69-я Всероссийская (с международным участием) научная конференция обучающихся и молодых ученых

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

Графовая модель виртуальных частных сетей в ИКТ-инфраструктуре локального поставщика сетевых услуг

Докладчик:

маг. 2-го года, Антон Андреев

Руководители:

к.т.н., доцент Ю. А. Богоявленский

ст.преп. А. С. Колосов

Виртуальные частные сети и лПСУ

лПСУ — организации, сопровождающие ИКТ-инфраструктуру (Сеть) и предоставляющие набор сетевых услуг для собственных нужд.

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

Цели построения ВЧС в Сетях лПСУ:

- защищенное подключение собственных пользователей;
- ограниченное подключение сторонних пользователей;
- защищенная передача данных между двумя узлами Сети;
- защищенное объединение сегментов Сетей филиалов через сеть другого ПСУ.

Задачи сетевого управления в Сетях с ВЧС

- проектирование и масштабирование топологии;
- обеспечение надежности, отказоустойчивости и достаточной пропускной способности соединений;
- моделирование и документирование Сети;
- локализация точек отказа;
- автоматическое представление структуры Сети.

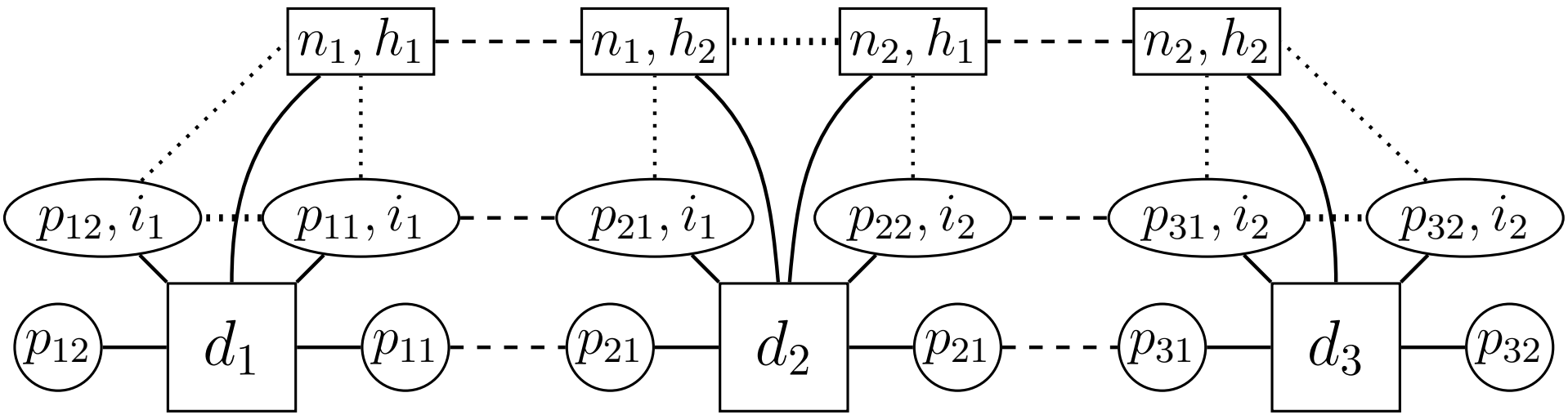
Решение многих задач требует описания структуры Сети:

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

Самый распространенный способ представления — граф.

Обобщенная 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 при автоматизации построения графа структуры сети.



Цели и задачи

Цель

Расширение существующей модели для отражения элементов и связей, служащих для построения ВЧС в Сетях лПСУ; модификация процесса построения графа структуры Сети для учета ВЧС.

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.

Механизмы ВЧС

- управление доступом к Сети;
- шифрование данных;
- туннелирование.

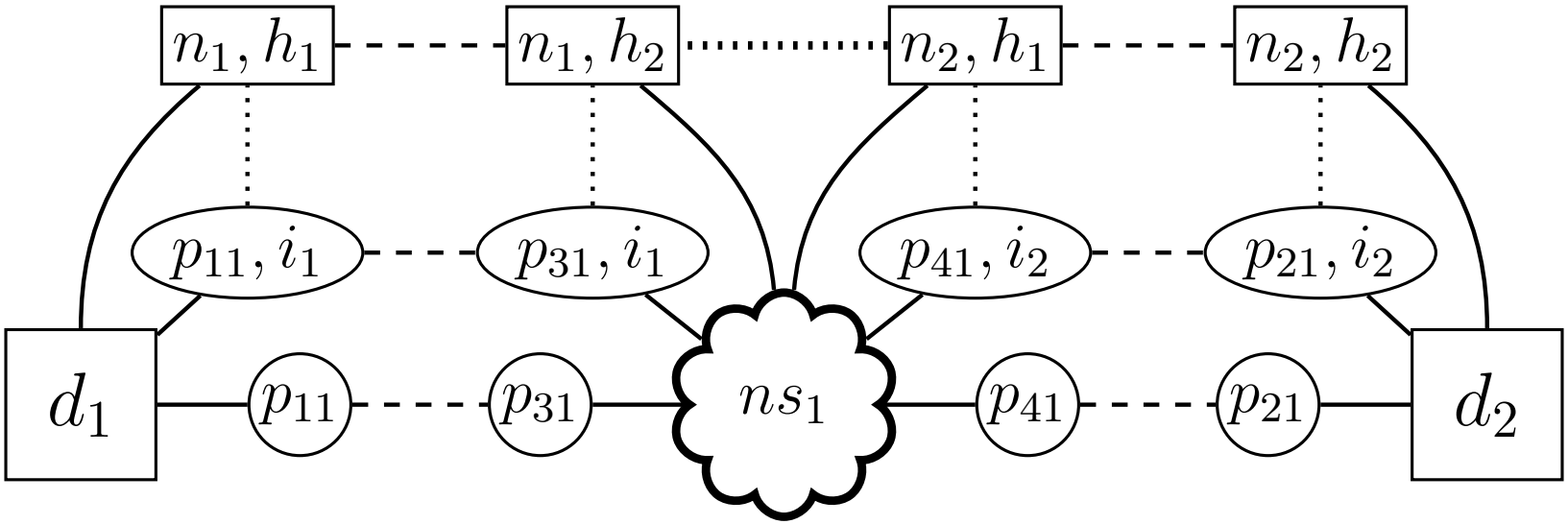
Технологии управления доступом и шифрования не оказывают влияния на структуру Сети.

