D-Link®

DSA-3110

Hotspot Service Gateway

User Manual

Rev. 2.4.3 (Jun. 2009)

RECYCLABLE

Contents

GENERAL INFORMATION

About DSA-3110 Hotspot Edition

The DSA-3110 Hotspot Edition is an access concentrator with HTTP authentication designed to connect users to global network services (e.g., the Internet). The device provides connection and authorization of users, as well as local delivery of connection statistics (to the web-based interface of the device).

The DSA-3110 Hotspot Edition is a complete solution that connects clients to the Internet and delivers statistics on traffic consumed and/or time used.

In addition, the DSA-3110 Hotspot Edition is a gateway specially developed for granting simultaneous broadband access to the Internet for users of public and private networks; the gateway separates and protects the private network against the public one through two individual connection interfaces for users of the public network and the private one.

Using the DSA-3110 Hotspot Edition, your organization is enabled to create a zone of public access (including wireless) keeping your private network secure and not accessible from outside and from the public access segment.

Regardless of the size and profile of the company, the DSA-3110 Hotspot Edition used jointly with an access point or switch is the best choice for quick creation of separate public and private access zones.

To simplify the maintenance of a public access (Hotspot) zone, the DSA-3110 Hotspot Edition can be used jointly with a cheque thermal printer (delivered separately), which helps to decrease overhead costs caused by the use of the device and to create user records (accounts) in the device local base automatically assisted by stuff inexperienced in IT (e.g., waiters, barmen, headwaiters).

The DSA-3110 Hotspot Edition device is compatible with most popular operating systems (including Macintosh, *BSD, UNIX, Linux, and Windows) and can be integrated into a large network.

Typical Connection Schemes

Pictures 1, 4, and 5 represent typical schemes for connecting the DSA-3110 Hotspot Edition.
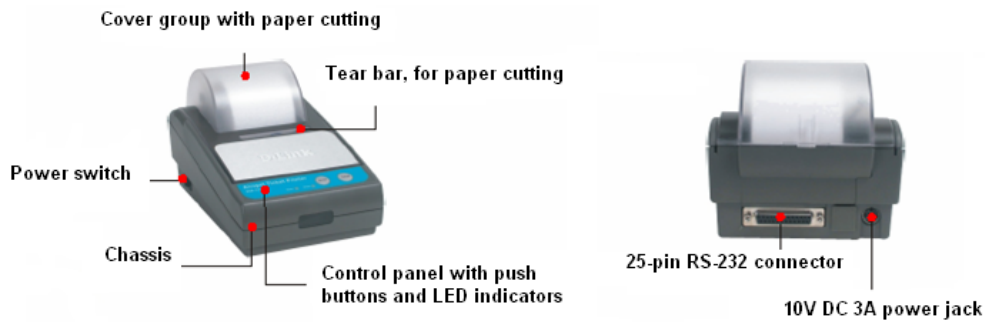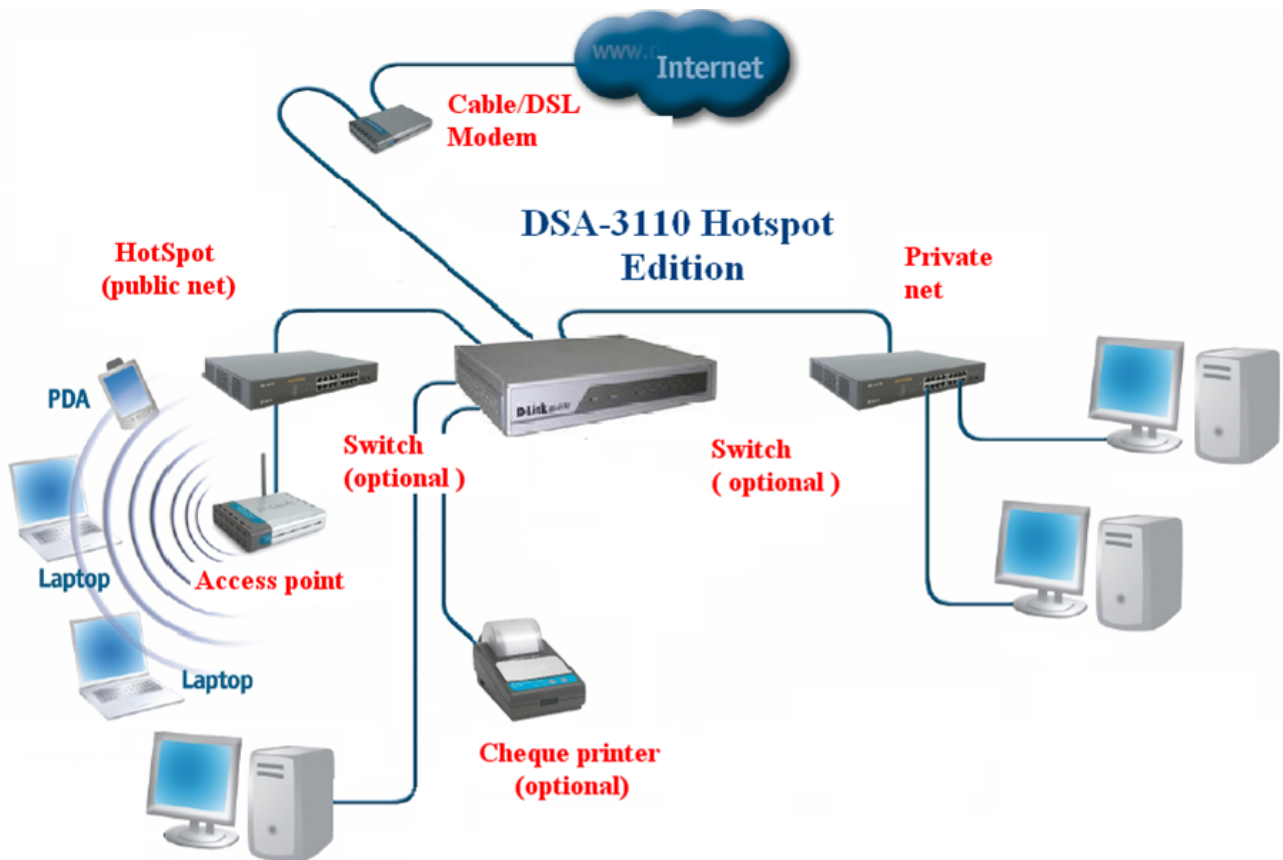
Picture 1. A general scheme of the DSA-3110 Hotspot Edition connection in a public access zone jointly with the DSA-3100P thermal printer.

Picture 2.The UNS-SP1 printer.   Picture 3.The CBM-910II printer.

Picture 4. A sample connection of the DSA-3110 Hotspot Edition in an Internet cafe.
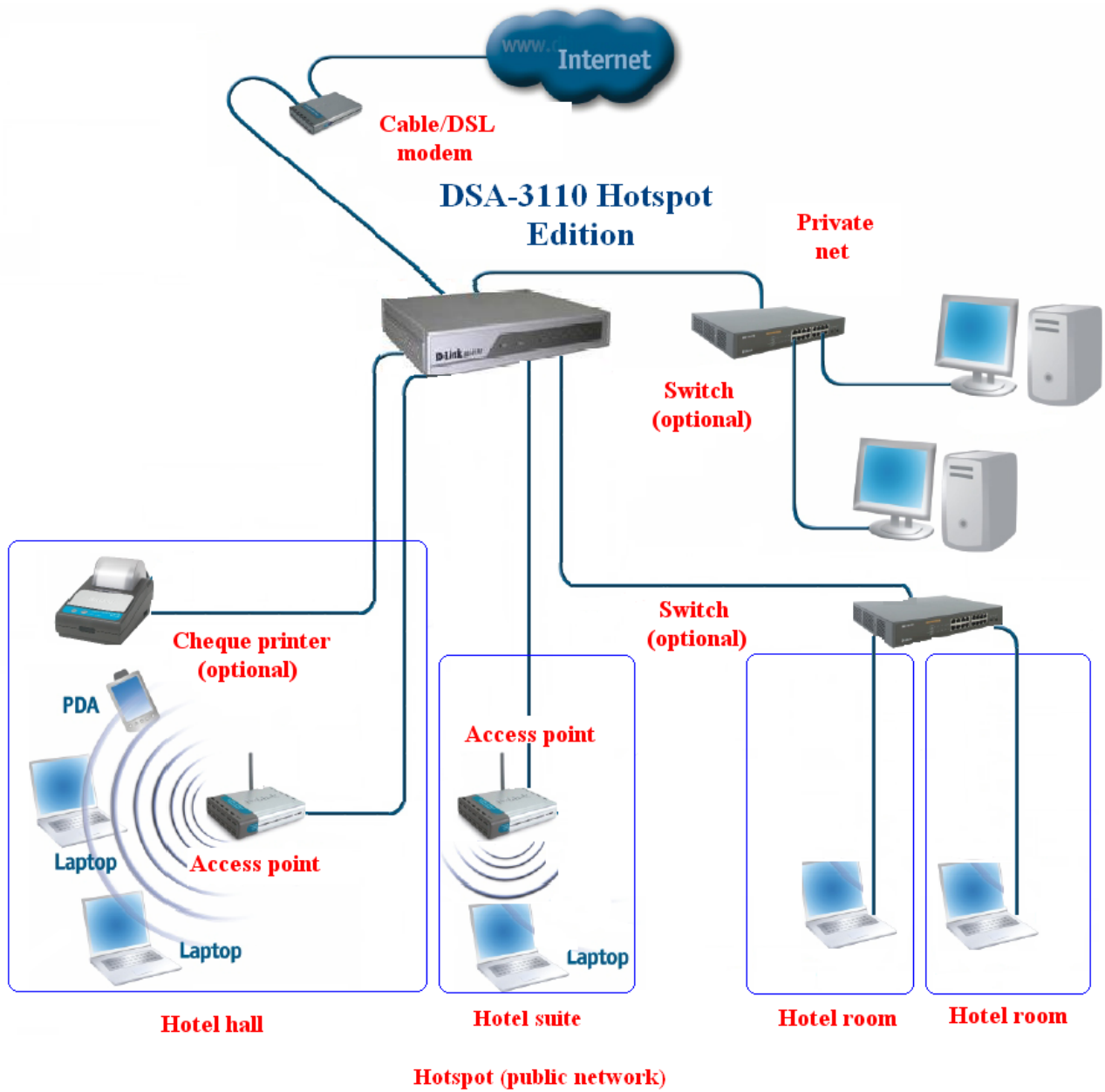
Picture 5. A sample connection of the DSA-3110 Hotspot Edition in a hotel.

NAT Function

The *NAT (Network Address Translation) service* allows using a single private IP addresses in several internal subnets, thereby fewer registered IP addresses are required.

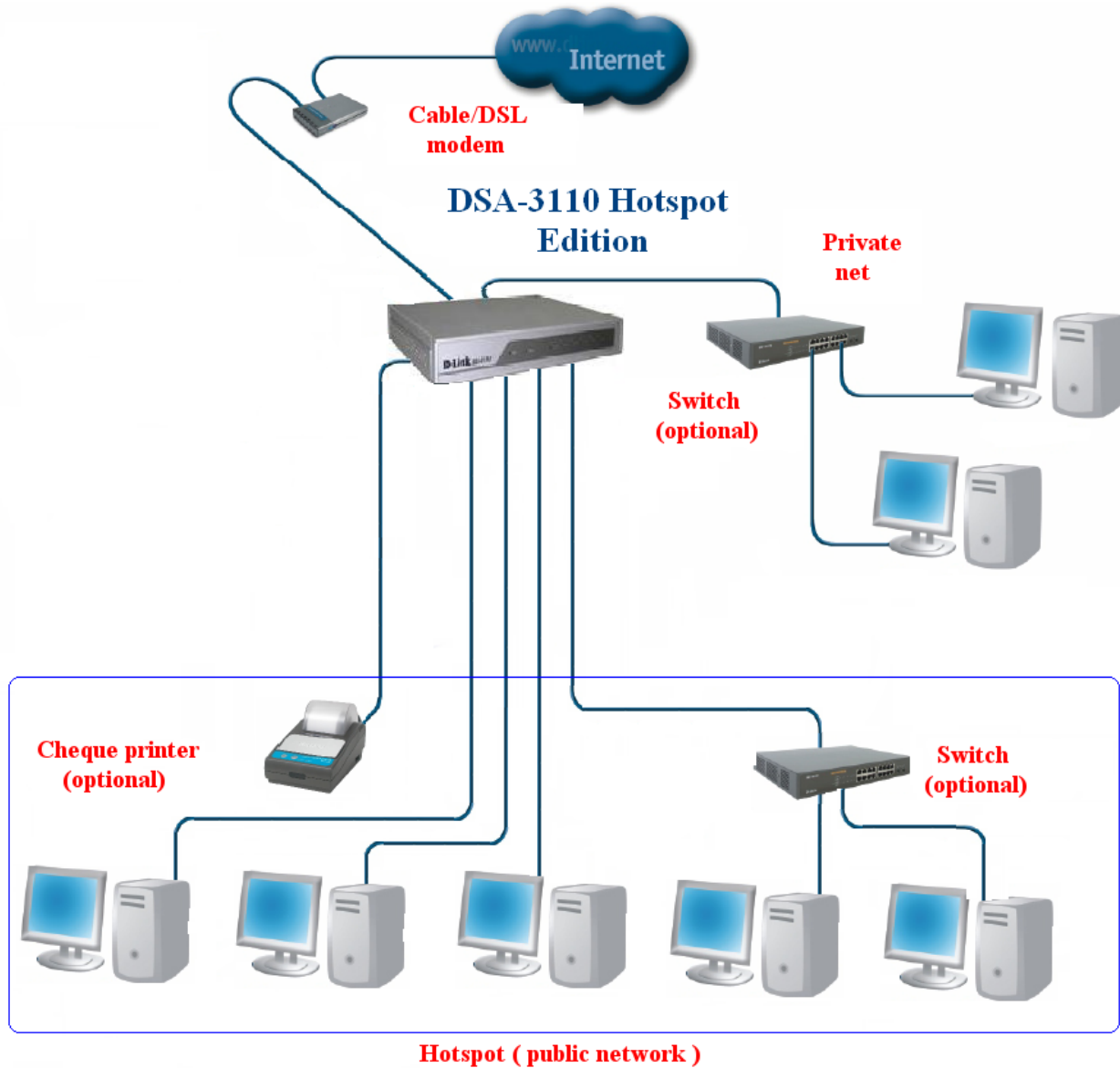A NAT-enabled device is located on the edge between the public and private networks and translates private IP addresses to unique global IP addresses before sending packets to the external network. The NAT service can perform *static* or *dynamic* translation. *Static NAT* is a type of translation where a user himself configures addresses in the mapping table. In this case, specific internal addresses are mapped to previously specified external addresses. *Dynamic NAT* is a type of translation when a NAT-enabled edge device is configured to translate internal (private) addresses to external (public) ones taken from a previously specified address pool. As well, several internal hosts of a network can use one external IP address, which helps to save address space.

DSA-3110 Hotspot Edition Features

Hardware

- CPU: Intel IXP-425 266MHz or Intel IXP-425 533MHz (for DSA-3110/E/B Hotspot Edition)
- 64 MB RAM
- 16 MB Flash ROM
- 7 10/100Base-TX Fast Ethernet ports
- 2 10/100Base-TX LAN interfaces (1 Public LAN, 1 Private LAN)
- Built-in 4-port switch (Public LAN interface)
- 2 WAN 10/100Base-TX interfaces
- Power and Connection Status LEDs
- RS-232 console port (for cheque printer)

Software

- Base OS: Linux
- Authentication: locally over HTTP
- HTTPS connection support
- Support of up to 250 users in local database
- Simultaneous support of local database and Radius DB users
- Radius accounting (for Radius DB users)
- Support of up to 100 user groups (tariffs) in local database
- Support of up to 50 or 80 (for DSA-3110/E/B Hotspot Edition) simultaneous users
- Time and traffic quota support
- Free Surfing Zone support (guest access areas)
- Cheque editor support (for joint use with the DSA-3100P, UNS-SP1, or Citizen CBM-910II-40RF230-A cheque printers)
- Built-in DHCP server
- NAT
- Static routing
- Web-based management interface
- SSH server
- CLI
- Configuration of interfaces with static address, DHCP, PPTP, PPPoE
- Numerous features of iptables, ip, etc., available from standard CLI of built-in Linux OS

Physical and Environmental

- Power supply: external DC power adapter 5V/3A
- Reset to Factory Defaults button
- Dimensions: 239 mm x 156 mm x 30 mm (9.4" x 6.1" x 1.2")
- Weight: 1.2 kg (2.7 lb)
- Cover: steel
- Operating temperature: 0°C to 40°C (32°F to 104°F) (provide sufficient ventilation)
- Storage temperature: -20°C to 70°C (-4°F to 158°F)
- Humidity: 5% to 95% non-condensing
- EMC/EMI: CE, FCC class A

DSA-3110 HOTSPOT EDITION INSTALLATION AND OPERATION

Power On

The DSA-3110 Hotspot Edition device provides configuration via the web-based interface, which allows using any computer with a web browser (regardless of OS) as a management station, and via SSH (for more details see the document "*DSA-3110 CLIGuide*").

Before you begin configuration of the DSA-3110 Hotspot Edition, you should establish a physical connection to the device. You will need the following:

- A computer with Linux, *BSD, UNIX, Windows, or Mac OS.

- A web browser supporting JavaScript (Mozilla, Netscape Navigator, Microsoft IE, Opera, etc.).

- RJ-45 Ethernet cables.

The next steps.

1. Connect an RJ-45 cable between **LAN1 interface (ports 4-7)** and any available Ethernet port of your computer or local network switch.

2. Connect the power adapter included in the delivery package to the device and plug it into a 220V electrical outlet.

Connecting to Web Interface

The web-based management interface includes a client-side GUI and a HTTP server running on the DSA-3110 Hotspot Edition device. Client-to-server communication is commonly realized via TCP/IP port 80.

To connect to the web-based management interface of the device, run a web browser on the management station and enter the IP address of the DSA-3110 Hotspot Edition device in the browser's address bar. The default IP address of the device is 192.168.1.254.

