Построение VPN соединения
с балансировкой и резервированием,
используя двух провайдеров с обеих сторон

(Building VPN connection
with ISP redundancy)

Russia, Moscow
Company: ООО «Роутерз»
Mikhail Moskalev

Построение VPN соединения с балансировкой и резервированием

Цель:

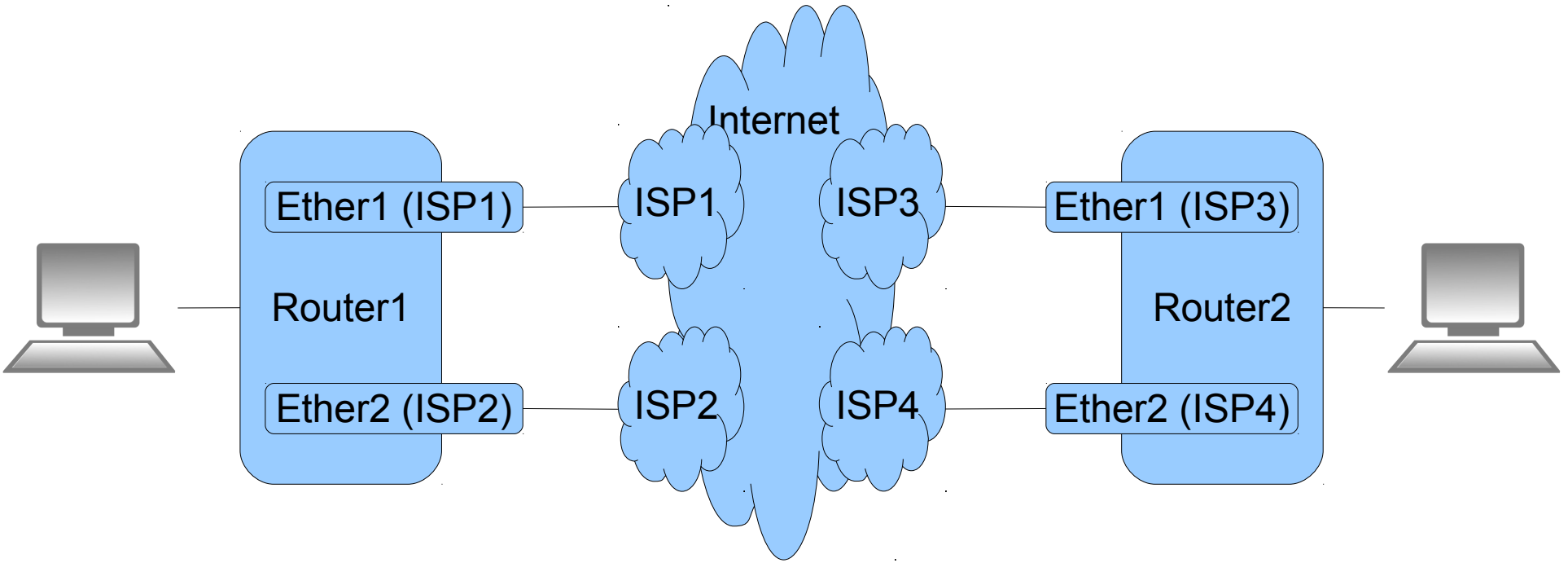
Соединить две LAN с помощью VPN, использую двух интернет провайдеров с каждой стороны с резерврованием и балансировкой нагрузки.

Проблема:

Часто подключение офиса к Интернет не надёжно. Перерывы в предоставлении услуг могут достигать 1 - 5 часов. Но для бизнеса отключение связи даже на час может быть чувствительно.

