QUICK START

Table des matières

1 Getting Started with Streamcore

1.1 CONNECTING TO SGM SYSTEM

- The **SGM System** is the SGM hardware operating system, think of it as the main control center for all operations. When an SGM is delivered, its IP address must be configured before it can be used. There are 3 ways to open the configuration screen.

1.1.1 Connecting a screen, keyboard and mouse

- After start-up, an SGM display is in text mode: enter the login **sgmconf** to activate the graphic mode. Subsequently the SGMconf application automatically launches.

1.1.2 Connecting via a virtual SGM using VSphere 5.0 or above

- The type of vSGM you install depends on the number of sites and rules that you will use:

	• SGM Av	• SGM Bv	• SGM Cv
• CPU	• 2 * 2 Ghz	• 4 * 2 Ghz	• 8 * 2 Ghz
• RAM (Gb)	• 1	• 2	• 4
• HD	• 80 GB • 7200 rpm	• 120 GB • 10 000 rpm	• 200 GB • 15 000 rpm
• Max number of rules	• 750	• 3 000	• 10 000

- **Note:** You must have administrator privileges on VSphere to deploy an OVA.
- Launch VSphere client and select **Delploy OVF Template**.
- Use the browse button to select the source location and then click **Next**.
- Verify the template details for example the "Product", "Description" and "Download size", then click **Next**.
- Specify a machine name then click **Next**.
- Select a specific host to deploy the OVA file then click **Next**.
- Select where you want to store the VM files then click **Next**.
- Map the network vlan then click **Next**.
- Finalise the deployed by reading details and then clicking **Finish**.

- Launch the VM and the connect to the console using
    - Login: **sgm**
    - Password **sgm**
    - Connect as a **su** – password: **streamcore**
- Change default IP address using the following command:
    - /sbin/ifconfig eth0 <@IP> netmask <mask>
- Add a default gateway if needed:
    - Route add default gw <@gw> eth0

1.1.3 Connecting via the network interface

- It is possible to connect a computer directly to SGM's GigaEthernet interface using a crossover cable. This computer's network interface then has to be configured in the same sub-network as the SGM, and a Web browser has to be started up from the following URL address: **http://<@IP-SGM>/sgmconf.** The SGM is delivered within the following IP address range: 172.16.0.150/24 to 172.16.0.159/24.
- From the SGMConf welcome page, enter the login "**cli**" with the password "**cli**", then click on **System** to open the SGM configuration screen.
- After entering the IP address, network mask and default gateway, click **Apply**. All modifications are dynamically applied. The SGM can now connect to your company's network.

1.2 LOGIN AND LANGUAGES

1.2.1 Login

- The SGM is accessible from any computer on a network once the IP address has been configured and the server positioned on the LAN. To access a configured SGM:

1. Open a browser.
2. Enter the URL: **http://<@IP-SGM>/sgmconf/** in which **<@IP-SGM>** is the SGM IP address (the name attributed by the DNS can also be used). For example: **http://127.0.0.1:8120/sgmconf/**

-
- **Note:** By replacing "http" with "https" in the URL above, the connection between the browser and the SGM is secure.

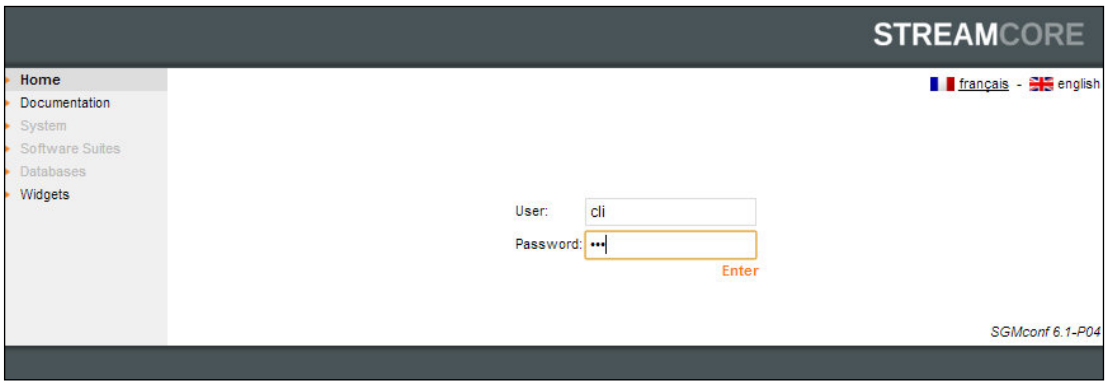
- 

Figure 1 – SGMconf Homepage

- There are two ways to use an SGM:

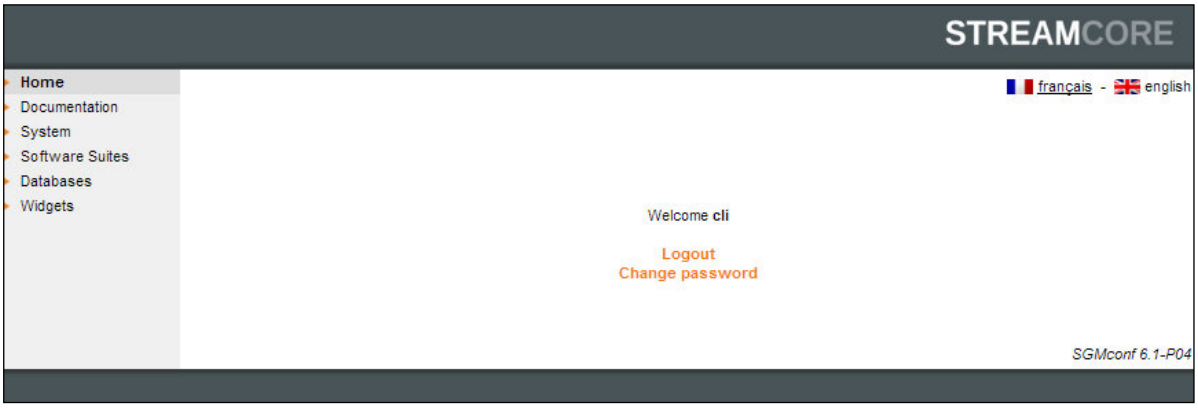
- **Anonymously:** access is given to consult documentation only, other actions cannot be accessed (menu options are greyed-out).
- **User and Password:** by identifying yourself using one of the user names stored in the application.
    - **cli** (default password **cli**). This user has unlimited (administrator) rights and has the ability to read all available documentation as well as perform any action.
- **Note:** User login credentials described above are related only to a SGMconf session and not to logins used for the StreamView, StreamReport, StreamDashboard, StreamAccess, and StreamMap applications.
- 

Figure 2 – Welcome Page after connecting as the user cli

- To change the "**cli**" password click the "change password" texted displayed on the welcome page.

Important: A new password must not contain the following characters: `' " <space> / ! \ [ ] * $`

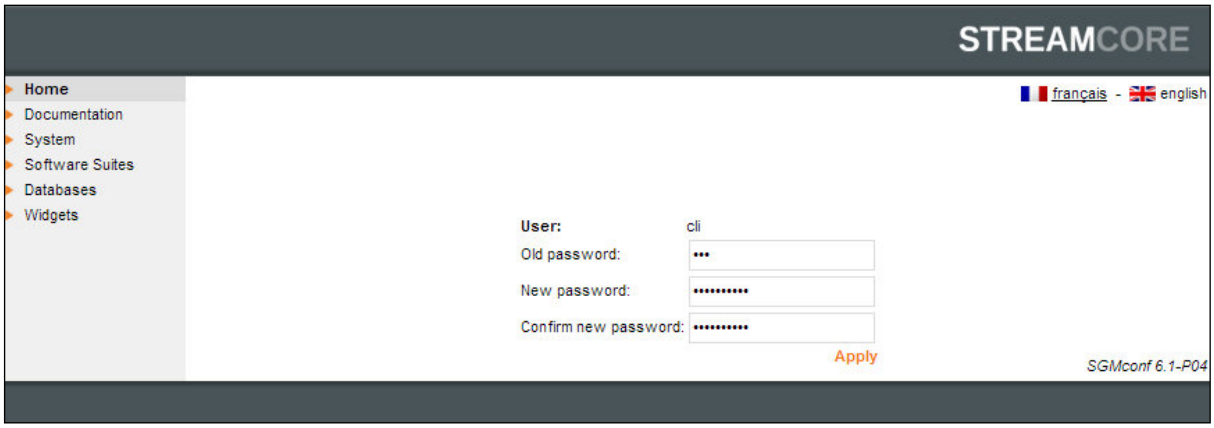


Figure 3 – Changing Password for User cli

1.2.2 Supported Interface Languages

- SGMconf supports 2 languages: English and French. To change to a language interface, click the flag icon displayed at the top right-hand corner of the homepage.
- It is also possible to add the option "**?LANG=fr or en**" to the current URL from any screen.
- For example:

http://172.16.100.1xx/sgmconf/local/?LANG=fr or ***http://172.16.100.1xx/sgmconf/local/?LANG=en***

1.3 SGM SYSTEM NETWORK CONFIGURATION

1 OVERVIEW

The functions offered, after selecting the **System** menu option, are used to:

- configure SGM server parameters
- manage alarms related to SGM performance
- customize SGM welcome page and logo
- access maintenance information
- manage licenses
- The SGM **System** network **Configuration** sub-tab is described below, however descriptions of the other sub-tabs (Configuration, Security, SNMP, SGM Backup, RADIUS, LDAP, and Time) can be found in the SGMConf Guide.

2 NETWORK CONFIGURATION SETTINGS

Go to **Parameters>Configuration** tab to view the SGM System network settings.

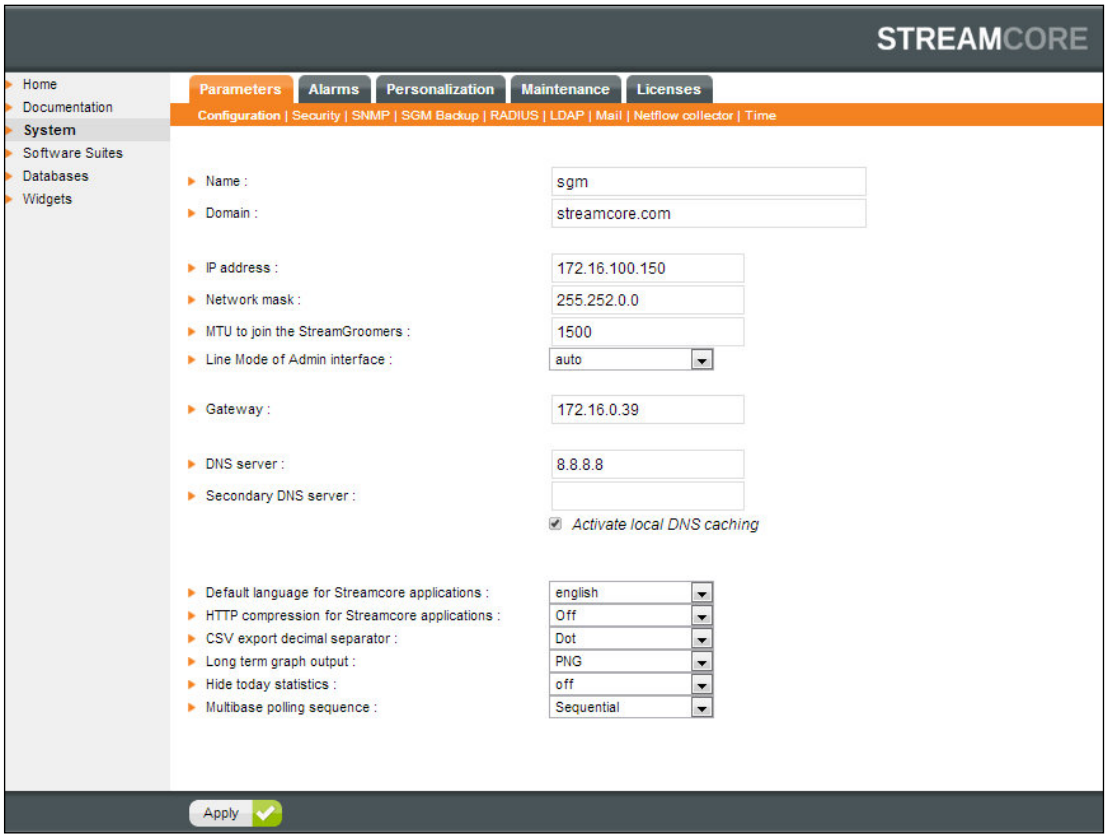


Figure 4 – SGM System Settings

The following options are displayed on the **Configuration** page:

Interface Label	Description
• Name	• The host name that identifies the SGM server ([1])
• Domain	• DNS domain name ([2])
• IP address	• Local IP address of SGM server
• Network mask	• Local IP mask identifying the local network
• MTU to join the StreamGroomers	• Smallest MTU on the WAN to join a StreamGroomer
• Line Mode of Ethernet Ports	• Mode and duplex of the SGM Ethernet Port
• Gateway	• Address identifying the default router
• DNS server	• Address identifying the DNS server (used by StreamView to display the names instead of IP addresses on some screens). By activating a local cache, you can speed up the DNS name translation.
• Secondary DNS server	• Backup DNS server
• Local DNS caching	• Activate a local caching of all DNS requests
• Default language	• Language used when the applications StreamView / StreamReport / StreamDashboard / StreamAccess / StreamMap are started.
• HTTP compression	• HTTP compression used or not automatically when the applications StreamView / StreamReport / StreamDashboard / StreamAccess are started.
• CSV export decimal separator	• Decimal separator used in CSV files generated by StreamView or StreamReport applications.
• Long term graph output	• Type of graph (Flash or PNG) generated by StreamView or StreamDashboard applications. Choose PNG for faster response or Flash to get information directly on the graph.
• Hide today statistics	• On a backup configuration, it displays or not the period: "day->today" in long-term graphs.

Click **Apply** after changing any of the above settings. All changes are dynamically applied.

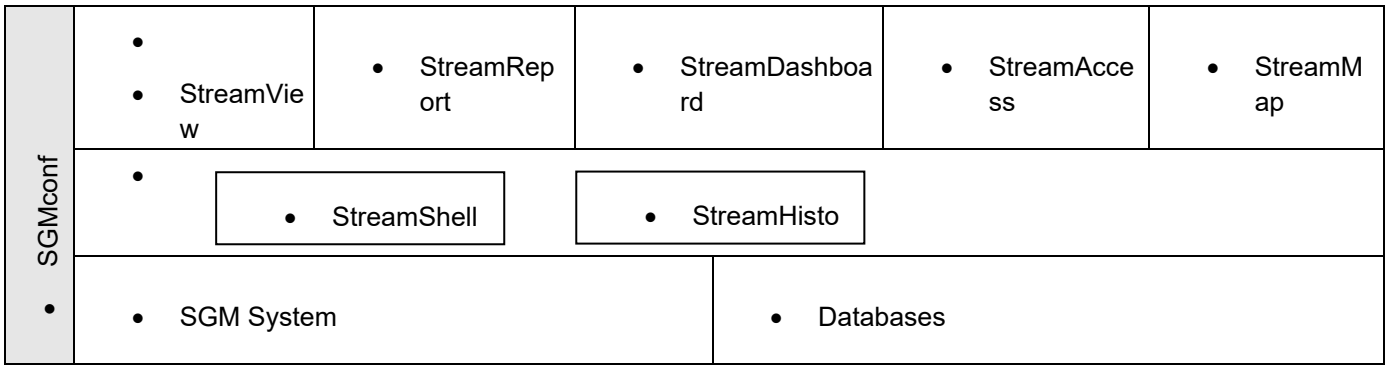
Note: When changing SGM IP settings, attention should be paid to the following points:
- [2]Remember to also change the IP address of the SGM in the StreamGroomers configurations.

([1]) The name must be made up of alphanumeric characters and start with a letter. The characters "_" and "-" are also authorized, unlike spaces (" ") or full stops (" . ")
([2]) Necessary in order to be able for the SGM to send requests to the DNS. The domain must be made up of alphanumeric characters and start with a letter. The characters "_", "-" and "."are also authorized, unlike spaces (" ")

- If the IP setting is changed remotely using another computer, it may become impossible to connect to the SGM: this is the case, for example, when the SGM is configured in a new sub-network.

