



Squid default configuration

Version: 2211

Copyright 2007-2010 ImageStream Internet Solutions, Inc., All rights Reserved.

Table of Contents

Squid default configuration.....	1
----------------------------------	---

Squid default configuration

```
# ImageStream defaults
visible_hostname Squid-Cache
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8
acl localnet src 10.0.0.0/8      # RFC1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443        # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access allow localnet
http_access deny all
icp_access allow localnet
icp_access deny all
htcp_access allow localnet
htcp_access deny all
http_port 3128
hierarchy_stoplist cgi-bin ?
access_log /usr/local/squid/var/logs/access.log squid
refresh_pattern ^ftp:          1440    20%    10080
refresh_pattern ^gopher:      1440    0%     1440
refresh_pattern (cgi-bin|\\?)  0       0%     0
refresh_pattern .              0      20%    4320
icp_port 3130
coredump_dir /usr/local/squid/var/cache

#      WELCOME TO SQUID 3.0.STABLE8
#      -----
#
#      This is the default Squid configuration file. You may wish
#      to look at the Squid home page (http://www.squid-cache.org/)
#      for the FAQ and other documentation.
#
#      The default Squid config file shows what the defaults for
#      various options happen to be. If you don't need to change the
#      default, you shouldn't uncomment the line. Doing so may cause
#      run-time problems. In some cases "none" refers to no default
#      setting at all, while in other cases it refers to a valid
#      option - the comments for that keyword indicate if this is the
```

```
# case.
#

# Configuration options can be included using the "include" directive.
# Include takes a list of files to include. Quoting and wildcards is
# supported.
#
# For example,
#
# include /path/to/included/file/squid.acl.config
#
# Includes can be nested up to a hard-coded depth of 16 levels.
# This arbitrary restriction is to prevent recursive include references
# from causing Squid entering an infinite loop whilst trying to load
# configuration files.

# OPTIONS FOR AUTHENTICATION
# -----

# TAG: auth_param
# This is used to define parameters for the various authentication
# schemes supported by Squid.
#
# format: auth_param scheme parameter [setting]
#
# The order in which authentication schemes are presented to the client is
# dependent on the order the scheme first appears in config file. IE
# has a bug (it's not RFC 2617 compliant) in that it will use the basic
# scheme if basic is the first entry presented, even if more secure
# schemes are presented. For now use the order in the recommended
# settings section below. If other browsers have difficulties (don't
# recognize the schemes offered even if you are using basic) either
# put basic first, or disable the other schemes (by commenting out their
# program entry).
#
# Once an authentication scheme is fully configured, it can only be
# shutdown by shutting squid down and restarting. Changes can be made on
# the fly and activated with a reconfigure. I.E. You can change to a
# different helper, but not unconfigure the helper completely.
#
# Please note that while this directive defines how Squid processes
# authentication it does not automatically activate authentication.
# To use authentication you must in addition make use of ACLs based
# on login name in http_access (proxy_auth, proxy_auth_regex or
# external with %LOGIN used in the format tag). The browser will be
# challenged for authentication on the first such acl encountered
# in http_access processing and will also be re-challenged for new
# login credentials if the request is being denied by a proxy_auth
# type acl.
#
# WARNING: authentication can't be used in a transparently intercepting
# proxy as the client then thinks it is talking to an origin server and
# not the proxy. This is a limitation of bending the TCP/IP protocol to
# transparently intercepting port 80, not a limitation in Squid.
# Ports flagged 'transparent' or 'tproxy' have authentication disabled.
#
# === Parameters for the basic scheme follow. ===
#
```

```
# "program" cmdline
# Specify the command for the external authenticator. Such a program
# reads a line containing "username password" and replies "OK" or
# "ERR" in an endless loop. "ERR" responses may optionally be followed
# by a error description available as %m in the returned error page.
# If you use an authenticator, make sure you have 1 acl of type proxy_auth.
#
# By default, the basic authentication scheme is not used unless a
# program is specified.
#
# If you want to use the traditional NCSA proxy authentication, set
# this line to something like
#
# auth_param basic program /usr/local/squid/libexec/ncsa_auth /usr/local/squid/etc/passwd
#
# "children" numberofchildren
# The number of authenticator processes to spawn. If you start too few
# Squid will have to wait for them to process a backlog of credential
# verifications, slowing it down. When password verifications are
# done via a (slow) network you are likely to need lots of
# authenticator processes.
# auth_param basic children 5
#
# "concurrency" concurrency
# The number of concurrent requests the helper can process.
# The default of 0 is used for helpers who only supports
# one request at a time. Setting this changes the protocol used to
# include a channel number first on the request/response line, allowing
# multiple requests to be sent to the same helper in parallel without
# waiting for the response.
# Must not be set unless it's known the helper supports this.
# auth_param basic concurrency 0
#
# "realm" realmstring
# Specifies the realm name which is to be reported to the
# client for the basic proxy authentication scheme (part of
# the text the user will see when prompted their username and
# password). There is no default.
# auth_param basic realm Squid proxy-caching web server
#
# "credentialsttl" timetolive
# Specifies how long squid assumes an externally validated
# username:password pair is valid for - in other words how
# often the helper program is called for that user. Set this
# low to force revalidation with short lived passwords. Note
# setting this high does not impact your susceptibility
# to replay attacks unless you are using an one-time password
# system (such as SecureID). If you are using such a system,
# you will be vulnerable to replay attacks unless you also
# use the max_user_ip ACL in an http_access rule.
#
# "casesensitive" on|off
# Specifies if usernames are case sensitive. Most user databases are
# case insensitive allowing the same username to be spelled using both
# lower and upper case letters, but some are case sensitive. This
# makes a big difference for user_max_ip ACL processing and similar.
# auth_param basic casesensitive off
#
# === Parameters for the digest scheme follow ===
#
```

```
# "program" cmdline
# Specify the command for the external authenticator.  Such
# a program reads a line containing "username":"realm" and
# replies with the appropriate H(A1) value hex encoded or
# ERR if the user (or his H(A1) hash) does not exists.
# See rfc 2616 for the definition of H(A1).
# "ERR" responses may optionally be followed by a error description
# available as %m in the returned error page.
#
# By default, the digest authentication scheme is not used unless a
# program is specified.
#
# If you want to use a digest authenticator, set this line to
# something like
#
# auth_param digest program /usr/local/squid/bin/digest_auth_pw /usr/local/squid/etc/digpass
#
# "children" numberofchildren
# The number of authenticator processes to spawn (no default).
# If you start too few Squid will have to wait for them to
# process a backlog of H(A1) calculations, slowing it down.
# When the H(A1) calculations are done via a (slow) network
# you are likely to need lots of authenticator processes.
# auth_param digest children 5
#
# "realm" realmstring
# Specifies the realm name which is to be reported to the
# client for the digest proxy authentication scheme (part of
# the text the user will see when prompted their username and
# password). There is no default.
# auth_param digest realm Squid proxy-caching web server
#
# "nonce_garbage_interval" timeinterval
# Specifies the interval that nonces that have been issued
# to client_agent's are checked for validity.
#
# "nonce_max_duration" timeinterval
# Specifies the maximum length of time a given nonce will be
# valid for.
#
# "nonce_max_count" number
# Specifies the maximum number of times a given nonce can be
# used.
#
# "nonce_strictness" on|off
# Determines if squid requires strict increment-by-1 behavior
# for nonce counts, or just incrementing (off - for use when
# useragents generate nonce counts that occasionally miss 1
# (ie, 1,2,4,6)). Default off.
#
# "check_nonce_count" on|off
# This directive if set to off can disable the nonce count check
# completely to work around buggy digest qop implementations in
# certain mainstream browser versions. Default on to check the
# nonce count to protect from authentication replay attacks.
#
# "post_workaround" on|off
# This is a workaround to certain buggy browsers who sends
# an incorrect request digest in POST requests when reusing
# the same nonce as acquired earlier on a GET request.
```



```
#
#   === NTLM scheme options follow ===
#
#   "program" cmdline
#   Specify the command for the external NTLM authenticator.
#   Such a program reads exchanged NTLMSSP packets with
#   the browser via Squid until authentication is completed.
#   If you use an NTLM authenticator, make sure you have 1 acl
#   of type proxy_auth. By default, the NTLM authenticator_program
#   is not used.
#
#   auth_param ntlm program /usr/local/squid/bin/ntlm_auth
#
#   "children" numberofchildren
#   The number of authenticator processes to spawn (no default).
#   If you start too few Squid will have to wait for them to
#   process a backlog of credential verifications, slowing it
#   down. When credential verifications are done via a (slow)
#   network you are likely to need lots of authenticator
#   processes.
#
#   auth_param ntlm children 5
#
#   "keep_alive" on|off
#   If you experience problems with PUT/POST requests when using the
#   Negotiate authentication scheme then you can try setting this to
#   off. This will cause Squid to forcibly close the connection on
#   the initial requests where the browser asks which schemes are
#   supported by the proxy.
#
#   auth_param ntlm keep_alive on
#
#   === Options for configuring the NEGOTIATE auth-scheme follow ===
#
#   "program" cmdline
#   Specify the command for the external Negotiate authenticator.
#   This protocol is used in Microsoft Active-Directory enabled setups with
#   the Microsoft Internet Explorer or Mozilla Firefox browsers.
#   Its main purpose is to exchange credentials with the Squid proxy
#   using the Kerberos mechanisms.
#   If you use a Negotiate authenticator, make sure you have at least one acl
#   of type proxy_auth active. By default, the negotiate authenticator_program
#   is not used.
#   The only supported program for this role is the ntlm_auth
#   program distributed as part of Samba, version 4 or later.
#
#   auth_param negotiate program /usr/local/squid/bin/ntlm_auth --helper-protocol=gss-spnego
#
#   "children" numberofchildren
#   The number of authenticator processes to spawn (no default).
#   If you start too few Squid will have to wait for them to
#   process a backlog of credential verifications, slowing it
#   down. When credential verifications are done via a (slow)
#   network you are likely to need lots of authenticator
#   processes.
#
#   auth_param negotiate children 5
#
#   "keep_alive" on|off
#   If you experience problems with PUT/POST requests when using the
#   Negotiate authentication scheme then you can try setting this to
```

```

#       off. This will cause Squid to forcibly close the connection on
#       the initial requests where the browser asks which schemes are
#       supported by the proxy.
#
#       auth_param negotiate keep_alive on
#
#Recommended minimum configuration per scheme:
#auth_param negotiate program <uncomment and complete this line to activate>
#auth_param negotiate children 5
#auth_param negotiate keep_alive on
#auth_param ntlm program <uncomment and complete this line to activate>
#auth_param ntlm children 5
#auth_param ntlm keep_alive on
#auth_param digest program <uncomment and complete this line>
#auth_param digest children 5
#auth_param digest realm Squid proxy-caching web server
#auth_param digest nonce_garbage_interval 5 minutes
#auth_param digest nonce_max_duration 30 minutes
#auth_param digest nonce_max_count 50
#auth_param basic program <uncomment and complete this line>
#auth_param basic children 5
#auth_param basic realm Squid proxy-caching web server
#auth_param basic credentialsttl 2 hours

# TAG: authenticate_cache_garbage_interval
#       The time period between garbage collection across the username cache.
#       This is a tradeoff between memory utilization (long intervals - say
#       2 days) and CPU (short intervals - say 1 minute). Only change if you
#       have good reason to.
#
#Default:
# authenticate_cache_garbage_interval 1 hour

# TAG: authenticate_ttl
#       The time a user & their credentials stay in the logged in
#       user cache since their last request. When the garbage
#       interval passes, all user credentials that have passed their
#       TTL are removed from memory.
#
#Default:
# authenticate_ttl 1 hour

# TAG: authenticate_ip_ttl
#       If you use proxy authentication and the 'max_user_ip' ACL,
#       this directive controls how long Squid remembers the IP
#       addresses associated with each user. Use a small value
#       (e.g., 60 seconds) if your users might change addresses
#       quickly, as is the case with dialups. You might be safe
#       using a larger value (e.g., 2 hours) in a corporate LAN
#       environment with relatively static address assignments.
#
#Default:
# authenticate_ip_ttl 0 seconds

# ACCESS CONTROLS
# -----

# TAG: external_acl_type
#       This option defines external acl classes using a helper program

```

```

#         to look up the status
#
#         external_acl_type name [options] FORMAT.. /path/to/helper [helper arguments..]
#
# Options:
#
#         ttl=n           TTL in seconds for cached results (defaults to 3600
#                        for 1 hour)
#         negative_ttl=n  TTL for cached negative lookups (default same
#                        as ttl)
#         children=n      Number of acl helper processes spawn to service
#                        external acl lookups of this type. (default 5)
#         concurrency=n   concurrency level per process. Only used with helpers
#                        capable of processing more than one query at a time.
#         cache=n         result cache size, 0 is unbounded (default)
#         grace=n         Percentage remaining of TTL where a refresh of a
#                        cached entry should be initiated without needing to
#                        wait for a new reply. (default 0 for no grace period)
#         protocol=2.5    Compatibility mode for Squid-2.5 external acl helpers
#
# FORMAT specifications
#
#         %LOGIN          Authenticated user login name
#         %EXT_USER       Username from external acl
#         %IDENT          Ident user name
#         %SRC            Client IP
#         %SRCPORT        Client source port
#         %URI            Requested URI
#         %DST            Requested host
#         %PROTO          Requested protocol
#         %PORT           Requested port
#         %PATH           Requested URL path
#         %METHOD         Request method
#         %MYADDR         Squid interface address
#         %MYPORT         Squid http_port number
#         %PATH           Requested URL-path (including query-string if any)
#         %USER_CERT      SSL User certificate in PEM format
#         %USER_CERTCHAIN SSL User certificate chain in PEM format
#         %USER_CERT_xx   SSL User certificate subject attribute xx
#         %USER_CA_xx     SSL User certificate issuer attribute xx
#         %{Header}       HTTP request header
#         %{Hdr:member}   HTTP request header list member
#         %{Hdr;;member} HTTP request header list member using ; as
#                        list separator. ; can be any non-alphanumeric
#                        character.
#
# In addition to the above, any string specified in the referencing
# acl will also be included in the helper request line, after the
# specified formats (see the "acl external" directive)
#
# The helper receives lines per the above format specification,
# and returns lines starting with OK or ERR indicating the validity
# of the request and optionally followed by additional keywords with
# more details.
#
# General result syntax:
#
#         OK/ERR keyword=value ...
    
```

```

#
#   Defined keywords:
#
#   user=           The users name (login)
#   password=       The users password (for login= cache_peer option)
#   message=        Message describing the reason. Available as %o
#                   in error pages
#   tag=            Apply a tag to a request (for both ERR and OK results)
#                   Only sets a tag, does not alter existing tags.
#   log=            String to be logged in access.log. Available as
#                   %ea in logformat specifications
#
#   If protocol=3.0 (the default) then URL escaping is used to protect
#   each value in both requests and responses.
#
#   If using protocol=2.5 then all values need to be enclosed in quotes
#   if they may contain whitespace, or the whitespace escaped using \.
#   And quotes or \ characters within the keyword value must be \ escaped.
#
#   When using the concurrency= option the protocol is changed by
#   introducing a query channel tag in front of the request/response.
#   The query channel tag is a number between 0 and concurrency-1.
#
#Default:
# none

# TAG: acl
#   Defining an Access List
#
#   Every access list definition must begin with an aclname and acltype,
#   followed by either type-specific arguments or a quoted filename that
#   they are read from.
#
#       acl aclname acltype argument ...
#       acl aclname acltype "file" ...
#
#   When using "file", the file should contain one item per line.
#
#   By default, regular expressions are CASE-SENSITIVE.  To make
#   them case-insensitive, use the -i option.
#
# ***** ACL TYPES AVAILABLE *****
#
#   acl aclname src ip-address/netmask ...           # clients IP address
#   acl aclname src addr1-addr2/netmask ...         # range of addresses
#   acl aclname dst ip-address/netmask ...         # URL host's IP address
#   acl aclname myip ip-address/netmask ...        # local socket IP address
#
#   acl aclname arp      mac-address ... (xx:xx:xx:xx:xx:xx notation)
#   # The arp ACL requires the special configure option --enable-arp-acl.
#   # Furthermore, the ARP ACL code is not portable to all operating systems.
#   # It works on Linux, Solaris, Windows, FreeBSD, and some other *BSD variants.
#   #
#   # NOTE: Squid can only determine the MAC address for clients that are on
#   # the same subnet.  If the client is on a different subnet, then Squid cannot
#   # find out its MAC address.
#
#   acl aclname srcdomain .foo.com ...             # reverse lookup, from client IP
#   acl aclname dstdomain .foo.com ...             # Destination server from URL

```

```

#      acl aclname srcdom_regex [-i] \.foo\.com ...      # regex matching client name
#      acl aclname dstdom_regex [-i] \.foo\.com ...      # regex matching server
#      # For dstdomain and dstdom_regex a reverse lookup is tried if a IP
#      # based URL is used and no match is found. The name "none" is used
#      # if the reverse lookup fails.
#
#      acl aclname src_as number ...
#      acl aclname dst_as number ...
#      # Except for access control, AS numbers can be used for
#      # routing of requests to specific caches. Here's an
#      # example for routing all requests for AS#1241 and only
#      # those to mycache.mydomain.net:
#      # acl asexample dst_as 1241
#      # cache_peer_access mycache.mydomain.net allow asexample
#      # cache_peer_access mycache_mydomain.net deny all
#
#      acl aclname time [day-abbrevs] [h1:m1-h2:m2]
#      # day-abbrevs:
#      #   S - Sunday
#      #   M - Monday
#      #   T - Tuesday
#      #   W - Wednesday
#      #   H - Thursday
#      #   F - Friday
#      #   A - Saturday
#      #   h1:m1 must be less than h2:m2
#
#      acl aclname url_regex [-i] ^http:// ...           # regex matching on whole URL
#      acl aclname urlpath_regex [-i] \.gif$ ...         # regex matching on URL path
#
#      acl aclname port 80 70 21 ...
#      acl aclname port 0-1024 ...                       # ranges allowed
#      acl aclname myport 3128 ...                       # (local socket TCP port)
#      acl aclname myportname 3128 ...                   # http(s)_port name
#
#      acl aclname proto HTTP FTP ...
#
#      acl aclname method GET POST ...
#
#      acl aclname http_status 200 301 500- 400-403 ...   # status code in reply
#
#      acl aclname browser [-i] regexp ...
#      # pattern match on User-Agent header (see also req_header below)
#
#      acl aclname referer_regex [-i] regexp ...
#      # pattern match on Referer header
#      # Referer is highly unreliable, so use with care
#
#      acl aclname ident username ...
#      acl aclname ident_regex [-i] pattern ...
#      # string match on ident output.
#      # use REQUIRED to accept any non-null ident.
#
#      acl aclname proxy_auth [-i] username ...
#      acl aclname proxy_auth_regex [-i] pattern ...
#      # list of valid usernames
#      # use REQUIRED to accept any valid username.
#
#      #
#      # NOTE: when a Proxy-Authentication header is sent but it is not
#      # needed during ACL checking the username is NOT logged

