



Мониторинг работоспособности информационно-телекоммуникационной среды поддержки виртуальных научных сообществ

А. Коршунов, И. Астапов, М. Дзыба,
М. Занчурин

Цели и задачи мониторинга



Штатное функционирование информационно-телекоммуникационной среды поддержки виртуальных научных сообществ является одним из необходимых условий ее эффективного использования.

Подобные среды, включают в себя, вычислительный комплекс высокой производительности, сетевую инфраструктуру, содержащую отдельные узлы, поддерживающие информационные активы, маршрутизаторы, коммутаторы и прочее коммуникационное оборудование, программные средства, реализующие системные и общецелевые сервисы.

Они потенциально подвержены множеству внешних и внутренних воздействий, нарушающих штатное функционирование:

- сбои в работе подсистем электропитания и кондиционирования;
- отказы оборудования;
- сбои программного обеспечения;
- компьютерные вирусы;
- атаки злоумышленников;

Цели и задачи мониторинга



Мониторинг в широком смысле – специально организованное, систематическое наблюдение за состоянием объектов, явлений, процессов с целью оценки их состояния с тех или иных заранее заданных позиций (аномальный характер поведения, работоспособность, надежность, эффективность использования).

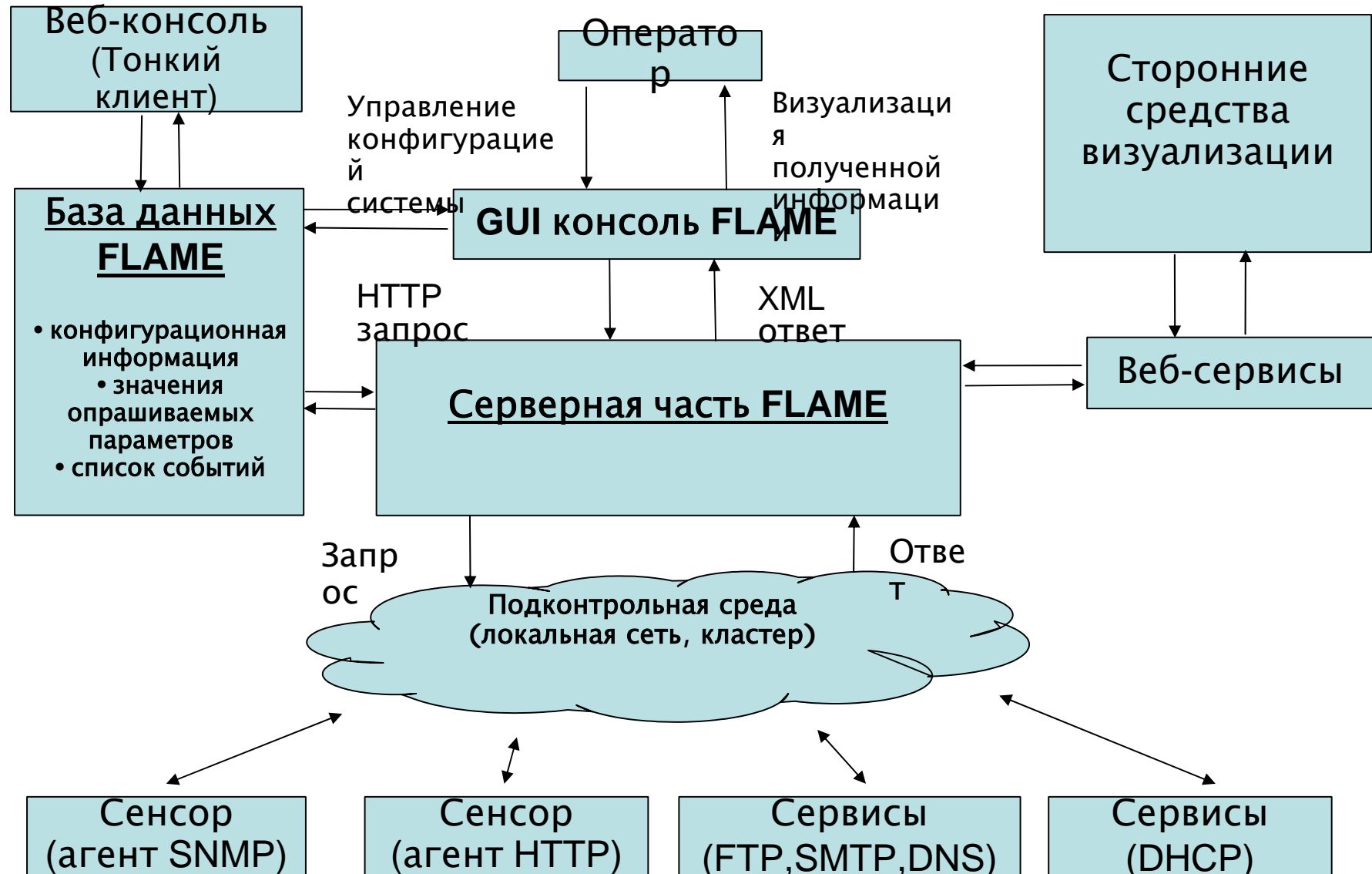
Выявление параметров, описывающих состояние базовых аппаратно-программных средств поддержки виртуальных научных сообществ в штатном, согласно принятому регламенту, режиме, обеспечение их постоянного мониторинга позволяет своевременно выявлять аномальные ситуации и добиваться стабильной, высокоэффективной работы как отдельных компонентов так и всего подконтрольного объекта в целом.

Функциональный подход к мониторингу

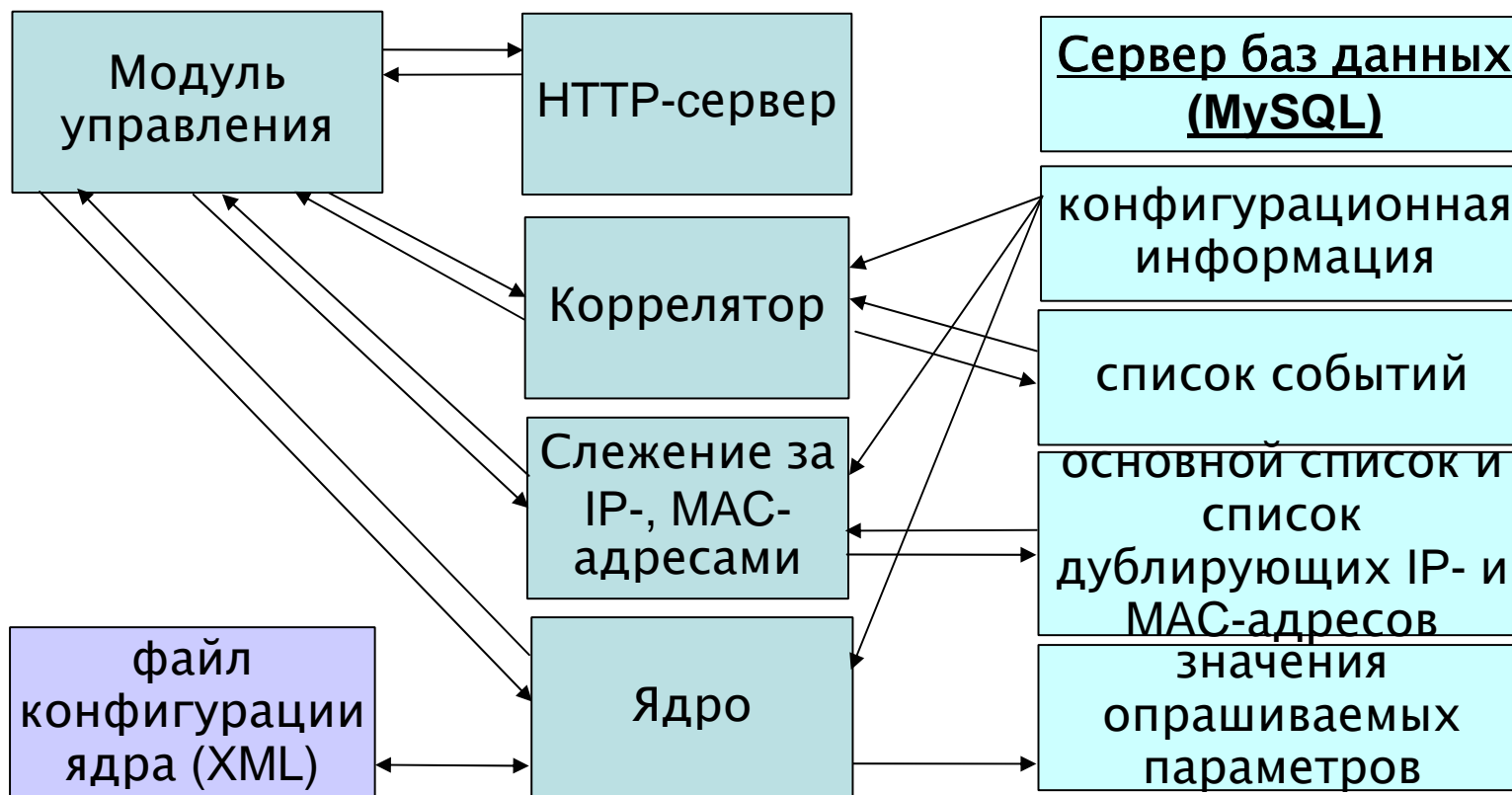


- Конфигурация системы мониторинга задается в виде набора функций
- Вычисление функций
- База данных с результатами вычисленных функций (кэширование)

Архитектура



Архитектура серверной части



Серверная часть: набор модулей, реализованных в виде отдельных процессов и взаимодействующих с помощью механизма IPC pipe.



Функции менеджера:

- маршрутизация внутренних сообщений между модулями;
- отслеживание ошибок в работе модулей и перезапуск их в случае сбоя.

Функции ядра:

- обращение к агентам подконтрольной среды (SNMP, HTTP) и получение значений параметров;
- проверка значений собираемых параметров на удовлетворение predetermined администратором ограничениям;
- порождение событий, если это определено администратором и отправка их модулю корреляции.