1.4 WHAT IS THE STREAMGROOMER MANAGER (SGM)

- StreamGroomer Manager (SGM) is a specific hardware platform, which hosts the following software applications:
- **SGMconf:** SGM management application
- **SGM System:** SGM operating system
- **Databases:** coherent sets of data associated with one or several StreamGroomers
- **StreamShell:** command mode (cli) on which all the applications are interfaced
- **StreamHistory:** access module to long-term data and graph generation
- **StreamView:** configuration and supervision application in graphic mode
- **StreamReport:** application for editing PDF reports
- **StreamDashboard:** application for managing personalized Web dashboards
- **StreamAccess:** application for managing flexible access rights to the Web applications
- **StreamMap:** application for alarms and performance summary display in a geographic map
- Although this quick guide will not go into detail about the majority of applications mentioned above, we will be focused on **SGMconf, SGM System,** basic **Database** setup and **StreamView.**
-
- This software suite can be represented as follows:



-
- The SGM "Databases" groups' parameters and statistics associated with one or more StreamGroomers into a coherent whole. Management of these databases (i.e., creation, deletion, back up, and restoration) is handled through the SGMconf application.
- A database is used through the middleware (StreamShell, StreamHistory) by the applications (StreamView, StreamReport, StreamDashboard, StreamAccess and StreamMap) in order to configure and manage all Streamcore solution features.

1.5 MANAGING SOFTWARE SUITES AND THE SGMCONF VERSION

1.5.1 Overview

To view the list of software installed on the SGM Server click **Software Suites** from the display menu option. Displayed is a listed of installed packages with the following information:

- Software Suite Version
  - OPE version
  - USINE version
  - ACC version

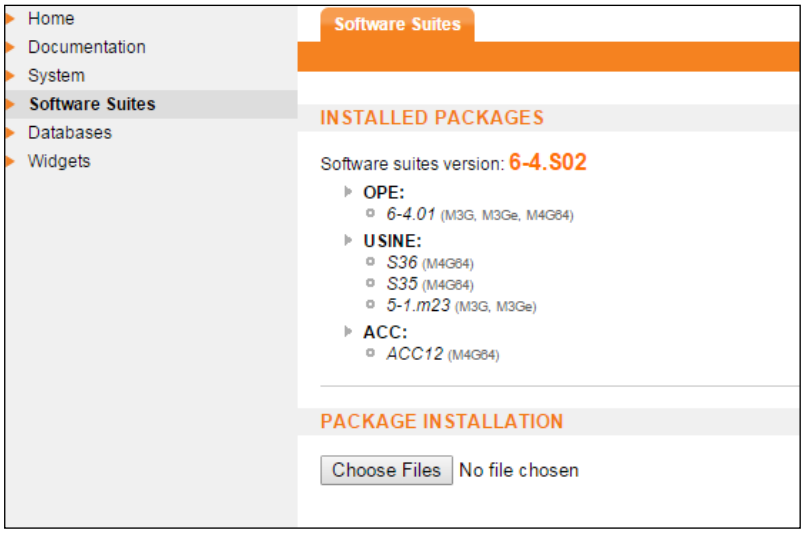


Figure 5 – Example of installed software suite

Important: It is not possible to downgrade from the installed ACCXX version. This software is automatically installed with the latest version of the Software Suite and therefore cannot be altered.

- **Note:** When you install an OPE on a SG, the SGM automatically deploys the appropriate BOOT version (Sxx) for the OPE. Therefore you do not have to be concerned that the boot version is not up to date.

Included in the software suite is:

- StreamGroomers embedded software:
  - OPE available for SGs
  - USINE (Boot software)
  - ACC (Acceleration software)
- SGM applications and middleware:
  - StreamView application
  - StreamReport application
  - StreamPortal application (StreamDashboard+StreamAccess)
  - StreamMap application
  - StreamSNMP middleware
  - StreamService middleware
  - StreamShell middleware
  - StreamHistory middleware

- StreamCollector middleware

- The **SGMconf** application
- Single **OPEs** for StreamGroomers
- All the **documentation** associated with a suite

If multiple software suites are installed on an SGM:

1. For each SGM application (as mentioned above) the most recently installed software version is used.
2. For StreamGroomer software, you choose the version to use on each StreamGroomer using the If several versions of SGMconf are present on the SGM, the most recently installed software version is used.

1.5.2 Installing Software

- Download the SCR file (using FTP or SCP) to the SGM repertory /var/tmp (or a sub directory)
- From the Package Installation section, select the Choose **File** button navigate to directory (/var/tmp for instance).

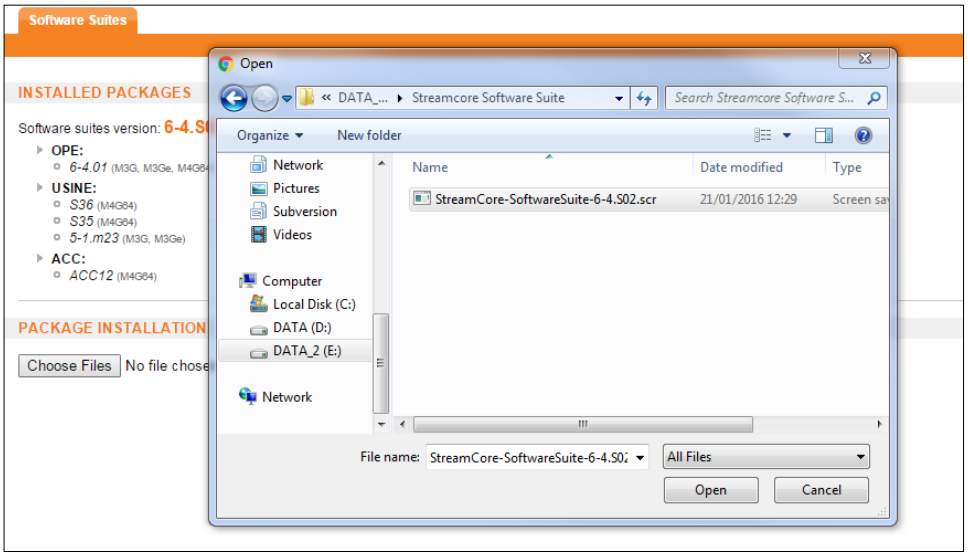


Figure 6 – Browsing for installation software

-
- Select the file and the contents of the file will automatically upload to display on the screen.

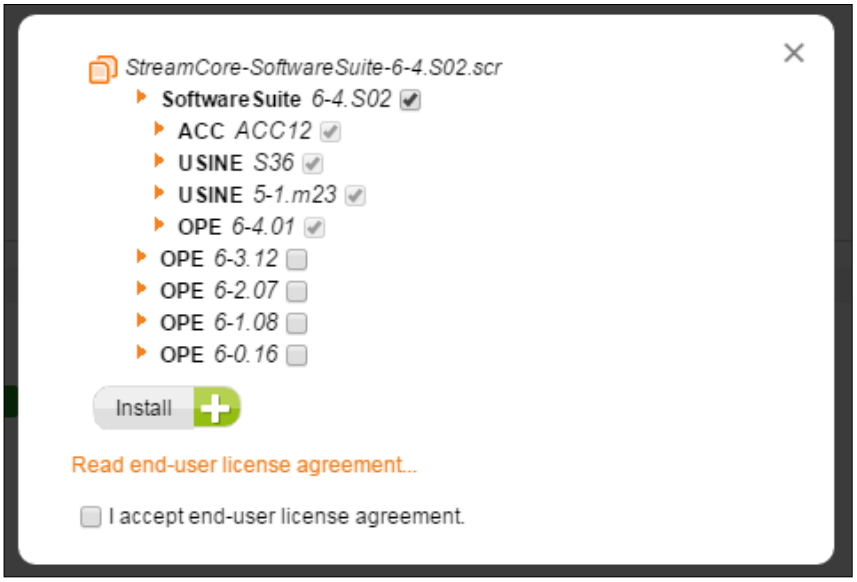


Figure 7 – Selecting software to install

- Select the individual components from the install list or check the Software Suite checkbox to install all suite components. If you select the Software Suite the items not part of the suite will be excluded. For example in Figure 7 only the latest OPE is included in the software suite.
- Read and accept to the end-user license to continue.
- Click the **Install** button to begin installation.

Note: If multiple software suites are installed on an SGM, it will not be possible to delete them individually (one by one). Ensure you delete all software suites (not the most recent SGMConf) before installing a new one. (cf §4.3.3.1)

- **OPE boot version:** When you install an OPE on a SG, the SGM automatically deploys the appropriate BOOT version (Sxx). This means you do not have be concerned that the boot version is not up to date.

2 StreamGroomer Deployment Architectures

2.1.1 Between a LAN and a Router

A StreamGroomer (SG) is usually deployed inline between the router and the LAN:

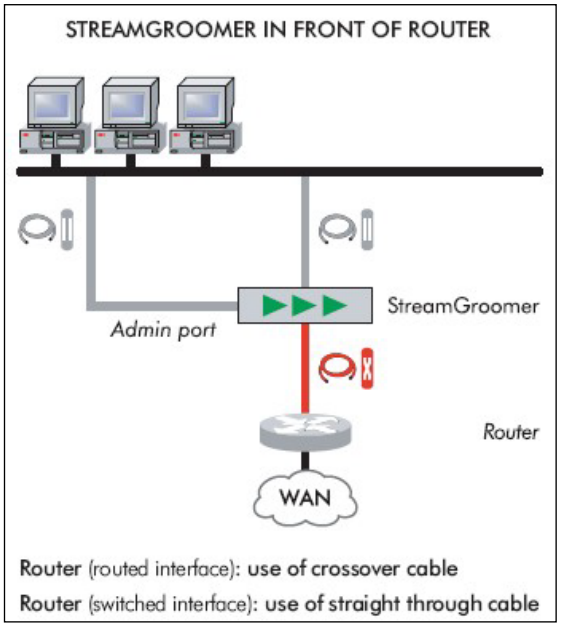


Figure 8 – StreamGroomer in front of router

- For StreamGroomer wiring consult individual SG Installation guide for detailed information.
- **Note:** When the equipment is turned on, check that the bypass LED is off. During installation, the StreamGroomer is in boot mode so the Bypass is **closed**: the flows go directly from one port to the other without being processed by the SG. The SG acts as a crossover cable.

2.1.2 Other Architectures

A SG can be transparently inserted in other types of architecture:

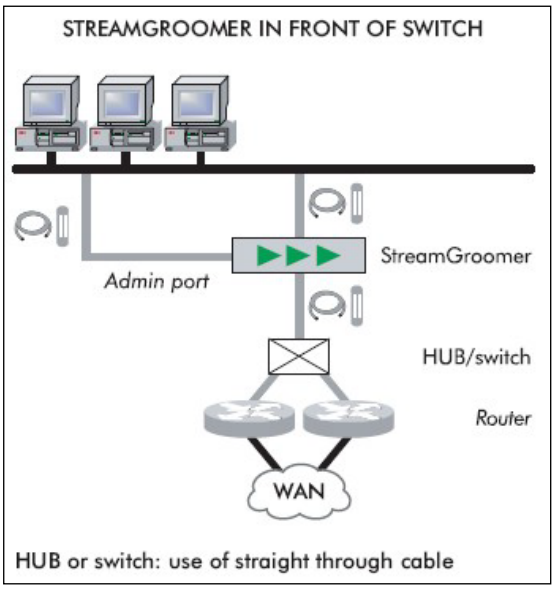


Figure 9 – StreamGroomer in front of switch

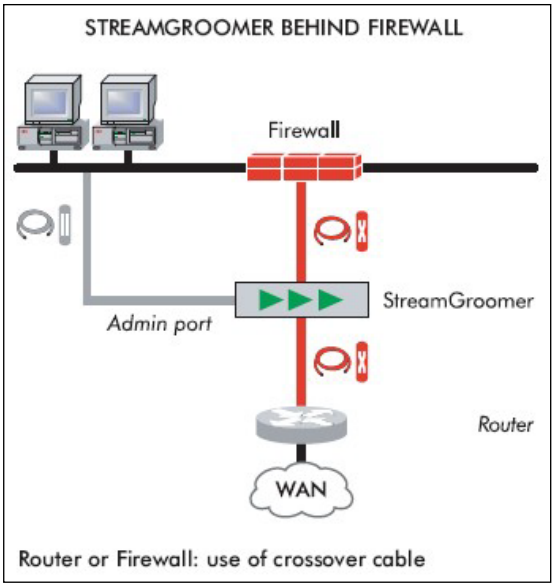


Figure 10 – StreamGroomer behind firewall

If there is a switch between the StreamGroomer and the router accessing the WAN, the crossover cable should be replaced with a straight-through cable; if the StreamGroomer is connected between two routers, or between a router and a firewall, 2 crossover cables should be used.

3 Initial StreamGroomer Configuration

- A StreamGroomer has the following embedded software:
- **Boot Software:** only the administration service is available (bypass is closed).
- **Operating (OPE) Software:** all services are available.
- The default active software on a StreamGroomer is the boot software. In order for the SGM to have access to the StreamGroomer, the boot parameters must be provisioned by one of the following methods:
- By asynchronous cable
- By USB key

3.1.1 Asynchronous Port Settings

- To access the BOOT menu, you have to connect to the StreamGroomer through the asynchronous port via a DB9 asynchronous cable. The most common utilities are HyperTerminal, Putty, SecureCRT or Teraterm for Windows.

3 GRAPHICAL MENU

- The graphical menu is available for the following StreamGroomers:
- SG250
- SG420
- SG800
- SG1600
- SG3200

4 OPENING A SESSION

- The terminal emulator configuration has to be done manually by entering the asynchronous port settings as follows:

1. Speed 38400 bit/*s*, no parity, 1 stop bit, 8 bits of data.
2. Delete key emulated by Backspace key, emulation of terminal VT100.
3. Terminal fonts.

-
- After a connection has been made. Press the Enter key and the following screen is displayed:

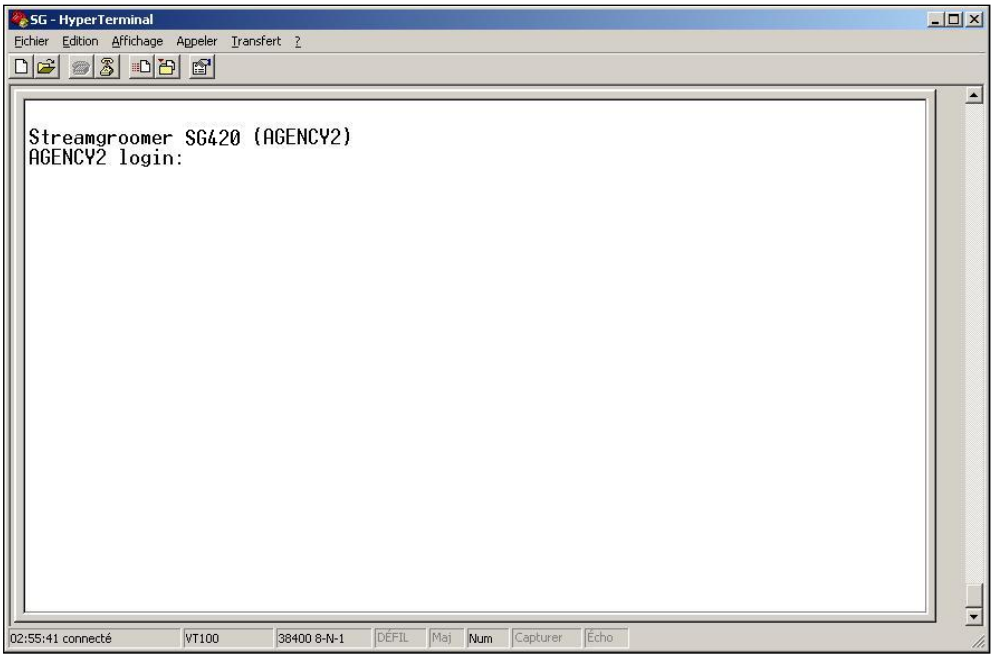


Figure 11 – Initial Login

- Enter the login: "**boot**".
- The configuration session is then opened and the **Main Menu** is displayed:

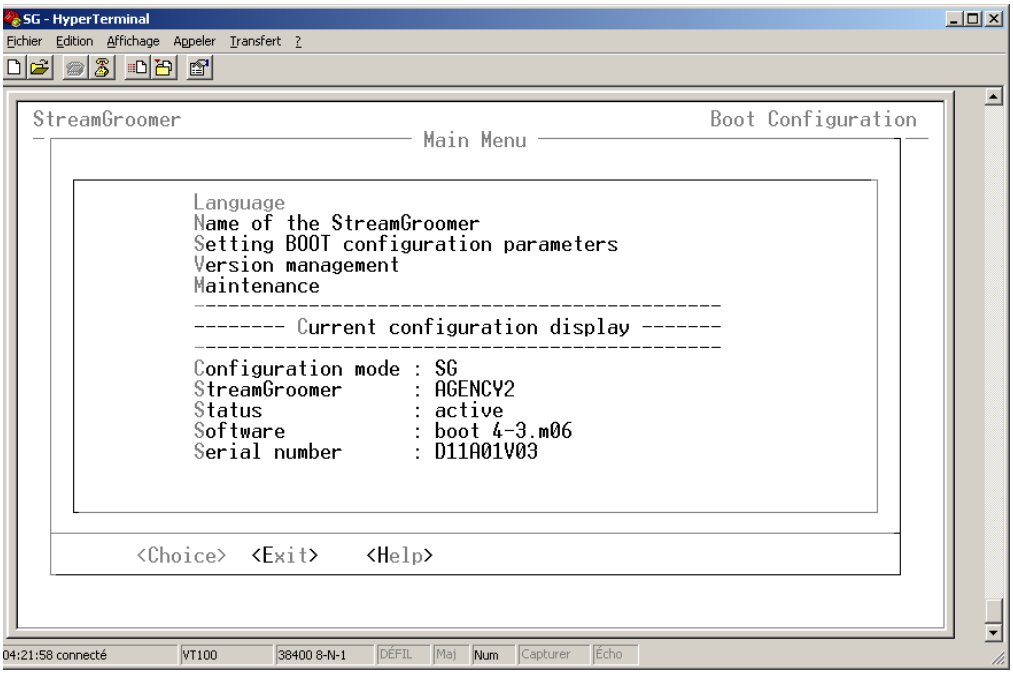


Figure 12 – Main Menu

-
- All the menus are similar to the main menu in term of navigation:
-

Cursor Key usage or command	Description
• ↑ and ↓	• Moves the cursor to the previous or next line. When the line is highlighted (or underlined), it indicates the current selection.
• ← and →	• Moves the cursor horizontally on the last line which, according to the menu, offers two or three options.
• OK	• Validates the data entries.
• Choice	• Validates the option selected.
• Help	• Displays a help message about the displayed screen.