Туннелирование:
передача инкапсулированных пакетов канального или сетевого уровня через логическое соединение с сохранением всех заголовков.

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

Соединения с Сетями внешних ПСУ

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



Виртуальные интерфейсы

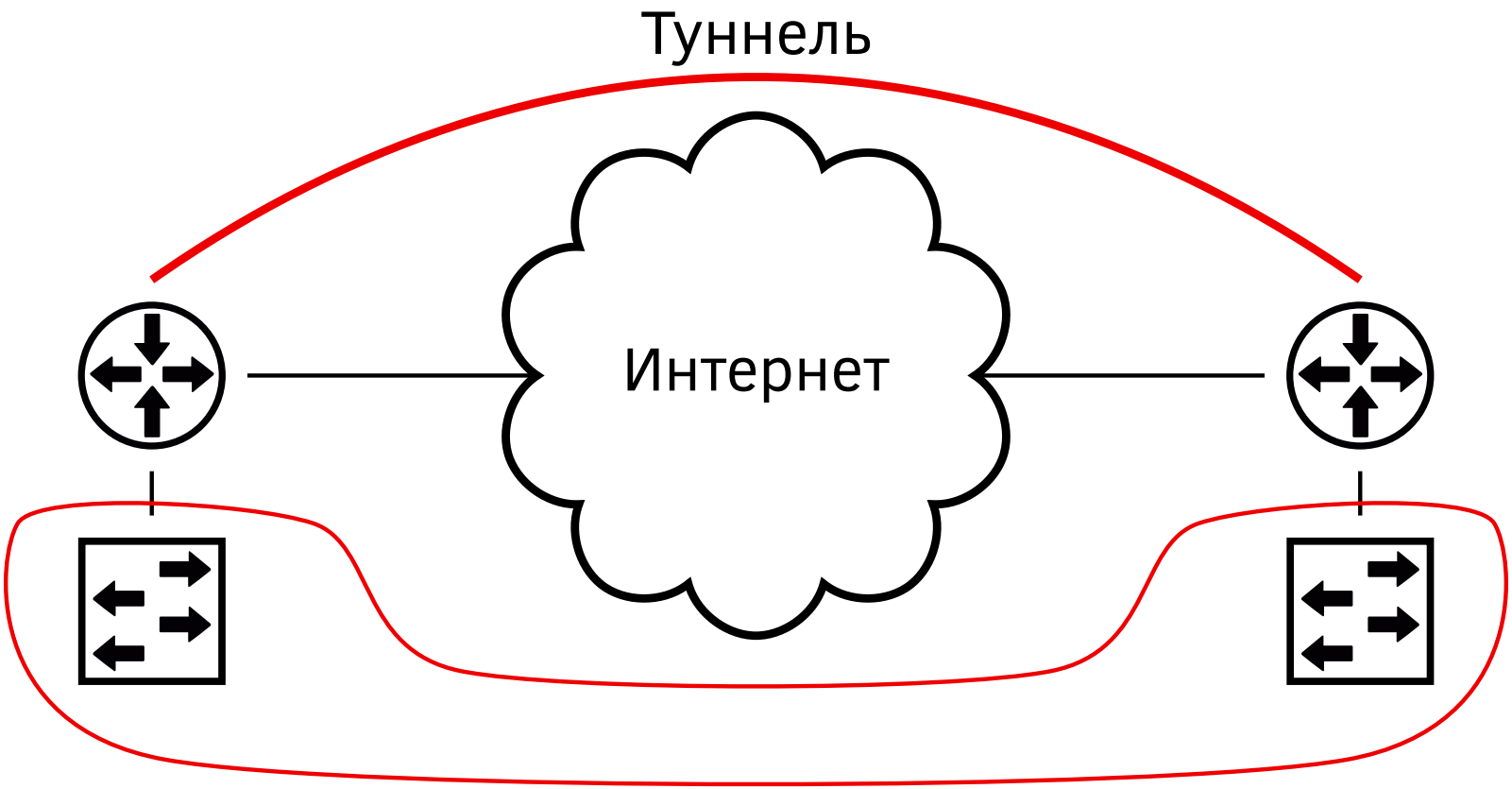
Являются точками входа/выхода для данных, передаваемых по туннелю.

