Сетевое управление и мониторинг

Введение в сетевое управление и мониторинг

Часть I: Обзор

Основные концепции:

- Что такое мониторинг сетей
- Что такое сетевое управление
- Начинаем
- Зачем нужно сетевое управление
- Большая тройка
- Обнаружение атаки на сеть
- Документирование
- Обработка данных из разных источников
- Общее представление

Детали сетевого управления

Мы осуществляем мониторинг

- **Системы и сервисы**
  - Доступность, достижимость
- **Ресурсы**
  - Планирование расширения и развития, поддержка доступности
- **Производительность**
  - Время “туда и обратно”, пропускная способность
- **Изменения и конфигурирование**
  - Документирование, контроль версий, логи

Детали сетевого управления

Мы следим за

- **Статистикой**
  - В целях учета и выполнения измерений
- **Ошибками (обнаружение вторжения)**
  - Обнаружение проблем
  - Устранение проблем и отслеживание истории проблем
- Для этого полезны системы отслеживания ошибок
  - “Справочные столы” удобны для внесения, модификации, и разрешения проблем, и для коммуникации между вашими сотрудниками и конечными пользователями – используя систему отслеживания ошибок.

Ожидания

Работающая сеть должна мониториться с целью:

- Соблюдение ожидаемых *SLA (соглашений об уровне сервиса)*
- SLA зависят от установленных правил
  - Чего ожидает ваше руководство?
  - Чего ожидают ваши пользователи?
  - Чего ожидают ваши клиенты?
  - Чего ожидает весь остальной Интернет?
- Что такое “достаточно”? 99.999% доступности?
  - 100% доступность недостижима (как мы увидим) →

Ожидания “доступности”

Что означает доступность 99.9 %?

30.5 дней x 24 часа = 732 часов в месяце

(732– (732 x .999)) x 60 = 44 минуты

всего лишь 44 минуты недоступности в месяц!

Нужно отключать систему 1 час в неделю?

(732 – 4) / 732x 100 = 99.4 %

Не забудьте учесть запланированное обслуживание в ваших расчетах, и дайте знать вашим пользователям и клиентам о том, включено ли время запланированного обслуживания в соглашение об уровне сервиса

Как измеряется доступность?

В базовой сети? Между абонентами? Из Интернет?

Определение базового уровня

Какова норма для вашей сети?

Если вы никогда не собирали статистику и не осуществляли мониторинг сети, вам нужно знать следующее:

- Типичная загрузка канала (➔ Cacti)
- Изменения времени задержки пакетов (➔ Smokeping)
- Типичная загрузка ресурсов в процентах
- Типичные уровни “шума”:
  - Сканирование сети
  - Потери данных
  - Отслеженные ошибки и проблемы

Зачем все это нужно?

Знать, когда пора делать модернизацию

- Слишком низкая пропускная способность?
- Куда идет ваш трафик?
- Нужна ли линия побыстрее, или несколько провайдеров?
- Устаревшее оборудование?

Вести учет изменений

- Учитывайте все изменения
- Проще найти проблемы, возникшие вследствие модернизаций либо изменений конфигурации

Хранить операционную историю

- Использование системы отслеживания ошибок дает возможность хранить историю происшедших событий.
- Позволит вам защитить себя и в любой момент проверить, что происходило в прошлом

Зачем нужно сетевое управление?

Учет

- Отслеживание использования ресурсов
- Клиенты платят за использование

Своевременно находите проблемы

- Узнавайте о проблемах прежде ваших клиентов; плюс к репутации
- Системы мониторинга автоматически информируют персонал о проблемах.

Тенденции

- Используйте собранную информацию для предсказания тенденций в ваших сетях
- Определение базового уровня, планирование загрузки и обнаружение атак на сеть

“Большая тройка”?

