МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)

«Классификация сетевых подсистем мониторинга ядра ОС Linux»

Студент: Мансуров Владислав Михайлович

Группа: ИУ7-56Б

Руководитель: Оленев Антон Александрович

Цели и задачи

Целью работы является провести анализ существующих средств мониторинга сетевой подсистемы ядра ОС Linux.

Задачи:

- провести анализ сетевой подсистемы ядра ОС Linux;
- провести обзор существующих подсистем и средств сетевого мониторинга ядра ОС Linux;
- сформулировать критерии сравнения средств сетевого мониторинга ядра ОС Linux;
- классифицировать существующие подсистемы и средства сетевого мониторинга.

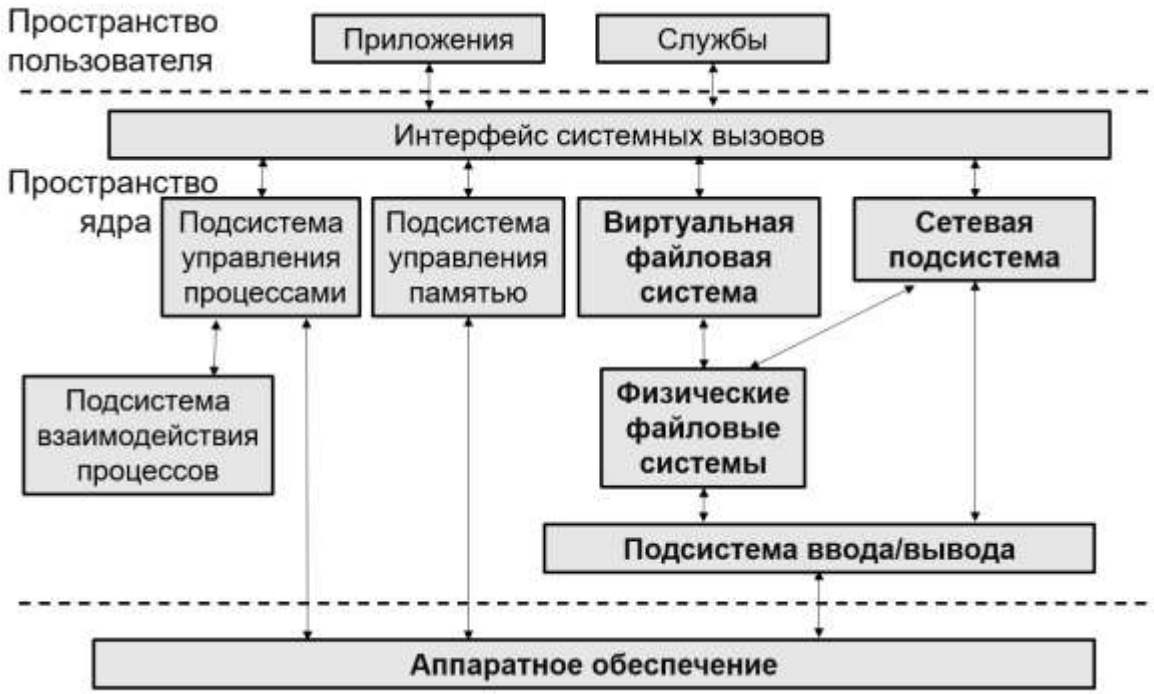
Ядро Linux

Ядро Linux:

- основной внутренний компонент
- монолитное

Задачи:

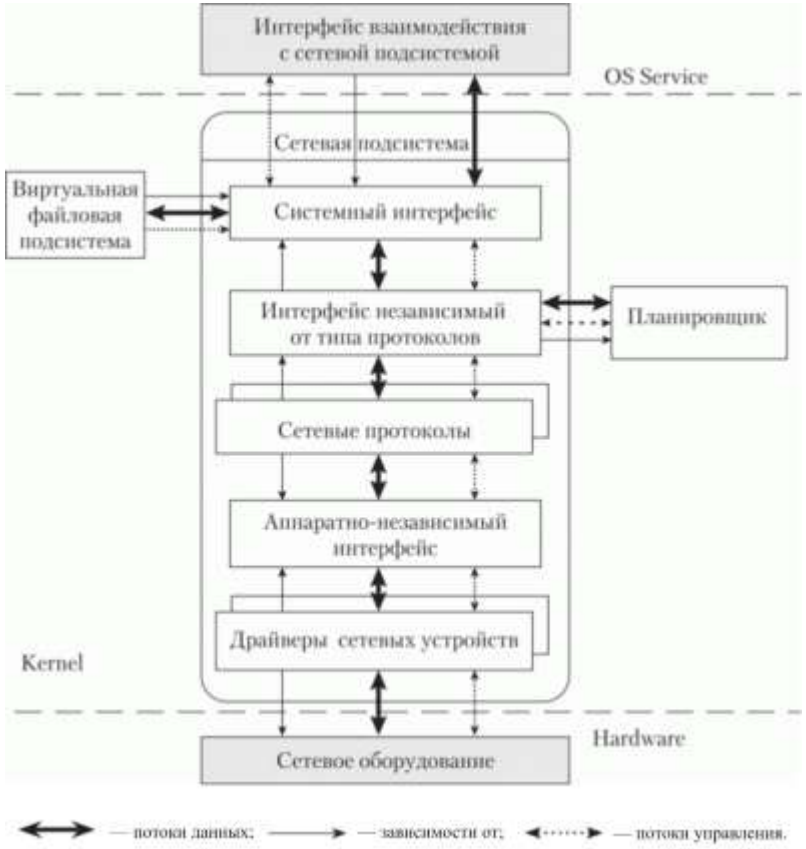
- взаимодействие с аппаратными компонентами
- обслуживание приложение с низкоуровневыми элементами