Do the following.

1. Open your web browser.

2. Enter the **IP address** of the **DSA-3110 Hotspot Edition** (http://192.168.1.254) in the address bar.

<u>Note</u>: *If you have changed the default IP address of the DSA-3110 Hotspot Edition device, make sure you are entering the correct IP address.*

<u>**Attention!**</u> *The HTTPS server is also available in the device. If needed, a user can log on the HTTPS server entering the IP address of the DSA-3110 Hotspot Edition device with the **https://** prefix in the web browser's address bar. Client-to-server communication for the HTTPS server is commonly realized via TCP/IP port 443.*

By default, the following username and password are set for the administrator (privileged) access:

User name – admin.

Password – admin.

Note: For security reasons, it is strongly recommended to change the administrator password. Please, go to the **System > Administrator password** page to change the password.

After successful registration the system statistics page is displayed.

Picture 6. The page displaying the system statistics.

The device allows changing the web-based interface language in one click. To do so, click the **English** or **Russian** link in the right top corner of the screen. You can switch to the other language from any page.
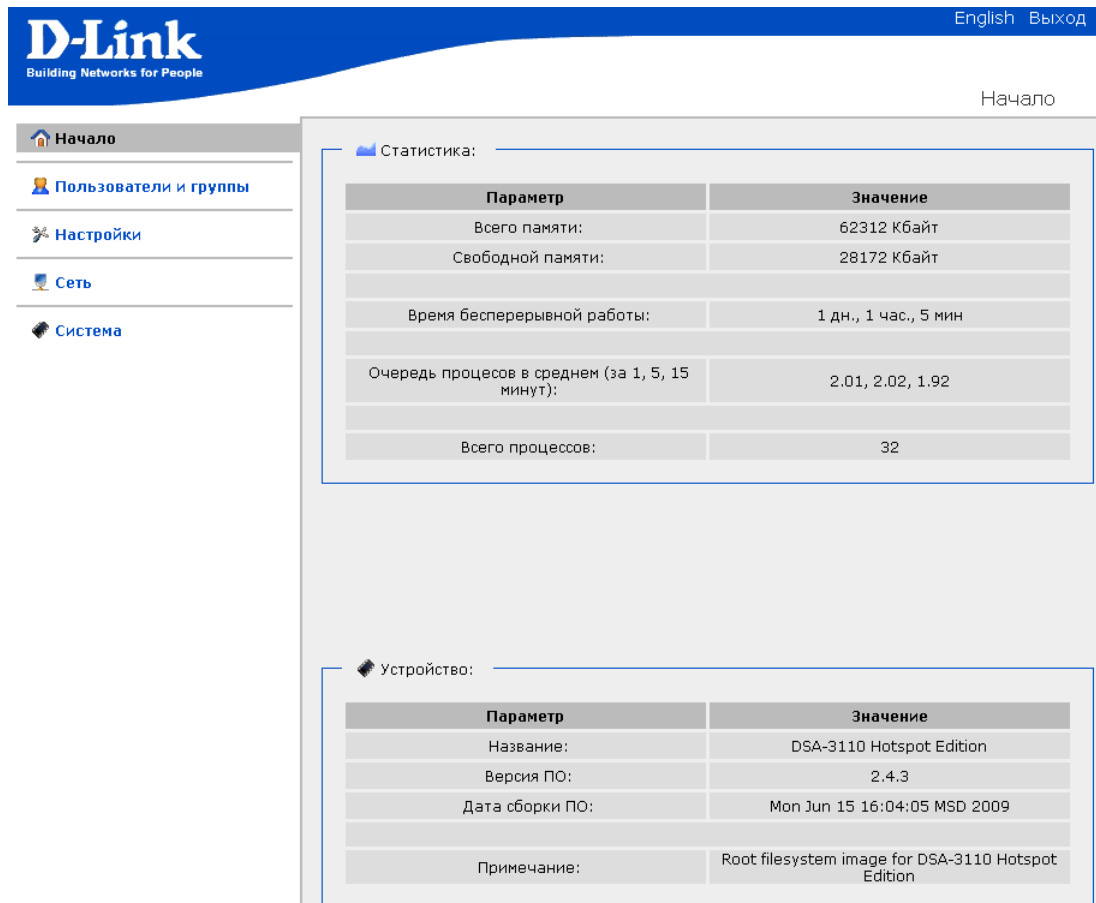
Picture 7. The same page in Russian.

Attention!

1. To keep the device settings in the non-volatile memory, you should save the changes on the **System > Configuration** page (click the **Save** button).

2. The **factory default settings can be restored** via the web-based interface (**System > Configuration > Factory**) or via the hardware **Reset** button. The hole of the button is located on the back panel of the device next to the power connector. Use a small paperclip to activate the button; insert it into the hole (with the device turned on), push, and hold for 10 seconds. If you act properly, first the **Status** LED turns off for 2 or 3 seconds, and then the LED blinks fast for some seconds, which means the device is restoring the default settings. After that the LED turns off for 2 or 3 seconds again, and then the device is completely reset.

NET MENU

This menu section is used to:

- Configure the network parameters of the device's physical interfaces.
- Configure p-t-p (point-to-point) interfaces (PPTP, PPPoE).
- Display network statistics on both physical and p-t-p interfaces.
- Configure NAT (network address translation).
- Configure DNSs (domain name servers) and a search list of domains.
- Configure the built-in DHCP server and create additional DHCP servers.
- Configure static routes.
- Configure settings for an external user database (RADIUS server).
- Configure access to the web-based interface of the device.

Port numbers 1-7 labeled on the cover of the device correspond to the following internal functional interfaces:

Ports 4-7	*LAN1 interface (Public LAN)*	These ports are designed to connect devices that form the Hotspot Public network (e.g., access points). Users connected to this interface must be authenticated over HTTP upon every attempt to access broadband resources (e.g., the Internet), and all transmitted data are accounted automatically on the basis of time and traffic.
		Ports 4-7 represent a switch with isolated ports (i.e., packets cannot be transferred between the ports of the switch; transferring packets to the other interfaces is only available).
Port 3	*LAN2 interface (Private LAN)*	This port is mostly used to connect devices that form the internal (Private) network of a company.
		Users connected to this interface can access a broadband channel without authentication.
Port 2	*WAN2 interface*	This interface is designed to connect to a broadband channel. The port is disabled by default.
Port 1	*WAN1 interface*	This interface is designed to connect to a broadband channel (an Ethernet connection or ADSL modem).

By default, the interfaces of the device are configured in the following way:

LAN1 – 192.168.1.254

LAN2 – 192.168.0.254

WAN1 – DHCP connection

WAN2 – disabled

Attention! *By default, the web-based interface of the device is accessible from the LAN (LAN1 or LAN2) interfaces only, and* **not accessible from the WAN (WAN1 and WAN2) interfaces. You can change these settings on the Net > Remote access page.**

Network Interfaces

This page is designed to modify the device settings and manage the physical interfaces of the device. To modify the settings of the network interfaces:

- Go to the **Net** menu.
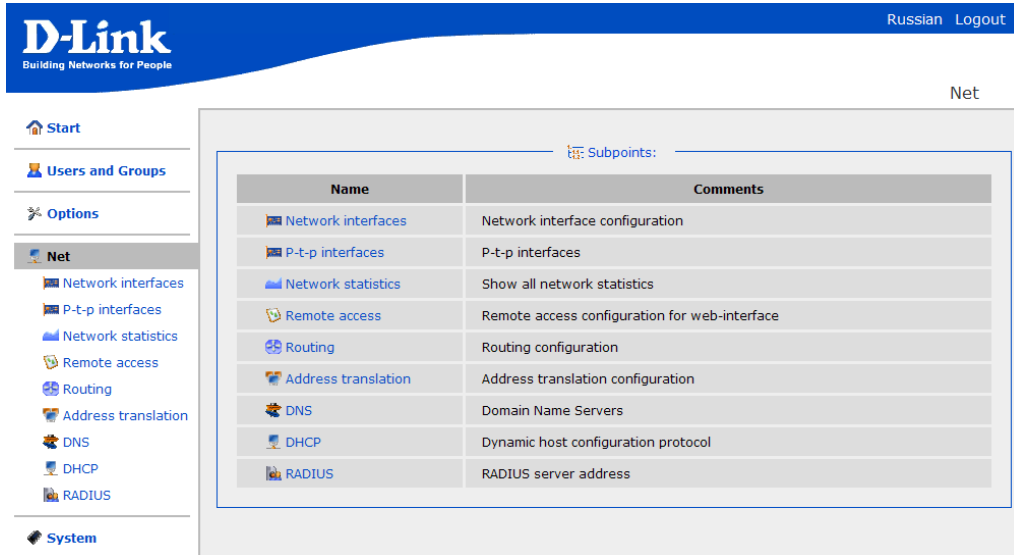
Picture 8. The **Net** menu.

- Follow the **Network interfaces** link.
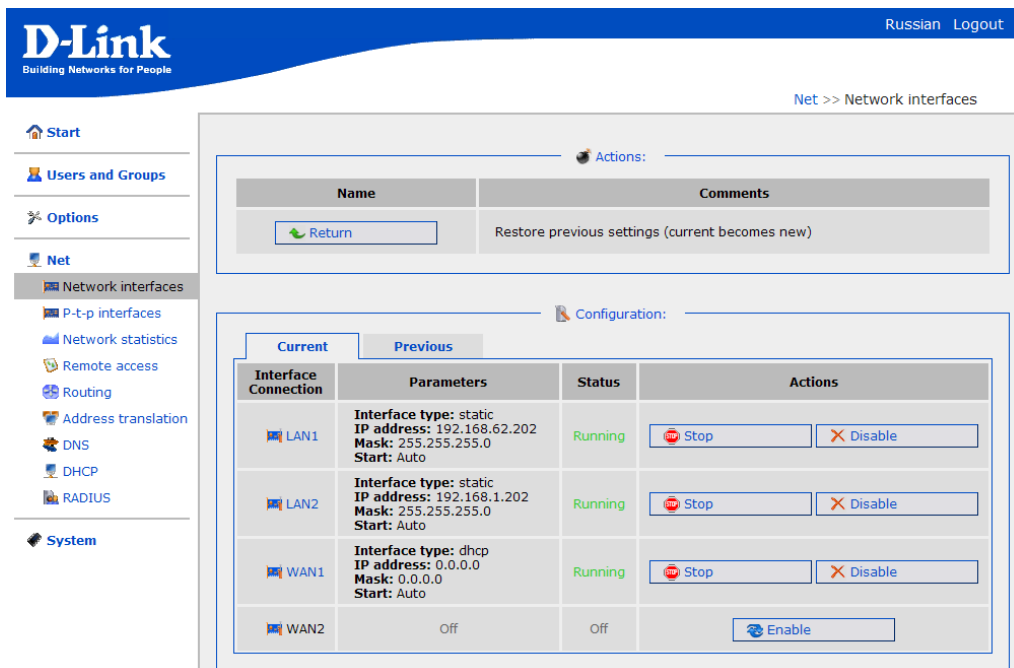
Picture 9. The **Net > Network interfaces** page.

- You can enable, disable, stop, or start any physical interface by clicking the relevant button located in the **Actions** column of the interface line.

- To modify the settings of one of these interfaces, follow the corresponding link (e.g., LAN1).

- On the page displayed, select the interface type: **Static** or **DHCP.**

Configuring Static Interface

For eth0 (LAN1) and eth1 (LAN2) interfaces, this interface type is the only available type. For eth2 (WAN1) and eth3 (WAN2) interfaces, both Static and DHCP types are available.
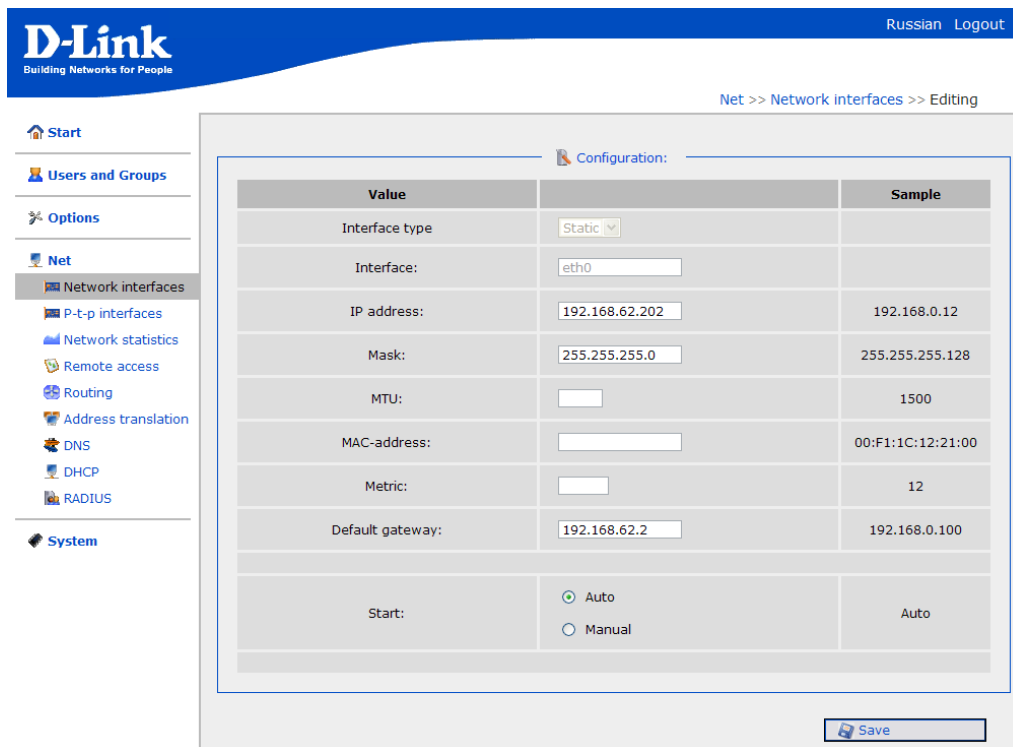
Picture 10. Configuring a static IP address for LAN1 interface.

You can modify the following fields:

IP address	The IP address assigned to the interface.
Mask	The subnet mask.
MTU	The maximum transmission unit in the interface. *Optional*.
MAC-address	The hardware address to be set for the interface *Optional*.
Metric	The metric of the interface. Allows assigning a priority for the interface. The lower the value, the higher is the interface priority. *Optional*.
Default gateway	The IP address of the default gateway. Sets the address for routing packets to external networks. Applicable for the WAN interfaces only. *Optional*.
Start	Select a radio button to enable or disable the interface auto-start upon the load of the device.

Click the **Save** button.

Configuring DHCP Interface
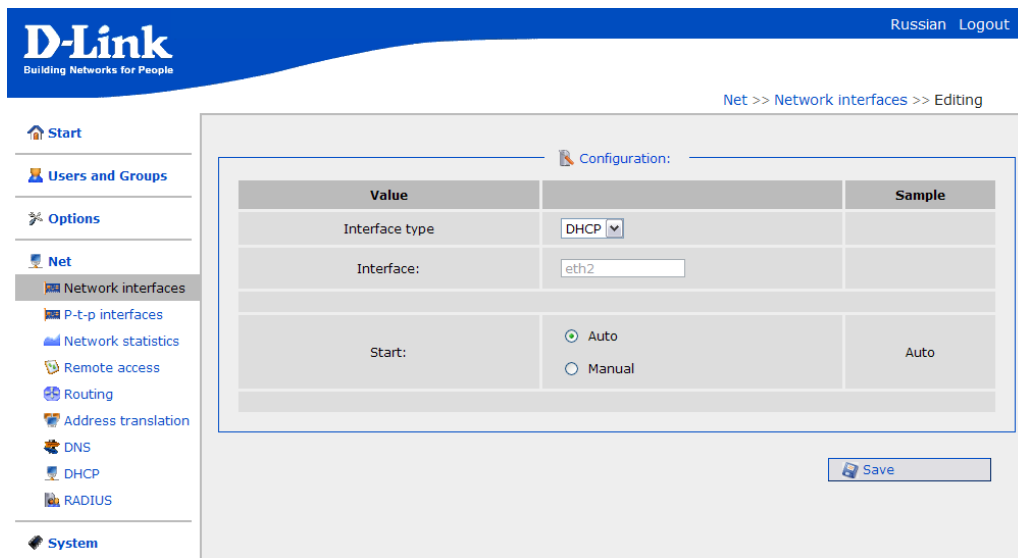
Picture 11. Configuring a DHCP client for the interface.

You can modify the following fields:

Interface type The type of configuration for this interface (DHCP).

Start Select a radio button to enable or disable the interface auto-start upon the load of the device.

Click the **Save** button.

P-T-P Interfaces

This page is designed to modify the device settings and manage the PPTP and PPPoE interfaces of the device.

- Go to the **Net** menu.
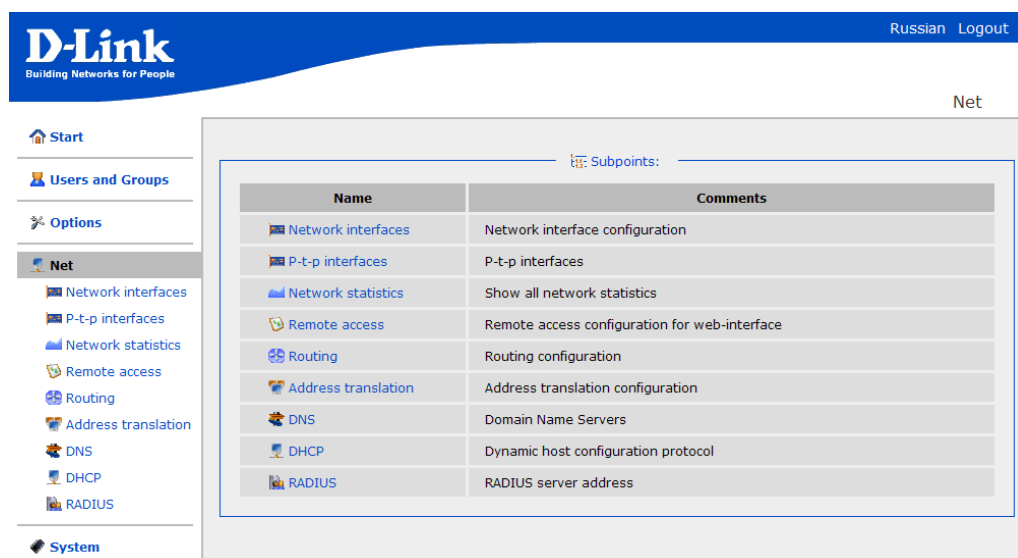
Picture 12. The **Net** menu.