Building VPN connection with redundancy

Имеется по два провайдера с каждой стороны

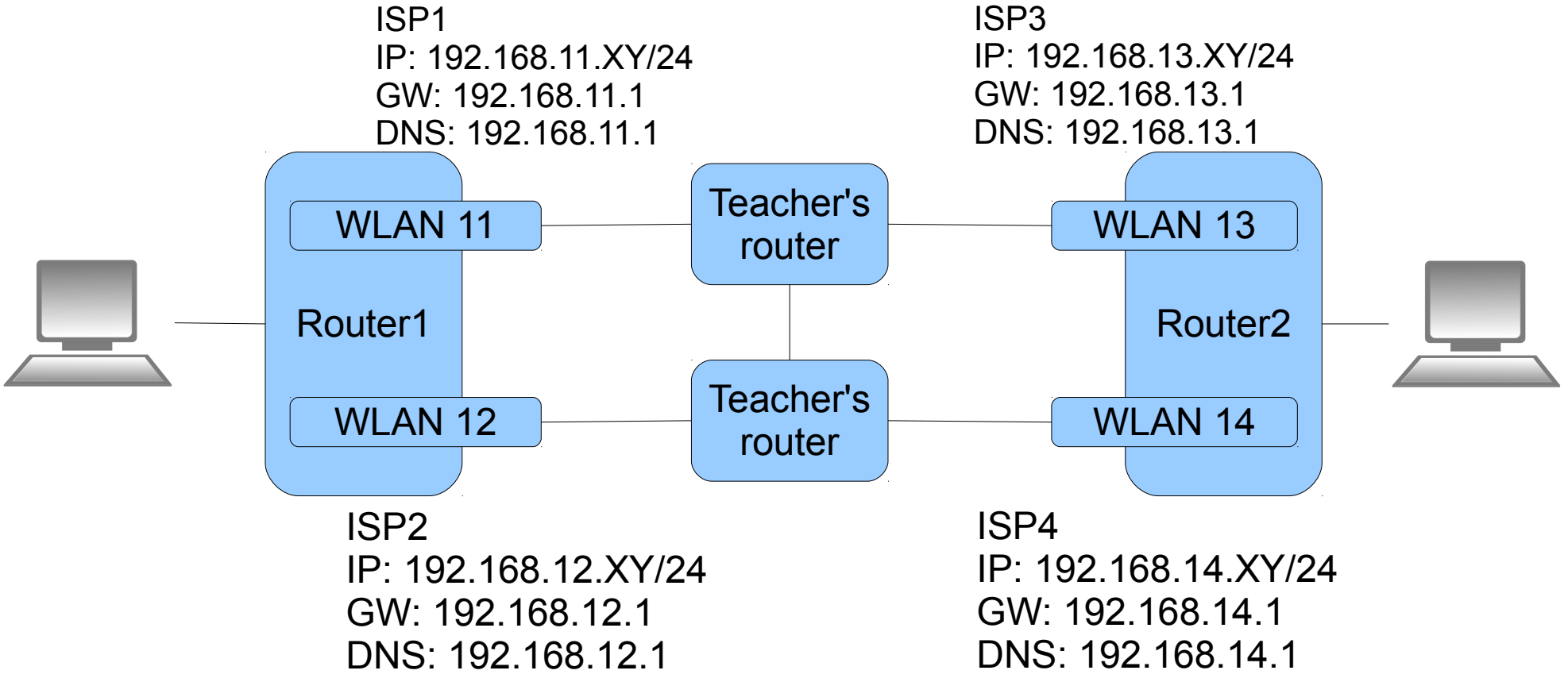


In this training Lab environment
we use teachers routers as Internet imitation and
WLAN`s as providers connections

Class setup

- Remember your class XY number.
- For next Lab group in pairs.

ISP IP setup



- Задавайте маршрут по умолчанию через одного провайдера!
- DNS можно использовать либо по одному DNS серверу от каждого провайдера, либо публичные DNS сервера

LAN setup

- LAN betwen your Laptop and your router 10.1.XY.0/24
- Laptop 10.1.XY.1, router 10.1.XY.254
- On Laptop set Default Gateway to router
- On router setup masquarade for both ISP *

- Test internet connection

* masquarade used to simple test internet connection and dont necessary to VPN work

Настройка policy routing для работы двух ISP

Чтобы Dial WAN мог работать, требуется настройка правил маршрутизации. Для каждого используемого провайдера нужно создать таблицу маршрутизации в которой как шлюз по умолчанию указан шлюз этого провайдера.

Create routing rules that route outbound packets from ISP1 IP throught ISP1 routing table. And packets of ISP2 throught ISP2 routing table. Throught default (main) routing table must

For example, router1 configuration:

```
/ip route
add dst-address=0.0.0.0/0 gateway=192.168.11.1 \
    pref-src=192.168.11.2 routing-mark=ISP1
add dst-address=0.0.0.0/0 gateway=192.168.12.1 \
    pref-src=192.168.12.2 routing-mark=ISP2


/ip route rule
add action=lookup src-address=192.168.11.XY/32 table=ISP1
add action=lookup src-address=192.168.12.XY/32 table=ISP2
```

Test WAN work

- Test ISP connection by pinging external IP of your partner. You can select ISP for pinging by specifying source IP using Src-address option.

```
/ping 192.168.11.xy src-address=192.168.13.XY
```

XY — your number
xy — your partner's number

Test WAN work

- You can ensure using right ISP connection by traceroute to external IP of your partner. You can select ISP for pinging by specifying source IP using Src-address option.