Язык конфигурации



```
<requests>
<request id="1" node_id="24" name="Port_Status">
<rvalues>
  <rvalue id="1" regexp="(%%1 == 1)AND(%%2 == 1)" value="OK" />
  <rvalue id="2" regexp="(%%1 == 1)AND(%%2 == 2)" value="FAILED" />
  <rvalue id="3" regexp="(%%1 == 2)" value="OFF" />
</rvalues>
<events>
  <event id="1" regexp="(%%1 == 1)AND(%%2 == 1)" type="OK" />
  <event id="2" regexp="(%%1 == 1)AND(%%2 == 2)" type="FAILED" />
  <event id="3" regexp="(%%1 == 2)" type="OFF" />
</events>
<timeout value="10"/>
<functions>
  <function id="1" name="SnmpRequest"
    arg="fat.imec.msu.ru,.1.3.6.1.2.1.2.2.1.7.15"/>
  <function id="2" name="SnmpRequest"
    arg="fat.imec.msu.ru,.1.3.6.1.2.1.2.2.1.8.15"/>
</functions>
</request>
</requests>
```

Файл конфигурации ядра состоит из запросов **request**, которые необходимо вычислить ядру для получения значений параметров от подконтрольных устройств. Запрос содержит уникальный идентификатор **id**, идентификатор объекта в полном перечне объектов известных системе **node_id**, имя запрашиваемого ресурса **name**. Значение **timeout** указывает время, в течении которого действительна полученная информация.

Язык конфигурации



```
<requests>

<request id="1" node_id="24" name="Port_Status">
<rvalues>
  <rvalue id="1" regexp="(%%1 == 1)AND(%%2 == 1)" value="OK" />
  <rvalue id="2" regexp="(%%1 == 1)AND(%%2 == 2)" value="FAILED" />
  <rvalue id="3" regexp="(%%1 == 2)" value="OFF" />
</rvalues>
<events>
  <event id="1" regexp="(%%1 == 1)AND(%%2 == 1)" type="OK" />
  <event id="2" regexp="(%%1 == 1)AND(%%2 == 2)" type="FAILED" />
  <event id="3" regexp="(%%1 == 2)" type="OFF" />
</events>

<timeout value="10"/>

<functions>
  <function id="1" name="SnmpRequest"
    arg="fat.imec.msu.ru,.1.3.6.1.2.1.2.2.1.7.15"/>
  <function id="2" name="SnmpRequest"
    arg="fat.imec.msu.ru,.1.3.6.1.2.1.2.2.1.8.15"/>
</functions>
</request>

</requests>
```

В блоке **functions** содержится список функций, используемых для опроса подконтрольной среды. Каждая функция имеет уникальный в рамках запроса номер **id**, имя **name** и набор аргументов **arg**.

Язык конфигурации



```
<requests>
<request id="1" node_id="24" name="Port_Status">
<rvalues>
  <rvalue id="1" regexp="(%%1 == 1)AND(%%2 == 1)" value="OK" />
  <rvalue id="2" regexp="(%%1 == 1)AND(%%2 == 2)" value="FAILED" />
  <rvalue id="3" regexp="(%%1 == 2)" value="OFF" />
</rvalues>
<events>
  <event id="1" regexp="(%%1 == 1)AND(%%2 == 1)" type="OK" />
  <event id="2" regexp="(%%1 == 1)AND(%%2 == 2)" type="FAILED" />
  <event id="3" regexp="(%%1 == 2)" type="OFF" />
</events>

<timeout value="10"/>

<functions>
  <function id="1" name="SnmpRequest"
    arg="fat.imec.msu.ru,.1.3.6.1.2.1.2.2.1.7.15"/>
  <function id="2" name="SnmpRequest"
    arg="fat.imec.msu.ru,.1.3.6.1.2.1.2.2.1.8.15"/>
</functions>
</request>

</requests>
```

В блоке **rvalues** (этот блок может отсутствовать) описываются возвращаемые значения, первое из которых с идентификатором будет возвращено ядром в качестве значения запроса при условии срабатывания **regexp** над результатами вычисления функций.

Язык конфигурации



```
<requests>
<request id="1" node_id="24" name="Port_Status">
<rvalues>
  <rvalue id="1" regexp="(%%1 == 1)AND(%%2 == 1)" value="OK" />
  <rvalue id="2" regexp="(%%1 == 1)AND(%%2 == 2)" value="FAILED" />
  <rvalue id="3" regexp="(%%1 == 2)" value="OFF" />
</rvalues>
<events>
  <event id="1" regexp="(%%1 == 1)AND(%%2 == 1)" type="OK" />
  <event id="2" regexp="(%%1 == 1)AND(%%2 == 2)" type="FAILED" />
  <event id="3" regexp="(%%1 == 2)" type="OFF" />
</events>
<timeout value="10"/>
<functions>
  <function id="1" name="SnmpRequest"
    arg="fat.imec.msu.ru,.1.3.6.1.2.1.2.2.1.7.15"/>
  <function id="2" name="SnmpRequest"
    arg="fat.imec.msu.ru,.1.3.6.1.2.1.2.2.1.8.15"/>
</functions>
</request>
</requests>
```

В блоке **events** указываются события, которые могут породиться при вычислениях XML-запроса. Каждое событие имеет 3 обязательных атрибута: **id**, **regexp**, **type**, и 2 необязательных: **level**, **description**.

Атрибуты:

- id** - уникальный идентификатор события для данного запроса;
- regexp** - условие порождения события;
- type** - тип порождаемого события;
- level** - уровень критичности события;
- description** - описание события.

Язык конфигурации



```
<requests>
<request id="1" node_id="24" name="Port_Status">
<rvalues>
  <rvalue id="1" regexp="(%%1 == 1)AND(%%2 == 1)" value="OK" />
  <rvalue id="2" regexp="(%%1 == 1)AND(%%2 == 2)" value="FAILED" />
  <rvalue id="3" regexp="(%%1 == 2)" value="OFF" />
</rvalues>
<events>
  <event id="1" regexp="(%%1 == 1)AND(%%2 == 1)" type="OK" />
  <event id="2" regexp="(%%1 == 1)AND(%%2 == 2)" type="FAILED" />
  <event id="3" regexp="(%%1 == 2)" type="OFF" />
</events>

<timeout value="10"/>

<functions>
  <function id="1" name="SnmpRequest"
    arg="fat.imec.msu.ru,.1.3.6.1.2.1.2.2.1.7.15"/>
  <function id="2" name="SnmpRequest"
    arg="fat.imec.msu.ru,.1.3.6.1.2.1.2.2.1.8.15"/>
</functions>
</request>

</requests>
```

В атрибутах `regexp` и `value` блоков **rvalues** и **events** используется специальный язык, позволяющий задавать логику запроса или сформировать значение запроса с использованием значений функций из блока **functions**.



Язык формирования логики и значений запросов содержит:

- логические операторы: **AND, OR, NOT**;
- операторы сравнения: **<, >, ==, <=, >=, !=**;
- арифметические операторы: **+, -, *, /**;
- скобки: **(,)**;
- оператор конкатенации со строкой: **"string"** - позволяет объединить вычисленные значения со строкой **string** (пример: **%%n"C"**);
- выражение **%%n** - означает ссылку на значение функции с индексом **n** из блока **functions**;
- конструкция **#<regular_expression>#%%n#**, где **regular_expression** - регулярное выражение; конструкция возвращает **1** (истина), если результат функции удовлетворяет регулярному выражению и **0** (ложь) - в противном случае.



Функции коррелятора:

- определение источника неполадки в сети и устранение явления шторма событий, связанного с этой неполадкой;
- устранение дублирования событий;
- сохранение значимых событий в базе данных.

Конфигурация подконтрольной среды



Конфигурация подконтрольной среды представляется в системе в виде набора компонентов (объектов) различного типа, соединенных друг с другом различного типа связями.

В системе существуют следующие predetermined типы объектов: router, switch, hub, host, host_only, service, interface, port, subnet, shared_segment, unmanaged_switch, unknown_entity, flame.

Конфигурационная информация хранится в базе данных в виде двух таблиц: таблицы узлов и таблицы связей.

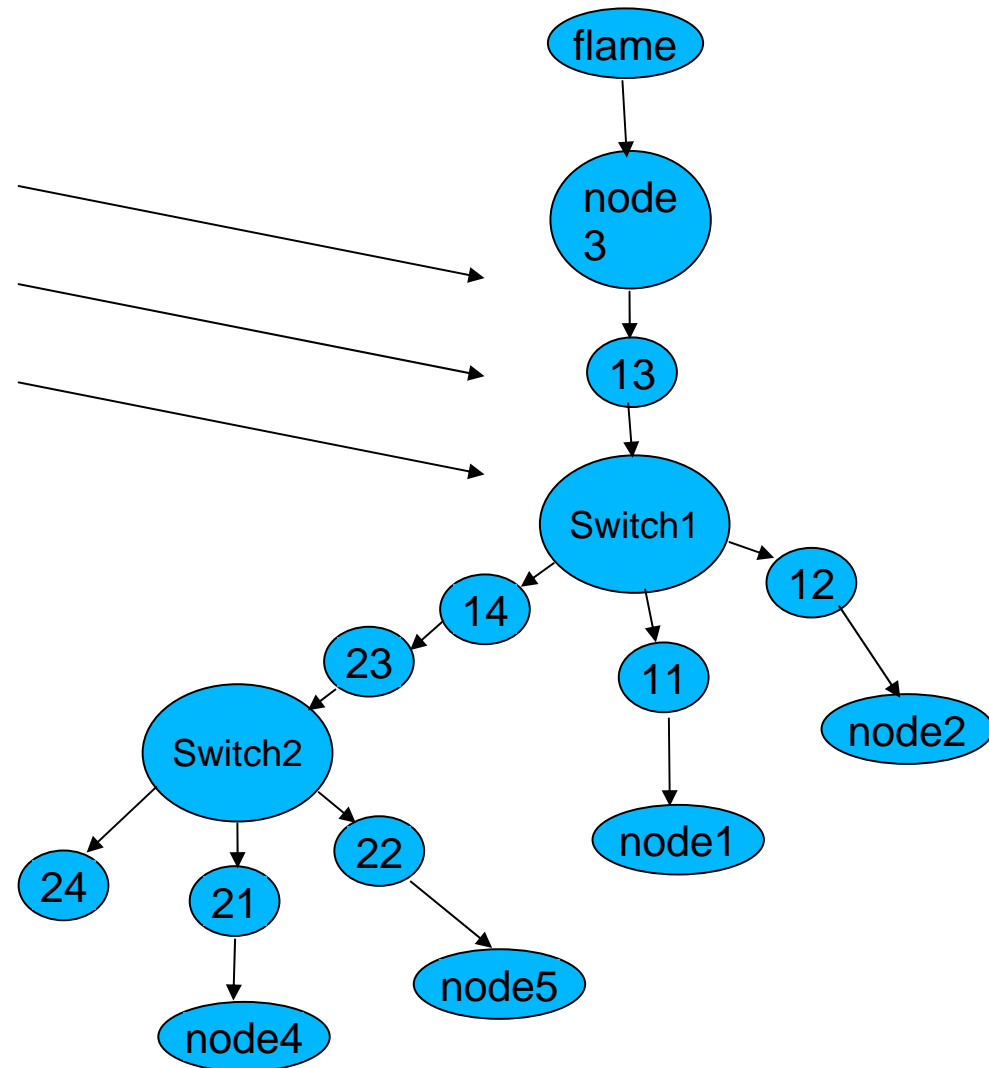
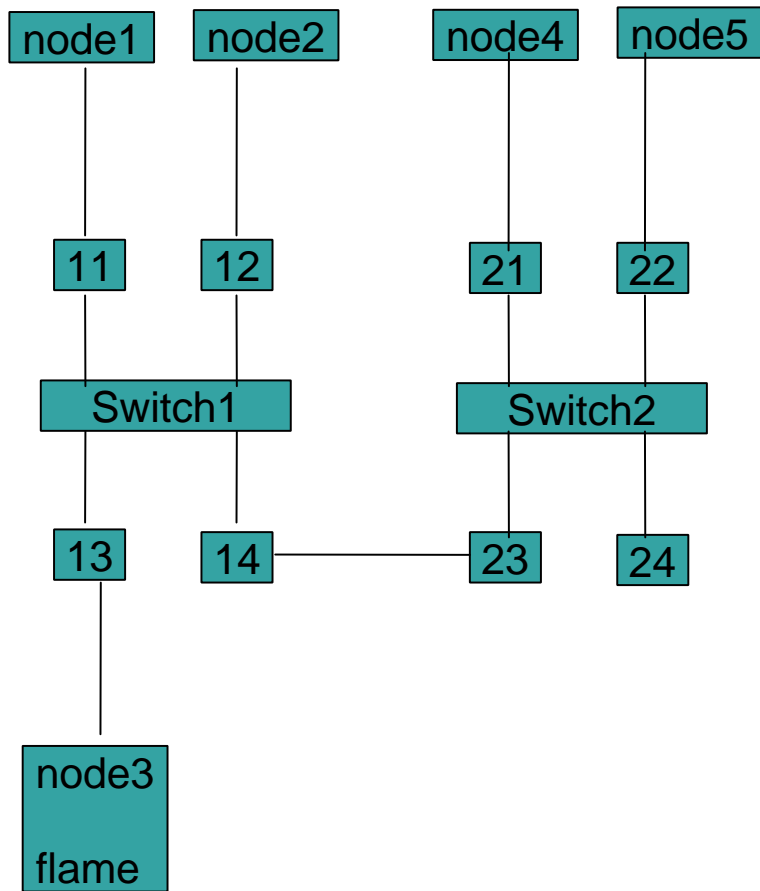
Коррелятор



