

GestióIP IPAM

v3.5

IP address management software

Documentation

v1.11

www.gestioip.net

Table of Contents

1	Introduction.....	7
2	Use.....	8
2.1	Access.....	8
2.2	Show networks.....	8
2.2.1	Root networks.....	10
2.3	Show hosts.....	11
2.3.1	Host list view.....	11
2.3.2	Host overview.....	13
2.3.3	Host status view.....	13
2.3.4	Host check.....	14
2.4	Search functions.....	15
2.4.1	Quick search.....	15
2.4.2	Advanced network search.....	17
2.4.3	Advanced host search.....	17
2.5	History.....	18
2.6	Audit.....	18
3	Administration.....	21
3.1	Administration of host entries/IP addresses.....	21
3.1.1	Insert or edit host entries.....	21
3.1.2	Delete host entries.....	22
3.1.3	Host mass update.....	23
3.1.3.1	Edit multiple host entries.....	23
3.1.3.2	Delete multiple host entries.....	24
3.2	Network administration.....	25
3.2.1	New - add networks manually.....	25
3.2.1.1	Create one network.....	25
3.2.1.2	Create multiple networks with same bitmasks.....	26
3.2.1.3	Create multiple networks with different bitmasks.....	27
3.2.2	Network actions.....	28
3.2.2.1	Edit.....	29
3.2.2.2	Reserved ranges.....	29
3.2.2.3	Manual update against DNS.....	31
3.2.2.3.1	Generic rDNS entries.....	31
3.2.2.4	Manual host update via SNMP.....	33
3.2.2.5	Split.....	33
3.2.2.6	Clear.....	35
3.2.2.7	Delete.....	35
3.2.2.8	Network mass update.....	35
3.2.2.8.1	Edit multiple network entries.....	36
3.2.2.8.2	Clear multiple networks.....	36
3.2.2.8.3	Delete multiple network entries.....	37
3.2.3	Join networks.....	37
3.2.4	Show free ranges.....	38

3.2.5 Subnet calculator.....	39
3.3 VLANs.....	40
3.3.1 show, edit, delete.....	40
3.3.2 New.....	41
3.3.3 Unify.....	41
3.3.4 VLAN provider.....	42
3.3.4.1 Show VLAN provider.....	42
3.3.4.2 New VLAN provider.....	42
3.3.5 Import VLANs via SNMP.....	43
3.4 Autonomous system management.....	44
3.4.1 show, edit, delete.....	44
3.4.2 new.....	44
3.4.3 show AS clients.....	45
3.4.4 new AS client.....	45
3.5 Line management.....	45
3.5.1 show, edit, delete.....	45
3.5.2 new.....	46
3.5.3 show line provider.....	46
3.5.4 new line provider.....	46
3.6 MAC management.....	46
3.6.1 show, edit, delete.....	47
3.6.2 Add.....	47
3.7 Clients.....	48
3.7.1 Manage clients.....	48
3.7.1.1 Add clients.....	49
3.7.1.2 Edit clients.....	49
3.7.1.3 Delete clients.....	50
3.8 Sites and categories.....	50
3.8.1 Sites.....	50
3.8.2 Network categories.....	51
3.8.3 Host categories.....	51
3.9 Tags.....	52
3.9.1 Show, edit, delete.....	52
3.9.2 Add.....	52
3.10 SNMP Groups.....	52
3.10.1 Show, edit, delete.....	53
3.10.2 Add.....	53
3.11 DNS Server Groups.....	53
3.11.1 Show, edit, delete.....	53
3.11.2 Add.....	54
3.12 Custom columns.....	54
3.12.1 Predefined custom host columns.....	54
3.12.2 Predefined custom network columns.....	57
3.12.3 Add columns.....	57

3.12.4 Edit columns.....	58
3.12.5 Delete columns.....	59
4 Manage GestióIP (global configuration parameters).....	60
4.1 Client independent configuration parameters.....	60
4.2 Client specific configuration parameters.....	62
4.2.1 <i>Smallest importable BM</i>	63
4.2.1.1 Ping timeout.....	63
4.2.2 <i>DNS server</i>	63
4.2.3 <i>Manual update</i>	64
4.2.4 Extended support for OCS Inventory NG.....	65
4.3 Manage audit db.....	67
4.3.1 Reset database.....	68
5 Statistics.....	68
5.1 Network/range occupation.....	70
5.2 Miscellaneous.....	70
6 Scheduled Jobs.....	71
6.1 Create new Jobs.....	72
6.2 Job types.....	73
6.2.1 Combined discovery (global discovery).....	73
6.2.2 Network discovery.....	73
6.2.3 Host discovery by DNS.....	74
6.2.4 Host discovery by SNMP.....	76
6.2.5 VLAN discovery.....	78
6.2.6 Import DHCP leases.....	79
6.2.6.1 ISC KEA API.....	79
6.2.6.2 Kea/ISC DHCPD/MS leases/Generic CSV file.....	80
6.2.6.3 How to pass the leases information to the GestióIP server.....	80
6.2.6.3.1 Kea lease file.....	81
6.2.6.3.2 ISC DHCPD lease file.....	81
6.2.6.3.3 Microsoft DHCP lease file.....	82
6.2.6.3.4 Generic lease file.....	83
7 Database initialization.....	84
7.1 Discovery.....	84
7.2 Import networks via SNMP.....	88
7.2.1 Manual import via SNMP.....	88
7.3 Import from spreadsheet.....	89
7.3.1 Import networks from spreadsheets.....	90
7.3.2 Import hosts from spreadsheet.....	92
7.3.3 Import VLANs from spreadsheet.....	94
8 Access control.....	94
8.1 Authentication.....	95
8.1.1 Default user.....	95
8.1.1.1 Create local accounts.....	95
8.1.1.2 Update local users passwords.....	96

8.1.1.3 Delete accounts.....	96
8.1.2 Authentication against LDAP.....	97
8.1.2.1 Create LDAP server.....	97
8.1.2.2 Authentication with LDAP accounts.....	98
8.1.2.3 Authentication with LDAP groups.....	99
8.2 Authorization.....	100
8.2.1 Activation.....	100
8.2.2 User Groups.....	100
8.2.2.1 Permissions.....	101
8.2.2.2 Create User Groups.....	103
8.2.2.3 Edit User Groups.....	103
8.2.2.4 Delete User Groups.....	103
8.2.3 User “gipoper” of GestióIP versions <3.2.....	104
9 Password Management.....	105
9.1 Enabling the password management system.....	105
9.2 Manage device passwords.....	106
9.2.1 Insert a new device password.....	106
9.2.2 Show device passwords.....	106
9.2.3 Edit device passwords.....	106
9.2.4 Delete device passwords.....	106
9.3 Changing the user password.....	107
9.4 Reset the user password.....	107
9.5 Changing the master key.....	107
10 Advanced functions.....	109
10.1 Update check.....	109
10.2 Database configuration (ip_config).....	110
10.3 Export networks, VLANs or hosts to CSV.....	110
10.4 Add a new language.....	112
11 IPv6 Address plan.....	113
11.1 Direct translation.....	113
11.1.1 Create the address plan.....	114
11.2 Hierarchical IPv6 address plan based on sites and categories.....	115
11.2.1 Create the address plan.....	116
12 DNS server integration.....	122
12.1 Updates from the master DNS server to the GestióIP.....	122
12.1.1 Microsoft as master DNS server.....	122
12.1.1.1 Configure automatic notification.....	122
12.1.2 BIND as master DNS server.....	124
12.1.2.1 Configure automatic notification.....	124
12.1.3 PowerDNS installation.....	124
12.1.3.1 Create the MySQL database “pdns”.....	124
12.1.3.2 PowerDNS configuration.....	127
12.1.3.2.1 Create the PowerDNS slave zones.....	129

12.1.3.3 Automatic synchronization between PowerDNS and GestióIP.....	130
12.1.3.3.1 Create a cron job.....	130
12.1.3.3.2 Configure the pdns database parameters.....	130
12.2 Dynamic updates from GestióIP to the master DNS servers.....	131
12.2.1 Microsoft DNS server as master server.....	131
12.2.2 Create an Active Directory user.....	131
12.2.3 Allow dynamic DNS updates.....	132
12.2.4 Installation of KERBEROS client tools.....	132
12.2.4.1 KERBEROS client configuration.....	132
12.2.4.2 Testing the KERBEROS authentication.....	133
12.2.5 BIND as master DNS server.....	134
12.3 Configuration of the GestióIP server.....	134
12.3.1 Enable support for dynamic DNS updates.....	134
12.3.2 Create a “DNS update user” for GSS-TSIG authentication.....	135
12.3.3 Create a “DNS key” for TSIG authentication (BIND).....	135
12.3.4 Create a DNS zone.....	136
12.3.5 Add the custom columns “DNSZone” and “DNSPTRZone” to the registered network columns.....	137
12.3.6 Configuring networks for the dynamic DNS updates.....	137
12.3.7 Test the dynamic updates from the GestióIP to the master DNS server.....	138
12.3.8 Test the dynamic updates from the DNS master to the GestióIP server.....	138
13 General information.....	139
13.1 Backup.....	139
13.2 Firewall rules.....	139
13.3 JavaScript.....	140
13.4 Cookies.....	140
14 Troubleshooting.....	140
14.1 SNMP.....	140
14.1.1 General SNMP problems.....	140
14.1.2 Problems with VLAN discovery.....	142
14.1.3 Problems with network discovery.....	142
14.1.4 Log files.....	143
14.2 Database.....	143
14.3 Uninstalling GestióIP.....	144
15 Licence.....	144
Appendix A.....	145

1 Introduction

GestióIP is an automated, web-based IP address management (IPAM) software. It supports IPv4 as well as IPv6. The software is designed to collect information in an automated way, making its maintenance cost low. It offers web forms to import networks from spreadsheets or from the routing tables of SNMP-enabled devices and web-based synchronization of the networks against the DNS. It also allows a scheduled automatic update of the host entries via “ping”, SNMP and by DNS that ensures that GestióIP's database is always up to date. Since version 3.5.5 it is also possible to synchronize the GestióIP database with DHCP leases information.

GestióIP is optimized in order to find easily and fast the desired information by featuring effective search functions which are accessible from every page, allowing the use of Internet-Search-Engine equivalent expressions (see 2.4).

Since the system disposes about customizable columns, GestióIP's network and host list views can be adapted to meet the specific needs for every organization (see 3.12).

However, it also depends on users. Users can introduce the information in user's field of responsibility which seems relevant for this user or for their colleagues: The windows admin can put e.g. comments like PDC domain XYZ, BDC... The database admin can introduce the SIDs... and the network admin can add a comment like "TFTP" or mark the administrative interfaces of the firewalls and routers. If this is done, GestióIP can be more than an overview of current networks and IP addresses. It is a knowledge base for the small things admin must remember every day.

2 Use

2.1 Access

Open the following URL to access GestióIP:
<http://servername/gestioip>

Replace "servername" with the DNS name or the IP address of the web server. Use the user and password which you created during the script based installation part. The default user name is "gipadmin".

2.2 Show networks

GestióIP's front page (network-list-view) gives an overview of all networks. On the left side you find the "Root-net tree". By clicking over a *Root network* (see 2.2.1) of the Root-net tree, only the networks which are included within this range will be displayed.

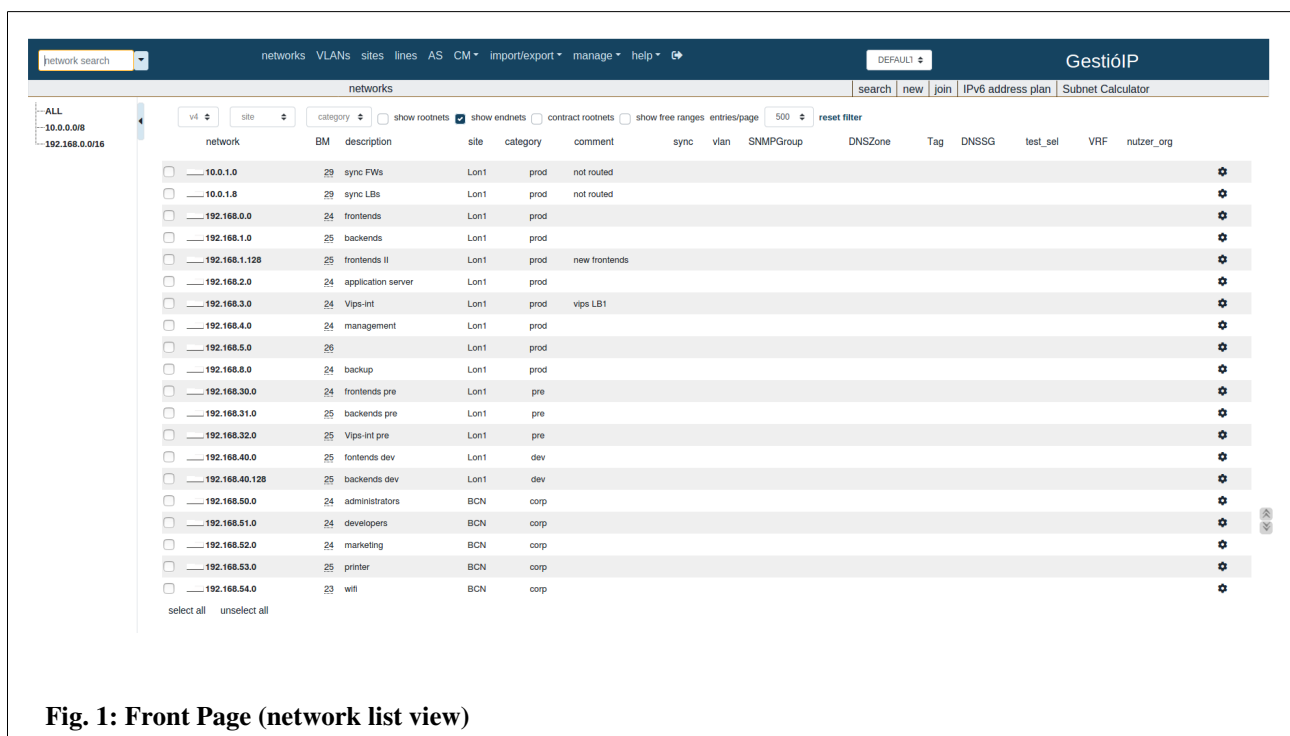


Fig. 1: Front Page (network list view)

The network-list-view offers the following filters:

IP version: to show only the networks of the selected IP version (only available if "IPv4 only mode" is set to "no" (*manage > manage GestióIP*)).

Site: to show the networks from a specific site only

Category: to show the networks from a specific category only

show rootnets: to show the root-networks within the network-list-view

show endnets: to show the end-networks within the network-list-view

contract rootnets: to show only root-networks and this end-networks ,which are not within the range of a root-network

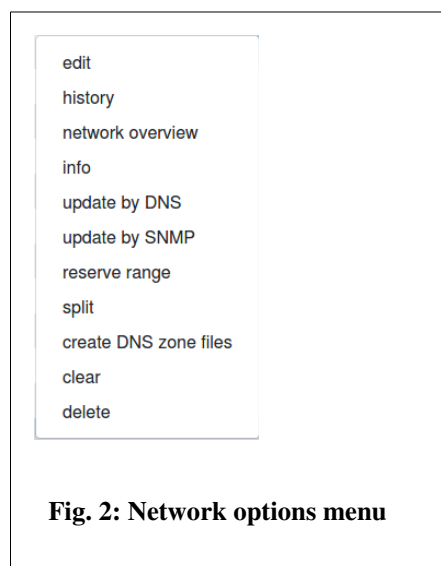
show free ranges: to show the unused IP ranges between end-networks

entries/page: to set the number of entries which should be displayed per page

reset filter: reset the filter to the default values

Click over a network to list all the IP addresses of this networks.

Clicking over the cog symbol opens the options menu for the networks.



The following menu items will give more information about the networks:

history: change-history of this network

network overview: overview about the hosts of this network

info: general information about this network (% usage and subnet-calculator like information)

See 3.2 for an description of all items.

Hover over the bitmask (BM) of the networks to display the netmask and the maximal number of hosts.

192.168.20.0	24	development	Berlin	Corp
192.168.30.0	25	frontends	Lond I	Pre
192.168.31.0	25	backends	Lond I	Pre
192.168.35.0	24	255.255.255.128 - 126 hosts	Berlin	other
192.168.37.0	24	backup	Lond I	Pre

Fig. 3: Details shown by hovering over a BM entry

Note

Use “network quick search” to locate individual networks. Search e.g. for “150” to find network 192.168.150.0. Or use “network quick search” or to display network ranges. Search e.g. for “192.168” to display all networks which IP include 192.168 (see 2.4).

2.2.1 Root networks

GestióIP supports to types of networks. *Root networks* which can contain other networks but no host entries and *end networks* which contain the host entries.

Root networks are containers for networks permitting to structure organization's networks hierarchically. *Root networks* can contain *end networks* as well as other *root networks*.

By clicking over a Root network of the root-net tree, only the networks within the range will be displayed.

networks													
network	BM	description	site	category	comment	sync	vlan	SNMPGroup	DNSZone	Tag	DNSSG	test_sel	VRF
<input type="checkbox"/> 192.168.0.0	24	frontends	Lon1	prod									
<input type="checkbox"/> 192.168.1.0	25	backends	Lon1	prod									
<input type="checkbox"/> 192.168.1.128	25	frontends II	Lon1	prod	new frontends								
<input type="checkbox"/> 192.168.2.0	24	application server	Lon1	prod									
<input type="checkbox"/> 192.168.3.0	24	Vips-int	Lon1	prod	vips LB1								
<input type="checkbox"/> 192.168.4.0	24	management	Lon1	prod									
<input type="checkbox"/> 192.168.5.0	26		Lon1	prod									
<input type="checkbox"/> 192.168.6.0	24	backup	Lon1	prod									
<input type="checkbox"/> 192.168.30.0	24	frontends pre	Lon1	pre									
<input type="checkbox"/> 192.168.31.0	25	backends pre	Lon1	pre									
<input type="checkbox"/> 192.168.32.0	25	Vips-int pre	Lon1	pre									
<input type="checkbox"/> 192.168.40.0	25	frontends dev	Lon1	dev									
<input type="checkbox"/> 192.168.40.128	25	backends dev	Lon1	dev									

Fig. 4: Free ranges view

Activate checkbox “show rootnets” to display the *root networks* within *network list view*. *Root networks* are displayed with a brown background.

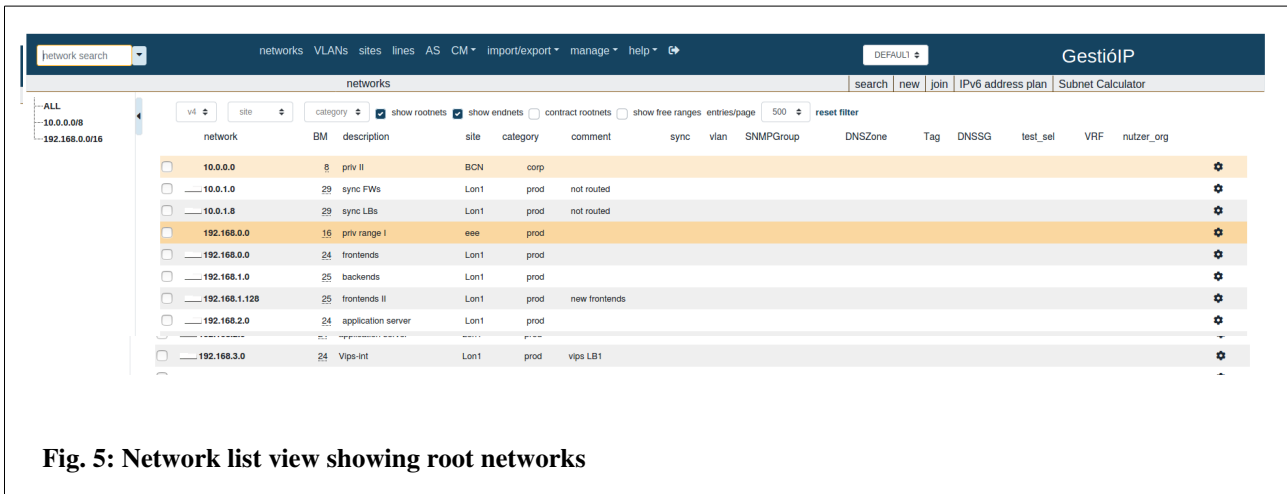


Fig. 5: Network list view showing root networks

Checking the checkbox “show free ranges” will display all networks which are included within this range as well as the free ranges between the defined *end networks*.

2.3 Show hosts

GestióIP offers three different views of networks: *host list view*, *host overview* and *host status view*.

2.3.1 Host list view

To list all IP address of a network, open the front page and click over the corresponding network.

free: 219 (86.2%) used: 35 (13.7%) all: 254		entries/page 254					
IP	hostname	description	site	type	AI	comment	
● 192.168.0.1	fw1-fw2_vrrp		Lond I	FW			
● 192.168.0.2	fw1		Lond I	FW			
● 192.168.0.3	fw2		Lond I	FW			
● 192.168.0.4			Lond I				
● 192.168.0.5	jupiter.gestioip.net		Lond I	L2 device			
● 192.168.0.6	saturn.gestioip.net		Lond I	L2 device			
● 192.168.0.7	pluto.gestioip.net		Lond I	L2 device			
● 192.168.0.8	europa.gestioip.net		Lond I	L2 device			
● 192.168.0.9	io.gestioip.net		Lond I	L2 device			
● 192.168.0.10	atair.gestioip.net		Lond I	L2 device			
● 192.168.0.11	unknown		Lond I	L2 device			

Fig. 6: Host list view (standard columns)

Click “free” to show only unassigned or “used” to show only assigned IP addresses.

The colored point in front of the IP addresses shows the result of the last check via “ping”. By hovering over the point, date of last check will be displayed. Clicking the point executes the *host check*.

host list view offers at the end of each line furthermore links to

access the *history* of this IP address

edit the entry

delete the entry

and links to the following network manipulation buttons at the top of the page.

edit – to resize bitmask or edit description, site, category, comment or status of automatic synchronization (see 3.2.2.1)

reserved ranges – to reserve or delete reserved IP address ranges (see 3.2.2.2)

manual update – to synchronize the network entries against the DNS (see 3.2.2.3)

manual update via SNMP – to synchronize the networks via SNMP (see 3.2.2.4)

split network – to split network into smaller subnets (see 3.2.2.5)

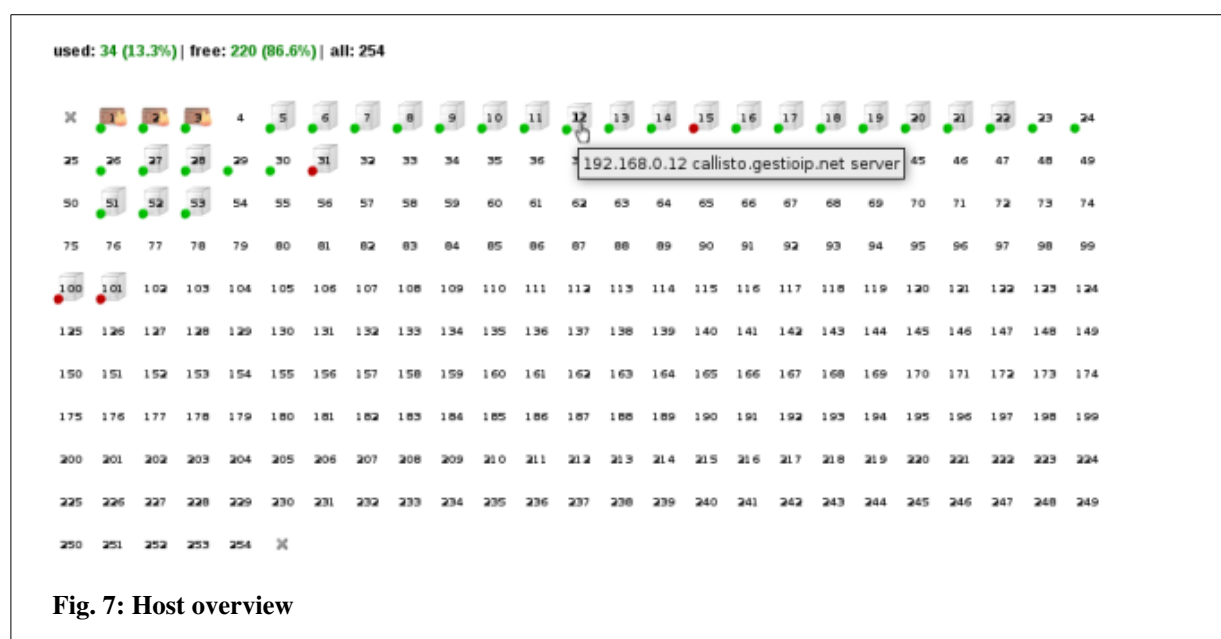
clear network – delete all entries of the network (entries of reserved ranges will be maintained) (see 3.2.2.2)

Note

Functions “reserved ranges”, “manual synchronization”, “network overview” and “host status view” are not available for IPv4 networks with a BM smaller than 20 and IPv6 networks with prefix length smaller than 120.

2.3.2 Host overview

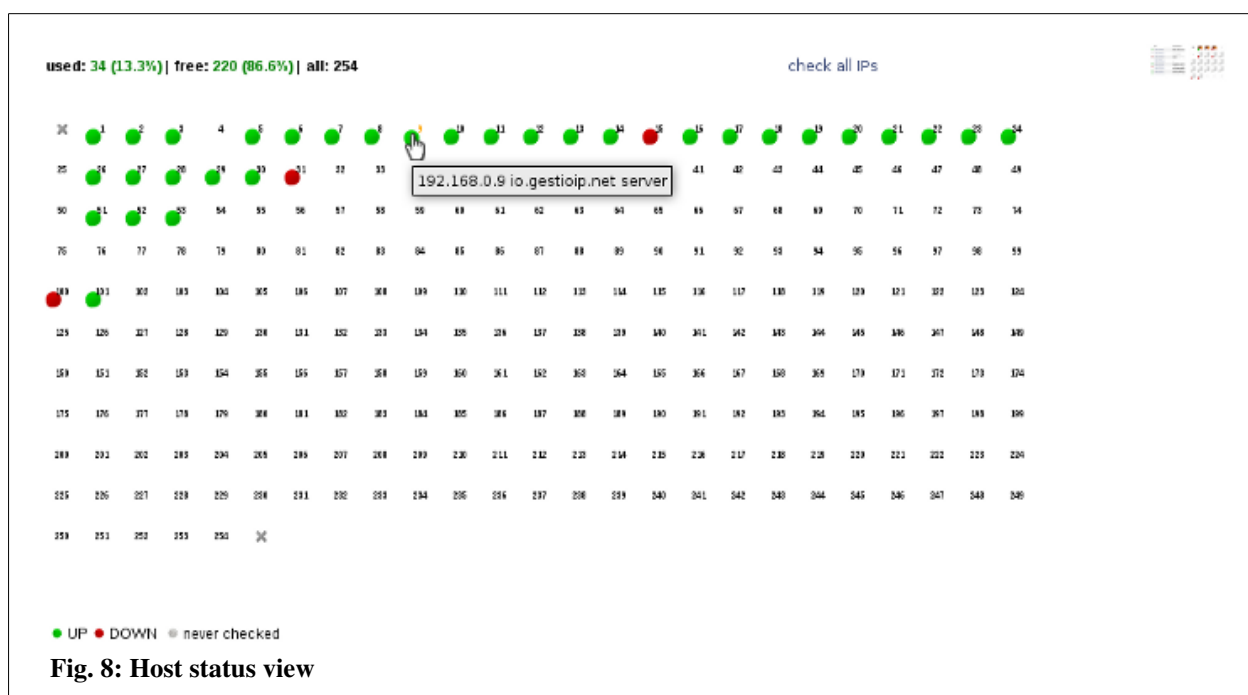
The *host overview* gives an overview about the host types of a network.



Access to *edit host* form by clicking on an IP address.

