JORGEN LANESSKOG

PING

Basic IP Network Troubleshooting

Need To Know Basis
Ping

By Jorgen Lanesskog

Need To Know Basis Series

Copyright 2014 by Jorgen Lanesskog.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system or transmitted by any means, electronic, mechanical, photocopying, recording or otherwise without written permission from the author. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information herein.

Every effort has been made to make this book as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

About the author

Jorgen Lanesskog, born 1972 in Bergen, Norway started his computer days back in 1984.
With the Commodore 64 and a BASIC manual the interest grew and became the start of a long journey into the exiting and ever expanding world of IT.

Though programming never became his profession, it has always been a great hobby and he is currently using Delphi Pascal and Visual Studio when need be.

In 1990, Jorgen started as an IT consultant and aside from 2 years of teaching computer software classes, he has worked as an IT consultant to this very day.

Today, Jorgen is working as a Senior Network Consultant at Rupta AS and the job description covers troubleshooting TCP/IP networks, designing and implementing IT network solutions, security and performance planning.

Jorgen currently holds a Microsoft Certified System Engineer (MCSE), Novel Master CNE (MCNE), Cisco Certified Internetworking Expert (CCIE #8744), VMWare Certified Professional (VCP) and a handful of other IT related certifications.

Jorgen Lanesskog
Senior Network Consultant
Bergen, Norway

About the “Need To Know Basis” series

“If you tell people something on a need-to-know basis, you only tell them the facts they need to know at the time they need to know them, and nothing more.”

Although the book series will go a little deeper, the point is, giving the reader the information he or she needs to get a certain problem solved, a device or system working or whatever the case may be without digging into all the theory, history or complexity that may be involved in the topic being written about.

It’s about getting “up and running” as fast as possible.

It’s about getting straight to the point. No fuss or delay. Just get it working.

Contents

Contact me

Technet24.ir

What is it good for?

During my typical workday I probably use Ping several times.

If you had a computer tool belt, I am pretty sure Ping would be somewhere in the front.

And it is always ready to be used. No installation needed, and universally equal (in use) to most computer systems.

It’s just a great tool. Honest.

Okay, so if you never used a command line utility before you may have to get your hands a little dirty poking around the black window with the blinking cursor. But relax, it’s all pretty easy. I promise.

Ping is named from active sonar terminology which sends a pulse of sound and listens for the echo to detect objects underwater.

And in that same sense we use Ping to discover if objects (computers or other devices) are responding to the requests we send out. This is useful if you need to know if a device is active or “alive” on the network.

Usually this is the first step in troubleshooting a network problem.

If you are trying to reach a service (like a web page for example) and you can’t get to it, Ping will tell you if it is responding at all, and if so, you can start to look at other solutions to the problem.

Another tool I will talk a little bit about is Traceroute.

Traceroute is a great tool for finding out what direction a packet leaving your computer takes to get to the destination.

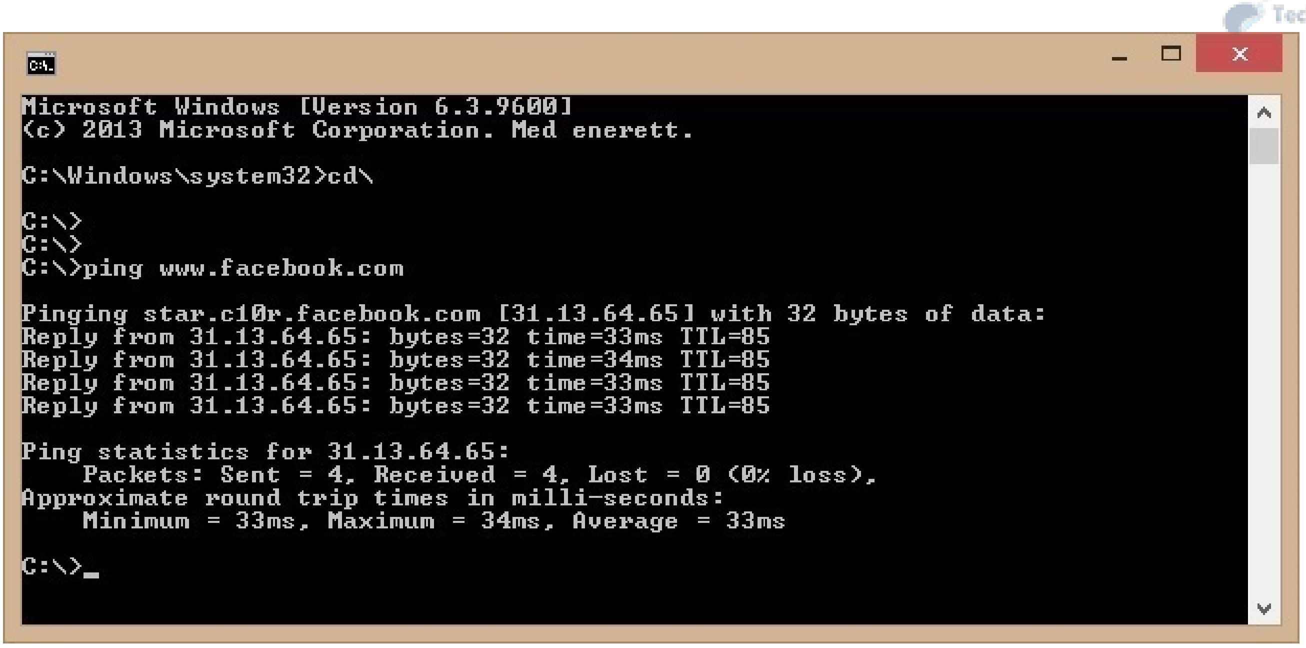
Maybe your packet takes the slow route? Maybe you can’t get to the destination and Ping tells you that the device you are trying to reach is not responding? Traceroute can tell you were on the path to the destination things go wrong.

If nothing is wrong, Traceroute gives you a step by step (or hop by hop) roadmap to the destination you are trying to reach. This can be very useful information in troubleshooting computer networks.

In this book I will be using Microsoft Windows command line to demonstrate the use of Ping.

The commands are used in the same way across all the different versions of Microsoft Windows.

Technet24.ir



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. Med enerett.

C:\Windows\system32>cd\

C:\>
C:\>
C:\>ping www.facebook.com

Pinging star.c10r.facebook.com [31.13.64.65] with 32 bytes of data:
Reply from 31.13.64.65: bytes=32 time=33ms TTL=85
Reply from 31.13.64.65: bytes=32 time=34ms TTL=85
Reply from 31.13.64.65: bytes=32 time=33ms TTL=85
Reply from 31.13.64.65: bytes=32 time=33ms TTL=85

Ping statistics for 31.13.64.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 33ms, Maximum = 34ms, Average = 33ms

C:\>_
```

Figure 1: Pinging www.facebook.com

Technet24.ir

IP addresses and host names

Version 4 and version 6

Every device connected to an IP network (like the Internet, your workplace or at home) has an IP address. Without an address you are not reachable and you cannot reach anything. That's the basic truth.

We are not going to get into the details of how IP works or how to manage IP addresses, but you need to know this one thing. Every IP device has an IP address.

The device can be your computer, your phone or even your washing machine if it has a network adapter.

So with all these devices and the ever expanding need to connect even more devices, the current scheme for IP addressing has gotten too restricted for the world to handle. This scheme is called IP version 4.
The new version 6, skipping 5, comes to the rescue.

We're not ready to drop version 4 altogether just yet and it will be a few years before version 6 is the common version being used all around. But we are getting there and most systems being built today supports both versions.

This book will focus on IP version 4.

IP version 4 uses an address format like this X.X.X.X, where X can be any number between 0 and 255.

In one episode of the US TV series "Castle" they consulted an IT geek trying to get the IP address used by some criminal and the end result was something like 300.23.277.2. I guess they just did not bother getting it right.

Not every IP address can be used and some has special meaning, but remember where to put the dots and that no number can be lower than 0 or higher than 255.

There is also something called a subnet mask. A mask or subnet mask groups IP addresses in logical units. Like all the houses in your street belongs to the same street and have the same street name, IP addresses can be grouped to belong to the same subnet or "street of addresses".

So in that sense the IP address is like the number of your house and the subnet mask is the name of your street.

Pushing that analogy even further you could say that at every crossing, there is a router connecting the streets.

Technet24.ir

The subnet mask is not a part of the IP address in itself.
The subnet mask tells you (and the computer) what part of the IP address belong to the network and what part belong to the host. So contained in the address is both the "street" and "house number".

So for example, IP address 192.168.1.10 with a subnet mask of 255.255.0.0 tells you that the 192.168 part is the network or "street" and the 1.10 is the actual host or "house".
Every number after 192.168 would then belong to the same network or "street".

DNS

Like phone numbers, IP addresses can be hard to keep track of or remember. When you need to dial a friend you can easily look him up in your list of contacts.

DNS or *Domain Name System* is like a list of contacts, but for IP addresses. So instead of typing in a lot of numbers you can type in www.facebook.com in your Internet browser and DNS will do a lookup for you and find the correct IP address.

Because, like the phone, you can't really call a name. You need to call a number.

So DNS is like the phone book to computers and other connected devices. It's just there to make things a bit easier. In the end, every device needs an IP address to connect to.

If you look at figure 1, you'll see that I did a Ping to www.facebook.com.
I got a reply. Well actually I got four replies and also the reply told me what IP address the replies came from.

So in this case, I could choose to ping www.facebook.com or I could ping 31.13.64.65. Which one is easier to remember?
Anyways. Facebook seems to be online.

When it comes to pinging Facebook I should probably tell you that you might not get the same reply if you tried the exact same Ping.
A lot of popular web sites spread their services across a lot of servers (which of course needs one IP address each) and it be random to what server you connect, and therefore you might get a different reply (from a different IP address) then the one shown here.
DNS will tell you to connect to an IP address in a "round-robin" fashion to share the load across multiple servers. So you might be connecting to a different Facebook server every time you open that web page.

The way this works is that www.facebook.com as a name is registered multiple times in the DNS system, but with different IP addresses.
This is very common.

Technet24.ir

Technet24.ir

So how does Ping work?

Also called “**P**acket **IN**ternet **G**roper”.

> *Ping verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution.*

Basically Ping works by sending a data packet from the IP source to the IP destination.
This source packet is called an **Echo Request**.
In reply to that request the destination sends a copy of that data packet back to the source as an **Echo Reply**.

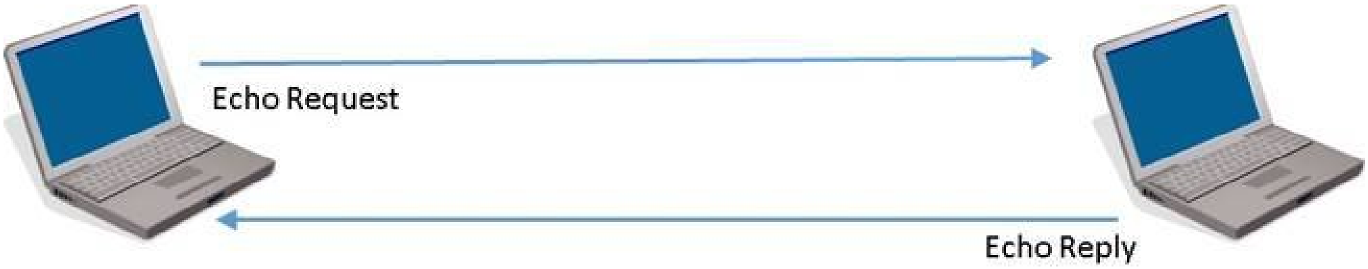


Figure 2: Echo Request and Echo Reply

Microsoft Windows Ping will send 4 requests as standard. You will then get 4 replies if the device you are trying to ping is available and online. You can set it up to send fewer or more requests in the command if you like.

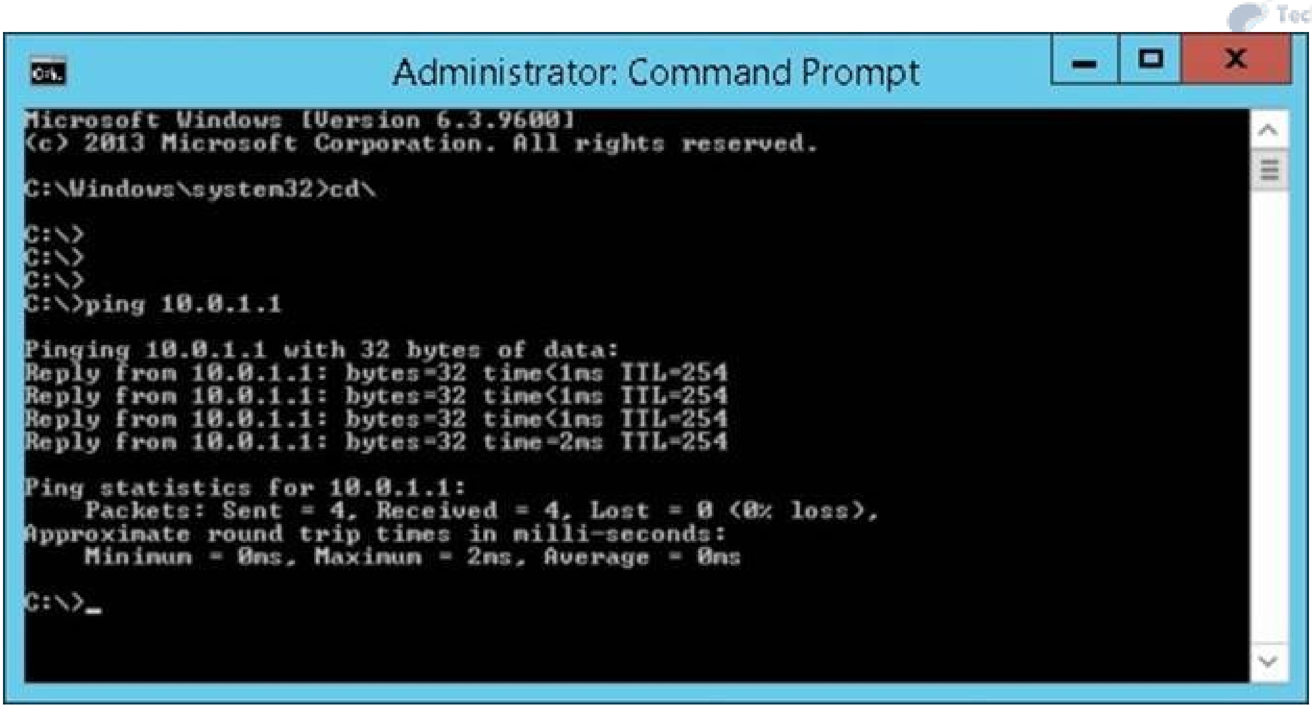
So in figure 2, if the destination machine has an IP address of 192.168.1.10 the command on the source machine would probably look something like this:

```
Ping 192.168.1.10
```

Easy enough!

You can choose to ping an IP address directly like the one we just used or you can ping an address by name. If you choose to ping by name, the Ping command must first do a DNS lookup to find what IP address it should actually ping.

Technet24.ir



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd\

C:\>
C:\>
C:\>
C:\>ping 10.0.1.1

Pinging 10.0.1.1 with 32 bytes of data:
Reply from 10.0.1.1: bytes=32 time<1ms TTL=254
Reply from 10.0.1.1: bytes=32 time<1ms TTL=254
Reply from 10.0.1.1: bytes=32 time<1ms TTL=254
Reply from 10.0.1.1: bytes=32 time=2ms TTL=254

Ping statistics for 10.0.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>_
```

Figure 3: Ping screenshot

So, you use Ping to discover if a host or device is available on the network. And that is great and sometimes all you need to know, but Ping also offer some more information.

If you look at figure 3 you’ll see a typical Ping command in action. Here, the source sends an Echo Request to the IP address 10.0.1.1.
From the screenshot you’ll notice that we got 4 Echo Replies to these requests, but also along with every reply you’ll get information about how much data is sent (bytes), the time it took to send and get the reply back (round trip time in milliseconds) and something called a Time To Live (TTL) value.

Some more statistics that shows how many packets are sent and received and round trip times averages.

Typically the round trip times will vary depending on the distance from the source to the destination. Pinging a device in your own network should be faster than pinging a host in a different country.

The TTL value is a safety parameter that assures that a packet sent don’t end up forever roaming the networks. The value decrements for every router it passes by and if the value gets to 0 before arriving at the destination, the packet is dropped.

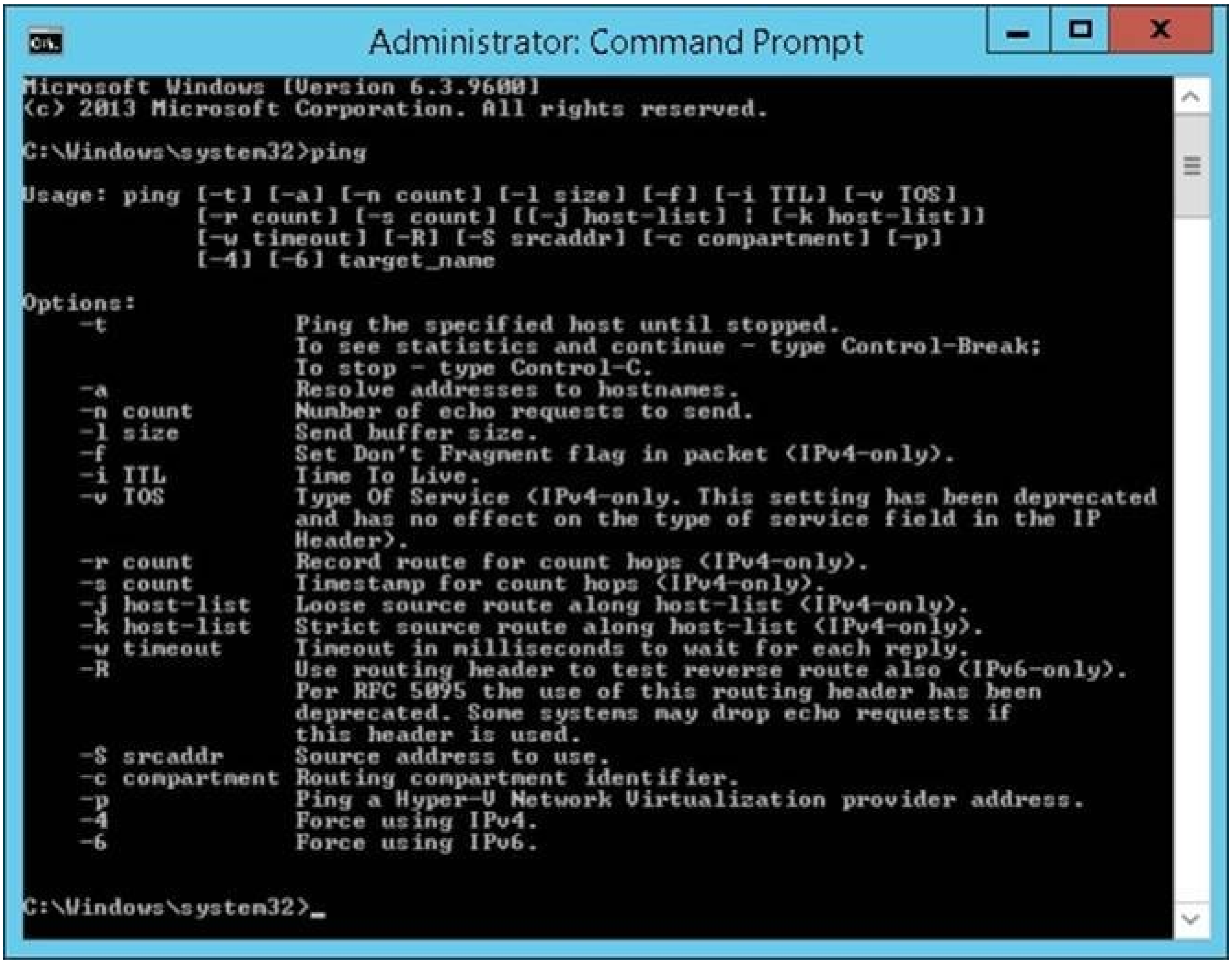
A value of 255 should be enough to get you anywhere in the world with a lot of hops to spare, but there are situations where packets will be dropped at TTL 0 anyway. Usually there is a routing loop involved when that happens. Like a ping pong match between 2 routers sending the packet back and forth.
This can happen when 2 routers believe that the IP packet destination is in the direction of the opposite router. TTL will then make sure that the packet is eventually dropped.

Technet24.ir

There are many reasons why this can happen, but usually it involves some misconfiguration of the routers.

When this happens, the Ping command will tell you that it happened as we'll see later on.

You can tweak the Ping command to act differently by using a few parameters. We'll be looking at the different parameters and seeing them in action later on.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.