```

```

#       # in access.log.
#       #
#       # NOTE: proxy_auth requires a EXTERNAL authentication program
#       # to check username/password combinations (see
#       # auth_param directive).
#       #
#       # NOTE: proxy_auth can't be used in a transparent/intercepting proxy
#       # as the browser needs to be configured for using a proxy in order
#       # to respond to proxy authentication.
#
# acl aclname snmp_community string ...
#       # A community string to limit access to your SNMP Agent
#       # Example:
#       #
#       #       acl snmppublic snmp_community public
#
# acl aclname maxconn number
#       # This will be matched when the client's IP address has
#       # more than <number> HTTP connections established.
#
# acl aclname max_user_ip [-s] number
#       # This will be matched when the user attempts to log in from more
#       # than <number> different ip addresses. The authenticate_ip_ttl
#       # parameter controls the timeout on the ip entries.
#       # If -s is specified the limit is strict, denying browsing
#       # from any further IP addresses until the ttl has expired. Without
#       # -s Squid will just annoy the user by "randomly" denying requests.
#       # (the counter is reset each time the limit is reached and a
#       # request is denied)
#       # NOTE: in acceleration mode or where there is mesh of child proxies,
#       # clients may appear to come from multiple addresses if they are
#       # going through proxy farms, so a limit of 1 may cause user problems.
#
# acl aclname req_mime_type [-i] mime-type ...
#       # regex match against the mime type of the request generated
#       # by the client. Can be used to detect file upload or some
#       # types HTTP tunneling requests.
#       # NOTE: This does NOT match the reply. You cannot use this
#       # to match the returned file type.
#
# acl aclname req_header header-name [-i] any\.regex\.here
#       # regex match against any of the known request headers. May be
#       # thought of as a superset of "browser", "referer" and "mime-type"
#       # ACLs.
#
# acl aclname rep_mime_type [-i] mime-type ...
#       # regex match against the mime type of the reply received by
#       # squid. Can be used to detect file download or some
#       # types HTTP tunneling requests.
#       # NOTE: This has no effect in http_access rules. It only has
#       # effect in rules that affect the reply data stream such as
#       # http_reply_access.
#
# acl aclname rep_header header-name [-i] any\.regex\.here
#       # regex match against any of the known reply headers. May be
#       # thought of as a superset of "browser", "referer" and "mime-type"
#       # ACLs.
#
# acl aclname external class_name [arguments...]
#       # external ACL lookup via a helper class defined by the

```

```

#       # external_acl_type directive.
#
#       acl aclname user_cert attribute values...
#       # match against attributes in a user SSL certificate
#       # attribute is one of DN/C/O/CN/L/ST
#
#       acl aclname ca_cert attribute values...
#       # match against attributes a users issuing CA SSL certificate
#       # attribute is one of DN/C/O/CN/L/ST
#
#       acl aclname ext_user username ...
#       acl aclname ext_user_regex [-i] pattern ...
#       # string match on username returned by external acl helper
#       # use REQUIRED to accept any non-null user name.
#
#Examples:
#acl macaddress arp 09:00:2b:23:45:67
#acl myexample dst_as 1241
#acl password proxy_auth REQUIRED
#acl fileupload req_mime_type -i ^multipart/form-data$
#acl javascript rep_mime_type -i ^application/x-javascript$
#
#Default:
# acl all src all
#
#Recommended minimum configuration:
#acl manager proto cache_object
#acl localhost src 127.0.0.1/32
#acl to_localhost dst 127.0.0.0/8
#
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
#acl localnet src 10.0.0.0/8      # RFC1918 possible internal network
#acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
#acl localnet src 192.168.0.0/16      # RFC1918 possible internal network
#
#acl SSL_ports port 443
#acl Safe_ports port 80          # http
#acl Safe_ports port 21         # ftp
#acl Safe_ports port 443        # https
#acl Safe_ports port 70         # gopher
#acl Safe_ports port 210        # wais
#acl Safe_ports port 1025-65535 # unregistered ports
#acl Safe_ports port 280        # http-mgmt
#acl Safe_ports port 488        # gss-http
#acl Safe_ports port 591        # filemaker
#acl Safe_ports port 777        # multiling http
#acl CONNECT method CONNECT

# TAG: http_access
#       Allowing or Denying access based on defined access lists
#
#       Access to the HTTP port:
#       http_access allow|deny [!]aclname ...
#
#       NOTE on default values:
#
#       If there are no "access" lines present, the default is to deny
#       the request.

```

```

#
#   If none of the "access" lines cause a match, the default is the
#   opposite of the last line in the list.  If the last line was
#   deny, the default is allow.  Conversely, if the last line
#   is allow, the default will be deny.  For these reasons, it is a
#   good idea to have an "deny all" or "allow all" entry at the end
#   of your access lists to avoid potential confusion.
#
#Default:
# http_access deny all
#
#Recommended minimum configuration:
#
# Only allow cachemgr access from localhost
#http_access allow manager localhost
#http_access deny manager
# Deny requests to unknown ports
#http_access deny !Safe_ports
# Deny CONNECT to other than SSL ports
#http_access deny CONNECT !SSL_ports
#
# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet

# And finally deny all other access to this proxy
#http_access deny all

# TAG: http_reply_access
#   Allow replies to client requests. This is complementary to http_access.
#
#   http_reply_access allow|deny [!] aclname ...
#
#   NOTE: if there are no access lines present, the default is to allow
#   all replies
#
#   If none of the access lines cause a match the opposite of the
#   last line will apply. Thus it is good practice to end the rules
#   with an "allow all" or "deny all" entry.
#
#Default:
# none

# TAG: icp_access
#   Allowing or Denying access to the ICP port based on defined
#   access lists
#
#   icp_access allow|deny [!]aclname ...
#
#   See http_access for details
#
#Default:

```



```
# icp_access deny all
#
#Allow ICP queries from local networks only
#icp_access allow localnet
#icp_access deny all

# TAG: htcp_access
#     Allowing or Denying access to the HTCP port based on defined
#     access lists
#
#     htcp_access allow|deny [!]aclname ...
#
#     See http_access for details
#
#     NOTE: The default if no htcp_access lines are present is to
#     deny all traffic. This default may cause problems with peers
#     using the htcp or htcp-oldsquid options.
#
#Default:
# htcp_access deny all
#
#Allow HTCP queries from local networks only
#htcp_access allow localnet
#htcp_access deny all

# TAG: htcp_clr_access
#     Allowing or Denying access to purge content using HTCP based
#     on defined access lists
#
#     htcp_clr_access allow|deny [!]aclname ...
#
#     See http_access for details
#
##Allow HTCP CLR requests from trusted peers
#acl htcp_clr_peer src 172.16.1.2
#htcp_clr_access allow htcp_clr_peer
#
#Default:
# htcp_clr_access deny all

# TAG: miss_access
#     Use to force your neighbors to use you as a sibling instead of
#     a parent. For example:
#
#         acl localclients src 172.16.0.0/16
#         miss_access allow localclients
#         miss_access deny !localclients
#
#     This means only your local clients are allowed to fetch
#     MISSES and all other clients can only fetch HITS.
#
#     By default, allow all clients who passed the http_access rules
#     to fetch MISSES from us.
#
#Default setting:
# miss_access allow all

# TAG: ident_lookup_access
#     A list of ACL elements which, if matched, cause an ident
#     (RFC 931) lookup to be performed for this request. For
```

```

# example, you might choose to always perform ident lookups
# for your main multi-user Unix boxes, but not for your Macs
# and PCs. By default, ident lookups are not performed for
# any requests.
#
# To enable ident lookups for specific client addresses, you
# can follow this example:
#
# acl ident_aware_hosts src 198.168.1.0/255.255.255.0
# ident_lookup_access allow ident_aware_hosts
# ident_lookup_access deny all
#
# Only src type ACL checks are fully supported. A src_domain
# ACL might work at times, but it will not always provide
# the correct result.
#
#Default:
# ident_lookup_access deny all

# TAG: reply_body_max_size      size [acl acl...]
# This option specifies the maximum size of a reply body. It can be
# used to prevent users from downloading very large files, such as
# MP3's and movies. When the reply headers are received, the
# reply_body_max_size lines are processed, and the first line where
# all (if any) listed ACLs are true is used as the maximum body size
# for this reply.
#
# This size is checked twice. First when we get the reply headers,
# we check the content-length value. If the content length value exists
# and is larger than the allowed size, the request is denied and the
# user receives an error message that says "the request or reply
# is too large." If there is no content-length, and the reply
# size exceeds this limit, the client's connection is just closed
# and they will receive a partial reply.
#
# WARNING: downstream caches probably can not detect a partial reply
# if there is no content-length header, so they will cache
# partial responses and give them out as hits. You should NOT
# use this option if you have downstream caches.
#
# WARNING: A maximum size smaller than the size of squid's error messages
# will cause an infinite loop and crash squid. Ensure that the smallest
# non-zero value you use is greater than the maximum header size plus
# the size of your largest error page.
#
# If you set this parameter none (the default), there will be
# no limit imposed.
#
#Default:
# none

# NETWORK OPTIONS
# -----

# TAG: http_port
# Usage: port [options]
#         hostname:port [options]
#         1.2.3.4:port [options]
#

```

```
# The socket addresses where Squid will listen for HTTP client
# requests. You may specify multiple socket addresses.
# There are three forms: port alone, hostname with port, and
# IP address with port. If you specify a hostname or IP
# address, Squid binds the socket to that specific
# address. This replaces the old 'tcp_incoming_address'
# option. Most likely, you do not need to bind to a specific
# address, so you can use the port number alone.
#
# If you are running Squid in accelerator mode, you
# probably want to listen on port 80 also, or instead.
#
# The -a command line option may be used to specify additional
# port(s) where Squid listens for proxy request. Such ports will
# be plain proxy ports with no options.
#
# You may specify multiple socket addresses on multiple lines.
#
# Options:
#
#     transparent    Support for transparent interception of
#                   outgoing requests without browser settings.
#                   NP: disables authentication on the port.
#
#     tproxy        Support Linux TPROXY for spoofing outgoing
#                   connections using the client IP address.
#                   NP: disables authentication on the port.
#
#     accel         Accelerator mode. Also needs at least one of
#                   vhost / vport / defaultsite.
#
#     defaultsite=domainname
#                   What to use for the Host: header if it is not present
#                   in a request. Determines what site (not origin server)
#                   accelerators should consider the default.
#                   Implies accel.
#
#     vhost         Accelerator mode using Host header for virtual
#                   domain support. Implies accel.
#
#     vport         Accelerator with IP based virtual host support.
#                   Implies accel.
#
#     vport=NN     As above, but uses specified port number rather
#                   than the http_port number. Implies accel.
#
#     protocol=    Protocol to reconstruct accelerated requests with.
#                   Defaults to http.
#
#     disable-pmtu-discovery=
#                   Control Path-MTU discovery usage:
#                   off          lets OS decide on what to do (default).
#                   transparent disable PMTU discovery when transparent
#                   support is enabled.
#                   always      disable always PMTU discovery.
#
# In many setups of transparently intercepting proxies
# Path-MTU discovery can not work on traffic towards the
# clients. This is the case when the intercepting device
# does not fully track connections and fails to forward
```

```

#           ICMP must fragment messages to the cache server. If you
#           have such setup and experience that certain clients
#           sporadically hang or never complete requests set
#           disable-pmtu-discovery option to 'transparent'.
#
#           name=           Specifies a internal name for the port. Defaults to
#                           the port specification (port or addr:port)
#
#           If you run Squid on a dual-homed machine with an internal
#           and an external interface we recommend you to specify the
#           internal address:port in http_port. This way Squid will only be
#           visible on the internal address.
#
# Squid normally listens to port 3128
#http_port 3128

# TAG: https_port
# Note: This option is only available if Squid is rebuilt with the
#       --enable-ssl option
#
# Usage: [ip:]port cert=certificate.pem [key=key.pem] [options...]
#
# The socket address where Squid will listen for HTTPS client
# requests.
#
# This is really only useful for situations where you are running
# squid in accelerator mode and you want to do the SSL work at the
# accelerator level.
#
# You may specify multiple socket addresses on multiple lines,
# each with their own SSL certificate and/or options.
#
# Options:
#
#       accel           Accelerator mode. Also needs at least one of
#                       defaultsite or vhost.
#
#       defaultsite=   The name of the https site presented on
#                       this port. Implies accel.
#
#       vhost           Accelerator mode using Host header for virtual
#                       domain support. Requires a wildcard certificate
#                       or other certificate valid for more than one domain.
#                       Implies accel.
#
#       protocol=      Protocol to reconstruct accelerated requests with.
#                       Defaults to https.
#
#       cert=          Path to SSL certificate (PEM format).
#
#       key=           Path to SSL private key file (PEM format)
#                       if not specified, the certificate file is
#                       assumed to be a combined certificate and
#                       key file.
#
#       version=       The version of SSL/TLS supported
#                       1   automatic (default)
#                       2   SSLv2 only
#                       3   SSLv3 only
#                       4   TLSv1 only

```

```
#
# cipher=      Colon separated list of supported ciphers.
#
# options=     Various SSL engine options. The most important
#              being:
#              NO_SSLv2   Disallow the use of SSLv2
#              NO_SSLv3   Disallow the use of SSLv3
#              NO_TLSv1   Disallow the use of TLSv1
#              SINGLE_DH_USE Always create a new key when using
#                          temporary/ephemeral DH key exchanges
#              See src/ssl_support.c or OpenSSL SSL_CTX_set_options
#              documentation for a complete list of options.
#
# clientca=    File containing the list of CAs to use when
#              requesting a client certificate.
#
# cafile=      File containing additional CA certificates to
#              use when verifying client certificates. If unset
#              clientca will be used.
#
# capath=      Directory containing additional CA certificates
#              and CRL lists to use when verifying client certificates.
#
# crlfile=     File of additional CRL lists to use when verifying
#              the client certificate, in addition to CRLs stored in
#              the capath. Implies VERIFY_CRL flag below.
#
# dhparams=    File containing DH parameters for temporary/ephemeral
#              DH key exchanges.
#
# sslflags=    Various flags modifying the use of SSL:
#              DELAYED_AUTH
#              Don't request client certificates
#              immediately, but wait until acl processing
#              requires a certificate (not yet implemented).
#              NO_DEFAULT_CA
#              Don't use the default CA lists built in
#              to OpenSSL.
#              NO_SESSION_REUSE
#              Don't allow for session reuse. Each connection
#              will result in a new SSL session.
#              VERIFY_CRL
#              Verify CRL lists when accepting client
#              certificates.
#              VERIFY_CRL_ALL
#              Verify CRL lists for all certificates in the
#              client certificate chain.
#
# sslcontext=  SSL session ID context identifier.
#
# vport        Accelerator with IP based virtual host support.
#
# vport=NN     As above, but uses specified port number rather
#              than the https_port number. Implies accel.
#
# name=        Specifies a internal name for the port. Defaults to
#              the port specification (port or addr:port)
#
#
#Default:
```

```

# none

# TAG: tcp_outgoing_tos
#   Allows you to select a TOS/Diffserv value to mark outgoing
#   connections with, based on the username or source address
#   making the request.
#
#   tcp_outgoing_tos ds-field (![aclname] ...)
#
#   Example where normal_service_net uses the TOS value 0x00
#   and good_service_net uses 0x20
#
#   acl normal_service_net src 10.0.0.0/255.255.255.0
#   acl good_service_net src 10.0.1.0/255.255.255.0
#   tcp_outgoing_tos 0x00 normal_service_net
#   tcp_outgoing_tos 0x20 good_service_net
#
#   TOS/DSCP values really only have local significance - so you should
#   know what you're specifying. For more information, see RFC2474 and
#   RFC3260.
#
#   The TOS/DSCP byte must be exactly that - a octet value 0 - 255, or
#   "default" to use whatever default your host has. Note that in
#   practice often only values 0 - 63 is usable as the two highest bits
#   have been redefined for use by ECN (RFC3168).
#
#   Processing proceeds in the order specified, and stops at first fully
#   matching line.
#
#   Note: The use of this directive using client dependent ACLs is
#   incompatible with the use of server side persistent connections. To
#   ensure correct results it is best to set server_persistent_connections
#   to off when using this directive in such configurations.
#
#Default:
# none

# TAG: clientside_tos
#   Allows you to select a TOS/Diffserv value to mark client-side
#   connections with, based on the username or source address
#   making the request.
#
#Default:
# none

# TAG: tcp_outgoing_address
#   Allows you to map requests to different outgoing IP addresses
#   based on the username or source address of the user making
#   the request.
#
#   tcp_outgoing_address ipaddr (![aclname] ...)
#
#   Example where requests from 10.0.0.0/24 will be forwarded
#   with source address 10.1.0.1, 10.0.2.0/24 forwarded with
#   source address 10.1.0.2 and the rest will be forwarded with
#   source address 10.1.0.3.
#
#   acl normal_service_net src 10.0.0.0/24
#   acl good_service_net src 10.0.2.0/24
#   tcp_outgoing_address 10.1.0.1 normal_service_net