2.3.3 Host status view

Host status view shows the status of all IP addresses of a network in a compact manner.



Execute the *host check* by clicking on an IP address. To check the status of all addresses of a network click "check all IPs". Unassigned addresses will be indicated with a blinking number.

2.3.4 Host check

To execute the host check access the relevant network and click over the point in front of the IP address.

IP	hostname	description	site	type	AI	comment	
● 192.168.1.1	fw1-2_virt		Lond I				h [icon] X
● 192.168.1.2	fw1		Lond I				h [icon] X
● 192.168.1.3	fw2		Lond I				h [icon] X
● 192.168.1.4		...	Lond I		h [icon]
● 192.168.1.5	leo	database	Lond I			oracle 9i applications extern	h [icon] X
● 192.168.1.6	hydra	database	Lond I			oracle 10g applications intern	h [icon] X

last check: 2010-01-31 22:46:59

Fig. 9: "Host check" execution from host list view

GestióIP checks the IP address with an ICMP echo request ("ping") and executes a DNS PTR query. When the IP address has an PTR entry, GestióIP executes a DNS A query with the result of the PTR query.

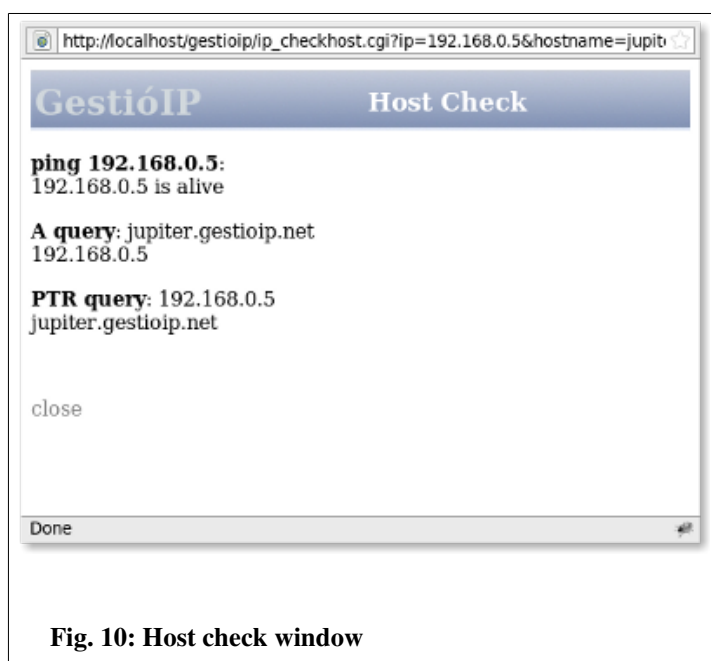


Fig. 10: Host check window

The *host check* is also available from *host status* view and from the *edit host*-form.

Note

If results of DNS A and PTR query don't correspond make sure that there is no DNS misconfiguration.

2.4 Search functions

GestióIP offers two different search engines. The *quick search* and the *advanced search*.

Note

You can export the search result to CSV format by clicking the link “export search result”.

2.4.1 Quick search

The *quick search* executes a search through all fields of the entries.

The quick search allows Internet Search Engine equivalent expressions like *-string_to_ignore*, *+exact_match* and *"exact match"*. A single string will be processed like *"%search-string%"*. By using search-string "192", GestióIP lists all networks with an ID containing "192". With search-string "dhcp", it lists all networks with descriptions or comments containing "dhcp". With search-

string “192 prod” it will list all networks of production environment whose ID contains “192”. The search isn't case sensitive.

Search expression examples:

entry: **foo bar**

<i>expression</i>	<i>result</i>
fo	match
FO	match
foo	match
bar foo	match
foo -ba	match
foo -bar	no match
+fo	no match
+foo	match
"bar foo"	no match
"foo bar"	match
"oo ba"	match

2.4.2 Advanced network search

The advanced search executes a search in specific database fields.

client independent ☐

network ID: * *

description: * *

comment: * *

site:

category:

Synchronized: ☒ all ☐ only synchronized networks ☐ only not synchronized networks

search ☐ to change/delete networks

Fig. 11: Advanced network search

You can search for instance all production networks which are not included within the automatic synchronization or all networks of site xy where the description contains "backup".

When the check-box "to change/delete networks" is checked, the network manipulation buttons *change*, *ranges*, *synchronize*, *split*, *clear* and *delete networks* are shown within the search result.

Note

If you have multiple clients configured, there appears the new check-box "client independent search" which permits to execute a search through GestioIP's database ignoring to which client the network belongs. The client will be shown within the search result.

2.4.3 Advanced host search

If the check-box "exact match" behind the hostname field is checked, only hosts with hostname entries identical to the search string would be listed. If not, the search string would be processed like "%search_string%".

Example: search for "foo"

Result without marked check-box: foo, foo1, foo.bar.com...

Result with marked check-box: foo

2.5 History

The history is available for both, networks and hosts. It lists IP address or network specific events from the audit db. Access network history from the *network list view* and host history from *host list view* by clicking the **h** icon.

Note

History information is extracted from audit log. Deleting old audit events causes history entries to also be deleted.

2.6 Audit

The audit system logs all events to GestioIP's database.

To access the audit log click on *manage > audit*.



Fig. 12: Audit log filter

The audit page offers flexible search and filter functions for all audit fields.

"time range" or **"date from ... to"** - mark the radio button to either show entries of a time range (e.g. last 4 weeks) or to specify a start and an end date.

"search string" - search for an individual search string. Searches all audit specific database fields.

"type" - search for a specific event type.

GestióIP recognizes the following event types:

<i>event type</i>	<i>description</i>
man	manual events launched from GestióIP's web interface
auto	event created by the automatic updating of GestióIP v2.2.5 (DNS, OCS, import

	via SNMP)
man dns	manual network synchronization against the DNS (via Web interface)
auto dns	automatic network synchronization against the DNS
auto ocs	automatic network synchronization against the OCS Inventory NG
man snmp	manual import of networks from snmp-enabled devices
auto snmp	automatic import of networks from snmp-enabled devices
man net sheet	manual import of networks from spreadsheet
man range	Events in relation with ranges (create, delete)
man host sheet	manual import of hosts from spreadsheet
red cleared	all entries of a network manually deleted

"class": Search for event class

GestióIP recognizes the following event classes:

<i>event class</i>	<i>description</i>
host	for events related to host entries (e.g. host deleted, host edited, ...)
net	for events related to networks (e.g. network added, network split, reserved range added, network synchronized against DNS, ...)
security	for events related to security (e.g. old audit events deleted)
dns	unused
admin	For changes in GestioIP's configuration
conf	automatic network synchronization against the DNS
man_vlan	manual events related to to VLANs
vlan_auto	automatic update of VLAN database
ini_man	Manual execution of discovery process
ini_auto	unused
AS	For events related to autonomous systems
AS client	For events related to autonomous systems clients
line	For events related to leased or dial-up lines
line client	For events related to leased or dial-up lines clients

"event": Search for events like (host edited, host deleted, range added, ...)

"entries/page": Define the number of found entries per page.

“user”: Can be found using the field “search string”.

The shown user can either be a system user (for AUTO events) or a GestióIP user (for MAN events created from actions carried out manually via front end Web).

Note

If you configure authentication with individual accounts, audit will show individual users (see 2.6). When using generic accounts (e.g. gipadmin) it is not possible to directly reproduce who has made which changes.

Format of entries:

Hosts events: IP, hostname, description, site, category, comment, administrative interface

Network events: IP/bitmask, description, site, category, comment, synchronized

Note

If you have multiple clients configured, there appears the new check-box “all clients” which permits to perform a client independent search through GestioIP's database. The client will be shown within the search result.

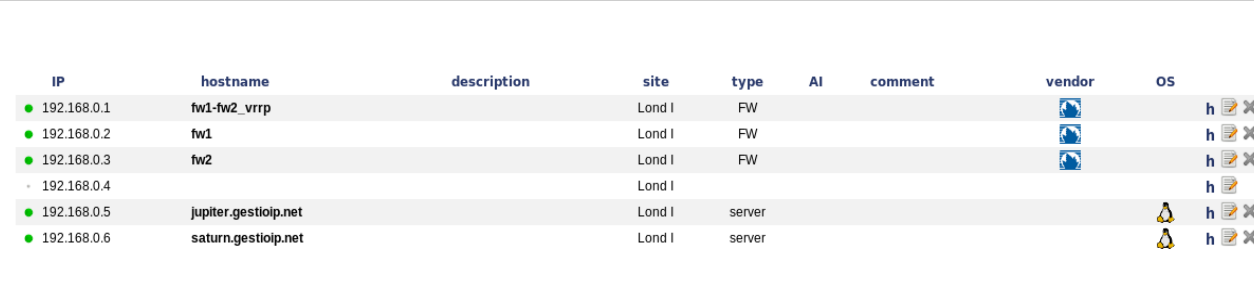
Note

To delete old audit events or to see how many events are currently stored in the database, go to manage > manage GestióIP.

3 Administration

3.1 Administration of host entries/IP addresses

To manage host entries/IP addresses, access *host list view* by clicking on the relevant network.

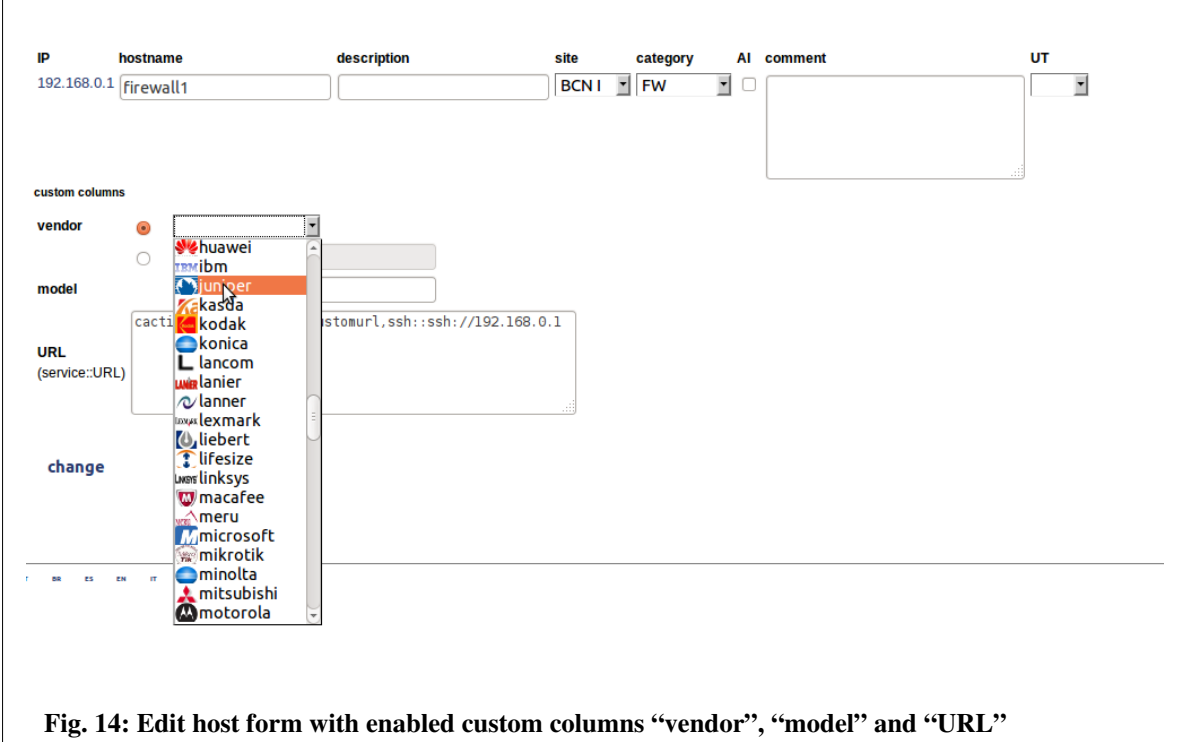


IP	hostname	description	site	type	AI	comment	vendor	OS
192.168.0.1	fw1-fw2_vrrp		Lond I	FW				h
192.168.0.2	fw1		Lond I	FW				h
192.168.0.3	fw2		Lond I	FW				h
192.168.0.4			Lond I					h
192.168.0.5	jupiter.gestioip.net		Lond I	server				h
192.168.0.6	saturn.gestioip.net		Lond I	server				h

Fig. 13: Host list view

3.1.1 Insert or edit host entries

Click on the "edit" icon behind the IP address to insert or edit host entries .



IP: 192.168.0.1 hostname: firewall1 description: site: BCN I category: FW AI: ☐ comment: UT:

custom columns

vendor: huawei ibm juniper kasa kodak konica lancom lanier lanner lexmark liebert lifesize linksys macafee meru microsoft mikrotik minolta mitsubishi motorola

model:

URL (service::URL):

change

Fig. 14: Edit host form with enabled custom columns “vendor”, “model” and “URL”

Hostname – Name to identify the node. If a node has more than one interface it is advisable to introduce the same hostname for all IPs or to introduce the hostname in the comment field of all IPs of the node – so that the search function finds all IPs of a node when searching for its hostname - mandatory field

Description – Short description of the node - optional field

Site – Physical location of the node – mandatory field

Category – Category of the node – optional field

AI (Administrative Interface) – To mark the IP address to access the node (to administrate it) in case the node has more than one network interface – optional field

Comment – To point out whatever seems to be interesting regarding this node – optional field

UT (Update Type): Relevant for manual synchronization against DNS and automatic update

- *man* – Entries which are marked as "man" will never be overwritten.
- *ocs* – Entries created by the automatic update against an OCS Inventory NG. Entries which are marked as "ocs" will not be overwritten by manual or automatic update against DNS.
- *dns* - For entries created by manual or automatic update against DNS. Entries which are marked as "dns" will be overwritten by automatic update against DNS and OCS.
- Entries with no update type will be overwritten by manual and automatic update against DNS and OCS.


Custom columns

When there are custom columns enabled, there appear fields for every of these columns, permitting to edit the value (see 3.12).

Note

To prevent an entry from being overwritten by the automatic update, it must be classified as "man".

3.1.2 Delete host entries

Click “delete”  to drop host entries from GestióIP's database.

3.1.3 Host mass update

Host mass update feature offers the possibility to perform actions on multiple host entries at once. It allows to edit one or multiple host column entries or to delete multiple host entries.

3.1.3.1 Edit multiple host entries

To edit multiple host entries access to *host list view*, mark the corresponding checkboxes in front of the host entries to edit, select action type “edit”, select the columns to edit and press “mass update”

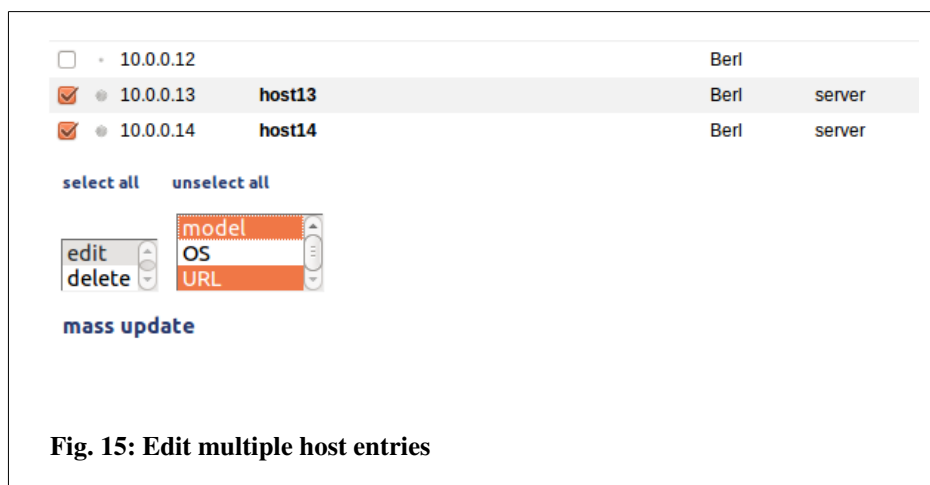


Fig. 15: Edit multiple host entries

Edit the values and press “change” to save them to the database.

The form contains the following fields and controls:

- site**: A dropdown menu with 'Berl' selected.
- category**: A dropdown menu with 'printer' selected.
- comment**: A large text area.
- vendor**: A radio button (selected) next to a dropdown menu with 'canon' selected.
- model**: A text input field.
- URL (service::URL)**: A text area containing the template 'telnet::telnet://[[IP]],http::http://[[IP]]'.
- change**: A button at the bottom.

Fig. 16: Edit multiple host entries form

Note

If a entry without assigned host is edited, the hostname will be automatically set to “unknown”

Note for custom column “URL”

Custom column “URL” allows to use variables for the IP-addresses and for the hostnames (see 3.12.1).

If the “URL” entry is equal for all selected host, the entry will be proposed as URL-value when entering multiple-host-entries-form.

3.1.3.2 Delete multiple host entries

To delete multiple host entries access to *host list view*, mark the corresponding checkboxes in front of the host entries to delete, select action type “delete” and press “change”.

3.2 Network administration

GestióIP offers several tools to create, delete or manipulate networks.

3.2.1 New - add networks manually

To add a new networks manually, click over *networks* > *new*.

The *new* form offers the possibility to create one network, multiple consecutive networks with the same bitmasks or multiple consecutive networks with different bitmasks.

3.2.1.1 Create one network

☒ IPv4 ☐ IPv6

Root network ☐

network*
 (e.g. 192.168.0.0)

BM* (255.255.255.255) calculate

description*

comment

Site*

category*

include networks within automatic update ☐

add

Fig. 17: "new network" form - create on network

network – ID of the network. e.g.: 192.168.0.0 – mandatory field

BM (bitmask) – Bitmask of the network – mandatory field

description – Short description of the network – mandatory field

comment - Optional comment

site – Where is the network “physically” located? When the site of the network is changed (or renamed), site of the host entries of the network will be changed as well – mandatory field

category - To categorize the network in e.g. production, pre-production, development – mandatory field

root network – check this box if the new network should be a root network

include network within automatic update – To include the network within the automatic update - only available for *endnets* - optional field.

Click on the “calculate” link to check whether network and bitmask are correctly.

3.2.1.2 Create multiple networks with same bitmasks

With the *create multiple networks* form it is possible to create up to 50 consecutive new networks in one step. Enter the network ID (e.g. 172.16.0.0), choose a bitmask and choose the number of networks to create.

create multiple networks with same BMs

☒ IPv4
 ☐ IPv6

Root networks ☐

first new network*
 (e.g. 192.168.0.0)

BM* calculate

number of networks*

Site*

category*

include networks within automatic update ☐

add

Fig. 18: "new network" form – create multiple networks with same BMs

3.2.1.3 Create multiple networks with different bitmasks

With this form you can create multiple networks with different bitmasks. Introduce the bitmasks in the following format: /BM1/BM2[/BMn].

create multiple networks with different BMs

☒ IPv4 ☐ IPv6

Root networks ☐

first new network*
(e.g. 192.168.0.0)

bitmasks*
(format: /BM1/BM2[/BMn] - e.g. /25/26/26) calculate

Site*

category*

include networks within automatic update ☐

add

Fig. 19: "new network" form – create new networks with different BMs

Example

To create networks 4.4.1.0/25, 4.4.1.128/27, 4.4.1.160/27, 4.4.1.192/26 in one step, introduce the following values:

first network: 4.4.1.0

bitmasks: /25/27/27/26

Note

"show free ranges"- view offers the possibility to create new networks directly by clicking a free range.

3.2.2 Network actions

Clicking over the cog symbol opens the options menu for the networks.

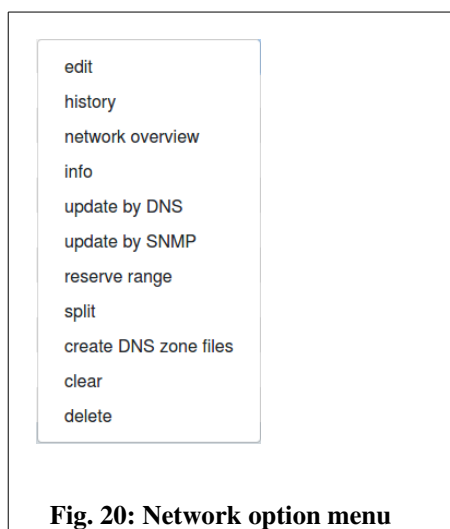


Fig. 20: Network option menu

edit – to edit the network parameters (see 3.2.2.1)

history – to show events in relation of this network (see 2.5).

network overview – to access to a overview of the free and used address of the network (see. 2.3.2).

info – subnet-calculator like information about the network.

update by DNS – to execute a DNS scan against this networks.

update by SNMP – to execute a SNMP scan against this network. This requires that you already have a SNMP Group defined.

reserved range – to reserve or delete reserved IP address ranges (see 3.2.2.2)

split – to split network into smaller subnets (see 3.2.2.5)

create DNS zone file – To create a Bind or Tinydns DNS zone files from the networks host information.

clear – delete all entries of the network (entries of reserved ranges will b maintained) (see 3.2.2.2)

delete – Delete network with all entries and reserved ranges (see 3.2.2.7)

3.2.2.1 Edit

The edit-network-form allows to edit all network attributes as well as to resize the Bitmask of the network. After editing the network attributes click “update” to save the changes.

The screenshot shows a web form for editing a network. The fields are as follows:

- network**: 192.168.1.0
- BM***: 24
- description***: descr
- Site***: Lon1 (dropdown menu)
- category***: corp (dropdown menu)
- comment**: comment (text area)
- sync**: ☐
- update**: button

Fig. 21: "edit network" form with enabled custom column "VLANs"

3.2.2.2 Reserved ranges

GestióIP offers the possibility to reserve ranges for special usage (e.g. for DHCP). This option is only for IPv4 networks available.

Creating a reserved range, GestióIP adds a comment to the corresponding network and to the hosts that are included in the range. The host type of the IP addresses of the reserved range is predetermined (but changeable). This means that automatic update sets host type automatically when creating new host entries within reserved ranges (e.g. range type: “workst (DHCP) => host type: “workst”).

Click “networks” -> “change/delete” -> “ranges”  to access range manipulation form.

Note

Host overview shows IP addresses of reserved ranges with a gray background.

Insert ranges

Mark the first and the last IP address of the range you want to add, insert a short descriptive

comment and mark the “range type” (host types of the reserved range). Then click “add” to create the new range.

Reserve range

Please select the first and the last IP address of the range which should be reserved

First IP: 192.168.35.1, 192.168.35.2, 192.168.35.3, **192.168.35.4**, 192.168.35.5

Last IP: 192.168.35.250, 192.168.35.251, 192.168.35.252, 192.168.35.253, **192.168.35.254**

Comment: SSID abcd

Range type: workst (DHCP), **wifi (DHCP)**, VoIP (DHCP)

Fig. 22: "new range" form

Note

If you set configuration parameter “dyn_ranges_only” to “yes” (see Error: Reference source not found), automatic update will only process entries of reserved ranges.

Note

When creating a reserved range, all entries between "First IP" and "Last IP" will be deleted.

Delete ranges

To delete a reserved range access to the range manipulation form, choose the range you want to delete and press "delete" button. This will delete the range with all of its entries from GestioIP's database.

Delete range

Please select a range to delete


192.168.35.4-192.168.35.254 (SSID abcd) ▼

Fig. 23: "delete range" form

Note

When splitting networks with reserved ranges, the ranges and all of their entries will be dropped.

3.2.2.3 Manual update against DNS

The function "sync"  (network synchronization against DNS) is intended to update all IP addresses of a network with the actual DNS entries. The network synchronization executes an ICMP echo request (ping) to all IP addresses and an rDNS query of all IP addresses of the network. The decision if and how an entry is updated follows the following scheme:

<i>Answers to ping?</i>	<i>rDNS entry configured?</i>	<i>Match ignore or ignore_generic_auto?</i>	<i>Update?</i>	<i>Hostname set to</i>
Yes	Yes	Yes	Yes	unknown
Yes	Yes	No	Yes	rDNS name
Yes	No	-	Yes	unknown
No	Yes	Yes	No	-
No	Yes	No	Yes	rDNS name
No	No	-	No	-

Note

Update type "ocs" or "man" avoids that manual synchronization updates these entries (see 3.1.1).

Note

To prevent that the networks being filled with generic rDNS entries read 3.2.2.3.1.

3.2.2.3.1 Generic rDNS entries

Generic rDNS (PTR) entries are often used in relation with dynamic assigned IP addresses or to prevent network reverse discovery. With configured rDNS entries you will get a valid answer to rDNS queries for all addresses of a network (but without useful information content). Generic rDNS entries may look like this:

```
1-2-4-5.domain.org
2-2-4-5.domain.org
3-2-4-5.domain.org
```

....

GestióIP's update functions (AUTO and MAN) update unassigned addresses when they receive a valid answer to an rDNS query. This causes the database to be filled with (undesired) rDNS entries. GestióIP offers two mechanisms to prevent the update from actualizing the network with generic rDNS entries (like 10-2-4-5.domain.org):

ignore generic auto: Set this value to "yes" if the update script should ignore DNS entries that match “auto generated generic rDNS strings” and that does not respond to “ping”.

Example:

<i>IP address</i>	<i>auto generated generic rDNS string (generated by GestióIP)</i>
192.168.200.8	<i>192-168-200</i> <i>200-168-192</i> 168-200-8 8-200-192

With ***ignore generic auto*** set to "yes" the “auto generated generic rDNS string” matches if your rDNS entries look like

192-168-200-15.some_string or *15-200-168-192.abc.de.fg*

IP addresses with rDNS entries that match “auto generated generic rDNS strings” but don’t answer to “ping” will be ignored. If the address answers to “ping” and matches “auto generated generic rDNS strings”, the hostname is set to “unknown”.

ignore: If you use a scheme for rDNS entries other than the schemes supported by GestióIP, the strings to be ignored can be set here manually. The field accepts a single string or a comma-separated list of strings to ignore.

Example:

To avoid that a network is filled with generic PTR entries like 10.200.168.192.domain.org and 55.0.16.172.domain.org set the "ignore" variable to:


200.168.192,0.16.172

Make sure that the string to ignore is specific for your rDNS entries. If you set ignore in the example above to "domain", the generic rDNS entries will be ignored but entries such as "host.domain.org" ("good entries") will be ignored as well.

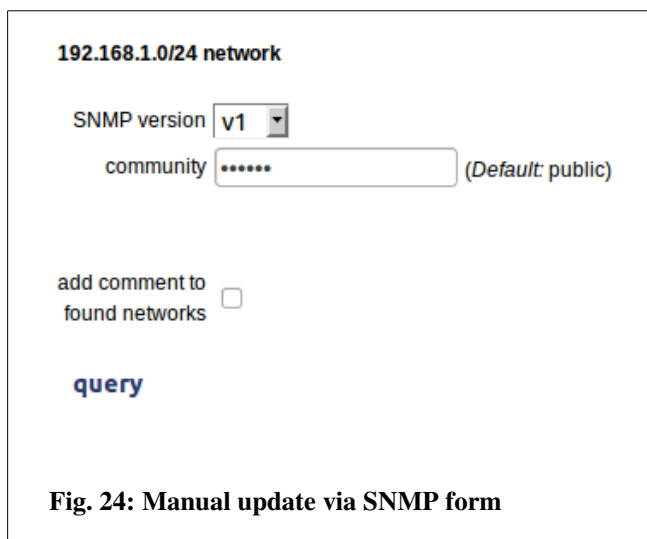
Note

Configure ignore and ignore generic auto global configuration parameters from manage GestióIP form (see 4).

3.2.2.4 Manual host update via SNMP

The *manual host update via SNMP* offers the option to update the host entries of a network by querying all IPs via SNMP. Click  to access to manual update form.

Manual update via SNMP will try to connect to every IP address of the network and actualize host information with found values.



The form is titled "192.168.1.0/24 network". It contains the following elements:

- SNMP version:** A dropdown menu currently set to "v1".
- community:** A text input field containing "*****" with a "(Default: public)" label to its right.
- add comment to found networks:** A checkbox that is currently unchecked.
- query:** A blue button to initiate the update process.

