



Linux Ubuntu 26.04 Manual Pages on command 'wsdd.1'

\$ man wsdd.1

wsdd(1) General Commands Manual wsdd(1)

NAME

wsdd - A Web Service Discovery host and client daemon.

SYNOPSIS

wsdd [options]

DESCRIPTION

wsdd implements both a Web Service Discovery (WSD) host and a WSD client daemon. The host implementation enables (Samba) hosts, like your local NAS device, to be found by Web Service Discovery clients like Windows. The client mode allows searching for other WSD hosts on the local network.

The default mode of operation is the host mode. The client or discovery mode must be enabled explicitly. Unless configured otherwise, the host mode is always active. Both modes can be used at the same time.

OPTIONS

General options

-4, --ipv4only

See below.

-6, --ipv6only

Restrict to the given address family. If both options are specified no addresses will be available and wsdd will exit.

-A, --no-autostart

Do not start networking activities automatically when the program is started. The API interface (see below) can be used to start and stop the networking activities

while the application is running.

-c DIRECTORY, --chroot DIRECTORY

chroot into the given DIRECTORY after initialization has been performed and right before the handling of incoming messages starts. The new root directory can be empty. Consider using the -u option as well.

-h, --help

Show help and exit.

-H HOPLIMIT, --hoplimit HOPLIMIT

Set the hop limit for multicast packets. The default is 1 which should prevent packets from leaving the local network segment.

-i INTERFACE/ADDRESS, --interface INTERFACE/ADDRESS

Specify on which interfaces wsdd will be listening on. If no interfaces are specified, all interfaces are used. Loop-back interfaces are never used, even when explicitly specified. For interfaces with IPv6 addresses, only link-local addresses will be used for announcing the host on the network. This option can be provided multiple times in order to restrict traffic to more than one interface. This option also accepts IP addresses that the service should bind to. For IPv6, only link local addresses are actually considered as noted above.

--metadata-timeout TIMEOUT

Set the timeout for HTTP-based metadata exchange. Default is 2.0 seconds.

-s, --shortlog

Use a shorter logging format that only includes the level and message. This is useful in cases where the logging mechanism, like systemd on Linux, automatically prepends a date and process name plus ID to the log message.

-u USER[:GROUP], --user USER[:GROUP]

Change user (and group) when running before handling network packets. Together with -c this option can be used to increase security if the execution environment, like the init system, cannot ensure this in another way.

-U UUID, --uuid UUID

The WSD specification requires a device to have a unique address that is stable across reboots or changes in networks. In the context of the standard, it is assumed that this is something like a serial number. Wsdd attempts to read the machine ID from /etc/machine-id and /etc/hostid (in that order) before potentially chrooting in

another environment. If reading the machine ID fails, wsdd falls back to a version 5 UUID with the DNS namespace and the host name of the local machine as inputs. Thus, the host name should be stable and not be modified, e.g. by DHCP. However, if you want wsdd to use a specific UUID you can use this option.

-v, --verbose

Additively increase verbosity of the log output. A single occurrence of **-v/--verbose** sets the log level to INFO. More **-v** options set the log level to DEBUG.

-V, --version

Show the version number and exit.

Host Mode Options

-d DOMAIN, --domain DOMAIN

Assume that the host running wsdd joined an ADS domain. This will make wsdd report the host being a domain member. It disables workgroup membership reporting. The (provided) hostname is automatically converted to lower case. Use the **-p** option to change this behavior.

-n HOSTNAME, --hostname HOSTNAME

Override the host name wsdd uses during discovery. By default the machine's host name is used (look at `hostname(1)`). Only the host name part of a possible FQDN will be used in the default case.

-o, --no-host

Disable host operation mode. If this option is provided, the host cannot be discovered by other (Windows) hosts. It can be useful when client/discovery mode is used and no announcement of the host that runs wsdd should be made.

-p, --preserve-case

Preserve the hostname as it is. Without this option, the hostname is converted as follows. For workgroup environments (see **-w**) the hostname is made upper case by default. Vice versa it is made lower case for usage in domains (see **-d**).

-t, --no-http

Do not service HTTP requests of the WSD protocol. This option is intended for debugging purposes where another process may handle the Get messages.

-w WORKGROUP, --workgroup WORKGROUP

By default wsdd reports the host is a member of a workgroup rather than a domain (use the **-d/--domain** option to override this). With **-w/--workgroup** the default workgroup

name can be changed. The default work group name is WORKGROUP. The (provided) host? name is automatically converted to upper case. Use the `-p`` option to change this behavior.

Client/Discovery Mode Options

`-D, --discovery`

Enable discovery mode to search for other WSD hosts/servers. Found hosts are logged with INFO priority. The server interface (see below) can be used for a programatic interface. Refer to the man page for details of the server interface.

`-l PATH/PORT, --listen PATH/PORT`

Specify the location of the socket for the server programming interface. If the option value is numeric, it is interpreted as numeric port for a TCP server port. Then, the server socket is bound to the localhost only. If the option value is non-numeric, it is assumed to be a path to UNIX domain socket to which a client can connect to.