```

```
# tcp_outgoing_address 10.1.0.2 good_service_net
# tcp_outgoing_address 10.1.0.3
#
# Processing proceeds in the order specified, and stops at first fully
# matching line.
#
# Note: The use of this directive using client dependent ACLs is
# incompatible with the use of server side persistent connections. To
# ensure correct results it is best to set server_persistent_connections
# to off when using this directive in such configurations.
#
#Default:
# none

# SSL OPTIONS
# -----
# TAG: ssl_unclean_shutdown
# Note: This option is only available if Squid is rebuilt with the
# --enable-ssl option
#
# Some browsers (especially MSIE) bugs out on SSL shutdown
# messages.
#
#Default:
# ssl_unclean_shutdown off

# TAG: ssl_engine
# Note: This option is only available if Squid is rebuilt with the
# --enable-ssl option
#
# The OpenSSL engine to use. You will need to set this if you
# would like to use hardware SSL acceleration for example.
#
#Default:
# none

# TAG: sslproxy_client_certificate
# Note: This option is only available if Squid is rebuilt with the
# --enable-ssl option
#
# Client SSL Certificate to use when proxying https:// URLs
#
#Default:
# none

# TAG: sslproxy_client_key
# Note: This option is only available if Squid is rebuilt with the
# --enable-ssl option
#
# Client SSL Key to use when proxying https:// URLs
#
#Default:
# none

# TAG: sslproxy_version
# Note: This option is only available if Squid is rebuilt with the
# --enable-ssl option
#
```

```
#      SSL version level to use when proxying https:// URLs
#
#Default:
# sslproxy_version 1

# TAG: sslproxy_options
# Note: This option is only available if Squid is rebuilt with the
#       --enable-ssl option
#
#      SSL engine options to use when proxying https:// URLs
#
#Default:
# none

# TAG: sslproxy_cipher
# Note: This option is only available if Squid is rebuilt with the
#       --enable-ssl option
#
#      SSL cipher list to use when proxying https:// URLs
#
#Default:
# none

# TAG: sslproxy_cafile
# Note: This option is only available if Squid is rebuilt with the
#       --enable-ssl option
#
#      file containing CA certificates to use when verifying server
#      certificates while proxying https:// URLs
#
#Default:
# none

# TAG: sslproxy_capath
# Note: This option is only available if Squid is rebuilt with the
#       --enable-ssl option
#
#      directory containing CA certificates to use when verifying
#      server certificates while proxying https:// URLs
#
#Default:
# none

# TAG: sslproxy_flags
# Note: This option is only available if Squid is rebuilt with the
#       --enable-ssl option
#
#      Various flags modifying the use of SSL while proxying https:// URLs:
#      DONT_VERIFY_PEER    Accept certificates even if they fail to
#                          verify.
#      NO_DEFAULT_CA       Don't use the default CA list built in
#                          to OpenSSL.
#
#Default:
# none

# TAG: sslpassword_program
# Note: This option is only available if Squid is rebuilt with the
#       --enable-ssl option
#
```



```

#       Specify a program used for entering SSL key passphrases
#       when using encrypted SSL certificate keys. If not specified
#       keys must either be unencrypted, or Squid started with the -N
#       option to allow it to query interactively for the passphrase.
#
#Default:
# none

# OPTIONS WHICH AFFECT THE NEIGHBOR SELECTION ALGORITHM
# -----

# TAG: cache_peer
#       To specify other caches in a hierarchy, use the format:
#
#           cache_peer hostname type http-port icp-port [options]
#
#       For example,
#
#           #
#           #           hostname           type      proxy  icp
#           #           -----           -
#           #           parent.foo.net     parent    3128   3130   proxy-only default
#           #           sib1.foo.net       sibling    3128   3130   proxy-only
#           #           sib2.foo.net       sibling    3128   3130   proxy-only
#
#           type:  either 'parent', 'sibling', or 'multicast'.
#
#       proxy-port:  The port number where the cache listens for proxy
#                   requests.
#
#       icp-port:   Used for querying neighbor caches about
#                   objects. To have a non-ICP neighbor
#                   specify '7' for the ICP port and make sure the
#                   neighbor machine has the UDP echo port
#                   enabled in its /etc/inetd.conf file.
#
#                   NOTE: Also requires icp_port option enabled to send/receive
#                           requests via this method.
#
#       options:   proxy-only
#                   weight=n
#                   basetime=n
#                   ttl=n
#                   no-query
#                   background-ping
#                   default
#                   round-robin
#                   weighted-round-robin
#                   carp
#                   userhash
#                   sourcehash
#                   multicast-responder
#                   closest-only
#                   no-digest
#                   no-netdb-exchange
#                   no-delay
#                   login=user:password | PASS | *:password
#                   connect-timeout=nn
#                   digest-url=url
#                   allow-miss
    
```

```
# max-conn=n
# htcp
# htcp-oldsquid
# originserver
# name=xxx
# forceddomain=name
# ssl
# sslcert=/path/to/ssl/certificate
# sslkey=/path/to/ssl/key
# sslversion=1|2|3|4
# sslcipher=...
# ssloptions=...
# front-end-https[=on|auto]
#
# use 'proxy-only' to specify objects fetched
# from this cache should not be saved locally.
#
# use 'weight=n' to affect the selection of a peer
# during any weighted peer-selection mechanisms.
# The weight must be an integer; default is 1,
# larger weights are favored more.
# This option does not affect parent selection if a peering
# protocol is not in use.
#
# use 'basetime=n' to specify a base amount to
# be subtracted from round trip times of parents.
# It is subtracted before division by weight in calculating
# which parent to fetch from. If the rtt is less than the
# base time the rtt is set to a minimal value.
#
# use 'ttl=n' to specify a IP multicast TTL to use
# when sending an ICP queries to this address.
# Only useful when sending to a multicast group.
# Because we don't accept ICP replies from random
# hosts, you must configure other group members as
# peers with the 'multicast-responder' option below.
#
# use 'no-query' to NOT send ICP queries to this
# neighbor.
#
# use 'background-ping' to only send ICP queries to this
# neighbor infrequently. This is used to keep the neighbor
# round trip time updated and is usually used in
# conjunction with weighted-round-robin.
#
# use 'default' if this is a parent cache which can
# be used as a "last-resort" if a peer cannot be located
# by any of the peer-selection mechanisms.
# If specified more than once, only the first is used.
#
# use 'round-robin' to define a set of parents which
# should be used in a round-robin fashion in the
# absence of any ICP queries.
#
# use 'weighted-round-robin' to define a set of parents
# which should be used in a round-robin fashion with the
# frequency of each parent being based on the round trip
# time. Closer parents are used more often.
# Usually used for background-ping parents.
#
```

```
#      use 'carp' to define a set of parents which should
#      be used as a CARP array. The requests will be
#      distributed among the parents based on the CARP load
#      balancing hash function based on their weight.
#
#      use 'userhash' to load-balance amongst a set of parents
#      based on the client proxy_auth or ident username.
#
#      use 'sourcehash' to load-balance amongst a set of parents
#      based on the client source ip.
#
#      'multicast-responder' indicates the named peer
#      is a member of a multicast group. ICP queries will
#      not be sent directly to the peer, but ICP replies
#      will be accepted from it.
#
#      'closest-only' indicates that, for ICP_OP_MISS
#      replies, we'll only forward CLOSEST_PARENT_MISSES
#      and never FIRST_PARENT_MISSES.
#
#      use 'no-digest' to NOT request cache digests from
#      this neighbor.
#
#      'no-netdb-exchange' disables requesting ICMP
#      RTT database (NetDB) from the neighbor.
#
#      use 'no-delay' to prevent access to this neighbor
#      from influencing the delay pools.
#
#      use 'login=user:password' if this is a personal/workgroup
#      proxy and your parent requires proxy authentication.
#      Note: The string can include URL escapes (i.e. %20 for
#      spaces). This also means % must be written as %%.
#
#      use 'login=PASS' if users must authenticate against
#      the upstream proxy or in the case of a reverse proxy
#      configuration, the origin web server. This will pass
#      the users credentials as they are to the peer.
#      This only works for the Basic HTTP authentication scheme.
#      Note: To combine this with proxy_auth both proxies must
#      share the same user database as HTTP only allows for
#      a single login (one for proxy, one for origin server).
#      Also be warned this will expose your users proxy
#      password to the peer. USE WITH CAUTION
#
#      use 'login=:password' to pass the username to the
#      upstream cache, but with a fixed password. This is meant
#      to be used when the peer is in another administrative
#      domain, but it is still needed to identify each user.
#      The star can optionally be followed by some extra
#      information which is added to the username. This can
#      be used to identify this proxy to the peer, similar to
#      the login=username:password option above.
#
#      use 'connect-timeout=nn' to specify a peer
#      specific connect timeout (also see the
#      peer_connect_timeout directive)
#
#      use 'digest-url=url' to tell Squid to fetch the cache
#      digest (if digests are enabled) for this host from
```

```
# the specified URL rather than the Squid default
# location.
#
# use 'allow-miss' to disable Squid's use of only-if-cached
# when forwarding requests to siblings. This is primarily
# useful when icp_hit_stale is used by the sibling. To
# extensive use of this option may result in forwarding
# loops, and you should avoid having two-way peerings
# with this option. (for example to deny peer usage on
# requests from peer by denying cache_peer_access if the
# source is a peer)
#
# use 'max-conn=n' to limit the amount of connections Squid
# may open to this peer.
#
# use 'htcp' to send HTCP, instead of ICP, queries
# to the neighbor. You probably also want to
# set the "icp port" to 4827 instead of 3130.
# You MUST also set htcp_access explicitly. The default of
# deny all will prevent peer traffic.
#
# use 'htcp-oldsquid' to send HTCP to old Squid versions
# You MUST also set htcp_access explicitly. The default of
# deny all will prevent peer traffic.
#
# 'originserver' causes this parent peer to be contacted as
# a origin server. Meant to be used in accelerator setups.
#
# use 'name=xxx' if you have multiple peers on the same
# host but different ports. This name can be used to
# differentiate the peers in cache_peer_access and similar
# directives.
#
# use 'forcedomain=name' to forcibly set the Host header
# of requests forwarded to this peer. Useful in accelerator
# setups where the server (peer) expects a certain domain
# name and using redirectors to feed this domain name
# is not feasible.
#
# use 'ssl' to indicate connections to this peer should
# be SSL/TLS encrypted.
#
# use 'sslcert=/path/to/ssl/certificate' to specify a client
# SSL certificate to use when connecting to this peer.
#
# use 'sslkey=/path/to/ssl/key' to specify the private SSL
# key corresponding to sslcert above. If 'sslkey' is not
# specified 'sslcert' is assumed to reference a
# combined file containing both the certificate and the key.
#
# use sslversion=1|2|3|4 to specify the SSL version to use
# when connecting to this peer
#     1 = automatic (default)
#     2 = SSL v2 only
#     3 = SSL v3 only
#     4 = TLS v1 only
#
# use sslcipher=... to specify the list of valid SSL ciphers
# to use when connecting to this peer.
#
```

```
#           use ssloptions=... to specify various SSL engine options:
#           NO_SSLv2  Disallow the use of SSLv2
#           NO_SSLv3  Disallow the use of SSLv3
#           NO_TLSv1  Disallow the use of TLSv1
#           See src/ssl_support.c or the OpenSSL documentation for
#           a more complete list.
#
#           use sslcafile=... to specify a file containing
#           additional CA certificates to use when verifying the
#           peer certificate.
#
#           use sslcapath=... to specify a directory containing
#           additional CA certificates to use when verifying the
#           peer certificate.
#
#           use sslcrlfile=... to specify a certificate revocation
#           list file to use when verifying the peer certificate.
#
#           use sslflags=... to specify various flags modifying the
#           SSL implementation:
#           DONT_VERIFY_PEER
#               Accept certificates even if they fail to
#               verify.
#           NO_DEFAULT_CA
#               Don't use the default CA list built in
#               to OpenSSL.
#           DONT_VERIFY_DOMAIN
#               Don't verify the peer certificate
#               matches the server name
#
#           use ssldomain= to specify the peer name as advertised
#           in it's certificate. Used for verifying the correctness
#           of the received peer certificate. If not specified the
#           peer hostname will be used.
#
#           use front-end-https to enable the "Front-End-Https: On"
#           header needed when using Squid as a SSL frontend in front
#           of Microsoft OWA. See MS KB document Q307347 for details
#           on this header. If set to auto the header will
#           only be added if the request is forwarded as a https://
#           URL.
#
#Default:
# none

# TAG: cache_peer_domain
#       Use to limit the domains for which a neighbor cache will be
#       queried. Usage:
#
#       cache_peer_domain cache-host domain [domain ...]
#       cache_peer_domain cache-host !domain
#
#       For example, specifying
#
#           cache_peer_domain parent.foo.net      .edu
#
#       has the effect such that UDP query packets are sent to
#       'bigserver' only when the requested object exists on a
#       server in the .edu domain. Prefixing the domainname
#       with '!' means the cache will be queried for objects
```

```

#       NOT in that domain.
#
#       NOTE:  * Any number of domains may be given for a cache-host,
#              either on the same or separate lines.
#              * When multiple domains are given for a particular
#              cache-host, the first matched domain is applied.
#              * Cache hosts with no domain restrictions are queried
#              for all requests.
#              * There are no defaults.
#              * There is also a 'cache_peer_access' tag in the ACL
#              section.
#
#Default:
# none

# TAG: cache_peer_access
#       Similar to 'cache_peer_domain' but provides more flexibility by
#       using ACL elements.
#
#       cache_peer_access cache-host allow|deny [!]aclname ...
#
#       The syntax is identical to 'http_access' and the other lists of
#       ACL elements.  See the comments for 'http_access' below, or
#       the Squid FAQ (http://www.squid-cache.org/FAQ/FAQ-10.html).
#
#Default:
# none

# TAG: neighbor_type_domain
#       usage: neighbor_type_domain neighbor parent|sibling domain domain ...
#
#       Modifying the neighbor type for specific domains is now
#       possible.  You can treat some domains differently than the the
#       default neighbor type specified on the 'cache_peer' line.
#       Normally it should only be necessary to list domains which
#       should be treated differently because the default neighbor type
#       applies for hostnames which do not match domains listed here.
#
#EXAMPLE:
#       cache_peer cache.foo.org parent 3128 3130
#       neighbor_type_domain cache.foo.org sibling .com .net
#       neighbor_type_domain cache.foo.org sibling .au .de
#
#Default:
# none

# TAG: dead_peer_timeout      (seconds)
#       This controls how long Squid waits to declare a peer cache
#       as "dead."  If there are no ICP replies received in this
#       amount of time, Squid will declare the peer dead and not
#       expect to receive any further ICP replies.  However, it
#       continues to send ICP queries, and will mark the peer as
#       alive upon receipt of the first subsequent ICP reply.
#
#       This timeout also affects when Squid expects to receive ICP
#       replies from peers.  If more than 'dead_peer' seconds have
#       passed since the last ICP reply was received, Squid will not
#       expect to receive an ICP reply on the next query.  Thus, if
#       your time between requests is greater than this timeout, you
#       will see a lot of requests sent DIRECT to origin servers

```

```
#         instead of to your parents.
#
#Default:
# dead_peer_timeout 10 seconds

# TAG: hierarchy_stoplist
#         A list of words which, if found in a URL, cause the object to
#         be handled directly by this cache.  In other words, use this
#         to not query neighbor caches for certain objects.  You may
#         list this option multiple times.
#         Note: never_direct overrides this option.
#We recommend you to use at least the following line.
#hierarchy_stoplist cgi-bin ?

# MEMORY CACHE OPTIONS
# -----

# TAG: cache_mem          (bytes)
#         NOTE: THIS PARAMETER DOES NOT SPECIFY THE MAXIMUM PROCESS SIZE.
#         IT ONLY PLACES A LIMIT ON HOW MUCH ADDITIONAL MEMORY SQUID WILL
#         USE AS A MEMORY CACHE OF OBJECTS.  SQUID USES MEMORY FOR OTHER
#         THINGS AS WELL.  SEE THE SQUID FAQ SECTION 8 FOR DETAILS.
#
#         'cache_mem' specifies the ideal amount of memory to be used
#         for:
#             * In-Transit objects
#             * Hot Objects
#             * Negative-Cached objects
#
#         Data for these objects are stored in 4 KB blocks.  This
#         parameter specifies the ideal upper limit on the total size of
#         4 KB blocks allocated.  In-Transit objects take the highest
#         priority.
#
#         In-transit objects have priority over the others.  When
#         additional space is needed for incoming data, negative-cached
#         and hot objects will be released.  In other words, the
#         negative-cached and hot objects will fill up any unused space
#         not needed for in-transit objects.
#
#         If circumstances require, this limit will be exceeded.
#         Specifically, if your incoming request rate requires more than
#         'cache_mem' of memory to hold in-transit objects, Squid will
#         exceed this limit to satisfy the new requests.  When the load
#         decreases, blocks will be freed until the high-water mark is
#         reached.  Thereafter, blocks will be used to store hot
#         objects.
#
#Default:
# cache_mem 8 MB

# TAG: maximum_object_size_in_memory  (bytes)
#         Objects greater than this size will not be attempted to kept in
#         the memory cache.  This should be set high enough to keep objects
#         accessed frequently in memory to improve performance whilst low
#         enough to keep larger objects from hoarding cache_mem.
#
#Default:
# maximum_object_size_in_memory 8 KB
```

```

# TAG: memory_replacement_policy
#   The memory replacement policy parameter determines which
#   objects are purged from memory when memory space is needed.
#
#   See cache_replacement_policy for details.
#
#Default:
# memory_replacement_policy lru

# DISK CACHE OPTIONS
# -----

# TAG: cache_replacement_policy
#   The cache replacement policy parameter determines which
#   objects are evicted (replaced) when disk space is needed.
#
#   lru          : Squid's original list based LRU policy
#   heap GDSF   : Greedy-Dual Size Frequency
#   heap LFUDA  : Least Frequently Used with Dynamic Aging
#   heap LRU    : LRU policy implemented using a heap
#
#   Applies to any cache_dir lines listed below this.
#
#   The LRU policies keeps recently referenced objects.
#
#   The heap GDSF policy optimizes object hit rate by keeping smaller
#   popular objects in cache so it has a better chance of getting a
#   hit.  It achieves a lower byte hit rate than LFUDA though since
#   it evicts larger (possibly popular) objects.
#
#   The heap LFUDA policy keeps popular objects in cache regardless of
#   their size and thus optimizes byte hit rate at the expense of
#   hit rate since one large, popular object will prevent many
#   smaller, slightly less popular objects from being cached.
#
#   Both policies utilize a dynamic aging mechanism that prevents
#   cache pollution that can otherwise occur with frequency-based
#   replacement policies.
#
#   NOTE: if using the LFUDA replacement policy you should increase
#   the value of maximum_object_size above its default of 4096 KB to
#   to maximize the potential byte hit rate improvement of LFUDA.
#
#   For more information about the GDSF and LFUDA cache replacement
#   policies see http://www.hpl.hp.com/techreports/1999/HPL-1999-69.html
#   and http://fog.hpl.external.hp.com/techreports/98/HPL-98-173.html.
#
#Default:
# cache_replacement_policy lru

# TAG: cache_dir
#   Usage:
#
#   cache_dir Type Directory-Name Fs-specific-data [options]
#
#   You can specify multiple cache_dir lines to spread the
#   cache among different disk partitions.
#

```



```
#      Type specifies the kind of storage system to use. Only "ufs"
#      is built by default. To enable any of the other storage systems
#      see the --enable-storeio configure option.
#
#      'Directory' is a top-level directory where cache swap
#      files will be stored.  If you want to use an entire disk
#      for caching, this can be the mount-point directory.
#      The directory must exist and be writable by the Squid
#      process.  Squid will NOT create this directory for you.
#
#      The ufs store type:
#
#      "ufs" is the old well-known Squid storage format that has always
#      been there.
#
#      cache_dir ufs Directory-Name Mbytes L1 L2 [options]
#
#      'Mbytes' is the amount of disk space (MB) to use under this
#      directory.  The default is 100 MB.  Change this to suit your
#      configuration.  Do NOT put the size of your disk drive here.
#      Instead, if you want Squid to use the entire disk drive,
#      subtract 20% and use that value.
#
#      'Level-1' is the number of first-level subdirectories which
#      will be created under the 'Directory'.  The default is 16.
#
#      'Level-2' is the number of second-level subdirectories which
#      will be created under each first-level directory.  The default
#      is 256.
#
#      The aufs store type:
#
#      "aufs" uses the same storage format as "ufs", utilizing
#      POSIX-threads to avoid blocking the main Squid process on
#      disk-I/O.  This was formerly known in Squid as async-io.
#
#      cache_dir aufs Directory-Name Mbytes L1 L2 [options]
#
#      see argument descriptions under ufs above
#
#      The diskd store type:
#
#      "diskd" uses the same storage format as "ufs", utilizing a
#      separate process to avoid blocking the main Squid process on
#      disk-I/O.
#
#      cache_dir diskd Directory-Name Mbytes L1 L2 [options] [Q1=n] [Q2=n]
#
#      see argument descriptions under ufs above
#
#      Q1 specifies the number of unacknowledged I/O requests when Squid
#      stops opening new files.  If this many messages are in the queues,
#      Squid won't open new files.  Default is 64
#
#      Q2 specifies the number of unacknowledged messages when Squid
#      starts blocking.  If this many messages are in the queues,
#      Squid blocks until it receives some replies.  Default is 72
#
#      When Q1 < Q2 (the default), the cache directory is optimized
#      for lower response time at the expense of a decrease in hit
```

```

#      ratio.  If Q1 > Q2, the cache directory is optimized for
#      higher hit ratio at the expense of an increase in response
#      time.
#
#      The coss store type:
#
#      block-size=n defines the "block size" for COSS cache_dir's.
#      Squid uses file numbers as block numbers.  Since file numbers
#      are limited to 24 bits, the block size determines the maximum
#      size of the COSS partition.  The default is 512 bytes, which
#      leads to a maximum cache_dir size of 512<<24, or 8 GB.  Note
#      you should not change the coss block size after Squid
#      has written some objects to the cache_dir.
#
#      The coss file store has changed from 2.5.  Now it uses a file
#      called 'stripe' in the directory names in the config - and
#      this will be created by squid -z.
#
#      The null store type:
#
#      no options are allowed or required
#
#      Common options:
#
#      no-store, no new objects should be stored to this cache_dir
#
#      max-size=n, refers to the max object size this storedir supports.
#      It is used to initially choose the storedir to dump the object.
#      Note: To make optimal use of the max-size limits you should order
#      the cache_dir lines with the smallest max-size value first and the
#      ones with no max-size specification last.
#
#      Note for coss, max-size must be less than COSS_MEMBUF_SZ,
#      which can be changed with the --with-coss-membuf-size=N configure
#      option.
#
#Default:
# cache_dir ufs /usr/local/squid/var/cache 100 16 256
#
# TAG: store_dir_select_algorithm
#      Set this to 'round-robin' as an alternative.
#
#Default:
# store_dir_select_algorithm least-load
#
# TAG: max_open_disk_fds
#      To avoid having disk as the I/O bottleneck Squid can optionally
#      bypass the on-disk cache if more than this amount of disk file
#      descriptors are open.
#
#      A value of 0 indicates no limit.
#
#Default:
# max_open_disk_fds 0
#
# TAG: minimum_object_size      (bytes)
#      Objects smaller than this size will NOT be saved on disk.  The
#      value is specified in kilobytes, and the default is 0 KB, which
#      means there is no minimum.
#