C:\Windows\system32>_
```

Figure 4: The Ping command parameters

If you enter the Ping command without any parameters, the screenshot in figure 4 will be shown. This is a list of all possible parameters to use in combination with the Ping command.

Technet24.ir

A little bit of Traceroute

Traceroute is a route tracing utility that display a list of near-side router interfaces of the routers along the path between a source host and a destination. Tracert uses the IP TTL field in ICMP Echo Requests and ICMP Time Exceeded messages to determine the path from a source to a destination through an IP internetwork.

Traceroute (or Tracert as the command is called in Microsoft Windows) tells you the path a data packet takes between the source and destination machine or device.

The path is calculated by manipulating the TTL field in the data packets being sent. This happens automatically. You don’t have to do it.

With the Tracert command you just specify the destination, and the path will be laid out.

By sending a Ping Echo Request to the destination with a TTL of 1, the packet will be dropped at the first router. The Echo Reply will tell the source the address of where the packet was dropped, and you have successfully discovered the first hop in the path to the destination.

Next, the procedure is repeated, but this time the TTL is set to 2. The packet will be dropped at the second router and an Echo Reply will be sent back to the source, telling the source where this happened. You’ll then have the second hop mapped out in the path to the destination.

This procedure is repeated until you eventually reach the destination.

Technet24.ir

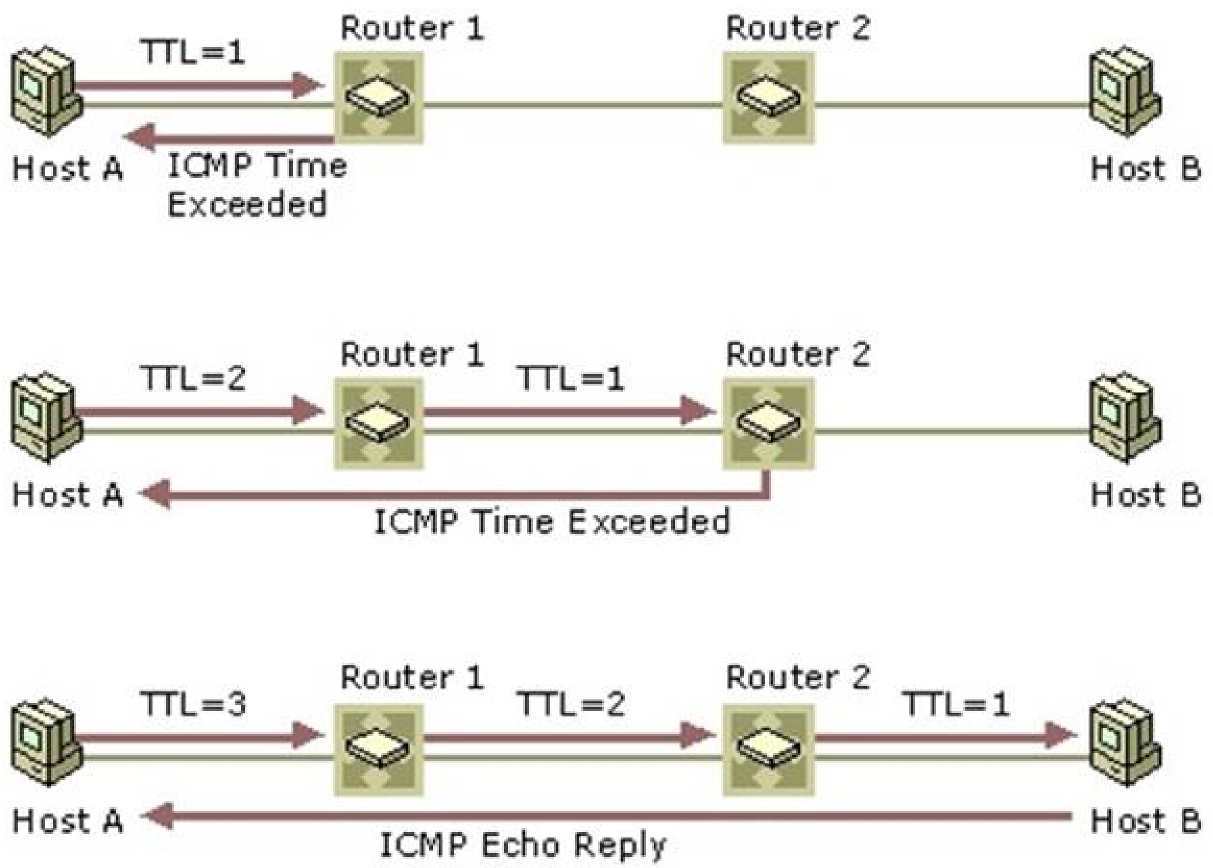
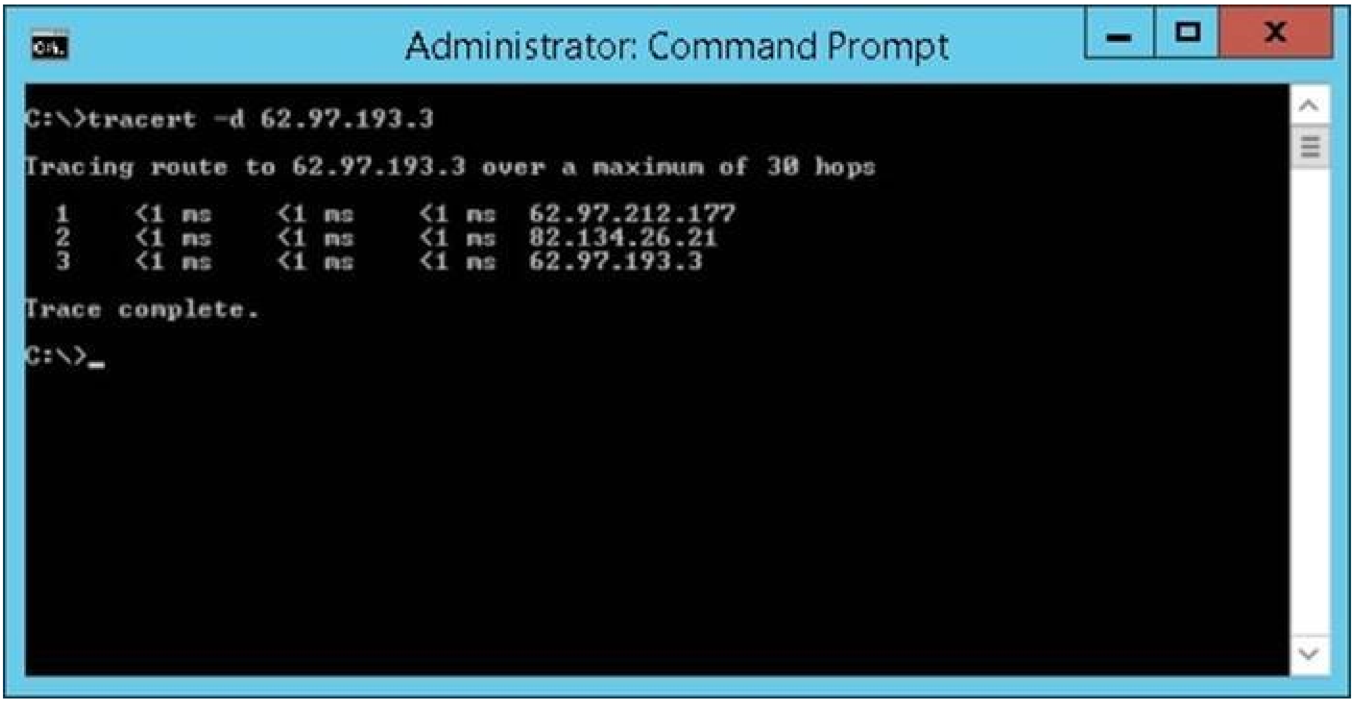


Figure 5: Traceroute overview

So then the TTL value is 0 the router handling the packet will never send the packet further. It will respond back to the source with a message that time exceeded (ICMP Time Exceeded).



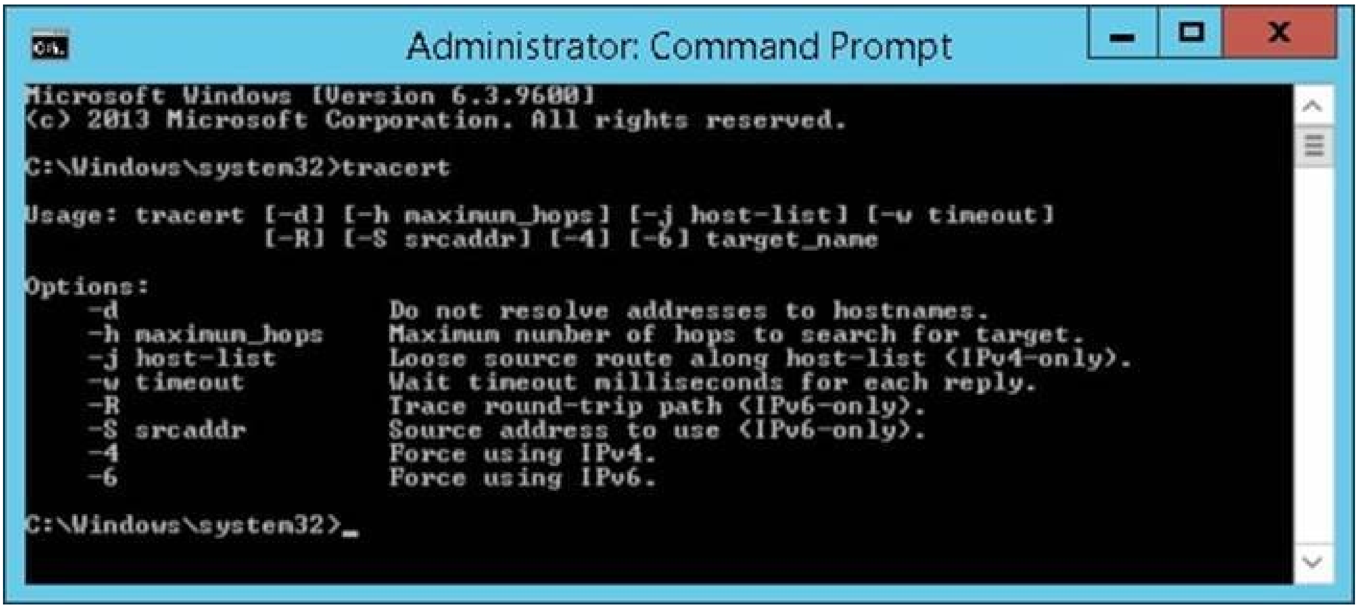
```
C:\>tracert -d 62.97.193.3

Tracing route to 62.97.193.3 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  62.97.212.177
  2    <1 ms    <1 ms    <1 ms  82.134.26.21
  3    <1 ms    <1 ms    <1 ms  62.97.193.3

Trace complete.

C:\>_
```

Figure 6: Traceroute example

Technet24.ir

In figure 6, a Tracert command is issued to IP address 62.97.193.3 and you can see that the destination is 3 routers (or hops) away and the round trip time for each.

Entering the Tracert command without any parameters will give you the following output:



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.

C:\Windows\system32>_
```

Figure 7: Tracert parameters

Technet24.ir

Technet24.ir

ICMP

So. A bit of technical stuff here.

If you just want to get started using Ping and Traceroute, you can go ahead and skip this chapter for now.

You can always come back to this later.

Internet Control Message Protocol (ICMP) is an error reporting and diagnostic utility and is considered a required part of any IP implementation. Understanding ICMP and knowing what can possibly generate a specific type of ICMP is useful in diagnosing network problems.

ICMPs are used by routers, intermediary devices, or hosts to communicate updates or error information to other routers, intermediary devices, or hosts.

Each ICMP message contains three fields that define its purpose and provide a checksum.
They are TYPE, CODE, and CHECKSUM fields.
The TYPE field identifies the ICMP message, the CODE field provides further information about the associated TYPE field, and the CHECKSUM provides a method for determining the integrity of the message.

Technet24.ir

Types

Type	Description
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect Message
8	Echo Request
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
17	Address Mask Request
18	Address Mask Reply

Echo Request & Echo Reply

This is the ICMP most used to test IP connectivity commonly known as PING. The Echo Request ICMP will have a Type field of 8 and a Code field of 0. Echo Replies have a Type field of 0 and a Code field of 0.

Destination Unreachable

When a packet is undeliverable, a Destination Unreachable, Type 3, ICMP is generated.

Type 3 ICMPs can have a Code value of 0 to 15:

Value	Description
0	Network Unreachable
1	Host Unreachable
2	Protocol Unreachable

Technet24.ir

3	Port Unreachable
4	Fragmentation needed and DF (Don't Fragment) set
5	Source route failed
6	Destination Network unknown
7	Destination Host unknown
8	Source Host isolated
9	Communication with Destination Network Administratively Prohibited
10	Communication with Destination Host Administratively Prohibited
11	Network Unreachable for Type Of Service
12	Network Unreachable for Type Of Service
13	Network Unreachable for Type Of Service
14	Network Unreachable for Type Of Service
15	Network Unreachable for Type Of Service

Source Quench

An ICMP Source Quench message has a Type field of 4 and Code 0. Source Quench messages are sent when the destination is unable to process traffic as fast as the source is sending it. The Source Quench ICMP tells the source to cut back the rate at which it is sending data. The destination will continue to generate Source Quench ICMPs until the source is sending at an acceptable speed.

Redirect Message

An intermediary device will generate an ICMP Redirect Message when it determines that a route being requested can be reached either locally or through a better path. Redirect Message ICMPs are Type 5 and are further defined by the following Code field values:

Value	Description
0	Redirect datagrams for the Network
1	Redirect datagrams for the Host

Technet24.ir

2	Redirect datagrams for the Type of Service and Network
3	Redirect datagrams for the Type of Service and Host

Time Exceeded

If a router or host discards a packet due to a time-out, it will generate a Time Exceeded Type 11 ICMP. The Time Exceeded ICMP will have a Code value of either 0 or 1. A Code 0 is generated when the hop count of a datagram is exceeded and the packet is discarded. A Code 1 is generated when the reassemble of a fragmented packet exceeds the time-out value.

Parameter Problem

When an intermediary device or host discards a datagram due to inability to process, an ICMP 12 is generated. Common causes of this ICMP are corrupt header information or missing options. If the reason for the ICMP is a required missing option, the ICMP will have a Code value of 1. If the Code value is 0, the Pointer field will contain the octet of the discarded datagram’s header where the error was detected.

Timestamp Request & Timestamp Reply

Timestamp Request and Timestamp Reply is a rudimentary method for synchronizing the time maintained on different devices. The Request has a Type field of 13 and the Reply is Type 14. This method for time synchronization is crude and unreliable. Therefore, it is not heavily used.

Technet24.ir

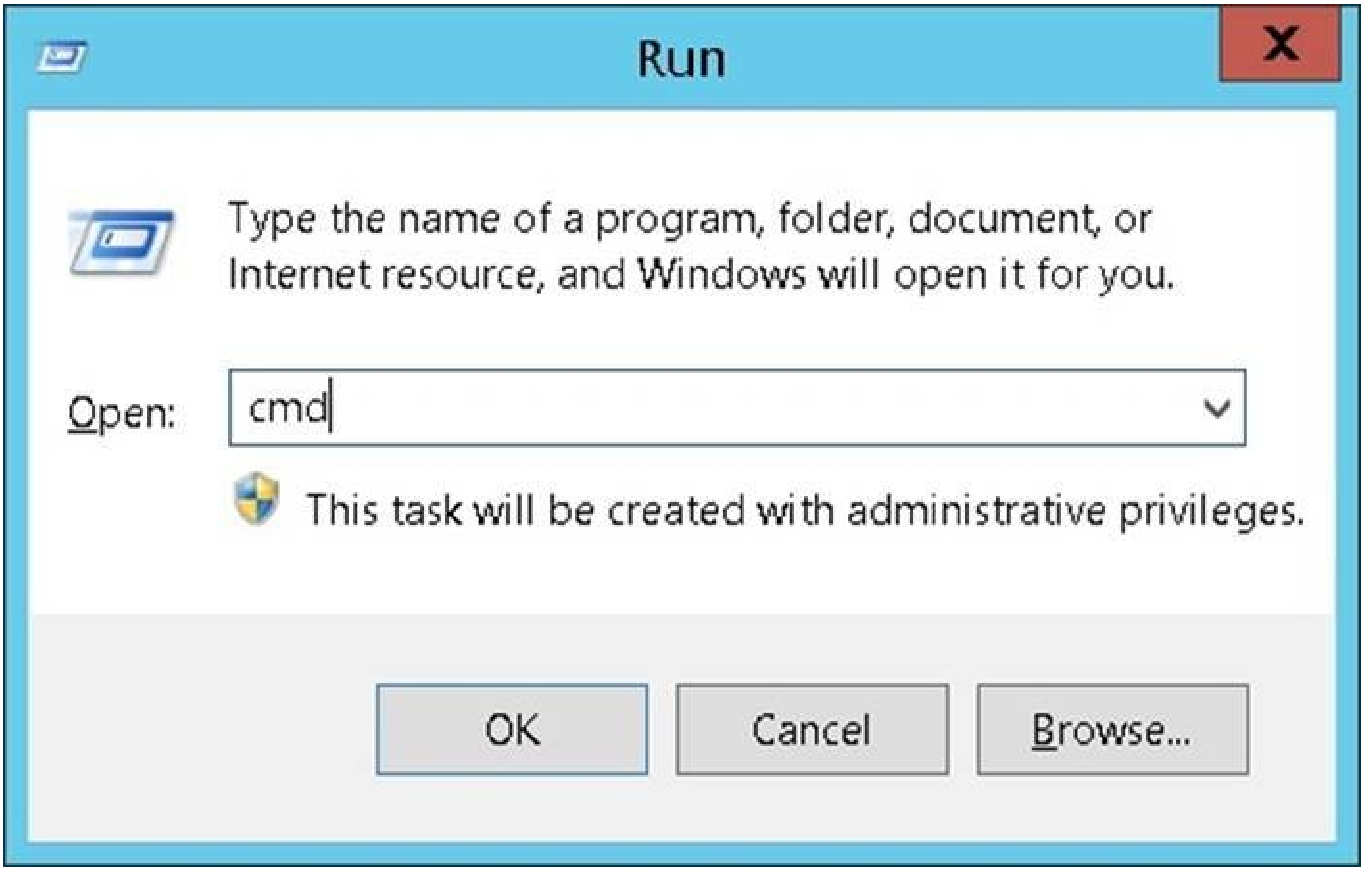
Technet24.ir

Using Ping

Okay, so now we'll get down to actually using the Ping command. With a bit of practice it's easy.

To get started you'll need to start the Microsoft Windows command line utility and there are several ways to do this.

One way is clicking the Start button, choose Run and then just enter **cmd** and finally clicking OK.



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

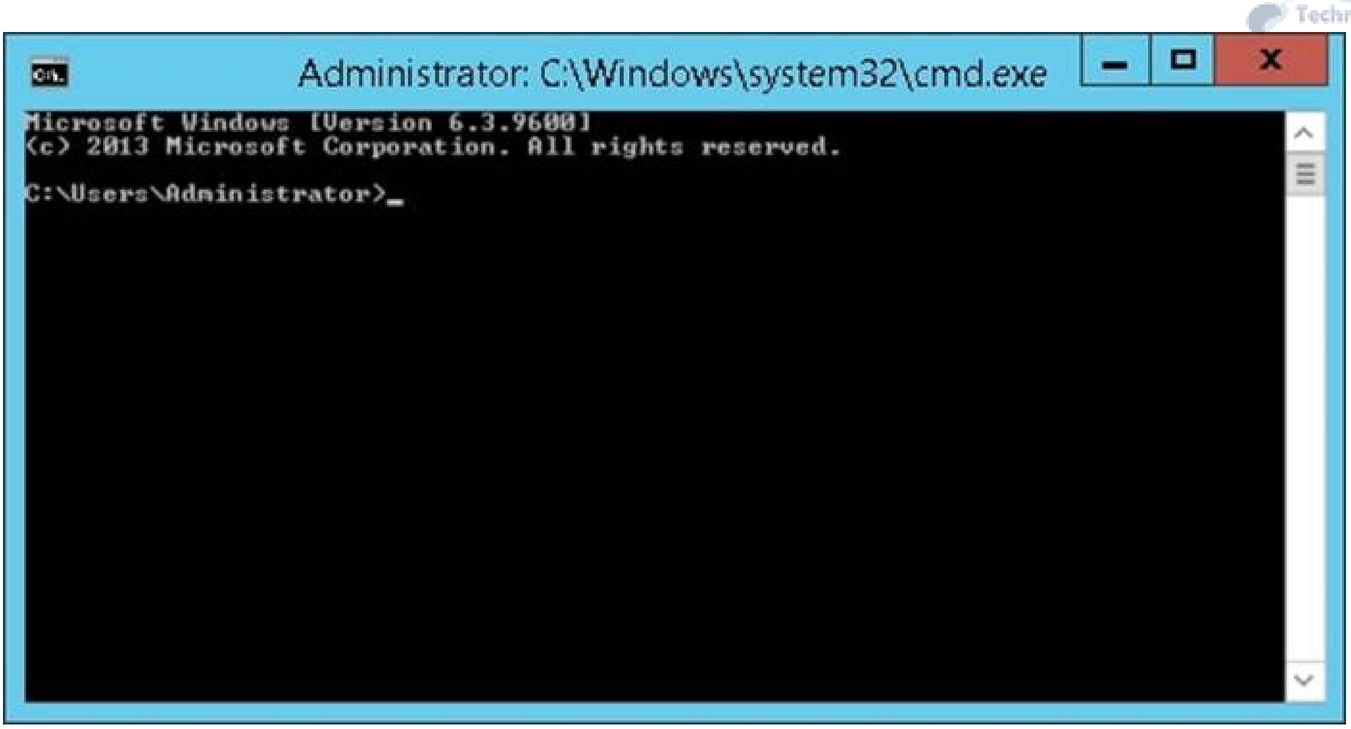
Open: cmd

This task will be created with administrative privileges.

