Развитие обобщённой графовой модели ИКТ-инфраструктуры локального поставщика сетевых услуг для учета виртуальных частных сетей

Антон Андреев

Кафедра Информатики и математического обеспечения
Институт Математики и информационных технологий
Петрозаводский государственный университет

Научный семинар «Проблемы современных информационно-вычислительных систем»

МГУ им. М. В. Ломоносова, 01.11.2016

Локальные поставщики сетевых услуг

Рост и усложнение сетей ПСУ:

- рост количества мобильных пользователей;
- широкое использование виртуализации и VPN.

лПСУ — организации, сопровождающие ИКТ-инфраструктуру и предоставляющие набор сетевых услуг для собственных нужд (возможно с небольшой долей транзита).

Примеры лПСУ:

- центры обработки данных;
- корпоративные сети;
- сети университетов.

Виртуальные частные сети

ВЧС (VPN) – защищенная от доступа извне Сеть, развернутая поверх другой, публичной Сети.

Цели построения ВЧС в Сетях лПСУ:

- Организация подключения пользователей к Сети:
  - защищенное подключение собственных пользователей;
  - ограниченное подключение сторонних пользователей (сервис);
  - защищенная передача данных между двумя узлами Сети.
- Соединение сегментов Сети через Сеть-посредник:
  - защищенное объединение сегментов Сетей филиалов через сеть другого ПСУ;
  - логическая структуризация сегментов в пределах собственной Сети.

Граф ИКТ-инфраструктуры лПСУ (Сети)

Решение большинства задач сетевого управления требует описания структуры Сети:

- устройства, их сетевые порты и физические связи между портами разных устройств;
- группировка устройств и портов:
  - широковещательные домены (VLAN);
  - IP-подсети;
  - виртуальное оборудование;
  - multicast-группы.

Применение:

- документирование Сети;
- локализация точек отказа;
- моделирование и проектирование Сетей;
- визуализация текущей нагрузки на элементы Сети.

Задача построения графа Сети

Основные проблемы для канального уровня:

1. стандартами IEEE 802.1 изначально не предусмотрены возможности обнаружения сетевых устройств;
2. стандартизованные сравнительно недавно механизмы обнаружения (LLDP) недостаточно распространены;
3. неполнота и разнородность данных;
4. различия в реализации стандартов производителями сетевого оборудования;
5. изменчивость структуры Сети;
6. сложность современных Сетей (VLAN, VPN, туннели, виртуализация).

Построение графа Сети: **1)** сбор данных об устройствах и соединениях между ними; **2)** представление собранных данных в виде графа.

Исходная модель структуры Сети

- Моделирование Сетей, построенных в соответствии со стандартами Ethernet (IEEE 802.1/802.3) и IP (RFC 791).
- Моделирование структуры 1, 2, 3 уровней модели OSI:
  - устройства и их порты на физическом уровне;
  - логические интерфейсы и VLAN на канальном уровне;
  - сетевые интерфейсы и IP-подсети на сетевом уровне.
- Основа для учета различных источников данных о структуре сети.

А. А. Андреев, А. С. Колосов, А. В. Воронин, Ю. А. Богоявленский.
Обобщенная графовая модель структуры физического, канального и сетевого уровней ИКТ-инфраструктуры локального поставщика сетевых услуг // Программная инженерия. 2016. Т. 7, № 9. С. 400–407

Цели и задачи

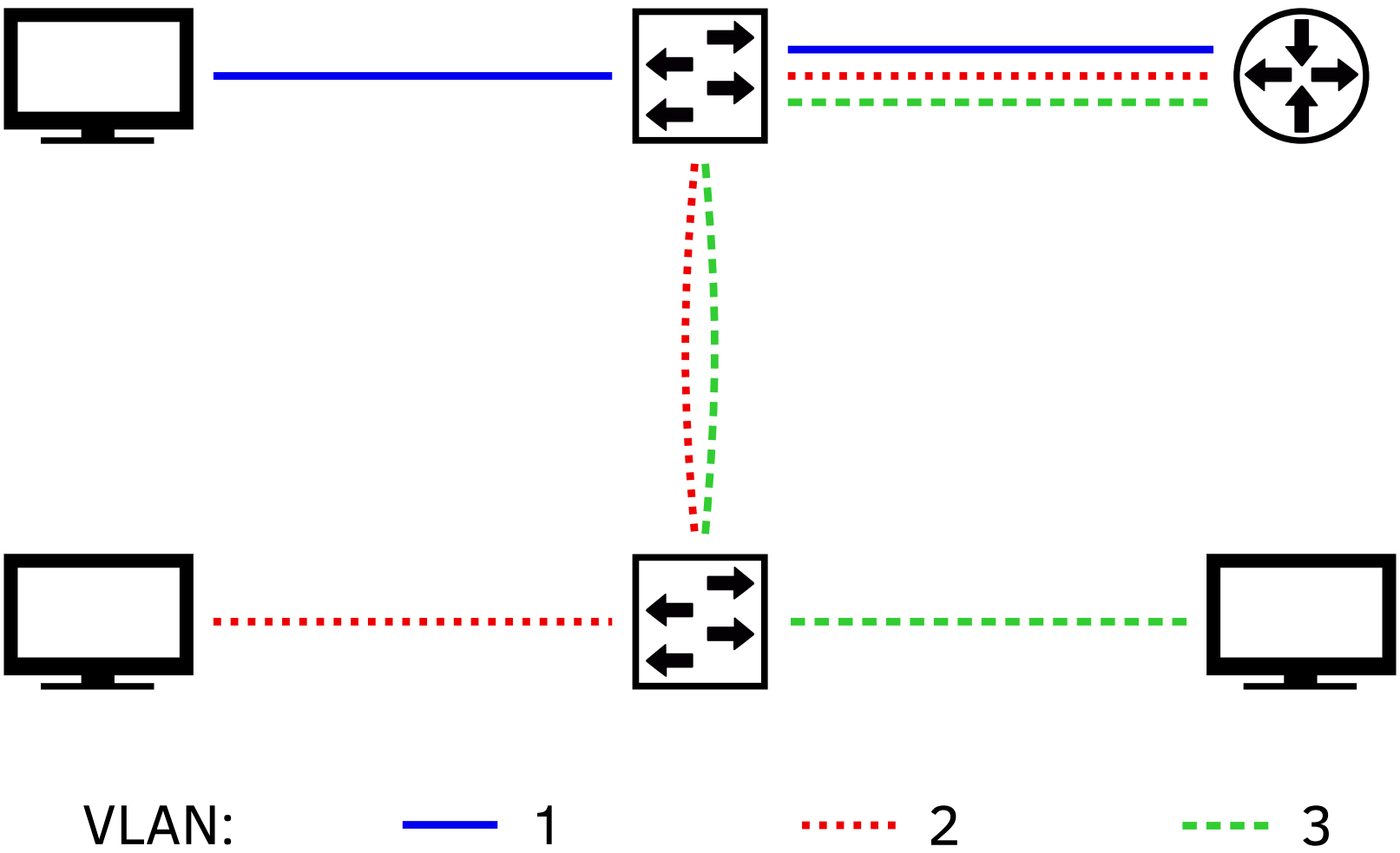
Цель

Отразить в рамках существующей модели элементы и связи, служащие для построения ВЧС в Сетях лПСУ.

Задачи:

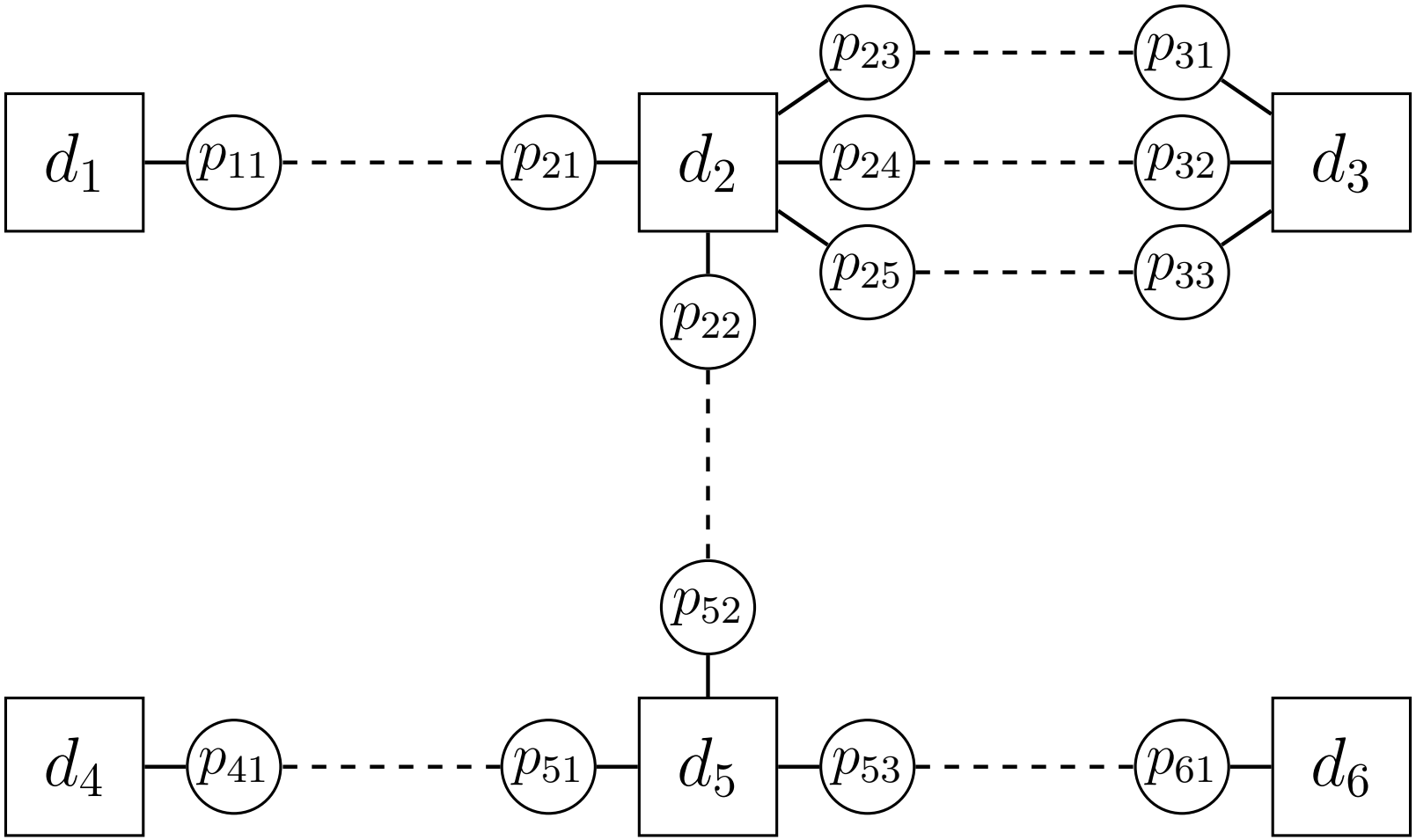
- классифицировать методы построения ВЧС с точки зрения структуры Сети;
- определить ключевые структурные элементы каждого класса;
- разработать расширение модели структуры Сети, отражающее структуру ВЧС;
- разработать методы обработки данных для автоматизации отражения ВЧС в графе структуры Сети.

