Базовая диагностика неполадок

Содержание модуля

1. Возможные сетевые неполадки
2. Инструменты диагностики

Возможные сетевые неполадки

1

Базовые принципы диагностики и решения инцидентов

Надежность, доступность и удобство обслуживания сети является критичным фактором работы любой организации.

Для того чтобы обеспечить работоспособность, помимо избыточности ресурсов, необходимо уметь диагностировать и решать сетевые проблемы.

Сетевые инциденты должны быстро обнаруживаться, а их последствия быстро устраняться.

Базовые принципы диагностики и решения инцидентов

Инцидент —
Незапланированное прерывание ИТ услуги или ухудшение качества ее предоставления

Базовые принципы диагностики и решения инцидентов

Инцидент → **Диагностика** → **Решение**

Диагностика

Принципы диагностики

- Соберите информацию
- Проанализируйте
- Устраните
- Проверьте сопутствующие компоненты
- Протестируйте

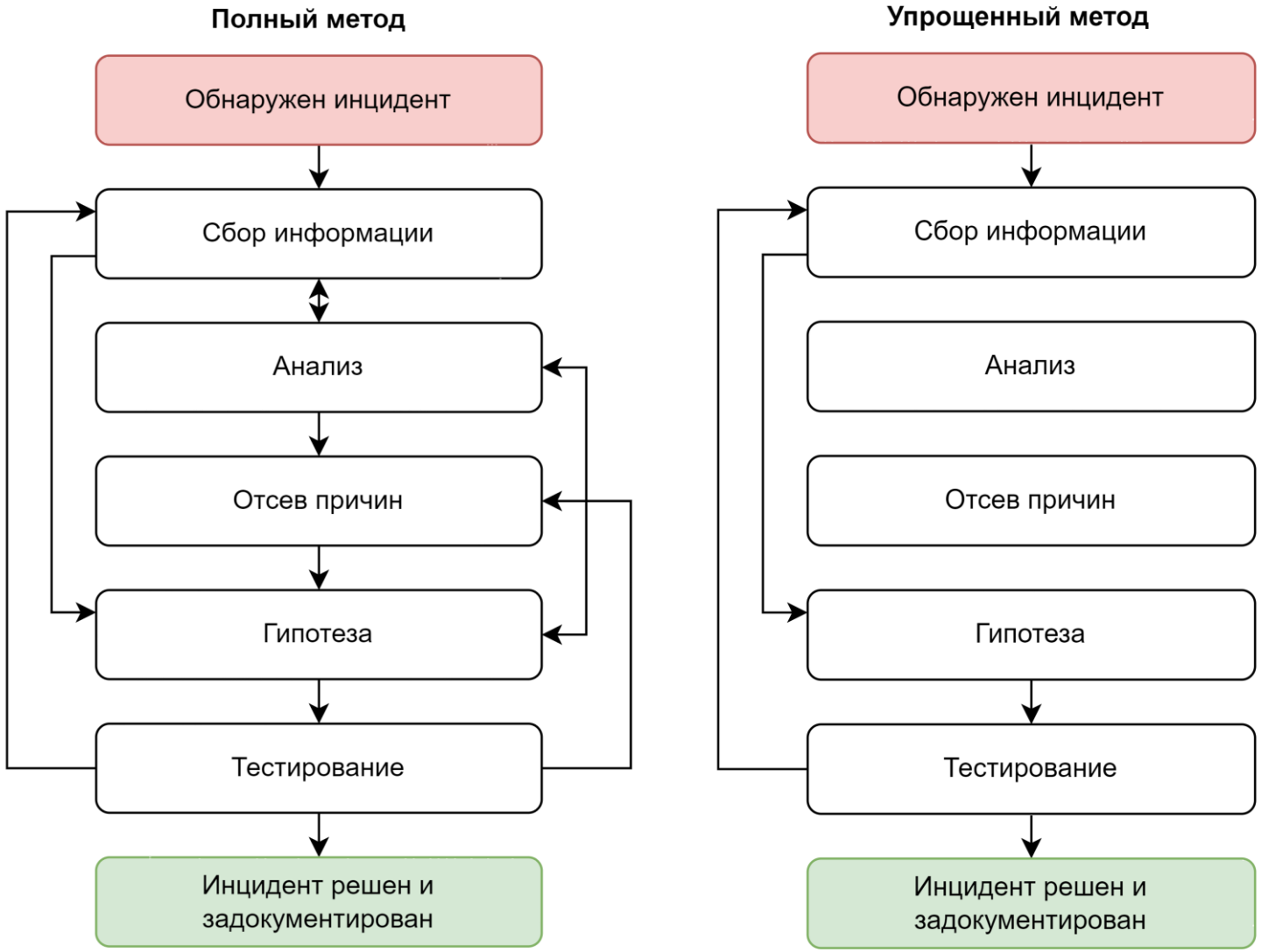
Сетевые инциденты

Симптомы

- Сетевая недоступность
- Не разрешаются имена
- Плохое качество связи
- Потеря пакетов

Методы решения инцидентов

Различные методы решения инцидентов определяют как мы двигаемся через фазы решения инцидента

