DNS Updater

bintec-Dm 785-I

Legal Notice

Warranty

This publication is subject to change.

bintec offers no warranty whatsoever for information contained in this manual.

bintec is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

Chapter 1 Introduction

1.1 Introduction

Addresses, made up of numbers, are used to access services and devices in the Internet. These are not easy for people to remember or handle. By using the Domain Name System (DNS), chains of text can be associated to IP addresses. DNS is based on server consultations able to translate these texts into IP addresses. Up until recently, information from these servers could be considered "quasi-static" (in the sense that it only changed as a result of registers or deregisters and specific changes).

Given how quickly the Internet has grown, there was soon a lack of free public addresses. To solve this, these addresses were reused as far as possible. Internet growth has affected both the commercial and the domestic markets, the latter more significantly.

From the DNS perspective, these changes implied an increase in the use of servers, an increase in the number of domain names and servers being used, and an increase in the exchange of associations between *hostnames* and IP addresses.

To tackle this problem, companies such as DynDNS (www.dyndns.com) have emerged, offering DNS services in a set of proprietary domains. The advantage with this is they offer free *hostnames* for private users and provide dynamic updating mechanisms.

DNS dynamic updating is particularly useful for SMEs and domestic environments, where the IP address, supplied by an access provider, changes from connection to connection (or even during it). These changes are the result of the service provider adjusting prices: the access cost could rise significantly if the service gives a fixed public address. By using DNS dynamic updating services, you can access devices using a known *hostname* without worrying about changes in the IP address (arising as a result of the service provider).

DNS dynamic updating is carried out in compliance with the IETF standard, or through HTTP-based protocols. These protocols are based on simple commands that specify the changes to be executed and the authentication information, in order to verify that whoever is making this change is authorized.

DynDNS uses a proprietary protocol based on HTTP, supplying information and programs that allow you to use their dynamic updating characteristics for personal computers. This information has been used so that our routers can update *hostnames* in DynDNS. For further information on this protocol, please see the DynDNS webpage: www.dyndns.com. Our routers support this protocol.

1.1.1 DNS-Updater and NAT

One specific case is where the router wants access, using a *hostname*, and is located behind an access router running NAT. This device is accessed through the Internet by configuring visible ports in the access router.

In this case, the IP address published through the DNS-Updater is the access router's public IP address (and not the IP address for the interface the router is going to be configured with, which is a private address). The problem lies in how the router, being configured, can find the access router's public IP address.

One solution is to implement mechanisms in the router to resolve the access router's IP address. Consequently, it is this particular router that is updated. The IP address is obtained based on HTTP requests to known servers, which return the received petitions source IP address in the HTTP response. Our routers implement this possibility and allow you to configure the checking rate for this public IP address, along with other possibilities.

1.1.2 DNS-Updater and DIAL Interfaces

The DNS-Updater feature is configured to publish/update an IP address for an interface. If this interface is not active, updating does not occur.

For DIAL interfaces (such as PPP or FR) this means that, while they are inactive, traffic from the DNS-Updater is not sent (i.e. DNS-Updater traffic doesn't activate these interfaces).

Chapter 2 Configuration

2.1 Accessing the Configuration

To access the DNS-Updater feature configuration, enter the **FEATURE DNS-UPDATER** command in the main configuration menu.

Syntax:

```
Config>feature dns-updater

-- DNS UPDATER configuration --
DNS UPDATER config>
```

2.2 Configuration commands

The following table summarizes the DNS-Updater feature configuration commands. These commands are detailed further on.

Command	Function
?(HELP)	Displays the configuration commands or their options.
ENABLE	Globally enables the feature.
ENTRY	Configures the data needed to update an interface's IP address, provided by a DNS service supplier.
NO	Negates a command or sets the default parameters.
PARAM	Configures the common feature parameters for all the entries.

2.2.1 ? (HELP)

Displays the list of available commands.

Syntax:

```
DNS UPDATER config>?
```

Example:

```
DNS UPDATER config>?
  enable    Enable DNSU feature
  entry     Configures an entry
  no        Negate a command or set its default
  param     Configures DNS UPDATER params
  exit
```

2.2.2 [NO] ENABLE

Allows you to globally enable the DNS-Updater feature. The feature needs to be globally enabled so every configured entry is operative. It is disabled by default.