- Open the **P-t-p interfaces** page.

Picture 13. The **Net > P-t-p interfaces** page.

- You can enable, disable, stop, or start any interface by clicking the relevant button located in the **Actions** column of the interface line.

- To modify the settings of one of these interfaces, follow the corresponding link; to create a new p-t-p interface, click the **Add** link.

- On the page displayed, select the interface type: **PPTP** or **PPPoE**.

Adding or Modifying PPTP Interface
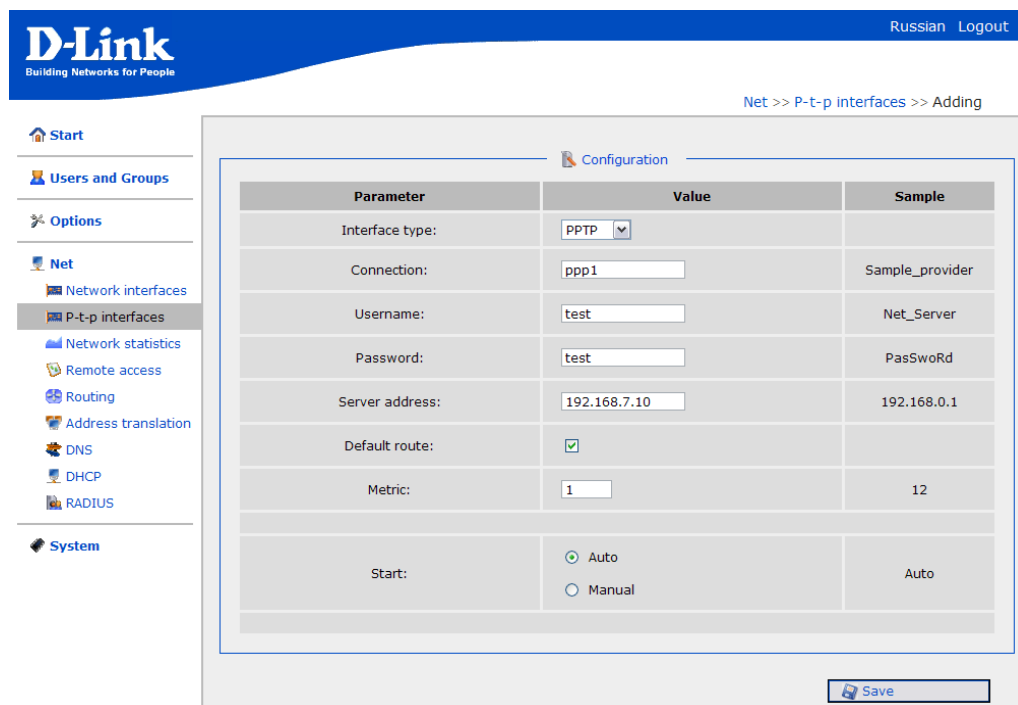
Picture 14. Configuring a PPTP client for the interface.

Interface type The type of configuration for this interface (PPTP).

Connection A name of the connection for easier identification.

Username The login to register on the PPTP server.

Password The password to register on the PPTP server.

Server address The IP address of the PPTP server.

Default route Select this checkbox to use the IP address of the server as the default route (the destination address for all packets, which routes have not been found).

Metric The parameter is used to assign a priority for this connection. The lower the value, the higher is the priority.

**Start** Select a radio button to enable or disable the interface auto-start upon the load of the device.

Click the **Save** button.

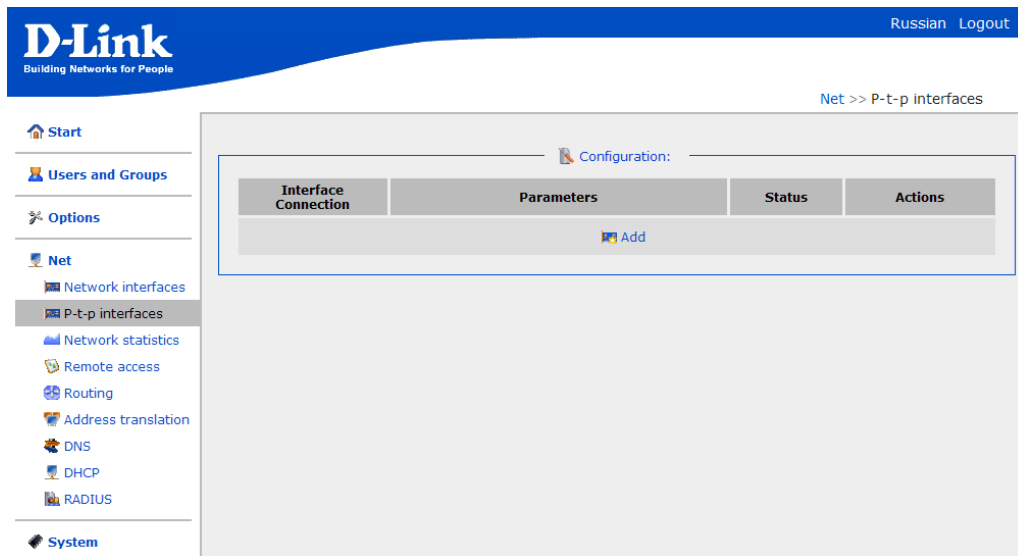## Adding or Modifying PPPoE Interface

Picture 15. Configuring a PPPoE client for the interface.

Interface type	The type of configuration for this interface (PPPoE).
Connection	A name of the connection for easier identification. *Optional*.
Interface	The name of the device physical interface, to which the configured PPPoE interface will be assigned.
Username	The login to register on the PPPoE server.
Password	The password to register on the PPPoE server.
Access concentrator name	The name of the provider's PPPoE server.
Service name	The name of the service on the provider's PPPoE server. *Optional*.
Default route	Select this checkbox to use the IP address of the server as the default route (the destination address for all IP packets, which routes have not been found).
Metric	The parameter is used to assign a priority for this connection. The lower the value, the higher is the priority.
Start	Select a radio button to enable or disable the interface auto-start upon the load of the device.

Click the **Save** button.

Applying/Returning Configuration of Network/P-T-P Interfaces

When you have modified the settings of physical interfaces, added p-t-p interfaces or modified the settings of p-t-p interfaces, a page displaying the newly created configuration of interfaces opens.

On this page you can save the new configuration by clicking the **Apply** button or reject the configuration by clicking the **Delete** button.
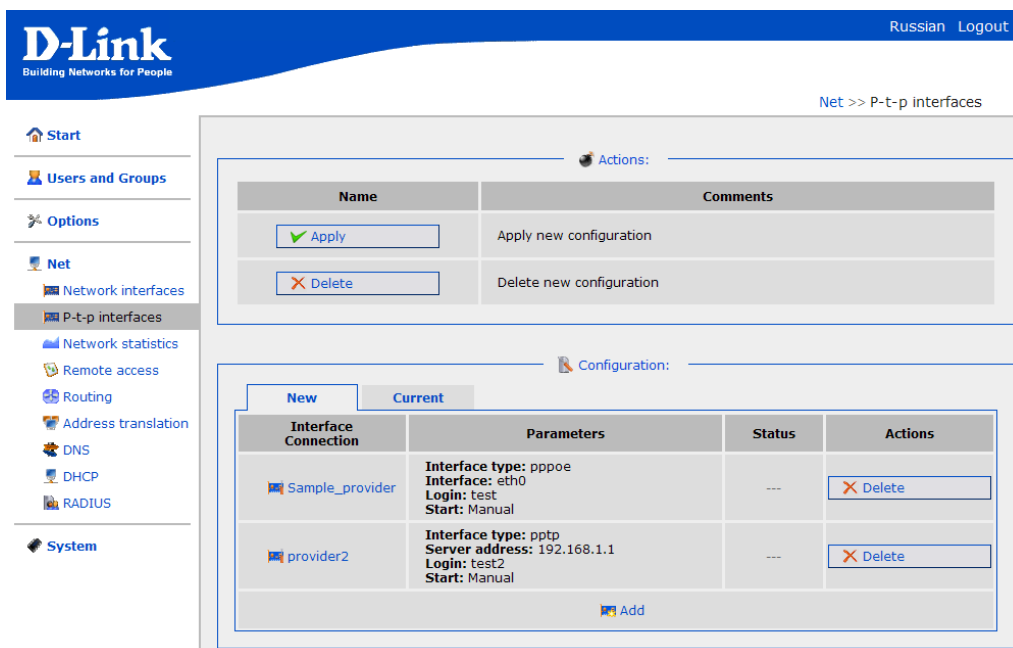
Picture 16. Saving the changes of configuration.

After application of the new configuration, you can roll back to the previous configuration and use it until some new changes are applied. At that moment the **New** configuration turns into the **Current** one, and the **Current** configuration turns into the **Previous** one.

This management scheme provides for so called "soft" application of configuration for all network interfaces.
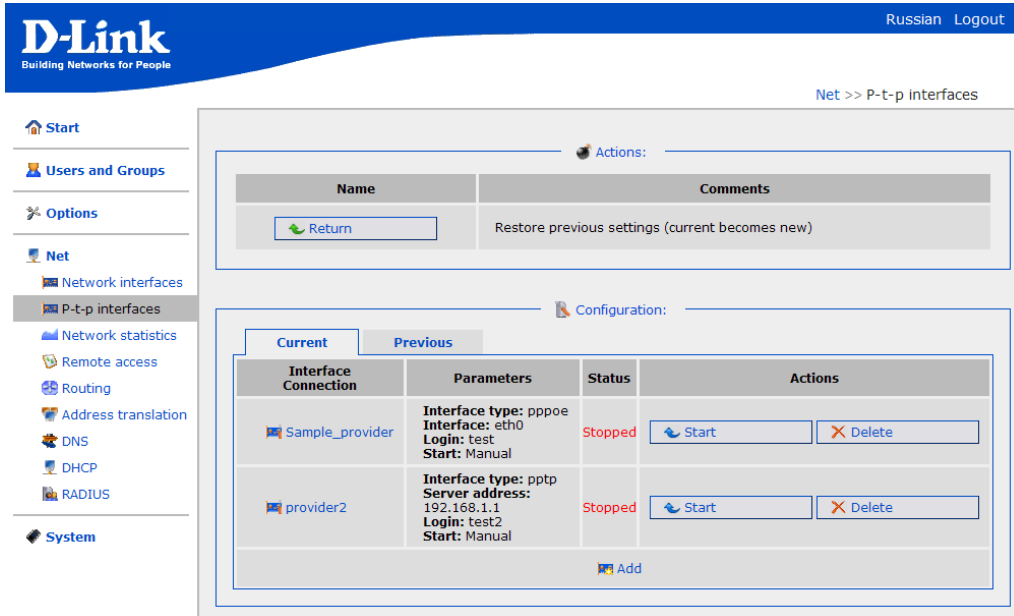
Picture 17. Rolling back to the previous configuration.

Network Statistics

This page is designed to display network statistics (the number of received/transmitted packets, errors, etc.) for all physical and p-t-p interfaces **running at the moment**.
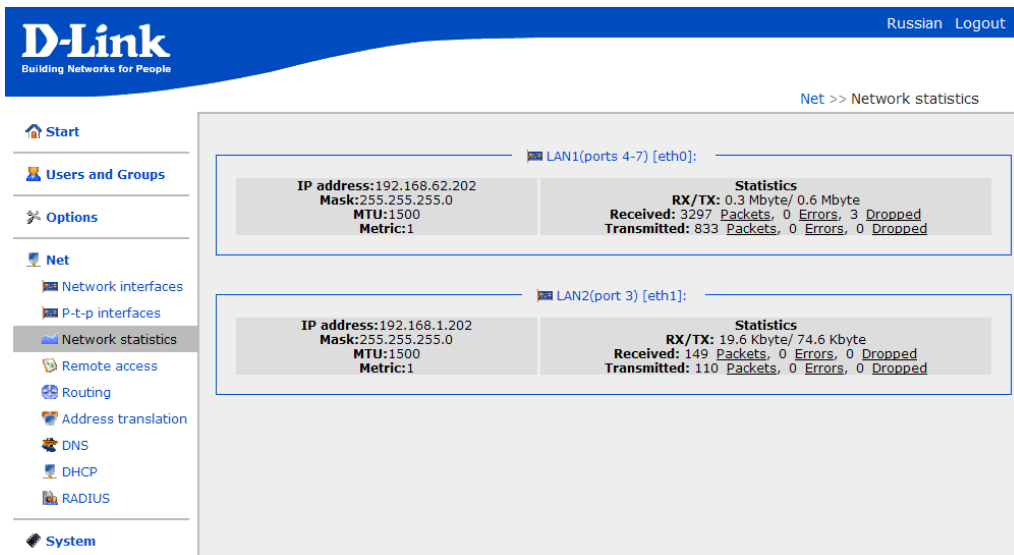
Picture 18. The **Network statistics** page.

Remote Access

This page is designed to configure access to the web-based and command-line interfaces of the device.

It provides flexible organization of access from the local (LAN) and global interfaces (WAN) with filtering by IP address, as well as by an access protocol – HTTP, HTTPS, HTTP+HTTPS (to access the web-based interface), or SSH (to access the CLI).

The page displays a set of rules that schedule access. The rules are processed in the listed order (downwards).

The arrow buttons located on the right of the rule table are used to change the order of the rules.
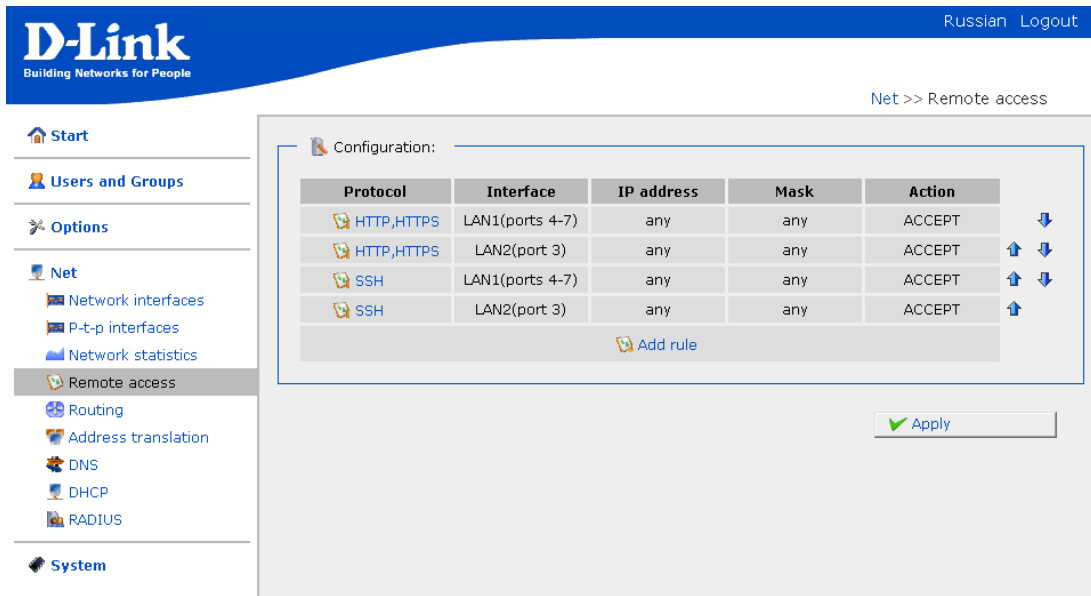
Picture 19. The **Remote access** page.

To add a new rule, proceed to the **Net > Remote access** page and follow the **Add rule** link.
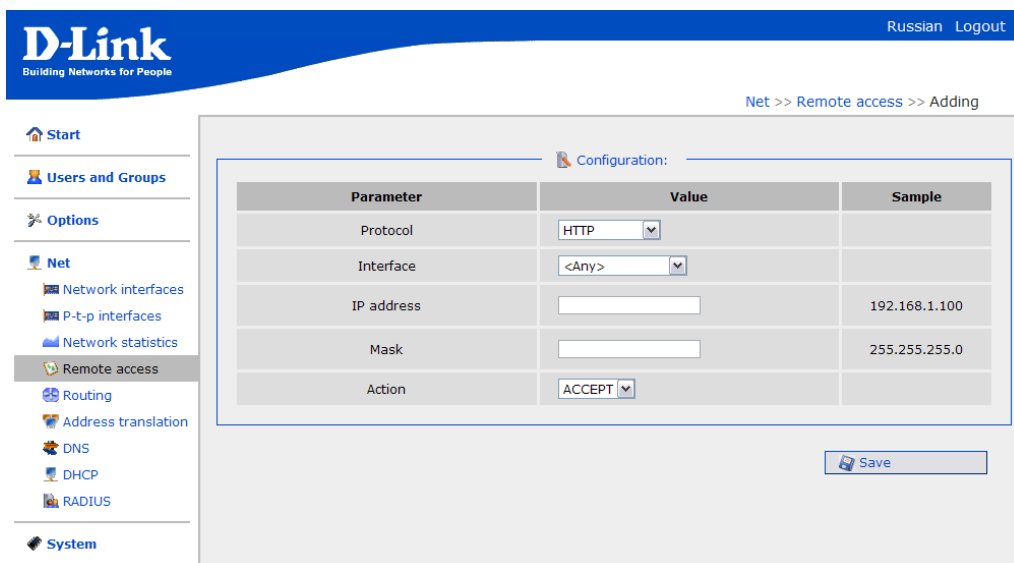
Picture 20. Adding a new rule for remote access.