Figure 8: The Run dialog

Clicking OK should give you the following window and you are ready to go:

Technet24.ir



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>_
```

Figure 9: The Command Line Utility

You can also find the Command Line Utility on the Microsoft Windows menu. Depending on what version of windows you are using the icon for the utility might be placed differently than the picture you see below taken from Microsoft Windows Server 2012.

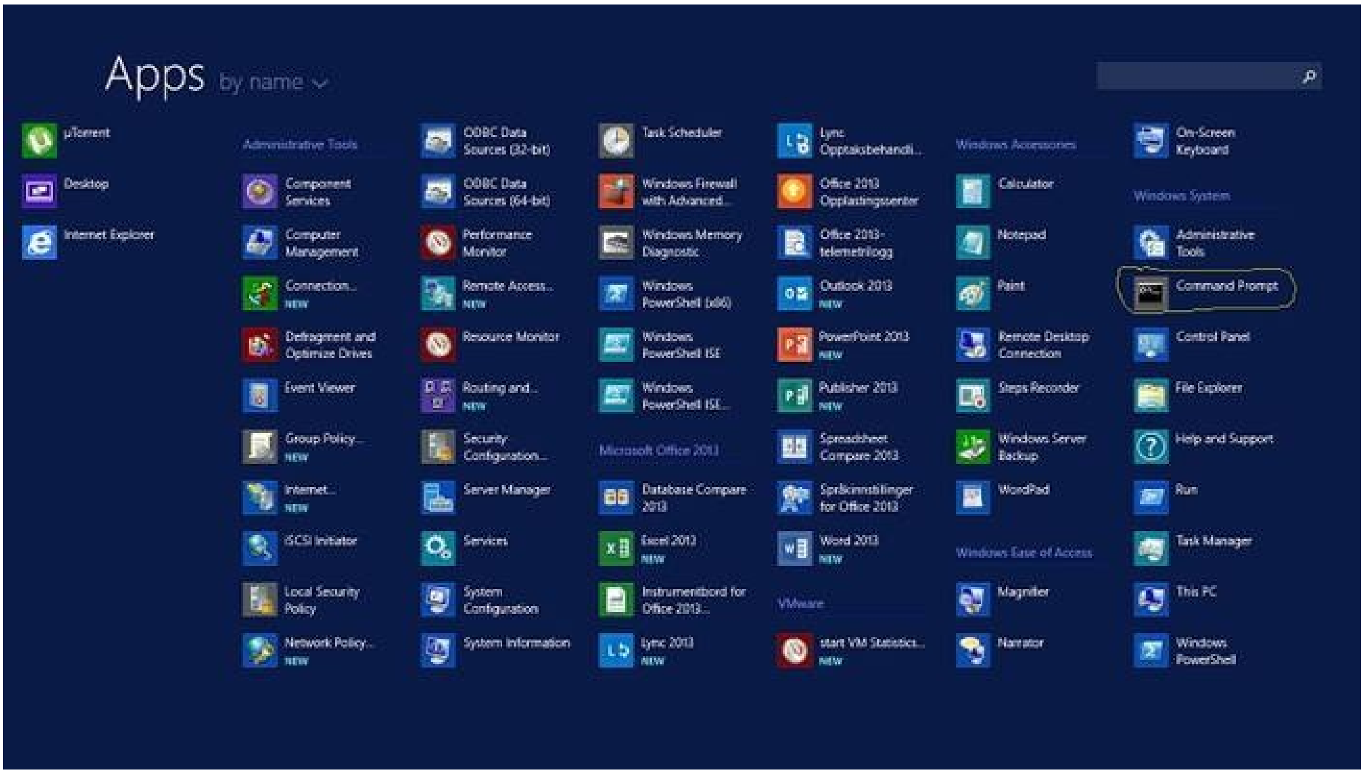


Figure 10: Microsoft Windows Menu

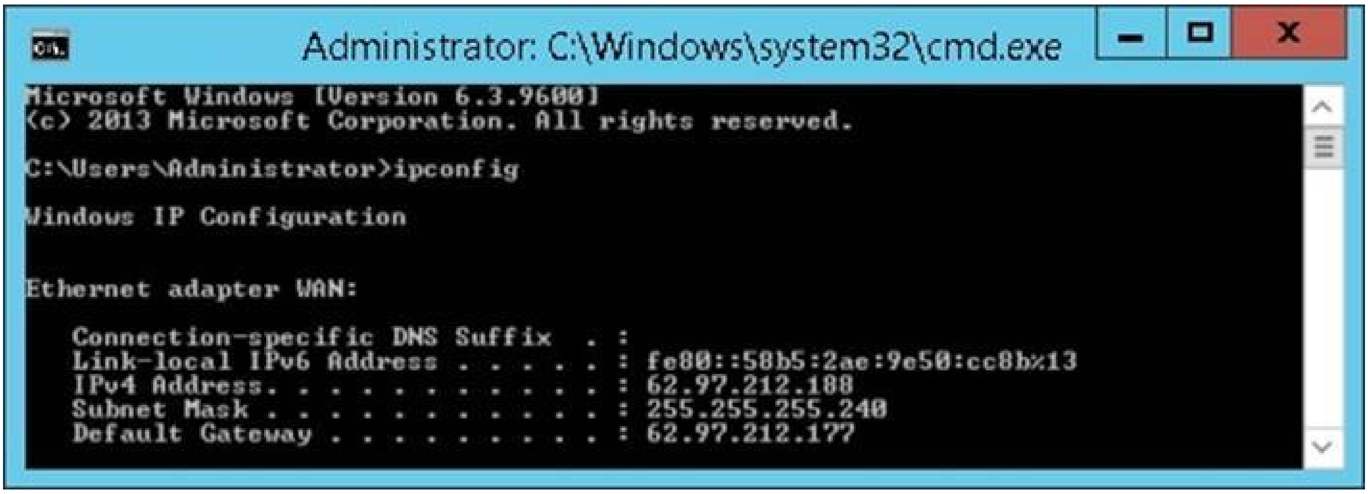
In figure 10 you'll see the Command Prompt icon (circled) and by clicking on the icon you’ll start the Windows Console for the Command Line Utility.

So go ahead and try to ping something.

You could try to ping your local router.

To find the IP address of your local router, you first need to find out what IP address it is using. A way to do this is using a utility without leaving the console you already got opened:

Type **IPCONFIG** at the prompt and hit enter. The command is not case sensitive.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter WAN:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::58b5:2ae:9e50:cc8b%13
   IPv4 Address. . . . . . . . . . . : 62.97.212.188
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . : 62.97.212.177
```

Figure 11: IPCONFIG

You might get a lot more information showing than what you see in figure 11 and you might have to scroll the window to get to the right information, but don’t worry.

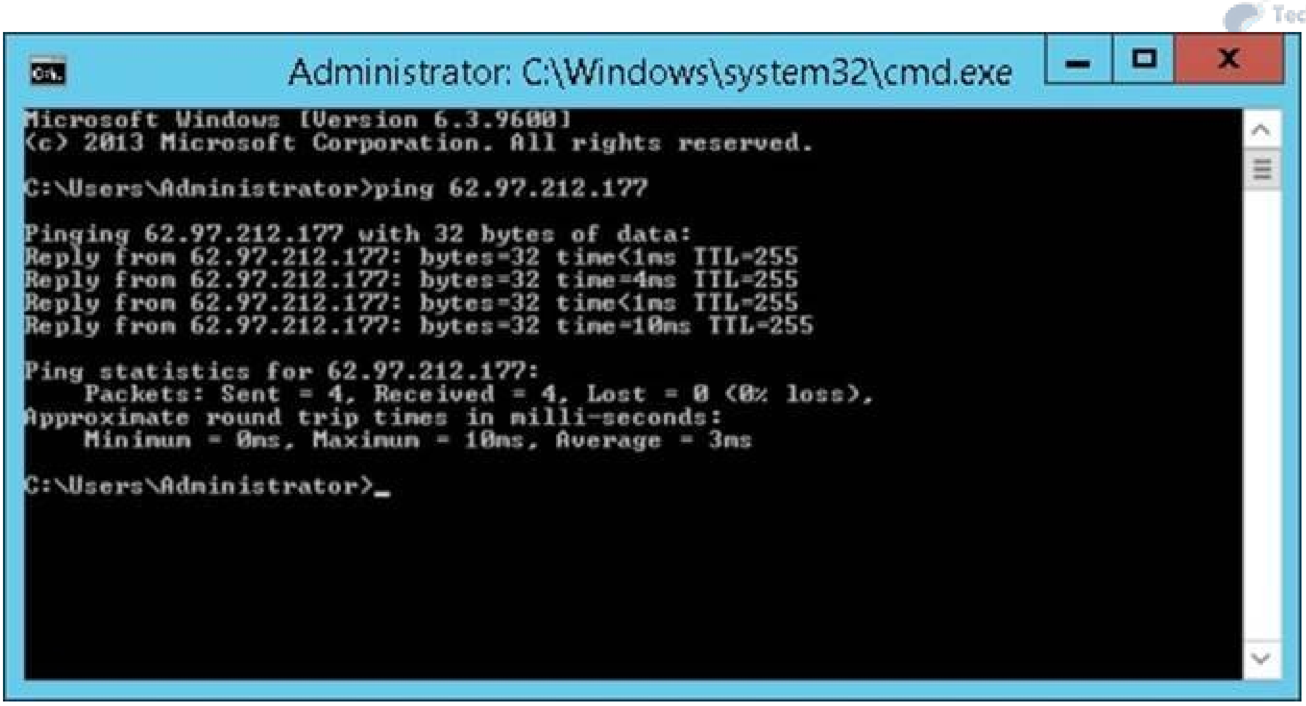
Depending on how many network cards are installed you might get more or less information. Also if IPv6 is enabled, some IPv6 related information will be showing as well.

From figure 11 I can see that my local IP address is 62.97.212.188.

What I also can see is that my Default Gateway is 62.97.212.177 and in most cases this is my local router for connecting to the outside world.

I’ll just go ahead and ping the Default Gateway:

Technet24.ir



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 62.97.212.177

Pinging 62.97.212.177 with 32 bytes of data:
Reply from 62.97.212.177: bytes=32 time<1ms TTL=255
Reply from 62.97.212.177: bytes=32 time=4ms TTL=255
Reply from 62.97.212.177: bytes=32 time<1ms TTL=255
Reply from 62.97.212.177: bytes=32 time=10ms TTL=255

Ping statistics for 62.97.212.177:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\Users\Administrator>_
```

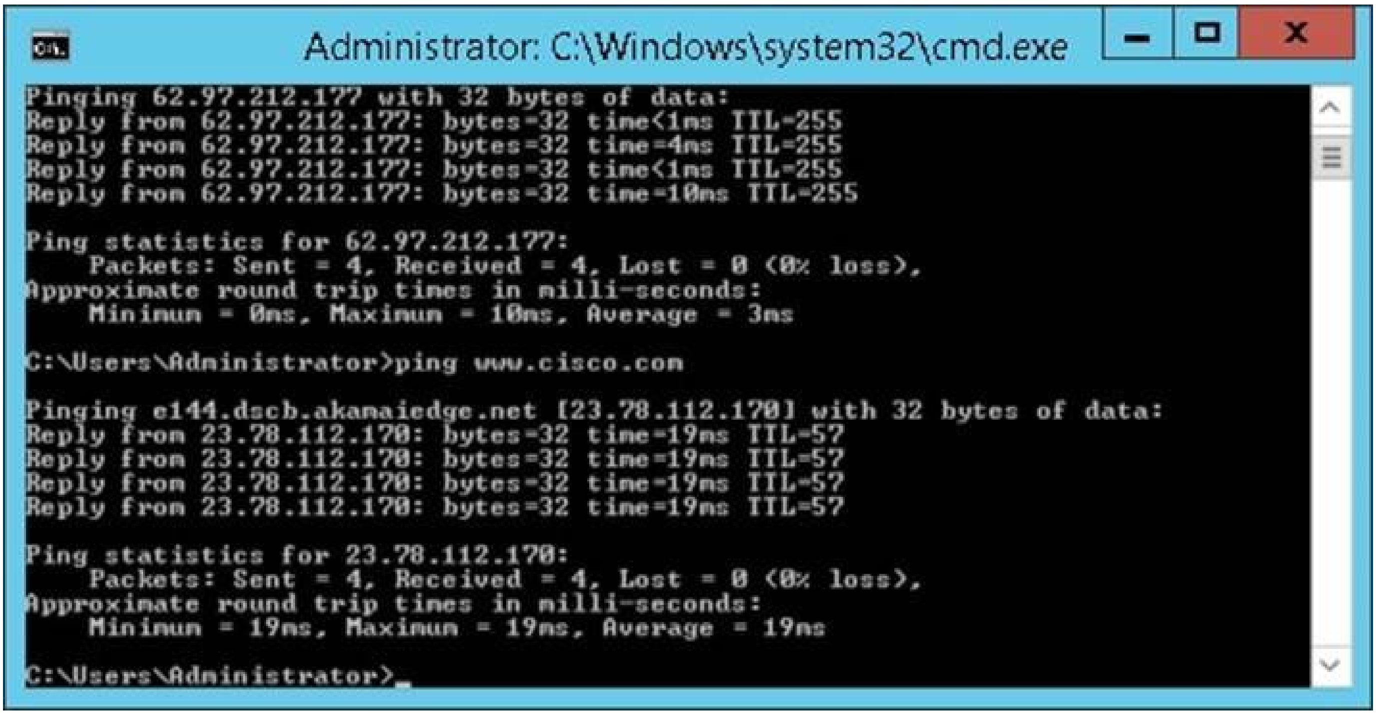
Figure 12: Pinging Default Gateway

It’s alive!!!

Good news. I can then probably surf the Internet if I want to.

To check if I can, I could probably just open up a browser and then open some of my favorite web sites, but I am not going to do that. I want to check with Ping.

So I would like to know if www.cisco.com is reachable from my computer. I don’t know the IP address to use, so I just ping the site using the name instead:



```
Pinging 62.97.212.177 with 32 bytes of data:
Reply from 62.97.212.177: bytes=32 time<1ms TTL=255
Reply from 62.97.212.177: bytes=32 time=4ms TTL=255
Reply from 62.97.212.177: bytes=32 time<1ms TTL=255
Reply from 62.97.212.177: bytes=32 time=10ms TTL=255

Ping statistics for 62.97.212.177:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\Users\Administrator>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.78.112.170] with 32 bytes of data:
Reply from 23.78.112.170: bytes=32 time=19ms TTL=57
Reply from 23.78.112.170: bytes=32 time=19ms TTL=57
Reply from 23.78.112.170: bytes=32 time=19ms TTL=57
Reply from 23.78.112.170: bytes=32 time=19ms TTL=57

Ping statistics for 23.78.112.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 19ms, Average = 19ms

C:\Users\Administrator>_
```

Figure 13: Pinging www.cisco.com

Technet24.ir

Hallelujah!

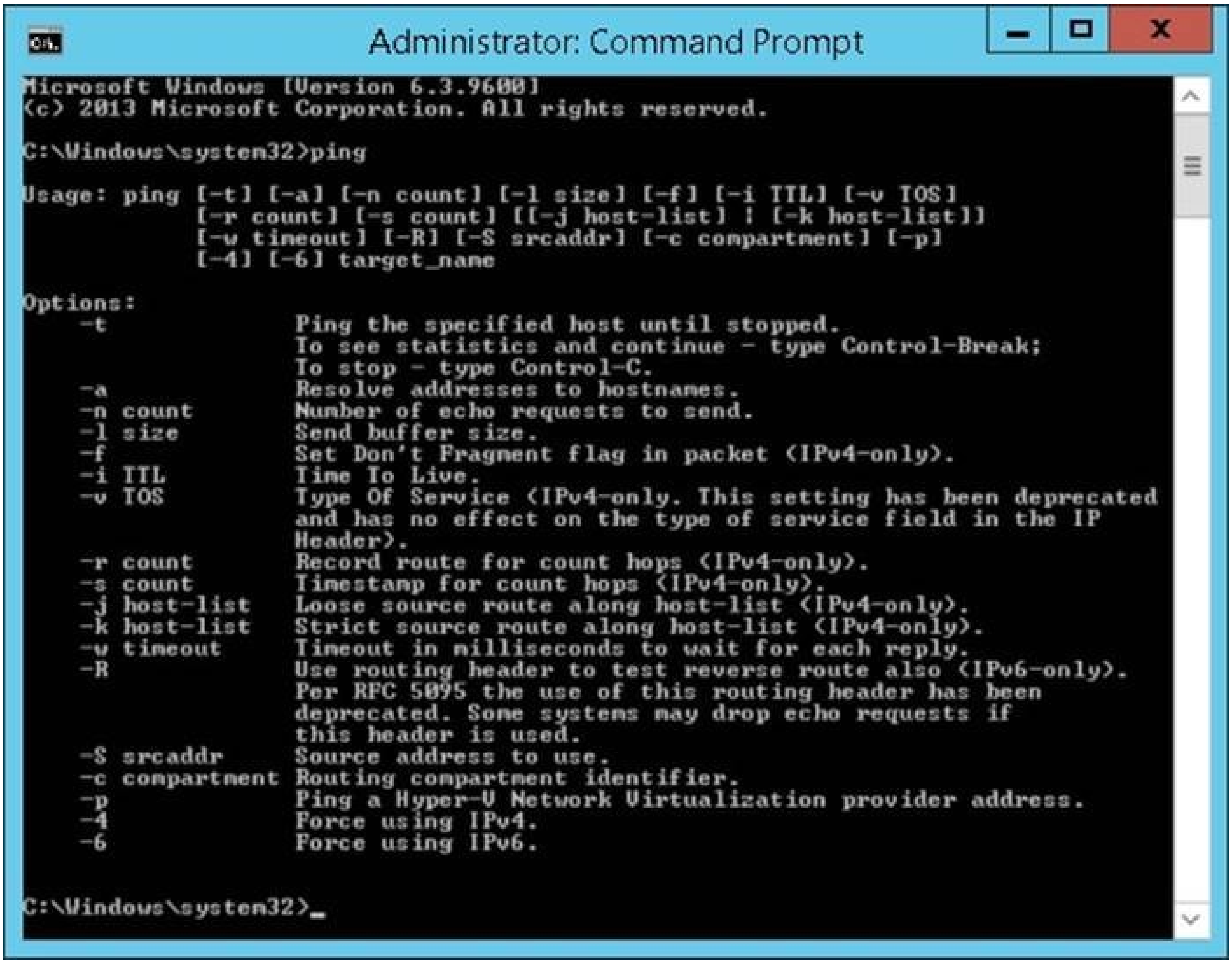
It’s up.
So here Ping first do a DNS lookup to get the IP address of www.cisco.com and then it pings that address which in this case is 23.78.112.170.

So from these few commands I now know that my Internet connection is ok. I know that DNS is working or else the Ping command would not be able to resolve www.cisco.com to an IP address and finally I know that www.cisco.com is up and running.

So let’s look at what else we can do with the Ping utility.

Technet24.ir

Parameters



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.

C:\Windows\system32>_
```

Figure 14: Ping parameters

Parameter (case sensitive)	Description
-t	Pings a host continually until the user breaks it by hitting Control key + Break Key or Control Key + C key. **Example: ping –t 192.168.1.10**
-a	Tries to look up the name of the IP address you are pinging. Like a reverse DNS lookup. Usually you get an IP address by pinging a name, but in this case you'll get back a name from the lookup. **Example: ping –a 193.212.1.10**
	Let you decide how many Echo Requests should be sent in the ping command. Usually 4 requests is more than enough but if you want to see if the

