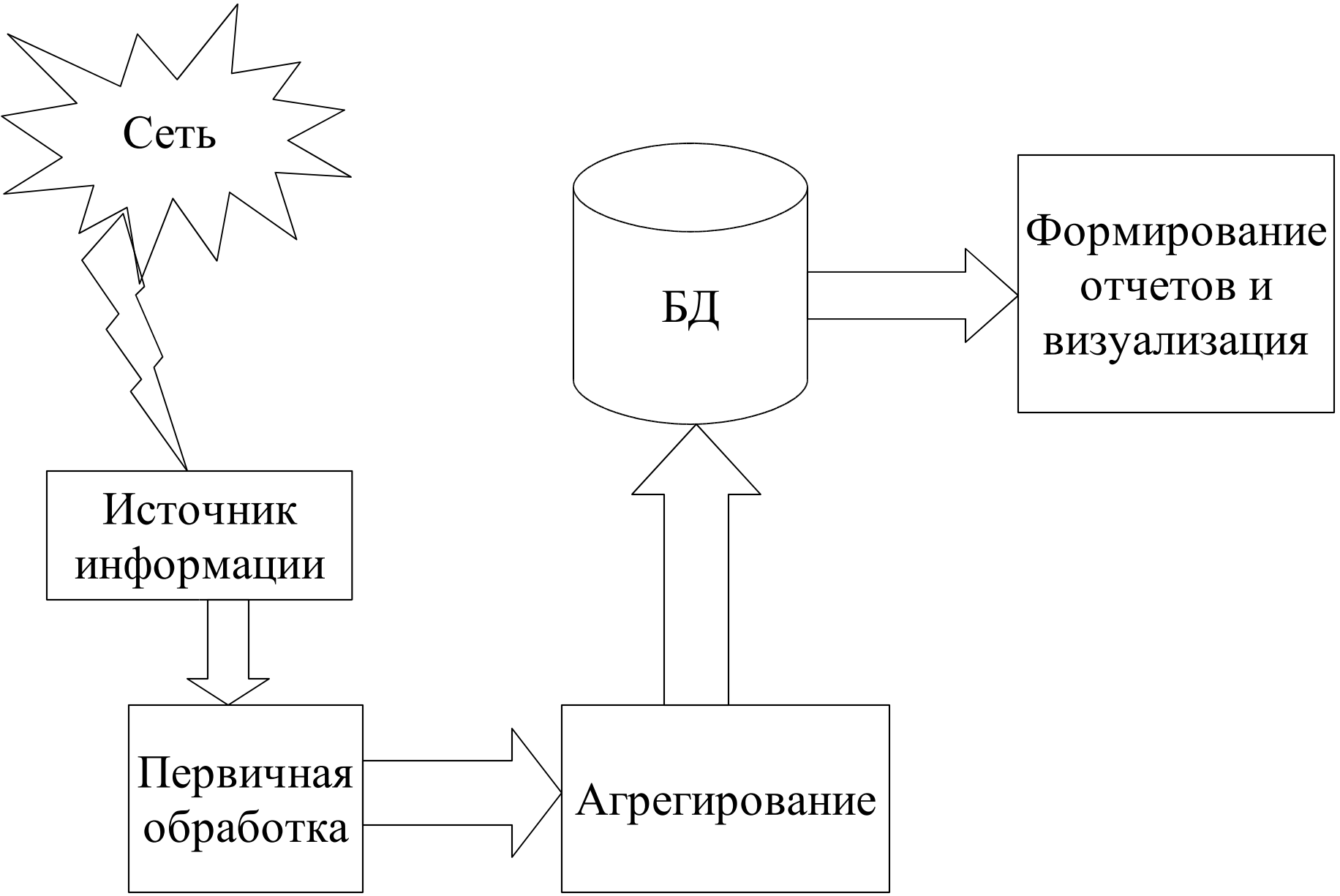
Методы анализа трафика

1. Целевой сбор информации
   - Tcpdump
   - Ethereal
   - Snort (различные IDS)
2. Фоновый сбор

Общая схема учета трафика



Источники информации

- Коммутаторы
- Маршрутизаторы
  - Cisco Netflow и accounting
  - Пакетные фильтры
  - Berkeley packet filter (libpcap)
  - divert
  - Ядерные модули

Коммутаторы

Достоинства:

- Малые накладные расходы
- Отдают информацию по SNMP и rsh (есть много утилит для обработки)

Недостатки:

- Обычно собирают информацию на уровне портов

Программы:

MRTG

Пакетные фильтры

Достоинства:

- Малые накладные расходы
- Невозможность прохода неучтенного трафика

Недостатки:

- Негибкость
- Ограниченный объем собираемой информации

Программы:

- IPSTAT (iptables)
- IPA (ipfw, ipf)
- ipcount (ipfw, ipf)

bpf (libpcap)

Достоинства:

- Возможность анализировать трафик, не проходящий через машину, где производится анализ
- Возможность задания фильтра для анализируемого трафика
- Кэширование данных в ядре и выдача на user level большими порциями

