DVX - 1000: Network Telephone Exchange

User Manual

Version 0.9

D-Link India Ltd.,
Software and R&D Center,
Bangalore.

Revision History

Originator	Comments	Revision Level	Release date
Hareesh N.S.	Initial Draft	0.1	18/05/2005
Sunil George	Updates for DVX-1000	0.5	16/06/2005
Sunil George	Added FAQ	0.6	21/06/2005
Sunil George	Added Conference server details	0.7	09/08/2005
Sunil George	Added product specs	0.8	08/09/2005
Sunil George	Updated for Rel-2.0	0.9	29/09/2005

Last Saved on 12/7/2005 10:25 AM

TABLE OF CONTENTS

1 Introduction

D-Link's Network Telephone Exchange (DVX-1000) is a SIP based solution, addressing the VoIP communication requirements of small and medium enterprises. DVX-1000 has built in Call Server, IVR/Auto-attendant and Voice Mail functionalities. It helps VoIP devices like SIP phones, gateways etc to make and receive calls, implements host of voice call features and manages accounts and provisioning of D-Link endpoints.

DVX-1000, developed around state of the art hardware and embedded software, are specially designed to address the requirements in the following environments:

- Installation of a new enterprise IP communications network.
- Expansion of an existing enterprise communications network.
- Cost effective branch office communications.

DVX-1000 has the following built-in components

- **Call Server**: A SIP based proxy server, that is responsible for call establishment, call control and call account management. In addition to the regular call processing, it offers a host of voice call features.
- **Auto Attendant**: The auto attendant is a complete automated attendant with customizable messages and configurable menu that helps the user to get to the required extension within the system.
- **Voice Mail Server**: DVX-1000 has a built-in voice mail server. Voice mail server is responsible for managing voice mail boxes of individual users.
- **License Server**: DVX-1000 comes with a license of maximum of 5 users and a set of basic features as default. A set of advanced features and more number of users can be added to the system. License Server manages licensing of users advanced features.
- **Provisioning Server**: Provisioning server is responsible for provisioning end points, that support D-Link's provisioning scheme.
- **Firewall**: A custom made firewall, this monitors and controls the packets going in and out of the DVX-1000
- **CLI**: The Command Line Interface (CLI) is accessible through the console port of DVX-1000. The CLI allows the administrator to view and modify system configuration parameters. The complete set of commands are described in detail in section *'Configuring the system through the Command Line Interface'*
- **Web Server**: DVX-1000 has a built-in web server, that helps administrators and users to access the system using a standard web browser.

1.1 About This Manual

This document provides information related to the installation and configuration of DVX-1000 along with a description of all its features. The tasks described in this document are intended for service providers and network administrators who guide the deployment of VoIP services.

Note:

Please contact Mr. Hareesh N.S. for suggestions regarding modifications to this document.

1.2 Conventions

This document uses the following notational conventions:

bold face	This convention is used to give **strong emphasis**.
0x0	Prefix to denote hexadecimal number.
0b0	Prefix to denote binary number.

1.3 Abbreviations

DVX – D-Link Voice Exchange
SIP – Session Initiation Protocol
CLI – Command Line Interface
IVR – Interactive Voice Response
DHCP – Dynamic Host Configuration Protocol
DNS – Domain Name Service
NTP – Network Time Protocol
CDR – Call Detail Record
PSTN – Public Switched Telephone Network

2 Getting started

To Set IP address through WEB, open the web browser and type in the default ip address of the board. The initial login page will appear. You will have to log in as administrator to set the system parameters. The default administrator user name and password is 'ippbx' and 'ippbx'.

1. Connect power supply to the DVX-1000 and power up.
2. Connect the LAN port to the HUB/Local Network
3. The power indicator and LAN indicator should be ON, if the corresponding LAN Port is connected to a Local Network.
4. DVX-1000 comes with the default ip address of 10.0.0.1. You can change the ip address through CLI (Command Line Interface) or web interface.

3 Configuring system parameters

DVX-1000 can be configured through the following interfaces

- The web interface
- Command Line Interface (CLI)

The following section provides details regarding how the DVX system can be configured through these interfaces. ***System configuration and call monitoring are solely the privileges of users configured as administrators.*** DVX-1000 ships with a single administrator already configured *(for security reasons, we recommend*

changing the default administrator password). Regular users are allowed to configure only their individual features.

3.1 Using the web interface to configure the system

The DVX-1000 web interface can be accessed from any web browser supporting frames and java script. Internet explorer (Version 4.0 and above) is the preferred browser. The web interface can be accessed using the URL http://IPADDRESS , where IPADDRESS is the address assigned to the DVX-1000 board. The system configuration page can be accessed by clicking the system configuration link from the DVX-1000 web interface.

3.1.1 DVX WEB Requirements

The following browsers have been tested to be fully compatible with the DVX-1000 web interface:

- Internet Explorer (Version 4.0 and above)
- Netscape (Version 7.0 and above)
- Mozilla (Version 5.0 and above)
- Galeon (Version 7.0 and above).

3.1.2 Configuring the IP

IP configuration for the DVX-1000 board can be static or through DHCP. The default factory setting for IP is 10.0.0.1. To bring the board up for the first time; configure an IP for the board from the CLI interface. Subsequently, all configurations can be done through the web interface by accessing the board's configured IP.

3.1.2.1 Configuring the IP address automatically using DHCP

DVX-1000 can be configured to get it's IP through Dynamic Host Configuration Protocol (DHCP). To enable this, select DHCP and click on Apply**. *Please note that on some browsers, redirection to the new IP is not possible***. In this case, the new IP has to be ascertained from the CLI interface and the corresponding web page should be accessed.

3.1.2.2 Configuring the IP address manually.

Assigning a static IP for the DVX-1000 is the recommended method for IP configuration as it is advisable to have the call server work on a fixed IP address. To configure a static IP for DVX-1000, click on the system configuration link. Now, under IP configuration, select static and enter a static IP, subnet mask and gateway. Click 'Apply'. ***Please note that on some browsers, redirection to the new IP is not possible.*** In this case simply access the new static IP that you have now configured for the board from the web.

3.1.3 Configuring the DNS server address.

DVX-1000 has a Domain Name Service (DNS) client built in that will resolve hostnames accessing the DNS server that is configured. To set the DNS server that is relevant to your network, access the system configuration page; modify the primary and secondary DNS servers and click apply.

3.1.4 Setting the system time.

DVX-1000 can either be configured to get its time through manual configuration or through Network Time Protocol (NTP). It ships with a factory default setting of 1st of January 2005 10.10 a.m. ***A large fraction of the call server data is dependent on the system time***. This data includes registrations, feature time settings and call detail records (CDR) amongst others. Changing the time configuration has to be done with a lot of caution. Changing the time to a time prior to the current time would be a malicious attempt to invalidate the call detail records and extend registrations. The administrator should be wary of this. Changing the time to one in the future should be done taking into account the fact that current registrations may expire at the new time specified and hence phones may have to re-register to get the calls started

3.1.4.1 Setting the system time manually.

In order to set the time manually, access the system configuration page. Under time configuration, choose manual and modify the time to the required value. Now click apply. The time should now be set to the new one.

3.1.4.2 Automatically configuring the system time using NTP

DVX-1000 can synchronize its system time with an NTP server that has been configured. This server could either be a local LAN NTP server, that in turn synchronizes with a stratum 1 or stratum 2 NTP server, or directly a stratum1 or 2 NTP server that is relevant to your network. Access the system configuration page, under time configuration, choose NTP and specify the primary and secondary NTP servers. Select the appropriate time zone. Click 'Apply'. The NTP servers will be tried for a predefined number of times and if these attempts fail, the present system time will be retained.

Note: Daylight savings time is automatically supported by DVX-1000 provided the system is configured to get the time from an NTP server and the correct time zone is selected.

3.1.5 Configuring the SMTP server.

DVX-1000 uses an Simple Mail Transfer Protocol (SMTP) server to send notifications by email. The server IP address and port have to be configured correctly for delivering mails. The default administrative user's email id will be used as the sender's address for sending notification mails. The SMTP server has to be an open relay mail server since DVX-1000 does not provide sender authentication credentials.

3.1.6 Setting other configurable parameters

The following options can be specified in this section.

RTP Port (Min & Max)	The minimum and maximum ports that DVX-1000 uses for its media. Changing this also modifies the firewall settings to block ports other than the ones configured.
Operator Number	The operator's extension that will be contacted if the call through the automated attendant fails, or if the caller dials an invalid extension or no extension at all.
Operator User Group	User Group of the operator.

3.2 Configuring the system through the Command Line Interface

This section describes the DVX-1000 system configuration through the command line interface. To access the command line interface, connect the console port of DVX-1000 to the 'com' port of your PC, using the supplied console cable. The terminal settings should be (15200 8-N-1). When the user connects to the DVX-1000 using the serial port, he will be prompted for login name & password. The user must be an administrator to log on to DVX-1000 and execute any CLI commands. Once the user name and password verification succeeds, the DVX command prompt will now appear and the user can now configure the system with the aid of the CLI commands described below.


Please make sure that the device is powered down before you connect the console port to avoid damage to the interface.

The CLI commands are structured in tree-style architecture. All the CLI commands are case insensitive & at any time the user can enter '?" to display what all commands are available at this level or depth.

3.2.1 Help Command:

Command Name: help

Command description: The 'help' command displays all the available commands to the console.

