IPwatchD 1.2.1 Test Scenarios

Table of Contents

1 Interface configuration mode

1.1 Automatic interface configuration

Configuration:	iface_configuration automatic defend_interval 10 user_script /usr/sbin/ipwatchd-script syslog_facility daemon
Actions:	/usr/sbin/ipwatchd -d -c /etc/ipwatchd.conf && \ sleep 1 && \ killall ipwatchd
Expected result:	IPwatchD must find all interfaces and syslog their names.
Syslog output:	ipwatchd[1203]: Skipping loopback device "lo" ipwatchd[1203]: Found device eth1 ipwatchd[1203]: Found device eth0 ipwatchd[1203]: Daemon can be executed because PID file /var/run/ipwatchd.pid does not exist ipwatchd[1205]: IPwatchD started ipwatchd[1205]: Entering pcap loop ipwatchd[1205]: Received signal 15 ipwatchd[1205]: IPwatchD stopped

1.2 Manual interface configuration

Configuration:	iface_configuration manual iface eth0 passive defend_interval 10 user_script /usr/sbin/ipwatchd-script syslog_facility daemon
Actions:	/usr/sbin/ipwatchd -d -c /etc/ipwatchd.conf && \ sleep 1 && \ killall ipwatchd
Expected result:	IPwatchD must find only interfaces specified in configuration and syslog their names.
Syslog output:	ipwatchd[1348]: Found interface eth0 ipwatchd[1348]: Daemon can be executed because process specified in PID file /var/run/ipwatchd.pid does not exist ipwatchd[1350]: IPwatchD started ipwatchd[1350]: Entering pcap loop ipwatchd[1350]: Received signal 15 ipwatchd[1350]: IPwatchD stopped

1.3 Manual interface configuration with non-existing device

Configuration:	iface_configuration manual iface eth0 passive iface non0 passive defend_interval 10 user_script /usr/sbin/ipwatchd-script syslog_facility daemon
Actions:	/usr/sbin/ipwatchd -d -c /etc/ipwatchd.conf
Expected result:	IPwatchD cannot start.
Syslog output:	ipwatchd[3085]: Found device eth0 ipwatchd[3085]: IPwatchD is unable to work with device "non0" ipwatchd[3085]: Unable to read configuration file

1.4 Manual interface configuration with no devices specified

Configuration:	iface_configuration manual defend_interval 10 user_script /usr/sbin/ipwatchd-script syslog_facility daemon
Actions:	/usr/sbin/ipwatchd -d -c /etc/ipwatchd.conf
Expected result:	IPwatchD cannot start.
Syslog output:	ipwatchd[3195]: No interfaces specified in configuration file ipwatchd[3195]: Unable to read configuration file

2 Defend interval

2.1 Defend interval with value 0

Configuration:	iface_configuration manual iface eth0 passive defend_interval 0 user_script /usr/sbin/ipwatchd-script syslog_facility daemon
Actions:	/usr/sbin/ipwatchd -t -d -c /etc/ipwatchd.conf && \ sleep 1 && \ arping -U -c 1 -I eth1 10.20.30.2 && \ sleep 1 && \ arping -U -c 1 -I eth1 10.20.30.2 && \ sleep 1 && \ killall ipwatchd
Expected result:	At least two conflicts must be detected and user-defined script must be executed for each conflict.
Syslog output:	ipwatchd[2065]: Found interface eth0 ipwatchd[2065]: Daemon can be executed because process specified in PID file /var/run/ipwatchd.pid does not exist ipwatchd[2066]: IPwatchD started ipwatchd[2066]: Entering pcap loop ipwatchd[2066]: Received ARP packet: S:10.20.30.2-0:d:87:fc:7c:ca D:10.20.30.2-ff:ff:ff:ff:ff:ff ipwatchd[2066]: Device info: eth0 10.20.30.2-0:e0:4c:77:15:fb ipwatchd[2066]: MAC address 0:d:87:fc:7c:ca causes IP conflict with address 10.20.30.2 set on interface eth0 - passive mode - reply not sent ipwatchd[2066]: Running user-defined script: /usr/sbin/ipwatchd-script "eth0" "10.20.30.2" "0:d:87:fc:7c:ca" ipwatchd[2066]: Received ARP packet: S:10.20.30.2-0:d:87:fc:7c:ca D:10.20.30.2-ff:ff:ff:ff:ff:ff ipwatchd[2066]: Device info: eth0 10.20.30.2-0:e0:4c:77:15:fb ipwatchd[2066]: MAC address 0:d:87:fc:7c:ca causes IP conflict with address 10.20.30.2 set on interface eth0 - passive mode - reply not sent ipwatchd[2066]: Running user-defined script: /usr/sbin/ipwatchd-script "eth0" "10.20.30.2" "0:d:87:fc:7c:ca" ipwatchd[2066]: Received signal 15 ipwatchd[2066]: IPwatchD stopped