Доступность

- Nagios Сервисы, серверы, роутеры, коммутаторы

Надежность

- Smokeping Состояние соединения, время “туда и обратно”, время отклика, задержка

Производительность

- Cacti Общий трафик, использование портов, процессора, памяти, диска, процессов

Эти программы имеют частично перекрывающиеся функции

Обнаружение атаки

- Отслеживание тенденций и автоматизация позволяют вам узнавать, что вашу сеть атакуют.
- Инструментарий может помочь смягчить последствия атаки:
  - Потоки данных сквозь сетевые интерфейсы
  - Загрузка определенных сервисов и/или серверов
  - Множественные отказы сервиса

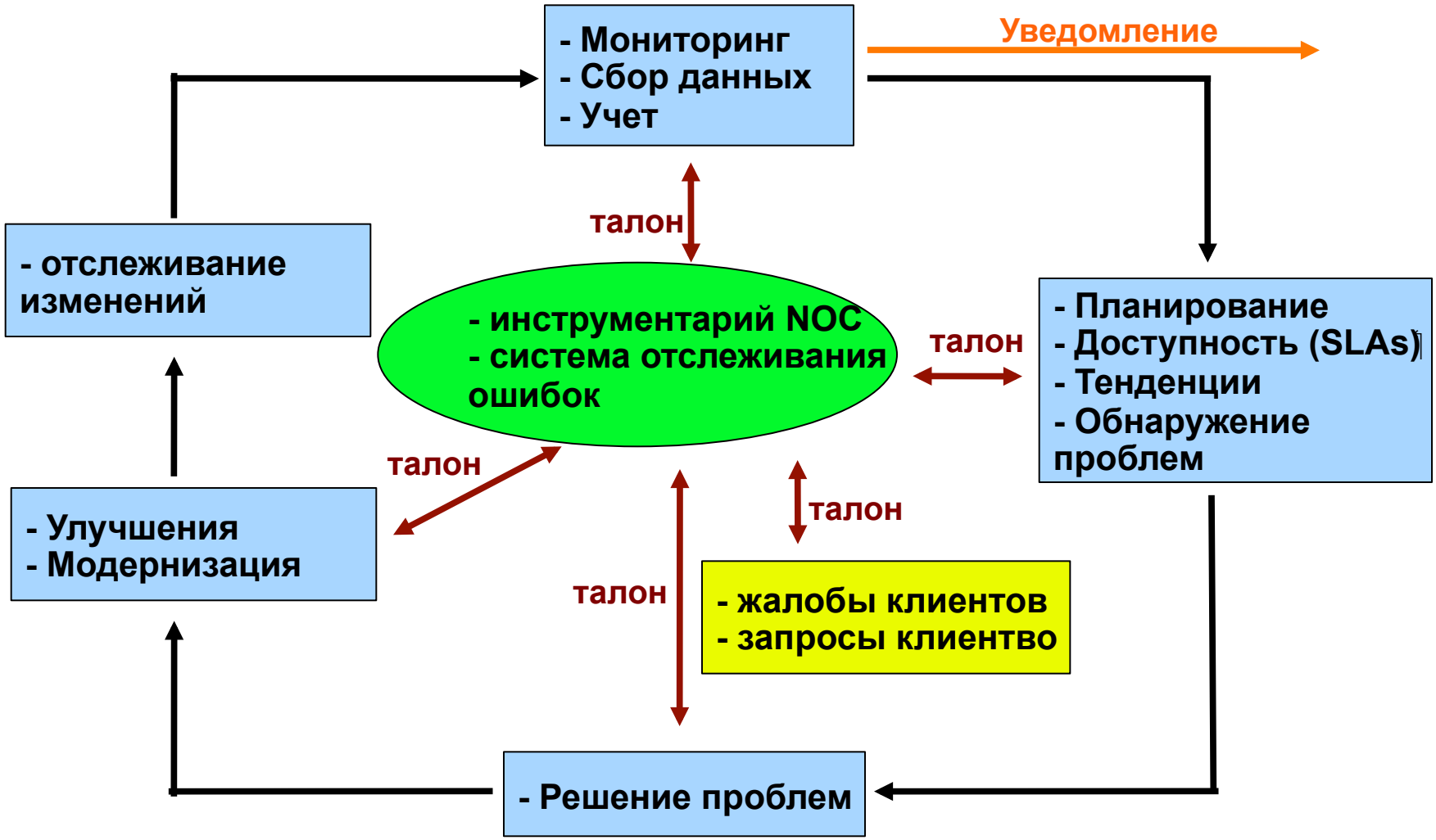
Консолидация данных

Сетевой операционный центр (NOC)

“центр всего”