Command Format: help

3.2.2 History Command:

Command Name: history

Command description: The 'history' command displays the list of previously executed commands in the current session to the user.

Command Format: history

3.2.3 Set IP Command:

Command Name: set ip

Command description: The 'set ip' command is used for setting the IP address statically.

Command Format: set ip <ipaddress> <netmask (optional)>

e.g. set ip 192.168.10.89 255.255.255.0"

3.2.4 Set Netmask Command:

Command Name: set netmask

Command description: The 'set netmask' command is used for setting the netmask statically.

Command Format: set netmask <net mask>

e.g. set netmask eth0 255.255.255.0"

3.2.5 Set DHCP Command:

Command Name: set dhcp

Command description: The 'set dhcp' command sets the network configuration (such as IP address, netmask, etc) using DHCP.

Command Format: set dhcp

E.g. set dhcp

3.2.6 Set Gateway Command:

Command Name: set gateway

Command description: The 'set gateway' command configures the default gateway.

Command Format: set gateway <gateway ipaddress>

E.g. set gateway 192.168.10.6

3.2.7 Set DNS Server Command:

Command Name: set dnsserver

Command description: The 'set dnsserver' command configures the primary & secondary DNS server address.

Command Format: set dnsserver <primary dns server ipaddress> <secondary dns server ipaddress (optional)>

e.g. set dnsserver 192.168.10.5 192.168.10.6

3.2.8 Set Primary DNS Server Command:

Command Name: set primarydnsserver

Command description: The 'set primarydnsserver' command configures the primary DNS server address.

Command Format: set primarydnsserver <ipaddress>

e.g. set primarydnsserver 192.168.10.5

3.2.9 Set Secondary DNS Server Command:

Command Name: set secondarydnsserver

Command description: The 'set secondarydnsserver' command configures the secondary DNS server address.

Command Format: set secondarydnsserver <ipaddress>

e.g. set secondarydnsserver 192.168.10.6

3.2.10 Set NTP Server Command:

Command Name: set ntpserver

Command description: The 'set ntpserver' command configures the primary & secondary NTP server address. It will automatically sync the time with the NTP server.

Command Format: set ntpserver <primary ntp server ipaddress> <secondary ntp server ipaddress (optional)>

e.g. set ntpserver 192.168.10.9 192.168.10.10

Warning: On executing the following NTP server commands the system will assume that the time configuration should be obtained from the NTP server and the time configuration will be set to 'NTP server' if it is in manual mode currently. If you do not want this to happen, please undo the change through the web page.

3.2.11 Set Primary NTP Server Command:

Command Name: set primaryntpserver

Command description: The 'set primaryntpserver' command configures the primary NTP server address. It will automatically sync the time with the NTP server.

Command Format: set primaryntpserver <ipaddress>

e.g. set primaryntpserver 192.168.10.9

3.2.12 Set Secondary NTP Server Command:

Command Name: set secondaryntpserver

Command description: The 'set secondaryntpserver' command configures the secondary NTP server address. It will automatically sync the time with the NTP server if not already sync with the primary NTP server.

Command Format: set secondaryntpserver <ipaddress>

e.g. set secondaryntpserver 192.168.10.10

Warning: Using the following commands to configure the system time will result in the time configuration mode being set to manual. If you do not want this to happen, please undo the change through the web page.

3.2.13 Set Zone Command:

Command Name: set zone

Command description: The 'set zone' command sets the system time zone. Use 'set zone ?' to get zone numbers.

Command Format: set zone <zone number>

e.g. set zone 4 to set pacific time zone.

3.2.14 Set Date Command:

Command Name: set date

Command description: The 'set date' command configures the system date and time manually. All the parameters have to be given in the same order as they appear in the format below. However, the user can give any number of parameter; all the other parameters will be set to current value.

Command Format: set date <year> <month> <day> <hour> <minute> <seconds>
e.g. set date 2005 Jan 30 10 35 45

3.2.15 Set Time Command:

Command Name: set time

Command description: The 'set time' command configures the system time manually. All the parameters have to be given in the same order as they appear in the format below. However, the user can give any number of parameter; all the other parameters will be set to current value.

Command Format: set time <hour> <minute> <seconds>

E.g. set time 15 35 45

3.2.16 Set Year Command:

Command Name: set year

Command description: The 'set year' command configures the year parameter of the system date.

Command Format: set year <year>

E.g. set year 2005

3.2.17 Set Month Command:

Command Name: set month

Command description: The 'set month' command configures the month parameter of the system date.

Command Format: set month <month>

E.g. set month Jan

3.2.18 Set Day Command:

Command Name: set day

Command description: The 'set day' command configures the day parameter of the system date.

Command Format: set day <day>
E.g. set day 30

3.2.19 Set Hour Command:

Command Name: set hour

Command description: The 'set hour' command configures the hour parameter of the system time.

Command Format: set hour <hour>

E.g. set hour 10

3.2.20 Set Minute Command:

Command Name: set minute

Command description: The 'set minute' command configures the minute parameter of the system time.

Command Format: set minute <minute>

E.g. set minute 35

3.2.21 Show IP Command:

Command Name: show ip

Command description: The 'show ip' command displays the configured IP address of the system.

Command Format: show ip

3.2.22 Show Netmask Command:

Command Name: show netmask

Command description: The 'show netmask' command displays configured system netmask parameter to the user.

Command Format: show netmask

3.2.23 Show Gateway Command:

Command Name: show gateway

Command description: The 'show gateway' command displays default gateway configured for the system.

Command Format: show gateway

3.2.24 Show DNS Server Command:

Command Name: show dnsserver

Command description: The 'show dnsserver' command displays the primary & secondary DNS server IP address.

Command Format: show dnsserver

3.2.25 Show Alarms Command:

Command Name: show alarms

Command description: The 'show alarms' command displays alarms being raised by the DVX.

Command Format: show alarms

3.2.26 Restore Certificate Command:

Command Name: restoreCert

Command description: The 'restoreCert' command restores the default SSL certificate that came installed with DVX-1000.

Command Format: restoreCert

3.2.27 Restart Command:

Command Name: restart

Command description: The 'restart' command restarts DVX-1000.

Command Format: restart

3.2.28 Ping Command:

Command Name: ping

Command description: The 'ping' command tests the network connectivity to another host.

Command Format: ping <ipaddress>

3.2.29 Traceroute Command:

Command Name: traceroute

Command description: The 'traceroute' command tarces the route to another network host.

Command Format: traceroute <ipaddress>

Note: Please make sure that the firewall is stopped before traceroute is used.

3.2.30 StartFirewall Command:

Command Name: startfirewall

Command description: The 'startfirewall' command starts the systemfirewall.

Command Format: startfirewall

3.2.31 StopFirewall Command:

Command Name: stopfirewall

Command description: The 'stopfirewall' command stops the system firewall.

Command Format: stopfirewall

Note: CLI help appears skewed in HyperTerminal because it wraps the lines at 80 columns and inserts a new line.

4 Configuring the Call Server

The following section explains the functionality of the various call server features and also provides information about how the features and the basic call server system parameters are to be configured.

4.1 General Configuration

The DVX-1000 Call Server configuration information can be viewed by clicking **Call Server -> Configuration**. To change the configuration, click on Edit. The following configuration options can be changed.

Domain	Specifies the SIP domain that this server manages. This will be used in all the SIP addresses on this server.

Port	Specifies the UDP port number on which call server would listen for SIP messages. ***Some ports are internally used by the call server, auto attendant and media server and are reserved.*** If the port specified here conflicts with one of the reserved ports, an error message will be displayed.
Default Authentication	Specifies the default authentication scheme that will be used to authenticate SIP user. Note that the authentication scheme is configurable per user (during user configuration).
Default Expiry Time	Specifies the default expiry time for SIP registrations. This value will be used for registration requests when neither the Expires header is present nor is an expires parameter specifed in contact header. Default Expiry Time is specified in seconds.
Min (Expiry Time)	Specifies the minimum expiry time the server would accept for SIP registrations. Registration requests with smaller expiry time will be rejected with a 423 (Interval too brief).
No Answer Timeout	The time for which a call will be tried, before it is assumed that the user is not answering. This can be specified anywhere between 10 and 30 secs.

4.2 User Configuration

A user needs to be configured before registration. The current user configuration information can be obtained by clicking, **Call Server->Users**.

4.2.1 Adding a new user

A new user can be added by clicking, '**ADD'**. User configuration changes done through web interface will take effect immediately. The following user configuration options can be added or modified.

User Name	Name of the user. Used only for display purposes.
User Extension	SIP (user Extension) user identifier with which the client would send registration. This could be the phone number of a sip phone. Example: for user extension 9001 and domain name dlink.co.in, the client would use the URI sip:9001@dlink.co.in for registration.
Email ID	User's Email id.
RouteGroup	Route group that the user belongs to. DVX-1000 comes with a default route group configured with a local route, for all local numbers to be contacted.
UserGroupId	UserGroup to which the user belongs. Every user belongs to alteast one of the user groups. Which users group a particular user belongs to will determine the functionality of some features like call pickup. *Please refer to the call pickup feature description for details.*
Authentication Required	This specifies whether the user needs to be authenticated by the call server for registration and

	for regular calls. Check the appropriate check box.
Password	This specifies the password for authenticating the user. This along with the user extension will be used to calculate the actual digest response for the user.
User Type	This specifies whether the user is to be given administrative privileges or not.
Password	Password to be used for logging into the user WebPages. Click on change password and enter the new password. The default password is the user extension of the user. ***Please note that this is the login password of the user NOT his SIP authentication password.***

4.2.2 Customizing features for users.

Clicking the  icon in the 'Feature' column in **Call Server->Users** page will show the Feature Information for the corresponding user. Activation and deactivation of all features for that user can be done from here.
The features currently available for configuration are described below.