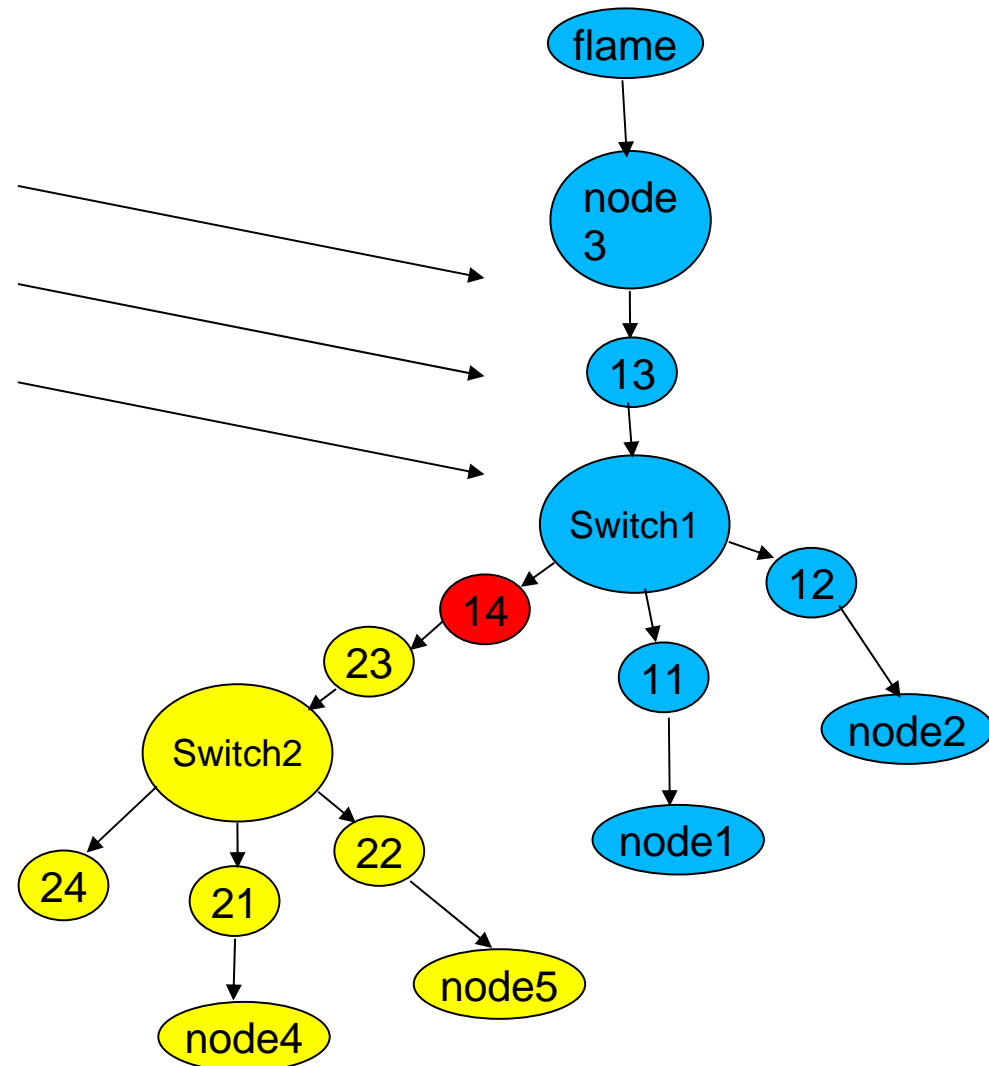
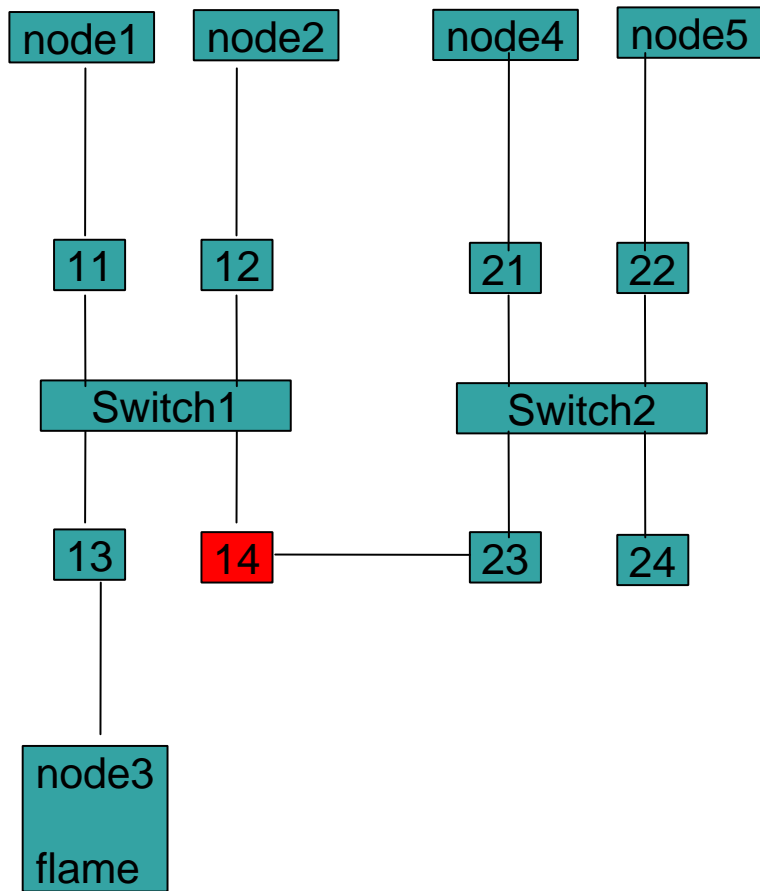
Определение источника проблемы осуществляется с использованием конфигурационной информации о связях между объектами подконтрольной среды на физическом уровне и о связях сервисов с узлами, на которых они запущены. Подмножество используемых коррелятором узлов и связей не должно содержать циклов, т.е. должно представлять собой дерево.

По данному дереву коррелятор строит дерево корреляции с вершиной – объектом типа flame.