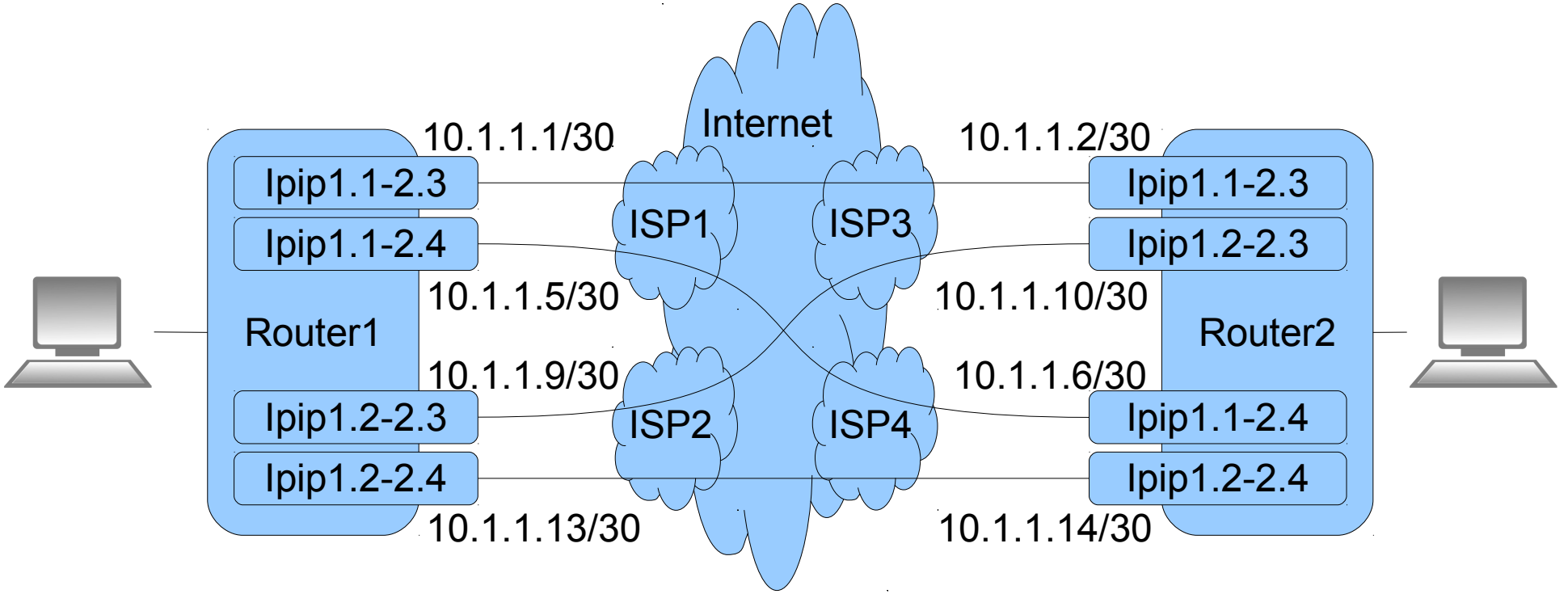
```
/tools traceroute 192.168.11.xy src-address=192.168.13.XY
/tools traceroute 192.168.11.xy src-address=192.168.14.XY
/tools traceroute 192.168.12.xy src-address=192.168.13.XY
/tools traceroute 192.168.12.xy src-address=192.168.14.XY
```

XY — your number
xy — your partner's number

Почему используются IPIP тунели?