Do not disturb	Redirect all your incoming calls to your voice mailbox
Follow me – call forwarding	Same as Call forward, but the options for forwarding incoming calls can be controlled more minutely based on the time, date and day of week. This is described in more detail in the Section 4.2.2.1.
Call forward	Forward all incoming calls to the specified number.
'Always'	Blindly forward all incoming calls.
'No answer'	Forward incoming calls if it is not answered within the 'No answer timeout'
'On Busy'	Forward incoming calls if the extension is busy.
Change feature password	Change the password used for feature activation and deactivation from a phone. This password is also used for accessing the user's mailbox.
No answer timeout	The time after which incoming calls are forwarded when Call forward on No Answer is enabled.

4.2.2.1 Configuring Follow me – call forwarding.

Follow me – call forwarding can be used to control the way incoming calls are handled based on the time of the day, date and/or the day of week. The configuration parameters can be accessed by clicking on the 'Setup' hyperlink on the feature configuration page.

The call is forwarded based on a set of rules that are displayed on the top pane of the web page (by default, this list will be empty). Each rule has the following configurable parameters.

Forwarded No.	The number to which the call will be forwarded if it matches this rule.
Time	Select a duration within which this rule will be active, or select 'Always' to make this rule active at all times.
Date	Select the dates between which this rule should be enforced.
Days of week	Select the weekdays on which this rule will be effective, or select 'All days' to activate this rule irrespective of the weekday.

4.2.3 Modifying user details.

Clicking  icon in the *EDIT* Column in **Call Server->Users** will allow you to edit user information. All the information that is configured while adding the user, except the 'User Extension' can be modified here. Please refer Section 4.2.1 for the details regarding the configuration parameters.

4.3 Registrations

Current user registrations can be monitored by accessing
Call Server->Registrations
The administrator may add or delete a registration if required. However, registration through SIP messaging is recommended. The following values need to be provided for adding a registration.

Note: A new registration for a particular user extension cannot be added unless a SIP user is configured with that extension.

User Extension	Specifies the user extension for registration. For the registration to be successfully added, the user extension should be a configured user in SIP users.
Contact	Specifies the contact for registration. Any SIP call to the user identified by User extension will be redirected to this Contact value. Example: sip:9001@192.168.100.101
Priority	Specifies the priority value for the contact. Priority value is a value between 0.0 and 1.0, with 0.0 indicating least priority and 1.0 indicating highest priority. This is used to prioritize between contacts if more than one contact exists for a user extension. Refer to Q Value in SIP RFC 3261 for more details
Expiry Time	Specifies the expiry time for the registration. The registration would expire after the specified expiry time. While adding a registration, Expiry Time is specified in seconds, whereas while displaying current registrations, it shows the time and date at which the registration would expire.

4.4 Configuring Gateways

Gateways are used to connect DVX-1000 to external SIP based servers or PSTN network. DVX-1000 can be connected to other SIP servers by configuring the servers as 'INET' gateways. DVX-1000 can connect to PSTN network through a 'PSTN' gateway. ***This is not to be confused with the default gateway configured during system configuration.***

The Gateway configuration information can be viewed by clicking **Call Server-> Gateways**. To add a new gateway, click on 'Add New'. The following parameters are to be configured.

Gateway Id	A unique Gateway Id
Gateway Type	The type of gateway. It can be INET / PSTN
Domain Name	Specifies the domain name / IP address of the Gateway. This is used and the domain name/IP Address when the call server has to register to the gateway.
Port	Specifies the port number that the gateway is configured on.
Max Calls Supported	Limits the number of simultaneous calls through this gateway if a value is entered or allows unlimited calls. If the checkbox is selected.
Outbound Proxy Enabled	Check this box if the gateway is connected through an outbound proxy.
IP Address	IP Address of the outbound proxy.
Port	Port number of the outbound proxy.
Registration Required	Check this box if DVX-1000 needs to register with the external gateway.
SIP User extension	SIP User extension associated with this gateway
User Name	SIP display name for the gateway user
Password	Specifies the password associated with this gateway. This will be used for authentication.

4.5 Configuring Routes

The Route configuration information can be obtained by clicking **Call Server->Routes**. To add a New RouteGroup configuration, click on Add New. Atleast one route should be created and added while creating a RouteGroup. The Route View Column helps in viewing all the Routes belonging to a RouteGroup. New Routes can be Added / Deleted / Edited from here. Routes can be moved from one RouteGroup to another by editing a Route. All Routes except the highest priority Route can be deleted from a RouteGroup. Deletion of a RouteGroup is possible only if it is not being used by any user.
The following are the route configuration options.

RouteGroupName	Specify a new unique RouteGroup Name (Max 20 Char)

Duration Parameters	Specify the time for which this Route is valid. All time parameters are mandatory.
Route Name	Specify a new unique Route Name (Max 20 Char)
DestinationType	Type of the Route Destination. It can be LOCAL/PSTN/INET.
Destination Id	Indicates the Gateway Id corresponding to this route. For LOCAL destination type Gateway Id need not be specified, hence disabled.
Priority	Indicates priority of this route in its RouteGroup. The value can be in the range of 1 to 25. If the new route is added with an existing priority, the priority of the old Route will be incremented to next value.
Min Digits	Indicates the minimum dial digits for this route
Max Digits	Indicates the maximum dial digits for this route.
No of Mask Digits	Indicates the number of Dial Digits to be masked.
Dialed Digits	Dialed strings to be matched to select this route entry. A dialed string of '*' matches any string of 0 or more elements.
Prefix	Prefix to be added to the number after masking.

4.6 Configuring Groups

The Group configuration information can be viewed by clicking **Call Server->Groups**. Groups can be of two types

- UserGroup
- Hunt Group

The user group is specifically used for determining user privileges during Call Pickup. A particular user can pick up calls for him on another extension only if that extension belongs to the same user group as him. A new Group can be added by clicking Add New. A unique Id needs to be given to each Group. Group Type distinguishes between a user group and a hunt group. The mode field is relevant only to a hunt group. A hunt group can be configured in three modes (First Only /Sequential /Parallel). Members in a user group are added when the user is actually added to the call server. Hunt Group members can be added/edited/deleted by clicking the edit button in the 'View members' page.
A group can be deleted only if it does not contain any user.
Note: Each Group (User/Hunt Group) can have a maximum of 20 users. Beyond this a new user group has to be created to add more users. Also, a user can belong to a maximum of 5 user groups.

5 Using the feature manager

The following section gives an overview of what the call server features are, how they are to be activated and what their functionality actually is.

5.1 Configuring features

Feature configurations can be viewed by following the links **Feature Manager->Feature Configuration**. Feature prefix and the list of features can be viewed. Feature prefix specifies the digit user needs to dial while activating/deactivating feature from the phone. The default value is '*'. The feature configuration page displays the following fields for each feature.

Feature Name	Specifies the name of the feature
Feature Code	Specifies the feature code. This feature code needs to be dialed when activating/deactivating a feature from the phone. This can be configured to be a custom number. Care should be taken that no two feature codes conflict.
Edit	This link can be followed to change the feature code for the feature

5.2 Activating and deactivating features

Feature activation can either be done from the web interface or from a phone. ***However, activation of sending voicemails through email can be done only through the web and for certain features where additional data is essential (for instance, a call forwarding number for call forward, or a time interval for follow me – call forwarding and so on), the additional data has to be entered through the web interface***. Once this information is available the feature can be activated/deactivated from either the web or the phone interface. Activating these features from the phone without entering the required additional data for them beforehand will create unpredictable scenarios.

5.2.1 Activating and deactivating features from the Web Interface

Features can be activated or deactivated from the web interface by clicking on the **Call Server->Users** link and then clicking on the feature column for the user whose features are to be modified. When logged in the user mode, this link is accessed as feature setting from the home page.

5.2.2 Activating and deactivating features from the phone

Feature activation/deactivation can also be done from the phone by dialing a sequence of digits in the format '**FCCAPPPP'.** Here **F** is the single digit feature prefix configured (default is *) **CC** is the 2 digit feature code for the feature, **A** is the activation/de-activation state for the feature (1 for activation or 0 for deactivation) and **PPPP** is the four digit feature password. For example, if * is the feature prefix, 14 is the feature code for 'Do Not Disturb – Forward to Voicemail' and 1234 is the password, user could dial *1411234 to activate 'Do Not Disturb – Forward to Voicemail' feature.

5.3 Call Feature Description

The following section discusses call features that DVX-1000 offers. An important thing to be considered is that each of these features has a priority, so that, if two features are enabled simultaneously, the feature with the higher priority will be the one that will get activated.

For instance, if Do Not Disturb: Always and Call Forwarding: Always are enabled simultaneously, when an incoming call comes, it will automatically get forwarded because Call Forwarding has a higher priority as compared to Do Not Disturb.
Refer the Feature Priority Table *for further details*.

5.3.1 Call Forward

This feature enables the user to forward incoming calls to a configured number based on the subtypes he has enabled.