2.2 Defend interval with value 10

Configuration:	iface_configuration manual iface eth0 passive defend_interval 10 user_script /usr/sbin/ipwatchd-script syslog_facility daemon
Actions:	/usr/sbin/ipwatchd -t -d -c /etc/ipwatchd.conf && \ sleep 1 && \ arping -U -c 1 -I eth1 10.20.30.2 && \ sleep 1 && \ arping -U -c 1 -I eth1 10.20.30.2 && \ sleep 1 && \ killall ipwatchd
Expected result:	At least two conflicts must be detected but user-defined script must run only once.
Syslog output:	ipwatchd[2156]: Found interface eth0 ipwatchd[2156]: Daemon can be executed because process specified in PID file /var/run/ipwatchd.pid does not exist ipwatchd[2158]: IPwatchD started ipwatchd[2158]: Entering pcap loop ipwatchd[2158]: Received ARP packet: S:10.20.30.2-0:d:87:fc:7c:ca D:10.20.30.2-ff:ff:ff:ff:ff:ff ipwatchd[2158]: Device info: eth0 10.20.30.2-0:e0:4c:77:15:fb ipwatchd[2158]: MAC address 0:d:87:fc:7c:ca causes IP conflict with address 10.20.30.2 set on interface eth0 - passive mode - reply not sent ipwatchd[2158]: Running user-defined script: /usr/sbin/ipwatchd-script "eth0" "10.20.30.2" "0:d:87:fc:7c:ca" ipwatchd[2158]: Received ARP packet: S:10.20.30.2-0:d:87:fc:7c:ca D:10.20.30.2-ff:ff:ff:ff:ff:ff ipwatchd[2158]: Device info: eth0 10.20.30.2-0:e0:4c:77:15:fb ipwatchd[2158]: MAC address 0:d:87:fc:7c:ca causes IP conflict with address 10.20.30.2 set on interface eth0 - no action taken because this happened within the defend interval ipwatchd[2158]: Received signal 15 ipwatchd[2158]: IPwatchD stopped

3 User-defined script

3.1 Configuration without user-defined script

Configuration:	iface_configuration manual iface eth0 passive defend_interval 10 syslog_facility daemon
Actions:	/usr/sbin/ipwatchd -t -d -c /etc/ipwatchd.conf && \\ sleep 1 && \\ arping -U -c 1 -I eth1 10.20.30.2 && \\ sleep 1 && \\ killall ipwatchd
Expected result:	At least one conflict must be detected and user-defined script cannot be executed.
Syslog output:	ipwatchd[2171]: Found interface eth0 ipwatchd[2171]: Daemon can be executed because process specified in PID file /var/run/ipwatchd.pid does not exist ipwatchd[2173]: IPwatchD started ipwatchd[2173]: Entering pcap loop ipwatchd[2173]: Received ARP packet: S:10.20.30.2-0:d:87:fc:7c:ca D:10.20.30.2-ff:ff:ff:ff:ff:ff ipwatchd[2173]: Device info: eth0 10.20.30.2-0:e0:4c:77:15:fb ipwatchd[2173]: MAC address 0:d:87:fc:7c:ca causes IP conflict with address 10.20.30.2 set on interface eth0 - passive mode - reply not sent ipwatchd[2173]: No user-defined script specified ipwatchd[2173]: Received signal 15 ipwatchd[2173]: IPwatchD stopped

