

# IP Quality Monitor

## Тестирование IQM на ОС Альт 10

---

### Руководство пользователя

версия 1.02



ООО «Нетпроб»  
123557, г.Москва,  
пер. Электрический, дом 3/10 стр. 3,  
офис 306А

---

Москва, 2025

# 1 Введение

Инструкция предназначена для использования персоналом, выполняющим тестирование работоспособности IP Quality Monitor (далее в тексте — IQM), установленной на операционную систему (далее в тексте — ОС) типа Linux ОС «Альт» версии 10. Указанная ОС входит в реестр российского программного обеспечения (далее в тексте — Реестр). Официальное название в Реестре — «Альт Платформа», правообладатель: Общество с ограниченной ответственностью «Базальт свободное программное обеспечение» (далее в тексте — Правообладатель). Установка IQM на ОС «Альт» позволяет осуществлять внедрения в тех случаях, когда требуется отсутствие зависимости от зарубежных поставщиков в целях информационной безопасности или импортозамещения. Программное обеспечение для краткости в дальнейшем тексте будет называться ПО.

Официальный адрес электронной почты ООО «Нетпроб» для пользователей IQM – [iqm-support@net-probe.ru](mailto:iqm-support@net-probe.ru).

От пользователя требуются следующие навыки:

- уверенное понимание настроек и поведения сетей TCP/IP,
- знание операционной системы Linux на уровне системного администратора.

## 2 Организация лаборатории

Процесс установки IP Quality Monitor agent (далее — IQMA), и системы управления IP Quality Monitor manager (далее — IQMM) описан в отдельной документации. Здесь мы предполагаем, что читающий уже знаком с этим.

В документации мы стараемся следовать соглашениям, которых придерживается ОС «Альт». В частности, если приглашение указано в виде доллара, то имеются ввиду команды `shell` под учётным именем обычного пользователя. Например,

```
$ id -u -n
```

означает вывести его имя, допустим `saе`. А команда, где приглашение указано в виде решётки означает необходимость исполнения этой команды под учётной записью супервизора ОС (`root`). Например

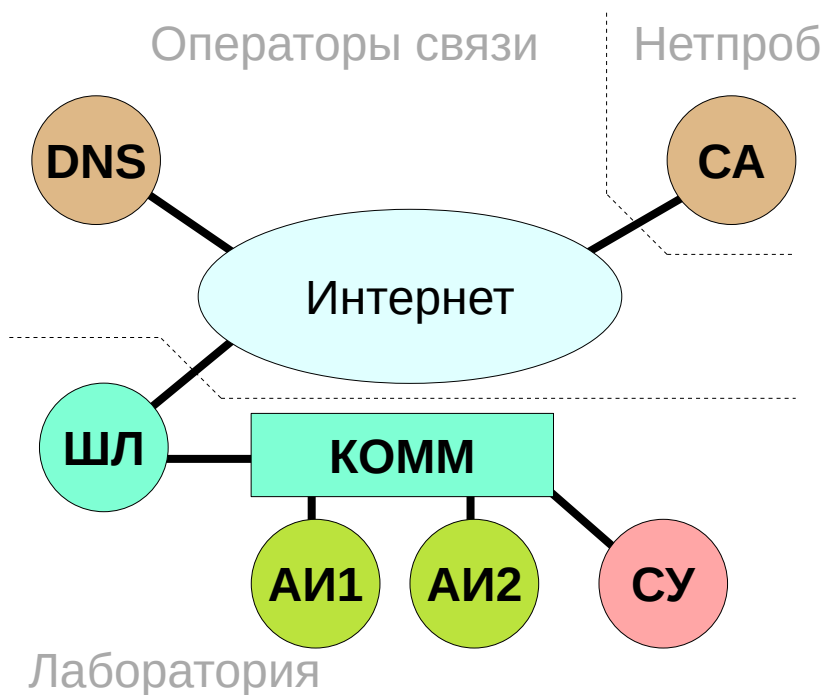
```
# id -u -n
```

выведет строку `root`.

Как тестирующему правильно переходить в режим супервизора ОС, хорошо описано в документации к ОС «Альт». Мы предполагаем, что вы это умеете. Указания в процессе тестирования по переходу в режим `root` и выходу из него опущены, просим внимательно следить за приглашениями указанных в тексте команд!

Общая схема лабораторного стенда для проведения тестирования приведена на рисунке 1.

**Рисунок 1.**



где

<p>Нетпроб</p> <p>Интернет</p> <p>—</p> <p>АИ1</p> <p>АИ2</p> <p>СУ</p> <p>ШЛ</p>	<p>Обозначение зон ответственности на время тестирования</p> <p>Общедоступная сеть протокола TCP/IP</p> <p>Соединения между сетевыми устройствами</p> <p>Агент-инициатор IQMA №1 на устройстве с ОС «Альт» 10</p> <p>Агент-инициатор IQMA №2 на устройстве с ОС «Альт» 10</p> <p>Система управления IQMM на сервере с ОС «Альт» 10</p> <p>Шлюз, обеспечивающий доступ из лаборатории в сеть Интернет.</p>
---	---

**KOMM**

Сетевой коммутатор для внутренних связей лаборатории

**DNS**

DNS-сервер ближайшего оператора связи, либо самой лаборатории

**CA**

Сопряжённый агент IQMA, доступный в сети Интернет на время тестирования.

Рабочее место проверяющего на схеме не показано. Его включение вы можете сделать так, как вам привычнее.

Требования к установке и сетевым настройкам для лаборатории.

1. Для простоты мы предполагаем, что все устройства, включенные в коммутатор KOMM, располагаются в одной подсети TCP/IP. Допустим, **10.55.1.0/24**. Вы можете сделать иначе, если достаточно квалифицированы. В настоящей документации мы будем придерживаться указанной адресации.

2. Шлюз ШЛ, обеспечивающий указанной подсети доступ в Интернет, при этом имеет адрес **10.55.1.1/24**. Если шлюз имеет особенные настройки безопасности, то следует обеспечить доступ:

2а. По протоколу DNS к серверу DNS от АИ1 и от АИ2.

2б. По протоколу ICMP (эхо-запрос (8:0), эхо-ответ (0:0), получатель не доступен (3:\*), время исчерпано (11:\*)) к самому шлюзу от АИ1 и от АИ2.

2в. По протоколу U0/U1 (TCP 1189, UDP 1024-65535) к сопряжённому агенту СА от АИ1, от АИ2 и от СУ.

2г. По протоколу HTTP (TCP 80) к сопряжённому агенту СА от АИ1 и от АИ2.

2д. По протоколу U9 (UDP 1024-65535) к сопряжённому агенту СА от АИ1 и от АИ2.

2е. По протоколу NTP (TCP/UDP 123) от АИ1, от АИ2 и от СУ. Это крайне желательно!

3. Агенты АИ1 и АИ2 имеют адреса **10.55.1.10/24** и **10.55.1.20/24** соответственно. Если на сети лаборатории применяются особенные настройки безопасности, то следует дополнительно к изложенному в пункте 2 обеспечить доступ:

3а. По протоколу FTP (passive) от агентов АИ1 и АИ2 к системе управления СУ.

3б. По протоколу SSH к агентам АИ1 и АИ2 от системы управления или рабочего места проверяющего.

3в. По протоколу U0/U1 (TCP 1189, UDP 1024-65535) к агентам АИ1 и АИ2 от СУ.

3г. По протоколу SNMP (UDP 161) к агентам АИ1 и АИ2 от СУ.

4. Система управления СУ имеет адрес **10.55.1.100/24**. Если на сети лаборатории применяются особенные настройки безопасности, то следует дополнительно к изложенному в пунктах 2 и 3:

4а. По протоколу SSH к системе управления от рабочего места проверяющего.

4б. По протоколу HTTP к системе управления от рабочего места проверяющего.

5. DNS-сервер имеет адрес, который заранее указать невозможно. Его следует установить проверяющему самостоятельно, возможно, с помощью персонала, имеющего эту информацию. В настоящей документации будет использоваться адрес **D.D.D.D.**

6. Сопряжённый агент СА на площадке Производителя сообщается проверяющему по согласованным каналам связи в рамках процесса проверки. Заранее его указать сложно. В настоящей документации будет использоваться адрес **C.C.C.C.**

7. Агенты АИ1 и АИ2 крайне рекомендуется устанавливать на реальном аппаратном обеспечении. Система управления СУ может быть установлена на виртуальной машине. В случае отсутствия в лаборатории подходящего аппаратного обеспечения, агенты АИ1 и АИ2 так же могут быть установлены на виртуальные машины, в этом случае точность измеряемых метрик качества может быть снижена за счёт недостатков, присущих виртуальным средам априори.

### 3 Начальные проверки агентов

Установка агентов на АИ1 и АИ2 выполняются согласно руководству «Запуск IQM на ОС Альт 10». При штатной работе после установки агента остальные действия осуществляются из web-интерфейса IQMM (СУ). Однако, так как проверка работы на новой ОС может требовать большего внимания, мы описываем контрольные точки для того, чтобы убедиться в правильном функционировании агента. Например для АИ1.

1. Прежде всего, следует убедиться, что агент запущен с использованием штатной системы управления процессами — `systemd`. Это делается командой

```
$ systemctl status iqma
```

Результат должен выглядеть, как показано на [рисунке 2](#).

**Рисунок 2.**

```
[cae@alt10-iqma1 ~]$ systemctl status iqma
● iqma.service - IQM Agent
   Loaded: loaded (/lib/systemd/system/iqma.service; enabled; vendor preset: |
   Active: active (running) since Wed 2025-11-19 08:20:13 UTC; 1h 21min ago
   Main PID: 2720 (iqm_agent)
     Tasks: 10 (limit: 2133)
    Memory: 11.3M
         CPU: 15.131s
    CGroup: /system.slice/iqma.service
           └─ 2720 /usr/local/iqm_agent/iqm_agent --pidfile=/var/run/iqm_agen|
Nov 19 08:20:13 alt10-iqma1 systemd[1]: Starting IQM Agent...
Nov 19 08:20:13 alt10-iqma1 systemd[1]: Started IQM Agent.
Nov 19 08:20:14 alt10-iqma1 systemd[1]: /lib/systemd/system/iqma.service:22: PI|
Nov 19 08:20:14 alt10-iqma1 systemd[1]: /lib/systemd/system/iqma.service:22: PI|
[cae@alt10-iqma1 ~]$
```

Основными важными моментами являются состояния `loaded` и `enabled`. То есть, процесс должен быть активным и настроенным на перезапуск на запуске устройства.

2. Так же стоит убедиться, что процесс запущен с верными ключами командной

строки. Это проще всего сделать командой

```
$ ps -axww | grep iqm_agent
```

Результат должен выглядеть, как показано на [рисунке 3](#).

### Рисунок 3.

```
[cae@alt10-iqmal ~]$ ps -axww|grep iqm_agent
 2720 ?          Ssl    0:07 /usr/local/iqm_agent/iqm_agent --pidfile=/var/run/iqm_agent.pid --log=/var/log/iqm_agent.log --level=5 --config=/etc/iqm_agent.conf @/usr/local/iqm_agent/iqm_agent.args
 3140 pts/0    S+     0:00 grep --color=auto iqm_agent
[cae@alt10-iqmal ~]$
```

Основными важными моментами являются правильное указание метода журналирования (в поставке — в файл) и его уровня, а так же файла конфигурации агента. Кроме того, настоятельно рекомендуется сохранять чтение параметров запуска из дополнительного файла для удобства тонкой настройки. Подробнее в отдельной документации.

3. В поставке файл дополнительных параметров запуска пуст. В этом можно убедиться командой

```
# cat /usr/local/iqm_agent/iqm_agent.args
```

Результат должен выглядеть, как показано на [рисунке 4](#).

### Рисунок 4.

```
[root@alt10-iqmal ~]# cat /usr/local/iqm_agent/iqm_agent.args
[root@alt10-iqmal ~]#
```

В указанном файле можно перечислить дополнительные настройки. Для данного тестирования они не применяются (файл существует, но пуст), однако, если потребуется, либо проверяющий, либо производитель агента может внести дополнительные изменения.

4. В корректности файла конфигурации можно убедиться командой

```
# cat /etc/iqm_agent.conf
```

Результат должен выглядеть, как показано на [рисунке 5](#).



**Рисунок 6.**

```
[cae@alt10-iqmal ~]$ tail -f /var/log/iqm_agent.log
2025/11/19 10:01:25 iqm_agent[2720;2779] Warn: send: put_stats: Cannot connect t
o iqmm: Net::FTP: Bad hostname 'iqmm' at /usr/local/iqm_agent/sender.pl line 39.
2025/11/19 10:01:27 iqm_agent[2720;2776] Err: ccc: Temporary failure in name res
olution at addr_inet46::setaddr(iqmm)
2025/11/19 10:01:47 iqm_agent[2720;2776] Err: ccc: Temporary failure in name res
olution at addr_inet46::setaddr(iqmm)
2025/11/19 10:02:07 iqm_agent[2720;2776] Err: ccc: Temporary failure in name res
olution at addr_inet46::setaddr(iqmm)
2025/11/19 10:02:09 iqm_agent[2720;3215] Err: SYS: Connection timed out at sockw
/buf::recvfrom(127.0.0.1:123)
2025/11/19 10:02:25 iqm_agent[2720;2779] Warn: send: put_stats: Cannot connect t
o iqmm: Net::FTP: Bad hostname 'iqmm' at /usr/local/iqm_agent/sender.pl line 39.
2025/11/19 10:02:27 iqm_agent[2720;2776] Err: ccc: Temporary failure in name res
olution at addr_inet46::setaddr(iqmm)
2025/11/19 10:02:47 iqm_agent[2720;2776] Err: ccc: Temporary failure in name res
olution at addr_inet46::setaddr(iqmm)
2025/11/19 10:03:07 iqm_agent[2720;2776] Err: ccc: Temporary failure in name res
olution at addr_inet46::setaddr(iqmm)
2025/11/19 10:03:09 iqm_agent[2720;3218] Err: SYS: Connection timed out at sockw
/buf::recvfrom(127.0.0.1:123)
^C
[cae@alt10-iqmal ~]$
```

Самым важным моментом является наличие журнала агента, как такового. Обычно не пустого, так как адрес устройства в сети с именем `iqmm` как правило не прописан, поэтому ошибки доставки как файлов результатов, так и попытки соединиться с демоном ССС для работы изнутри NAT будут безуспешными, и, следовательно, отразятся в журнале.

Например, на рисунке видно обращение модуля `send`, который запускает программу отсылки файлов результатов, но та не может найти имя `iqmm`. Так же видно, что попытка модуля `ccc` связаться с демоном на имя `iqmm` так же безуспешна. Агент же при этом продолжает нормальную работу, в частности системный тест `SYS` (сбор данных устройства), успешно завершается за исключением обращения в демон `ntpd` (в демон `chronyd` при этом обращение проходит успешно, так как записей об этом нет).

В целом, при отсутствии грубых ошибок в журнале (допустим, аварийного останова), можно считать, что агент работает нормально.

Аналогично можно провести и проверку агента АИ2. Агент СА в схеме тестирования находится в зоне ответственности Производителя и в проверке не нуждается.

## 4 Начальные проверки системы управления

Установка системы управления на СУ выполняются согласно руководству «Запуск IQM на ОС Альт 10». После установки все сервисы обычно запускаются автоматически. И основная работа проводится через `web`-интерфейс. Однако, поскольку система управления состоит из многих модулей, а у тестирующего скорее всего мало опыта в работе с IQMM, то мы приводим подробные шаги для проверки работоспособности.

1. Для того, чтобы иметь возможность работать на родном языке следует выполнить следующие команды

```
$ cat <<EOFEOF >~/ .i18n
LANG=ru_RU.UTF-8
EOFEOF
```

после чего следует выйти и повторно зайти на СУ на тот же логический терминал, либо по SSH другой сессией. Более подробная настройка языка вывода shell выходит за рамки настоящей документации. В случае SSH не забудьте о настройке клиента! Результат может выглядеть, как показано на [рисунке 7](#).

**Рисунок 7.**

```
[cae@alt10-iqmm ~]$ cat <<EOFEOF >~/ .i18n
> LANG=ru_RU.UTF-8
> EOFEOF
[cae@alt10-iqmm ~]$
```

Теперь, просматривая в shell те файлы, где будут встречаться русские сообщения, вы сможете их видеть без проблем.

2. Чтобы убедиться, что основная структура каталогов имеет правильный вид и права, можно выполнить команду

```
# ls -la /home/iqm
```

Результат может выглядеть, как показано на [рисунке 8](#).

**Рисунок 8.**

```
[root@alt10-iqmm ~]# ls -la /home/iqm
итого 28
drwx--x---  7 iqm  iqm  4096 ноя 21 15:45 .
drwxr-xr-x  4 root root  4096 ноя 19 11:51 ..
drwxrwx---  2 iqm  iqm  4096 ноя 21 15:45 cfg
drwxr-x--- 12 iqm  iqm  4096 ноя 21 16:01 iqmm
drwxr-x---  2 iqm  iqm  4096 ноя 21 15:45 log
drwxrwx---  4 iqm  iqm  4096 дек  3 12:58 stat
drwxrwx---  2 iqm  iqm  4096 ноя 21 15:45 upload
[root@alt10-iqmm ~]#
```

Каталог `iqmm` содержит системные файлы, каталог `log` – журналы, `stat` – файлы результатов тестов, `upload` – для временных файлов, `cfg` – для хранения конфигураций агентов типа `REMOTE_IQM`. Все каталоги должны принадлежать пользователю `iqm` и группе `iqm`.

3. Поскольку IQMM хранит результаты в базе данных, следует проверить работоспособность соответствующего сервера. Первичную проверку можно исполнить

следующей командой

```
$ systemctl status mysqld
```

Результат может выглядеть, как показано на [рисунке 9](#).

### Рисунок 9.

```
[cae@alt10-iqmm ~]$ systemctl status mysqld
● mysqld.service - MariaDB database server
   Loaded: loaded (/lib/systemd/system/mysqld.service; enabled; vendor pre
   Drop-In: /etc/systemd/system/mysqld.service.d
           └─notify-chroot.conf, notify.conf, user.conf
   Active: active (running) since Fri 2024-02-09 18:58:35 UTC; 1 year 9 mo
   Docs: man:mysqld(8)
         https://mariadb.com/kb/en/library/systemd/
   Process: 2325 ExecStartPre=/usr/sbin/mysql_install_db (code=exited, stat
   Process: 2394 ExecStartPre=/etc/chroot.d/mysql.all (code=exited, status=
   Main PID: 2839 (mysqld)
     Tasks: 14 (limit: 4555)
    Memory: 84.0M
       CPU: 7.816s
    CGroup: /system.slice/mysqld.service
           └─ 2839 /usr/sbin/mysqld

фев 09 18:58:17 alt10-iqmm systemd[1]: Starting MariaDB database server...
фев 09 18:58:35 alt10-iqmm systemd[1]: Started MariaDB database server.
[cae@alt10-iqmm ~]$
```

Основными важными моментами являются состояния `loaded`, `enabled` и `active`. Дополнительно следует проверить схему данных IQMM внутри сервера баз данных. Это можно сделать командами

```
$ mysql -uiqmadm -p iqm
> select * from classes where class_name in ('BE', 'BC', 'RT');
> \q
```

Пароль для входа в клиент базы данных следует использовать из тех, что записаны на этапе установки IQMM, описанном в руководстве «Запуск IQM на ОС Альт 10». Результат может выглядеть, как показано на [рисунке 10](#).

**Рисунок 10.**

```
[cae@alt10-iqmm ~]$ mysql -uiqmadm -p iqm
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 11
Server version: 10.6.24-MariaDB-alt1 (ALT p10)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [iqm]> select * from classes where class_name in ('BE','BC','RT');
+-----+-----+-----+-----+
| class_id | class_name | precedence | class_description |
+-----+-----+-----+-----+
|         2 | BC         |          1 | Business critical |
|         1 | BE         |          0 | Best effort       |
|         6 | RT         |          5 | Realtime          |
+-----+-----+-----+-----+
3 rows in set (0,002 sec)

MariaDB [iqm]> \q
Bye
[cae@alt10-iqmm ~]$
```

Следует обратить внимание, чтобы содержимое результата `select` было не только не пустым, но и соответствующим по полям `precedence` изображённому на рисунке 9. Содержимое поля `class_description` факультативно.

4. Агент IQMA доставляет результаты тестов на IQMM по протоколу FTP, поэтому следует проверить работоспособность соответствующего сервера. Первичную проверку можно исполнить следующей командой

```
# ss -anp|grep xinetd
```

Результат может выглядеть, как показано на [рисунке 11](#).

**Рисунок 11.**

```
[root@alt10-iqmm ~]# ss -anp|grep xinetd
u_dgr ESTAB 0      0                                     * 13309
      * 1863  users:(("xinetd",pid=2312,fd=7))

tcp    LISTEN 0      64                                     0.0.0.0:21
      0.0.0.0:*   users:(("xinetd",pid=2312,fd=6))

[root@alt10-iqmm ~]#
```

Основным признаком верной работы является наличие `tcp`-сокета на порту `:21`, который «слушает» суперсервер `xinetd`.

Поскольку по умолчанию ОС «Альт» не поставляется `ftp`-клиент, его следует поставить. Это выполняется командой

```
# apt-get install ftp
```

Результат может выглядеть, как показано на [рисунке 12](#).

**Рисунок 12.**

```
[root@alt10-iqmm ~]# apt-get install ftp
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие НОВЫЕ пакеты будут установлены:
  ftp
0 будет обновлено, 1 новых установлено, 0 пакетов будет удалено и 86 не будет
новлено.
Необходимо получить 0В/52,0кВ архивов.
После распаковки потребуется дополнительно 104кВ дискового пространства.
Совершаем изменения...
Подготовка... ##### [10
Обновление / установка...
1: ftp-0.18-alt0.pre1.3 ##### [10
Завершено.
[root@alt10-iqmm ~]# █
```

Теперь можно проверить доступность ftp-сервера для доставки результатов. Это делается командами

```
$ ftp localhost
Name: iqmmmon
Password: Пароль
ftp> cd stat
ftp> put .i18n i18n
ftp> ls -la
ftp> quit
```

В качестве **пароля** следует использовать ftp-пароль, указанный при установке по руководству «Запуск IQM на ОС Альт 10». Результат может выглядеть, как показано на [рисунке 13](#).

**Рисунок 13.**

```

[cae@alt10-iqmm ~]$ ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPD 3.0.3)
Name (localhost:cae): iqmmmon
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd stat
250 Directory successfully changed.
ftp> put .i18n i18n
local: .i18n remote: i18n
227 Entering Passive Mode (127,0,0,1,202,22).
150 Ok to send data.
226 Transfer complete.
17 bytes sent in 0,000197 secs (86,29 Kbytes/sec)
ftp> ls -la
227 Entering Passive Mode (127,0,0,1,253,51).
150 Here comes the directory listing.
drwxrwx---      3 ftp      ftp      4096 Nov 19 18:10 .
dr-xr-x---      4 ftp      ftp      4096 Nov 19 08:49 ..
-rw-r--r--      1 ftp      ftp           17 Nov 19 18:10 i18n
drwxrwx---      2 ftp      ftp      4096 Oct 24 16:38 old
226 Directory send OK.
ftp> quit
221 Goodbye.
[cae@alt10-iqmm ~]$ █

```

Следует внимательно исследовать результаты. Должен быть зафиксирован корректный вход (то есть верные имя и пароль), успешный переход в каталог хранения результатов (stat), успешная передача файла .i18n на ftp-сервер под именем i18n, проверка доставки файла командой `ls -la`.

5. В процессе работы IQMM могут доставляться SNMP-сообщения (traps) о проблемах. Одним из вариантов их приёма является запуск принимающего демона прямо на IQMM. Проверку запуска такого сервера можно сделать следующей командой

```
# ss -anp|grep snmptrap
```

Результат может выглядеть, как показано на [рисунке 14](#).

**Рисунок 14.**

```
[root@alt10-iqmm ~]# ss -anp|grep snmptrapd
u_str ESTAB 0      0                                     * 14212
      * 14213 users:(("snmptrapd",pid=2350,fd=2), ("snmptrapd",pid=2350,fd
=1))

udp      UNCONN 0      0                                     127.0.0.1:162
      0.0.0.0:*      users:(("snmptrapd",pid=2350,fd=8))

[root@alt10-iqmm ~]#
```

На UDP-сокете :162 должен быть демон snmptrapd в приёмном режиме.

6. Основную работу с IQMM проводят через web-интерфейс. Первичную проверку доступности можно провести командами

```
# ss -anp|grep :80
```

Результат может выглядеть, как показано на [рисунке 15](#).

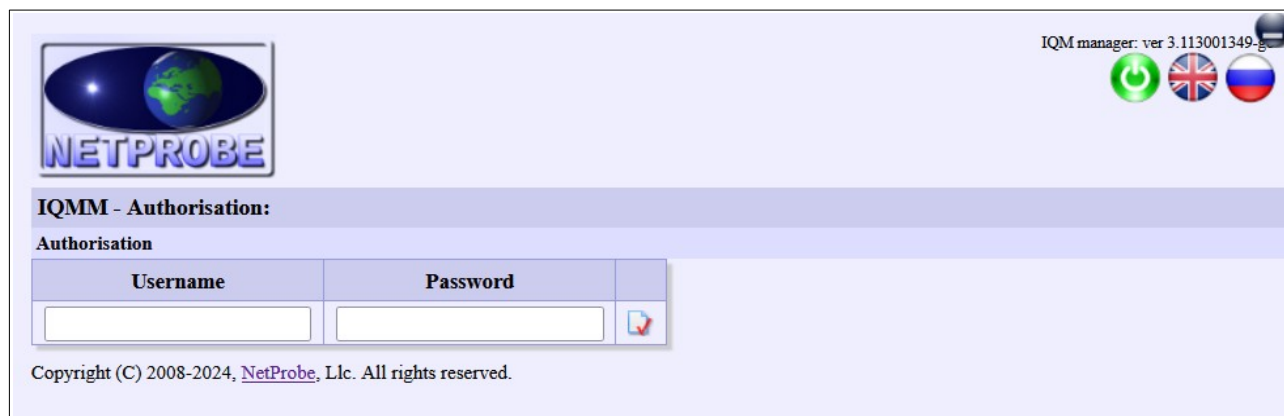
**Рисунок 15.**

```
[root@alt10-iqmm ~]# ss -anp|grep :80
tcp      LISTEN 0      511                                     *:80
      *:*      users:(("httpd2",pid=2908,fd=4), ("httpd2",pid=2907,fd=4), ("
httpd2",pid=2358,fd=4))

[root@alt10-iqmm ~]#
```

В ответе следует обратить внимание, что есть демон httpd2, прослушивающий TCP-сокеты :80. Иначе доступа к web-интерфейсу не будет, что сделает невозможным полноценную работу с IQMM.

Окончательную проверку доступности web-интерфейса можно провести через браузер (Firefox, Chrome), установленный на рабочем месте проверяющего. Следует вызвать URL `http://10.55.1.100/iqmm/`. Доступность сети от рабочего места до IQMM мы полагаем уже существующей, так как вы дошли до этого места. Результат может выглядеть, как показано на [рисунке 16](#).

**Рисунок 16.**

В случае недоступности страницы авторизации пользователей IQMM следует связаться с Производителем. Наиболее распространённой ошибкой является неверные имена и пароли к базе данных. При штатной установке по командам, приведённым в документации, этого происходить не должно. Дальнейшая работа через web-интерфейс будет проводиться позже, пока следует вернуться в командный режим shell.

7. Важным элементом IQMM являются системные демоны, выполняющие функции, необходимые помимо web-интерфейса. Одним из демонов является опросник активности агентов (aac). Проверку его активности можно провести командами

```
$ systemctl status iqmm-aac
```

Результат может выглядеть, как показано на [рисунке 17](#).

**Рисунок 17.**

```
[cae@alt10-iqmm ~]$ systemctl status iqmm-aac
● iqmm-aac.service - IQM Manager agents checker
   Loaded: loaded (/lib/systemd/system/iqmm-aac.service; enabled; vendor pre
   Active: active (running) since Wed 2025-11-19 18:00:37 UTC; 1h 21min ago
   Process: 2194 ExecStart=/home/iqm/iqmm/scripts/iqmm-aac3.pl (code=exited,
   Main PID: 2278 (iqmm-aac3: sleep)
   Tasks: 1 (limit: 4555)
   Memory: 22.5M
   CPU: 2.513s
   CGroup: /system.slice/iqmm-aac.service
           └─ 2278 "iqmm-aac3: sleep"

ноя 19 18:00:22 alt10-iqmm systemd[1]: Starting IQM Manager agents checker...
ноя 19 18:00:36 alt10-iqmm iqmm-aac3.pl[2194]: Subroutine main::_ redefined at
ноя 19 18:00:37 alt10-iqmm systemd[1]: Started IQM Manager agents checker.
[cae@alt10-iqmm ~]$
```

Процесс должен быть активен, загружен и включен. Дополнительную проверку можно провести просмотром журнала демона. Это можно сделать командами

```
$ tail -f /home/iqm/log/iqmm-aac3.log
```

Результат может выглядеть, как показано на [рисунке 18](#).

**Рисунок 18.**

```
[cae@alt10-iqmm ~]$ tail -f /home/iqm/log/iqmm-aac3.log
Wed Nov 19 09:14:22 2025 notice, Main[7328]: start iqmm-aac3 NetProbe::IQM::Alar
mer::AacDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Fri Feb 9 18:58:31 2024 notice, Main[2246]: start iqmm-aac3 NetProbe::IQM::Alar
mer::AacDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Fri Feb 9 18:58:32 2024 err, __ANON__ [2246]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
Fri Feb 9 18:58:30 2024 notice, Main[2393]: start iqmm-aac3 NetProbe::IQM::Alar
mer::AacDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Fri Feb 9 18:58:32 2024 err, __ANON__ [2393]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
Wed Nov 19 18:00:37 2025 notice, Main[2278]: start iqmm-aac3 NetProbe::IQM::Alar
mer::AacDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Wed Nov 19 18:00:38 2025 err, __ANON__ [2278]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
^C
[cae@alt10-iqmm ~]$
```

В журнале могут быть редкие сообщения о недоступности базы данных. В текущее же время ошибок доступа быть не должно, а доступность агентов пока не показывается ввиду отсутствия их в базе.

8. Одним из системных демонов является обработчик файлов данных (r2). Проверку его активности можно провести командами

```
$ systemctl status iqmm-r2
```

Результат может выглядеть, как показано на [рисунке 19](#).