▷ 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

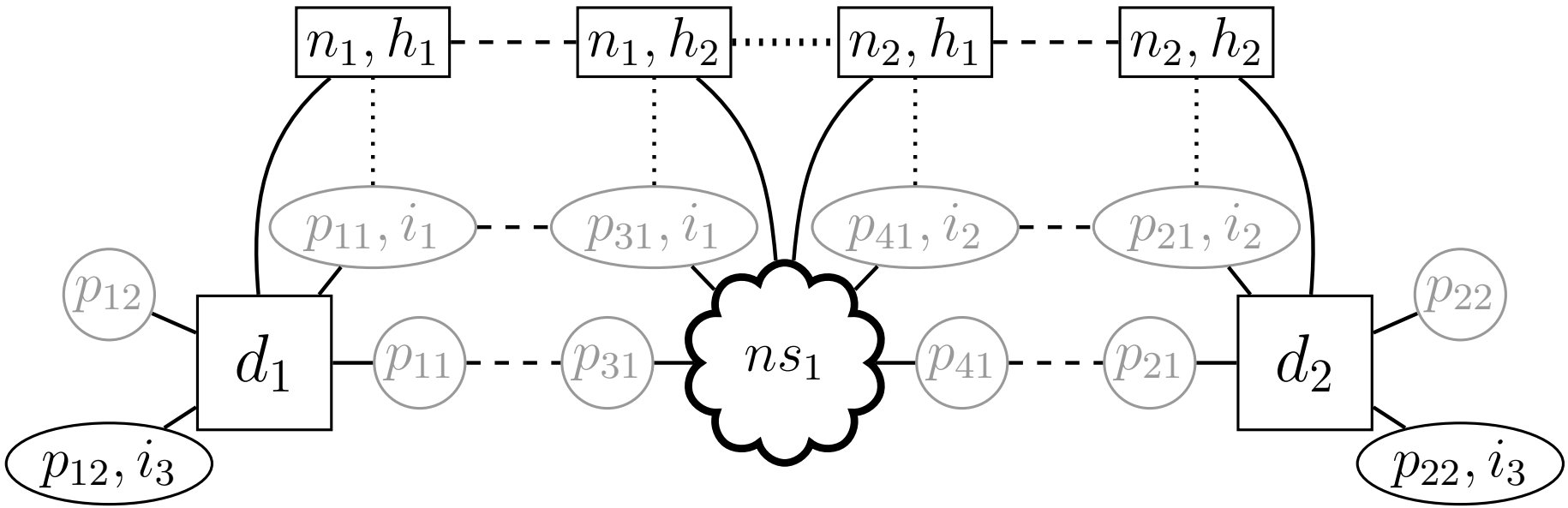
▷ $VI^3 \subset I^2$ – множество интерфейсов сетевого уровня, построенных поверх только канальных интерфейсов из множества VI^2.