3.2 Configuration with user-defined script

Configuration:	iface_configuration manual iface eth0 passive defend_interval 10 user_script /usr/sbin/ipwatchd-script syslog_facility daemon
Actions:	/usr/sbin/ipwatchd -t -d -c /etc/ipwatchd.conf && \\ sleep 1 && \\ arping -U -c 1 -I eth1 10.20.30.2 && \\ sleep 1 && \\ killall ipwatchd
Expected result:	At least one conflict must be detected and user-defined script must be executed.
Syslog output:	ipwatchd[2182]: Found interface eth0 ipwatchd[2182]: Daemon can be executed because process specified in PID file /var/run/ipwatchd.pid does not exist ipwatchd[2184]: IPwatchD started ipwatchd[2184]: Entering pcap loop ipwatchd[2184]: Received ARP packet: S:10.20.30.2-0:d:87:fc:7c:ca D:10.20.30.2-ff:ff:ff:ff:ff:ff ipwatchd[2184]: Device info: eth0 10.20.30.2-0:e0:4c:77:15:fb ipwatchd[2184]: MAC address 0:d:87:fc:7c:ca causes IP conflict with address 10.20.30.2 set on interface eth0 - passive mode - reply not sent ipwatchd[2184]: Running user-defined script: /usr/sbin/ipwatchd-script "eth0" "10.20.30.2" "0:d:87:fc:7c:ca" ipwatchd[2184]: Received signal 15 ipwatchd[2184]: IPwatchD stopped

4 Protection modes

4.1 Active protection mode

Configuration:	iface_configuration manual iface eth0 active defend_interval 10 syslog_facility daemon
Actions:	/usr/sbin/ipwatchd -t -d -c /etc/ipwatchd.conf && \ sleep 1 && \ arping -U -c 1 -I eth1 10.20.30.2 && \ sleep 1 && \ killall ipwatchd
Expected result:	At least one conflict must be detected and ARP reply must be sent.
Syslog output:	ipwatchd[2194]: Found interface eth0 ipwatchd[2194]: Daemon can be executed because process specified in PID file /var/run/ipwatchd.pid does not exist ipwatchd[2196]: IPwatchD started ipwatchd[2196]: Entering pcap loop ipwatchd[2196]: Received ARP packet: S:10.20.30.2-0:d:87:fc:7c:ca D:10.20.30.2-ff:ff:ff:ff:ff:ff ipwatchd[2196]: Device info: eth0 10.20.30.2-0:e0:4c:77:15:fb ipwatchd[2196]: MAC address 0:d:87:fc:7c:ca causes IP conflict with address 10.20.30.2 set on interface eth0 - active mode - reply sent ipwatchd[2196]: Packet with size of 42 bytes sent ipwatchd[2196]: Packet with size of 42 bytes sent ipwatchd[2196]: Running user-defined script: /usr/sbin/ipwatchd-script "eth0" "10.20.30.2" "0:d:87:fc:7c:ca" ipwatchd[2196]: Received signal 15 ipwatchd[2196]: IPwatchD stopped

4.2 Passive protection mode

Configuration:	iface_configuration manual iface eth0 passive defend_interval 10 syslog_facility daemon
Actions:	/usr/sbin/ipwatchd -t -d -c /etc/ipwatchd.conf && \\ sleep 1 && \\ arping -U -c 1 -I eth1 10.20.30.1 && \\ sleep 1 && \\ killall ipwatchd
Expected result:	At least one conflict must be detected and ARP reply cannot be sent.
Syslog output:	ipwatchd[2206]: Found interface eth0 ipwatchd[2206]: Daemon can be executed because process specified in PID file /var/run/ipwatchd.pid does not exist ipwatchd[2208]: IPwatchD started ipwatchd[2208]: Entering pcap loop ipwatchd[2208]: Received ARP packet: S:10.20.30.2-0:d:87:fc:7c:ca D:10.20.30.2-ff:ff:ff:ff:ff:ff ipwatchd[2208]: Device info: eth0 10.20.30.2-0:e0:4c:77:15:fb ipwatchd[2208]: MAC address 0:d:87:fc:7c:ca causes IP conflict with address 10.20.30.2 set on interface eth0 - passive mode - reply not sent ipwatchd[2208]: Running user-defined script: /usr/sbin/ipwatchd-script "eth0" "10.20.30.2" "0:d:87:fc:7c:ca" ipwatchd[2208]: Received signal 15 ipwatchd[2208]: IPwatchD stopped