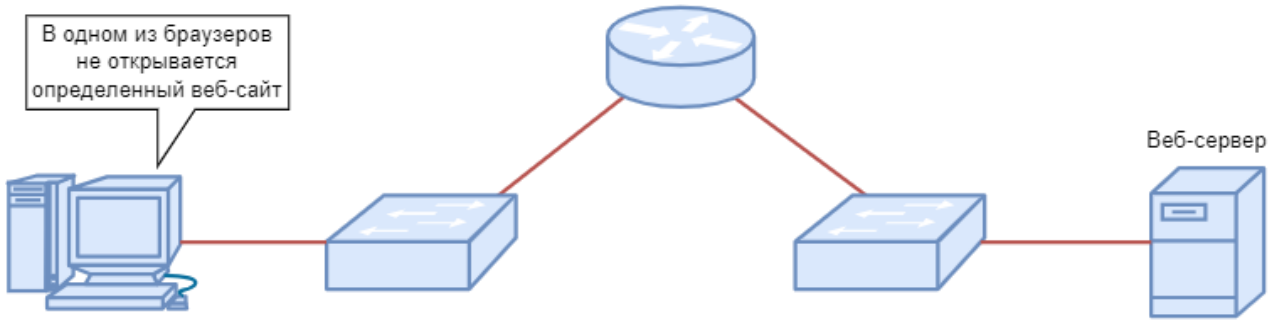


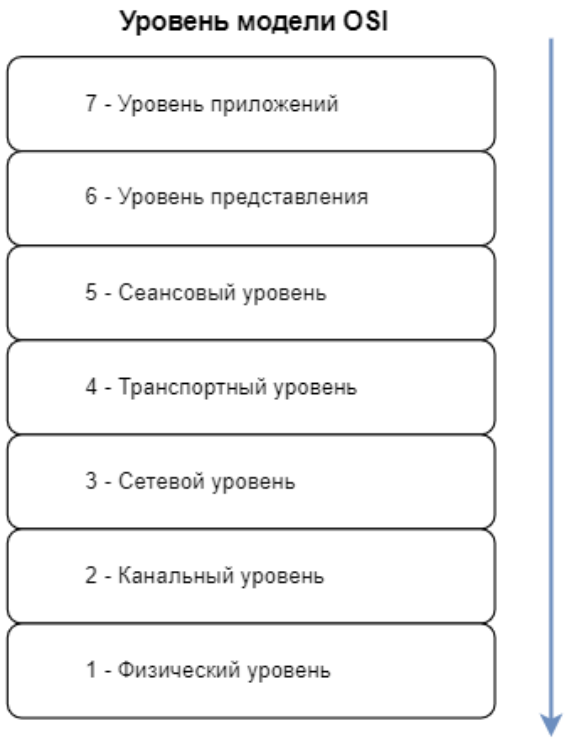
Решение инцидентов

Методы решения

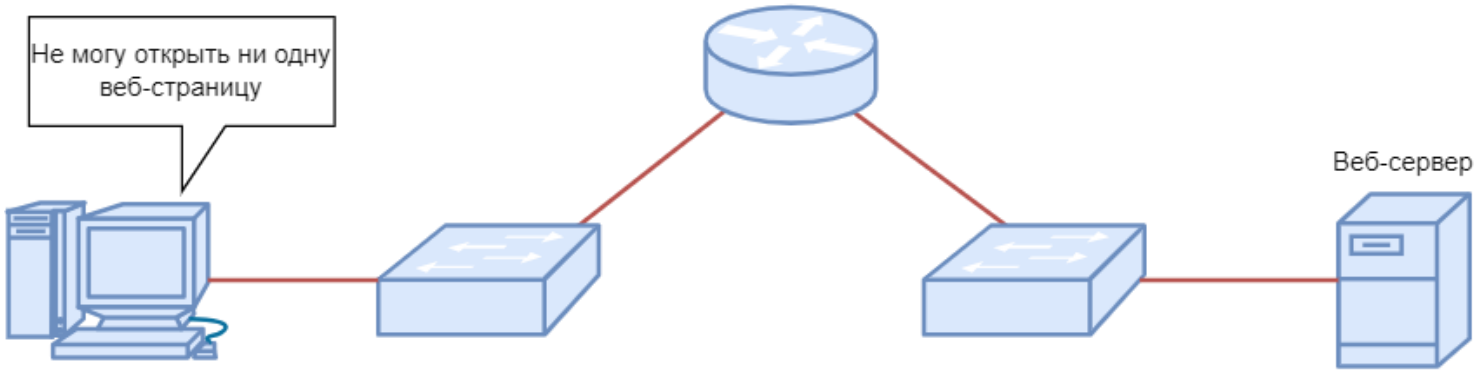
- Сверху вниз
- Снизу вверх
- Разделение
- Найди отличия
- Следуй по пути
- Замена компонентов