-
- Screens that offer a multiple-choice list, you should:
- Place the cursor on the parameter required.
- Select **Choice** with the **Enter** key.
-
- In the main menu, place the cursor on **Setting BOOT configuration parameters**.
- Select Choice. The following screen appears:

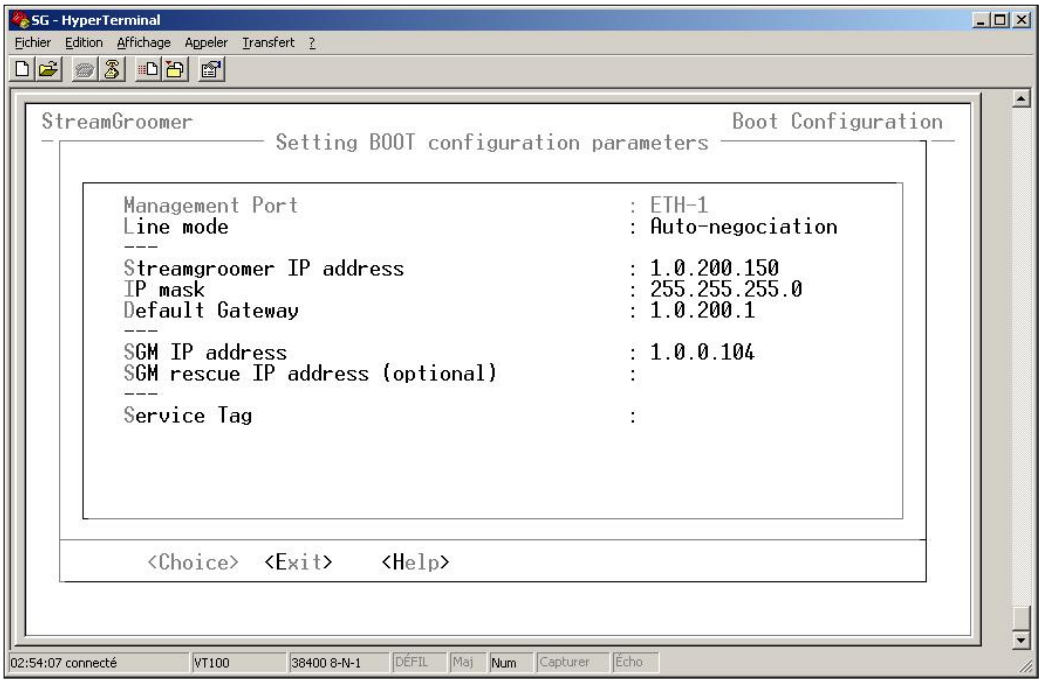


Figure 13 – Setting Boot Configuration Parameters

Menu Item	Description
• Management Port	• The administration port is configured on the Eth port for a SG wired with three ports.
• Line mode • < ETH-1 > port	• The Ethernet ports of the StreamGroomer can be adapted to half-duplex and full-duplex modes, and speeds of 10 / 100 / 1000 Mbit/s. • Recommendations on configuration: • - If the vis-à-vis is in auto-negotiation or half-duplex 10 Mbit/s mode, choose the auto-negotiation value. • - In other cases, force the same mode as on the vis-à-vis.
• StreamGroomer IP Address	• Defines the IP address at which the StreamGroomer is accessible.
• IP Mask	• Together with the IP address, it defines the IP network through which StreamGroomer should pass.
• Default Gateway	• Identifies the IP address of the gateway allowing you to contact the SGM from the SG.
• SGM IP Address	• IP address of the SGM server which administers the SG
• SGM Rescue IP Address	• IP address of the backup SGM server which administers the SG (optional)
• Service Tag	• Not used

- To ensure that the new configuration is taken into account, it is necessary to save it and restart the SG in boot mode.
- In the main menu, select **Version Management**. The following screen appears:

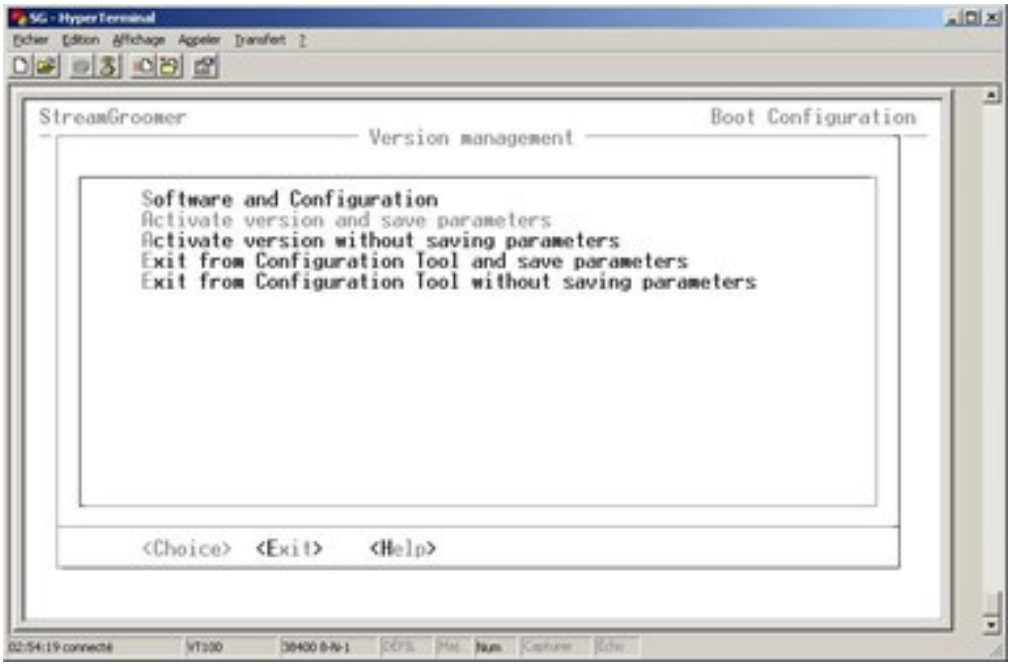


Figure 14 – Version Management

-
- Select **Activate version and save parameters**. You are then requested to confirm which software and configuration should be activated after the rebooting (taking into account any changes made in the previous menus).
- Press **Choice** to confirm activation of the equipment.

5 CLI MENU

- The CLI menu is used for the following StreamGroomers:
- SG250e
- SG350e and SG360e
- SG850e and SG860e
- SG1650e and SG1660e
- SG3200e, SG3250e and SG3260e
-
- Press **Enter** key. The following screen appears:

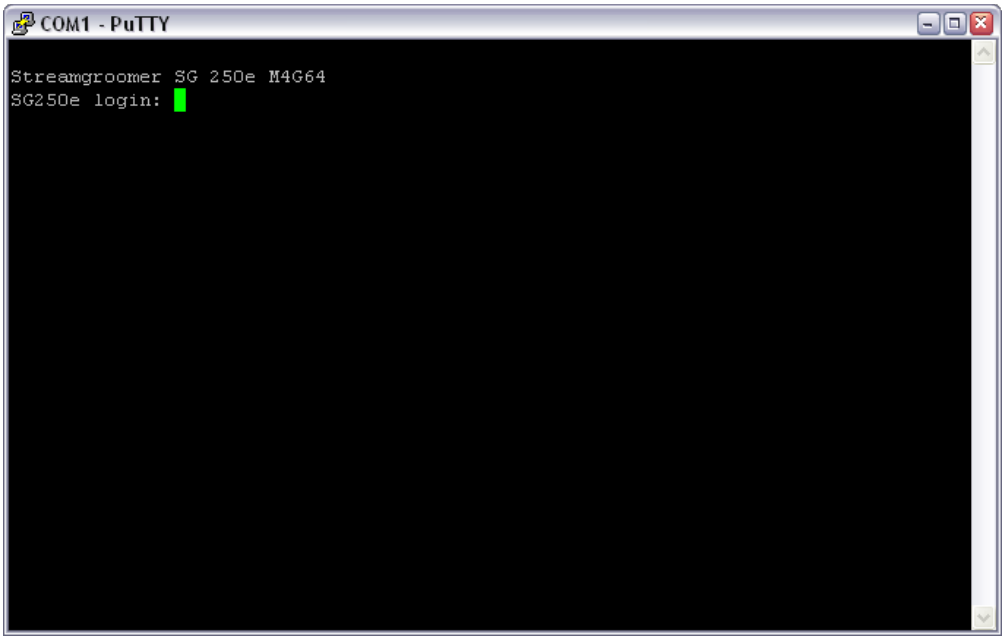


Figure 15 – CLI Menu Initial Login using PuTTY

-
- Enter user name (login): **boot** and a password: **boot**
- There are two levels are available in the Boot menu: **Maintenance menu** (default) and **Configuration menu.**

1. Enter the keyword **configure** to enter the Configuration menu.
2. Enter the following commands to configure the IP boot parameters (all commands can be completed with the tab key).

Configuration Commands	Description
• admin_address [IP_Add]	• Define the IP address at which the StreamGroomer is reachable
• admin_mask [IP_Add]	• Define the IP network through which the admin of the SreamGroomer should pass
• admin_gateway [Mask_Add]	• Identify the IP address of the gateway allowing you to contact the SGM from the SG
• admin_port_speed [speed]	• Choose the speed of the interface [100M-fd/100M-hd/10M-fd/10M-hd/1G-fd/auto]
• sgm_address [IP_Add]	• IP address of the SGM server which manages the SG

3. Enter **apply** to update the configuration with the pending changes
4. Enter **exit** to exit the configuration menu
5. Enter **show configuration** to check the updated configuration

- **Note:** A StreamGroomer restart is not required.
- For StreamGroomers with Web caching, it is also necessary to configure the following parameters:

Configuration Commands	Description
• dns_server1 [IP_Add]	• DNS server used by the SG (for admin purpose).
• dns_server2 [IP_Add]	• Second DNS server used by the SG in case the first one does not answer.
• dns_suffix1 [domain_name]	• DNS suffix for local DNS query
• dns_suffix2 [domain_name]	• Second DNS suffix for local DNS query

3.1.2 Boot parameters provisioning with a USB Key

- Boot parameters can be imported into a StreamGroomer by using a configuration file loaded on a USB key. The process is as follows:
-

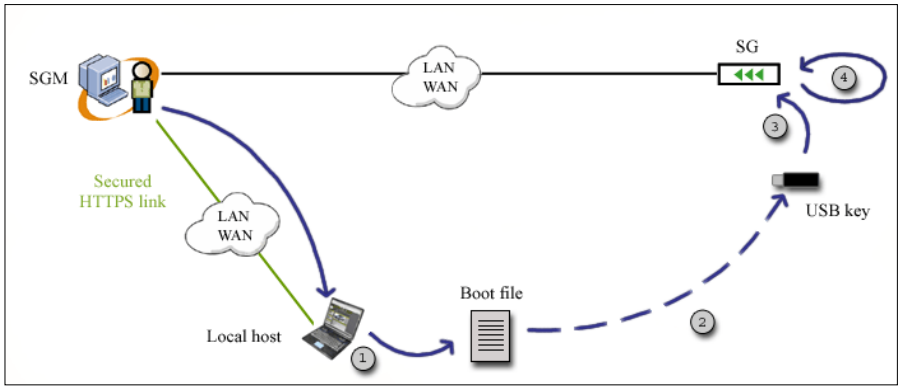


Figure 16 – USB boot flow

1. Click on **STREAMGROOMERS>xx** in the tree menu, on the **Parameters>Boot file** sub-tab. Then click on the **Download the boot file on the local computer** link. Download the boot file to a local PC.
2. Copy the boot file onto a USB key.
3. Insert the USB key into the StreamGroomer.
4. Power down and up. Wait for a few minutes till the StreamGroomer has booted entirely.
5. When the USB key is plugged in a StreamGroomer and it is rebooted, the following operations are automatically performed:

- USB key mount + USB key writing check
- Search for a sgconfig_<sgname>.txt file
- Security parameters checking (password, optional strong SSH authentication…)
- Boot file parameters import
- Status file push on the USB key

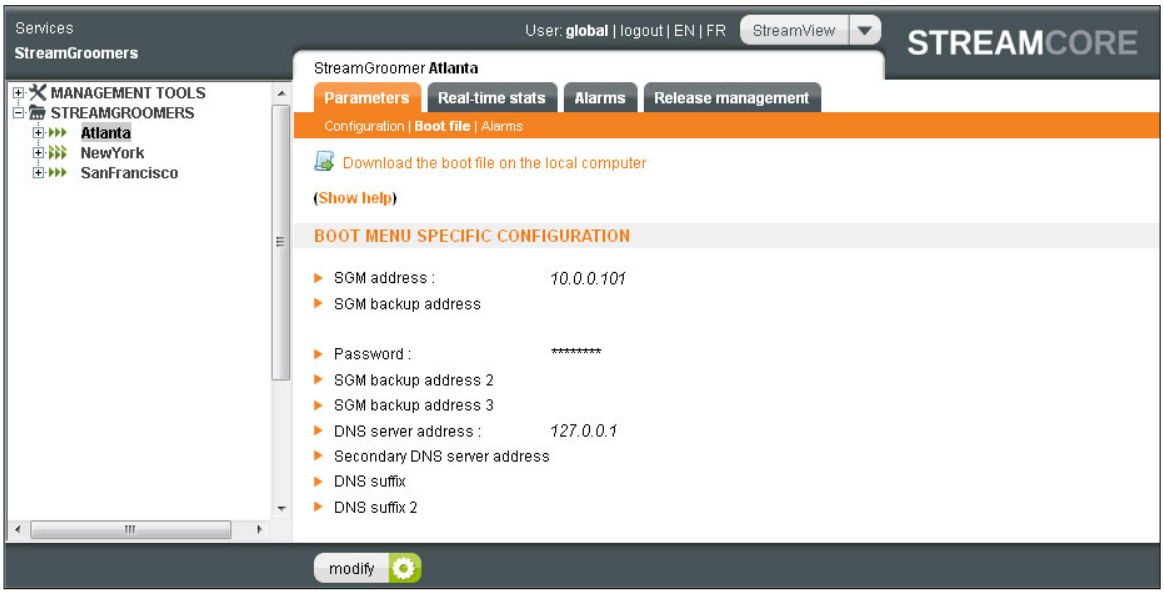


Figure 17 – Download a boot file

- A StreamGroomer will make different kinds of "beep" sounds at the end of these operations:

Beep	Event
• Double short high-pitched beep and then deep beep	• The 5 steps described above have been successful. A status file summarizing the configuration has been pushed on the USB key.
• Several short high-pitched beeps	• A strong SSH authentication has been required and the StreamGroomer is generating its pair of public/private RSA keys during step 4.
• Several long deep beeps	• Step 1 has failed (USB key mount)
• Single long deep beep	• Step 2, 3 or 4 has failed. • If step 2 has failed, then a *sgstatus_ERROR.txt* file is pushed on the key (for instance if the StreamGroomer has found several file starting with sgconfig). • If step 3 or 4 has failed, then a *sgstatus_<sgname>.txt* is pushed on the key and contains a message explaining the failure.