- Координирование задач
- Статус сети и сервисов
- Выезд на место возникновения проблемы или сообщения о проблеме
- Где находится инструментарий (”сервер NOC”)
- Документация:
  - Сетевые диаграммы
  - База данных (или просто файл) с информация о каждом порте на каждом свиче
  - Описание сети
  - И многое другое, как мы убедимся в дальнейшем

Общая картина



Некоторые решения с открытым исходным кодом…

Производительность

- Cricket
- IFPFM
- flowc
- mrtg*
- NetFlow*
- NfSen*
- ntop
- perfSONAR
- pmacct
- RRDtool*
- SmokePing*

Отслеживание ошибок

- RT*
- Trac*
- Redmine

Отслеживание изменений

- Mercurial
- Rancid* (routers)
- CVS*
- Subversion*
- git*

Безопасность

- Nessus
- OSSEC
- Prelude
- Samhain
- SNORT
- Untangle

Работа с логами

- swatch*
- syslog-ng/rsyslog*
- tenshi*

Сетевое управление

- Big Brother
- Cacti*
- Hyperic
- Munin
- Nagios*
- OpenNMS*
- Observium*
- Sysmon
- Zabbix

Документирование

- IPplan
- Netdisco
- Netdot*
- Rack Table

Протоколы/утилиты

- SNMP*, Perl, ping

Вопросы?

?

Часть II: Подробности

Основные понятия - подробности:

- Документирование сети, продолжение
- Диагностические инструменты
- Инструменты для мониторинга
- Средства анализа производительности
- Активный и пассивный инструментарий
- SNMP
- Системы отслеживания ошибок
- Отслеживание изменений

Вопросы?

?

Часть III: Подробности

Основные понятия - подробности:

- Диагностические инструменты
- Инструменты для мониторинга
- Средства анализа производительности
- Активный и пассивный инструментарий
- SNMP
- Системы отслеживания ошибок
- Отслеживание изменений

Системы и инструменты сетевого мониторинга

Три вида инструментов

1. **Диагностические инструменты** – используются для проверки соединения либо сетевой доступности устройства – обычно активные инструменты
2. **Инструменты мониторинга** – программы, выполняющиеся в фоновом режиме (”демоны” или сервисы), воспринимающие различные события – но также могут инициировать активное зондирование при использовании диагностических инструментов – и сохраняющие эту информацию по расписанию.
3. **Инструменты для измерения производительности** – показывают нам, как сеть справляется с нагрузкой.

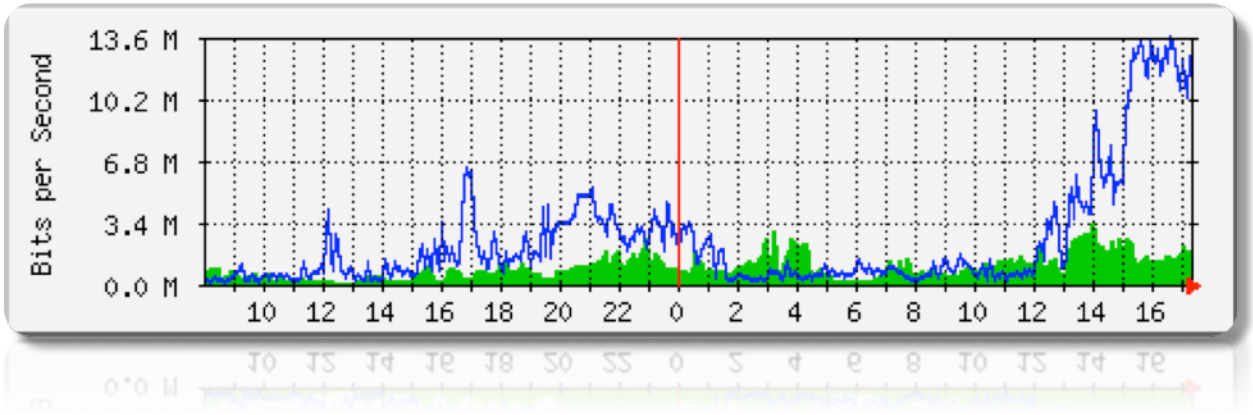
Системы и инструменты сетевого мониторинга

3. Измерение производительности

Важно отслеживать все интерфейсы на роутере (обычно не требуется отслеживать порты на коммутаторах).

