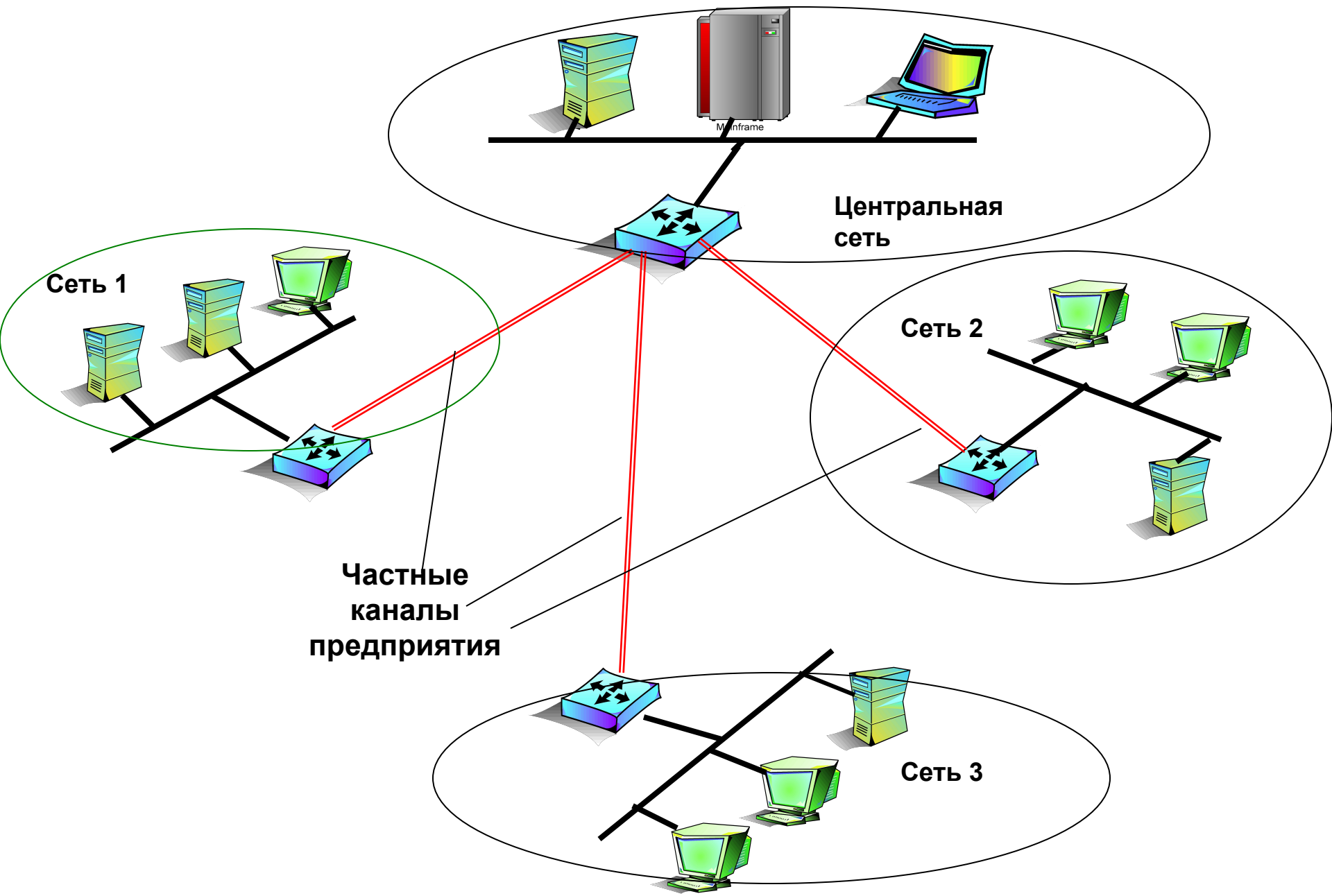
Виртуальные частные сети

Частная корпоративная сеть

- Предприятие единолично владеет всей сетевой инфраструктурой



Частная сеть с собственными территориальными каналами

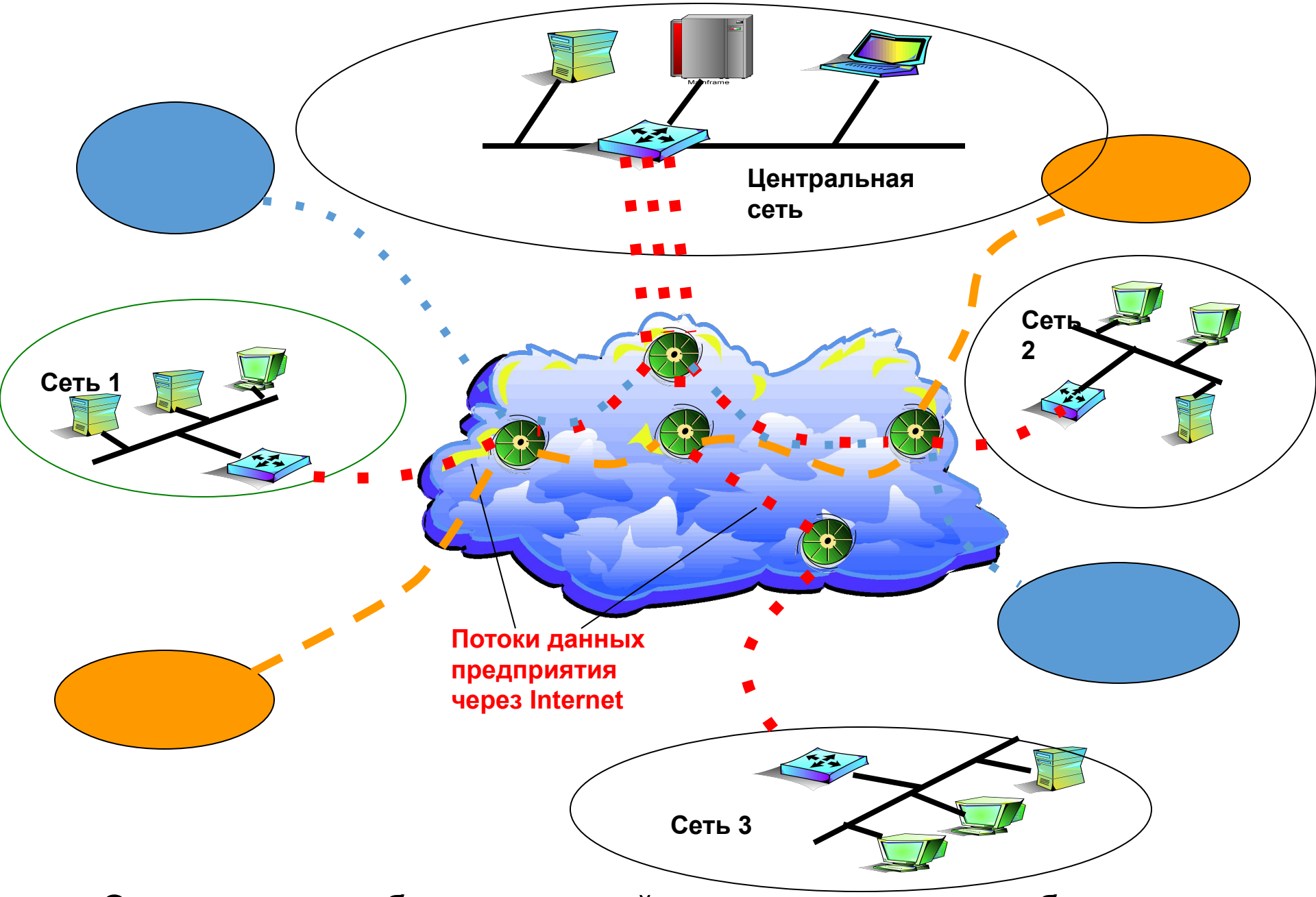
Частная сеть – главное свойство –

изолированность

Следствия (независимо от использованной сетевой технологии):

- **Независимая система адресации**
- **Предсказуемая производительность**
- **Максимально возможная безопасность**