5 Local ARP packets

5.1 Packets generated by watched interface

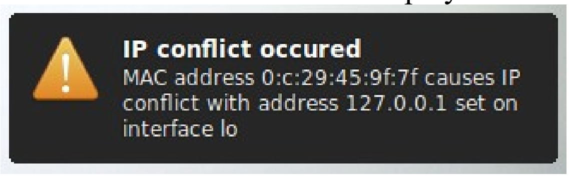
Configuration:	iface_configuration manual iface eth0 passive defend_interval 10 syslog_facility daemon
Actions:	/usr/sbin/ipwatchd -t -d -c /etc/ipwatchd.conf && \ sleep 1 && \ arping -U -c 1 -I eth0 10.20.30.2 && \ sleep 1 && \ killall ipwatchd
Expected result:	ARP packet must be ignored.
Syslog output:	ipwatchd[2223]: Found interface eth0 ipwatchd[2223]: Daemon can be executed because process specified in PID file /var/run/ipwatchd.pid does not exist ipwatchd[2225]: IPwatchD started ipwatchd[2225]: Entering pcap loop ipwatchd[2225]: Received ARP packet: S:10.20.30.2-0:e0:4c:77:15:fb D:10.20.30.2-ff:ff:ff:ff:ff:ff ipwatchd[2225]: Device info: eth0 10.20.30.2-0:e0:4c:77:15:fb ipwatchd[2225]: ARP packet ignored because it comes from local interface. ipwatchd[2225]: Received signal 15 ipwatchd[2225]: IPwatchD stopped

5.2 More than one interface connected to the same subnet

Configuration:	iface_configuration manual iface eth0 passive defend_interval 10 syslog_facility daemon
Actions:	/usr/sbin/ipwatchd -t -d -c /etc/ipwatchd.conf && \ sleep 1 && \ arping -U -c 1 -I eth1 10.20.30.1 && \ sleep 1 && \ killall ipwatchd
Expected result:	ARP packet must be ignored.
Syslog output:	ipwatchd[2233]: Found interface eth0 ipwatchd[2233]: Found interface eth1 ipwatchd[2233]: Daemon can be executed because process specified in PID file /var/run/ipwatchd.pid does not exist ipwatchd[2235]: IPwatchD started ipwatchd[2235]: Entering pcap loop ipwatchd[2235]: Received ARP packet: S:10.20.30.2-0:d:87:fc:7c:ca D:10.20.30.2-ff:ff:ff:ff:ff:ff ipwatchd[2235]: Device info: eth0 10.20.30.2-0:e0:4c:77:15:fb ipwatchd[2235]: Device info: eth1 10.20.40.3-0:d:87:fc:7c:ca ipwatchd[2235]: ARP packet ignored because it comes from local machine. ipwatchd[2235]: Received signal 15 ipwatchd[2235]: IPwatchD stopped

6 Miscellaneous

6.1 Desktop notification support

Configuration:	Default
Actions:	• Build and install ipwatchd and ipwd-gnotify • Edit /etc/init.d/ipwatchd and change daemon arguments to: DAEMON_ARGS="-t -d -c /etc/ipwatchd.conf" • Make sure IPwatchD is running in your runlevel. If needed run: update-rc.d ipwatchd defaults • Restart OS and login into GNOME • To cause IP conflict execute: arping -U -c 1 -I eth1 10.20.30.1
Expected result:	Notification bubble must be displayed after arping.  **IP conflict occured** MAC address 0:c:29:45:9f:7f causes IP conflict with address 127.0.0.1 set on interface lo
Syslog output:	ipwatchd[4928]: Received ARP packet: S:10.20.30.1-0:c:f1:4d:e8:b5 D:10.20.30.1-ff:ff:ff:ff:ff:ff ipwatchd[4928]: Device info: eth0 10.20.30.1-0:40:d0:6f:66:87 ipwatchd[4928]: MAC address 0:c:f1:4d:e8:b5 causes IP conflict with address 10.20.30.1 set on interface eth0 - passive mode - reply not sent ipwatchd[4928]: Running user-defined script: /usr/sbin/ipwatchd-script "eth0" "10.20.30.1" "0:c:f1:4d:e8:b5"