Две часто используемые программы:

- Netflow/NfSen: http://nfsen.sourceforge.net/
- MRTG: http://oss.oetiker.ch/mrtg/



MRTG = “Multi Router Traffic Grapher”

Системы и инструменты сетевого мониторинга

Активные инструменты

- Ping – проверить соединение с узлом сети
- Traceroute – показывает путь к сетевому узлу
- MTR – ping + traceroute вместе
- Коллектор SNMP (опрашивание)

Пассивные инструменты

- Мониторинг логов, коллектор SNMP-прерываний, NetFlow

Автоматизированные инструменты

- SmokePing – сохраняет и строит графики времени ожидания набора сетевых узлов используя ICMP (ping) или другие протоколы
- MRTG/RRD – периодически сохраняет и строит графики использования пропускной способности портов и каналов связи

Системы и инструменты сетевого мониторинга

Инструменты мониторинга сетей и сервисов

- Nagios – мониторинг серверов и сервисов
  - Может осуществлять мониторинг практически чего угодно
  - HTTP, SMTP, DNS, свободное место на диске, загрузку процессора, ...
  - Легко создавать новые модули-расширения
- Для создания простых инструментов мониторинга требуются базовые навыки написания скриптов, например на Perl, php, shell и т.д.
- Много хороших разработок с открытыми кодом
  - Zabbix, ZenOSS, Hyperic, OpenNMS ...

Пользуйтесь ими для мониторинга доступности и времени задержки в вашей сети

- Очень полезны механизмы отслеживания зависимостей предок/потомок!

Системы и инструменты сетевого мониторинга

Осуществляйте мониторинг критических сервисов сети

- DNS/Web/Email
- Radius/LDAP/SQL
- SSH на роутеры

Как вы узнаете о проблеме?

Не забудьте про логи!

- Каждое сетевое устройство (а также UNIX и Windows серверы) может сообщать о системных событиях используя syslog
- Вы **ДОЛЖНЫ сохранять** и **осуществлять мониторинг** логов!
- Невыполнение этого является одной из самых часто встречающихся ошибок в сетевом мониторинге

Протоколы сетевого управления

SNMP – “простой протокол сетевого управления”

- Стандарт, сотни инструментов его использующих
- Поддреживается любыми хорошими сетевыми устройствами
  - → Пропускная способность, ошибки, загрузка процессора, температура, ...
- Также поддерживается UNIX и Windows
  - → Свободное место на диске, активные процессы, ...

SSH и telnet

- Можно написать скрипты для автоматизации мониторинга узлов и сервисов

SNMP инструменты

Набор инструментов Net SNMP

- http://net-snmp.sourceforge.net/

Подходит для создания простых инструментов

- Узнать, какой IP адрес используется каким мак-адресом
- Узнать, какие мак-адресы на каком порту на каком коммутаторе
- Запросить состояние удаленного RAID-массива
- Узнать температуру сервера, коммутатора, роутера
- И т.д…

Инструменты для сбора статистики и учета

Учет и анализ трафика

- Для чего и насколько используется ваша сеть
- Полезно для качества обслуживания (QoS), определения злоупотреблений, и биллинга (“оплата по счетчику”)
- Специальный протокол: NetFlow
- Идентификация потоков трафика: протокол, источник, место назначения, сколько байт
- Существуют различные программы для обработки этой информации
  - Flowtools, flowc
  - NFSen
  - Многие другие: http://www.networkuptime.com/tools/netflow/

Управление ошибками

Временная проблема?

- Перегрузка, временная нехватка ресурсов

Постоянная проблема?

- Дефект оборудования, отсутствие соединения

Как обнаруживать ошибки?

- Мониторинг!
- Жалобы клиентов

Система отслеживания ошибок необходима

- Создание “тикета” для отслеживания события (запланированного или нет)
- Определение правил диспетчеризации и эксалации
  - Кто обработает ошибку?
  - Кто станет ее обрабатывать если все заняты?

Системы отслеживания ошибок

Почему они важны?