**Рисунок 19.**

```
[cae@alt10-iqmm ~]$ systemctl status iqmm-r2
● iqmm-r2.service - IQM Manager Receive Daemon
   Loaded: loaded (/lib/systemd/system/iqmm-r2.service; enabled; vendor prese
   Active: active (running) since Wed 2025-11-19 18:00:36 UTC; 1h 44min ago
   Process: 2198 ExecStart=/home/iqm/iqmm/scripts/iqmm-r2.pl (code=exited, sta
   Main PID: 2273 (iqmm-r2: sleep)
     Tasks: 1 (limit: 4555)
    Memory: 18.5M
         CPU: 53.319s
    CGroup: /system.slice/iqmm-r2.service
           └─ 2273 "iqmm-r2: sleep"

ноя 19 18:00:22 alt10-iqmm systemd[1]: Starting IQM Manager Receive Daemon...
ноя 19 18:00:36 alt10-iqmm systemd[1]: Started IQM Manager Receive Daemon.
[cae@alt10-iqmm ~]$
```

Процесс должен быть активен, загружен и включен. Дополнительную проверку можно провести просмотром журнала демона. Это можно сделать командами

```
$ tail -f /home/iqm/log/iqmm-r2.log
```

Результат может выглядеть, как показано на [рисунке 20](#).

**Рисунок 20.**

```
[cae@alt10-iqmm ~]$ tail -f /home/iqm/log/iqmm-r2.log
Wed Nov 19 09:14:22 2025 notice, Main[7340]: start iqmm-r2 NetProbe::IQM::Alarme
r::RawDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Fri Feb 9 18:58:31 2024 notice, Main[2238]: start iqmm-r2 NetProbe::IQM::Alarme
r::RawDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Fri Feb 9 18:58:32 2024 err, __ANON__[2238]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
Wed Nov 19 15:20:54 2025 err, __ANON__[2238]: Receive SIGTERM
Wed Nov 19 15:20:54 2025 notice, Main[2238]: finish iqmm-r2 NetProbe::IQM::Alarm
er::RawDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Fri Feb 9 18:58:30 2024 notice, Main[2391]: start iqmm-r2 NetProbe::IQM::Alarme
r::RawDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Fri Feb 9 18:58:32 2024 err, __ANON__[2391]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
Wed Nov 19 18:00:36 2025 notice, Main[2273]: start iqmm-r2 NetProbe::IQM::Alarme
r::RawDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Wed Nov 19 18:00:38 2025 err, __ANON__[2273]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
^C
[cae@alt10-iqmm ~]$
```

В журнале могут быть редкие сообщения о недоступности базы данных. В текущее же время ошибок доступа быть не должно, а вставка данных от агентов пока не показывается ввиду отсутствия их в базе.

9. Одним из системных демонов является инспектор выхода за границы порогов (a2). Проверку его активности можно провести командами

```
$ systemctl status iqmm-a2
```

Результат может выглядеть, как показано на [рисунке 21](#).

**Рисунок 21.**

```
[cae@alt10-iqmm ~]$ systemctl status iqmm-a2
● iqmm-a2.service - IQM Manager Alarm Daemon
   Loaded: loaded (/lib/systemd/system/iqmm-a2.service; enabled; vendor prese
   Active: active (running) since Wed 2025-12-03 13:17:32 MSK; 1h 10min ago
   Process: 2817 ExecStart=/home/iqm/iqmm/scripts/iqmm-al2.pl (code=exited, st
   Main PID: 2863 (iqmm-al2: sleep)
      Tasks: 1 (limit: 4555)
     Memory: 14.1M
           CPU: 2.112s
    CGroup: /system.slice/iqmm-a2.service
            └─ 2863 "iqmm-al2: sleep"

дек 03 13:17:28 alt10-iqmm systemd[1]: Starting IQM Manager Alarm Daemon...
дек 03 13:17:30 alt10-iqmm iqmm-al2.pl[2817]: Useless use of a variable in void
дек 03 13:17:31 alt10-iqmm iqmm-al2.pl[2817]: Name "cfg::np_alarmdaemon_sleep_t
дек 03 13:17:32 alt10-iqmm systemd[1]: Started IQM Manager Alarm Daemon.
[cae@alt10-iqmm ~]$
```

Процесс должен быть активен, загружен и включен. Дополнительную проверку можно

провести просмотром журнала демона. Это можно сделать командами

```
$ tail -f /home/iqm/log/iqmm-a12.log
```

Результат может выглядеть, как показано на [рисунке 22](#).

### Рисунок 22.

```
Fri Feb 9 18:58:30 2024 notice, Main[2385]: start iqmm-a12 NetProbe::IQM::Alarm
er::AlDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Fri Feb 9 18:58:32 2024 err, __ANON__ [2385]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
Wed Nov 19 18:00:36 2025 notice, Main[2272]: start iqmm-a12 NetProbe::IQM::Alarm
er::AlDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Wed Nov 19 18:00:38 2025 err, __ANON__ [2272]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
Fri Feb 9 18:58:31 2024 notice, Main[2235]: start iqmm-a12 NetProbe::IQM::Alarm
er::AlDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Fri Feb 9 18:58:32 2024 err, __ANON__ [2235]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
Fri Feb 9 18:58:31 2024 notice, Main[2338]: start iqmm-a12 NetProbe::IQM::Alarm
er::AlDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Fri Feb 9 18:58:32 2024 err, __ANON__ [2338]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
^C
[cae@alt10-iqmm ~]$
```

В журнале могут быть редкие сообщения о недоступности базы данных. В текущее же время ошибок доступа быть не должно, а обработка данных от агентов на пороги пока не показывается ввиду отсутствия их в базе.

10. Одним из системных демонов является экспедитор уведомлений о проблемах на сети (n2). Проверку его активности можно провести командами

```
$ systemctl status iqmm-n2
```

Результат может выглядеть, как показано на [рисунке 23](#).

**Рисунок 23.**

```
[cae@alt10-iqmm ~]$ systemctl status iqmm-n2
● iqmm-n2.service - IQM Manager Notify Daemon
   Loaded: loaded (/lib/systemd/system/iqmm-n2.service; enabled; vendor prese
   Active: active (running) since Wed 2025-12-03 13:17:36 MSK; 1h 20min ago
   Process: 2821 ExecStart=/home/iqm/iqmm/scripts/iqmm-no2.pl (code=exited, st
   Main PID: 2885 (iqmm-no2: sleep)
      Tasks: 1 (limit: 4555)
     Memory: 33.0M
          CPU: 2.179s
    CGroup: /system.slice/iqmm-n2.service
           └─ 2885 "iqmm-no2: sleep"

дек 03 13:17:28 alt10-iqmm systemd[1]: Starting IQM Manager Notify Daemon...
дек 03 13:17:35 alt10-iqmm iqmm-no2.pl[2821]: Subroutine main::_ redefined at /
дек 03 13:17:35 alt10-iqmm iqmm-no2.pl[2821]: trace: netsnmp_ds_set_boolean():
дек 03 13:17:35 alt10-iqmm iqmm-no2.pl[2821]: netsnmp_ds_set_boolean: Setting L
дек 03 13:17:35 alt10-iqmm iqmm-no2.pl[2821]: Name "cfg::np_alarmdaemon_sleep_t
дек 03 13:17:36 alt10-iqmm systemd[1]: Started IQM Manager Notify Daemon.
[cae@alt10-iqmm ~]$
```

Процесс должен быть активен, загружен и включен. Дополнительную проверку можно провести просмотром журнала демона. Это можно сделать командами

```
$ tail -f /home/iqm/log/iqmm-no2.log
```

Результат может выглядеть, как показано на [рисунке 24](#).

**Рисунок 24.**

```
[cae@alt10-iqmm ~]$ tail -f /home/iqm/log/iqmm-no2.log
Wed Nov 19 18:00:43 2025 err, __ANON__[2755]: snmp_read_mib: reading MIB: /home/
iqm/iqmm/doc/NP-IQM3-NOTIFICATION-MIB.txt
Wed Nov 19 18:00:43 2025 err, __ANON__[2755]: done
Fri Feb 9 18:58:35 2024 notice, Main[2604]: start iqmm-no2 NetProbe::IQM::Alarm
er::NoDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Fri Feb 9 18:58:35 2024 err, __ANON__[2604]: snmp_read_mib: reading MIB: /home/
iqm/iqmm/doc/NP-IQM3-NOTIFICATION-MIB.txt
Fri Feb 9 18:58:35 2024 err, __ANON__[2604]: done
Fri Feb 9 18:58:35 2024 err, __ANON__[2604]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
Fri Feb 9 18:58:35 2024 notice, Main[2699]: start iqmm-no2 NetProbe::IQM::Alarm
er::NoDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Fri Feb 9 18:58:35 2024 err, __ANON__[2699]: snmp_read_mib: reading MIB: /home/
iqm/iqmm/doc/NP-IQM3-NOTIFICATION-MIB.txt
Fri Feb 9 18:58:35 2024 err, __ANON__[2699]: done
Fri Feb 9 18:58:35 2024 err, __ANON__[2699]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
^C
[cae@alt10-iqmm ~]$
```

В журнале могут быть редкие сообщения о недоступности базы данных. В текущее же время ошибок доступа быть не должно, а поскольку данных от агентов нет, то и уведомлений тоже не будет.

11. Одним из системных демонов является чистильщик старых данных(d2). Проверку его активности можно провести командами

```
$ systemctl status iqmm-d2
```

Результат может выглядеть, как показано на [рисунке 25](#).

**Рисунок 25.**

```
[cae@alt10-iqmm ~]$ systemctl status iqmm-d2
● iqmm-d2.service - IQM Manager Delete old Daemon
   Loaded: loaded (/lib/systemd/system/iqmm-d2.service; enabled; vendor prese
   Active: active (running) since Wed 2025-12-03 13:17:31 MSK; 1h 25min ago
   Process: 2819 ExecStart=/home/iqm/iqmm/scripts/iqmm-dl2.pl (code=exited, st
   Main PID: 2859 (iqmm-dl2: sleep)
     Tasks: 1 (limit: 4555)
    Memory: 17.2M
         CPU: 997ms
    CGroup: /system.slice/iqmm-d2.service
           └─ 2859 "iqmm-dl2: sleep"

дек 03 13:17:28 alt10-iqmm systemd[1]: Starting IQM Manager Delete old Daemon..
дек 03 13:17:30 alt10-iqmm iqmm-dl2.pl[2819]: Subroutine main::_ redefined at /
дек 03 13:17:31 alt10-iqmm systemd[1]: Started IQM Manager Delete old Daemon.
[cae@alt10-iqmm ~]$
```

Процесс должен быть активен, загружен и включен. Дополнительную проверку можно провести просмотром журнала демона. Это можно сделать командами

```
$ tail -f /home/iqm/log/iqmm-dl2.log
```

Результат может выглядеть, как показано на [рисунке 26](#).

**Рисунок 26.**

```
[cae@alt10-iqmm ~]$ tail -f /home/iqm/log/iqmm-dl2.log
Fri Feb  9 18:58:32 2024 err,  __ANON__ [2337]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
Thu Nov 20 13:21:17 2025 note, check_delete[2337]: Deleted from alarm_aggrs 0 te
st rows where <2024-11-20 13:21:17
Thu Nov 20 13:21:17 2025 note, check_delete[2337]: Deleted from alarm_aggrs 0 sy
s rows where <2024-11-20 13:21:17
Thu Nov 20 13:21:17 2025 note, check_delete[2337]: Deleted from ddraw 0 rows whe
re <2024-11-20 13:21:17
Thu Nov 20 13:21:17 2025 note, check_delete[2337]: Deleted from dtaggr1 0 rows w
here <2024-11-20 13:21:17
Thu Nov 20 13:21:17 2025 note, check_delete[2337]: Deleted from dtaggr2 0 rows w
here <2024-11-20 13:21:17
Thu Nov 20 13:21:17 2025 note, check_delete[2337]: Deleted from ddrawppp 0 rows
where <2024-11-20 13:21:17
Thu Nov 20 13:21:17 2025 note, check_delete[2337]: Deleted from ddrawsys 0 rows
where <2024-11-20 13:21:17
Thu Nov 20 13:21:17 2025 note, check_delete[2337]: Deleted from dtond 0 rows whe
re <2024-11-20 13:21:17
Thu Nov 20 13:21:17 2025 note, check_delete[2337]: Deleted from mnts 0 rows wher
e <2024-11-20 13:21:17
^C
[cae@alt10-iqmm ~]$
```

В журнале могут быть редкие сообщения о недоступности базы данных. В текущее же

время ошибок доступа быть не должно, а сообщения об очистке данных, как правило, должны быть с числом записей равных нулю.

12. Одним из системных демонов является синхронизатор периодов работ(m2). Проверку его активности можно провести командами

```
$ systemctl status iqmm-m2
```

Результат может выглядеть, как показано на [рисунке 27](#).

**Рисунок 27.**

```
[cae@alt10-iqmm ~]$ systemctl status iqmm-m2
● iqmm-m2.service - IQM Manager Mwaudit Daemon
   Loaded: loaded (/lib/systemd/system/iqmm-m2.service; enabled; vendor prese
   Active: active (running) since Fri 2024-02-09 18:58:31 UTC; 1 year 9 month
   Process: 2272 ExecStart=/home/iqm/iqmm/scripts/iqmm-mw2.pl (code=exited, st
   Main PID: 2334 (iqmm-mw2: sleep)
   Tasks: 1 (limit: 4555)
   Memory: 14.0M
   CPU: 1.072s
   CGroup: /system.slice/iqmm-m2.service
           └─ 2334 "iqmm-mw2: sleep"

Фев 09 18:58:18 alt10-iqmm systemd[1]: Starting IQM Manager Mwaudit Daemon...
Фев 09 18:58:31 alt10-iqmm systemd[1]: Started IQM Manager Mwaudit Daemon.
[cae@alt10-iqmm ~]$
```

Процесс должен быть активен, загружен и включен. Дополнительную проверку можно провести просмотром журнала демона. Это можно сделать командами

```
$ tail -f /home/iqm/log/iqmm-mw2.log
```

Результат может выглядеть, как показано на [рисунке 28](#).

**Рисунок 28.**

```
Fri Feb 9 18:58:30 2024 notice, Main[2387]: start iqmm-mw2 NetProbe::IQM::Alarm
er::MwDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Fri Feb 9 18:58:32 2024 err, __ANON__ [2387]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
Wed Nov 19 18:00:36 2025 notice, Main[2267]: start iqmm-mw2 NetProbe::IQM::Alarm
er::MwDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Wed Nov 19 18:00:38 2025 err, __ANON__ [2267]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
Fri Feb 9 18:58:31 2024 notice, Main[2233]: start iqmm-mw2 NetProbe::IQM::Alarm
er::MwDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Fri Feb 9 18:58:32 2024 err, __ANON__ [2233]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
Fri Feb 9 18:58:31 2024 notice, Main[2334]: start iqmm-mw2 NetProbe::IQM::Alarm
er::MwDaemon version 2.02 (C) Sergey A.Eremenko and NetProbe Llc
Fri Feb 9 18:58:32 2024 err, __ANON__ [2334]: sql error DBI connect('database=iq
m;host=localhost;port=3306','iqmweb',...) failed: Can't connect to local MySQL s
erver through socket '/var/lib/mysql/mysql.sock' (111)
^C
[cae@alt10-iqmm ~]$
```

В журнале могут быть редкие сообщения о недоступности базы данных. В текущее же время ошибок доступа быть не должно, а иных сообщений быть не может, так как в первичной схеме данных периоды работ отсутствуют.

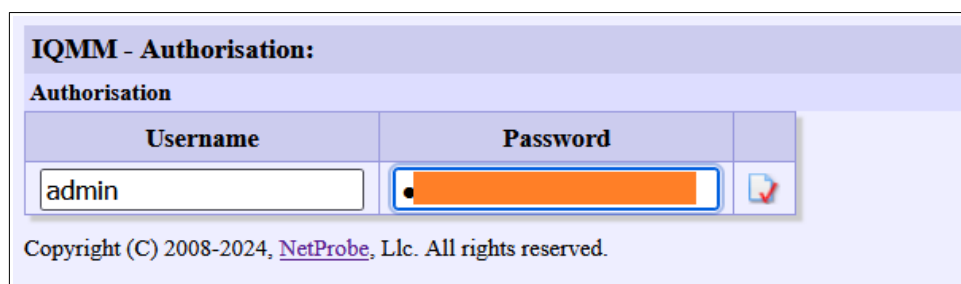
После окончания всех указанных этапов можно считать первичную проверку функционирования СУ на новой ОС пройденной.

## 5 Заведение агента АИ1 в системе управления

Теперь можно перейти в web-интерфейс. Мы будем все задачи выполнять под супервизором системы — имя `admin`. Тестирование дополнительных ролей данной документацией не предусмотрено. Поэтому тестирующему необходимо зайти с рабочего места браузером (Firefox, Chrome) на URL <http://10.55.1.100/igm/>.

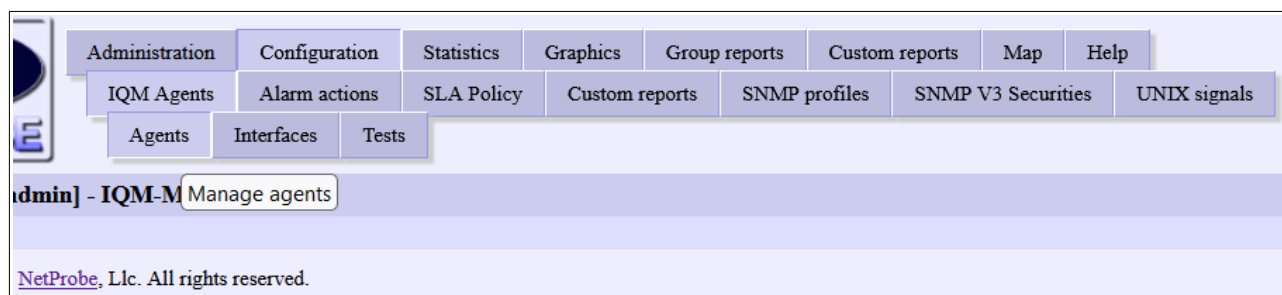
Вы увидите приглашение ввести пароль. Следует ввести имя `admin` и пароль, полученный от Производителя по согласованным каналам связи. Это должно выглядеть, как показано на [рисунке 29](#). Имя уже набрано, пароль на картинке намеренно закрыт. Не забудьте включить JavaScript в браузере, если вы ограничиваете использование языков программирования!

Рисунок 29.



После нажатия на кнопку с галочкой или Enter, тестирующий увидит основное меню системы вверху экрана. При ведении указателя мыши по меню, происходит открытие более нижних слоёв. Для добавления агента следует выбрать последовательно Configuration → IQM Agents → Agents, и на самом нижнем меню нажать кнопку мыши. Как это показано на [рисунке 30](#).

Рисунок 30.




После такого выбора ниже меню появится форма ввода параметров агентов и кнопки дополнительного меню, автоматически уходящего за левый срез окна в случае прокрутки

формы. Для заведения АИ1 в систему управления следует вначале заполнить в форме следующие поля (если вы исправляли пароль FTP-сервера в процессе установки СУ согласно документации «Запуск IQM на ОС Альт 10», вам следует применять свой пароль):

Имя поля	Вводимое значение
Agent name	alt10-iqma1
Agent IP	10.55.1.10
Agent type	IQM
SNMP profile	netiqm
Core IP	10.55.1.100
FTP user	iqmmon
FTP password	ftpPassword
License key	6a76d919c35d803436323aa2779f1ecc

После ввода следует либо прокрутить страницу вверх до появления меню формы автоматически, либо навести мышь на небольшую панель у левого среза окна, показывающую, куда скрылось меню, в этом случае кнопки управления появятся обратно (до прокрутки). Следует нажать мышью кнопку add. Результат работы в таких формах показывается ниже формы, поэтому следует после нажатия на кнопку прокрутить форму вверх, тем самым переместившись в самый конец страницы. При корректной вставке будет сообщение сколько записей в базу данных занесено. А ниже будут автоматические подстановки, если значение было выбрано по умолчанию. Это должно выглядеть как показано на [рисунке 31](#). Как правило, это одна запись в таблице agents и несколько интерфейсов в таблице ifcfg. Будьте внимательны! При неверном указании либо IP-адреса агента, либо SNMP-профиля будет выдана ошибка.

Рисунок 31.

Save one-way delays	<input type="text"/>	
List of administrator's IPs	<input type="text"/>	
License key	6a76d919c35d803436323aa2779f1ec	
Creation date	<input type="text"/>	
Modify date	<input type="text"/>	
Status	UP <input type="text"/>	UP
Operational status	UNKNOWN <input type="text"/>	UNKNOWN
Customer ID	<input type="text"/>	
SYS policy profile	<input type="text"/>	
Longitude and Latitude 	<input type="text"/>	
Tags	<input type="text"/>	
Description	<input type="text"/>	
Contract	<input type="text"/>	
Postal address	<input type="text"/>	

**1 row added to agents (alt10-iqma1)**

**2 row(s) added to ifcfg**

Если прокрутить форму сразу после корректного ввода вверх, будет видно как меню, так и все введённые значения, включая умолчания. Верх формы показан на [рисунке 32](#). Пароли агента намеренно закрыты.

Рисунок 32.

Parameter	Value	Default
Deploy on:	<input checked="" type="checkbox"/> On agent <input checked="" type="checkbox"/> On DB <input checked="" type="checkbox"/> Drop statistics when deleting	
Multiconf	Обзор... Файл не выбран. Separation char Quotation char	Enter CSV configuration file
Agent ID	<input type="text"/>	
Agent name *	alt10-iqma1	
Agent IP *	10.55.1.10	
Agent password *	<input type="password"/>	<input type="password"/>
Control password *	<input type="password"/>	<input type="password"/>
Agent type	IQM	IQM
Network layer	CORE	CORE
SNMP profile	netiqm	
Zone *	Столицы	1
Core IP *	10.55.1.100	127.0.0.1
CDR filesize (NoR)	60	60
CDR file timeout (min)	5	5

Поскольку тестирующий скорее всего не имеет опыта работы с IQM, а небольшими ошибками при вводе легко создать неверную конфигурацию, после занесения первого агента АИ1 следует перейти в консоль (SSH) системы управления для контроля поступления файлов результатов. В консоли надо исполнить команду

```
# tail -f /var/log/vsftpd.log
```

и подождать около 5-10 минут до фиксации поступления файлов результатов. В текущей версии агента файлы результата создаются с именем `iqmcae-имя-агента-xxxxxx`. А если агент только установлен на устройство, но не занесён в систему управления, у него обычно установлено системное имя `@auto@`, преобразующееся в процессе запуска в `IQMA_XXXXXXXXXX`. Такие файлы результатов, естественно, не обрабатываются в СУ, так как имена не соответствуют тому, что настроено в базе данных. Именно так и можно зафиксировать, что после занесения агента передаются верные файлы результатов. В начале [рисунка 33](#) видно, что сразу после занесения агента в базу и передачи на него верного Core IP (адреса системы управления), FTP-клиент агента передал уже накопленные файлы с автоматическим именем. После некоторого времени будут доставлены верные файлы. Это видно в конце [рисунка 33](#). После этого можно нажать Ctrl-C для выхода из tail.

**Рисунок 33.**

```
[root@alt10-iqmm ~]# tail -f /var/log/vsftpd.log
Thu Nov 20 14:24:35 2025 [pid 3110] CONNECT: Client "10.55.1.10"
Thu Nov 20 14:24:35 2025 [pid 3109] [iqmmon] OK LOGIN: Client "10.55.1.10"
Thu Nov 20 14:25:35 2025 [pid 3116] CONNECT: Client "10.55.1.10"
Thu Nov 20 14:25:35 2025 [pid 3115] [iqmmon] OK LOGIN: Client "10.55.1.10"
Thu Nov 20 14:26:24 2025 [pid 3139] CONNECT: Client "10.55.1.10"
Thu Nov 20 14:26:24 2025 [pid 3138] [iqmmon] OK LOGIN: Client "10.55.1.10"
Thu Nov 20 14:26:24 2025 [pid 3140] [iqmmon] OK UPLOAD: Client "10.55.1.10", "/stat/.iqmcae-IQMA_DO:WN:IN:TR:FA:CE-o9rv6L.results.2527", 4197 bytes, 568.70Kbyte/sec
Thu Nov 20 14:26:24 2025 [pid 3140] [iqmmon] OK RENAME: Client "10.55.1.10", "/stat/.iqmcae-IQMA_DO:WN:IN:TR:FA:CE-o9rv6L.results.2527 /stat/iqmcae-IQMA_DO:WN:IN:TR:FA:CE-o9rv6L.results"
Thu Nov 20 14:27:24 2025 [pid 3152] CONNECT: Client "10.55.1.10"
Thu Nov 20 14:27:24 2025 [pid 3151] [iqmmon] OK LOGIN: Client "10.55.1.10"
Thu Nov 20 14:28:24 2025 [pid 3161] CONNECT: Client "10.55.1.10"
Thu Nov 20 14:28:24 2025 [pid 3160] [iqmmon] OK LOGIN: Client "10.55.1.10"
Thu Nov 20 14:29:25 2025 [pid 3166] CONNECT: Client "10.55.1.10"
Thu Nov 20 14:29:25 2025 [pid 3165] [iqmmon] OK LOGIN: Client "10.55.1.10"
Thu Nov 20 14:30:25 2025 [pid 3173] CONNECT: Client "10.55.1.10"
Thu Nov 20 14:30:25 2025 [pid 3172] [iqmmon] OK LOGIN: Client "10.55.1.10"
Thu Nov 20 14:31:24 2025 [pid 3176] CONNECT: Client "10.55.1.10"
Thu Nov 20 14:31:24 2025 [pid 3175] [iqmmon] OK LOGIN: Client "10.55.1.10"
Thu Nov 20 14:31:24 2025 [pid 3177] [iqmmon] OK UPLOAD: Client "10.55.1.10", "/stat/.iqmcae-alt10-iqmal-QPKDEL.results.2543", 4183 bytes, 556.46Kbyte/sec
Thu Nov 20 14:31:24 2025 [pid 3177] [iqmmon] OK RENAME: Client "10.55.1.10", "/stat/.iqmcae-alt10-iqmal-QPKDEL.results.2543 /stat/iqmcae-alt10-iqmal-QPKDEL.results"
^C
[root@alt10-iqmm ~]#
```

Поскольку простое поступление файлов на СУ — это ещё не полная обработка, стоит убедиться, что FTP-сервер и обработчик файлов результатов (iqmm-r2) корректно работают. Это можно сделать следующими командами. Первая

```
$ ls -la /home/iqm/stat/old
```

Внутри этого каталога должны появиться дополнительные подкаталоги с датами файлов результатов. Например 2025-11-20 (в вашем случае будет другая дата, обозначим её через YYYY-MM-DD, пожалуйста, исправьте команду нужным образом сами). Вторая команда

```
$ ls -la /home/iqm/stat/old/YYYY-MM-DD
```

Внутри каталога с датой будут дополнительные подкаталоги с именами агентов, данные с которых корректно обработаны. В нашем случае это пока один подкаталог alt10-iqmal. Третья команда

```
$ ls -la /home/iqm/stat/old/YYYY-MM-DD/alt10-iqmal
```

Внутри этого каталога с именем агента будут видны все файлы результатов, полученные за дату YYYY-MM-DD. В нашем случае это пока только один файл. Пример всех команд и их результатов приведён на [рисунке 34](#).

**Рисунок 34.**

```
[cae@alt10-iqmm ~]$ ls -la /home/iqm/stat/old/
[sudo] password for cae:
итого 12
drwxrwx--- 3 iqm iqm 4096 ноя 20 14:31 .
drwxrwx--- 4 iqm iqm 4096 ноя 20 14:31 ..
drwxr-x--x 3 iqm iqm 4096 ноя 20 14:31 2025-11-20
[cae@alt10-iqmm ~]$ ls -la /home/iqm/stat/old/2025-11-20
итого 12
drwxr-x--x 3 iqm iqm 4096 ноя 20 14:31 .
drwxrwx--- 3 iqm iqm 4096 ноя 20 14:31 ..
drwxr-x--x 2 iqm iqm 4096 ноя 20 14:31 alt10-iqma1
[cae@alt10-iqmm ~]$ ls -la /home/iqm/stat/old/2025-11-20/alt10-iqma1
итого 16
drwxr-x--x 2 iqm      iqm      4096 ноя 20 14:31 .
drwxr-x--x 3 iqm      iqm      4096 ноя 20 14:31 ..
-rw-r--r-- 1 iqmstat iqmstat 4183 ноя 20 14:31 iqmcae-alt10-iqma1-QPKDEL.results
[cae@alt10-iqmm ~]$
```

После этих дополнительных проверок можно вернуться в web-интерфейс. Агент АИ1 на этот момент существует в базе данных и имеет корректную конфигурацию на самом ПО IQMA.

## 6 Заведение агента АИ2 в системе управления

После заведения первого агента следует либо в меню формы вызвать `clear` для очистки формы в первоначальное состояние, либо вновь зайти через меню `Configuration → IQM Agents → Agents`. После чего добавить второй агент типа IQM. Со следующими значениями:

Имя поля	Вводимое значение
Agent name	alt10-iqma2
Agent IP	10.55.1.20
Agent type	IQM
SNMP profile	netiqm
Core IP	10.55.1.100
FTP user	iqmmon
FTP password	ftpPassword
License key	6a76d919c35d803436323aa2779f1ecc

Сделайте всё самостоятельно по аналогии с АИ1. После чего можно для контроля использовать команды формы `clear` и вслед за этим `view`. В этом случае после формы (прокрутите страницу вниз) будет показана таблица `agents` с двумя введенными агентами, как показано на [рисунке 35](#).

Рисунок 35.

Postal address																			
Data requested:																			
<input type="checkbox"/> XLS <input type="checkbox"/> CSV <input type="checkbox"/> CSV export <input type="checkbox"/> CSV popup <input type="checkbox"/> expert <input type="checkbox"/> filter reset																			
Agent ID	Agent name *	Agent IP *	Agent password *	Control password *	Agent type	Network layer	SNMP profile	Zone *	Core IP *	CDR filesize (NoR)	CDR file timeout (min)	CDR send timeout (min)	Spool dir	CDR transport script	FTP user	FTP password	Config source	Listen port	Server timeout (sec)
1	alt10-iqma1	10.55.1.10			IQM	CORE	netiqm	Столпы	10.55.1.100	60	5	5	/tmp	/usr/local/iqm_agent/sender.pl	iqmmon	ftpPassword		1189	3
2	alt10-iqma2	10.55.1.20			IQM	CORE	netiqm	Столпы	10.55.1.100	60	5	5	/tmp	/usr/local/iqm_agent/sender.pl	iqmmon	ftpPassword		1189	3

2 rows  
Copyright (C) 2008-2024, NetProbe, Llc. All rights reserved.