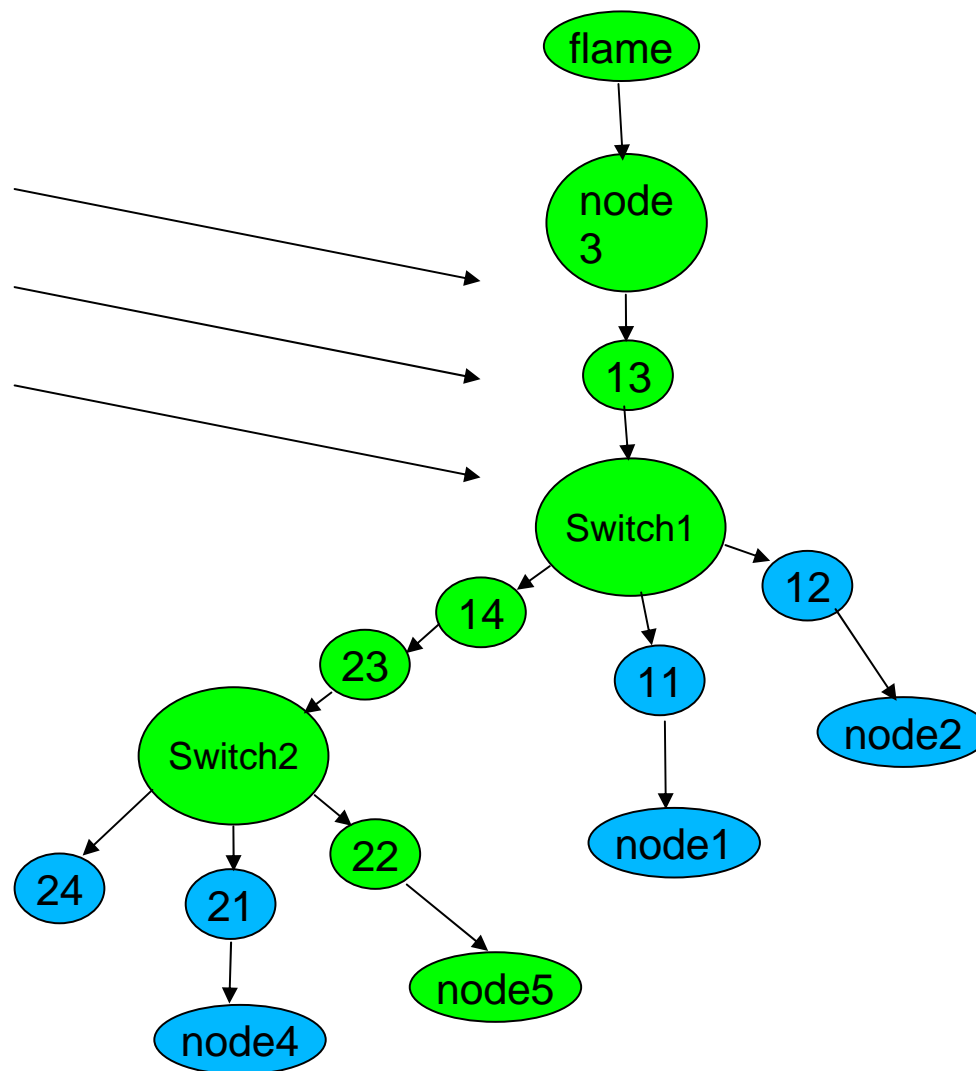
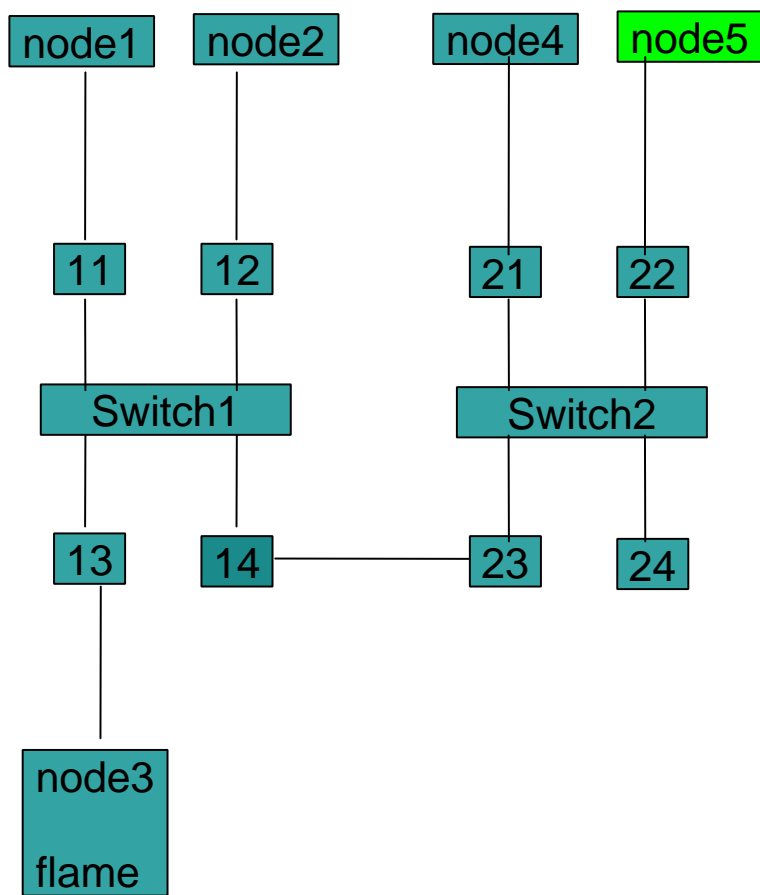
Корреляция



Корреляция



Корреляция



Подсистема автоконфигурации



Функции подсистемы автоконфигурации:

- определение топологии сетевых объектов подконтрольной среды на уровне 3 модели OSI;
- сохранение полученной информации в базе данных системы мониторинга;
- создание файла конфигурации для модуля ядра;
- определение новых подключенных узлов.

Подсистема автоконфигурации



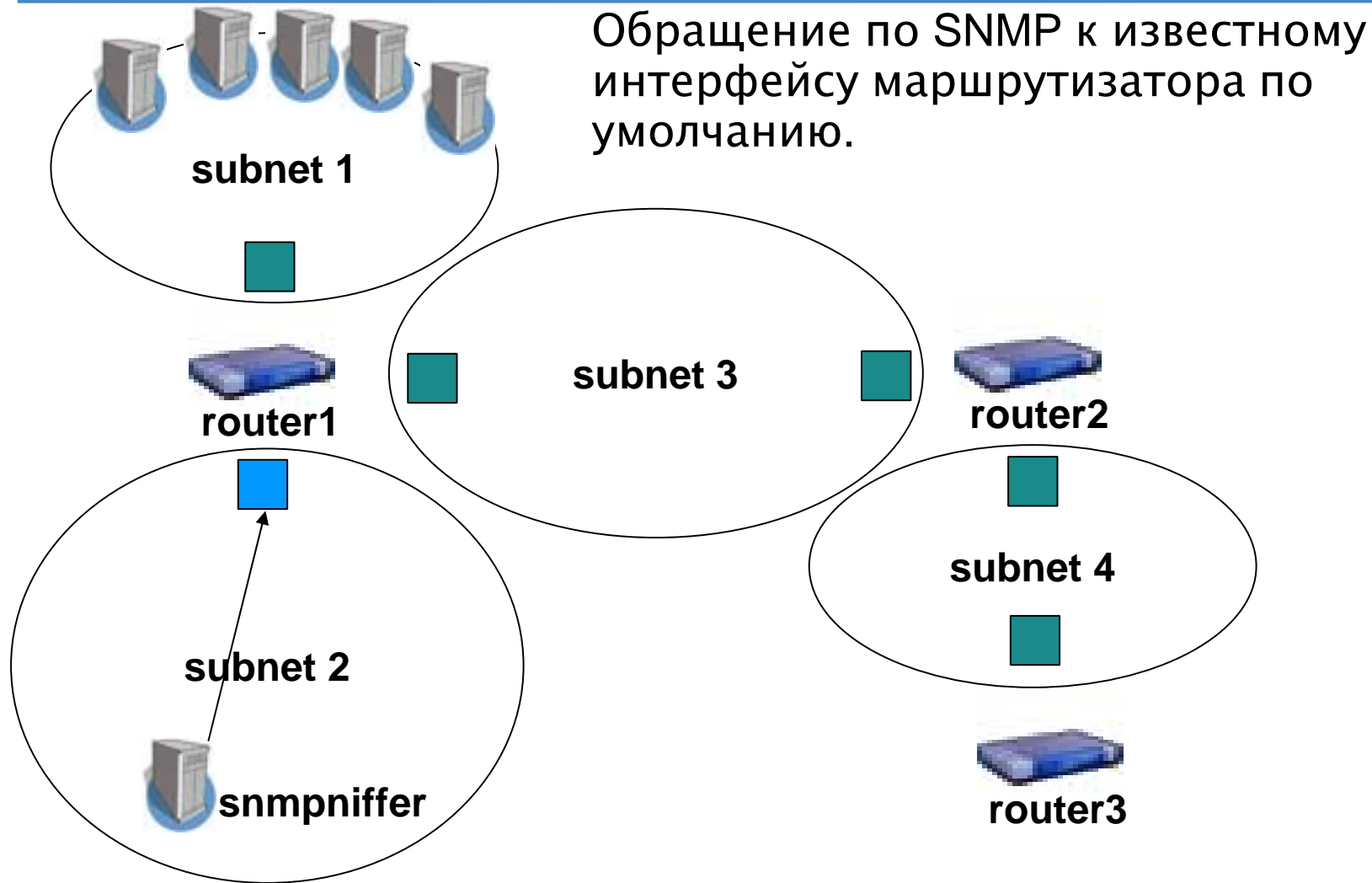
Определение топологии сети:

Разработана программа snmpniffer.

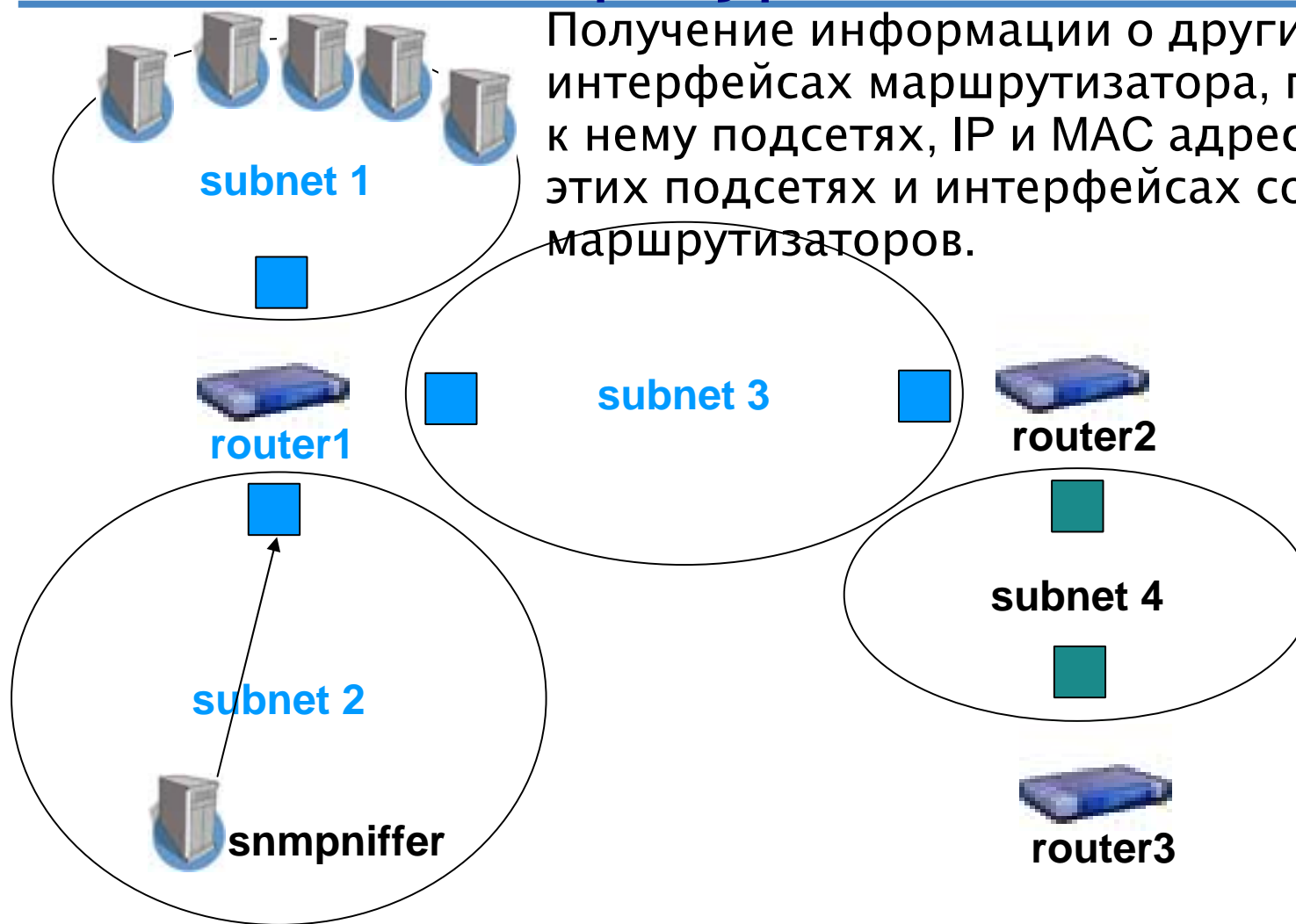
Алгоритм определения топологии основан на использовании протокола SNMP. В качестве вспомогательных средств используются алгоритмы на основе broadcast ping и перебора IP адресов.