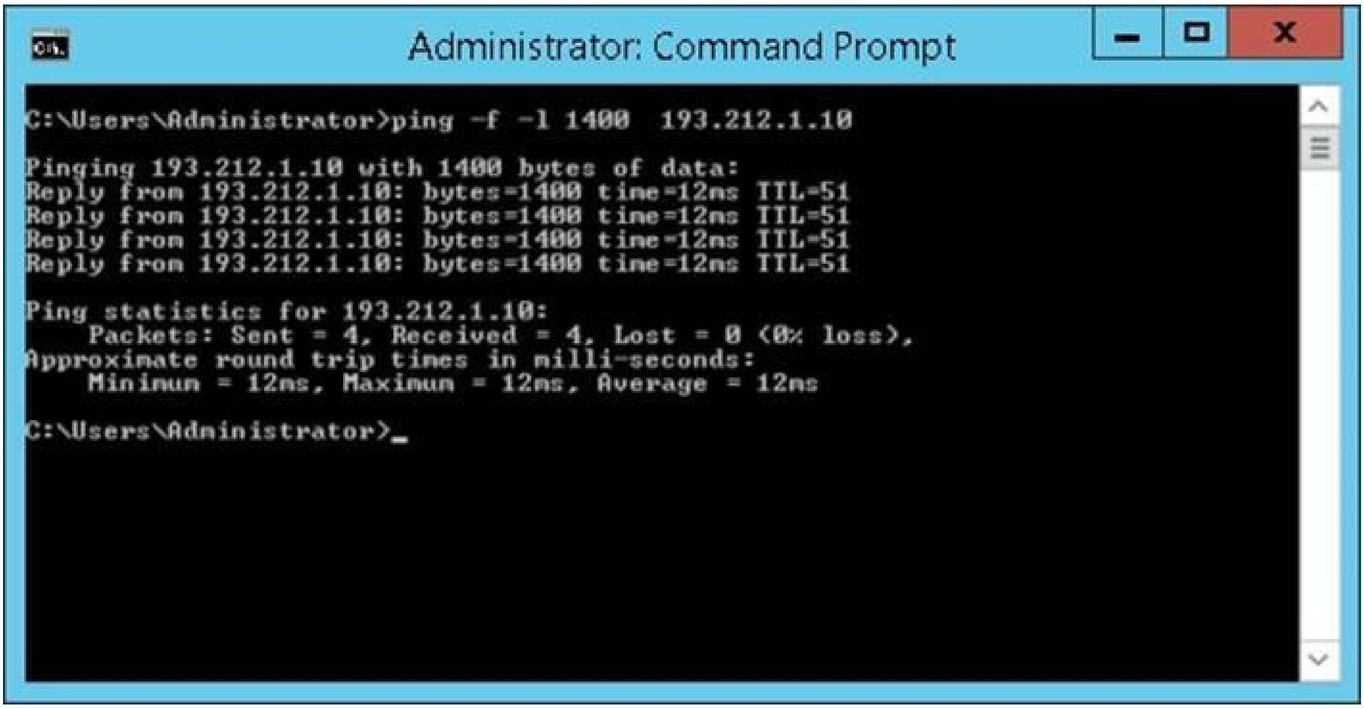
Technet24.ir

-n count	destination replies in a stable manner, you could try to send a lot. In that case the –t parameter is just as useful. The following will send 10 Echo Requests to 193.212.1.10 **Example: ping –n 10 193.212.1.10**
-l Size	A standard Echo Request is sent with a data portion of 32 bytes per packet. This is very small and normal data packets are usually around 1500 bytes. You can choose to send Echo Request with larger data sizes. The following example send an Echo Request with 900 bytes data portion. Look at section on MTU for more information about data packet sizes. **Example: ping –l 900 193.212.1.10**
-f	Set the “don’t fragment” bit in the Echo Request packet being sent. All devices connected to a network will have a definition of how big the data portion of a packet can be when sending them out on the cable. Some standard values exists. In some cases the path a packet takes encounters hops were the packet must pass that don’t support the size of the packet. The packet is too big. Normally when this happens, the packet is split up into smaller segments and then shipped. The packet will be reassembled later on. If you set the “don’t fragment” bit, this will not happen. The packet will not be segmented and shipped, but dropped instead. This is useful if you need to find the maximum packet size you can use between 2 points. Look at the MTU section for more information. **Example: ping –f 193.212.1.10**
-I TTL	With the –I parameters you can manipulate the Time To Live value. This is normally 255, but you can set it to any value between 1 and 255. You can do a manual Traceroute this way if you like. The following example sets the TTL to 2. The packet will be dropped after 2 hops. **Example: ping –I 2 193.212.1.10**
	Specifies the amount of time, in milliseconds, to wait for the echo reply message that corresponds to a

Technet24.ir

-w timeout	given echo request message. If the echo reply message is not received within the time-out, ping displays the “Request timed out” error message. The default time-out value is 4000 (4 seconds). Usually the default value is good enough, but in slow networks or with slow responding hosts you can adjust the timeout. **Example: ping –w 2000 193.212.1.10**
-S source address	If the source device has more than one network adapter you can choose to specify which adapters IP address should be used as the source IP address of the Echo Request. In the following example 10.0.1.5 is used as the source address. **Example: ping –S 10.0.1.5 193.212.1.10**
-4	Force the use of IPv4.
-6	Force the use of IPv6.

You can also combine multiple parameters in the same command, and sometimes you need to. Look at the following example:



```
C:\Users\Administrator>ping -f -l 1400  193.212.1.10

Pinging 193.212.1.10 with 1400 bytes of data:
Reply from 193.212.1.10: bytes=1400 time=12ms TTL=51
Reply from 193.212.1.10: bytes=1400 time=12ms TTL=51
Reply from 193.212.1.10: bytes=1400 time=12ms TTL=51
Reply from 193.212.1.10: bytes=1400 time=12ms TTL=51

Ping statistics for 193.212.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 12ms, Average = 12ms

C:\Users\Administrator>_
```

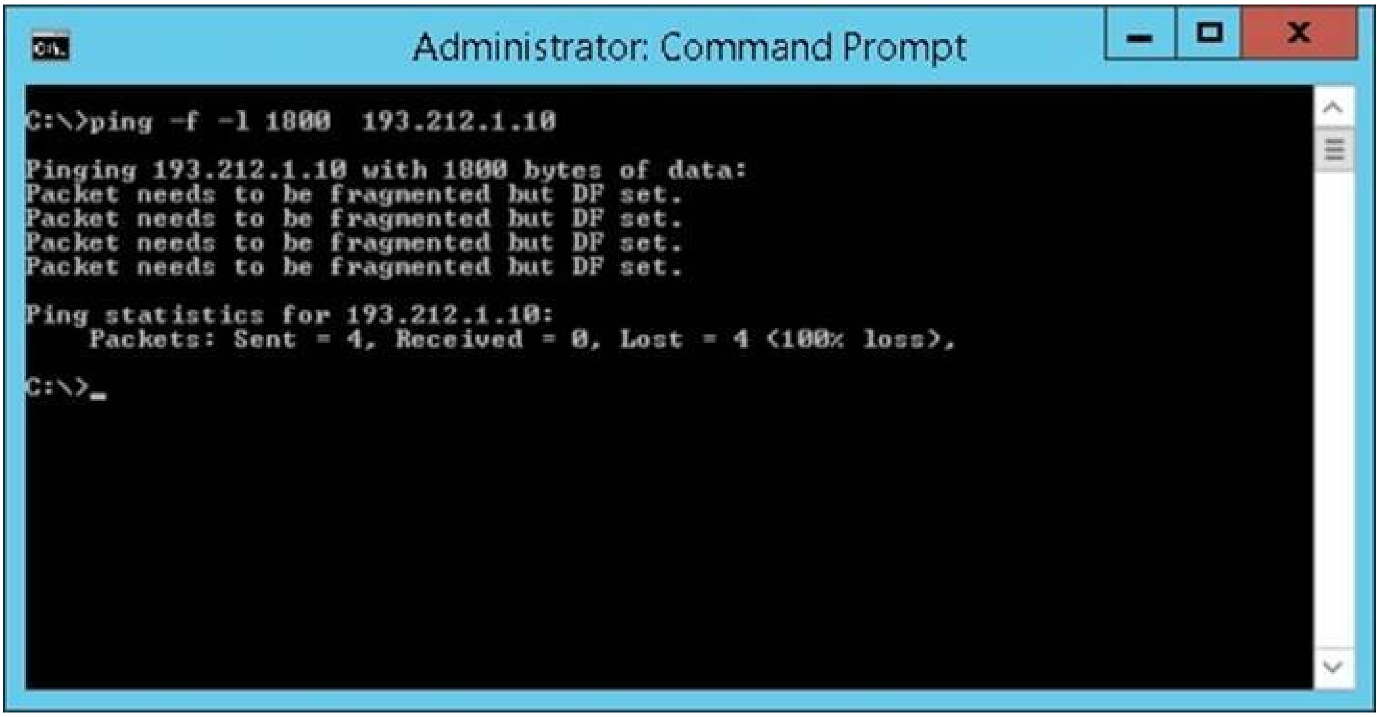
Figure 15: Ping with multiple parameters

In figure 15 we ping IP address 193.212.1.10 with both the –f and the –l parameters. Here we are telling Ping to send Echo requests with the “don’t fragment” bit set and a data portion size of 1400 bytes.

You can see from the Echo Replies that we are getting 1400 bytes packets in return.

If somewhere along the path the requests should encounter a hop that did not accommodate for 1400 bytes packets, the request would be dropped by that hop or router.

Let’s look at what happens when the data portion is too big:



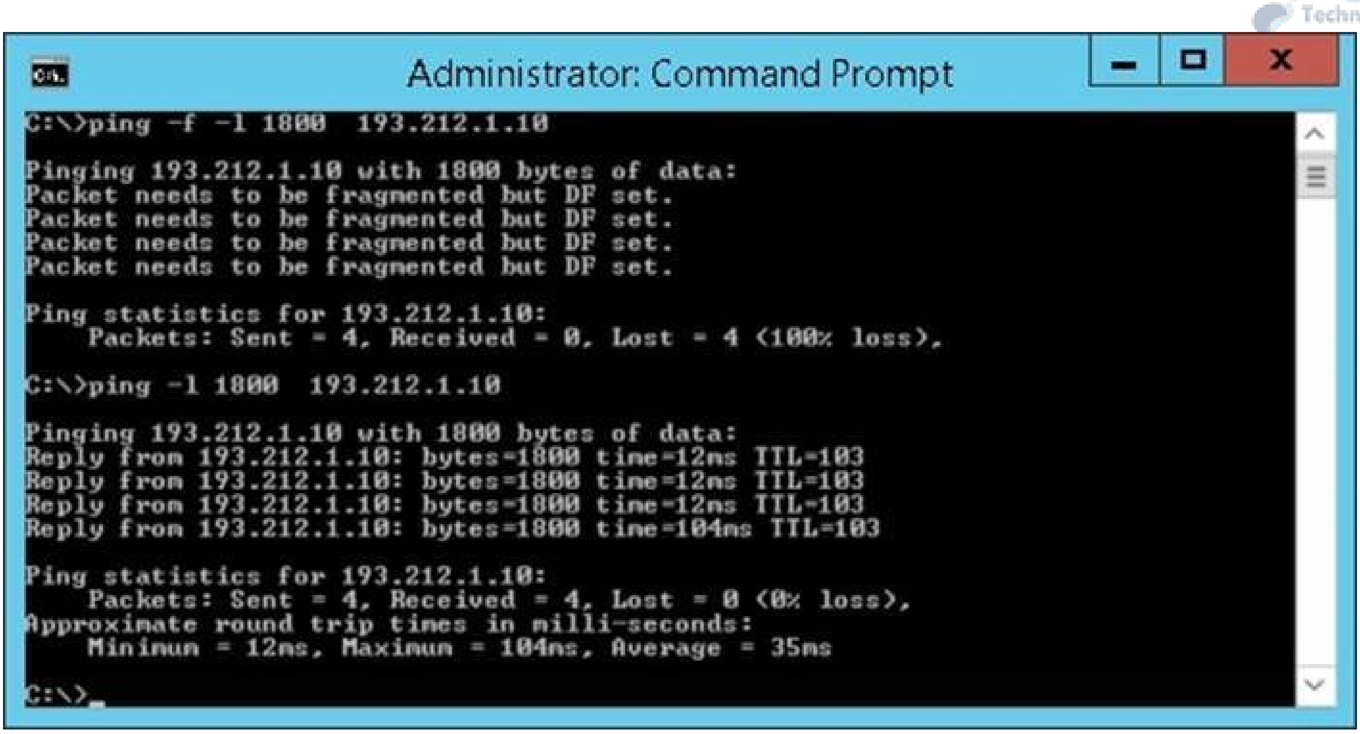
```
C:\>ping -f -l 1800  193.212.1.10

Pinging 193.212.1.10 with 1800 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 193.212.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>_
```

Figure 16: Ping with data portion too big

Here you see that the packets do not reach its destination and the reason being that the packets are too big to be sent through.

If we drop the “don’t fragment” options, we’ll get the following result:

Technet24.ir



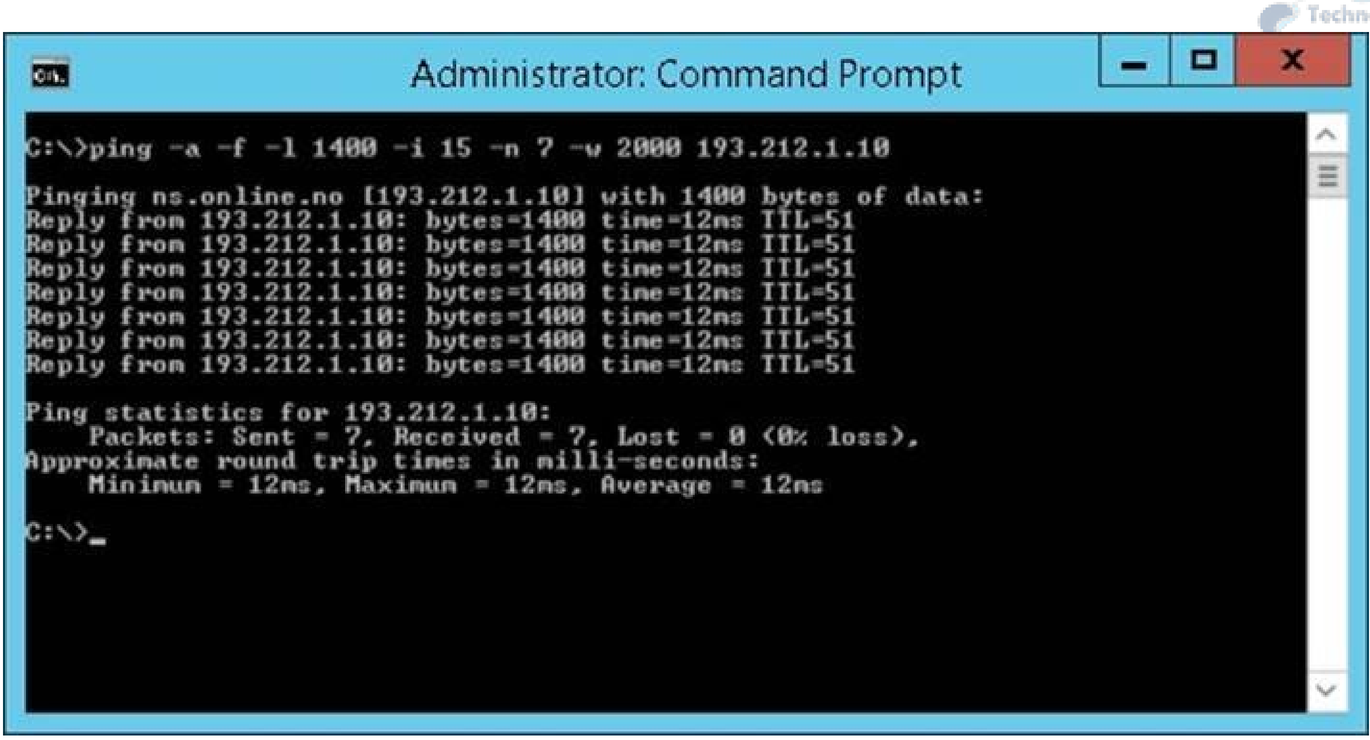
```
C:\>ping -f -l 1800  193.212.1.10

Pinging 193.212.1.10 with 1800 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 193.212.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping -l 1800  193.212.1.10

Pinging 193.212.1.10 with 1800 bytes of data:
Reply from 193.212.1.10: bytes=1800 time=12ms TTL=103
Reply from 193.212.1.10: bytes=1800 time=12ms TTL=103
Reply from 193.212.1.10: bytes=1800 time=12ms TTL=103
Reply from 193.212.1.10: bytes=1800 time=104ms TTL=103

Ping statistics for 193.212.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 104ms, Average = 35ms

C:\>_
```

Figure 17: Big packet with OK to fragment

The packet is still too big, but since we allow fragmentation of packets, the router having problems with big packets just divide it into smaller portions. The packet gets reassembled later on.

Not every systems or applications are too happy about fragmentation and this is often a problem. In such cases you can witness slow responses, web pages not being loaded fully or even mail with attachments not getting through to the receiver.
For more information, look at the MTU section later on.

One last example of multiple parameters:



```
C:\>ping -a -f -l 1400 -i 15 -n 7 -w 2000 193.212.1.10

Pinging ns.online.no [193.212.1.10] with 1400 bytes of data:
Reply from 193.212.1.10: bytes=1400 time=12ms TTL=51
Reply from 193.212.1.10: bytes=1400 time=12ms TTL=51
Reply from 193.212.1.10: bytes=1400 time=12ms TTL=51
Reply from 193.212.1.10: bytes=1400 time=12ms TTL=51
Reply from 193.212.1.10: bytes=1400 time=12ms TTL=51
Reply from 193.212.1.10: bytes=1400 time=12ms TTL=51
Reply from 193.212.1.10: bytes=1400 time=12ms TTL=51

Ping statistics for 193.212.1.10:
    Packets: Sent = 7, Received = 7, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 12ms, Average = 12ms

C:\>_
```

Figure 18: One last example of multiple parameters

Looks good.

Usually you won’t need to add this many parameters. It’s just to show you that you can. So in this example we ping 193.212.1.0 with name lookup (ns.online.no), “don’t fragment” bit set, a data portion of 1400 bytes, TTL value of 15, send 7 Echo Requests and finally a timeout value of 2000 milliseconds. Nice one.

Technet24.ir

Ping and firewall’s

You might need this information if you ever need to ping a destination and a firewall is in the path to that very destination.

Today’s firewalls are said to be state full. What this means is that they keep state of traffic passing through. This is a good thing. It allows us to create rules that dictates what is allowed and denied, but we don’t have to worry about returning traffic.

So if you allow HTTP traffic (like web browsing) from your local network to the Internet, you don’t have to worry about or make rules accepting the traffic returning back to you. The firewall keeps track of those packets.

But when it comes to ICMP this is not the case.

The reason is that ICMP do not work the same way as TCP. TCP keeps a session going when you communicate over the network. So when you fire up that Facebook page, a TCP session is initiated from your computer to www.facebook.com and that session stays open until you leave that page. The session is then closed.

To connect and use a TCP session your device first asks the server if it can connect. Then they agree on some terms before the session is activated.

With those kind of sessions it’s relatively easy for the firewall to allow the returning traffic from the Facebook page, back to your computer without you making any extra firewall rules.

Ping on the other hand, do not use sessions.

When you ping a device, you initiate a packet send, without a session first being made, to the destination. You do not ask the destination if you can connect, you just send.

The device that is sending you a reply to that request is doing exactly the same. It does not ask to connect or piggyback on the packet you first sent. It initiates a packet send on its own.

So when the firewall is unable to keep state of the packets, you have to specifically permit those packets through the firewall.

If you create a rule in your firewall allowing ping out on the Internet, the Ping Requests will probably make it to the destination. The problem is that the Echo Reply will be dropped by the firewall and you’ll get a destination unreachable in you console window.

So in that case you need to permit ICMP or just Echo Reply from the Internet through your firewall.

A lot of computers also have personal firewalls. Microsoft Windows even has one built in. These firewalls can prevent you from getting an Echo Reply in many cases. Just things to be aware of.