Теперь можно переходить к вводу служебных агентов (фактически, сетевых устройств, поддерживающих разные протоколы).

## 7 Заведение сопряжённого агента СА в системе управления

Очевидно, что для выполнения сетевого тестирования нужно два устройства. Одно является генератором запросов, а второе ему отвечает. В терминологии Производителя это агент-инициатор и сопряжённый агент. Понятно, что полный спектр поддерживаемых протоколов в лаборатории обеспечить вряд ли возможно. Поэтому выбран путь — какие-то протоколы поддерживать на мощностях Производителя (агент СА), какие-то прямо на шлюзе лаборатории (ICMP), протокол DNS на мощностях оператора связи, а протокол UDP echo на системе управления.

Каждый агент, включая те, которые не управляются IQMM, необходимо, тем не менее, завести в таблицу agents. Так как тесты любого протокола всегда исполняются между двумя устройствами. Для разделения поведения системы управления в процессе заведения агентов и их сопровождения используется понятие Agent type (тип агента).

Сопряжённый агент СА с адресом С.С.С.С (следует получить адрес у Производителя по согласованным каналам связи) будет заведён с типом STUB. Это даст возможность опроснику активности агентов (iqmm-aac) корректно запрашивать состояние.

Зайдите через меню Configuration → IQM Agents → Agents в форму заведения агентов. После чего следует добавить сопряжённый агент СА типа STUB. Со следующими значениями:

Имя поля	Вводимое значение
Agent name	ca-np
Agent IP	С.С.С.С
Agent type	STUB

Пример того, как это делается, можно видеть на [рисунке 36](#) (пароли закрыты, реальный IP-адрес Производителя так же). После ввода следует исполнить команду формы add.

Рисунок 36.

Agent name *	<input type="text" value="ca-np"/>	
Agent IP *	<input type="text" value=""/>	
Agent password *	<input type="text" value=""/>	<input type="text" value=""/>
Control password *	<input type="text" value=""/>	<input type="text" value=""/>
Agent type	STUB ▾	IQM
Network layer	▾	CORE
SNMP profile	▾	
Zone *	▾	1
Core IP *	<input type="text" value=""/>	127.0.0.1
CDR filesize (NoR)	<input type="text" value=""/>	60
CDR file timeout (min)	<input type="text" value=""/>	5
CDR send timeout (min)	<input type="text" value=""/>	5
Spool dir	<input type="text" value=""/>	/tmp
CDR transport script	<input type="text" value=""/>	/usr/local/iqm_agent/sender.pl
FTP user	<input type="text" value=""/>	iqm
FTP password	<input type="text" value=""/>	sla
Config source	<input type="text" value=""/>	










Поскольку по причинам, находящимся вне текущей документации, автоматически поле Operational status не выставляется в UP при заведении, а в дальнейшем такая настройка упростит тестирующему процесс работы, следует сразу научиться исправлять запись в таблице agents. Для этого мы вызываем уже знакомую команду `clear`, выбираем в поле Agent ID имя `ca-np` и запускаем команду `fill form`, как показано на [рисунке 37](#).

Рисунок 37.

Parameter	Value	Default
Multiconf	Обзор... Файл не выбран. Separation char Quotation char	Enter CSV configuration file
Agent ID	ca-np	
Agent name *		
Agent IP *		
Agent password *		123


После этого следует прокрутить форму с заполненными полями в конец страницы, найти поле Operational status и исправить его значение на UP вместо умолчания UNKNOWN. Это показано на [рисунке 38](#). После выбора наведите мышь на панель у левого среза окна, чтобы появилось выплывающее меню формы и постарайтесь не допускать прокрутки после этого. Выберите команду change и нажмите её мышью.

Рисунок 38.

SNMP profile								
 add	 get	 fill form	 CSV	 view	 change	 delete	 clear	 expert
Core IP *	127.0.0.1	127.0.0.1						
CDR filesize (NoR)	60	60						
CDR file timeout (min)	5	5						
CDR send timeout (min)	5	5						
Spool dir	/tmp	/tmp						
CDR transport script	/usr/local/iqm_agent/sender.pl	/usr/local/iqm_agent/sender.pl						
FTP user	iqm	iqm						
FTP password	sla	sla						
Config source								
Listen port	1189	1189						
Server timeout (sec)	3							
Save one-way delays	▼							
List of administrator's IPs								
License key								
Creation date	2025-11-20 15:12:17.286333							
Modify date	2025-11-20 15:12:17.286333							
Status	UP ▼	UP						
<b>Operational status</b>	UP ▼	UNKNOWN						
Customer ID	▼							

Чтобы убедиться, что команда change произвела все нужные изменения, можно прокрутить форму до конца, там будут сообщения обновления записи в таблице, включая сообщения, что исправления на агенте за пределами типов IQM, CIQM, REMOTE\_IQM не производятся. Фактически исправления ведутся только в базе данных. Результат показан на [рисунке 39](#).

Рисунок 39.

Creation date	<input type="text" value="2025-11-20 15:12:17.286333"/>	
Modify date	<input type="text" value="2025-11-20 15:12:17.286333"/>	
Status	<input type="text" value="UP"/>	UP
Operational status	<input type="text" value="UP"/>	UNKNOWN
Customer ID	<input type="text"/>	
SYS policy profile	<input type="text"/>	
Longitude and Latitude 	<input type="text"/>	
Tags	<input type="text"/>	
Description	<input type="text"/>	
Contract	<input type="text"/>	
Postal address	<input type="text"/>	

**1 row updated (ca-np)**

`on_agent=false for agent_type=(!=IQM,CIQM,REMOTE_IQM)`

Copyright (C) 2008-2024, NetProbe, Llc. All rights reserved.

Теперь агент ca-np (в документации именуется как CA) будет всегда в состоянии UP для базы данных вне зависимости от реальной доступности в сети.

## 8 Заведение шлюза ШЛ в системе управления

Зайдите уже знакомым методом через меню Configuration → IQM Agents → Agents в форму заведения агентов. После чего следует добавить сопряжённый агент ШЛ типа ICMP. Со следующими значениями:

Имя поля	Вводимое значение
Agent name	gw
Agent IP	10.55.1.1
Agent type	ICMP

Пример того, как это делается, можно видеть на [рисунке 40](#). После ввода следует исполнить команду формы add.

Рисунок 40.

Deploy on:	<input checked="" type="checkbox"/> On agent <input checked="" type="checkbox"/> On DB <input checked="" type="checkbox"/> Drop statistics when deleting
Parameter	Value
Multiconf	Обзор... Файл не выбран. <input type="text"/>
	Separation char <input type="text"/>
	Quotation char <input type="text"/>
Agent ID	<input type="text" value="v"/>
Agent name *	<input type="text" value="gw"/>
Agent IP *	<input type="text" value="10.55.1.1"/>
Agent password *	<input type="text"/>
Control password *	<input type="text"/>
Agent type	<input type="text" value="ICMP"/>
Network layer	<input type="text" value="v"/>
SNMP profile	<input type="text" value="v"/>
Zone *	<input type="text" value="v"/>

Теперь данный агент может использоваться для создания тестов, на которые он будет отвечать (естественно, не всех типов, ниже вы увидите подробности).

## 9 Заведение сервера DNS в системе управления

Для демонстрации, что IQM умеет работать не только с транспортными протоколами, но и с сервисными, потребуется завести DNS-агент. Фактически это DNS-сервер. Поскольку для лаборатории сложно предсказать, какой именно IP-адрес будет использоваться для разрешения имён, мы будем в документации обозначать этот адрес как D.D.D.D. Тестирующему следует уточнить какой именно адрес используется в сети лаборатории либо самостоятельно (просмотр настроек ОС, допустим), либо с помощью ответственного сетевого инженера. Представление неопытных сетевиков, что можно везде свободно использовать общедоступные DNS-сервера, вроде 8.8.8.8 из округа Санта-Клара, на деле ошибочно. Производитель достаточно часто видел, что данные адреса по протоколу DNS не доступны, а оператор настоятельно рекомендует пользоваться только его серверами. Уточните это самостоятельно!

Для внесения данных зайдите уже знакомым методом через меню Configuration → IQM Agents → Agents в форму заведения агентов. После чего следует добавить сопряжённый агент DNS типа ICMP. Со следующими значениями:

Имя поля	Вводимое значение
Agent name	dns-oper
Agent IP	D.D.D.D
Agent type	ICMP

Пример того, как это делается, можно видеть на [рисунке 41](#). После ввода следует исполнить команду формы add.

**Рисунок 41.**

Parameter	Value
Multiconf	Обзор... Файл не выбран. <input type="text"/>
	Separation char <input type="text"/>
	Quotation char <input type="text"/>
Agent ID	<input type="text" value="v"/>
Agent name *	<input type="text" value="dns-oper"/>
Agent IP *	<input type="text" value="21"/> <span style="background-color: yellow; display: inline-block; width: 100px; height: 1em;"></span>
Agent password *	<input type="text"/>
Control password *	<input type="text"/>
Agent type	<input type="text" value="ICMP"/> v
Network layer	<input type="text" value="v"/>
SNMP profile	<input type="text" value="v"/>

Адрес мы частично закрыли намеренно в целях безопасности. Тип ICMP выбран специально, чтобы `iqmm-aac` проверял доступность сервера с помощью ICMP echo. Теперь данный агент может использоваться в качестве сопряжённого для создания тестов по протоколу DNS.

## 10 Заведение агента U7 в системе управления

Для целей тестирования сети по протоколу UDP echo, нам потребуется сопряжённый агент с поддержкой этой возможности. Вы можете использовать и стороннее оборудование, самостоятельно включив нужный режим на нём. Но мы предлагаем использовать уже существующую систему управления под ОС «Альт» как агента U7. Для этого тестирующему следует вернуться в консоль `shell`. Там следует выполнить несколько команд.

Первая — включение UDP echo в конфигурации суперсервера `xinetd`. Это делается так:

```
# sed -r -i \  
-e 's&^[[[:space:]]*disable[[[:space:]]]*=[[[:space:]]]*yes$& disable = no&' \  
/etc/xinetd.d/echo-udp
```

Будьте внимательны при ручном вводе, мы не просто так написали сложное регулярное выражение. Если у вас небольшой опыт работы с sed, а в регулярных выражениях вы путаетесь, но текстовым редактором вполне владеете, возможно, вам будет проще исправить yes на no в файле /etc/xinetd.d/echo-udp через редактирование. Мы же предпочитаем автоматизацию. Пример исполнения sed показан на [рисунке 42](#).

#### Рисунок 42.

```
[root@alt10-igmm ~]# sed -r -i \  
> -e 's&^[[[:space:]]*disable[[[:space:]]]*=[[[:space:]]]*yes$& disable = no&' \  
> /etc/xinetd.d/echo-udp  
[root@alt10-igmm ~]# █
```

Понятно, что sed, следуя хорошей традиции Unix, при корректной работе не выдаёт никаких сообщений.

Вторая — перезапуск суперсервера xinetd, чтобы он запустил UDP echo. Это делается так:

```
# kill -HUP $(cat /var/run/xinetd.pid)
```

Пример показан на [рисунке 43](#).

#### Рисунок 43.

```
[root@alt10-igmm ~]# kill -HUP $(cat /var/run/xinetd.pid)  
[root@alt10-igmm ~]# █
```

Вновь мы видим, что при корректной работе ошибки и сообщения не выдаются.

Третья — проверка, что суперсервер xinetd запустил UDP echo. Это делается так:

```
# ss -anp|grep xinetd
```

Пример запуска и результат показан на [рисунке 44](#).

**Рисунок 44.**

```
[root@alt10-iqmm ~]# ss -anp|grep xinetd
u_dgr ESTAB 0      0                      * 13115
      * 13943 users: (("xinetd",pid=2380,fd=7))

udp    UNCONN 0      0                      0.0.0.0:7
      0.0.0.0:*      users: (("xinetd",pid=2380,fd=6))

tcp    LISTEN 0      64                    0.0.0.0:21
      0.0.0.0:*      users: (("xinetd",pid=2380,fd=5))

[root@alt10-iqmm ~]# █
```

Можно легко видеть, что суперсервер `xinetd` слушает UDP-сокеты с портом 7 (UDP echo, красное подчёркивание) и TCP-сокеты с портом 21 (FTP, зелёное подчёркивание). Тем самым он выполняет двойственную функцию — принимает файлы результатов от агентов-инициаторов и даёт им возможность использовать сервер UDP echo как сопряжённый агент протокола U7.

Теперь тестирующий может вернуться в web-интерфейс для заведения UDP-агента. Вновь выбирается меню Configuration → IQM Agents → Agents для захода в форму заведения агентов. После чего следует добавить сопряжённый агент U7 типа UDP. Со следующими значениями:

Имя поля	Вводимое значение
Agent name	u7
Agent IP	10.55.1.100
Agent type	UDP

Пример того, как это делается, можно видеть на [рисунке 45](#). После ввода следует исполнить команду формы `add`.

Рисунок 45.

Parameter	Value
Multiconf	Обзор... Файл не выбран.
	Separation char
	Quotation char
Agent ID	<input type="text" value=""/>
Agent name *	u7
Agent IP *	10.55.1.100
Agent password *	<input type="text" value=""/>
Control password *	<input type="text" value=""/>
Agent type	UDP <input type="text" value=""/>
Network layer	<input type="text" value=""/>
SNMP profile	<input type="text" value=""/>

После заведения последнего агента мы полагаем, что было бы не лишним проконтролировать данные в базе. Подождав 5-10 минут, чтобы точно отработала проверка доступности всех агентов (iqmm-aac), вызовем просмотр. Для этого нажимаем в меню формы clear и потом view, чтобы вывести всю таблицу agents без исключений. Результат должен быть похож на рисунки 46 и 47. Левая сторона таблицы на первом (IP-адреса и пароли намеренно закрыты), правая сторона — на втором.

Рисунок 46.

Data requested:															
<input type="button" value="XLS"/> <input type="button" value="CSV"/> <input type="button" value="CSV export"/> <input type="button" value="CSV popup"/> <input type="button" value="expert"/> <input type="button" value="filter reset"/>															
Agent ID	Agent name *	Agent IP *	Agent password *	Control password *	Agent type	Network layer	SNMP profile	Zone *	Core IP *	CDR filesize (NoR)	CDR file timeout (min)	CDR send timeout (min)	Spool dir	CDR transport script	
1	alt10-iqma1	10.55.1.10			IQM	CORE	netiqm	Столицы	10.55.1.100	60	5	5	/tmp	/usr/local/iqm_agent/sender.pl	
2	alt10-iqma2	10.55.1.20			IQM	CORE	netiqm	Столицы	10.55.1.100	60	5	5	/tmp	/usr/local/iqm_agent/sender.pl	
3	ca-np				STUB	CORE		Столицы	127.0.0.1	60	5	5	/tmp	/usr/local/iqm_agent/sender.pl	
5	dns-oper				ICMP	CORE		Столицы	127.0.0.1	60	5	5	/tmp	/usr/local/iqm_agent/sender.pl	
4	gw	10.55.1.1			ICMP	CORE		Столицы	127.0.0.1	60	5	5	/tmp	/usr/local/iqm_agent/sender.pl	
7	u7	10.55.1.100			UDP	CORE		Столицы	127.0.0.1	60	5	5	/tmp	/usr/local/iqm_agent/sender.pl	

6 rows

Copyright (C) 2008-2024, NetProbe, Llc. All rights reserved.

Рисунок 47.

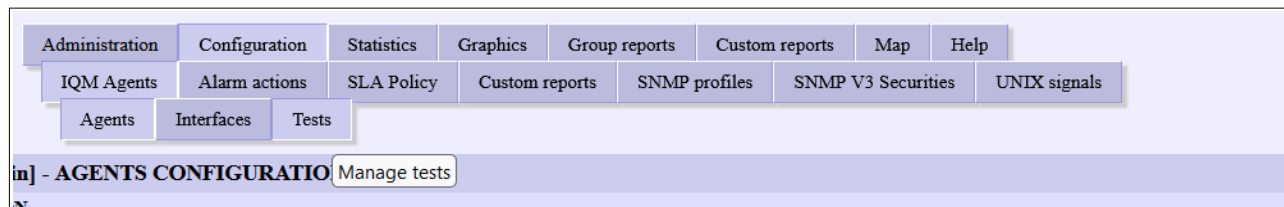
agents											
FTP user	FTP password	Config source	Listen port	Server timeout (sec)	Save one-way delays	List of administrator's IPs	License key	Creation date	Modify date	Status	Operational status
iqmmon	ftpPassword		1189	3			6a76d919c35d803436323aa2779f1ecc	2025-11-20 14:22:21.812778	2025-11-21 11:13:43.582642	UP	UP
iqmmon	ftpPassword		1189	3			6a76d919c35d803436323aa2779f1ecc	2025-11-20 14:43:50.977714	2025-11-21 11:13:43.582852	UP	UP
iqm	sla		1189	3				2025-11-20 15:12:17.286333	2025-11-21 13:45:02.751569	UP	UP
iqm	sla		1189	3				2025-11-21 08:22:37.892209	2025-11-21 08:24:01.164938	UP	UP
iqm	sla		1189	3				2025-11-21 08:20:58.345714	2025-11-21 08:24:01.155639	UP	UP
iqm	sla		1189	3				2025-11-21 13:31:18.315088	2025-11-21 13:33:39.855602	UP	UP

Теперь можно начинать заводить тесты между агентами.

## 11 Тест U0 между АИ1 и АИ2

Для заведения тестов между агентами используется отдельное меню. Поэтому тестирующему следует выбрать Configuration → IQM Agents → Tests, как показано на рисунке 48 и нажать мышью на Tests. В этом случае откроется форма для редактирования тестов.

Рисунок 48.



Краткая информация о том, что такое тест для лучшего понимания, если у вас мало опыта тестирования сетей TCP/IP. Это трафик от точки создания (агент-инициатор) до точки получения (сопряжённый агент) и обратно, созданный искусственно и предназначенный для расчёта метрик качества сети. Параметрами, определяющими характер создаваемого трафика являются:  $C_s$  (целое) — класс сервиса (TOS/DSCP) теста,  $P_s$  (байт) — полезный размер пакета теста внутри протокола UDP или ICMP,  $O_s$  (байт) — размер служебных данных пакета,  $N_s$  (единицы) — число пакетов в тесте,  $V_s$  (Кбит/с) — скорость генерации. В этом случае общее время тестирования без учёта накладных расходов на контрольное соединение можно выразить через  $T_{test} = 8 * (P_s + O_s) * N_s / (V_s * 1024)$ . Эта информация приводится вам для лучшего понимания того, что вы делаете при создании теста.

Таблица соответствия параметров в форме тестов IQM:

Параметр	Поле в форме тестов
C <sub>s</sub>	Class (IP Precedence or DSCP)
P <sub>s</sub>	Packet size (B)
O <sub>s</sub>	Определяется автоматически
N <sub>s</sub>	Number of probes
B <sub>s</sub>	Bandwidth for UDP tests (Kb/s)

Форма редактирования тестов несколько велика и описание всех полей выходит за рамки настоящей документации. Мы при создании тестов указываем самые важные поля, которые необходимо устанавливать для наилучшего тестирования IQM и ОС. Остальные будут выставлены по умолчанию. Поскольку форма большая, то следует использовать прокрутку страницы в браузере, чтобы найти указанные. Для создания теста между АИ1 и АИ2 по протоколу U0 (подробности по протоколам в отдельной документации) следует выставить следующие поля в форме:

Имя поля	Вводимое значение
Test name	a1-a2-U0
Class	RT
SRC agent	alt10-iqma1
DST agent	alt10-iqma2
Test type	U0
Packet size	128
On demand test	0

После ввода следует исполнить команду формы add. Пример того, как заполняется форма, можно видеть на [рисунке 49](#) (верх) и [рисунке 50](#) (низ). Обращаем ваше внимание, что поле On demand test стоит не забывать выставлять в 0, иначе тестирование по расписанию исполняться не будет. По умолчанию выставлена 1, то есть тест делать только по запросу администратора. Это сделано в системе намеренно, чтобы ненароком не создать проблемы на сети!

Рисунок 49.













 add  get  fill form  CSV  view  change  delete  clear  expert	
Deploy on:	<input checked="" type="checkbox"/> On agent <input checked="" type="checkbox"/> On DB <input checked="" type="checkbox"/> Drop statistics when deleting
 Create template  Delete template	<input type="text" value=""/>  Load template
Parameter	Value
<b>Multiconf</b>	<input type="text" value="Обзор... Файл не выбран."/> Separation char <input type="text"/> Quotation char <input type="text"/>
<b>Test ID</b>	<input type="text" value="OnDemand"/>
<b>Test name *</b>	<input type="text" value="ai1-ai2-U0"/>
<b>Class (IP Precedence or DSCP)</b>	<input type="text" value="RT"/>
<b>SLA policy profile</b>	<input type="text"/>
<b>Service</b>	<input type="text"/>
<b>Provider</b>	<input type="text"/>
<b>SRC agent *</b>	<input type="text" value="alt10-iqma1"/>
<b>DST agent *</b>	<input type="text" value="alt10-iqma2"/>
<b>Source IP</b>	<input type="text"/>

Рисунок 50.

<b>HTTP User-Agent</b>	<input type="text"/>	
<b>Content download timeout</b>	<input type="text"/>	
<b>DST agent type</b>	<input type="text" value="v"/>	A
<b>Test type</b>	<input type="text" value="U0"/>	U0
<b>VoIP profile</b>	<input type="text" value="v"/>	
<b>Test command (for LOCAL or CMD tests)</b>	<input type="text" value="v"/>	
<b>CMD options</b>	<input type="text"/>	
<b>CMD timeout kill signal</b>	<input type="text" value="v"/>	
<b>Test timeout (sec)</b>	<input type="text"/>	
<b>Test-specific parameters</b>	<input type="text"/>	
<b>Send config to CMD's STDIN</b>	<input type="text" value="v"/>	
<b>Log CMD's STDOUT</b>	<input type="text" value="v"/>	
<b>Redirect CMD's STDERR to STDOUT</b>	<input type="text" value="v"/>	
<b>Enabled</b>	<input type="text" value="v"/>	1
<b>Packet size (B)</b>	<input type="text" value="128"/>	60
<b>On demand test</b>	<input type="text" value="0"/>	1

После добавления теста, как и в случае работы с агентами, в конце формы после нажатия add выдаётся результат работы. Пример приведён на [рисунке 51](#).

**Рисунок 51.**

Для тех тестирующих, которые желают узнать, что же произошло на агенте после заведения в СУ самого агента и теста ai1-ai2-U0, мы приводим состояние файла конфигурации агента на [рисунке 52](#). Информацию как зайти по SSH на агент и саму команду просмотра файла мы не приводим, как очевидные.



## 12 Тест U9 между АИ1 и СА

Как и в случае заведения агентов для ввода очередного теста следует выбрать Configuration → IQM Agents → Tests в меню или в форме редактирования clear. В этот раз следует выставить следующие поля в форме:

Имя поля	Вводимое значение
Test name	a1-ca-U9
Class	RT
SRC agent	alt10-iqma1
DST agent	ca-np
Test type	U9
Packet size	100
On demand test	0

Выглядеть это будет как на [рисунках 53](#) и [54](#). После чего следует дать команду add.

Рисунок 53.




 Create template  Delete template	<input type="text"/>  Load template
Parameter	Value
<b>Multiconf</b>	Обзор... Файл не выбран. <input type="text"/>
	Separation char <input type="text"/>
	Quotation char <input type="text"/>
<b>Test ID</b>	<input type="text"/> OnDemand
<b>Test name *</b>	ai1-ca-U9
<b>Class (IP Precedence or DSCP)</b>	RT
<b>SLA policy profile</b>	<input type="text"/>
<b>Service</b>	<input type="text"/>
<b>Provider</b>	<input type="text"/>
<b>SRC agent *</b>	alt10-iqma1
<b>DST agent *</b>	ca-np
<b>Source IP</b>	<input type="text"/>

Рисунок 54.

Content download timeout	<input type="text"/>	
DST agent type	<input type="text" value="v"/>	A
Test type	<input type="text" value="U9"/>	U0
VoIP profile	<input type="text" value="v"/>	
Test command (for LOCAL or CMD tests)	<input type="text" value="v"/>	
CMD options	<input type="text"/>	
CMD timeout kill signal	<input type="text" value="v"/>	
Test timeout (sec)	<input type="text"/>	
Test-specific parameters	<input type="text"/>	
Send config to CMD's STDIN	<input type="text" value="v"/>	
Log CMD's STDOUT	<input type="text" value="v"/>	
Redirect CMD's STDERR to STDOUT	<input type="text" value="v"/>	
Enabled	<input type="text" value="v"/>	1
Packet size (B)	<input type="text" value="100"/>	60
On demand test	<input type="text" value="0"/>	1

Более подробно излагать заведение тестов, аналогично первому, мы не будем, полагаем, вы уже достаточно знакомы с процессом.

## 13 Тест U7 между AI2 и СУ

Для ввода очередного теста вновь следует выбрать Configuration → IQM Agents → Tests в меню или в форме редактирования clear. В этот раз следует выставить следующие поля в форме:

Имя поля	Вводимое значение
Test name	ai2-su-U7
Class	BC
SRC agent	alt10-iqma2
DST agent	u7
Test type	U7
Packet size	256
On demand test	0

Выглядеть это будет как на [рисунках 55](#) и [56](#). После чего следует дать команду add.

Рисунок 55.

	Quotation char	
Test ID	<input type="text" value="OnDemand"/>	
Test name *	<input type="text" value="ai2-su-U7"/>	
Class (IP Precedence or DSCP)	<input type="text" value="BC"/>	1
SLA policy profile	<input type="text"/>	
Service	<input type="text"/>	1
Provider	<input type="text"/>	1
SRC agent *	<input type="text" value="alt10-iqma2"/>	
DST agent *	<input type="text" value="u7"/>	
Source IP	<input type="text"/>	NA
DST agent IP *	<input type="text"/>	

Рисунок 56.

add                  get                  fill form                  CSV                  view                  change                  delete                  clear                  expert		
DST agent type	<input type="text"/>	A
Test type	<input type="text" value="U7"/>	U0
VoIP profile	<input type="text"/>	
Test command (for LOCAL or CMD tests)	<input type="text"/>	
CMD options	<input type="text"/>	
CMD timeout kill signal	<input type="text"/>	
Test timeout (sec)	<input type="text"/>	
Test-specific parameters	<input type="text"/>	
Send config to CMD's STDIN	<input type="text"/>	
Log CMD's STDOUT	<input type="text"/>	
Redirect CMD's STDERR to STDOUT	<input type="text"/>	
Enabled	<input type="text"/>	1
Packet size (B)	<input type="text" value="256"/>	60
On demand test	<input type="text" value="0"/>	1

Проверку правильности заведения мы оставляем на вашу ответственность.

## 14 Тест T1 между AI2 и CA

Снова выбираем Configuration → IQM Agents → Tests в меню или в форме редактирования clear. В этот раз следует выставить следующие поля в форме:

Имя поля	Вводимое значение
Test name	a2-ca-T1
Class	BC
SRC agent	alt10-iqma2
DST agent	ca-np
Test type	T1
Packet size	512
On demand test	0

Выглядеть это будет как на [рисунках 57](#) и [58](#). После чего следует дать команду add.

**Рисунок 57.**

	Обзор... Файл не выбран.
<b>Multiconf</b>	Separation char
	Quotation char
<b>Test ID</b>	OnDemand
<b>Test name *</b>	ai2-ca-T1
<b>Class (IP Precedence or DSCP)</b>	BC
<b>SLA policy profile</b>	
<b>Service</b>	
<b>Provider</b>	
<b>SRC agent *</b>	alt10-iqma2
<b>DST agent *</b>	ca-np
<b>Source IP</b>	

Протокол T1 это TWAMP (RFC-5357). Его поддерживает некоторое число производителей сетевого оборудования и некоторые производители ПО.

Рисунок 58.

DST agent type	<input type="text" value="v"/>
Test type	T1 <input type="text" value="v"/>
VoIP profile	<input type="text" value="v"/>
Test command (for LOCAL or CMD tests)	<input type="text" value="v"/>
CMD options	<input type="text"/>
CMD timeout kill signal	<input type="text" value="v"/>
Test timeout (sec)	<input type="text"/>
Test-specific parameters	<input type="text"/>
Send config to CMD's STDIN	<input type="text" value="v"/>
Log CMD's STDOUT	<input type="text" value="v"/>
Redirect CMD's STDERR to STDOUT	<input type="text" value="v"/>
Enabled	<input type="text" value="v"/>
Packet size (B)	512 <input type="text"/>
On demand test	0 <input type="text" value="v"/>

И хотя вы уже освоились, мы просим вас быть аккуратными и проверять свои действия.

## 15 Тест I0 между АИ1 и ШЛ

Протокол I0 – это ICMP echo. Его скорее всего поддерживает ваш шлюз. В случае если он не поддерживает, следует либо разрешить его, либо сменить оборудование. Либо вы можете выбрать иное оборудование в качестве сопряжённого агента. Снова выбираем Configuration → IQM Agents → Tests в меню или в форме редактирования clear. В этот раз следует выставить следующие поля в форме:

Имя поля	Вводимое значение
Test name	a1-gw-I0
Class	RT
SRC agent	alt10-iqma1
DST agent	gw
Test type	I0
Packet size	128
On demand test	0

Выглядеть это будет как на [рисунках 59](#) и [60](#). После чего следует дать команду add.

Рисунок 59.

Parameter	Value
Multiconf	Обзор... Файл не выбран.
	Separation char
	Quotation char
Test ID	<input type="text" value="OnDemand"/>
Test name *	a1-gw-I0
Class (IP Precedence or DSCP)	RT
SLA policy profile	<input type="text"/>
Service	<input type="text"/>
Provider	<input type="text"/>
SRC agent *	alt10-iqma1
DST agent *	gw
Source IP	<input type="text"/>

Рисунок 60.

Test type	IO
VoIP profile	<input type="text"/>
Test command (for LOCAL or CMD tests)	<input type="text"/>
CMD options	<input type="text"/>
CMD timeout kill signal	<input type="text"/>
Test timeout (sec)	<input type="text"/>
Test-specific parameters	<input type="text"/>
Send config to CMD's STDIN	<input type="text"/>
Log CMD's STDOUT	<input type="text"/>
Redirect CMD's STDERR to STDOUT	<input type="text"/>
Enabled	<input type="text"/>
Packet size (B)	128
On demand test	0

Поздравляем, в сущности, этим тестом вы настроили так называемый «flood ping». Будьте аккуратны со скоростью генерации трафика! Мы специально оставили её по умолчанию (64 килобита в секунду).

