What is Ident?

Ident originates from UNIX machines, where it is used to discover the account name that the user logged in with. It's principal advantage for IRC users is that a properly set ident will make it harder for you to be 'blamed' for the actions of other users. This is particularly important for those who connect via shell acounts, bouncers or similar multi-user gateways - such machines will normally have an ident server which is maintained by the system administrator. DALnet server send an ident query to the IP address of any client as part of the initial connection sequence, if no response is received a tilde (~) is inserted into the user's address immediatly after the exclamation mark (nick!~user@some.isp.com). Full details of the ident protocol can be found in RFC9??

identd allows the interactive user to be identified bysuch applications as the **squid** proxy which will call the ident service to identify the source of the request and allow it not.

Isn't Ident insecure?

Some Sysadmins believe ident is insecure. It does give out valid usernames, however if you have a reasonably secure system with a properly defined security policy this is a minor risk. Ident itself does not pose a security risk to the system which runs it providing the version being run is current. As with all software, it should be updated if and when necessary. Truly paranoid sysadmins may wish to investigate fakeidentd (see Unix Ident on the menu) which allows you to mask valid usernames while still returning working ident responses.

How Ident Works

The Ident Protocol is designed to work as a server daemon, on a user's computer, where it receives requests to a specified port, generally 113. The server will then send a specially designed response that identifies the username of the current user.

Usefulness of Ident

Ident is considered useful due to the fact that it is able to distinguish the name of the person most likely to make a connection to the requesting server, which can then be used as identification for abuse control and/or general reporting purposes. This is useful because on most operating systemsmore than one user can be logged in at a time. The

protocol is of no help for users where the source of abuse is the computer administrator. To some extent the trustworthiness of the ident can be determined by seeing if the reverse DNS hostname is a typical ISP host (e.g. user12345.dsl.myisp.com) or a hostname more likely to be of a server.

Security

Filtering the ident port will often cause timeout delays when connecting to servers. Unless you are determined to leave your system totally invisible to the Internet it is best to either run an ident server or to leave the port cleanly rejecting connections using a firewall. It is possible to set up your system to filter ident connections from all systems you haven't made a connection to recently but this can be tricky to set up and few people bother.

The ident protocol is considered dangerous because it allows hackers to gain a list of usernames on a computer system which can later be used for attacks. A generally accepted solution to this is to setup a generic/generated identifier, returning node/ hop Ids or Kerberos tickets, rather than usernames.

On Unix-like systems the identd service is generally either started from inetd/tcpd, xinetd or itself linked against libwrap, allowing TCP Wrapper filter rules to be set on some hosts (or entire subnets):

/etc/hosts.allow

identd, authd:. intranet.lan, mail.isp.tld,.isp.tld, irc.isp.tld ftp.isp.tld

On denied requests the default timeout is 5 seconds. However since it is the 'protected' machine waiting to become a client to some other service, most probably, one wants to disable this timeout. Using something similar to the following:

/etc/hosts.deny

identd, authd: ALL: twist(/bin/true &)

Uses

Ident is important on IRC as a large number of people connect to IRC servers via bouncers which either serve multiple users or are hosted on shared servers. Some users also use clients on Unix shells. Without ident there would be no way to ban a single user of a bouncer from a channel or network without banning the entire bouncer. It's also needed when complaining to the bouncer operator so they can identify which user is causing trouble. When an IRC server fails to get an identd response it has to fall back on the username given by the client. Ircds usually prefix usernames obtained directly from the client software with ~ (tilde) to indicate that they are not ident usernames and may be

faked by the user (although with modern single-user home computers, the ident username itself may be set to whatever the user wants and is often returned by the same IRC client as the rest of the client information). Some IRC servers even go so far as blocking clients without an ident response, the main reason being that it makes it much harder to connect via an “open proxy” " or a system where you have compromised a single account of some form but do not have root.

Special identds are used by those running large numbers of bouncers or a single bouncer that supports multiple users to allow bouncer usernames to be returned rather than simply the name of the user account on the system the bouncer is running under. The best known of these is probably oidentd and Windows Ident Server.

IDENTD :

This is a freeware (GPL) ident server for windows 95. 98 & NT. It may also work on Windows 2000 and ME however this has not been tested and cannot be guaranteed. Full instructions are included in the download package. Requires winzip to extract the files. *Please note that this Ident Daemon is now unsupported by it's authors. If possible you should use one of the currently supported packages referenced below.*

Stand-Alone Windows Ident Servers.

http://info.ost.eltele.no/freeware/identd/ (Windows NT)

http://identd.sourceforge.net/ (Windows 9x)

These packages are currently supported by their respective authors and are both provided as freeware.

identd for NT,W2000,XP

1.0.0.1

Author: Bernard Bou, the service was rewritten from scratch, the old version was designed by Pål Baltzersen and implemented by Lars Erik Håland and resorting toreading a value in the registry. Once the session closed, the same key was returned. The present service calls a COM object that executes in the context of the interactive user and returns his/her name. The idea was Keith Brown's. The implementation is mine.

Web: http://identd.sourceforge.net/ GPL

~~~~~~
~~~~~~

identd for W9x

1.1.0

Author: Robie Basak   Web: http://identd.sourceforge.net/ GPL

~~~~~~
~~~~~~~~~~~~~~~~

identc

1.0.1.0.

Author: Bernard Bou Web: ftp://ftp.ac-toulouse.fr/pub/outils/bbou/ident GPL

~~~~~~
~~~~~~~~~~~~~~~~