On the page displayed, specify the following:

Protocol (HTTP, HTTPS, HTTP+HTTPS, or SSH). For global interfaces (WAN) we recommend you to use secure HTTPS protocol; a protocol for local interfaces can be chosen by the employee that is maintaining the device.

Interface A physical interface, through which the web-based interface of the device is accessed.

IP address A subnet to which the rule is applied.

Mask A mask of the subnet (along with the **IP address** field, specifies the subnet to which the rule is applied).

Action The ACCEPT action of a rule means that the access is granted. The DROP action of a rule means that the access is denied.

When you have specified all the parameters, click the **Save** button.

Routing

This page is designed to add new static routes to the system (routes for networks that are not connected directly to the device but are available through the interfaces of the device).

To modify the settings of static routing:

- Open the **Net > Routing** page.

- Follow the **Add routing** link.

- Enter the settings for the new route:

Destination network A destination network to which this route is assigned.

Destination netmask A mask of the destination network.

Gateway An IP address through which the destination network can be accessed.

Metric A metric for the route. The lower the value, the higher is the route priority.

Via Interface Select an interface through which the destination network can be accessed. If you have selected the **Automatically** value of this drop-down list, the device itself sets the interface on the basis of data on connected networks.

- Click the **Save** button.

Picture 21. Adding a new static route.
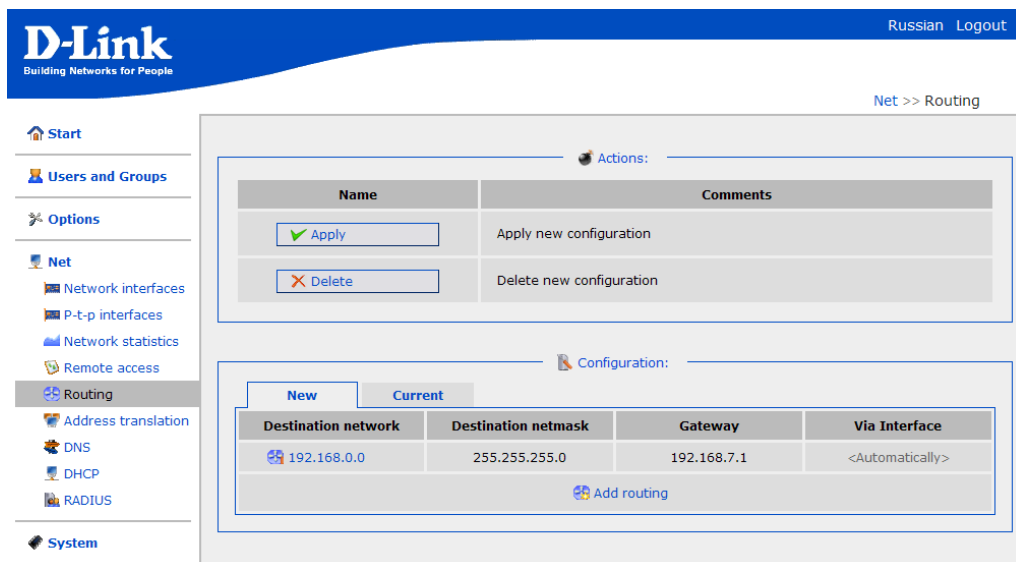
Picture 22. Applying the newly created static route.

Click the **Apply** button to apply the new configuration of routing.

Network Address Translation

Proceed to the **Address translation** page to configure the NAT (Network Address Translation) function.

This page is used to declare subnets which require address translation. A physical interface used for translating a network is selected automatically on the basis of network settings configured on the **Net > Network interfaces** page.

The **Off** button is used to completely disable the NAT function in the device.

The **Factory** button is used to restore the default setting of the NAT function.

By default, the NAT function is enabled for the following networks: 192.168.1.0/24, 192.168.0.0/24, 10.0.0.0/8.

To modify the NAT settings, do the following:

- Open the **Net > Address translation** page.

- Click the **Edit** button.
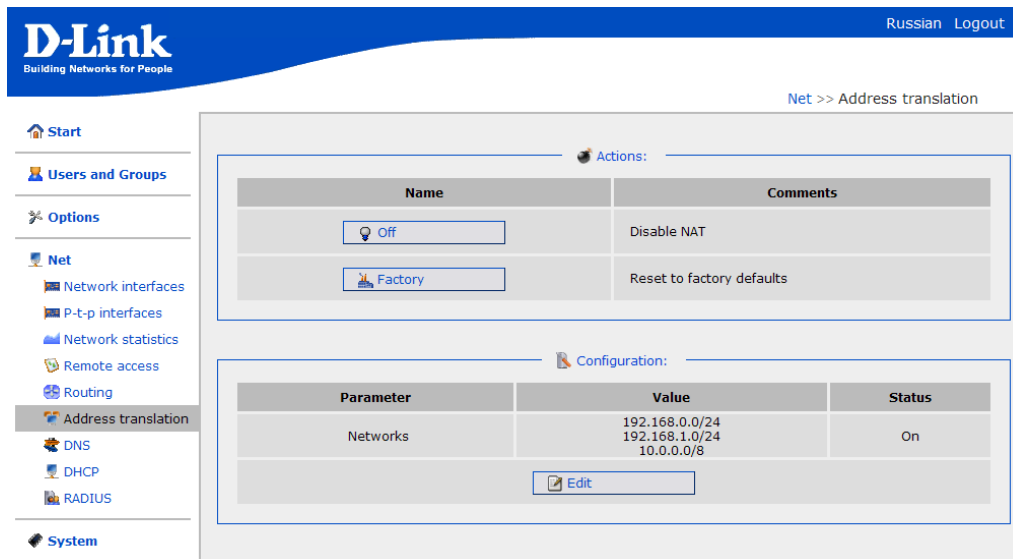
Picture 23. The **Net > Address translation** page.

- Enter the slash-separated pair of the subnet and subnet mask. The subnet mask can be entered in the common (4-octet) format (e.g., 255.255.255.0) or in so called variable-length subnet mask (VLSM) format (e.g., /16 corresponds to 255.255.0.0, /24 – to 255.255.255.0, / 30 – to 255.255.255.252, etc.).

- Click the **Save** button.

DNS

This page is designed to add domain name servers (DNS) to the system and domains to the search list.

Name servers are used to determine the IP address from the name of a server in Intranets or the Internet (as a rule, they are specified by an ISP or assigned by a network administrator). The search list is used to automatically add top-level and second-level domains when a user enters an incomplete URL (e.g., if the field value is **.com**, a user enters *google* in the address bar, and it is automatically substituted by *google.com*).

The device can also perform the DNS relay function, i.e., it can redirect the DNS requests of users to external DNS servers (including the ones distributed by an ISP). In this case, the IP address of the device's LAN1 interface is specified as the DNS server, and external DNS servers are specified in the device.

*Note: When you use the built-in DHCP server, the network parameters (including DNS servers) are distributed to clients automatically, so you only need to specify external DNS servers on the **Net > DNS** page.*

Adding DNS Server

- Open the **Net > DNS** page.

- Enter the IP addresses of DNS servers in the **Name servers** field.

- Click the **Save** button.

Adding Domain to Search List

- Open the **Net > DNS** page.

- Enter the names of top-level or second-level domains (in total up to 3) in the **Search list** field.

- Click the **Save** button.
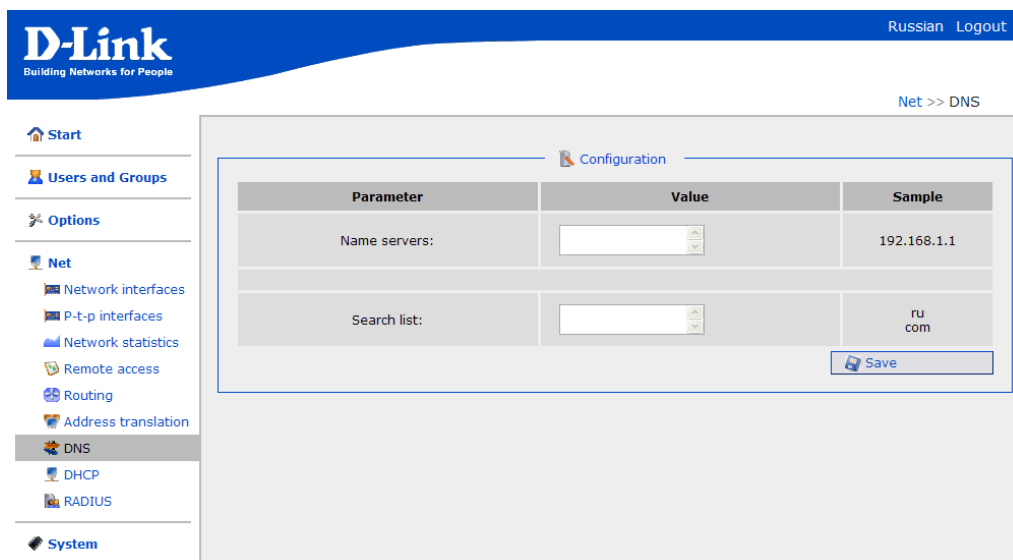
Picture 24. Adding a name server to the system or a domain to the search list.

DHCP

This page is designed to configure internal DHCP servers of the device.

These servers are used to automatically distribute IP addresses to Hotspot users.

From version 2.4.0 of the firmware, the device can have several DHCP servers (e.g., separate DHCP servers for LAN1 and LAN2 interfaces).

By default, one DHCP server for LAN1 interface is created in the device.

For every DHCP server you can configure the following:

- Directly add or remove.

- Assign a symbolic name.

- Specify a physical interface of the device to which this DHCP server is assigned.

- Specify the start and end IPs of the pool of addresses used to distribute DHCP IP addresses to clients (the **Start address** and **End address** fields).

- Specify the number of IP addresses in the DHCP pool.

- Specify the "lifetime" of the leased IP address of the DHCP server, in minutes (the time period of IP address lease; at the end of this period the IP address is revoked and can be distributed to another device, unless the previous device has confirmed the need to keep the address).

- Specify the DNS (the name server IP address distributed by this DHCP server).

- Specify the default gateway for this DHCP server (the **Router** field).

- Specify the IP address for broadcast packets.

To add a new DHCP server, proceed to the **Net > DHCP** page, follow the **Add DHCP** link, and then enter the settings of the new DHCP server.
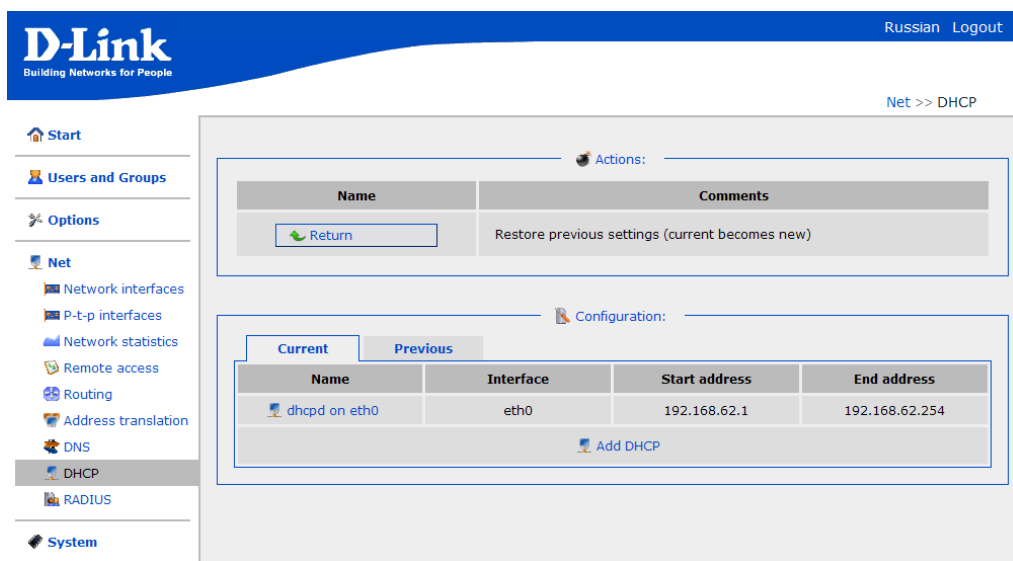
Picture 25. Configuring DHCP servers.

When you have specified the settings for your new DHCP server, click the **Save** button on the **Net > DHCP > Adding** page, and then click the **Apply** button on the **Net > DHCP** page.

Picture 26. Adding a new DHCP server.

RADIUS

This page is designed to configure the device operation with an external centralized database via the RADIUS protocol.

Such a scheme is useful if there are several devices (objects) that work with single database of users.

In addition, the system performs traffic accounting for the users of the RADIUS database via the RADIUS protocol (RADIUS accounting).

The **radius** group serves for configuring the parameters of the external DB users (see the **Users and Groups > Groups** page). This group is required only to specify the bandwidth for the group and for users, so, there is no use creating local users in this group (such users are considered to be the users of the local database).

*Attention! The data on the next time of authentication (username and password) check are contained in the SESSION_TIMEOUT field of the RADIUS packet. For this reason, the **Account length** parameter for the **radius** group users is useless (though available on the page).*

Attention! The device can operate in both internal (local) DB and external (located on the Radius server) DB simultaneously. This feature provides the system with more flexibility and the opportunity to work with both centralized users from different objects (in case of the network of objects) and local users from the current object.

However, you must keep in mind that the authentication data of local users are kept in the device (locally), and the authentication data of RADIUS users – on the RADIUS authentication server.
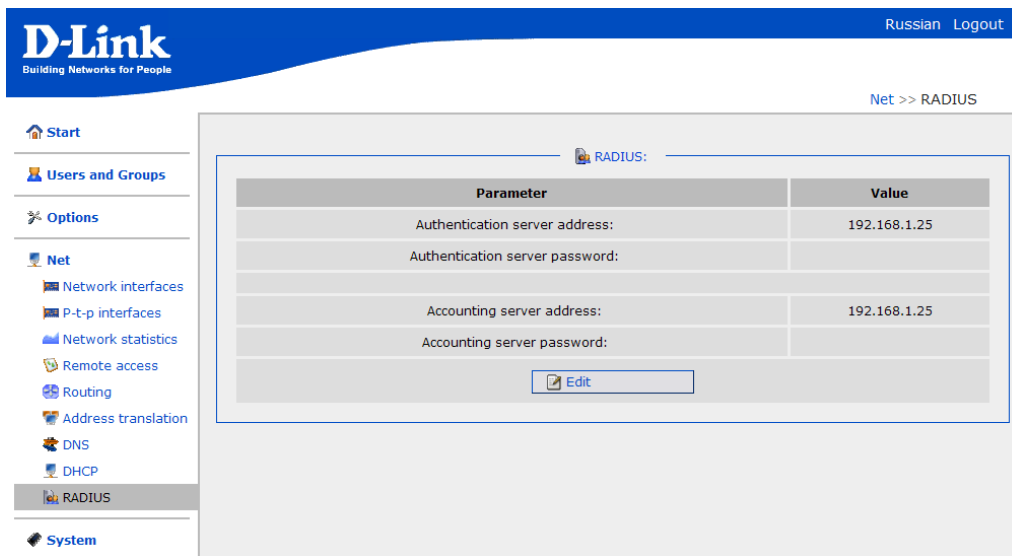
Picture 27. Configuring the device operation with the RADIUS server.
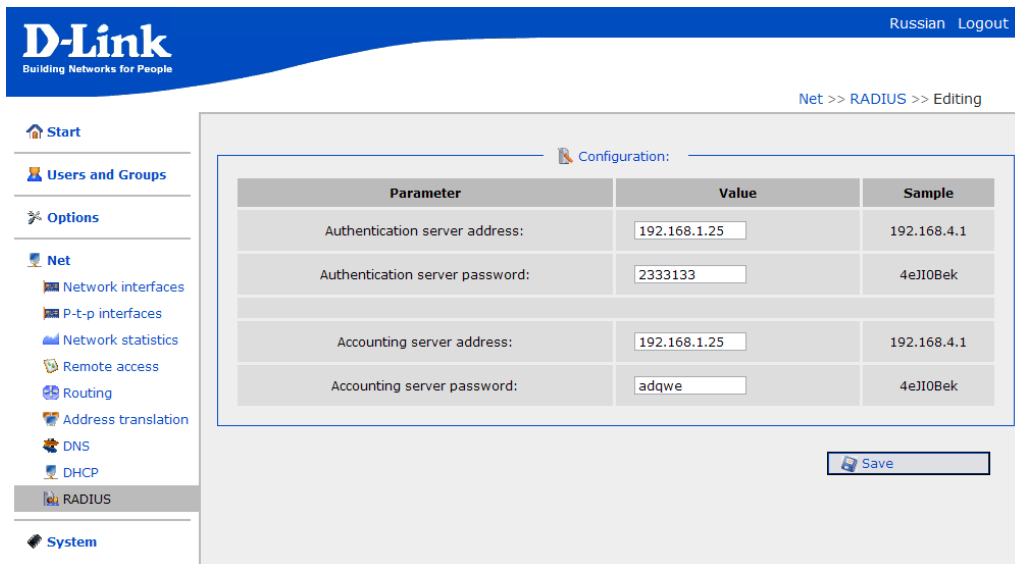
Picture 28. Modifying the settings of the device operation with the RADIUS server.

To modify the settings for operation with the RADIUS server, do the following:

- Open the **Net > RADIUS** page.

- Click the **Edit** button and change the following settings:

Authentication server address	The IP address of the RADIUS authentication server (the server where the external DB is kept).
Authentication server password	The password to access the RADIUS authentication server.
Accounting server address	The IP address of the RADIUS accounting server (the server to which the data on users' traffic are sent).
Accounting server password	The password to access the RADIUS accounting server.

Click the **Save** button.

