NAME

dynmnd.conf – Dynamics - HUT Mobile IP Mobile Node configuration file

DESCRIPTION

Upon execution, **dynmnd** reads its configuration information from a configuration file which, by default, is */usr/local/etc/dynmnd.conf* . A different file can be selected with command line option --config.

The configuration file has the following format:

File may contain empty lines and lines starting with ´#´. These lines will be ignored.

Otherwise a line is of the format "keyword arguments". The configuration file may also contain various lists. Lists are enclosed between the words "keyword_BEGIN" and "keyword_END". The specific format of the list is described in the appropriate keyword section.

The configurations file must end in the keyword **END**.

To get a minimal test working, you will need to check the following items: **MNHomeIPAddress, HAIPAddress, EnableFADecapsulation** and **HomeNetPrefix** (if using FA decapsulation), **SPI,** and **SharedSecret.**

The rest of the items should work with their preset values in most cases and they can be used to fine tune the operations after the basic operation have been tested successfully.

The following keywords may be used:

MNHomeIPAddress
The Mobile Node's own IP address in the home network. Given in "dotted decimal notation". The Home Agent will capture packets for this address and tunnel them to the Mobile Node. This is the address with which the Mobile Node can be connected even when the MN is roaming in foreign networks.

MNNetworkAccessIdentifier
The Mobile Node's Network Access Identifier (NAI) [RFC2794] If configured, this NAI is used in registration requests to identify the mobile user for AAA services.

UseAAA
Boolean parameter for enabling AAA extensions (key requests using material from AAA, HA and home address discovery using AAA, etc.). This requires that MN NAI and other AAA related items are configured. FALSE disables these extensions. Defaults to **FALSE** (i.e., do not use AAA).

HAIPAddress
The Home Agent address, given in "dotted decimal notation". Registration requests are targeted to this Home Agent. In case of a private HA address this is the address of the surrogate HA. If the HA address is unknown, set this to 0.0.0.0 and make sure that HomeNetPrefix is correct for dynamic HA address resolution or use AAA to discover HA address.

AlternativeHAIPAddress
If the HA has more than one interfaces, HAIPAddress should be configured to be the one reachable from the Internet (i.e., from the foreign networks the MN may visit). To allows MN to detect other HA's interfaces, their IP addresses may be configured here. MN will use this list in addition to HAIPAddress when determining whether an agent advertisement is from its own HA (i.e., when MN is at home). Multiple lines containing different addresses may be used to configure more than one alternative HA address.

AllowHomeAddrFromForeignNet

TRUE allows AAA to assign a home agent and home address from the foreign network (assuming they are set to 0.0.0.0). **FALSE** means that both the home agent and the home address must be from the home domain.

Configuration ofr HA using a private IP address

The following configuration options PrivateHAIPAddress, PrivateHAIdentifier, and HANetworkAccessIdentifier are only used with home networks that use private IP addresses and a surrogate HA. In other cases they should be left commented.

PrivateHAIPAddress

The private IP address of Mobile Node's Home Agent. Needed only, if surrogate HA is used.

PrivateHAIdentifier

The identifier for the private HA in SHA (unique 32-bit number)

EnableFADecapsulation

Boolean parameter for allowing or disallowing FA decapsulation. **TRUE** selects a mode where the FA decapsulates the IP-within-IP encapsulated IP packets. **FALSE** disables this mode and sets the default mode where the MN decapsulates the IP-within-IP encapsulated IP packets. With FA decapsulation the MN uses its home address in the interface even in the foreign network and with MN decapsulation MN needs to acquire a co-located care-of address from the visited network (this needs an external program; see **dynmnd**(8) for more information). The two modes cannot be used simultaneously. Defaults to **TRUE** (i.e., FA decapsulation).

HomeNetPrefix

Net route in the home network (a.b.c.d/prefix_length). This home net routing entry must be removed in the foreign network in order to force all the packets to the correct destination. This is used mainly with FA decapsulation. If commented, the routing entry is not removed nor added. The home net entry may optionally be used with MN decapsulation - see MNDecapsRouteHandling option below.

For example, C-class networks has 24 bits for the network part, then HomeNetPrefix could be something like 192.168.10.0/24.

HomeNetGateway

Home net default gateway entry can be used to force a gateway that the MN uses when it is at home. If this is left commented, the MN tries to use the default route that was in use when the program was started.