Fig. 24: Manual update via SNMP form

Insert a community name (SNMPv1/2c) or a username (SNMPv3), choose SNMP version and click “discover” to start the update process.

Note

Execution of manual host update via SNMP may take some minutes.

Note


Host update via SNMP actualizes predefined host columns, too (see 3.12).

Note

GestióIP currently supports only SNMPv3 with the Security Level 'noAuthNoPriv'.

3.2.2.5 Split

The split network form offers the possibility to split a network either into smaller networks with the same bitmasks or into smaller networks with different bitmasks.

Click “networks” -> “change/delete” -> "split"  to access the “split network” form.

Split network into smaller networks with same bitmasks

BM

☐ keep site ☐ keep category

Split network into smaller networks with different bitmasks

bitmasks

☐ keep site ☐ keep category

Wrong "bitmasks" format

Please introduce the bitmasks of the new subnets using the following format: **/BM1/BM2[/BMn]**

Example network 192.168.0.0:

bitmasks **/24/25/25** -> 192.168.0.0/24, 192.168.1.0/25, 192.168.1.128/25

bitmasks **/26/27/27/25** -> 192.168.0.0/26, 192.168.0.64/27, 192.168.0.96/27, 192.168.0.128/25

Fig. 25: "split network" form

To split networks into smaller networks with the same bitmask select the new bitmask and click “send”.

To split networks into smaller networks with different bitmasks insert a “/” (slash)-separated list of the bitmasks of the new subnets in the “bitmasks” field (/bitmask1/bitmask2[/bitmaskN]) and click “send”.

Example

*If you want to split network 172.16.5.0/24 into the networks
172.16.5.0/25
172.16.5.128/26
172.16.5.192/26
introduce /25/26/26 into the “bitmasks” field.*

When the "bitmasks" are correctly introduced, a list of the new subnets is shown. If the list is correct, introduce description; choose sites and categories for the new networks and press "send" to split the original network into the new subnets. If the bitmasks are incorrectly introduced, a detailed error notification will be displayed.

192.168.220.0/24 - /25/25

The network will be split into the following subnets

192.168.220.0/25
192.168.220.128/25

If correct edit the parameters of the new networks and press "split"

network	description	site	category	comment	sync
192.168.220.0/25	<input type="text"/>	Lond I ▾	Pre ▾	<input type="text"/>	<input type="checkbox"/>
192.168.220.128/25	<input type="text"/>	Lond I ▾	Pre ▾	<input type="text"/>	<input type="checkbox"/>

☐ keep host entries

(reserved ranges will be dropped)


Fig. 26: Confirm split network

If the new networks don't include the entire original network, a warning will be displayed. By clicking "send" the new networks will be created and the hosts of the original network that are not included within the new ranges will be dropped.


Note

Splitting a network causes all reserved ranges of this network to be dropped.

3.2.2.6 Clear

Click "networks" -> "change/delete" -> "clear"  to delete all entries of a network.

3.2.2.7 Delete

Click "networks" -> "change/delete" -> "delete"  to delete the network with all of its entries and reserved ranges from GestióIP's database.

3.2.2.8 Network mass update

Networks mass update feature offers the possibility to perform actions on multiple network entries

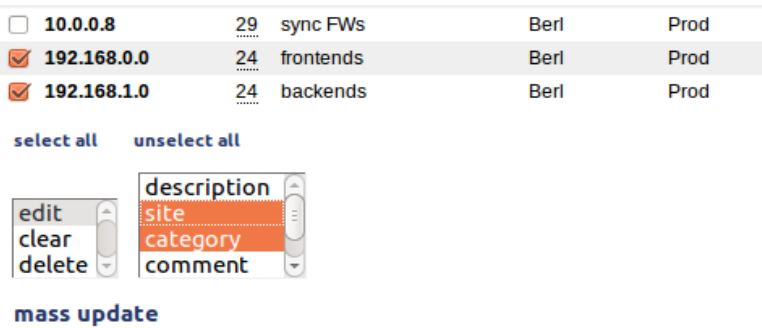
at once.

It allows to edit one or multiple network column entries, to clear networks (delete all host entries) and to delete multiple networks.

Go to “network” → “change/delete” to access to network mass update form.

3.2.2.8.1 Edit multiple network entries

To edit multiple networks mark the checkbox in front of the networks to edit, select “edit” from action select box, select the columns to edit and press “mass update”.



The screenshot shows a table with the following data:

Network	Count	Description	Site	Category
<input type="checkbox"/> 10.0.0.8	29	sync FWs	Berl	Prod
<input checked="" type="checkbox"/> 192.168.0.0	24	frontends	Berl	Prod
<input checked="" type="checkbox"/> 192.168.1.0	24	backends	Berl	Prod

Below the table are buttons for "select all" and "unselect all".

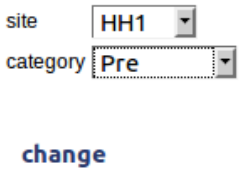
There is a selection interface with a list of actions: "edit", "clear", and "delete". The "edit" action is selected.

Below the actions is a list of columns to edit: "description", "site", "category", and "comment". The "category" column is highlighted in orange.

At the bottom is a "mass update" button.

Fig. 27: Network mass update

Edit/select the new values and press “change” to save them to the database.



The screenshot shows the edit form with the following fields:

- site: HH1
- category: Pre

Below the fields is a "change" button.

Fig. 28: Network mass update edit form

3.2.2.8.2 Clear multiple networks

To delete the host entries of multiple networks mark the checkbox in front of the corresponding networks, select action type “clear” and press “change”.

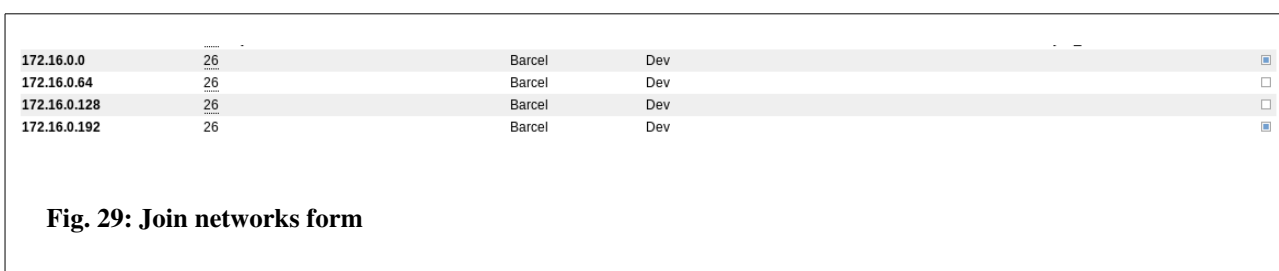
3.2.2.8.3 Delete multiple network entries

To delete multiple networks and all of their host entries mark the checkbox in front of the corresponding networks, select action type “delete” and press “change”.

3.2.3 Join networks

To join networks click “networks” -> “change/delete” -> "join" on the menu bar.

Mark two networks that you wish to join and press ENTER or click "join" at the bottom of the page.

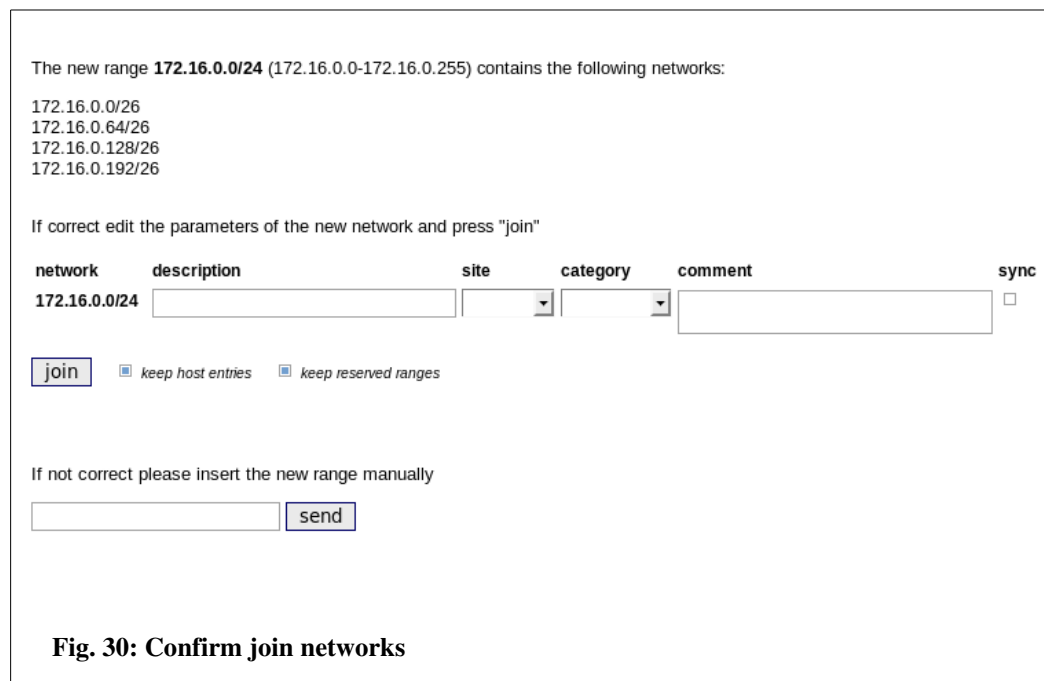


172.16.0.0	26	Barcel	Dev	<input checked="" type="checkbox"/>
172.16.0.64	26	Barcel	Dev	<input type="checkbox"/>
172.16.0.128	26	Barcel	Dev	<input type="checkbox"/>
172.16.0.192	26	Barcel	Dev	<input checked="" type="checkbox"/>

Fig. 29: Join networks form

The networks do not need to be consecutive. GestióIP suggests one way to join the networks. The suggestion can be accepted or the new network can be introduced manually. In case it is not possible to join the networks directly, GestióIP offers the possibility to introduce the new network manually.

Format of network for manual introduction: network/bitmask e.g. 192.168.0.0/24



The new range **172.16.0.0/24** (172.16.0.0-172.16.0.255) contains the following networks:

- 172.16.0.0/26
- 172.16.0.64/26
- 172.16.0.128/26
- 172.16.0.192/26

If correct edit the parameters of the new network and press "join"

network	description	site	category	comment	sync
172.16.0.0/24	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

☒ join ☐ keep host entries ☐ keep reserved ranges

If not correct please insert the new range manually

Fig. 30: Confirm join networks

3.2.4 Show free ranges

For an overview of the unused spaces between the existing networks click “networks” -> "show free ranges" on the menu bar. Click on the unused space to create one or multiple networks directly from the unused space.

network	BM	description	site	category	comment	sync	vlan	SNMPGroup	DNSZone	Tag	DNSSG	test_sel	VRF	nutzer_org
10.0.0.0	8	priv II	BCN	corp										
10.0.0.0-10.0.0.255 (256 free addresses)														
10.0.1.0	29	sync FWs	Lon1	prod	not routed									
10.0.1.8	29	sync LBs	Lon1	prod	not routed									
10.0.1.16-10.255.255.255 (16776944 free addresses)														
192.168.0.0	16	priv range I	eee	prod										
192.168.0.0	24	frontends	Lon1	prod										
192.168.1.0	25	backends	Lon1	prod										
192.168.1.128	25	frontends II	Lon1	prod	new frontends									
192.168.2.0	24	application server	Lon1	prod										
192.168.3.0	24	Vips-int	Lon1	prod	vips LB1									
192.168.4.0	24	management	Lon1	prod										
192.168.5.0	26		Lon1	prod										
192.168.5.64-192.168.7.255 (704 free addresses)														
192.168.8.0	24	backup	Lon1	prod										
192.168.9.0-192.168.29.255 (5276 free addresses)														

Fig. 31: Free ranges

3.2.5 Subnet calculator

GestióIP's subnet calculator supports both classful and classless networks.

Click “networks” -> "subnet calculator" on the menu bar to open the subnet calculator window.

[illegible]

Fig. 32: Integrated subnet calculator

Note

The subnet calculator accepts IPs in integer format, too.

Note

The subnet calculator is also available as online version: http://www.gestioip.net/cgi-bin/subnet_calculator.cgi

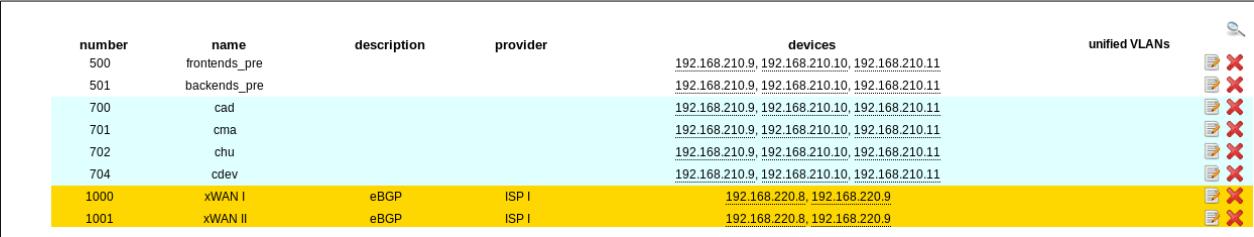
3.3 VLANs

GestióIP incorporates an automated VLAN management system integrating the possibility to import VLANs easily from network devices via SNMP.

The predefined network column “VLANs” is aimed to associate VLANs to specific networks. With configured VLAN column, VLAN information will be shown within *network list view* (see 3.12).

3.3.1 show, edit, delete

Access to *VLAN list view* ("VLANs" -> "show") to show, edit or delete VLANs.




















number	name	description	provider	devices	unified VLANs
500	frontends_pre			192.168.210.9, 192.168.210.10, 192.168.210.11	 
501	backends_pre			192.168.210.9, 192.168.210.10, 192.168.210.11	 
700	cad			192.168.210.9, 192.168.210.10, 192.168.210.11	 
701	cma			192.168.210.9, 192.168.210.10, 192.168.210.11	 
702	chu			192.168.210.9, 192.168.210.10, 192.168.210.11	 
704	cdev			192.168.210.9, 192.168.210.10, 192.168.210.11	 
1000	xWAN I	eBGP	ISP I	192.168.220.8, 192.168.220.9	 
1001	xWAN II	eBGP	ISP I	192.168.220.8, 192.168.220.9	 

Fig. 33: Show VLANs

Click over the -symbol to open the VLAN search form.

VLAN list view features the following columns

number - VLAN number (mandatory).

name - VLAN name (mandatory).

description - A description for the VLAN (optional).

provider - There might be VLANs with different Internet Service Providers (ISPs) contracted. This column allows to specify an Internet Service Provider (optional).

devices - This column lists the network devices where the VLAN was found by *VLAN discovery*. Hovering over the IP address displays the device name. This field can not be edited manually.

unified VLANs - To associate same VLANs which appears in different devices with different names (e.g. VLAN 1 may have the name "default" on one and "default_vlan" on another device) (see 3.3.3).

3.3.2 New

Click over "VLANs" -> "new" to introduce new VLANs manually.

number

name

comment

provider

bg font

add

Fig. 34: "New VLAN" form

3.3.3 Unify

Unify VLANs is aimed to associate same VLANs which appear in different devices with different names, so that they appear like one VLAN in GestióIP's database.

Because VLAN name is configured manually by network administrators, same VLANs may appear in different devices with different names (e.g. VLAN 1 may have the name "default" on one and "default_vlan" on another device). Automatic VLAN importation will import that kind of VLANs like different VLANs. That causes that this VLANs will appear like two VLANs in *VLAN list view*. With *unify* option it's possible to associate this VLANs so that they appear like one VLAN in GestióIP's *VLAN list view*.

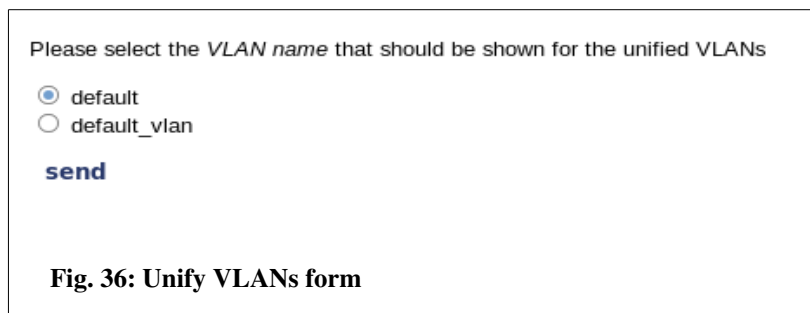
Click "VLANs" -> "unify" to access *VLAN unify form*. There appear only VLANs with same number but different names. Mark two or more VLANs with same numbers that should be unified and click "unify" at the bottom of the VLAN list.

	number	name	description	provider	devices
<input type="checkbox"/>	1	default_vlan			192.168.210.9, 192.168.210.11
<input type="checkbox"/>	1	default			192.168.210.9, 192.168.210.10, 192.168.210.11

unify

Fig. 35: Unify VLANs form

Select the name that should appear for the unified VLAN and click "send" to unify the VLANs.



Please select the *VLAN name* that should be shown for the unified VLANs

☒ default
☐ default_vlan

send

Fig. 36: Unify VLANs form

3.3.4 VLAN provider

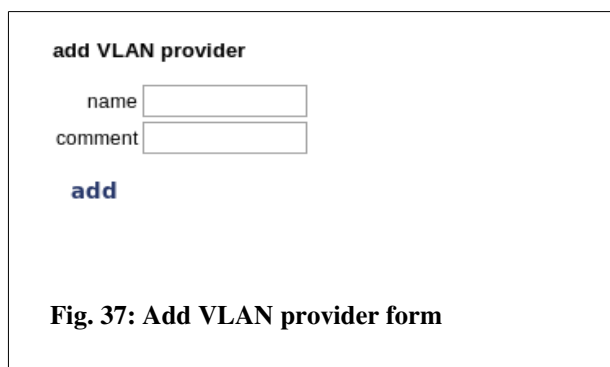
An organization may have VLANs with ISPs contracted. Option *VLAN provider* is intended to associate this VLANs with an ISP.

3.3.4.1 Show VLAN provider

Click "VLANs" -> "show VLAN providers" to list, edit or delete VLAN providers.

3.3.4.2 New VLAN provider

Click "VLANs" -> "new VLAN providers" to access *new VLAN provider* form



add VLAN provider

name

comment

add

Fig. 37: Add VLAN provider form

To add a new provider introduce a name and an optional comment and click "add".

3.3.5 Import VLANs via SNMP

Click “import/export” -> “import VLANs via SNMP” to access to VLAN importation form.

node ☒ (IP address)

Layer II devices ☐ 192.168.0.2 - switch1
192.168.0.3 - switch2

Layer III devices ☐ No Layer III devices defined

community/username (Default: public)

SNMPv1 ☒
SNMPv2c ☐
SNMPv3 ☐

query

Fig. 38: Import VLANs form

Import VLANs function can be lanced against one device by introducing an IP Address (text-filed “node”) or against multiple devices which are classified like “L2 device” or “L3 device” by making them in the “Layer II devices” or “Layer III devices” select-box.

Note

If there are no devices classified with host type L2 or L3 device, there appears the note "No layer II/III devices defined". To change the host type of a device go to "show networks", access to the corresponding network and click device "edit host" button.

Note

Column "switches" of VLAN overview will only be updated if discovery is lanced against a device from Layer II or Layer III devices select box.

Note

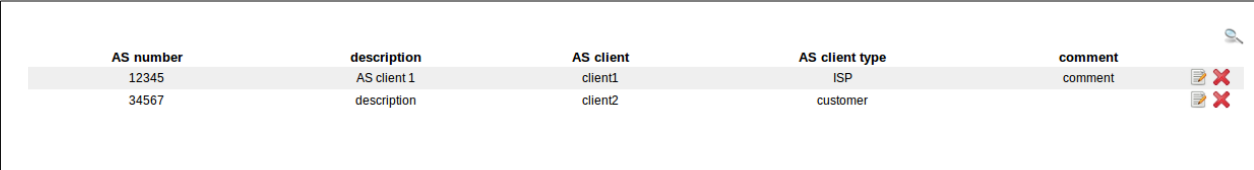
VLAN discovery is base on the Perl Module SNMP::Info (see Error: Reference source not found). VLAN discovery works only with devices supported by SNMP::Info. Consult the device compatibility matrix to verify if your devices are supported (<http://netdisco.org/DeviceMatrix.html>). If the device is not supported or if it is not possible to connect to the device, GestióIP will display the message “CAN NOT CONNECT”.

3.4 Autonomous system management

GestióIP features a simple management system for autonomous systems. To use this feature you need to enable “autonomous system support” from “manage”->”gestioip” (see 4.1). This feature is thought to be use by Internet service providers (ISP).


3.4.1 show, edit, delete

Access to *autonomous systems list view* to show, edit or delete AS ("AS" -> "show").



AS number	description	AS client	AS client type	comment
12345	AS client 1	client1	ISP	
34567	description	client2	customer	

Fig. 39: “Autonomous system list view ”

Click over the -symbol to open the AS search form.


AS number - AS number (mandatory).

description - A description for the AS (optional).

AS client – The client to which the AS is assigned to (optional).

AS client type – The type of client to which the AS is assigned to (optional).

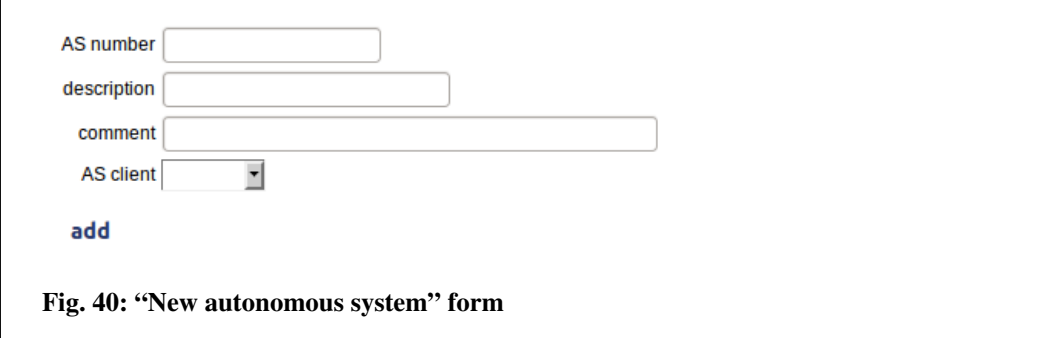
comment – A optional comment.

Click  to edit the AS

Click  to delete the AS from GestióIP's database

3.4.2 new

Click over "AS" -> "new" to introduce new AS manually.



AS number

description

comment

AS client

add

Fig. 40: “New autonomous system” form

3.4.3 show AS clients

Autonomous system clients allow to specify to which client an autonomous system is assigned to. Access to *AS client list view* to show, edit or delete AS clients.

3.4.4 new AS client

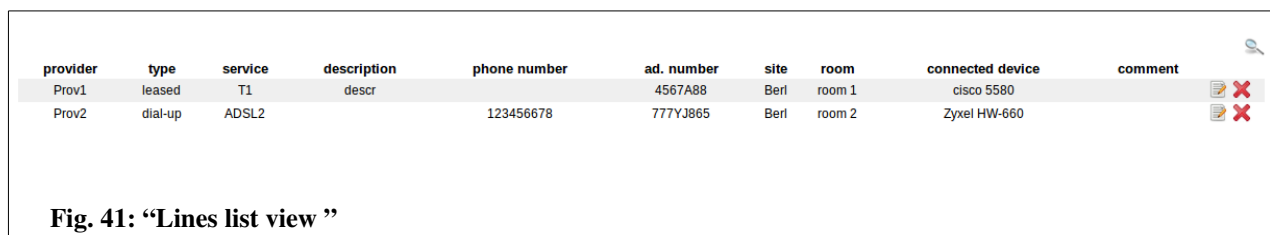
To introduce a new AS client click over “AS” → “new AS client”.

3.5 Line management

GestióIP features a management system for leased and dial-up lines. To use this feature you need to enable “line support” from “manage”->”gestioip” (see 3.5)

3.5.1 show, edit, delete

Access to *least line list view* to show, edit or delete the leased lines ("lines" -> "show").








provider	type	service	description	phone number	ad. number	site	room	connected device	comment
Prov1	leased	T1	descr		4567A88	Berl	room 1	cisco 5580	 
Prov2	dial-up	ADSL2		123456678	777YJ865	Berl	room 2	Zyxel HW-660	 

Fig. 41: “Lines list view ”

Click over the  -symbol to open the AS search form.

provider – ISP from which the line is contracted

type - type of the dial-up line (e.g. leased or dial-up)

service – service (e.g T1,T3,... for leased or ADSL, SDSL, ISDN, ... for dial-up)

description – an optional description

phone number – phone number provided by the IPS (for dial-up lines)

ad number – Administrativ number assigned by the ISP

site – the site where dial-up line ends

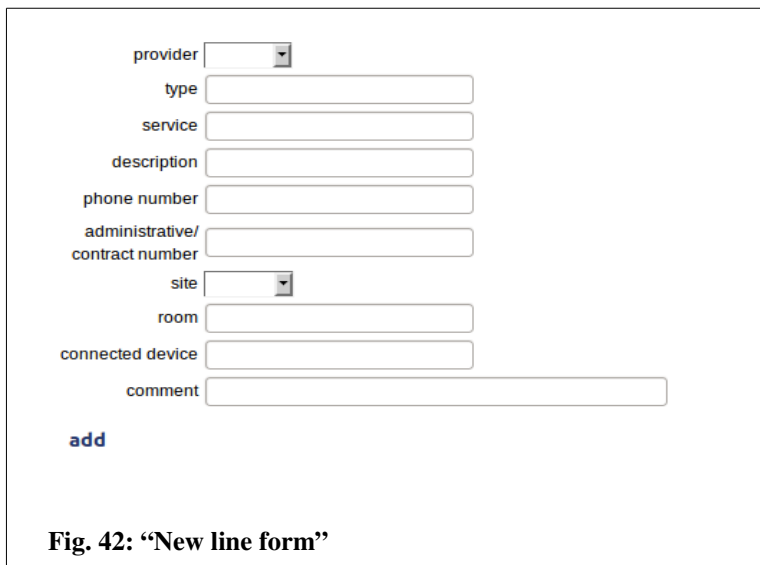
room – the room where the dial-up line ends

connected device – device which is connected to the leased line (e.g. manufacturer, model)

comment – any kind of comments

3.5.2 new

Click over "lines" -> "new" to introduce new leased or dial-up lines manually.



provider

type

service

description

phone number

administrative/
contract number

site

room

connected device

comment

add

Fig. 42: "New line form"

3.5.3 show line provider

Line provider allow to specify from which provider a leased or dial-up line is contracted.

3.5.4 new line provider

To introduce a new line provider click over "line" → "new line client".

3.6 MAC management

The MAC management feature allows to manage an external database with MAC information. This database can be the MySQL database of the GestióIP itself or a remote MySQL database. A MAC database can be for example used as backend by a RADIUS server for MAC based authentication.

This feature is disabled by default. To enable it access to "manage" > "manage GestióIP" and set "MAC management enabled" to "yes" (see 3.5).

Configure the database parameter for the database which stores the MAC information in the configuration file `/usr/share/gestioip/etc/ip_update_gestioip.conf`. Open it with an editor and configure the following values:

```

sid_mac=mac_auth
user_mac=mac_admin
pass_mac=XXXXX
bbdd_host_mac=192.168.100.10
bbdd_port_mac=3306
table_name_mac=allowed_macs
column_name_mac=mac

```

In this example, server which runs the MAC database has the IP address 192.168.100.10, the database is called “mac_auth” and the table with the stored MAC addresses is called “allowed_macs” and looks like this:

```

mysql> use mac_auth;
Database changed
mysql> desc allowed_macs;
+-----+-----+-----+-----+-----+-----+
| Field | Type          | Null | Key | Default | Extra          |
+-----+-----+-----+-----+-----+-----+
| id    | mediumint(6) | NO   | PRI | NULL    | auto_increment |
| mac   | varchar(18)   | YES  |     | NULL    |                |
+-----+-----+-----+-----+-----+-----+
2 rows in set (0,00 sec)

```

3.6.1 show, edit, delete

Access to *MAC list view* to show, edit or delete MAC entries (“manage” > “MACs”).