Technet24.ir

Technet24.ir

Basic troubleshooting

If Ping indicates a high packet loss or slow round-trip response on a LAN, your network might have a hardware problem. On a WAN, these results may be normal, and TCP/IP is designed to handle the variability. On a LAN, round-trip time is very low, and you see little or no packet loss. If this isn’t the case, test your cables, cable terminations, hubs, switches, and transceivers.

Problem	Test / Solution
What’s my IP address?	Use command line ipconfig to find the address.
What’s my routers IP address?	Use command line ipconfig and look at the default gateway address.
What’s my subnet mask?	Use command line ipconfig and look at the subnet mask field.
I cannot connect to the Internet. Web page not found.	Try another web site just to make sure. Try pinging website by name. If you get a reply then the Internet connection should be fine. If you do not get a reply, try pinging something on the Internet by address, like 8.8.8.8 (Google server). If you get a reply when doing this, you might have a DNS lookup problem. Check your DNS settings. If you don’t get a reply from 8.8.8.8, try pinging your default gateway/router. If you get a reply, you know that the connection from your PC to the router is OK and that the problem must be somewhere outside your router. If you do not get a reply from your default gateway, check the router,

Technet24.ir

	maybe restart it. Other than that, check cables and other connectors between your computer and the router.
Ipconfig tells me that I have no default gateway	Without a default gateway you will never be able to use the Internet service. A lack of default gateway is in many cases related to IP address assignment problems. Usually there is a DHCP server in your network (in most home networks this is also the default gateway or router). The DHCP server is responsible for assigning IP addresses to all the computers connecting to that network. If the DHCP server is not available for any reason, you will often see that there is no default gateway configured on the computer and most likely you will have an IP address starting with 169.254.x.x Restart router and check cabling. Then restart computer.
Everything works fine but I cannot ping anything on the Internet even though I know the destinations are online.	You firewall is probably dropping the Echo Reply packets or some personal firewall is dropping these packets. Check firewall configuration.
When I ping some host the first Echo Reply is never received. The 3 following replies comes through fine.	Computers and routers have an internal table with local MAC address to IP address binding. This is called the ARP table. If the destination you are trying to ping is not in that table (this is only important for the device nearest the destination you are trying to ping) the computer or router needs to first do an ARP request to get that IP address corresponding MAC address. This can cause the first Echo Request to time out.

Technet24.ir

	If you do a new ping shortly after, all requests and replies should come through fine.
When I try to ping a destination I only get “TTL expired in transit”.	This is normally caused by either routing loops or you are trying to ping an address that is too far away. If you ping an address that does not respond in an existing network, let’s say your home network, you should get a “Destination host unreachable”. When you get a TTL expired message it means that the packet has travelled for so long that the TTL value has gotten to 0.

Technet24.ir

About MTU

> ***Maximum transmission unit***
>
> *In computer networking, the maximum transmission unit (MTU) of a communications protocol of a layer is the size (in bytes) of the largest protocol data unit that the layer can pass onwards. MTU parameters usually appear in association with a communications interface (for example an Ethernet interface).*
>
> *A larger MTU brings greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU also means processing of fewer packets for the same amount of data. In some systems, per-packet-processing can be a critical performance limitation.*
>
> *However, this gain is not without some downside. Large packets can occupy a slow link for some time, causing greater delays to following packets and increasing lag and minimum latency.*
>
> *Large packets are also problematic in the presence of communications errors. Corruption of a single bit in a packet requires that the entire packet be retransmitted. At a given bit error rate, larger packets are more likely to be corrupted. Retransmissions of larger packets takes longer. Despite the negative effects on retransmission duration, large packets can still have a net positive effect on end-to-end TCP performance.*

The MTU being used between 2 systems decides how much data can be passed along in each packets. Theoretically larger packets (larger MTU) should be faster and better. This is not always the case in practice.

In a local network where you have full control over all the equipment you can force a larger MTU with success, but when you connect this local net to the “outside”, problems can arise.

In Ethernet (which is standard for most TCP/IP communication) the MTU is usually around 1500 bytes. In a typical packet you have a header, data and some other portions that make up the Ethernet packet.

Technet24.ir

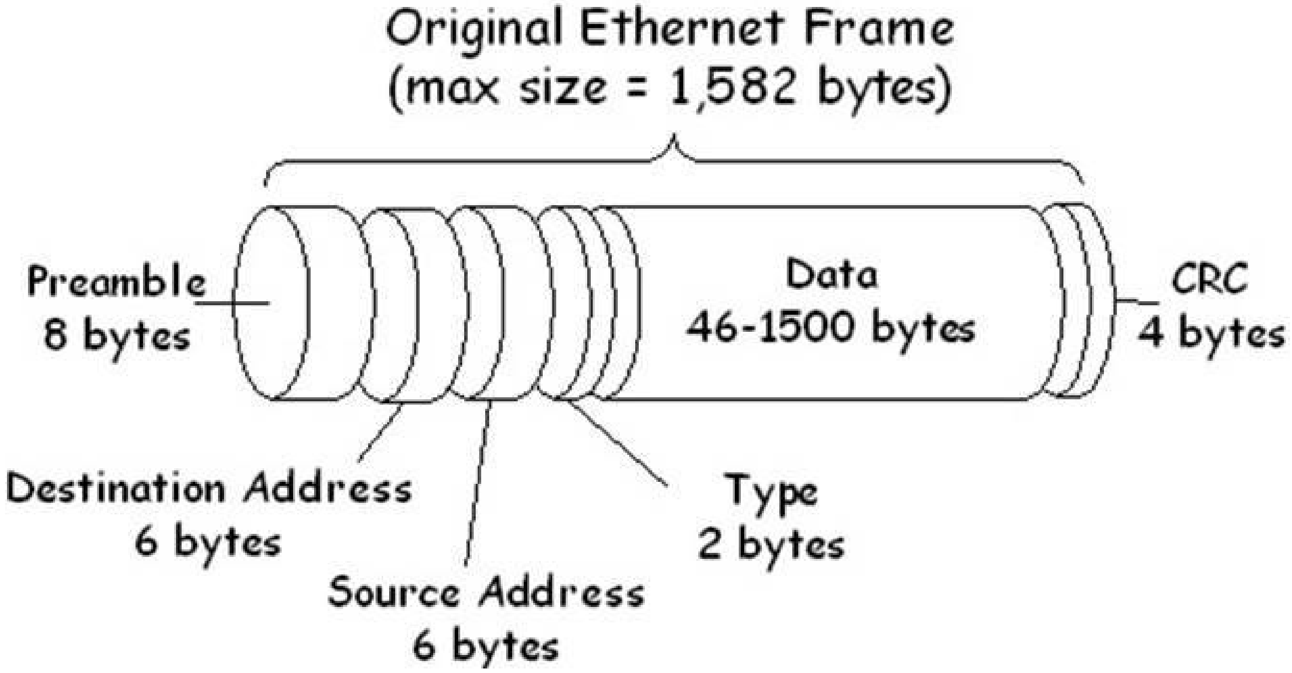


Figure 19: Ethernet frame

In some situations extra headers gets added to the packet. For example VPN tunnels and PPPoE connections add extra headers, making the packet larger. This could mean trouble in some situations.

When 2 systems need to communicate, one of the first thing they decide on, is the MTU size to use. This happens every time a new session is started.

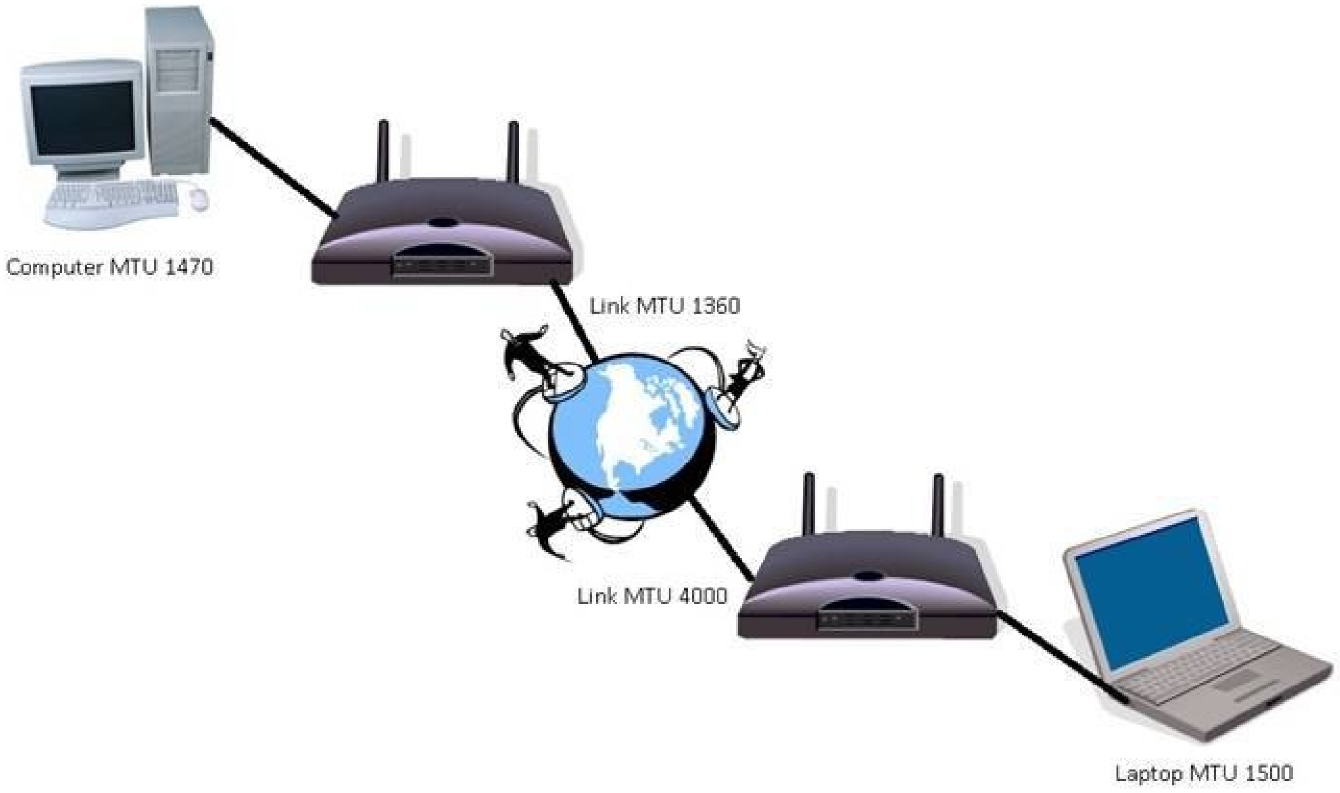


Figure 20: Session MTU

Technet24.ir

If you look at figure 20 the desktop computer has a MTU of 1470 and the laptop has a MTU of 1500.

If these 2 devices sets up a session, they will agree on MTU before starting to exchange more packets. They will always agree on the smallest MTU and therefore agree on 1470 bytes in this case.

So the laptop will never send packets with a larger MTU then 1470 when communicating with the desktop computer.

So far so good.

If you look at the link between the router at the top and the Internet you'll see that the link has a MTU of 1360 bytes. This is not a problem if the router is accepting to fragment packets and in this case that router needs to fragment every packet between the desktop computer and the laptop.

Not every router allow the use of fragmentation and some applications does not like fragmented packets. In these cases the communication will not work at all.

If the desktop computer were to be a Microsoft Exchange server and the laptop had an Outlook client, you would experience problem delivering mail with more contents then a few lines of text.

Web pages with graphics or much content would not load. You might get www.google.com up and running.

So how do we deal with this?

A lot of firewalls and routers automatically enters the session between systems and change the MTU to a setting that works. The administrator of these firewalls and routers usually decides what value that should be.

You can also set the MTU on the computers themselves, but this is a lot of administration and cumbersome if you have a lot of computers to manage.
So to force the MTU by some other means is the better solution. But what value should you use? How can you decide what is the best MTU?

You can use ping to determine the largest packet size to be used between two endpoints.

Technet24.ir

Using ping to troubleshoot MTU

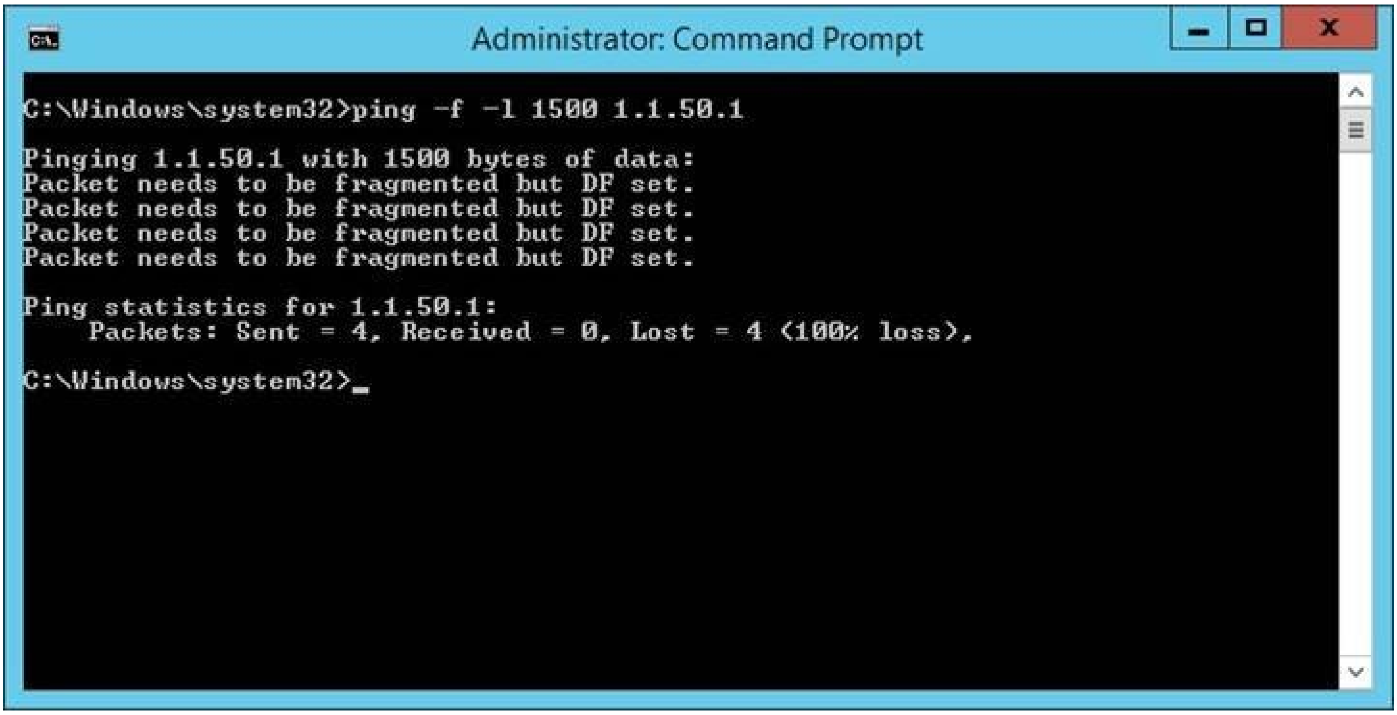
To determine the largest MTU you can use between two endpoints, Ping can be utilized with the correct set of parameters.

The first thing you need to do is login to one of the endpoints and start the command line.

Using the “don’t fragment” and –l size parameters you can determine what MTU is best.

Start off with a large number and work your way down to you find the correct value.

Look at the following screenshots:

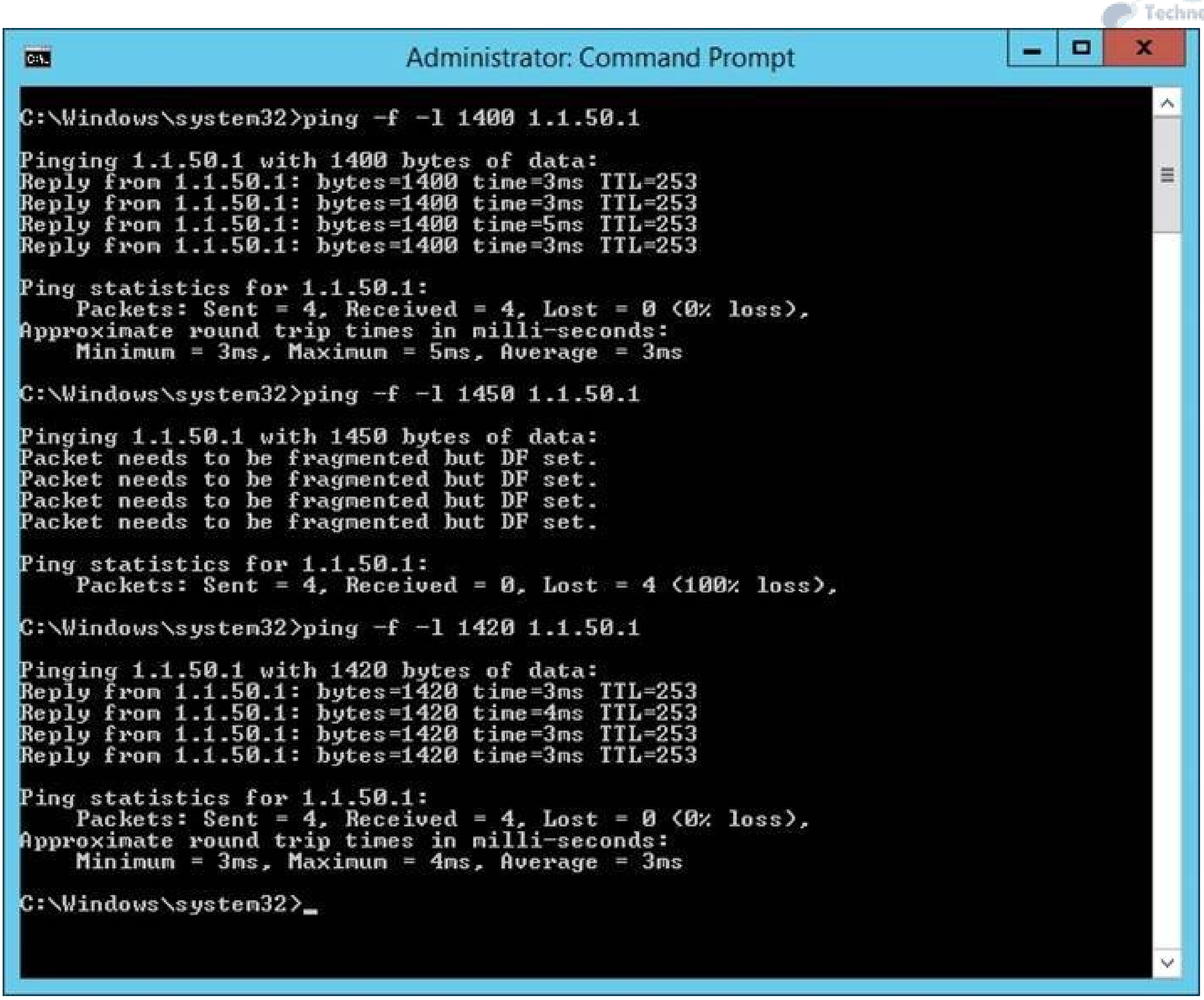


```
C:\Windows\system32>ping -f -l 1500 1.1.50.1

Pinging 1.1.50.1 with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 1.1.50.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>_
```

Figure 21: MTU Troubleshooting

In figure 21 I start off with a large MTU of 1500. This clearly is a problem, and Ping tells me that the packets needs to be fragmented to make this work.