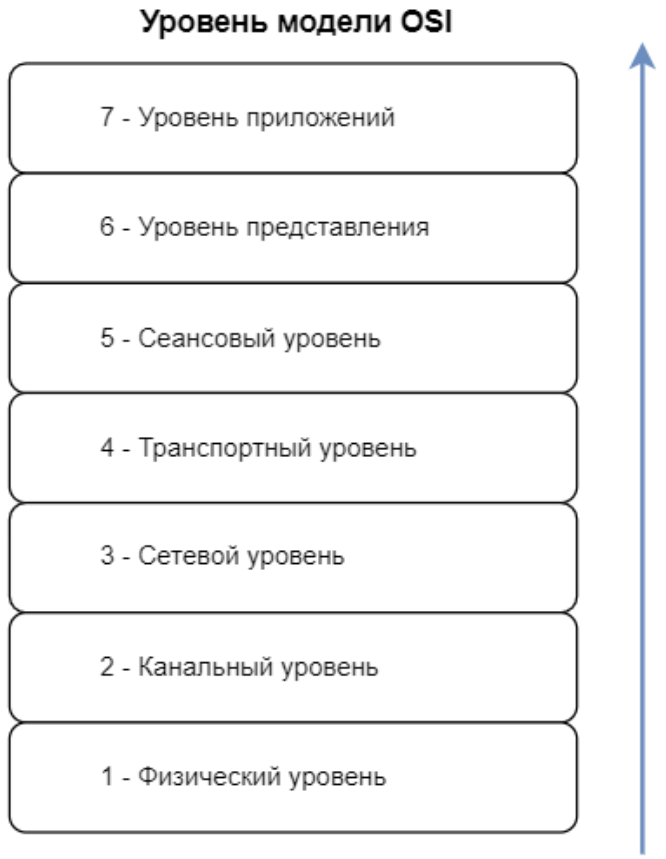
Сверху вниз


В одном из браузеров не открывается определенный веб-сайт
Веб-сервер

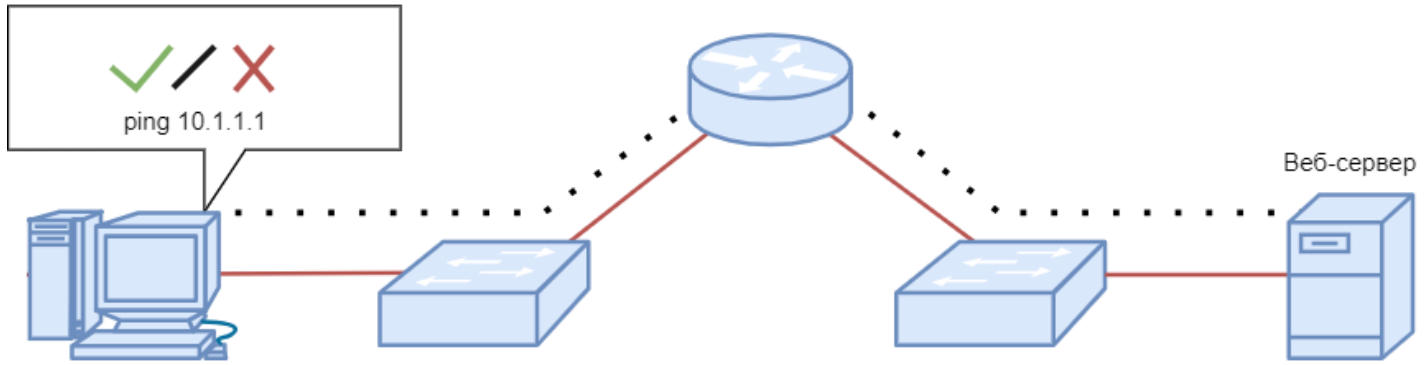

Уровень модели OSI
7 - Уровень приложений
6 - Уровень представления
5 - Сеансовый уровень
4 - Транспортный уровень
3 - Сетевой уровень
2 - Канальный уровень
1 - Физический уровень