Syntax:

```
DNS UPDATER config>enable
```

2.2.3 [NO] ENTRY

Allows you to define a DNS updating entity for a certain interface with a given DNS service provider. No entry has been defined by default.

Syntax:

```
DNS UPDATER config>entry <entry-id>
  disable           Disables an entry
  interface         Interface whose address will be used
  source-address    Ip address that will be used
```

```
protocol          Sets DNS updater protocol
   DynDNS           DynDNS protocol
      system           DynDNS system to use
         dynamic           Dynamic DNS system
         static            Static DNS system
         custom            Custom DNS system
   Standard         Dynamic Updates in DNS Protocol (RFC2136)
hostname          Hostname to update
servername        Server where update is sent to
user              User account login
   ciphered-pwd     User ciphered password
   password         User account password
external-ip       Sets External IP Checking options
   enable           Enables external IP checking
   server           Server where IP request is sent to
   time             Time between checks
server-timeout    Seconds to wait for the server response
track             Track the state of a controlling entity
   nsla-advisor     Track a NSLA advisor
```

entry-id	Entry identifier. All data referring to the same entry has the same identifier. This value ranges between 1 and 99. No entry has been defined by default.
disable	Disables the entry (this command is available when something has already been configured in the entry). Entries are disabled until all activation parameters required have been configured. These parameters are: updater protocol, interface (whose IP address is published through the DNS-Updater feature), *hostname, servername* and the user data (user name and password).
interface	Interface whose IP address is published/updated through the DNS-Updater feature. This IP address is associated to the *hostname* registered with the DNS services provider. Where you have a device running NAT, this address is ignored and the IP obtained through the mechanisms described in the EXTERNAL-IP command is used.
source-address	Source IP address published/updated through the DNS-Updater feature. If this is configured, the IP address of the interface indicated through the *interface* command is ignored. This IP address is associated with the *hostname* registered with the DNS service provider. In cases where a device is running NAT, this address is ignored and the IP received through the mechanisms described in the EXTERNAL-IP command is used.
protocol	Protocol used to update the associated IP address- *hostname*.
dyndns	Specifies that the updater protocol is provided by the DynDNS company. Traffic used in HTTP goes through port 80 (for further information, please visit their webpage: www.dyndns.com).
system	For the DynDNS supplier, this specifies the updating method, or how the IP address is managed in compliance with the DynDNS company criteria. No method is defined by default.
dynamic	The IP address is dynamic (i.e. one likely to undergo changes and require frequent updating).
static	The IP address is static.
custom	The IP address can be static or dynamic. The client can remotely execute DNS management.
standard	Specifies the upgrading protocol (i.e., the one defined in RFC2136).
hostname	*Hostname* associated to the published/updated IP address. The *hostname* belongs to one of the domains defined by the DNS provider.
servername	Address updates are sent to. This is specified through a DNS *hostname*. For DynDNS, this is members.dyndns.org, although we recommend you check their webpage to see if there are any changes.
user	To subscribe to the DNS provider service, you need a user name and password. This data is used when updating the IP address. The password always appears ciphered.
ciphered-pwd	Configures a ciphered password.
password	Configures a clear password.
externl-ip	Configures the change check mechanisms for the public IP address. This is for the device running NAT; the device you are configuring resides behind the former. By default, no parameters are configured. The address is obtained through an HTTP query and the public IP address is received in the response.
enable	Enables the public IP address check for the device running NAT. Default is disabled.
server	Address for the server returning the public IP address, used by the device running NAT. Based on what is returned, the device determines whether there are changes or not. This is specified through a DNS *hostname*. DynDNS offers a server, accessible through checkip.dyndns.org, although we recommend that you check their website to see if there are any changes.
time	Time period used to check for possible changes to the public IP address, for the device running

	NAT. Values ranging from 10 to 60 minutes are allowed. Default is 10 minutes. Due to overload and protection against attacks, servers providing this service do not permit a high query rate. DynDNS does not support more than one query every 10 minutes.
server-timeout	Maximum wait time for responses coming from the servers. This timeout only applies to DynDNS, not other protocols. Values ranging from 1 to 120 seconds are allowed. Default is 10 seconds.
track	Configuration of a controlling entity to dynamically enable or disable this entry.
nsla-advisor	The status of the entry tracks the status of a NSLA advisor. If the status of the advisor is TRUE, the entry is enabled.