- IPIP задает как удалённый так и локальный IP адрес
- IPIP имеет меньший оверхед энкапсуляции
- IPIP достаточно для IP маршрутизации

Диаграмма VPN соединений



IP setup in tunnels		
Tunnel	**IP router 1**	**IP router 2**
Ipip1.1-2.3	10.1.1.1/30	10.1.1.2/30
Ipip1.1-2.4	10.1.1.5/30	10.1.1.6/30
Ipip1.2-2.3	10.1.1.9/30	10.1.1.10/30
Ipip1.2-2.4	10.1.1.13/30	10.1.1.14/30

Testing VPN tunnels

Ping from your router other side of each tunnel to check if it is working properly.

```
# for router1
/ping 10.1.1.2
/ping 10.1.1.6
/ping 10.1.1.10
/ping 10.1.1.14
```

```
# for router2
/ping 10.1.1.1
/ping 10.1.1.5
/ping 10.1.1.9
/ping 10.1.1.13
```

VPN ECMP routes

- Add route to your partner's LAN subnet over all four tunnels. Set check-gateway=ping

- Next show route where xy is your partner's number

```
/ip route
add check-gateway=ping dst-address=10.1.xy.0/24
gateway=10.1.1.6,10.1.1.2,10.1.1.10,10.1.1.14
```

- Test ping to partner's LAN IP (10.1.xy.254 where xy is your partner's number)

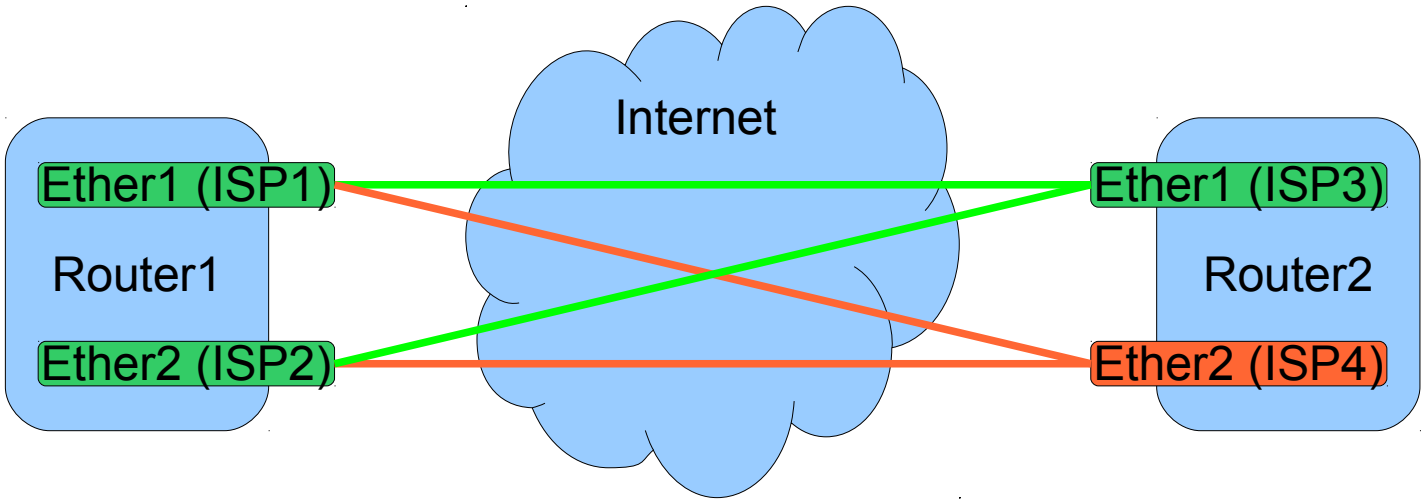
ECMP + check-gateway

- В ROS v4 и v5 check-gateway для маршрутов с ECMP включается только для первого шлюза!
  Используем workaround, добавим не ECMP маршруты с chck-gateway