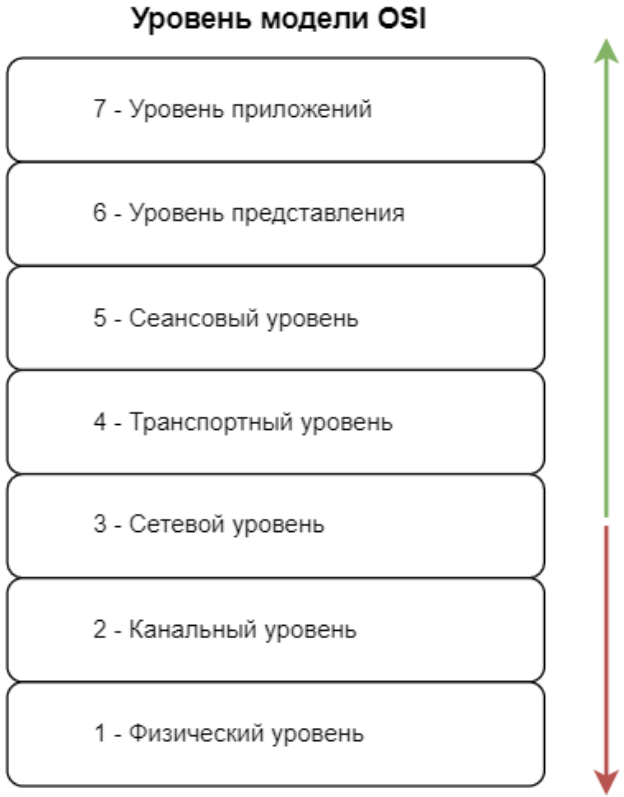
Снизу вверх


Не могу открыть ни одну веб-страницу
Веб-сервер

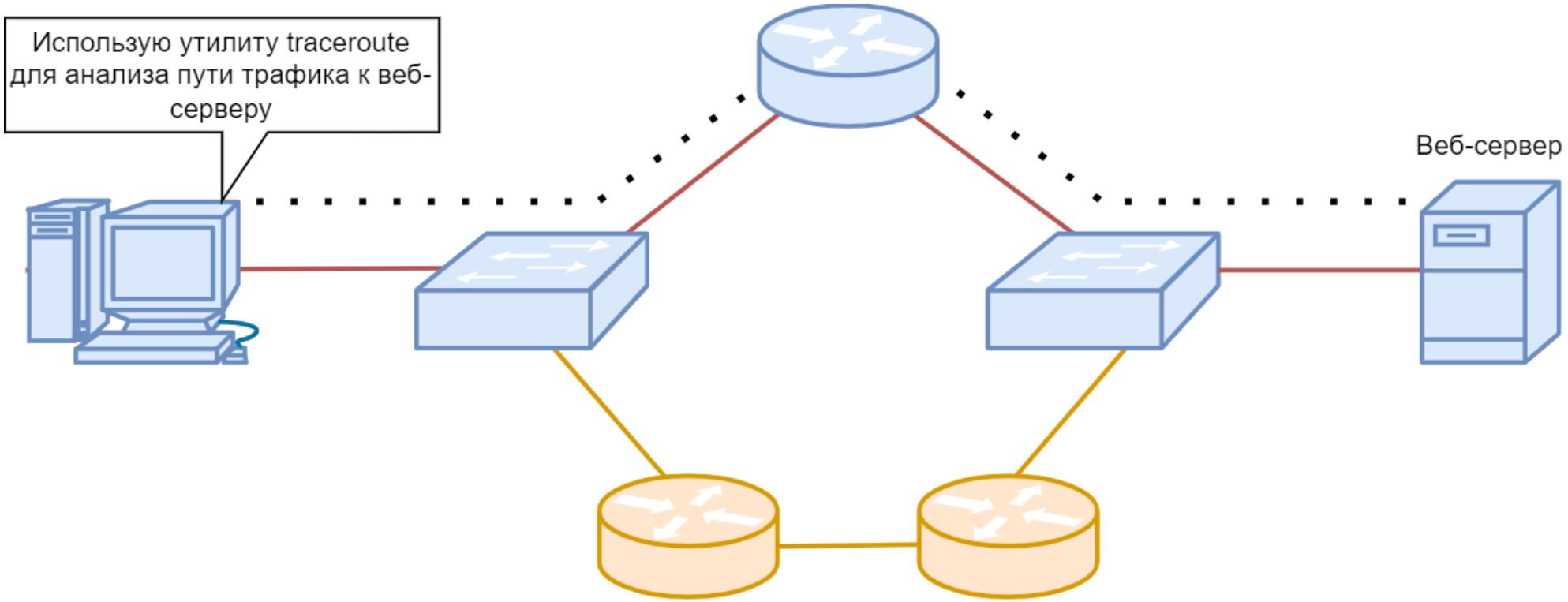

Уровень модели OSI
7 - Уровень приложений
6 - Уровень представления
5 - Сеансовый уровень
4 - Транспортный уровень
3 - Сетевой уровень
2 - Канальный уровень
1 - Физический уровень