Демонстрационная Сеть



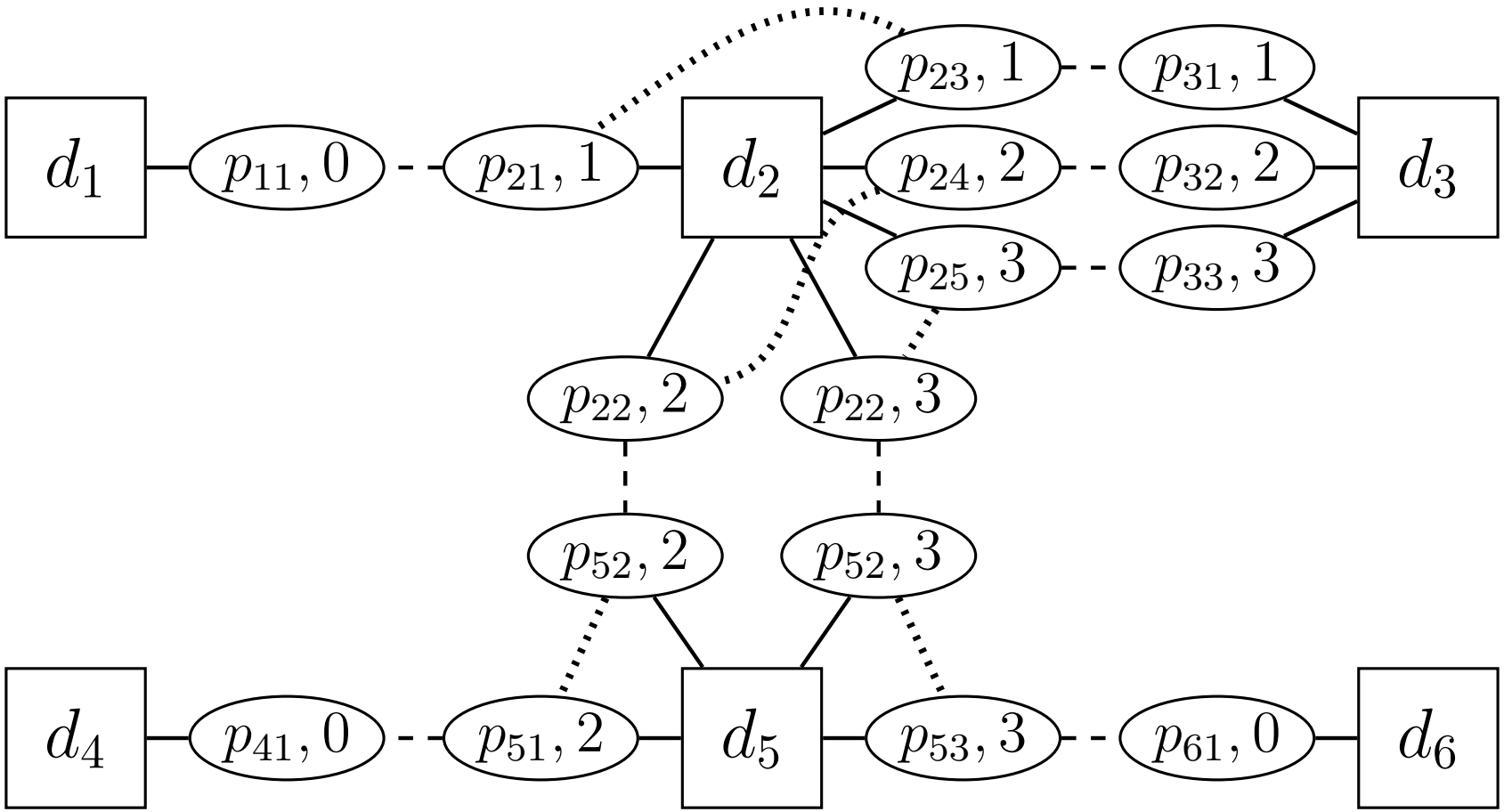
Модель структуры физического уровня

D — Множество устройств; P — множество портов;
A^1 — множество ребер ассоциации портов с устройствами;
L^1 — множество ребер соединений физического уровня;



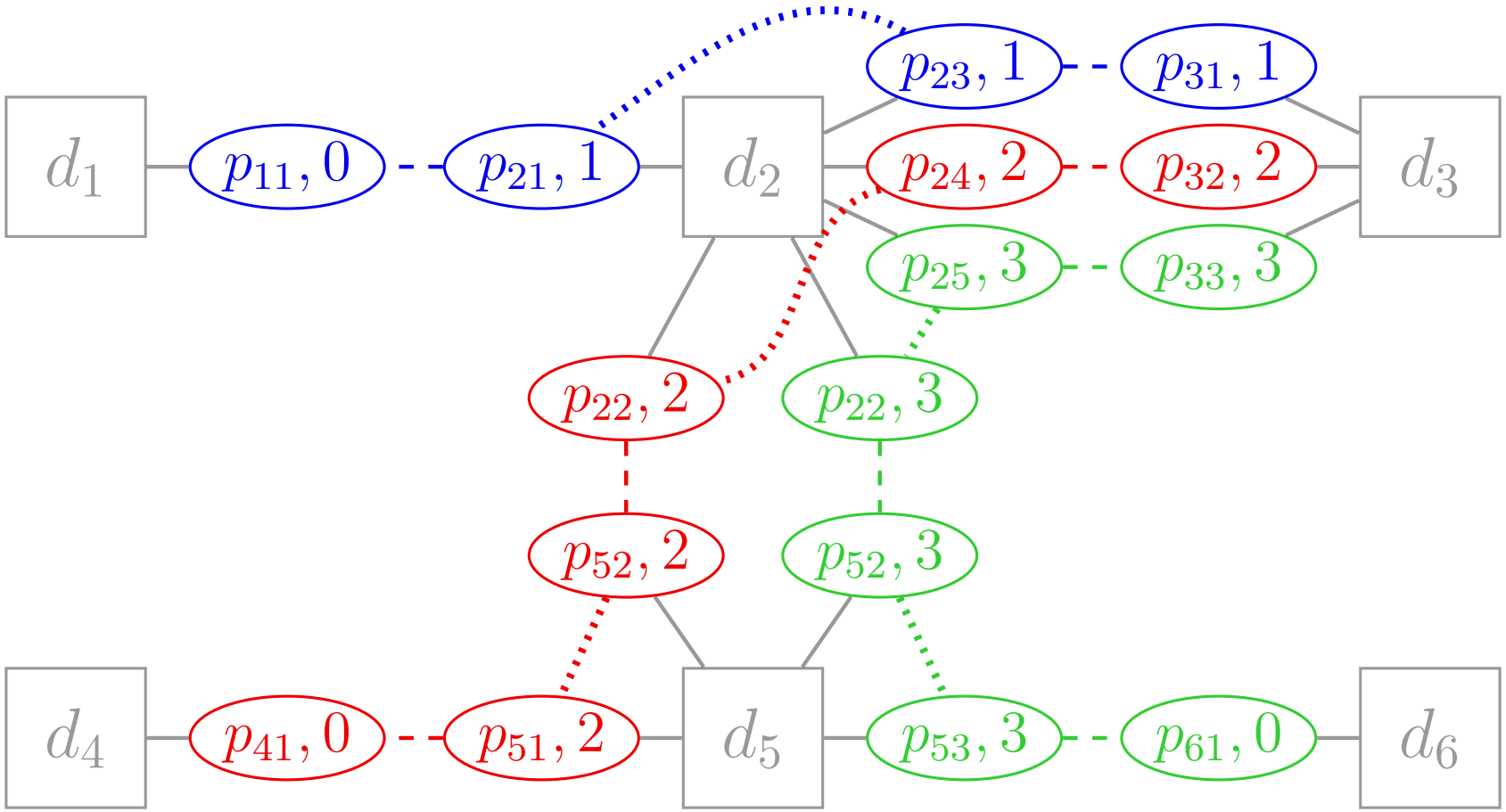
Модель структуры канального уровня

I^2 — множество интерфейсов канального уровня;
A^2, F^2, L^2 — множество ребер ассоциации интерфейсов, коммутации и соединений канального уровня;