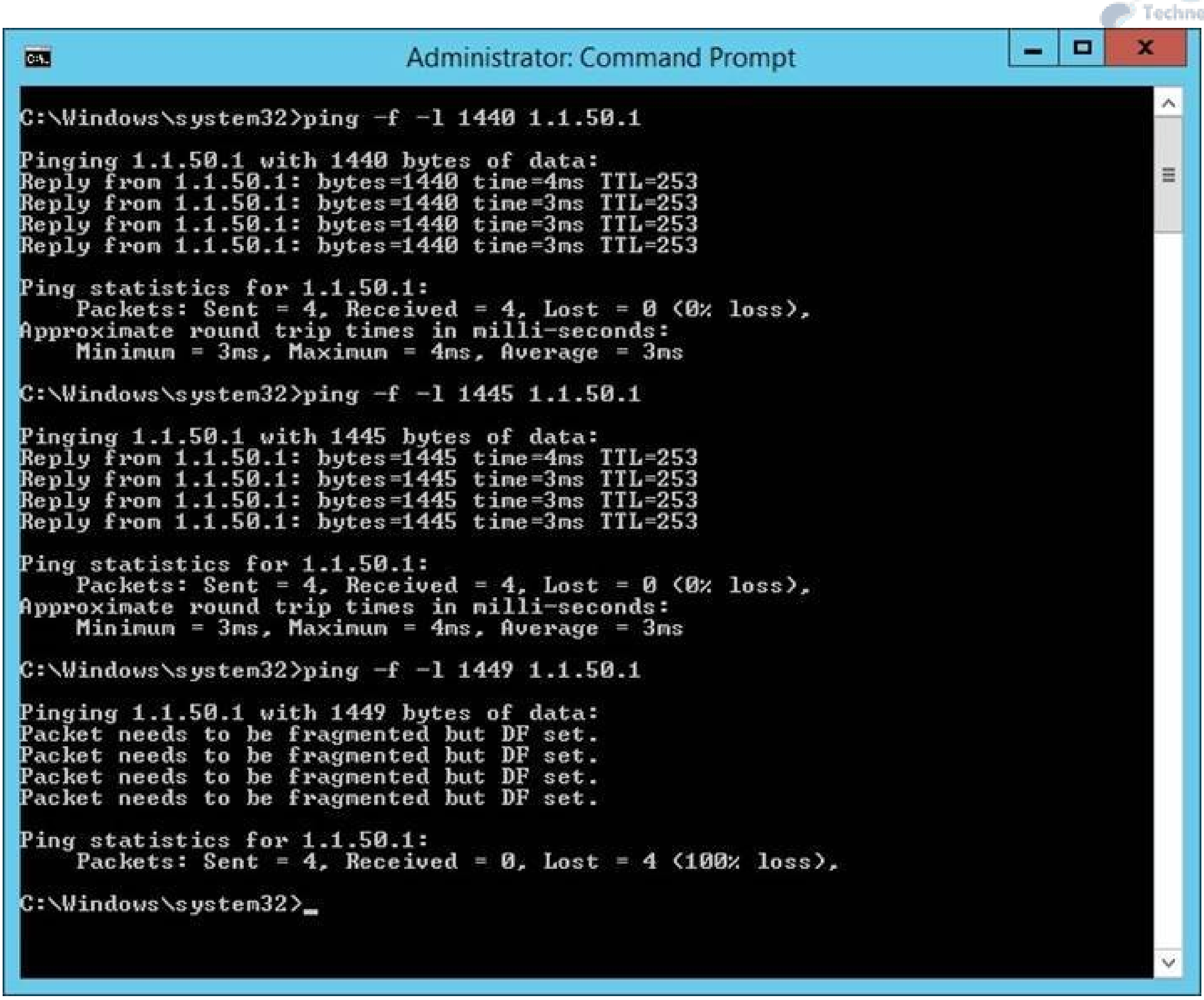
Technet24.ir



```
C:\Windows\system32>ping -f -l 1400 1.1.50.1

Pinging 1.1.50.1 with 1400 bytes of data:
Reply from 1.1.50.1: bytes=1400 time=3ms TTL=253
Reply from 1.1.50.1: bytes=1400 time=3ms TTL=253
Reply from 1.1.50.1: bytes=1400 time=5ms TTL=253
Reply from 1.1.50.1: bytes=1400 time=3ms TTL=253

Ping statistics for 1.1.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 5ms, Average = 3ms

C:\Windows\system32>ping -f -l 1450 1.1.50.1

Pinging 1.1.50.1 with 1450 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 1.1.50.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>ping -f -l 1420 1.1.50.1

Pinging 1.1.50.1 with 1420 bytes of data:
Reply from 1.1.50.1: bytes=1420 time=3ms TTL=253
Reply from 1.1.50.1: bytes=1420 time=4ms TTL=253
Reply from 1.1.50.1: bytes=1420 time=3ms TTL=253
Reply from 1.1.50.1: bytes=1420 time=3ms TTL=253

Ping statistics for 1.1.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\Windows\system32>_
```

Figure 22: MTU Troubleshooting

In figure 22 I first try out 1400 bytes, and that is no problem. I increase the value to 1450 and that is clearly too large. Then I try 1420 which is ok.

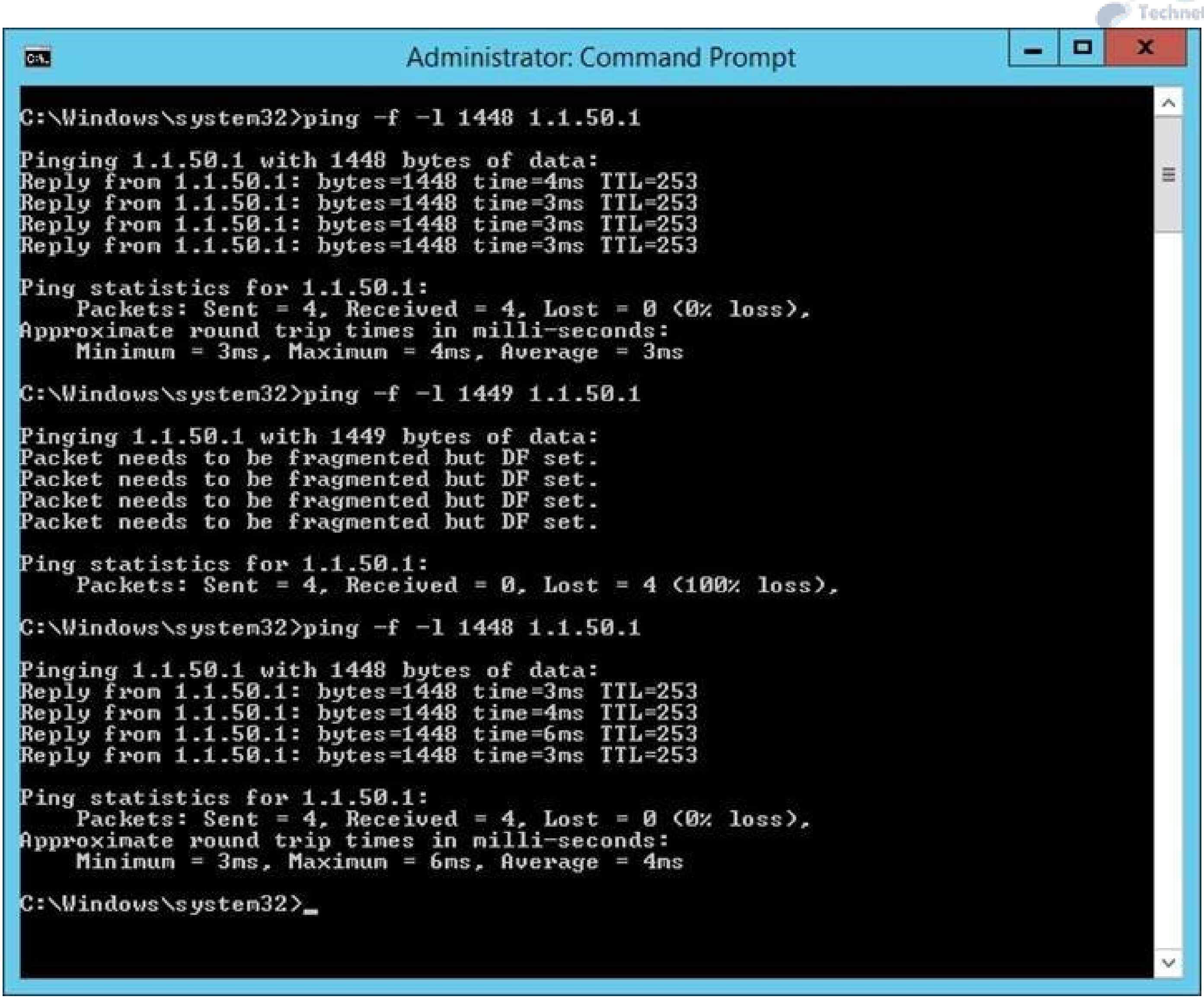


```
C:\Windows\system32>ping -f -l 1440 1.1.50.1

Pinging 1.1.50.1 with 1440 bytes of data:
Reply from 1.1.50.1: bytes=1440 time=4ms TTL=253
Reply from 1.1.50.1: bytes=1440 time=3ms TTL=253
Reply from 1.1.50.1: bytes=1440 time=3ms TTL=253
Reply from 1.1.50.1: bytes=1440 time=3ms TTL=253

Ping statistics for 1.1.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\Windows\system32>ping -f -l 1445 1.1.50.1

Pinging 1.1.50.1 with 1445 bytes of data:
Reply from 1.1.50.1: bytes=1445 time=4ms TTL=253
Reply from 1.1.50.1: bytes=1445 time=3ms TTL=253
Reply from 1.1.50.1: bytes=1445 time=3ms TTL=253
Reply from 1.1.50.1: bytes=1445 time=3ms TTL=253

Ping statistics for 1.1.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\Windows\system32>ping -f -l 1449 1.1.50.1

Pinging 1.1.50.1 with 1449 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 1.1.50.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>_
```

Figure 23: MTU Troubleshooting

In figure 23 I further close the gap between the values. Getting close.

Technet24.ir



```
C:\Windows\system32>ping -f -l 1448 1.1.50.1

Pinging 1.1.50.1 with 1448 bytes of data:
Reply from 1.1.50.1: bytes=1448 time=4ms TTL=253
Reply from 1.1.50.1: bytes=1448 time=3ms TTL=253
Reply from 1.1.50.1: bytes=1448 time=3ms TTL=253
Reply from 1.1.50.1: bytes=1448 time=3ms TTL=253

Ping statistics for 1.1.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\Windows\system32>ping -f -l 1449 1.1.50.1

Pinging 1.1.50.1 with 1449 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 1.1.50.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>ping -f -l 1448 1.1.50.1

Pinging 1.1.50.1 with 1448 bytes of data:
Reply from 1.1.50.1: bytes=1448 time=3ms TTL=253
Reply from 1.1.50.1: bytes=1448 time=4ms TTL=253
Reply from 1.1.50.1: bytes=1448 time=6ms TTL=253
Reply from 1.1.50.1: bytes=1448 time=3ms TTL=253

Ping statistics for 1.1.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 6ms, Average = 4ms

C:\Windows\system32>_
```

Figure 24: MTU Troubleshooting

Got it!

1449 bytes is too much, but 1448 bytes fits perfect.

So between these two systems a MTU size of 1448 will do without fragmentation.

To force this MTU I need to make the necessary change on the router or firewall between the two endpoints or I could choose to make the change on one of the endpoints directly.

So using Ping to determine maximum MTU size is pretty easy and straightforward.

Technet24.ir

Technet24.ir

Using Ping to monitor your network

Ping can be a great tool to get a quick status of your workplace or home network.

There are countless monitor systems. Some expansive, some cheap and some free.
But you do not really need a complicated or expansive system just to get an overview of how your network is doing.

With Ping you can get a quick status using your computer or even your mobile phone.

Technet24.ir

Using a ping batch file

Using a computer and no other applications at all you can create a batch file that quickly Pings every device you need to get a status on.

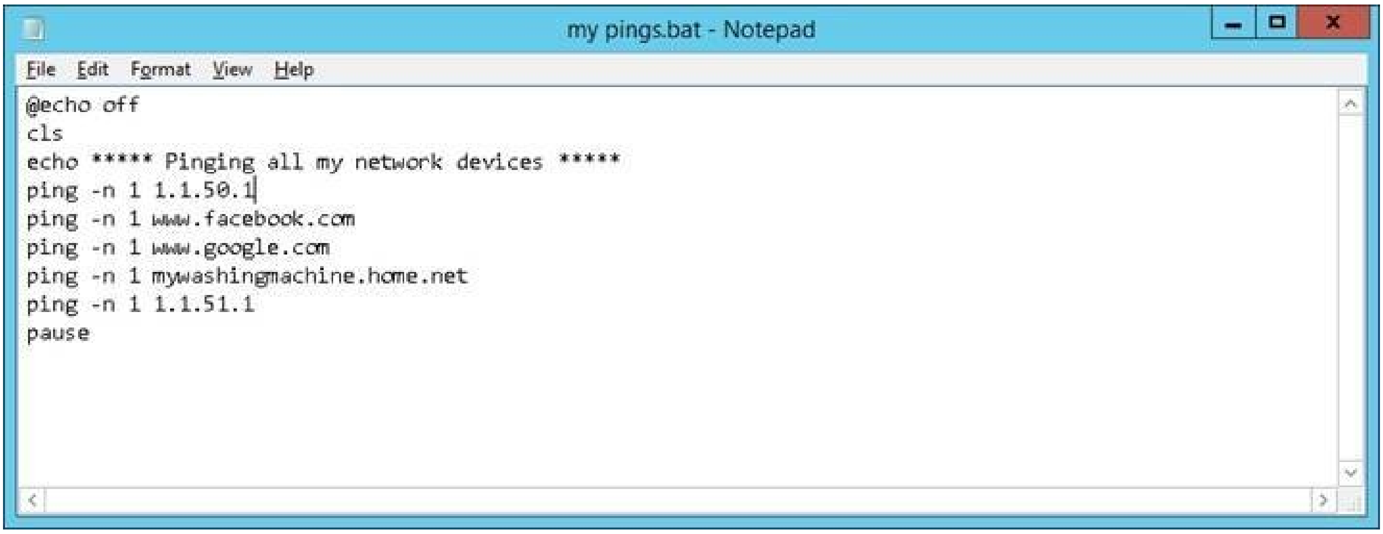
In the batch file you enter the commands like you would in the command line window, but you collect all the commands in a notepad text document.

When you are done you just save it as a batch file, keeping sure to use the .bat or .cmd file extension for the saved file.

When you need to run the batch file you just double click it or click it once with the right mouse button and choose run.

You can even put it on your desktop for easy and quick access.

Maybe you don’t need to send 4 Echo Request to every device?
Use the –n parameters to specify the number of requests you like to send. Fewer is quicker.

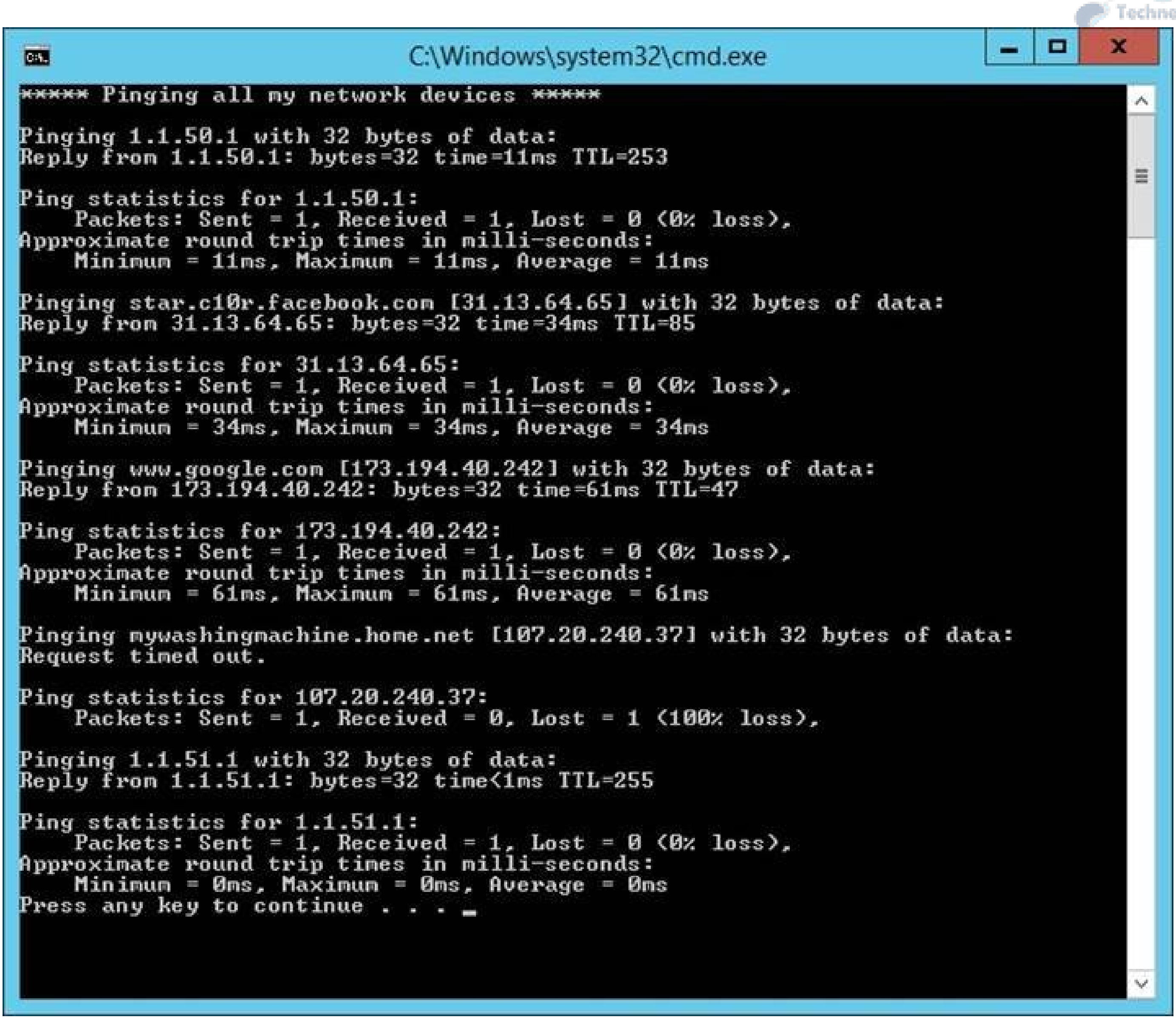


```
@echo off
cls
echo ***** Pinging all my network devices *****
ping -n 1 1.1.50.1
ping -n 1 www.facebook.com
ping -n 1 www.google.com
ping -n 1 mywashingmachine.home.net
ping -n 1 1.1.51.1
pause
```

Figure 25: Notepad file with Ping commands

The echo off suppresses unneeded output, and the cls command clear the screen before starting the ping process. The pause at the end makes sure you can read the output before the window is closed.

Running this batch file gives me the following output:



```
***** Pinging all my network devices *****

Pinging 1.1.50.1 with 32 bytes of data:
Reply from 1.1.50.1: bytes=32 time=11ms TTL=253

Ping statistics for 1.1.50.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 11ms, Average = 11ms

Pinging star.c10r.facebook.com [31.13.64.65] with 32 bytes of data:
Reply from 31.13.64.65: bytes=32 time=34ms TTL=85

Ping statistics for 31.13.64.65:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 34ms, Maximum = 34ms, Average = 34ms

Pinging www.google.com [173.194.40.242] with 32 bytes of data:
Reply from 173.194.40.242: bytes=32 time=61ms TTL=47

Ping statistics for 173.194.40.242:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 61ms, Maximum = 61ms, Average = 61ms

Pinging mywashingmachine.home.net [107.20.240.37] with 32 bytes of data:
Request timed out.

Ping statistics for 107.20.240.37:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Pinging 1.1.51.1 with 32 bytes of data:
Reply from 1.1.51.1: bytes=32 time<1ms TTL=255

Ping statistics for 1.1.51.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Press any key to continue . . . _
```

Figure 26: Batch file output

And there you go. Everything is up except for my washing machine.