EXAMPLE USAGE

Handle traffic on eth0 and eth2 only, but only with IPv6 addresses

```
wsdd -i eth0 -i eth2 -6
```

or

```
wsdd --interface eth0 --interface eth2 --ipv6only
```

Set the Workgroup according to smb.conf, be verbose, run with dropped privileges, and change the root directory to an (empty) directory

```
SMB_GROUP=$(grep -i '^s*workgroup\s*=' smb.conf | cut -f2 -d= | tr -d '[:blank:]')
```

```
wsdd -v -w $SMB_GROUP -u daemon:daemon -c /var/run/wsdd/chroot
```

FIREWALL SETUP

Traffic for the following ports, directions and addresses must be allowed:

- Incoming and outgoing traffic to udp/3702 with multicast destination: 239.255.255.250 for IPv4 and ff02::c for IPv6
- Outgoing unicast traffic from udp/3702
- Incoming traffic to tcp/5357

You should further restrict the traffic to the (link-)local subnet, e.g. by using the ``fe80::/10`` address space for IPv6. Please note that IGMP traffic must be enabled in order to get IPv4 multicast traffic working.

API INTERFACE

Wsdd provides a text-based, line-oriented API interface to query information and trigger actions. The interface can be used with TCP and UNIX domain sockets (see `-l/--listen` option).

The TCP socket is bound to the local host only. The following commands can be issued:

`clear` - Clear list of discovered devices

Clears the list of all discovered devices. Use the `probe` command to search for devices again. This command does not return any data and is only available in discover mode.

`list [TYPE]` - List discovered devices

Returns a tab-separated list of discovered devices of the provided TYPE (e.g. "pub:Computer") with the following information. If no type is provided, all discovered devices are listed. The possibly empty list of detected hosts is always terminated with a single dot (".") in an otherwise empty line. This command is only available in discover mode.

UUID UUID of the discovered device. Note that a multi-homed device should appear only once but with multiple addresses (see below)

name The name reported by the device. For discovered Windows hosts, it is the configured computer name that is reported here.

association

Specifies the domain or workgroup to which the discovered host belongs to. The type of the association (workgroup or domain) is separated from its value by a colon.

last_seen

The date and time the device was last seen as a consequence of Probe/Hello messages provided in ISO8601 with seconds.

addresses

List of all transport addresses that were collected during the discovery process delimited by commas. Addresses are provided along with the interface (separated by "%") on which they were discovered. IPv6 addresses are reported on square brackets. Note that the reported addresses may not match the actual device on which the device may be reached.

types Types of the detected device, delimited by commas.

`probe [INTERFACE]` - Search for devices

Triggers a Probe message on the provided INTERFACE (eth0, e.g.) to search for WSD hosts. If no interface is provided, all interfaces wsdd listens on are probed. A Probe message initiates the discovery message flow. It may take some time for hosts to be actually discovered. This command does not return any data and is only available in discovery mode.

start - Start networking activities

This command starts the networking activities of wsdd if they haven't been started yet.

"Hello" messages are emitted and the host is announced on the network(s) when the host mode is active. If the discovery mode is enabled a probe process is also started.

stop - Stop networking activities

This is the reverse operation to start. When this command is received, "Bye" messages are sent in order to notify hosts in the network about the host's disappearance. All networking sockets used for the WSD protocol are closed as well. Activities can be restarted with the start operation.

SECURITY

wsdd does not implement any security feature, e.g. by using TLS for the http service. This is because wsdd's intended usage is within private, i.e. home, LANs. The Hello message contains the host's transport address, i.e. the IP address which speeds up discovery (avoids Resolve message).

KNOWN ISSUES

Using only IPv6 on FreeBSD

If wsdd is running on FreeBSD using IPv6 only, the host running wsdd may not be reliably discovered. The reason appears to be that Windows is not always able to connect to the HTTP service for unknown reasons. As a workaround, run wsdd with IPv4 only.

Tunnel/Bridge Interface

If tunnel/bridge interfaces like those created by OpenVPN or Docker exist, they may interfere with wsdd if executed without providing an interface that it should bind to (so it binds to all). In such cases, the wsdd host appears after wsdd has been started but it disappears when an update of the Network view in Windows Explorer is forced, either by refreshing the view or by a reboot of the Windows machine. To solve this issue, the interface that is connected to the network on which the host should be announced needs to be specified with the `-i/--interface` option. This prevents the usage of the tunnel/bridge interfaces.

Background: Tunnel/bridge interfaces may cause Resolve requests from Windows hosts to be delivered to wsdd multiple times, i.e. duplicates of such request are created. If wsdd receives such a request first from a tunnel/bridge it uses the transport address (IP address) of that interface and sends the response via unicast. Further duplicates are not processed due to the duplicate message detection which is based on message UUIDs. The Windows host which receives the response appears to detect a mismatch between the transport address in

the ResolveMatch message (which is the tunnel/bridge address) and the IP of the sending host/interface (LAN IP, e.g.). Subsequently, the wsdd host is ignored by Windows.

wsdd(1)