SYMMETRY™

Technical Bulletin

Microsoft PortQry Guide

DATE: **September 2016**

AUTHOR: **J.Lawrence**

REVISION: **1.0**

Contents

Introduction

This guide details how to use Microsoft's PortQry utility. This simple tool is used to establish whether a target system has specific ports open or not to aid with troubleshooting.

Downloading PortQry

Version 2 of PortQry can be downloaded free of charge from Microsoft's web site:

https://www.microsoft.com/en-us/download/details.aspx?id=17148

Version 1 of PortQry is for older Windows operating systems (Windows 2000-based computers).

This guide covers Version 2 which works on all of the latest operating systems (as of September 2016).

How PortQry Works

PortQry scans the port(s) specified on a target system and provides feedback on the port's status. This feedback is detailed as below:

Listening	PortQry has successfully received a response from the port specified in the query. A process such as an application or service is listening on this port and indicates the port is likely open.
Not Listening	PortQry has reached the target machine but a process such as an application or service is not listening on this port. This indicates the port is not in use but is not necessarily blocked.
Filtered	PortQry did not receive a response from the port. A process may or may not be listening on this port. This indicates the port is blocked and a firewall on the router/switch or target machine is managing access to this port.

Using PortQry

Run PortQry on a machine which is attempting to connect to the target using the port in question. PortQry can be used on any other machine on the network but it would need to cross the same network path to rule out filtering done by routers/switches.

PortQry can be opened in Command Prompt by going to:

Start | Run, type **CMD**, press OK

In Command Prompt, locate to the folder where PortQry is stored. For example, if in C:\PortQryV2\ type:

cd
cd c:\portqryv2

Type **portqry** to display the list of command options available as seen below:

```
c:\PortQryV2>portqry

PortQry version 2.0

Displays the state of TCP and UDP ports


Command line mode:  portqry -n name_to_query [-options]
Interactive mode:   portqry -i [-n name_to_query] [-options]
Local Mode:         portqry -local | -wpid pid| -wport port [-options]

Command line mode:

portqry -n name_to_query [-p protocol] [-e ¦¦ -r ¦¦ -o endpoint(s)] [-q]
        [-l logfile] [-sp source_port] [-sl] [-cn SNMP community name]

Command line mode options explained:
        -n [name_to_query] IP address or name of system to query
        -p [protocol] TCP or UDP or BOTH (default is TCP)
        -e [endpoint] single port to query (valid range: 1-65535)
        -r [end point range] range of ports to query (start:end)
        -o [end point order] range of ports to query in an order (x,y,z)
        -l [logfile] name of text log file to create
        -y overwrites existing text log file without prompting
        -sp [source port] initial source port to use for query
        -sl 'slow link delay' waits longer for UDP replies from remote systems
        -nr by-passes default IP address-to-name resolution
            ignored unless an IP address is specified after -n
        -cn specifies SNMP community name for query
            ignored unless querying an SNMP port
            must be delimited with !
        -q 'quiet' operation runs with no output
           returns 0 if port is listening
           returns 1 if port is not listening
           returns 2 if port is listening or filtered

Notes:  PortQry runs on Windows 2000 and later systems
        Defaults: TCP, port 80, no log file, slow link delay off
        Hit Ctrl-c to terminate prematurely

examples:
portqry -n myserver.com -e 25
portqry -n 10.0.0.1 -e 53 -p UDP -i
portqry -n host1.dev.reskit.com -r 21:445
portqry -n 10.0.0.1 -o 25,445,1024 -p both -sp 53
portqry -n host2 -cn !my community name! -e 161 -p udp
```

PortQry Commands

The following command will query the target IP address 192.168.1.1 and provide the status of TCP port 25:

portqry –n 192.168.1.1 –p tcp –e 25

-n IP or hostname of target
-p Type of port, i.e. TCP, UDP or BOTH
-e Port number, i.e. 25

```
c:\PortQryV2>portqry -n 192.168.1.1 -p tcp -e 25

Querying target system called:

 192.168.1.1

Attempting to resolve IP address to a name...

TCP port 25 (smtp service): FILTERED
```

From the results shown, the scan has detected the default service listening on port 25 but has come back with a FILTERED status indicating this port is likely blocked by a firewall system.

Additional feedback will be given if a PortQry is successful - depending on the port queried.