Example:

```
   feature dns-updater
; -- DNS UPDATER configuration --
      enable
;
      entry 1 protocol DynDNS system dynamic
      entry 1 interface ppp1
      entry 1 hostname test-hostname.getmyip.com
      entry 1 servername members.dyndns.org
      entry 1 user testusername ciphered-pwd 0xE337A56B515214DFEF0D3AD93DC2C969
;
   exit
```

Example:

Configuring an incomplete entry. Please note this is disabled.

```
feature dns-updater
; -- DNS UPDATER configuration --
      enable
;
      entry 1 protocol DynDNS system dynamic
      entry 1 interface ppp1
      entry 1 hostname test-hostname.getmyip.com
      entry 1 user testusername ciphered-pwd 0xE337A56B515214DFEF0D3AD93DC2C969
      entry 1 disable
;
   exit
```

Command history:

Release	Modification
11.01.07	The *track nsla-advisor* option has been introduced as of version 11.01.07.

2.2.4 NO

Sets the parameter to its default value.

Syntax:

```
DNS UPDATER config>no ?
  enable    Enable DNSU feature
  entry     Configures an entry
  param     Set default values
```

2.2.5 [NO] PARAM

Configures the DNS-Updater feature global parameters. Configures how often changes to the IP address for the configured interface are checked. It also configures the amount of time the IP address remains in said state, without being updated by the DNS service provider.

Syntax:

```
DNS UPDATER config>param ?
  check-interval    Time between IP checks
  forced-update     Time between forced updates
```

2.2.5.1 [NO] PARAM CHECK-INTERVAL

Allows you to set a check interval for changes to the IP made in the configured interface.

Syntax:

```
DNS UPDATER config>param check-interval <30s..1h>
```

Admits values between 30 seconds and 1 hour. Default is 5 minutes.

Please note that DNS service providers restrict the number of updates to a minimum to avoid overloads and attacks on the service. Configure this parameter so it is adjusted to the requirements set by your provider.

Note

In the following cases, IP address publication is executed immediately (i.e., the time configured in the check-interval command is ignored):

- An IP address is assigned to a PPP interface through IPCP. This address is different to the current one.

- An IP address is assigned to a Direct IP interface. This address is different to the current one.

- An IP address is assigned to an interface through DHCP. This address is different to the current one.

Command history:

Release	Modification
11.01.03	Values of the **check-interval** option range from 30 seconds to 1 hour as of version 11.01.03.

2.2.5.2 [NO] PARAM FORCED-UPDATE

Configures the maximum valid lifetime for the device, without configured entries being updated.

Syntax:

```
DNS UPDATER config>param forced-update <30s..4w2d>
```

Values ranging from 30 seconds to 30 days are allowed. Default is 25 days. DynDNS recommends updating the entry every 28 days to avoid expiry.

Command history:

Release	Modification
10.09.31	Spelling of the **forzed-update** option has been corrected and will appear as "forced".
11.00.07	Spelling of the **forzed-update** option has been corrected and will appear as "forced".
11.01.03	Values of the **forzed-update** option range from 30 seconds to 30 days.
11.01.04	Spelling of the **forzed-update** option has been corrected and will appear as "forced" from here onwards.

2.2.6 EXIT

Allows you to exit the DNS-Updater feature configuration console and access the device's general configuration prompt.

Syntax:

```
DNS UPDATER config>exit
Config>
```

Chapter 3 Monitoring

3.1 Accessing the Monitoring

To access DNS-Updater monitoring, enter the **FEATURE DNS-UPDATER** command in the main monitoring menu.

Syntax:

```
+features dns-updater

-- DNS Updater console --
DNS Updater+?
```

3.2 Monitoring commands

The following table describes the available monitoring commands.

Command	Function
?(HELP)	Displays the monitoring commands or their options.
CLEAR	Deletes the DNS-Updater feature statistics for one or all entries.
LIST	Displays the status and statistics for all configured entries.
UPDATE	Allows you to force updating for one or all defined entries.
EXIT	Exits the feature monitoring menu.

3.2.1 ? (HELP)

Displays the monitoring commands or their options.