3.6.2 Add

Access to *MAC list view* (“manage” > “MACs”) and click over “add MAC”.

3.7 Clients

GestioIP permits to manage different clients with independent networks and VLANs. If there is more than one client defined, there appears a new select box in the menu bar indicating the actual client.

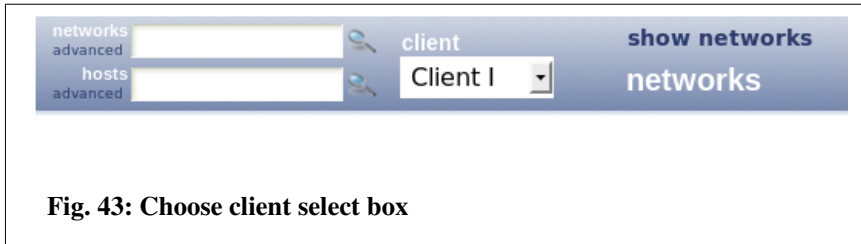


Fig. 43: Choose client select box


To change actual client choose the new client from *client select box* and click refresh  button



Fig. 44: Change actual client refresh button

Note

Client option can be also used to sub-divide a complex network infrastructure into sections. You may create "clients" like "off-range" for your official networks, "priv-range" for your private networks,... In the case you that discover a infrastructure that is sub-divide into sections via the "client" option, the network devices may hold official and private networks in it's routing tables. That means that you need to specify the networks which should be imported to make sure, that only the networks for this "client" will be imported. Specify the first octets of the Networks which should be imported for this "client" with the option "Process only IPv4/6 networks beginning with" within the import forms ("discovery" (see 7.1)), "import networks via SNMP" (see 7.2.1) and script "get_networks_snmp.pl" (see Error: Reference source not found)).

3.7.1 Manage clients

Manage clients form offers the following options:

- list client details

- add clients
- edit clients
- delete clients

Click "manage" -> "clients" to access to *manage clients form*.

3.7.1.1 Add clients


When creating the first client, all existing networks, VLANs and sites will be associated with this client. Because sites are managed client independently you have to insert at least one site for every new client (text field "sites") . Multiple sites must be introduced in form of a comma separated list.

Note

You can change sites from "manage" -> "sites and categories".

To add the new client complete *add client form* and click "add". The new client will now appear in client select box in the menu.

3.7.1.2 Edit clients

Click "manage" -> "clients" to access to *edit client form*. Choose the client you want to edit and click edit button .



Click

"update" at the bottom of the *edit client form* to save the changes.

3.7.1.3 Delete clients

To delete a client choose the client to delete from *delete client form* and click "delete".



The screenshot shows a web form titled "delete client". It contains a dropdown menu with the text "Client I" and a blue button labeled "delete".

Fig. 46: Delete clients form

Deleting a client causes that all information specific to this client will be deleted (networks, hosts, sites, audit events).

3.8 Sites and categories

To introduce, rename or delete *sites*, *host categories* or *network categories*, open "manage" -> "sites and categories" on the menu bar.

3.8.1 Sites

GestioIP's *sites* are intended to associate a physical location (e.g. a data center) within the networks and hosts.

Note

Sites for network and host are independently configurable. If you have networks that are distributed over different sites (e.g. A and B) you can create an additional site A_B, assign this new site to the

network and assign site A or B individually to the hosts.

Note

With multiple clients configured there will only the sites of the actual client be displayed.

3.8.2 Network categories

During installation GestióIP proposes the following networks categories:

Prod – For networks of the production environment

Pre – For networks of pre-production environment

Test – For networks of test environment

Dev – For networks of development environment










Dev-test – For networks of development-test environment

Corp – For corporate networks (e.g. with PC of end-users, printers,...)

other – For all other networks

3.8.3 Host categories

GestióIP comes with the following *host categories*:

	L2 device	devices that work in layer 2 (e.g. hubs or switches)
	L3 device	devices that work in layer 3 (e.g. multilayer-switches or router)
	FW	firewalls
	DB	for database servers
	server	any kind of server
	workstation	workstations
	wifi	wireless devices
	VoIP	VoIP phones
	printer	printers

	other	all other types of devices
---	-------	----------------------------

Note

Self defined host categories appear in network overview with the "other" - symbol.

Note

Default host categories can't be deleted nor renamed.

3.9 Tags

GestióIP allows to assign Tags to networks and hosts. Tags can be used to execute the automatic update functions against a group of tagged networks or host or to find a group of tagged objects easily via the quick-search function.

To use Tags, enable the predefined column “Tag” for networks and/or hosts first (“manage” > “custom columns”, see 3.12).

Tags are assigned via the network and the host-edit-forms. Once the column “Tag” is enabled, there will appear a new drop-down menu in the edit-forms.

3.9.1 Show, edit, delete

Access to *Tag list view* ("manage" > “Tags”) to show, create, edit or delete Tags.

3.9.2 Add

Access to *Tag list view* ("manage" > “Tags”) and click over “add tag”.

3.10 SNMP Groups

SNMP Groups define different SNMP authentication methods and options. SNMP Groups can be assigned to networks and hosts. They will be used by the automatic host and network discovery mechanisms.

To use SNMP Groups, enable the predefined column “SNMPGroup” for networks and/or hosts

(“manage” > “custom columns”, see 3.12).

SNMP Groups can be assigned via the network and the host-edit-forms. Once the column “SNMPGroups” is enabled, there will appear a new drop-down menu in the edit-forms.

3.10.1 Show, edit, delete

Access to *SNMP Group list view* (“manage” > “SNMP Groups”) to show, create, edit or delete SNMP Groups.

3.10.2 Add

Access to *SNMP Group list view* (“manage” > “SNMP Groups”) and click over “add SNMP Groups”.

3.11 DNS Server Groups

DNS Server Groups allow to create a group of up to three DNS servers. DNS Server Groups can be assigned to networks. They are used by the automatic host and network discovery mechanisms. An assigned DNS Server Group will overwrite the “client specific configuration parameters” for the “DNS Server” (see 4.2.2).

To use DNS Server Groups, enable the predefined column “DNSSG” for networks and/or hosts (“manage” > “custom columns”, see 3.12).

DNS Server Groups can be assigned via the network and the host-edit-forms. Once the column “DNSSG” is enabled, there will appear a new drop-down menu in the edit-forms.

3.11.1 Show, edit, delete

Access to *DNS Server Group list view* (“manage” > “DNS Server Groups”) to show, create, edit or delete DNS Server Groups.

3.11.2 Add

Access to *DNS Server Groups list view* ("manage" > "DNS Server Groups") and click over "add DNS Server Group".

3.12 Custom columns

GestióIP offers the possibility to define custom columns to be shown in *network*, *host*, *site* or *line list-views*, making it adaptable to organization specific needs.

IP	hostname	description	site	type	AI	comment	vendor	model	OS
192.168.0.1	firewall		BCN II	FW					h x
192.168.0.2	switch1		BCN II	L2 device				C2H124x48	h x
192.168.0.3	switch2		BCN II	L2 device				2950t24	h x
192.168.0.4			BCN II						h x
192.168.0.5	server1		BCN II	server					h x

Fig. 47: Network list view with predefined host columns updated by SNMP discovery

Click *manage* > *custom columns* to define new or to delete columns for networks and hosts.

GestióIP features two types of custom columns: predefined and self defined columns. Predefined host columns will be updated by SNMP discovery mechanisms, self defined columns not.

Custom columns can be defined as text field or as select-box.

Custom column fields can be defined as mandatory or not mandatory fields.

3.12.1 Predefined custom host columns

Predefined custom host columns will be processed by SNMP based discovery mechanisms. For this reason it's preferable to use predefined columns if available instead of self defined columns.

GestióIP offers the following predefined host columns:

vendor - manufacturer (will be displayed with an icon). GestióIP distinguishes actually between more than 140 manufactures (vendors) which will automatically be recognized by SNMP discovery

functions (see Appendix A for a complete list of the manufacturers)

model - model

contact - contact (OID system.sysContact)

serial - serial number

MAC - MAC address

OS - operating system (will be displayed with an icon). GestióIP distinguishes actually between 22 operating systems which will automatically be recognized by SNMP discover functions (see Appendix A for a complete list of the operating systems)

device_descr - description (OID system.sysDescr.)

device_name - hostname (OID system.sysName)

device_loc - location (OID system.sysLocation)

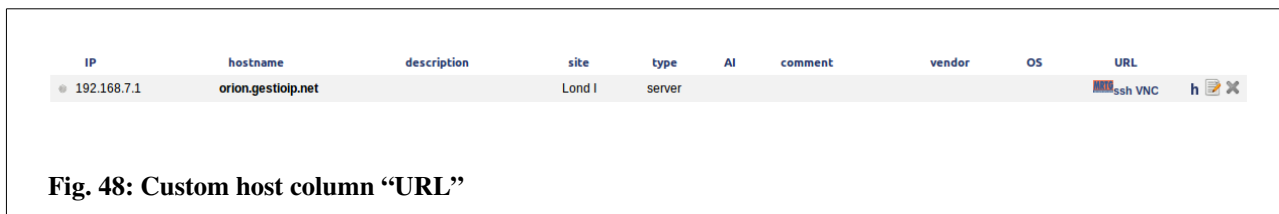
URL – external link (will be displayed with an icon). This column allows to configure links to external web pages as well as to open remote sessions against the host (e.g. ssh, telnet, rdesktop (rdp), vnc, ...). Specify the link in the following format: SERVICE::URL[,SERVICE1::URL1]

Example:

With the following URL entry

`mrtg::http://mrtg_server/mrtg/server_192.168.7.1.rrd,ssh::ssh//192.168.7.1,VNC::vnc://192.168.7.1`

URL-column will displayed as shown in Fig. 48



Custom column “URL” allows to use variables (actually two variables). This is useful in conjunction with *mass update feature* (see 3.2.2.8) which gives the possibility to edit multiple hosts at once.

Variable	Replaced by
[[IP]]	IP address of the host
[[HOSTNAME]]	“hostname” entry of the host

Example:

Entry: 192.168.0.10 jupiter description Lond I ...

Entry with variable	Displayed entry
---------------------	-----------------

telnet::telnet://[[IP]]	telnet::telnet://192.168.0.10
telnet::telnet://[[HOSTNAME]]	telnet::telnet://jupiter
telnet::telnet://[[HOSTNAME]].domain.org	telnet::telnet://jupiter.domain.org
mrtg::http://mrtg_server/mrtg/server_[[IP]].rrd	mrtg::http://mrtg_server/mrtg/server_192.168.0.10.rrd

Note

Not all browser support the format “service://...” for all services.

Note for Firefox users

*If you get the error message like “**Firefox doesn't know how to open this address, because the protocol (rdp) isn't associated with any program**” open a new Firefox window, type about:config into the URL-field, click right mouse button → add → new → Boolean, insert the value “network.protocol-handler.expose.rdp” → false.*

When clicking next time over the link, Firefox will ask with which application it should open the link.

Rack – identifier of the rack where the device is mounted physically

RU – rack unit where the device is mounted physically

switch – network node where the device is connected to. This columns might be processed in a futur version of GestióIP by network discovery

port – port of the network node where the device is connected to. This columns might be processed in a futur version of GestióIP by network discovery

linked IP – Allows to associate an IP with one IP or a list of other IP addresses (for example to associate an internal IP with it's VIP address). Configuring a *linked IP* for an IP will automatically create a *linked IP* entry for the associated IP, too.

Tag – Associated Tags

Note

Predefined as well as self defined custom columns will be processed by network and host quick search.

Note

Predefined network column "VLAN" and predefined host columns “MAC”, ” Rack”, ”switch” and “port” will not be updated by SNMP based discovery.

Note

If you have multiple clients defined there appears a radio button which let you choose to either add columns for all or only for the actual client.

3.12.2 Predefined custom network columns

GestióIP disposes about the following predefined custom network columns:

VLAN - VLAN column is aimed to associate VLANs with networks to be shown in network list view.

Fav – To mark networks as favorite networks. Activating the Fav column will add the favorite-button (★) to network-list-view to easily list the favorite networks.

VRF – To indicate the VRF name for networks within VRFs.

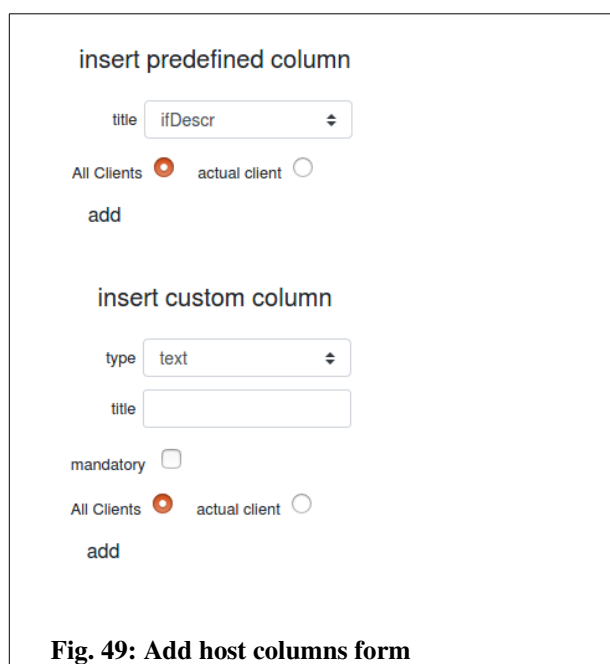
DNSZone – DNS zone (see 12.3.4)

DNSPTRZone - DNS PTR zone (see 12.3.4)

Tag – Associated Tags

3.12.3 Add columns

You can define new columns to be shown in network or host list view.



The screenshot shows a web form titled "Add host columns form". It contains two main sections:

- insert predefined column:**
 - A dropdown menu for "title" with "ifDescr" selected.
 - Two radio buttons: "All Clients" (selected) and "actual client".
 - An "add" button.
- insert custom column:**
 - A dropdown menu for "type" with "text" selected.
 - A text input field for "title".
 - A "mandatory" checkbox (unchecked).
 - Two radio buttons: "All Clients" (selected) and "actual client".
 - An "add" button.

Fig. 49: Add host columns form

Check if there is already a predefined column for the purpose you need available. Some predefined columns will be automatically updated by the network discovery via SNMP if the device supports the required OIDs (OS, vendor, MAC, device_*).

Choose if the column should either be shown for all or only for actual client and click “add”.

Custom columns can be defined to appear in the host-edit-form either as text field or as select-box

with predefined values.

To create a select field select the type “select” and add the items in form of a coma separated list.

The form is titled "insert custom column". It contains the following fields and controls:

- type:** A dropdown menu with "select" selected.
- title:** A text input field containing "my_col".
- items:** A text input field containing "itemA,itemB,itemC".
- mandatory:** An unchecked checkbox.
- Client selection:** Two radio buttons. "All Clients" is selected (indicated by a red dot), and "actual client" is unselected.
- add:** A button at the bottom.

Fig. 50: Custom column field as select-box

Note:

When editing the item list after creating the column you can only insert, delete or change one item per time. To change multiple items you need to do that one by one.

3.12.4 Edit columns

To edit the name or change if the field is mandatory or not use the “edit column” form.

The form is titled "edit column". It contains the following fields and controls:

- Name:** A dropdown menu with "RACK" selected.
- New name:** A text input field.
- mandatory:** An unchecked checkbox.
- update:** A button at the bottom.

Fig. 51: Edit columns form

To change the items of a column type “select” use the “edit select items” form.

It is only possible to insert, delete or change one item per time. To change multiple items you need to do that one by one. Change one item, save the change, then change the next, save and so on.

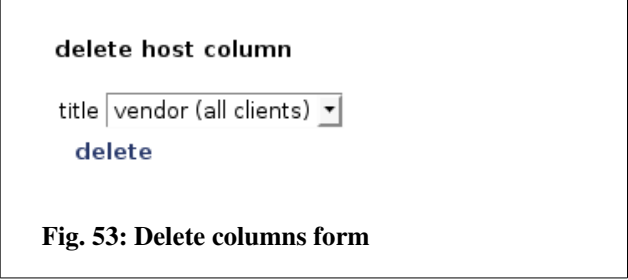
The form is titled "edit select items". It contains the following fields and controls:

- title:** A dropdown menu with "RACK (all clients)" selected.
- items:** A text input field containing "R1,R2,R3".
- update:** A button at the bottom.

Fig. 52: Edit columns form

3.12.5 Delete columns

Choose the column which should be deleted and click “delete”.



delete host column

title vendor (all clients) ▼

[delete](#)

Fig. 53: Delete columns form

Note

The “delete column form” will only be displayed if there are custom columns defined.

Note

Deleting a column causes that all entries of this column will be deleted from GestióIP's database.

4 Manage GestióIP (global configuration parameters)

GestióIP's configuration is divided in four sections:

- Client independent configuration parameters
- Client specific configuration parameters
- Delete audit events
- Reset database/delete networks

To configure global configuration parameters or to delete old audit events from the database click “manage” -> "manage GestióIP" from the menu bar.

4.1 Client independent configuration parameters

default client - Client to display when accessing to GestióIP.

IPv4 only mod - To enable IPv6 support set this parameter to “no”. With enabled IPv6 support there will appear new IPv6 related elements within many forms allowing e.g. to import/export, discover and manage IPv6 networks and hosts.

Autonomous system support – Set this parameter to “yes” to enable the autonomous system (AS) management system. With enabled AS support there appear a new item “AS” within the menu bar allowing to access to the AS relevant forms (see 3.4).

Lines support - Set this parameter to “yes” to enable the leased and dial-up line management system. With enabled line support there appear a new item “lines” within the menu bar allowing to access to the Least line management relevant forms (see 3.5).

ask for confirmation - If this parameter is set to “yes”, there will be a confirmation window display when executing “critical” actions like *clear network* or *delete network*.

MIB directory - Directory where Netdisco MIBs are stored (see Error: Reference source not found).

Vendor specific MIBs - Manufacturer specific directories. This parameter should be only be edited after updating to a newer version of Netdisco MIBs.

show only networks within rootnets (free-ranges-view): Set this option to “yes” to prevent that networks, which are not within the range of a rootnet, are shown in the free-ranges-view. Uncheck “collapse rootnets” in free-ranges view when using this option.

For information how to configure the “Network Configuration Backup and Management Module” have a look at it's user guide (http://www.gestioip.net/documentation_gestioip_en.html).

After changing the parameters click “set” to save the new values.

Configuration

default client **DEFAULT**

IPv4 only mode **yes** ▾

User management **yes** ▾

Autonomous System support **no** ▾

line support **no** ▾

ask for confirmation **yes** ▾

MIB directory

Vendor specific MIBs (Coma separated list)

show only networks within rootnets **yes** ▾
(free-ranges-view)

configuration management support **no** ▾

License Key

Configuration backup directory

Log directory

Device XML directory

Fig. 54: Client independent configuration parameters

Note

After enabling “AS” or “line” support by clicking “set”, the new menu elements “AS” (autonomous systems) and “lines” will not appear instantly. They will appear after clicking the next time over any link.

4.2 Client specific configuration parameters

With the client specific configuration parameters it's possible to influence GestióIP's comportment.

4.2.1 Smallest importable BM

smallest importable BM – IPv4 networks with a bitmask smaller than this parameter will not be imported.

Example

If GestióIP's SNMP based discovery mechanism imports the network 192.168.0.0/16 from a router, all other networks within this range (e.g. 192.168.0.0/24, 192.168.1.0/24, ...) which are found later would be ignored because they are “overlapping” with the network 192.168.0.0/16. To avoid that networks with a bitmask of /16 will be imported set this parameter to a value ≥ 17 .

Note

This parameter has changed from older version. In versions before GestióIP v3.0, networks with a bitmask $<$ the value of “smallest importable BM” were not presentable in the host views. GestióIP v3.0 has eliminated this limit and allows now to list IPv4 networks with any kind of bitmask.

Note

This parameter is not relevant for IPv6 discovery. All IPv6 networks with a prefix length smaller than 64 will be automatically classified as “root-network” and because of this, these networks will not cause “overlapping” errors.

4.2.1.1 Ping timeout

"ping" timeout – GestióIP works with Net::Ping::External Perl module. Because the module ignores timeout argument under Linux, host check and update against DNS work with the default timeout of 10s. Patch Net::Ping::External Perl module to make the functions which use "ping" faster (with a timeout of 2 seconds it would be 5x faster).

See http://www.gestioip.net/docu/Ping_External_Timeout_Problem.txt for instructions on how to patch it.

4.2.2 DNS server

To define the default DNS servers for the actual client. You can use DNS Server Groups (3.11) to assign specific DNS servers to specific networks.

use default resolver - Check this radio-button if DNS queries for this client should be lanced against the default DNS server (specified in /etc/resolv.conf) (default)

specify DNS server - Check this radio-button if DNS queries for this client should be lanced against custom DNS servers (*host check, update against DNS, update via SNMP*).

DNS server I-III - Specify here the DNS Server to query in the case that “specify DNS server”

radio button is checked.

Note

You can assign specific DNS servers to specific networks by using DNS Server Groups (see 3.11)

4.2.3 Manual update

The following parameters are related to manual update:

ignore - String that match generic rDNS entries in the case that your generic rDNS entries don't match "generic auto PTR entries" (see *ignore generic auto*). This option allows the update process to recognize generic rDNS entries. Example: rDNS entry: dhcp-2.3.5.2.gestioip.net -> *ignore*: dhcp-

ignore generic auto - Set this value to "yes" if the update script should ignore rDNS entries which follow the "generic-auto" scheme. Example: IP: 1.2.3.4 -> "generic auto" PTR entries generated by GestióIP: 4-3-2 and 2-3-4 (default: yes).

See 3.2.2.3.1 for more information about *ignore* and *ignore generic auto* variables

ignore DNS – With this option set to "yes" the update against DNS will use ping only to decide if a host should be added to the database. rDNS entries will be ignored.

generic-dynamic name - Set here generic names that match the hostnames associated by an DHCP server. If an IP address has an entry in the database that match generic-dynamic name and does not respond to "ping" it would be deleted. If you use both update against DNS and update against OCS Inventory NG, this parameter also avoids actualization created by update against OCS that match "*generic-dynamic name*" from being overwritten by update against DNS (in the case that synchronization against OCS's configuration value "set_update_type_to_ocs" is set to "no")

Example: If your dynamically assigned names look like PC-001, PC-002, LAP-001, LAP-002 set *generic-dynamic name* to "PC-,LAP-".

(coma separated list, case sensitive).

max number parallel processes - Maximum number of parallel processes to fork when updating networks (each process executes a "ping" to, and a DNS A and PTR query of one IP address). Increasing this value reduces execution time but increases CPU load; decreasing the value increases execution time but reduces CPU load.

(If the machine that runs GestióIP isn't too occupied, a value of 254 shouldn't be a problem).

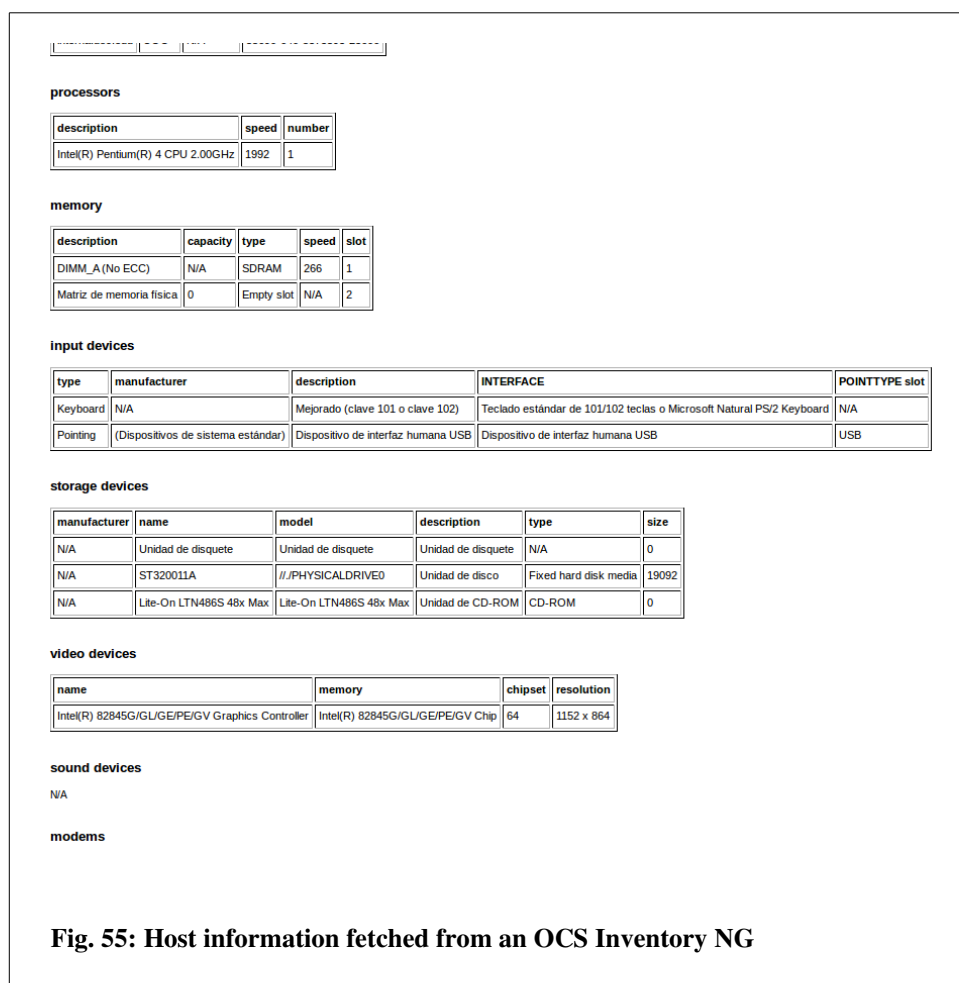
After changing the parameters click "set" to save the new values.

Note

High values of max number parallel processes may also cause peaks of the CPU load of the DNS server.

4.2.4 Extended support for OCS Inventory NG

With enabled OCS support there will be the new button  behind every entry within *host list view* be displayed, allowing to fetch directly the information for this IP from an OCS Inventory NG.



Click link “update entry” to update the defined host columns with the information found in the OCS database.

To enable OCS support set parameter “enable OCS support” to yes and click “save”. After enabling OCS support there will be new form element to configure the parameter for the OCS displayed. Edit the parameters and click “save” to save the configuration.

The following parameters are related to OCS Inventory NG support:

enable OCS support - set this parameter to yes to enable OCS support. This parameter is only related to the frontend web and does not affect the automatic update against OCS.

OCS DB name - name of OCS database

OCS DB user - name of OCS database user

OCS DB password - OCS database password

OCS DB IP address - IP address of the OCS database server

OCS DB port - Port where the OCS database is listening (default: 3306)

4.3 Manage audit db

Audit database will grow with time. You can delete events created by automatic update against DNS, SNMP or OCS (AUTO events) or events created by actions made via GestióIPs frontend Web (MAN events) independently (see 2.6).

The screenshot shows a web interface titled "manage audit db". It contains two sections for deleting audit events. The first section is for "Delete AUTO audit events older than" with a dropdown menu set to "3 month" and a note "(1 AUTO events client 1)". Below this are radio buttons for "actual client" (selected) and "all clients". There is a "delete" button and a checked checkbox labeled "keep network events". The second section is for "Delete MAN audit events older than" with a dropdown menu set to "1 year" and a note "(7 MAN events client 1)". Below this are radio buttons for "actual client" (selected) and "all clients". There is a "delete" button. At the bottom, it displays "DB size total: 0.11MB (AA: 0.01MB, MA: 0.00MB)".

Fig. 56: Manage audit db

To delete old audit events:

- Choose a time from which the events should be deleted.
- Select if either only events for the actual client or the events for all clients should be deleted.
- Mark check box “keep networks events” if network specific events should be kept.
- Click “delete” to delete the audit events.