6. Remove the USB key and check the *sgstatus_<sgname>.txt* file.

- **Important:** If a file named ***sgstatus_<sgname>.txt*** is present on the USB key, the configuration file will not be taken into account.
- **Note:** (Optional) The boot password can be defined and changed before downloading the boot file. Additional boot parameters can be defined as well.

Note: In case SSH administration with strong authentication is enabled, then the last step is to import the SG public-key into the SGM.

- After approximately two minutes, the StreamGroomer should be reachable by the SGM (assuming its administration port is plugged on the network).

4 Site Management

4.1 STEP 1: CREATE A DATABASE

After setting up and configuring the **SGM System** (Operating System) you can now proceed to setup **Sites** and their associated **StreamGroomers (SG)**. However in order to do this, you need to create a database using **SGMConf** (SGM management application).

You will then be able to access StreamView via your newly created database to start the Site and StreamGroomer provisioning process.

Database creation is a straight forward process, however a database name construct must abide by the following rules:

- It must be unique on the SGM server (a test to check that it is unique is carried out).
- It must be exclusively made-up of alphanumeric, lower-class characters and start with a letter.

1. Select **Databases>Create** tab, the following screen is displayed:

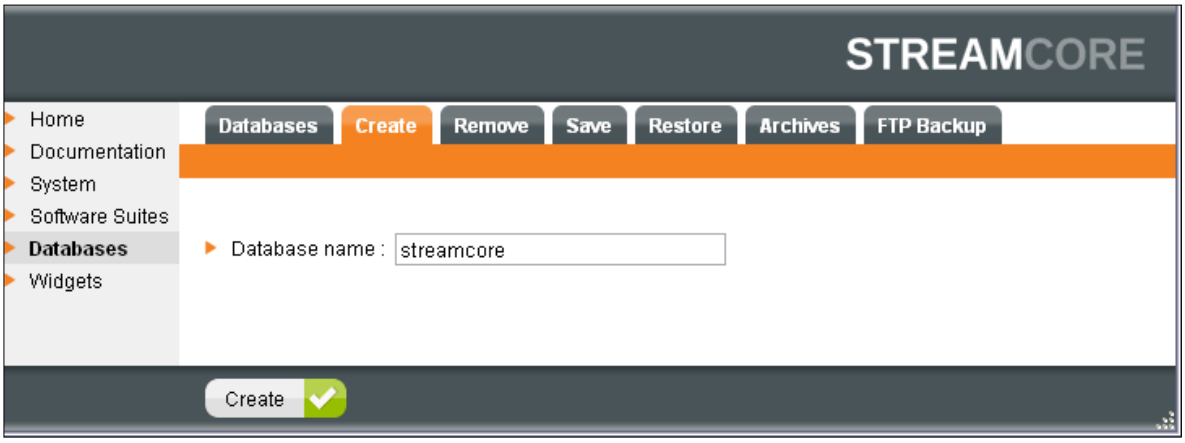


Figure 18 – Create Database Tab

2. Enter a unique name following the rules as described above.
3. Click on **Create** to create the database.

Figure 19 –The result of a successful database creation

-

- **Note:** For further information regarding **Remove, Save, Restore** and other features, see the SGMconf User Guide.

4.2 STEP 2: LOGIN TO DATABASE

- After creating your database you can access it and start provisioning Sites and SGs via the StreamView application.
- A database can be logged into via the following methods:
-

1. **Direct Access:** http://<@IP-SGM>/streamview/<database_name>/

- **<@IP-SGM>:** the SGM IP address (the name assigned by DNS can also be used)
- **<database_name>:** database name, as defined when it was created with the SGMconf application
- Access via the Welcome Screen: `http://<@IP-SGM>/`
- **<@IP-SGM>:** the SGM IP address (the name assigned by DNS can also be used).
- The SGM welcome page then presents links for launching various applications. To access a database click a displayed database name.

- **Note:** To provide a secure connection between a browser and an SGM replace "http" with "https".

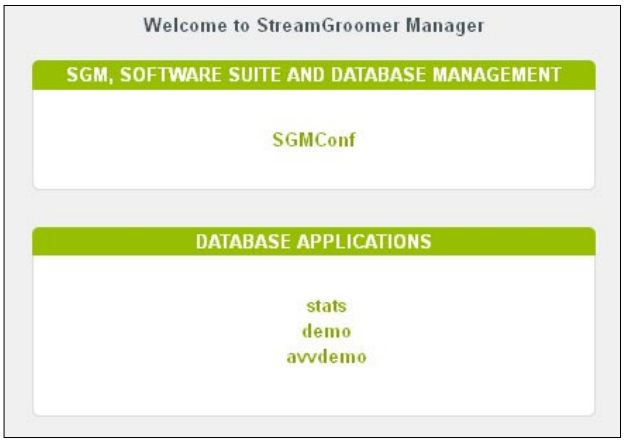


Figure 20 – Access via the SGM welcome screen

-

2. From the welcome screen, enter your user name and password. If you have created a new database and accessing it for the first time, use the user name **global** and no password.

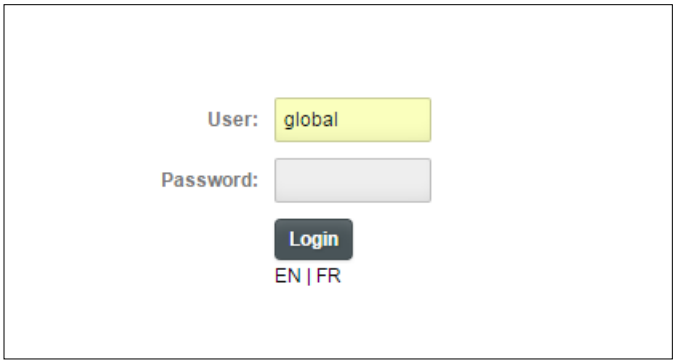


Figure 21 – First time login to newly created database

- **Note:** The default language for all Streamcore applications can be set via the SGMconf application.

- The diagram below outlines the various sections displayed in StreamView.

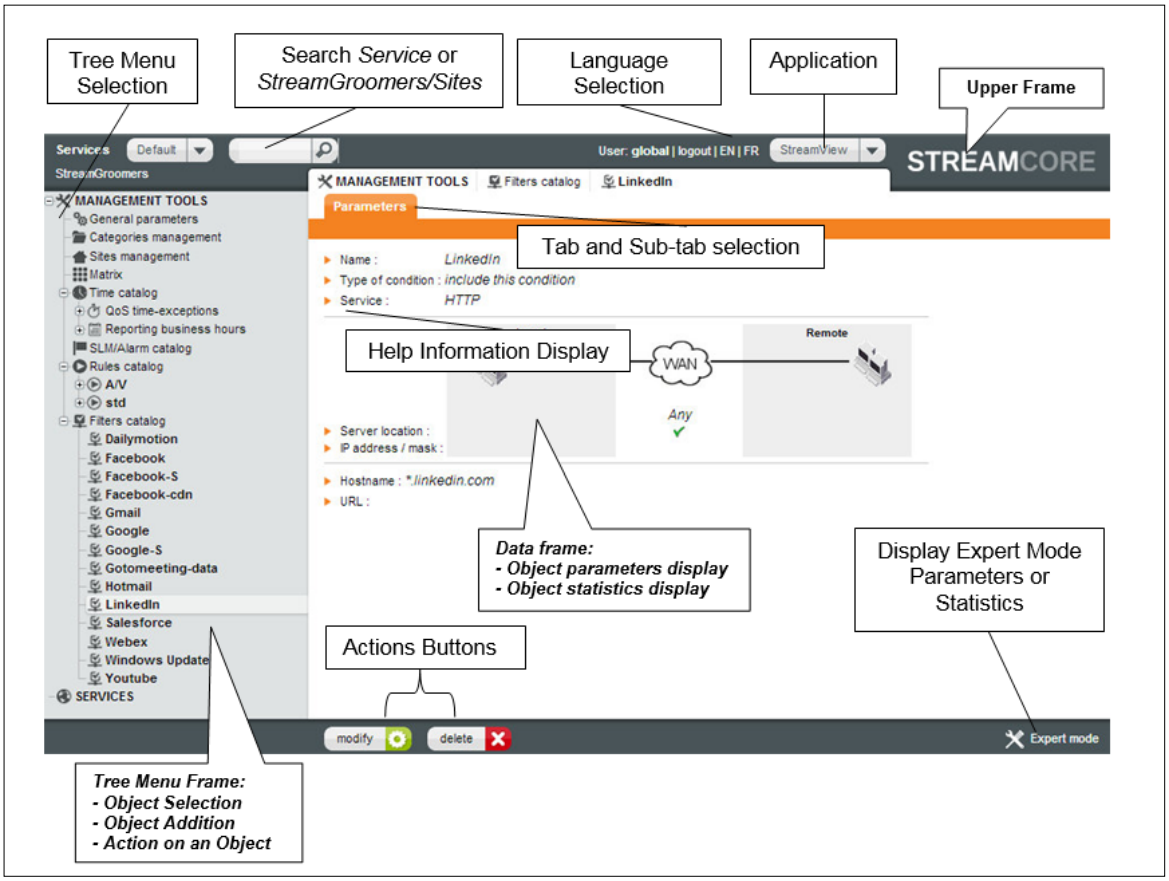


Figure 22 – StreamView frames at a glance

-
- In the "Upper Frame", the "Application" menu gives you direct access to various Streamcore applications including StreamView.
- The "Data frame" enables the configuration and display of database objects.
- To navigate in StreamView use the "Tree Menu Frame" located on the left-side of the screen. There are two tree menus which are associated with:
- **Services:** categories, sites and rules management the Unified Mapping Tree (UMT).
- **StreamGroomers:** used for StreamGroomer management.

4.3 STEP 3: PROVISION A SITE

The main parameters required per site are network parameters:

- access link characteristics
- subnets (directly connected to the WAN router or not)

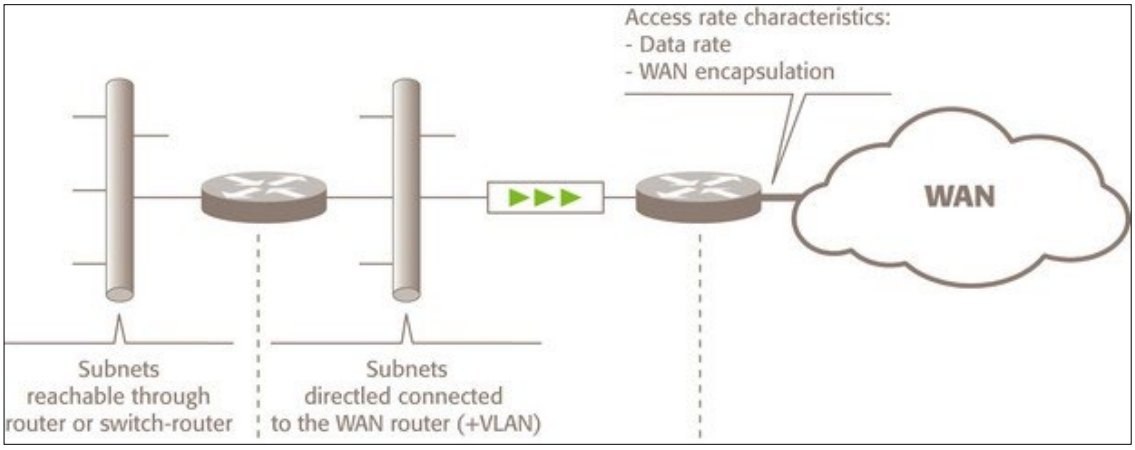


Figure 23 – Creating a Site – Main Network Parameters

To add a site with a single access link to manage:

1. Right-click on **SERVICES**. Select **Add…** → **Site**
2. Enter the required parameters.
3. Click **Submit**.

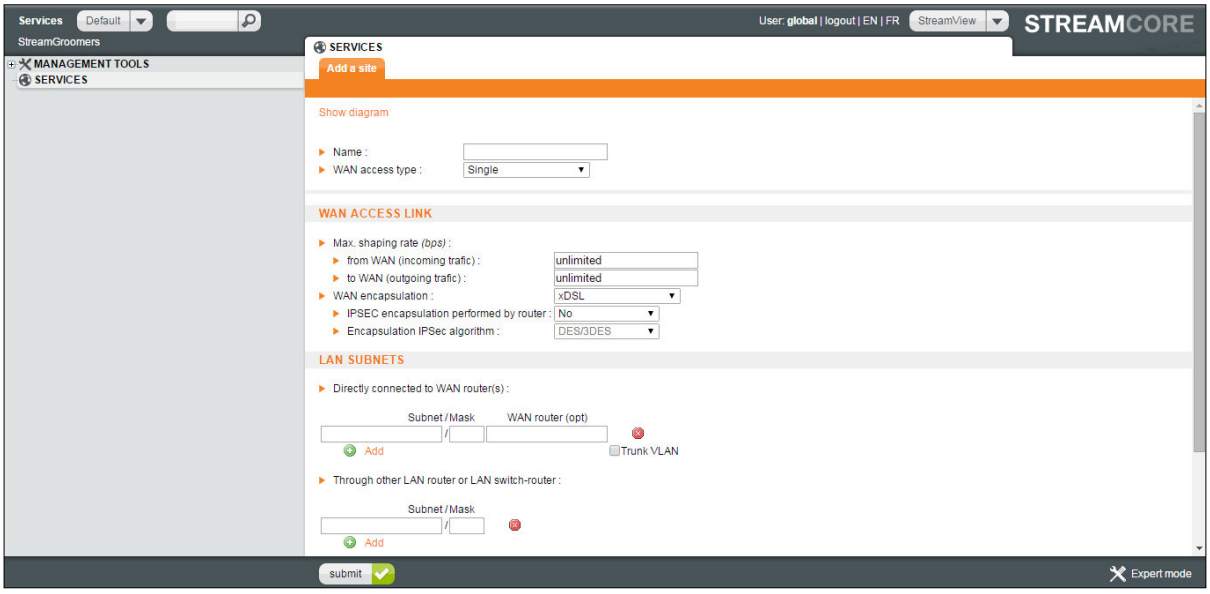


Figure 24 – Add a Site

Parameter	Description / Values	
	Site with a StreamGroomer	Site without a StreamGroomer

• WAN Access Link Parameters	
• WAN access type	• Select Single (default)
• Max shaping rate (bps) - Access link characteristics: • • The max shaping rate is used: • - For visibility purpose: to compute the access link usage rate • • - For performance control purpose: to schedule traffic and prevent inbound/outbound congestion on the access link •	• **From WAN (incoming traffic):** Set to unlimited by default • • **From WAN (outgoing traffic):** Set to unlimited by default
• WAN encapsulation • The WAN encapsulation is used to take into account the frame format when scheduling traffic.	• IPSEC encapsulation performed by router: Set to "No" by default. • • **Encapsulation IPSec algorithm:** Set to "DES/3DES" by default.
• LAN Subnet Parameters	
• Subnet + Mask + VLAN + WAN router (opt)	• When defining subnets associated with the site, it is key to distinguish subnets: • - directly connected to WAN router (s): these subnets will be used by the SG to identify local traffic, and when provisioning grooming rules. These subnets will also be used on remote StreamGroomers to identify this site traffic. • - through other LAN router or switch-router: these subnets will only be used on remote StreamGroomers to identify this site traffic.
• Other Parameters	
• Location	• Geographic address used to locate the site automatically in StreamMap
• Netflow export	• (Default = No) This parameter activates the netflow export for the site: • - Total: all traffic classified in the access link rule • - Per application: all traffic classified in terminal rules with the netflow export parameter set to yes • - Audio / Video: all traffic classified in audio/video rules

	• - Shaping other sites: all traffic classified in "Shaping other sites" rule
• Business hours	• (Default = None) Select a business hours profile (defined in Management tools). This information is only used by StreamReport when generating reports with business hours option.

5 StreamGroomer Management

All StreamGroomers are managed through the Streamcore StreamView application. This section is only to provide you with the basic setup configuration details and management. See the StreamView User Guide for further information.

- Before you provision a StreamGroomer you must fulfill 3 prerequisites:
- a database must be created in the SGMConf
- you must be logged to the database
- you must provision a least 1 site to associated a StreamGroomer
- If you have not completed the above see Site Management before you continue with StreamGroomer Management.