USERS AND GROUPS MENU

This menu section is designed to create and handle the internal database of the device users.
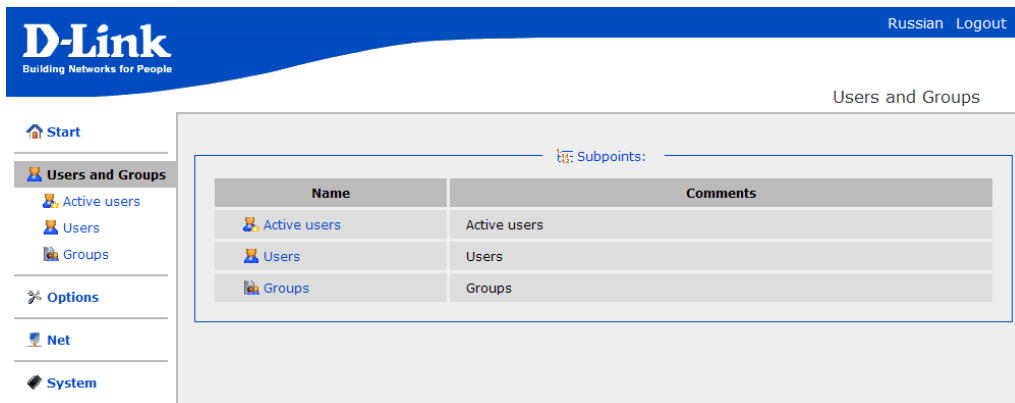
Picture 29. The **Users and Groups** page.

Groups

This page is used to handle the local database of groups.

A group itself represents the description of an access tariff for public (Hotspot) users to a broadband communication channel.

The parameters of a group completely define the access parameters (profile) for the users of this group (such parameters as the bandwidth (maximum access rate) for the group and each group user individually, the price per unit of information, and the preset number of units in the group).

Groups may be of two types:

- With time-based access.
- With traffic-based access (on the basis of consumed data).

For the first type of the groups, the **minute** or **hour** measurement unit should be set.

For the second type of the groups, the **kilobyte** or **megabyte** measurement unit should be set.

In total, you can create up to 50 user groups.

Picture 30. The **Users and Groups > Groups** page.

Working with Group Table

You can add groups to the local groups database, edit groups, or delete them.

The **Add** button is designed to create new groups. (See the information on adding new groups below.)

To handle a group that has already been created, left-click the relevant line of the group table. The line becomes highlighted.

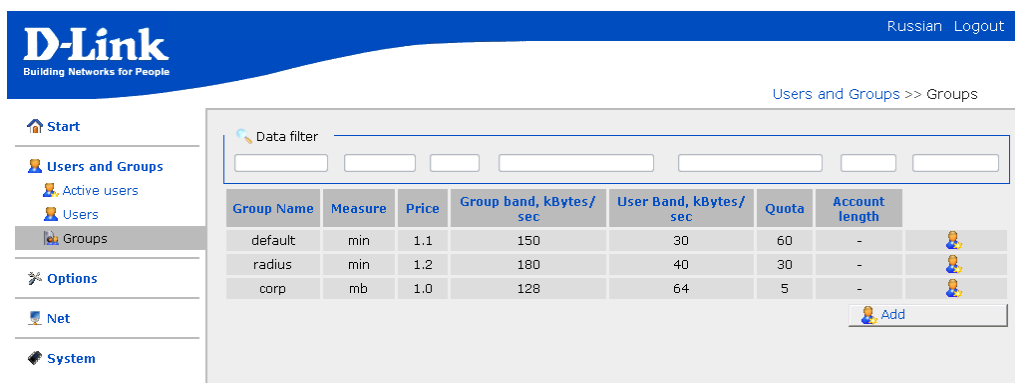| Group Name	Measure	Price	Group band, kBytes/sec	User Band, kBytes/sec	Quota	Account length	
default	min	1.1	150	30	60	-	👤
radius	min	1.2	180	40	30	-	👤
corp	mb	1.0	128	64	5	-	👤
			👤 Add	👤 Change	✖ Delete		

Picture 31. Selecting a group.

In addition, the **Change** and **Delete** buttons appear on the page.

The "man" icon (👤) located in the last cell of the group line allows direct jump to the **Users and Groups > Users > Adding** page, where you can add a new user to the group. See how to add users in the next section of the present manual.

Attention! *For user comfort, there have been introduced the* ***sorting option*** *and the fields for* ***filtering*** *groups (the* ***Data filter*** *section).*

1. Groups are sorted alphabetically by any column of the table. To sort the groups, left-click the column heading. An arrow appears in the heading of the column by which the table has just been sorted (**Price** ⬆).

2. Groups are filtered manually by entering the sequence of symbols by which groups should be filtered in the relevant fields of the **Data filter** section (located above the columns of the group table). The lines are selected by presence of the symbol sequence in the cells of the column. For example, when you enter '**def**' in the field above the **Group Name** column, all groups, which names contain this very sequence of symbols (in the beginning/end or in the middle), are selected.

Picture 32. The **Data filter** section.

Note: The filtering function is only available for browsers based on the Gecko engine, such as Firefox. This function is not yet available for the Microsoft Internet Explorer browser.

Preset Groups – Default

This group is assigned to the cheque printer (delivered separately). Initially, the **default** group is of the time-based type. You can change the type of the group on the **Users and Groups > Groups > Editing** page (see below on how to configure the settings of a group).

If a cheque printer is used, after pressing the **Print** button on the control panel of the DSA-3100P printer (or the **SEL** button in case of the Citizen CBM-910 printer), a **default** group user with a **random name** is created (with the parameters specified for the group).

Attention! *Do not remove the **default** group if you use a cheque printer. The printer will not function is there is no group named 'default' on the page.*

*Note 1: The cheque printer is assigned to the **default** group only. You **cannot** assign the cheque printer to a group with another name. To change the parameters of the tariff operated by your cheque printer, edit the settings of the **default** group.*

*Note 2: Initially, the accounts of the **default** group have unlimited expiration period, so, the cheque printer automatically creates new users but does not delete them from the system. If you want the users created by the printer to be deleted automatically upon expiration of a specified time period, edit the **Account length** parameter of the **default** group settings (see below on how to configure the settings of a group).*

The template of cheques issued by the printer can be modified on the **Option > Cheque printing** page.

Preset Groups – Radius

This group is assigned to the external RADIUS database (see the **Net > RADIUS** page). This group is used only to specify parameters of external DB users (e.g., the bandwidth). For this reason, there is no use adding users to this group locally, as such users are considered to be the users of the local database.

Creating New Group

To create a new group, do the following:

- Proceed to the **Users and Groups > Groups** page.
- Click the **Add** button.

Picture 33. Adding a new group.

- Enter the parameters for the group.

Group Name A name of the group (tariff). It is recommended to specify meaningful group names to avoid confusion when there have been created a large number of groups.

Measure A unit of measurement for the tariff. The values are: **MIN** (minute), **HOUR**, **KB** (kilobyte), **MB** (megabyte).Therefore, in this drop-down list you select not only the unit of measurement, but also the type of the group (time-based – when the **MIN** or **HOUR** value is selected, or traffic-based – when the **KB** or **MB** value is selected).

Price A price per unit (of time or traffic) for this group (tariff) in a conventional currency unit (USD, RUB, EUR, etc.).

Group band, kBytes/sec A bandwidth allocated for the **whole** group (the maximum rate in KBps for all group users in total, which can be used to transfer data to the users through the device). If the value '**0**' has been specified for the field, then the bandwidth is not limited and regarded as the maximum rate of the device (**90 MBps=11520 KBps**).

User band, Kbytes/sec A bandwidth allocated for **each** user of the group (the maximum rate in KBps for **one** user of the group, which can be used to transfer data to the users through the device). If the value '**0**' has been specified for the field, then the bandwidth is not limited and regarded as the maximum rate of the device (**90 MBps=11520 KBps**).

Quota A preset quota for users of this group (the number of time or traffic units, which can be paid for and used at once upon creating a user).

Account length A time period during which **each** user of **this** group can exist in the system (from the moment of creation). Options are **unlimited** (the time period for the account is not limited) and **manual** (the time period from the moment of creation is specified in days, hours, and minutes.

Upon the expiration of the specified period:

- Users created by the cheque printer are removed from the system automatically (even if the account balance is positive).

- Users created in the local DB manually are blocked (switched to the END_OF_ACCOUNT state). The user will still exist in the system, but the access for this user will be closed.

- Click the **Add** button.

**Attention!**

1. _**The total number of users in each group is not limited.** Therefore, **if the summary bandwidth of all users** from the group that work simultaneously **exceeds the group bandwidth**, then the latter **is shared equally for all users that work at the moment**. (For example, if the bandwidth of a group equals 100 KBps, and the bandwidth of its users is 50 KBps, then for 2 or less users the bandwidth equals to 50 KBps, for 3 users – 100/3=33.3 KBps, for 4 users –100/4=25 KBps, etc.)_

2. *A part of network connection bandwidth is often spent on service information (up to 7-8% of the bandwidth). Therefore, when a user whose bandwidth equals to 100 KBps copies a file from a remote server via FTP, the user's actual band rate may be equal to 92-93 KBps.*

Users

This page is used to handle the local user database.

Note: In the previous firmware versions, the parameter group **Username – IP address – MAC address** *served as a unique user key. In the current software version, the system doesn't check whether a MAC address is unique in order to handle users connected via VPN routers (such users have the same MAC address, but different IP addresses).*

Attention! The note above is related to VPN routers only. **For users connected via devices with the NAT (Network Address Translation) function, IP addresses are not kept. Therefore, users connected via a device with the NAT function are handled as** <u>**one**</u> **user.**

The local database contains accounts for **all** users of the public Hotspot network that are authenticated via HTTP.

In total, you can create up to 250 users in the local database.

Each user belongs to a group, which defines service data related to user data accounting: the type of accounting, the price unit, the bandwidth, etc. (for more details, see the previous section).

The picture below represents the **Users and Groups > Users** page.
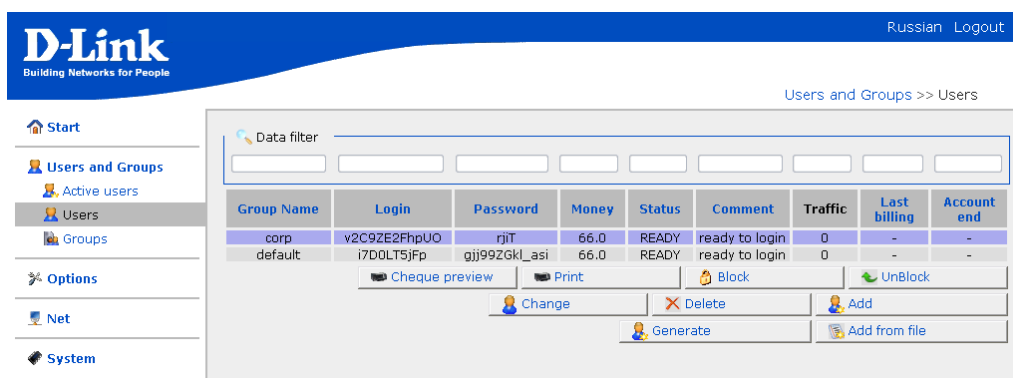
Picture 34. The **Users and Groups > Users** page.

Working with User Table

You can add users to the local user database, edit user accounts, or remove users from the database.

Initially, three buttons are available on the page: **Add**, **Generate**, and **Add from file**.

The **Add** button is designed to create new users. For more details, see below.

The **Generate** button adds a new user with a random username and password (subject to the settings of the **Options > Generator** page) to the **default** group. Practically, the action of this button is similar to the action of the relevant (**Print** or **SEL**) button of a thermal printer.

For description of the **Add from file** button, see below.

To work with a user that has already been created, select the needed user by left-clicking the relevant line in the user table. The line becomes highlighted.

Group Name	Login	Password	Money	Status	Comment	Traffic	Last billing	Account end
corp	corp1	rVoMevAhrfs6zQa	10.0	READY	ready to login	0	-	-
default	zKuwvwb8	xMAXuHZ5	66.0	READY	ready to login	0	-	-
default	tgMfFET	GiQKHluZgVt6	66.0	READY	ready to login	0	-	-

Picture 35. Selecting a user.

In addition, the following buttons appear on the page: **Change**, **Delete**, **Block**, **Unblock**, **Cheque preview**, **Print**.

The **Delete** and **Change** buttons serve to remove users that have already been created or to edit their settings.

Also you can affect user accounts, e.g., to unblock or temporarily block particular user accounts without deleting them (use the **Block** and **Unblock** buttons on the **Users and Groups > Users** page).

The **Cheque preview** and **Print** buttons serves to preview the cheque for the specified user before printing out and to reprint the cheque by the used thermal printer correspondingly.

Attention! *For user comfort, there have been introduced the* **sorting option** *and the fields for* *filtering users (the* **Data filter** *section).*

1. Users are sorted alphabetically by any column of the table. To sort the users, left-click the column heading. An arrow appears in the heading of the column by which the table has just been sorted (**Login ⬆**).

2. Users are filtered manually by entering the sequence of symbols by which users should be filtered in the relevant fields of the **Data filter** section (located above the columns of the user table). For example, when you enter '**def**' in the field above the **Login** column, all users, which names contain this very sequence of symbols (in the beginning/end or in the middle), are selected.

Picture 36. The **Data filter** section.

Note: *The filtering function is only available for browsers based on the Gecko engine, such as* *Firefox. This function is not yet available for the Microsoft Internet Explorer browser.*

Loading User Database from File

Note the function of the **Load from file** button. This button allows loading the list of users from a previously saved text file.

Each line of this file should have the following format:

login password group

Spaces serve as delimiters; spaces in logins, passwords and group names are not allowed.

To load a previously created file containing the list of users, click the **Add from file** button on the **Users and Groups > Groups** page; then click the "**Choose…**" button, select a file on your local computer, and click the **Upload** button.

The system checks the syntax of the file; if the syntax is correct, the file is displayed in the **Files with user lists** section.

When the loaded file is displayed, you can do the following:

- Add users specified in the file to the current user database (the **Add to base** button).

- Create a new database from the file (the **Rewrite base** button). Upon that all users existing in the user database are removed, and all users working at the moment are automatically logged out.

- Delete the file (the **Delete** button).

The selected **Overwrite existing** checkbox allows creating new users with the names that have been already specified for users existing in the system (the current ones are removed).

When you have performed the needed action for the file, click the **Return** button.
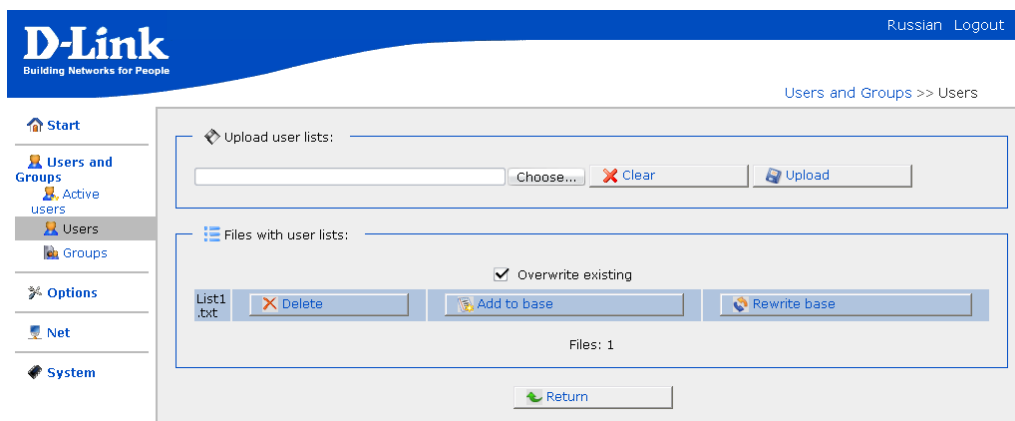
Picture 37. Adding users from a file.

Additional Information on Users Page

On this page you can obtain the information on:

- Any user account from the local database (the **Login** column).

- A group to which the account is assigned (the **Group Name** column).

- The password of the account (the **Password** column).

- The status (current state) of the account (the **Status** column).

- The balance of the local user account in conventional currency units (the **Money** column).

- The traffic consumed by the local user account at the moment irrespective of the type of the user's group (the **Traffic** column).

The displayed traffic relates to the current user session only, i.e., if a user logged out and after a time logged in, the traffic counting starts over again.

· The date and time of the latest billing action (the **Last billing** column). Billing is performed once a minute for all types of groups and users. Upon a regular billing action, when the number of tariff units is less than 1, the user's public access is blocked.

· The end date and time of the user expiration period (the **Account end** column). For an unlimited account, a dash is displayed in the column of the user line.

The following states can be displayed in the **Status** field:

READY	Ready to log in (the account has been created and is waiting for user's connection).
USER_BLOCKED	The user has been blocked by the system administrator (manually).
END_OF_ACCOUNT	The account lifetime is expired. A user with such a status cannot be authorized by the system.
INTROERR	Authentication error (e.g., an incorrect password has been entered).
INTRODUCED	Authentication has been passed successfully. The access parameters are being configured.
SHAPED	Authentication has been passed successfully. The access parameters have been configured successfully. The user is active.
SHAPERR	Authentication has been passed successfully. An error has occurred while configuring the access parameters.
DBINITERR	Errors have occurred while loading the user from the local database; the system cannot continue regular work with the user.

Adding New User

To add a new user, click the **Add** button on the **Users and Groups > Users** page.

Picture 38. Adding a new user to the local database.

You can specify the following parameters:

Group Name   The name of the group to which this user account should be assigned.

Login   A name of the account. It is used to pass authentication.

The **Clear** button is used to clear the value of the **Login** field.

The **Generate** button is used generate the login automatically subject to the **Generator** settings (see the **Options > Generator** page).

Password   A password for the account.

The **Clear** button is used to clear the value of the **Password** field.

The **Generate** button is used generate the password automatically subject to the **Generator** settings (see the **Options > Generator** page).

Money   Number of tariff units on the local account of the user. You can set this parameter at the moment of user creation, and then change it at any time by clicking the **Change** button on the **Users and Groups > Users** page when the needed user is selected.

Account end   This parameter specifies the type of the user with respect to the user's lifetime in the system.

auto – the expiration period equals to the summary of the current system time and the value of the **Account length** field specified for the user's group.

manual – the expiration period of the account is set manually irrespective of the value of the **Account length** field specified for the user's group.

unlimited – the expiration period for the account is not set (manual deletion is the only way to remove this user).