Note

With older versions of Mysql “DB total size” may not be displayed.

Note

History information for networks and hosts is extracted from audit log. Deleting old audit events causes history entries to also be deleted.

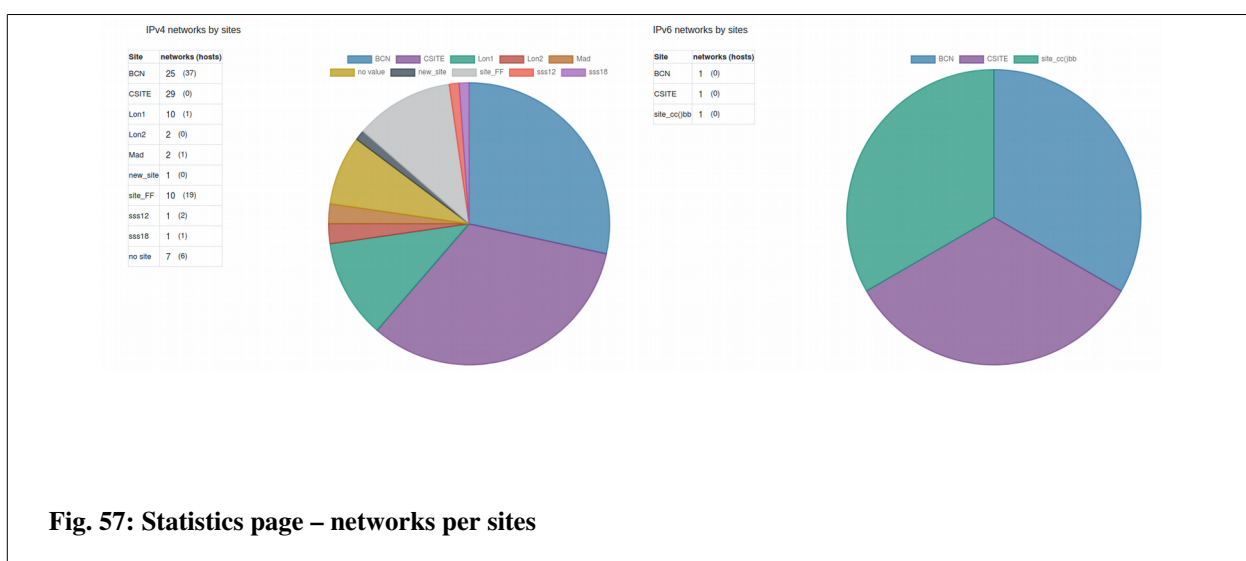
4.3.1 Reset database

Resetting the database causes that all networks and hosts of the selected IP version will be deleted for the actual client. If both, IPv4 and IPv6 is selected, VLANs will also be deleted from GestióIPs database.

5 Statistics

GestióIP's statistics page shows the number of managed networks, hosts and VLAN. It gives an overview of how many networks and hosts are in the different environments (*network categories*) and in the different *sites*, as well as of the manufacturers of the devices. It offers the possibility to show the occupation of the networks and network ranges and it allows to list the networks which only contain host with status “down”.

To access the statistics page go to "manage" -> "statistics".



Since GestióIP v3.5.6 there are also custom statistics for networks and hosts available. The custom statistic allows to list networks or host by one attribute and then to optionally filter the result by a different attribute.

This allows for example, to show statistics of the following type:

Show IPv4 networks by Tag (no filter)

Show IPv6 networks by Tag with are on Site “X”

Show IPv4 host distribution by OS which are in the production environment

Show IPv6 host by manufacturer which are on Site “Y”

Show custom statistic

Show networks by filter by send

Show hosts by filter by send

Fig. 58: Create custom statistic

Note

With multiple clients configured, only client specific statistics will be displayed here. To see the total number of managed clients, networks and host go to “help” -> “about”.

5.1 Network/range occupation

In addition, the statistics page offers the possibility to show an overview of net or range occupation. This may be useful to detect poorly utilized address ranges. You can filter the networks that should appear in the report by IP (or parts of IP), description, site, category and comment.

Network occupation

show networks with an occupation > 90 % filter v4 ☒ v6 ☐ show

show networks with an occupation < 10 % filter v4 ☒ v6 ☐ show

Range occupation

show ranges with an occupation > 90 % v4 ☒ show

show ranges with an occupation < 10 % v4 ☒ show

Miscellaneous

Networks which only contain hosts with status "down" v4 ☒ v6 ☐ show

Networks which only contain hosts with status "down" or "never checked" v4 ☒ v6 ☐ show

Fig. 59: Network and range occupation form

5.2 Miscellaneous

This option allow to list networks only containing hosts with status “down” or networks only containing host with status “down” or status “never checked”.

Miscellaneous

Networks which only contain hosts with status "down" v4 ☒ v6 ☐ **show**

Networks which only contain hosts with status "down" or "never checked" v4 ☒ v6 ☐ **show**

Fig. 60: Show networks with status “down”

Note

The reason because all hosts of a network appear as “down” may be the missing of firewall rules.

6 Scheduled Jobs

GestióIP disposes about powerful mechanisms to discover the network infrastructure. This can be used for an initial discovery and/or to keep the GestióIP database automatically up to date.

GestióIP allows to schedule Job. Jobs can be executed one-time or can be executed periodically.

There are the following Jobs available:

- 1. Combined Jobs (global discovery)** – allows to combine the Jobs 2), 3), 4) and 5) so that new discovered networks will be automatically processed by the host discovery. It allows also to execute the VLAN discovery. This job type is specially useful for an initial discovery of a network infrastructure.
- 2. Network discovery** – imports networks from the routing table of layer 3 devices with SNMP.
- 3. Host discovery (DNS)** – discovers devices with DNS and ping.
- 4. Host discovery (SNMP)** – discovers devices with SNMP.
- 5. VLAN discovery** – imports VLANs with SNMP.
- 6. Import DHCP leases** – imports hosts from DHCP leases data.
- 7. local database backup** – Creates a local backup of the actual database.

Go to “manage > Jobs” to open the Job management page.

6.1 Create new Jobs

Click over “new” to create new Jobs.

The screenshot shows a web form for creating a new job. The fields are as follows:

- Name***: A text input field with a yellow border.
- type***: A dropdown menu showing "global discovery".
- status***: A dropdown menu showing "enabled".
- run only once**: An unchecked checkbox.
- start date***: A text input field containing "24/05/2020 19:41". Below it, the format "Format: dd/mm/yy hh:ss" is indicated.
- end date**: A text input field. Below it, the format "Format: dd/mm/yy hh:ss" is indicated.
- execution interval**: A dropdown menu showing "daily", followed by "at", a spinner showing "all", "0", and "1", then "hour(s) and", another spinner showing "0", "1", and "2", and finally "minute(s)".
- comment**: A text input field.

Fig. 61: Create Job

Name: name to identify the Job. The Job name must be unique.

Type: type of the job (see 6.2).

Status: enabled or disabled. Only enabled Jobs will be executed.

Run only once: execute the job only one-time. When this checkbox is checked there will appear the new field “**execution date**” instead of the fields “start date” and “end date” which allows to introduce the time when the job should be executed. Use the format “dd/mm/yy hh:ss” (example: 24/05/2020 19:41).

Start date: date when the Job should start to be executed like specified in “execution interval”.

End date: after this date, the job will not longer be executed.

Execution interval: to specify the interval in which the job should be executed.

Comment: an optional comment.

6.2 Job types

6.2.1 Combined discovery (global discovery)

The global discovery is thought to combine the “network discovery” with other Jobs. This allows to discover new networks and scan them directly with the host discovery. This is especially useful for an initial discovery of a network infrastructure. Combined Jobs will always execute the “network discovery”.

By checking the options “execute VLAN discovery”, “execute host discovery DNS” and/or “execute host discovery SNMP” one can specify which other types of discoveries should be executed. The host discoveries will be executed against the networks which were found before by the network discovery. See the discovery specific chapters for a description of the available options.

6.2.2 Network discovery

The network discovery reads the routing tables of SNMP enabled layer 3 devices like router, layer 3 switches or firewalls and imports the found networks into the GestióIP database.

The network discovery offers the following configuration options:

SNMP Group: select the SNMP Group which holds the SNMP credentials for the devices which should be queried. This option is mandatory. If you do not have any SNMP groups defined go first to “manage > SNMP Groups” to create new SNMP Groups.

Choose one of the following three options to specify the devices which should be queried:

Nodes list: to introduce a comma separated list of the IPs of devices (example: 192.168.1.1,172.16.3.1).

Nodes file: a file with a list of IPs of devices (one IP per line). The file must be saved in /usr/share/gestioip/etc.

Example:

192.168.1.1

172.16.3.1

Tags: the discovery will be executed against devices which have the selected Tags assigned.

Delete not found networks: delete the networks from the GestióIP database which are not longer found within the routing tables of the nodes specified in “nodes list”, “nodes file” or “nodes Tags”.

Report not found networks: report the networks which are found in the GestióIP database but

which are not longer found within the routing tables of the nodes specified in “nodes list”, “nodes file” or “nodes Tags”.

IPv4: import IPv4 networks.

IPv6: import IPv6 networks.

Site: assign the selected site to the new discovered networks.

Assign tags: assign the selected Tags to the new discovered networks.

import VRF routes: import VRF routes (only Cisco devices supporting MPLS-VPN-MIB or MPLS-L3VPN-STD-MIB) (requires SNMP version 2c).

import host routes: import routes with a bitmask of /32 as host.

Add interface description: use ifDescr/ifAlias of the routes interface as description of the new network.

Interface description identifier: specify if ifDescr or ifAlias should be used as network description.

send result by mail: check this checkbox if you wish to receive an email with the Job result. This option requires that you already have a SMTP server defined. If you do not have any SMTP defined go first to “manage > SMTP Server” and create a SMTP server.

report only changes: report only added, deleted or modified entries.

Mail recipients: coma separated list of the addresses the Job result to be send to.

SMTP server: mail server to use. Create mail servers from “manage > SMTP server”.

Mail from: the “from” of the result mail.

verbose: enable verbose logging.

debug: enable debug logging.

6.2.3 Host discovery by DNS

The host discovery is thought to scan networks for new or changed devices. The “discovery by DNS” is based on ping to determine if an IP is up and DNS PTR queries or DNS zone transfers to determine the DNS name of IPs.

The host discovery by DNS offers the following configuration options:

Choose one of the following five options to specify the networks which should be processed:

Network list: to introduce a coma separated list of the networks which should be processed (example: 192.168.0.0/25,172.16.23.0/24).

Network file: a file with a list of networks (one network per line). The file must be saved under /usr/share/gestioip/etc/.

Example:
192.168.0.0/25
172.16.23.0/24

Tags: the discovery will be process networks which have one of the the selected Tags assigned.

IP range: process only the IPs of the specified IP range (example: 192.168.0.1-192.168.1.100).

Sites: processes all networks of the selected sites.

IPv4: process IPv4.

IPv6: import IPv6.

Delete hosts: delete host entries which do not answer to ping and which do not have an DNS entry configured.

Site: process only IPs from this Site.

Child number: number of parallel process to fork during the discovery.

send result by mail: check this checkbox if you wish to receive an email with the Job result. This option requires that you already have a SMTP server defined. If you do not have any SMTP defined go first to “manage > SMTP Server” and create a SMTP server.

report only changes: report only added, deleted or modified entries.

Mail recipients: coma separated list of the addresses the Job result to be send to.

SMTP server: mail server to use. Create mail servers from “manage > SMTP server”.

Mail from: the “from” of the result mail.

ignore generic auto - Set this value to "yes" if the update script should ignore rDNS entries which follow the "generic-auto" scheme. Example: IP: 1.2.3.4 -> "generic auto" PTR entries generated by GestióIP: 4-3-2 and 2-3-4.

See 3.2.2.3.1 for more information about *ignore* and *ignore generic auto* variables
ignore generic auto.

ignore - String that match generic rDNS entries in the case that your generic rDNS entries don't match "generic auto PTR entries" (see *ignore generic auto*). This option allows the update process to recognize generic rDNS entries. Example: rDNS entry: dhcp-2.3.5.2.gestioip.net -> *ignore*: dhcp-

use zone transfers: Use zone transfer to obtain DNS information. Without this parameter the discovery will execute a DNS PTR query for every IP to determine the DNS entry of the IP. With this option checked, the discovery will fetch the whole DNS zone from the DNS server. This makes a query for every IP not longer necessary. It also allows, apart from using the DNS PTR entry, to use the DNS A entry of an IP address to obtain it's DNS entry. This option requires to allow zone transfers from the DNS server to the GestióIP server.

Here a configuration example for BIND:

```
zone "myzone.net" {
    type master;
    file "/var/lib/bind/myzone.net";
    allow-transfer { IP_ADDRESS_GESTIOIP_SERVER; };
};
```

Go to chapter 12.1.1.1 to see how this can be configured in a Microsoft DNS server.

verbose: enable verbose logging.

debug: enable debug logging.

6.2.4 Host discovery by SNMP

The host discovery is thought to scan networks for new or changed devices. This discovery type will try to connect to ever IP of the specified networks. For most devices it is able to fetch information like the hostname, manufacturer, OS and some other information. To see information like manufacturer (vendor) in the GestióIP front end you need to enable the corresponding custom columns first (see. 3.12.1).

The host discovery by SNMP offers the following options:

SNMP Group: select the SNMP Group which holds the SNMP credentials for the devices which should be queried. Go to “manage > SNMP Groups” to create new SNMP Groups.

Choose one of the following four options to specify the networks which should be processed:

Network list: to introduce a coma separated list of the networks which should be processed (example: 192.168.0.0/25,172.16.23.0/24).

Network file: a file with a list of networks (one network per line). The file must be saved in /usr/share/gestioip/etc.

Example:

```
192.168.0.0/25
172.16.23.0/24
```

Tags: the discovery will be process networks which have one of the the selected Tags assigned.

IP range: process only the IPs of the specified IP range (example: 192.168.0.1-192.168.1.100)

Sites: processes all networks of the selected sites.

IPv4: process IPv4.

IPv6: process IPv6.

Site: process only IPs from this Site.

Child number: number of parallel process to fork during the discovery.

send result by mail: check this checkbox if you wish to receive an email with the Job result. This option requires that you already have a SMTP server defined. If you do not have any SMTP defined go first to “manage > SMTP Server” and create a SMTP server.

report only changes: only report added, deleted or modified entries.

Mail recipients: coma separated list of the addresses the Job result to be send to.

SMTP server: mail server to use. Create mail servers from “manage > SMTP server”.

Mail from: the “from” of the result mail

verbose: enable verbose logging.

debug: enable debug logging.

6.2.5 VLAN discovery

The VLAN discovery is able to fetch the information of the configured VLANs from SNMP enabled devices.

The VLAN discovery offers the following options:

SNMP Group: select the SNMP Group which holds the SNMP credentials for the devices which should be queried. Go to “manage > SNMP Groups” to create new SNMP Groups.

Choose one of the following three options to specify the devices which should be queried:

Nodes list: to introduce a coma separated list of the IPs of devices (example: 192.168.1.1,172.16.3.1).

Nodes file: a file with a list of IPs of devices (one IP per line). The file must be saved in /usr/share/gestioip/etc.

Example:

192.168.1.1
172.16.3.1

Tags: the discovery will be executed against devices which have the selected Tags assigned.

send result by mail: check this checkbox if you wish to receive an email with the Job result. This option requires that you already have a SMTP server defined. If you do not have any SMTP defined go first to “manage > SMTP Server” and create a SMTP server.

report only changes: only report added, deleted or modified entries.

Mail recipients: coma separated list of the addresses the Job result to be send to.

SMTP server: mail server to use. Create mail servers from “manage > SMTP server”.

Mail from: the “from” of the result mail.

verbose: enable verbose logging.

debug: enable debug logging.

6.2.6 Import DHCP leases

The job type “import DHCP leases” allows to synchronize GestióIP’s host entries on the base of information from DHCP leases data. It reads the actual leases information from the configured data source, compares it with the leases information from the last run and updates the GestióIP database with the detected changes.

There are the following lease data sources supported.

- ISC Kea API
- ISC Kea leases file
- ISC DHCPD leases file
- Microsoft DHCP leases file
- Generic CSV file

Note: if you are using a DHCP server which is not supported yet mail to contact@gestioip. Probably we can add support for your data source in short term.

6.2.6.1 ISC KEA API

This “Leases type” allows to query leases data directly from the KEA API.

The following parameters are supported:

KEA URL: the URL of the KEA control agent

IP version: IP version

Use basic authentication: if there is basic authentication for the KEA API configured, select this checkbox and configure the username and password in the file /usr/share/gestioip/etc/kea-users.

Tags: process only IP addresses which fall in the range of the networks which have one of this Tags assigned. Other IP address will be ignored.

send result by mail: check this checkbox if you wish to receive an email with the Job result. This option requires that you already have a SMTP server defined. If you do not have any SMTP defined go first to “manage > SMTP Server” and create a SMTP server.

report only changes: only report added, deleted or modified entries.

Mail recipients: coma separated list of the addresses the Job result to be send to.

SMTP server: mail server to use. Create mail servers from “manage > SMTP server”.

Mail from: the “from” of the result mail.

debug: enable debug logging.

6.2.6.2 Kea/ISC DHCPD/MS leases/Generic CSV file

The types “Kea leases file”, “ISC DHCPD leases file” and “MS leases file” support following parameters:

Leases file name: path and name of the file holding the leases information. Make sure that file is readable by the user which is running the Apache web server.

Tags: process only IP addresses which fall in the range of the networks which have one of this Tags assigned. Other IP address will be ignored.

send result by mail: check this checkbox if you wish to receive an email with the Job result. This option requires that you already have a SMTP server defined. If you do not have any SMTP defined go first to “manage > SMTP Server” and create a SMTP server.

report only changes: only report added, deleted or modified entries.

Mail recipients: coma separated list of the addresses the Job result to be send to.

SMTP server: mail server to use. Create mail servers from “manage > SMTP server”.

Mail from: the “from” of the result mail.

debug: enable debug logging.

6.2.6.3 How to pass the leases information to the GestióIP server.

Actually there are two types of data sources supported. The KEA API and different formats of leases files. The KEA API will be queried directly by the GestióIP DHCP synchronization mechanism. In the case that the information is available in form of leases files you need to create a job on the DHCP server to upload the lease file to the GestióIP server. GestióIP offers a web based upload mechanism for this task.

Leases files can be uploaded to the URL

<http://localhost/gestioip/api/upload.cgi>

The script upload.cgi requires the parameter “file_name”:

`file_name=file_name` – The leases file will be copied with this name to the directory `/usr/share/gestioip/var/data/` on the GestióIP server. The same name must be configured as option “Lease file” when creating the corresponding Job with the GestióIP Gui.

`leases_file=file` – The file with the leases information

Create a script to upload the leases file to the GestióIP server and schedule it with the cron daemon.

Here an example for a command to upload the leases file the GestióIP server.

```
/usr/bin/curl -u USER:PASSWORD -F "file_name=leases.csv" -F "leases_file=@/var/lib/kea/kea-leases4.csv" http://gestioip\_server/gestioip/api/upload.cgi
```

To execute the script periodically (for example every 10 minutes) you can create a cron job like this:

```
*/10 * * * * /path/to/upload_script.sh
```

On Windows Servers you can use the “Task Scheduler” to execute a PowerShell script to create and to upload the leases file. See 6.2.6.3.3 for an example script.

6.2.6.3.1 Kea lease file

The leases file is expected to have the following format:

```
address,hwaddr,client_id,valid_lifetime,expire,subnet_id,fqdn_fwd,fqdn_rev,hostname,state,user_context
```

For example

```
192.168.100.101,08:00:27:86:f0:92,01:08:00:27:86:f0:92,4000,1603408941,1,1,1,nodolan2,0,
```

6.2.6.3.2 ISC DHCPD lease file

Here an example for the format the leases file is expected to have:

```
lease 192.168.1.199 {
starts 1 2020/02/01 08:26:41;
ends 1 2020/02/01 08:36:41;
tstp 1 2010/02/01 08:36:41;
cltt 1 201/02/01 08:26:41;
binding state free;
hardware ethernet 0a:0b:33:9c:18:db;
uid "\011\010\010\225\023K";
client-hostname "host199";
}
```

6.2.6.3.3 Microsoft DHCP lease file

To Process Microsoft DHCP server leases information with GestióIP you need first to export the data to a file and the upload the file to the GestióIP server.

MS leases data is expected to come in the following format:

```
"IPAddress","ScopeId","AddressState","ClientId","ClientType","Description","DnsRegistration","
DnsRR","HostName","LeaseExpiryTime","NapCapable","NapStatus","PolicyName","ProbationEn
ds","ServerIP","PSComputerName"
```

For example:

```
"192.168.1.200","192.168.1.0","Active","08-00-27-15-9d-
7a","Dhcp","NotApplicable","NoRegistration","12/31/2020 3:04:14
PM","False","FullAccess",,"192.168.1.50",
"192.168.1.201","192.168.1.0","Active","e2-34-3f-3e-00-02-00-00-ab-11-af-ed-cf-84-a7-77-7d-
e9","Dhcp","Complete","PTR","ubuntu18.GestioIPTest.local","10/31/2020 3:22:23
PM","False","FullAccess",,"192.168.1.50",
```

Here are two examples of Powershell commands which can be used to export the MS lease information to the expected format.

Export data of a specific IPv4 scope (replace the x.x.x.x with the scope which should be exported):

```
Get-DhcpServerv4Lease -ComputerName "server.domain.com" -ScopeId x.x.x.x |
select Hostname, ClientId, IPAddress | Export-csv -path "\\UNC\leases.csv"
```

Export all IPv4 lease data:

```
Get-DhcpServerv4Lease -ComputerName "server.domain.com" | select Hostname,
ClientId, IPAddress, ScopeID, AddressState | Export-csv -path "\\UNC\leases.csv"
```

Upload the leases file to the GestióIP server:

```
$file_name = 'leases.csv'
$u, $p = 'username', 'password'
$uri = 'http://gestioip_server/gestioip/api/upload.cgi'

$b64 = [Convert]::ToBase64String([Text.Encoding]::ASCII.GetBytes("$u:$p"))

$invokerestmethodParams = @{
    'Uri'                = $uri
    'Method'              = 'POST'
    'Headers'             = @{ Authorization = "Basic $b64" }
    'leases_file'         = 'C:\path\to\leases.csv'
    'file_name'           = $file_name
}

$output = Invoke-RestMethod @invokerestmethodParams

write-output $output
```

6.2.6.3.4 Generic lease file

If your lease data is not available in one of the predefined formats you can create a file in the “generic” leases CSV file format.

If the leases information of your DHCP server is for example stored in a database, you can create a script which exports the leases information from the database to a file in “generic” format and upload this file then to the GestióIP server.

The generic format consists in four fields

IP address, hostname, hardware address, valid to (in epoch time)

For example:

192.168.1.100, host_100,08:00:27:86:f0:92,1603408941

7 Database initialization

GestióIP offers several mechanisms to import data into its database.

Note: The discovery functions which are described in this chapter are still available and functional but since GestióIP version 3.5.4 superseded by the *Scheduled Jobs* (see 6). They may be deleted from the software in the future.

- a) networks/hosts/VLANs via SNMP query (superseded by the “combined discovery” - see 6.2.1).
- b) hosts via DNS queries (superseded by the “host discovery by DNS” - see 6.2.3).
- c) networks/hosts from spreadsheets.

7.1 Discovery

The Discovery is intended to initialize GestióIP's database after a new installation. It explores the network infrastructure using SNMP and DNS and adds found VLANs, networks and hosts to GestióIP's database. Alternatively you can define a “Combined discovery” Job (6.2.1) for the same task. “Combined Jobs” offer more configuration options.

It executes the following processes:

- VLAN discovery via SNMP using Perl Module SNMP::Info
- Network discovery via SNMP querying routing tables from network devices

- Host discovery of new found networks via SNMP using SNMP::Info and own discovery mechanisms
- Host discovery of new found networks via DNS

The discovery process needs about 45s for one class C networks with 254 addresses, depending on the value of max-procs (number of parallel discovery processes) and the CPU/memory of the server. Note that discovery for one class B network with a bitmask of /16 (65.534 addresses) may take hours because discovery processes the network portionwise each with 128 parallel processes (depending of the global configuration parameter *max-procs*).

Click “import/export” → “Discovery” to access discovery form.

Note

Discovery process will optionally process networks found by last run of “import networks from spreadsheets”. So import your network spreadsheets before you execute the discovery process.

Note

Discovery process will update predefined columns, too. So configure predefined columns first before executing the discovery process.

Network devices
holding routing tables
(e.g routers or multilayer switches)

(Coma separated list of IP addresses)

Import networks
IP version v4 ☒ v6 ☐

Import routes
learned from local ☒ static ☒ other ☐ OSPF ☐ RIP ☐ IS-IS ☐ Cisco EIGRP ☐

SNMP version v1
community (Default: public)

Process only IPv4 networks
beginning with

Process only IPv6 networks
beginning with

max number of parallel
discovery processes 128

Include networks which were added
by last run of import networks from
spreadsheet within discovery ☒

Discover new found
networks only ☒

add comment to
found networks ☐ (e.g. Local route from 192.168.46.1)

discover

Fig. 62: "Discovery" form

Network devices - One or a list of IP addresses of devices holding routing and/or VLAN information. These are typically network devices like routers or multilayer switches.

Import networks IP version – To choose for with IP version the discovery should be executed (this option is only available when global configuration parameter “IPv4 only” is set to “no”)

Import routes learned from – To define from which routing protocols the learned networks should be imported.

SNMP version – To choose the SNMP version which should be used for discovery

SNMPv1 and SNMPv3:

community – SNMP community string

SNMPv3

Selecting SNMP version “v3” there appear SNMPv3 specific options.

The image shows a web form for configuring SNMPv3. It includes the following fields and controls:

- SNMP version:** A dropdown menu with 'v3' selected.
- username:** A text input field.
- Security Level:** A dropdown menu with 'authNoPriv' selected.
- Auth algorithm:** A dropdown menu with a hyphen selected.
- Auth password:** A text input field.
- Privacy algorithm:** A dropdown menu with a hyphen selected.
- Privacy password:** A text input field.

Fig. 63: SNMPv3 form

username – SNMPv3 username

Security Level – SNMPv3 security level

Auth algorithm – Authentication algorithm (only authNoPriv and authPriv)

Auth password – Authentication password (only authNoPriv and authPriv)

Privacy algorithm – Privacy algorithm (only authPriv)

Privacy password – Privacy password (only authPriv)

Process only IPv4 networks beginning with – If you divide a complex network infrastructure into smaller sections via the “client” option (see 3.7) you can specify here the first octets of the networks which should be imported and processed during the discovery process. To import only networks starting with 192.168 introduce “192.168”. The field accepts a comma-separated list of networks (e.g.

10,172.16,192.168)

Process only IPv6 networks beginning with – Like “Process only IPv4 networks beginning with” but for IPv6 networks. Example: 2001::ab,2002::

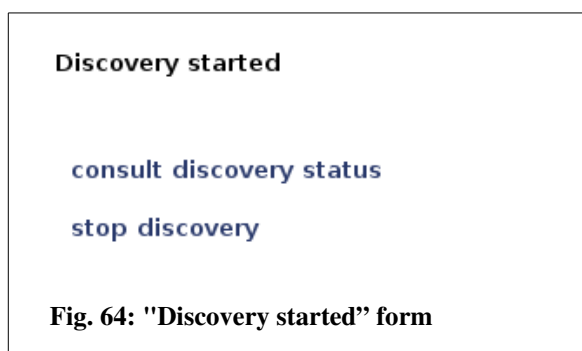
maximal number of parallel discovery processes - Number of child processes lanced by discovery. Augment of this value will speed up discovery process but increase CPU load and memory usage.

Include networks which were added by last run of *import networks from spreadsheet* within discovery - mark this check-box if you want that discovery processes the networks which were imported by last run of *import networks from spreadsheet*, too.