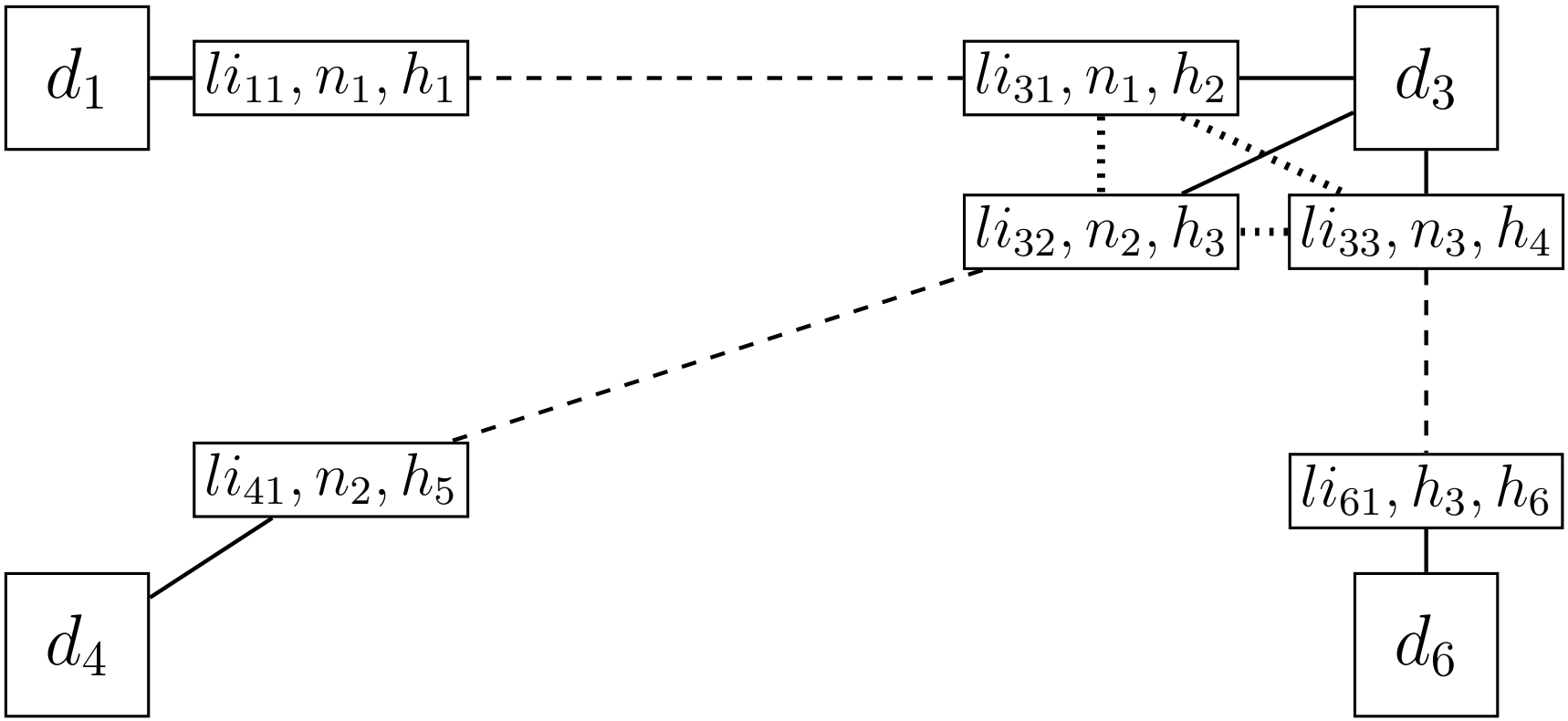
Модель широковещательных доменов Сети

Компоненты связности графа $\langle I^2, L^2 \cup F^2 \rangle$



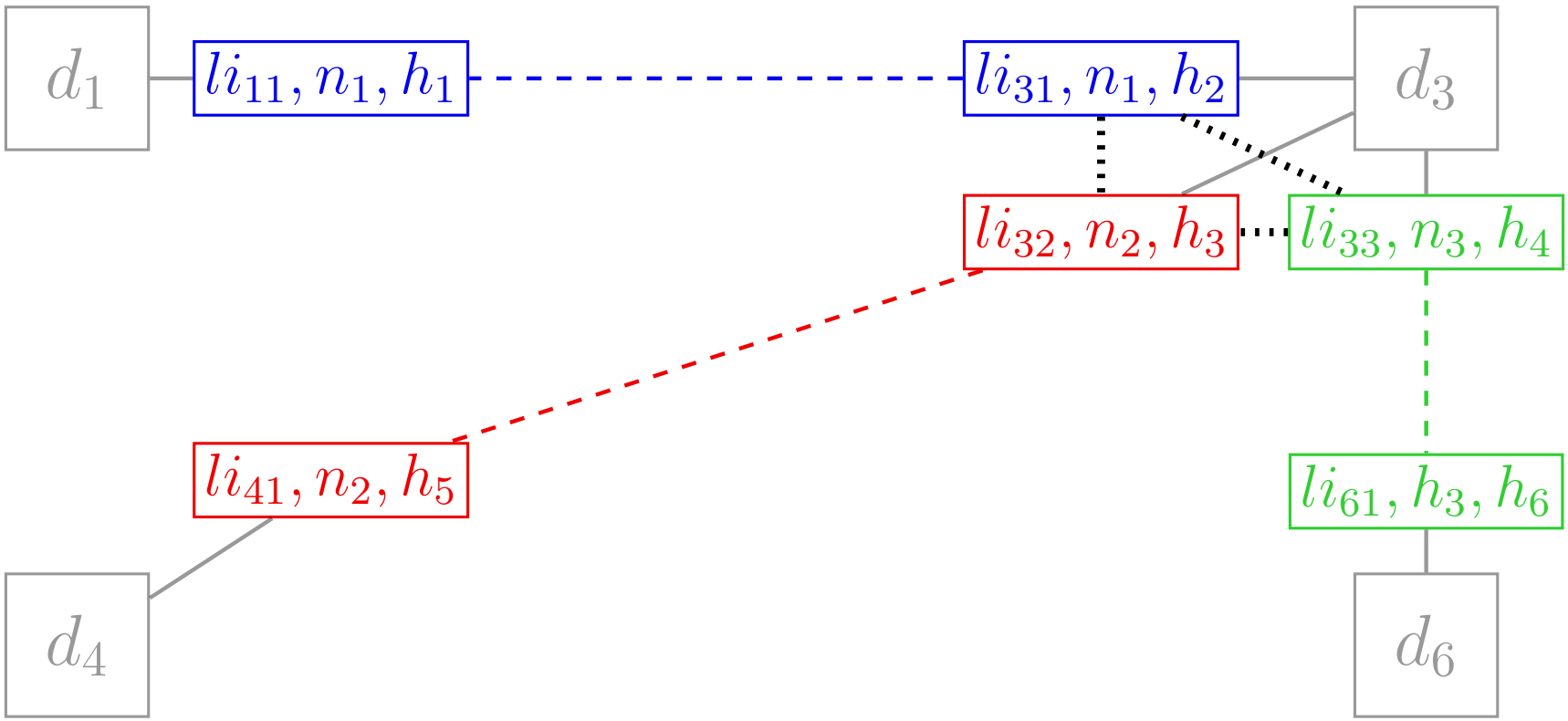
Модель структуры сетевого уровня

I^3 — множество интерфейсов сетевого уровня;
A^3, F^3, L^3 — множество ребер ассоциации интерфейсов, маршрутизации и соединений сетевого уровня;



Модель IP-подсетей

Компоненты связности графа $\langle I^3, L^3 \rangle$



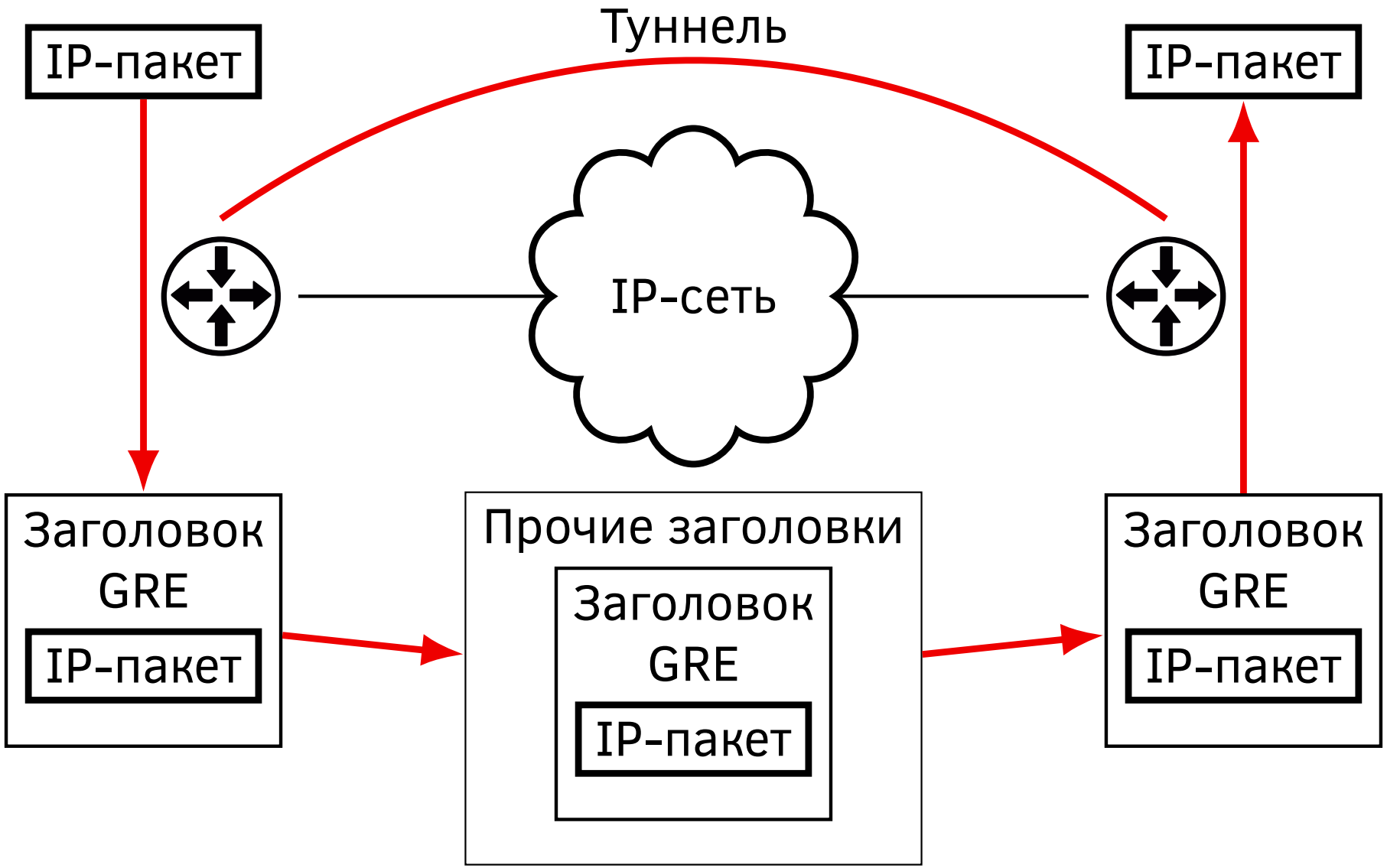
Механизмы ВЧС

- аутентификация и авторизация доступа к Сети;
- шифрование данных;
- туннелирование.

Технологии аутентификации, авторизации и шифрования не оказывают влияния на структуру Сети.

Туннелирование позволяет прозрачно связать сегменты Сети, не соединенные физически.

Туннелирование

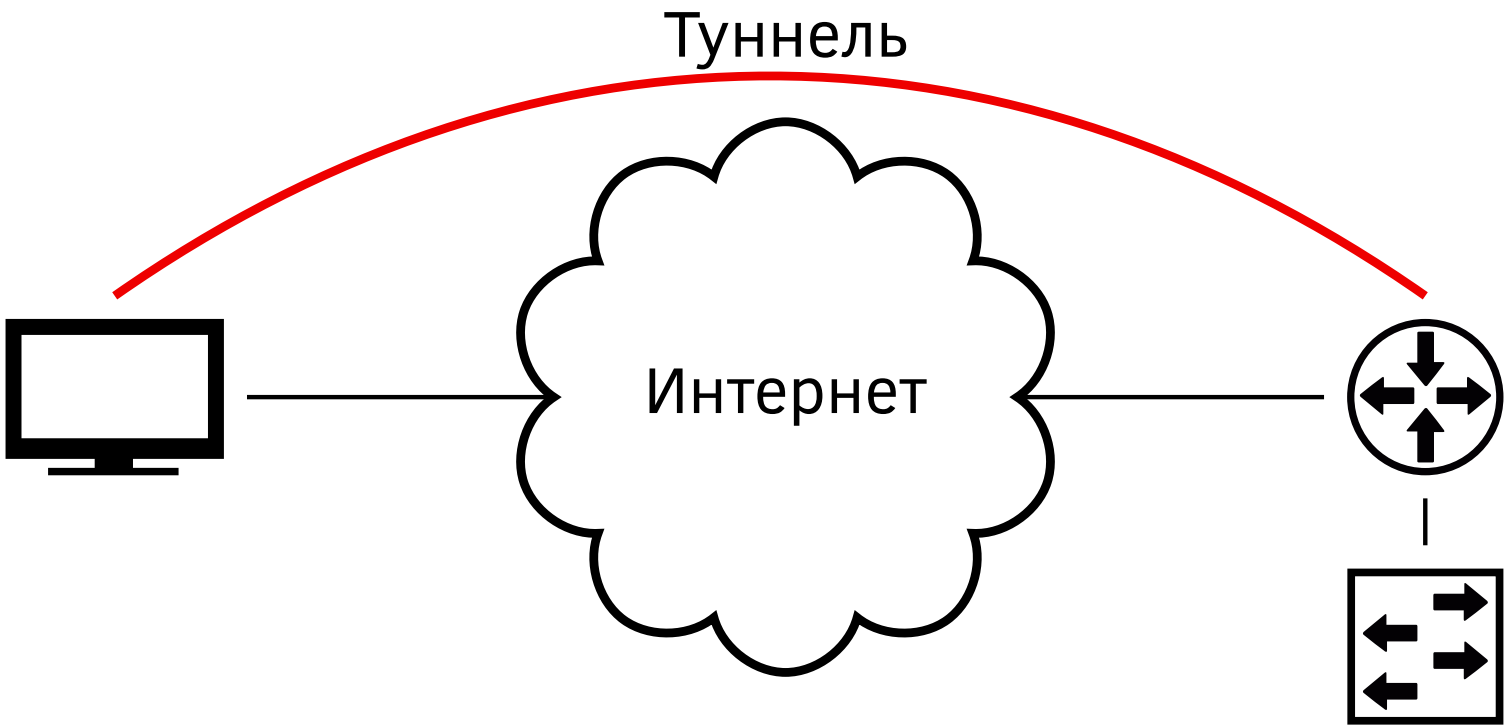


Классификация туннелей по уровню несущего протокола

- Канальный: PPPoE, PPPoA
- Сетевой: GRE, IPSec
- Транспортный: L2TP, PPTP
- Сеансовый: SSL/TLS (OpenVPN, SSTP)
- Прикладной: SSH