Technet24.ir

Monitor from a computer or mobile smartphones

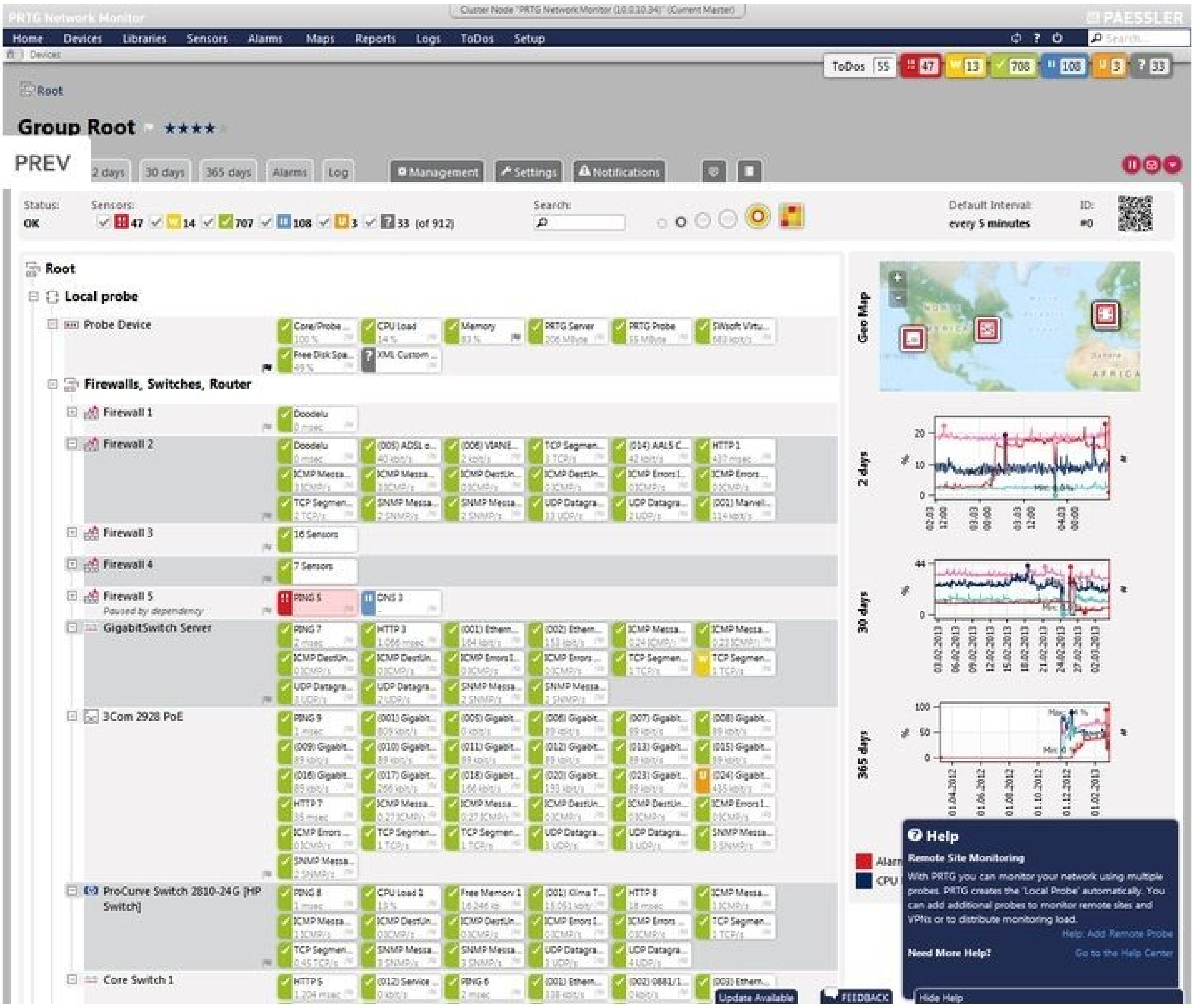
A batch file is quick and easy to setup. It is not that beautiful to look at and you might have to scroll up and down in the command window to get to all the information.

Luckily, there are quite a lot of free Ping monitoring tools that are easy to use. They look better too.

If you do a google search for Ping monitor tools I am sure you'll find something you like.

I would recommend PRTG free monitoring tools. They are free to monitor up to 10 devices.

http://www.paessler.com/tools


PRTG Network Monitor
PAESSLER
Home Devices Libraries Sensors Alarms Maps Reports Logs ToDos Setup
ToDos 55 47 13 708 108 3 33
Root
Group Root ★★★★
PREV
2 days 30 days 365 days Alarms Log Management Settings Notifications
Status: OK
Sensors: 47 14 707 108 3 33 (of 912)
Search:
Default Interval: every 5 minutes
ID: #0
Root
Local probe
Probe Device
Firewalls, Switches, Router
Firewall 1
Firewall 2
Firewall 3
Firewall 4
Firewall 5
Paused by dependency
GigabitSwitch Server
3Com 2928 PoE
ProCurve Switch 2810-24G [HP Switch]
Core Switch 1
Geo Map
2 days
30 days
365 days
Update Available
FEEDBACK
Hide Help

Help

Remote Site Monitoring

With PRTG you can monitor your network using multiple probes. PRTG creates the 'Local Probe' automatically. You can add additional probes to monitor remote sites and VPNs or to distribute monitoring load.

Help: Add Remote Probe

Need More Help? Go to the Help Center

Figure 27: PRTG network monitor

There's also PRTG tools for Android and iOS mobile phones.

Technet24.ir

PRTG is good for statistics as well. If you need to know if some devices or maybe a link is stable, this tool can give you statistics over time.

The software needs a little fiddle about before you get it the way you like, so if you are just looking for some easy tools, take a look at a few free tools I've created.

Technet24.ir

GUI Ping

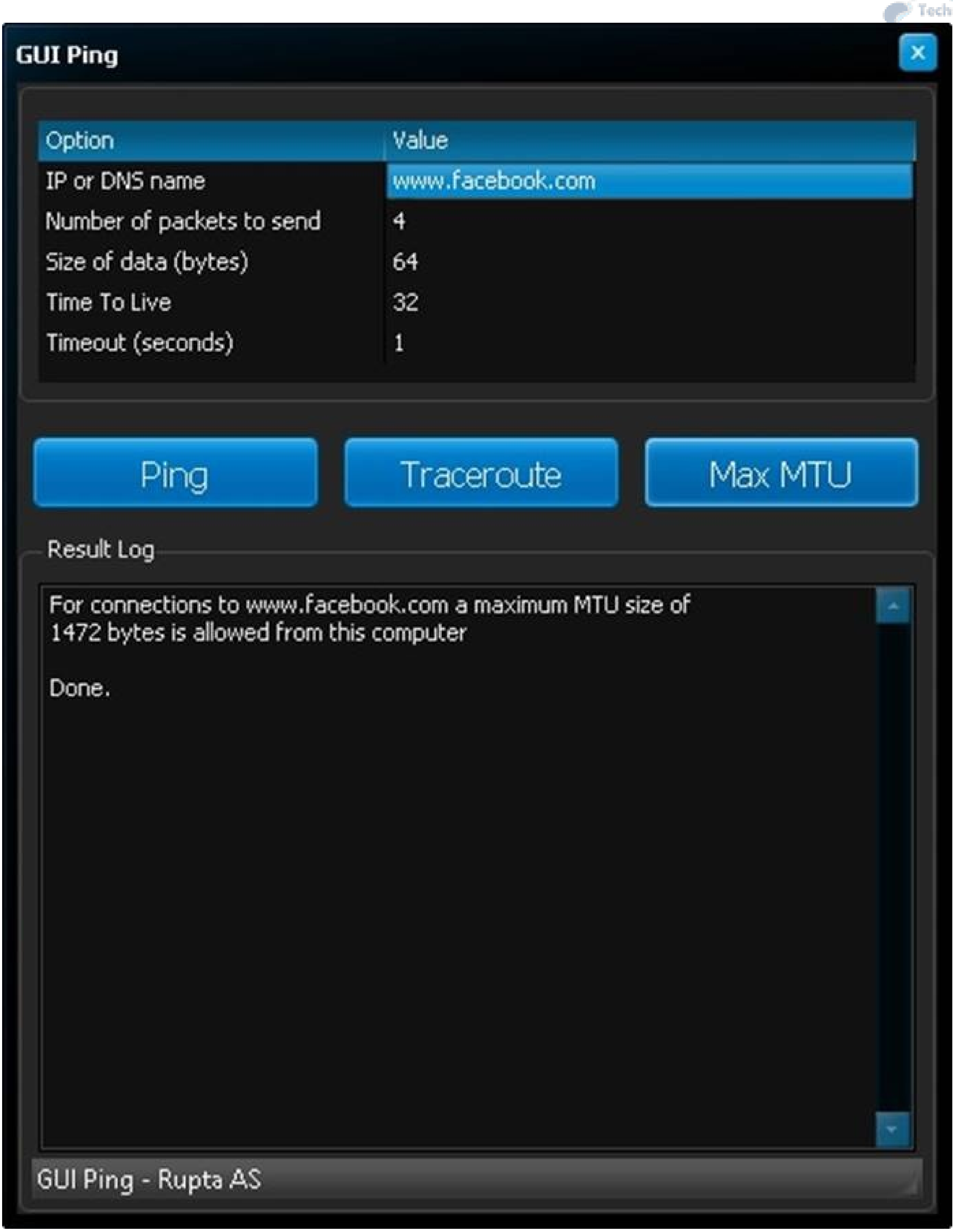
GUI Ping is a small Windows application (written in Delphi Pascal) to help you with 3 basic tasks:

PING A DEVICE FROM YOUR COMPUTER
TRACEROUTE A DEVICE FROM YOUR COMPUTER
FIND BIGGEST MTU SIZE YOU CAN USE TO A DEVICE FROM YOUR COMPUTER

This tool has no learning curve involved. It’s straightforward.

Click the button you need.

Technet24.ir



Option	Value
IP or DNS name	www.facebook.com
Number of packets to send	4
Size of data (bytes)	64
Time To Live	32
Timeout (seconds)	1

```
For connections to www.facebook.com a maximum MTU size of
1472 bytes is allowed from this computer

Done.
```

GUI Ping - Rupta AS

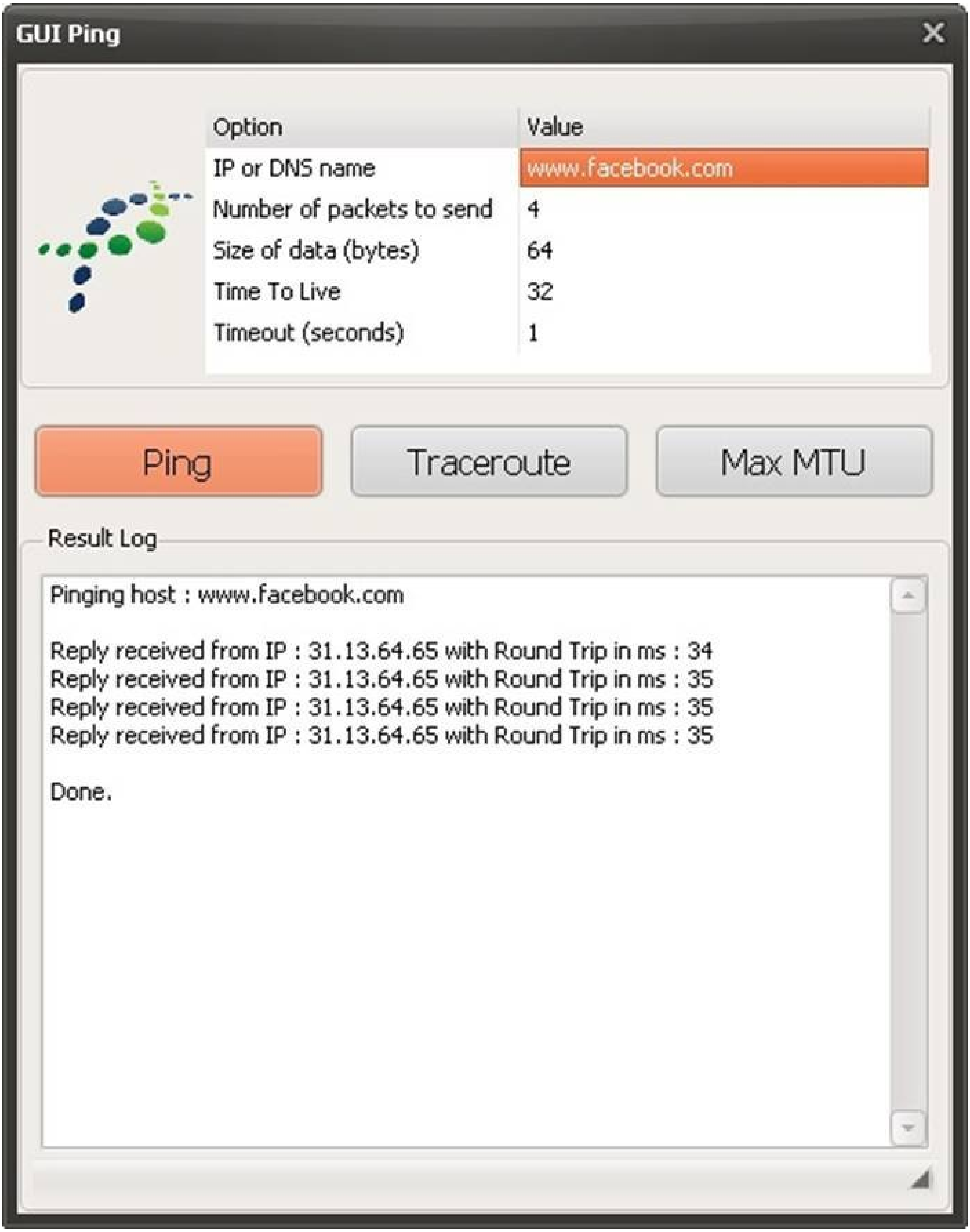
Figure 28: GUI Ping

Enter the device you need to work on in the top part of the window and you are good to go.

It defaults to www.facebook.com, but you can change it into anything you like.

Let’s give it a try.

Technet24.ir



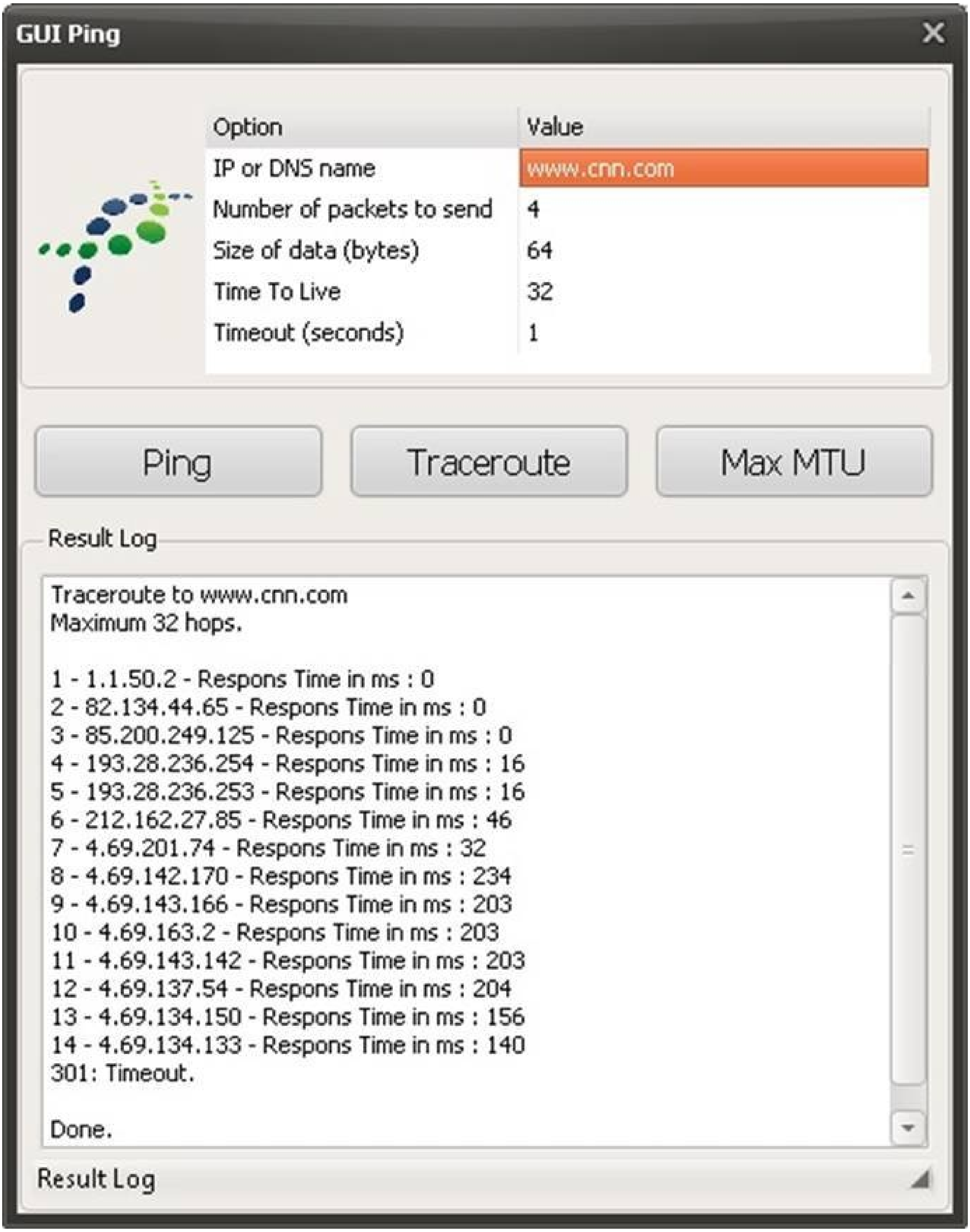
Option	Value
IP or DNS name	www.facebook.com
Number of packets to send	4
Size of data (bytes)	64
Time To Live	32
Timeout (seconds)	1

```
Pinging host : www.facebook.com

Reply received from IP : 31.13.64.65 with Round Trip in ms : 34
Reply received from IP : 31.13.64.65 with Round Trip in ms : 35
Reply received from IP : 31.13.64.65 with Round Trip in ms : 35
Reply received from IP : 31.13.64.65 with Round Trip in ms : 35

Done.
```

Figure 29: Pinging www.facebook.com (again)

A simple click at the Ping button and the program gives you instant response. Let’s try the Traceroute button:

Technet24.ir



Option	Value
IP or DNS name	www.cnn.com
Number of packets to send	4
Size of data (bytes)	64
Time To Live	32
Timeout (seconds)	1

Result Log

```
Traceroute to www.cnn.com
Maximum 32 hops.

1 - 1.1.50.2 - Respons Time in ms : 0
2 - 82.134.44.65 - Respons Time in ms : 0
3 - 85.200.249.125 - Respons Time in ms : 0
4 - 193.28.236.254 - Respons Time in ms : 16
5 - 193.28.236.253 - Respons Time in ms : 16
6 - 212.162.27.85 - Respons Time in ms : 46
7 - 4.69.201.74 - Respons Time in ms : 32
8 - 4.69.142.170 - Respons Time in ms : 234
9 - 4.69.143.166 - Respons Time in ms : 203
10 - 4.69.163.2 - Respons Time in ms : 203
11 - 4.69.143.142 - Respons Time in ms : 203
12 - 4.69.137.54 - Respons Time in ms : 204
13 - 4.69.134.150 - Respons Time in ms : 156
14 - 4.69.134.133 - Respons Time in ms : 140
301: Timeout.

Done.
```

Figure 30: GUI Ping - Traceroute

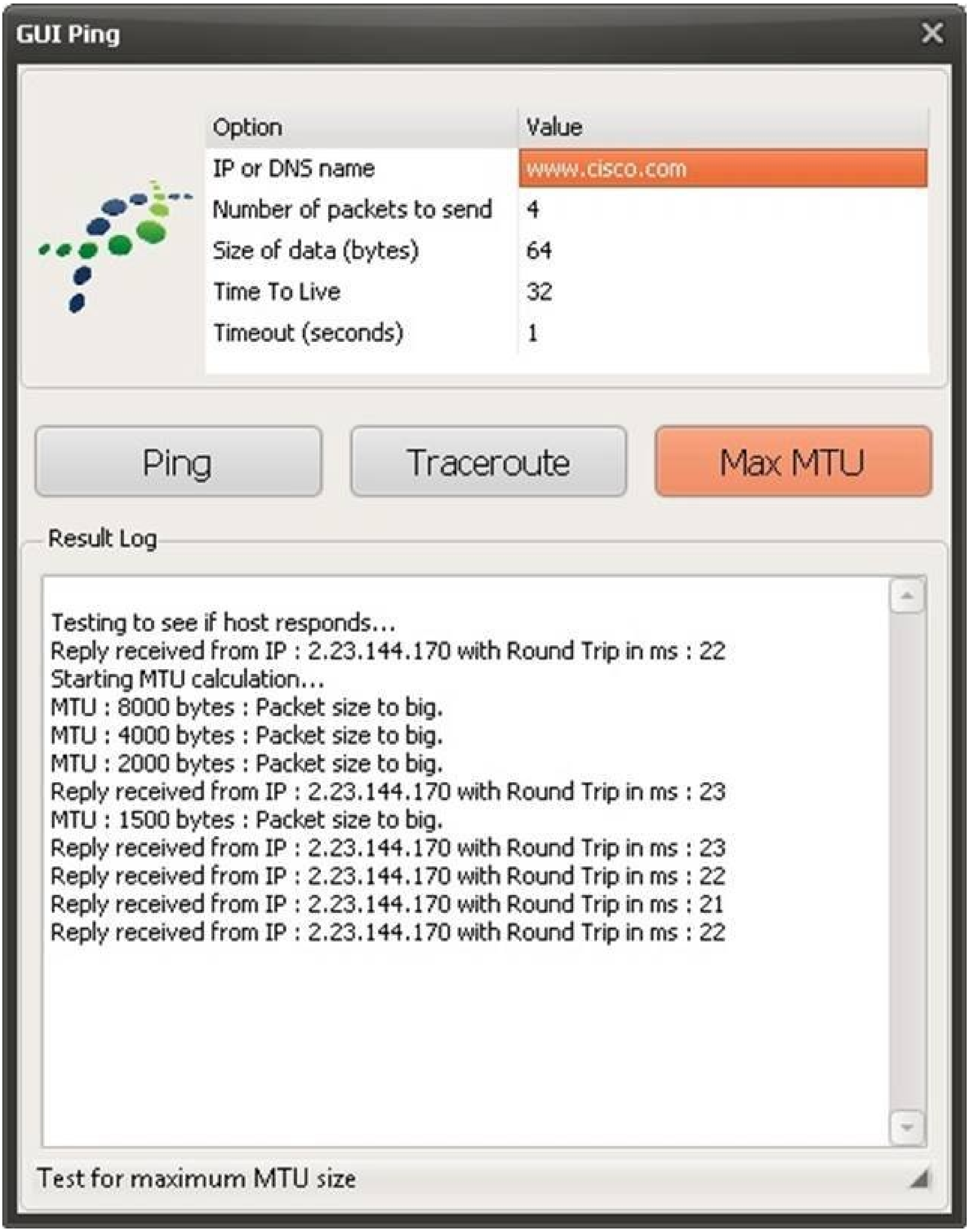
Works like a charm.