Discover new found networks only – If this checkbox is checked, only new found networks will be processed. If you uncheck it, all found network will be processed.

add comment to found networks - mark this check-box if discovery should add automatically comment like “*Static route from 192.168.239*”.
Click “discover” to lance discovery process.

It appears a new page offering the options to consult the status of the discovery process or to interrupt the discovery process.



Discovery started

[consult discovery status](#)

[stop discovery](#)

Fig. 64: "Discovery started" form

Clicking “consult discovery status” opens a new window showing the actual status of discovery process (Fig. 65). The status page refreshes automatically every 10s during discovery.

Click “stop discovery” to interrupt the discovery process. It may take up to 15s to stop all discovery child processes.



Click link “log file” to display detailed log information of the discovery process. Type “CTR R” to refresh log file window. The log file will be deleted when discovery process is executed again.

Note

If you use a SNMP community other than the default “public”, SNMP based parts of the discovery process will try to query the devices with community string “public”, too. That makes sure that devices with the custom community “public” configured, not to be ignored (e.g. it's a common error to forget to set community for printers or to configure a custom community for a device but not disable the community “public”). Execute a search for “public” through the audit log to identify devices with default community strings configured.

Note

You can also consult the audit log to see the details of the discovery process.

7.2 Import networks via SNMP

The "import networks via SNMP" function queries routing tables from SNMP enabled devices and adds the found networks to the database. Let it run against your layer III devices (e.g. routers or multilayer switches).

7.2.1 Manual import via SNMP

To import networks via SNMP click “import/export” → "import networks via SNMP" .

host to query (IP address)

Import networks
IP version v4 ☒ v6 ☐

Import routes
learned from local ☒ static ☒ other ☐ OSPF ☐ RIP ☐ IS-IS ☐ Cisco EIGRP ☐

SNMP version v1
community (Default: public) [?](#)

Process only IPv4 networks
beginning with

Process only IPv6 networks
beginning with

add comment to
found networks ☐

include networks
within automatic
update ☒

query

Fig. 66: "import via SNMP" form

See 7.1 for a description of the options

If the found networks should be included within *automatic update*, mark "include networks within the automatic update" checkbox.

Note

If you query devices with enabled dynamic routing protocols (e.g. BGP), a query may take quite a long time and can cause a "web-server timeout" error (because the routing tables can be very large). In this case, use script "get_networks_snmp.pl" from the directory "/usr/share/gestioip/bin".

Note

Network import via SNMP will although be executed during discovery process (see 7.1)


7.3 Import from spreadsheet

GestióIP possesses flexible mechanisms to import networks or hosts from spreadsheets. Spreadsheets must have .xls extension (MS Excel). If you use OpenOffice use the "Save As..." option to save the spreadsheet in .xls format.

7.3.1 Import networks from spreadsheets

Go to "import/export" -> mark "networks" radio button and upload the spreadsheet with the networks to import.

Your spreadsheet may consists of different sheets. In step II you have the possibility to import all sheets, one sheet by its name or multiple sheets by numbers.

Step II 

Mark radio button and introduce the sheets to import

all sheets ☒

sheet name ☐


sheets ☐ 

Fig. 67: "Import from spreadsheet" form

To import all sheets mark "all sheets". To import one sheet mark the radio button "sheet name" and introduce the sheet name (e.g. "server") (see Fig. 68). To import multiple sheets mark the "sheets" radio button and introduce the numbers of the sheets to import. The form accepts a single number, a comma-separated list or a range of sheets (e.g. 2-4 to import sheets "LAN I, LAN II and Sheet4" in the example below).

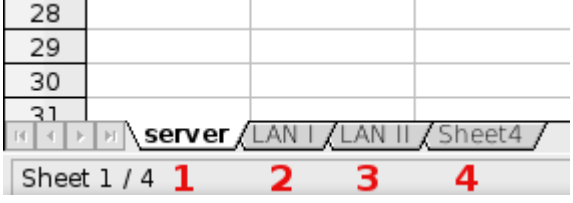


Fig. 68: Sheet numbers

Next, indicate what information is in each column: Associate the letters of the columns with the corresponding content.

The letters of the columns are found at the top of each column of your spreadsheet.

networks - Column with networks. Example of format supported entries: 192.168.0.0 - entries that don't match the format will be ignored.

netmask/bitmask - Column with netmask or bitmask (columns with mixed netmask and bitmask

are also supported). Example of format supported entries: 24, 255.255.255.0 - entries that don't match the format will be ignored.

networks and netmask/bitmask in one column - Column with both network and net/bitmask. If your spreadsheet contains one column with both networks and net/bitmasks, leave *networks* and *netmask/bitmask* blank.

Examples of supported formats:

1.1.1.0/24, 1.1.1.0/255.255.255.255, 1.1.1.0-24, 1.1.1.0 – 255.255.255.0, 1.1.1.0 xyz 24

Network entries that don't match the supported formats will be ignored.

description - Column with network descriptions – optional.

site - Column with sites. The sites of the networks to import must be identical to the sites in GestióIP's database. If the site doesn't exist in the database it will be ignored – case-sensitive – optional.

category - Column with categories. The category must be identical to the categories in GestióIP's database. If the category doesn't exist it will be ignored – case-sensitive – optional.

comment - Column with comments – optional.

Mark "include networks within automatic update" if the network should be processed by automatic update.

Custom Columns

vlan: VLANs must be introduced in the format *vlan_id* - *vlan_name* (e.g. "1 - default"). The VLANs must exist in the GestióIP database

custom select box columns: To populate columns which are defined as select-box, the items which should be imported must exist.

	A	B	C	D	E	F
1	network	bitmask or subnetmask	description	site	category	comment
2						
3	192.168.0.0	24	some description	Lond I		
4	192.168.1.0	24		Lond I	Prod	
5	192.168.2.0	255.255.255.0			Dev	
6	192.168.3.0	24	some description	Barcel	Pre	some comment
7	xxxxxxxxxxx			Barcel	Pre	
8	192.168.4.0	27				
9						
10	192.168.5.0	25	some description			some comment
11	192.168.5.128	255.255.255.128	some description	Lond I		
12	10.0.10.0	24		Lond I		
13						

column entries

A ▼

networks

B ▼

netmask/bitmask/bitmask's last octet

or

☐ ▼

networks and netmask/bitmask in one column

Fig. 69: Spreadsheet to import

7.3.2 Import hosts from spreadsheet

To import hosts from spreadsheets into GestioIP's database click "import" -> mark "hosts" radio button and upload the spreadsheet containing host entries to import.

Note

The networks containing the hosts to import must exist; so import or introduce networks first. If import function doesn't find an adequate network for the host entries, they will be ignored.

Indicate if you want to import all sheets, one sheet by its name or multiple sheets (see. 7.3.1).

Indicate the format of the IP addresses in the spreadsheet:

Indicate the format of the IP addresses in the spreadsheet

☒ standard (e.g. 192.168.250.3)

☐ only last octet (e.g. 3 or .3) field which contains the network address (e.g. B3)

Fig. 70: Indicate IP address format

If your spreadsheet contains IP addresses in standard format (e.g. 82.98.146.69) select “standard” radio button. If your spreadsheet contains only the last octet of the IP address, mark “only last octet” and specify the field containing the network address (e.g. A1). Networks must have one of the following formats:

NetworkID/netmask (192.168.9.0/255.255.255.0)

NetworkID/bitmask (192.168.9.0/24)

Leading or following strings will be ignored (e.g. the entry “Network 192.168.9.0/24 XXX” will also be accepted) (see Fig. 71).

	A	B	C	D
1	Production network 192.168.9.0/255.255.255.0			
2				
3				
4		.1	gtw-vrrp	
5		.2	gtw1	
6		.3	gtw2	
7		.7	serverA1	
8		.8	serverA2	

Fig. 71: Spreadsheet containing last octet of IP addresses to import

Indicate the format of the IP addresses in the spreadsheet

- ☐ standard (e.g. 192.168.250.3)
☒ only last octet (e.g. 3 or .3) field which contains the network address (e.g. B3)

Indicate the corresponding letters and columns

column	entries
<input type="text" value="B"/>	IP address
<input type="text" value="C"/>	hostname

Fig. 72: Import spreadsheet containing last octet of IP addresses

Next, associate the letters of the columns with the corresponding content (see 7.3.1) and click “import”.

7.3.3 Import VLANs from spreadsheet

To import VLANs from spreadsheets into GestioIP's database click “import” -> mark ”VLANs” radio button and upload the spreadsheet containing VLANs to import. Choose the sheets that should be imported, associate letters and columns and click “import”.

8 Access control

GestióIP supports authentication and authorization. For the *authentication* process create local users or GestióIP LDAP users/groups. Use the *authorization* system to assign specific permissions to

local users or the GestióIP LDAP users/groups. Authorization is in the default configuration disabled.

8.1 Authentication

GestióIP's authentication process is carried out through Apache's mod_auth. You can use any kind of authentication which is supported by the Apache web server (e.g. local user/groups, LDAP, MS Active Directory, certificates, ...).

Local users as well as LDAP users and LDAP groups can be configured since GestióIP v3.5.4 via the web interface. Other types of authentication (e.g. Kerberos) must be configured manually in the GestióIP Apache configuration file. The web based configuration for local and LDAP users is only available for new installations >= v3.5.4. If you have upgraded from a version earlier than v3.5.4 you need to adapt your Apache configuration manually to make this feature available. You can download detailed instructions how to update the Apache configuration from the GestióIP web page:

https://www.gestioip.net/docu/Update_GestioIP_config_354.pdf

You can find sample Apache configurations with authentication against KERBEROS 5 on the GestióIP web page: <http://www.gestioip.net>.

8.1.1 Default user

During the setup there will be a administrative user account created. The default username is "gipadmin". The user is authenticated with the password which were created during setup. The default user has access to all functions of GestióIP.

Note

To enhance security it is recommended to configure individual accounts for every GestióIP user. This has the advantage that audit events can be associated with a specific user.

8.1.1.1 Create local accounts

To create new local accounts go to *manage > Users > add*.

The screenshot shows a web form titled 'Create local user'. It has the following fields and controls:

- Name***: A text input field.
- type***: A dropdown menu with 'local' selected.
- Login password**: A text input field.
- retype Login password**: A text input field.
- email**: A text input field.
- phone**: A text input field.
- comment**: A text input field.
- add**: A button to submit the form.

Fig. 73: Create local user

Name: Username

type: User type. Here “local”.

Login password/retype Login password: login password for the user.


email: email address of the user – optional

phone: phone number of the user – optional


comment: a comment – optional

Click “add” to create the new account. After this you should be able to log in to GestióIP's web Gui using this account.

8.1.1.2 Update local users passwords

To update the password for a local user go to manage > Users and click over the user's “change password” button ().

8.1.1.3 Delete accounts

To update the password for a local user go to manage > Users and click over the user's delete button ().

8.1.2 Authentication against LDAP

GestióIP supports the authentication against LDAP directories, for example Microsoft Active Directory. The authentication can be made with individual LDAP accounts or against LDAP groups. Since GestióIP v3.5.4, all parameters can be configured via the web Gui.

To configure authentication against a LDAP directory with individual LDAP accounts you need to

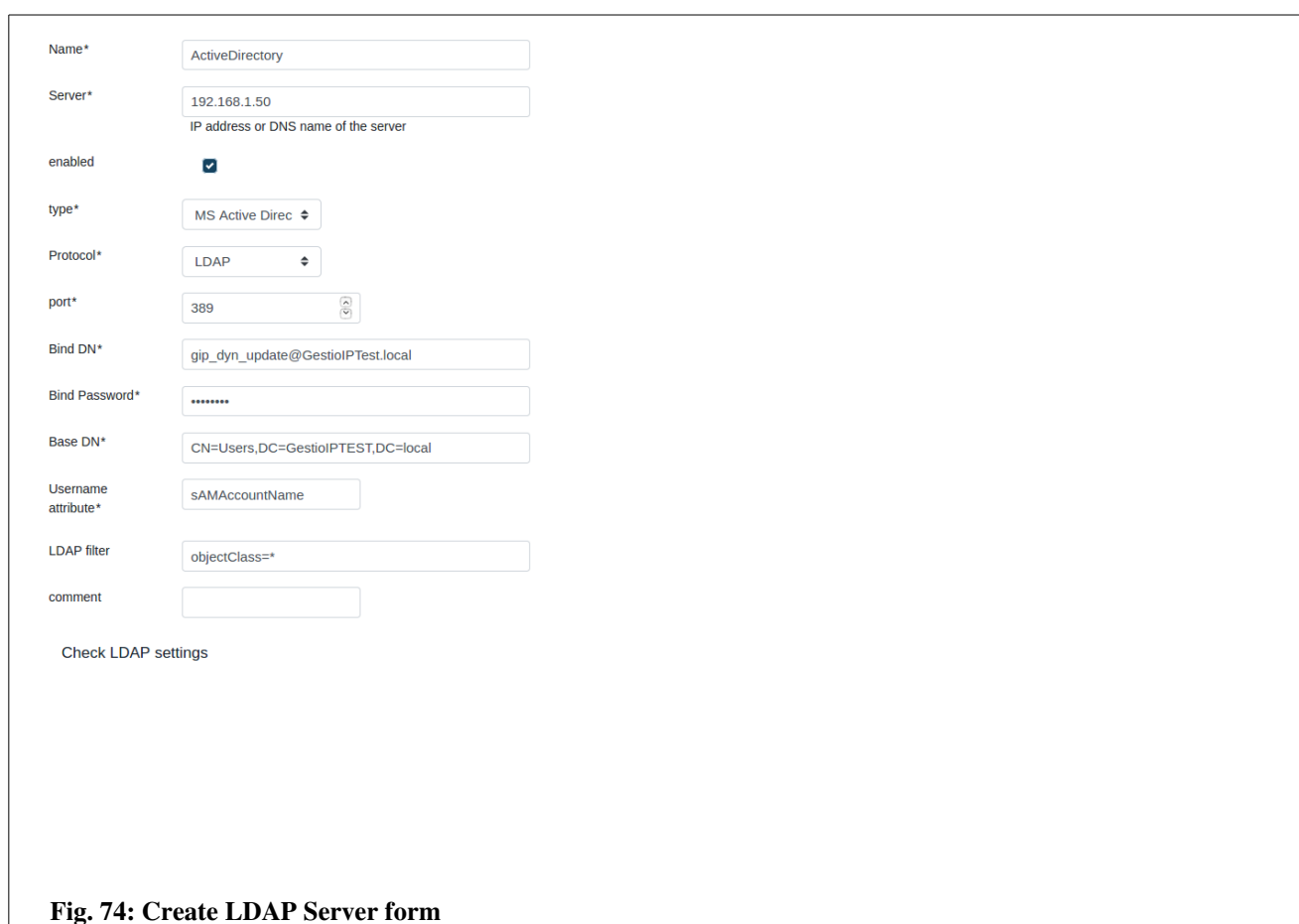
- Create a LDAP server
- Create the LDAP users

To configure authentication against a LDAP directory with LDAP groups you need to

- Create a LDAP server
- Create the LDAP groups

8.1.2.1 Create LDAP server

To create a new LDAP Server go to “manage > LDAP servers” and click over “new”.



The screenshot shows the 'Create LDAP Server' form with the following fields and values:

- Name***: ActiveDirectory
- Server***: 192.168.1.50 (with a note: IP address or DNS name of the server)
- enabled**: ☒
- type***: MS Active Direc (dropdown)
- Protocol***: LDAP (dropdown)
- port***: 389 (with a note icon)
- Bind DN***: glip_dyn_update@GestióIPTest.local
- Bind Password***: (masked with dots)
- Base DN***: CN=Users,DC=GestióIPTEST,DC=local
- Username attribute***: sAMAccountName
- LDAP filter**: objectClass=*
- comment**: (empty)

At the bottom of the form is a button labeled 'Check LDAP settings'.

Fig. 74: Create LDAP Server form

Name: A name to identify the LDAP server.

Server: DNS name or IP address of the LDAP server.

enabled: mark this checkbox to make this server active. Only one active server is supported.

type: server type.

Protocol: LDAP or LDAPS.

port: LDAP port.

Bind DN: LDAP user account that has privileges to search for users.

Bind Password: password for the Bind DN.

Base DN: Distinguished Name (DN) of the starting point for directory server search.

Username attribute: LDAP attribute which holds the username.

LDAP filter: an optional filter.

comment: an optional comment.

Click over “Check LDAP setting” to check if it is possible to bind to the LDAP server.
If the check is successful, click “add” to create the LDAP server.

8.1.2.2 Authentication with LDAP accounts

For an authentication with a LDAP user, create an GestióIP user with the same name. To do so, go to manage > Users > add.



The screenshot shows a web form titled "Create LDAP User form". It contains the following elements:

- A text input field labeled "Name*" with the value "ldap_user".
- A dropdown menu labeled "type*" with the value "LDAP".
- An empty text input field labeled "email".
- An empty text input field labeled "phone".
- An empty text input field labeled "comment".
- A button labeled "add" at the bottom left.

Fig. 75: Create LDAP User form

Name: the name of the account (must be identical with the name of the LDAP account).

type: type of the user. Here “LDAP”.

email: the email address of the user – optional

phone: the phone number of the user – optional

comment: a comment – optional

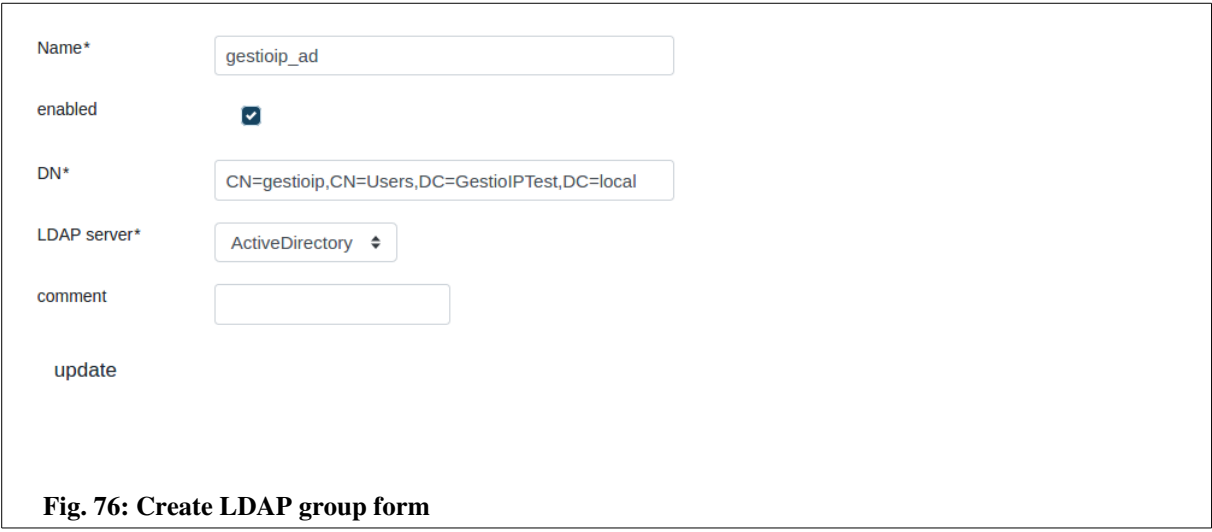
Click “add” to create the account. After this you should be able to log in with the new account.

If the “**User Management**” feature is enabled, there appear also the field **User Group**, which allows to select the User Group, the user should be assigned to.

8.1.2.3 Authentication with LDAP groups

For an authentication with LDAP groups, GestióIP fetches the groups the login user belongs to from the LDAP server and compares the groups with the active LDAP groups which are known by GestióIP. When there is a matching active group is found, the access will be granted.

To create an LDAP group go to manage > LDAP groups > add.



The screenshot shows a web form for creating an LDAP group. It contains the following fields and controls:

- Name***: A text input field containing the value "gestioip_ad".
- enabled**: A checkbox that is checked.
- DN***: A text input field containing the value "CN=gestioip,CN=Users,DC=GestioIPTest,DC=local".
- LDAP server***: A dropdown menu with "ActiveDirectory" selected.
- comment**: An empty text input field.
- update**: A button located below the comment field.

Fig. 76: Create LDAP group form

Name: A name to identify the group in GestióIP.

enabled: with “enabled” checked, the group will be used for authentication.

DN: Distinguished Name (DN) of the group.

LDAP Server: the LDAP server where the group is defined.

comment: an optional comment

If the “**User Management**” feature is enabled, there appear also the field **User Group**, which allows to select the User Group, the user should be assigned to. The User Group defines the permissions of the user. If there are multiple LDAP Groups defined which the user belongs to, the permissions of all this groups will be merged.

8.2 Authorization

The authorization system allows to assign different permissions to different users or LDAP groups. The authorization system is disabled by default.

The permissions to access the different features of GestióIP are defined for the User Groups. To assign permissions to a User/LDAP group make it member of an adequate User Group.

To enable the authorization feature you need to execute the following steps:

- Activate the authorization feature.
- Adapt the default user groups to you requirements or create user groups.
- Create users and assign the adequate user group to the user.

Note:

If you use the authorization feature it is recommended to use individual accounts for every GestióIP user.

8.2.1 Activation

To activate the authentication go to “manage” → “manage GestióIP”, set the parameter “User management” to “yes” and click “save”. This will create an entry for the actual user in the user database and make it member of the group “GestióIP Admin”, which has all permissions, including the permission to create new users and user groups.

Activating the authorization feature creates the new menu items “User Groups” under “manage” item (after activating authorization click over any link to make the new menu item appear).

8.2.2 User Groups

User Groups are used to determine the User permissions. Go to “manage”->”Users Groups” to create, update or delete GestióIP User Groups.



name	description	
Admin	Default group with rights to create, update, delete GestióIP objects like networks, hosts and VLANs	 
GestióIP Admin	Default group with all rights including rights to create, update and delete Users, clients and the GestióIP configuration	 
Read Only	Default group with rights to show GestióIP objects like networks, hosts and VLANs	 

[add User Group](#)

Fig. 77: User Group list view

GestióIP comes with three default User Groups:

- **GestióIP Admin:** Group with all permissions
- **Admin:** Group with all permission except the permissions to manage users and to change the GestióIP configurations
- **Read only:** Group with permissions to show, but not to edit networks, host, VLANs, AS and leased lines.

8.2.2.1 Permissions

The authorization system offers the following permission:

Global Permissions

- Manage GestióIP permissions – permission to display and change all function under “manage”->”manage GestióIP”
- Manage user permissions – permissions to create, read, update and delete Users and User Groups
- Manage sites and categories - permissions to create, read, update and delete sites and categories
- Manage custom columns - permissions to create, update and delete custom host and network columns.
- Read audit – permissions to access audit log
- clients - to select if the non-global permissions should be available for all or only for a specific client.
- Objects from Sites RO – gain RO access to the objects (networks, hosts, ...) from this sites
- Objects from Sites RW – gain RW access to the objects (networks, hosts, ...) from this sites

Client specific permissions (non-global permissions)

Manage Tags - create, update, delete Tags

Manage SNMP groups - create, update, delete SNMP Groups

Manage DNS server groups - create, update, delete DNS server groups

Manage dynamic DNS updates - configure dynamic DNS updates

Manage MACs – manage MACs

Networks

- create networks - permission to create networks
- read network information - permission to list networks
- update network information - permission to update networks
- delete networks - permission to delete networks

Hosts

- create hosts - permissions to create host
- read host information - permission to list host entries
- update host information - permissions update hosts
- delete hosts - permission to delete hosts
- Execute update against DNS
- Execute update against DNS
- Execute update against DNS

VLANs

- create VLANs – permissions to create VLANs
- read VLAN information – permissions to list VLANs
- update VLAN information – permissions to update VLANs
- delete VLANs – permissions to delete VLANs

Configuration Management (CM)

- Show backedup device configurations – permissions to show the stored configurations of the network devices
- Upload device configurations – permissions to upload configurations or files to devices which are under control of the CM module
- Administrate CM – permissions to change the CM configuration for devices

Autonomous Systems

- create AS – permissions to create ASs
- read AS information – permission to list ASs
- update AS information – permissions to update ASs
- delete AS – permissions to delete ASs

Leased Lines (LLs)

- create Leased Lines – permissions to create LLs
- read Leased Line information – permissions to list LLs
- update Leased Line information – permissions to update LLs
- delete Leased Lines – permission to delete LLs

8.2.2.2 Create User Groups

Click “add User Group” to create new Users Groups.

name

description

Global permissions

Manage GestióIP permissions ☐

Manage user permissions ☐

Manage sites and categories ☐

Manage custom columns ☐

Read audit ☐

clients ☒ All Clients

Client specific permissions

networks

create networks ☐

read network information ☒

update network information ☐

delete networks ☐

hosts

create hosts ☐


Fig. 78: Add User Group form

name – User Group name (mandatory)


description – an optional descriptions

Assign the desired permission to the User Group by selecting the adequate permission checkboxes.

8.2.2.3 Edit User Groups

Click over the -symbol to access the edit-User form.

8.2.2.4 Delete User Groups

Click over the -symbol to delete users.

Note:

The actual User Group can not be deleted.

8.2.3 User “gipoper” of GestióIP versions <3.2

The authorization system which was implemented in release 3.2 eliminates the need of the old user “gipoper”. That affects the Apache configuration. As the authorization is now made by the GestióIP software, there is not longer the need of the directives for the directory **[DocumentRoot]/gestioip/res**. It is recommended to delete the configuration part for the “res”-directory from the Apache configuration file for GestióIP (gestioip.conf):

```
<Directory "/var/www/gestioip/res">
    AddHandler cgi-script .cgi
    AddDefaultCharset utf8
    AllowOverride None
    Options +ExecCGI
    AuthType Basic
    AuthName GestioIP
    AuthUserFile /etc/apache2/users-gestioip
    Require user gipadmin
    ErrorDocument 401 /gestioip/errors/error401.html
    ErrorDocument 403 /gestioip/errors/error403.html
    ErrorDocument 404 /gestioip/errors/error404.html
    ErrorDocument 500 /gestioip/errors/error500.html
</Directory>
```

Restart the Apache web server to take the change affect.

9 Password Management

GestióIP incorporates a password management system which allows to store and show device password. All keys are stored in encrypted form in the database. The password management feature requires that the Authorization system is enabled (see 8.2).

The password management system uses the following keys:

- One global master key – to encrypt/decrypt the device passwords
- Individual user passwords for each user – to encrypt/decrypt the master key. The master key is stored for every user individually, encrypted by the user password.
- Device passwords – stored passwords of the devices

Every user has it's individual user key. The user key is used to encrypt/decrypt the master key. The master key is used to encrypt/decrypt the device password.

9.1 Enabling the password management system

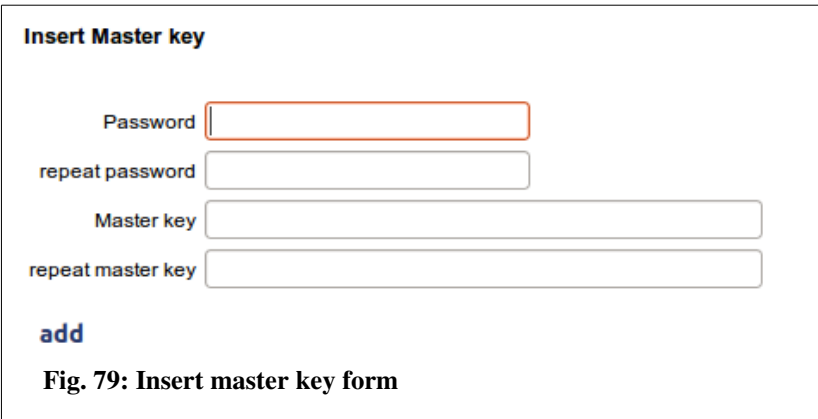
The password management system is per default disabled. To use it, you need to enable it first. To enable the password management system go to manage > manage GestióIP, set “Password management enabled” to yes and press “set”.

Note

To use the password management you need also enable the user management system (see 8.2.1).

After clicking over any link there appears the new menu item manage > manage password.