Классификация туннелей по назначению

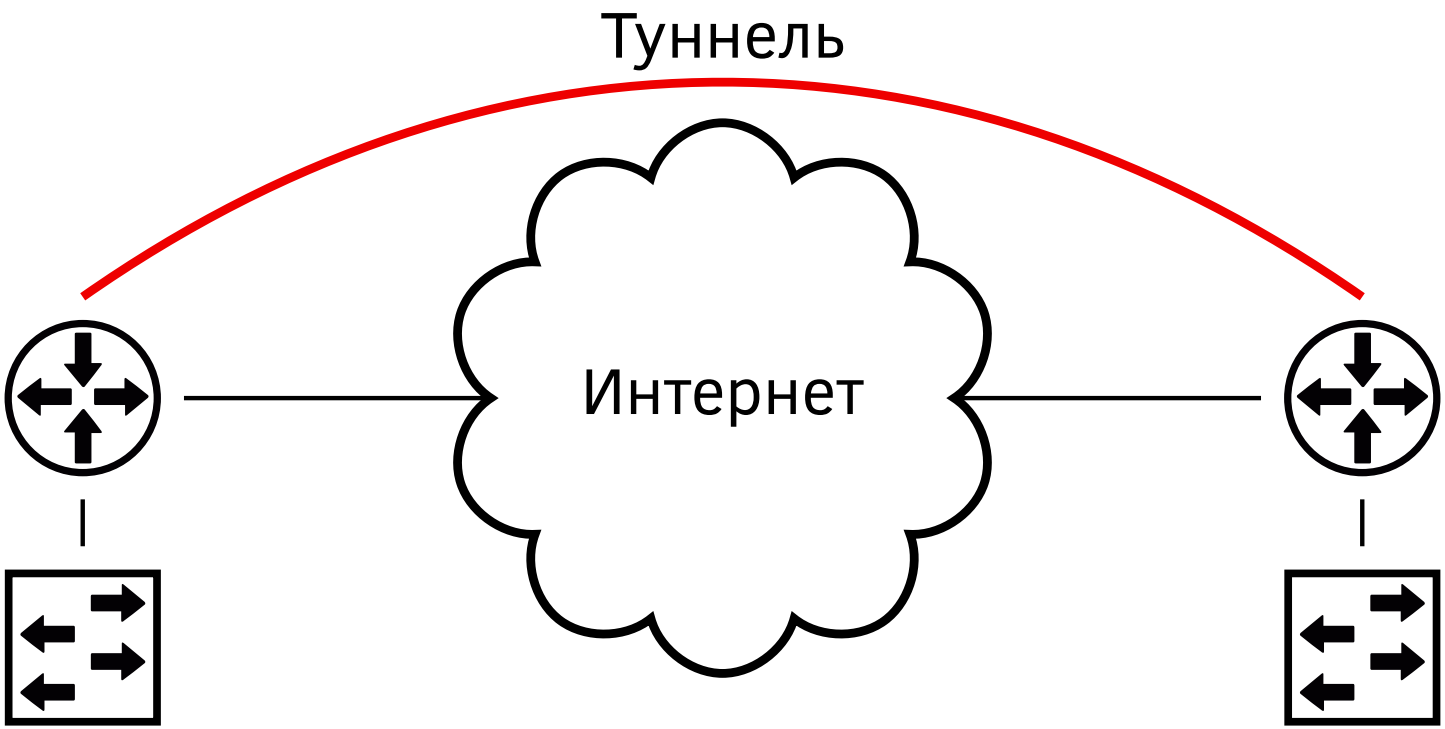
ВЧС удаленного доступа



Основные технологии: L2TP, PPTP, OpenVPN

Классификация туннелей по назначению

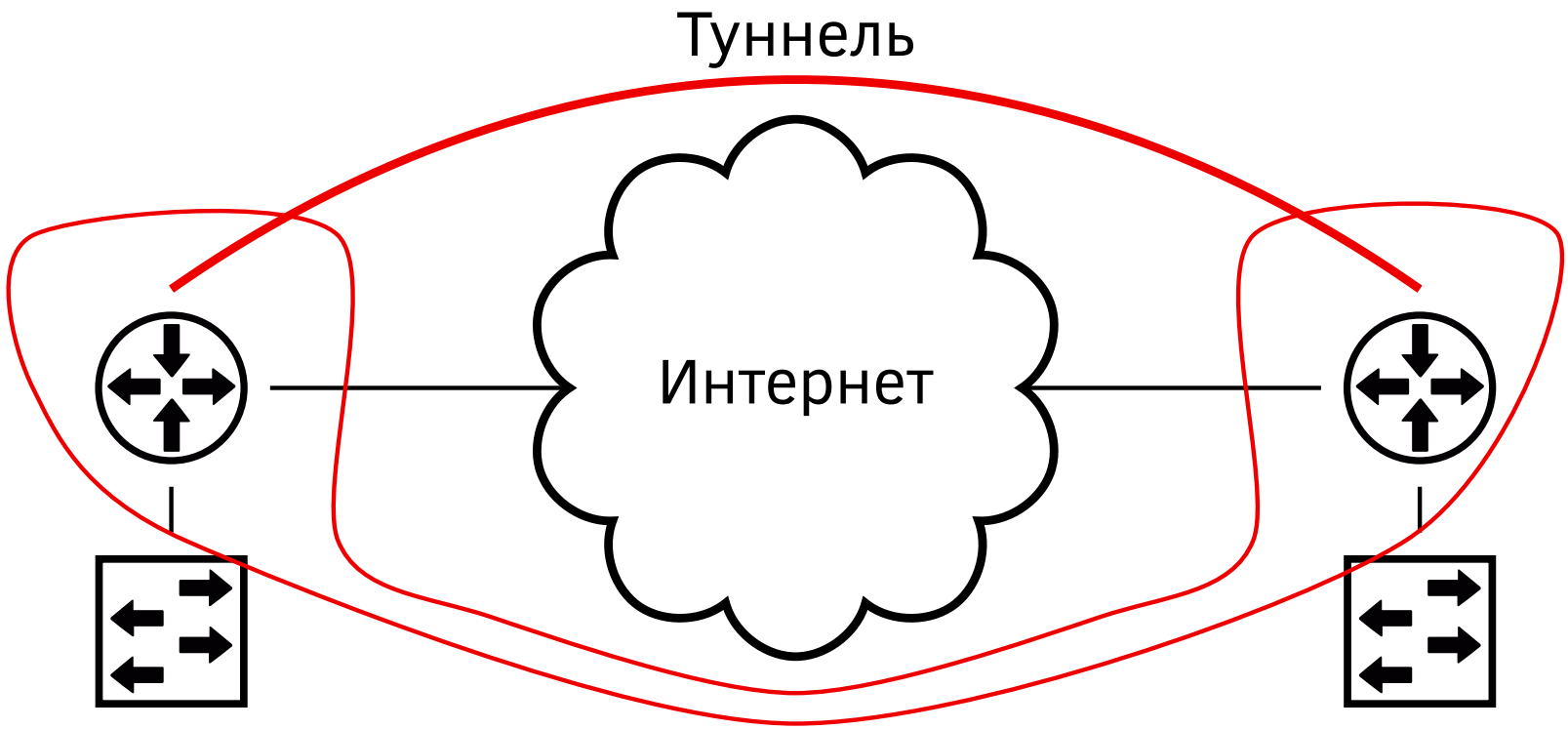
Межучасточная (site-to-site) ВЧС



Основные технологии: GRE, IPSec

Классификация туннелей по уровню инкапсулируемого протокола

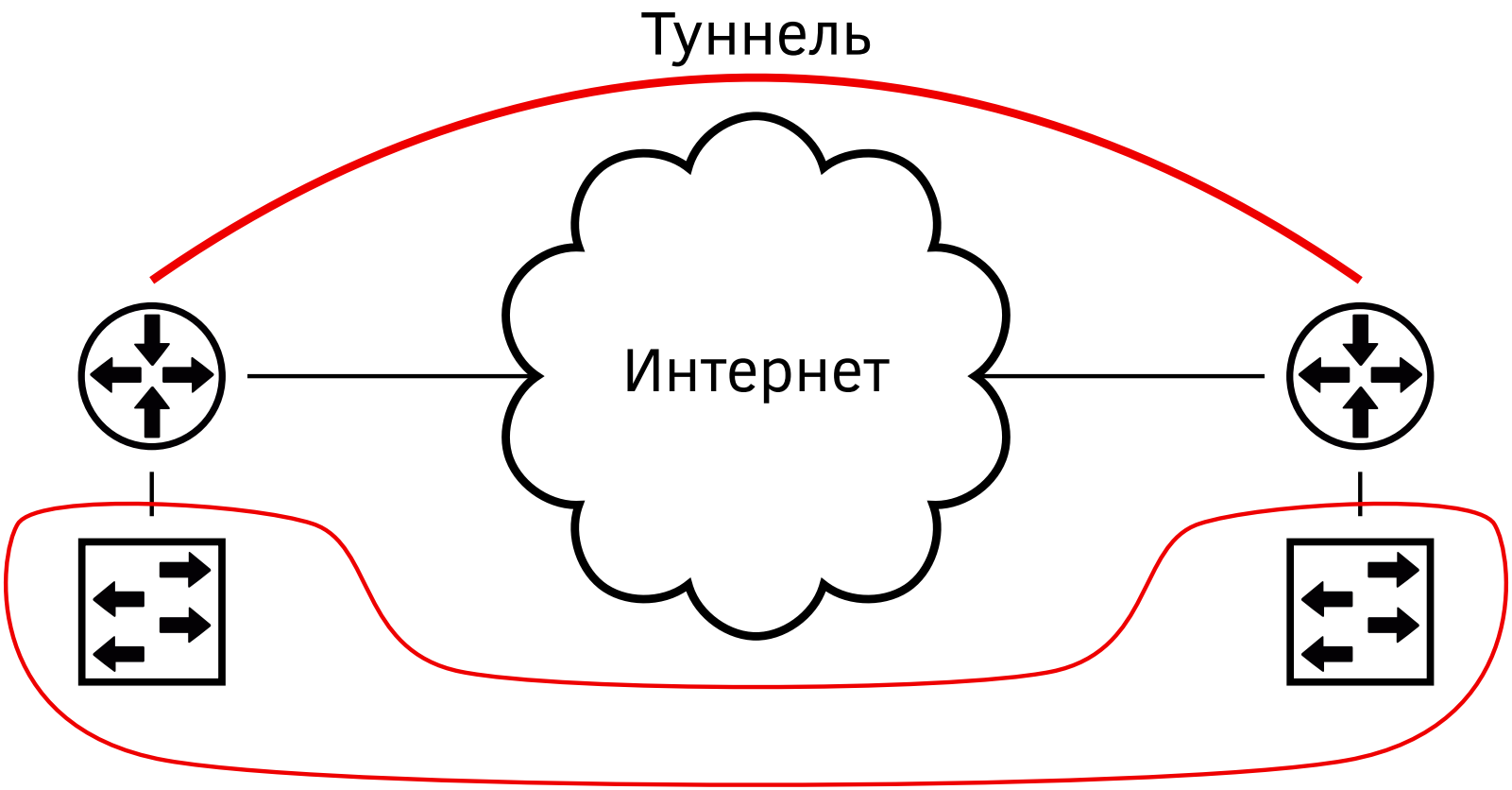
Сетевой уровень



Основные технологии: GRE, IPSec, OpenVPN

Классификация туннелей по уровню инкапсулируемого протокола

Канальный уровень



Основные технологии: L2TP, PPTP, MPPE

Структура туннельного соединения

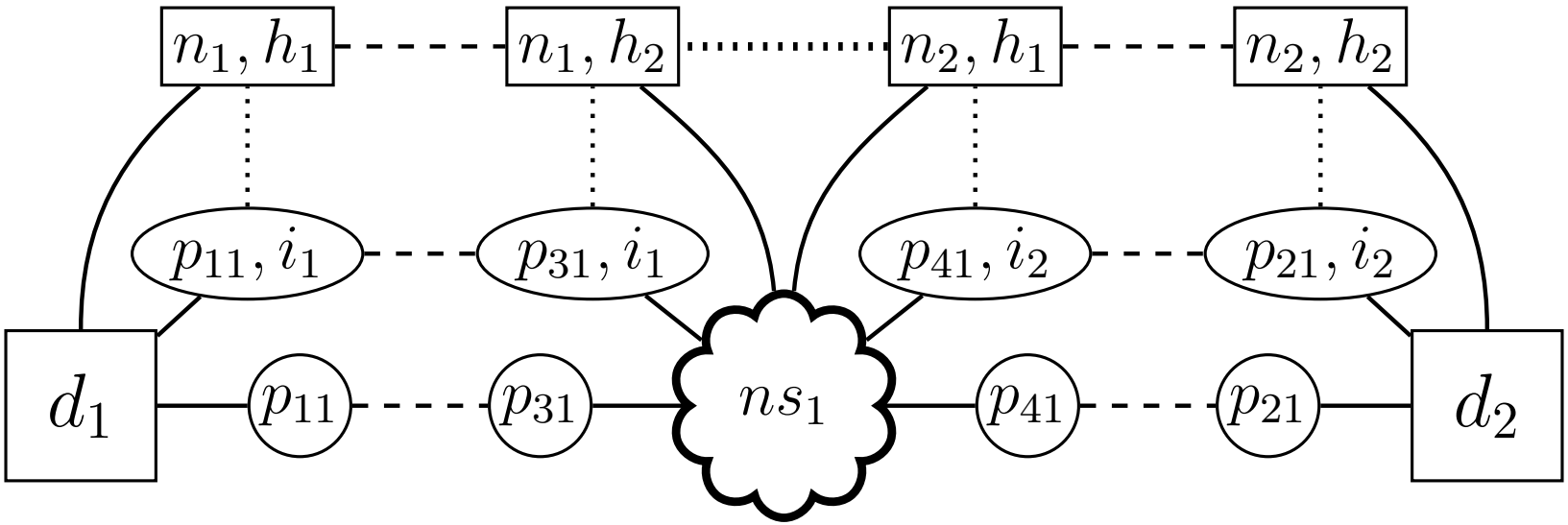
- сегменты Сети, подлежащей объединению;
- сеть-посредник;
- пограничные устройства и их интерфейсы.

Требования к расширению модели:

- моделирование соединений с Сетями других ПСУ;