5.3.2 Call Forward: Always

When this particular subtype of call forwarding is enabled, all incoming calls will be forwarded to the configured forward number. This subtype overrides all other selections for call forwarding.

5.3.3 Call Forward: On Busy

This subtype allows the user to configure a number where all calls will be forwarded if the user is busy. This can be activated with Call Forward: No Answer.

5.3.4 Call Forward: No Answer

This subtype allows the user to configure a number where all calls will be forwarded if there is no answer from the user. The time defined for No Answer can be configured. (For e.g., if the No Answer Timeout interval is configured as 20 secs, when there is no response from the user for 20 secs, the call will get forwarded).

5.3.5 Do Not Disturb – Forward To Voicemail

This feature can be configured when the user doesn't want to be disturbed. All the calls would be forwarded to voicemail.

5.3.6 Follow Me – Call Forwarding

This feature allows a user to configure DVX-1000 to forward calls to different numbers based on time. This feature is very useful when a user knows where he will be during a particular interval of time on some day, and all calls to him will be forwarded to a number he has configured for that time interval. The advantage of this is that the whole process is transparent to the calling user. So, irrespective of where the called user is, he will be able to receive his calls normally.

A typical scenario is described below:
User 4000 is in the office on Mondays, Wednesdays and Fridays between 10:00 a.m. and 4:00 p.m. He can directly be contacted at his official number (say sip:4000@dlink.co.in) at this time. He works from home on all other days within that time and all his calls should be directed to his home number (sip:home@dlink.co.in).His setup will be as follows:

- In the follow me time setup, add a time configuration with the time interval as 10:00 to 16:00, date as 1:08:04 to 31:12:04 and day of week as Monday, Wednesday and Friday and forwarded number as his office number.

- Add another time configuration with the time interval as 10:00 to 16:00, date as 1:08:04 to 31:12:04 and day of week as Tuesday, Thursday, Saturday and Sunday and the forwarded number as his home number.

With this setup, depending on the time and day of week all his calls will be allowed to "Follow" him. The location of the user will be completely transparent to the caller.

5.3.7 Receive voicemail by email

If this feature is enabled, the voicemail messages will be forwarded as a wave file attachment in the voicemail notification mail sent to the users email id. Please note that the users email id should be provided in the user configuration for this feature to work.

5.3.8 Hunt Group

This feature allows multiple users to be contacted by dialing into one configured hunt group number. Any call to the hunt group number will be forwarded to all the users configured in that number based on the mode of hunt group. Hunt Group can have three modes, FIRST-ONLY, SEQUENTIAL and PARALLEL. For First-Only only the first hunt group number will be tried, for sequential all hunt group numbers will be tried but in a sequential manner and in case of Parallel mode all hunt group members will be tried parallel.

6 Configuring the Auto Attendant

Auto attendant is a licensed feature of DVX-1000. The features described in this section will be available only after purchasing the license for the same.

6.1 Configuring voice prompts

DVX allows you to use your recorded voice prompts in the menus. You can upload and delete voice prompts through the web page provided. Click on 'voice prompts ' to get to the upload page.

The left pane of this page is used to upload the voice prompts and the right pane shows a listing of the prompts that are currently available to the user.

6.2 Uploading voice prompts.

DVX allows upload of one or more prompts simultaneously (limited to a maximum of nine at a time). The box labeled 'Number of voice prompts' can be used to specify the number of voice prompts you want to upload at a time, by default this is set to one.

Set this number and click on 'OK', a corresponding number of upload boxes will appear in the left pane. Click 'Browse' to select the voice prompt to be uploaded.

Click on upload to upload the selected prompts.

Currently, only files with the following parameters are supported

Format: wav (8kHz, 8bit, mono, muLaw).

Max file size: 200 Kb.

Note: Please make sure that the voice prompt name is unique to avoid overwriting built in prompts. For the names of the built in prompts please refer prompts list included in the release (DVX-1000 Media Files List.xls).

6.3 Deleting voice prompts.

The right pane of the voice prompts configuration screen lists all the prompts currently available to the user. Select the prompts you want to delete by clicking on the name; you can select multiple prompts by holding down *'shift'* or *'ctrl'* while clicking on the prompts. Now, click on 'Delete' to delete the selected prompts.

6.4 Customizing your menus.

You can customize the way the IPPBX presents options to users who dial into the auto attendant, select your preferred prompts which are to be played when certain common events occur and specify an auto attendant number into which users can dial into access this menu.

6.5 Configuring auto attendant parameters and selecting preferred prompts.

The number to which the users dial in to access the menu can be set in the input box titled *'Auto Attendant Number'.* Second, part of the page allows you to select the preferred voice prompts. The drop down list contains all the voice prompts that have been uploaded by the user.

The various prompts given and their use is given below.

Welcome Message	Played at the start of the first menu. This can contain the greeting message.
Transfer Message	Played when the user is forcefully transferred to the operator. eg. When there is no input.
Error Message	Played when the digit dialed by the user is unrecognizable or invalid in the context of the current menu.
Retry Message	Played when there is no input from the user for an interval of 6 seconds.
Music on hold	Played when the call is being transferred.

6.6 Configuring menus.

Click on 'main menu' or 'holiday menu' hyperlink to get to the menu configuration screen. Each option to be presented as a part of the menu can be configured here.

The top half of the page can be used for configuring and adding the menu options and the bottom half lists the menu items that have been configured.

You can specify the *'Key'* that activates each option, the *'voice prompt'* to be played to announce the availability of that option and the *'action'* to be performed when that key is pressed by the user.

Each of the parameters that can be configured for the menu options is explained below.

Key: This is the DTMF digit that activates the menu option. If the user dials this digit the action specified will be executed.

Prompt: Select the voice prompt that describes the menu option here. eg. "*Dial zero to contact sales".* The voice prompts can be uploaded through the voice prompts

configuration screen. All the voice prompts that have been uploaded will be available for selection from the drop down box.

Action: The four types of actions are possible for menu options.

Transfer to number	Transfer the call to the number specified in the input box.
Dial Extension	Prompt the user to dial an extension and transfer the call to this extension.
Sub-menu	Transition to another menu which contains further options.
Previous menu	Go back to the menu from which the current menu was invoked. This action will not be available in the top level menu.

If you have selected 'sub-menu' as the action for any of the menu options, the sub menu configuration page for that option can be accessed by clicking on the sub-menu hyperlink that appears in the menu option listing.

6.6.1 Adding menu options

1. Select the key that activates this option from the drop down list.
2. Select the prompt that describes this option.
3. Select the action that is to be performed when the key is pressed.
4. If the action is Transfer to number, enter the number to which the call should be transferred.
5. Click on 'ADD' to add the menu option to the list of configured options.
6. If the action selected was 'sub-menu', click on the sub-menu hyperlink to go to the sub-menu configuration page.

6.6.2 Editing menu options

1. Click on the edit icon next to the menu option you want to change.
2. The fields on the top half of the page will be filled with the values from the option you want to edit. Change the required fields.
3. Click on Update, The changes will reflect in the configured options list.
4. If the action was changed to 'sub-menu', click on the sub-menu hyperlink to go to the sub-menu configuration page.

6.6.3 Deleting menu options

1. Select the check box corresponding to the option you want to delete.
2. Click on 'Delete' at the bottom of the screen.
3. The selected menu options will be deleted from the list.

6.7 Holiday menu configuration.

The Holiday menu configuration can be accessed by selecting the 'holiday menu' hyperlink from the configuration page. The configuration tasks are identical to the main menu mentioned above.

6.8 Configuring calendar information

DVX provides support for configuring the work information and a list of holidays, based on which it will automatically select between the main menu and holiday menu if both are configured.

The work week configuration includes configuring the work week, i.e. selecting the days of week that are working days, and also the start time and end time of a typical working day.

The work week can be specified by selecting the corresponding check box and the start time and end time can be entered in twenty four hour format.

A list of holidays can also be configured by doing the following.

1 Click on the calendar icon and select a date, or enter the date in (dd-mm-yyyy format) manually.

2 Click on 'Add' to add it to the list of holidays listed on the right side.

To delete, select the holidays in the listing and click on 'delete'.

After all the changes have been made, click 'Apply' to update the configuration.

6.9 Restoring the default menu

DVX gives you an option to revert back to the original menu that it came configured with. Selecting this option will result in all your configured menus being removed.

Please note that the voice prompt configuration will not be restored. The prompts that you have configured in the Configuration page will remain active for the default menu.

6.10 Making calls through the auto attendant

1. Configure a SIP enabled phone to register with the DVX-1000 NTE.
2. Dial the auto attendant number configured by the administrator.
3. Follow the instructions to contact the desired extension.

7 Configuring the Voicemail Server

7.1 Configuring voicemail parameters

The voice mail server configuration includes setting the voice mail number, i.e. the number to which a user has to dial in to access his mailbox. The administrator can also specify a mail box size. This will be enforced on a per user basis. These configuration parameters can be accessed from **Voicemail -> Configuration**.

7.2 Using the Mail Box Admin

List of current voice mails can be viewed by following the link **Voice Mail -> Mail Box Admin**. The administrator can view voice mails based on User or All.

In order to see all voice mails, select the 'All' option and click on 'Show Voice Mail Info' icon. To view the voice mails for one or more users, select 'user', then add users into 'Selected Users List' and then click on 'Show Voice Mail Info' icon. The following information is displayed for each voice mail.