Go to manage > manage password and introduce a user password and the master key (“Insert Master key” form). The user password is individual for each user and is used to insert and show the device passwords. It may be different to the login password.



Insert Master key

Password

repeat password


Master key

repeat master key

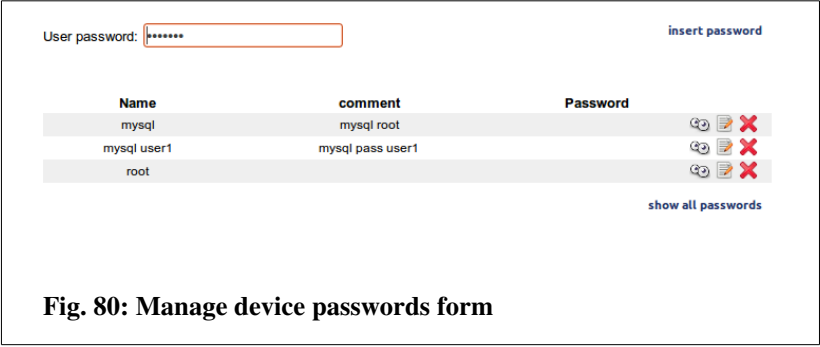
add










Fig. 79: Insert master key form

9.2 Manage device passwords

After enabling the password management system there appears a new key-button for every IP within the host-list-view ().

Clicking over the button opens the manage device passwords form:



Name	comment	Password
mysql	mysql root	  
mysql user1	mysql pass user1	  
root		  

show all passwords

Fig. 80: Manage device passwords form


To insert, show or edit device passwords introduce your user password, first.

9.2.1 Insert a new device password

Introduce your user password and click over “insert password”.

Introduce a name, the device password and an optional comment and click “add”.


9.2.2 Show device passwords

To show a password introduce the user password and click over the eye -symbol. To show all passwords click “show all passwords”

9.2.3 Edit device passwords

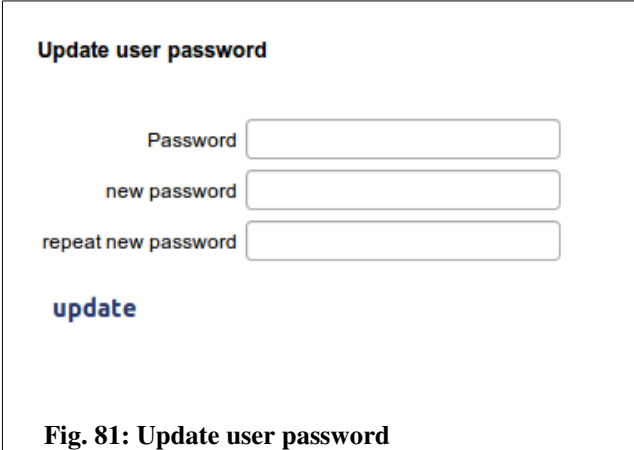
To edit password click over the edit -symbol

9.2.4 Delete device passwords

To delete a password click over the delete -symbol

9.3 Changing the user password

To change the user password go to manage > manage passwords and insert the old and the new user password and press update.



The screenshot shows a web form titled "Update user password". It contains three input fields: "Password", "new password", and "repeat new password". Below the fields is a blue "update" button. The form is enclosed in a thin black border.

Fig. 81: Update user password

9.4 Reset the user password

Click over reset to delete the user passwords



The screenshot shows a web form titled "Reset user password". It contains a single blue "reset" button. The form is enclosed in a thin black border.

Fig. 82: Reset user password

9.5 Changing the master key

The master key is stored for every user individually, encrypted by the user's password. Every user must update its version of the master key when the master key was changed. That requires that the new master key must be communicated via a secure channel to every user. GestióIP does not dispose about a mechanism for that.

To update the master key go to manage > manage passwords, insert your user password and the new master key. Click "update" to save the changes.

Update master key

(Requires that all other users change their user password)

Password

new Master key

repeat new Master key

update

Fig. 83: Update master key

After changing the master key, every user will be forced to update it's version of the master key when accessing to the manage-password-form.

Master key changed. Update your user's master key.

Update master key for this user

Password

new Master key

repeat new Master key

update

Fig. 84: Reset user password


10 Advanced functions

10.1 Update check

GestióIP disposes about a mechanism to check if there are software updates available. Click over “help” → “check for updates” to execute the update check.

In the case that there are updates available, the update-check shows a link to download the last actualization tar-ball, as well as a link to the *change log* and an explication how to apply the update.

Update check



Patches available

Actual patch version: **7**
Your patch version: **6**

Download [actual patch](#)

See [change log](#)

Installation instructions

Untar actualize_gestioip30.tar.gz

```
$ tar vzxvf actualize_gestioip30.tar.gz
```

Change to directory actualize_gestioip30

```
$ cd actualize_gestioip30
```

Execute actualize_gestioip.sh like root

```
$ sudo ./actualize_gestioip.sh
```

Fig. 85: Online update check

10.2 Database configuration (*ip_config*)

The database configuration of GestióIP is stored in /DocumentRoot/priv/ip_config

Because the database password is stored in clear text, the Apache web server must be correctly configured and the permissions of the configuration file (500) must be correctly set. To check whether the Apache2 web server is correctly configured, you can try to access the configuration of GestióIP with a browser. Open the following URL with a browser:

http://servername/gestioip/priv/ip_config

You should receive an "access denied" message. In case it is possible to access the file "ip_config", check file permissions of "ip_config" and review the configuration of Apache2.

Configuration parameter description:

<i>parameter</i>	<i>description</i>
bddd_host	Host where the GestióIP Mysql database runs
bddd_port	Port on which the database listens
sid_gestioip	SID of the GestióIP database
user_gestioip	GestióIP database user
pass_gestioip	GestióIP database user password

10.3 Export networks, VLANs or hosts to CSV

GestióIP includes the possibility to export networks as well as host to CSV files (comma separated list) which you can import easily e.g. into LibreOffice or MS Excel.

Click "import/export" → "export networks or hosts to CSV" to access the export form.

Export networks to CSV

all networks ☒ ☐

IP version v4 ☒ v6 ☐

networks which match ☐

export

Export hosts to CSV

all hosts ☒ ☐

IP version v4 ☒ v6 ☐

from network ☐ (e.g. 192.168.0.0)

hosts which match ☐

export

Export VLANs to CSV

all VLANs ☒ ☐

VLANs which match ☐

export

Fig. 86: Network, VLAN or host export form

There is either the option to export all networks/VLANs/hosts or to export networks, VLANs or hosts with match a specific string. The string could be an IP address (or a part of an IP address), a part of the description, site, category or comment.

Host export offers furthermore the option to export all IP addresses of a dedicated network by introducing the network ID (e.g. 172.16.4.0) into the text-box “from network”.

Click “export” to execute export function. After a successful export a link to download the exported data is shown.

export successfully finished

[download CSV file](#)

Fig. 87: Link to download the exported data

When importing the data into a spreadsheet application choose “UTF8” like character set and “,” (coma) like separator.

10.4 Add a new language

Currently GestióIP supports the following languages: Catalan, Spanish, Italian, German and English. GestióIP possesses a system that makes it easy to add new languages. To add a new language you need to translate on of the files containing the language variables.:

To translate the language-file make a copy of one of the existing language files (e.g. /DocumentRoot/vars/vars_en) and name it vars_xy (replace the xy with the abbreviation of the new language – for French "vars_fr", for Danish "vars_dk". The abbreviation must contain two or three characters). The file contains variables such as:

name_of_the_variable=value of the variable

example file /DocumentRoot/vars/vars_en

```
mostrar_redes_message=show networks  
mostrar_red_message=show network  
busqueda_detallada_message=advanced search  
crear_red_message=create new network
```

Translate the text starting at the right of the "="

Special characters must be introduced encoded in HTML (ú -> ú)

And...

Send the new language file to contact@gestioip.net. It would be a pleasure to include support for your language within the next actualization of GestióIP!

11 IPv6 Address plan

GestióIP offers tools which can help to build to your organization adapted IPv6 address planes.

It supports two different methods to create IPv6 address plans: Translation of the existing IPv4 subnet scheme to IPv6 on the base of an IPv6 address block or to create an hierarchical IPv6 address plan on the base of *sites* and *categories*.

11.1 Direct translation

With this method you can translate the whole or a recognizable, unique part of the IPv4 address ranges to IPv6. It bases on an specified IPv6 address block. The octets of the IPv4 addresses are translated one by one to an hexadecimal value. The corresponding IPv6 networks are created from the given IPv6 address range plus the to hexadecimal converted values of the individual octets of the IPv4 address.

Example

IPv6 address block to build the plan from: 2001:bd8::

IPv4 address range used by organization: 192.168.0.0-192.168.255.255

Example network: 192.168.190.32/27

Octett	Decimal	hexadecimal
oct1	192	C0
oct2	168	A8
oct3	190	BE
oct4	32	20

If it is possible to traduce all IPv4 networks or only a part of them to IPv6 depends in the prefix length of the specified IPv6 address block. Prefix Length > 32 do not offer enough bits to map the whole IPv4 address space. If you use an IPv6 address blocks with a prefix length > 32 you must curtail the IPv4 address range you want to translate. Table above shows the translated IPv6 address for different combinations of Prefix Length, IPv4 octets and the IPv4 bitmasks (IPv6 address block 2001:bd8:: and IPv4 network 192.168.190.32/27).

Prefix length	Required IPv4 octets	Translation only for networks with IPv4 Bitmask	translated IPv6 address
<=32	-	all	2001:db8:C0A8:BE20::
33-40	oct1	all	2001:db8:A8BE:2000::
41-48	oct1 + oct2	17-24	N/A (network Bitmask is 27)
	oct1 + oct3 + oct4	25-32	2001:db8:0:2000::

11.1.1 Create the address plan

To translate your existing IPv4 networks to IPv6 click over “networks”-> “IPv6 address plan”.

Step (1)

Introduce the IPv6 address block you want to create the plan from and “press send”.

Direct translation

Translate IPv4 networks based on the following IPv6 address block (e.g. 2001:DB8::/48)

Fig. 88: Create hierarchical IPv6 address by translation existing IPv4 networks

Step (2)

Curtail the IPv4 address range you want to translate by introducing the required or optional octets of the IPv4 address range. If you work with an IPv6 address block with a prefix length > 40 you need to specify at least the first two octets. By introducing the first two octets, only the IPv4 networks with bitmask from 17-24 will be translated. By introducing the first three octets, only the IPv4 networks with bitmasks for 25-32 will be translated.

Translate IPv4 networks based on the following IPv6 address block (from IP address block 2001:DB8::/48)

A prefix length of /48 does not offer enough bits to map the whole IPv4 address space. Please introduce either the *first two octets* of the IPv4 address range that should be translated to IPv6 (to map networks with bitmasks from 17 to 24) or the *first three octets* (to map the networks with bitmasks from 24 to 32)

☒ Map only IPv4 networks whose first two octets match

☐ Map only IPv4 networks whose first three octets match

[send](#)

Fig. 89: Curtail address range to translate

After clicking “send”, a list with the networks to create will be displayed. To create the new IPv6 networks within GestióIP's database edit the networks fields and press “create”. To avoid that specific networks will be created, unselect the checkbox “create” behind the regarding networks.

11.2 Hierarchical IPv6 address plan based on sites and categories

GestióIP's hierarchical address plan builder offers the possibility to map the network structure of an organization to the (physical) structure of it's sites and networks categories. Therefore it's necessary to define well the different sites and categories of your organization before you begin to create a hierarchical address plan.

One of the benefits of a hierarchical plan is that you can recognize directly from the IP address to which site the address belongs.

Example

A organization has three sites (site1, site2, site3), seven categories (prod, preprod, test, dev, test, corpA, corpB) and at most 95 networks per category. It's ISP has assigned it the IPv6 address block 2001:AAAA:BBBB:/48.

With a prefix length of 48 remain 4 bits to map the existing sites, categories and networks per category. How many bits will be reserved for each one depends on it's number.

The following table shows how GestióIP would distribute the free four bits in relation with the number of sites, categories and networks per categories for this example:

IPv6 address block: 2001:aaaa:bbbb:0000:0000:0000:0000/48

site	2001:aaaa:bbbb: 0 000::
categories	2001:aaaa:bbbb: 00 00::
Networks per category	2001:aaaa:bbbb: 0000 ::

The table above shows some addresses that could be created within this plan.

Level I (sites)	Level II (categories)	Level III networks/categorie
2001:aaaa:bbbb: 0 000::	2001:aaaa:bbbb: 00 00::	2001:aaaa:bbbb: 0000 ::
		2001:aaaa:bbbb: 0001 ::
	2001:aaaa:bbbb: 01 00::	2001:aaaa:bbbb: 0100 ::
		2001:aaaa:bbbb: 0101 ::
		2001:aaaa:bbbb: 0102 ::
	2001:aaaa:bbbb: 02 00::	2001:aaaa:bbbb: 0200 ::
2001:aaaa:bbbb: 1 000::	2001:aaaa:bbbb: 1 000::	2001:aaaa:bbbb: 1000 ::
2001:aaaa:bbbb: 2 000::	2001:aaaa:bbbb: 2 000::	2001:aaaa:bbbb: 2000 ::

11.2.1 Create the address plan

To create a hierarchical IPv6 address plan click over “networks”-> “IPv6 address plan”

Step (1)

Introduce the IPv6 address block you want to create the plan from and “press send”.

Hierarchical address plan based on sites and categories

IPv6 address block to build address plan from (e.g. 2001:DB8::/48)

[send](#)

Fig. 90: create hierarchical IPv6 address plan from an IPv6 block

Step (2)

Choose the number of sites, categories and networks per category which you need to map your organization's structure (take future growing in mind).

Hierarchical address plan based on sites and categories (IP address block 2001:aaaa:bbbb:0000:0000:0000:0000/48)

Up to how many sites (regions) do you may need in the future? (actually you are using **3** sites)

Up to how many categories (facility) do you may need in the future? (actually you are using **7** categories)

How many networks will be maximal needed for a single category (facility)? (The maximum number of networks of a single category is **95** (Lon1/corp))

Carry over the descriptions and comments of existing IPv4 networks ☒

Create new end-networks independently of the number of existing sites and categories ☒

[send](#)

Fig. 91: Number of site and category networks and networks per category

GestióIP makes here a proposal based on existing sites, categories and networks per category. With marked checkbox “Carry over the descriptions and comments of existing IPv4 networks”, the descriptions of the existing IPv4 networks will be assigned to the new IPv6 networks with the corresponding sites and categories. GestióIP's default behavior is to create as many new networks per site and category as existing IPv4 networks. With selected checkbox “Create new end-networks independently of the number of existing sites and categories” you will have in a later step the possibility to introduce the number of networks to create for each site and category independently. Once you have chosen the numbers click “next”.

Step (3)

GestióIP calculates all possible combinations of network distributions on the base of the numbers which were introduced in the previous step and displays a list with possible numbers of level I subnets (designated for the *location* root-networks).

Hierarchical address plan based on sites and categories (IP address block 2001:aaaa:bbbb:0000:0000:0000:0000/48)

Subnet level I: sites

Please choose the amount of super-networks you want to reserve for your *sites*

- [4 networks /50](#) 0 surplus location network
- [8 networks /51](#) 4 surplus location network
- [16 networks /52](#) 12 surplus location network
- [32 networks /53](#) 28 surplus location network

Fig. 92: Level I networks (sites)

Click over the link with the number of networks you want to reserve for the locations.

Step (4)

In this step there will be a list of possible numbers of level II subnets displayed (designated for the *category* root-networks).

Hierarchical address plan based on sites and categories (IP address block 2001:aaaa:bbbb:0000:0000:0000:0000/48)

Subnet level II: categories

Please choose the amount of super-networks you want to reserve for your *categories*

- Subnet level I: *sites* **8 networks /51** (required: 4)
 (2001:aaaa:bbbb::/51 - 2001:aaaa:bbbb:e000::/51) [back](#)
- Subnet level II: *categories* **16 networks /55** 7 surplus category networks (512 networks /64 per category)
 32 networks /56 23 surplus category networks (256 networks /64 per category)
 64 networks /57 55 surplus category networks (128 networks /64 per category)

Fig. 93: Level II networks (categories)

Choose the number of networks you want to reserve for the categories and click over the corresponding link. A list of level II and level III networks will be displayed (the number of level III subnets will automatically be calculated from the prefix length of the layer II networks). If you are not satisfied with the result use the back-link to return to previous page to change the number of level I subnets.

Step (5)

A list of level II and level III networks will be displayed (the number of level III subnets will automatically be calculated from the prefix length of the layer II networks).

Hierarchical address plan based on sites and categories (IP address block 2001:aaaa:bbbb:0000:0000:0000:0000/48)

Please click "send" to show the address plan

Subnet level I: <i>sites</i>	8 networks /51 (required: 4) (2001:aaaa:bbbb::/51 - 2001:aaaa:bbbb:e000::/51)
Subnet level II: <i>categories</i>	32 networks /56 (required: 9) (2001:aaaa:bbbb::/56 - 2001:aaaa:bbbb:ff00::/56)
Subnet level III: <i>end-networks per category</i>	256 networks /64 (required: 120) (2001:aaaa:bbbb::/64 - 2001:aaaa:bbbb:ffff::/64) back

[send](#)

Fig. 94: Level III networks (networks per category)

If you are satisfied with the result click over “send”. If the checkbox “Create new end-networks independently of the number of existing sites and categories” from step (2) was selected, there will be a form displayed which allows to introduce the definitive number of new networks per location and category that should be created.

Step (6) (optional)

Introduce the number of networks which you want to be created for each location/category and click “next”

Hierarchical address plan based on sites and categories (IP address block 2001:aaaa:bbbb:0000:0000:0000:0000/48)

Choose the amount of networks which should be created for every site/category

Lon1

corp	<input type="text" value="95"/>
corp1	<input type="text" value="20"/>
dev	<input type="text" value="9"/>
dev-test	<input type="text" value="2"/>
pre	<input type="text" value="25"/>
prod	<input type="text" value="56"/>
test	<input type="text" value="17"/>

Lon2

corp	<input type="text" value="5"/>
corp1	<input type="text" value="0"/>
dev	<input type="text" value="0"/>
.	<input type="text"/>

Fig. 95: Number of networks to create

Step (7)

A list of the networks which should be created will be displayed. With marked checkbox “Carry over the descriptions and comments of existing IPv4 networks” (Step (2)), the comments of the IPv4 networks are taken over for the new IPv6 networks. Edit the descriptions of the networks, add an optional comment and select the “sync” checkbox if you want that the new network will be processed by automatic actualization (see Error: Reference source not found). If you want to avoid networks from being created unselect the check box “create”. Only networks with selected “create” checkbox will be created.

Hierarchical address plan based on sites and categories (IP address block 2001:aaaa:bbbb:0000:0000:0000:0000/48)

Lon1

IP address	BM description	site	category	comment	sync	create
2001:aaaa:bbbb:0000:0000:0000:0000	51	Lon1	---		---	<input checked="" type="checkbox"/>

Lon1 - corp

IP address	BM description	site	category	comment	sync	create
2001:aaaa:bbbb:0000:0000:0000:0000	55	Lon1	---		---	<input checked="" type="checkbox"/>

IP address	BM description	site	category	comment	sync	create
2001:aaaa:bbbb:0000:0000:0000:0000	64	Lon1	corp		<input type="checkbox"/>	<input checked="" type="checkbox"/>
2001:aaaa:bbbb:0001:0000:0000:0000	64	Lon1	corp		<input type="checkbox"/>	<input checked="" type="checkbox"/>
2001:aaaa:bbbb:0002:0000:0000:0000	64	Lon1	corp		<input type="checkbox"/>	<input checked="" type="checkbox"/>
2001:aaaa:bbbb:0003:0000:0000:0000	64	Lon1	corp		<input type="checkbox"/>	<input checked="" type="checkbox"/>
2001:aaaa:bbbb:0004:0000:0000:0000	64	Lon1	corp		<input type="checkbox"/>	<input checked="" type="checkbox"/>

Fig. 96: Edit network paramters

Click link “create” at the bottom of the page to insert the new networks into GestióIP's database.

12 DNS server integration

GestióIP can be integrated with DNS servers. It allows either to push changes which are made via the GestióIP front end to the master DNS servers or to update the GestióIP database automatically when there where changes in the DNS server made.

The update *from the GestióIP server to the DNS server* is made by secure dynamic DNS updates. GestióIP supports DDNS updates to Microsoft DNS server (GSS-TSIG) as well as to DNS servers like BIND or PowerDNS with support for TSIG keys.

Dynamic updates *from the DNS servers to the GestióIP server*, requires that there is a PowerDNS server installed on the GestióIP server. The PowerDNS server will be configured as DNS slave server and will receive notifications from the master DNS server about changes in the DNS zones. GestióIP will periodically check the PowerDNS zones for changes and will update it's database respectively.

The DNS integration supports A and PTR entries only.

12.1 Updates from the master DNS server to the GestióIP

GestióIP uses PowerDNS to receive dynamic DNS updates. GestióIP will check periodically if there are changes in the PowerDNS zone files and update it's database respectively if there are changes detected.

To enable updates from the master DNS server to GestióIP you need to:

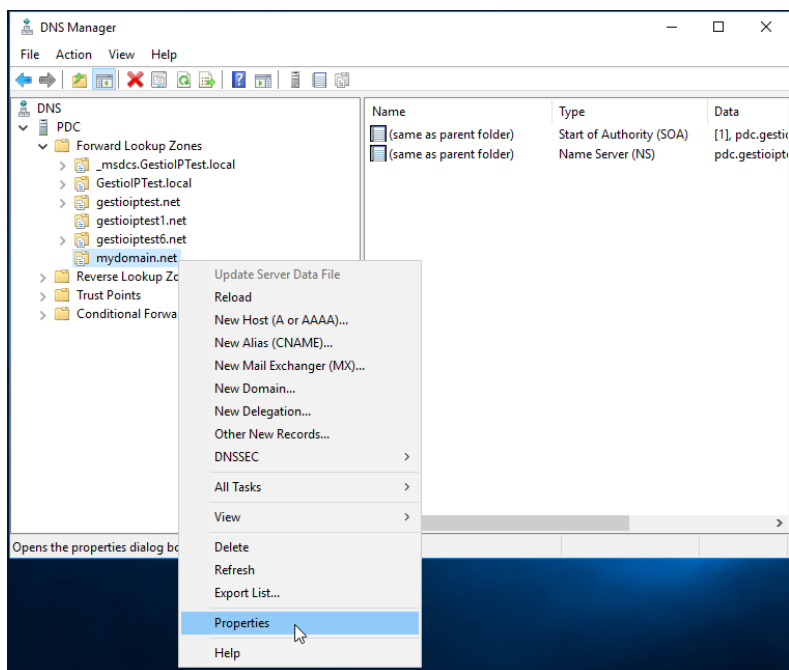
- Configure notifications on the master DNS server.
- Install and configure PowerDNS on the GestióIP server.

12.1.1 Microsoft as master DNS server

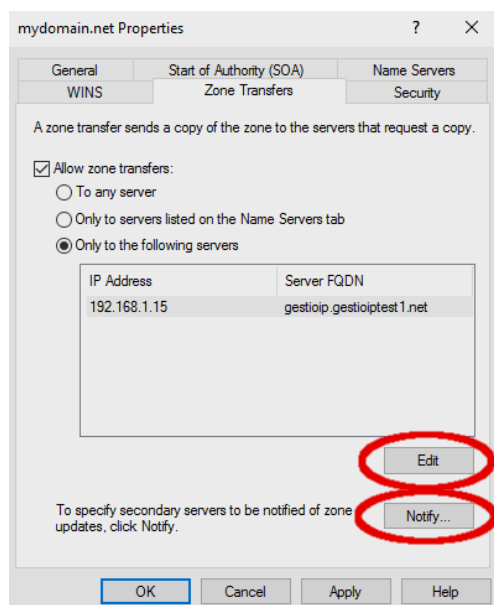
To prepare the MS master DNS server you need enable notifications of zone updates.

12.1.1.1 Configure automatic notification

Open the “DNS manager” > right click over the zone > click “Properties”.



Go to the “Zone Transfer” tab.



Click “Edit” and add the GestióIP server to the list of servers to which zone transfers are allowed.
Click “Notify...” and add the GestióIP server to list of servers to be notified of zone updates.
Click “OK”

Repeat the steps for the corresponding reverse zone(s).

12.1.2 BIND as master DNS server

To prepare the BIND master DNS server you need enable notifications of zone updates for the GestióIP server.

12.1.2.1 Configure automatic notification

To force a BIND master DNS server to send DNS update notifications to the GestióIP server add the “also-notify” statement to the configuration of the corresponding zones.

```
Zone      "domain.com" IN {
    type master;
    file "domain.com.zone";
    also-notify {A.B.C.D;};
};
```

Replace the A.B.C.D with the IP address of the GestióIP server.

Reload the DNS server to apply the configuration change.

12.1.3 PowerDNS installation

Install PowerDNS (pdns) with MySQL backend with your Linux distribution specific packet manager.

Ubuntu:

```
sudo apt-get install pdns-server pdns-backend-mysql
```

Suse:

```
sudo zypper install pdns pdns-backend-mysql
```

Redhat:

```
sudo yum install pdns pdns-backend-mysql
```

12.1.3.1 Create the MySQL database “pdns”

Create a new Mysql database as backend for the Powerdns nameserver.

Access to the MySQL.

```
$ mysql -u root -p
```

Create the pdns database.

```
mysql> CREATE DATABASE pdns;
```

Create a user for the pdns database (here “pdns_admin”).

```
mysql> CREATE USER 'pdns_admin'@'localhost' IDENTIFIED BY 'new_pdns_admin_password';
```

```
mysql> GRANT ALL PRIVILEGES ON pdns.* TO 'pdns_admin'@'localhost';
```

```
mysql> FLUSH PRIVILEGES;
```

Change to the new created database “pdns”.

```
mysql> use pdns;
```

Copy the following lines and paste them into the MySQL terminal to create the required tables:

```
CREATE TABLE domains (
  id                INT AUTO_INCREMENT,
  name              VARCHAR(255) NOT NULL,
  master            VARCHAR(128) DEFAULT NULL,
  last_check        INT DEFAULT NULL,
  type              VARCHAR(6) NOT NULL,
  notified_serial    INT DEFAULT NULL,
  account           VARCHAR(40) DEFAULT NULL,
  PRIMARY KEY (id)
) Engine=InnoDB;
```

```
CREATE UNIQUE INDEX name_index ON domains(name);
```

```
CREATE TABLE records (
  id                INT AUTO_INCREMENT,
  domain_id         INT DEFAULT NULL,
  name              VARCHAR(255) DEFAULT NULL,
  type              VARCHAR(10) DEFAULT NULL,
  content           TEXT(64000) DEFAULT NULL,
  ttl               INT DEFAULT NULL,
  prio              INT DEFAULT NULL,
  change_date       INT DEFAULT NULL,
  disabled          TINYINT(1) DEFAULT 0,
  ordername         VARCHAR(255) BINARY DEFAULT NULL,
  auth              TINYINT(1) DEFAULT 1,
  PRIMARY KEY (id)
```

```

) Engine=InnoDB;

CREATE INDEX nametype_index ON records(name,type);
CREATE INDEX domain_id ON records(domain_id);
CREATE INDEX recordorder ON records (domain_id, ordername);


CREATE TABLE supermasters (
    ip                VARCHAR(64) NOT NULL,
    nameserver        VARCHAR(255) NOT NULL,
    account            VARCHAR(40) NOT NULL,
    PRIMARY KEY (ip, nameserver)
) Engine=InnoDB;


CREATE TABLE comments (
    id                INT AUTO_INCREMENT,
    domain_id         INT NOT NULL,
    name              VARCHAR(255) NOT NULL,
    type              VARCHAR(10) NOT NULL,
    modified_at       INT NOT NULL,
    account            VARCHAR(40) NOT NULL,
    comment            TEXT(64000) NOT NULL,
    PRIMARY KEY (id)
) Engine=InnoDB;

CREATE INDEX comments_domain_id_idx ON comments (domain_id);
CREATE INDEX comments_name_type_idx ON comments (name, type);
CREATE INDEX comments_order_idx ON comments (domain_id, modified_at);


CREATE TABLE domainmetadata (
    id                INT AUTO_INCREMENT,
    domain_id         INT NOT NULL,
    kind              VARCHAR(32),
    content            TEXT,
    PRIMARY KEY (id)
) Engine=InnoDB;

CREATE INDEX domainmetadata_idx ON domainmetadata (domain_id, kind);


CREATE TABLE cryptokeys (
    id                INT AUTO_INCREMENT,
    domain_id         INT NOT NULL,
    flags             INT NOT NULL,
    active            BOOL,
    content            TEXT,
    PRIMARY KEY(id)
) Engine=InnoDB;

CREATE INDEX domainidindex ON cryptokeys(domain_id);


CREATE TABLE tsigkeys (
    id                INT AUTO_INCREMENT,
    name              VARCHAR(255),

```

```

    algorithm          VARCHAR(50),
    secret             VARCHAR(255),
    PRIMARY KEY (id)
) Engine=InnoDB;

CREATE UNIQUE INDEX namealgoindex ON tsigkeys(name, algorithm);

```

Exit from the MySQL database.

```
mysql> quit;
```

12.1.3.2 PowerDNS configuration

Debian/Ubuntu

Open the file `/etc/powerdns/pdns.conf` with an editor and add the lines “`launch=gmysql`” and “`slave=yes`”.

```

#####
# launch      Which backends to launch and order to query them in
#
# launch=
launch=gmysql

#####
...

#####
# slave Act as a slave
#
# slave=no
slave=yes

#####

```

Rename all files in `/etc/powerdns/pdns.d/` to filename.*orig*.