## 16 Тест URL между АИ1 и СА

Для тестирования доступности уровня приложения, в IQM-агенте предусмотрен тест типа URL. Полное описание доступно отдельно. Здесь мы просто кратко описываем задачи, выполняемые тестом. Как и в прошлый раз выбираем Configuration → IQM Agents → Tests в меню или в форме редактирования clear. В этот раз следует выставить следующие поля в форме:

Имя поля	Вводимое значение
Test name	a1-ca-URL
Class	BE
SRC agent	alt10-iqma1
DST agent	ca-np
Number of probes	10
URL	http://C.C.C.C/cat.bin
Test type	URL
On demand test	0

Вместо C.C.C.C следует использовать правильный адрес. Обратите внимание, что в целях безопасности, число запросов к серверу ограничено! Как выглядит заполнение формы видно на [рисунках 61-63](#). После чего следует дать команду add.

Рисунок 61.

Test ID	<input type="text" value="OnDemand"/>
Test name *	<input type="text" value="a1-ca-URL"/>
Class (IP Precedence or DSCP)	<input type="text" value="BE"/>
SLA policy profile	<input type="text"/>
Service	<input type="text"/>
Provider	<input type="text"/>
SRC agent *	<input type="text" value="alt10-iqma1"/>
DST agent *	<input type="text" value="ca-np"/>

Рисунок 62.

Number of probes	<input type="text" value="10"/>	200
Number of probes to ignore	<input type="text"/>	
URL	<input type="text" value="http://[REDACTED]/cat.bin"/>	
URL-test query interval (ms)	<input type="text"/>	
Cookie file	<input type="text"/>	

Рисунок 63.

Test type	URL
VoIP profile	
Test command (for LOCAL or CMD tests)	
CMD options	
CMD timeout kill signal	
Test timeout (sec)	
Test-specific parameters	
Send config to CMD's STDIN	
Log CMD's STDOUT	
Redirect CMD's STDERR to STDOUT	
Enabled	
Packet size (B)	
On demand test	0

Размер пакета для этого теста не используется.

## 17 Тест URLUP между АИ2 и СА

Тест URL используется для оценки скорости загрузки на агент. Скорость же выгрузки с агента делается тестов URLUP. Для его создания выбираем Configuration → IQM Agents → Tests в меню или в форме редактирования clear. В этот раз следует выставить следующие поля в форме:

Имя поля	Вводимое значение
Test name	a2-ca-URLUP
Class	BE
SRC agent	alt10-iqma2
DST agent	ca-np
Number of probes	10
URL	http://C.C.C.C/cgi-bin/urlup-load
Test type	URLUP
Test-specific parameters	/bin/cat
On demand test	0

В поле «Test-specific parameters» мы указываем бинарный файл, который будет загружаться на сервер. Не стоит выбирать большие файлы, мы специально выбрали

стандартный /bin/cat. Вместо С.С.С.С вновь следует поставить адрес сопряжённого агента CA. Так же, не следует делать слишком много запросов, 10 мы выбрали как разумный компромисс. Как заполняется форма, видно на [рисунках 64-66](#).

Рисунок 64.

	Quotation end
Test ID	<input type="text" value="OnDemand"/> <a href="#">OnDemand</a>
Test name *	a2-ca-URLUP
Class (IP Precedence or DSCP)	BE <input type="text"/>
SLA policy profile	<input type="text"/>
Service	<input type="text"/>
Provider	<input type="text"/>
SRC agent *	alt10-iqma2 <input type="text"/>
DST agent *	ca-np <input type="text"/>
Source IP	<input type="text"/>

Рисунок 65.

Number of probes	<input type="text" value="10"/>	200
Number of probes to ignore	<input type="text"/>	
URL	http:// <input type="text"/> /cgi-bin/urlup-load	
URL-test query interval (ms)	<input type="text"/>	
Cookie file	<input type="text"/>	
HTTP User-Agent	<input type="text"/>	
Content download timeout	<input type="text"/>	
DST agent type	<input type="text"/>	A
Test type	URLUP <input type="text"/>	U0
VoIP profile	<input type="text"/>	

Рисунок 66.

<b>CMD timeout kill signal</b>	<input type="text" value="v"/>
<b>Test timeout (sec)</b>	<input type="text"/>
<b>Test-specific parameters</b>	<code>/bin/cat</code>
<b>Send config to CMD's STDIN</b>	<input type="text" value="v"/>
<b>Log CMD's STDOUT</b>	<input type="text" value="v"/>
<b>Redirect CMD's STDERR to STDOUT</b>	<input type="text" value="v"/>
<b>Enabled</b>	<input type="text" value="v"/>
<b>Packet size (B)</b>	<input type="text"/>
<b>On demand test</b>	<input type="text" value="0"/>

Теперь в системе есть и тест на загрузку данных по указанному URL.

## 18 Тест DNS между АИ2 и DNS

Для тестирования DNS-серверов (без использования системного транслятора имён, конечно же) как на доступность, так и на производительность, предназначен DNS-тест. Фактически, это нагрузочное тестирование. Разумеется, поскольку мы будем использовать сервер **D.D.D.D** оператора связи, стоит ограничить количество запросов. В данном документе мы используем 5 запросов, это более-менее разумный компромисс между самим тестированием и нежеланием получить поток запросов, которые может нанести вред самому оператору. Будьте аккуратны! В случае необходимости используйте свои DNS-сервера как сопряжённый агент. В этом случае вы сможете под руководством своего персонала сделать всё корректно. Мы же рекомендуем пока придерживаться указанных в таблице настроек. Для создания выбираем Configuration → IQM Agents → Tests в меню или в форме редактирования clear. В этот раз следует выставить следующие поля в форме:

Имя поля	Вводимое значение
Test name	a2-dns-DNS
Class	BE
SRC agent	alt10-iqma2
DST agent	dns-oper
Number of probes	5
URL	dns://www.nalog.gov.ru
Test type	DNS
Packet size	512
On demand test	0

Как и в прошлых главах документации, приведены копии экранов для лучшего

понимания, что именно вы делаете. Форма заполняется, как показано на [рисунках 67-69](#). Команда add вам уже знакома.

**Рисунок 67.**

	Quotation char
Test ID	<input type="text" value="OnDemand"/>
Test name *	a2-dns-DNS
Class (IP Precedence or DSCP)	BE
SLA policy profile	<input type="text"/>
Service	<input type="text"/>
Provider	<input type="text"/>
SRC agent *	alt10-iqma2
DST agent *	dns-oper

**Рисунок 68.**

Number of probes	<input type="text" value="5"/>	200
Number of probes to ignore	<input type="text"/>	
URL	dns://www.nalog.gov.ru	
URL-test query interval (ms)	<input type="text"/>	
Cookie file	<input type="text"/>	
HTTP User-Agent	<input type="text"/>	
Content download timeout	<input type="text"/>	
DST agent type	<input type="text"/>	A
Test type	DNS	U0

**Рисунок 69.**

Send config to CMD's STDIN	<input type="text"/>
Log CMD's STDOUT	<input type="text"/>
Redirect CMD's STDERR to STDOUT	<input type="text"/>
Enabled	<input type="text"/>
Packet size (B)	512
On demand test	0

Основные тесты заведены, теперь можно сделать один дополнительный.

## 19 Тест CMD между АИ1 и STUB

Одним из способов расширения возможностей IQM это CMD-тесты. Их агент-инициатор запускает как обычные программы, выдающих результат на стандартный вывод. Полное описание выходит за рамки настоящей документации. До заведения теста в СУ следует создать тестовую программу на агенте АИ1. Для этого следует зайти по SSH, либо с консоли под пользователем (в документации пользователь cae). Команда создания файла выглядит так:

```
$ cat <<EOFEOF >~/cmd-test.pl
#!/usr/bin/perl

use strict ;
use warnings ;

print "SDLostPercent ",rand()*100.0
,"\nDSLostPercent ",rand()*100.0,"\n" ;
exit 0 ;
EOFEOF
```

Так же следует не забыть дать на свежесозданную программу нужные права (запуска в первую очередь). Команда следующая:

```
$ chmod 555 ~/cmd-test.pl
```

Пример исполнения указанных команд показан на [рисунке 70](#).

**Рисунок 70.**

```
[cae@alt10-iqmal ~]$ cat <<EOFEOF >~/cmd-test.pl
> #!/usr/bin/perl
>
> use strict ;
> use warnings ;
>
> print "SDLostPercent ",rand()*100.0
> ,"\nDSLostPercent ",rand()*100.0,"\n" ;
> exit 0 ;
> EOFEOF
[cae@alt10-iqmal ~]$ chmod 555 ~/cmd-test.pl
[cae@alt10-iqmal ~]$ █
```

После создания самой программы можно вернуться в web-интерфейс СУ и уже знакомым способом начать создавать тест со следующими параметрами:

Имя поля	Вводимое значение
Test name	a1-stub-CMD
Class	BE
SRC agent	alt10-iqma1
DST agent	gw
Test type	CMD
Test command ...	/home/cae/cmd-test.pl
On demand test	0

В качестве сопряжённого агента в этом случае можно выбирать, в принципе, любой, так как реального обращения к нему не ведётся. Мы выбираем, например, gw, вы можете сделать иначе, итоговый результат от этого не изменится. После ввода всех полей следует нажать add, как и в прошлых главах. Как заполняются поля, видно на [рисунке 71](#) и [рисунке 72](#).

**Рисунок 71.**

<b>Test name *</b>	a1-stub-CMD
<b>Class (IP Precedence or DSCP)</b>	BE ▾
<b>SLA policy profile</b>	▾
<b>Service</b>	▾
<b>Provider</b>	▾
<b>SRC agent *</b>	alt10-iqma1 ▾
<b>DST agent *</b>	gw ▾

Рисунок 72.

Test type	CMD
VoIP profile	
Test command (for LOCAL or CMD tests)	 /home/cae/cmd-test.pl
CMD options	
CMD timeout kill signal	
Test timeout (sec)	
Test-specific parameters	
Send config to CMD's STDIN	
Log CMD's STDOUT	
Redirect CMD's STDERR to STDOUT	
Enabled	
Packet size (B)	
On demand test	0

Теперь все тесты, запланированные для этапа тестирования IQM, заведены. Данные с АИ1 и АИ2 должны поступать на СУ по мере исполнения тестов.

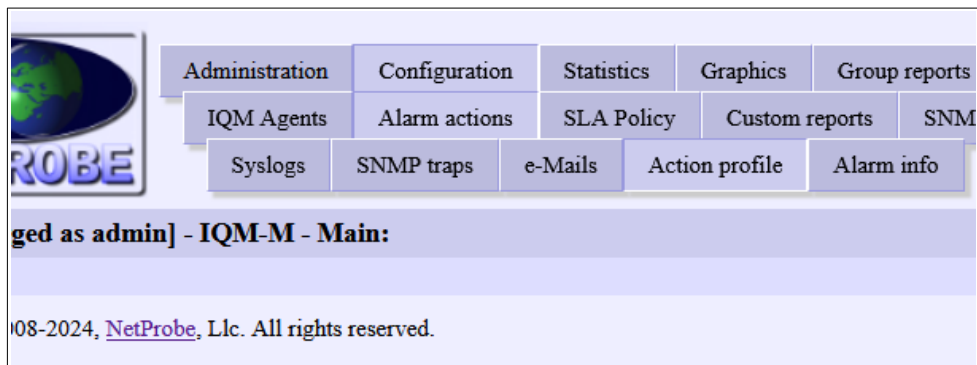
## 20 Настройка политик контроля

Запущенные на агентах тесты выдают данные в СУ, которая имеет возможность провести анализ. В частности, сверить результаты статистического наблюдения за метриками сети с порогами, которые либо требуются по руководящим документам, либо по дополнительным соглашениям о качестве предоставляемых услуг. Подробности доступны отдельно, здесь мы просто констатируем возможность для целей тестирования в новой ОС.

Сразу отметим, что простой контроль — это хорошо, но в системе имеются и реакции, которые могут создаваться, если пороги нарушены тем или иным образом. Поскольку в политике есть ссылка на реакции, создадим вначале специальный профиль сообщений.

Заходим в меню Configuration → Alarm actions → Action profile. Это может выглядеть, как показано на [рисунке 73](#). Мы попадём в форму редактирования нужных нам профилей.

Рисунок 73.



В самой форме, как показано на [рисунке 74](#), записываем имя `trap-n-syslog` в поле «Alarm action name», в поле «Trap hosts» делаем отметку мышью на `trap_local` (встроенная отсылка по SNMP), удерживая `Ctrl`, а в поле «Syslog hosts» делаем аналогично на `syslog_local` (встроенная отсылка по `syslog`). После чего нажимаем уже знакомую команду `add` в меню формы редактирования.

Рисунок 74.

The screenshot shows the configuration form for adding a new alarm action. At the top is a toolbar with icons for: add (green plus), fill form (orange arrow), CSV (document with 'd'), view (magnifying glass), change (green checkmark), delete (red X), and clear (document with 'x'). The form contains the following fields:

- Deploy on: (empty)
- Parameter: (empty)
- Value: (empty)
- Default: (empty)
- Alarm action ID: (dropdown menu)
- Alarm action name \*: `trap-n-syslog`
- Alarm action description: (empty)
- IQMM URL: (empty) | Default: `http://localhost/iqm/`
- External program: (empty)
- Trap hosts: (list box with `trap_local` selected)
- Syslog hosts: (list box with `syslog_local` selected)
- mail\_root@local: (list box with `mail_root@local` selected)

Для контроля верности заведения можете использовать уже знакомые команды `clear` и `view`, после чего прокрутить форму вниз. Таблица с профилями реакций должна выглядеть, как показано на [рисунке 75](#).

Рисунок 75.

Alarm action ID	Alarm action name *	Alarm action description	IQMM URL	External program	Trap hosts	Syslog hosts	Email
1	action_syslog	send local syslog	http://localhost/iqm/			syslog_local	
2	trap-n-syslog	send local syslog	http://localhost/iqm/		trap_local	syslog_local	

2 rows  
Copyright (C) 2008-2024, NetProbe, Llc. All rights reserved.

Теперь, когда заведена нужная реакция (отослать SNMP trap и отослать сообщение в syslog, если зафиксирована проблема), можно заводить и саму политику контроля. Выбираем в меню Configuration → SLA Policy → SLA profile. Как это выглядит, показано на [рисунке 76](#).

Рисунок 76.

Administration Configuration Statistics Graphics Group reports Custom reports Map Help  
 IQM Agents Alarm actions SLA Policy Custom reports SNMP profiles SNMP V3 Securities UNIX signals  
 Services Providers Classes Zones Thresholds SLA profile Maintenance window Total quality

admin] - ALARM\_ACTIONS CONFIGURATION: Manage SLA profiles  
 CONFIGURATION

Поля формы политики контроля заполняем следующим образом.

Имя поля	Вводимое значение
Policy name	policy-test
Crimson action	trap-n-syslog
Red action	trap-n-syslog
Yellow action	trap-n-syslog
Green action	trap-n-syslog
Thresholds	DSLloss-0.5-1-3 SDLoss-0.5-1-3

Обращаем внимание, что поскольку в поле «Thresholds» большой список и можно выбрать несколько элементов, следует не просто выбирать нужное кликом мышью, а удерживать при этом Ctrl (стандартный множественный выбор в браузере). Список порогов следует при необходимости прокрутить вниз. Как заполняется форма политики показано на [рисунках 77, 78](#) и (после прокрутки поля) [79](#).

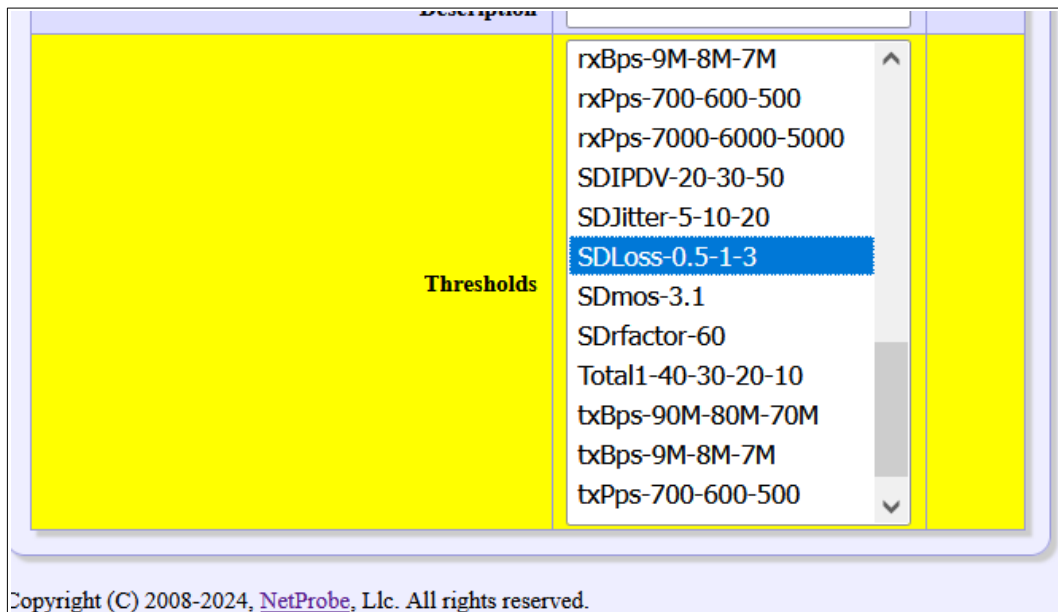
**Рисунок 77.**

Deploy on:		
Parameter	Value	Default
Policy ID	<input type="text" value=""/>	
Policy name	<input type="text" value="policy-test"/>	
Class (IP Precedence or DSCP)	<input type="text" value=""/>	
Source zone	<input type="text" value=""/>	
Destination zone	<input type="text" value=""/>	
Number of violations enough to rise a problem	<input type="text" value=""/>	1
Number of violations enough to down a problem	<input type="text" value=""/>	0
Check horizon (min)	<input type="text" value=""/>	60
Crimson action	<input type="text" value="trap-n-syslog"/>	
Red action	<input type="text" value="trap-n-syslog"/>	
Yellow action	<input type="text" value="trap-n-syslog"/>	
Green action	<input type="text" value="trap-n-syslog"/>	
Blue action	<input type="text" value=""/>	
Description	<input type="text" value=""/>	

**Рисунок 78.**

Description	
Thresholds	<ul style="list-style-type: none"> <li>cpuUser-50-40-30</li> <li>cpuWait-50-40-30</li> <li>DSIPDV-20-30-50</li> <li>DSJitter-5-10-20</li> <li style="background-color: #0070C0; color: white;">DSLoss-0.5-1-3</li> <li>DSmos-3.1</li> <li>DSrfactor-60</li> <li>NTP-sync-0.9</li> <li>PPP-bad-5-3-0</li> <li>PPP-cont-0.9</li> <li>PPP-early-0.9</li> <li>PPP-ip-0.9</li> </ul>

Рисунок 79.



После заполнения следует нажать команду `add` в меню формы (либо вверху, либо на выплывающем по требованию). Затем можно проконтролировать состояние политик знакомым вызовом команд `clear` и `view`. Результат должен быть таким же, как на [рисунке 80](#).

Рисунок 80.

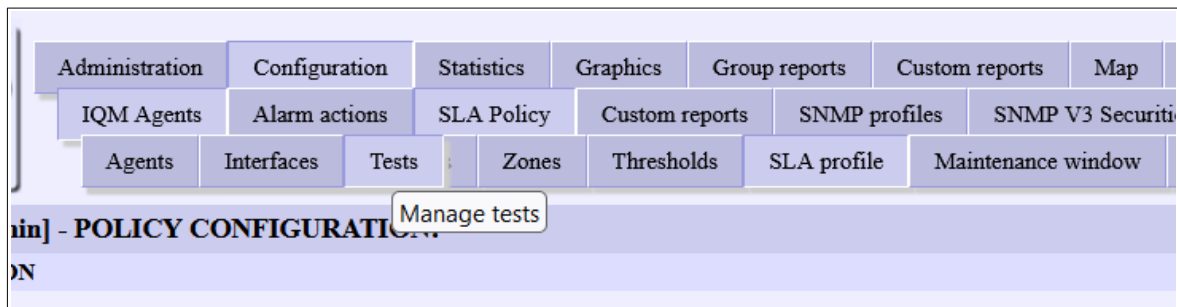
Policy ID	Policy name	Class (IP Precedence or DSCP)	Source zone	Destination zone	Number of violations enough to rise a problem	Number of violations enough to down a problem	Check horizon (min)	Crimson action	Red action	Yellow action	Green action	Blue action	Description	Thresholds
10	policy-test				1	0	60	trap-n-syslog	trap-n-syslog	trap-n-syslog	trap-n-syslog			SDLoss-0.5-1-3 DSLoss-0.5-1-3 SDLoss-0.5-1-3 DSLoss-0.5-1-3

Видно, что в политике `policy-test`, при получении одного или более события по превышению одного из порогов, описанных в соответствующей таблице с именами `SDLoss-0.5-1-3` либо `DSLoss-0.5-1-3`, за последние 60 минут, то для порогов `Crimson`, `Red`, `Yellow` будет вызвана реакция `trap-n-syslog`, а если будет ноль таких событий, а до этого было превышение, то по `Green action` будет вызвано так же реакция `trap-n-syslog`. Более подробно политики контроля описаны отдельно от настоящей документации.

После создания политики контроля следует выбрать тот тест, метрики от которого будут проверяться. Для наших целей наилучшим образом подходит тест под именем `a1-stub-CMD`, который, как вы помните, был создан на языке программирования Перл специально с вызовом функции `rand()`. Таким образом, у нас практически всегда этот тест будет возвращать хотя бы одно значение метрики `SDLostPercent` или `DSLostPercent` большее, чем 0.5. Следовательно, политика контроля будет вызывать реакции `trap-n-syslog`, предусмотренные в её настройках.

Выбираем редактирование тестов в меню `Configuration` → `IQM Agents` → `Tests`, как показано на [рисунке 81](#).

Рисунок 81.



Выбираем в поле Test ID имя a1-stub-CMD, как показано на [рисунке 82](#), и нажимаем в меню команду fill form. Произойдёт заполнение формы данными теста с выбранным именем.

Рисунок 82.

Parameter	Value	
fill form	<input checked="" type="checkbox"/> On agent <input checked="" type="checkbox"/> On DB <input checked="" type="checkbox"/> Drop statistics when deleting	
★ Create template	<input type="text"/>	
✖ Delete template	<input type="text"/>	
	Load template	
Multiconf	Обзор... Файл не выбран. <input type="text"/> Separation char <input type="text"/> Quotation char <input type="text"/>	Enter C
Test ID	a1-stub-CMD <input type="button" value="OnDemand"/>	
Test name *	<input type="text"/>	
Class (IP Precedence or DSCP)	<input type="text"/>	1
SLA policy profile	<input type="text"/>	
Service	<input type="text"/>	1

В поле «SLA policy profile» выбираем нужную нам политику policy-test. Это показано на [рисунке 83](#).

Рисунок 83.

Parameter	Value
Multiconf	Обзор... Файл не выбран.
	Separation char
	Quotation char
Test ID	a1-stub-CMD <a href="#">OnDemand</a>
Test name *	a1-stub-CMD
Class (IP Precedence or DSCP)	BE
SLA policy profile	▼
Service	<ul style="list-style-type: none"> <li>null</li> <li>policy-test</li> <li>policy_basic</li> <li>policy_basic_web</li> <li>policy_PPPOE</li> <li>policy_voip</li> </ul>
Provider	
SRC agent *	
DST agent *	
Source IP	

После выбора политики наводим мышь на команду меню формы change и нажимаем её, как показано на [рисунке 84](#).

Рисунок 84.

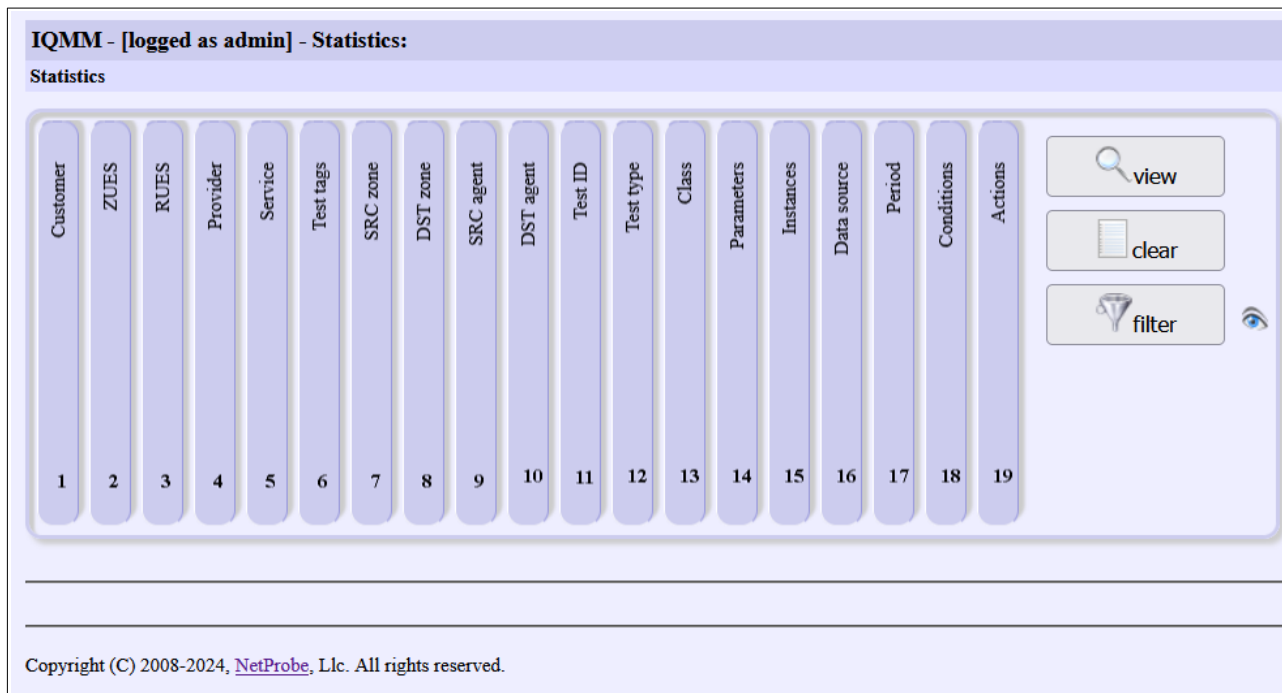
Parameter	Value
	<input checked="" type="checkbox"/> On agent <input type="button" value="change"/> <input checked="" type="checkbox"/> On DB <input checked="" type="checkbox"/> Drop statistics when deleting
<input type="button" value="Create template"/> <input type="button" value="Delete template"/>	<input type="text" value=""/> <input type="button" value="Load template"/>
<b>Multiconf</b>	<input type="button" value="Обзор..."/> Файл не выбран. Separation char <input type="text" value=""/> Quotation char <input type="text" value=""/>
<b>Test ID</b>	a1-stub-CMD <input type="button" value="OnDemand"/>
<b>Test name *</b>	a1-stub-CMD
<b>Class (IP Precedence or DSCP)</b>	BE <input type="button" value="v"/>
<b>SLA policy profile</b>	policy-test <input type="button" value="v"/>
<b>Service</b>	L4 Internet <input type="button" value="v"/>
<b>Provider</b>	Default <input type="button" value="v"/>
<b>SRC agent *</b>	alt10-iqma1 <input type="button" value="v"/>
<b>DST agent *</b>	gw <input type="button" value="v"/>

Теперь тест a1-stub-CMD использует политику контроля. И при поступлении данных о сетевых метриках «Процент потерянных пакетов от источника к получателю» (SDLostPercent) или «Процент потерянных пакетов от получателя к источнику» (DSLostPercent) система управления проведёт анализ и, в случае проблем, сделает сообщения в syslog и snmptrapd. Так же будет сообщение, если проблема уже фиксировалась, но после выхода за горизонт событий больше не происходит.

## 21 Просмотр графиков

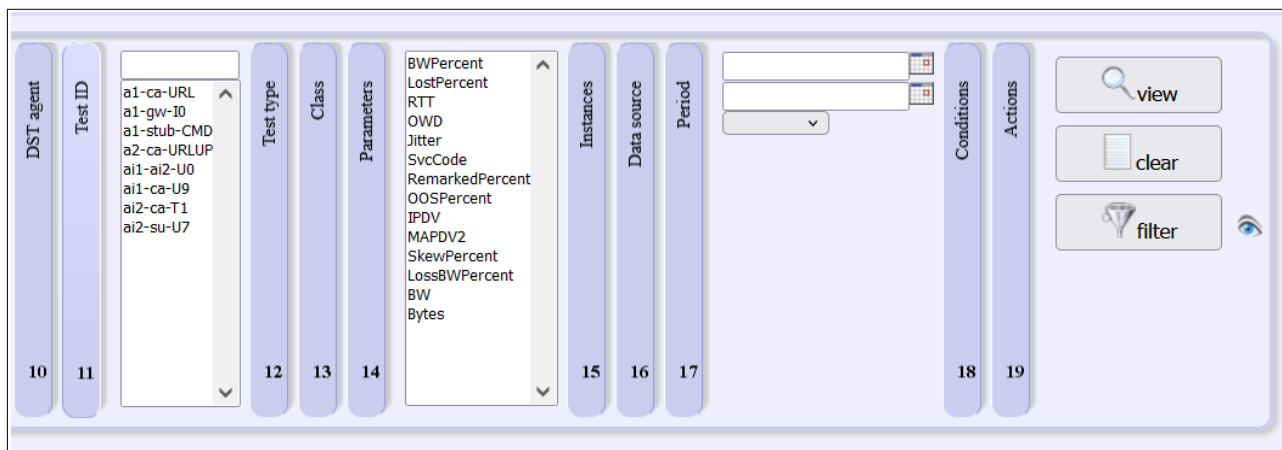
Для того, чтобы в системе управления накопились некоторые данные, полученные от тестирования, разумеется, нужно время. Поэтому мы рекомендуем к данному этапу переходить не менее, чем через сутки-двое после настроек. Графики — достаточно часто используемое меню системы, поэтому они вынесены на главный уровень. После вызова этого пункта меню появится фильтр. В штатной СУ обычно содержится много тестов и их результатов. В отличие от нашей лаборатории. Поэтому фильтрация только того, что реально нужно администратору — важный фактор. На рисунке 85 можно видеть фильтр в виде так называемого «баяна», где вкладки можно открывать и закрывать аналогично мехам.

Рисунок 85.