Syntax:

```
DNS Updater+?
  clear     Clear statistics
  list      List the distinct DNS UPDATER operating parameters
  update    Update entries
  exit
```

3.2.2 CLEAR

Deletes the statistics for one or all configured entries.

Syntax:

```
DNS Updater+clear ?
  all       Clear all entries
  entry     Clear an entry
```

3.2.2.1 CLEAR ALL

Deletes the statistics for all configured entries.

Syntax:

```
DNS Updater+clear all
```

3.2.2.2 CLEAR ENTRY

Deletes the statistics for a selected entry. When asked, enter the number of the entry to be deleted. Values ranging from 1 to 99 are allowed. If the entry does not exist, an error message appears.

Syntax:

```
DNS Updater+clear entry <entry id>
```

3.2.3 LIST

Displays the status and statistics for all configured entries.

Syntax:

```
DNS Updater+list
```

Example:

```
DNS Updater+list

Entry    Protocol                Hostname                                  Status
-----  --------------  ------------------------------------------  ------
  1    DynDNS dynamic  myworkplace.office-on-the.net                 nochg

Entry       Last Update        Current IP         Updated IP
-----    -----------------  ----------------   -----------------
  1      01/15/08 15:20:32      88.29.41.7          88.29.41.7

          DNS query            External IP                   DNS Updates
Ent    done      error      done       error      asked      done       error
--- ---------- ---------- ---------- ---------- ---------- ---------- ----------
  1          4          1          0          0          3          3          0

Checking interval: 5 minutes
Time between forced updates: 25 days
DYNDNS-HSDPA DNS Updater+
```

This first shows the protocol, the retained *hostname* and the updating status for each entry. This is a response from DynDNS containing the latest updating.

Secondly, this displays the last updating date and the IP addresses for the interface used in the latest updating for each entry. Whenever the device is behind a router running NAT, these will be different.

The next block shows the successful and failed DNS petition statistics, the number of successful and failed checks on the IP address for the router running NAT and the number of successful and failed updates for each entry. These statistics can be deleted through the **CLEAR** command.

Finally, this shows the change checking rates and the maximum lifetime permitted without updates.

3.2.4 UPDATE

Allows you to force updating for one or all enabled entries. If an error occurs in the process (such as an error in DNS resolution on the *hostnames* used), an error message appears.

Syntax:

```
DNS Updater+update ?
  all      Update all entries
  entry    Update an entry
```

3.2.4.1 UPDATE ALL

Allows you to force updating for all enabled entries

Syntax:

```
DNS Updater+update all
```

Example:

```
DNS Updater+update all
Starting updating process of entry 1 ... Completed!!!, status: nochg
DNS Updater+
```

This leads to the following events:

```
01/15/08 15:37:57  DNSU.013 Entry 1 Resolved server IP 63.208.196.96
01/15/08 15:37:57  DNSU.005 Entry 1 Creating DynDNS Dynamic prot message
01/15/08 15:37:57  DNSU.007 Entry 1 Received resp nochg
```

```
01/15/08 15:37:57  DNSU.009 Entry 1 IP updated
```

3.2.4.2 UPDATE ENTRY

Allows you to force updating for a specific entry. The entry is selected through a number ranging from 1 to 99. If it doesn't exist, an error message appears.

Syntax:

```
DNS Updater+update entry <entry id>
```

Example:

```
DNS Updater+update entry 1
Starting updating process of entry 1 ... Completed!!!, status: nochg
DNS Updater+
```

This results in the following events:

```
01/15/08 15:20:31  DNSU.013 Entry 1 Resolved server IP 63.208.196.96
01/15/08 15:20:31  DNSU.005 Entry 1 Creating DynDNS Dynamic prot message
01/15/08 15:20:32  DNSU.007 Entry 1 Received resp nochg
01/15/08 15:20:32  DNSU.009 Entry 1 IP updated
```

3.2.5 EXIT

Exits the DNS-Updater monitoring console and accesses the device's general monitoring prompt.