Туннели канального уровня



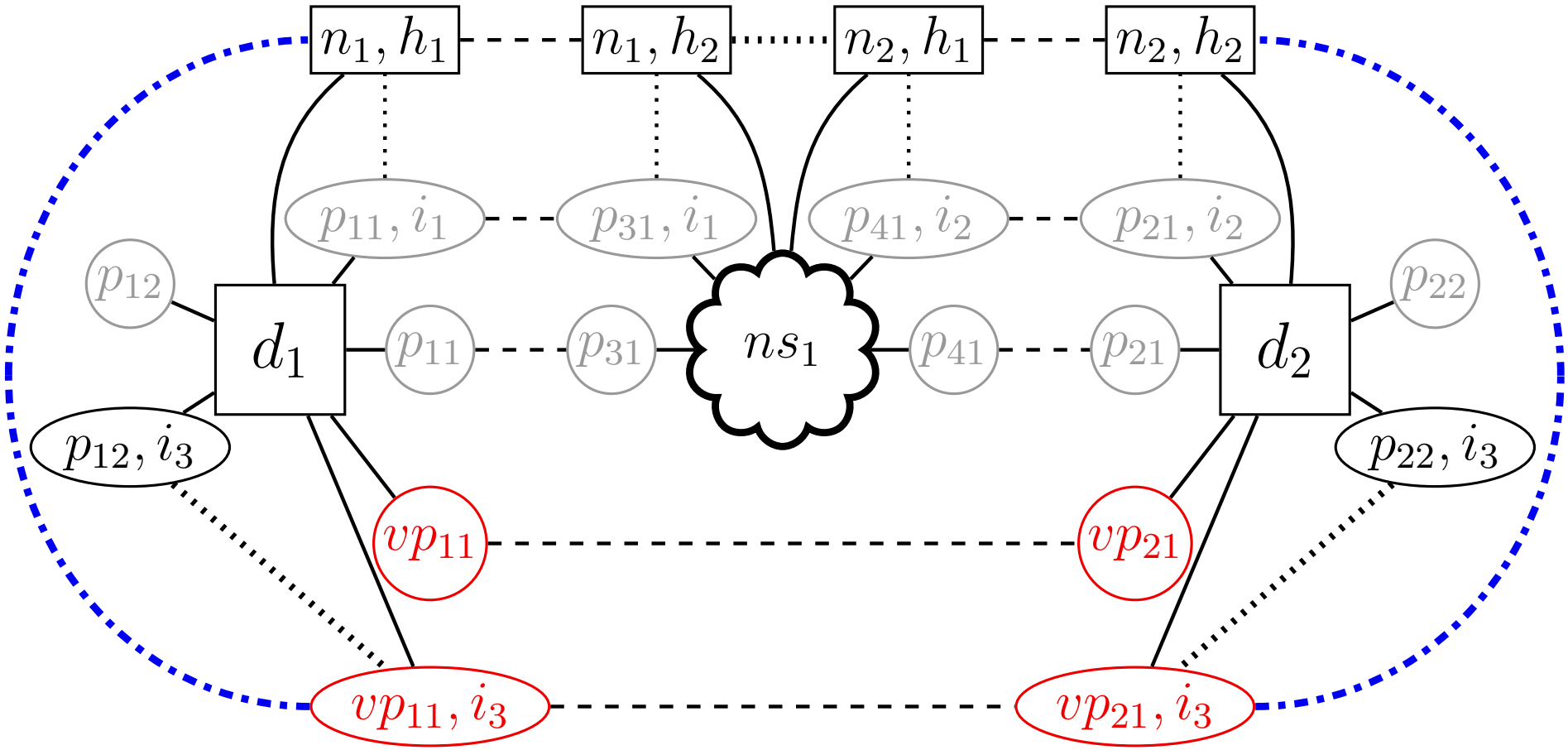
Туннели канального уровня

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

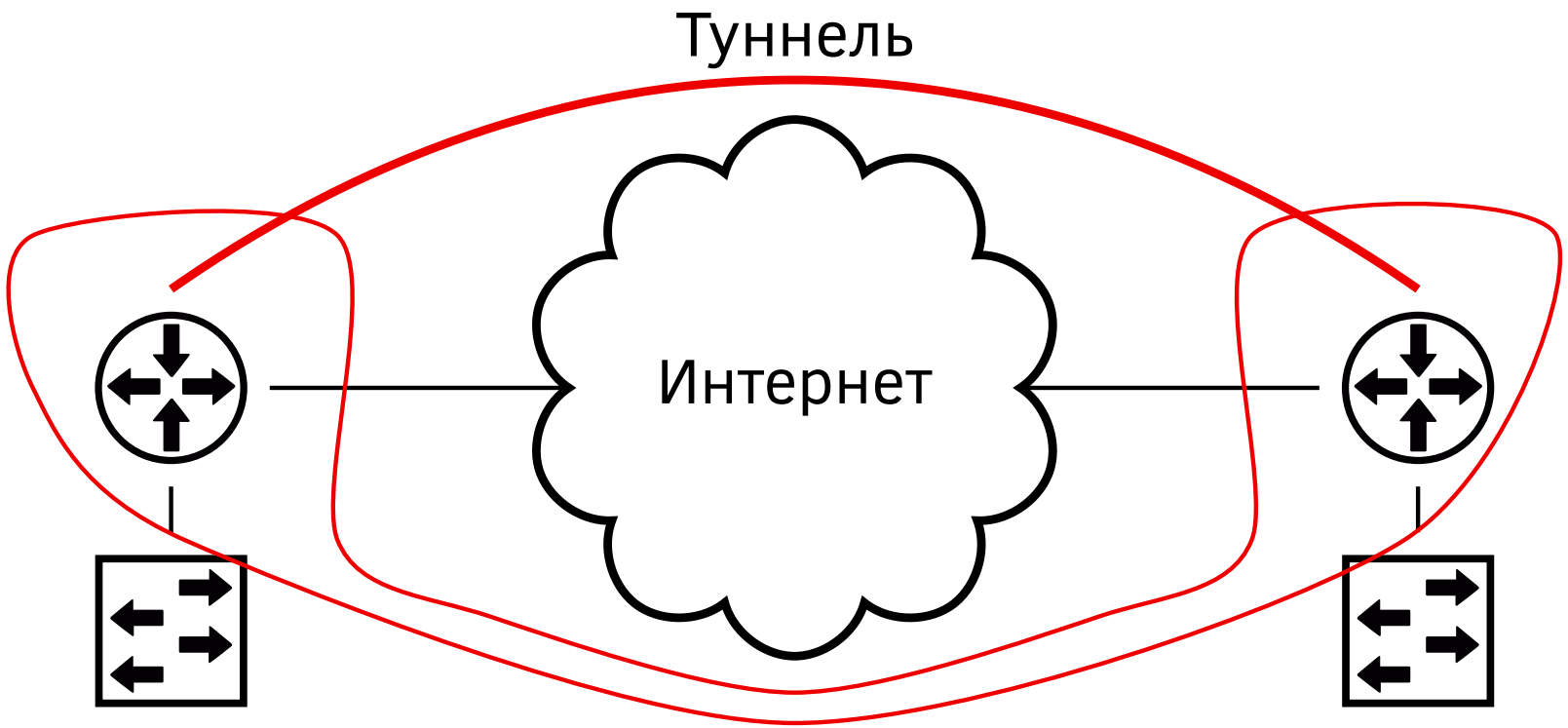


Туннели канального уровня