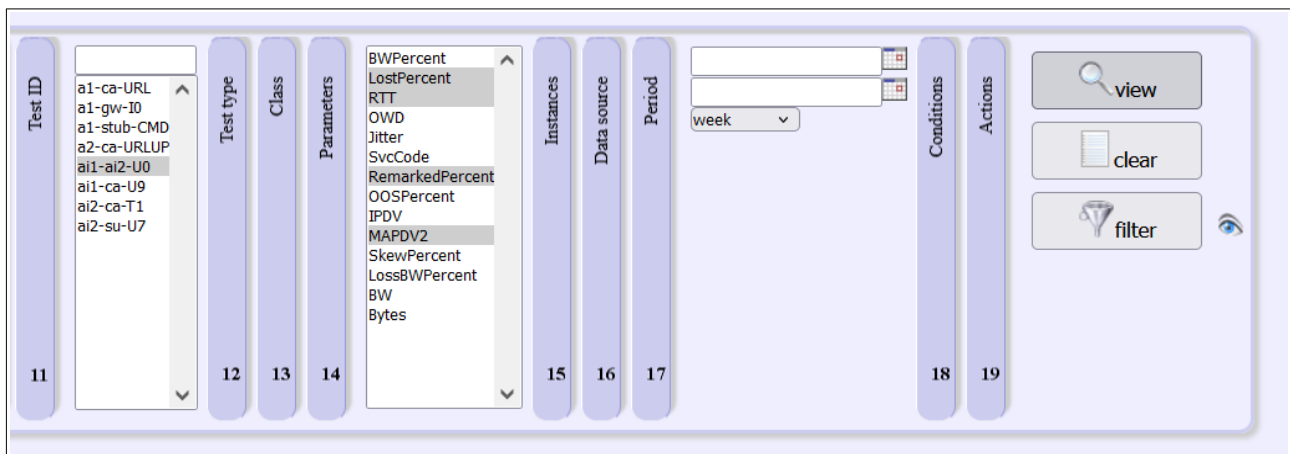
Внутри каждой вкладки возможность выбора того или иного варианта фильтрации. Поскольку у нас данных немного, мы будем использовать только вкладки Test ID, Parameters, Period. Откроем их, как показано на [рисунке 86](#), кликнув мышью на соответствующие разделы.

Рисунок 86.



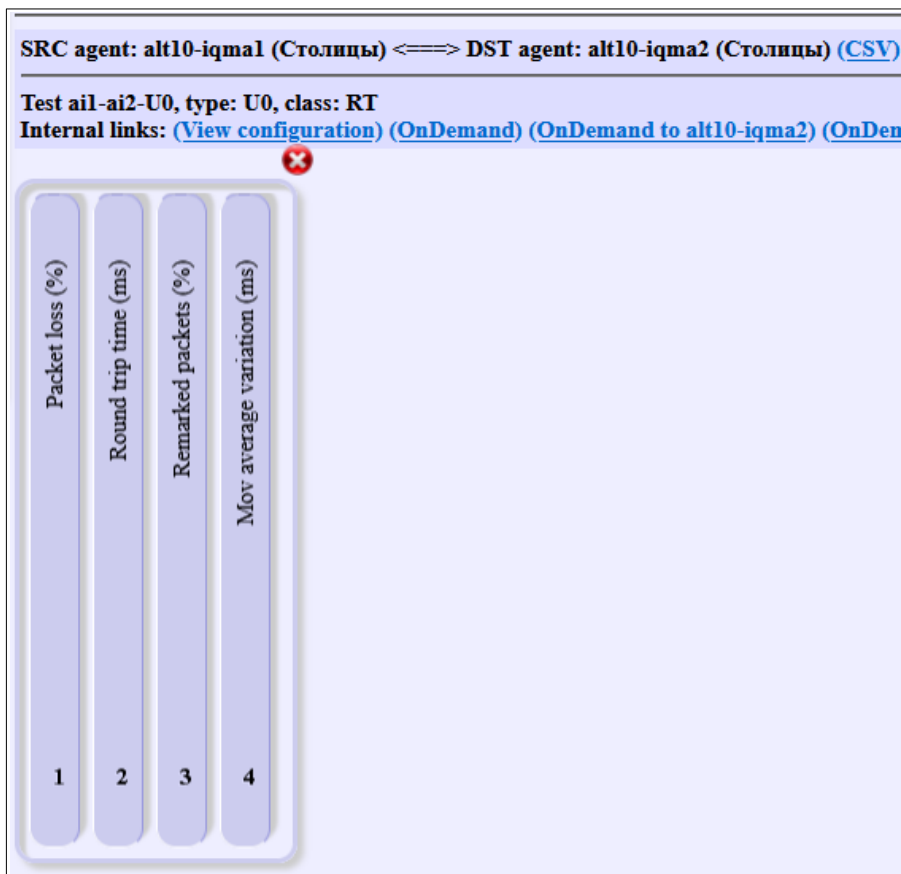
При входе и выходе из меню графиков в дальнейшем, состояние вкладок фильтра должно сохраняться в хранилище браузера. Мы будем выбирать каждый тест по одному (можно выбирать и несколько, но для тестирования так проще), при этом все параметры не будем использовать, а выберем только некоторые. Для первых тестов LostPercent, RTT, RemarkedPercent и MAPDV2. Когда будет нужно, мы укажем, что следует выбрать другие параметры. Полное описание параметров не входит в наше тестирование. Период же мы рекомендуем выбирать в неделю (week), но вы можете выбрать и иной. Пример того, что для просмотра графиков выбран тест ai1-ai2-U0, параметры указанные выше и период «неделя» показан на [рисунке 87](#). Далее следует нажать кнопку view.

Рисунок 87.



После нажатия указанной кнопки ниже фильтра появятся разделы посвящённые тесту ai1-a2-U0 в виде заголовка и новых вкладки так называемого «баяна», на этот раз с графиками.

Рисунок 88.

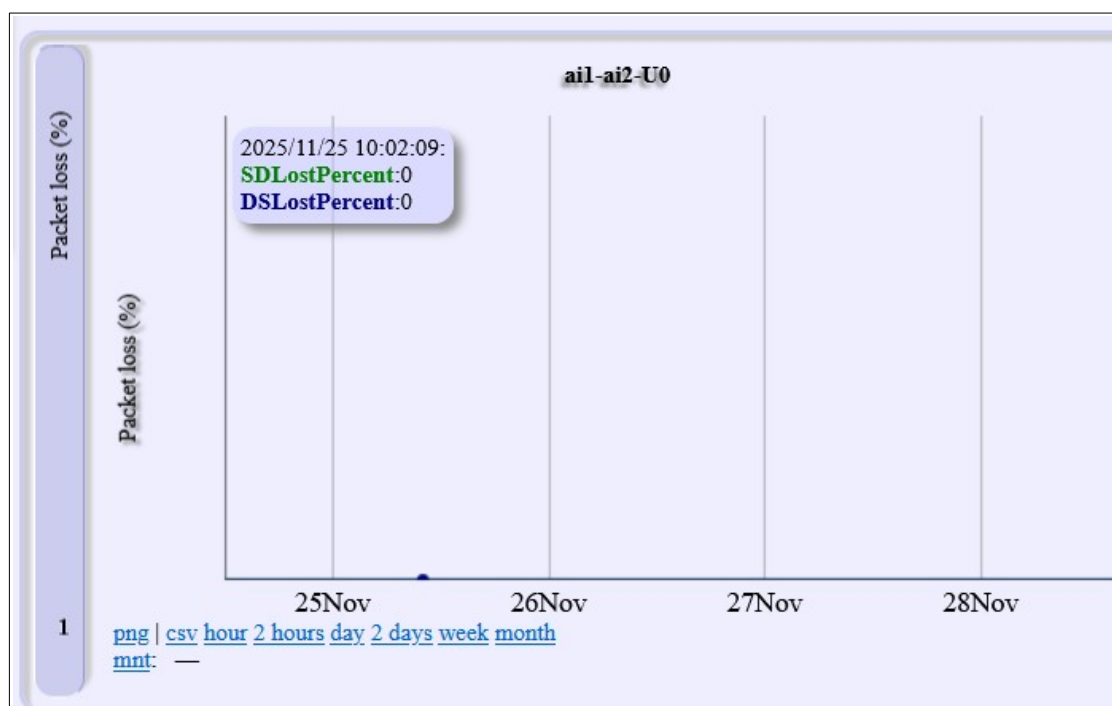


Уже знакомым вам методом можно открывать нужные графики. Полное описание возможностей графиков не входит в наши планы, мы просто просматриваем результаты и оцениваем их. Однако, базовое понимание вам необходимо. Каждый протокол тестирования может возвращать результаты о метриках качества по пропуску сетью трафика в двух

направлениях — от агента-инициатора к сопряжённому (SD) и от сопряжённого к инициатору (DS). По оси абсцисс отложено текущее время. А по оси ординат — от двух до четырёх параметров. Вверх от оси абсцисс — для параметров SD, а вниз (в псевдо-отрицательную зону) — для параметров DS. Это удобно, так как позволяет на одном и том же графике иметь сразу два направления. Если метрика предусматривает расчёт минимальных, максимальных, средних или квадратичных за сессию тестирования, то в одном направлении показываются все такие результаты.

При движении мыши по графику (по оси времени) дополнительно показываются всплывающей подсказкой числовые значения параметров. Теперь перейдём к конкретике. Открываем вкладку «проценты потерь». Она внутри выглядит, как показано на [рисунке 89](#).

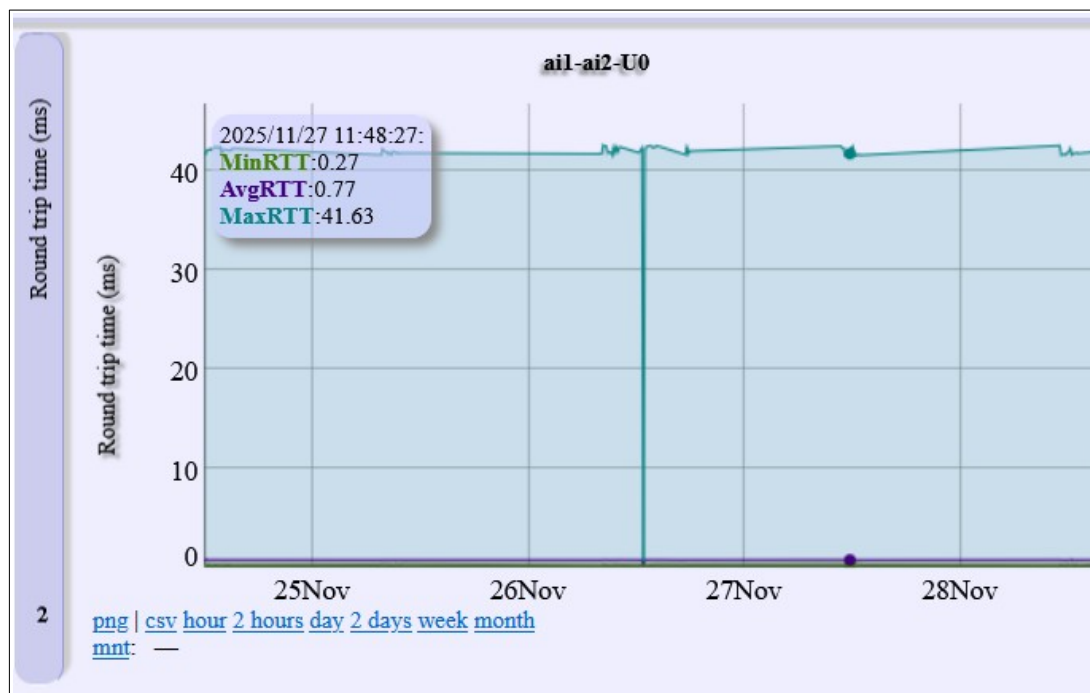
**Рисунок 89.**



На первый взгляд кажется, что значений нет. Но в реальности они просто нулевые, в чём можно убедиться, двигая мышью по графику влево и вправо (на рисунке всплывающая подсказка со значениями потерь от АИ1 к АИ2 (зелёный цвет) и от АИ2 к АИ1 (синий цвет)).

Теперь посмотрим круговую задержку (RTT). Она выглядит, как показано на [рисунке 90](#). На прямые линии на графиках не обращайте внимания, это артефакты графиков. Дело в том, что лаборатория, с которой происходило копирование экранов для данной документации, включалась и выключалась по мере возможности ввиду ограничений доступности оборудования. В связи с чем, допустим от условного времени в 18:00 до условного времени в 08:00 будут «пробелы» в данных, о которых построитель графика не имеет информации и пытается достроить график между периодами времени. Это не является ошибкой!

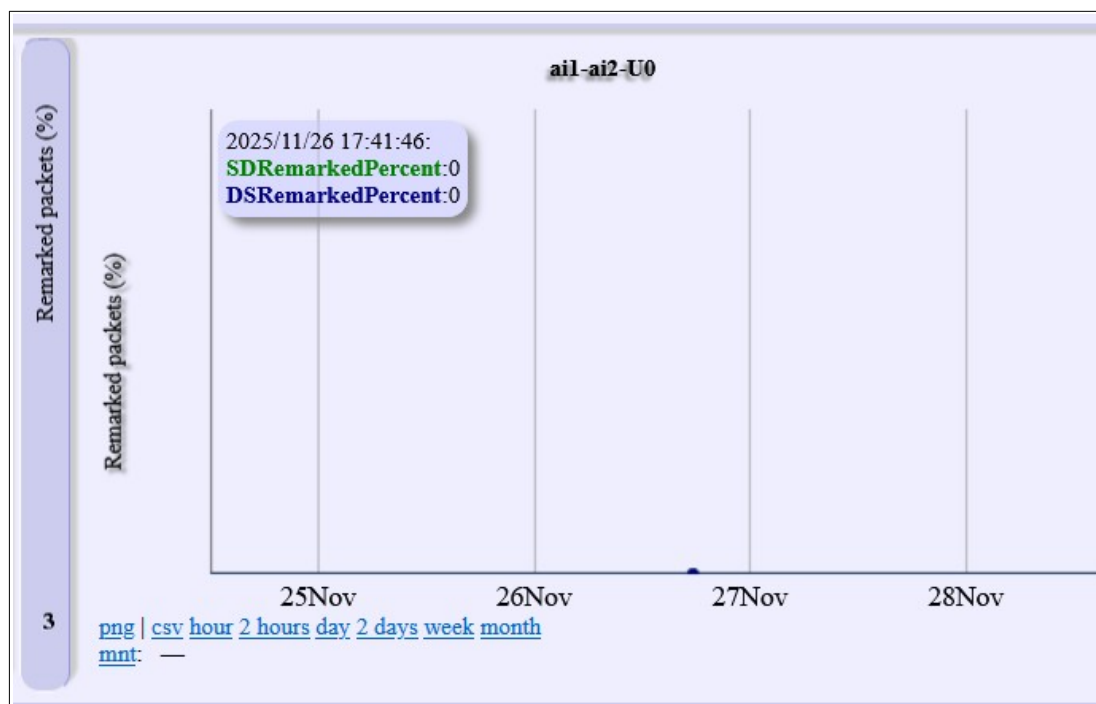
Рисунок 90.



А вот то, что максимальная круговая задержка за сессию составляет 40 миллисекунд, хотя оба агента были фактически включены в один неуправляемый коммутатор, возможно, следует дополнительно исследовать. Собственно, это один из тех случаев, для которых IQM как система и применяется в реальных установках.

Теперь рассмотрим процент перекрашенных пакетов. Смотрим на [рисунок 91](#).

Рисунок 91.



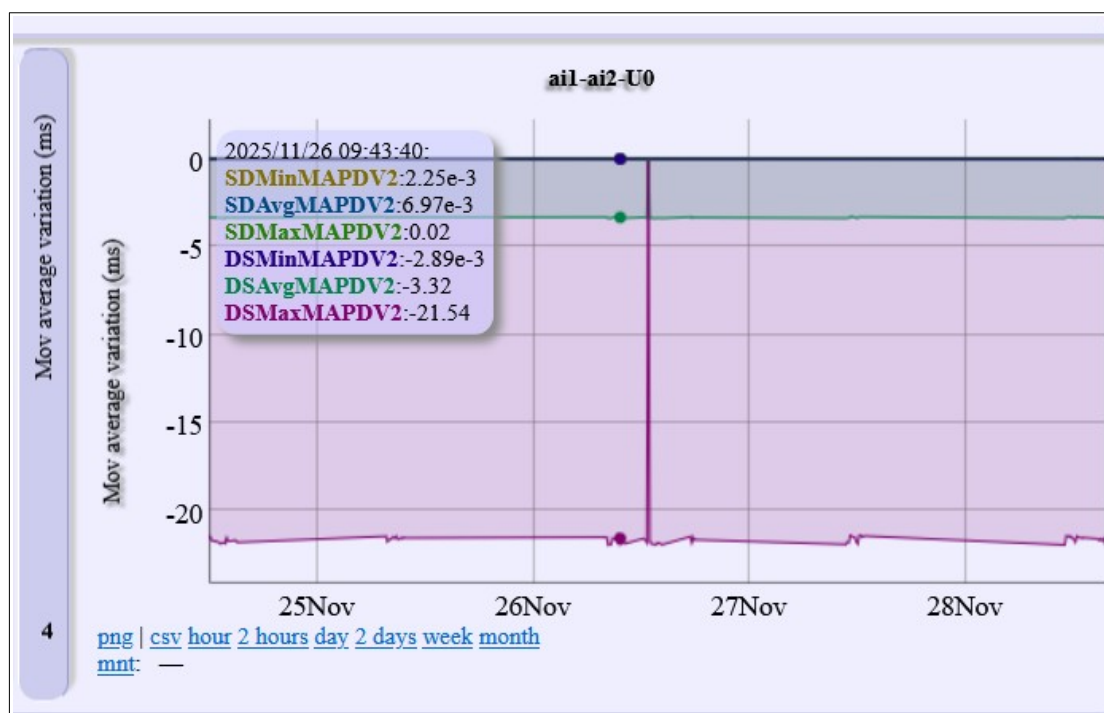
Напомним, что в настройках теста был указан класс сервиса RT. То есть, каждый пакет

в сессии тестирования имел поле TOS/DSCP, выставленное в приоритет 5 (подробности маркировки трафика обсуждаются отдельно от тестирования). При традиционных настройках сети IP/MPLS, либо Metro Ethernet, разметка трафика определённым образом позволяет оператору пропускать одни пакеты в первую очередь, другие — во вторую, а тем, кому не повезло (это обычно Интернет) — в самую последнюю и то, если есть возможность. Многие операторы даже гарантируют, что пользователю, если он пометит пакеты типом RT, будет предоставлена полоса в этом виде трафика в N мегабит на всей сети. Однако, как пользователь может превысить лимит, так и оператор может недосмотреть за всеми устройствами на сети. Именно поэтому возможность отследить переокраску трафика настолько важна. Это позволяет заранее узнать о проблемах, до реальных потерь на сети!

В данном случае, поскольку (см. выше) агенты включены в один коммутатор, и переокраска трафика не проводится, он полностью доставляется с нужным приоритетом (нули на графике).

Теперь рассмотрим так называемое «дрожание» времени доставки. Мы будем в настоящей документации использовать один из видов (G.1020). На [рисунке 92](#) видно, что максимальное дрожание фиксируется от АИ2 к АИ1 (обратный трафик). Возможно, причины либо в сетевой карте, либо в настройках сети, это следует выяснять дополнительно.

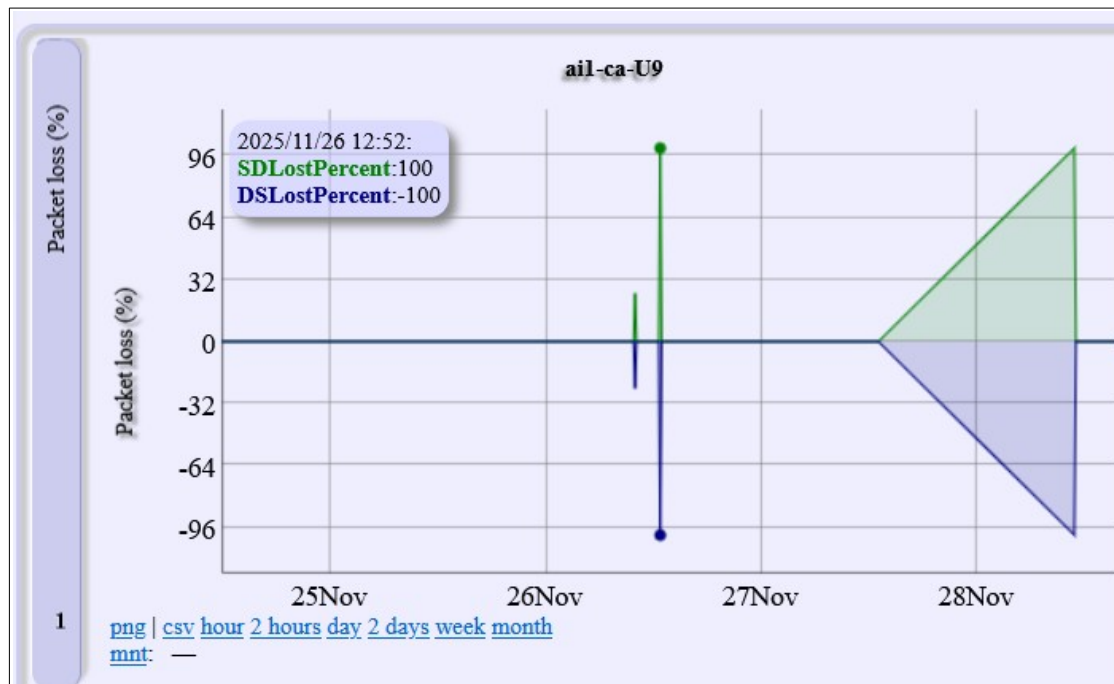
**Рисунок 92.**



Помимо этого, мы полагаем, что имеется общая причина у максимальной круговой задержки и максимального дрожания по G.1020.

Теперь рассмотрим графики теста a1-ca-U9. Сбрасываем в фильтре кнопкой clear текущий выбор, выбираем указанный тест, параметры такие же, как и раньше, и период в неделю. Далее нажимаем кнопку view. Вы вновь получите графики на вкладках. Рассмотрим их подробнее. На [рисунке 93](#) вновь потери.

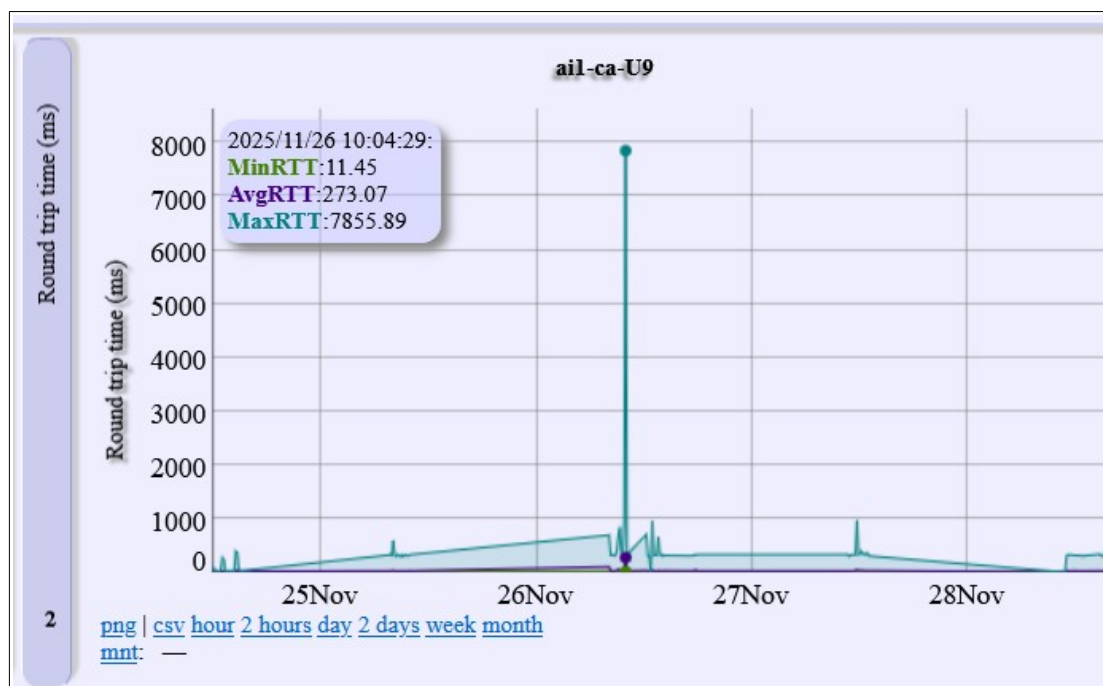
Рисунок 93.



Здесь видны потери уже по реальной сети Интернет от 10.55.1.10 до С.С.С.С. Включая 100% в обе стороны. Так, 26 ноября 2025 года в 12:52 все попытки установить связь между агентом АИ1 и СА были безуспешными. В целом, поскольку лаборатория для создания документации запускалась не всегда при наличии внешней сети (по технологическим причинам), это вполне допустимо.

Теперь переходим к круговой задержке. Видим на [рисунке 94](#), что тоже есть странности.

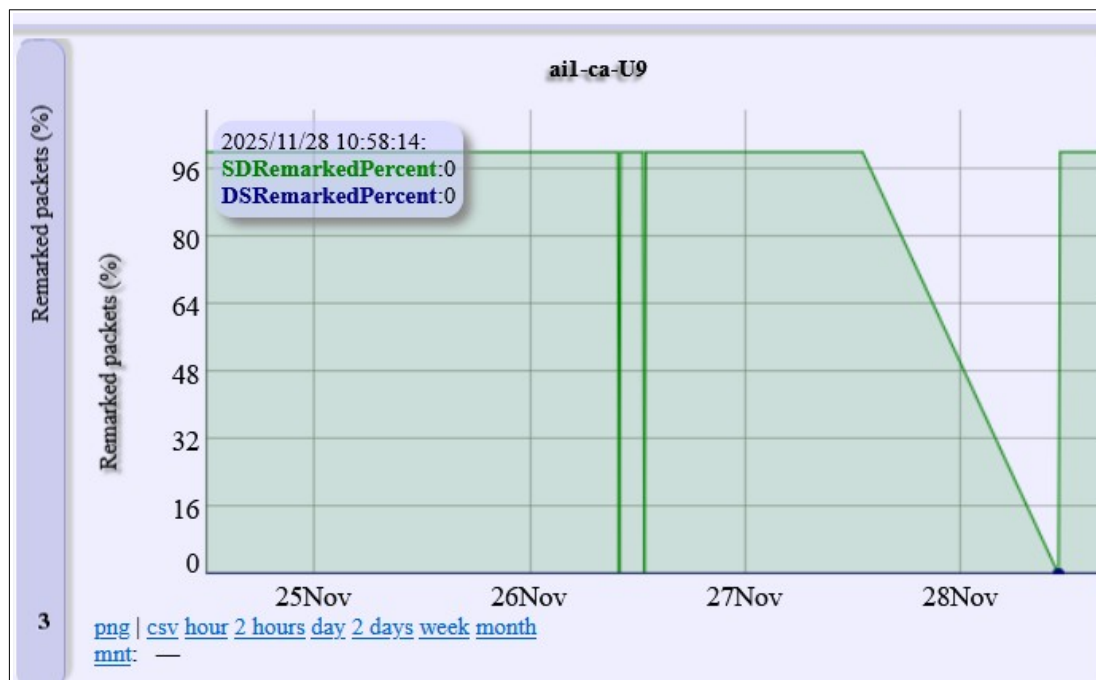
Рисунок 94.



В 10:04:29 максимальная круговая задержка за сессию составил 7.855 секунд! Это ненормально, конечно, но если трафик принимается и передаётся с промежуточным хранением на каких-либо устройствах, то вполне допустимо. Так же это могут быть особенности поведения так называемых SDN. Среднее же значение в этот момент, скорее всего «наведено» максимальным всплеском (пакетов-то всего 200).

Рассмотрим перекраску на [рисунке 95](#).

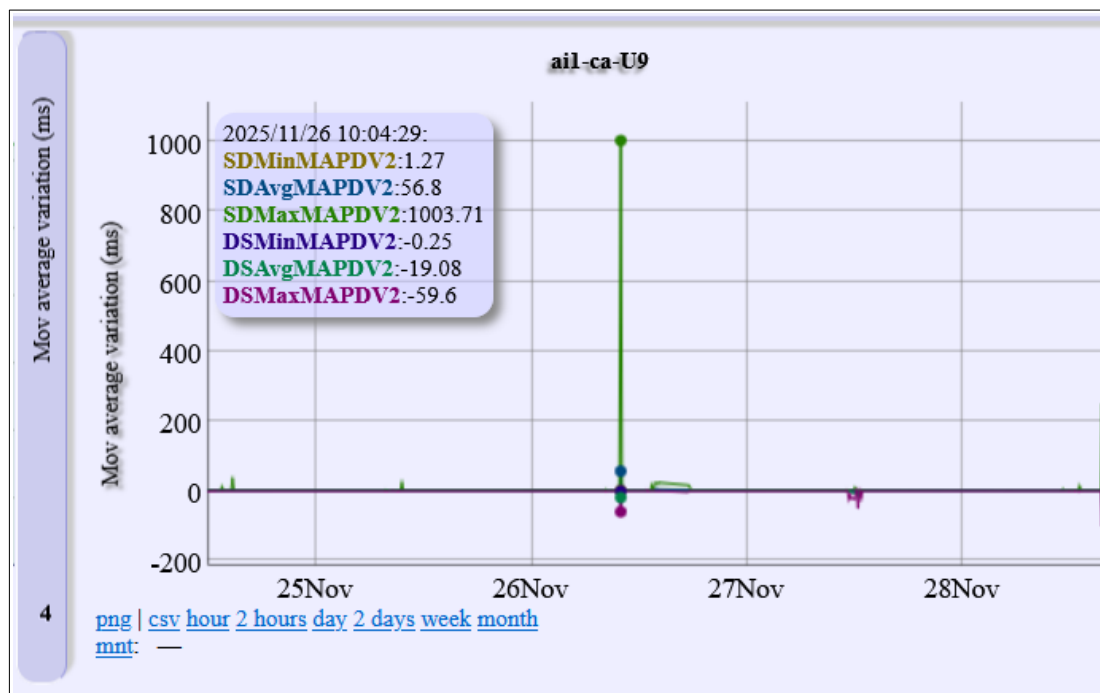
**Рисунок 95.**



Видно, что перекраска трафика осуществляется только от 10.55.1.10 к С.С.С.С. А в обратную сторону, хотя разметка и проводится сопряжённым агентом, тем не менее, доставляется с правильным классом RT. Для интернет включения лаборатории (а это именно так) первое — неудивительно. Любой оператор связи принудительно выставляет приоритет в 0 для всех пакетов, принимаемых для сети Интернет. Иначе можно легко выйти из бюджета. Поэтому и фиксируется перекраска. А вот обратный пример, когда от точки включения сопряжённого в сеть без подписанного дополнительного соглашения о качестве до 10.55.1.10 трафик приходит с пометкой RT — явно ошибка в конфигурации, причём, скорее всего, внутри целого конгломерата операторов связи.