Account end (date)   Appears when the **manual** option of the **Account end** field is selected. Specified the end date and time of account expiration period.

When you have specified the parameters, click the **Add** button.

Active users

To ease the work of the administrator that configures and maintains this device, the **Users and Groups > Active users** page has been designed. It displays the list of users accessing the Internet through the device at the present moment. On this page you can also review statistics on these active users and immediately block (i.e., close public access through the device) any active user.

This page displays all users active at the present moment (both registered through the local DB and through the centralized Radius DB).
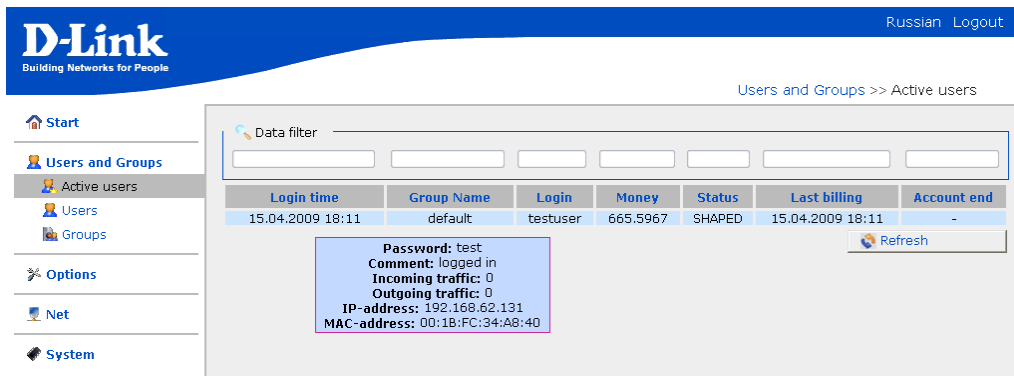
Picture 39. The **Users and Groups > Active users** page.

Working with Active User Table

To handle the active user table, select the needed user by left-clicking the relevant line in the table. The line becomes highlighted, and the **Block** and **Logout** buttons appears.
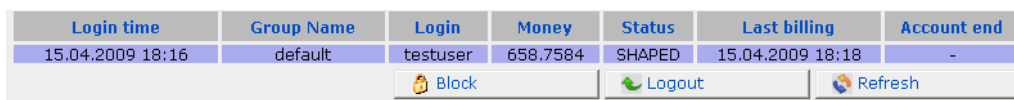

Picture 40. Working with the database of active users.

To ease the work of the administrator, pop-up help containing the detailed information on the user (MAC-address, IP address, traffic statistics, status) appears when the mouse cursor is over any line of the table.

Attention! *For user comfort, there have been introduced the **sorting option** and the fields for **filtering** active users (the **Data filter** section).*

1. Active users are sorted alphabetically by any column of the table. To sort the users, left-click the column heading. An arrow appears in the heading of the column by which the table has just been sorted ().

2. Active users are filtered manually by entering the sequence of symbols by which the users should be filtered in the relevant fields of the **Data filter** section (located above the columns of the active user table). For example, when you enter '**def**' in the field above the **Login** column, all active users, which names contain this very sequence of symbols (in the beginning/end or in the middle), are selected.
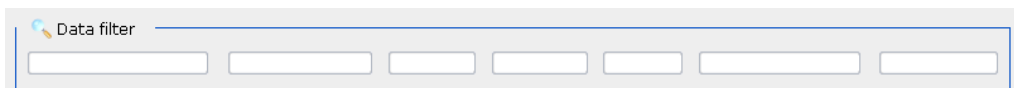
Picture 41. The **Data filter** section.

Note: The filtering function is only available for browsers based on the Gecko engine, such as Firefox. This function is not yet available for the Microsoft Internet Explorer browser.
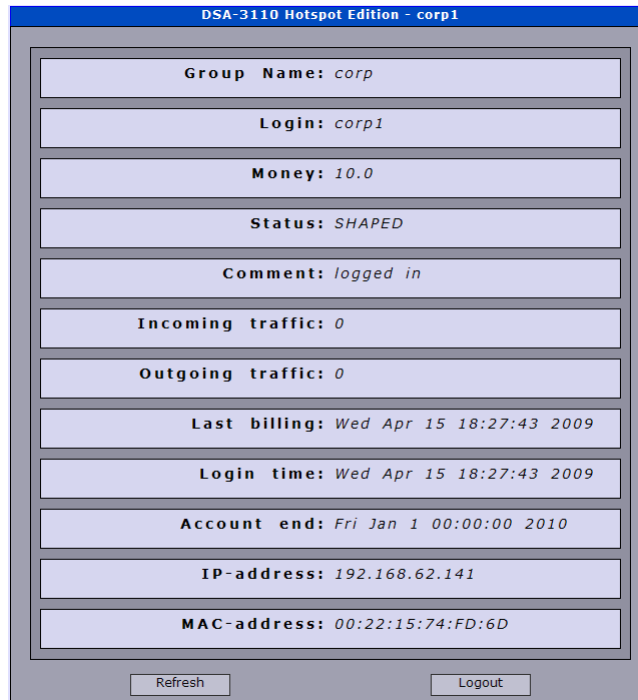
Public User Statistics

Any device user created in the local or centralized RADIUS database has unprivileged access to the web-based interface of the device through the user's account (username and password).

In the unprivileged mode, the IP address of the device's LAN interfaces is used to access the web-based interface of the device.

Unprivileged users cannot change the settings of the device and are able to view statistics on their accounts only (the same fields as on the **Groups and Users > Active users** page are displayed).

The **Refresh** button is used to refresh the account statistics. Note that the statistics is refreshed at most once per minute.

Picture 42. The user statistics page.

Attention! *A public user can close the statistics page right after entering the data for authentication over HTTP. This does not cause immediate termination of access to the global network through the device.*

To suspend public access (e.g., access to the Internet), you **must** click the **Logout** button located at the bottom of the user statistics page. Time and traffic are accounted until the button is clicked.

Note: If a user has been inactive for 250 seconds, this user is automatically logged out and public access for this user is blocked. Inactivity is considered to be the absence of data (0 byte) transmitted through the device. In this situation, you should re-enter the authentication data to resume public access.

For users registered in the centralized RADIUS DB, the period of inactivity equals to the Idle-Timeout parameter transmitted in RADIUS packets.

The value for the period of inactivity equals to the relevant value for local database (250 seconds) only when RADIUS packets do not contain the Idle-Timeout parameter.

OPTIONS MENU

This menu section contains various additional settings and functions designed to ease the operation of the device.
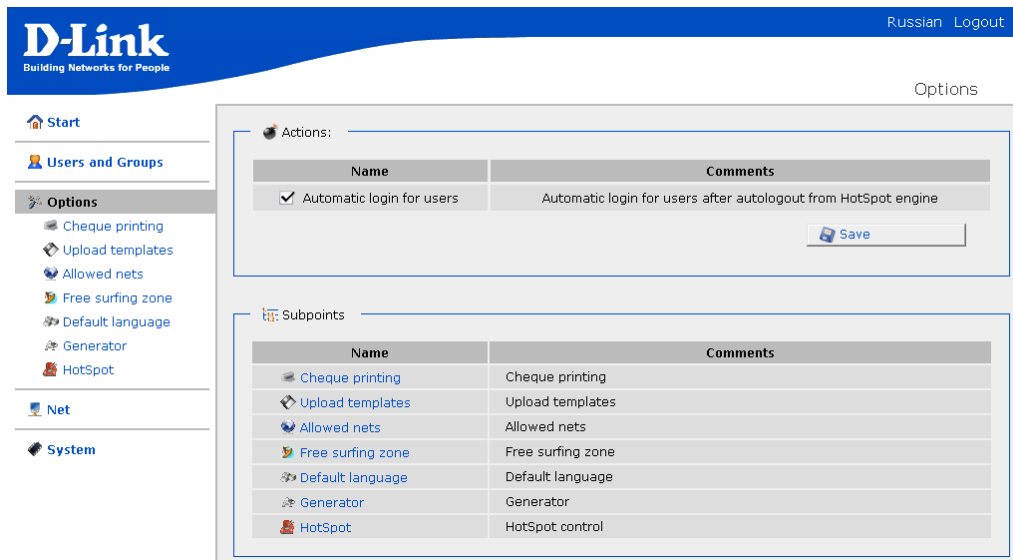
Picture 43. The **Options** page.

Note the option of automatic logging in for users that have been logged out from the Hotspot network (the **Automatic login for users** checkbox). The option is used to store the account data of the last logged-in user by his/her web browser if the connection to the Hotspot network has been terminated due to inactivity. So, when the checkbox is selected, users need not re-enter their authentication data manually after a period of temporary absence (the username and password are automatically placed to the relevant fields of the browser window). However, the user should be authenticated again.

Note: As this option is based on browser's cookies, it does not function when this browser feature is disabled.

Cheque Printing

This page is designed to configure the cheque template issued by the connected thermal printer.

On the page, you can change the values of fields and use every field to output textual or authentication data required for Hotspot users (user name, user password, supplementary data for connection to the wireless network – the network name, encryption keys and type, etc.).

Authentication data are set by special service variables beginning with the service symbol '**$**' (the values for most variables are described directly on the **Options > Cheque printing** page).

For example, the variable **$login** means that this cheque item will contain the name of the current user for whom the cheque is being generated.

The number of symbols and lines, as well as arrangement of lines on the **Options > Cheque printing** page completely corresponds to the symbols, lines and line arrangement of the cheques issued by the thermal printer. Use the **Add** and **Delete** buttons to add or remove lines of the cheque. Use the **Up** and **Down** buttons to change the positions of items (to interchange the lines).

To change the positions of cheque items or remove a line, left-click the line to select it, then click the relevant button.

The values of the **Select printer** drop-down list represent all supported types of printers.

<u>Attention!</u>

1. **Not all printers support Cyrillic symbols.** The printers that support Cyrillic symbols are labeled as **(RUS)** in the drop-down list. When you specify descriptions in Russian in the fields of the **Options > Cheque printing** page for printers that do not support Cyrillic symbols, the fields containing such descriptions are presented in unreadable characters.

2. When the special printer firmware designed for working with the DSA 3110 Hotspot Edition (see <u>here</u>) has been installed, the UNS-SP1 printer is represented DSA-3100P in the **Select printer** drop-down list.

The **Save** button is used to save the cheque template to the device memory.

The **Print** button is used to automatically generate a user in the system and print a cheque for this user with the template specified on this page.

The **Test** button is used to print a cheque with the template specified on this page without generating a user in the system.

Picture 44. The cheque template.
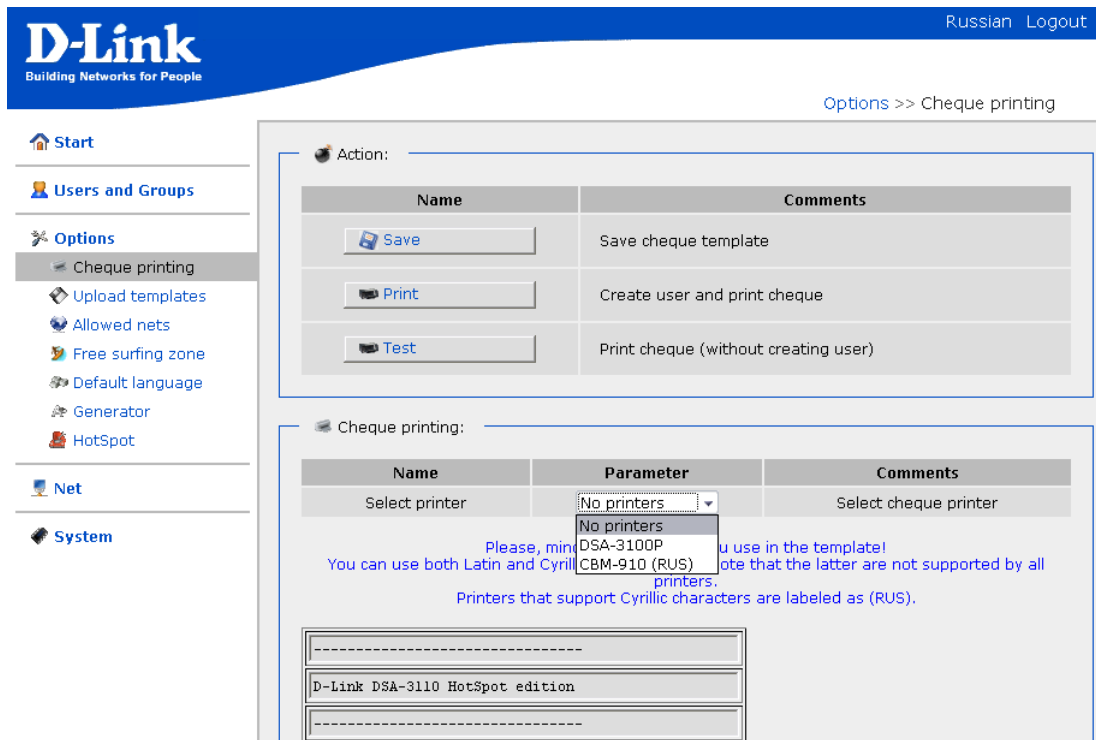
Picture 45. The **Options > Cheque printing** page. Selecting a printer.

Loading Templates

This page is designed to specify templates for the homepage (this page opens when unauthorized users try to access the Internet; here users can enter their authentication data) and the statistics page.

The owners of the system (administrators, etc.) are able to create their own home- and statistics pages for users, so they may create comfortable and useful interface. The name of the entity, advertisement, additional information, etc., can be placed on the home- and statistics pages.

If needed, the administrator can substitute a previously created **HTML page with the logo and design of the entity** for standard HTML pages with the D-link logo.

In addition, the administrator can load all other files connected to the previously created HTML page or declared in it:

- Images (png, gif, jpeg, etc.)

- Cascading style sheet files (css)

- Script files (JavaScript, VBScript, etc.).

To prepare your own (home- and statistics) pages for users, do the following:

1. Develop the design of the pages.

2. Write a HTML page with respect to the templates and restrictions specified in the present documents. See Appendix A for detailed information on the rules and restrictions for creating pages.

3. Upload files to the web-based interface of the device.

4. Control the results.

Attention! *The template files must have specific names. The names specified below are the only allowed names for template files. In other words, if you create a template and save it with, for example, the name 'my_login', the default template will be used.*

The predefined file names are:

- **udlogin_pc** – the homepage (login page) custom file designed for a personal computer (PC).

- **udlogin_pda** – the homepage (login page) custom file designed for a pocket PC (PDA).

- **udstat_pc** – the statistics page custom file designed for a personal computer (PC).

- **udstat_pda** - the statistics page custom file designed for a pocket PC (PDA).

Note: This restriction is applied for HTML pages only. You can give any names to css and script files; however, these names must be specified in the code of the HTML page.

To upload a custom template, do the following:

1. Proceed to the **Options > Upload templates** page.

2. Click the "**Choose…"** button and select the required file on your local computer.

3. Click the **Upload** button (the name of the uploaded file appears in the **Templates file list** section).

4. If the uploaded template uses css and script files, repeat the last two steps for all files needed.

*Note: If the uploaded file has appeared in the list, but the default template is still displayed, then the name specified for your template file is not correct (see the list of allowed names above). Delete the template (click the **Delete** link on the right of the relevant template), rename your template, and repeat steps 2 and 3.*
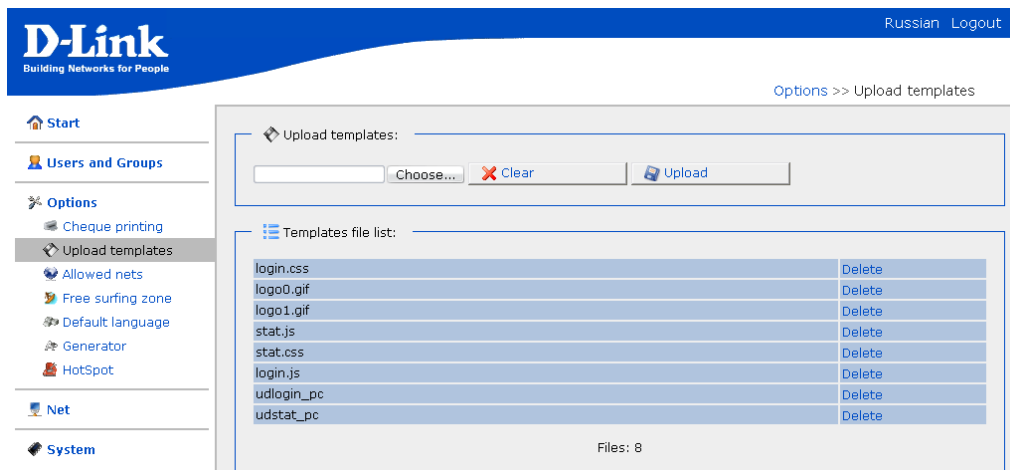
Picture 46. Uploading templates.

Note: **You can find several sample templates on the D-Link website (see** ftp://ftp.dlink.ru/pub/FireWall/DSA-3110/Firmware/HotSpot_example_templates.zip***)***

Example of Custom Homepage (Login Page)

Note: This is a demo template (see other templates on the D-Link website).