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

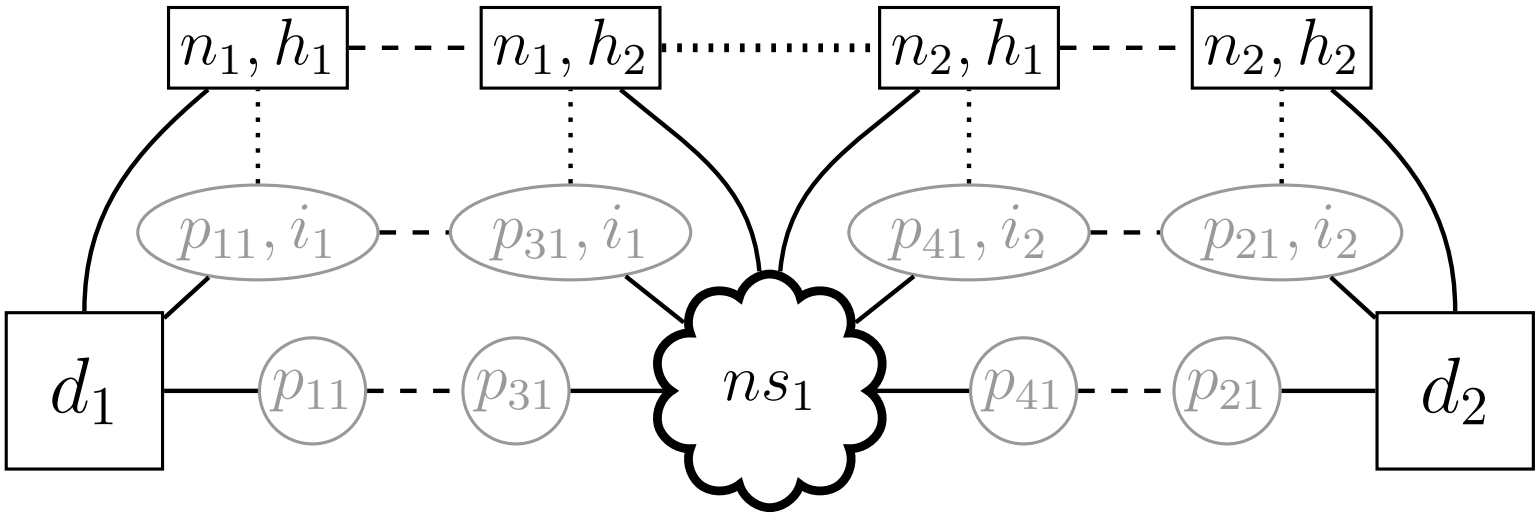


Туннели сетевого уровня



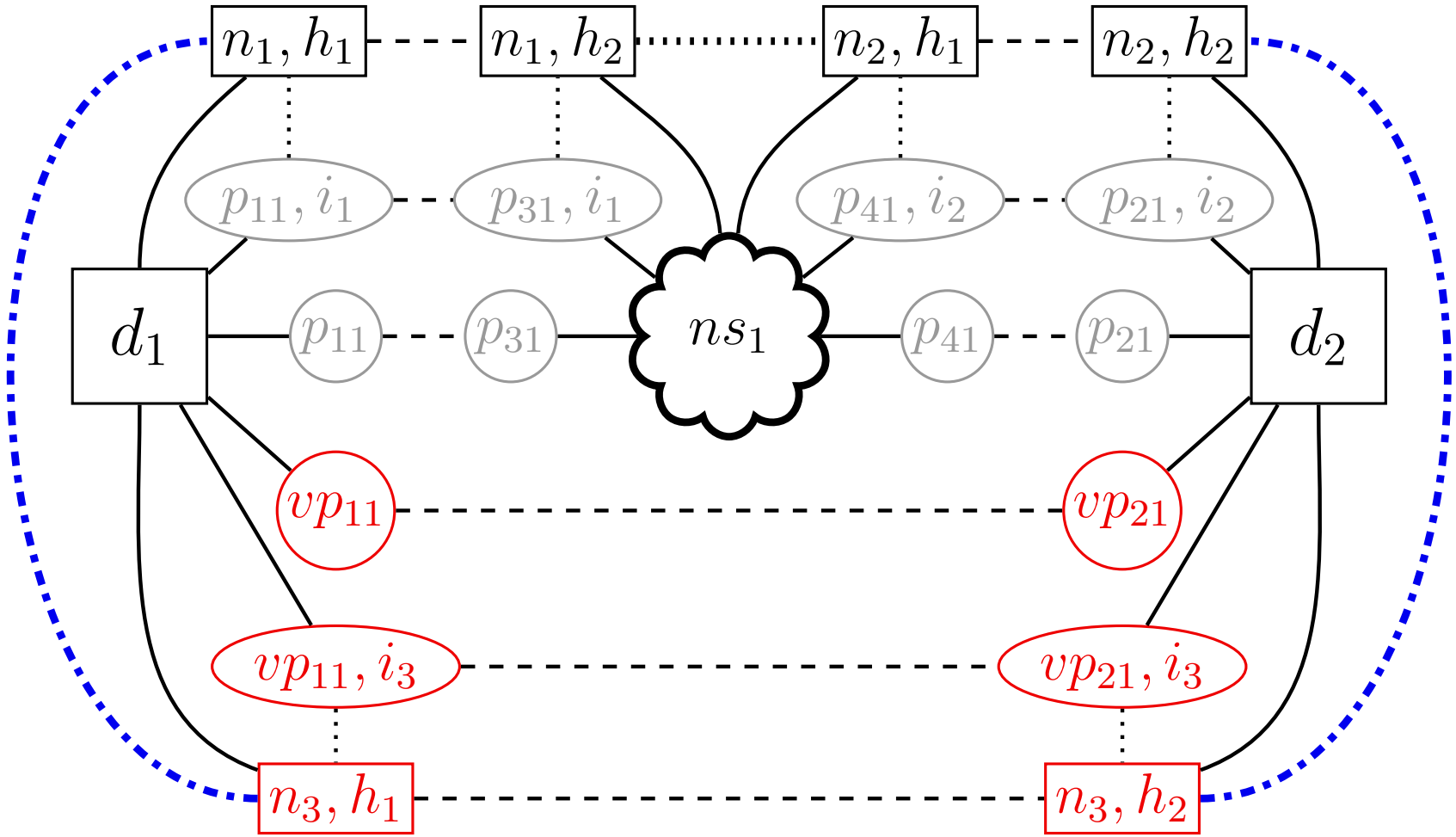
Туннели сетевого уровня

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 $I^3 \setminus VI^3$.