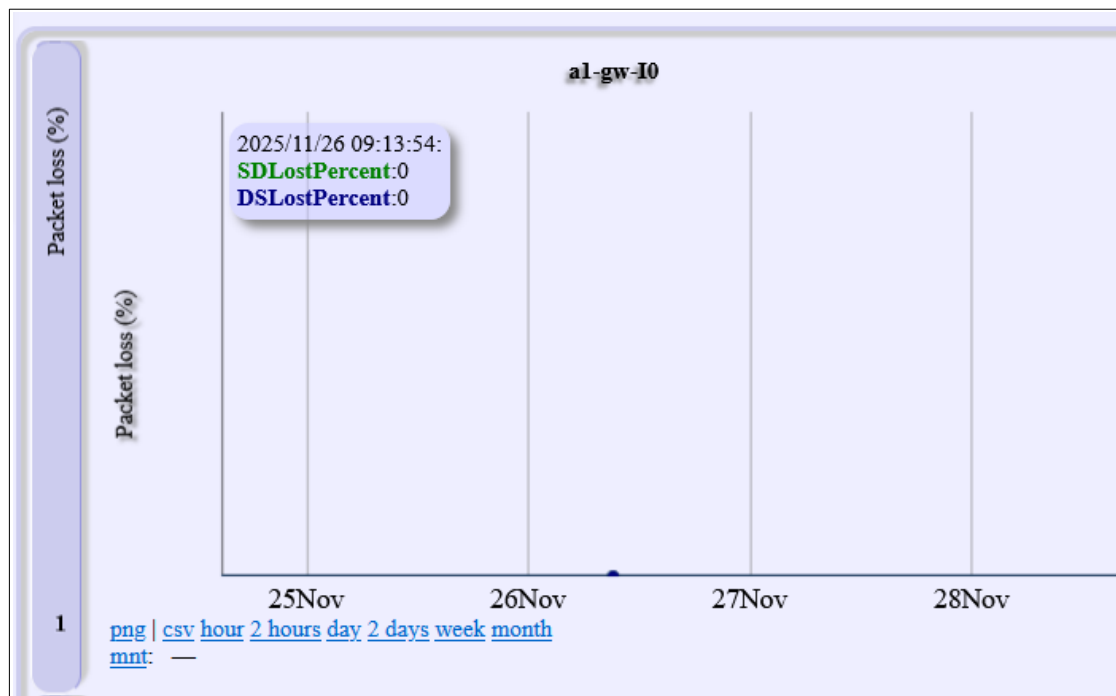
На [рисунке 96](#) показан график «дрожания» доставки пакетов для теста U9. Там видно, как и в случае круговой задержки, что есть проблема проксирования трафика где-то между устройствами, причём скорее всего от источника к получателю. Числовое же значение «дрожания» в одну секунду здесь скорее вторично и не может рассматриваться как ошибка. Важен сам факт такого поведения сетевых устройств. Его следует исправить.

Рисунок 96.



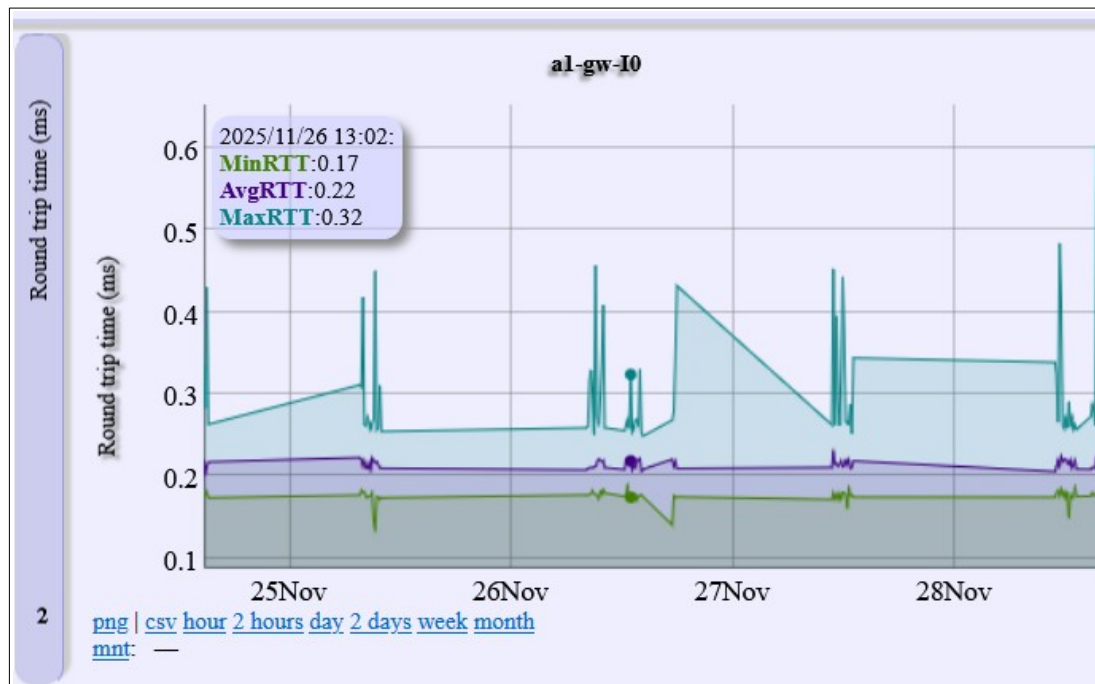
Переходим к тесту a1-gw-I0. То есть к ICMP-эхо. В фильтре делаем вновь clear, выбор теста и view. Смотрим на рисунок 97.

Рисунок 97.



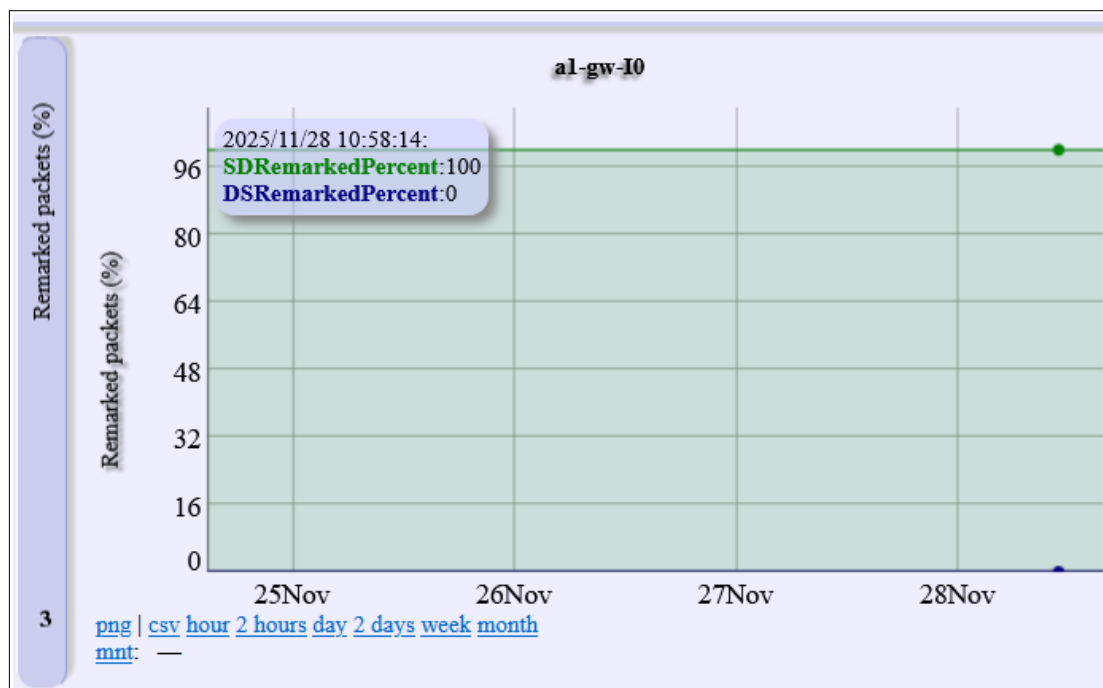
Собственно, и не удивительно, что между АИ1 и шлюзом нет потерь. Они, конечно, могут быть, если вы укажете скорость побольше. Но у нас 64 килобита в секунду и 200 пакетов, они прекрасно принимаются. Переходим на рисунок 98.

Рисунок 98.



С круговой задержкой всё в порядке, 400 микросекунд в пике, в среднем 220 — вполне нормально для включения через коммутатор. Артефакты выключения лаборатории тоже наглядно видны. Смотрим дальше, [рисунок 99](#).

Рисунок 99.

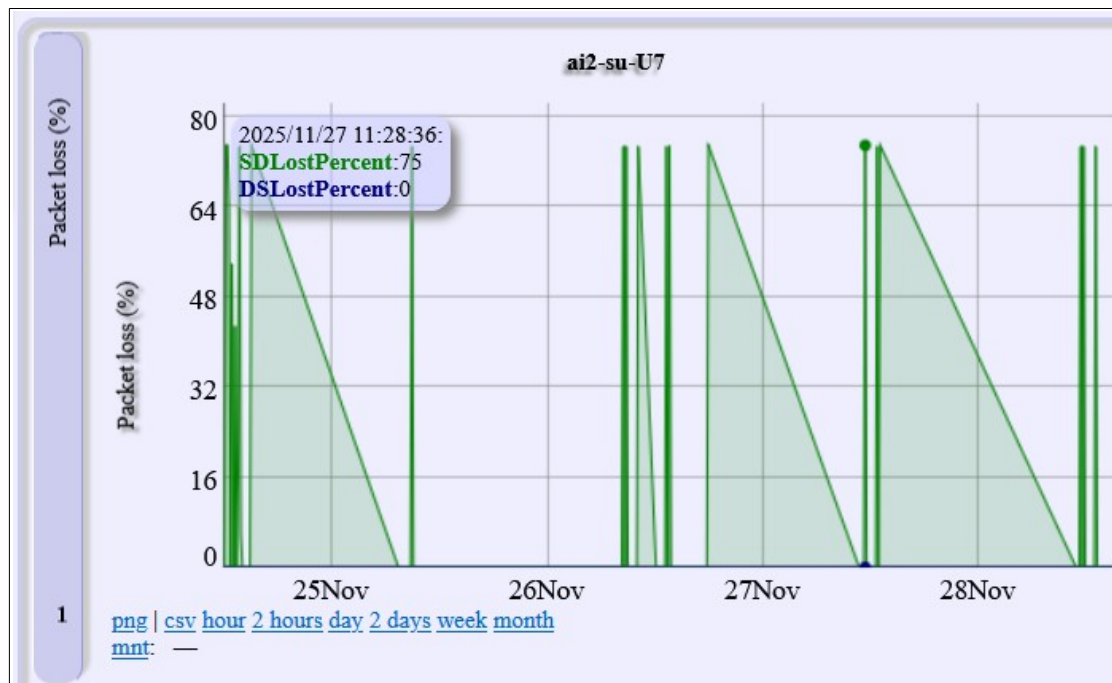


А вот с перекраской трафика (была метка RT) какая-то странность. Ведь мы уже видели, что транзитом через шлюз в тесте U9 всё проходило без проблем. Скорее всего, шлюз (а он простой) при отсылке эхо-ответа по ICMP просто-напросто создаёт пакет сам, не используя информацию о поле TOS/DSCP в принимаемых пакетах. Эта гипотеза всё

прекрасно объясняет. Но требует подтверждения.

Далее исследуем тест ai2-su-U7. Это уже UDP-эхо с использованием встроенного в систему управления суперсервера xinetd. Смотрим потери с [рисунка 100](#).

**Рисунок 100.**



Удивительно! То нет потерь, то 75 процентов. Кажется, что это явная ошибка. Но не будет торопиться. Запускаем для начала команду на подходящем хосте, например СУ

```
$ man xinetd.conf
```

Внутри man ищем раздел, посвящённый встроенному ограничению обработки входящих соединений (он для всех, включая UDP echo!). Раздел показан на [рисунке 101](#).

**Рисунок 101.**

<code>cps</code>	Limits the rate of incoming connections. Takes two arguments. The first argument is the number of connections per second to handle. If the rate of incoming connections is higher than this, the service will be temporarily disabled. The second argument is the number of seconds to wait before re-enabling the service after it has been disabled. The default for this setting is 50 incoming connections and the interval is 10 seconds.
------------------	--

Видно, что по умолчанию на вход к xinetd разрешается не более 50 соединений в секунду, а если произошло превышение, включится «интервал охлаждения», равный 10 секундам, когда никакие входящие соединения у сервиса, где произошла проблема, обрабатываться не будут. Это выглядит причиной, однако вновь не торопимся и проверяем. Используя знаменитую формулу расчёта межпакетного интервала из документации «Основы

тестирования сетей ТСП/IP для служб эксплуатации»

$$IPI_s = \frac{(P_s + O_s) \times 8}{B_s} \quad (c)$$

и вспоминая собственные настройки теста из [главы 13](#), проводим вычисления. Для простоты используем популярный язык программирования Перл в виде так называемого «однотрочника».

```
$ perl -e 'print((256+28)*8/64/1024,"\n")'
```

Результат виден на [рисунке 102](#).

### Рисунок 102.

```
[cae@alt10-iqmm ~]$ perl -e 'print((256+28)*8/64/1024,"\n")'
0.03466796875
[cae@alt10-iqmm ~]$ █
```

Межпакетный интервал составит 0.03466796875 секунд. То есть, для создания трафика по протоколу UDP echo скоростью 64 килобита в секунду размером пакета 256 байт требуется выслать пакет и подождать 0.03466796875 секунд до отсылки следующего. Поскольку  $IPI_s$  удобен нам, но `xinetd` использует обратную величину  $IPI_s^{-1}$ , рассчитаем получаемую пакетную скорость (в англоязычной литературе — pps). Вновь используем «однотрочник».

```
$ perl -e 'print(1/0.03466796875,"\n")'
```

Результат — на [рисунке 103](#).

### Рисунок 103.

```
[cae@alt10-iqmm ~]$ perl -e 'print(1/0.03466796875,"\n")'
28.8450704225352
[cae@alt10-iqmm ~]$ █
```

Итак, первое впечатление — всё-таки ошибка. Видимо, в IQM! Создаём всего-то 28.845 пакетов в секунду (это расчётная скорость, конечно же, реальная всегда округляется до целого в большую сторону), в `xinetd` указано 50 в секунду. Но торопиться в данном вопросе — последнее дело. Ибо сказано: «Спешка ошибки порождает». Проведём исследование. Посмотрим исходные тексты `xinetd`. Опустим подробности получения, так как это для целей тестирования несущественно, опустим процесс нахождения нужной части кода, сразу перейдём к делу. Смотрите на [рисунк 104](#).

**Рисунок 104.**

```
[redacted xinetd]$ sed -e '287,308p;d' xinetd-2.3.15/xinetd/access.c
/* CPS handler */
if( SC_TIME_CONN_MAX(scp) != 0 ) {
    int time_diff;
    nowtime = time(NULL);
    time_diff = nowtime - SC_TIME_LIMIT(scp) ;

    if( SC_TIME_CONN(scp) == 0 ) {
        SC_TIME_CONN(scp)++;
        SC_TIME_LIMIT(scp) = nowtime;
    } else if( time_diff < SC_TIME_CONN_MAX(scp) ) {
        SC_TIME_CONN(scp)++;
        if( time_diff == 0 ) time_diff = 1;
        if( SC_TIME_CONN(scp)/time_diff > SC_TIME_CONN_MAX(scp) ) {
            cps_service_stop(sp, "excessive incoming connections");
            return(AC_CPS);
        }
    } else {
        SC_TIME_LIMIT(scp) = nowtime;
        SC_TIME_CONN(scp) = 1;
    }
}
}
```

Вот и причина ошибки. Первый недочёт в коде `xinetd` — использование для расчёта периода времени целых чисел с точностью до одной секунды (зелёная метка). Второй недочёт — неверное использование единиц измерения. Время в секундах сравнивается с максимальной пакетной скоростью, которая измеряется в обратной величине к секундам (1/секунда, фиолетовая метка). Проверяем гипотезу, как и положено в науке. Создаём с помощью подручных средств файл проверяющей программы прямо в shell на СУ.

```
$ cat <<EOFEOF >>~/check-u7.pl
use strict ;
use warnings ;
my $start = $ARGV[0] || 10.01 ;
for (my $i = 0 ; $i<200 ; $i++) {
    my $current = $i*0.03466796875+$start ;
    my $diff = int($current)-int($start) ;
    my $rate = int(($i+1)/(($diff//0)||1)) ;
    print "N=".(($i+1))."\tT=".sprintf("%07.4f", $current)
        ."\tdiff=".$diff."\trate=".$rate."\n" ;
}
EOFEOF
```

Естественно, что в проверяющей программе мы прилежно повторяем поведение оригинала. Время (`$diff` и `time_diff`) рассчитываем в целых величинах, получаемую пакетную скорость (`$rate` и `SC_TIME_CONN/time_diff`) так же в целых. Интересующиеся могут самостоятельно прочесть нужный раздел в документации на язык Си, который используется для создания `xinetd`. Само же время мы делаем, естественно, почти как в ОС — в секундах с плавающей точкой (самостоятельно приведите `timespec` к этой форме).

Для контроля вы можете видеть исходный текст проверяющей программы на [рисунке 105](#).

**Рисунок 105.**

```
[cae@alt10-iqmm ~]$ cat check-u7.pl
use strict ;
use warnings ;
my $start = $ARGV[0] || 10.01 ;
for (my $i = 0 ; $i<200 ; $i++) {
    my $current = $i*0.03466796875+$start ;
    my $diff = int($current)-int($start) ;
    my $rate = int(($i+1)/(($diff//0)||1)) ;
    print "N=".$(i+1)."\tT=".sprintf("%07.4f", $current)
        ."\tdiff=".$diff."\trate=".$rate."\n" ;
}
[cae@alt10-iqmm ~]$
```

Теперь сделаем несколько запусков

```
$ perl check-u7.pl 10.01
```

Результат в интересующий нас момент приведён на [рисунке 106](#).

**Рисунок 106.**

N=46	T=11.5701	diff=1	rate=46
N=47	T=11.6047	diff=1	rate=47
N=48	T=11.6394	diff=1	rate=48
N=49	T=11.6741	diff=1	rate=49
N=50	T=11.7087	diff=1	rate=50
N=51	T=11.7434	diff=1	rate=51
N=52	T=11.7781	diff=1	rate=52
N=53	T=11.8127	diff=1	rate=53
N=54	T=11.8474	diff=1	rate=54
N=55	T=11.8821	diff=1	rate=55
N=56	T=11.9167	diff=1	rate=56
N=57	T=11.9514	diff=1	rate=57
N=58	T=11.9861	diff=1	rate=58
N=59	T=12.0207	diff=2	rate=29

Пробуем иное начало сессии

```
$ perl check-u7.pl 10.21
```

Итоги (опять только в нужное время) приведены на [рисунке 107](#).

**Рисунок 107.**

N=34	T=11.3540	diff=1	rate=34
N=35	T=11.3887	diff=1	rate=35
N=36	T=11.4234	diff=1	rate=36
N=37	T=11.4580	diff=1	rate=37
N=38	T=11.4927	diff=1	rate=38
N=39	T=11.5274	diff=1	rate=39
N=40	T=11.5621	diff=1	rate=40
N=41	T=11.5967	diff=1	rate=41
N=42	T=11.6314	diff=1	rate=42
N=43	T=11.6661	diff=1	rate=43
N=44	T=11.7007	diff=1	rate=44
N=45	T=11.7354	diff=1	rate=45
N=46	T=11.7701	diff=1	rate=46
N=47	T=11.8047	diff=1	rate=47
N=48	T=11.8394	diff=1	rate=48
N=49	T=11.8741	diff=1	rate=49
N=50	T=11.9087	diff=1	rate=50
N=51	T=11.9434	diff=1	rate=51
N=52	T=11.9781	diff=1	rate=52
N=53	T=12.0127	diff=2	rate=26
N=54	T=12.0474	diff=2	rate=27

Сдвигаем ещё

\$ perl check-u7.pl 10.33

Видим улучшение на [рисунке 108](#).

**Рисунок 108.**

N=42	T=11.7514	diff=1	rate=42
N=43	T=11.7861	diff=1	rate=43
N=44	T=11.8207	diff=1	rate=44
N=45	T=11.8554	diff=1	rate=45
N=46	T=11.8901	diff=1	rate=46
N=47	T=11.9247	diff=1	rate=47
N=48	T=11.9594	diff=1	rate=48
N=49	T=11.9941	diff=1	rate=49
N=50	T=12.0287	diff=2	rate=25
N=51	T=12.0634	diff=2	rate=25
N=52	T=12.0981	diff=2	rate=26
N=53	T=12.1327	diff=2	rate=26
N=54	T=12.1674	diff=2	rate=27
N=55	T=12.2021	diff=2	rate=27

Смотрим приблизительную середину интервала

```
$ perl check-u7.pl 10.25
```

Итоги на [рисунке 109](#).

**Рисунок 109.**

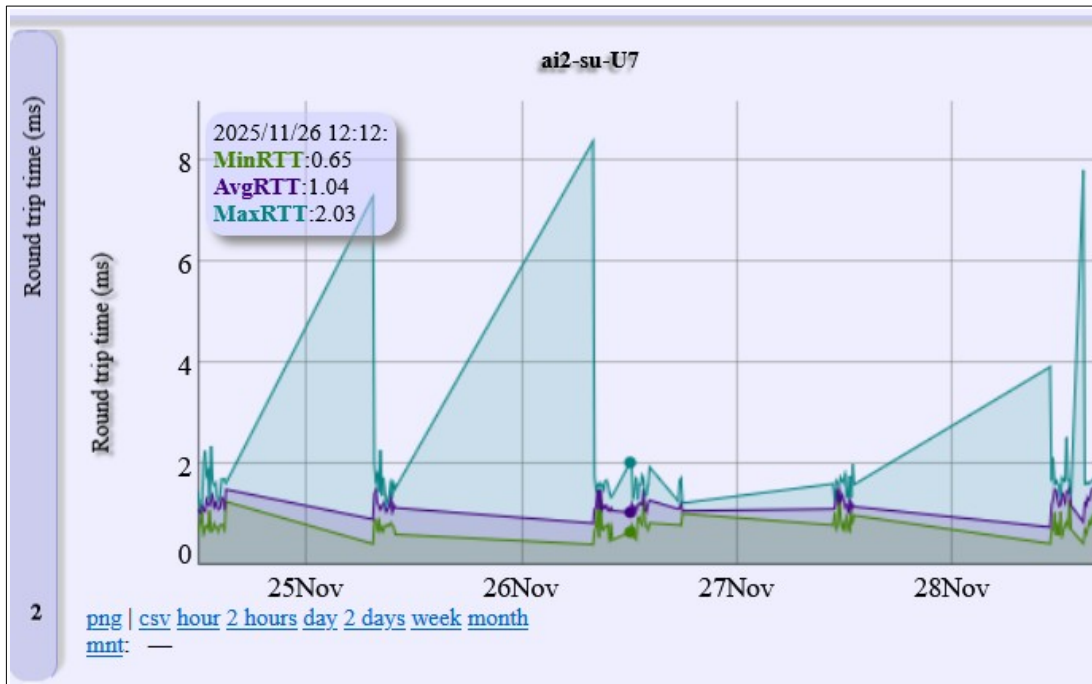
N=40	T=11.6021	diff=1	rate=40
N=41	T=11.6367	diff=1	rate=41
N=42	T=11.6714	diff=1	rate=42
N=43	T=11.7061	diff=1	rate=43
N=44	T=11.7407	diff=1	rate=44
N=45	T=11.7754	diff=1	rate=45
N=46	T=11.8101	diff=1	rate=46
N=47	T=11.8447	diff=1	rate=47
N=48	T=11.8794	diff=1	rate=48
N=49	T=11.9141	diff=1	rate=49
N=50	T=11.9487	diff=1	rate=50
N=51	T=11.9834	diff=1	rate=51
N=52	T=12.0181	diff=2	rate=26
N=53	T=12.0527	diff=2	rate=26
N=54	T=12.0874	diff=2	rate=27

Теперь ясно, кто виноват — авторы `xinetd`, которые несколько поспешно реализовали отслеживание слишком большого числа обращений к суперсерверу. В результате, даже если мы создаём трафик частотой всего лишь 28-29 пакетов в секунду, в середине второй секунды приёма приблизительно в одном случае из четырёх (1/0.25, доказательство очевидно) `xinetd` ошибочно считает, что получает слишком много пакетов, и пора 10 секунд отдохнуть. Наша сессия длится 6.93359375 секунд (докажите самостоятельно), то есть после отсылки 51 пакета ответа не будет до конца, что и фиксируется IQMA агентом как 75% потерь (докажите самостоятельно).

Как видите, проблема проверки качества связи на сетях TCP/IP не так проста на первый взгляд, как кажется. А пресловутую максиму «в открытом ПО все ошибки легко находятся» тоже следует подвергнуть сомнению.

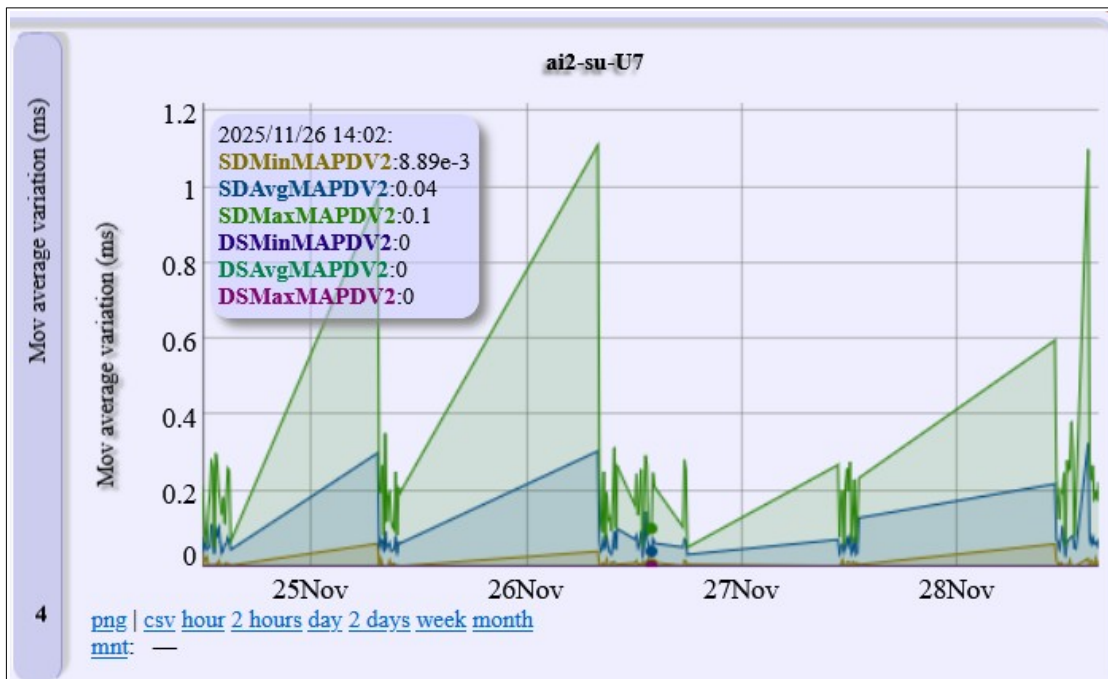
Долго в тесте U7 разбирались с потерями, но разобрались. Переходим к круговой задержке. Смотрим [рисунок 110](#).

Рисунок 110.



Видим, что ничего необычного нет, средняя около 1 миллисекунды. Смотрим «дрожание» на [рисунке 111](#).

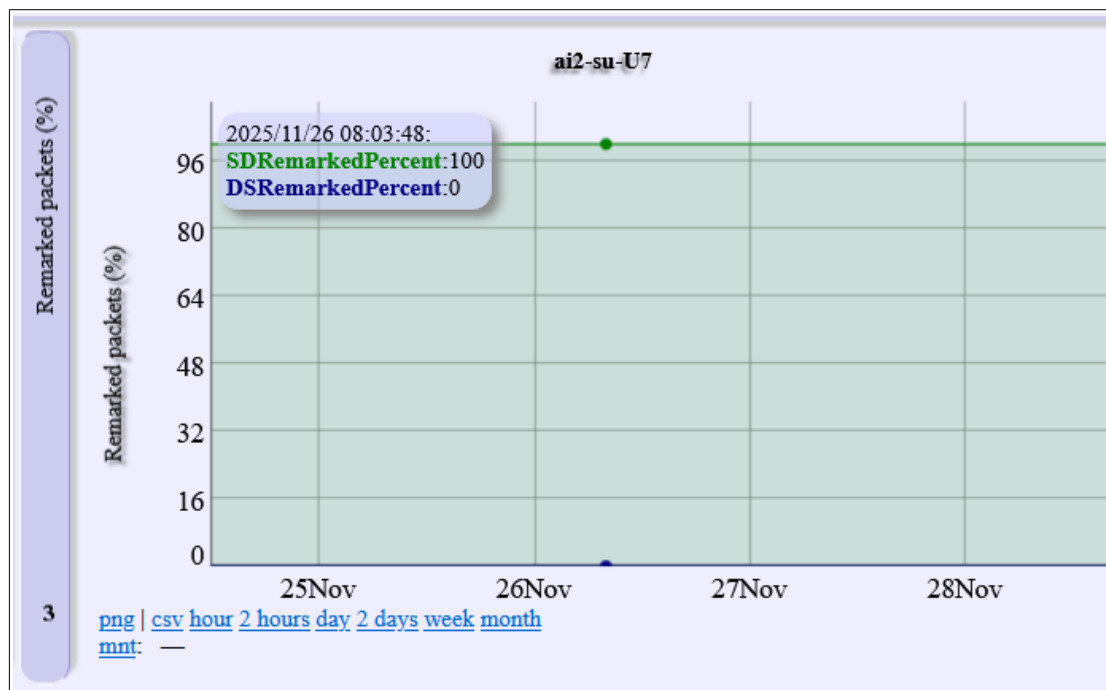
Рисунок 111.



Тоже ничего необычного. Кроме того, что второе направление нулевое! Но ведь так и должно быть. Протокол-то не интеллектуальный, и алгоритм G.1020 может быть применён только к круговому «дрожанию». Для простоты оно выдаётся по направлению «от инициатора к получателю», а обратная ставится принудительно в ноль.