To	Shows the user for whom the voice mail is recorded.
From	Shows the user from whom the voice mail is received
Size	Specifies the size of the recorded voice mail file.
Received	Specifies the time at which the voicemail was received.
Priority	A '!' in this column indicates a high priority voice mail.

New voice mails are displayed in **bold** font. Click on any of the column headings to sort the voice mails

7.3 Using the voice mail server

7.3.1 Leaving a voice message for another user

1. Dial the user's extension.
2. If the user does not answer his phone and has enabled voicemail feature, you will be transferred to his mailbox.
3. Speak into your phone to record your message, press any key on the phone when you are finished.
4. The message will be replayed for you, Press '0' to save the message, '1' to discard the message and end the call, or '2' to re record the message.
5. If you pressed '2', you will have to repeat the steps starting at Step 3.
6. If you pressed '0', you will be asked to set a priority for the message. Press '1' to set the priority as 'Normal', or '2' to set the priority to 'Urgent'.

7.3.2 Accessing your voice mailbox

1. Dial the Voice Mail number from your phone (Default number is 350).
2. If you want to check the mail box of the extension you are currently dialing from, enter your PIN (Feature password), using the phone keypad. If you want to check the mailbox of another extension, press '*', you will be prompted to enter the extension number followed by the PIN number.
3. After the PIN number and extension is validated. Press '1' to retrieve message from your mailbox or press '2' to customize your mailbox.

Note: You can dial '*' to end the call, or dial '0' to go to previous menu from any of the menus

7.3.3 Retrieving voice messages from your voice mailbox.

When you enter your mailbox the number of messages currently in the mailbox will intimated. You can Dial '1' to listen to current message, '2' to listen to next message, '3' to move to previous message, '4' to delete the current message, '5' to forward current message,'6' to listen to the message information or '#' to call back the user.

7.3.3.1 Forwarding a voice message

1. If you dialed '5' in voice mailbox you will be played the forwarding menu.
2. Dial '1' if you want to send a forwarding note with the forwarded message. Dial '2' if you want to forward without a forwarding note.
3. If you dialed '1', you will be asked to record the forwarding note. Speak into the phone to record the message, press any key when you are done.
4. You will be asked to save or discard the forwarding note dial '0' to save the note or '1' to discard it.
5. After you complete steps 3 and 4 or if you dialed '2' in Step 2, you will be asked to enter the forwarding extension. Dial the extension you want to forward the message to.
6. You will be played a confirmation message indicating the status of the forward.
7. You can choose to forward the same message to another extension or you can dial '0' to go back to your mailbox.

Note: if you forward a message to the same extension more than once, only one copy of the message will actually be forwarded, except if it has a forwarding note.

7.3.3.2 Listening to message information

1. If you dialed '6' in the voice mailbox, you will be taken to the message information menu.
2. Dial '1' for caller id, '2' for time of recording and '3' for date of recording.

7.3.4 Customizing your mailbox greeting

1. If you dial '2' after PIN validation. You will be taken to the greeting customization menu the following options can be configured here.
2. Dial '1' to play default greeting, '2' to play user greeting, '3'play active greeting, '4' to record user greeting, '5' enable default greeting, or '6'enable user greeting.

The enabled greeting will be played when any user dials into your mailbox.

7.4 Voicemail notification by email.

Users can receive notifications through email when a new voicemail is available in his voice mailbox. In addition each user can indicate whether he wants to receive the actual voicemail message as attachment to this notification mail. For voicemail notification to work properly the user's email id has to be configured correctly. The default administrators email id will be used as the id of the sender for the notification. Please note that this is a licensed feature of DVX-1000 and will be activated only if the license is purchased.

8 Configuring the conference server

Multi-party conferences can be scheduled and conducted using the conferencing facility built into DVX-1000. Conferences can be conducted among SIP based phones. Three are two kinds of users, Creators and participants. Only the users with 'Creator' privileges can create and delete conferences. By default the IPPBX Administrator has the 'Creator' privileges. A conference can be one of two types, DIAL-IN conference

and DIAL-OUT conference. In a DIAL-OUT conference the server will automatically start the conference by dialing out to the participants at the scheduled start of the conference, whereas, in a DIAL-IN conference the participants are required to dial the conference number to join the conference. However, participants can dial in to the conference number at any time during the conference period irrespective of the type of the conference.
The following are the global parameters that the conference uses; these remain the same across conferences. They can be accessed through 'Conference->Configuration'

Retry count	This specifies the number of times a participant will be dialed out, if he/she is busy.
Timeout	This specifies the time interval (in seconds) after which a participant will be dialed out he/she is busy.
Mute	This specifies the digits the participant has to enter through his phone keypad to Mute.
Unmute	This specifies the digits the participant has to enter through his phone keypad to unmute himself.

8.1 Adding users to the conference creator list

Normal users can be given conference creation privileges by adding them the to conference creator list. This can be done by accessing 'Conference->Creator List'. Click on Edit and select the users you want to give creator privileges to. Creators can edit and delete conferences created by them. In addition the Administrator can delete conferences created by him or any other creator, but can edit only conferences he scheduled himself. The administrator by default has creator permissions, but a normal user who has been given admin privilege will not be automatically given creator privileges, this has to be done explicitly through the CLI or Web.

8.2 Scheduling a conference

Conferences can be scheduled by accessing the link 'Conference->Conference List'.

Click the "Add New" button and fill the following fields.

Conference Number		Specify a unique Conference Number
Conference Type		Specify the type of conference (Dial-In/ Dial-Out).
Duration Parameters	**Time**	Specify the time parameters for the conference. The start and stop time (24hour clock), Start and Stop Date, and the Days on which to start the conference.
	Date	
	Days of week	
Conference Parameters	**Topic**	Specify the Topic for the conference (should be brief) this will be displayed in the conference list
	Description	A more detailed description of the conference (optional)
	Allow	Select 'All Users' to allow any user to log on to the conference, (provided he knows the PIN if authentication is required for the conference).
Authentication Parameters	**Authentication required**	Fill these values if authentication is required for the conference. Click on the 'authentication required' check box and enter the pin number in the 'PIN' and 'Retype PIN' fields. Participants can join the conference only by entering these digits from their phone.
	PIN	

8.3 Viewing conference details

Conference details can be viewed by accessing the link 'Conference->Conference List'. Click the "  " icon.

8.3.1 Icons explained


This appears next to the user with administrative rights


This appears next to a user who is not active in this conference


This appears next to a user who is currently participating in the conference


Conference is inactive; this conference has not started yet.


Conference is active.


Conference is over; this indicates one of the following three conditions.

- The scheduled time of the conference is over.
- The conference cannot be started due to some configuration error.
- The conference was stopped manually by the creator.

8.3.2 Editing the participants list

Participants can be added and removed from the conference by clicking on the "Edit" button. A window will popup with the user list and the current participant list which can be used for editing the participant list.

8.4 Viewing conference reports

Conference reports can be viewed by accessing the link 'Conference->Conference List'. Click the "  " icon. Then click on the Click the "  " icon next to the report you want to view .The report of the conference will be displayed. This will show the last log on and log off time of each user and also other conference details such as the Topic description, start and end time of the conference. Please note that if a user has been manually removed from a conference his details will not appear on the report. When a conference is deleted, the report is also deleted with it.

9 Licensing

DVX-1000 comes preloaded with a license of maximum of five users and a set of basic features as default. A set of advanced features and more number of users can be added to the system.

The basic set of features are:

- Caller ID
- Call waiting
- Call History
- Call Hold
- Call Transfer
- Cross-Connect to other DVX-1000

The following advanced features are available through licensing

- Auto Attendant
- Customizable greetings
- Interactive Voice Response (IVR)
- Follow-Me Call Forwarding
- Forward all calls
- Forward calls when busy
- Forward calls when no answer
- Do Not Disturb—forward all calls to voicemail
- Voicemail
- Voicemail notification via email

The license for the advanced features/additional users can be purchased. Please contact D-Link customer support for more information. After purchasing the license, the license code can by applied to DVX-1000 either by copy-pasting the license code or by uploading the file containing the license code.

Administrator can view all the successfully applied license codes along with its details from the **License->History** page.

10 Provisioning

The provisioning server is used to configure compatible devices to interoperate with DVX. The Administrator needs to add the mac address of the device which is to be provisioned. This is used for initial authentication and to send the sip credentials to the device. Addition of a new device or deletion of an existing one can be done through **Provisioning->DeviceList** page of DVX web interface. User has to provide the MAC address of the device and the sip users that are to be used with the device. These sip users should have been created earlier through **CallServer->Users->Add users** page. Provisioning server supplies an Authentication key (a 48 hex bytes) to the device on the first communication. This authentication key along with the sip credentials and MAC address can be seen on the **Provision->DeviceList->view ports** page for each device. The authentication key can be cleared by clicking the **'Clear Key'** button. The sip user list can be edited by clicking the **'edit'** button.

The configuration file that has to be sent to each of these devices has to be uploaded to DVX through the web interface. These files are identified by Vendor id and Model no. Administrator has the option to add a new configuration file or delete a configuration file from the **'Provisioning->Configuration file'** page.

11 Software Upgrade

It is possible to remotely upgrade the DVX-1000 software. This is done by accessing the web link software upgrade from the home page of the DVX-1000 web interface. The software to be upgraded will be sent to the administrator in the form of a zipped tar file DVX_v1.0.0.tgz.The following steps are to be followed to upgrade the software.