Недостатки:

- Работает в user level (накладные расходы на переключение контекстов)
- Возможны переполнения буферов и потери информации

Программы:

- bpft (trafd)
- ipcad

divert

Достоинства:

- Возможна конфигурация, когда выход из строя счетчика обеспечивает невозможность прохождения трафика
- Возможна очень гибкая настройка критериев анализа
- Можно написать счетчик так, что при корректном завершении работы не будет потерь информации

Недостатки:

- Работает в user level (накладные расходы на переключение контекстов для каждого пакета)

Программы:

- ipacctd

Ядерные модули

Достоинства:

- Малые накладные расходы

Недостатки:

- Занимает память ядра
- При ошибках рушит всю систему (ядро сложнее отлаживать)

Программы:

- ng_ipaact
- ipacc (патч к ядру FreeBSD)

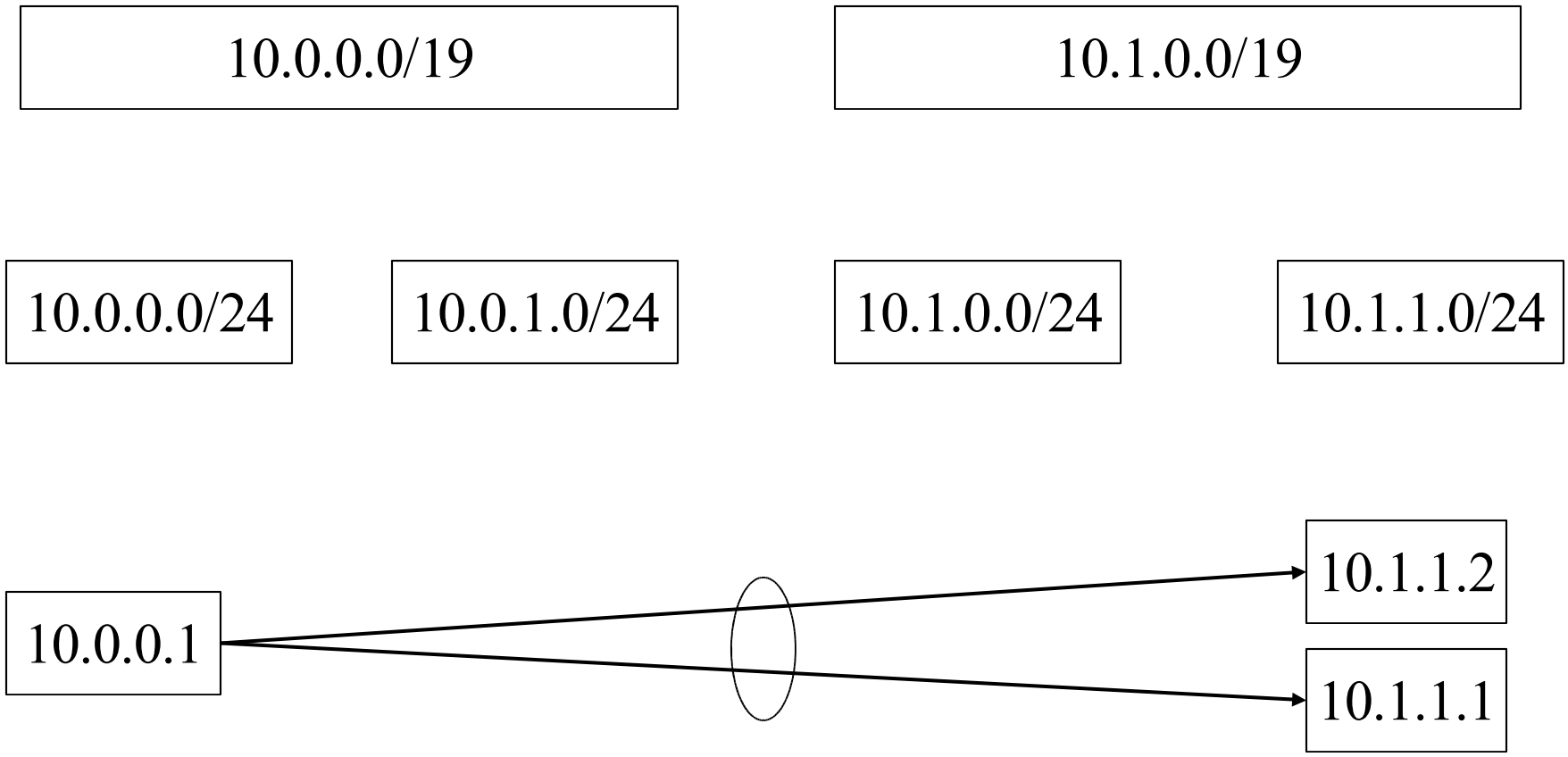
На что обратить внимание

- Есть ли checkpoint
- Как поведет себя при перезагрузке (не потеряются ли данные)
- Есть ли поддержка квот (умеет ли сам отключать адреса)
- В каком виде выдает данные (сам кладет в БД или нужно писать обвязку.