5.1 STEP 1: PROVISIONING A STREAMGROOMER

- After logging into StreamView application:

1. Right-click on **STREAMGROOMERS** in the tree menu then select **Add…Sg**.

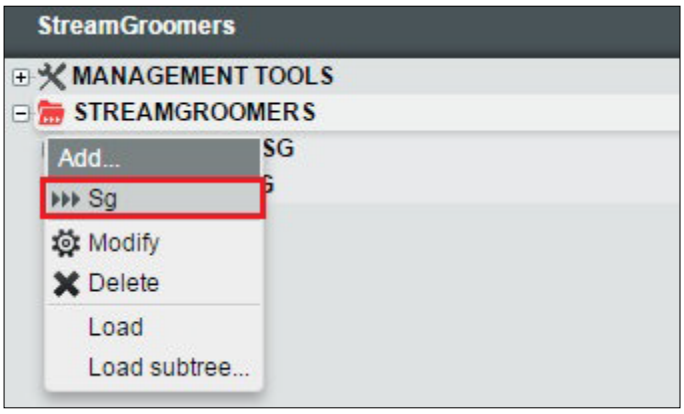
- 

Figure 25 - Adding a new StreamGroomer

- Alternatively, click on **STREAMGROOMERS** in the tree menu then click the **Add StreamGroomer** button.

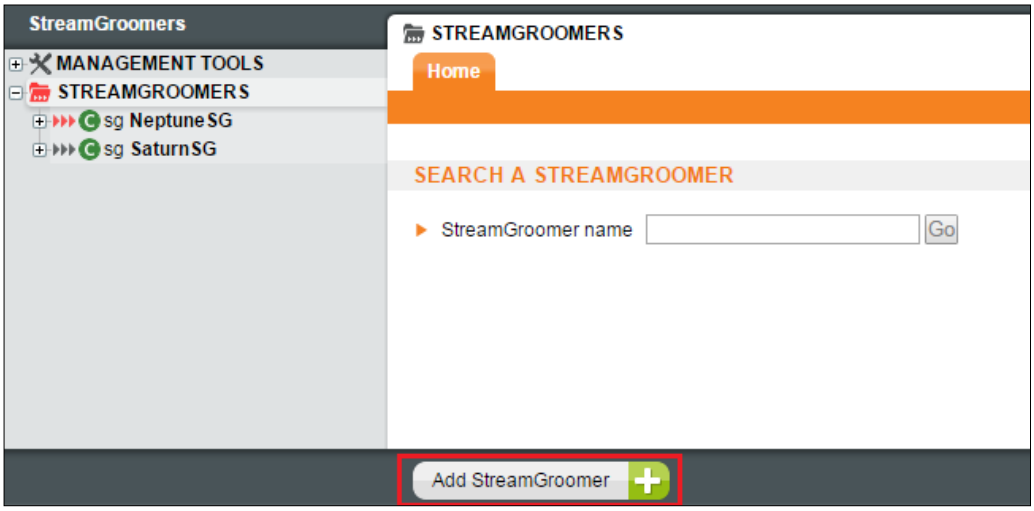


Figure 26 - Add button to add new StreamGroomer

2. Next, enter the required parameters then click the **Next** button.

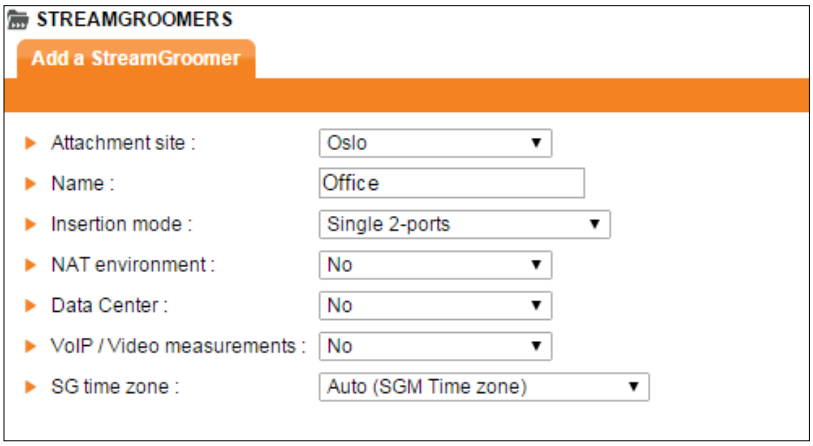


Figure 27 - StreamGroomer Parameters

Parameter	Description / Values
• Attachment site	• Select the site where the StreamGroomer will be created.
• Name	• StreamGroomer name
• Insertion mode	• Select one of the following choices: • **Single 2-ports (default):** a single StreamGroomer is deployed inline with 2 LAN/WAN ports connected on a single LAN segment. • **Single 4-ports:** a single StreamGroomer is deployed inline with 4 LAN/WAN ports connected on two LAN segments. • **Dual (2 SG):** two StreamGroomers are deployed inline in front of two separate WAN access routers, and are interconnected together through the EXT port to interact. • **Tandem 2-ports:** two StreamGroomers are deployed inline with 2 LAN/WAN ports connected on a single LAN segment, and are interconnected together through the EXT port to interact. • **Tandem 4-ports:** two StreamGroomers are deployed inline with 4 LAN/WAN ports connected on two LAN segments, and are interconnected together through the EXT port to interact.
• NAT environment	• The default value is set to "No". This must be set to "Yes" if the SG administration address is seen by the SGM as NATed. Public IP addresses will be provisioned in addition to the private IP addresses.
• Data Center	• The default value is set to "No". This must be set to “Yes” if the site is a Data Center.
• VoIP/Video measurements	• The default value is set to "No". The "VoIP/Video measurements" parameter is available per site with a SG.
• SG time zone	• The default parameter is set to **Auto – SGM timezone**. This parameter is used by time-based QoS policies.

3. Next enter the StreamGroomer network information:
    a. For a Single 2-ports and Single 4-ports insertion mode

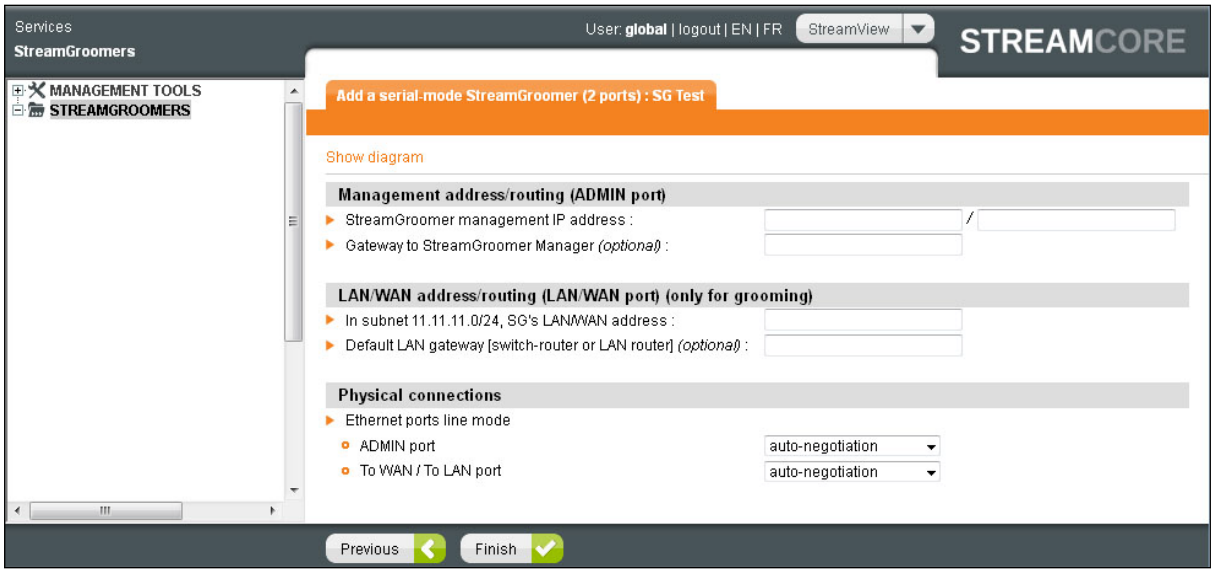


Figure 28 - Adding StreamGroomer Parameters

Parameter	Description / Values
• Management address/routing (ADMIN port)	
• StreamGroomer management IP address	• This refers to the StreamGroomer administration IP address. • The mask can be entered in the following form: 24 or 255.255.255.0
• Gateway to SGM (Optional)	• Enter the gateway address used to reach the SGM. This parameter is required only if the SGM is located on a different subnet than the StreamGroomer.
• LAN/WAN address/routing (LAN/WAN port) only for **Grooming** and **WAN Optimization**	
• In subnet x.x.x.x, SG's LAN/WAN address	• LAN/WAN IP address of the StreamGroomer. • Required if Grooming network rules are configured. • Required for WAN Optimization. The mask can be entered in the following form: 24 or 255.255.255.0
• Default LAN gateway	• LAN gateway. • Required if Grooming network rules are configured, as well as tunnel mode. • Required for WAN Optimization.
• Physical connections	
• ADMIN port •	• The default is set to **auto-negotiation**. StreamGroomer Ethernet ports can adapt to half-duplex and full-duplex modes as well as to speeds of 10 Mbps, 100 Mbps and 1 Gbps. • Configuration recommendations: if the opposing device is in auto-negotiation or half-duplex 10 Mbps mode, use auto-negotiation, otherwise, force the same mode as that of the opposing device.
• To WAN / To LAN port	

Note: If the WAN access type of the site is set to redundant active/active, the management of the access links can be defined as aggregated or independent when adding the StreamGroomer. For a **Dual, Tandem 2-ports, Tandem 4-ports** insertion mode

Parameter	Description / Values
• Terminology	
• Master suffix	• Suffix added to the name of the SG.
• Slave suffix	
• Management address/routing (ADMIN port)	
• Shared IP address (statistics)	• Shared IP address between the StreamGroomers used by the SGM to poll statistics. The mask can be entered in the following form: 24 or 255.255.255.0
• Master IP address	• IP address of the Master StreamGroomer (Administration).
• Slave IP address	• IP address of the Slave StreamGroomer (Administration).
• Gateway to SGM	• Address of the gateway used to reach the SGM. This parameter is required only if the SGM is located on a different subnet than the StreamGroomer.
• LAN/WAN address/routing (LAN/WAN port) only for **Grooming** and **WAN Optimization**	
• In subnet x.x.x.x, SG's LAN/WAN address	• LAN/WAN IP address of the StreamGroomer. • Required if Grooming network rules are configured. • Required for WAN Optimization is being used. The mask can be entered in the following form: 24 or 255.255.255.0
• Default LAN gateway	• LAN gateway. • Required if Grooming network rules are configured, as well as tunnel mode. • Required for WAN Optimization.
• InterSG address/routing (EXT port)	
• Master InterSG IP address	• IP addresses used by the dual StreamGroomers to exchange packets in the InterSG link. • Any IP addresses can be chosen, whether the Master and Slave StreamGroomers EXT ports are connected directly or via a VLAN trunk.
• Slave InterSG IP address	
• Physical connections	
• ADMIN port •	• The StreamGroomers Ethernet ports can adapt to half-duplex and full-duplex modes as well as to speeds of 10 Mbps, 100 Mbps and 1 Gbps. • Configuration recommendations: if the opposing device is in auto-negotiation or half-duplex 10 Mbps mode, use auto-negotiation, otherwise, force the same mode as that of the opposing device.
• To WAN / To LAN port •	
• EXT port	

Note: If the WAN access type of the site is set to redundant active/active, the management of the access links can be defined as aggregated or independent when adding the StreamGroomer.

- 4. Click **Finish**.

5.2 STEP 2: INSTALLING THE STREAMGROOMER OPE

1. Click on **STREAMGROOMERS>xx** in the tree menu, and then on the ***Release Management > Read Status*** sub-tab to check the availability of the StreamGroomer. To install the OPE software you must use the installation sub-tab.

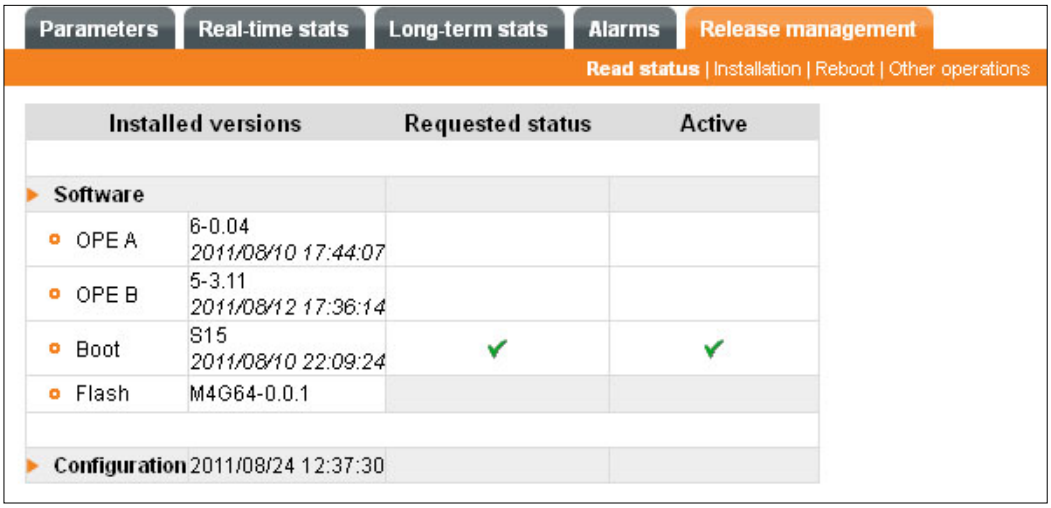


Figure 29 – Reading the StreamGroomer status

2. Next click on the **Installation** sub-tab. Use the "Available releases" and "Destination" combo box to select a release and partition to install the OPE software.

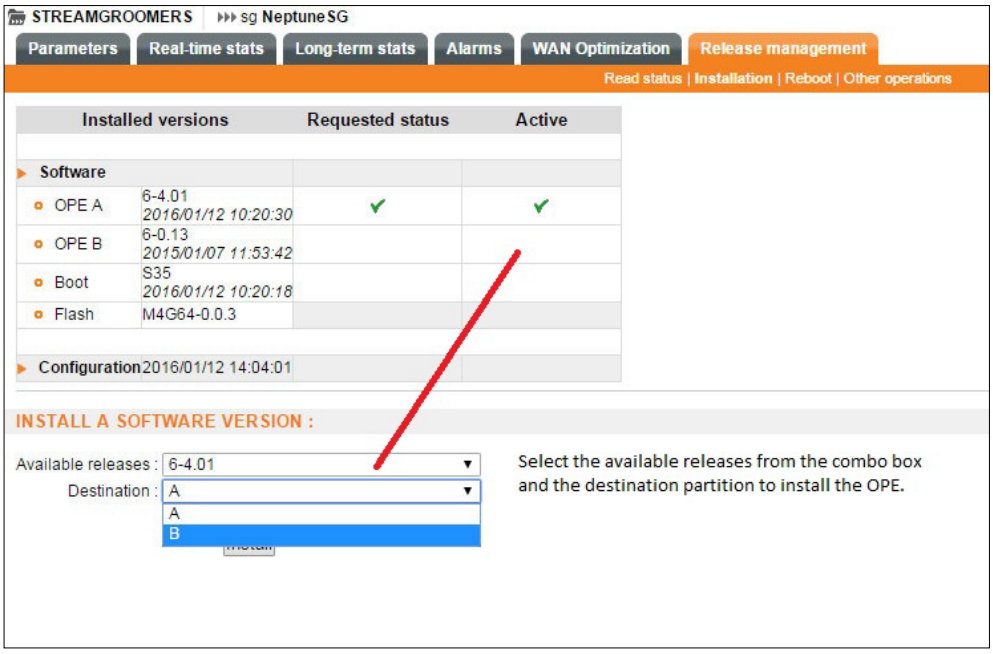


Figure 30 – Activating the OPE Software

3. After clicking the **Install** button, the software should be visible in the "Installed versions" column.

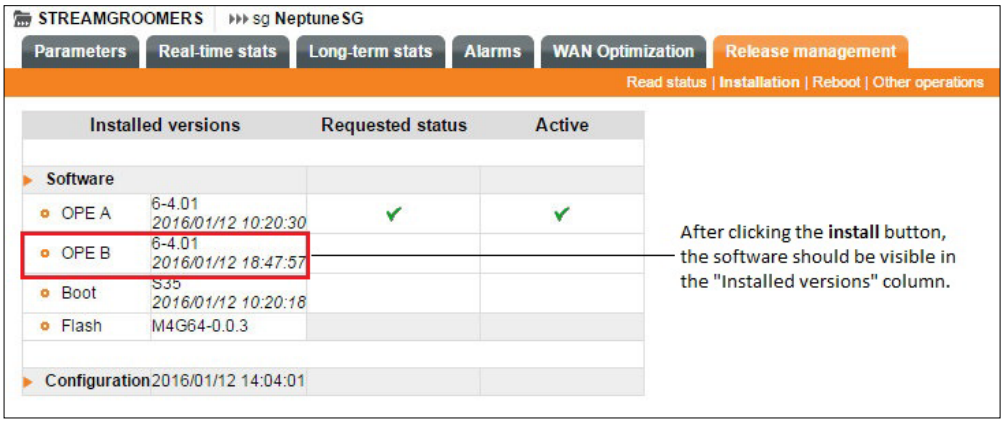


Figure 31 – Installed OPE Software on partition B

4. In order to activate the Software click on the **Reboot** sub-tab and click the **Activate** button. If the activation is successful you will notice a green check in the "Active" column.