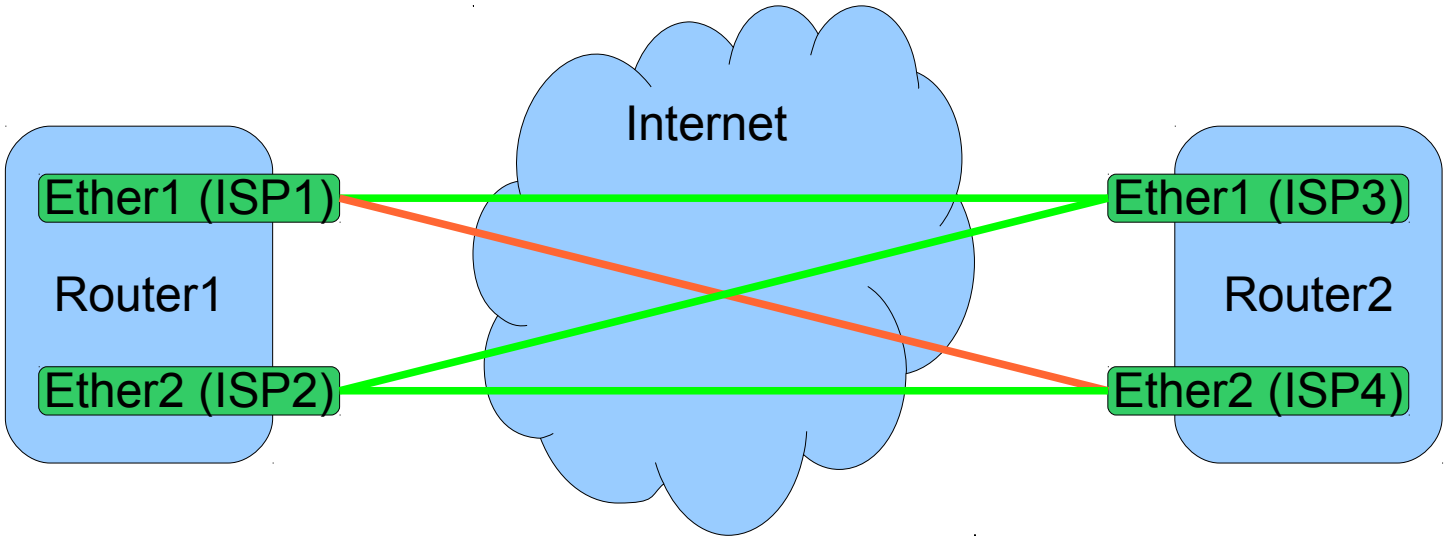
```
/ip route
add check-gateway=ping dst-address=10.1.xy.0/24 \
 gateway=10.1.1.6 distance=200
add check-gateway=ping dst-address=10.1.xy.0/24 \
 gateway=10.1.1.2 distance=200
add check-gateway=ping dst-address=10.1.xy.0/24 \
 gateway=10.1.1.10 distance=200
add check-gateway=ping dst-address=10.1.xy.0/24 \
 Gateway=10.1.1.14 distance=200
```