11.1 Upgrading from a Windows machine

- Extract the file to a directory say c:\DVX_v.1.0.0
- Access the web interface of DVX-1000 and login as the administrator user
- Click on software upgrade
- A new window will pop up asking you to enter the script file name
- Here browse and choose the script upgrade.sh from the c:\DVX_v.1.0.0 directory and click upgrade
- If the script was accepted correctly you will now see a prompt with a request for the various modules to be upgraded one by one
- .All these binaries will be in the c:\DVX_v1.0.0 directory where you extracted the upgrade package.
- Specify this path and click on upgrade.
- When upgrade for that particular module is successfully complete, It will prompt for the next module.
- Follow the same procedure as given above for the rest of the modules
- Once all the modules have been upgraded you will now see the upgrade status of all the modules.

11.2 Upgrading from a Linux machine

The procedure in this case is similar except that instead of extracting it to c:\DVX_1.0.0 the directory would now be /root/tmp/DVX_1.0.0.The rest of the process is similar to the windows procedure

11.3 Viewing Upgrade History

It is possible to view the upgrade history of the DVX-1000 from its web interface. When the link History is clicked from the home page of the DVX-1000 web interface, a pop up window appears. This page contains details regarding what upgrades have been made on the board, whether these upgrades succeeded, who performed these upgrades, the time of upgrade and so on. These details can help to ascertain the patches applied to the system, thereby helping in troubleshooting.

12 Installing an SSL certificate

The administrator can upload an SSL certificate to be used for site validation. The web page for certificate upload can be accessed by clicking on the SSL-certificate link in the main menu tree. Select the certificate and the Key provided by the verification agency and click upload. The certificate and key will be installed automatically and will come into effect after the system is restarted.
Please note that until the next restart the old certificate will remain effective. If for any reason you wish to revert back to the default SSL certificate that was supplied with the NTE, you can use the CLI to do so. Please refer to the relevant section in Configuring the system through the Command Line Interface

13 Factory Reset

DVX-1000 configuration parameters can be set to factory default values through web or 'RESET' switch on DVX-1000. The following section describes the functionality of the factory reset feature.

13.1 Factory Reset procedure

13.1.1 Factory Reset through web

Click in the link 'Factory Reset' in the menu. Click on the 'Apply button' and select 'yes'. The factory reset will start now.

13.1.2 Factory Reset using 'RESET' switch.

Press and release the RESET button on the panel of the board. Please take care not to keep the button pressed for more than 2 seconds.

13.2 Factory Reset Functionality

Factory Reset has to be enabled with caution. This is because several settings/configuration options that have been modified will be restored to the factory defaults. When factory reset is enabled from the web interface of the DVX-1000 the following changes will be effected to the system:

- **Licensing and feature information:** All the licensed features that exist at the time of factory reset will be retained across the reset.
- **Users and User Groups:** Users and the user groups that have been configured will remain as they are (i.e. after factory reset, the administrator does not have to add the users and their groups again).Though the users are still configured, all the features that have been enabled for the users are now disabled. The users now have no features activated and the feature password is reset back to the user extension of the user.
- **Route Groups:** All the configured users will be moved to the default route group (LocalRouteGroup) with only a single local route group configured. Any special routes that need to be added for the users will have to be reconfigured after factory reset.
- **Hunt Groups:** All hunt groups that have been configured will be deleted after factory reset. These have to be added again after reset.
- **Registrations:** All current active registrations will be retained in the DVX database. This is so that the configured users are not forced to re-register every time the DVX-1000 goes back to the factory default settings.
- **Gateways:** All the PSTN and INET gateways configured will be deleted on factory reset. These have to be reconfigured after reset.
- **Call Detail Records and alarms:** All the call detail records and alarms will be deleted on factory reset.
- **Default Authentication:** Default Authentication after factory reset is set to "False".
- **Auto Attendant, Voice mail and Operator Number:** The current values of auto attendant, voice mail and operator number will be retained across a factory reset.
- **Voice mails:** All voice mail messages will be deleted during a factory reset.
- **Feature Configuration:** The feature access codes for all the features will be retained during a factory reset.
- **Conference information:** Mute/Unmute strings, number of dial out attempts and timeout will be reset to the default values, All other conference related information will be retained across factory resets.
- **RTP Port Range:** After factory reset, the RTP port range will be reset to 7000-16000 (the factory default range).
- **System IP Configuration:** After factory reset, the IP configuration method goes back to "Manual". The IP of the system is reset to "10.0.0.1", the default

gateway (the system gateway, not to be confused with the INET and PSTN gateways configured for DVX) is set to "10.0.0.1" and the subnet mask becomes "255.0.0.0"

- **DNS Server Configuration:** After factory reset, both the primary and secondary DNS servers are now configured to "202.62.77.2"
- **Active Calls, Call Statistics, Alarms and Events:** All the active call details, call statistics, alarms and events are deleted after factory reset.
- **System Time Configuration:** After factory reset, the time configuration mechanism will go back to "Manual" but the current system time will be retained.

14 System Reboot

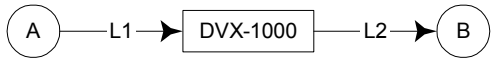
DVX-1000 can be rebooted from the web interface by clicking on the reboot link. It causes the system to restart. This gives the admin the added advantage of being able to reboot the system from the web interface.

15 Firmware Information

The DVX Firmware version is visible whenever the home page of DVX-1000 is accessed. To view the detailed version information for all the modules running in DVX, click on the link more next to the DVX firmware version display. This opens up a new page with a detailed list of all the module versions.

16 Viewing Call Detail Records (CDR)

DVX – 1000 captures relevant call information into concise call detail records which can be viewed on the web interface. The Call Detail Records for the call server can be viewed by accessing the link **System Monitor->CDR Details** from the web interface.



Typical call

Each CDR will contain the details of call legs corresponding to that call. In the illustration of a typical call shown above, L1 and L2 correspond to the call legs, and the CDR will contain two entries, one for each call leg. In the case of a transfer, 3 CDRs will be generated, one for each of the initial calls, and one for the final transferred call. In case any of the phones do not support Call transfer, DVX-1000 will attempt to bridge this call, in such a scenario, the third CDR generated will contain the same details as the initial CDR of the phone that does not support call transfer.

The Call Detail Records can be sorted by multiple methods. The sort can be based on the user extension, destination number and start/end date. Call Direction and Call Type help to filter the information further. Call Direction can be All / Incoming or Outgoing. Call Type can be Local(Loc) or External(Ext). The 'ShowAll' button helps to view all Call History for this call server without applying any filter. Any record can be deleted by selecting the checkbox corresponding to that entry and clicking the 'Delete' button.
Please note that only 50 CDRs will be stored at any given time in the call server database. Beyond this, CDRs will be deleted based on age.

All the deleted entries will be logged in to a backup file which can be downloaded whenever required. Downloading can be done by accessing the link **'Archive'** on the top-right of the CDR Details web page, selecting the required file and providing the suitable path. The CDR Archives are sorted and named based on the Day. The CDR archive for a particular day becomes available as soon as the number of CDRs is greater than 100 and it gets appended by the non-active calls every time the CDRs exceed this limit. At the beginning of each day, CDR Archive Page will show only last 31 CDR files. The downloaded file will have 6 columns named as

Type	Type of call (values 1 – Local, 2 – External)
Calling Party	Phone number of the caller
Other Party	Phone number of the called party
Start Time	Time at which the call started
End Time	Time at which the call ended
Validity	Validity for billing (0 – Invalid call, 1 – Valid Call)

The file will contain values in a tab separated format which is best viewed using an advanced editor such as Microsoft word, Excel or OpenOffice writer.

17 Viewing alarms

DVX – 1000 generates information pertaining to failure conditions of each of it's constituent modules. The alarms are displayed on the web interface and can be accessed through the link **System Monitor-> Alarms**. The alarms can be downloaded as a text file by clicking on the link Download in this page.

Alarm ID	Alarm	Component	Comments
001	DHCP Configuration Failure	System	This alarm is Generated when the 'IP Mode' in 'System Configuration' page is 'DHCP' and the system could not get an IP from DHCP server.
002	No Gateway Configured	System	This alarm is Generated when the 'Configured Gateway' in 'System Configuration' page is not in the same subnet as 'IP Address'.
003	SMTPC failure	System	This alarm is generated when ever the SMTP Client module fails to send a mail, due to various reasons.
004	Database Backup/Restore Alarm	System	This alarm is generate when a Database table is restored from the backup copy
005	Not Used		
006	Corrupted files restored	System	This alarm is generate when the internal backup/restore mechanism restores some mandatory files.

18 Configuration backup and restore.

DVX-1000 provides a means to backup configuration to a host and to upload a previously backed up configuration through the web interface. This feature can be accessed by clicking on **Backup/restore** in the menu tree. Click on Backup and the configuration backup file will be downloaded to your system. You can specify a file path in the text box provided and click 'Restore' to restore a previously downloaded configuration.

The following configuration information is stored in the backup file.

- System Configuration
- Call Server Configuration
- Auto Attendant Configuration
- User and Feature Configurations

- Gateway configuration
- Conference information
- User uploaded voice prompts.

The following information is not backed up and cannot be restored

- CDRs
- Alarms
- Registration information.
- Feature configuration.
- Voicemail mail box information.

When the configuration is downloaded, all the configuration information needs to be applied back to the system.