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

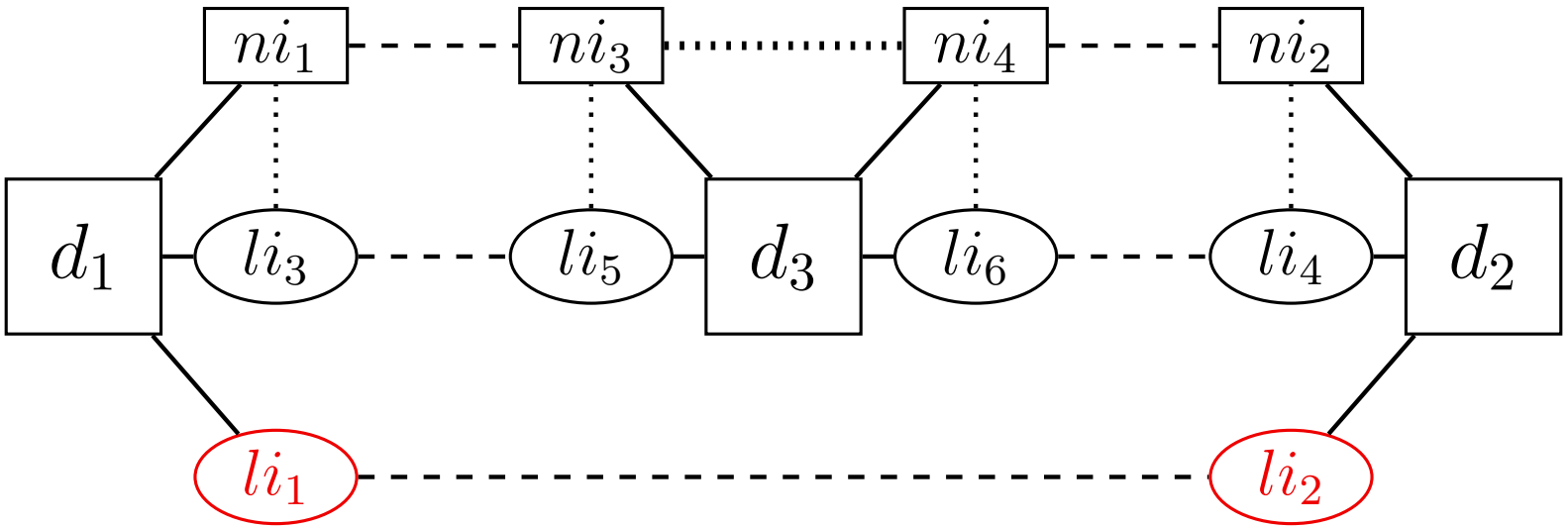
Могут быть получены с помощью протокола SNMP (Simple Network Management Protocol)

- 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

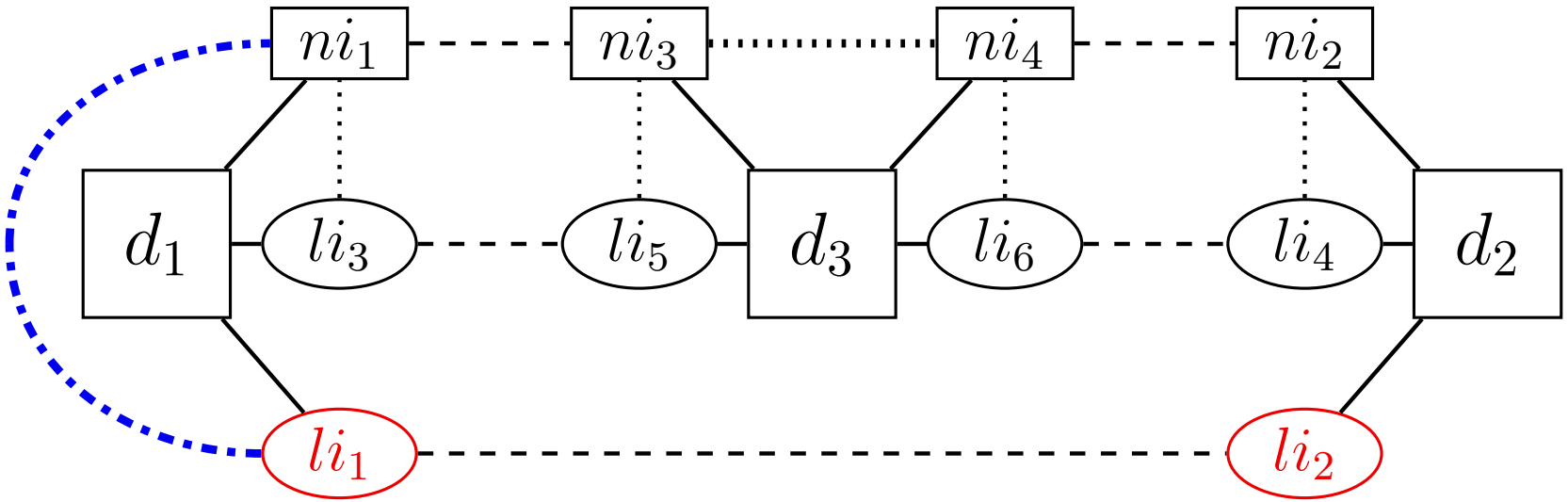
Пусть $li_1 \in VI^2$ устройства d_1 соединен с li_2 устройства d_2 и нет ни одного основанного на одном из них интерфейса сетевого уровня. Если $\exists\,!\, ni_1$ устройства d_1 такой, что от него существует путь до ni_2 устройства d_2, то между li_1 и ni_1 есть ребро T^2.