- **Высокий уровень доступности**

Но решение неэкономичное



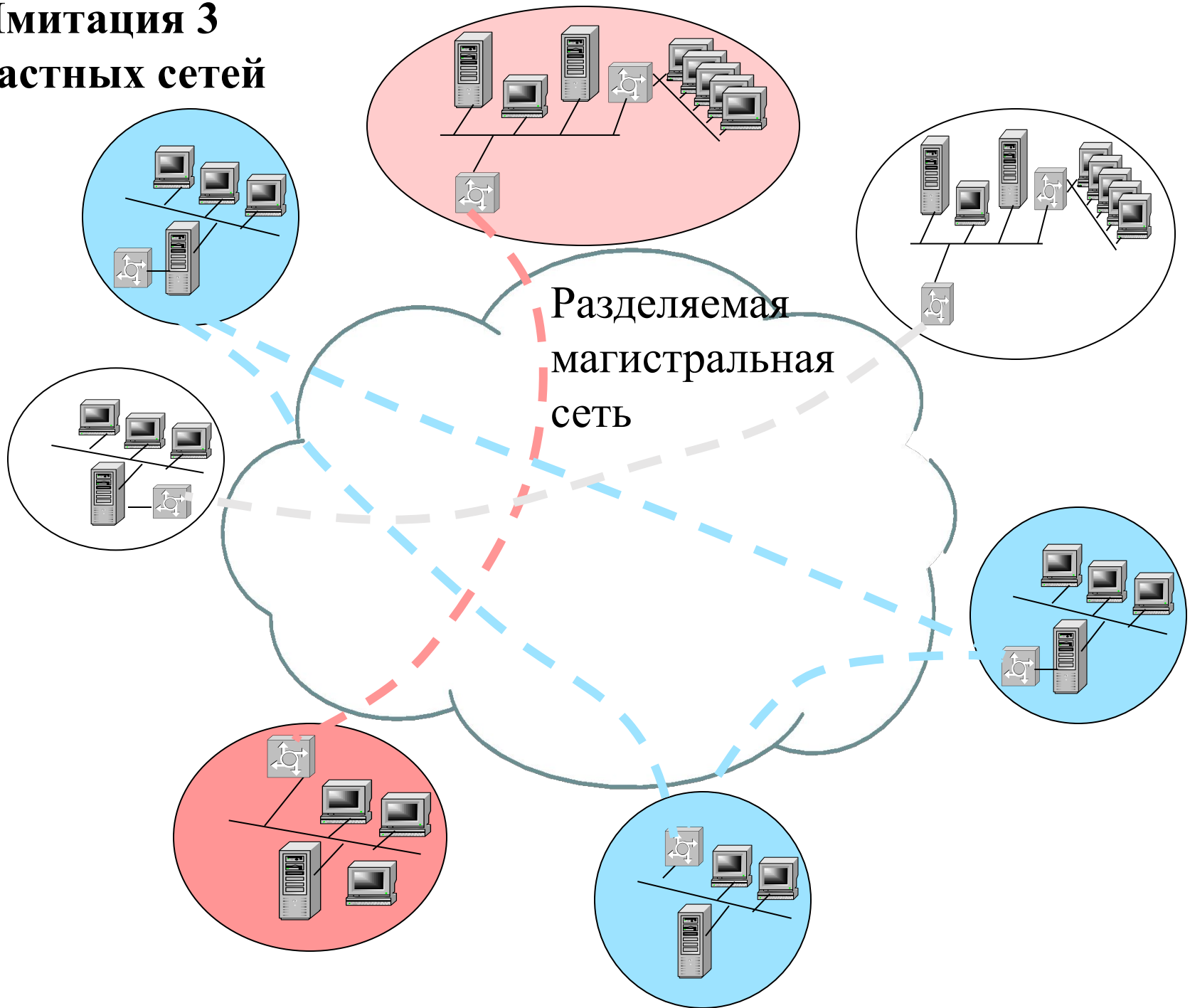
Организация глобальных связей предприятия через публичную сеть

VPN – это технология

позволяющая средствами **разделяемой (shared)** несколькими предприятиями сетевой инфраструктуры реализовать сервисы, по качеству (безопасность, доступность, предсказуемая пропускная способность, независимость в выборе адресов) приближенные к сервисам **частной (private)** сети.