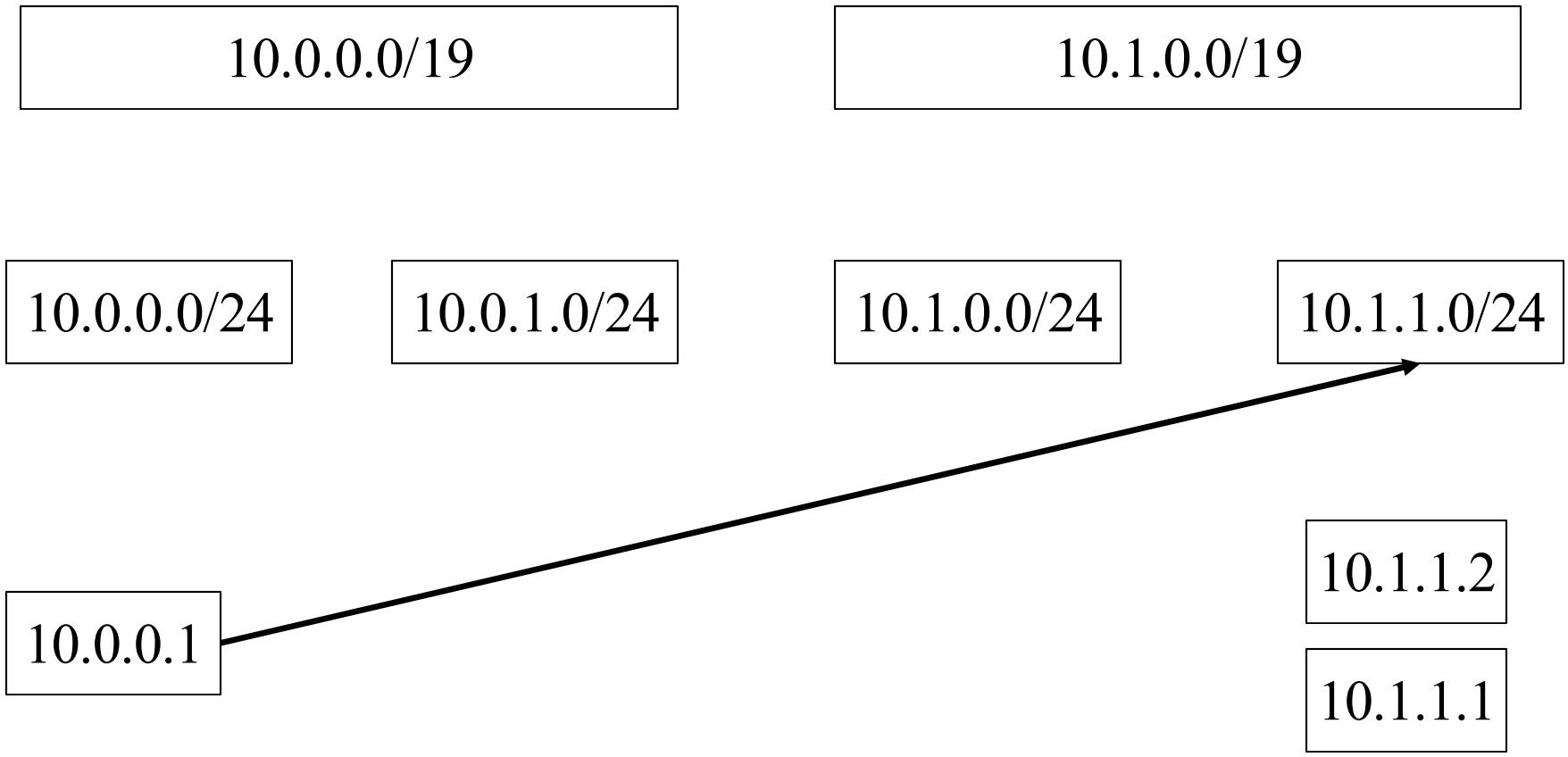
Агрегирование

- Первичная
- По времени
- Входящий и исходящий
- Классы трафика (внутренний и зарубежный)
- Адаптивное

Адаптивное агрегирование



Адаптивное агрегирование



Как информацию хранить

- Текстовый файл
  - Легко запихивать в хранилище
  - Не требует спец. софта (awk и perl обычно есть)
  - Эффективен в обработке
  - Для каждого нового отчета требуется писать новый скрипт.
- СУБД
  - Нужна сама СУБД
  - Нужна обвязка для запихивания
  - Медленнее в обработке
  - Гибкость, быстрота генерации новых видов отчетов
- Специальные БД

Выдача информации

- Разделение доступа.
  - Завести пользователей в БД или ходить к внешнему аутентикатору, но права хранить в базе.
  - Делать единую базу (LDAP?)
- Выдача в удобном виде
  - Табличка
  - MRTG
  - RRD tools
  - Графические библиотеки.