Syntax:

```
DNS Updater+exit
```

Chapter 4 Examples

4.1 Use in an access router

The device accesses Internet through an HSDPA card. The DynDNS account has *testusername* as user and *test-password* as password. The hostname is *test-hostname.getmyip.com*.

```
   log-command-errors
   no configuration
   set hostname DYNDNS-HSDPA
   add device ppp 1
   set data-link at cellular1/0
   set data-link at cellular1/1
   set data-link x25 serial0/1
   global-profiles dial
; -- Dial Profiles Configuration --
      profile HSDPA1 default
      profile HSDPA1 dialout
      profile HSDPA1 3gpp-apn movistar.es
      profile HSDPA1 idle-time 300
;
   exit
;
;
   network ethernet0/0
; -- Ethernet Interface User Configuration --
      ip address 172.24.78.94 255.255.0.0
;
   exit
;
   network cellular1/0
; -- Interface AT. Configuration  --
      pin ciphered 0xA4D54CCB0C042FB6
      sim-select internal-socket-2
;
   exit
;
;
   network cellular1/1
; -- Interface AT. Configuration  --
      ppp lcp-options acfc
      ppp lcp-options pfc
      ppp lcp-options accm a0000
   exit
;
   network ppp1
; -- Generic PPP User Configuration --
      ip address unnumbered
;
      ppp
; -- PPP Configuration --
         authentication sent-user MOVISTAR ciphered-pwd 0xD2650CEF62FBEF55D3AC33
7DA700103F
         ipcp local address assigned
         no ipcp peer-route
         lcp echo-req off
      exit
;
      base-interface
; -- Base Interface Configuration --
         base-interface cellular1/1 link
         base-interface cellular1/1 profile HSDPA1
;
      exit
```

```
;
   exit
;
   event
; -- ELS Config --
      enable trace subsystem DNSU ALL
      enable filter
      ev-buffer 3000 200
   exit
;
;
   protocol ip
; -- Internet protocol user configuration --
      route 0.0.0.0 0.0.0.0 ppp1
;
      classless
;
   exit
;
;
;
   feature dns
; -- DNS resolver user configuration --
      server 62.36.225.150
   exit
;
   feature dns-updater
; -- DNS UPDATER configuration --
      enable
;
      entry 1 protocol DynDNS system dynamic
      entry 1 interface ppp1
      entry 1 hostname myworkplace.office-on-the.net
      entry 1 servername members.dyndns.org
      entry 1 user testusername ciphered-pwd 0xE337A56B515214DFEF0D3AD93DC2C969
;
   exit
;
   dump-command-errors
   end
```

On startup, nothing is sent while the PPP interface is inactive. As soon as the interface activates and has an IP address, it sends an update and receives a response (as shown in the following events):

```
01/15/08 14:42:45  DNSU.018 DNS UPDATER Initialized
01/15/08 14:42:45  DNSU.020 Entry 1 added
01/15/08 14:43:25  DNSU.021 Entry 1 needs to be updated
01/15/08 14:48:25  DNSU.021 Entry 1 needs to be updated
01/15/08 14:53:25  DNSU.021 Entry 1 needs to be updated
01/15/08 14:58:25  DNSU.021 Entry 1 needs to be updated
01/15/08 15:03:25  DNSU.021 Entry 1 needs to be updated
01/15/08 15:03:27  DNSU.013 Entry 1 Resolved server IP 63.208.196.96
01/15/08 15:03:27  DNSU.005 Entry 1 Creating DynDNS Dynamic prot message
01/15/08 15:03:27  DNSU.007 Entry 1 Received resp good
01/15/08 15:03:27  DNSU.009 Entry 1 IP updated
```

The entry status and additional statistics can be seen in the monitoring process:

```
DYNDNS-HSDPA DNS Updater+list

Entry    Protocol               Hostname                              Status
-----  --------------  ------------------------------------------  ------
  1    DynDNS dynamic  myworkplace.office-on-the.net                 good

Entry       Last Update        Current IP         Updated IP
-----    -----------------  ----------------   -----------------
  1      01/15/08 15:03:27      88.29.41.7          88.29.41.7
```

```
          DNS query            External IP                   DNS Updates
Ent    done      error      done       error      asked      done       error
--- ---------- ---------- ---------- ---------- ---------- ---------- ----------
  1          1          0          0          0          1          1          0

Checking interval: 5 minutes
Time between forced updates: 25 days
```