VPN – компромисс
между качеством и стоимостью

Имитация 3 частных сетей



VPN – это сеть предприятия

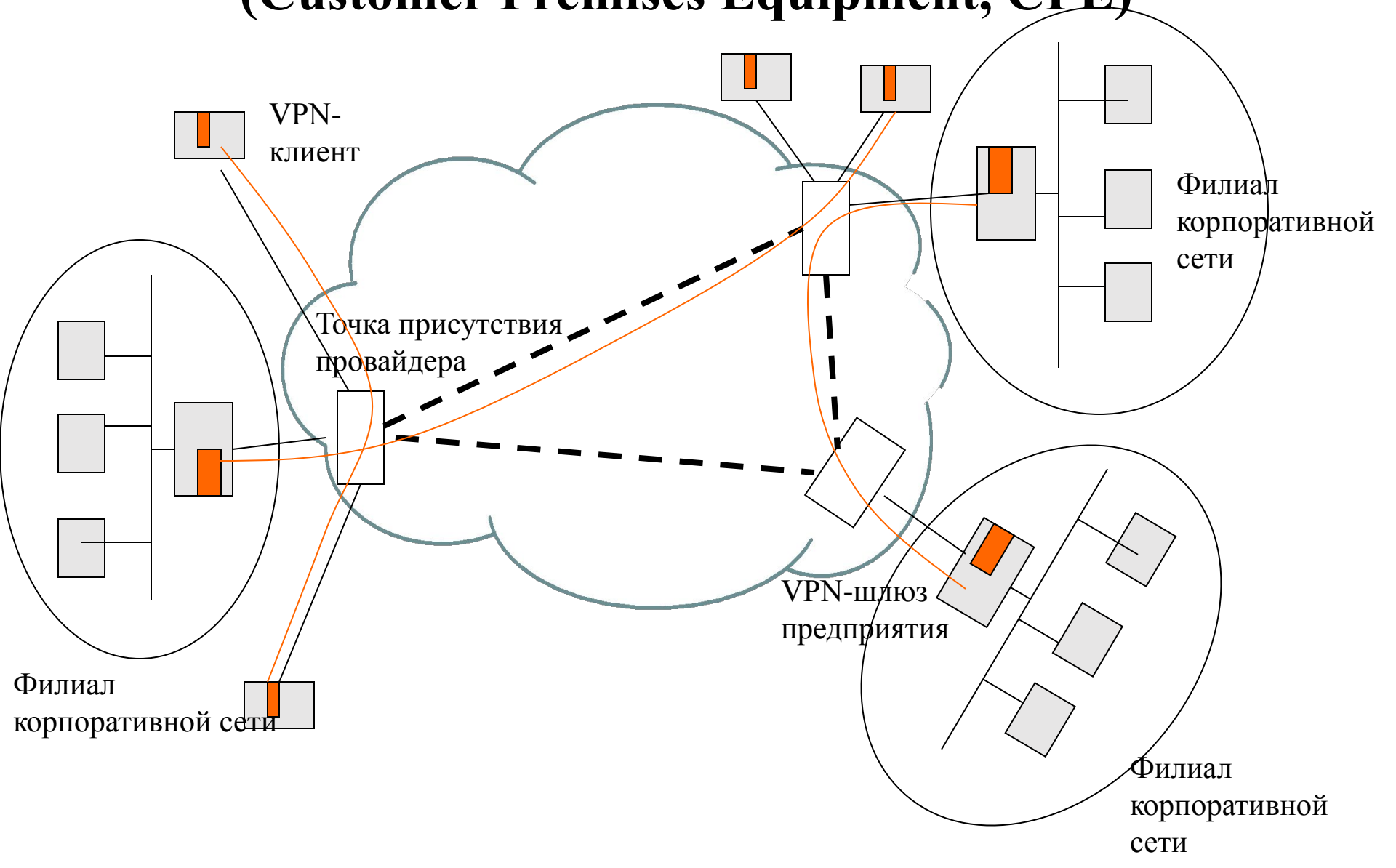
в которой разнесенные географически филиалы (сайты) объединены магистральной сетью, проложенной через совместно используемую сетевую инфраструктуру

VPN - это услуга

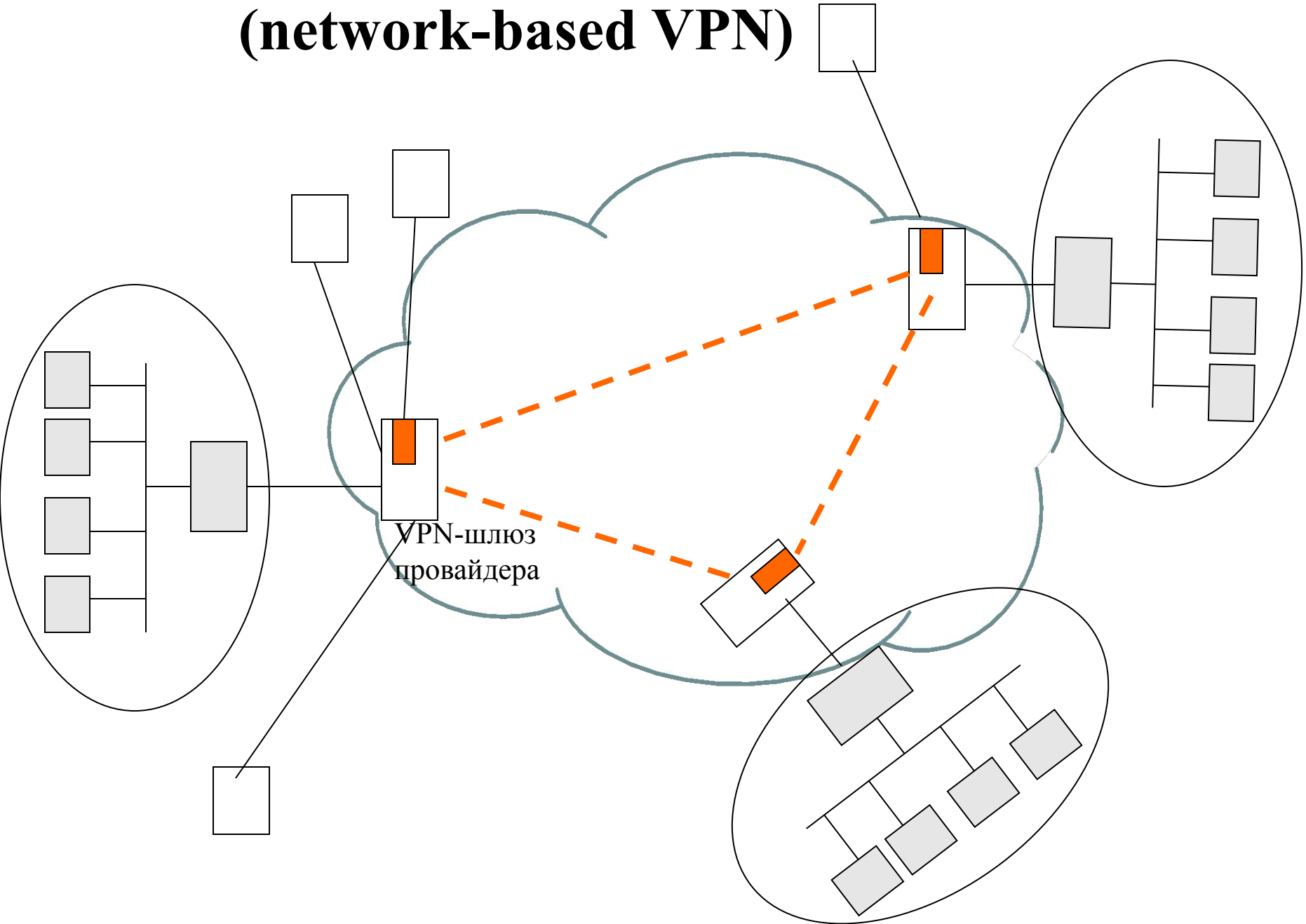
- Технология VPN может быть использована самим предприятием для объединения своих филиалов, а может и быть основой для предоставления услуг провайдером
- Услуги VPN могут характеризоваться:
  - типом имитируемых сервисов частной сети (выделенные каналы, сети с коммутацией пакетов)
  - качеством имитации сервисов частной сети (высокая безопасность, изолированность адресных пространств, гарантированность пропускной способности)
  - стоимостью, легкостью развертывания и поддержки