Для работы алгоритма необходим доступ к SNMP-агентам на маршрутизаторах или шлюзах подконтрольной среды.

Подсистема автоконфигурации

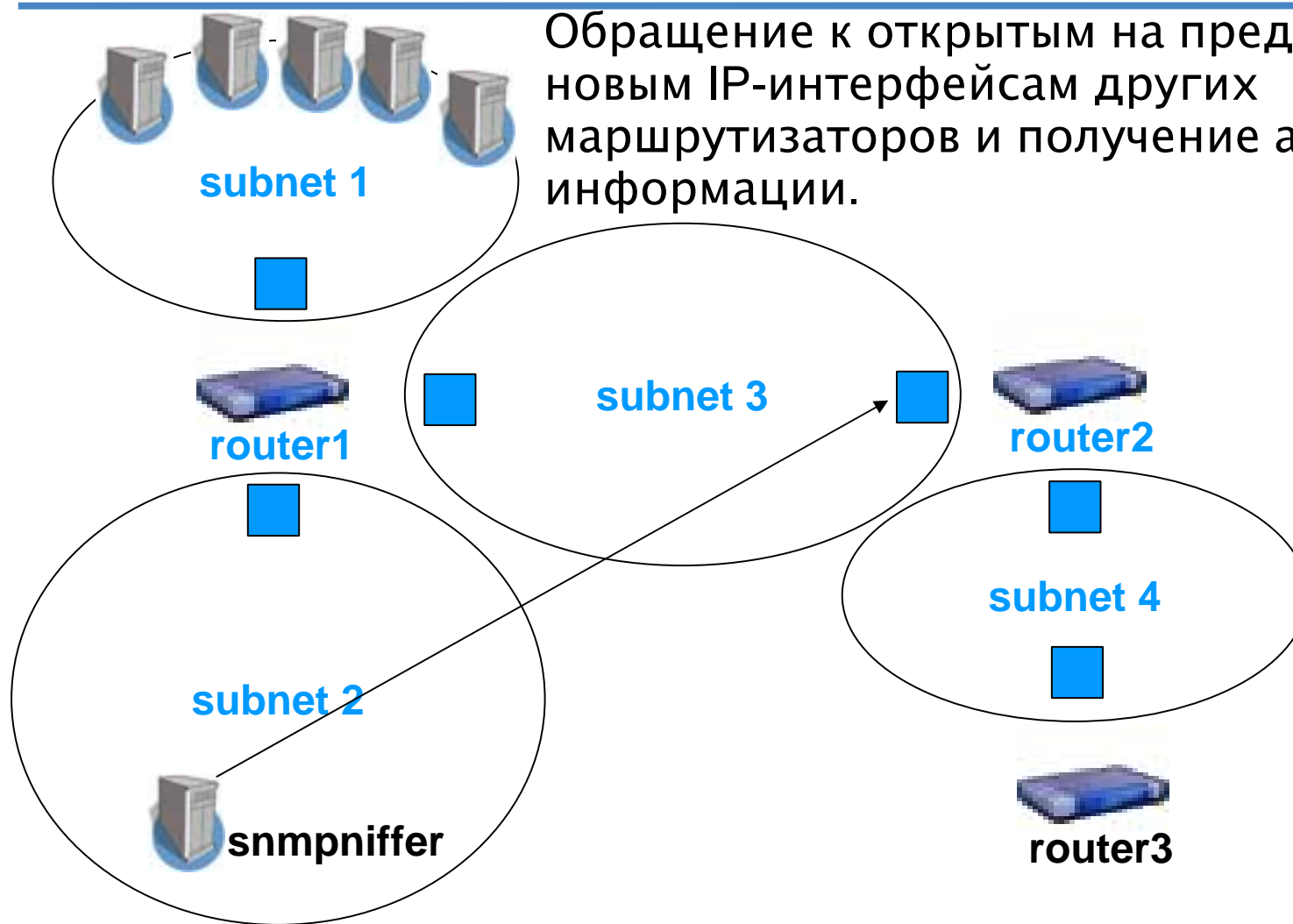


Подсистема автоконфигурации



Получение информации о других интерфейсах маршрутизатора, примыкающих к нему подсетях, IP и MAC адресах узлов в этих подсетях и интерфейсах соседних маршрутизаторов.

Подсистема автоконфигурации

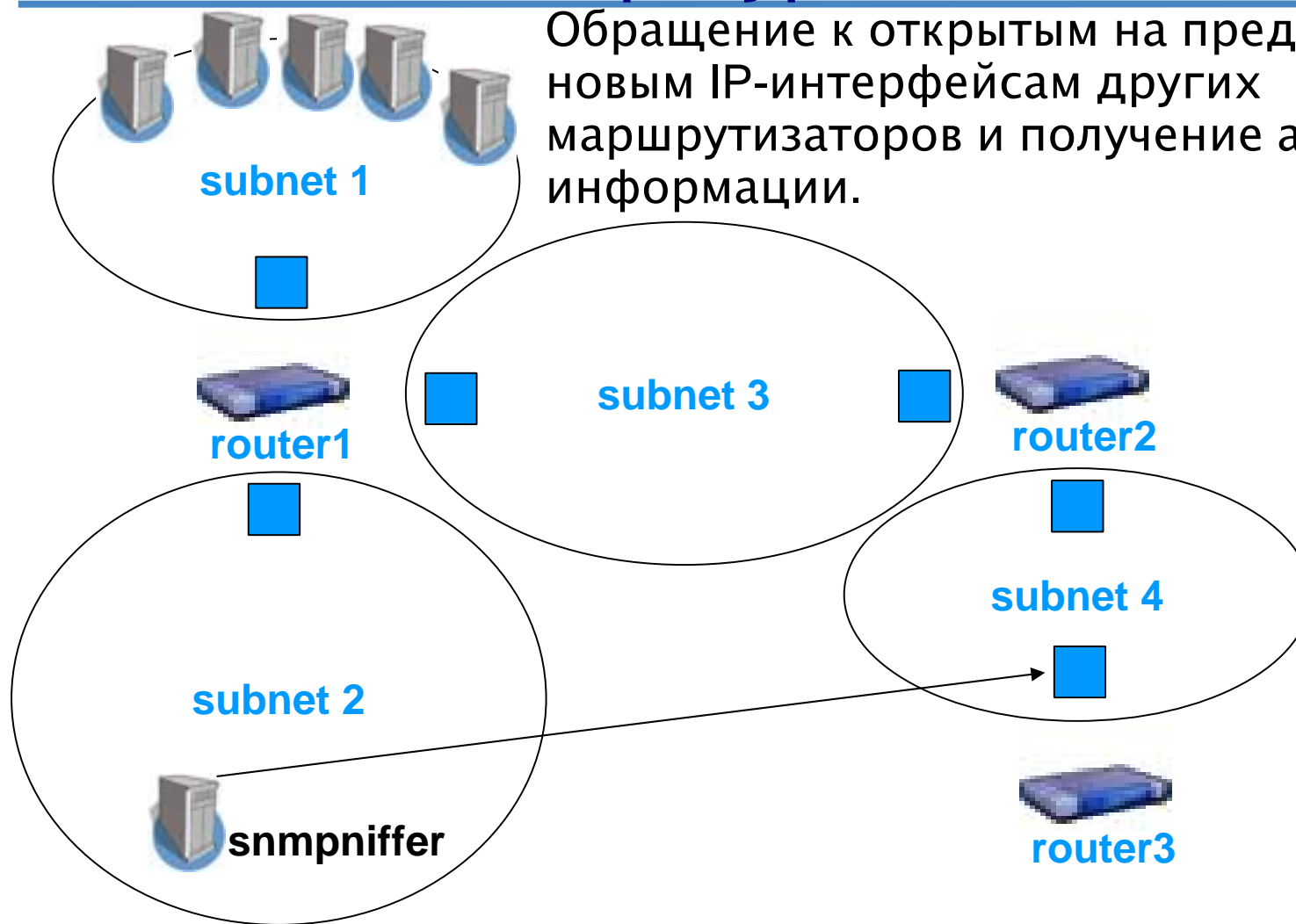


Обращение к открытым на предыдущем шаге новым IP-интерфейсам других маршрутизаторов и получение аналогичной информации.

Подсистема автоконфигурации



Обращение к открытым на предыдущем шаге новым IP-интерфейсам других маршрутизаторов и получение аналогичной информации.



Слежение за IP и MAC адресами



Функции модуля:

- определение изменений соответствия MAC адресов устройств сети IP адресам выделенным администратором;
- информирование администратора о найденных изменениях.

Слежение за IP и MAC адресами



Конфигурационной информацией для модуля служит:

- список маршрутизаторов доступных по протоколу SNMP;
- список интересующих администратора подсетей.

Информация хранится в двух таблицах: базовой таблице и таблице изменений.

Модуль последовательно опрашивает ARP-кэши заданных маршрутизаторов.

При нахождении очередной пары IP-MAC, отсутствующей в базовой таблице, проверяется, существует ли пара с данным IP- либо(хот) MAC- адресом в базовой таблице. Если нет, пара заносится в базовую таблицу. В противном случае пара заносится в таблицу изменений и модуль посылает соответствующее сообщение в модуль корреляции.