SPI A SPI (Security Parameter Index) must be defined for every MN. It is used for indexing the security association at the Home Agent. SPI is used to identify used authentication and encryption methods. This value is a integer number and it must match with the one configured in this MN's Home Agent.

SharedSecret

Shared secret, which is used for authentication between the Mobile Node and its Home Agent. Shared Secret is given in hexadecimal notation (even number of digits 0..9,A..F) or as a character string separated by quotation mark (e.g. "secret"). Note: RFC 2002 (Mobile IP) specifies that the default key size is 128 bits (i.e., 16 bytes or 32 hex 'characters'). Dynamics supports also other key lengths.

AuthenticationAlgorithm

Authentication algorithm:
1: MD5/prefix+suffix (a.k.a. keyed-MD5) [RFC 2002]
4: HMAC-MD5 [RFC 2104]
5: SHA-1 [FIPS 180-1]
6: HMAC-SHA1 [RFC 2104]

Note! MD5/prefix+suffix has known weaknesses and use of HMAC-MD5 is recommented. MD5/prefix+suffix algorithm is for backwards compatability with older versions that do not support more secure HMAC-MD5.

ReplayMethod

Replay prevention method:
0: none
1: time stamps (default)
2: nonces

This option is used to select the method that is used between the Mobile Node and its Home Agent to prevent the replay attacks. It must match with the one configured in the Home Agent.

FA_SECURITY_BEGIN .. FA_SECURITY_END

The Mobile Node may have optional security associations with Foreign Agents. If the security association exists an additional Mobile Node - Foreign Agent Authentication Extension is added to the registration requests.

This list contains the shared secrets indexed by SPI (and Foreign Agent IP address). The algorithm field specifies the method used for key distribution (currently only one is implemented, i.e. 1: encryption using MD5). The format of the share secret field is identical to the one used with the MN-HA security association list above.

Each line of the list should have following items separated by spaces or tabulators: SPI, FA IP address, algorithm, and shared secret.

MN-AAA Authentication and Challenge/Response [RFC3012]

If the MN does not have a security association with an FA, it may use AAA infrastructure for authentication. If this is used, also MN NAI (MNNetworkAccessIdentifier) should be configured.

MN-AAA-SPI

SPI to be used in MN-AAA authentication. Reserved SPI values:
2 = CHAP_SPI, CHAP style authentication using MD5 [RFC 3012]
3 = MD5/prefix+suffix [draft-ietf-mobileip-aaa-key-03.txt]
4 = HMAC MD5 [draft-ietf-mobileip-aaa-key-03.txt]

MN-AAA-SharedSecret

Shared secret for MN-AAA authentication (see 'SharedSecret' above for format instructions)

MN-AAA-AuthenticationAlgorithm

and

MN-AAA-KeyGenerationAlgorithm

Algorithms to be used for MN-AAA authentication and key generation
1 = MD5/prefix+suffix (RFC 2002)
2 = RADIUS authentication (Sec. 8 of RFC 3012)
3 = MD5/prefix+suffix (RFC 2002) (alias for 1 above)
4 = HMAC-MD5 (Sec. 6 of RFC 3012; RFC 2104)
5 = SHA-1 (FIPS 180-1)
6 = HMAC-SHA1 (RFC 2104)

Note: with algorithm 2, 'MN-AAA-SPI' should be set to reserved number CHAP_SPI (default: 2).

TunnelingMode

The packets between the MN and a Correspondent Node (CN; i.e. other nodes in the network) can be routed using different routes. This option can be used to select, which mode will be selected.

Possible values:
1 = automatic, prefer reverse tunnel
(i.e. bi-directional tunnel)
2 = automatic, prefer triangle tunnel
(i.e. tunnel only in CN->MN direction)
3 = accept only reverse tunnel
4 = accept only triangle tunnel

In modes 1 and 2 the MN can operate with all the FAs, but in modes 3 and 4 a FA will be ignored, if it does not support the configured tunneling mode. Default value: 1.

MNDecapsRouteHandling

When the MN can get its own co-located care-of address and use reverse tunneling, the normal method is to set the default route to the tunnel. This means that all the packets destined to other networks than the current subnet in the visited network are send via the HA. If the co-located COA is public, it can be used for sessions that do not need constant IP address (e.g. most of the web browsing). The following configuration option specifies the routing operation that is used with the co-located COA.