- **Warning:** That this will affect your organizations current SG setup, especially if you do not have failsafe SGs in place (i.e. Duel/Tandem mode)

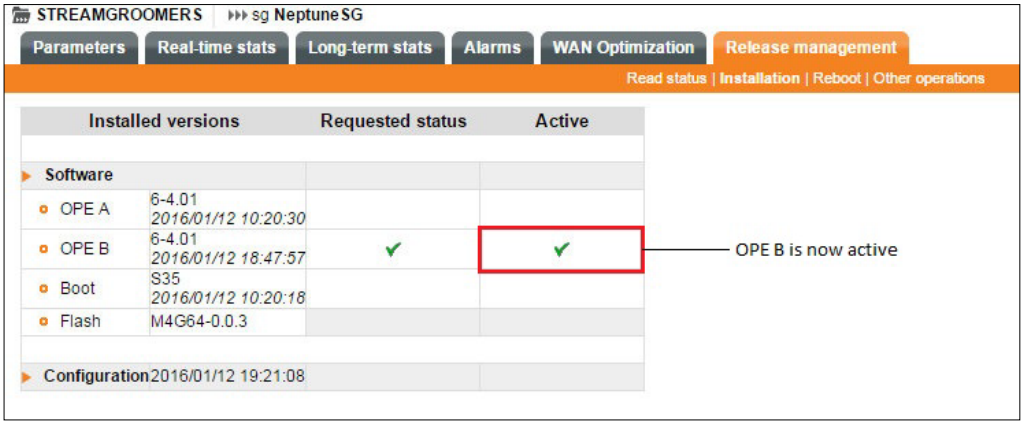


Figure 32 – Activating OPE software

5. After a restart confirm that the StreamGroomer is accessible and that it is in the operating software, by clicking again on the ***Release Management – Read Status*** sub-tab.

-
- It is possible to configure some StreamGroomers in high performance processing mode, enabling Multi-Gigabit traffic rates that are above 1-Gbps (Gigabit/second). The SG3200e series can operate using high performance mode.
- If you upgrade from v6.1 to v6.2 and your StreamGroomer supports high performance processing you will be presented with a drop-down list that offers you a choice to active it. By default high performance processing is not activated.

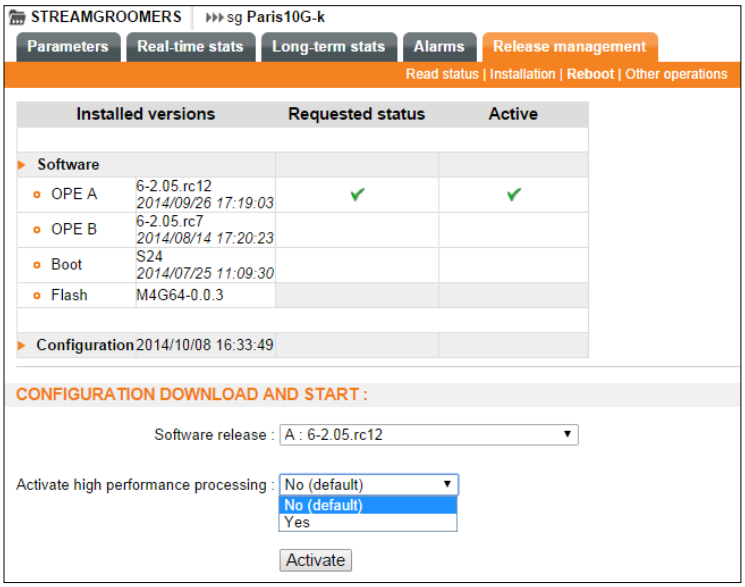


Figure 33 – High Performance Processing

5.3 STEP 3: ENABLE TRAFFIC MANAGEMENT

By default, a StreamGroomer is started in Bypass mode:

- Traffic management is inactive
- The mechanical bypass is closed, and therefore the LAN and WAN ports are de-activated.
- The management ADMIN port remains active

To change the mode or the main parameters of a StreamGroomer:

1. Click on **STREAMGROOMERS > xx** in the tree menu, on the *Parameters-Configuration* sub-tab, then on the **Modify** button.
2. Select the desired mode:
   - **Monitoring+Tagging+Control:** Traffic management is active. The following features are available: Monitoring & Reporting, UCP engine / Advanced QoS, Compression / Web caching / WAN Load balancing. Streamcore QoS management is also activated.
   - **Monitoring+Tagging:** Traffic management is active. The following features are available: Monitoring & Reporting, UCP engine / Advanced QoS, Compression / Web caching / WAN Load balancing.
   - **Monitoring:** Traffic management is passive. Only the Monitoring & Reporting features are available.
3. Click the **Submit** button.

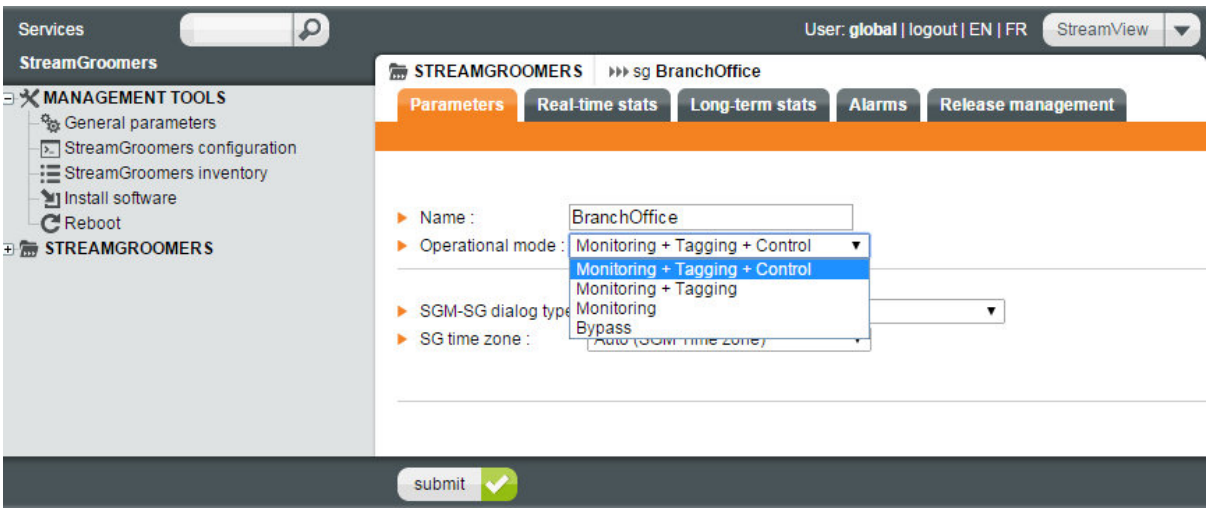


Figure 34 –Traffic Management

StreamGroomers manage all traffic exchanged between the LAN and the WAN: visibility, performance control, or optimization services can be configured and enabled.

- **Note:** Activating the **Monitoring+Control** mode is recommended only when full traffic classification has been completed and QoS policies have been defined.

6 Service Configuration - Examples

All further steps are related to the Unified Mapping Tree (UMT) configuration to define traffic classification, visibility, and control policies.

The following examples only describe some additional configuration steps to use visibility services.

For further information regarding visibility services or how to configure performance control and optimization services, See the StreamView User Guide.

6.1 ACCESS LINK VISIBILITY SERVICES

By default, only an "Access link rule" is defined on a site with a StreamGroomer, into which all IP traffic exchanged over the WAN is classified. When clicking on the Access link rule in the tree, tabs give a direct access to ready-to-use visibility services:

REAL-TIME STATS

The ***Real-time stats>Indicators*** visibility services provide statistics over the last 10 sec., 1 min. and 10 min. periods. The statistics displayed are aggregated for all the classified traffic in the access link rule, such as the data rate.

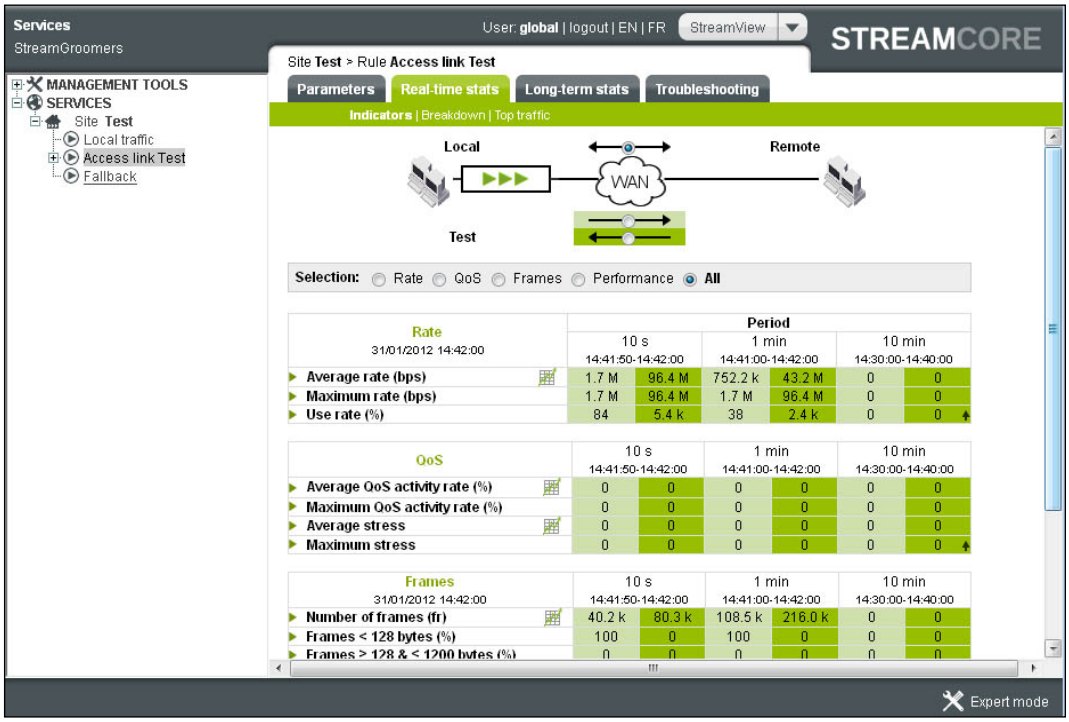


Figure 35 – Access Link Real-time Stats

- **Note:** ***Real-time stats>Breakdown*** and ***Top traffic*** can be used when rules have been defined below the access link.
-

LONG-TERM STATS

The ***Long-term stats>Indicators*** visibility services provide statistics over the long-term (day, week, month, year). The provided statistics are aggregated for all classified traffic in the access link rule, such as the data rate. Use the period menu to select a display period:

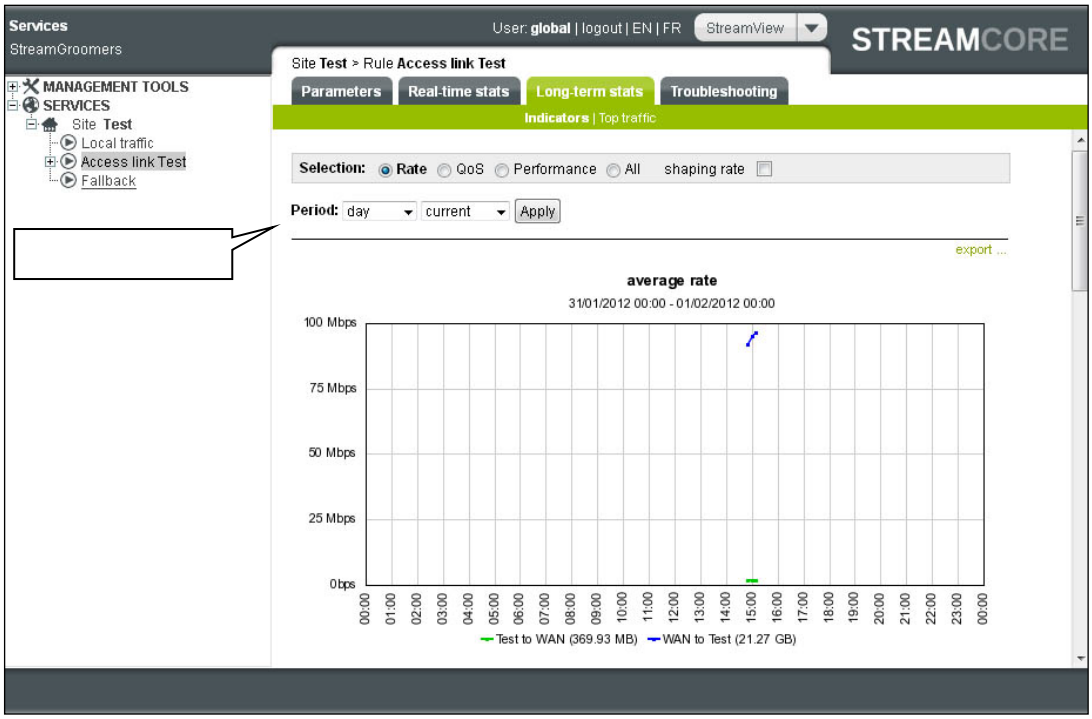
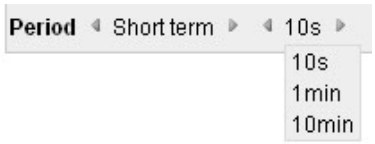


Figure 36 – Access Link Long-term Stats

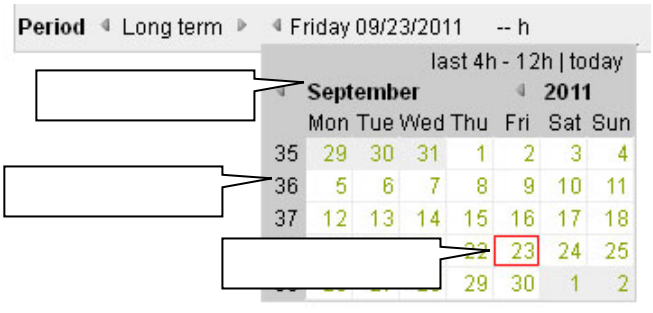
-
- **Note:** ***Long-term stats>Top traffic*** can be used when rules are defined below the access link.

TROUBLESHOOTING TOOLS

The ***Troubleshooting*** (***TOP***, ***Connections***) visibility services provide very granular information down to the session. All ***Troubleshooting*** services are always offered over the short-term (last 10 sec, 1 min., 10 min.):

Last 10 sec., 10 sec., 10 min. period selection	

To get long-term troubleshooting tools, the netflow export must be activated on the site (see netflow parameters on a site described in chapter 5.1). When activated on the rule, an additional long-term period selection menu is available:

Specific month, week or day selection	

The ***Troubleshooting – TOP*** sub-tab displays the top hosts consuming the most bandwidth among all the traffic classified in the rule. When analyzing the TopNs, you can display various types:

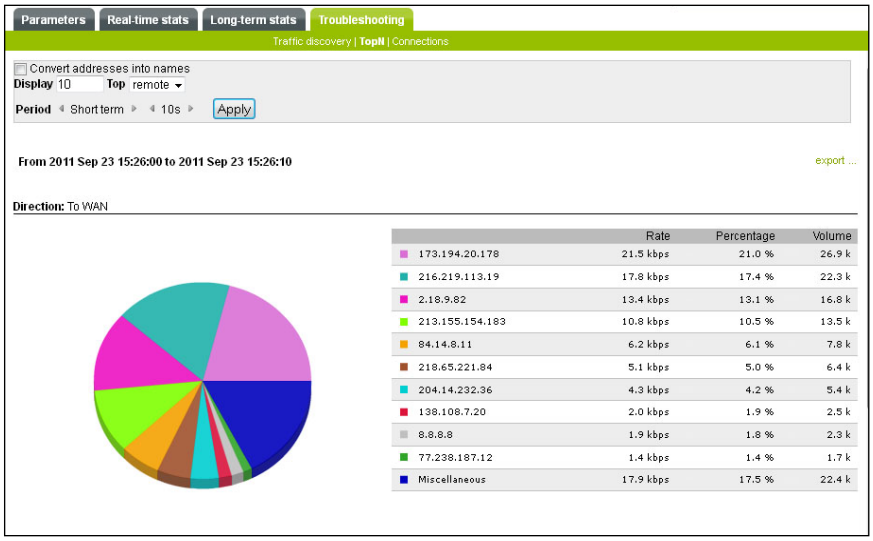


Figure 37– TOP

The ***Troubleshooting – Connections*** sub-tab displays all connections or communications classified in the rule.