Разделение

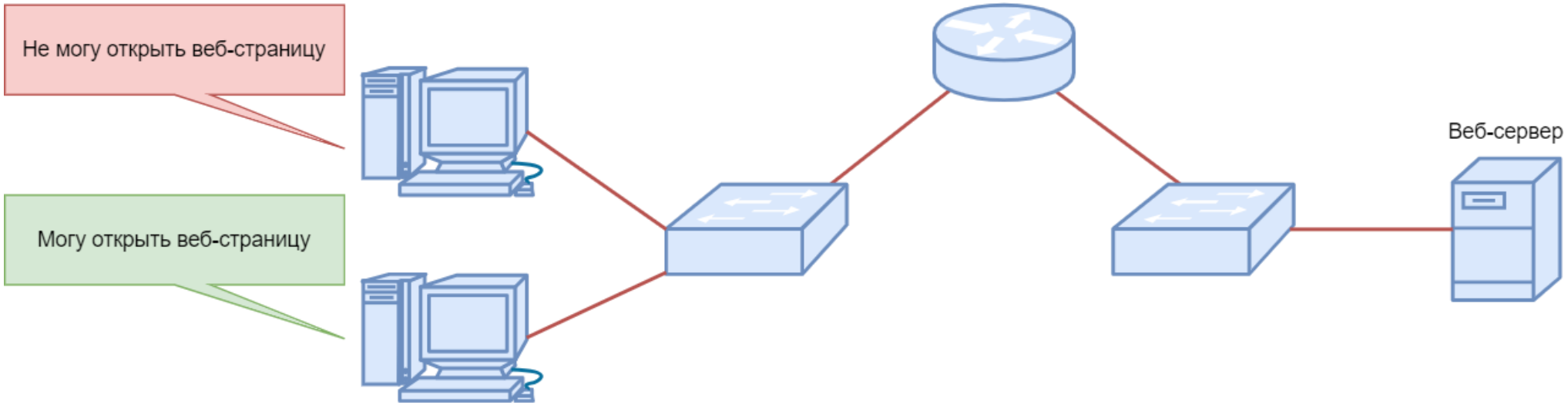

ping 10.1.1.1
Веб-сервер


Уровень модели OSI
7 - Уровень приложений
6 - Уровень представления
5 - Сеансовый уровень
4 - Транспортный уровень
3 - Сетевой уровень
2 - Канальный уровень
1 - Физический уровень