- моделирование устройств и интерфейсов, осуществляющих туннелирование;
- моделирование структуры туннелей сетевого и канального уровней.

Соединения с Сетями других ПСУ

NS – множество сегментов Сетей других провайдеров, которые не являются частью описываемой Сети.



Виртуальные интерфейсы

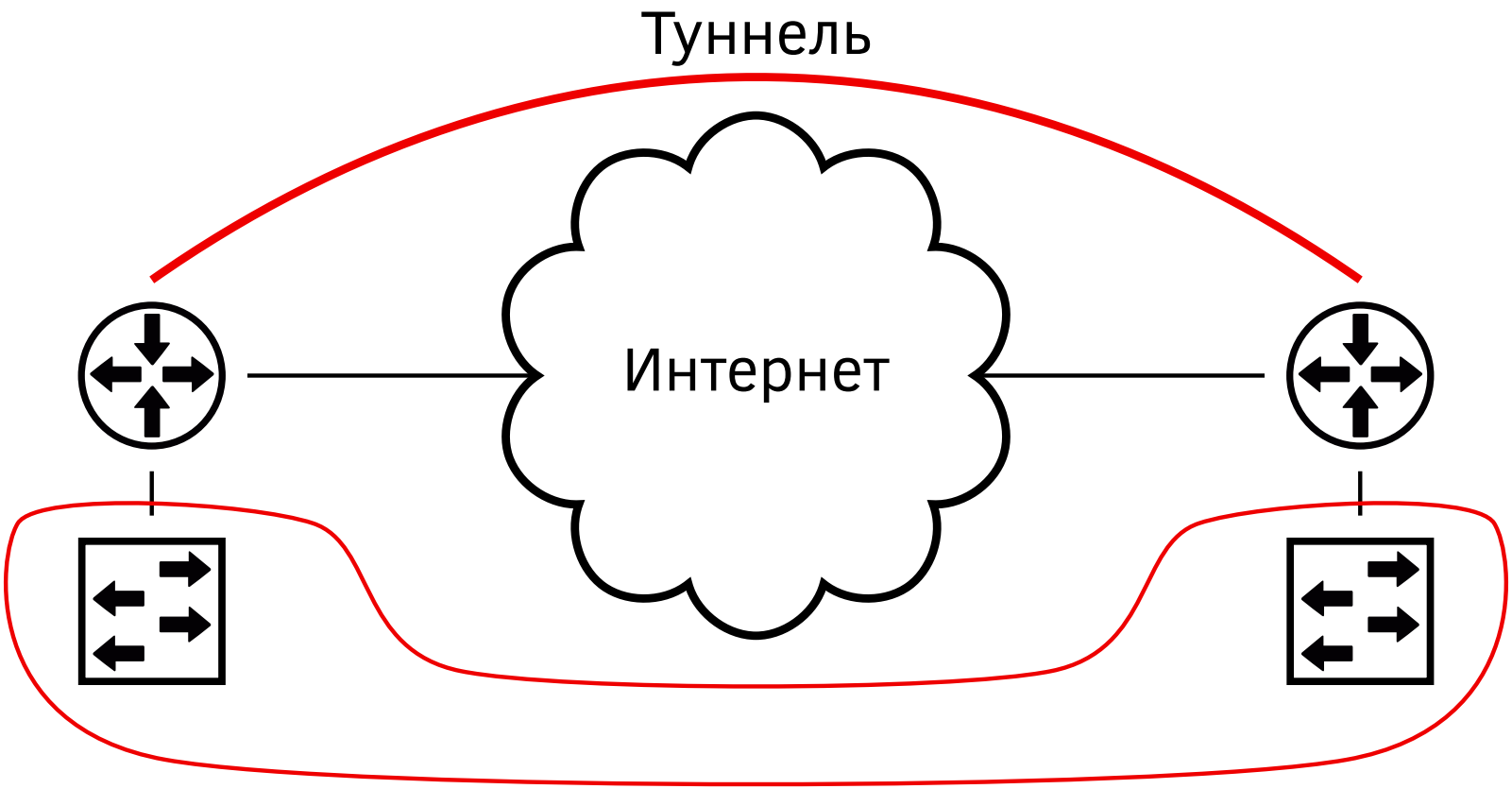
Необходимы устройствам для иммитации работы всего стека протоколов прозрачно для верхних уровней.

▷ Порт $p \in VP \subset P$ – виртуальный если он не существует физически, т. е. имитируется программными средствами. $VP \subset P$ – множество всех виртуальных портов.

▷ $VI^2 \subset I^2$ – множество интерфейсов канального уровня, построенные поверх только виртуальных портов из множества VP

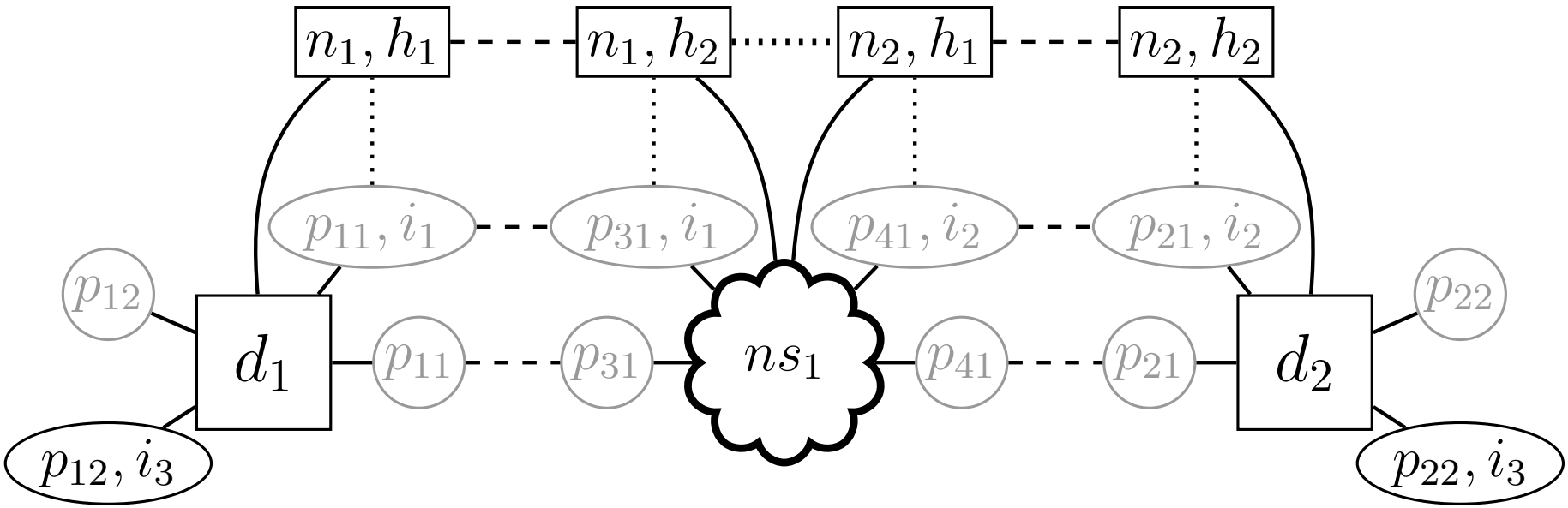
▷ $VI^3 \subset I^2$ – множество интерфейсов сетевого уровня, построенных поверх только канальных интерфейсов из множества VI^2.