Обнаружение туннелей канального уровня

Утверждение 1

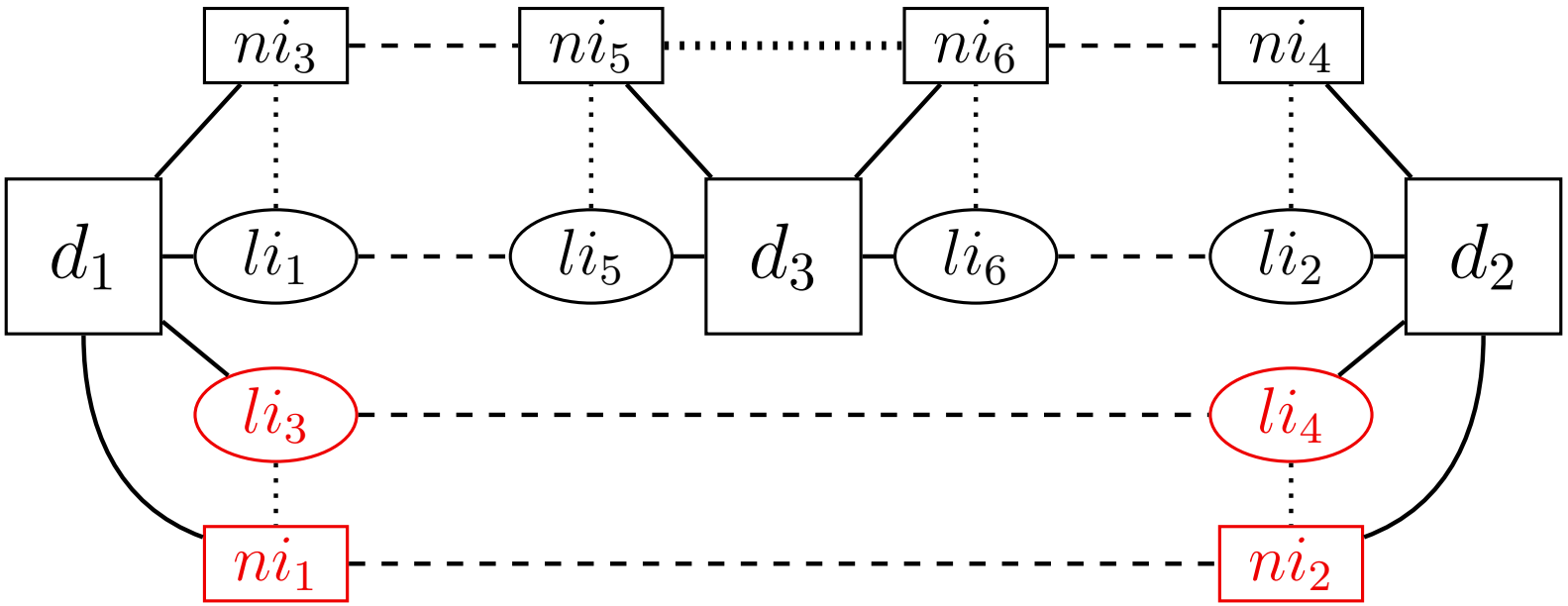
Пусть $li_1 \in VI^2$ устройства d_1 соединен с li_2 устройства d_2 и нет ни одного основанного на одном из них интерфейса сетевого уровня. Если $\exists\,!\, ni_1$ устройства d_1 такой, что от него существует путь до ni_2 устройства d_2, то между li_1 и ni_1 есть ребро T^2.



Обнаружение туннелей сетевого уровня

Утверждение 2

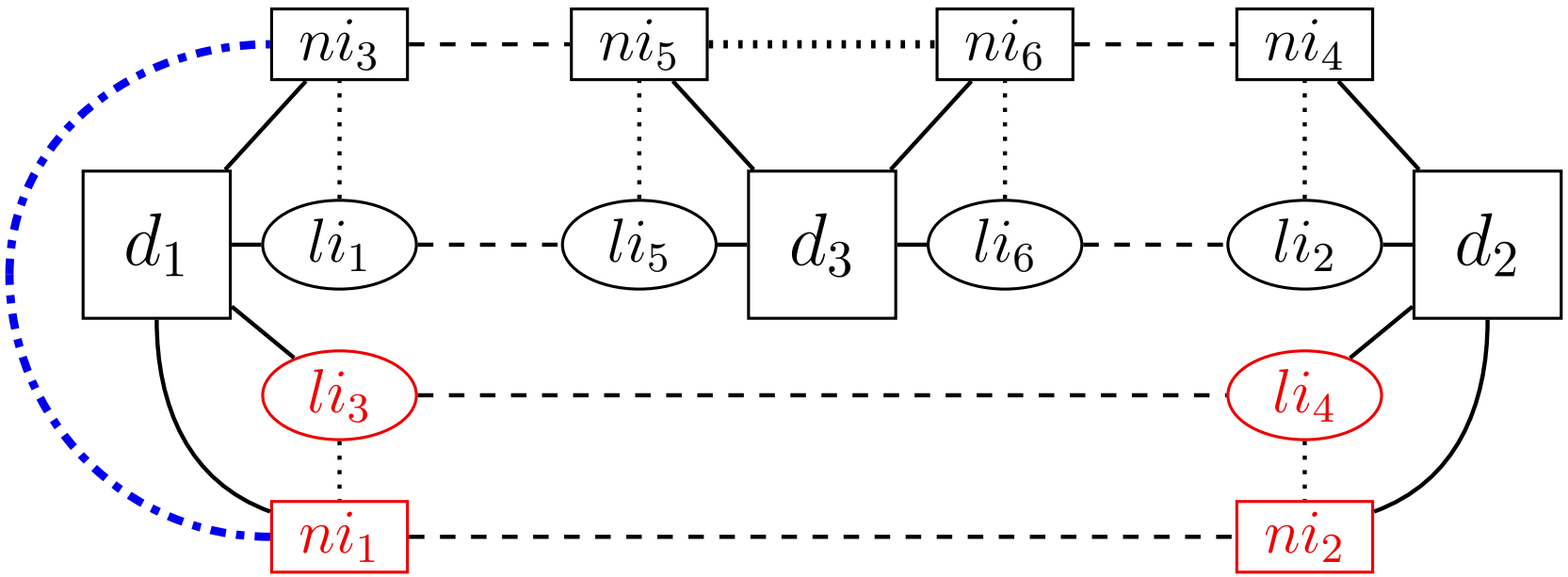
Если $ni_1 \in VI^3$ устройства d_1 соединен с ni_2 устройства d_2 и $\exists\,!\, ni_3$ устройства d_1 такой, что от него существует путь до ni_4 устройства d_2, то между ni_1 и ni_3 есть ребро T^3.