Possible values:
0 = set default route to the tunnel
1 = set only the home net route to the tunnel
(the above HomeNetPrefix options must be set)
2 = do not change the routing entries
(i.e. some external means must be used to direct traffic
to the tunnel, e.g. manually adding host route to a
specific host)

MNDefaultTunnelLifetime

Default tunnel lifetime is used to select the requested lifetime. The actual selected lifetime is the minimum of this value and the lifetime advertised by the selected FA. The lifetime is defined in seconds and the default value is **300**.

UDPPort

The port number for sending Registration Requests to. Port 434 is allocated for Mobile IP signaling and this should not be changed unless the network is known to use some other port (i.e. all the FAs and HAs must have the same port configured).

NOTE! The Mobile Node is unable to connect to Foreign Agents, if either Mobile Node itself or the Foreign Agents in the visited network use nonstandard UPD port for signaling protocol traffic.

SocketPriority

Socket priority for signaling sockets (UDP) can be set with SO_PRIORITY to allow easier QoS configuration. If this argument is set, the given value is used as a priority for the signaling socket. E.g., CBQ class can be used to make sure that signaling is not disturbed by other traffic on a congested link.

SyslogFacility

The log messages are written through syslog service. The facility to be used defaults to **LOG_LOCAL0**, but it can be set with this parameter to any of the possible facilities (**LOG_AUTHPRIV**, **LOG_DAEMON**, and so on). The processing of log messages is defined in the */etc/syslog.conf* file. See **syslog.conf**(5) for more information.

IGNORE_INTERFACES_BEGIN .. IGNORE_INTERFACES_END

List of interfaces to be ignored. No agent advertisements are received nor agent solicitations sent for these interfaces.

EnforceRoutes

Other programs may set routing entries so that the data connection may fail. The MN can try to enforce the routes that it believes should be used. This operation should currently be used only with FA decapsulation. If the route enforcement is activated the MN daemon prevents certain route changes.

APPollingInterval

MN can be instructed to poll for current AP address when using a wireless LAN driver that supports wireless extensions. This can be used to speed up handoffs when using managed mode (BSS). Polling interval is configured in micro seconds (i.e., 1000000 equals to 1 second). -1 = AP polling disabled.

SolicitationInterval

MN can be instructed to send periodic agent solicitations to find new FAs. Normally, MN uses agent solicitations when it does not have a valid agent advertisement. Periodic solicitation occurs even if the connection seems to be up. This will cause more broadcast messages and is thus disabled in the default configuration, but it can speed up handoffs in some environments. Solicitation interval is configured in micro seconds (usec) (i.e., 1000000 usec equals to 1 second). A rnadom time between 0 and 0.5 second will be added to solicitation intervals to prevent unwanted synchronization of broadcast messages. In addition, solicitations will not be send more often than once per second, so this interval should not be configured to be less than 1000000 usec. -1 = Periodic agent solicitation disabled.

MNAPIReadSocketPath,

Path for the read only socket for API calls given as a text string. This socket can be used only for reading the MN statistical data. All the modifications and commands affecting the connections must be done throught the administration socket. An example path: **/var/run/dynamics_mn_read**.

MNAPIReadSocketGroup

Group for the read only socket for API calls given as a text string. The group must be a name as a string, no groupIDs are allowed. The groups are usually defined in /etc/group file. For example

root.

MNAPIReadSocketOwner
Owner for the read only socket for API calls given in text string. User names are usually defined in /etc/passwd file. The owner must be a name as a string, no userIDs are allowed. For example **root**.

MNAPIReadSocketPermissions
Read socket permissions given in octal form like in **chmod**(1). For example **0666**.

MNAPIAdminSocketPath
Path for the administration socket. Calls through this socket can modify the dynamic data in MN. An example path: **/var/run/dynamics_mn_admin**.

MNAPIAdminSocketGroup
Group for the administration socket given as a text string. Look in /etc/group file. For example **root**.

MNAPIAdminSocketOwner
Owner for the administration socket given as a text string. Look in /etc/passwd **root**.

MNAPIAdminSocketPermissions
Permissions for the administration socket given in octal format like in **chmod**(1). For example **0700**.

END The configuration file terminator.

FILES

/usr/local/etc/dynmnd.conf
The system wide configuration file for Mobile Agent.

AUTHOR AND COPYRIGHT

Dynamics group <dynamics@cs.hut.fi>

SEE ALSO

dynmnd(8), **dynmn_tool**(8), **dynfad**(8), **dynfad.conf**(5), **dynhad**(8), **dynhad.conf**(5), **dynamics**(8)