Туннели канального уровня



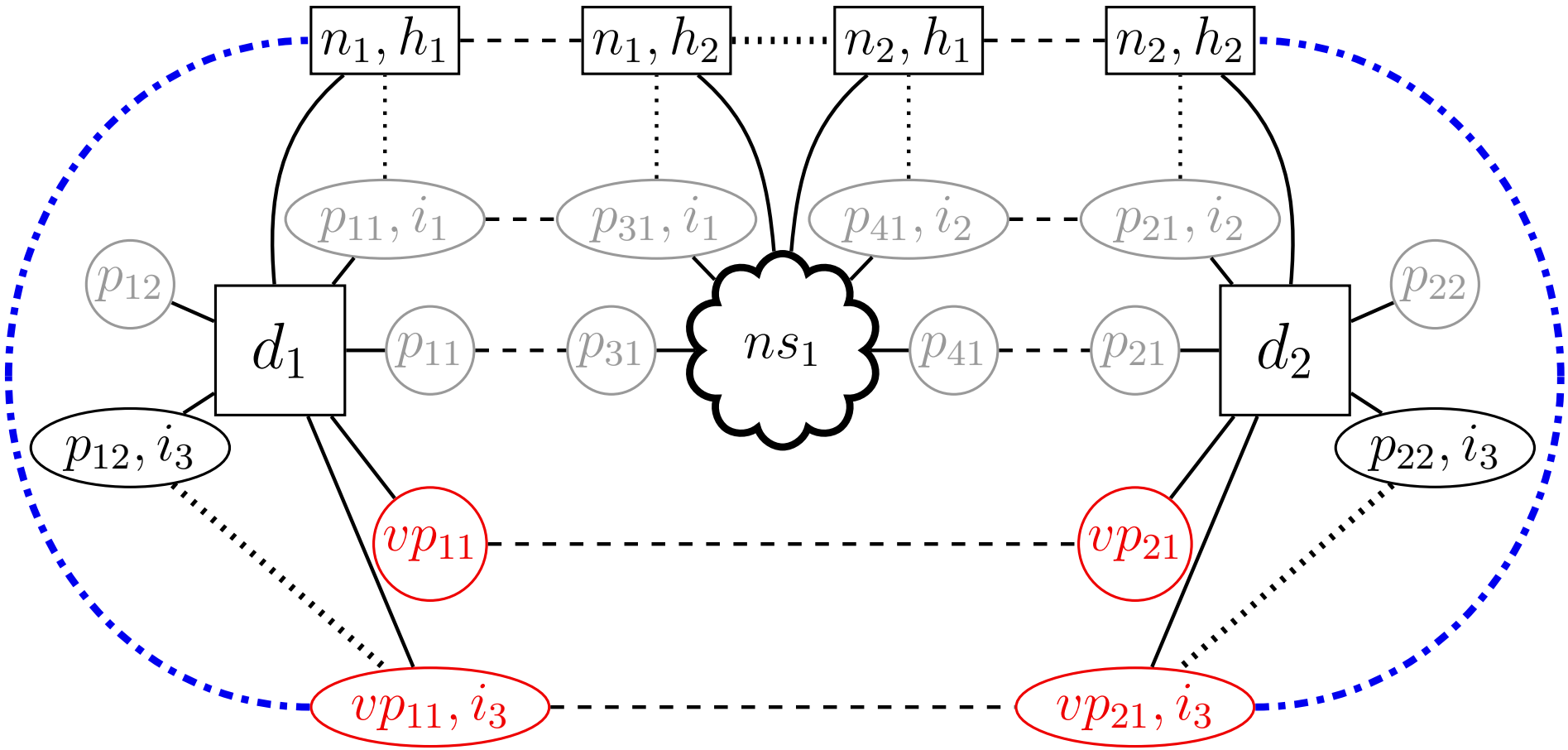
Туннели канального уровня

T^2 – множество ребер туннелирования канального уровня. Ребра между интерфейсами из VI^2 и $I^3 \setminus VI^3$.

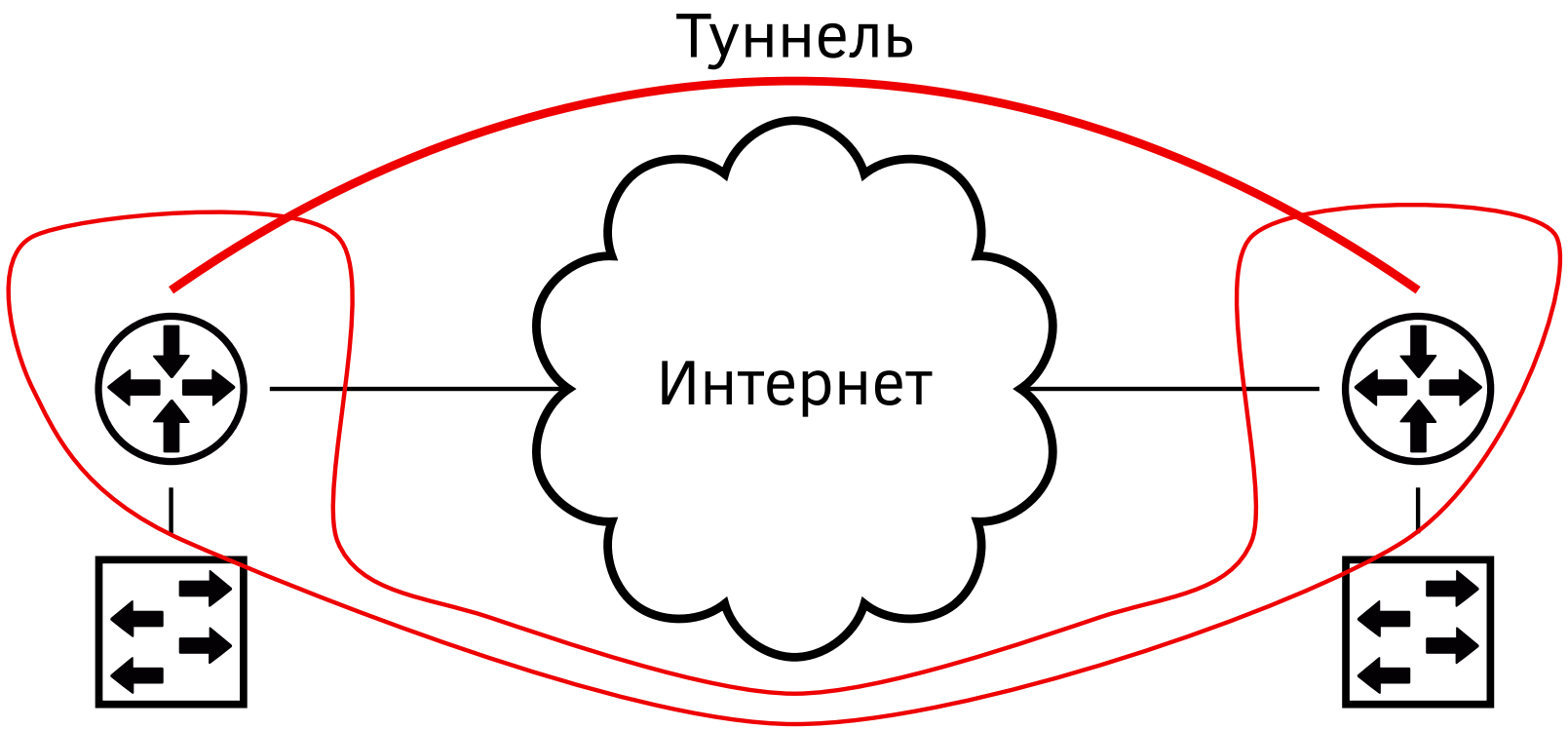


Туннели канального уровня

T^2 – множество ребер туннелирования канального уровня.
Ребра между интерфейсами из VI^2 и $I^3 \setminus VI^3$.