```

```
#Default:
# minimum_object_size 0 KB

# TAG: maximum_object_size      (bytes)
#   Objects larger than this size will NOT be saved on disk.  The
#   value is specified in kilobytes, and the default is 4MB.  If
#   you wish to get a high BYTES hit ratio, you should probably
#   increase this (one 32 MB object hit counts for 3200 10KB
#   hits).  If you wish to increase speed more than your want to
#   save bandwidth you should leave this low.
#
#   NOTE: if using the LFUDA replacement policy you should increase
#   this value to maximize the byte hit rate improvement of LFUDA!
#   See replacement_policy below for a discussion of this policy.
#
#Default:
# maximum_object_size 4096 KB

# TAG: cache_swap_low  (percent, 0-100)
# TAG: cache_swap_high (percent, 0-100)
#
#   The low- and high-water marks for cache object replacement.
#   Replacement begins when the swap (disk) usage is above the
#   low-water mark and attempts to maintain utilization near the
#   low-water mark.  As swap utilization gets close to high-water
#   mark object eviction becomes more aggressive.  If utilization is
#   close to the low-water mark less replacement is done each time.
#
#   Defaults are 90% and 95%.  If you have a large cache, 5% could be
#   hundreds of MB.  If this is the case you may wish to set these
#   numbers closer together.
#
#Default:
# cache_swap_low 90
# cache_swap_high 95

# LOGFILE OPTIONS
# -----

# TAG: logformat
#   Usage:
#
#   logformat <name> <format specification>
#
#   Defines an access log format.
#
#   The <format specification> is a string with embedded % format codes
#
#   % format codes all follow the same basic structure where all but
#   the formatcode is optional.  Output strings are automatically escaped
#   as required according to their context and the output format
#   modifiers are usually not needed, but can be specified if an explicit
#   output format is desired.
#
#       % ["|[]'|#] [-] [[0]width] [{argument}] formatcode
#
#       "      output in quoted string format
#       [      output in squid text log format as used by log_mime_hdrs
#       #      output in URL quoted format
```

```

#           '           output as-is
#
#           -           left aligned
#           width       field width. If starting with 0 the
#                       output is zero padded
#           {arg}       argument such as header name etc
#
# Format codes:
#
#           >a           Client source IP address
#           >A           Client FQDN
#           >p           Client source port
#           <A           Server IP address or peer name
#           la           Local IP address (http_port)
#           lp           Local port number (http_port)
#           ts           Seconds since epoch
#           tu           subsecond time (milliseconds)
#           tl           Local time. Optional strftime format argument
#                       default %d/%b/%Y:%H:%M:%S %z
#           tg           GMT time. Optional strftime format argument
#                       default %d/%b/%Y:%H:%M:%S %z
#           tr           Response time (milliseconds)
#           >h           Request header. Optional header name argument
#                       on the format header[:[separator]element]
#           <h           Reply header. Optional header name argument
#                       as for >h
#           un           User name
#           ul           User name from authentication
#           ui           User name from ident
#           us           User name from SSL
#           ue           User name from external acl helper
#           Hs           HTTP status code
#           Ss           Squid request status (TCP_MISS etc)
#           Sh           Squid hierarchy status (DEFAULT_PARENT etc)
#           mt           MIME content type
#           rm           Request method (GET/POST etc)
#           ru           Request URL
#           rp           Request URL-Path excluding hostname
#           rv           Request protocol version
#           et           Tag returned by external acl
#           ea           Log string returned by external acl
#           <st         Reply size including HTTP headers
#           >st         Request size including HTTP headers
#           st           Request+Reply size including HTTP headers
#           <sH         Reply high offset sent
#           <sS         Upstream object size
#           %           a literal % character
#
#           The default formats available (which do not need re-defining) are:
#
#logformat squid %ts.%03tu %6tr %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt
#logformat squidmime %ts.%03tu %6tr %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt [%>h] [%<h]
#logformat common %>a %ui %un [%tl] "%rm %ru HTTP/%rv" %Hs %<st %Ss:%Sh
#logformat combined %>a %ui %un [%tl] "%rm %ru HTTP/%rv" %Hs %<st "%{Referer}>h" "%{User-Agent}>h" %Ss:%
#
#Default:
# none
#
# TAG: access_log
#           These files log client request activities. Has a line every HTTP or

```

```
# ICP request. The format is:
# access_log <filepath> [<logformat name> [acl acl ...]]
# access_log none [acl acl ...]]
#
# Will log to the specified file using the specified format (which
# must be defined in a logformat directive) those entries which match
# ALL the acl's specified (which must be defined in acl clauses).
# If no acl is specified, all requests will be logged to this file.
#
# To disable logging of a request use the filepath "none", in which case
# a logformat name should not be specified.
#
# To log the request via syslog specify a filepath of "syslog":
#
# access_log syslog[:facility.priority] [format [acl1 [acl2 ...]]]
# where facility could be any of:
# authpriv, daemon, local0 .. local7 or user.
#
# And priority could be any of:
# err, warning, notice, info, debug.
#access_log /usr/local/squid/var/logs/access.log squid

# TAG: log_access allow|deny acl acl...
# This options allows you to control which requests gets logged
# to access.log (see access_log directive). Requests denied for
# logging will also not be accounted for in performance counters.
#
#Default:
# none

# TAG: cache_log
# Cache logging file. This is where general information about
# your cache's behavior goes. You can increase the amount of data
# logged to this file with the "debug_options" tag below.
#
#Default:
# cache_log /usr/local/squid/var/logs/cache.log

# TAG: cache_store_log
# Logs the activities of the storage manager. Shows which
# objects are ejected from the cache, and which objects are
# saved and for how long. To disable, enter "none". There are
# not really utilities to analyze this data, so you can safely
# disable it.
#
#Default:
# cache_store_log /usr/local/squid/var/logs/store.log

# TAG: cache_swap_state
# Location for the cache "swap.state" file. This index file holds
# the metadata of objects saved on disk. It is used to rebuild
# the cache during startup. Normally this file resides in each
# 'cache_dir' directory, but you may specify an alternate
# pathname here. Note you must give a full filename, not just
# a directory. Since this is the index for the whole object
# list you CANNOT periodically rotate it!
#
# If %s can be used in the file name it will be replaced with a
# a representation of the cache_dir name where each / is replaced
# with '.'. This is needed to allow adding/removing cache_dir
```

```

#       lines when cache_swap_log is being used.
#
#       If have more than one 'cache_dir', and %s is not used in the name
#       these swap logs will have names such as:
#
#           cache_swap_log.00
#           cache_swap_log.01
#           cache_swap_log.02
#
#       The numbered extension (which is added automatically)
#       corresponds to the order of the 'cache_dir' lines in this
#       configuration file.  If you change the order of the 'cache_dir'
#       lines in this file, these index files will NOT correspond to
#       the correct 'cache_dir' entry (unless you manually rename
#       them).  We recommend you do NOT use this option.  It is
#       better to keep these index files in each 'cache_dir' directory.
#
#Default:
# none

# TAG: logfile_rotate
#       Specifies the number of logfile rotations to make when you
#       type 'squid -k rotate'.  The default is 10, which will rotate
#       with extensions 0 through 9.  Setting logfile_rotate to 0 will
#       disable the file name rotation, but the logfiles are still closed
#       and re-opened.  This will enable you to rename the logfiles
#       yourself just before sending the rotate signal.
#
#       Note, the 'squid -k rotate' command normally sends a USR1
#       signal to the running squid process.  In certain situations
#       (e.g. on Linux with Async I/O), USR1 is used for other
#       purposes, so -k rotate uses another signal.  It is best to get
#       in the habit of using 'squid -k rotate' instead of 'kill -USR1
#       <pid>'.
#
#Default:
# logfile_rotate 10

# TAG: emulate_httpd_log      on|off
#       The Cache can emulate the log file format which many 'httpd'
#       programs use.  To disable/enable this emulation, set
#       emulate_httpd_log to 'off' or 'on'.  The default
#       is to use the native log format since it includes useful
#       information Squid-specific log analyzers use.
#
#Default:
# emulate_httpd_log off

# TAG: log_ip_on_direct      on|off
#       Log the destination IP address in the hierarchy log tag when going
#       direct.  Earlier Squid versions logged the hostname here.  If you
#       prefer the old way set this to off.
#
#Default:
# log_ip_on_direct on

# TAG: mime_table
#       Pathname to Squid's MIME table.  You shouldn't need to change
#       this, but the default file contains examples and formatting
#       information if you do.

```

```
#
#Default:
# mime_table /usr/local/squid/etc/mime.conf

# TAG: log_mime_hdrs on|off
# The Cache can record both the request and the response MIME
# headers for each HTTP transaction. The headers are encoded
# safely and will appear as two bracketed fields at the end of
# the access log (for either the native or httpd-emulated log
# formats). To enable this logging set log_mime_hdrs to 'on'.
#
#Default:
# log_mime_hdrs off

# TAG: useragent_log
# Note: This option is only available if Squid is rebuilt with the
# --enable-useragent-log option
#
# Squid will write the User-Agent field from HTTP requests
# to the filename specified here. By default useragent_log
# is disabled.
#
#Default:
# none

# TAG: referer_log
# Note: This option is only available if Squid is rebuilt with the
# --enable-referer-log option
#
# Squid will write the Referer field from HTTP requests to the
# filename specified here. By default referer_log is disabled.
# Note that "referer" is actually a misspelling of "referrer"
# however the misspelt version has been accepted into the HTTP RFCs
# and we accept both.
#
#Default:
# none

# TAG: pid_filename
# A filename to write the process-id to. To disable, enter "none".
#
#Default:
# pid_filename /usr/local/squid/var/logs/squid.pid

# TAG: debug_options
# Logging options are set as section,level where each source file
# is assigned a unique section. Lower levels result in less
# output, Full debugging (level 9) can result in a very large
# log file, so be careful. The magic word "ALL" sets debugging
# levels for all sections. We recommend normally running with
# "ALL,1".
#
#Default:
# debug_options ALL,1

# TAG: log_fqdn on|off
# Turn this on if you wish to log fully qualified domain names
# in the access.log. To do this Squid does a DNS lookup of all
# IP's connecting to it. This can (in some situations) increase
# latency, which makes your cache seem slower for interactive
```

```

#      browsing.
#
#Default:
# log_fqdn off

# TAG: client_netmask
#      A netmask for client addresses in logfiles and cachemgr output.
#      Change this to protect the privacy of your cache clients.
#      A netmask of 255.255.255.0 will log all IP's in that range with
#      the last digit set to '0'.
#
#Default:
# client_netmask 255.255.255.255

# TAG: forward_log
# Note: This option is only available if Squid is rebuilt with the
#       -DWIP_FWD_LOG define
#
#       Logs the server-side requests.
#
#       This is currently work in progress.
#
#Default:
# none

# TAG: strip_query_terms
#       By default, Squid strips query terms from requested URLs before
#       logging. This protects your user's privacy.
#
#Default:
# strip_query_terms on

# TAG: buffered_logs  on|off
#       cache.log log file is written with stdio functions, and as such
#       it can be buffered or unbuffered. By default it will be unbuffered.
#       Buffering it can speed up the writing slightly (though you are
#       unlikely to need to worry unless you run with tons of debugging
#       enabled in which case performance will suffer badly anyway..).
#
#Default:
# buffered_logs off

# OPTIONS FOR FTP GATEWAYING
# -----

# TAG: ftp_user
#       If you want the anonymous login password to be more informative
#       (and enable the use of picky ftp servers), set this to something
#       reasonable for your domain, like wwwuser@somewhere.net
#
#       The reason why this is domainless by default is the
#       request can be made on the behalf of a user in any domain,
#       depending on how the cache is used.
#       Some ftp server also validate the email address is valid
#       (for example perl.com).
#
#Default:
# ftp_user Squid@

```



```
# TAG: ftp_list_width
#     Sets the width of ftp listings. This should be set to fit in
#     the width of a standard browser. Setting this too small
#     can cut off long filenames when browsing ftp sites.
#
#Default:
# ftp_list_width 32

# TAG: ftp_passive
#     If your firewall does not allow Squid to use passive
#     connections, turn off this option.
#
#Default:
# ftp_passive on

# TAG: ftp_sanitycheck
#     For security and data integrity reasons Squid by default performs
#     sanity checks of the addresses of FTP data connections ensure the
#     data connection is to the requested server. If you need to allow
#     FTP connections to servers using another IP address for the data
#     connection turn this off.
#
#Default:
# ftp_sanitycheck on

# TAG: ftp_telnet_protocol
#     The FTP protocol is officially defined to use the telnet protocol
#     as transport channel for the control connection. However, many
#     implementations are broken and does not respect this aspect of
#     the FTP protocol.
#
#     If you have trouble accessing files with ASCII code 255 in the
#     path or similar problems involving this ASCII code you can
#     try setting this directive to off. If that helps, report to the
#     operator of the FTP server in question that their FTP server
#     is broken and does not follow the FTP standard.
#
#Default:
# ftp_telnet_protocol on

# OPTIONS FOR EXTERNAL SUPPORT PROGRAMS
# -----

# TAG: diskd_program
#     Specify the location of the diskd executable.
#     Note this is only useful if you have compiled in
#     diskd as one of the store io modules.
#
#Default:
# diskd_program /usr/local/squid/libexec/diskd

# TAG: unlinkd_program
#     Specify the location of the executable for file deletion process.
#
#Default:
# unlinkd_program /usr/local/squid/libexec/unlinkd

# TAG: pinger_program
# Note: This option is only available if Squid is rebuilt with the
```

```

#      --enable-icmp option
#
#      Specify the location of the executable for the pinger process.
#
#Default:
# pinger_program /usr/local/squid/libexec/pinger

# OPTIONS FOR URL REWRITING
# -----

# TAG: url_rewrite_program
#      Specify the location of the executable for the URL rewriter.
#      Since they can perform almost any function there isn't one included.
#
#      For each requested URL rewriter will receive on line with the format
#
#      URL <SP> client_ip "/" fqdn <SP> user <SP> method [<SP> kvpairs]<NL>
#
#      In the future, the rewriter interface will be extended with
#      key=value pairs ("kvpairs" shown above).  Rewriter programs
#      should be prepared to receive and possibly ignore additional
#      whitespace-separated tokens on each input line.
#
#      And the rewriter may return a rewritten URL.  The other components of
#      the request line does not need to be returned (ignored if they are).
#
#      The rewriter can also indicate that a client-side redirect should
#      be performed to the new URL.  This is done by prefixing the returned
#      URL with "301:" (moved permanently) or 302: (moved temporarily).
#
#      By default, a URL rewriter is not used.
#
#Default:
# none

# TAG: url_rewrite_children
#      The number of redirector processes to spawn.  If you start
#      too few Squid will have to wait for them to process a backlog of
#      URLs, slowing it down.  If you start too many they will use RAM
#      and other system resources.
#
#Default:
# url_rewrite_children 5

# TAG: url_rewrite_concurrency
#      The number of requests each redirector helper can handle in
#      parallel.  Defaults to 0 which indicates the redirector
#      is a old-style single threaded redirector.
#
#Default:
# url_rewrite_concurrency 0

# TAG: url_rewrite_host_header
#      By default Squid rewrites any Host: header in redirected
#      requests.  If you are running an accelerator this may
#      not be a wanted effect of a redirector.
#
#      WARNING: Entries are cached on the result of the URL rewriting
#      process, so be careful if you have domain-virtual hosts.