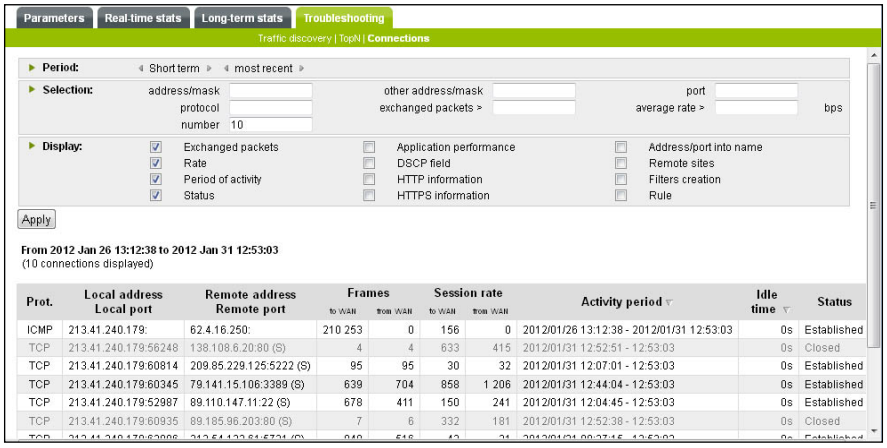


Figure 38 – Connections

6.2 SINGLE RULE CREATION

Specific types of traffic can be classified using a specific rule, in order to get dedicated *Real-time stats, Long-term stats,* and *Troubleshooting tools*.

To add a specific rule directly in a site rules tree: Right-click on the rule (for instance Fallback) before which the new rule should be inserted, and select "**Insert before… → Terminal data rule** or **Terminal audio/video rule**".

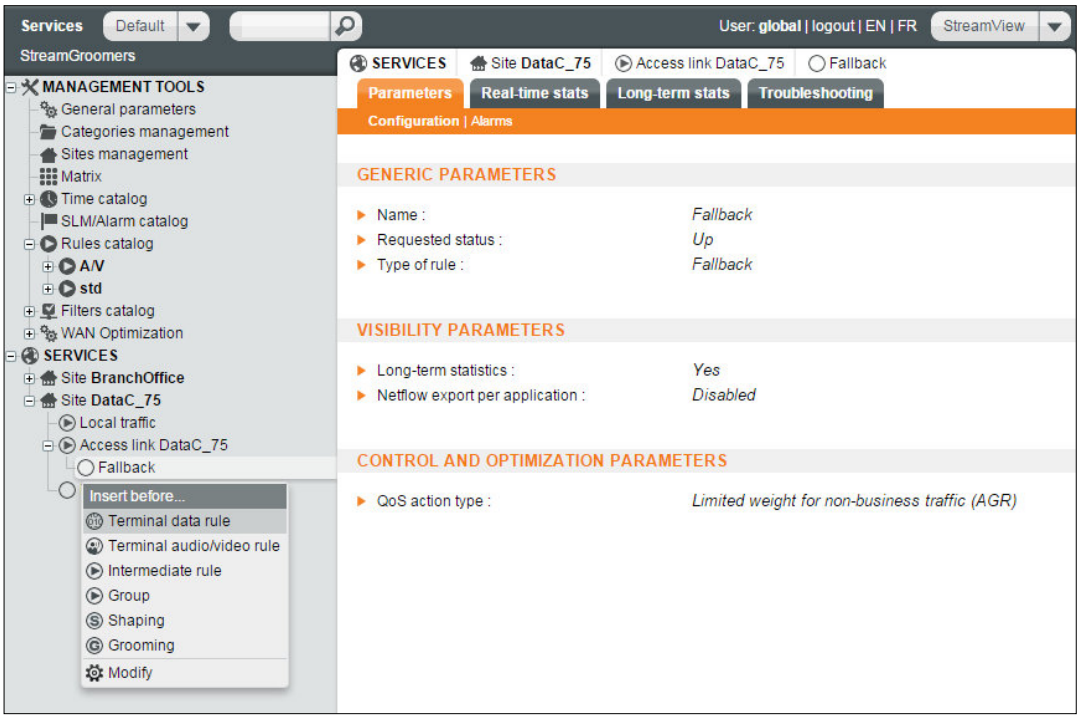


Figure 39 – Terminal Data Rule

- Note:
- In data rules, dedicated TCP-based measurements performance measurement are automatically enabled
- In audio/video rules, RTP-based performance measurements are automatically enabled

1. Enter the name of the rule (the other parameters are mainly for QoS purpose), and click on the "**Submit**" button.

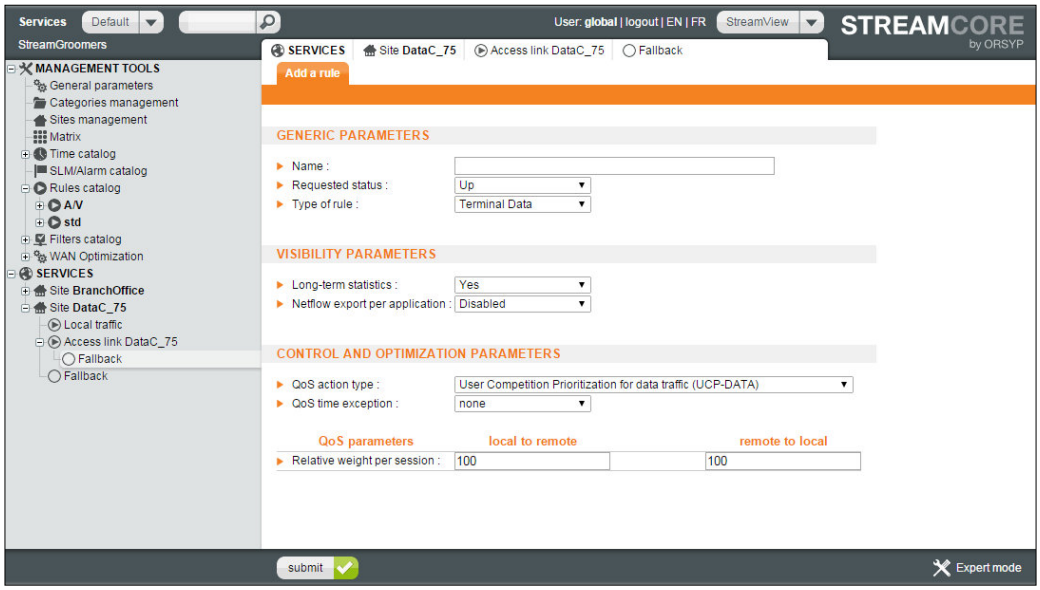


Figure 40 – Add a Rule

2. The filter creation assistant is displayed automatically:

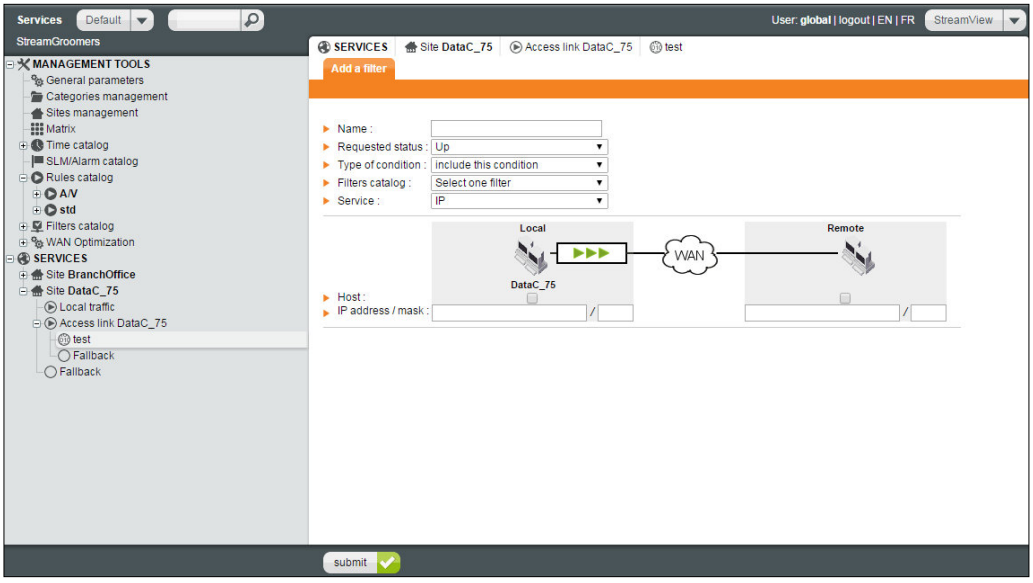


Figure 41– Filter Configuration

Parameter	Description / Values
• Name	• Name of the filter (automatically filled if left blank)
• Requested status	• Up (default), Down

• Type of condition	• Include (default), Exclude
• Filters catalog	• When selecting a filter in the list, it automatically pre-fill all the parameters. L7 predefined filters are available by default (salesforce, facebook…).
• Service	• Select a value among the list of predefined protocols and applications.
• Server location	• For all services running over UDP/TCP, this parameter defines on which side the server port is located. The possible values are: • - "Any": the classification does not take into account the UDP/TCP call direction • - "Local" or "Remote": the classification takes into account the UDP/TCP call direction
• Host	• Check this box to enforce the IP mask to /32
• IP address/mask	• Enter a local and/or remote xx.xx.xx.xx value

When a **L7-specific criteria service** is selected, additional parameters are available:

L7-specific criteria service	*Parameter*	Description / Values
• HTTP HTTP-PROXY	• Hostname	• Hostname of the web traffic to be classified
	• URL	• URL of the web traffic to be classified
• HTTPS	• Common name	• SSL certificate common name of the encrypted traffic
	• Organization name	• SSL certificate organization name of the encrypted traffic
	• Organization unit name	• SSL certificate organization unit name of the encrypted traffic
	• Locality name	• SSL certificate locality name of the encrypted traffic
• RTP+RTCP	• Payload	• List of predefined RTP payload type: audio+video (default), audio, video, audio/G.711, audio/MS…

3. Click the **Submit** button. The creation of the rule with a first filter is completed.

Note: Other filters can be added on this rule by clicking on the ***Parameters>Filters*** tab.

Visibility services (***Real-time stats, Long-term stats, Troubleshooting tools)*** are automatically available on the new rule, exactly as for the access link.

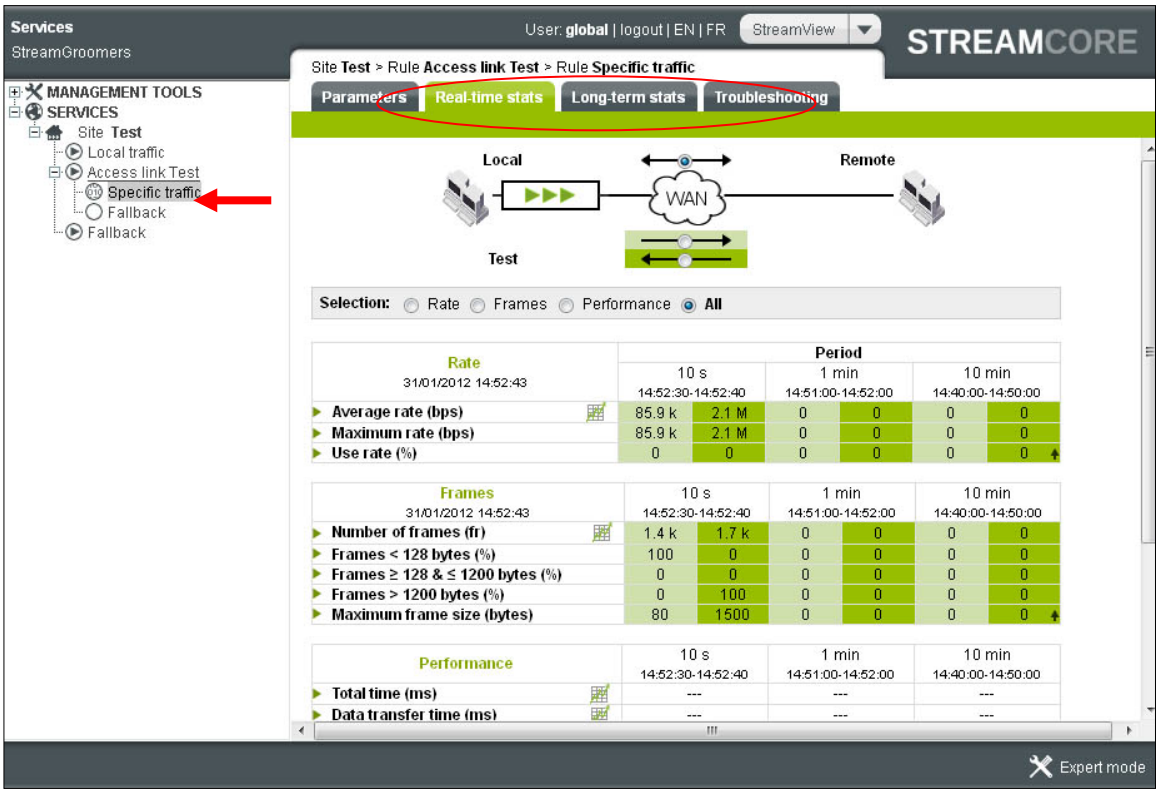
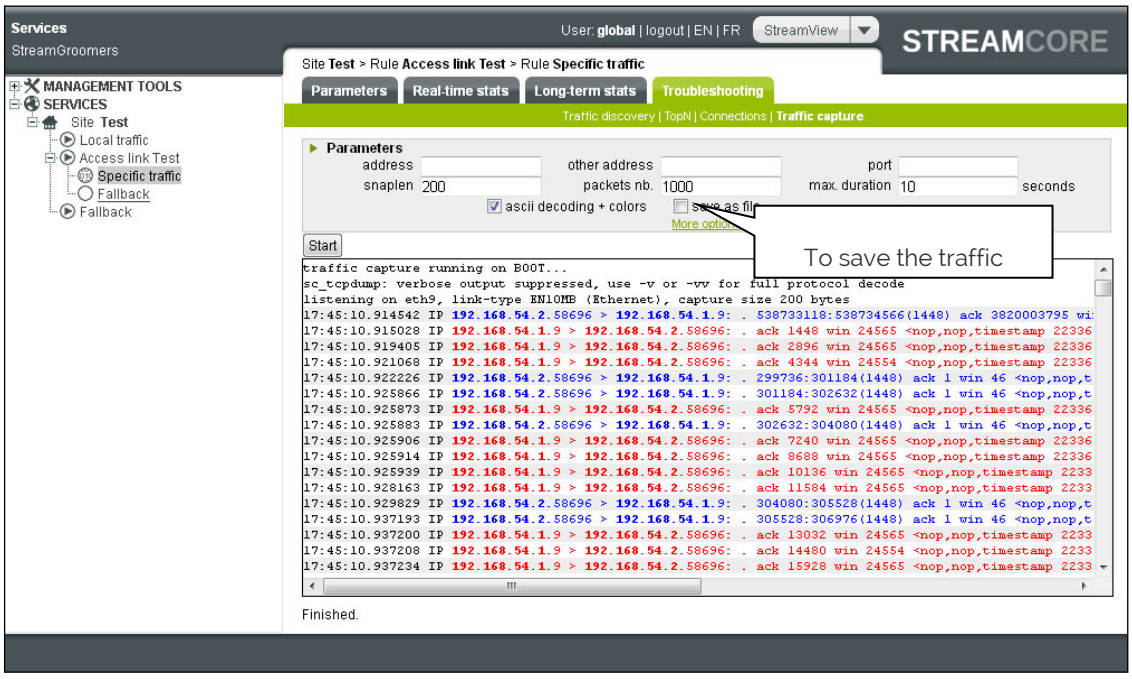


Figure 42 – Long-term Stats

Additional features are also enabled:

- ***Real-time stats*** and ***Long-term stats****:* in addition to data rate information, aggregated performance measurements are automatically available (response time, MOS…) for all the data or audio/video traffic classified in this rule.
- ***Troubleshooting tools***: in addition to *TOP* and *Live sessions* tools, a *Traffic capture* tool is also available to display packets classified in the rule:



6.3 GROUP OF RULES CREATION

Predefined group of rules can be used to accelerate the rule creation process. Reference group of rules are managed in the **MANAGEMENT TOOLS > Rules catalog**. For any new database, "std" and "A/V" groups of rules are automatically created to provide a first level of traffic classification for standard applications (std) and for Audio/Video traffic (A/V).