- Услуга VPN может предоставляться:
  - на базе оборудования установленного на территории заказчика **(Customer Premises Equipment, CPE)**
  - средствами собственной инфраструктуры провайдера **(network-based VPN)** – (аутсорсинг услуг VPN, провайдерская схема)
  - Аутсорсинг VPN дает возможность провайдерам, кроме оказания основного набора услуг, предоставление дополнительных централизованных сервисов (контроль за работой сети, аутсорсинг приложений)

VPN на базе оборудования, размещенного в помещении заказчика (Customer Premises Equipment, CPE)



VPN на базе сети провайдера (network-based VPN)



Характеристики технологии VPN:

- Тип имитируемых сервисов
- Приближенность предлагаемых сервисов к свойствам сервисов частной сети
- Масштабируемость
- Стоимость внедрения и обслуживания
- Управляемость

Требования к разделяемой сети

- Магистральная сеть должна быть хорошо защищена
- Сеть должна гарантировать клиентской VPN определенный уровень производительности
- Накладные расходы на обеспечение частного характера сервисов не должны быть слишком велики

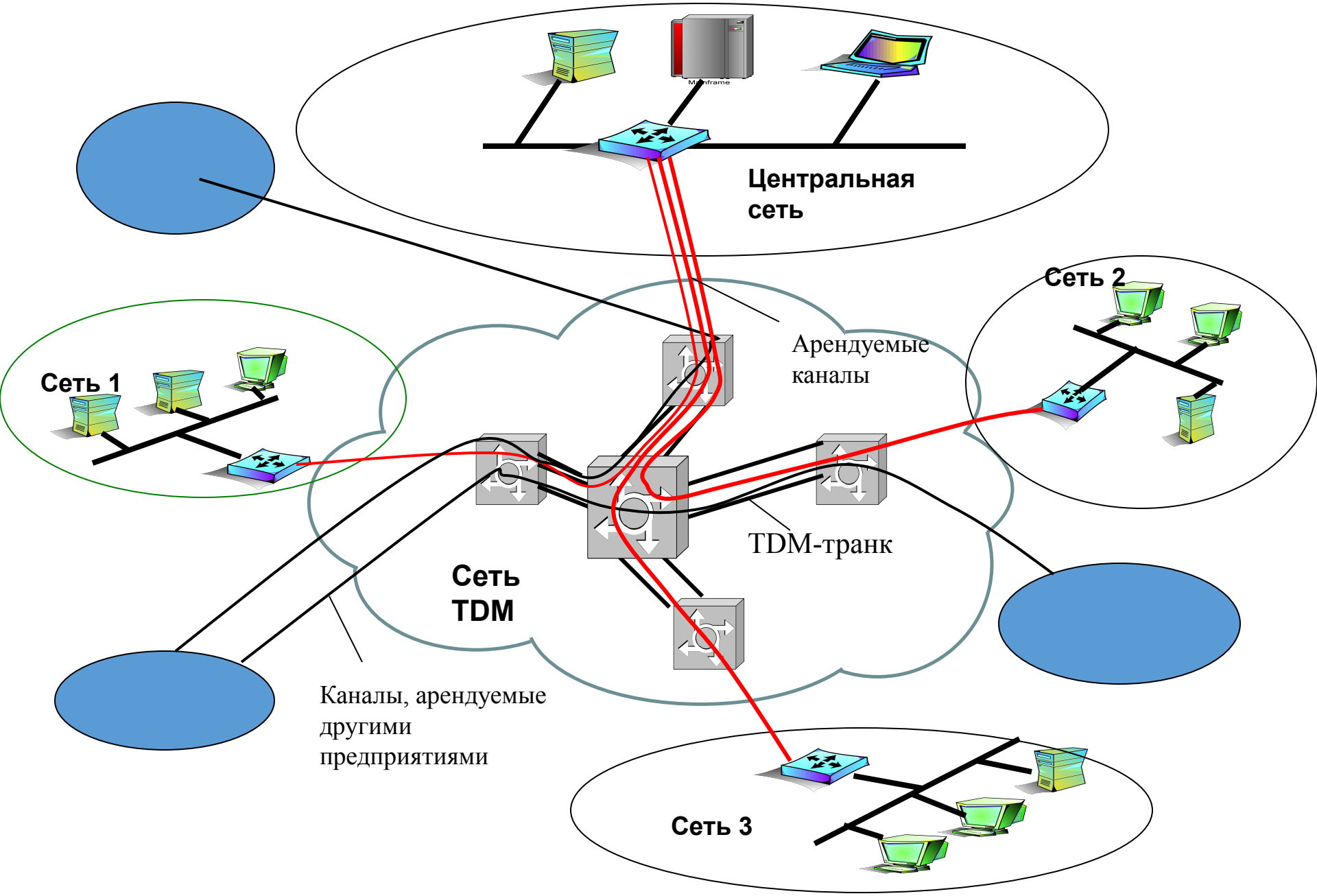
Требования к безопасности разделяемой сети