```

```
#
#Default:
# url_rewrite_host_header on

# TAG: url_rewrite_access
#     If defined, this access list specifies which requests are
#     sent to the redirector processes. By default all requests
#     are sent.
#
#Default:
# none

# TAG: url_rewrite_bypass
#     When this is 'on', a request will not go through the
#     redirector if all redirectors are busy. If this is 'off'
#     and the redirector queue grows too large, Squid will exit
#     with a FATAL error and ask you to increase the number of
#     redirectors. You should only enable this if the redirectors
#     are not critical to your caching system. If you use
#     redirectors for access control, and you enable this option,
#     users may have access to pages they should not
#     be allowed to request.
#
#Default:
# url_rewrite_bypass off

# OPTIONS FOR TUNING THE CACHE
# -----

# TAG: cache
#     A list of ACL elements which, if matched and denied, cause the request to
#     not be satisfied from the cache and the reply to not be cached.
#     In other words, use this to force certain objects to never be cached.
#
#     You must use the words 'allow' or 'deny' to indicate whether items
#     matching the ACL should be allowed or denied into the cache.
#
#     Default is to allow all to be cached
#
#Default:
# none

# TAG: refresh_pattern
#     usage: refresh_pattern [-i] regex min percent max [options]
#
#     By default, regular expressions are CASE-SENSITIVE. To make
#     them case-insensitive, use the -i option.
#
#     'Min' is the time (in minutes) an object without an explicit
#     expiry time should be considered fresh. The recommended
#     value is 0, any higher values may cause dynamic applications
#     to be erroneously cached unless the application designer
#     has taken the appropriate actions.
#
#     'Percent' is a percentage of the objects age (time since last
#     modification age) an object without explicit expiry time
#     will be considered fresh.
#
#     'Max' is an upper limit on how long objects without an explicit
```

```
#      expiry time will be considered fresh.
#
#      options: override-expire
#                override-lastmod
#                reload-into-ims
#                ignore-reload
#                ignore-no-cache
#                ignore-no-store
#                ignore-private
#                ignore-auth
#                refresh-ims
#
#      override-expire enforces min age even if the server
#      sent an explicit expiry time (e.g., with the
#      Expires: header or Cache-Control: max-age). Doing this
#      VIOLATES the HTTP standard. Enabling this feature
#      could make you liable for problems which it causes.
#
#      override-lastmod enforces min age even on objects
#      that were modified recently.
#
#      reload-into-ims changes client no-cache or ``reload''
#      to If-Modified-Since requests. Doing this VIOLATES the
#      HTTP standard. Enabling this feature could make you
#      liable for problems which it causes.
#
#      ignore-reload ignores a client no-cache or ``reload''
#      header. Doing this VIOLATES the HTTP standard. Enabling
#      this feature could make you liable for problems which
#      it causes.
#
#      ignore-no-cache ignores any ``Pragma: no-cache'' and
#      ``Cache-control: no-cache'' headers received from a server.
#      The HTTP RFC never allows the use of this (Pragma) header
#      from a server, only a client, though plenty of servers
#      send it anyway.
#
#      ignore-no-store ignores any ``Cache-control: no-store''
#      headers received from a server. Doing this VIOLATES
#      the HTTP standard. Enabling this feature could make you
#      liable for problems which it causes.
#
#      ignore-private ignores any ``Cache-control: private''
#      headers received from a server. Doing this VIOLATES
#      the HTTP standard. Enabling this feature could make you
#      liable for problems which it causes.
#
#      ignore-auth caches responses to requests with authorization,
#      as if the originserver had sent ``Cache-control: public''
#      in the response header. Doing this VIOLATES the HTTP standard.
#      Enabling this feature could make you liable for problems which
#      it causes.
#
#      refresh-ims causes squid to contact the origin server
#      when a client issues an If-Modified-Since request. This
#      ensures that the client will receive an updated version
#      if one is available.
#
#      Basically a cached object is:
#
```

```
#           FRESH if expires < now, else STALE
#           STALE if age > max
#           FRESH if lm-factor < percent, else STALE
#           FRESH if age < min
#           else STALE
#
# The refresh_pattern lines are checked in the order listed here.
# The first entry which matches is used.  If none of the entries
# match the default will be used.
#
# Note, you must uncomment all the default lines if you want
# to change one. The default setting is only active if none is
# used.
#
#Suggested default:
#refresh_pattern ^ftp:          1440      20%      10080
#refresh_pattern ^gopher:      1440      0%       1440
#refresh_pattern (cgi-bin|\/?)  0         0%       0
#refresh_pattern .              0         20%     4320
#
# TAG: quick_abort_min (KB)
# TAG: quick_abort_max (KB)
# TAG: quick_abort_pct (percent)
# The cache by default continues downloading aborted requests
# which are almost completed (less than 16 KB remaining). This
# may be undesirable on slow (e.g. SLIP) links and/or very busy
# caches.  Impatient users may tie up file descriptors and
# bandwidth by repeatedly requesting and immediately aborting
# downloads.
#
# When the user aborts a request, Squid will check the
# quick_abort values to the amount of data transfered until
# then.
#
# If the transfer has less than 'quick_abort_min' KB remaining,
# it will finish the retrieval.
#
# If the transfer has more than 'quick_abort_max' KB remaining,
# it will abort the retrieval.
#
# If more than 'quick_abort_pct' of the transfer has completed,
# it will finish the retrieval.
#
# If you do not want any retrieval to continue after the client
# has aborted, set both 'quick_abort_min' and 'quick_abort_max'
# to '0 KB'.
#
# If you want retrievals to always continue if they are being
# cached set 'quick_abort_min' to '-1 KB'.
#
#Default:
# quick_abort_min 16 KB
# quick_abort_max 16 KB
# quick_abort_pct 95
#
# TAG: read_ahead_gap  buffer-size
# The amount of data the cache will buffer ahead of what has been
# sent to the client when retrieving an object from another server.
#
#Default:
```

```
# read_ahead_gap 16 KB

# TAG: negative_ttl      time-units
#   Time-to-Live (TTL) for failed requests.  Certain types of
#   failures (such as "connection refused" and "404 Not Found") are
#   negatively-cached for a configurable amount of time.  The
#   default is 5 minutes.  Note that this is different from
#   negative caching of DNS lookups.
#
#   WARNING: Doing this VIOLATES the HTTP standard.  Enabling
#   this feature could make you liable for problems which it
#   causes.
#
#Default:
# negative_ttl 5 minutes

# TAG: positive_dns_ttl  time-units
#   Upper limit on how long Squid will cache positive DNS responses.
#   Default is 6 hours (360 minutes).  This directive must be set
#   larger than negative_dns_ttl.
#
#Default:
# positive_dns_ttl 6 hours

# TAG: negative_dns_ttl  time-units
#   Time-to-Live (TTL) for negative caching of failed DNS lookups.
#   This also sets the lower cache limit on positive lookups.
#   Minimum value is 1 second, and it is not recommendable to go
#   much below 10 seconds.
#
#Default:
# negative_dns_ttl 1 minutes

# TAG: range_offset_limit (bytes)
#   Sets a upper limit on how far into the the file a Range request
#   may be to cause Squid to prefetch the whole file.  If beyond this
#   limit Squid forwards the Range request as it is and the result
#   is NOT cached.
#
#   This is to stop a far ahead range request (lets say start at 17MB)
#   from making Squid fetch the whole object up to that point before
#   sending anything to the client.
#
#   A value of -1 causes Squid to always fetch the object from the
#   beginning so it may cache the result.  (2.0 style)
#
#   A value of 0 causes Squid to never fetch more than the
#   client requested.  (default)
#
#Default:
# range_offset_limit 0 KB

# TAG: minimum_expiry_time (seconds)
#   The minimum caching time according to (Expires - Date)
#   Headers Squid honors if the object can't be revalidated
#   defaults to 60 seconds.  In reverse proxy environments it
#   might be desirable to honor shorter object lifetimes.  It
#   is most likely better to make your server return a
#   meaningful Last-Modified header however.  In ESI environments
#   where page fragments often have short lifetimes, this will
```

```
#         often be best set to 0.
#
#Default:
# minimum_expiry_time 60 seconds

# TAG: store_avg_object_size    (kbytes)
#         Average object size, used to estimate number of objects your
#         cache can hold.  The default is 13 KB.
#
#Default:
# store_avg_object_size 13 KB

# TAG: store_objects_per_bucket
#         Target number of objects per bucket in the store hash table.
#         Lowering this value increases the total number of buckets and
#         also the storage maintenance rate.  The default is 20.
#
#Default:
# store_objects_per_bucket 20

# HTTP OPTIONS
# -----

# TAG: request_header_max_size (KB)
#         This specifies the maximum size for HTTP headers in a request.
#         Request headers are usually relatively small (about 512 bytes).
#         Placing a limit on the request header size will catch certain
#         bugs (for example with persistent connections) and possibly
#         buffer-overflow or denial-of-service attacks.
#
#Default:
# request_header_max_size 20 KB

# TAG: reply_header_max_size   (KB)
#         This specifies the maximum size for HTTP headers in a reply.
#         Reply headers are usually relatively small (about 512 bytes).
#         Placing a limit on the reply header size will catch certain
#         bugs (for example with persistent connections) and possibly
#         buffer-overflow or denial-of-service attacks.
#
#Default:
# reply_header_max_size 20 KB

# TAG: request_body_max_size   (bytes)
#         This specifies the maximum size for an HTTP request body.
#         In other words, the maximum size of a PUT/POST request.
#         A user who attempts to send a request with a body larger
#         than this limit receives an "Invalid Request" error message.
#         If you set this parameter to a zero (the default), there will
#         be no limit imposed.
#
#Default:
# request_body_max_size 0 KB

# TAG: broken_posts
#         A list of ACL elements which, if matched, causes Squid to send
#         an extra CRLF pair after the body of a PUT/POST request.
#
#         Some HTTP servers has broken implementations of PUT/POST,
```

```
# and rely on an extra CRLF pair sent by some WWW clients.
#
# Quote from RFC2616 section 4.1 on this matter:
#
# Note: certain buggy HTTP/1.0 client implementations generate an
# extra CRLF's after a POST request. To restate what is explicitly
# forbidden by the BNF, an HTTP/1.1 client must not preface or follow
# a request with an extra CRLF.
#
#Example:
# acl buggy_server url_regex ^http://....
# broken_posts allow buggy_server
#
#Default:
# none

# TAG: via on|off
# If set (default), Squid will include a Via header in requests and
# replies as required by RFC2616.
#
#Default:
# via on

# TAG: ie_refresh on|off
# Microsoft Internet Explorer up until version 5.5 Service
# Pack 1 has an issue with transparent proxies, wherein it
# is impossible to force a refresh. Turning this on provides
# a partial fix to the problem, by causing all IMS-REFRESH
# requests from older IE versions to check the origin server
# for fresh content. This reduces hit ratio by some amount
# (~10% in my experience), but allows users to actually get
# fresh content when they want it. Note because Squid
# cannot tell if the user is using 5.5 or 5.5SP1, the behavior
# of 5.5 is unchanged from old versions of Squid (i.e. a
# forced refresh is impossible). Newer versions of IE will,
# hopefully, continue to have the new behavior and will be
# handled based on that assumption. This option defaults to
# the old Squid behavior, which is better for hit ratios but
# worse for clients using IE, if they need to be able to
# force fresh content.
#
#Default:
# ie_refresh off

# TAG: vary_ignore_expire on|off
# Many HTTP servers supporting Vary gives such objects
# immediate expiry time with no cache-control header
# when requested by a HTTP/1.0 client. This option
# enables Squid to ignore such expiry times until
# HTTP/1.1 is fully implemented.
# WARNING: This may eventually cause some varying
# objects not intended for caching to get cached.
#
#Default:
# vary_ignore_expire off

# TAG: extension_methods
# Squid only knows about standardized HTTP request methods.
# You can add up to 20 additional "extension" methods here.
#
```



```
#Default:
# none

# TAG: request_entities
# Squid defaults to deny GET and HEAD requests with request entities,
# as the meaning of such requests are undefined in the HTTP standard
# even if not explicitly forbidden.
#
# Set this directive to on if you have clients which insists
# on sending request entities in GET or HEAD requests. But be warned
# that there is server software (both proxies and web servers) which
# can fail to properly process this kind of request which may make you
# vulnerable to cache pollution attacks if enabled.
#
#Default:
# request_entities off

# TAG: request_header_access
# Usage: request_header_access header_name allow|deny [!]aclname ...
#
# WARNING: Doing this VIOLATES the HTTP standard. Enabling
# this feature could make you liable for problems which it
# causes.
#
# This option replaces the old 'anonymize_headers' and the
# older 'http_anonymizer' option with something that is much
# more configurable. This new method creates a list of ACLs
# for each header, allowing you very fine-tuned header
# mangling.
#
# This option only applies to request headers, i.e., from the
# client to the server.
#
# You can only specify known headers for the header name.
# Other headers are reclassified as 'Other'. You can also
# refer to all the headers with 'All'.
#
# For example, to achieve the same behavior as the old
# 'http_anonymizer standard' option, you should use:
#
#     request_header_access From deny all
#     request_header_access Referer deny all
#     request_header_access Server deny all
#     request_header_access User-Agent deny all
#     request_header_access WWW-Authenticate deny all
#     request_header_access Link deny all
#
# Or, to reproduce the old 'http_anonymizer paranoid' feature
# you should use:
#
#     request_header_access Allow allow all
#     request_header_access Authorization allow all
#     request_header_access WWW-Authenticate allow all
#     request_header_access Proxy-Authorization allow all
#     request_header_access Proxy-Authenticate allow all
#     request_header_access Cache-Control allow all
#     request_header_access Content-Encoding allow all
#     request_header_access Content-Length allow all
#     request_header_access Content-Type allow all
#     request_header_access Date allow all
```

```

#         request_header_access Expires allow all
#         request_header_access Host allow all
#         request_header_access If-Modified-Since allow all
#         request_header_access Last-Modified allow all
#         request_header_access Location allow all
#         request_header_access Pragma allow all
#         request_header_access Accept allow all
#         request_header_access Accept-Charset allow all
#         request_header_access Accept-Encoding allow all
#         request_header_access Accept-Language allow all
#         request_header_access Content-Language allow all
#         request_header_access Mime-Version allow all
#         request_header_access Retry-After allow all
#         request_header_access Title allow all
#         request_header_access Connection allow all
#         request_header_access Proxy-Connection allow all
#         request_header_access All deny all
#
#         although many of those are HTTP reply headers, and so should be
#         controlled with the reply_header_access directive.
#
#         By default, all headers are allowed (no anonymizing is
#         performed).
#
#Default:
# none
#
# TAG: reply_header_access
# Usage: reply_header_access header_name allow|deny [!]aclname ...
#
# WARNING: Doing this VIOLATES the HTTP standard.  Enabling
# this feature could make you liable for problems which it
# causes.
#
# This option only applies to reply headers, i.e., from the
# server to the client.
#
# This is the same as request_header_access, but in the other
# direction.
#
# This option replaces the old 'anonymize_headers' and the
# older 'http_anonymizer' option with something that is much
# more configurable.  This new method creates a list of ACLs
# for each header, allowing you very fine-tuned header
# mangling.
#
# You can only specify known headers for the header name.
# Other headers are reclassified as 'Other'.  You can also
# refer to all the headers with 'All'.
#
# For example, to achieve the same behavior as the old
# 'http_anonymizer standard' option, you should use:
#
#         reply_header_access From deny all
#         reply_header_access Referer deny all
#         reply_header_access Server deny all
#         reply_header_access User-Agent deny all
#         reply_header_access WWW-Authenticate deny all
#         reply_header_access Link deny all
#

```

```
#      Or, to reproduce the old 'http_anonymizer paranoid' feature
#      you should use:
#
#          reply_header_access Allow allow all
#          reply_header_access Authorization allow all
#          reply_header_access WWW-Authenticate allow all
#          reply_header_access Proxy-Authorization allow all
#          reply_header_access Proxy-Authenticate allow all
#          reply_header_access Cache-Control allow all
#          reply_header_access Content-Encoding allow all
#          reply_header_access Content-Length allow all
#          reply_header_access Content-Type allow all
#          reply_header_access Date allow all
#          reply_header_access Expires allow all
#          reply_header_access Host allow all
#          reply_header_access If-Modified-Since allow all
#          reply_header_access Last-Modified allow all
#          reply_header_access Location allow all
#          reply_header_access Pragma allow all
#          reply_header_access Accept allow all
#          reply_header_access Accept-Charset allow all
#          reply_header_access Accept-Encoding allow all
#          reply_header_access Accept-Language allow all
#          reply_header_access Content-Language allow all
#          reply_header_access Mime-Version allow all
#          reply_header_access Retry-After allow all
#          reply_header_access Title allow all
#          reply_header_access Connection allow all
#          reply_header_access Proxy-Connection allow all
#          reply_header_access All deny all
#
#      although the HTTP request headers won't be usefully controlled
#      by this directive -- see request_header_access for details.
#
#      By default, all headers are allowed (no anonymizing is
#      performed).
#
#Default:
# none
#
# TAG: header_replace
#      Usage:   header_replace header_name message
#      Example: header_replace User-Agent Nutscape/1.0 (CP/M; 8-bit)
#
#      This option allows you to change the contents of headers
#      denied with header_access above, by replacing them with
#      some fixed string. This replaces the old fake_user_agent
#      option.
#
#      This only applies to request headers, not reply headers.
#
#      By default, headers are removed if denied.
#
#Default:
# none
#
# TAG: relaxed_header_parser   on|off|warn
#      In the default "on" setting Squid accepts certain forms
#      of non-compliant HTTP messages where it is unambiguous
#      what the sending application intended even if the message
```

```

#      is not correctly formatted. The messages is then normalized
#      to the correct form when forwarded by Squid.
#
#      If set to "warn" then a warning will be emitted in cache.log
#      each time such HTTP error is encountered.
#
#      If set to "off" then such HTTP errors will cause the request
#      or response to be rejected.
#
#Default:
# relaxed_header_parser on

# TIMEOUTS
# -----

# TAG: forward_timeout time-units
#      This parameter specifies how long Squid should at most attempt in
#      finding a forwarding path for the request before giving up.
#
#Default:
# forward_timeout 4 minutes

# TAG: connect_timeout time-units
#      This parameter specifies how long to wait for the TCP connect to
#      the requested server or peer to complete before Squid should
#      attempt to find another path where to forward the request.
#
#Default:
# connect_timeout 1 minute

# TAG: peer_connect_timeout time-units
#      This parameter specifies how long to wait for a pending TCP
#      connection to a peer cache. The default is 30 seconds. You
#      may also set different timeout values for individual neighbors
#      with the 'connect-timeout' option on a 'cache_peer' line.
#
#Default:
# peer_connect_timeout 30 seconds

# TAG: read_timeout time-units
#      The read_timeout is applied on server-side connections. After
#      each successful read(), the timeout will be extended by this
#      amount. If no data is read again after this amount of time,
#      the request is aborted and logged with ERR_READ_TIMEOUT. The
#      default is 15 minutes.
#
#Default:
# read_timeout 15 minutes

# TAG: request_timeout
#      How long to wait for an HTTP request after initial
#      connection establishment.
#
#Default:
# request_timeout 5 minutes

# TAG: persistent_request_timeout
#      How long to wait for the next HTTP request on a persistent
#      connection after the previous request completes.