A predefined "Traffic discovery" group of rules can also be used to automatically auto-discover a wide range of well-known applications. To create this reference traffic discovery group of rules:

1. Open the **MANAGEMENT TOOLS**, right-click on **Rules catalog**, and then select **Add… → Group**
2. Enter the group name, select *Predefined traffic discovery:*

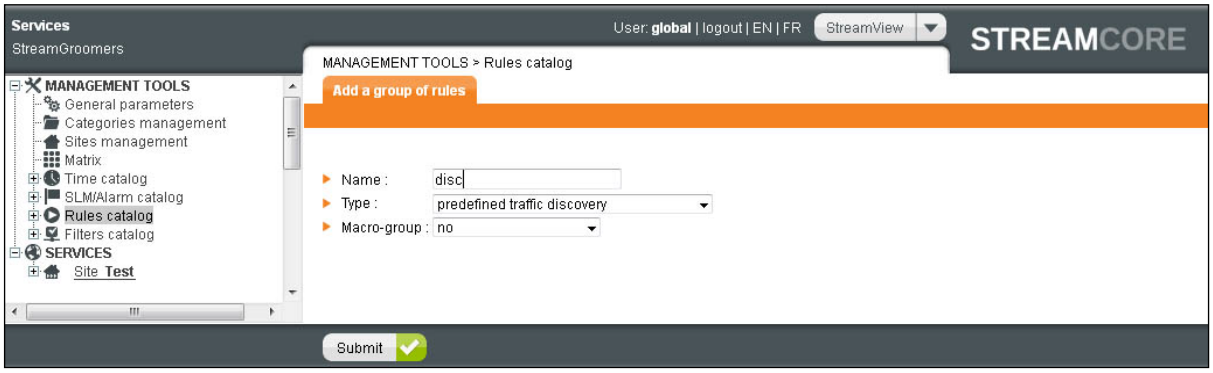


Figure 43 – Rules Catalog

3. Click the **Submit** button.

This reference group of rules can be inserted directly on an existing site:

1. Right-click on the rule that will be placed under the Group of rules, and select **Insert before… > Group of rules**.

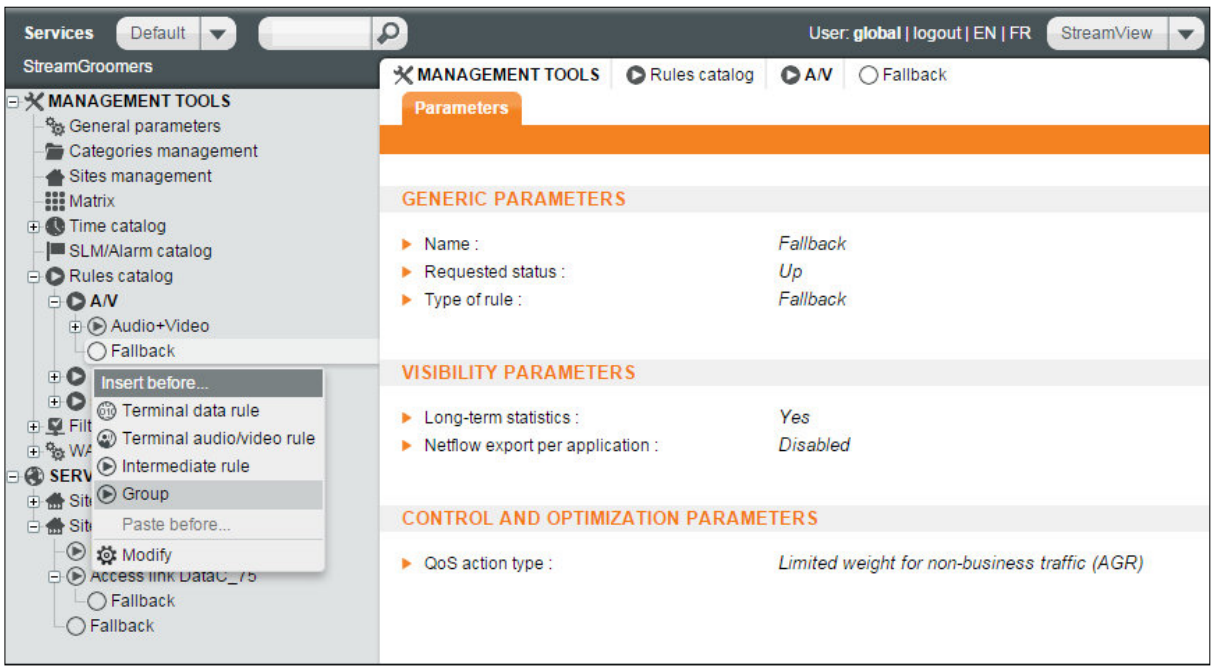


Figure 44 – Group of Rules

2. Select the reference *Traffic discovery* group of rules, and then click on the **Submit** button.

Visibility services (***Real-time stats, Long-term stats, Troubleshooting tools)*** are automatically available on any rule within the group, exactly as for the access link or the specific traffic rule:

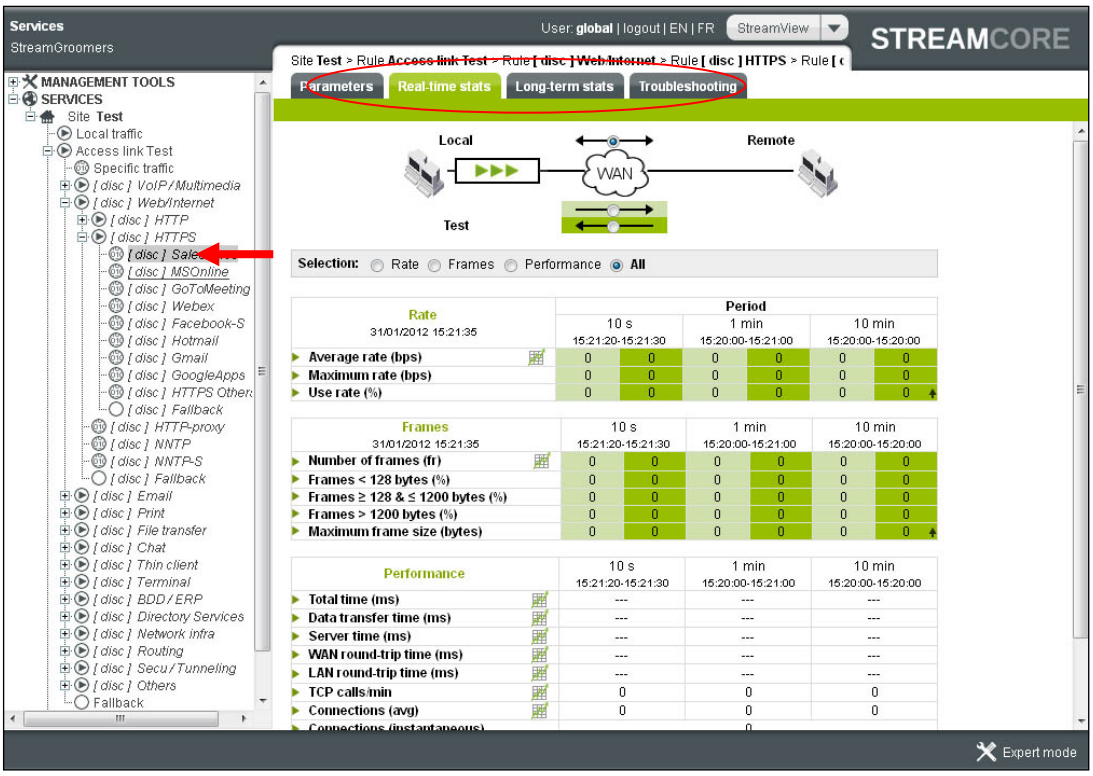


Figure 45 – Long-term Stats

6.4 REMOTE SITE MANAGEMENT

In order to automatically classify traffic exchanged with a remote site without any StreamGroomer, the steps to follow are:

Add the site with a single access link to manage:

1. Right-click on **SERVICES.** Select **Add…** → **Site**.
2. Enter the required parameters (access link data rate, subnets).
3. Click the **Submit** button.

Create a Shaping rule directly from the tree menu of the site with a StreamGroomer:

1. Right-click on **SERVICES > … > Site xx > Access link xx > Fallback** and select **Insert before… → Shaping**

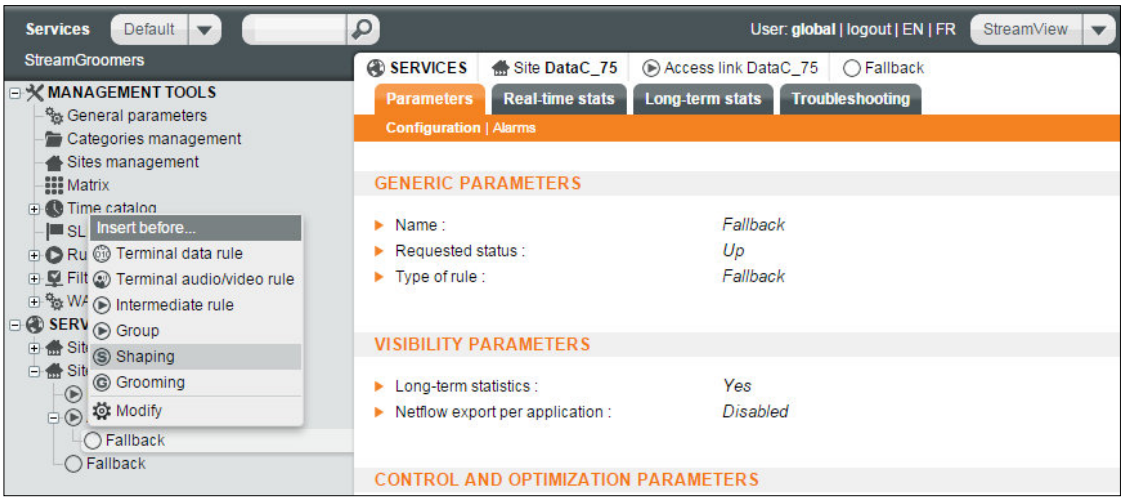


Figure 46 – Shaping

2. The creation wizard is automatically launched. Select the remote site and the different parameters.

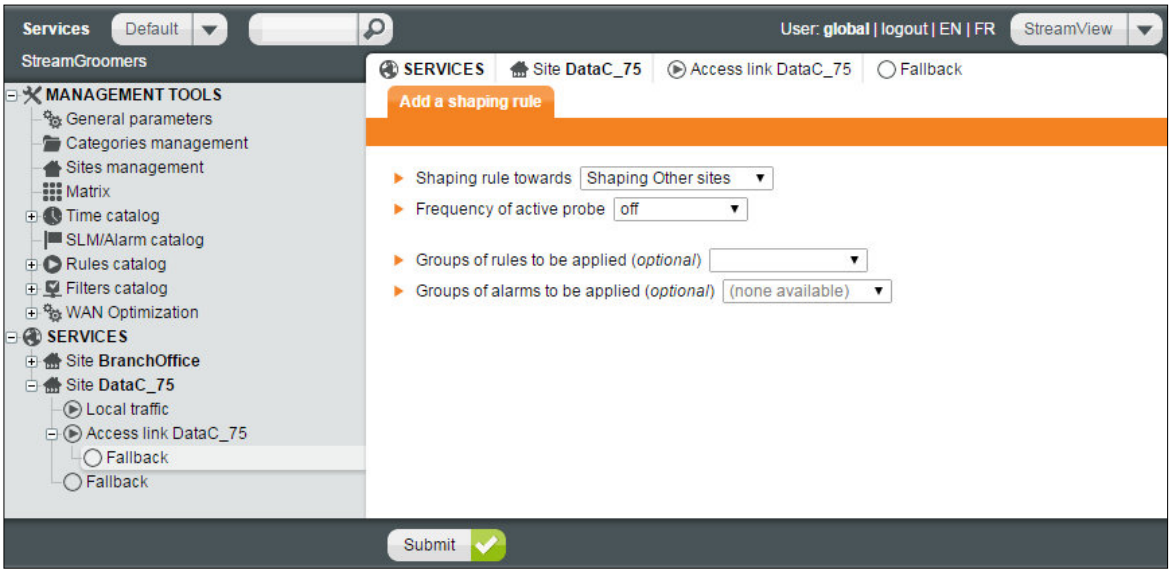


Figure 47 – Shaping Rule

Parameter	Description / Values
• Shaping rule towards	• Select a site in the list
• Frequency of active probe	• (default=Off) Activate a ping to measure availability and network performance
• Groups of rules to be applied (optional)	• Select one or more application groups of rules to classify the traffic below the shaping rule (for example "std")
• Group of alarms to be applied (optional)	• Select one or more network group of alarms to detect abnormal service levels

3. Click on the **Finish** button.

Visibility services (***Real-time stats, Long-term stats, Troubleshooting tools)*** are automatically available on this shaping rule, exactly as for the access link or the specific traffic rule:

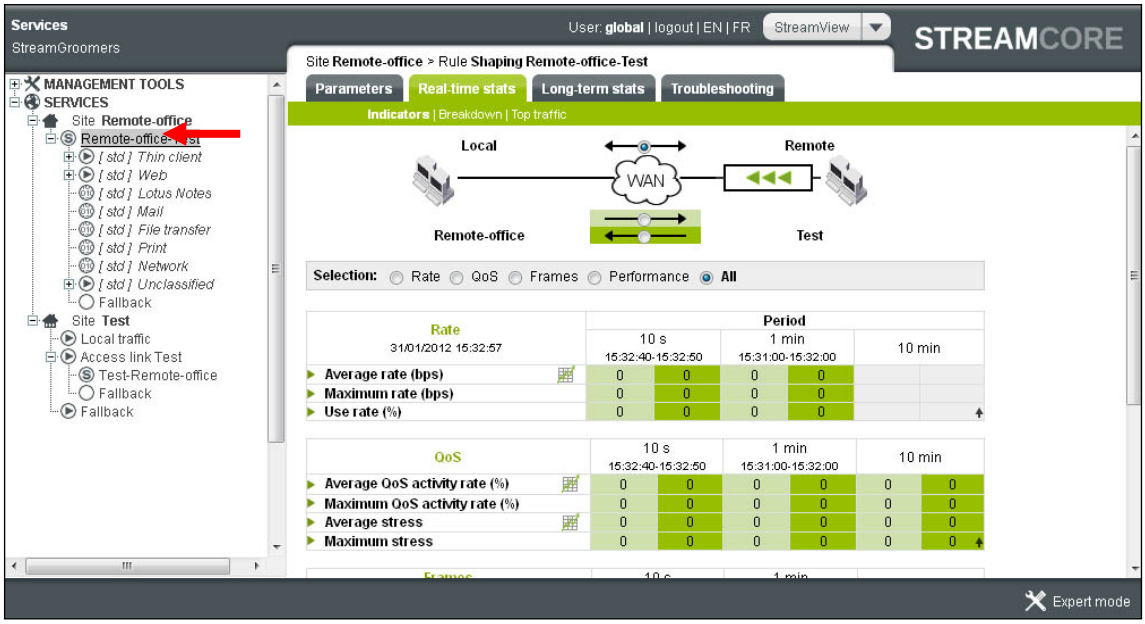


Figure 48 – Real-time Stats on Shaping Rule

The advantages of using a shaping rule towards a remote site instead of a standard Intermediate rule are the following ones:

1. Automated network measurements (based on ping towards the remote access router)
2. Automated subnet filters and QoS parameters
3. Site "object" presenting all rules (in case there are multiple data centers with a StreamGroomer managing traffic exchange with this site):
    a. By opening the site tree, a user can have a direct access to all traffic exchanged with the site
    b. By clicking on the site, all statistics are automatically aggregated, even if they were provided from different StreamGroomers