- Должно существовать разделение адресов и маршрутов – клиенты не должны знать друг о друге
- Магистральная сеть провайдера скрыта от внешнего мира. Клиенту следует знать только ту информацию, которая ему необходима для получения сервиса
- Разделяемая сеть должна быть устойчива к атакам отказ в обслуживании DoS

Типы технологий виртуальных частных сетей

- На базе арендованных каналов в TDM-сети (вырожденный случай VPN)
- На базе сети с установлением виртуальных каналов – ATM, Frame Relay
- На базе публичной IP-сети
  - с использованием протокола IPSec
- На базе MPLS

Виртуальная частная сеть на арендованных каналах



Виртуальная частная сеть на арендованных каналах

Сеть, построенная на арендованных каналах, имеет очень сходные характеристики с «истинно» частной сетью:

- Гарантированная пропускная способность
- Высокая степень безопасности
- Изолированность адресных пространств

НО

- **Высокая стоимость**
- **Плохая масштабируемость**

VPN на основе сетей ATM и Frame Relay

В VPN на основе сетей ATM и Frame Relay:

Виртуальные каналы имитируют сервис выделенных каналов (гарантированная пропускная способность, изоляция трафика)

Трафик не шифруется

Услуга реализуется средствами 2 Уровня, следовательно нет возможности предложить более развитые централизованные сервисы

Безопасность VPN на базе ATM и Frame Relay

- Трафик изолируется
- Адресные пространства разделены
- Магистраль скрыта от заказчиков
- Магистраль защищена от атак

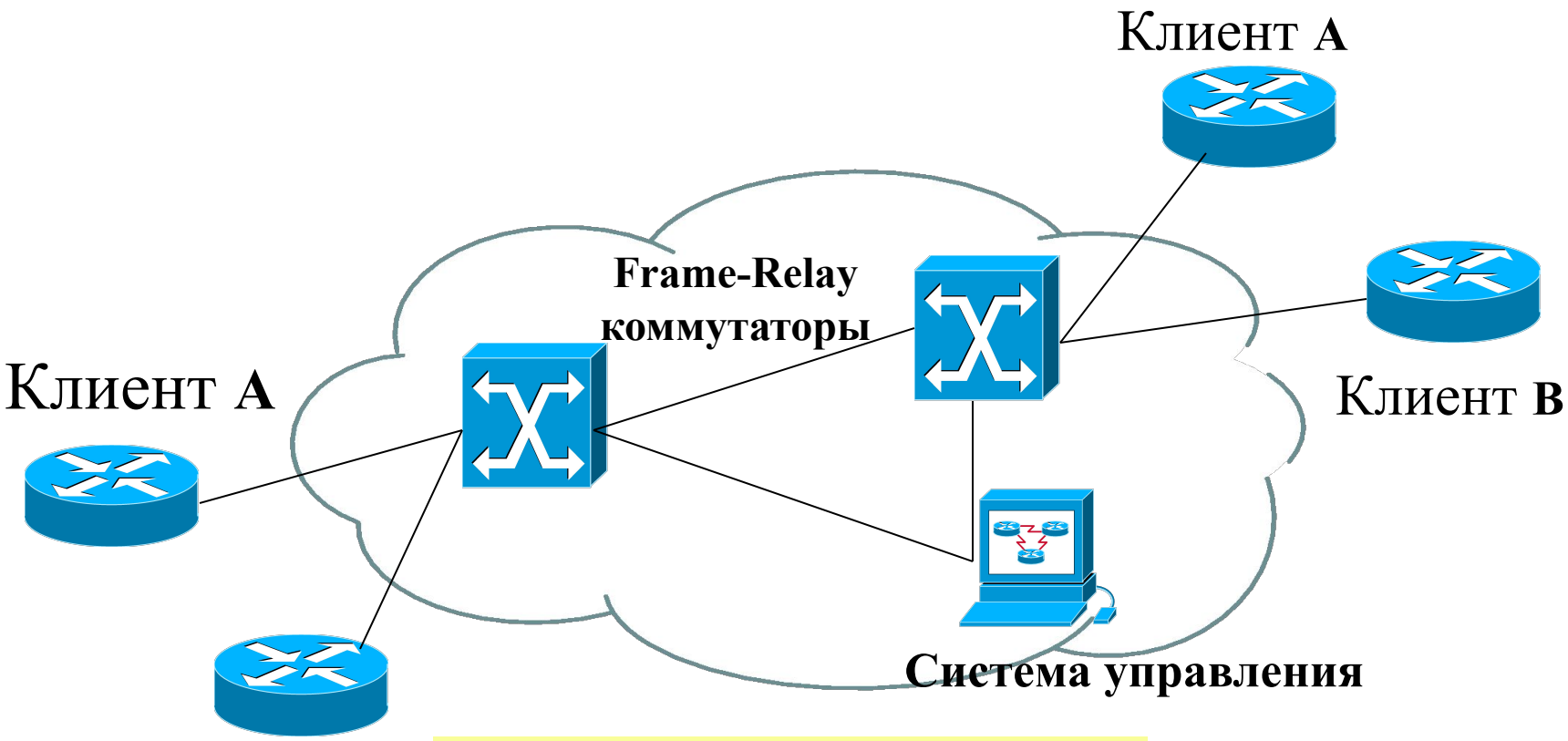
Разделение адресных пространств и маршрутов в ATM и Frame Relay

- Трафик коммутируется на основе меток VPI/VCI или DLCI
- Информация 3 Уровня никогда не анализируется и не меняется
- Весь трафик в магистральной сети коммутируется, а не маршрутизируется

Сокрытие магистральной сети провайдера в ATM и Frame Relay

- Информация, которой провайдер делится с клиентом, это лишь информация о клиентских виртуальных каналах DLCI и VPI/VCI
- Никаких других знаний о сети провайдера клиент иметь не должен

Что видит клиент?