- Отслеживать все события, аварии и проблемы

Точка фокуса для всей коммуникации службы техподдержки

Используйте ее для отслеживания всей коммуникации

- В пределах организации и за ее пределами

События за пределами организации:

- Жалобы клиентов

События в пределах организации:

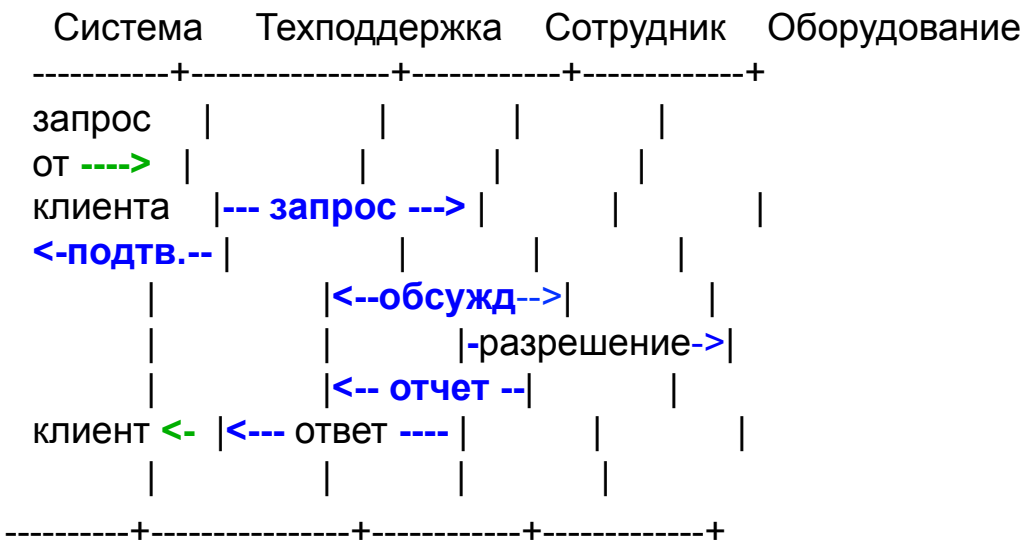
- Аварии систем (прямые и непрямые)
- Запланированное обслуживание и обновления – не забудьте проинформаировать клиентов!

Системы отслеживания ошибок

- Используйте систему отслеживания ошибок для отслеживания каждого события, включая общение технического персонала внутри организации
- Каждое событие получает свой номер
- Каждое событие проходит примерно следующие этапы:
  - Новое
  - Открытое
  - ...
  - Решенное
  - Закрытое

Системы отслеживания ошибок

Рабочий процесс:



Системы отслеживания ошибок: примеры

rt (request tracker)

- Широко используется во всем мире
- Классическая система, может быть настроена для ваших нужд
- Довольно сложна в установе и настройке
- Поддерживает работу крупного масштаба

trac

- Гибридная система, включает wiki и возможности управления проектами
- Отслеживание ошибок не настолько надежно как в rt, но тем не менее работает нормально
- Часто используется для отслеживания групповых проектов

redmine

- Похожа на trac, но более надежна. Установка более сложная

Сетевые системы обнаружения вторжений (NIDS)

Это системы, следящие за трафиком в вашей сети и сообщающие о проблемах определенных типов, таких как:

- Инфицированные машины в сети либо машины, используемые спамерами

Некоторые программы:

- **SNORT** – часто используемая система с открытыми исходными текстами
  http://www.snort.org/
- **Prelude –** Система управления информационной безопасностью
  https://dev.prelude-technologies.com/
- **Samhain –** Централизованная NIDS
  http://la-samhna.de/samhain/
- **Nessus** – сканирование уязвимостей:
  http://www.nessus.org/download/