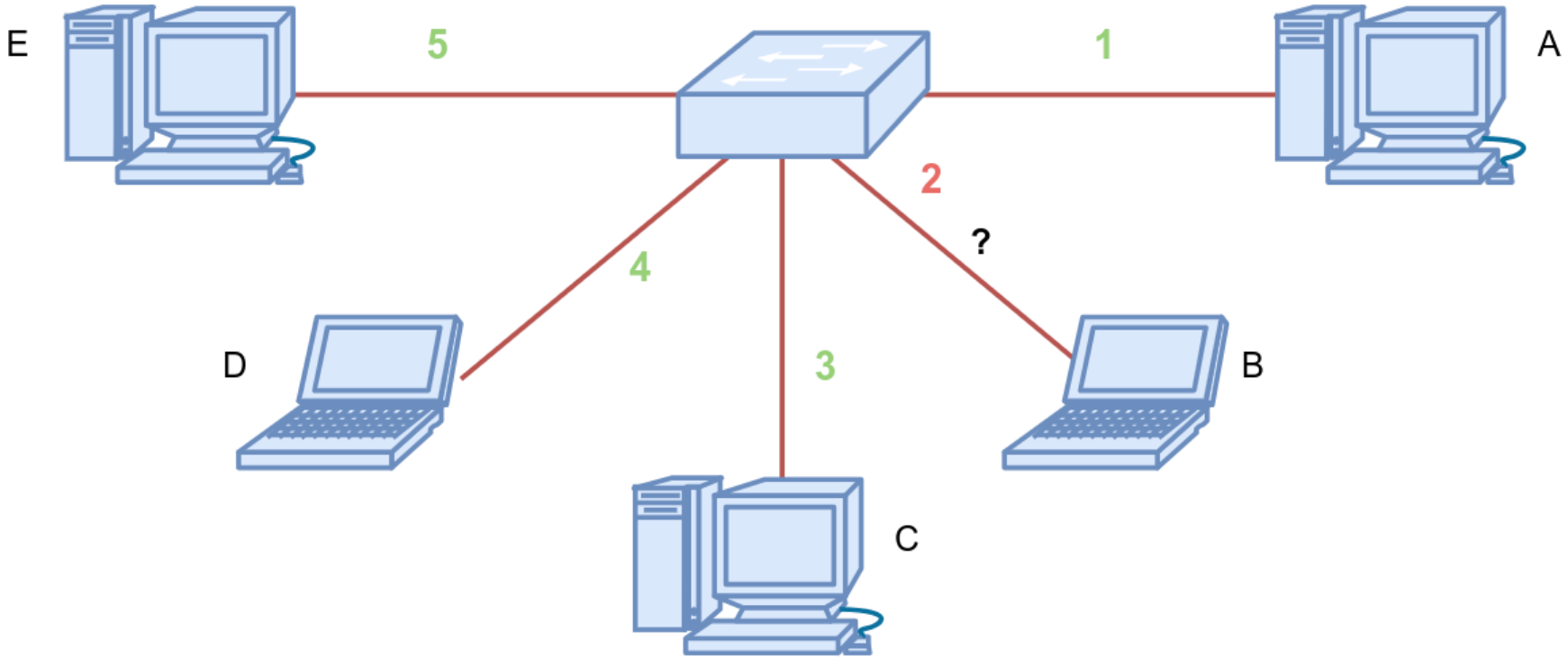
Следуй по пути



Найди отличия



Замена компонентов



Инструменты диагностики

2

ping

Ping (Packet InterNet Grouper) –
утилита, которая замеряет время прохождения и обработки пакета от узла до точки назначения и обратно

Оценка качества с ping

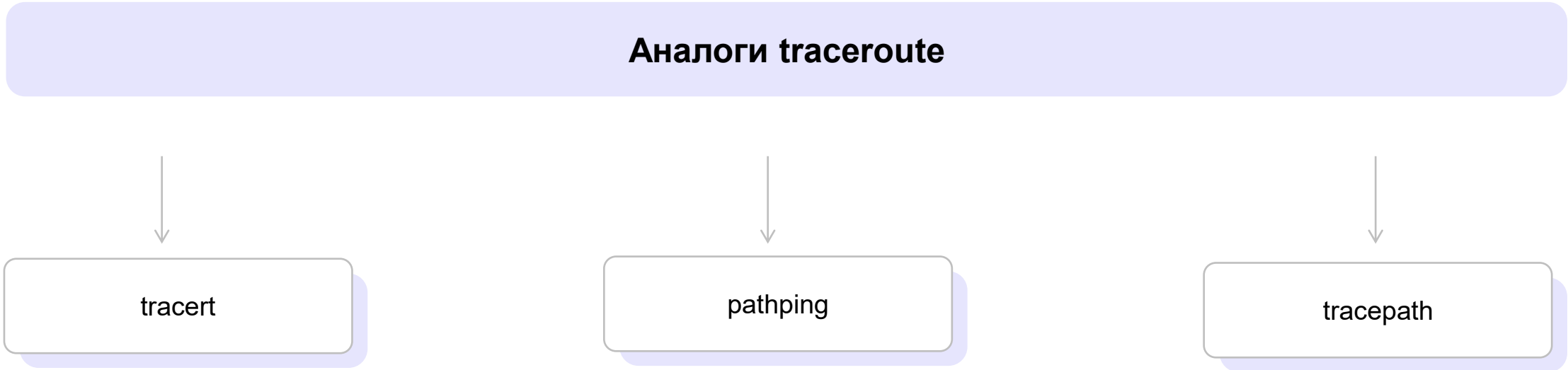
Факторы оценки качества

- Стабильность соединения
- Задержка
- Джиттер
- Потеря пакетов

traceroute

traceroute показывают через какие узлы (маршрутизаторы) проходит пакет, сколько времени занимает обработка пакета на каждом узле.

Утилиты трассировки



Терминология

iperf –
утилита, которая позволяет измерить скорость соединения между двумя узлами

tcpdump и wireshark

Tcpdump –
консольная утилита для захвата и анализа трафика, позволяет проверять заголовки пакетов TCP/IP

Wireshark –
графическая утилита для захвата и анализа трафика

Утилита Tcpdump полезна для систем без GUI.

Утилита Wireshark работает практически со всеми протоколами модели OSI, обладает понятным для обычного пользователя интерфейсом и удобной системой фильтрации данных.

Демонстрация

- Проверка связи с узлом посредством ping
- Выяснение максимально допустимого MTU с ping
- Проверка пути доставки пакетов (UDP, ICMP, TCP)
- Анализ скорости соединения
- Захват и анализ пакетов

Что мы изучили?

1. Возможные сетевые проблемы
2. Инструменты диагностики

Спасибо за внимание!