Слежение за IP и MAC адресами



Получение сообщения о измененном соответствии IP-MAC адресов может означать:

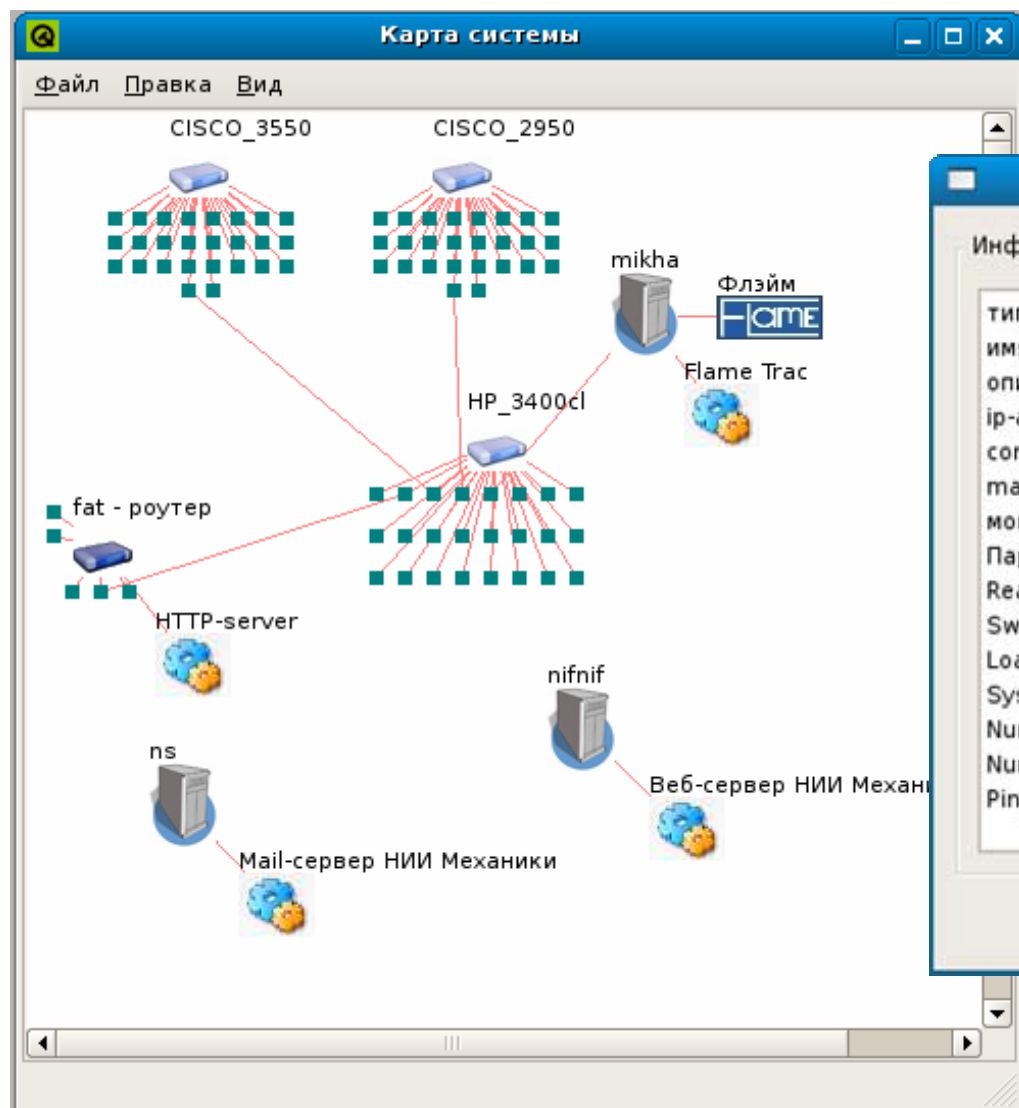
- **данный IP-адрес выдается DHCP-сервером** (в этом случае администратор должен удалить сообщение об изменении соответствия из таблицы изменений и исключить IP-адрес из конфигурационной таблицы подсетей);
- **данный IP-адрес является одним из IP-интерфейсов, соответствующих одной и той же сетевой карте** (в этом случае пара должна быть добавлена в базовую таблицу);
- **произошла плановая замена сетевой карты или плановое изменение IP адреса** (в этом случае пара должна быть добавлена в базовую таблицу, из базовой таблицы должны быть удалены записи имеющие тот же MAC- или IP-адрес);
- **произошло несанкционированное администратором изменение IP-адреса** (в этом случае вопрос должен быть решен в административном порядке, после чего пара должна быть удалена из таблицы изменений).



Функции визуализатора:

- управление работой серверной части:
создание и редактирование конфигурации подконтрольной среды, конфигурации ядра, перезапуск модулей серверной части;
- отображение полученной серверной частью системы FLAME информации: значения собираемых параметров, списки событий;
- построение, редактирование и визуализация карты подконтрольной среды с индикацией состояния объектов;
- средство просмотра файлов описания MIB (MIB-browser).

Визуализатор, карта сети



The "Информация об узле" window displays the following information for a selected node:

Информация об узле

тип узла: router; id узла: 1
имя узла: fat - роутер
описание: Роутер НИИ Механики МГУ (fat.imes.msu.ru)
ip-адрес: 193.232.114.64
community: public
mac: 00:30:05:46:08:80
мониторинг включен

Параметры:

Real Memory Available: 4.22249 % -- 00:34:32 17.04.2008
Swap Memory Available: 99.9999 % -- 00:34:27 17.04.2008
Load Average (1 min): 0.94 -- 00:34:33 17.04.2008
System CPU Time: 24220798 -- 00:34:26 17.04.2008
Number of Processes: 163 -- 00:34:26 17.04.2008
Number of Users: 2 -- 00:34:26 17.04.2008
Ping (fat): OK -- 00:34:48 17.04.2008

Esc - выход

Визуализатор, редактор конфигурации



Система запросов ядра

Запросы для подконтрольных устройств

	id	узел	имя ресурса	частота опроса
1	10	порт2 (fat)	Port_Status	10
2	13	порт3 (fat)	Port_Status	10
3	14	порт4 (fat)	Port_Status	10
4	15	fat - роутер	Real Memory Available	40
5	16	fat - роутер	Swap Memory Available	40
6	17	fat - роутер	Load Average (1 min)	60
7	18	fat - роутер	System CPU Time	60
8	19	fat - роутер	Number of Processes	60
9	20	fat - роутер	Number of Users	60
10	21	Порт1 (HP)	Port Status	30
11	22	Порт2 (HP)	Port Status	30
12	23	Порт3 (HP)	Port Status	30
13	24	Порт4 (HP)	Port Status	30
14	25	Порт5 (HP)	Port Status	30
15	26	Порт6 (HP)	Port Status	30
16	27	Порт7 (HP)	Port Status	30
17	28	Порт8 (HP)	Port Status	30
18	29	Порт9 (HP)	Port Status	30
19	30	Порт10 (HP)	Port Status	30
20	31	Порт11 (HP)	Port Status	30
21	32	Порт12 (HP)	Port Status	30
22	33	Порт13 (HP)	Port Status	30

Добавить Добавить по шаблону Изменить Удалить

Функции для опроса подконтрольной среды

id	имя функции	аргумент
1	SnmpRequest	193.232.114.1..1.3.6.1.2.1.2.2.1.7.2
2	SnmpRequest	193.232.114.1..1.3.6.1.2.1.2.2.1.8.2

Добавить Изменить Удалить

Условия преобразования возвращаемых значений запроса

id	условия преобразования	значение
1	(%1==1) AND (%2==1)	"OK"
2	(%1==1) AND (%2==2)	"FAILED"
3	(%1==2)	"OFF"

Добавить Изменить Удалить

События, порождаемые при выполнении запроса

id	условие порождения	тип	уровень критичности	описание
1	(%1==1) AND (%2==1)	OK		
2	(%1==1) AND (%2==2)	FAILED		
3	(%1==2)	OFF		

Добавить Изменить Удалить

Визуализатор, MIB-броузер



Изменение функции для опроса

id функции: 1
имя функции: SnmpRequest
ip-адрес: 193.232.114.1
community:
OID: 1.3.6.1.2.1.2.2.1.7.2
[Запомнить] [Отменить]

Название/Идентификатор (oid)
1.3.6.1.2.1.25.2.2
hrMemorySize(2) from module: HOST-RESOURCES-MIB
[Выбрать oid]

Тип доступа
read-only

Статус
current

Тип MIBа
SYNTAX Integer32
Range: 0..2147483647
Textual convention: KBytes

Дерево MIBов

- (2) mgmt
 - (1) mib-2
 - (25) host
 - (1) hrSystem
 - (1) hrSystemUptime
 - (2) hrSystemDate
 - (3) hrSystemInitialLoadDevice
 - (4) hrSystemInitialLoadParameters
 - (5) hrSystemNumUsers
 - (6) hrSystemProcesses
 - (7) hrSystemMaxProcesses
 - (2) hrStorage
 - (1) hrStorageTypes
 - (2) hrMemorySize
 - (3) hrStorageTable
 - (1) hrStorageEntry
 - (1) hrStorageIndex
 - (2) hrStorageType
 - (3) hrStorageDescr
 - (4) hrStorageAllocationUnits
 - (5) hrStorageSize
 - (6) hrStorageUsed
 - (7) hrStorageAllocationFailures
 - (3) hrDevice
 - (1) hrDeviceTypes
 - (2) hrDeviceTable
 - (1) hrDeviceEntry
 - (1) hrDeviceIndex
 - (2) hrDeviceType
 - (3) hrDeviceDescr

[Построить дерево]

Анализируемые файлы
HOST-RESOURCES-MIB.txt
[Добавить файл] [Удалить]

Анализируемые директории
mibs
[Добавить директорию] [Удалить]

Описание
The amount of physical read-write main memory, typically RAM, contained by the host.