```

```
#
#Default:
# persistent_request_timeout 2 minutes

# TAG: client_lifetime time-units
#     The maximum amount of time a client (browser) is allowed to
#     remain connected to the cache process.  This protects the Cache
#     from having a lot of sockets (and hence file descriptors) tied up
#     in a CLOSE_WAIT state from remote clients that go away without
#     properly shutting down (either because of a network failure or
#     because of a poor client implementation).  The default is one
#     day, 1440 minutes.
#
#     NOTE:  The default value is intended to be much larger than any
#     client would ever need to be connected to your cache.  You
#     should probably change client_lifetime only as a last resort.
#     If you seem to have many client connections tying up
#     filedescriptors, we recommend first tuning the read_timeout,
#     request_timeout, persistent_request_timeout and quick_abort values.
#
#Default:
# client_lifetime 1 day

# TAG: half_closed_clients
#     Some clients may shutdown the sending side of their TCP
#     connections, while leaving their receiving sides open.  Sometimes,
#     Squid can not tell the difference between a half-closed and a
#     fully-closed TCP connection.  By default, half-closed client
#     connections are kept open until a read(2) or write(2) on the
#     socket returns an error.  Change this option to 'off' and Squid
#     will immediately close client connections when read(2) returns
#     "no more data to read."
#
#Default:
# half_closed_clients on

# TAG: pconn_timeout
#     Timeout for idle persistent connections to servers and other
#     proxies.
#
#Default:
# pconn_timeout 1 minute

# TAG: ident_timeout
#     Maximum time to wait for IDENT lookups to complete.
#
#     If this is too high, and you enabled IDENT lookups from untrusted
#     users, you might be susceptible to denial-of-service by having
#     many ident requests going at once.
#
#Default:
# ident_timeout 10 seconds

# TAG: shutdown_lifetime      time-units
#     When SIGTERM or SIGHUP is received, the cache is put into
#     "shutdown pending" mode until all active sockets are closed.
#     This value is the lifetime to set for all open descriptors
#     during shutdown mode.  Any active clients after this many
#     seconds will receive a 'timeout' message.
#
```

```

#Default:
# shutdown_lifetime 30 seconds

# ADMINISTRATIVE PARAMETERS
# -----

# TAG: cache_mgr
#     Email-address of local cache manager who will receive
#     mail if the cache dies.  The default is "webmaster."
#
#Default:
# cache_mgr webmaster

# TAG: mail_from
#     From: email-address for mail sent when the cache dies.
#     The default is to use 'appname@unique_hostname'.
#     Default appname value is "squid", can be changed into
#     src/globals.h before building squid.
#
#Default:
# none

# TAG: mail_program
#     Email program used to send mail if the cache dies.
#     The default is "mail".  The specified program must comply
#     with the standard Unix mail syntax:
#     mail-program recipient < mailfile
#
#     Optional command line options can be specified.
#
#Default:
# mail_program mail

# TAG: cache_effective_user
#     If you start Squid as root, it will change its effective/real
#     UID/GID to the user specified below.  The default is to change
#     to UID of nobody.
#     see also; cache_effective_group
#
#Default:
# cache_effective_user nobody

# TAG: cache_effective_group
#     Squid sets the GID to the effective user's default group ID
#     (taken from the password file) and supplementary group list
#     from the groups membership.
#
#     If you want Squid to run with a specific GID regardless of
#     the group memberships of the effective user then set this
#     to the group (or GID) you want Squid to run as.  When set
#     all other group privileges of the effective user are ignored
#     and only this GID is effective.  If Squid is not started as
#     root the user starting Squid MUST be member of the specified
#     group.
#
#     This option is not recommended by the Squid Team.
#     Our preference is for administrators to configure a secure
#     user account for squid with UID/GID matching system policies.
#

```

```
#Default:
# none

# TAG: httpd_suppress_version_string on|off
#     Suppress Squid version string info in HTTP headers and HTML error pages.
#
#Default:
# httpd_suppress_version_string off

# TAG: visible_hostname
#     If you want to present a special hostname in error messages, etc,
#     define this. Otherwise, the return value of gethostname()
#     will be used. If you have multiple caches in a cluster and
#     get errors about IP-forwarding you must set them to have individual
#     names with this setting.
#
#Default:
# none

# TAG: unique_hostname
#     If you want to have multiple machines with the same
#     'visible_hostname' you must give each machine a different
#     'unique_hostname' so forwarding loops can be detected.
#
#Default:
# none

# TAG: hostname_aliases
#     A list of other DNS names your cache has.
#
#Default:
# none

# TAG: umask
#     Minimum umask which should be enforced while the proxy
#     is running, in addition to the umask set at startup.
#
#     For a traditional octal representation of umasks, start
#     your value with 0.
#
#Default:
# umask 027

# OPTIONS FOR THE CACHE REGISTRATION SERVICE
# -----
#
#     This section contains parameters for the (optional) cache
#     announcement service. This service is provided to help
#     cache administrators locate one another in order to join or
#     create cache hierarchies.
#
#     An 'announcement' message is sent (via UDP) to the registration
#     service by Squid. By default, the announcement message is NOT
#     SENT unless you enable it with 'announce_period' below.
#
#     The announcement message includes your hostname, plus the
#     following information from this configuration file:
#
#         http_port
```

```

#           icp_port
#           cache_mgr
#
# All current information is processed regularly and made
# available on the Web at http://www.ircache.net/Cache/Tracker/.
#
# TAG: announce_period
# This is how frequently to send cache announcements. The
# default is `0' which disables sending the announcement
# messages.
#
# To enable announcing your cache, just uncomment the line
# below.
#
#Default:
# announce_period 0
#
#To enable announcing your cache, just uncomment the line below.
#announce_period 1 day
#
# TAG: announce_host
# TAG: announce_file
# TAG: announce_port
# announce_host and announce_port set the hostname and port
# number where the registration message will be sent.
#
# Hostname will default to 'tracker.ircache.net' and port will
# default default to 3131. If the 'filename' argument is given,
# the contents of that file will be included in the announce
# message.
#
#Default:
# announce_host tracker.ircache.net
# announce_port 3131
#
# HTTPD-ACCELERATOR OPTIONS
# -----
# TAG: httpd_accel_surrogate_id
# Note: This option is only available if Squid is rebuilt with the
# -DUSE_SQUID_ESI define
#
# Surrogates (http://www.esi.org/architecture\_spec\_1.0.html)
# need an identification token to allow control targeting. Because
# a farm of surrogates may all perform the same tasks, they may share
# an identification token.
#
#Default:
# httpd_accel_surrogate_id unset-id
#
# TAG: http_accel_surrogate_remote on|off
# Note: This option is only available if Squid is rebuilt with the
# -DUSE_SQUID_ESI define
#
# Remote surrogates (such as those in a CDN) honour Surrogate-Control: no-store-remote.
# Set this to on to have squid behave as a remote surrogate.
#
#Default:
# http_accel_surrogate_remote off

```



```

# TAG: esi_parser      libxml2|expat|custom
# Note: This option is only available if Squid is rebuilt with the
#       -DUSE_SQUID_ESI define
#
#       ESI markup is not strictly XML compatible. The custom ESI parser
#       will give higher performance, but cannot handle non ASCII character
#       encodings.
#
#Default:
# esi_parser custom

# DELAY POOL PARAMETERS
# -----

# TAG: delay_pools
# Note: This option is only available if Squid is rebuilt with the
#       --enable-delay-pools option
#
#       This represents the number of delay pools to be used. For example,
#       if you have one class 2 delay pool and one class 3 delays pool, you
#       have a total of 2 delay pools.
#
#Default:
# delay_pools 0

# TAG: delay_class
# Note: This option is only available if Squid is rebuilt with the
#       --enable-delay-pools option
#
#       This defines the class of each delay pool. There must be exactly one
#       delay_class line for each delay pool. For example, to define two
#       delay pools, one of class 2 and one of class 3, the settings above
#       and here would be:
#
#Example:
# delay_pools 4      # 4 delay pools
# delay_class 1 2    # pool 1 is a class 2 pool
# delay_class 2 3    # pool 2 is a class 3 pool
# delay_class 3 4    # pool 3 is a class 4 pool
# delay_class 4 5    # pool 4 is a class 5 pool
#
#       The delay pool classes are:
#
#           class 1      Everything is limited by a single aggregate
#                       bucket.
#
#           class 2      Everything is limited by a single aggregate
#                       bucket as well as an "individual" bucket chosen
#                       from bits 25 through 32 of the IP address.
#
#           class 3      Everything is limited by a single aggregate
#                       bucket as well as a "network" bucket chosen
#                       from bits 17 through 24 of the IP address and a
#                       "individual" bucket chosen from bits 17 through
#                       32 of the IP address.
#
#           class 4      Everything in a class 3 delay pool, with an
#                       additional limit on a per user basis. This

```

```

#           only takes effect if the username is established
#           in advance - by forcing authentication in your
#           http_access rules.
#
#           class 5           Requests are grouped according their tag (see
#                           external_acl's tag= reply).
#
# NOTE: If an IP address is a.b.c.d
#       -> bits 25 through 32 are "d"
#       -> bits 17 through 24 are "c"
#       -> bits 17 through 32 are "c * 256 + d"
#
#Default:
# none

# TAG: delay_access
# Note: This option is only available if Squid is rebuilt with the
#       --enable-delay-pools option
#
#       This is used to determine which delay pool a request falls into.
#
#       delay_access is sorted per pool and the matching starts with pool 1,
#       then pool 2, ..., and finally pool N. The first delay pool where the
#       request is allowed is selected for the request. If it does not allow
#       the request to any pool then the request is not delayed (default).
#
#       For example, if you want some_big_clients in delay
#       pool 1 and lotsa_little_clients in delay pool 2:
#
#Example:
# delay_access 1 allow some_big_clients
# delay_access 1 deny all
# delay_access 2 allow lotsa_little_clients
# delay_access 2 deny all
# delay_access 3 allow authenticated_clients
#
#Default:
# none

# TAG: delay_parameters
# Note: This option is only available if Squid is rebuilt with the
#       --enable-delay-pools option
#
#       This defines the parameters for a delay pool. Each delay pool has
#       a number of "buckets" associated with it, as explained in the
#       description of delay_class. For a class 1 delay pool, the syntax is:
#
#delay_parameters pool aggregate
#
#       For a class 2 delay pool:
#
#delay_parameters pool aggregate individual
#
#       For a class 3 delay pool:
#
#delay_parameters pool aggregate network individual
#
#       For a class 4 delay pool:
#
#delay_parameters pool aggregate network individual user

```

```

#
#       For a class 5 delay pool:
#
#delay_parameters pool tag
#
#       The variables here are:
#
#           pool           a pool number - ie, a number between 1 and the
#                           number specified in delay_pools as used in
#                           delay_class lines.
#
#           aggregate      the "delay parameters" for the aggregate bucket
#                           (class 1, 2, 3).
#
#           individual     the "delay parameters" for the individual
#                           buckets (class 2, 3).
#
#           network        the "delay parameters" for the network buckets
#                           (class 3).
#
#           user           the delay parameters for the user buckets
#                           (class 4).
#
#           tag            the delay parameters for the tag buckets
#                           (class 5).
#
#       A pair of delay parameters is written restore/maximum, where restore is
#       the number of bytes (not bits - modem and network speeds are usually
#       quoted in bits) per second placed into the bucket, and maximum is the
#       maximum number of bytes which can be in the bucket at any time.
#
#       For example, if delay pool number 1 is a class 2 delay pool as in the
#       above example, and is being used to strictly limit each host to 64kbps
#       (plus overheads), with no overall limit, the line is:
#
#delay_parameters 1 -1/-1 8000/8000
#
#       Note that the figure -1 is used to represent "unlimited".
#
#       And, if delay pool number 2 is a class 3 delay pool as in the above
#       example, and you want to limit it to a total of 256kbps (strict limit)
#       with each 8-bit network permitted 64kbps (strict limit) and each
#       individual host permitted 4800bps with a bucket maximum size of 64kb
#       to permit a decent web page to be downloaded at a decent speed
#       (if the network is not being limited due to overuse) but slow down
#       large downloads more significantly:
#
#delay_parameters 2 32000/32000 8000/8000 600/8000
#
#       There must be one delay_parameters line for each delay pool.
#
#       Finally, for a class 4 delay pool as in the example - each user will
#       be limited to 128Kb no matter how many workstations they are logged into.:
#
#delay_parameters 4 32000/32000 8000/8000 600/64000 16000/16000
#
#Default:
# none
#
# TAG: delay_initial_bucket_level      (percent, 0-100)
    
```

```

# Note: This option is only available if Squid is rebuilt with the
#       --enable-delay-pools option
#
#       The initial bucket percentage is used to determine how much is put
#       in each bucket when squid starts, is reconfigured, or first notices
#       a host accessing it (in class 2 and class 3, individual hosts and
#       networks only have buckets associated with them once they have been
#       "seen" by squid).
#
#Default:
# delay_initial_bucket_level 50

# WCCPv1 AND WCCPv2 CONFIGURATION OPTIONS
# -----

# TAG: wccp_router
# TAG: wccp2_router
#       Use this option to define your WCCP ``home'' router for
#       Squid.
#
#       wccp_router supports a single WCCP (v1) router
#
#       wccp2_router supports multiple WCCPv2 routers
#
#       only one of the two may be used at the same time and defines
#       which version of WCCP to use.
#
#Default:
# wccp_router 0.0.0.0

# TAG: wccp_version
#       This directive is only relevant if you need to set up WCCP (v1)
#       to some very old and end-of-life Cisco routers. In all other
#       setups it must be left unset or at the default setting.
#       It defines an internal version in the WCCP (v1) protocol,
#       with version 4 being the officially documented protocol.
#
#       According to some users, Cisco IOS 11.2 and earlier only
#       support WCCP version 3. If you're using that or an earlier
#       version of IOS, you may need to change this value to 3, otherwise
#       do not specify this parameter.
#
#Default:
# wccp_version 4

# TAG: wccp2_rebuild_wait
#       If this is enabled Squid will wait for the cache dir rebuild to finish
#       before sending the first wccp2 HereIAm packet
#
#Default:
# wccp2_rebuild_wait on

# TAG: wccp2_forwarding_method
#       WCCP2 allows the setting of forwarding methods between the
#       router/switch and the cache. Valid values are as follows:
#
#       1 - GRE encapsulation (forward the packet in a GRE/WCCP tunnel)
#       2 - L2 redirect (forward the packet using Layer 2/MAC rewriting)
#

```

```
#      Currently (as of IOS 12.4) cisco routers only support GRE.
#      Cisco switches only support the L2 redirect assignment method.
#
#Default:
# wccp2_forwarding_method 1

# TAG: wccp2_return_method
#      WCCP2 allows the setting of return methods between the
#      router/switch and the cache for packets that the cache
#      decides not to handle.  Valid values are as follows:
#
#      1 - GRE encapsulation (forward the packet in a GRE/WCCP tunnel)
#      2 - L2 redirect (forward the packet using Layer 2/MAC rewriting)
#
#      Currently (as of IOS 12.4) cisco routers only support GRE.
#      Cisco switches only support the L2 redirect assignment.
#
#      If the "ip wccp redirect exclude in" command has been
#      enabled on the cache interface, then it is still safe for
#      the proxy server to use a l2 redirect method even if this
#      option is set to GRE.
#
#Default:
# wccp2_return_method 1

# TAG: wccp2_assignment_method
#      WCCP2 allows the setting of methods to assign the WCCP hash
#      Valid values are as follows:
#
#      1 - Hash assignment
#      2 - Mask assignment
#
#      As a general rule, cisco routers support the hash assignment method
#      and cisco switches support the mask assignment method.
#
#Default:
# wccp2_assignment_method 1

# TAG: wccp2_service
#      WCCP2 allows for multiple traffic services.  There are two
#      types: "standard" and "dynamic".  The standard type defines
#      one service id - http (id 0).  The dynamic service ids can be from
#      51 to 255 inclusive.  In order to use a dynamic service id
#      one must define the type of traffic to be redirected; this is done
#      using the wccp2_service_info option.
#
#      The "standard" type does not require a wccp2_service_info option,
#      just specifying the service id will suffice.
#
#      MD5 service authentication can be enabled by adding
#      "password=<password>" to the end of this service declaration.
#
#      Examples:
#
#      wccp2_service standard 0          # for the 'web-cache' standard service
#      wccp2_service dynamic 80         # a dynamic service type which will be
#                                       # fleshed out with subsequent options.
#      wccp2_service standard 0 password=foo
```

```

#Default:
# wccp2_service standard 0

# TAG: wccp2_service_info
#   Dynamic WCCPv2 services require further information to define the
#   traffic you wish to have diverted.
#
#   The format is:
#
#   wccp2_service_info <id> protocol=<protocol> flags=<flag>,<flag>..
#       priority=<priority> ports=<port>,<port>..
#
#   The relevant WCCPv2 flags:
#   + src_ip_hash, dst_ip_hash
#   + source_port_hash, dst_port_hash
#   + src_ip_alt_hash, dst_ip_alt_hash
#   + src_port_alt_hash, dst_port_alt_hash
#   + ports_source
#
#   The port list can be one to eight entries.
#
#   Example:
#
#   wccp2_service_info 80 protocol=tcp flags=src_ip_hash,ports_source
#       priority=240 ports=80
#
#   Note: the service id must have been defined by a previous
#   'wccp2_service dynamic <id>' entry.
#
#Default:
# none

# TAG: wccp2_weight
#   Each cache server gets assigned a set of the destination
#   hash proportional to their weight.
#
#Default:
# wccp2_weight 10000

# TAG: wccp_address
# TAG: wccp2_address
#   Use this option if you require WCCP to use a specific
#   interface address.
#
#   The default behavior is to not bind to any specific address.
#
#Default:
# wccp_address 0.0.0.0
# wccp2_address 0.0.0.0

# PERSISTENT CONNECTION HANDLING
# -----
#
# Also see "pconn_timeout" in the TIMEOUTS section

# TAG: client_persistent_connections
# TAG: server_persistent_connections
#   Persistent connection support for clients and servers. By
#   default, Squid uses persistent connections (when allowed)

```

```
#       with its clients and servers.  You can use these options to
#       disable persistent connections with clients and/or servers.
#
#Default:
# client_persistent_connections on
# server_persistent_connections on

# TAG: persistent_connection_after_error
#       With this directive the use of persistent connections after
#       HTTP errors can be disabled. Useful if you have clients
#       who fail to handle errors on persistent connections proper.
#
#Default:
# persistent_connection_after_error off

# TAG: detect_broken_pconn
#       Some servers have been found to incorrectly signal the use
#       of HTTP/1.0 persistent connections even on replies not
#       compatible, causing significant delays. This server problem
#       has mostly been seen on redirects.
#
#       By enabling this directive Squid attempts to detect such
#       broken replies and automatically assume the reply is finished
#       after 10 seconds timeout.
#
#Default:
# detect_broken_pconn off

# CACHE DIGEST OPTIONS
# -----

# TAG: digest_generation
# Note: This option is only available if Squid is rebuilt with the
#       --enable-cache-digests option
#
#       This controls whether the server will generate a Cache Digest
#       of its contents.  By default, Cache Digest generation is
#       enabled if Squid is compiled with --enable-cache-digests defined.
#
#Default:
# digest_generation on

# TAG: digest_bits_per_entry
# Note: This option is only available if Squid is rebuilt with the
#       --enable-cache-digests option
#
#       This is the number of bits of the server's Cache Digest which
#       will be associated with the Digest entry for a given HTTP
#       Method and URL (public key) combination.  The default is 5.
#
#Default:
# digest_bits_per_entry 5

# TAG: digest_rebuild_period (seconds)
# Note: This option is only available if Squid is rebuilt with the
#       --enable-cache-digests option
#
#       This is the wait time between Cache Digest rebuilds.
#
```

```

#Default:
# digest_rebuild_period 1 hour

# TAG: digest_rewrite_period (seconds)
# Note: This option is only available if Squid is rebuilt with the
#       --enable-cache-digests option
#
#       This is the wait time between Cache Digest writes to
#       disk.
#
#Default:
# digest_rewrite_period 1 hour

# TAG: digest_swapout_chunk_size (bytes)
# Note: This option is only available if Squid is rebuilt with the
#       --enable-cache-digests option
#
#       This is the number of bytes of the Cache Digest to write to
#       disk at a time. It defaults to 4096 bytes (4KB), the Squid
#       default swap page.
#
#Default:
# digest_swapout_chunk_size 4096 bytes

# TAG: digest_rebuild_chunk_percentage (percent, 0-100)
# Note: This option is only available if Squid is rebuilt with the
#       --enable-cache-digests option
#
#       This is the percentage of the Cache Digest to be scanned at a
#       time. By default it is set to 10% of the Cache Digest.
#
#Default:
# digest_rebuild_chunk_percentage 10

# SNMP OPTIONS
# -----

# TAG: snmp_port
#       The port number where Squid listens for SNMP requests. To enable
#       SNMP support set this to a suitable port number. Port number
#       3401 is often used for the Squid SNMP agent. By default it's
#       set to "0" (disabled)
#Default:
# snmp_port 0
#
#snmp_port 3401

# TAG: snmp_access
#       Allowing or denying access to the SNMP port.
#
#       All access to the agent is denied by default.
#       usage:
#
#       snmp_access allow|deny [!]aclname ...
#
#Example:
# snmp_access allow snmppublic localhost
# snmp_access deny all
#