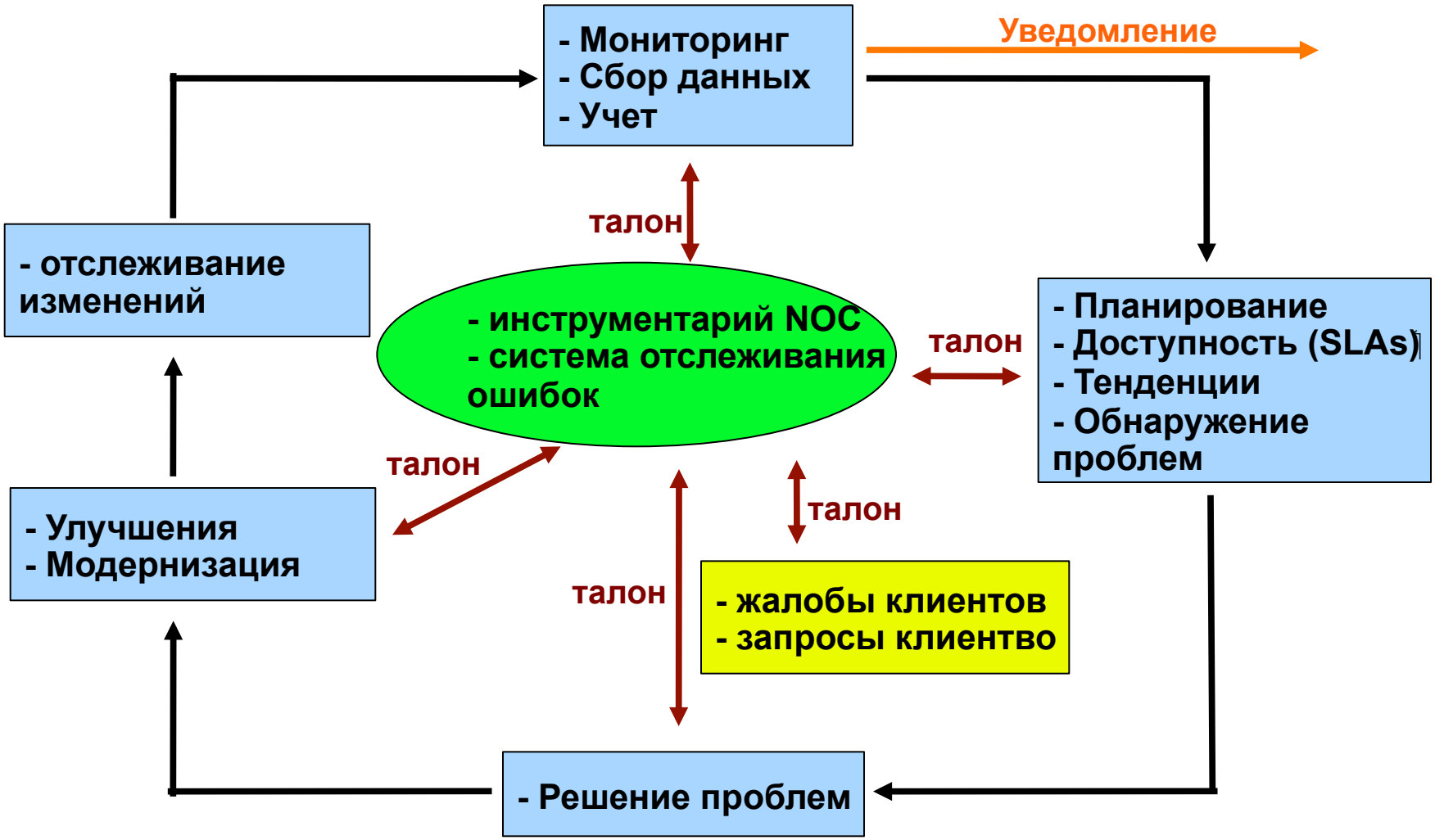
Сетевое управление и мониторинг

- Сохраняйте изменения конфигурации оборудования в *системах контроля версий* (включая файлы конфигурации)
- Управление инвентарем (оборудование, IP адреса, интерфейсы)
- Используйте контроль версий
  - В самом простом случае:
    ”`cp named.conf named.conf.20070827-01`”
- Для текстовых файлов конфигурации:
  - **CVS, Subversion (SVN)**
  - **Mercurial**
- Для роутеров:
  - **RANCID**

Сетевое управление и мониторинг

- Традиционно используется для исходных текстов программ
- Хорошо работает с любыми текстовыми файлами
  - Также с двоичными файлами, но тяжелее видеть модификации
- Для сетевого оборудования:
  - **RANCID** (автоматическое скачивание и хранение конфигурации Cisco, поддерживаются другие типы оборудования)
- Встроенные возможности таких систем управления проектами, как:
  - **Trac**
  - **Redmine**
  - Многие wiki прекрасно подходят для документирования вашей сети

Общая картина, еще раз



Вопросы

?