

Operating Systems can be Detected Using Ping Command

Operating Systems can be detected using Ping Command, Ping is a computer network administration software utility, which used to find the Availability of a host on an Internet Protocol (IP) network.

Ping operates by sending Internet Control Message Protocol (ICMP) Echo Request packets to the target host and waiting for an ICMP Echo Reply.

TTL is simply meant, how long a resolver is supposed to cache the DNS query before the query expires and a new one needs to be done.

These TTL values differ between the Operating system.

The default initial TTL value for Linux/Unix is 64, and TTL value for Windows is 128.

Here you find TTL value for Range of servers.

Device / OS	Version	Protocol	TTL
AIX		TCP	60
AIX		UDP	30
AIX	3.2, 4.1	ICMP	255
BSDI	BSD/OS 3.1 and 4.0	ICMP	255
Compa	Tru64 v5.0	ICMP	64
Cisco		ICMP	254
DEC Pathworks	V5	TCP and UDP	30
Foundry		ICMP	64
FreeBSD	2.1R	TCP and UDP	64
FreeBSD	3.4, 4.0	ICMP	255
FreeBSD	5	ICMP	64
HP-UX	9.0x	TCP and UDP	30

HP-UX	10.01	TCP and UDP	64
HP-UX	10.2	ICMP	255
HP-UX	11	ICMP	255
HP-UX	11	TCP	64
Irix	5.3	TCP and UDP	60
Irix	6.x	TCP and UDP	60
Irix	6.5.3, 6.5.8	ICMP	255
juniper		ICMP	64
MPE/IX (HP)		ICMP	200
Linux	2.0.x kernel	ICMP	64
Linux	2.2.14 kernel	ICMP	255
Linux	2.4 kernel	ICMP	255
Linux	Red Hat 9	ICMP and TCP	64
MacOS/MacTCP	2.0.x	TCP and UDP	60
MacOS/MacTCP	X (10.5.6)	ICMP/TCP/UDP	64
NetBSD		ICMP	255
Netgear FVG318		ICMP and UDP	64
OpenBSD	2.6 & 2.7	ICMP	255
OpenVMS	07.01.2002	ICMP	255
OS/2	TCP/IP 3.0		64
OSF/1	V3.2A	TCP	60
OSF/1	V3.2A	UDP	30
Solaris	2.5.1, 2.6, 2.7, 2.8	ICMP	255
Solaris	2.8	TCP	64
Stratus	TCP_OS	ICMP	255
Stratus	TCP_OS (14.2-)	TCP and UDP	30
Stratus	TCP_OS (14.3+)	TCP and UDP	64
Stratus	STCP	ICMP/TCP/UDP	60
SunOS	4.1.3/4.1.4	TCP and UDP	60
SunOS	5.7	ICMP and TCP	255
Ultrix	V4.1/V4.2A	TCP	60
Ultrix	V4.1/V4.2A	UDP	30
Ultrix	V4.2 – 4.5	ICMP	255
VMS/Multinet		TCP and UDP	64
VMS/TCPware		TCP	60
VMS/TCPware		UDP	64
VMS/Wollongong	1.1.1.1	TCP	128
VMS/Wollongong	1.1.1.1	UDP	30
VMS/UCX		TCP and UDP	128
Windows	for Workgroups	TCP and UDP	32
Windows	95	TCP and UDP	32

Windows	98	ICMP	32
Windows	98, 98 SE	ICMP	128
Windows	98	TCP	128
Windows	NT 3.51	TCP and UDP	32
Windows	NT 4.0	TCP and UDP	128
Windows	NT 4.0 SP5-		32
Windows	NT 4.0 SP6+		128
Windows	NT 4 WRKS SP 3, SP 6a	ICMP	128
Windows	NT 4 Server SP4	ICMP	128
Windows	ME	ICMP	128
Windows	2000 pro	ICMP/TCP/UDP	128
Windows	2000 family	ICMP	128
Windows	Server 2003		128
Windows	XP	ICMP/TCP/UDP	128
Windows	Vista	ICMP/TCP/UDP	128
Windows	7	ICMP/TCP/UDP	128
Windows	Server 2008	ICMP/TCP/UDP	128
Windows	10	ICMP/TCP/UDP	128

Example how to detect OS

We should run the traceroute command first to determine the hops between the Target and the destination.

Tracert example.com (domain name)

```
Tracing route to example.com [93.65.122.99]
over a maximum of 30 hops:

 1  <1 ms    <1 ms    1 ms    10.108.50.1
 2  1 ms     1 ms     3 ms    182.74.23.21
 3  35 ms    35 ms    35 ms    182.79.245.66
 4  36 ms    36 ms    35 ms    116.51.27.225
 5  35 ms    35 ms    35 ms    ae-1.r20.sngpsi05.sg.bb.gin.ntt.net [129.250.3.146]
 6  205 ms   204 ms   206 ms   ae-8.r22.snjsca04.us.bb.gin.ntt.net [129.250.3.48]
 7  204 ms   204 ms   204 ms   ae-0.r23.snjsca04.us.bb.gin.ntt.net [129.250.2.183]
 8  218 ms   218 ms   218 ms   ae-0.incapsula.snjsca04.us.bb.gin.ntt.net [129.250.205.206]
 9  *        *        *        Request timed out.
10  *        *        *        Request timed out.
11  228 ms   228 ms   228 ms   s171.web-hosting.com [93.65.122.99]

Trace complete.
```

Total number of hops = 11

Now we need to Ping the Domain ping example.com (domain name)

```
Pinging (ping) example.com [60.65.122.99] with 32 bytes of data:  
Reply from 60.65.122.99: bytes=32 time=229ms TTL=53  
Reply from 60.65.122.99: bytes=32 time=229ms TTL=53  
Reply from 60.65.122.99: bytes=32 time=229ms TTL=53  
Reply from 60.65.122.99: bytes=32 time=229ms TTL=53  
  
Ping statistics for 60.65.122.99:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 229ms, Maximum = 229ms, Average = 229ms
```

TTL value is TTL=53, By making the Sum of TTL value and number of hops we can define the operating system (**53 + 11 = 64**), we can conclude that there is a Linux Machine Running.

This method may not be accurate all the time. However, it will give an idea of the underlying operating system in a remote system.