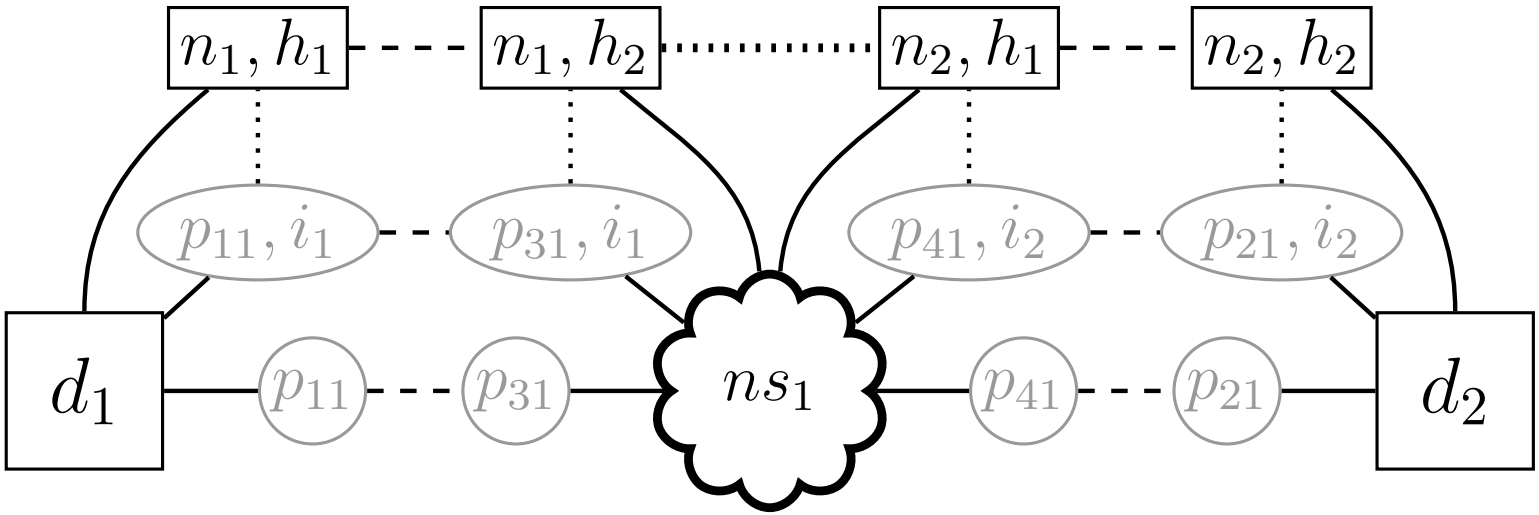


Туннели сетевого уровня



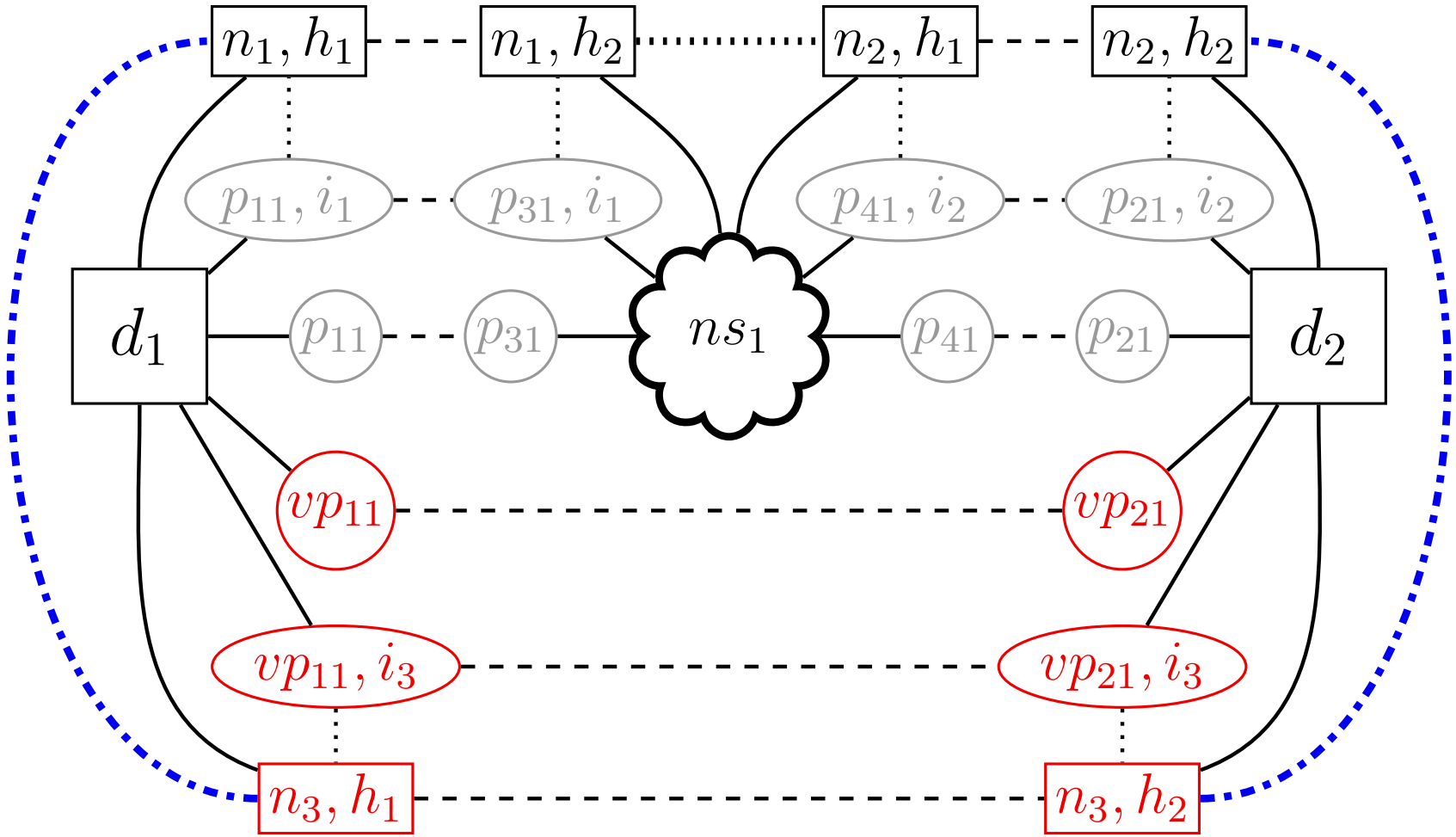
Туннели сетевого уровня

T^3 – множество ребер туннелирования сетевого уровня.
Ребра между интерфейсами из VI^3 и $I^3 \setminus VI^3$.

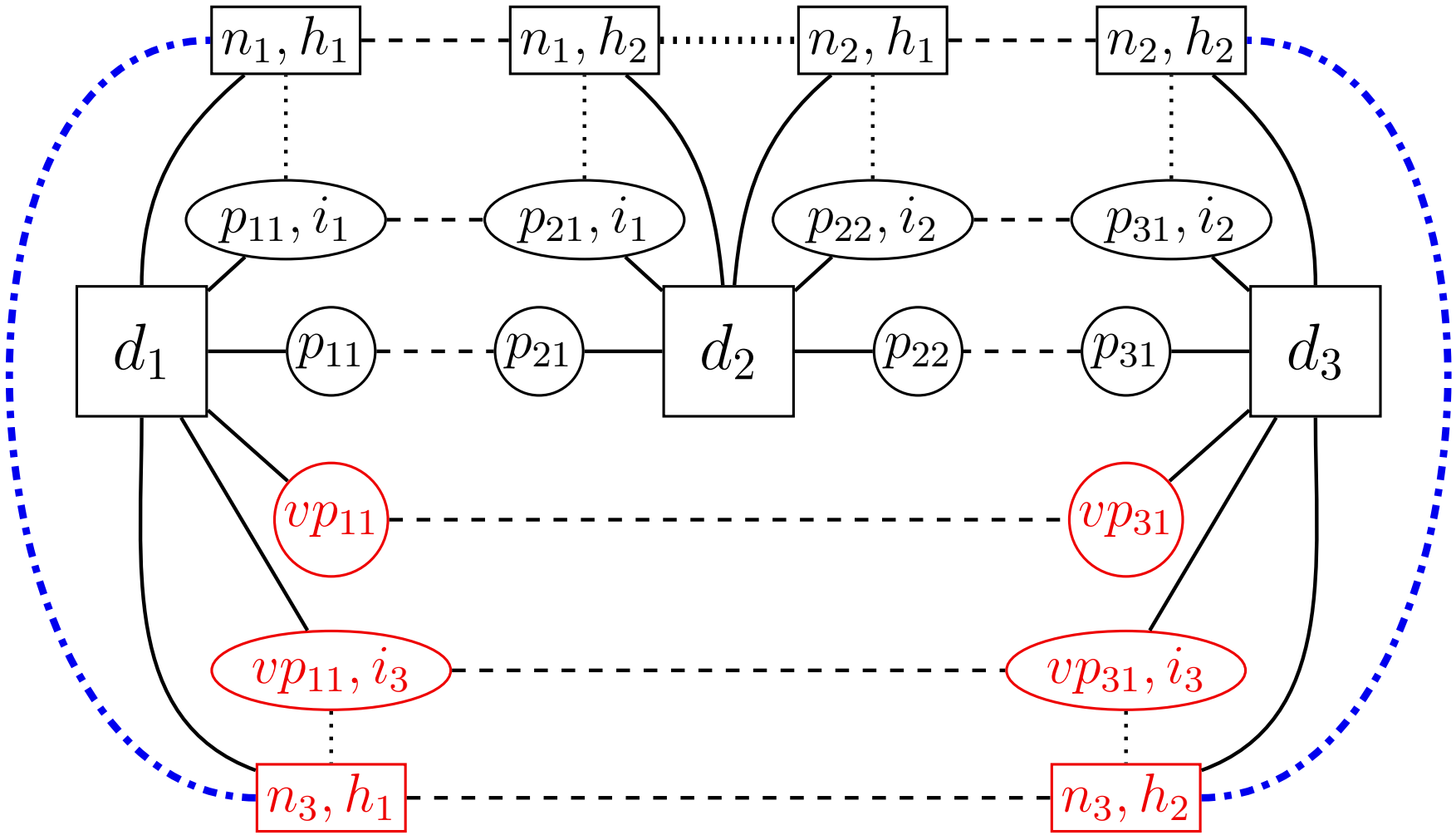


Туннели сетевого уровня

T^3 – множество ребер туннелирования сетевого уровня.
Ребра между интерфейсами из VI^3 и $I^3 \setminus VI^3$.



Туннели через собственную Сеть



Алгоритм построения графа Сети

1. **Сбор данных, предоставляемых устройствами**
   - Данные об устройствах (адреса портов, имена и т.д.)
   - Данные о конфигурации VLAN и IP
   - Данные о связях
2. **Идентификация вершин графа**
   - Построение известных устройств, портов, интерфейсов, сетевых интерфейсов, ребер ассоциации, ребер коммутации
3. **Построение ребер графа**
   1. Дополнение собранных данных по свойствам модели
   2. Построение ребер по дополненным данным и свойствам модели
   3. Устранение неопределенностей

Методы построения связей туннелирования

Данные доступны в MIB (Management Information Base) сетевых устройств

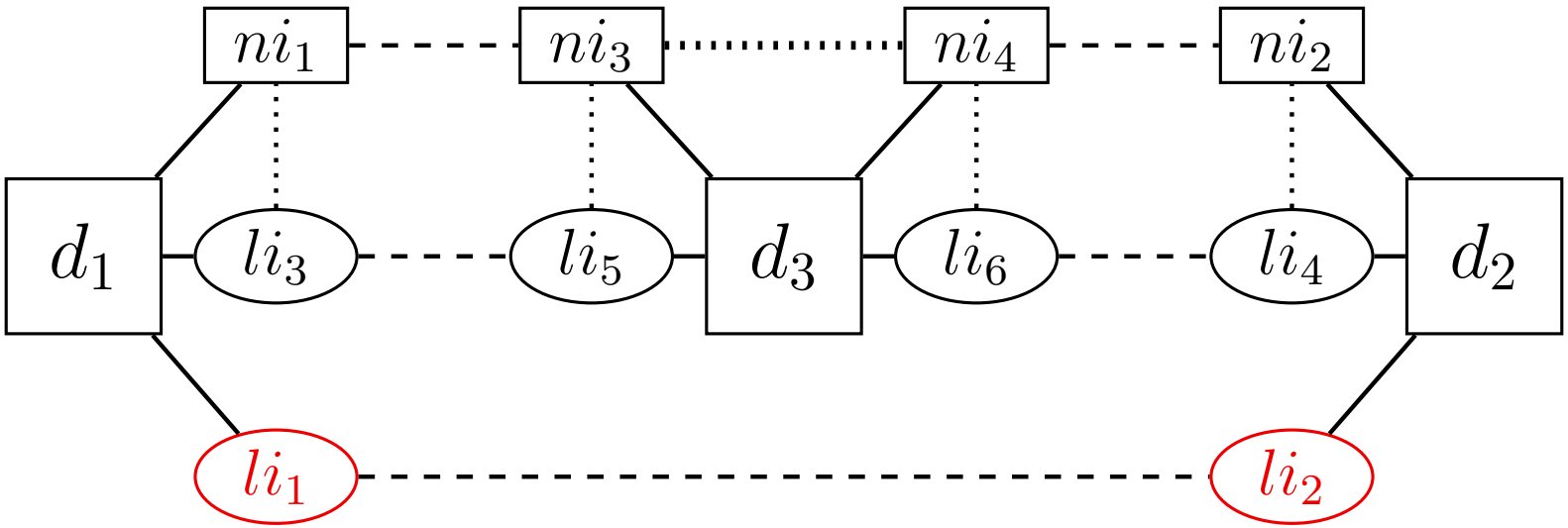
Могут быть получены с помощью протокола SNMP (Simple Network Management Protocol)

- данные о виртуальных портах: IF-MIB;
- данные о связях туннелирования: TUNNEL-MIB, L2TP-MIB и др.;
- данные о связях между виртуальными портами и интерфейсами: LLDP-MIB, CDP-MIB, BRIDGE-MIB, IP-MIB.