```



```
#Default:
# snmp_access deny all

# TAG: snmp_incoming_address
# TAG: snmp_outgoing_address
#     Just like 'udp_incoming_address' above, but for the SNMP port.
#
#     snmp_incoming_address   is used for the SNMP socket receiving
#                             messages from SNMP agents.
#     snmp_outgoing_address   is used for SNMP packets returned to SNMP
#                             agents.
#
#     The default snmp_incoming_address (0.0.0.0) is to listen on all
#     available network interfaces.
#
#     If snmp_outgoing_address is set to 255.255.255.255 (the default)
#     it will use the same socket as snmp_incoming_address. Only
#     change this if you want to have SNMP replies sent using another
#     address than where this Squid listens for SNMP queries.
#
#     NOTE, snmp_incoming_address and snmp_outgoing_address can not have
#     the same value since they both use port 3401.
#
#Default:
# snmp_incoming_address 0.0.0.0
# snmp_outgoing_address 255.255.255.255

# ICP OPTIONS
# -----

# TAG: icp_port
#     The port number where Squid sends and receives ICP queries to
#     and from neighbor caches.  The standard UDP port for ICP is 3130.
#     Default is disabled (0).
#Default:
# icp_port 0
#
#icp_port 3130

# TAG: htcp_port
#     The port number where Squid sends and receives HTCP queries to
#     and from neighbor caches.  To turn it on you want to set it to
#     4827. By default it is set to "0" (disabled).
#Default:
# htcp_port 0
#
#htcp_port 4827

# TAG: log_icp_queries on|off
#     If set, ICP queries are logged to access.log. You may wish
#     do disable this if your ICP load is VERY high to speed things
#     up or to simplify log analysis.
#
#Default:
# log_icp_queries on

# TAG: udp_incoming_address
#     udp_incoming_address   is used for UDP packets received from other
#     caches.
```

```
#
#   The default behavior is to not bind to any specific address.
#
#   Only change this if you want to have all UDP queries received on
#   a specific interface/address.
#
#   NOTE: udp_incoming_address is used by the ICP, HTCP, and DNS
#   modules. Altering it will affect all of them in the same manner.
#
#   see also; udp_outgoing_address
#
#   NOTE, udp_incoming_address and udp_outgoing_address can not
#   have the same value since they both use the same port.
#
#Default:
# udp_incoming_address 0.0.0.0

# TAG: udp_outgoing_address
#   udp_outgoing_address      is used for UDP packets sent out to other
#                               caches.
#
#   The default behavior is to not bind to any specific address.
#
#   Instead it will use the same socket as udp_incoming_address.
#   Only change this if you want to have UDP queries sent using another
#   address than where this Squid listens for UDP queries from other
#   caches.
#
#   NOTE: udp_outgoing_address is used by the ICP, HTCP, and DNS
#   modules. Altering it will affect all of them in the same manner.
#
#   see also; udp_incoming_address
#
#   NOTE, udp_incoming_address and udp_outgoing_address can not
#   have the same value since they both use the same port.
#
#Default:
# udp_outgoing_address 255.255.255.255

# TAG: icp_hit_stale    on|off
#   If you want to return ICP_HIT for stale cache objects, set this
#   option to 'on'.  If you have sibling relationships with caches
#   in other administrative domains, this should be 'off'.  If you only
#   have sibling relationships with caches under your control,
#   it is probably okay to set this to 'on'.
#   If set to 'on', your siblings should use the option "allow-miss"
#   on their cache_peer lines for connecting to you.
#
#Default:
# icp_hit_stale off

# TAG: minimum_direct_hops
#   If using the ICMP pinging stuff, do direct fetches for sites
#   which are no more than this many hops away.
#
#Default:
# minimum_direct_hops 4

# TAG: minimum_direct_rtt
#   If using the ICMP pinging stuff, do direct fetches for sites
```

```
#       which are no more than this many rtt milliseconds away.
#
#Default:
# minimum_direct_rtt 400

# TAG: netdb_low
# TAG: netdb_high
#       The low and high water marks for the ICMP measurement
#       database. These are counts, not percents. The defaults are
#       900 and 1000. When the high water mark is reached, database
#       entries will be deleted until the low mark is reached.
#
#Default:
# netdb_low 900
# netdb_high 1000

# TAG: netdb_ping_period
#       The minimum period for measuring a site. There will be at
#       least this much delay between successive pings to the same
#       network. The default is five minutes.
#
#Default:
# netdb_ping_period 5 minutes

# TAG: query_icmp      on|off
#       If you want to ask your peers to include ICMP data in their ICP
#       replies, enable this option.
#
#       If your peer has configured Squid (during compilation) with
#       '--enable-icmp' that peer will send ICMP pings to origin server
#       sites of the URLs it receives. If you enable this option the
#       ICP replies from that peer will include the ICMP data (if available).
#       Then, when choosing a parent cache, Squid will choose the parent with
#       the minimal RTT to the origin server. When this happens, the
#       hierarchy field of the access.log will be
#       "CLOSEST_PARENT_MISS". This option is off by default.
#
#Default:
# query_icmp off

# TAG: test_reachability  on|off
#       When this is 'on', ICP MISS replies will be ICP_MISS_NOFETCH
#       instead of ICP_MISS if the target host is NOT in the ICMP
#       database, or has a zero RTT.
#
#Default:
# test_reachability off

# TAG: icp_query_timeout      (msec)
#       Normally Squid will automatically determine an optimal ICP
#       query timeout value based on the round-trip-time of recent ICP
#       queries. If you want to override the value determined by
#       Squid, set this 'icp_query_timeout' to a non-zero value. This
#       value is specified in MILLIseconds, so, to use a 2-second
#       timeout (the old default), you would write:
#
#           icp_query_timeout 2000
#
#Default:
# icp_query_timeout 0
```

```

# TAG: maximum_icp_query_timeout      (msec)
#     Normally the ICP query timeout is determined dynamically.  But
#     sometimes it can lead to very large values (say 5 seconds).
#     Use this option to put an upper limit on the dynamic timeout
#     value.  Do NOT use this option to always use a fixed (instead
#     of a dynamic) timeout value.  To set a fixed timeout see the
#     'icp_query_timeout' directive.
#
#Default:
# maximum_icp_query_timeout 2000

# TAG: minimum_icp_query_timeout      (msec)
#     Normally the ICP query timeout is determined dynamically.  But
#     sometimes it can lead to very small timeouts, even lower than
#     the normal latency variance on your link due to traffic.
#     Use this option to put an lower limit on the dynamic timeout
#     value.  Do NOT use this option to always use a fixed (instead
#     of a dynamic) timeout value.  To set a fixed timeout see the
#     'icp_query_timeout' directive.
#
#Default:
# minimum_icp_query_timeout 5

# TAG: background_ping_rate          time-units
#     Controls how often the ICP pings are sent to siblings that
#     have background-ping set.
#
#Default:
# background_ping_rate 10 seconds

# MULTICAST ICP OPTIONS
# -----

# TAG: mcast_groups
#     This tag specifies a list of multicast groups which your server
#     should join to receive multicasted ICP queries.
#
#     NOTE!  Be very careful what you put here!  Be sure you
#     understand the difference between an ICP _query_ and an ICP
#     _reply_.  This option is to be set only if you want to RECEIVE
#     multicast queries.  Do NOT set this option to SEND multicast
#     ICP (use cache_peer for that).  ICP replies are always sent via
#     unicast, so this option does not affect whether or not you will
#     receive replies from multicast group members.
#
#     You must be very careful to NOT use a multicast address which
#     is already in use by another group of caches.
#
#     If you are unsure about multicast, please read the Multicast
#     chapter in the Squid FAQ (http://www.squid-cache.org/FAQ/).
#
#     Usage: mcast_groups 239.128.16.128 224.0.1.20
#
#     By default, Squid doesn't listen on any multicast groups.
#
#Default:
# none

```

```
# TAG: mcast_miss_addr
# Note: This option is only available if Squid is rebuilt with the
#       -DMULTICAST_MISS_STREAM define
#
#       If you enable this option, every "cache miss" URL will
#       be sent out on the specified multicast address.
#
#       Do not enable this option unless you are absolutely
#       certain you understand what you are doing.
#
#Default:
# mcast_miss_addr 255.255.255.255

# TAG: mcast_miss_ttl
# Note: This option is only available if Squid is rebuilt with the
#       -DMULTICAST_MISS_STREAM define
#
#       This is the time-to-live value for packets multicasted
#       when multicasting off cache miss URLs is enabled.  By
#       default this is set to 'site scope', i.e. 16.
#
#Default:
# mcast_miss_ttl 16

# TAG: mcast_miss_port
# Note: This option is only available if Squid is rebuilt with the
#       -DMULTICAST_MISS_STREAM define
#
#       This is the port number to be used in conjunction with
#       'mcast_miss_addr'.
#
#Default:
# mcast_miss_port 3135

# TAG: mcast_miss_encode_key
# Note: This option is only available if Squid is rebuilt with the
#       -DMULTICAST_MISS_STREAM define
#
#       The URLs that are sent in the multicast miss stream are
#       encrypted.  This is the encryption key.
#
#Default:
# mcast_miss_encode_key XXXXXXXXXXXXXXXXXXXX

# TAG: mcast_icp_query_timeout (msec)
#       For multicast peers, Squid regularly sends out ICP "probes" to
#       count how many other peers are listening on the given multicast
#       address.  This value specifies how long Squid should wait to
#       count all the replies.  The default is 2000 msec, or 2
#       seconds.
#
#Default:
# mcast_icp_query_timeout 2000

# INTERNAL ICON OPTIONS
# -----

# TAG: icon_directory
#       Where the icons are stored.  These are normally kept in
```

```

# /usr/local/squid/share/icons
#
#Default:
# icon_directory /usr/local/squid/share/icons

# TAG: global_internal_static
# This directive controls is Squid should intercept all requests for
# /squid-internal-static/ no matter which host the URL is requesting
# (default on setting), or if nothing special should be done for
# such URLs (off setting). The purpose of this directive is to make
# icons etc work better in complex cache hierarchies where it may
# not always be possible for all corners in the cache mesh to reach
# the server generating a directory listing.
#
#Default:
# global_internal_static on

# TAG: short_icon_urls
# If this is enabled Squid will use short URLs for icons.
# If disabled it will revert to the old behavior of including
# it's own name and port in the URL.
#
# If you run a complex cache hierarchy with a mix of Squid and
# other proxies you may need to disable this directive.
#
#Default:
# short_icon_urls on

# ERROR PAGE OPTIONS
# -----

# TAG: error_directory
# If you wish to create your own versions of the default
# (English) error files, either to customize them to suit your
# language or company copy the template English files to another
# directory and point this tag at them.
#
# The squid developers are interested in making squid available in
# a wide variety of languages. If you are making translations for a
# language that Squid does not currently provide please consider
# contributing your translation back to the project.
#
#Default:
# error_directory /usr/local/squid/share/errors/English

# TAG: err_html_text
# HTML text to include in error messages. Make this a "mailto"
# URL to your admin address, or maybe just a link to your
# organizations Web page.
#
# To include this in your error messages, you must rewrite
# the error template files (found in the "errors" directory).
# Wherever you want the 'err_html_text' line to appear,
# insert a %L tag in the error template file.
#
#Default:
# none

# TAG: email_err_data on|off

```

```
#      If enabled, information about the occurred error will be
#      included in the mailto links of the ERR pages (if %W is set)
#      so that the email body contains the data.
#      Syntax is <A HREF="mailto:%w%W">%w</A>
#
#Default:
# email_err_data on

# TAG: deny_info
#      Usage:  deny_info err_page_name acl
#      or      deny_info http://... acl
#      Example: deny_info ERR_CUSTOM_ACCESS_DENIED bad_guys
#
#      This can be used to return a ERR_ page for requests which
#      do not pass the 'http_access' rules. Squid remembers the last
#      acl it evaluated in http_access, and if a 'deny_info' line exists
#      for that ACL Squid returns a corresponding error page.
#
#      The acl is typically the last acl on the http_access deny line which
#      denied access. The exceptions to this rule are:
#      - When Squid needs to request authentication credentials. It's then
#        the first authentication related acl encountered
#      - When none of the http_access lines matches. It's then the last
#        acl processed on the last http_access line.
#
#      You may use ERR_ pages that come with Squid or create your own pages
#      and put them into the configured errors/ directory.
#
#      Alternatively you can specify an error URL. The browsers will
#      get redirected (302) to the specified URL. %s in the redirection
#      URL will be replaced by the requested URL.
#
#      Alternatively you can tell Squid to reset the TCP connection
#      by specifying TCP_RESET.
#
#Default:
# none

# OPTIONS INFLUENCING REQUEST FORWARDING
# -----

# TAG: nonhierarchical_direct
#      By default, Squid will send any non-hierarchical requests
#      (matching hierarchy_stoplist or not cacheable request type) direct
#      to origin servers.
#
#      If you set this to off, Squid will prefer to send these
#      requests to parents.
#
#      Note that in most configurations, by turning this off you will only
#      add latency to these request without any improvement in global hit
#      ratio.
#
#      If you are inside an firewall see never_direct instead of
#      this directive.
#
#Default:
# nonhierarchical_direct on
```

```

# TAG: prefer_direct
# Normally Squid tries to use parents for most requests. If you for some
# reason like it to first try going direct and only use a parent if
# going direct fails set this to on.
#
# By combining nonhierarchical_direct off and prefer_direct on you
# can set up Squid to use a parent as a backup path if going direct
# fails.
#
# Note: If you want Squid to use parents for all requests see
# the never_direct directive. prefer_direct only modifies how Squid
# acts on cacheable requests.
#
#Default:
# prefer_direct off

# TAG: always_direct
# Usage: always_direct allow|deny [!]aclname ...
#
# Here you can use ACL elements to specify requests which should
# ALWAYS be forwarded by Squid to the origin servers without using
# any peers. For example, to always directly forward requests for
# local servers ignoring any parents or siblings you may have use
# something like:
#
#     acl local-servers dstdomain my.domain.net
#     always_direct allow local-servers
#
# To always forward FTP requests directly, use
#
#     acl FTP proto FTP
#     always_direct allow FTP
#
# NOTE: There is a similar, but opposite option named
# 'never_direct'. You need to be aware that "always_direct deny
# foo" is NOT the same thing as "never_direct allow foo". You
# may need to use a deny rule to exclude a more-specific case of
# some other rule. Example:
#
#     acl local-external dstdomain external.foo.net
#     acl local-servers dstdomain .foo.net
#     always_direct deny local-external
#     always_direct allow local-servers
#
# NOTE: If your goal is to make the client forward the request
# directly to the origin server bypassing Squid then this needs
# to be done in the client configuration. Squid configuration
# can only tell Squid how Squid should fetch the object.
#
# NOTE: This directive is not related to caching. The replies
# is cached as usual even if you use always_direct. To not cache
# the replies see no_cache.
#
# This option replaces some v1.1 options such as local_domain
# and local_ip.
#
#Default:
# none

# TAG: never_direct

```



```
# Usage: never_direct allow|deny [!]aclname ...
#
# never_direct is the opposite of always_direct. Please read
# the description for always_direct if you have not already.
#
# With 'never_direct' you can use ACL elements to specify
# requests which should NEVER be forwarded directly to origin
# servers. For example, to force the use of a proxy for all
# requests, except those in your local domain use something like:
#
#     acl local-servers dstdomain .foo.net
#     never_direct deny local-servers
#     never_direct allow all
#
# or if Squid is inside a firewall and there are local intranet
# servers inside the firewall use something like:
#
#     acl local-intranet dstdomain .foo.net
#     acl local-external dstdomain external.foo.net
#     always_direct deny local-external
#     always_direct allow local-intranet
#     never_direct allow all
#
# This option replaces some v1.1 options such as inside_firewall
# and firewall_ip.
#
#Default:
# none

# ADVANCED NETWORKING OPTIONS
# -----

# TAG: incoming_icp_average
# TAG: incoming_http_average
# TAG: incoming_dns_average
# TAG: min_icp_poll_cnt
# TAG: min_dns_poll_cnt
# TAG: min_http_poll_cnt
# Heavy voodoo here. I can't even believe you are reading this.
# Are you crazy? Don't even think about adjusting these unless
# you understand the algorithms in comm_select.c first!
#
#Default:
# incoming_icp_average 6
# incoming_http_average 4
# incoming_dns_average 4
# min_icp_poll_cnt 8
# min_dns_poll_cnt 8
# min_http_poll_cnt 8

# TAG: accept_filter
# FreeBSD:
#
# The name of an accept(2) filter to install on Squid's
# listen socket(s). This feature is perhaps specific to
# FreeBSD and requires support in the kernel.
#
# The 'httpready' filter delays delivering new connections
# to Squid until a full HTTP request has been received.
```

```

# See the accf_http(9) man page for details.
#
# The 'dataready' filter delays delivering new connections
# to Squid until there is some data to process.
# See the accf_dataready(9) man page for details.
#
# Linux:
#
# The 'data' filter delays delivering of new connections
# to Squid until there is some data to process by TCP_ACCEPT_DEFER.
# You may optionally specify a number of seconds to wait by
# 'data=N' where N is the number of seconds. Defaults to 30
# if not specified. See the tcp(7) man page for details.
#EXAMPLE:
## FreeBSD
#accept_filter httpready
## Linux
#accept_filter data
#
#Default:
# none

# TAG: tcp_recv_bufsize      (bytes)
# Size of receive buffer to set for TCP sockets. Probably just
# as easy to change your kernel's default. Set to zero to use
# the default buffer size.
#
#Default:
# tcp_recv_bufsize 0 bytes

# ICAP OPTIONS
# -----

# TAG: icap_enable          on|off
# Note: This option is only available if Squid is rebuilt with the
# -DICAP_CLIENT define
#
# If you want to enable the ICAP module support, set this to on.
#
#Default:
# icap_enable off

# TAG: icap_connect_timeout
# Note: This option is only available if Squid is rebuilt with the
# -DICAP_CLIENT define
#
# This parameter specifies how long to wait for the TCP connect to
# the requested ICAP server to complete before giving up and either
# terminating the HTTP transaction or bypassing the failure.
#
# The default for optional services is peer_connect_timeout.
# The default for essential services is connect_timeout.
# If this option is explicitly set, its value applies to all services.
#
#Default:
# none

# TAG: icap_io_timeout time-units
# Note: This option is only available if Squid is rebuilt with the

