Apple Business Systems
Technical Notes

Product Technical Support

IPG01: IP Gateway Tuning

Written by : Sari Harrison September, 1994

Introduction

This document describes how to tune the Apple IP Gateway’s low-level parameters to suit your specific needs. You should attempt this tuning only if you are an experienced Macintosh administrator with a solid working knowledge of ResEdit, the application program that is used to make these modifications.

Warning: Apple Computer, Inc., is not liable for any damage done to the Apple IP Gateway through the use of ResEdit to tune the software.

The 'cnfg' resource

All of the tuning procedures detailed here are carried out on the 'cnfg' resource, which contains configuration information about the gateway. The 'cnfg' resource in the Gateway Prefs file (stored in the Preferences folder in the System Folder) contains the current configuration. If no Gateway Prefs file exists, the gateway will create one with the default 'cnfg' resource in the Apple IP Gateway Extension.

Important: It is strongly recommended that all modifications be done to the Gateway Prefs 'cnfg' resource. By doing so, if problems arise, the defaults can be restored by throwing away the Gateway Prefs file or moving it out of the Preferences folder.

The following example shows what you might see if you opened a 'cnfg' resource with ResEdit:

```
000000     0002 11BE 2883 0002
000008     11BE 2883 0000 003C
000010     0000 0000 0000 05A0
000018     0000 0000 0000 0005
000020     0000 001E 0014 0002
000028     0004 0005 0100 01
```

Many variables within the 'cnfg' resource can be configured using the Gateway Manager program. The necessary procedures are covered in the *Apple IP Gateway Administrator’s Guide.* This document covers those variables that you can only modify with ResEdit, not with the Gateway Manager. The following table illustrates the 'cnfg' resource and describes the modifiable fields within it. Once changes in the resource are made, the gateway will adopt those changes the next time it is started.

Hex Offset	*Decimal Offset*	*Length in bytes*	*sample data*	*Description*
$0C	12	4	0000 003C	Interval to be used for aging clients.
$10	16	4	0000 0000	Dynamic clients' idle timeout.
$14	20	4	0000 05A0	Static clients' idle timeout.
$18	24	4	0000 0000	NBP Confirm timeout.
$1C	28	4	0000 0005	PING timeout.

$20	32	4	0000 001E	How often to check for address conflicts on Ethernet.
$24	36	2	0014	Number of Ethernet ARP table entries.
$28	40	2	0004	Number of NBP Lookup retries.
$2A	42	2	0005	Timeout for each NBP Lookup.

Aging of Clients

Timing out or “aging” of clients allows automatic (dynamic) addresses to be reused. The gateway is configured by default to PING each dynamic client every minute to see if it is still up and running. If the gateway does not receive a PING response from a client within five minutes, it assumes the client is down and makes the address available for reassignment. Manual (static) addresses are never aged out. The following five fields can be used to modify how the gateway ages clients.

Interval to be used for aging clients:

This field controls what the base interval (in seconds) is for timing out gateway clients. The next five fields in the resource (Dynamic clients' idle timeout, Static clients' idle timeout, NBP Confirm timeout, PING timeout, How often to check for address conflicts on Ethernet) depend on this field in that they are multiples of this interval. For example, if you set the base interval to 30 and the dynamic clients’ idle timeout to 10, the gateway assumes a client is no longer using a particular address if a client is idle for 5 minutes (10 intervals of 30 seconds). The default is 60 seconds.

In the example 'cnfg' resource, the interval shown is a hex value of 0000003C, which translates to a decimal value of 60.

Dynamic clients' idle timeout

This field controls the timing out of dynamic clients based on their idle time. It is in multiples of the base interval described above. When the field is nonzero, clients who are idle for the specified amount of time are assumed to be finished using their addresses, and their addresses are made available for reassignment. This may cause a former address holder to lose connection to the gateway until the client computer is restarted. When this field is 0 (the default), dynamic clients will not be timed out based on idle time.

In the example 'cnfg' resource, the dynamic clients' idle timeout is a hex 00000000 which translates to a decimal 0. Thus dynamic clients will not be aged out based on idle time.