Смотрим перекраску трафика на [рисунке 112](#).

**Рисунок 112.**



А тут-то почему произошла перекраска? Ведь протокол типа «эхо». То есть, что пришло, то и ушло! И сеть в один коммутатор! Верно, но лишь частично. Смотрим вновь в исходный текст `xinetd` на [рисунке 113](#).

**Рисунок 113.**

```
[redacted xinetd]$ sed -e '166,183p;d' xinetd-2.3.15/xinetd/builtins.c
static void dgram_echo( const struct server *serp )
{
    char          buf[ DATAGRAM_SIZE ] ;
    union xsockaddr lsin;
    ssize_t       cc ;
    socklen_t     sin_len = 0;
    int           descriptor = SERVER_FD( serp ) ;

    if( SC_IPV4( SVC_CONF( SERVER_SERVICE( serp ) ) ) )
        sin_len = sizeof( struct sockaddr_in );
    else if( SC_IPV6( SVC_CONF( SERVER_SERVICE( serp ) ) ) )
        sin_len = sizeof( struct sockaddr_in6 );

    cc = recvfrom( descriptor, buf, sizeof( buf ), 0, (struct sockaddr *)(&lsin
), &sin_len ) ;
    if ( cc != (ssize_t)-1 ) {
        (void) sendto( descriptor, buf, (size_t)cc, 0, SA( &lsin ), sizeof( lsin )
) ;
    }
}

```

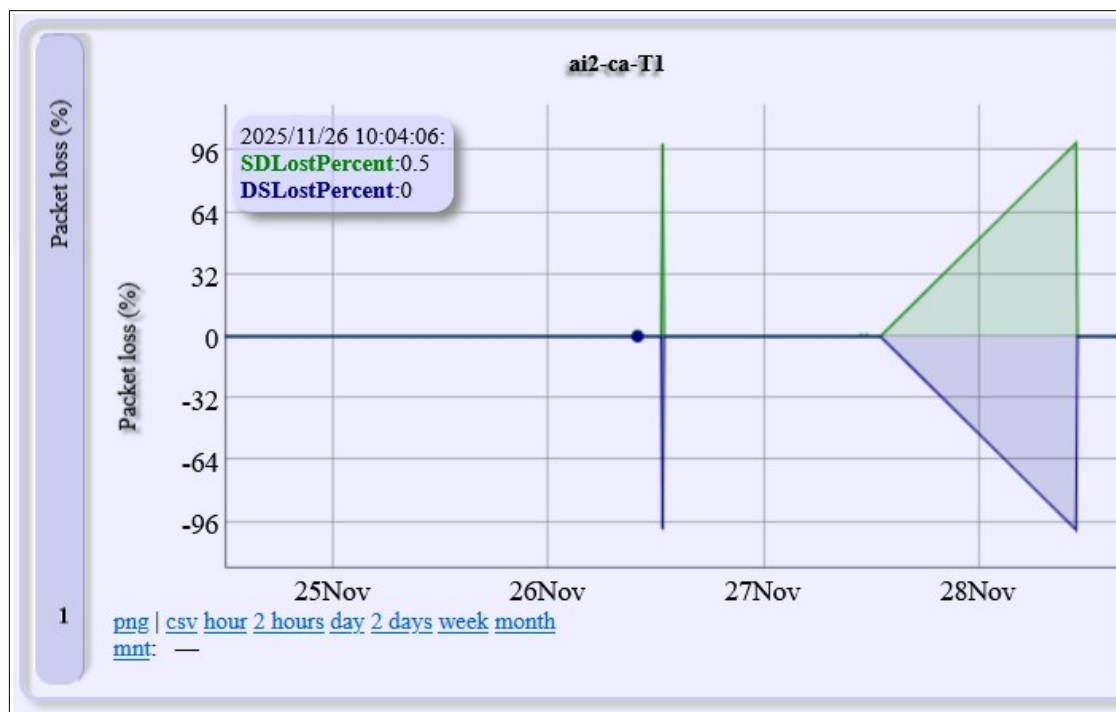
Реализация проста. Принять пакет через `recvfrom(2)` и выслать обратно через `sendto(2)`. НО! Если вы прочтёте документацию по данным вызовам системной библиотеки, то узнаете, что они не отвечают за поле TOS/DSCP в IP-пакете. Для чтения и

записи данного поля следует предпринимать дополнительные действия. Подробное объяснение методов правильного приёма трафика с учётом класса сервиса выходит за рамки настоящей документации. Таким образом, даже если пакет с классом сервиса ВС пришёл на `xinetd`, то ушёл обратно пакет, не помеченный нужным образом, то есть для правильного «эхо» следует либо исправить реализацию, либо сделать свою. Иначе перекраска трафика не будет учитываться верно.

Как легко видеть по данному разбору, даже простой эхо-протокол (правда, с хорошей реализацией) может дать информацию о сети, находящейся между агентом-инициатором и сопряжённым, пусть и не полную.

Более же полную можно увидеть в тесте `ai2-ca-T1`. То есть в реализации TWAMP. Это более-менее полноценный протокол тестирования сетей, не без недостатков, однако имеющийся в реализации у сторонних производителей. Что позволяет использовать IQMA в связке с уже имеющимся оборудованием. Смотрим потери на [рисунке 114](#).

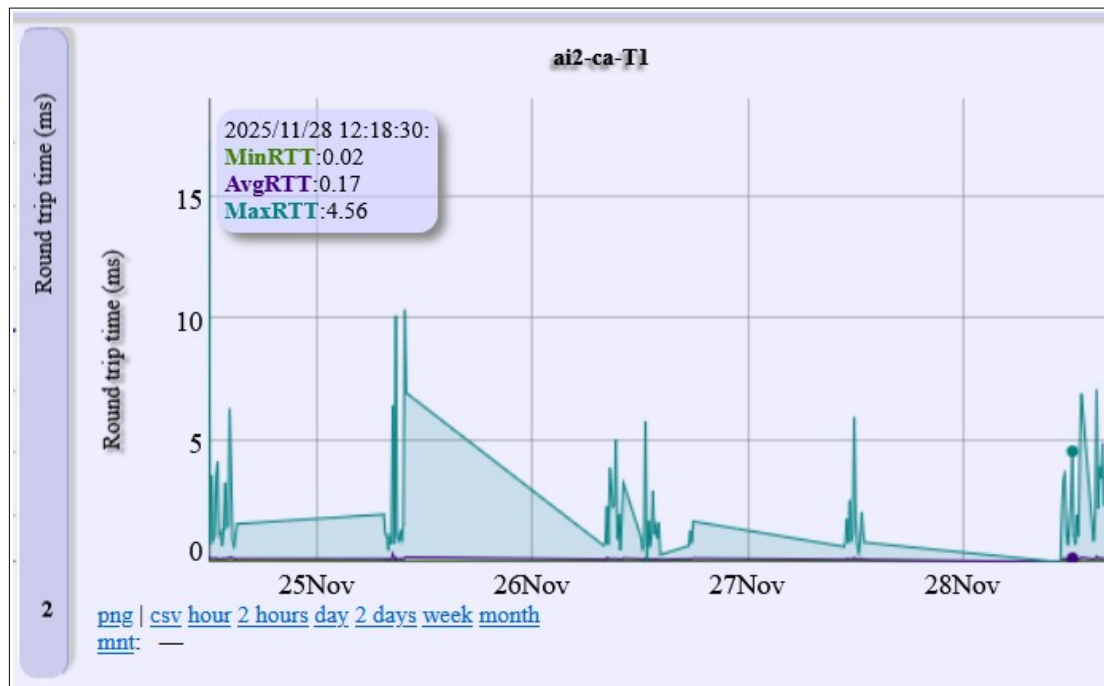
**Рисунок 114.**



Как и в случае теста 26 ноября 2025 года в 10:04 фиксировались 0.5 потерь в сторону агента СА, а чуть позже все попытки установить связь между агентом АИ2 и СА по TWAMP были безуспешными (100% потеря). То есть налицо фиксация проблем на сети в это время двумя разными агентами и двумя разными тестами. Проблема явно в самой сети! Хотя на данном графике из-за автомасштабирования не видны мелкие потери, тем не менее, поверьте, в остальные моменты их не было. Ну а про артефакты графиков, связанные с регулярным выключением лаборатории, мы уже писали.

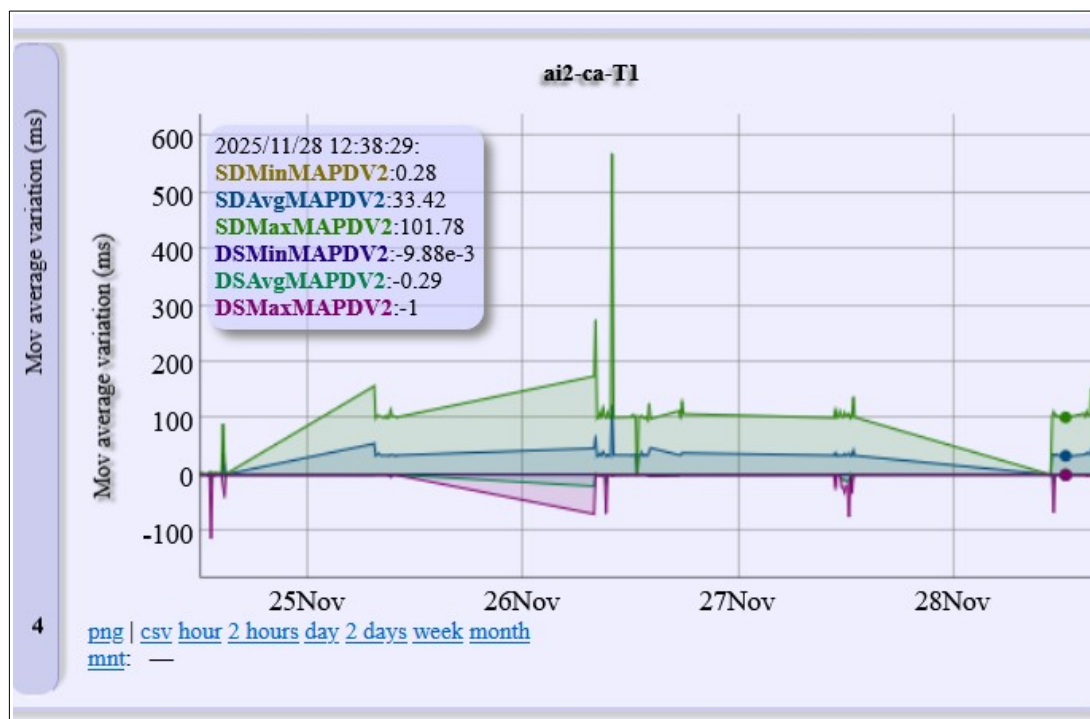
Переходим к круговой задержке. Это [рисунке 115](#).

Рисунок 115.



Здесь ничего неожиданного, и среднее и максимальное — вполне допустимые. Смотрим «дрожание» на [рисунке 116](#).

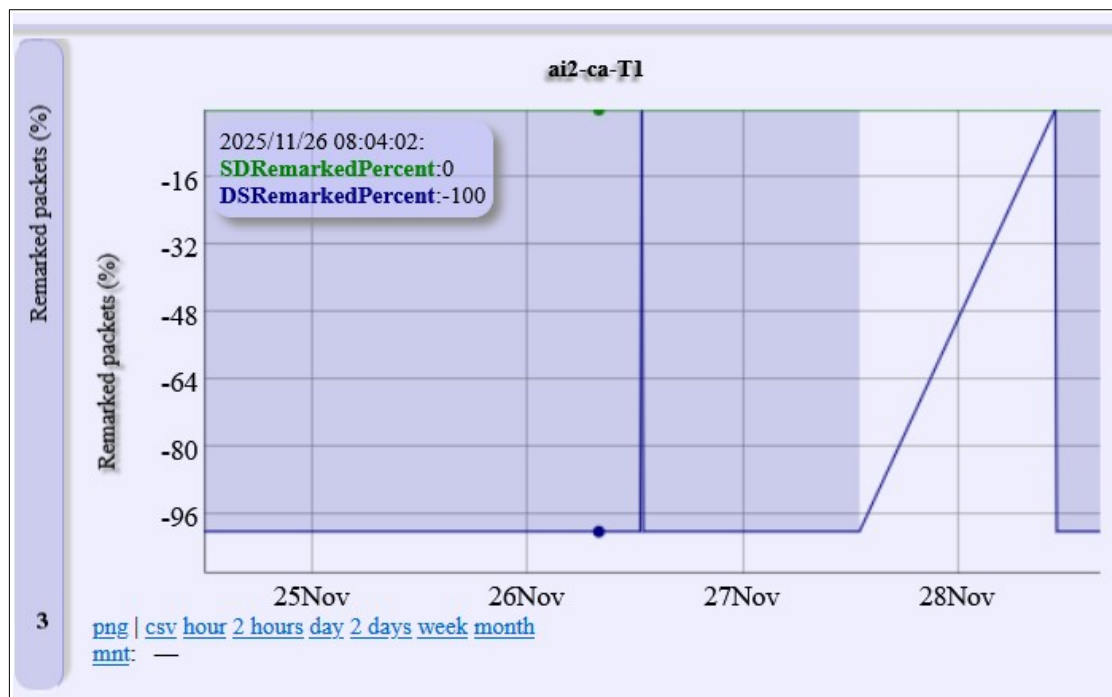
Рисунок 116.



Тут как раз есть неясности. От сопряжённого к инициатор (DS) всё более-менее нормально. А вот направление от инициатор к сопряжённому (SD) требует дальнейшего исследования. В рамках тестирования мы его по понятным причинам не проводим.

Теперь смотрим перекраску трафика на [рисунке 117](#).

**Рисунок 117.**

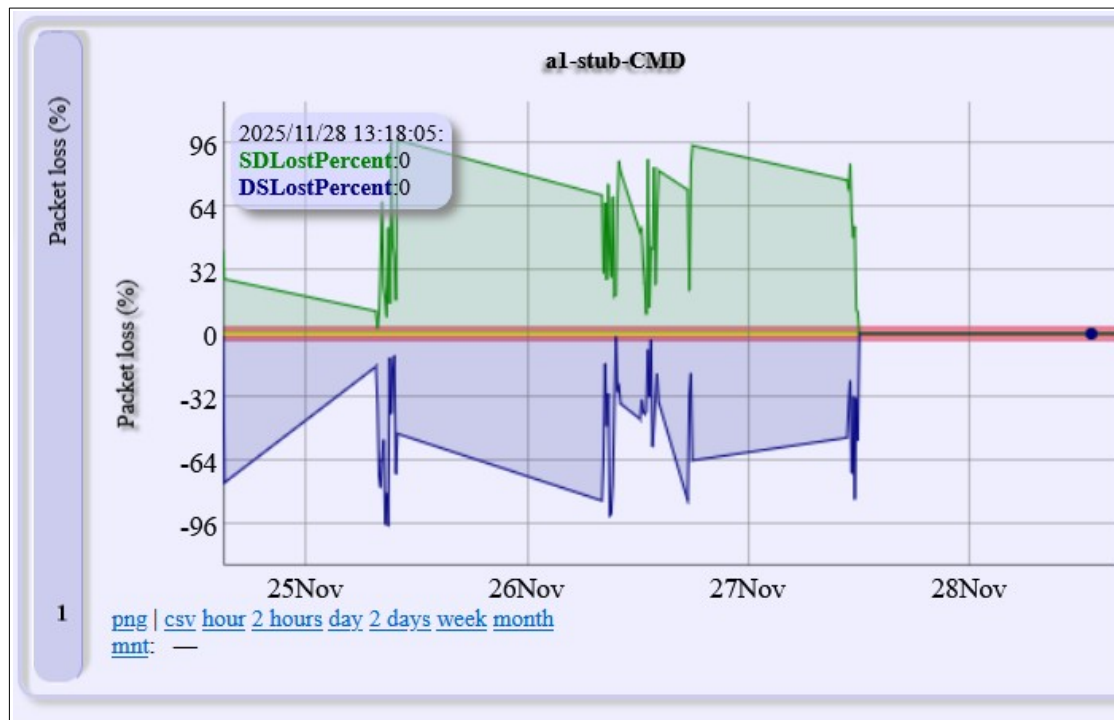


Тут что-то непонятное. Собственно, TWAMP в сторону SD и не поддерживает расчёт перекраски трафика. А вот со стороны DS следует разобраться. Так как альтернативный протокол U9 не фиксировал перекраску в эту сторону. Дальнейшее исследование данного вопроса, впрочем, так же выходит за тестирование.

Теперь коротко рассмотрим тест `a1-stub-CMD`. Этот тест, как результат исполнения программы на агенте-инициаторе, просто показывает возможность расширения IQM для поддержки тех протоколов, которые ещё не содержатся в самом агенте. В данном случае мы записываем случайные значения от 0 до 100. Поэтому график на [рисунке 118](#) очень своеобразный — помимо артефактов выключения лаборатории постоянные скачки туда-сюда. Всерьёз такую программу как итоги тестирования рассматривать, конечно нельзя.

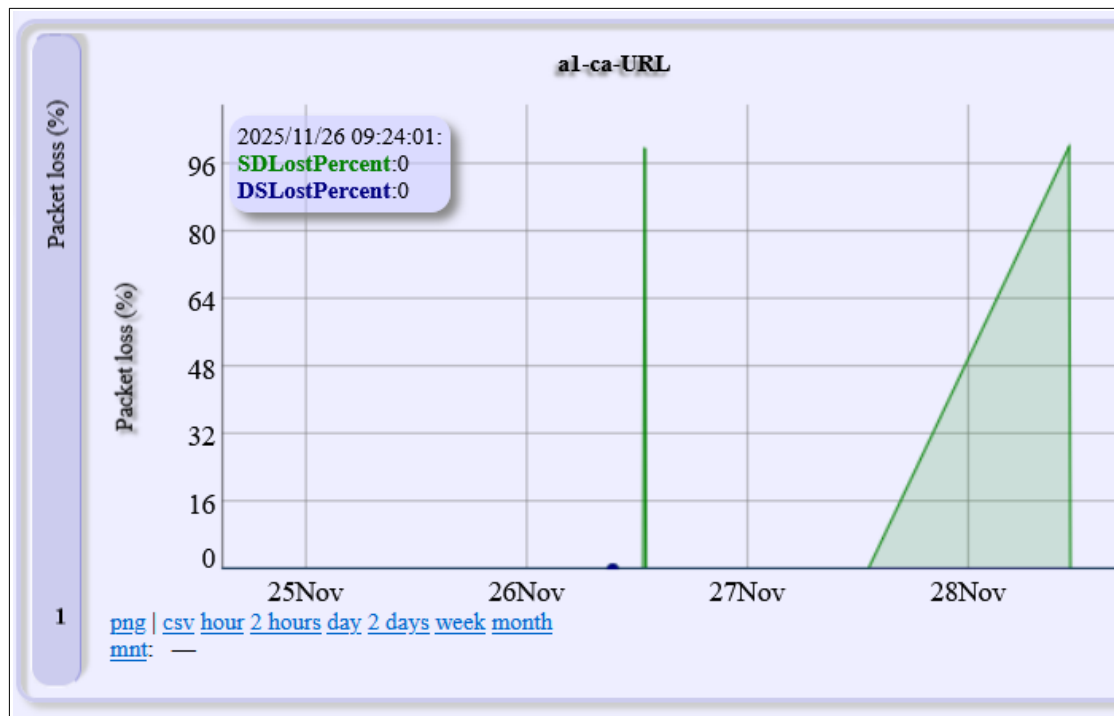
А вот внезапное обнуление результатов в конце графика объяснить можно. Это последствия того, что мы сделали в следующей главе.

**Рисунок 118.**



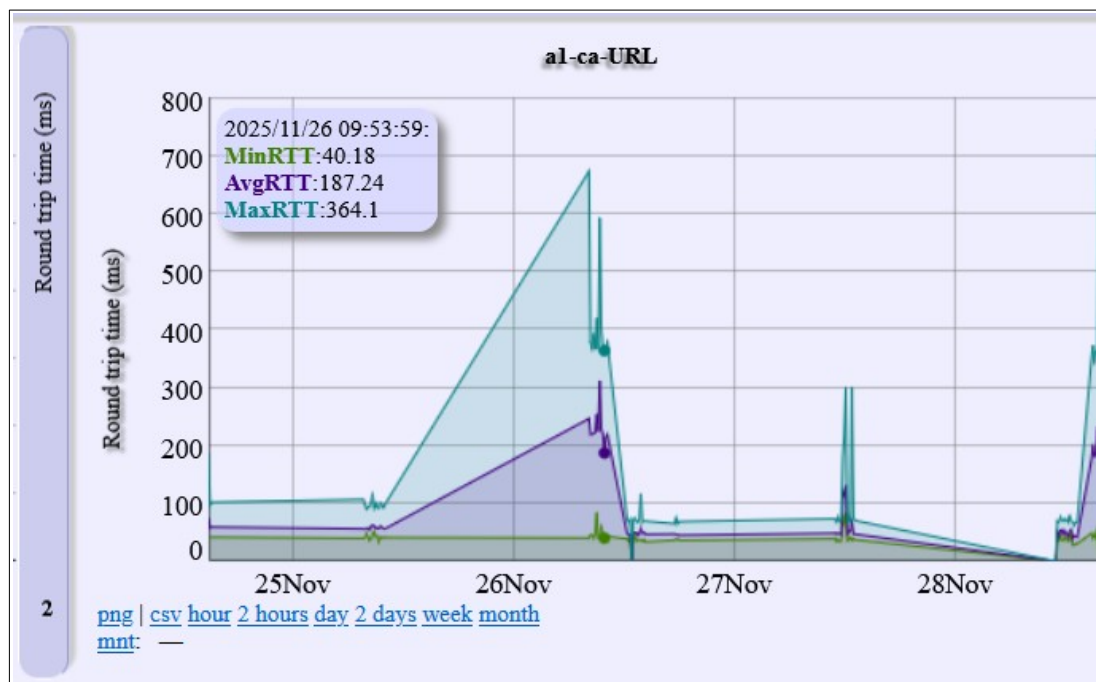
Теперь переходим к тестам уровня приложения. Начнём с `al-ca-URL`. Вначале доля незавершённых запросов за всю сессию. Она показана на рисунке 119.

**Рисунок 119.**



За исключением двух случаев проблем доставки `http`-протокола нет. Смотрим дальше на время обработки одного запроса за всю сессию. Это рисунке 120.

Рисунок 120.



Следует отметить, что в это время (даже среднее) включено всё, от начала запроса до окончания. Очевидно, что каждый запрос http может работать непредсказуемое время на сервере. Поэтому всерьёз, для использования как параметра транспортной сети, этот параметр использовать нельзя. Однако для статистики может быть интересно.

Тест a2-ca-URLUP практически ничем от предыдущего не отличается. Основной объём трафика поступает на сервер — в этом вся разница. Доля незавершённых сессий на [рисунке 121](#). А время обработки одного запроса на [рисунке 122](#). Оно в среднем больше, чем у URL-теста, так как сервер запускает программу приёма.

Рисунок 121.

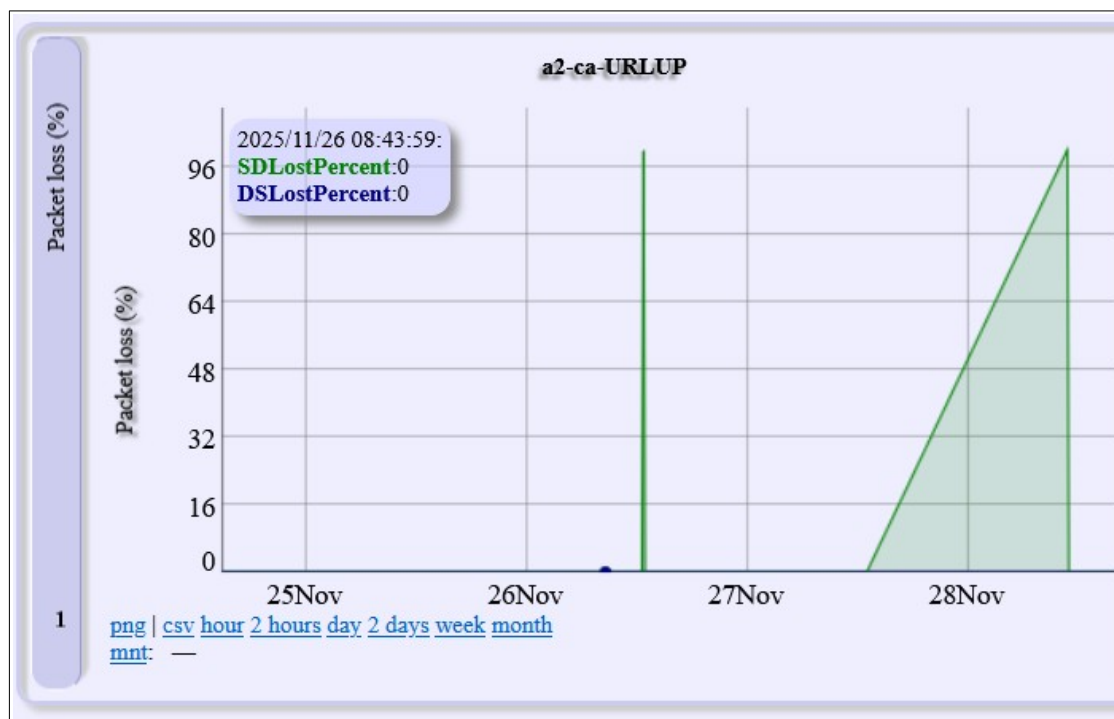
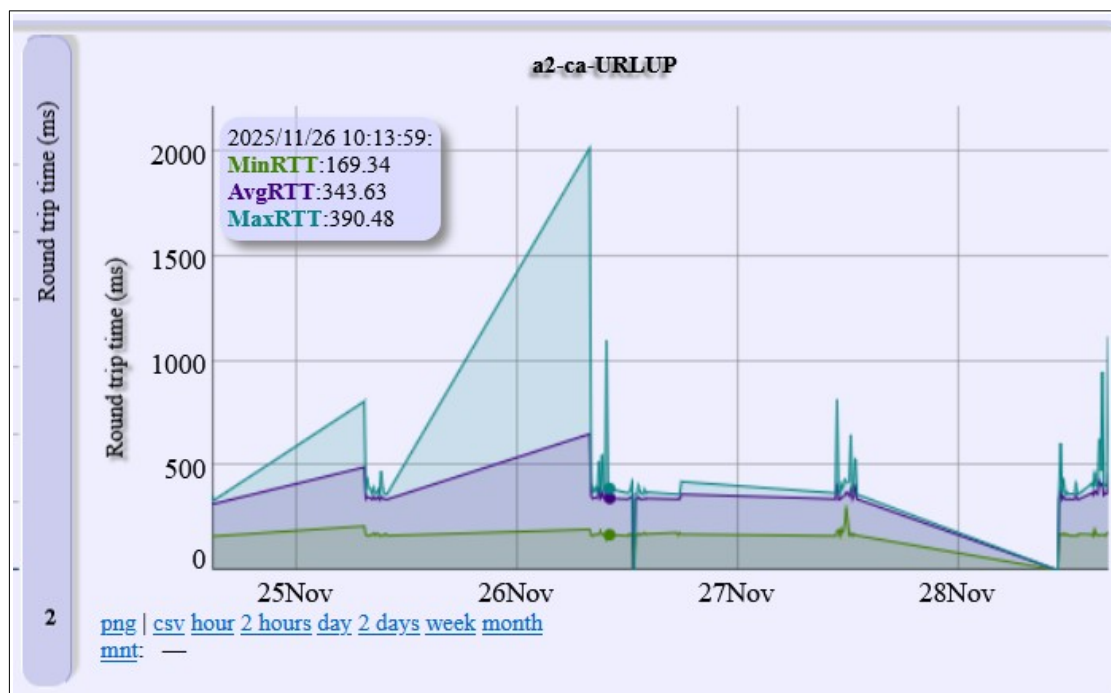


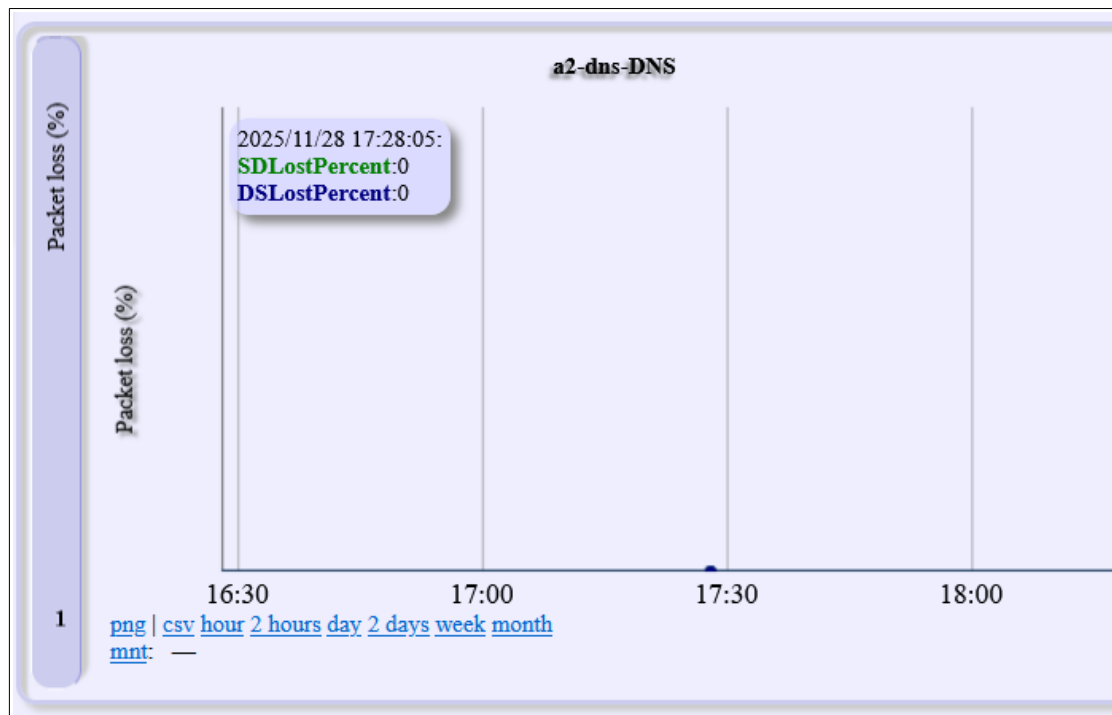
Рисунок 122.