```

```
# -DICAP_CLIENT define
#
# This parameter specifies how long to wait for an I/O activity on
# an established, active ICAP connection before giving up and
# either terminating the HTTP transaction or bypassing the
# failure.
#
# The default is read_timeout.
#
#Default:
# none

# TAG: icap_service_failure_limit
# Note: This option is only available if Squid is rebuilt with the
# -DICAP_CLIENT define
#
# The limit specifies the number of failures that Squid tolerates
# when establishing a new TCP connection with an ICAP service. If
# the number of failures exceeds the limit, the ICAP service is
# not used for new ICAP requests until it is time to refresh its
# OPTIONS. The per-service failure counter is reset to zero each
# time Squid fetches new service OPTIONS.
#
# A negative value disables the limit. Without the limit, an ICAP
# service will not be considered down due to connectivity failures
# between ICAP OPTIONS requests.
#
#Default:
# icap_service_failure_limit 10

# TAG: icap_service_revival_delay
# Note: This option is only available if Squid is rebuilt with the
# -DICAP_CLIENT define
#
# The delay specifies the number of seconds to wait after an ICAP
# OPTIONS request failure before requesting the options again. The
# failed ICAP service is considered "down" until fresh OPTIONS are
# fetched.
#
# The actual delay cannot be smaller than the hardcoded minimum
# delay of 30 seconds.
#
#Default:
# icap_service_revival_delay 180

# TAG: icap_preview_enable on|off
# Note: This option is only available if Squid is rebuilt with the
# -DICAP_CLIENT define
#
# The ICAP Preview feature allows the ICAP server to handle the
# HTTP message by looking only at the beginning of the message body
# or even without receiving the body at all. In some environments,
# previews greatly speedup ICAP processing.
#
# During an ICAP OPTIONS transaction, the server may tell Squid what
# HTTP messages should be previewed and how big the preview should be.
# Squid will not use Preview if the server did not request one.
#
# To disable ICAP Preview for all ICAP services, regardless of
# individual ICAP server OPTIONS responses, set this option to "off".
```

```
#Example:
#icap_preview_enable off
#
#Default:
# icap_preview_enable on

# TAG: icap_preview_size
# Note: This option is only available if Squid is rebuilt with the
#       -DICAP_CLIENT define
#
#       The default size of preview data to be sent to the ICAP server.
#       -1 means no preview. This value might be overwritten on a per server
#       basis by OPTIONS requests.
#
#Default:
# icap_preview_size -1

# TAG: icap_default_options_ttl
# Note: This option is only available if Squid is rebuilt with the
#       -DICAP_CLIENT define
#
#       The default TTL value for ICAP OPTIONS responses that don't have
#       an Options-TTL header.
#
#Default:
# icap_default_options_ttl 60

# TAG: icap_persistent_connections      on|off
# Note: This option is only available if Squid is rebuilt with the
#       -DICAP_CLIENT define
#
#       Whether or not Squid should use persistent connections to
#       an ICAP server.
#
#Default:
# icap_persistent_connections on

# TAG: icap_send_client_ip      on|off
# Note: This option is only available if Squid is rebuilt with the
#       -DICAP_CLIENT define
#
#       This adds the header "X-Client-IP" to ICAP requests.
#
#Default:
# icap_send_client_ip off

# TAG: icap_send_client_username      on|off
# Note: This option is only available if Squid is rebuilt with the
#       -DICAP_CLIENT define
#
#       This sends authenticated HTTP client username (if available) to
#       the ICAP service. The username value is encoded based on the
#       icap_client_username_encode option and is sent using the header
#       specified by the icap_client_username_header option.
#
#Default:
# icap_send_client_username off

# TAG: icap_client_username_header
# Note: This option is only available if Squid is rebuilt with the
```

```
# -DICAP_CLIENT define
#
# ICAP request header name to use for send_client_username.
#
#Default:
# icap_client_username_header X-Client-Username

# TAG: icap_client_username_encode on|off
# Note: This option is only available if Squid is rebuilt with the
# -DICAP_CLIENT define
#
# Whether to base64 encode the authenticated client username.
#
#Default:
# icap_client_username_encode off

# TAG: icap_service
# Note: This option is only available if Squid is rebuilt with the
# -DICAP_CLIENT define
#
# Defines a single ICAP service
#
# icap_service servicename vectoring_point bypass service_url
#
# vectoring_point = reqmod_precache|reqmod_postcache|respmod_precache|respmod_postcache
# This specifies at which point of transaction processing the
# ICAP service should be activated. *_postcache vectoring points
# are not yet supported.
#
# bypass = 1|0
# If set to 1, the ICAP service is treated as optional. If the
# service cannot be reached or malfunctions, Squid will try to
# ignore any errors and process the message as if the service
# was not enabled. No all ICAP errors can be bypassed.
# If set to 0, the ICAP service is treated as essential and all
# ICAP errors will result in an error page returned to the
# HTTP client.
#
# service_url = icap://servername:port/service
#
#Example:
#icap_service service_1 reqmod_precache 0 icap://icap1.mydomain.net:1344/reqmod
#icap_service service_2 respmod_precache 0 icap://icap2.mydomain.net:1344/respmod
#
#Default:
# none

# TAG: icap_class
# Note: This option is only available if Squid is rebuilt with the
# -DICAP_CLIENT define
#
# Defines an ICAP service chain. Eventually, multiple services per
# vectoring point will be supported. For now, please specify a single
# service per class:
#
# icap_class classname servicename
#
#Example:
#icap_class class_1 service_1
#icap_class class_2 service_1
#icap_class class_3 service_3
#
```

```

#Default:
# none

# TAG: icap_access
# Note: This option is only available if Squid is rebuilt with the
#       -DICAP_CLIENT define
#
#       Redirects a request through an ICAP service class, depending
#       on given acls
#
#       icap_access classname allow|deny [!]aclname...
#
#       The icap_access statements are processed in the order they appear in
#       this configuration file. If an access list matches, the processing stops.
#       For an "allow" rule, the specified class is used for the request. A "deny"
#       rule simply stops processing without using the class. You can also use the
#       special classname "None".
#
#       For backward compatibility, it is also possible to use services
#       directly here.
#Example:
#icap_access class_1 allow all
#
#Default:
# none

# DNS OPTIONS
# -----

# TAG: check_hostnames
#       For security and stability reasons Squid can check
#       hostnames for Internet standard RFC compliance. If you want
#       Squid to perform these checks turn this directive on.
#
#Default:
# check_hostnames off

# TAG: allow_underscore
#       Underscore characters is not strictly allowed in Internet hostnames
#       but nevertheless used by many sites. Set this to off if you want
#       Squid to be strict about the standard.
#       This check is performed only when check_hostnames is set to on.
#
#Default:
# allow_underscore on

# TAG: cache_dns_program
# Note: This option is only available if Squid is rebuilt with the
#       --disable-internal-dns option
#
#       Specify the location of the executable for dnslookup process.
#
#Default:
# cache_dns_program /usr/local/squid/libexec/dnsserver

# TAG: dns_children
# Note: This option is only available if Squid is rebuilt with the
#       --disable-internal-dns option
#

```

```
#       The number of processes spawn to service DNS name lookups.
#       For heavily loaded caches on large servers, you should
#       probably increase this value to at least 10.  The maximum
#       is 32.  The default is 5.
#
#       You must have at least one dnsserver process.
#
#Default:
# dns_children 5

# TAG: dns_retransmit_interval
#       Initial retransmit interval for DNS queries.  The interval is
#       doubled each time all configured DNS servers have been tried.
#
#
#Default:
# dns_retransmit_interval 5 seconds

# TAG: dns_timeout
#       DNS Query timeout.  If no response is received to a DNS query
#       within this time all DNS servers for the queried domain
#       are assumed to be unavailable.
#
#Default:
# dns_timeout 2 minutes

# TAG: dns_defnames    on|off
#       Normally the RES_DEFNAMES resolver option is disabled
#       (see res_init(3)).  This prevents caches in a hierarchy
#       from interpreting single-component hostnames locally.  To allow
#       Squid to handle single-component names, enable this option.
#
#Default:
# dns_defnames off

# TAG: dns_nameservers
#       Use this if you want to specify a list of DNS name servers
#       (IP addresses) to use instead of those given in your
#       /etc/resolv.conf file.
#       On Windows platforms, if no value is specified here or in
#       the /etc/resolv.conf file, the list of DNS name servers are
#       taken from the Windows registry, both static and dynamic DHCP
#       configurations are supported.
#
#       Example: dns_nameservers 10.0.0.1 192.172.0.4
#
#Default:
# none

# TAG: hosts_file
#       Location of the host-local IP name-address associations
#       database.  Most Operating Systems have such a file on different
#       default locations:
#       - Un*X & Linux:    /etc/hosts
#       - Windows NT/2000: %SystemRoot%\system32\drivers\etc\hosts
#                         (%SystemRoot% value install default is c:\winnt)
#       - Windows XP/2003: %SystemRoot%\system32\drivers\etc\hosts
#                         (%SystemRoot% value install default is c:\windows)
#       - Windows 9x/Me:  %windir%\hosts
#                         (%windir% value is usually c:\windows)
```

```

#       - Cygwin:           /etc/hosts
#
#       The file contains newline-separated definitions, in the
#       form ip_address_in_dotted_form name [name ...] names are
#       whitespace-separated. Lines beginning with an hash (#)
#       character are comments.
#
#       The file is checked at startup and upon configuration.
#       If set to 'none', it won't be checked.
#       If append_domain is used, that domain will be added to
#       domain-local (i.e. not containing any dot character) host
#       definitions.
#
#Default:
# hosts_file /etc/hosts

# TAG: dns_testnames
#       The DNS tests exit as soon as the first site is successfully looked up
#
#       This test can be disabled with the -D command line option.
#
#Default:
# dns_testnames netscape.com internic.net nlanr.net microsoft.com

# TAG: append_domain
#       Appends local domain name to hostnames without any dots in
#       them.  append_domain must begin with a period.
#
#       Be warned there are now Internet names with no dots in
#       them using only top-domain names, so setting this may
#       cause some Internet sites to become unavailable.
#
#Example:
# append_domain .yourdomain.com
#
#Default:
# none

# TAG: ignore_unknown_nameservers
#       By default Squid checks that DNS responses are received
#       from the same IP addresses they are sent to.  If they
#       don't match, Squid ignores the response and writes a warning
#       message to cache.log.  You can allow responses from unknown
#       nameservers by setting this option to 'off'.
#
#Default:
# ignore_unknown_nameservers on

# TAG: ipcache_size      (number of entries)
# TAG: ipcache_low      (percent)
# TAG: ipcache_high     (percent)
#       The size, low-, and high-water marks for the IP cache.
#
#Default:
# ipcache_size 1024
# ipcache_low 90
# ipcache_high 95

# TAG: fqdn_cache_size  (number of entries)
#       Maximum number of FQDN cache entries.

```



```
#
#Default:
# fqdncache_size 1024

# MISCELLANEOUS
# -----

# TAG: memory_pools    on|off
#     If set, Squid will keep pools of allocated (but unused) memory
#     available for future use.  If memory is a premium on your
#     system and you believe your malloc library outperforms Squid
#     routines, disable this.
#
#Default:
# memory_pools on

# TAG: memory_pools_limit    (bytes)
#     Used only with memory_pools on:
#     memory_pools_limit 50 MB
#
#     If set to a non-zero value, Squid will keep at most the specified
#     limit of allocated (but unused) memory in memory pools.  All free()
#     requests that exceed this limit will be handled by your malloc
#     library.  Squid does not pre-allocate any memory, just safe-keeps
#     objects that otherwise would be free()d.  Thus, it is safe to set
#     memory_pools_limit to a reasonably high value even if your
#     configuration will use less memory.
#
#     If set to zero, Squid will keep all memory it can.  That is, there
#     will be no limit on the total amount of memory used for safe-keeping.
#
#     To disable memory allocation optimization, do not set
#     memory_pools_limit to 0.  Set memory_pools to "off" instead.
#
#     An overhead for maintaining memory pools is not taken into account
#     when the limit is checked.  This overhead is close to four bytes per
#     object kept.  However, pools may actually _save_ memory because of
#     reduced memory thrashing in your malloc library.
#
#Default:
# memory_pools_limit 5 MB

# TAG: forwarded_for    on|off
#     If set, Squid will include your system's IP address or name
#     in the HTTP requests it forwards.  By default it looks like
#     this:
#
#             X-Forwarded-For: 192.1.2.3
#
#     If you disable this, it will appear as
#
#             X-Forwarded-For: unknown
#
#Default:
# forwarded_for on

# TAG: cachemgr_passwd
#     Specify passwords for cachemgr operations.
#
```

```

#      Usage: cachemgr_passwd password action action ...
#
#      Some valid actions are (see cache manager menu for a full list):
#          5min
#          60min
#          asndb
#          authenticator
#          cbdata
#          client_list
#          comm_incoming
#          config *
#          counters
#          delay
#          digest_stats
#          dns
#          events
#          filedescriptors
#          fqdnocache
#          histograms
#          http_headers
#          info
#          io
#          ipcache
#          mem
#          menu
#          netdb
#          non_peers
#          objects
#          offline_toggle *
#          pconn
#          peer_select
#          reconfigure *
#          redirector
#          refresh
#          server_list
#          shutdown *
#          store_digest
#          storedir
#          utilization
#          via_headers
#          vm_objects
#
#      * Indicates actions which will not be performed without a
#      valid password, others can be performed if not listed here.
#
#      To disable an action, set the password to "disable".
#      To allow performing an action without a password, set the
#      password to "none".
#
#      Use the keyword "all" to set the same password for all actions.
#
#Example:
# cachemgr_passwd secret shutdown
# cachemgr_passwd lessssssssecret info stats/objects
# cachemgr_passwd disable all
#
#Default:
# none

# TAG: client_db          on|off

```

```
#       If you want to disable collecting per-client statistics,
#       turn off client_db here.
#
#Default:
# client_db on

# TAG: refresh_all_ims on|off
#       When you enable this option, squid will always check
#       the origin server for an update when a client sends an
#       If-Modified-Since request.  Many browsers use IMS
#       requests when the user requests a reload, and this
#       ensures those clients receive the latest version.
#
#       By default (off), squid may return a Not Modified response
#       based on the age of the cached version.
#
#Default:
# refresh_all_ims off

# TAG: reload_into_ims on|off
#       When you enable this option, client no-cache or ``reload''
#       requests will be changed to If-Modified-Since requests.
#       Doing this VIOLATES the HTTP standard.  Enabling this
#       feature could make you liable for problems which it
#       causes.
#
#       see also refresh_pattern for a more selective approach.
#
#Default:
# reload_into_ims off

# TAG: maximum_single_addr_tries
#       This sets the maximum number of connection attempts for a
#       host that only has one address (for multiple-address hosts,
#       each address is tried once).
#
#       The default value is one attempt, the (not recommended)
#       maximum is 255 tries.  A warning message will be generated
#       if it is set to a value greater than ten.
#
#       Note: This is in addition to the request re-forwarding which
#       takes place if Squid fails to get a satisfying response.
#
#Default:
# maximum_single_addr_tries 1

# TAG: retry_on_error
#       If set to on Squid will automatically retry requests when
#       receiving an error response.  This is mainly useful if you
#       are in a complex cache hierarchy to work around access
#       control errors.
#
#Default:
# retry_on_error off

# TAG: as_whois_server
#       WHOIS server to query for AS numbers.  NOTE: AS numbers are
#       queried only when Squid starts up, not for every request.
#
#Default:
```

```
# as_whois_server whois.ra.net
# as_whois_server whois.ra.net

# TAG: offline_mode
#     Enable this option and Squid will never try to validate cached
#     objects.
#
#Default:
# offline_mode off

# TAG: uri_whitespace
#     What to do with requests that have whitespace characters in the
#     URI. Options:
#
#     strip: The whitespace characters are stripped out of the URL.
#            This is the behavior recommended by RFC2396.
#     deny:  The request is denied. The user receives an "Invalid
#            Request" message.
#     allow: The request is allowed and the URI is not changed. The
#            whitespace characters remain in the URI. Note the
#            whitespace is passed to redirector processes if they
#            are in use.
#     encode: The request is allowed and the whitespace characters are
#             encoded according to RFC1738. This could be considered
#             a violation of the HTTP/1.1
#             RFC because proxies are not allowed to rewrite URI's.
#     chop:  The request is allowed and the URI is chopped at the
#            first whitespace. This might also be considered a
#            violation.
#
#Default:
# uri_whitespace strip

# TAG: coredump_dir
#     By default Squid leaves core files in the directory from where
#     it was started. If you set 'coredump_dir' to a directory
#     that exists, Squid will chdir() to that directory at startup
#     and coredump files will be left there.
#
#Default:
# coredump_dir none
#
# Leave coredumps in the first cache dir
#coredump_dir /usr/local/squid/var/cache

# TAG: chroot
#     Use this to have Squid do a chroot() while initializing. This
#     also causes Squid to fully drop root privileges after
#     initializing. This means, for example, if you use a HTTP
#     port less than 1024 and try to reconfigure, you will may get an
#     error saying that Squid can not open the port.
#
#Default:
# none

# TAG: balance_on_multiple_ip
#     Some load balancing servers based on round robin DNS have been
#     found not to preserve user session state across requests
#     to different IP addresses.
#
```

```
#       By default Squid rotates IP's per request. By disabling
#       this directive only connection failure triggers rotation.
#
#Default:
# balance_on_multiple_ip on

# TAG: pipeline_prefetch
#       To boost the performance of pipelined requests to closer
#       match that of a non-proxied environment Squid can try to fetch
#       up to two requests in parallel from a pipeline.
#
#       Defaults to off for bandwidth management and access logging
#       reasons.
#
#Default:
# pipeline_prefetch off

# TAG: high_response_time_warning      (msec)
#       If the one-minute median response time exceeds this value,
#       Squid prints a WARNING with debug level 0 to get the
#       administrators attention. The value is in milliseconds.
#
#Default:
# high_response_time_warning 0

# TAG: high_page_fault_warning
#       If the one-minute average page fault rate exceeds this
#       value, Squid prints a WARNING with debug level 0 to get
#       the administrators attention. The value is in page faults
#       per second.
#
#Default:
# high_page_fault_warning 0

# TAG: high_memory_warning
#       If the memory usage (as determined by mallinfo) exceeds
#       this amount, Squid prints a WARNING with debug level 0 to get
#       the administrators attention.
#
#Default:
# high_memory_warning 0 KB

# TAG: sleep_after_fork                (microseconds)
#       When this is set to a non-zero value, the main Squid process
#       sleeps the specified number of microseconds after a fork()
#       system call. This sleep may help the situation where your
#       system reports fork() failures due to lack of (virtual)
#       memory. Note, however, if you have a lot of child
#       processes, these sleep delays will add up and your
#       Squid will not service requests for some amount of time
#       until all the child processes have been started.
#       On Windows value less then 1000 (1 milliseconds) are
#       rounded to 1000.
#
#Default:
# sleep_after_fork 0

# TAG: windows_ipaddrchangemonitor    on|off
#       On Windows Squid by default will monitor IP address changes and will
#       reconfigure itself after any detected event. This is very useful for
```

```
# proxies connected to internet with dial-up interfaces.
# In some cases (a Proxy server acting as VPN gateway is one) it could be
# desirable to disable this behaviour setting this to 'off'.
# Note: after changing this, Squid service must be restarted.
#
#Default:
# windows_ipaddrchangemonitor on
```