Обнаружение туннелей канального уровня

Утверждение 1

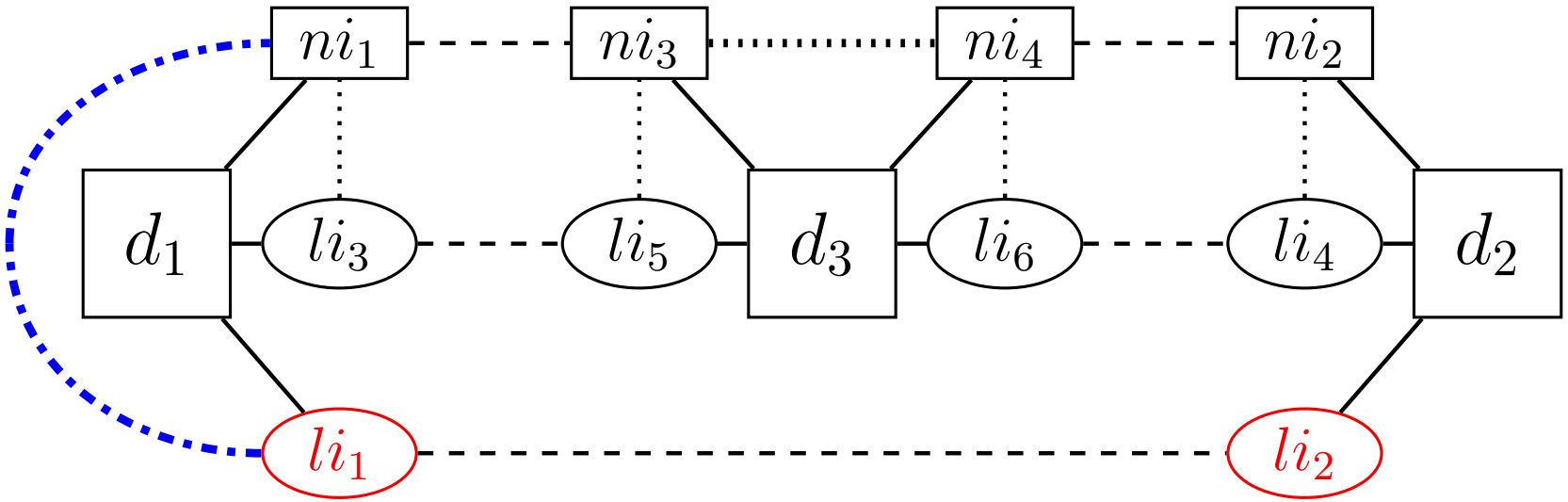
Если $li_1 \in VI^2$ устройства d_1 соединен с li_2 устройства d_2 и $\exists\,!\, ni_1$ устройства d_1 такой, что от него существует путь до ni_2 устройства d_2, то между li_1 и ni_1 есть ребро T^2.



Обнаружение туннелей канального уровня

Утверждение 1

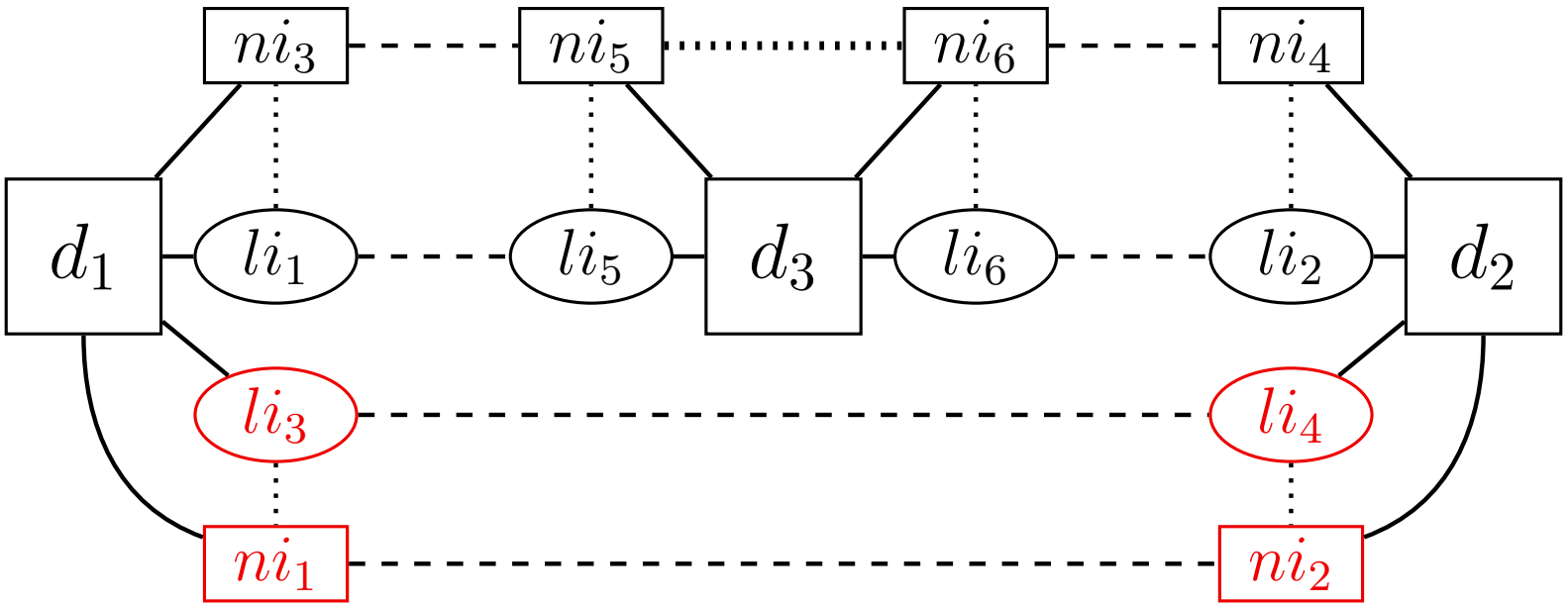
Если $li_1 \in VI^2$ устройства d_1 соединен с li_2 устройства d_2 и $\exists\,!\, ni_1$ устройства d_1 такой, что от него существует путь до ni_2 устройства d_2, то между li_1 и ni_1 есть ребро T^2.



Обнаружение туннелей сетевого уровня

Утверждение 2

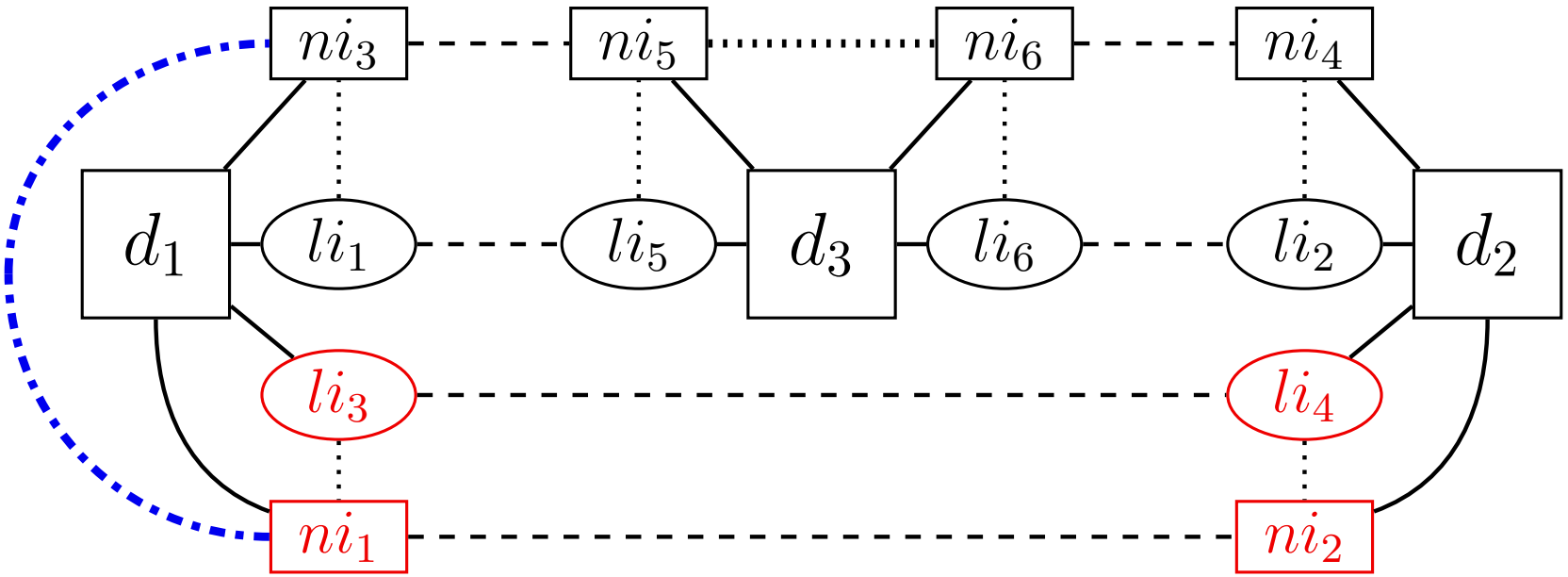
Если $ni_1 \in VI^3$ устройства d_1 соединен с ni_2 устройства d_2 и $\exists\,!\, ni_3$ устройства d_1 такой, что от него существует путь до ni_4 устройства d_2, то между ni_1 и ni_3 есть ребро T^3.



Обнаружение туннелей сетевого уровня

Утверждение 2

Если $ni_1 \in VI^3$ устройства d_1 соединен с ni_2 устройства d_2 и $\exists\,!\, ni_3$ устройства d_1 такой, что от него существует путь до ni_4 устройства d_2, то между ni_1 и ni_3 есть ребро T^3.



Алгоритм построения графа Сети

1. *Сбор данных, предоставляемых устройствами*
   - Данные об устройствах (адреса портов, имена и т.д.)
   - Данные о конфигурации VLAN и IP
   - Данные о связях
   - **Данные о туннелировании**
2. *Идентификация вершин графа*
   - Построение известных устройств, портов, интерфейсов, ребер ассоциации и коммутации, **виртуальных портов и интерфейсов, ребер туннелирования**
3. *Построение ребер графа*
   1. Дополнение собранных данных по свойствам модели
   2. Построение ребер по дополненным данным и свойствам
   3. Устранение неопределенностей
   4. **Построение ребер туннелирования по утверждениям 1, 2**

Результаты

- разработано расширение обобщенной графовой модели структуры Сети для учета ВЧС;
- разработан метод автоматизированного построения структурных элементов ВЧС в графе структуры Сети.

Планы на будущее

- реализовать метод построения ВЧС в графе Сети в рамках существующей системы построения графа;
- разработать расширения модели для учета беспроводных сетей, виртуальных машин и multicast.

Благодарность научным руководителям –
Ю. А. Богоявленскому и А. С. Колосову

Спасибо за внимание!

andreev@cs.petrsu.ru