Визуализатор, список событий



События

Список событий

	узел	время	событие	статус
53	Порт24 (Cisco)	16.04.2008 23:45:03	From FLAME_KERNEL (FAILED)	FAILED
54	Порт20 (Cisc...	16.04.2008 23:45:03	From FLAME_KERNEL (OK)	OK
55	Порт6 (Cisco2)	16.04.2008 23:45:02	From FLAME_KERNEL (OK)	OK
56	HTTP-server	16.04.2008 23:45:02	From FLAME_KERNEL (OK)	OK
57	порт4 (fat)	16.04.2008 23:45:01	From FLAME_KERNEL (OK)	OK
58	порт2 (fat)	16.04.2008 23:45:00	From FLAME_KERNEL (OFF)	OFF
59	Порт12 (Cisc...	16.04.2008 23:45:00	From FLAME_KERNEL (OK)	OK
60	Порт15 (Cisc...	16.04.2008 23:45:00	From FLAME_KERNEL (OK)	OK
61	Порт9 (Cisco2)	16.04.2008 23:45:00	From FLAME_KERNEL (OK)	OK
62	Порт17 (Cisc...	16.04.2008 23:45:00	From FLAME_KERNEL (FAILED)	FAILED
63	Порт16 (Cisc...	16.04.2008 23:45:00	From FLAME_KERNEL (FAILED)	FAILED
64	Порт2 (HP)	16.04.2008 23:45:00	From CORRELATOR (OK), Ro...	OK
65	порт3 (fat)	16.04.2008 23:45:00	From CORRELATOR (OK), Ro...	OK
66	fat - роутер	16.04.2008 23:45:00	From FLAME_KERNEL (OK)	OK
67	Порт16 (Cisco)	16.04.2008 23:44:59	From FLAME_KERNEL (FAILED)	FAILED
68	Порт13 (Cisc...	16.04.2008 23:44:59	From FLAME_KERNEL (FAILED)	FAILED
69	Порт18 (Cisc...	16.04.2008 23:44:59	From FLAME_KERNEL (OK)	OK
/0	Порт22 (Cisco)	16.04.2008 23:44:59	From FLAME_KERNEL (OFF)	OFF
/1	Порт23 (Cisco)	16.04.2008 23:44:59	From FLAME_KERNEL (OK)	OK
/2	Порт21 (Cisco)	16.04.2008 23:44:59	From FLAME_KERNEL (FAILED)	FAILED
/3	Порт11 (Cisc...	16.04.2008 23:44:59	From FLAME_KERNEL (OK)	OK
/4	Порт19 (Cisco)	16.04.2008 23:44:58	From FLAME_KERNEL (FAILED)	FAILED
/5	Порт10 (Cisc...	16.04.2008 23:44:57	From FLAME_KERNEL (FAILED)	FAILED
/6	Порт3 (HP)	16.04.2008 23:44:56	From CORRELATOR (OK), Ro...	OK
/7	Порт25 (Cisc...	16.04.2008 23:44:56	From CORRELATOR (OK), Ro...	OK
/8	CISCO_3550	16.04.2008 23:44:56	From CORRELATOR (OK), Ro...	OK
/9	Порт7 (Cisco2)	16.04.2008 23:44:56	From FLAME_KERNEL (OK)	OK

время начала: 14.04.2008 20:32:!! время окончания: 31.12.2008 00:00:!!

частота обновления (100) показывать событий: 100

Фильтр

имя узла: Все

уровень критичности: ■ Normal ■ Notice ■ Warning ■ Error ■ Fatal

Визуализатор, слежение за IP и MAC



The screenshot displays the FLAME software interface with three main windows:

- Подсети и маршрутизаторы** (Subnets and Routers):
 - Подсети** (Subnets) table:

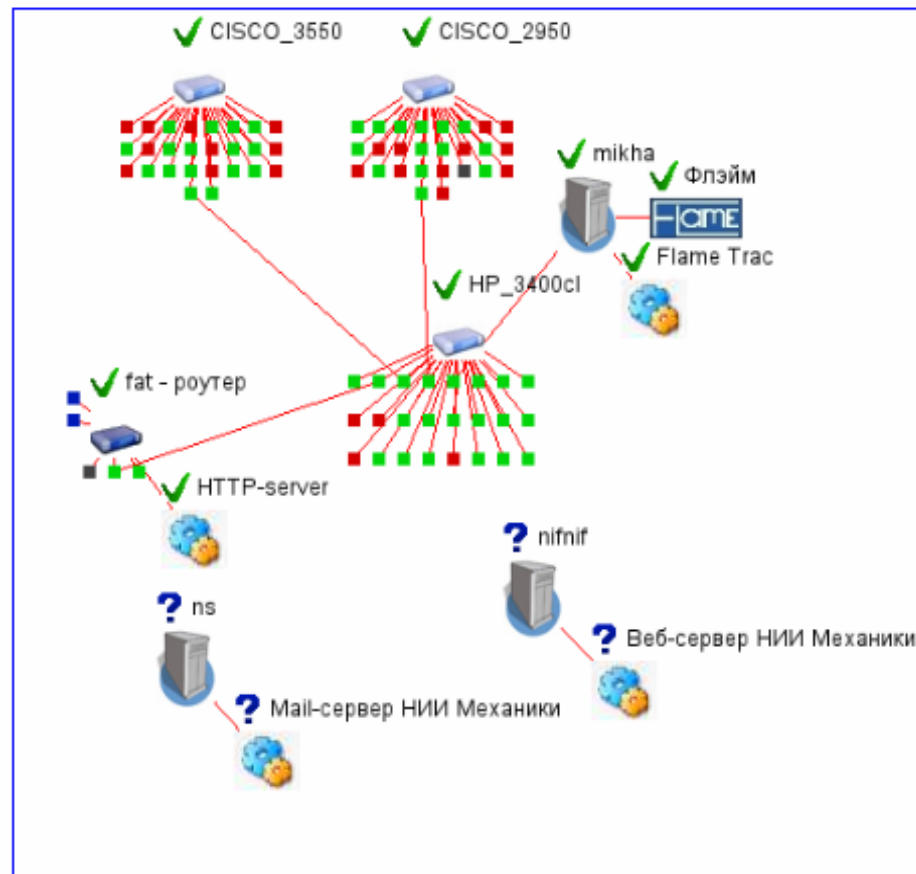
id	подсеть	маска
1	192.168.0.0	255.255.0.0
2	172.17.0.0	255.255.255.0
3	172.17.1.0	255.255.255.0
4	193.232.114.0	255.255.255.0
5	193.232.119.0	255.255.255.0
 - Маршрутизаторы** (Routers) table:

id	IP-адрес	community
1	193.232.114.1	NllMech
- Изменение IP и MAC адресов** (IP and MAC Address Change):

id	IP-адрес	MAC-адрес	время обнаружения
62	193.232.119.69	00:0E:0C:59:53:D0	07.04.2008 17:35:36
63	193.232.119.82	00:30:05:46:0D:19	07.04.2008 17:35:36
64	42 212.192.229.87	00:14:5E:64:BC:8C	11.04.2008 11:13:43
65	23 212.192.229.87	00:14:85:85:08:69	08.04.2008 18:13:54
66	13 212.192.229.87	00:18:F3:54:9C:C7	07.04.2008 19:32:53
67	19 212.192.229.108	00:50:DA:35:99:CE	08.04.2008 12:53:15
68	1 212.192.229.127	00:03:47:A5:75:C4	07.04.2008 17:35:35
69	35 212.192.229.186	00:0C:F1:13:AB:F7	10.04.2008 13:23:26
70	47 212.192.229.186	00:08:02:DD:FD:C6	11.04.2008 12:40:50
- Соответствие IP- и MAC- адресов** (IP and MAC Address Correspondence):
 - Fields: идентификатор: 23, IP-адрес: 212.192.229.87, MAC-адрес: 00:14:85:85:08:69, время обнаружения: 08.04.2008 18:13:54
 - Buttons: Переместить в базовую таблицу, Переместить, удалив в историю все дубли, Удалить данную запись, Выход
 - Основная таблица и история соответствия IP- и MAC- адресов** table:

	IP-адрес	MAC-адрес	время актуализации / удаления	время обнаружения
1	172.17.0.164	00:14:85:85:08:69	10.04.2008 17:09:58	07.04.2008 20:09:20
2	212.192.229.87	52:54:AB:1A:B9:D8	07.04.2008 19:17:39	07.04.2008 17:37:04

Карта устройств



Интервал:

Веб-клиент, список функций



Список функций

узел	запрос	время	таймаут	значение
Веб-сервер НИИ Механики	HTTP-server Status	17 April 2008, 00:48:42	10	OK
CISCO_2950	Ping (cisco)	17 April 2008, 00:48:32	20	OK
CISCO_3550	Ping (cisco2)	17 April 2008, 00:48:32	20	OK
fat - роутер	Load Average (1 min)	17 April 2008, 00:48:34	60	0.44
fat - роутер	Number of Processes	17 April 2008, 00:48:26	60	167
fat - роутер	Number of Users	17 April 2008, 00:48:26	60	2
fat - роутер	Ping (fat)	17 April 2008, 00:48:34	20	OK
fat - роутер	Real Memory Available	17 April 2008, 00:48:33	40	(null)
fat - роутер	Swap Memory Available	17 April 2008, 00:48:30	40	99.9999 %
fat - роутер	System CPU Time	17 April 2008, 00:48:26	60	24245679
Flame Trac	Trac-server Status	17 April 2008, 00:48:47	1	OK
HP_3400cl	Ping (hp)	17 April 2008, 00:48:32	20	OK
HTTP-server	HTTP-server Status	17 April 2008, 00:48:42	10	OK
Порт1 (Cisco)	Port Status	17 April 2008, 00:48:24	30	OK
Порт1 (Cisco2)	Port Status	17 April 2008, 00:48:32	30	FAILED
Порт1 (HP)	Port Status	17 April 2008, 00:48:45	30	OK
Порт10 (Cisco)	Port Status	17 April 2008, 00:48:38	30	FAILED
Порт10 (Cisco2)	Port Status	17 April 2008, 00:48:43	30	FAILED
Порт10 (HP)	Port Status	17 April 2008, 00:48:21	30	FAILED
Порт11 (Cisco)	Port Status	17 April 2008, 00:48:38	30	FAILED
Порт8 (HP)	Port Status	17 April 2008, 00:49:16	30	OK
Порт9 (Cisco)	Port Status	17 April 2008, 00:48:54	30	OK
Порт9 (Cisco2)	Port Status	17 April 2008, 00:49:15	30	OK
Порт9 (HP)	Port Status	17 April 2008, 00:49:16	30	FAILED
Mail-сервер НИИ Механики	Mail-server Status	17 April 2008, 00:49:08	10	Service is unavaliable

частота обновления:

сортировать по:

имя узла:

имя запроса:

время обновления:

17 April 2008, 00:49:18 MSD, Thursday

Веб-клиент, список событий



Список событий

узел	время	событие	статус
Порт17 (Cisco)	16 April 2008, 23:45:24	From FLAME_KERNEL (FAILED)	FAILED
Порт18 (Cisco)	16 April 2008, 23:45:24	From FLAME_KERNEL (OK)	OK
Порт8 (Cisco2)	16 April 2008, 23:45:24	From FLAME_KERNEL (FAILED)	FAILED
Порт15 (Cisco)	16 April 2008, 23:45:24	From FLAME_KERNEL (OK)	OK
Порт5 (Cisco2)	16 April 2008, 23:45:23	From FLAME_KERNEL (OK)	OK
Порт4 (Cisco2)	16 April 2008, 23:45:23	From FLAME_KERNEL (FAILED)	FAILED
Порт14 (Cisco)	16 April 2008, 23:45:23	From FLAME_KERNEL (FAILED)	FAILED
Порт3 (Cisco2)	16 April 2008, 23:45:22	From FLAME_KERNEL (OK)	OK
Порт12 (Cisco)	16 April 2008, 23:45:21	From FLAME_KERNEL (OK)	OK
Порт2 (Cisco2)	16 April 2008, 23:45:20	From FLAME_KERNEL (FAILED)	FAILED
Порт11 (Cisco)	16 April 2008, 23:45:20	From FLAME_KERNEL (FAILED)	FAILED
Порт6 (Cisco)	16 April 2008, 23:45:20	From FLAME_KERNEL (OK)	OK
Порт13 (Cisco)	16 April 2008, 23:45:20	From FLAME_KERNEL (OK)	OK
Порт10 (Cisco)	16 April 2008, 23:45:20	From FLAME_KERNEL (FAILED)	FAILED
Порт1 (Cisco2)	16 April 2008, 23:45:20	From FLAME_KERNEL (FAILED)	FAILED
Порт5 (Cisco)	16 April 2008, 23:45:16	From FLAME_KERNEL (OK)	OK
Порт9 (Cisco)	16 April 2008, 23:45:15	From FLAME_KERNEL (OK)	OK
Порт8 (Cisco)	16 April 2008, 23:45:15	From FLAME_KERNEL (FAILED)	FAILED
Порт7 (Cisco)	16 April 2008, 23:45:11	From FLAME_KERNEL (FAILED)	FAILED
Порт4 (Cisco)	16 April 2008, 23:45:11	From FLAME_KERNEL (OK)	OK

время начала: время окончания:

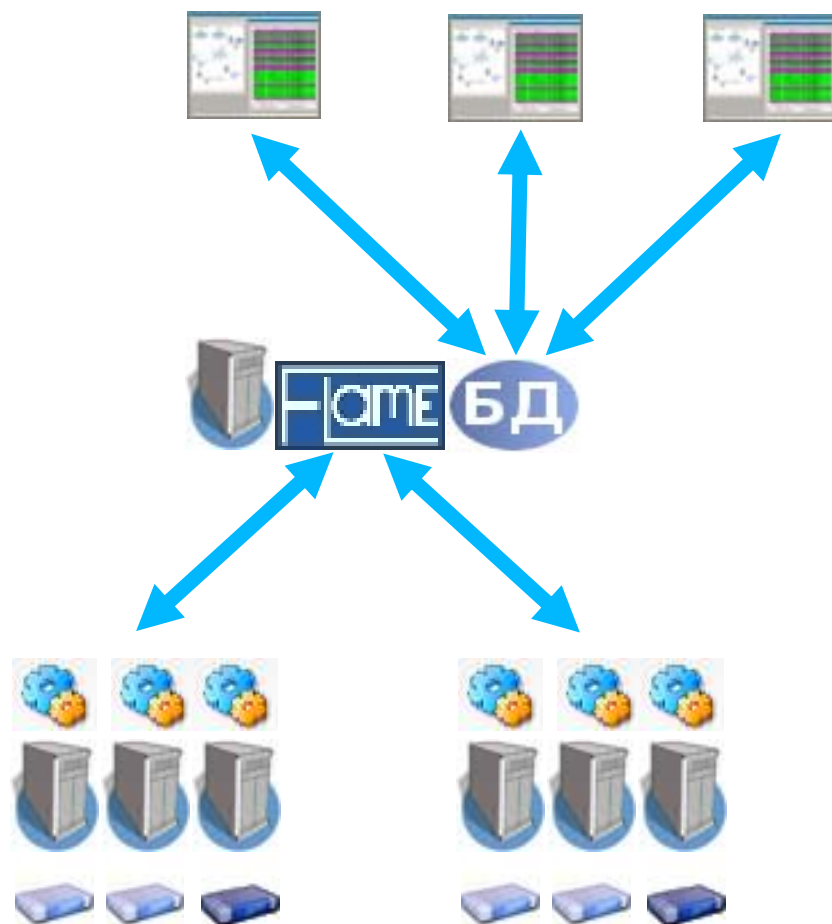
частота обновления: показывать событий:

имя узла:

уровень критичности: Normal Notice Warning Error Fatal

время обновления: 17 April 2008, 00:57:47 MSD, Thursday

Подходы к построению распределенного мониторинга



Классическая центральная
схема опроса двух
подконтрольных объектов.

Одна серверная часть FLAME
обращается через сеть к
каждому объекту и сохраняет
информацию в единой базе
данных.

Подходы к построению распределенного мониторинга

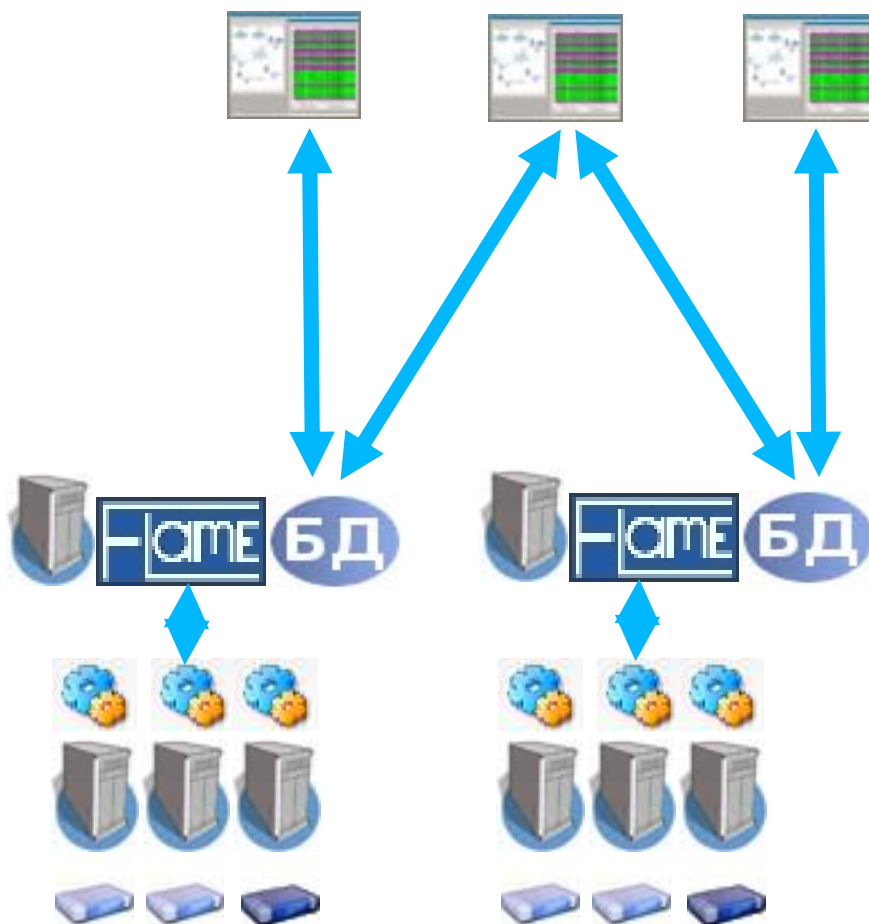
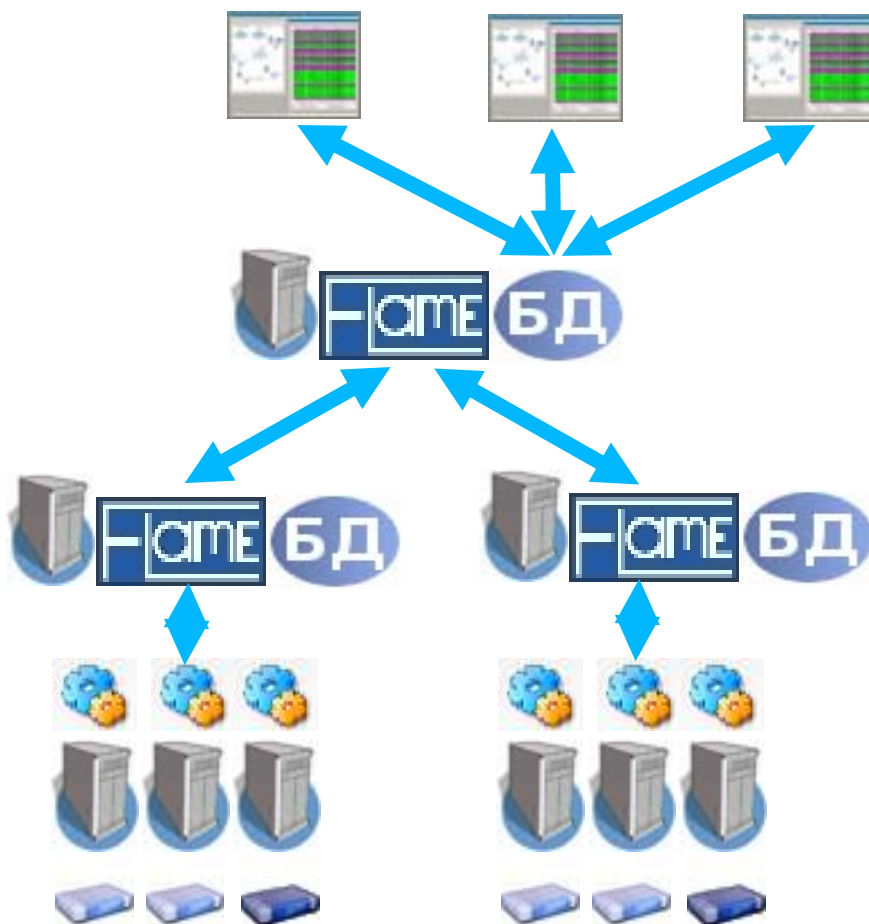


Схема опроса с двумя независимыми серверными частями **FLAME**.

Каждая серверная часть **FLAME** расположена в непосредственной близости к контролируемому объекту.

Собранная системой мониторинга информация поступает на общую консоль.

Подходы к построению распределенного мониторинга



Иерархическая схема опроса со взаимодействующими серверными частями **FLAME**.

Серверные части FLAME нижнего уровня расположены в непосредственной близости к контролируемым объектам.

Серверная часть FLAME верхнего уровня взаимодействует с ними запрашивая и получая необходимую информацию: значения вычисленных параметров, списки событий.

Возможные реализации взаимодействия серверных частей FLAME



Непосредственное взаимодействие серверных частей по специальному протоколу.



Потребуется разработки протокола взаимодействия и реализации соответствующего модуля серверной части.



Взаимодействие модуля ядра серверной части со специализированным **SNMP**-агентом.



Потребуется разработки и реализации SNMP-агента. Например, с помощью расширения агента snmpd пакета net-snmp.



Взаимодействие модуля ядра серверной части с веб-сервисом.



Потребуется разработки и реализации специализированных веб-сервисов.