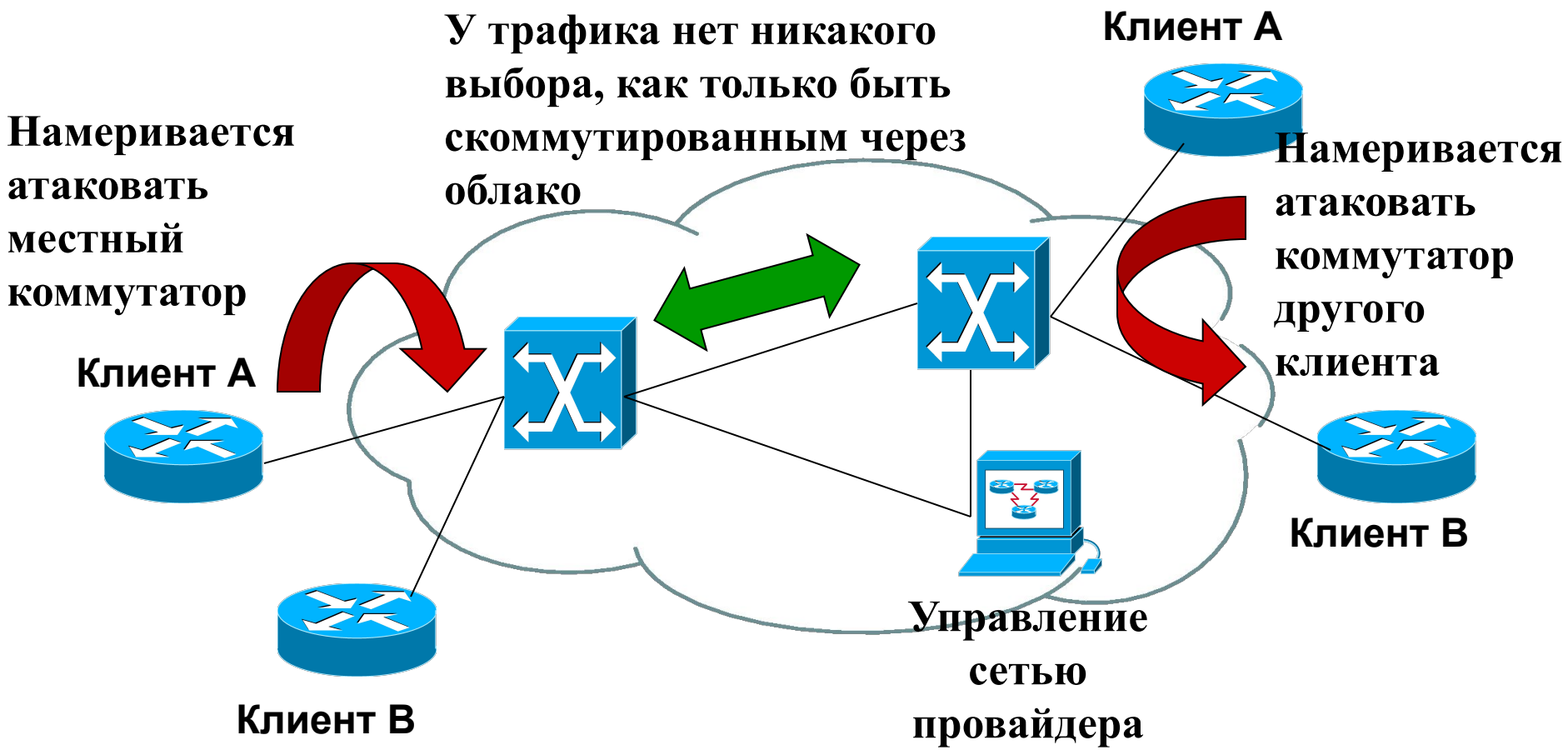
Клиент не видит:

- **других клиентов**
- **коммутаторов магистрали**
- **систему управления**

Устойчивость к атакам ATM и Frame Relay

- Без информации Уровня 3 и лишь на основании информации Уровня 2 вряд ли можно атаковать коммутаторы магистральной сети
- Атака DoS невозможна – сеть коммутирует все пакеты на другую сторону виртуального канала
- Атака вторжения – нет возможностей 3 Уровня