Возможные сбои

✔ Отказ одного провайдера

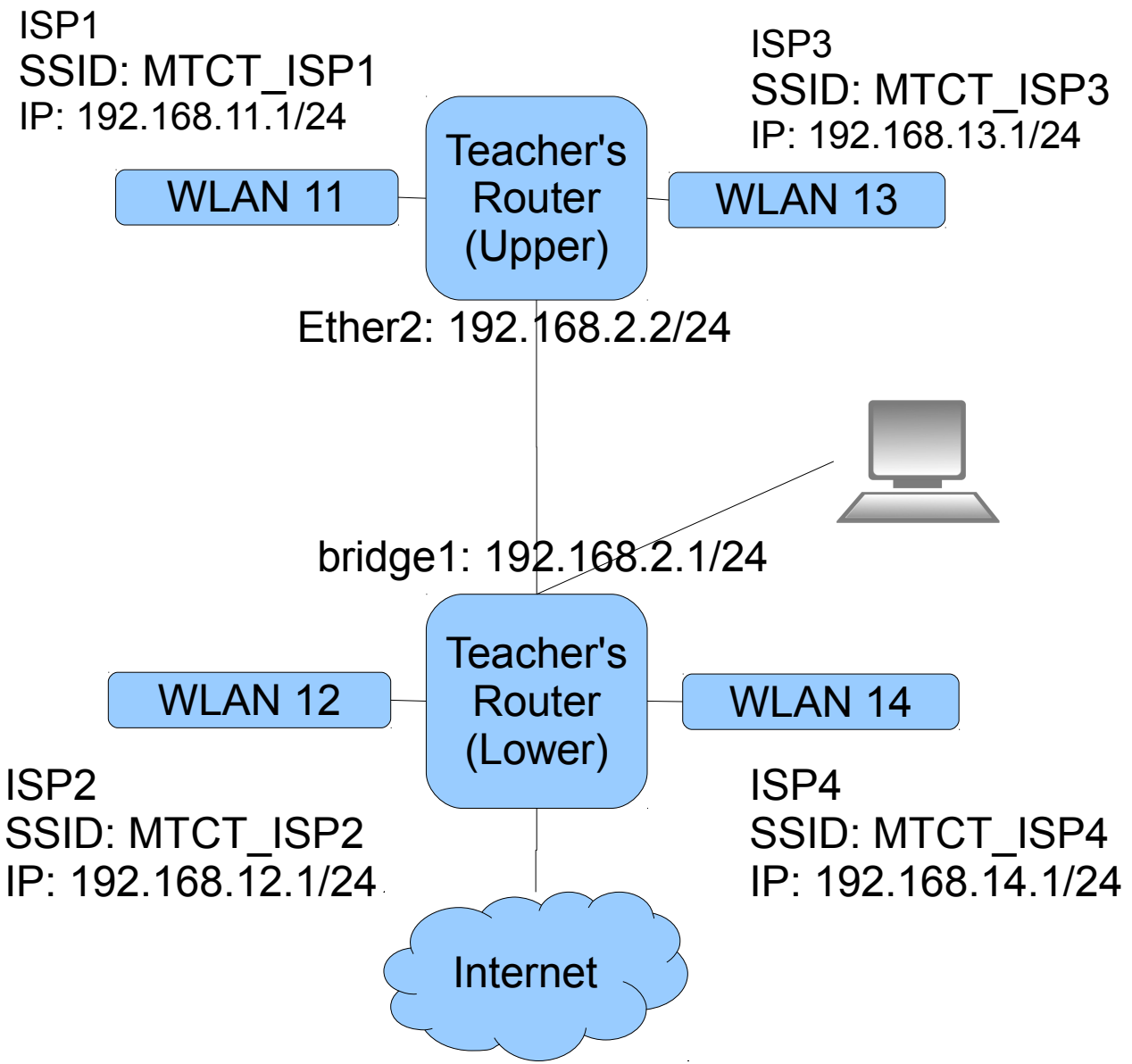


✔Отказ пиринга между двумя провайдерами



Спасибо за внимание!

Teacher's routers setup



Lover Teacher's routers script

```
# Lover router

/system identity
set name=Lover

/interface wireless
set 1 antenna-gain=27 band=2.4ghz-b frequency=2422 mode=ap-bridge name=wlan_isp2 \
    radio-name=MTCT_Lover ssid=MTCT_ISP2
add master-interface=wlan_ISP2 name=wlan_isp4 ssid=MTCT_ISP4

# bridge to easy setup Upper router
/interface bridge
add name=bridge1
/interface bridge port
add bridge=bridge1 interface=ether1
add bridge=bridge1 interface=ether2


/ip address
add address=192.168.2.1/24 interface=bridge1
add address=192.168.11.1/24 interface=wlan_isp2
add address=192.168.13.1/24 interface=wlan_isp4

/ip route
add dst-address=192.168.11.0/24 gateway=192.168.2.2
add dst-address=192.168.13.0/24 gateway=192.168.2.2

# Firwall ISP failures imitation
/ip firewall filter
add action=drop chain=forward comment="ISP2 Failure" disabled=yes \
    in-interface=wlan_isp2
add action=drop chain=forward comment="ISP2 Failure" disabled=yes \
    out-interface=wlan_isp2
add action=drop chain=forward comment="ISP4 Failure" disabled=yes \
    in-interface=wlan_isp4
add action=drop chain=forward comment="ISP4 Failure" disabled=yes \
    out-interface=wlan_isp4
```

Upper Teacher's routers script

```
# Upper Router

/system identity
set name=Upper

/interface wireless
set 1 antenna-gain=27 band=2.4ghz-b frequency=2422 mode=ap-bridge name=wlan_isp1 \
    radio-name=MTCT_Upper ssid=MTCT_ISP1
add master-interface=wlan_isp1 name=wlan_isp3 ssid=MTCT_ISP3

/ip address
add address=192.168.2.2/24 interface=ether2
add address=192.168.11.1/24 interface=wlan_isp1
add address=192.168.13.1/24 interface=wlan_isp3

/ip route
add dst-address=0.0.0.0/0 gateway=192.168.2.1

/ip dns
set allow-remote-requests=yes servers=192.168.2.1

# Firwall ISP failures imitation
/ip firewall filter
add action=drop chain=forward comment="ISP1 Failure" disabled=yes \
    in-interface=wlan_isp1
add action=drop chain=forward comment="ISP1 Failure" disabled=yes \
    out-interface=wlan_isp1
add action=drop chain=forward comment="ISP3 Failure" disabled=yes \
    in-interface=wlan_isp3
add action=drop chain=forward comment="ISP3 Failure" disabled=yes \
    out-interface=wlan_isp3
```