Сетевая подсистема ядра Linux

Обеспечивает функциональность:

- поддержку взаимодействия процессов с помощью механизмов сокетов;
- реализацию стеков сетевых протоколов;
- поддержку сетевых интерфейсов или драйверов;
- обеспечение маршрутизации пакетов;
- обеспечение фильтрации пакетов;



Сетевой мониторинг ядра Linux

Сетевой мониторинг ядра Linux — отслеживание пути пакетов и выявление наличие ошибок сетевых интерфейсов сетевой подсистемы, что относится к вмешательству в работу сетевой подсистемы.

Путем использования сетевого мониторинга можно выявить:

- проблемы производительности диска (хранилища);
- проблемы производительности памяти и процессора;
- узкие места в сети.

Обзор методов сетевого мониторинга ядра Linux

Утилиты сетевого мониторинга ядра

Преимущества:

- Гарантия работы без сбоев;
- Низкие накладные ресурсы;
- Работа при работающей системе;
- Независимость от версии ядра

Недостатки:

- Заточены под определенные задачи;

Обзор методов сетевого мониторинга ядра Linux

Модификация кода ядра

Преимущества:

- Универсальность;
- Скорость работы;

Недостатки:

- Риск нарушить работу системы;
- Сложность добавление кода в ядро Linux
- Перекомпиляция для каждого измененного или нового модуля

Обзор методов сетевого мониторинга ядра Linux

Зондирование ядра

Преимущества:

- Динамическая загрузка модулей ядра;
- Работа при работающей системе;
- Независимость от версии ядра, адаптируются только имена функций

Недостатки:

- Риск нарушить работы системы;
- Пересборка модулей при изменении фильтра
-

Обзор методов сетевого мониторинга ядра Linux

Точки трассировки

Преимущества:

- Стабильный интерфейс;
- Низкие расход ресурсов;
- Точки трассировки запускаются при необходимости

Недостатки:

- Если точка трассировки добавлена ее нельзя убрать или переместить;
- Минимальное количество или необходимость вести учет точек трассировки.

Обзор методов сетевого мониторинга ядра Linux

Function Trace

Преимущества:

- Не требует изменение и добавления кода в ядро Linux;
- Независимость от версии сборки ядра.

Недостатки:

- Ухудшается универсальность решаемость задач;
- Невозможность добавления новых модулей

Обзор методов сетевого мониторинга ядра Linux

Extended Berkeley Packet Filter

Преимущества:

- Модификация кода сопровождается проверка до внесения в ядро Linux;
- Динамическая или статическая загрузка;
- Поддержка высокоуровневых языков
- Поддержка JIT компилятора

Недостатки:

- Новая развивающая технология;
- Ограниченность
- Проблема с безопасностью, но риск нарушить работу систему минимален

Классификация сетевых подсистем мониторинга ядра Linux

Критерии сравнения методов сетевого мониторинга

Критерии	Описание
Производительность	Работа при реальной нагрузки и низкие расход системных ресурсов
Безопасность	Наличие гарантии, что внесенный код не вызовет сбой системы или нет необходимости к внедрению написанного кода
Скорость разработки	Быстрота разработки программ для сетевого мониторинга
Работоспособность	Запуск на работающей системе без сбоев или требования перезапуска
Гибкость	Возможность выполнить любые поставленные задачи
Независимость	Независимость от сборки ядра
Простота развертывания	Насколько сложно развертывать средства мониторинга на машине и сопровождением документации

Классификация сетевых подсистем мониторинга ядра Linux

Критерий	Модификация кода ядра	Утилиты	kprobes	tracepoint	ftrace	BPF/eBPF
Производительность	✓/✗	✓	✓/✗	✓	✓	✓
Безопасность	✗	✓	✓/✗	✓/✗	✓	✓
Скорость разработки	✗	—	✗	✓	—	✓
Работоспособность	✗	✓	✓/✗	✓/✗	✓	✓
Гибкость	✗	✗	✓	✓	✗	✗
Независимость	✗	✓/✗	✓/✗	✓	✓	✓
Простота развертывания	✓	✓	✓/✗	✓/✗	✗	✓

Заключение

В ходе данной работы были изучены:

- структура и принципы работы сетевой подсистемы ядра Linux;
- методы сетевого мониторинга ядра Linux или средства и подсистемы мониторинга сетевой подсистемы ядра Linux;
- критерии сравнения методов сетевого мониторинга;
- принципы работы методов касательно сетевой подсистемы;
- преимущества и недостатки каждого из методов.

Были сформирована критерии классификации методов сетевого мониторинга ядра Linux. Была проведена классификация методов сетевого мониторинга ядра Linux по критериям, сформированным в ходе работы.