Теперь о тесте a2-dns-DNS. Он в первую очередь предназначен для проверки доступности сервера имён оператора связи, а во вторую — для нагрузочного тестирования собственных серверов. В первом случае не рекомендуется выставлять больше 5-10 пакетов, а во втором — побольше, до 1000. Скорость же генерации трафика позволяет создавать нагрузку. Поскольку мы рекомендуем для тестирования проверять сервер оператора, то скорость следует оставить по умолчанию — 64 килобита в секунду.

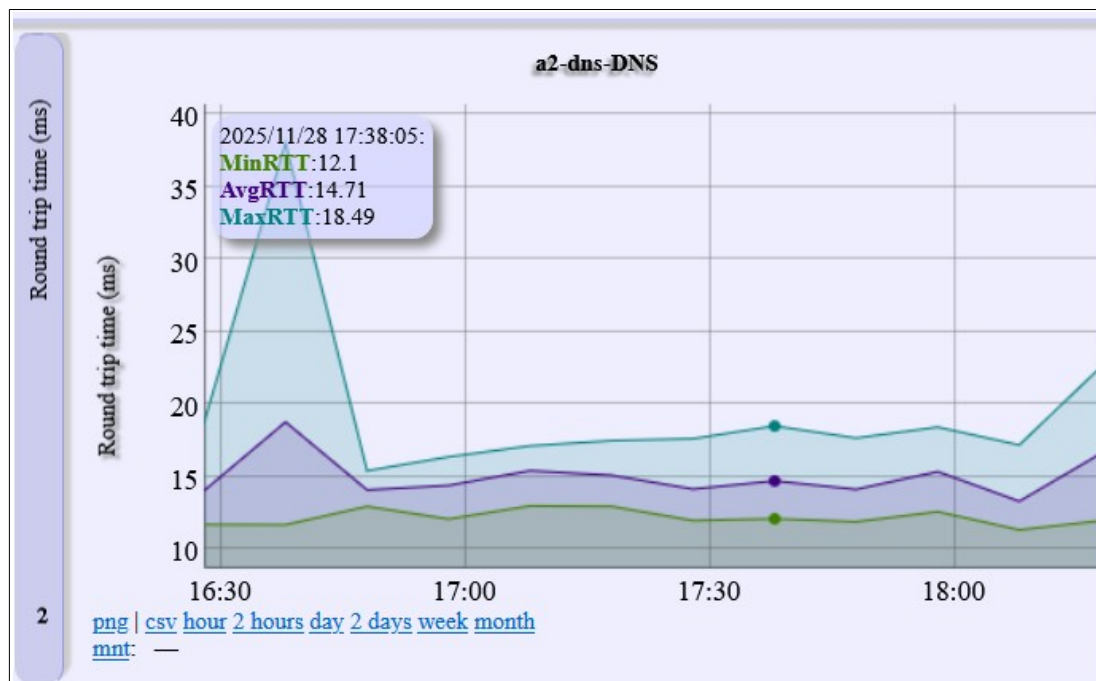
Результаты видны на [рисунке 123](#) (потери пакетов), [рисунке 124](#) (круговая задержка), [рисунке 125](#) (пакеты, прибывшие вне порядка).

**Рисунок 123.**



Потерь нет, так и должно быть. Это правильно.

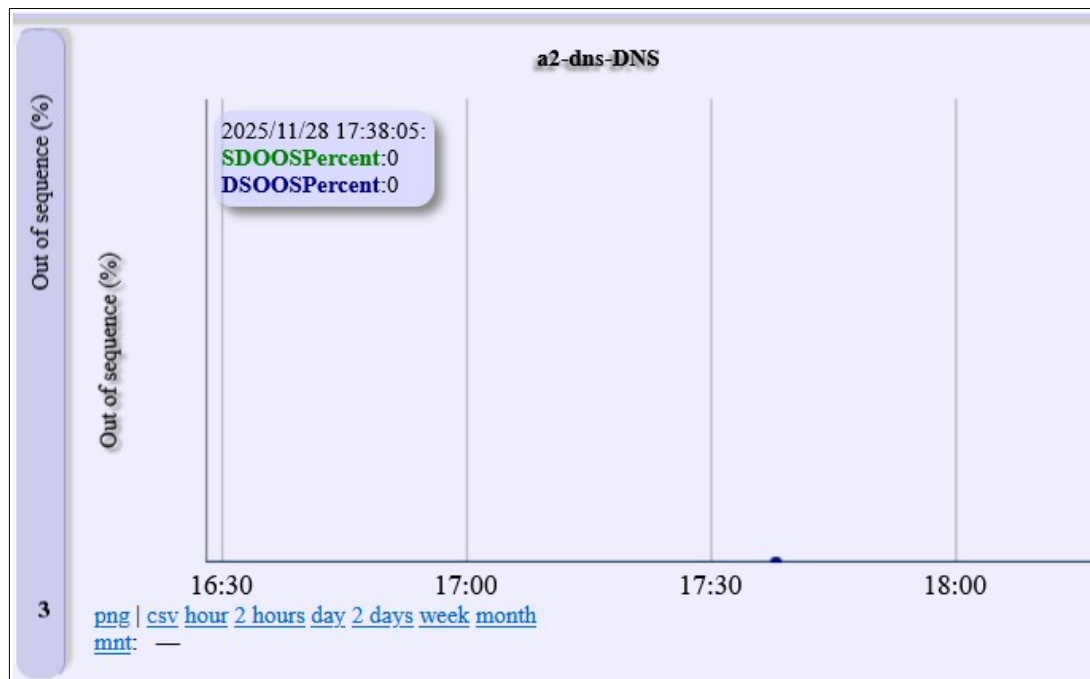
**Рисунок 124.**



Какие должны быть верные параметры круговой задержки, никто из профильных организаций до сих пор не регламентировал. Поэтому следует полагать простую истину —

чем меньше, тем лучше, а если больше 1000 миллисекунд (1 секунда на обработка одного запроса) — это недопустимо.

**Рисунок 125.**



Зачем отслеживать этот параметр? В самом протоколе DNS не имеет значения, в правильном ли порядке обработаны запросы. Но обычно, если сам сервер испытывает нагрузку, то первым признаком будет повышение количества ответов, вернувшихся на агент-инициатор не в том порядке, в котором они отосланы. Поэтому для нагрузочного тестирования следует оценивать как параметр, так и загрузку сервера. Для запросов в публичные сервера имён на этот параметр не стоит обращать внимания, так как исправить что-либо вы всё равно не сможете.

По итогам главы мы отметим, что в вашем тестировании скорее всего будет всё иначе, так как и сеть будет другая и устройства тоже иные. Возможно, нам и не следовало так подробно описывать графики, но мы полагаем, что пусть лучше у вас будет больше знаний для объяснения, чем меньше.

## 22 Просмотр табло алармов и реакций

Поскольку в [главе 20](#) мы настроили политики контроля и уже прошло некоторое время, посвящённое другим этапам тестирования, можно проверить результаты обработки по порогам и отсылки тревожных сообщений. Часть рисунков будет отображаться с помощью SSH, их вы узнаете по белому фону, часть — через web-интерфейс, их вы узнаете по светло-сиреневой палитре. Как между ними переключаться, вы уже знаете.

Когда сообщений о проблемах нет, то в syslog на системе управления под разделом (facility) local6 не видно ничего (естественно, в нашей лаборатории, так как штатно local6 никто не запрещает использовать какому-либо иному процессу). Проверка делается командой

```
$ journalctl -S today --facility local6 --no-pager
```

Пример виден на [рисунке 126](#).

#### Рисунок 126.

```
[cae@alt10-iqmm ~]$ journalctl -S today --facility local6 --no-pager
-- No entries --
```

Равно как и демон snmptrapd тоже не сохраняет в файле своего журнала (настроенного при установке СУ, см. руководство «Запуск IQM на ОС Альт 10») ничего, кроме записи о собственном запуске. В чём можно убедиться командой

```
$ tail /var/log/trapd.log
```

Пример виден на [рисунке 127](#).

#### Рисунок 127.

```
[cae@alt10-iqmm ~]$ tail /var/log/trapd.log
NET-SNMP version 5.8
```

Когда же сообщения о превышении порогов потерь в любую из двух сторон прохождения трафика по тесту al-stub-CMD поступают, то в журнале syslog видны сообщения, приведенные на [рисунке 128](#).

#### Рисунок 128.

```
[cae@alt10-iqmm ~]$ journalctl -S today --facility local6 --no-pager
ноя 27 10:54:03 alt10-iqmm iqm-manager[3079]: check_horizon=60;class_name=BE;policy_name=policy-test;severity=CRIMSON;status=UP;test_name=al-stub-CMD;threshold=3;time_end=2025-11-27 10:53:45.000000;time_start=2025-11-27 10:53:45.000000;value_field=SDLostPercent;value_table=dtraw;violations_count=1
ноя 27 10:54:03 alt10-iqmm iqm-manager[3080]: check_horizon=60;class_name=BE;policy_name=policy-test;severity=CRIMSON;status=UP;test_name=al-stub-CMD;threshold=3;time_end=2025-11-27 10:53:45.000000;time_start=2025-11-27 10:53:45.000000;value_field=DSLostPercent;value_table=dtraw;violations_count=1
```

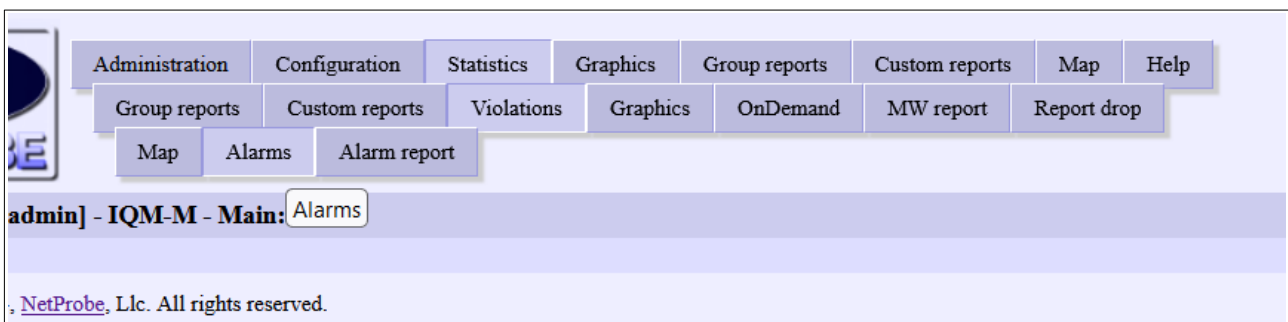
В это же время у демона snmptrapd в журнале видно то, что представлено на [рисунке 129](#).

**Рисунок 129.**

```
[cae@alt10-iqmm ~]$ tail /var/log/trapd.log
NET-SNMP version 5.8
2025-11-27 10:54:03 localhost.localdomain [UDP: [127.0.0.1]:44090->[127.0.0.1]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (97515) 0:16:15.15      SNMPv2-MIB::snmpTrapOID.0 = OID: NP-IQM3-NOTIFICATION-MIB::StartTrap      NP-IQM3-NOTIFICATION-MIB::Status.0 = STRING: UP NP-IQM3-NOTIFICATION-MIB::Horizon.0 = INTEGER: 60
NP-IQM3-NOTIFICATION-MIB::Count.0 = INTEGER: 1 NP-IQM3-NOTIFICATION-MIB::Param.0 = STRING: SDRestPercent      NP-IQM3-NOTIFICATION-MIB::Threshold.0 = STRING: 3      NP-IQM3-NOTIFICATION-MIB::TimeStart.0 = STRING: 2025-11-27 10:53:45.000000      NP-IQM3-NOTIFICATION-MIB::Test.0 = STRING: al-stub-CMD      NP-IQM3-NOTIFICATION-MIB::Severity.0 = STRING: CRIMSON      NP-IQM3-NOTIFICATION-MIB::Class.0 = STRING: BE      NP-IQM3-NOTIFICATION-MIB::Table.0 = STRING: draw      NP-IQM3-NOTIFICATION-MIB::TimeEnd.0 = STRING: 2025-11-27 10:53:45.000000      NP-IQM3-NOTIFICATION-MIB::Policy.0 = STRING: policy-test      NP-IQM3-NOTIFICATION-MIB::URL.0 = STRING: empty
2025-11-27 10:54:03 localhost.localdomain [UDP: [127.0.0.1]:40510->[127.0.0.1]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (97516) 0:16:15.16      SNMPv2-MIB::snmpTrapOID.0 = OID: NP-IQM3-NOTIFICATION-MIB::StartTrap      NP-IQM3-NOTIFICATION-MIB::Status.0 = STRING: UP NP-IQM3-NOTIFICATION-MIB::Count.0 = INTEGER: 1 NP-IQM3-NOTIFICATION-MIB::Horizon.0 = INTEGER: 60      NP-IQM3-NOTIFICATION-MIB::Param.0 = STRING: SDRestPercent      NP-IQM3-NOTIFICATION-MIB::Threshold.0 = STRING: 3      NP-IQM3-NOTIFICATION-MIB::TimeStart.0 = STRING: 2025-11-27 10:53:45.000000      NP-IQM3-NOTIFICATION-MIB::Test.0 = STRING: al-stub-CMD      NP-IQM3-NOTIFICATION-MIB::Severity.0 = STRING: CRIMSON      NP-IQM3-NOTIFICATION-MIB::Class.0 = STRING: BE      NP-IQM3-NOTIFICATION-MIB::Table.0 = STRING: draw      NP-IQM3-NOTIFICATION-MIB::TimeEnd.0 = STRING: 2025-11-27 10:53:45.000000      NP-IQM3-NOTIFICATION-MIB::Policy.0 = STRING: policy-test      NP-IQM3-NOTIFICATION-MIB::URL.0 = STRING: empty
[cae@alt10-iqmm ~]$
```

Разумеется, в качестве приёмников syslog либо SNMP trap могут выступать и более сложные системы, наша задача на этапе тестирования, напомним, всего лишь убедиться в работоспособности IQM на новой ОС.

Перейдём в web-интерфейсе СУ. Выберем меню Statistics → Violations → Alarms, чтобы увидеть список проблемных событий. Меню видно на [рисунке 130](#).

**Рисунок 130.**

Нажимаем кнопку view и получаем внизу список текущих проблем. Результат виден на [рисунке 131](#).

Рисунок 131.

**IQMM - [logged as admin] - Alarms:**

Alarms

Customer ZUES RUES Provider Service Test tags SRC zone DST zone SRC agent DST agent Test ID a1-stub-CMD Test type Class Severity Status Table Period Conditions Actions

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19

view clear filter

Alarms									
Source agent	Test ID	Time event	Service	History	Status	Selected	Info	Input info	Delete
alt10-iqma1	a1-stub-CMD (View)(Run ondemand)(Config)	2025-11-27 10:53:45	L4 Internet	2 events (View)	UP	<input type="checkbox"/>	null	Press	<input type="checkbox"/>
Source agent	Test ID	Time event	Service	History	Status	Selected	Info	Input info	Delete

Copyright (C) 2008-2024 NetProbe LLC. All rights reserved.

Виден агент-инициатор, тест, по результатам которого зафиксирована проблема, время начала события и история. Выбираем ссылку View на History. Показывается история, которая показана на [рисунке 132](#). По нажатию X в правом верхнем углу, всплывающее окно закрывается.

Рисунок 132.

Alarm events														
Alarm time	Last alarm time	Duration	Policy	Horizon	Threshold	Count	Test	Table	Value	Class	Severity	Info	Info time	User
2025-11-27 10:53:45	2025-11-27 11:55:59	1:02:14 h	policy-test	60 min	3	1	a1-stub-CMD	dtraw	DSLostPercent	BE	CRIMSON			
2025-11-27 10:53:45	2025-11-27 11:55:59	1:02:14 h	policy-test	60 min	3	1	a1-stub-CMD	dtraw	SDLostPercent	BE	CRIMSON			

Видно, что проблему создали оба параметра. Ещё бы, ведь там `rand()` стоит и у того, и у другого! Попробуем «решить» проблему, тем более, что она у нас создана намеренно. Для этого заходим на агент `alt10-iqma1` по SSH, чтобы поправить `cmd-test.pl`. Это делается командой

```
$ sed -i -e 's&rand()&0.0&' cmd-test.pl
```

Вы, как это уже рассказывалось, можете воспользоваться альтернативным методом, если это удобнее. Задача простая — заменить генератор псевдослучайных чисел на ноль. Мы же предпочитаем «поточковый редактор» `sed`, как старое и проверенное решение. Убедиться, что всё сделано верно, можно командой

```
$ cat cmd-test.pl
```

Обе команды приведены на [рисунке 133](#).

**Рисунок 133.**

```
[cae@alt10-iqmal ~]$ sed -i -e 's&rand()&0.0&' cmd-test.pl
[cae@alt10-iqmal ~]$ cat cmd-test.pl
#!/usr/bin/perl

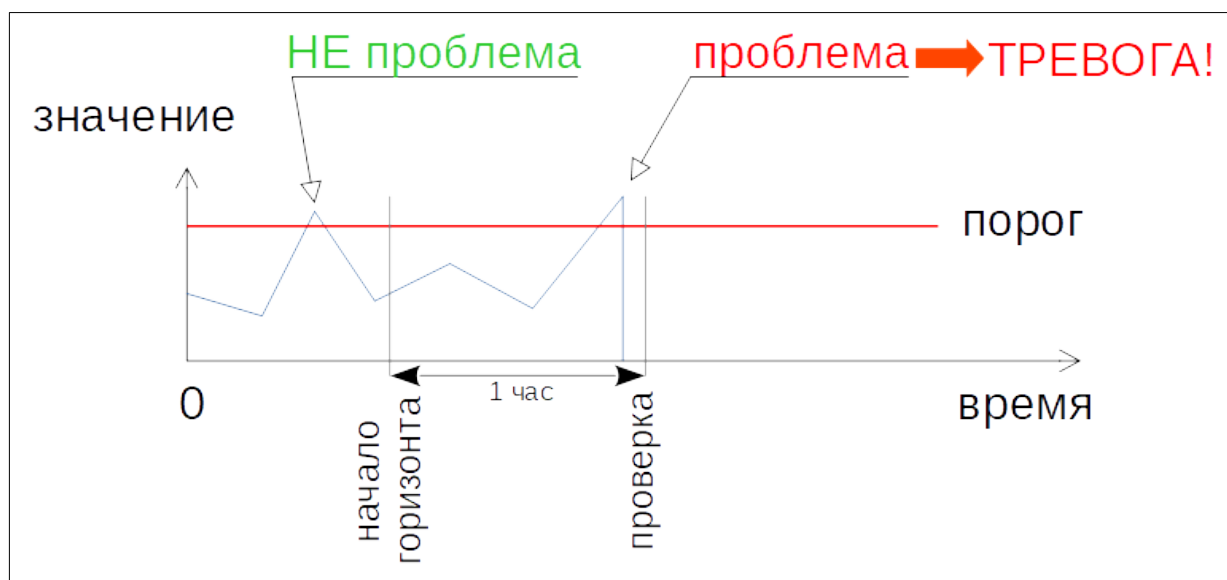
use strict ;
use warnings ;

print "SDLostPercent ",0.0*100.0
,"\nDSLostPercent ",0.0*100.0,"\n" ;
exit 0 ;
[cae@alt10-iqmal ~]$
```

После того, как вы сделали изменение кода, симулирующего проведение реального теста с выдачей формальных результатов, необходимо некоторое время провести, ожидая реакции системы. Дело в том, что логика политик проверки параметров на выход за пороги устроена следующим образом:

1. Если за горизонт событий (в нашем случае 60 минут) от времени проверки было 1 (одно) плохое событие, то создаём тревогу. Такую работу системы мы уже видели.
2. Для того, чтобы после факта создание тревоги, она могла очиститься, следует получить от агента за горизонт событий только корректные значения (0 плохих событий).

Более наглядно это можно изобразить так. На [рисунке 134](#) первое событие — получение от агента слишком большой метрики, проверка её по политике с горизонтом событий и порогом, затем создание тревоги.

**Рисунок 134.**

Далее, на [рисунке 135](#), развитие события — возврат метрики, полученной от того же агента, в нормальное положение, но проблема всё ещё существует, так как горизонт событий хоть и сдвинулся в будущее, пока содержит проблемную точку. Новая тревога не создаётся, так как она уже создана.

Рисунок 135.



А теперь, на [рисунке 136](#), после получения на всём горизонте событий корректных значений метрики от агента-инициатора, мы не только фиксируем, что проблемы завершились, но и можем с чистой совестью отослать очистку тревоги в нужные каналы.

Рисунок 136.



Таким образом, легко видеть, что мало выставить в программе `cmd-test.pl` нули для передачи в СУ! Следует ещё и дождаться периода, когда горизонт событий от времени проверки будет содержать только корректные значения. В табло тревог системы управления это будет выглядеть, как показано на [рисунке 137](#).

Рисунок 137.

The screenshot shows the IP Quality Monitor interface. At the top, there is a filter configuration panel with 19 vertical tabs labeled 1 through 19. Tabs 1-11 are: Customer, ZUES, RUES, Provider, Service, Test tags, SRC zone, DST zone, SRC agent, DST agent, Test ID. Tab 12 is a dropdown menu currently showing 'a1-stub-CMD'. Tabs 13-19 are: Test type, Class, Severity, Status, Table, Period, Conditions, Actions. To the right of the tabs are three buttons: 'view' (with a magnifying glass icon), 'clear' (with a document icon), and 'filter' (with a funnel icon). Below the filter panel is a table titled 'Alarms'.

Source agent	Test ID	Time event	Service	History	Status	Selected	Info	Input info	Delete
alt10-iqmal	a1-stub-CMD ( <a href="#">View</a> )( <a href="#">Run ondemand</a> )( <a href="#">Config</a> )	2025-11-27 10:53:45	L4 Internet	4 events ( <a href="#">View</a> )	UP	<input type="checkbox"/>	null	<input type="button" value="Press"/>	<input type="button" value="Delete"/>

А история развития проблемы (History → View) будет выглядеть, как показано на [рисунке 138](#).

Рисунок 138.

Alarm time	Last alarm time	Duration	Policy	Horizon	Threshold	Count	Test	Table	Value	Class	Severity	Info	Info time	User
2025-11-27 10:53:45	2025-11-27 12:58:14	2:04:29 h	policy-test	60 min	3	1	a1-stub-CMD	dtraw	DSLostPercent	BE	CRIMSON			
2025-11-27 10:53:45	2025-11-27 12:58:14	2:04:29 h	policy-test	60 min	3	1	a1-stub-CMD	dtraw	SDLostPercent	BE	CRIMSON			
2025-11-27 12:58:14	2025-11-27 12:59:14	0:01:00 h	policy-test	60 min	0	0	a1-stub-CMD	dtraw	DSLostPercent	BE	GREEN			
2025-11-27 12:58:14	2025-11-27 12:59:14	0:01:00 h	policy-test	60 min	0	0	a1-stub-CMD	dtraw	SDLostPercent	BE	GREEN			

Что же касается того, как были доставлены реакции на очистку тревоги, то проверка доставки в syslog делается командой

```
$ journalctl --facility local6 -r --no-pager|more
```

Пример виден на [рисунке 139](#).

**Рисунок 139.**

```
[cae@alt10-iqmm ~]$ journalctl --facility local6 -r --no-pager|more
ноя 27 12:59:27 alt10-iqmm iqm-manager[3808]: check_horizon=60;class_name=BE;pol
icy_name=policy-test;severity=GREEN;status=UP;test_name=al-stub-CMD;threshold=0;
time_end=2025-11-27 12:59:14.000000;time_start=2025-11-27 12:58:14.000000;valu
e_field=DSLostPercent;value_table=dtraw;violations_count=0
ноя 27 12:59:27 alt10-iqmm iqm-manager[3807]: check_horizon=60;class_name=BE;pol
icy_name=policy-test;severity=GREEN;status=UP;test_name=al-stub-CMD;threshold=0;
time_end=2025-11-27 12:59:14.000000;time_start=2025-11-27 12:58:14.000000;valu
e_field=SDLostPercent;value_table=dtraw;violations_count=0
ноя 27 12:54:26 alt10-iqmm iqm-manager[3780]: check_horizon=60;class_name=BE;pol
icy_name=policy-test;severity=CRIMSON;status=UP;test_name=al-stub-CMD;threshold=
3;time_end=2025-11-27 12:54:13.000000;time_start=2025-11-27 10:53:45.000000;valu
e_field=DSLostPercent;value_table=dtraw;violations_count=1
ноя 27 12:54:26 alt10-iqmm iqm-manager[3779]: check_horizon=60;class_name=BE;pol
icy_name=policy-test;severity=CRIMSON;status=UP;test_name=al-stub-CMD;threshold=
3;time_end=2025-11-27 12:54:13.000000;time_start=2025-11-27 10:53:45.000000;valu
e_field=SDLostPercent;value_table=dtraw;violations_count=1
ноя 27 11:54:05 alt10-iqmm iqm-manager[3420]: check_horizon=60;class_name=BE;pol
icy_name=policy-test;severity=CRIMSON;status=UP;test_name=al-stub-CMD;threshold=
3;time_end=2025-11-27 11:53:59.000000;time_start=2025-11-27 10:53:45.000000;valu
e_field=DSLostPercent;value_table=dtraw;violations_count=6
ноя 27 11:54:05 alt10-iqmm iqm-manager[3419]: check_horizon=60;class_name=BE;pol
[cae@alt10-iqmm ~]$
```

А по команде

```
$ tail /var/log/trapd.log
```

можно убедиться, что snmptrapd так же успешно принял очистку тревоги по двум параметрам. Пример виден на [рисунке 140](#).

**Рисунок 140.**

```

2025-11-27 12:59:27 localhost.localdomain [UDP: [127.0.0.1]:48017->[127.0.0.1]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (849848) 2:21:38.48      SNMPv2-MIB::snmpTrapOID.0 = OID: NP-IQM3-NOTIFICATION-MIB::StartTrap      NP-IQM3-NOTIFICATION-MIB::Count.0 = INTEGER: 0      NP-IQM3-NOTIFICATION-MIB::Horizon.0 = INTEGER: 60      NP-IQM3-NOTIFICATION-MIB::Status.0 = STRING: UP      NP-IQM3-NOTIFICATION-MIB::Param.0 = STRING: SDLostPercent      NP-IQM3-NOTIFICATION-MIB::TimeStart.0 = STRING: 2025-11-27 12:58:14.000000      NP-IQM3-NOTIFICATION-MIB::Threshold.0 = STRING: 0      NP-IQM3-NOTIFICATION-MIB::Test.0 = STRING: al-stub-CMD      NP-IQM3-NOTIFICATION-MIB::Severity.0 = STRING: GREEN      NP-IQM3-NOTIFICATION-MIB::Table.0 = STRING: dtraw      NP-IQM3-NOTIFICATION-MIB::Class.0 = STRING: BE      NP-IQM3-NOTIFICATION-MIB::TimeEnd.0 = STRING: 2025-11-27 12:59:14.000000      NP-IQM3-NOTIFICATION-MIB::Policy.0 = STRING: policy-test      NP-IQM3-NOTIFICATION-MIB::URL.0 = STRING: empty
2025-11-27 12:59:27 localhost.localdomain [UDP: [127.0.0.1]:59402->[127.0.0.1]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (849849) 2:21:38.49      SNMPv2-MIB::snmpTrapOID.0 = OID: NP-IQM3-NOTIFICATION-MIB::StartTrap      NP-IQM3-NOTIFICATION-MIB::Table.0 = STRING: dtraw      NP-IQM3-NOTIFICATION-MIB::Class.0 = STRING: BE      NP-IQM3-NOTIFICATION-MIB::TimeEnd.0 = STRING: 2025-11-27 12:59:14.000000      NP-IQM3-NOTIFICATION-MIB::Policy.0 = STRING: policy-test      NP-IQM3-NOTIFICATION-MIB::Horizon.0 = INTEGER: 60      NP-IQM3-NOTIFICATION-MIB::Count.0 = INTEGER: 0      NP-IQM3-NOTIFICATION-MIB::Status.0 = STRING: UP      NP-IQM3-NOTIFICATION-MIB::Param.0 = STRING: DSLostPercent      NP-IQM3-NOTIFICATION-MIB::TimeStart.0 = STRING: 2025-11-27 12:58:14.000000      NP-IQM3-NOTIFICATION-MIB::Threshold.0 = STRING: 0      NP-IQM3-NOTIFICATION-MIB::Test.0 = STRING: al-stub-CMD      NP-IQM3-NOTIFICATION-MIB::Severity.0 = STRING: GREEN      NP-IQM3-NOTIFICATION-MIB::URL.0 = STRING: empty

```

Основные задачи проверки на этом можно считать выполненными. То есть IQM, как в виде агента, так и в виде системы управления вполне работоспособен на ОС «Альт» 10. Это можно считать наглядно показанным.

По-хорошему, конечно, по окончании тестирования следует выключить агенты и процессы системы управления из автозапуска. Можно даже удалить соответствующие пакеты ПО. Надеемся, вы справитесь в этом самостоятельно, никаких дополнительных знаний, кроме стандартных об администрировании ОС «Альт», не требуется. Кроме того, поскольку тестовое оборудование будет в будущем так или иначе использоваться иным образом, вы можете этого и не делать вовсе.

## Содержание

1 Введение.....	2
2 Организация лаборатории.....	2
3 Начальные проверки агентов.....	5
4 Начальные проверки системы управления.....	8
5 Заведение агента АИ1 в системе управления.....	22
6 Заведение агента АИ2 в системе управления.....	27
7 Заведение сопряжённого агента СА в системе управления.....	28
8 Заведение шлюза ШЛ в системе управления.....	32
9 Заведение сервера DNS в системе управления.....	33
10 Заведение агента U7 в системе управления.....	34
11 Тест U0 между АИ1 и АИ2.....	38
12 Тест U9 между АИ1 и СА.....	44
13 Тест U7 между АИ2 и СУ.....	45
14 Тест T1 между АИ2 и СА.....	47
15 Тест I0 между АИ1 и ШЛ.....	48
16 Тест URL между АИ1 и СА.....	50
17 Тест URLUP между АИ2 и СА.....	51
18 Тест DNS между АИ2 и DNS.....	53
19 Тест CMD между АИ1 и STUB.....	55
20 Настройка политик контроля.....	57
21 Просмотр графиков.....	64
22 Просмотр табло алармов и реакций.....	89

Настоящим подтверждается, что все исключительные авторские права на данную документацию принадлежат ООО «НетПроб». Предоставление прав на данную документацию осуществляется по договору поставки или технической поддержки программного обеспечения, юридический текст которого поставляется отдельно. Неотчуждаемые личные неимущественные права на данную документацию принадлежат физическим лицам – авторам, перечисленным в документации.

Copyright © 2008-2025

ООО «Нетпроб»

Copyright © 2010-2025



Сергей Александрович Еременко