" https://technet.microsoft.com/en-au/library/bb490921.aspx
"Ping" https://technet.microsoft.com/en-au/library/bb490968.aspx
"Dynamic Host Configuration Protocol for IPv6 (DHCPv6)" https://tools.ietf.org/html/rfc3315
"Tracert" https://technet.microsoft.com/en-us/library/cc940128.aspx
"PathPing" https://technet.microsoft.com/en-us/library/cc958876.aspx
"Netstat" https://technet.microsoft.com/en-au/library/bb490947.aspx
"MTU Path" http://www.iea-software.com/products/mtupath.cfm
"Netsh overview" https://technet.microsoft.com/en-us/library/cc778925(v=ws.10).aspx

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

Copyright 2018 © http://ITFreeTraining.com