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

разработать расширения модели для отражения технологии multiprotocol label switching (MPLS)

Спасибо за внимание!

andreev@cs.petrsu.ru

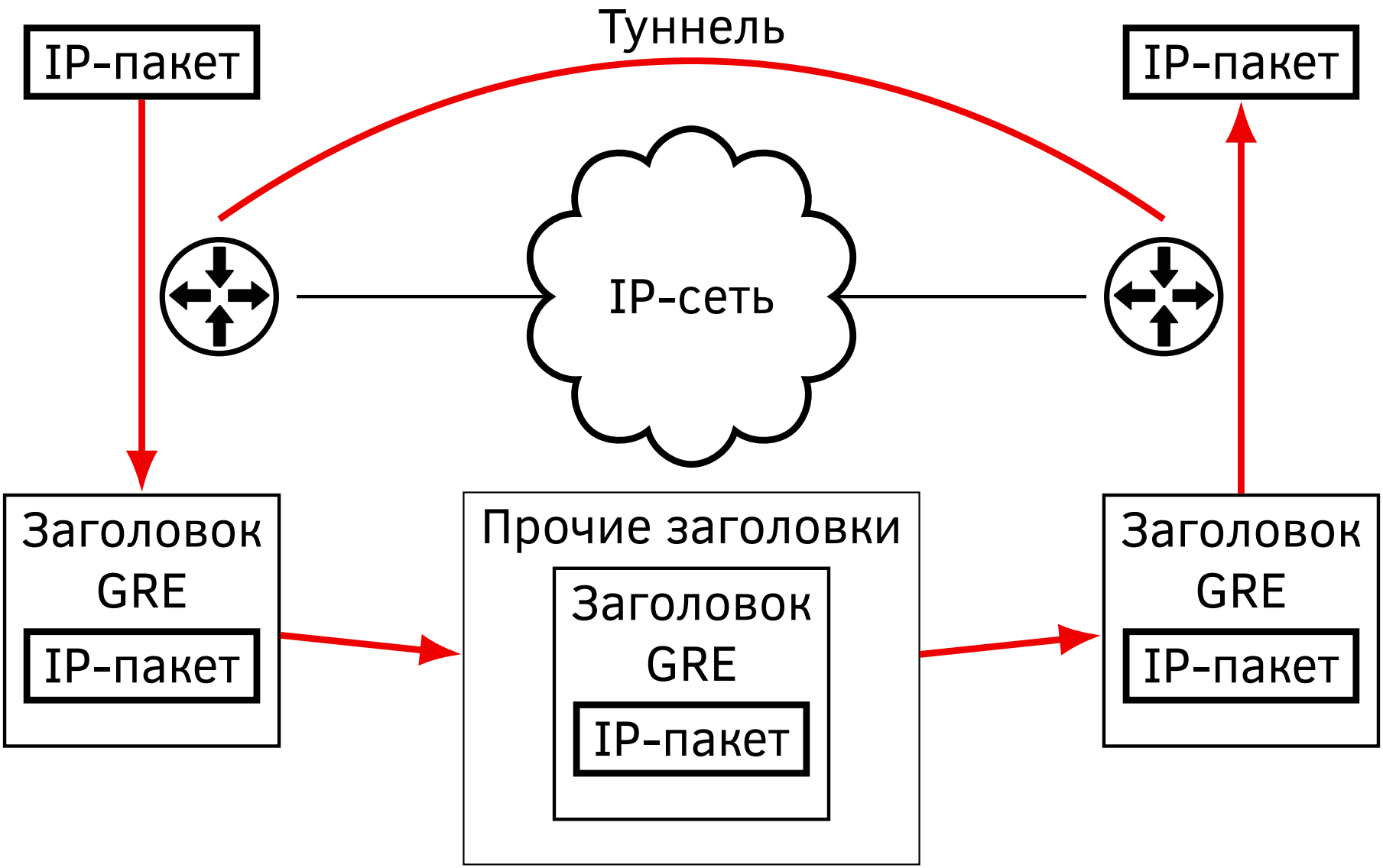
Графовые модели структуры Сетей с ВЧС

Существующие модели:

- представляют только один из уровеней OSI;
- не описывают VLAN, способы агрегирования каналов и маршрутизации;
- игнорируют возможную блокировку каналов.

Существующие модели для автоматизации построения графа структуры Сети не учитывают ВЧС.

Туннелирование



Классификация туннелей

По уровню несущего протокола:

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

По назначению:

- ВЧС удаленного доступа: L2TP, PPTP, OpenVPN
- Межучасточная (site-to-site) ВЧС: GRE, IPSec

По уровню инкапсулируемого протокола:

- Сетевой уровень: GRE, IPSec, OpenVPN
- Канальный уровень: L2TP, PPTP, MPPE