Static clients' idle timeout

This field controls the timing out of static clients based on their idle time. It is in multiples of the base interval described above. When the field is nonzero, clients who are idle for the specified amount of time are assumed to be finished using their addresses and will disappear from the Gateway Information window in the Gateway Manager program. Unlike the case with dynamic addresses, this will not cause the user to lose connection to the gateway. The entry will simply reappear in the information window when the client next uses IP services. When this field is 0 (the default), static clients will not be aged out based on idle time.

In the example 'cnfg' resource, the static clients' idle timeout is a hex 000005A0, which translates to a decimal 1440. Static clients that are idle for 24 hours (1440 X 60 seconds) will disappear from the Gateway Information window in the Gateway Manager.

NBP Confirm timeout:

This field controls the timing out of dynamic clients based on Name Binding Protocol (NBP) Confirms. This method makes use of the fact that IP addresses are registered with NBP so long as clients are up and running. If this field is nonzero, an NBP Confirm will be sent to each client every interval (see the previous discussion under “Interval to be used for aging clients.”). If the gateway does not get a Confirm response in the number of intervals specified by this field, the client is assumed to be down and the address will be made available for reassignment. If this field is 0 (the default), dynamic clients will not be aged out using this method.

In the example 'cnfg' resource, the NBP Confirm timeout is hex 00000000, thus dynamic clients will not be aged out using this method.

A major drawback of this approach is that for NBP Confirms to recieve a response, clients must be in the same zone as the gateway. Clients in different zones may age out quickly. It is therefore recommended that this field stay 0 unless all clients are in the same zone as the gateway.

PING timeout:

This field controls the timing out of dynamic clients based on ICMP ECHO or PING. If this field is nonzero (default is 5), the gateway will send out PING packets to each dynamic client every base interval. If no response is received in the number of intervals specified by the field value, the gateway assumes the client is down and makes the address available for reassignment. Loss of connection to the gateway is unlikely because the client would automatically respond to PINGs if it were still up and running. This is the recommended method for aging dynamic clients. If this field is 0, PING will not be used to time out clients.

In the example 'cnfg' resource, the PING timeout is hex 00000005, so dynamic clients will be aged out after five minutes with no PING response received.

Address Conflicts

Address conflicts are very common in the IP world because the user is often responsible for configuring his or her own address. The gateway automatically checks the IP network to make sure that none of the addresses it is allotted to assign automatically are already in use. The next field controls this check.

How often to check for address conflicts on Ethernet

This field controls how often the gateway checks the IP network for addresses conflicting with the gateway's automatic range of addresses. The gateway sends out Address Resolution Protocol (ARP) packets for each dynamic address after the number of specified base intervals has passed. For example, if the interval is 120 (2 minutes), and the check for address conflicts field is 10, the gateway will send out ARP packets every 20 minutes. If an ARP response is received, an entry appears in the gateway information window indicating an address conflict, and the address is removed from the pool of available addresses.

In the example 'cnfg' resource, the address-conflict check time is hex 0000001E, which translates to decimal 30, so the gateway will send out ARP packets on the IP network every 30 minutes.

ARP Table

The Ethernet addresses of IP hosts are stored in a table, the size of which is controlled by the next field.

Number of Ethernet ARP entries

This field controls how many Ethernet ARP entries can be stored at the same time. The default is 20. Increasing this number will incrementally increase the amount of memory the gateway uses, but will allow the gateway to “talk to” more IP hosts at the same time. This may increase performance under heavy usage.

In the example 'cnfg' resource, the number of Ethernet ARP entries is hex 00000014, which translates to decimal 20, so there is room to store 20 Ethernet addresses of IP hosts at the same time.

Macintosh Name

The gateway obtains Macintosh names to display in the Gateway Information window by sending NBP lookups to clients. The next two fields allow the tuning of this lookup. If nameless clients appear, increasing the frequency or number of lookups may help.

Number of NBP Lookup retries

This field controls how many times the NBP Lookup is tried before the gateway gives up on getting the client’s Macintosh name. The default is 4.

In the example 'cnfg' resource, the number of retries is hex 00000004, so the gateway will try 5 times (once plus 4 retries) to get each Macintosh name.

Timeout for each NBP Lookup

This field controls the time between each NBP Lookup in seconds. The default is 5.

In the example 'cnfg' resource, the timeout for each NBP Lookup is hex 00000005, so the gateway will wait 5 seconds before sending another NBP Lookup for a Macintosh name.