For the Max MTU function the software will do a series of Ping requests to determine the maximum MTU size. It will first of all check to see if the host you

Technet24.ir

are pinning out is actually answering Ping requests. If it does not, the function will not work.

When you click the Max MTU button the calculation will start.



Option	Value
IP or DNS name	www.cisco.com
Number of packets to send	4
Size of data (bytes)	64
Time To Live	32
Timeout (seconds)	1

```
Testing to see if host responds...
Reply received from IP : 2.23.144.170 with Round Trip in ms : 22
Starting MTU calculation...
MTU : 8000 bytes : Packet size to big.
MTU : 4000 bytes : Packet size to big.
MTU : 2000 bytes : Packet size to big.
Reply received from IP : 2.23.144.170 with Round Trip in ms : 23
MTU : 1500 bytes : Packet size to big.
Reply received from IP : 2.23.144.170 with Round Trip in ms : 23
Reply received from IP : 2.23.144.170 with Round Trip in ms : 22
Reply received from IP : 2.23.144.170 with Round Trip in ms : 21
Reply received from IP : 2.23.144.170 with Round Trip in ms : 22
```

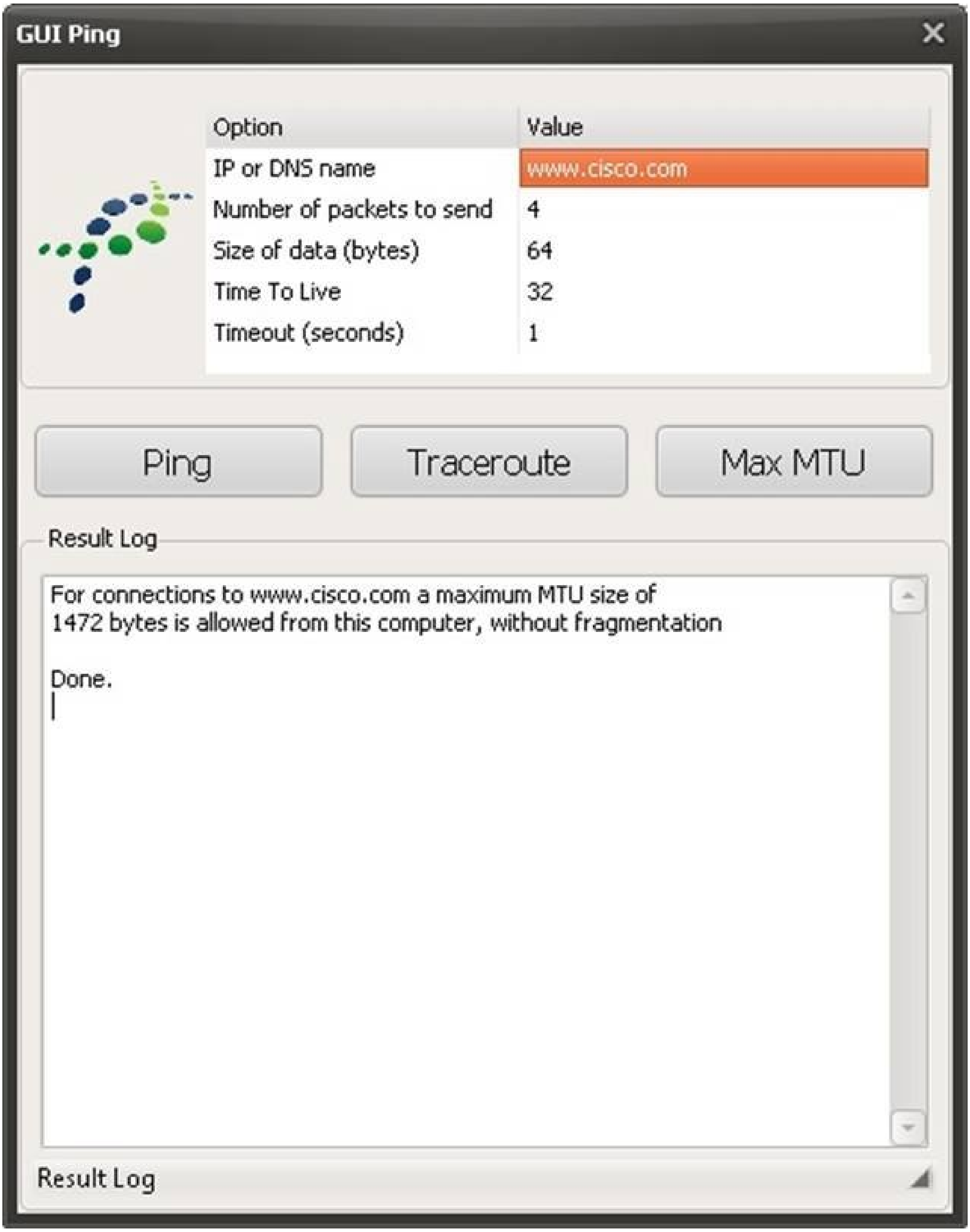
Test for maximum MTU size

Figure 31: GUI Ping – Max MTU

The calculation works by dividing the numbers in half for each try, ending up in the only number being the highest one. When it is finished calculating it will show the

Technet24.ir

final result:



Option	Value
IP or DNS name	www.cisco.com
Number of packets to send	4
Size of data (bytes)	64
Time To Live	32
Timeout (seconds)	1

```
For connections to www.cisco.com a maximum MTU size of
1472 bytes is allowed from this computer, without fragmentation

Done.
```

Figure 32: GUI Ping – Max MTU done.

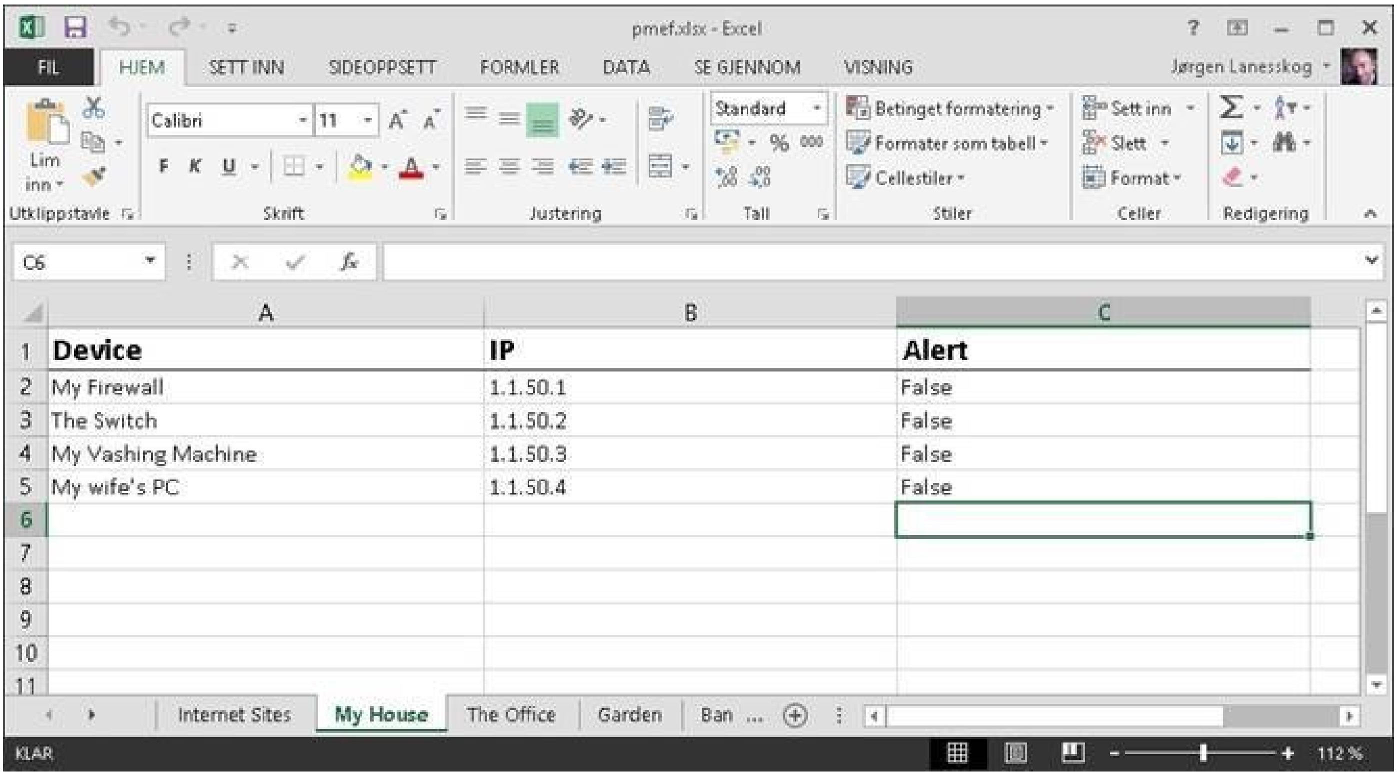
Technet24.ir

Ping My Excel File

I've created a simple Ping monitoring software that can monitor any device that answers to Ping requests.

All you have to do is enter all the devices you would like to monitor into a Microsoft Excel file. The file is already bundled with the application, but you'll need Microsoft Excel to edit the file.

When the application starts it will look for the Excel file and read it.



	A	B	C
1	**Device**	**IP**	**Alert**
2	My Firewall	1.1.50.1	False
3	The Switch	1.1.50.2	False
4	My Vashing Machine	1.1.50.3	False
5	My wife's PC	1.1.50.4	False
6			
7			
8			
9			
10			
11			

Figure 33: Ping My Excel File – Excel Pages

If you look at Figure 33 you'll notice how the devices a lined up underneath each other.

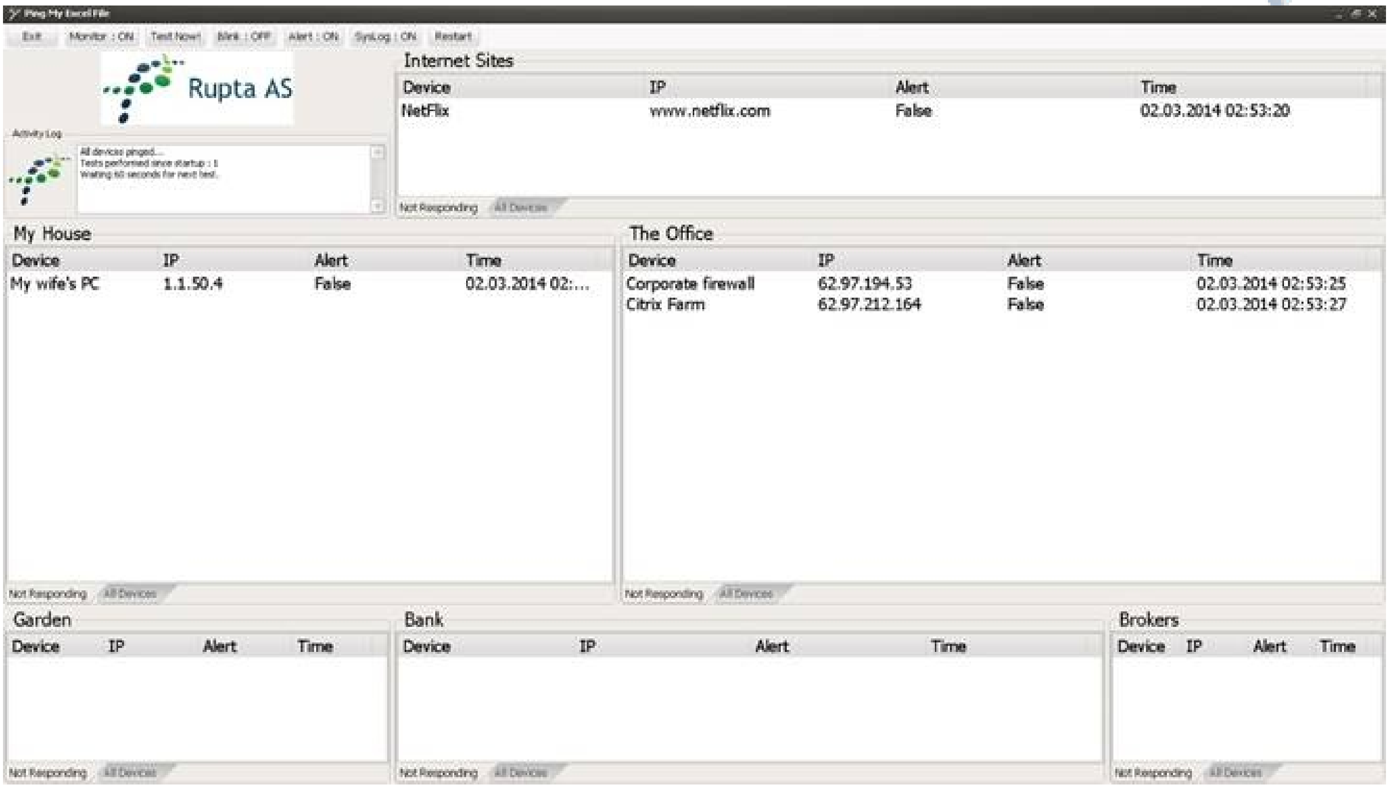
You can enter as many devices as you like.

The devices show here are in the My House Excel Sheet. There are a total of 5 device sheets and 1 settings sheets.

You can name the sheets any way you like. It will reflect in the application when you start it. The only thing to worry about is not changing the position of settings in the Settings sheet.

So fill the file with all the information you need and start the application to find the following easy Ping Monitoring tool:

Technet24.ir



Activity Log

```
All devices pinged...
Tests performed since startup : 1
Waiting 60 seconds for next test.
```

Internet Sites

Device	IP	Alert	Time
NetFlix	www.netflix.com	False	02.03.2014 02:53:20

My House

Device	IP	Alert	Time
My wife's PC	1.1.50.4	False	02.03.2014 02:...

The Office

Device	IP	Alert	Time
Corporate firewall	62.97.194.53	False	02.03.2014 02:53:25
Citrix Farm	62.97.212.164	False	02.03.2014 02:53:27

Garden

Device	IP	Alert	Time

Bank

Device	IP	Alert	Time

Brokers

Device	IP	Alert	Time

Figure 34: Ping My Excel File application

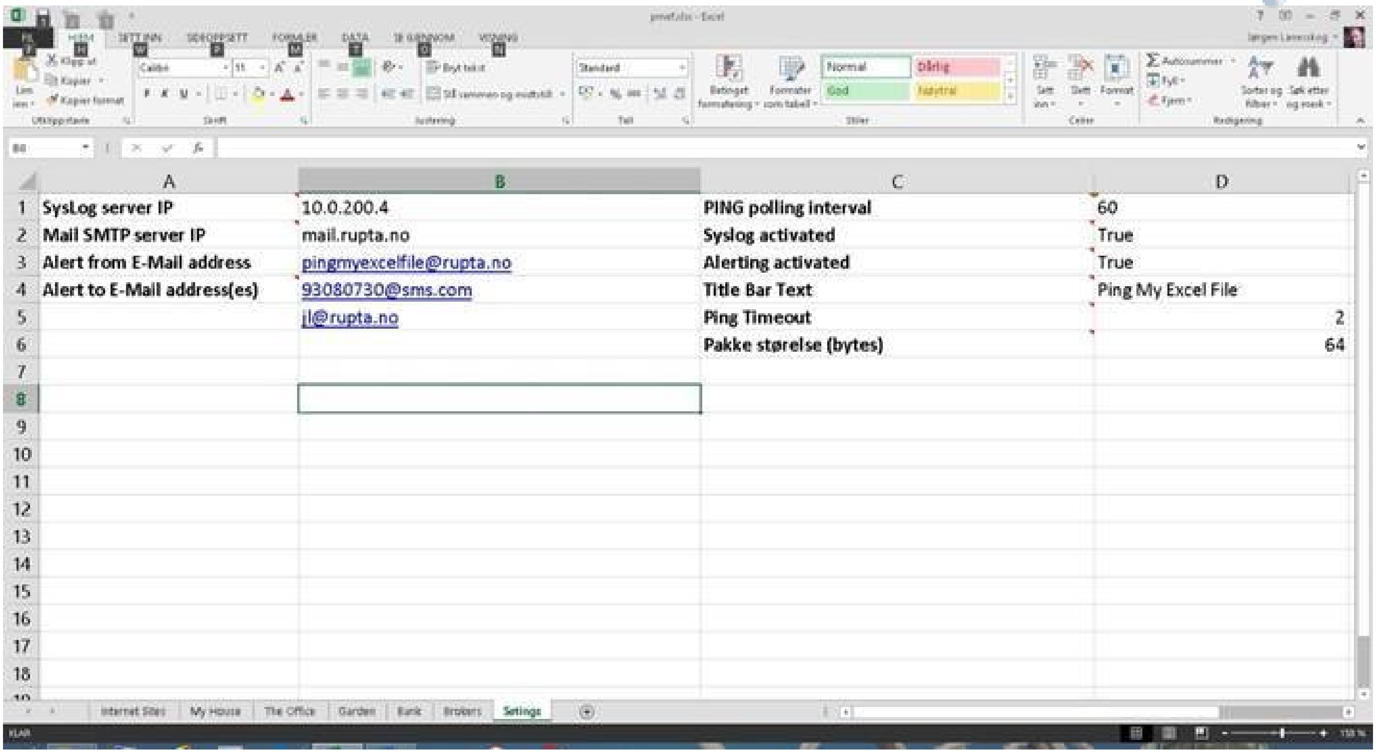
This as a great application to have running on a monitor somewhere on the wall.

The logo showing in the top left corner can be changed to anything you want, and the logo itself can be blinking when someone is not answering. If you like. There is a blink ON/OFF button.

You’ll notice that the names of the 5 areas in the application is reflecting the names of the sheets in the Excel file.

Also, the application will by default only show the devices not responding. If you need to look at all the devices, you should click the “All Devices” banner in the bottom of each area.

Technet24.ir



	A	B	C	D
1	SysLog server IP	10.0.200.4	PING polling interval	60
2	Mail SMTP server IP	mail.rupta.no	Syslog activated	True
3	Alert from E-Mail address	pingmyexcelfile@rupta.no	Alerting activated	True
4	Alert to E-Mail address(es)	93080730@sms.com	Title Bar Text	Ping My Excel File
5		jl@rupta.no	Ping Timeout	2
6			Pakke størelse (bytes)	64

Figure 35: Ping My Excel File Settings

A few settings to be aware of:

You can change the text in the Title bar of the application window in cell D4.

Ping timeout and size of packets to send (in bytes) can be entered in B5 and B6.

The polling interval is set to 60 seconds, but change it to the number you see fit. This is the amount of seconds between each running test of “are you alive” ping the application will send.

Alerting

If you need to be altered when things “go down” / are not responding, you can set this up right here in the Excel file.

There are 2 types of alerting available: e-mail and Syslog.

E-Mail can be great if you would like an E-Mail when something is wrong. You will also get an e-mail if and when the failing device come back online.

You need to set an outgoing mail server in the B2 cell. You can enter as many e-mail addresses as you like starting from cell B4 and down. The B3 cell (from e-mail address) is the address you would like to be the sender of the e-mail.

If you know Syslog and how it works, Ping My Excel File can send Syslog messages to a Syslog server. Just enter the IP address in cell B1.

To activate alerting, cell C2 and/or C3 needs to be “True”, with capitol T. If you

Technet24.ir

don’t want alerting you can enter whatever you like in those cells.

Also you need to enter True for every device you would like to be alerted about in the devices sheets.

Logo

If you need to change the Logo, just create a JPG file and place it in the application folder. It needs to be named logo.jpg.

Contact me

If you would like these free tools (GUI Ping and PMEF), just drop me an e-mail at jl@rupta.no and I’ll be happy to send them to you.

I’m in the process of setting up a site with lots of free tools and I promise I will make a few more Ping tools.

Good luck on your Ping journey!

Jorgen