The content of udlogin_pc:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/
DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title>D-Link DSA</title>
<meta http-equiv="content-type" content="application/xhtml+xml; charset=utf-8" />
<meta http-equiv="cache-control" content="no-cache" />
<meta http-equiv="content-style-type" content="text/css" />
<link rel="stylesheet" href="templates/user/login.css" type="text/css" />

</head>

<body inhibited_load="on_load();">
<div id="id_div_main_container">
<form id="id_form_main" method="post" enctype="application/x-www-form-urlencoded"
action="index.cgi">
<div id="id_div_login_input">
@LNG:hs_login@:
<input id="A1" name="A1" type="text" maxlength="15" />
<br />
<br />
@LNG:hs_password@:
<input id="A2" name="A2" type="password" maxlength="30" />
<input id="auth" name="auth" type="hidden" value="auth" />
<br />
<br />
</div>
<div id="id_div_login_buttons">
<br />
<input name="bt" type="submit" value="@LNG:button_enter@" />
</div>
</form>
</div>
</body>
</html>
```

The content of login.css (this name of the css file is specified in the demo template):

#id_div_login_input{
width: 350px;
height: 80px;
max-width: 348px;
max-height: 78px;
text-align: center;
margin: auto;
background-color: #A0A0B0;
border-left-color: #000000;
border-right-color: #000000;
border-top-color: #000000;
border-bottom-color: #000000;
border-left-style: solid;
border-right-style: solid;
border-top-style: solid;
border-bottom-style: solid;
border-left-width: 1px;
border-right-width: 1px;
border-top-width: 1px;
border-bottom-width: 1px;
}
#id_div_login_input div{
width: 320px;
height: 60px;
max-width: 320px;
max-height: 60px;
margin: auto;
margin-top: 10px;
text-align: right;
}
#id_div_login_input div input{
width: 160px;
height: 20px;
max-width: 158px;
max-height: 18px;
border-left-style: solid;
border-right-style: solid;
border-top-style: solid;
border-bottom-style: solid;
border-left-color: #303030;
border-right-color: #303030;
border-top-color: #303030;
border-bottom-color: #303030;
border-left-width: 1px;

border-right-width: 1px;
border-top-width: 1px;
border-bottom-width: 1px;
}
#A1, #A2{
width: 160px;
background-color: #F0F0FF;
color: #0A0A0A;
cursor: text;
}
#id_div_login_buttons{
margin: auto;
text-align: center;
}

**The content of login.js (this name of the script file is specified in the demo template):**

function on_load(){
alert("Your template has been uploaded!");
}

Allowed Networks

This page is used as an access filter (to specify separate IP networks that can be authorized through the device).

Enter the ranges of IP addresses (IP subnets) in the **Allowed nets** field and click the **Save** button.

When you enter several IP subnets, separate them by a space.
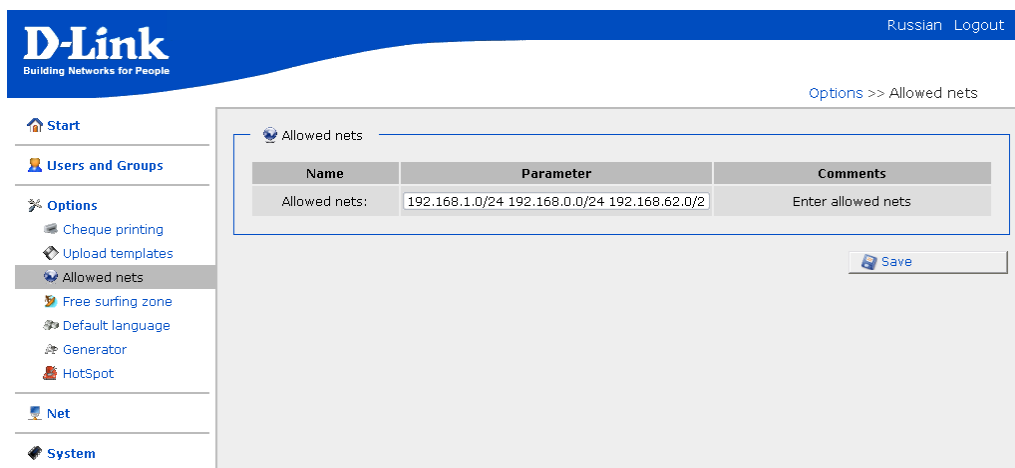
Picture 47. The **Options > Allowed nets** page.

Free Surfing Zones

This page is used to specify separate IP addresses or IP networks, access to which is not charged (e.g., the website of the entity operating the device, guest access to a website).

Enter the required IP addresses of IP address ranges (IP subnets) in the **Free surfing nets** field and click the **Save** button.

When you enter several IP addresses or IP subnets, separate them by a space.

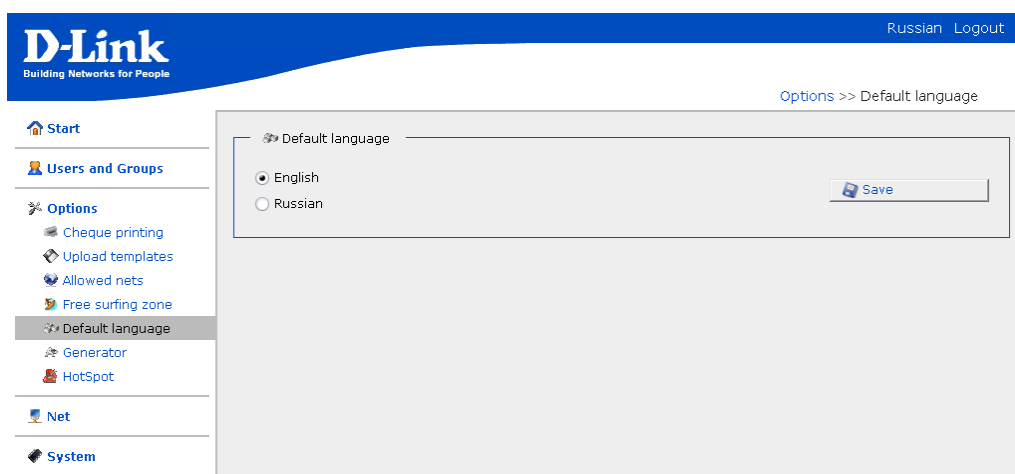Enter the rate of access to free resources (in kbps) in the **RATE KBPS** field.

Attention! Domain names are not supported. In this field, you can enter IP addresses or IP address ranges (IP subnets) only.
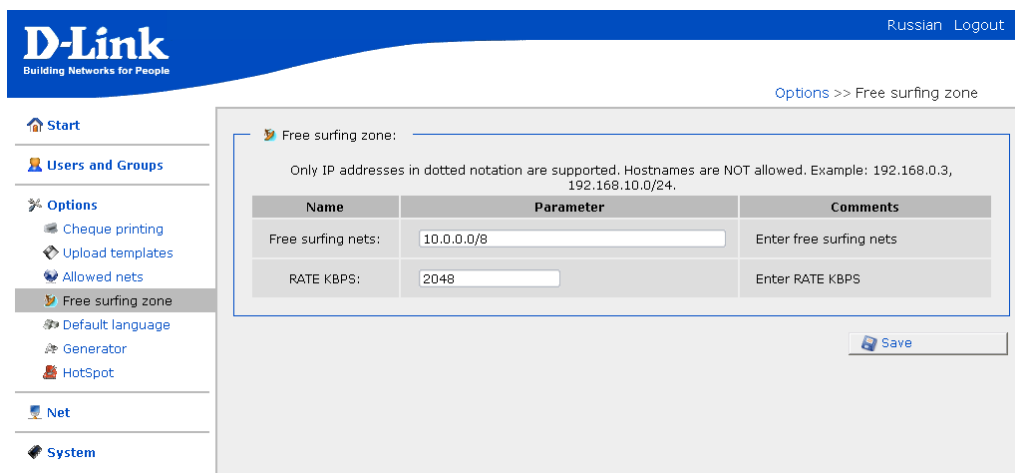
Picture 48. The **Options > Free surfing zone** page.

Default Language

This page is used to specify the default language of the device web-based interface. English is set by default.
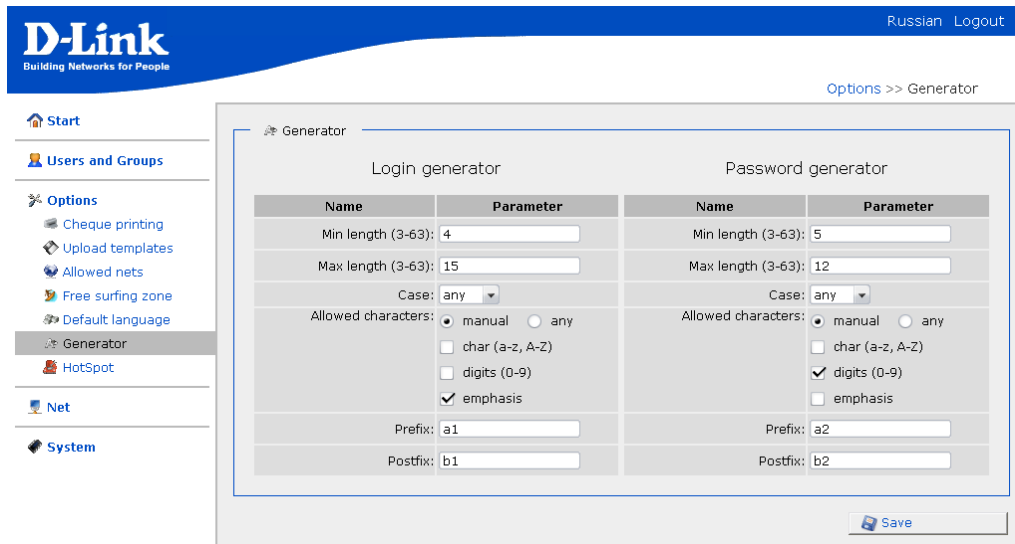

Picture 49. The **Options > Default language** page.

Generator

This page is used to specify settings of the automatic username/password generator (this generator is used on the **Users and Groups > Users** page).

This feature helps to generate local database users in accordance with the predefined format.

Picture 50. The username/password generator.

The settings are the same for both username (login) generator and password generator.

Min length	The minimal length of the login (username) or password, in characters. The default value is 4.
Max length	The maximum length of the login (username) or password, in characters. The default value is 15.
Case	The case of characters (upper, lower, any).
Allowed characters	The values are **manual** or **any**. When the **manual** option is selected, the **char**, **digit** and **emphasis** checkboxes are available. You can select any of these checkboxes or all of them.
Prefix	Specify characters that will be added to the beginning of every generated login (username) or password.
Postfix	Specify characters that will be added to the end of every generated login (username) or password.

When you have modified the settings of the generator, click the **Save** button.
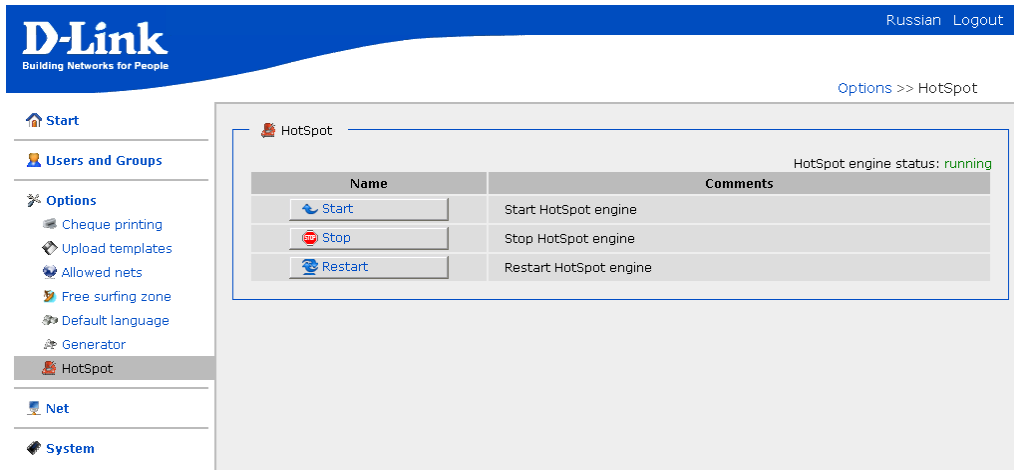
Hotspot

This page is designed to start or stop the engine for user authorization.

You can use this page to open or close the public access zone, and to disconnect all users from the access network simultaneously.

The **Start** button is used to enable the engine for user authorization.

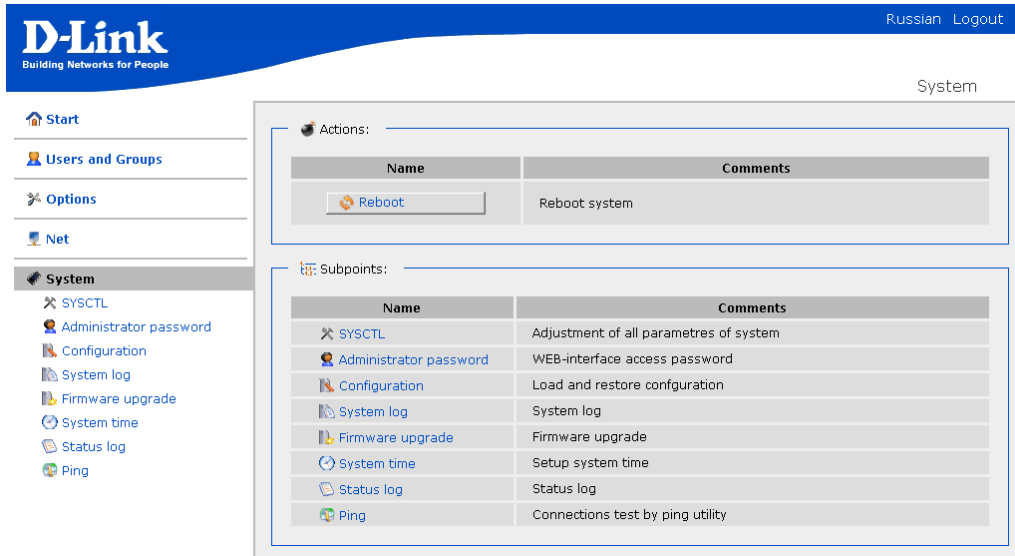The **Stop** button is used to disable the engine for user authorization.

The **Restart** button is used to suspend and then resume the engine for user authorization.

Picture 51. The **Options > HotSpot** page.

SYSTEM MENU

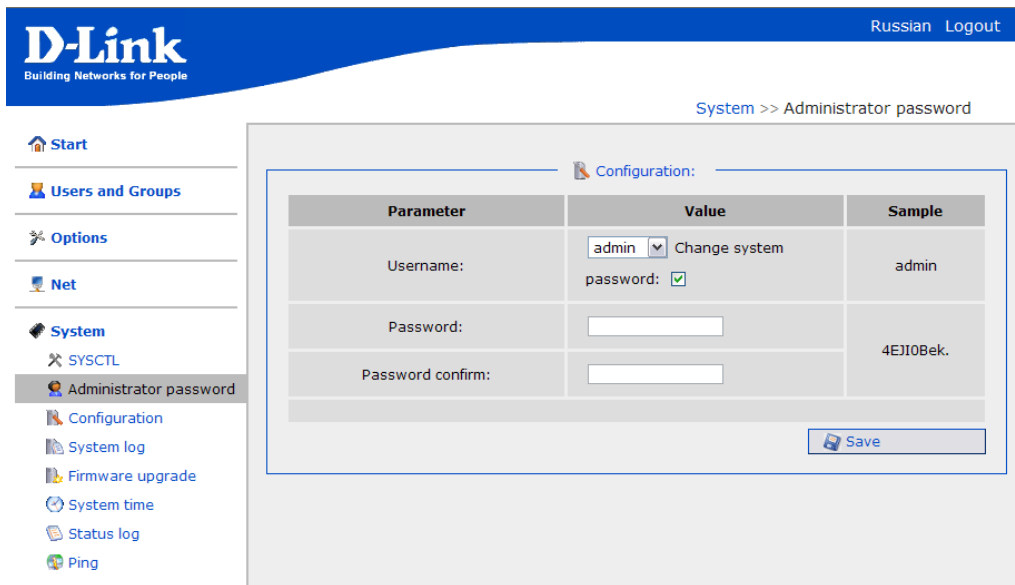This menu section is used to modify various system settings.

Picture 52. The **System** page.

The **Reboot** button is used to restart the device.

Administrator Password

Proceed to this page if you want to modify the settings of the administrator account used to access the web-based configuration interface.

Picture 53. Changing the administrator password.

User The current name of the user with administrator rights.

Three users types with different privileges exist in the system:

admin: The administrator of the device. Full authority.

owner: The owner of the device. Such a user can create and modify tariffs.

cashier: The cashier. Such a user can only sell the Internet access service according to the predefined tariffs.

**Password** Enter a new password for the selected user.

Password confirm Reenter the new password to avoid mistakes or misprints.

When you have modified the settings, click the **Save** button.

*Note: When you select the **Change system password** checkbox, the administrator password is changed not only for the web-based interface, but also for the CLI mode (it is recommended to keep this checkbox selected).*

Configuration

Proceed to this page if you want to save the modified settings or restore the factory defaults of the device.
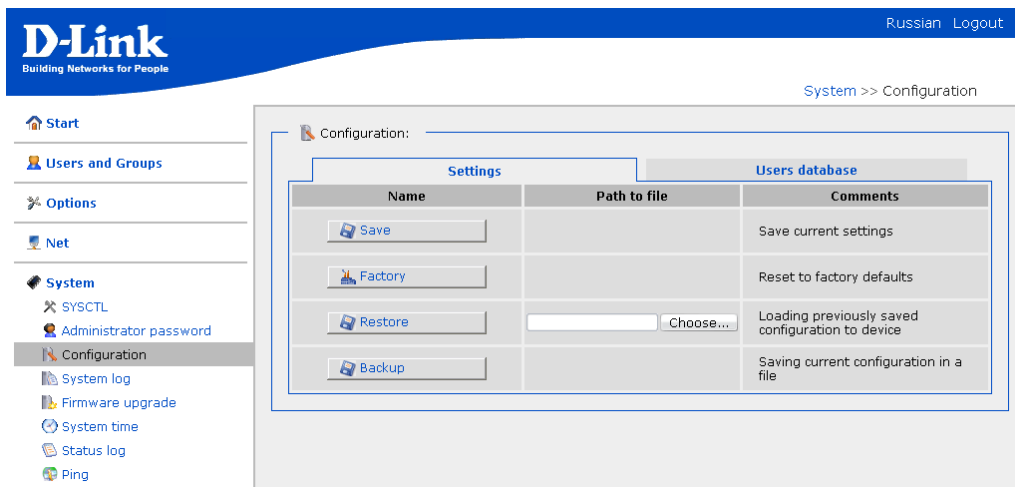
Picture 54. The **System > Configuration** page. The **Settings** tab.

The **Settings** tab:

Save   Click this button to save the modified configuration of the device in the non-volatile memory.

*__Attention!__ This button saves modifications made on all pages of this web-based interface in the non-volatile memory. Please, proceed to this page and click the **Save** button after every change of the device settings. Otherwise all changes will be lost upon reboot of the device.*

Factory   Click this button to restore the factory defaults.

*__Attention!__ Also you can reset the device settings to the factory defaults through the hardware **Reset** button. The hole of the button is located on the back panel of the device next to the power connector. Use a small paperclip to activate the button; insert it into the hole (with the device turned on), push, and hold for 10 seconds. If you act properly, first the **Status** LED turns off for 2 or 3 seconds, and then the LED blinks fast for some seconds, which means the device is restoring the default settings. After that the LED turns off for 2 or 3 seconds again, and then the device is completely reset.*

Restore   Click this button to upload a previously saved configuration from a file on your local computer. Click the "**Choose…**" button to select a saved configuration file located on your computer.

__Attention!__ Upon loading a previously saved configuration, the system checks the contents of the file you try to upload. When you upload a file created by the current version of firmware for the DSA-3110 Hotspot Edition, the system will apply the uploaded configuration. When you upload a file created by previous versions of firmware for the DSA-3110 Hotspot Edition, the system will notify you of the discrepancy between firmware versions, but will let you apply the configuration. When you upload a file created by firmware for another device, the system will not apply the uploaded configuration.

Backup   Click this button and follow the dialog box appeared to save the configuration (all parameters) of the device to your local computer.
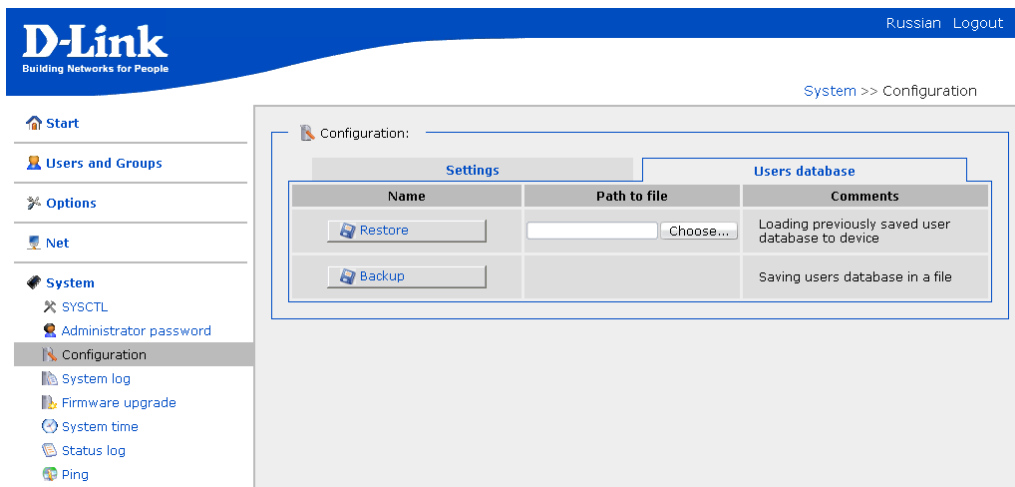
Picture 55. The **System > Configuration** page. The **User database** tab.

The **User database** tab:

Restore   Click this button to upload a previously saved user database. Click the "**Choose…**" button to select a saved database file located on your computer.

Backup   Click this button and follow the dialog box appeared to save the user database to your local computer.

Firmware Upgrade

Proceed to this page to upgrade the firmware (the built-in software) of the device.
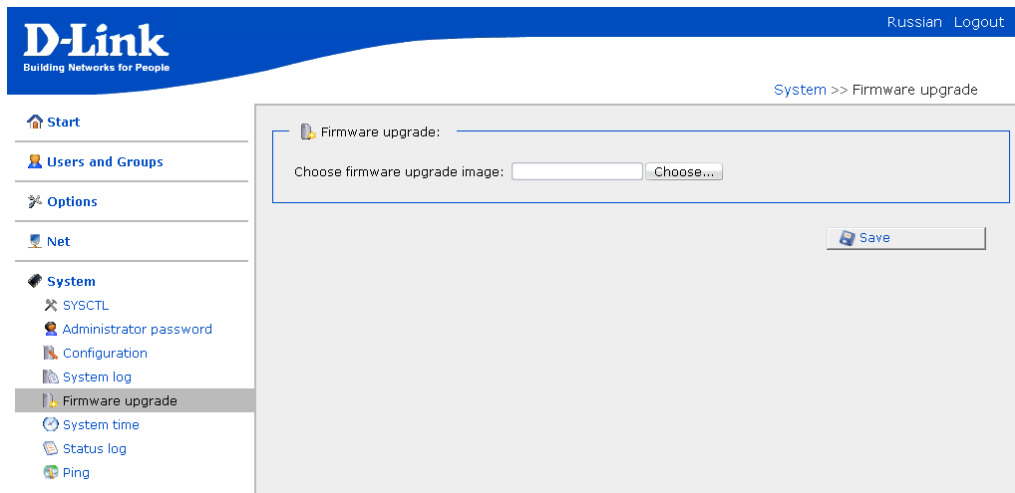
Picture 56. Upgrading the firmware through the web-based interface.

To upgrade the firmware, do the following:

- Click the "**Choose…**" button.

- Select a firmware image file on your local computer.

- Click the **Save** button.

- Wait for several minutes. **Do not interrupt the upgrade process!** While the firmware is being installed, the **System > Status log** page of the device's web-based interface displays the stages of the upgrade process. Upon the completion of the process the device is rebooted automatically.

System Time

Proceed to this page to set the date and time of the device manually.

The device is also able to perform automatic synchronization of its clock.

By default, automatic synchronization via NTP is specified. If you want to select another time server, enter its domain name in the **NTP servers** field.
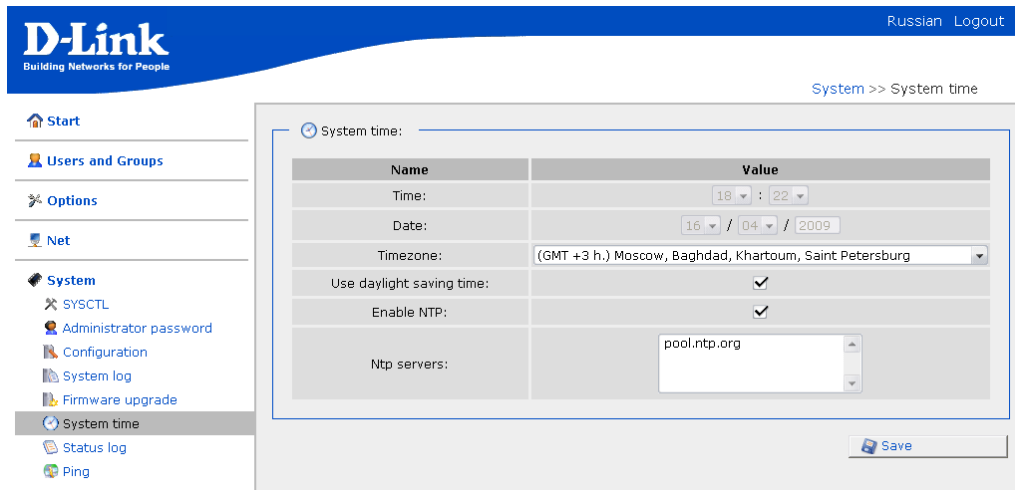
Picture 57. Configuring the system time.

To manually specify the date and time, deselect the **Enable NTP** button; then do the following:

- Enter the current time and date to the fields **Time** and **Date** correspondingly.

- Select your time zone (e.g., Moscow time is **GMT+3**).

- Enable or disable automatic transition to daylight saving time/standard time by selecting or deselecting the **Use daylight saving time** checkbox.

- Click the **Save** button.

System Log

Proceed to this page to view the system log file.

The following activities are logged: the results of the device load, the work of the internal operating system of the device, the time of users log-in and log-out.

If you select the **Remote logging** checkbox and enter an IP address in the **Server** field, the log will be transmitted to UDP port 514 of the specified IP address.

Picture 58. The **System log** page.

Status Log

Proceed to this page to view the results of the last maintenance activities (the status log).

Picture 59 displays a log describing the steps of upgrading the firmware.
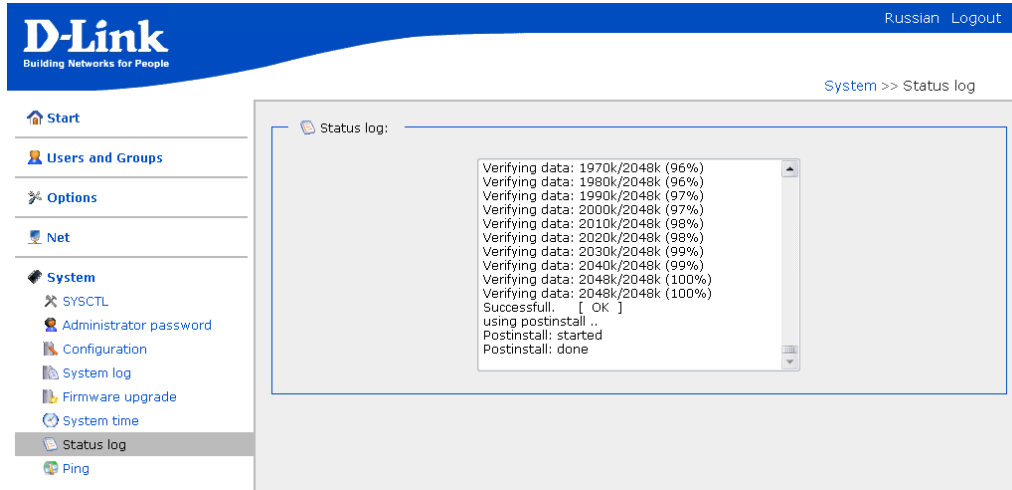
Picture 59. The **Status log** page.

Ping (Echo Request)

Proceed to this page to test whether an IP address is reachable directly via the web-based interface of the device.
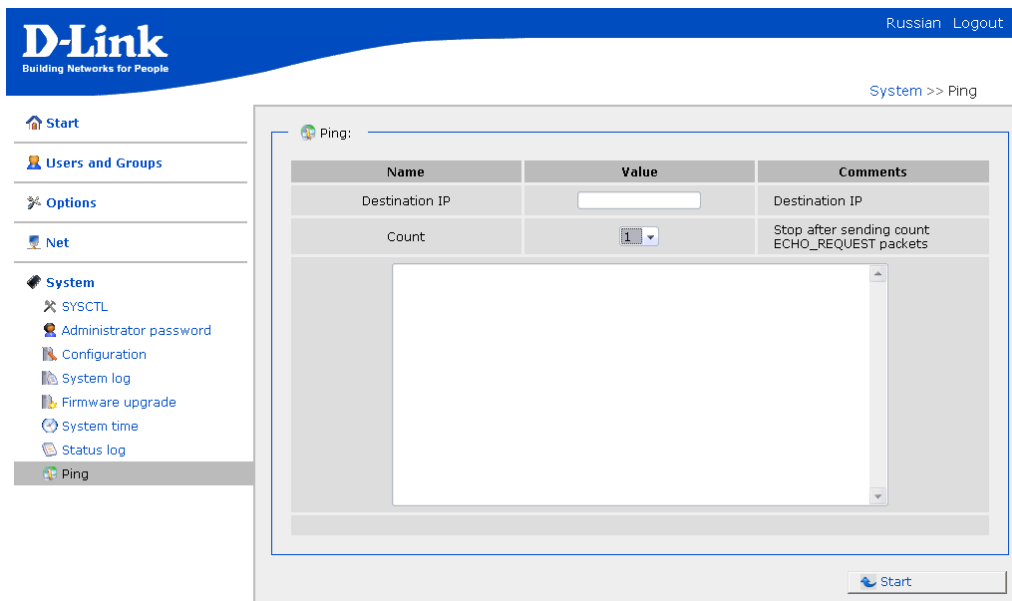
To ping an IP address, do the following:

- · Enter the relevant value in the **Destination IP** field.

- · Select the number of echo requests from the **Count** drop-down list.

- · Click the **Start** button.

The output of pinging the specified IP address will be displayed on the page.

Picture 60. The **Ping** page.

SYSCTL

This page is designed <u>for advanced users only</u>! On this page you can finely tune internal parameters of the Linux OS which is built in the DSA-3110 Hotspot Edition device.

<u>Attention</u>! Incorrect settings may lead to complete malfunction of the system.

Please study documentation on the Linux OS (man sysctl) before configuring settings on this page.
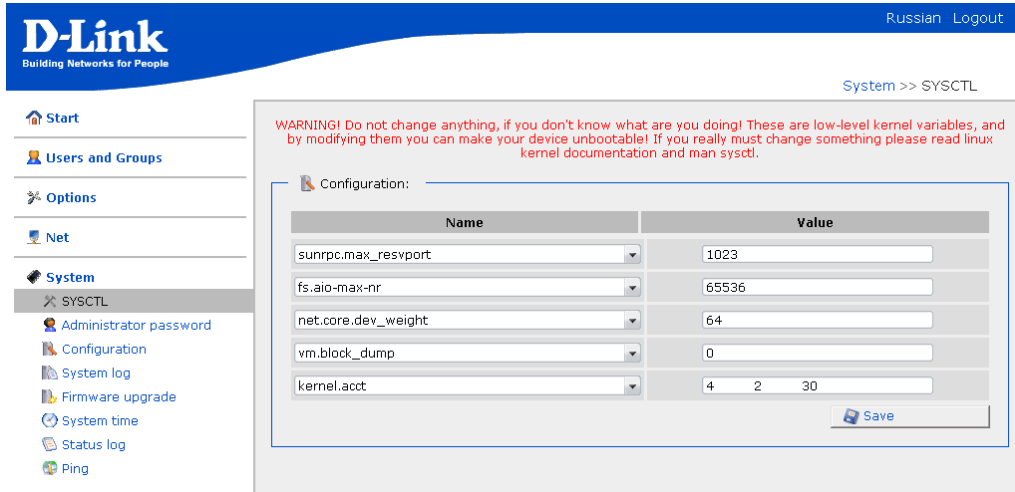
Picture 61. System parameters of the Linux OS.

APPENDIX A. RULES AND RESTRICTIONS FOR CREATING CUSTOM TEMPLATES

Page Format

You can create custom pages with help of any markup language considering whether the selected language is supported by browsers (XHTML, HTML, WML, SGML, etc.).

Below are examples of XHTML 1.0 Strict and XHTML Mobile Profile (<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> and <!DOCTYPE html PUBLIC "-//WAPFORUM//DTD XHTML Mobile 1.0//EN" "http://www.wapforum.org/DTD/xhtml-mobile10.dtd">) pages, and JavaScript scripts. You may use other markup languages in the same way.

General Structure

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title>D-Link DSA</title>
<meta name="author" content="D-Link, Russia" />
<meta name="date" content="" />
<meta name="generator" content="no generator" />
<meta name="copyright" content="Copyright (C) 2008 D-Link Russia" />
<meta name="keywords" content="D-Link DSA" />
<meta name="description" content="D-Link DSA" />
<meta http-equiv="content-type" content="application/xhtml+xml; charset=utf-8" />
<meta http-equiv="pragma" content="no-cache" />
<meta http-equiv="cache-control" content="no-cache" />
<meta http-equiv="content-style-type" content="text/css" />
<meta http-equiv="content-script-type" content="text/javascript" />
<link rel="shortcut icon" href="favicon.ico" type="image/x-icon" />
<link rel="stylesheet" href="templates/user/ttt.css" type="text/css" />
<script type="text/javascript" src="templates/user/ttt.js"></script>
</head>
<body onload="javascript:OnLoad();">
<div id="id_test">
Test
</div>
<div>
<form id="id_form_main" method="post" enctype="application/x-www-form-urlencoded" action="index.cgi">
<div>
```