19 Frequently asked questions

1. What is the username and password for access to the configuration web pages and CLI?

   The default administrator user extension is 'ippbx' and the password is 'ippbx'. We recommend changing these default values for security reasons.

2. Why does DVX-1000 automatically switch to manual mode for time configuration?

   If you change the time or date manually using the CLI, DVX-1000 will assume that you want to switch to manual time configuration, since, NTP time cannot be changed. If you wish to continue using NTP time, you will have to set the time configuration back to NTP using the configuration pages.

3. Why does DVX-1000 automatically start using NTP server mode for time configuration?

   If the NTP server addresses are modified using the CLI, DVX-1000 will apply the changes and switch automatically to NTP time. If you wish to continue using manually configured time, you will have to set the time configuration back to 'Manual' using the configuration pages.

4. Does DVX-1000 support daylight savings time?

   DVX-1000 supports daylight savings time provided the time configuration is set to NTP and the correct time zone is selected.

5. I installed the wrong SSL certificate now I cannot log into the administration web pages, how do I revert to the default certificate?

   You can use the 'restorecert' command from the CLI to restore the default certificate. Please refer the relevant section 'Restore Certificate Command:'.

6. Why doesn't DVX-1000 allow me to add users to Hunt/User group?

   Hunt/User groups can have a maximum of 20 users per group. If you have exceeded this number, further addition of users will fail.

7. Why doesn't DVX-1000 allow me to add a user to multiple Hunt/User groups?

   Any user can be a member of at most 5 groups. If you try to add a user to more than 5 groups the request will be declined.

8. Why can't I add a registration manually?

   The user you are trying to add a registration for might not be configured yet. You can add registrations only for users who have already been added to the call server following the procedure described in 'Adding a new user'. Please note that the recommended method for adding registration is through a SIP compliant endpoint.

9. Why can't I add more users to DVX-100?

   DVX-1000 comes pre configured with a max number of 5 users. If you want to add more than 5 users; a separate license has to be purchased.

10. Why doesn't a feature work even after I have enabled it from the web?

    All the features are activated according to their priority. If you have a higher priority feature configured for the same user, which could be overriding the currently activated feature. Please refer 'Feature Priority Table' for more details.

11. Why doesn't Follow me – Call forwarding work, even though I've enabled it from the phone?

    Some features like Follow me – call forwarding, require additional configuration which can only be done through the web page. Unless this configuration is done, the feature will not work even though it is activated.

12. Why do my calls go to unexpected targets?

    The call server routes your calls using the routing information you have provided. Please check if you have any routes configured which could be interfering with the correct routing of your call. Please refer 'Configuring Routes' for more information on how to configure routes.

13. Why does my voicemail log on fail even though I've dialed the correct PIN?

    DVX-1000 tries to capture information regarding the voice mailbox you are trying to access from the extension you are calling from. In certain cases where the network infrastructure does not forward such information, log on might fail because of the unavailability of caller information. In such an eventuality, you can dial '*' as soon as you dial into the voice mail number and you will be prompted for your extension and password.

14. How do I stop recording a voice message?

    You can press any key to stop recording voice messages.

15. How many voice messages can I have in my mailbox?

    With the maximum mailbox size for a user (5000KB), you can have approximately 26 voicemail messages of duration 20Secs.

16. Why can't I forward a message multiple times to the same user?

DVX-1000 does not allow forwarding the same information multiple times to the same user to satisfy stringent memory utilization requirements. If the message is accompanied by a forwarding note then it can be forwarded multiple times.

17. Why is voice prompt upload failing for certain voice prompts that my media player can play comfortably?

    DVX-1000 supports only media files satisfying the following criterion

    Format: wav (8kHz, 8bit, mono, muLaw).

    Max file size: 200 Kb

    All other formats will be rejected.

18. Why does the CDR archive that I downloaded appear misaligned?

    CDR Archives are stored in a tab separated format, we recommend viewing them in an advanced editor such as Microsoft word, Excel or Openoffice.

19. How can I export CDR's to Microsoft Excel?

    You can open the downloaded CDR text file from Excel. The tab separated values will be automatically separated into columns by Excel.

20. In what scenarios are the configured DNS servers queried?

    Currently domain names resolution is used only for SIP servers. So any sip message that requires a domain name resolution will result in these servers being queried.

21. Can I configure features to work across offices with Remote office connectivity?

    Features such as 'Call Forward', 'Follow me' and hunt groups cannot be configured across offices. Remote office locations are generally connected over the public internet. Security considerations warrant that call features that entail automatic transfer across locations be avoided to discourage eavesdropping and service theft.

22. Why do Voicemail and Auto attendant calls fail immediately after I change the respective extensions?

    The change in Auto Attendant and voicemail extensions are updated to the running configuration after a refresh interval. This refresh can take as much as 5 minutes in the worst case.

23. Why don't conferences end when system parameters such as IP and time are changed?

    Changing system parameters such as system IP, time and ports are **not recommended** when calls or conferences are active. The graceful termination of these calls and conferences are purely best effort and depend on the state of the calls, restart intervals for each of the servers and existing network conditions which cannot be predicted and hence cannot be guaranteed.

24. Why don't I see voicemail notifications in my mailbox even though I have enabled the feature?

There are two reasons why this could happen.

1. If the email id configured for the user is incorrect, the mail will be sent to the next hop and will appear to have been successfully sent as far as the voicemail server is concerned; this mail could fail on a subsequent hop and might not be delivered.
2. If the Administrative user's mail id is not valid on the domain it is sent from, then the mail could be detected as Spam and delivered to your Spam mails folder. Please make sure that the administrator has a valid mail id or add the administrator's mail id to your trusted list.

25. Can I use public SMTP servers configuring voicemail notifications?

    DVX-1000 can be configured to use public domain SMTP servers which do not require authentication. Please note that SMTP client on DVX-1000 does not support authentication.

26. When I upload a voice prompt with the correct format DVX says "Invalid file"?

    Please check the file size, the maximum file size for prompt upload is 200 KB.

27. Why does the traceroute command never work?

    The firewall has to be stopped for traceroute to work correctly. See stopFirewall command for more information.

28. Can I dial into DVX-1000 through a gateway and call an external (not registered to DVX-1000) number?

    Calls that come in through gateways can only call extensions that are directly registered to DVX-1000. This restriction is placed to avoid service theft.

29. The configuration does not work as described in the manual, or the device does not work as expected.

    Please read this manual thoroughly, chances are that you have overlooked some minor detail that is important to the functioning of the product.

20 References

[1]SIP RFC 3261
[2]RTP RFC 1889
[3]RTP OOB RFC 2883

21 Appendix

21.1 Feature Priority Table

Priority	Feature
Highest  Lowest	Do Not Disturb –Forward to Voicemail Call Forward – Always Follow Me – Call Forwarding Call Forward – On Busy, Call Forward – No Answer

21.2 Firewall

21.2.1 Firewall Feature List

- Blocking malicious DHCP Server
- Allowing/blocking SIP packets
- Allowing/blocking RTP/RTCP packets
- Refusing directed broadcast
- Refusing limited broadcast
- Disallowing packets which can be used for port scanning, based on
  - All bits of TCP flag are cleared
  - SYN & FIN bits set
  - SYN & RST bits set
  - FIN & RST bits sets
  - FIN set while ACK is not
  - PSH set while ACK is not
  - URG set while ACK is not
  - SYN Flood attack where out of SYN, ACK and RST bits only SYN is set
- Enabling broadcast echo protection
- Disable source routed packets
- Enabling TCP SYN cookie protection
- Disable ICMP Redirect Acceptance
- Disable sending ICMP redirect messages
- Refuse connection from IANA-reserved blocks
- Allowing source quench messages (ICMP)
- Allowing parameter problem messages (ICMP)
- Allowing destination unreachable, service unavailable messages (ICMP)
- Allowing time exceeded messages (ICMP)
- Allowing ping (ICMP)
- Disallowing connections to SOCKS, X-Windows, Open-Windows & NFS ports
- Support for enabling Telnet/SSH/FTP/HTTP/HTTPS Servers
- Support for enabling NTP Client
- Refusing packets from machine claiming to have external IP address
- Refusing packets from machine having private class-A/B/C addresses

- Refusing packets having source IP address as loop back address
- Refusing malformed broadcast packets
- Refusing packets having source IP address as multicast IP Addresses
- Refusing packets having class E addresses

21.2.2 Firewall Feature Description

The following section discusses firewall features that the DVX-1000 offers

21.2.2.1 Malicious DHCP Server/DHCP Server Spoofing Attack

This attack can happen only when DHCP Client is enabled. DHCP Client can be enabled or disabled selectively

Before learning the DHCP Server's IP Address, all the DHCP offers are accepted by the DHCP Client. Once the DHCP Client learns the DHCP Server's IP Address, firewall updates the rules with DHCP Server's IP Address to allow DHCP traffic from the specific DHCP Server.

21.2.2.2 SIP Packets

SIP packets' reception/transmission can be allowed or disallowed selectively.

21.2.2.3 RTP/RTCP Packets

RTP/RTCP packets' reception/transmission can be allowed or blocked.

21.2.2.4 Directed Broadcast

A traditional IP network has two "special" members, the subnet and network addresses. In many configurations, pinging either IP gives the same result as pinging every IP in the network; namely, every machine replies.