4.2 Router behind a device running NAT

The router being configured is behind an access router running NAT. Due to this, the public IP address check for said router is configured using a service provided by DynDNS (chekip). The DynDNS account has *testusername* as user and *testpassword* as password. The hostname is *test-hostname.getmyip.com*.

```
   log-command-errors
   no configuration
   set hostname DYNDNS-LAN
   set data-link x25 serial0/1
;
   network ethernet0/0
; -- Ethernet Interface User Configuration --
      ip address 172.24.78.94 255.255.0.0
;
   exit
;
   event
; -- ELS Config --
      enable trace subsystem DNSU ALL
      ev-buffer 2000 200
   exit
;
;
   protocol ip
; -- Internet protocol user configuration --
      route 0.0.0.0 0.0.0.0 172.24.0.98
;
   exit
;
;
;
   feature dns
; -- DNS resolver user configuration --
      server 172.24.0.57
   exit
;
   feature dns-updater
; -- DNS UPDATER configuration --
      enable
;
      entry 1 protocol DynDNS system dynamic
      entry 1 interface ethernet0/0
      entry 1 hostname test-hostname.getmyip.com
      entry 1 servername members.dyndns.org
      entry 1 user testusername ciphered-pwd 0xE337A56B515214DFEF0D3AD93DC2C969
      entry 1 external-ip enable
      entry 1 external-ip server checkip.dyndns.org
;
   exit
;
   dump-command-errors
   end
```

Once the device is restarted, it checks the public IP address for the access router running NAT and executes the update in DynDNS.

```
01/15/08 11:28:16  DNSU.018 DNS UPDATER Initialized
01/15/08 11:28:16  DNSU.020 Entry 1 added
```

```
01/15/08 11:28:56  DNSU.021 Entry 1 needs to be updated
01/15/08 11:28:56  DNSU.013 Entry 1 Resolved server IP 63.208.196.96
01/15/08 11:28:56  DNSU.023 Entry 1 Dyndns check_ip successfully
01/15/08 11:28:56  DNSU.005 Entry 1 Creating DynDNS Dynamic prot message
01/15/08 11:28:56  DNSU.007 Entry 1 Received resp good
01/15/08 11:28:56  DNSU.009 Entry 1 IP updated
DYNDNS-LAN *
```

You can check the status through the statistics:

```
DYNDNS-LAN +feature dns-updater

-- DNS Updater console --
DYNDNS-LAN DNS Updater+list all

Entry    Protocol                Hostname                                Status
-----  --------------  ------------------------------------------  ------
  1    DynDNS dynamic  test-hostname.getmyip.com                    good

Entry       Last Update        Current IP         Updated IP
-----    -----------------  ----------------   -----------------
  1      01/15/08 11:28:56    172.24.78.94       xxx.yyy.zzz.1 (Ext)

          DNS query            External IP                  DNS Updates
Ent    done      error      done       error      asked      done       error
--- ---------- ---------- ---------- ---------- ---------- ---------- ----------
  1          2          0          1          0          1          1          0

Checking interval: 5 minutes
Time between forced updates: 25 days
DYNDNS-LAN DNS Updater+
```

Where xxx.yyy.zzz.1 is the public address for the router running NAT. There are two DNS checks: one to chekip.dyndns.org and the other to members.dyndns.org.

From this point on, checks are executed to see if there are changes to the public IP address.

```
DYNDNS-LAN *01/15/08 11:43:57  DNSU.023 Entry 1 Dyndns check_ip successful
DYNDNS-LAN *01/15/08 11:58:57  DNSU.023 Entry 1 Dyndns check_ip successfully
```

These changes can be seen in the statistics:

```
Entry    Protocol                Hostname                                Status
-----  --------------  ------------------------------------------  ------
  1    DynDNS dynamic  test-hostname.getmyip.com                    good

Entry       Last Update        Current IP         Updated IP
-----    -----------------  ----------------   -----------------
  1      01/15/08 11:28:56    172.24.78.94        213.4.21.187 (Ext)

          DNS query            External IP                  DNS Updates
Ent    done      error      done       error      asked      done       error
--- ---------- ---------- ---------- ---------- ---------- ---------- ----------
  1          4          0          3          0          1          1          0

Checking interval: 5 minutes
Time between forced updates: 25 days
DYNDNS-LAN DNS Updater+
```