@LNG:hs_login@:
*<input id="A1" **name="A1" type="text"** maxlength="15" />*
@LNG:hs_password@:
*
*
*<input id="A2" **name="A2" type="password"** maxlength="30" />*
*
*
*
*
*<input id="auth" **name="auth"** type="hidden" value="auth" />*
*
*
*
*
<input id="bt" name="bt" type="submit" value="@LNG:button_enter@" />
</div>
</form>
</div>
</body>
</html>

Attention:

The *input* tag for login entry should have the parameter *name="A1"*.

The *input* tag for password entry should have the parameter *name="A2"*.

The *input* tag with the parameter *name="auth"* should be included.

Finally, all these *input* tags should be placed within the *form* tag.

The above conditions are MANDATORY!

Also note the correct way to specify the path to a file you want to upload:

templates/user/file_name

CSS Files

Css files are connected via the following syntax:

<link rel="stylesheet" href="templates/user/<name of css-file>" type="text/css" />.

As the CGI program is located in the directory **/var/www/**, upon connection of a css-file you should specify the path to the file with regard to this directory. That is, you should add the prefix **templates/user/**.

Example: *<link rel="stylesheet" href="templates/user/ttt.css" type="text/css" />*

Script Files

The way of connecting script files (JavaScript, JScript, VBScript, etc.) is similar to the one of css-files. As the CGI program is located in the directory **/var/www**, and all files uploaded by a user are located in the directory **/var/www/templates/user**, you should add the prefix **templates/user/**.

Example: <script type="text/javascript" src="templates/user/ttt.js"></script>

Images

There are several ways to add an image to a page. Two of them (through the *img* tag in the markup code and through css) are described below.

In markup code

When you specify an image directly in the markup code (not in the css-file), for example, in the *img* tag, you should specify the prefix **templates/user** before the name of the file, as the CGI program is located in the directory **/var/www**, and all files uploaded by a user are located in the **/var/www/templates/user/**.

Example: **

Through css

To add an image, specify the name of the file containing the image in the css-file without any prefixes.

Example:

div{
color: #FF0000;
background-image: url('ttt.jpg');
}

Other Files (xml, txt)

Other files are located in the same directory – **/var/www/templates/user/**. Using such files, note that the CGI program is located in the directory **/var/www**.