Traditionally, this was used to see which devices were up or down on a network. More recently, it's used to attack other users across the Internet. Since one ping (ICMP echo request) generates many echo replies, attackers simply pretend the ping is coming from the victim's computer. For every fake ("spoofed") ping they send, the victim is flooded with many replies.

The directed broadcast is blocked by default.

21.2.2.5 Limited Broadcast

The limited broadcast is blocked.

21.2.2.6 Port Scanning

For disallowing an intruder from obtaining information on the ports opened on the system. Port scanning is blocked and is implemented by using ScanD chain.

21.2.2.7 Broadcast Echo Protection

The system is protected against broadcast echo requests, since an attacker may try to create a denial of service attack on subnets by sending many broadcast echo requests to which all systems will respond. This also provides information on systems that are available on the network. The system blocks ICMP Echo broadcast requests.

21.2.2.8 Source routed packets

Source routed packets are blocked on all the available interfaces.

21.2.2.9 TCP SYN cookie protection

A SYN Attack is a denial of service (DoS) attack that consumes all the resources on your machine, forcing you to reboot. Denial of service attacks -attacks which incapacitate a server due to high traffic volume or ones that tie-up system resources enough that the server cannot respond to a legitimate connection request from a remote system) are easily achievable from internal resources or external connections via extranets and Internet.

The system is protected against TCP SYN attacks.

21.2.2.10 ICMP Redirect Acceptance

An ICMP Redirect tells the recipient system to over-ride something in its routing table. It is legitimately used by routers to tell hosts that the host is using a non-optimal or defunct route to a particular destination, i.e. the host is sending it to the wrong router. The wrong router sends the host back an ICMP Redirect packet that tells the host what the correct route should be. If the attacker can forge ICMP Redirect packets, and if the target host pays attention to them, the attacker can alter the routing tables on the host and possibly subvert the security of the host by causing traffic to flow via a path the network manager didn't intend. ICMP Redirects are also employed for denial of service attacks, where a host is sent a route that loses it connectivity.

For protecting against this, the ICMP redirect is not accepted.

21.2.2.11 Sending ICMP redirect messages

For the same reason as mentioned above, it is not advisable to send ICMP redirect messages.

21.2.2.12 Connections from IANA-reserved blocks

IANA has generated a list of reserved blocks of IP Address, from/to where the connection is not allowed.

21.2.2.13 ICMP Source Quench Messages

An ICMP source quench is generated by a gateway or the destination host and tells the sending end to ease up because it cannot keep up with the speed at which it's receiving the data. This service is allowed.

21.2.2.14 ICMP Parameter Problem Messages

The ICMP Parameter Problem message is sent to the source host for any problem not specifically covered by another ICMP message. Receipt of a Parameter Problem message generally indicates some local or remote implementation error. These messages are allowed.

21.2.2.15 ICMP Destination Unreachable/Service Unavailable Messages

The Destination Unreachable message is an ICMP message which is generated by the router to inform the client that the destination host is unreachable, unless the datagram has a multicast address. Reasons for this message may include the physical connection to the host does not exist (distance is infinite), the indicated protocol or port is not active, or the data must be fragmented but the 'don't fragment' flag is on.This message is allowed.

21.2.2.16 ICMP Time Exceeded Messages

The ICMP time exceeded message is generated when the gateway processing the datagram (or packet, depending on how you look at it) finds the Time To Live field (this field is in the IP header of all packets) is equal to zero and therefore must be discarded. The same gateway may also notify the source host via the time exceeded message.

21.2.2.17 ICMP Ping

ICMP echo request and echo reply messages are allowed, by default.

21.2.2.18 Connections to SOCKS, X-Windows, Open-Windows & NFS ports

The ports to SOCKS, X-Windows, Open-Windows and NFS are blocked, by default, so as to protect the system from protocol and system administration problems.

21.2.2.19 Telnet/SSH/FTP/HTTP/HTTPS/TFTP Server/Client

The settings related to either of Telnet/SSH/FTP/HTTP/HTTPS/TFTP server/client can be altered as required.

21.2.2.20 NTP Client

The setting for allowing the packets related to NTP Client can be modified as required. Currently, these packets are allowed.

21.2.2.21 Packets having source address as target system's external IP address

For natural reasons, such packets are blocked.

21.2.2.22 Packets from machine having private class-A/B/C addresses

Packets from either of the private class A, class B, or class C address received on the external interface are blocked. Since these address can only be assigned to LANs.

21.2.2.23 Packets having source IP address as loop back address

Packets claiming to have loop back address as the source IP address are blocked.

21.2.2.24 Malformed broadcast packets

Malformed broadcast packets are blocked. The packets having "0.0.0.0" as the destination address and/or "255.255.255.255" as the source address are dropped.

21.2.2.25 Packets having source IP address as multicast IP Addresses

Multicast IP address cannot be put in the source IP address of the packet. Packet found with such IP address is blocked.

21.2.2.26 Packets having class E addresses

Class E being a reserved class, as yet, the packets having source/destination IP as Class E address are blocked.

21.3 FCC Compliance and Advisory

CLASS B EQUIPMENT

THIS EQUIPMENT HAS BEEN TESTED AND FOUND TO COMPLY WITH THE LIMITS FOR A CLASS B DIGITAL DEVICE, PURSUANT TO PART 15 OF OHE FCC RULES. THESE LIMITS ARE DESIGNED TO PROVIDE REASONABLE PROTECTION AGAINST HARMFUL INTERFERENCE IN A RESIDENTIAL INSTALLATION. THIS EQUIPMENT GENERATES, USES, AND CAN RADIATE RADIO FREQUENCY ENERGY AND, IF NOT INSTALLED AND USED IN ACCORDANCE WITH THE INSTRUCTIONS, MAY CAUSE HARMFUL INTERFERENCE TO RADIO COMMUNICATIONS. HOWEVER, THERE IS NO GUARANTEE THAT INTERFERENCE WILL NOT OCCUR IN A PARTICULAR INSTALLATION. IF THIS EQUIPMENT DOES CAUSE HARMFUL INTERFERENCE TO RADIO OR TELEVISION RECEPTION, WHICH CAN BE DETERMINED BY TURNING THE EQUIPMENT OFF AND ON, THE USER IS ENCOURAGED TO TRY TO CORRECT THE INTERFERENCE BY ONE OR MORE OF THE FOLLOWING MEASURES:

- REORIENT OR RELOCATE THE RECEIVING ANTENNA.
- INCREASE THE SEPARATION BETWEEN THE EQUIPMENT AND RECEIVER.
- CONNECT THE EQUIPMENT INTO AN OUTLET ON A CIRCUIT DIFFERENT FROM THAT TO WHICH THE RECEIVER IS CONNECTED.
- CONSULT THE DEALER OR AN EXPERIENCED RADIO OR TELEVISION TECHNICIAN FOR HELP.

21.4 Technical Specifications

Features

- 5 to 100 users
- Flexible Dial Plan with Multiple Gateway Support
- Internet Call Routing (ITSP Support)
- Remote Office Connectivity
- System Manager
- Web-based Monitoring and Administration
- Call Detail Records
- Basic Call Features
  - Caller ID
  - Call Transfer
  - Call History
  - Call Hold
- Advanced Call Features
  - Call Forwarding - Always
  - Call Forwarding - on Busy
  - Call Forwarding - on No Answer
  - Call Forwarding - Follow Me
  - Do Not Disturb

IVR/Auto Attendant

- VXML Based
- Music on Hold
- Attendant Override (Barge-In)
- Customizable Greetings
- Configurable IVR Menu
- Holiday List Configuration

Voicemail

- VXML Based
- Mailbox Access Control (PIN)
- Configurable Mailbox Size
- Customizable Greetings
- Message Priority
- Notification Via Email

Conference Server

- Dial IN/Dial Out Conferences
- Access Control (PIN)

Performance

- 25 Simultaneous Calls
- 10 Simultaneous Auto Attendant Calls
- 10 Simultaneous Voicemail Calls
- 2.5 Calls Per Second

Audio Capabilities

- Codec: G711,
- Voice Activity Detection
- Comfort Noise Generation
- Packet Loss Concealment
- Low Delay Adaptive Jitter Buffer
- Out of Band DTMF Tone Detection

Management

- Secure Web Based Management
- Console CLI
- Configuration Backup/Restore
- Software Upgrade
- Dlink Endpoint Provisioning
- License Control for Advanced Features

Protocols

- SIP (RFC 3261) *
- SDP (RFC 2327) *
- RTP (RFC 1889) *
- RTCP (RFC 1889) *
- Out-Of-Band DTMF (RFC 2833) *
- RTSP (RFC 2326)

Security

- Built-in Firewall
- MD5 Authentication for SIP
- Secure Administrative and User access for configuration

Hardware

- IXP-425-B Processor (533 MHz)
- 16 MB Flash
- 64 MB SDRAM (Expandable to 256 MB)
- Up to 1 GB of storage
- Reset to Factory Defaults
- 10/100 Ethernet Port (RJ 45)
- RS232 Console Port

LEDs

- Power LED
- LAN Link/Act

Physical & Environmental

- Dimensions: (LxWxH)
  235 x 165 x 33 mm
- Power Input: 5 V DC, 3 A
- Power Adaptor: 90~265 V AC
- Power Consumption: 15 Watt Max
- Operating Temperature Range: 0 to 50° C
- Humidity: 5-95% (non-condensing)

*** Endpoints should comply with these RFCs for interoperability**

D-Link India Limited
+(91)-80-26788345
www.dlink.co.in