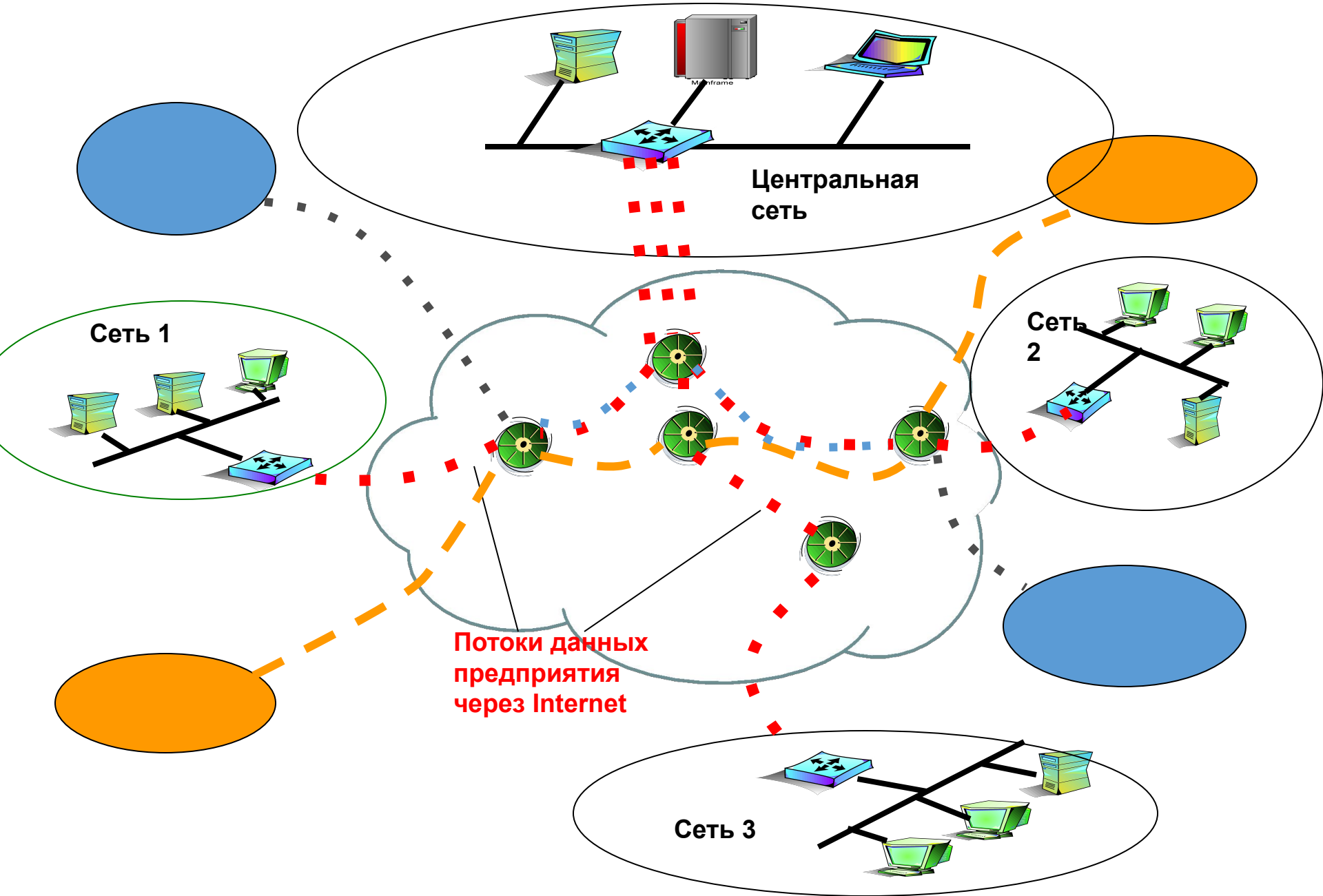
Атака в сети ATM и Frame-Relay



ATM и Frame-Relay безопасны?

- Адреса и маршруты разделены?
  - Да – анализируется только информация Уровня 2, Уровень 3 игнорируется
- Магистраль провайдера скрыта?
  - Да – клиент обладает только минимальной информацией о магистрали
- Устойчива к атакам?
  - Да – Никаких реальных возможностей для атак нет

VPN на базе IP-сети



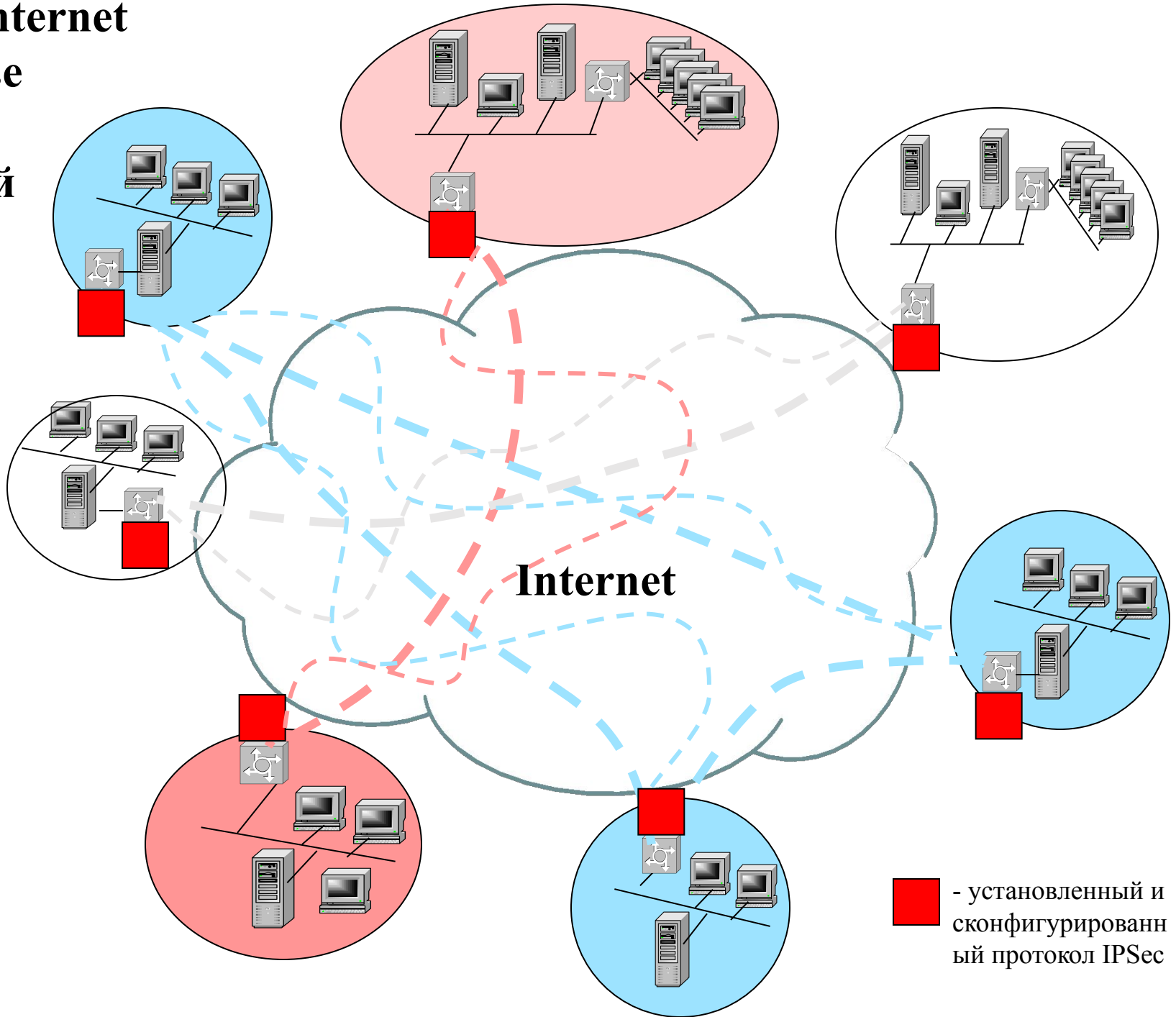
IP VPN на основе протокола IPSec

IPSec позволяет строить **защищенные логические соединения – туннели.**

Логическое соединение IPSec:

- Относится к определенному классу трафика (селектор – IP-адрес отправителя и получателя, порты отправителя и получателя)
- Определяет процедуру обработки для защиты данного класса трафика (обеспечение целостности или конфиденциальности, туннельный режим или транспортный) и криптографический материал
- Не фиксирует маршрут
- Требует предварительного конфигурирования

VPN в Internet на основе IPSec-туннелей



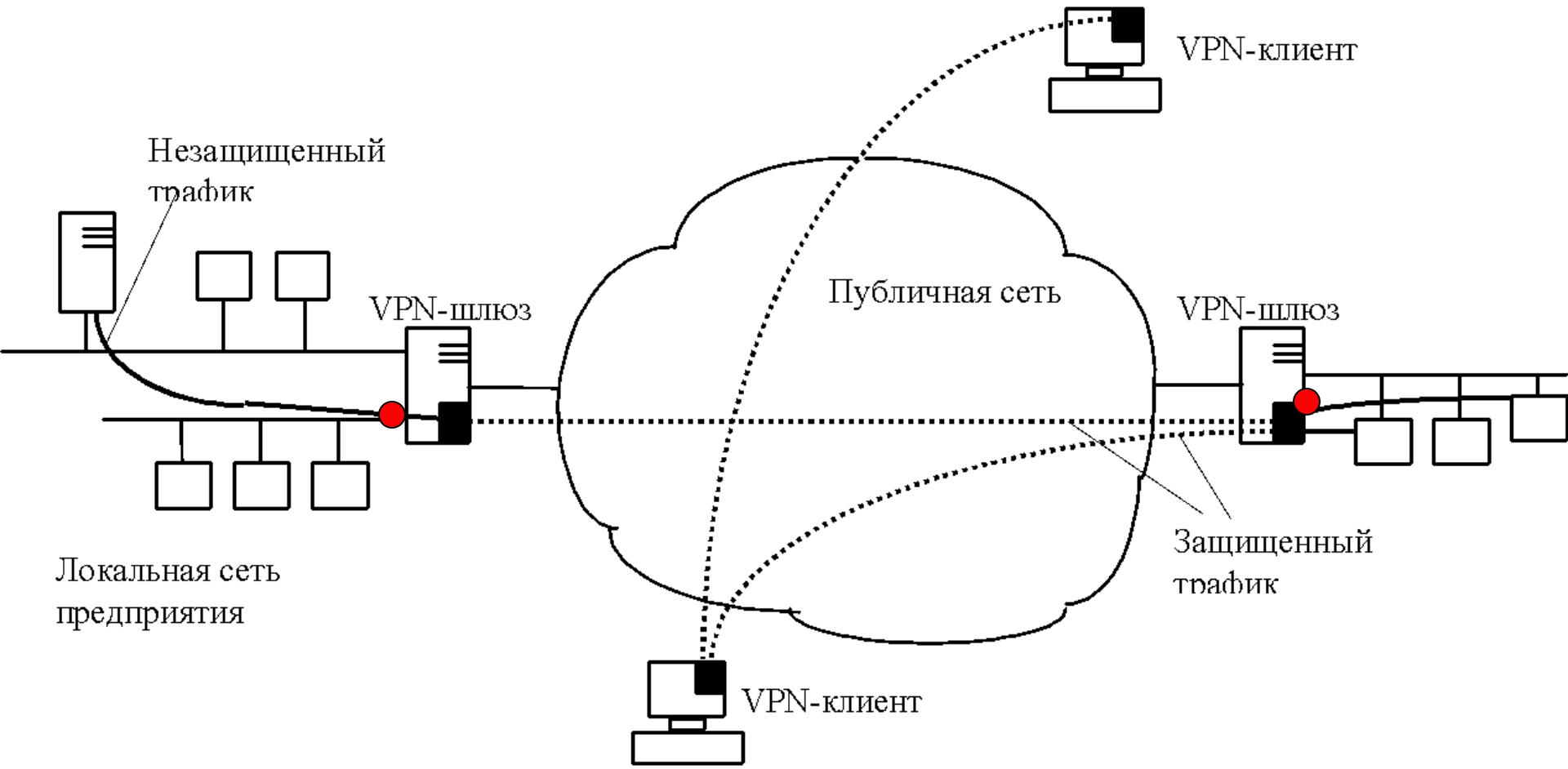
Типы VPN-устройств

- *отдельное аппаратное устройство*
- *отдельное программное решение*, которое дополняет стандартную операционную систему функциями VPN;
- *расширение брандмауэра* защищенного канала; за счет дополнительных функций
- *средства VPN, встроенные в маршрутизатор* или коммутатор
- гибридное решение, в котором VPN-приложение работает на стандартной вычислительной платформе, использующей внешний криптографический процессор для выполнения функций VPN.

(1) **Шлюз VPN** — сетевое устройство, подключенное к нескольким сетям, которое выполняет функции шифрования и аутентификации для многочисленных хостов позади него

(2) **Клиент VPN** - это устройство, подключенное к одной сети, у которого сетевое транспортное обеспечение модифицировано для выполнения шифрования и аутентификации трафика между шлюзами VPN и/или другими VPN-клиентами.

VPN-шлюзы и VPN-клиенты



Услуги VPN на базе IP-сетей

- Недостаточная степень гарантий пропускной способности и безопасности
- Гибкость и эффективность в предоставлении дополнительных услуг

Степень безопасности IP VPN на основе IPSec

- Трафик пользователей передается по общей инфраструктуре
- Трафик разных VPN не изолируется, в таблицах маршрутизации содержится информация о чужих сетях
- Различные VPN не могут иметь независимое адресное пространство (даже при наличии NAT)
- Магистральная разделяемая сеть не защищена от атак типа DoS
- Моделирование изолированности трафика отдельных VPN достигается за счет **шифрования**

Безопасна ли VPN на базе IP-сети?

- Адреса и маршруты разделены?
  - Нет, при перемещении пакета анализируется информация Уровня 3,
- Магистраль провайдера скрыта?
  - Нет – клиент обладает информацией об IP-адресах точек входа в сеть провайдера и другой информацией о магистрали
- Устойчива к атакам?
  - Нет – возможны атаки типа DoS