For example

```

$ cd /etc/powerdns/pdns.d/
$ ls
pdns.local.sqlite3.conf

$ sudo mv pdns.local.sqlite3.conf pdns.local.sqlite3.conf.orig

```

Open or create the file `/etc/powerdns/pdns.d/pdns.local.gmysql.conf` with the following content. Use the username (pdns-admin) and the password which you created during the installation of the pdns MySQL database.

```
gmysql-host=127.0.0.1
gmysql-user=pdns_admin
gmysql-dbname=pdns
gmysql-password=new_pdns_admin_password
```

Restart the PowerDNS server

```
$ sudo service pdns restart
```

Check the status of pdns

```
$ sudo service pdns status
```

Suse

Open the file `/etc/pdns/pdns.conf` and replace the whole content with the following lines. Use the username and the password which you created during the installation of the pdns MySQL database.

```
launch=gmysql
slave=yes
gmysql-host=127.0.0.1
gmysql-user=pdns_admin
gmysql-dbname=pdns
gmysql-password=new_pdns_admin_password
```

Restart you PowerDNS server

```
$ sudo service pdns restart
```

Check the status of pdns

```
$ sudo service pdns status
```

Fedora/Redhat/Centos

Open the file `/etc/pdns/pdns.conf` and replace the whole content with the following lines. Use the username and the password which you created during the installation of the pdns MySQL database.

```
launch=gmysql
slave=yes
gmysql-host=127.0.0.1
gmysql-user=pdns_admin
gmysql-dbname=pdns
gmysql-password=new_pdns_admin_password
```


Restart you PowerDNS server

```
$ sudo service pdns restart
```

Check the status of pdns

```
$ sudo service pdns status
```

If pdns is not running, disable SELinux temporally

```
$ sudo setenforce 0
```

and restart the PowerDNS server.

12.1.3.2.1 Create the PowerDNS slave zones

Create the DNS slave zones which the tool “pdnsutil”.

(replace mydomain.net with your forward zone name and the IP 192.168.100.50 with the IP of the master DNS server)

Create a forward zone:

```
$ sudo pdnsutil create-slave-zone mydomain.net 192.168.100.50
```

Create a reverse zone

```
$ sudo pdnsutil create-slave-zone 1.168.192.in-addr.arpa 192.168.100.50
```

Check if your zones where correctly created

```
$ sudo pdnsutil list-all-zones
mydomain.net.
1.168.192.in-addr.arpa.
All zonecount: 2
```

I you allowed zone transfers on the master server, the PowerDNS server should receive the zone records from the master DNS server.

List the records of the new zones (check if the synchronization with the master is working).

```
$ sudo pdnsutil list-zone mydomain.net.
mydomain.net.3600 IN NS pdc.mydomain.net.
mydomain.net.3600 IN SOA pdc.mydomain.net hostmaster.mydomain.net
5 900 600 86400 3600
test1.mydomain.net. 3600 IN A 192.168.1.1
test2.mydomain.net. 3600 IN A 192.168.1.2
```

Try “pndutil –help” to see all options.

12.1.3.3 Automatic synchronization between PowerDNS and GestióIP

To reflect changes in the DNS server, GestióIP needs to be synchronized periodically with the local PowerDNS server. The synchronization is made by the script `/usr/share/gestioip/bin/gip_pdns_sync.pl`. To enable the automatic synchronization create a cron job to run the script periodically and configure the connection parameter for the MySQL pdns database in the configuration file.

12.1.3.3.1 Create a cron job

Open the crontab for editing:

```
$ crontab -e
```

and add the following line to run the synchronization script every 10 minutes:

```
*/10 * * * * /usr/share/gestioip/bin/gip_pdns_sync.pl > /dev/null
2>&1
```

12.1.3.3.2 Configure the pdns database parameters

Open the configuration file `/usr/share/gestioip/etc/ip_update_gestioip.conf` and configure the GestióIP and pdns database parameters.

```
# MYSQL GestioIP
sid_gestioip=gestioip
user_gestioip=gestioip
pass_gestioip=hola123
bbdd_host_gestioip=localhost
bbdd_port_gestioip=3306

...

# MYSQL PowerDNS Configuration
# only necessary if you want to accept dynamic DNS updates to update the Gestioip DB.
# See the documentation how to setup dynamic DNS updates
sid_pdns=pdns
user_pdns=pdns_admin
pass_pdns=pdns_admin_password
bbdd_host_pdns=localhost
bbdd_port_pdns=3306
```

12.2 Dynamic updates from GestióIP to the master DNS servers

With automatic DNS updates from GestióIP to the DNS server enabled, changes of host entries in GestióIP (create/update hostname/delete) will automatically be notified to the corresponding master DNS server.

12.2.1 Microsoft DNS server as master server

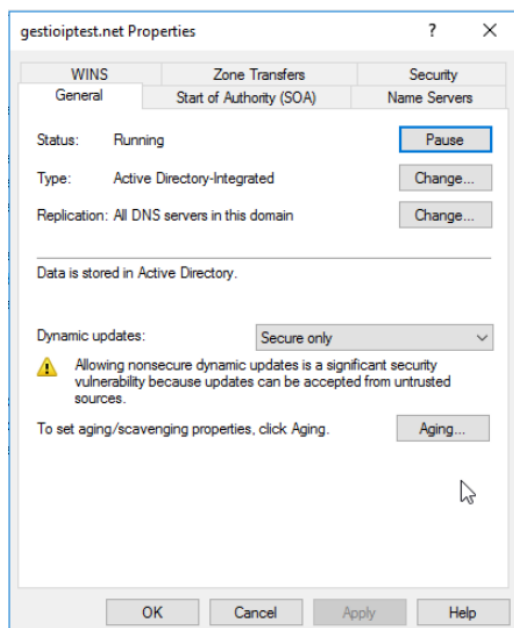
GestióIP supports secure dynamic GSS-TSIG DNS updates. The authentication is made by the Kerberos v5 authentication protocol. To enable secure dynamic updates one need to:

- install the KERBEROS client on the GestióIP server.
- create an account in your Active Directory.
- allow dynamic DNS updates on the DNS master server.

12.2.2 Create an Active Directory user

Create an user in your Active Directory (AD). This user will be used for the authentication of the dynamic DNS updates. In this example we created the user `gip_dyn_update@MYDOMAIN.LOCAL`.

12.2.3 Allow dynamic DNS updates



12.2.4 Installation of KERBEROS client tools

Install the KERBEROS client with your distribution specific packet manager.

Ubuntu:

```
sudo apt-get install krb5-user
```

Suse:

```
sudo zypper install krb5-client
```

Redhat:

```
sudo yum install krb5-workstation
```

12.2.4.1 KERBEROS client configuration

Open the file `/etc/krb5.conf` and replace the entire content with the following lines. Replace “MYDOMAIN.LOCAL” with the name of your Windows domain and “pdc.mydomain.net” with the DNS name of your primary domain controller (PDC).

```
[logging]
    kdc = FILE:/var/log/krb5/krb5kdc.log
    admin_server = FILE:/var/log/krb5/kadmind.log
    default = SYSLOG:NOTICE:DAEMON

[libdefaults]
```

```

default_realm = MYDOMAIN.LOCAL
dns_lookup_realm = true
dns_lookup_kdc = true
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true

[realms]
  MYDOMAIN.LOCAL = {
    default_domain = mydomain.local
    kdc = pdc.mydomain.net
    admin_server = pdc.mydomain.net
  }

[domain_realm]
  .mydomain.local = MYDOMAIN.LOCAL

```

12.2.4.2 Testing the KERBEROS authentication

Once you have configured the KERBEROS client and have created the AD user, check if it is possible to create a KERBEROS ticket:

From a terminal of the GestióIP server generate a KERBEROS ticket with the command “kinit”.

```

$ kinit gip_dyn_update@MYDOMAIN.LOCAL
Password for gip_dyn_update@MYDOMAIN.LOCAL:
$

```

Check with “klist” if the ticket was correctly created.

```

$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: gip_dyn_update@MYDOMAIN.LOCAL

Valid starting    Expires          Service principal
26/03/18 07:48:11 26/03/18 17:48:11 krbtgt/MYDOMAIN.LOCAL@MYDOMAIN.LOCAL
    renew until 27/03/18 07:48:07
$

```

If the ticket was not created, check the log-files under /var/log/ for errors.

Important note:

The creation of the krb ticket requires that the Apache user is allowed to create the krb cache file in the /tmp directory. Make sure that the Apache variable “PrivatTmp” is set to “false”. You find the variable in the following files:

```

Debian/Ubuntu: /usr/lib/systemd/system/apache2.service
RH/CentOS: /usr/lib/systemd/system/httpd.service

```

If the variable is set to “true”, copy the file to /etc/systemd/system/, open the new file with an editor and change the value for PrivatTmp to “false” and save the file. Then restart the systemd (sudo systemctl daemon-reload) and restart the Apache web server.

12.2.5 BIND as master DNS server

Configure the BIND server to accept dynamic DNS updates from the GestióIP.

Here an example of a BIND configuration allowing dynamic updates using the key “mydomain.net”

```
key "mydomain.net" {
    algorithm hmac-md5;
    secret "qhDFTRtmxZ/ywbz7YUQcoFOFKSE9AMg30DjxEc20PGTmNxT1q6
PG8m20Fhqu4M7jD2MqrnjIu+eGWwBCwwTpsA==";
};

zone "mydomain.net" {
    type master;
    file "/var/lib/bind/mydomain.net";
    allow-update { key mydomain.net; };
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/var/lib/bind/1.168.192.in-addr.arpa";
    allow-update { key mydomain.net; };
};
```

Go to 12.3.3 to see how to create a TSIG key.

12.3 Configuration of the GestióIP server

12.3.1 Enable support for dynamic DNS updates

manage > manage GestióIP > set “Dynamic DNS update enabled” to “yes” > click “set”
Click over any link to make the new menu items appear (for example, click over “show networks”).

Once dynamic DNS updates are enabled there appear the new items “DNS zones”, “DNS

keys” and “DNS update user” under the “manage” menu.

12.3.2 Create a “DNS update user” for GSS-TSIG authentication

This is the user which is used to authenticate with the AD (the user you created in your AD).

manage > DNS update user > add User

12.3.3 Create a “DNS key” for TSIG authentication (BIND)

This is the key which is used to authenticate with the BIND server.

You can use the command “dnssec-keygen” to create TSIG keys.

The following command will generate the two files Kmyzone.com.+157+54936.key and Kmyzone.com.+157+54936.private, containing the privat and the public key.

```
dnssec-keygen -r /dev/urandom -a HMAC-MD5 -b 512 -n HOST myzone.com
```

Check the dnssec-keygen documentation for further details about creating TSIG keys.

Use the privat key to configure the BIND server and the public key as “TSIG key” in GestióIP.

manage > DNS keys > add

network search ▾ networks VLANs sites lines AS CM ▾ import/export ▾ manage ▾ help ▾ ↗

Add TSIG key

Name

TSIG key

description

add

12.3.4 Create a DNS zone

manage > DNS zones > add zone

network search ▾ networks VLANs sites lines AS CM ▾ import/export ▾ manage ▾ help ▾ ↗

Create DNS zone

Name

Server type

DNS update user

type

DNS server

tll

description

send

Name: the name of your zone. Must be the same name as defined in the DNS master server and which you created with the pdnsutil tool before.

Server Type: choose DSS-TSIG for MS server and TSIG for BIND

DNS update user: the user which you created in your AD (server type DSS-TSIG)

TSIG key: the key which is used to authenticate the GestióIP server with the BIND server (server type TSIG)

type: A for IPv4, AAAA for IPv6 zones or PTR for reverse zones.

DNS server: coma separated list of the master DNS servers for this zone. To this servers, GestióIP will send and receive updates.

tll: time to live for the entries of this zone

12.3.5 Add the custom columns “DNSZone” and “DNSPTRZone” to the registered network columns.

manage > custom columns > Insert predefined network column >

select “DNSZone” > click add

select “DNSPTRZone” > click add

The screenshot shows the 'manage custom columns' interface. On the left, under 'Network columns', the 'insert predefined column' section has a dropdown menu open showing options: Fav, ifDescr, ifAlias, local, and DNSPTRZone (highlighted). Below this is an 'add' button and a 'type' dropdown set to 'text'. On the right, under 'Host columns', the 'insert predefined column' section has a dropdown menu open showing 'contact'. Below this is an 'add' button and a 'type' dropdown set to 'text'.

After adding the new columns, they will appear within the network-list-view.

12.3.6 Configuring networks for the dynamic DNS updates.

After enable dynamic DNS updates and adding the custom network column “DNSZone”, there appear the new form fields “DNSZone” and “DNS update mode” within the network-edit-form.

From network-list-view click over the network and click the edit-symbol on the right above.

The screenshot shows the 'change network' form. At the top, there's a 'show networks' button and a 'client' dropdown set to 'DEFAULT'. Below this is a table with columns: network, BM, description, site, category, comment, and sync. The first row shows network 192.168.1.0, BM 24, description, site Lon1, category corp, comment, and a checked sync checkbox. Below the table is a section for 'custom columns' with two rows: DNSZone (gestioip-test1.net) and DNSPTRZone (1.168.192.in-addr.arpa). Below this is a section for 'Secure Dynamic DNS update' with a 'DNS update mode' dropdown set to 'update A and PTR records'. At the bottom is a 'change' button.

DNSZone: select the zone the network is associated to.

DNSPTRZone: select the reverse zone the network is associated to.

DNS update mode:

- no dynamic updates – no dynamic DNS updates for this network
- update A and PTR records – update DNS A and PTR records for this network
- update A records only – only update the A records
- update PTR records only – only update the the PTR records for this network

Note: The “DNS update mode” field appears also within the host-edit-form. This allows to overwrite the networks setting for individual hosts.

12.3.7 Test the dynamic updates from the GestióIP to the master DNS server

To check if changes in GestióIP are correctly passed to the master DNS server, create a new host entry in the network for which you configured the DNS zone. Then execute a DNS query for the IP and the hostname you just changed to check if the DNS server responses with the new record.

If there occurs any problem during the dynamic DNS update, enable debug mode and check the messages in `/usr/share/gestioip/var/log/make_update.log`. For GestióIP version `<= 3.5.5` you additionally need to enable debugging directly in the script by opening it with an editor and changing the variable “VERBOSE” to 1:

```
VERBOSE=1
```

12.3.8 Test the dynamic updates from the DNS master to the GestióIP server

To check if changes on the master DNS server are passed to the GestióIP server, open the “DNS manger” on the DNS server and create a new A or AAAA record. It may take some minutes till the changes on the DNS server are visible in GestióIP (depending on the frequency with which you execute the synchronization script `gip_pdns_sync.pl`). In GestióIP, click over the network for which the DNS record was created and check if the host entry was correctly created/updated.

13 General information

13.1 Backup

Don't forget to include GestióIP's database within your backup strategy.

To make a manual backup of GestióIP's database execute the following command:

```
$ mysqldump -u gestioip -p gestioip > backup_gestioip.sql
```

To recover a backup made with “mysqldump” execute the following command:

```
$ mysql -u gestioip -p gestioip < backup_gestioip.sql
```

13.2 Firewall rules

GestióIP's Web-based, as well as the script based discovery and update functions are working with with DNS and SNMP queries plus ICMP echo requests (ping). That means that the nameservers must be accessible and that the target networks must be reachable with SNMP and ICMP from the host with the installation of GestióIP and the host where the update scripts (see Error: Reference source not found) are running (if not the same). All connections are initialized by GestióIP. That means that the following firewall rules are necessary to run GestióIP's update functions properly.

protocol	src address	src port	dest address	dest port
ICMP echo request (type 8)	GestióIP host	-	destination networks	-
UDP	GestióIP host	> 1023	destination networks	161
UDP	GestióIP host	> 1023	DNS servers	53
TCP (for zone transfers)	GestióIP host	> 1023	DNS servers	53
ICMP echo reply (type 0)	destination networks	-	GestióIP host	-
UDP	destination networks	161	GestióIP host	> 1023
UDP	DNS servers	> 1023	GestióIP host	53
TCP (for zone transfers)	DNS servers	> 1023	GestióIP host	53

13.3 JavaScript

GestióIP uses JavaScript. You have to enable JavaScript in your browser to use GestióIP.

13.4 Cookies

GestióIP uses the following cookies:

- GestiIPLang - to remember the last used language
- EntriesRedPorPage - to remember the last value of *entries/page* (network entries shown per page)
- scrollx and scrolly - to scroll to last position after manipulating host from “list”-view
- net_scrollx and net_scrolly - to scroll to last position after manipulating networks from “list”-view
- ShowRootNet – to decide of root-networks should be displayed
- ShowEndNet – to decide of end-networks should be displayed

14 Troubleshooting

In this chapter you find tips how to troubleshoot some common problems while running GestióIP. If this chapter doesn't help you to resolve a problem please visit the Help Forum (<http://sourceforge.net/projects/gestioip/forums/forum/981984>) or report the problem to contact@gestioip.net.

14.1 SNMP

Problem related con SNMP based discovery mechanisms are frequently caused by missing of required standard MIBs or a incorrect installation of Netdisco MIBs (required by SNMP::Info).

14.1.1 General SNMP problems

(1) snmpwalk

Run the command *snmpwalk* from a shell of the server with the GestióIP installation to check if the target machine is reachable and if the required standard MIBs (SNMPv2-MIB, IP-FORWARD-MIB, RFC1213-MIB) are correctly installed (MIBs are correctly installed if OIDs appear as string).

```
$ snmpwalk -v1 -c COMMUNITY IP_ADDRESS_TO_QUERY | head -10
```

```
SNMPv2-MIB::sysDescr.0 = STRING: Linux hostname 2.6.38-11-generic
#50-Ubuntu SMP Mon Sep 12 21:18:14 UTC 2011 i686
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (372953) 1:02:09.53
SNMPv2-MIB::sysContact.0 = STRING: Me <me@example.org>
SNMPv2-MIB::sysName.0 = STRING: hostname
SNMPv2-MIB::sysLocation.0 = STRING: Sitting on the Dock of the Bay
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORID.1 = OID:
SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
```

and not

```
.1.3.6.1.2.1.1.1.0 = STRING: Linux hostname 2.6.38-11-generic #50-Ubuntu
SMP Mon Sep 12 21:18:14 UTC 2011 i686
.1.3.6.1.2.1.1.2.0 = OID: .1.3.6.1.4.1.8072.3.2.10
.1.3.6.1.2.1.1.3.0 = Timeticks: (380424) 1:03:24.24
.1.3.6.1.2.1.1.4.0 = STRING: Me <me@example.org>
.1.3.6.1.2.1.1.5.0 = STRING: hostname
.1.3.6.1.2.1.1.6.0 = STRING: Sitting on the Dock of the Bay
.1.3.6.1.2.1.1.7.0 = INTEGER: 72
.1.3.6.1.2.1.1.8.0 = Timeticks: (1) 0:00:00.01
.1.3.6.1.2.1.1.9.1.2.1 = OID: .1.3.6.1.6.3.10.3.1.1
.1.3.6.1.2.1.1.9.1.2.2 = OID: .1.3.6.1.6.3.11.3.1.1
```

If OIDs appear numerically the required MIB files are missing. Install them to resolve the problem. E.g. Ubuntu:

```
$ sudo apt-get install snmp-mibs-downloader
$ sudo download-mibs
```

Execute the `snmpwalk` command from above again. If the OIDs still appear numerically open `/etc/snmp/snmp.conf` and comment out the line

```
#mibs :
```

Note

Error message “Unknown Object Identifier” is habitually caused by missing of required standard MIBs or a bad configuration of snmp client.

(2) Check dependencies

Execute the following script from a shell of the server with the GestióIP installation to check if the dependencies are complied:

http://www.gestioip.net/files/gestioip_snmp_test.tar.gz

Please configure a device and the community directly in the script.

14.1.2 Problems with VLAN discovery

VLAN discovery depends on the Perl module SNMP::Info. VLAN discovery only works with devices which are supported by SNMP::Info. Consult Netdisco (SNMP::Info) Device Compatibility Matrix to check if your device is supported

<https://github.com/42wim/snmp-info/blob/master/DeviceMatrix.txt>

Note

Network discovery does not depend in SNMP::Info. SNMP::Info is only required for VLAN discovery and partially for the host discovery via SNMP.

14.1.3 Problems with network discovery

A fail of the network import via SNMP may be caused by missing MIB files (see 14.1.1) or because the device does not support the required OIDs.

IPv4 based network import depends on either the OIDs *ipCidrRouteDest*, *ipCidrRouteMask*, *ipCidrRouteProto* or the OIDs *ipRouteDest*, *ipRouteMask*, *ipRouteProto*.

IPv6 based network import depends on either the OID *inetCidrRouteProto* or the OID *ipv6RouteProtocol*.

You can check if the required OIDs are supported by your device by running the command `snmpwalk` (this may take some time):

```
$ snmpwalk -v1 -c COMMUNITY IP_ADDRESS_TO_QUERY | grep "inetCidrRouteProto"
...
IP-FORWARD-
MIB::inetCidrRouteProto.ipv6."fe:80:00:00:00:00:00:00:03:c4:df:f3:fe:95:ac:12".1
28.1.4.ipv6."00:00:00:00:00:00:00:00:00:00:00:00:00:00:00" = INTEGER:
local(2)
...
```

14.1.4 Log files

If there occurs a problem with GestióIP have a look at the Apache error log-files

Debian/Ubuntu: /var/log/apache2/

Redhat/CentOS: /var/log/httpd/

Suse: /var/log/apache2/

Enable the debug mode (manage > manage GestióIP) to see more log messages.

The discovery process write their log files to /usr/share/gestioip/var/log/.

14.2 Database

GestióIP comes with the script “gip_health_check.pl” which executes a couple of consistency checks for the Mysql database. Before you execute the script you need to configure the database parameters directly in the script. You find the script in the “script” directory of the GestióIP tar-ball. Open it with your favorite editor and configure SID, username, password and the IP of the host where the database is running.

```
#####
#### Change from here... ####
#####

my $sid_gestioip="gestioip"; # SID of the GestioIP Mysql database
my $user_gestioip="gestioip"; # GestioIP's database user
my $pass_gestioip ="xxxxxx"; # Password of GestioIP's database user
my $bbdd_host_gestioip="localhost"; # Hostname or IP where the GestioIP Mysql
database is running

#####
#### ... to here #####
#####
```

Save and close the script. To execute the script change to the “script” directory and execute the following command:

```
$ ./gip_health_check.pl
```

14.3 Uninstalling GestióIP

GestióIP does not dispose about an automatic deinstallation script. Deinstallation must be performed manually. GestióIP consists in CGI-files, the update scripts, the apache configuration and the Mysql database. To uninstall GestióIP remove this files, disable the Cron-jobs (if configured) and delete GestióIP's database.

Open a shell and execute the following commandos:

- Remove the CGI files:

```
$ sudo rm -r [DocumentRoot]/gestioip
```

(replace [DocumentRoot] with the DocumentRoot of your Apache web server)

- Disable the cronjobs.

- Remove the script files:

-

```
$ sudo rm -r /usr/share/gestioip
```

- Remove the apache configuration:

```
$ sudo rm APACHE_INCLUDE_DIR/gestioip.conf
```

(e.g. Ubuntu: rm /etc/apache/conf.d/gestioip.conf)

- Remove GestióIP's Apache user file

```
$ sudo rm APACHE_CONF_DIR/users-gestioip
```

(e.g. Ubuntu: rm /etc/users-gestioip)

- Delete GestióIP's Mysql database:

Login to mysql CLI:

```
$ mysql -u root -p
```

```
...
```

```
mysql> drop database gestioip;
```

```
mysql> exit;
```

15 Licence

GestióIP is free software. It is distributed under the GNU GENERAL PUBLIC LICENSE version 3 (GPLv3).

Appendix A

List of manufactures recognized by GestioIP's SNMP discovery mechanisms (displayed with icons in host-list-view)

3com, Accton, Actiontec, Adder, Adtran, Aerohive, Aficio, Allied, Alps, Altiga, Alvaco, Anitech, Apc, Apple, Arista, Arquimedes, Aruba, Asante, Astaro, Avaya, Avocent, Axis, Barracuda, Belair, Billion, Bluecoat, Broadcom, Brocade, Brother, Calix, Canon, Checkpoint, Cisco, Citrix, Cyberoam, Dell, Dialogic, Dlink, Dothill, Draytek, Eci, Edgewater, Eeye, Emc, Emerson, Enterasys, Epson, Ericsson, Extreme, Extricom, F5, Fluke, Force10, Fortinet, Foundry, Fujitsu, Gta, H3c, Heidelberg, Hitachi, Hp, Huawei, Ibm, Iboss, Imperva, Juniper, Kasda, Kemp, Kodak, Konica, Lancom, Lanier, Lanner, Lantronix, Lenovo, Lexmark, LG, Liebert, Lifesize, Linksys, Lucent-alcatel, Lucent, Macafee, Megaware, Meru, Microsemi, Microsoft, Mikrotik, Mitsubishi, Mobileiron, Motorola, Moxa, Multitech, Nec, Netapp, Netgear, Netsweeper, Nitro, Nokia, Nortel, Novell, Oce, Oki, Olivetti, Olympus, Optibase, Oracle, Ovislink, Packetfront, Paloalto, Panasonic, Passport, Patton, Peplink, Pica8, Polycom, Procurve, Proxim, Qnap, Radvision, Radware, Rapid7, Realtek, Redback, Reflex, Ricoh, Riverbed, Riverstone, Ruckus, Samsung, Savin, Seiko_infotec, Shinko, Siemens, Silverpeak, Sipix, Smc, Sonicwall, Sony, Sourcefire, Star, Stillsecure, Stonesoft, Storagetek, Sun, Supermicro, Symantec, Tallygenicom, Tandberg, Tenda, Thomson, Tippingpoint, Toplayer, Toshiba, Ubiquiti, Vegastream, Vidyo, Vmware, Vyatta, Watchguard, Websense, Westbase, Xante, Xerox, Xiro, Zebra, Zyxel

List of operation systems recognized by GestioIP's SNMP discovery mechanisms (displayed with icons)

AIX, ArchLinux, CentOS, Debian, Fedora, FreeBSD, FunToo, GenToo, JunOS, Linux, NetBSD, Netware, OpenBSD, Redhat, Slackware, Solaris, Suse, Ubuntu, Turbolinux, Unix, Windows