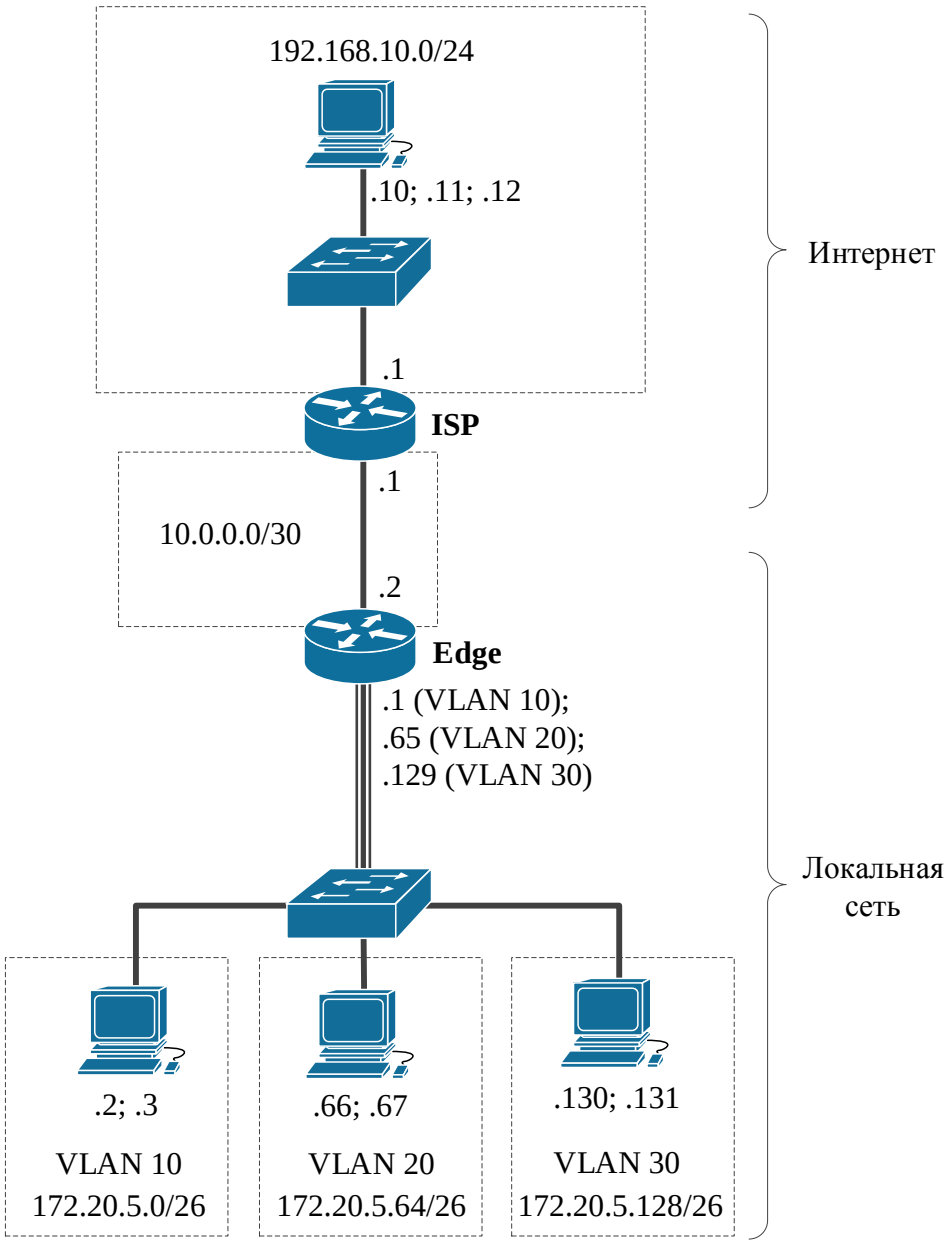
Работа со стандартными списками контроля доступа Cisco IOS (версия 2)

Порядок выполнения работы.

1. Настроить стенд, согласно топологии сети и схеме адресации, приведённым на рисунке 1.



Условные обозначения:

---------- — граница подсети IP.

═══ — транковый канал (IEEE 802.1Q).

.13 — узловая чать IP-адреса.

Рисунок 1 — Топология сети и схема адресации

Обратите внимание, что на каждом ПК настраивается несколько адресов, а для пересылки трафика между VLAN используется метод «router-on-a-stick».

2. Настроить фильтрацию сетевого трафика для локальной сети (на маршрутизаторе Edge) с помощью стандартных списков контроля доступа. Необходимо реализовать следующую политику безопасности:

- сетевой доступ, в явном виде не запрещённый данной политикой безопасности, должен быть разрешён;
- разграничение доступа к локальной сети из Интернета должно осуществляться на основе чёрного списка. В чёрном списке находится адрес 192.168.10.10;
- VLAN 10, за исключением узла 172.20.5.2, запрещён доступ к VLAN 20;
- узлу 192.168.10.11 запрещён доступ к VLAN 10;
- узлу 192.168.10.12 запрещён доступ к VLAN 30;
- запретить доступ в Интернет всех узлов VLAN 10, VLAN 20 и VLAN 30, узловая часть IP-адреса которых в двоичном представлении равна 00 0010 (узлов 172.20.5.2, 172.20.5.66 и 172.20.5.130). **Данное требование необходимо реализовать с помощью одной записи (ACE) списка контроля доступа;**
- удалённый доступ по Telnet/SSH к маршрутизатору Edge по должен быть разрешён только с узла 172.20.5.67.

3. Настроить фильтрацию сетевого трафика, выполняемую на стороне Интернет-провайдера (на маршрутизаторе ISP), с помощью стандартных списков контроля доступа. Необходимо реализовать следующую политику безопасности:

- с целью блокирования атаки подмены IP-адреса (IP spoofing) доступ в Интернет из локальной сети должен осуществляться только с IP-адресов, выданных Интернет-провайдером. Для локальной сети Интернет-провайдером были выделены подсеть 172.20.5.0/24 и адрес 10.0.0.2.

4. Продемонстрировать результаты работы и ответить на контрольные вопросы по теме лабораторной работы.

Проверка разграничения доступа выполняется с помощью утилиты «ping»:

```
ping -I <адрес отправителя> <адрес получателя>
```

Проверку блокирования атаки подмены IP-адреса удобнее осуществлять с помощью генератора пакетов «nping» и анализатора сетевого трафика «Wireshark». Отправка ICMP echo-запросов с подменённым адресом отправителя:

```
sudo nping \
    --icmp \
    --source-ip <адрес отправителя> \
    <адрес получателя>
```

Фильтр для отображаемых «Wireshark» пакетов:

```
ip.addr == <IP-адрес отправителя>
```

Приложение. CLI-команды Cisco IOS

Переключение порта коммутатора на работу в режиме порта доступа для определённой VLAN:

```
switchport mode access
switchport access vlan <номер VLAN>
```

Переключение порта коммутатора на работу в режиме транкового порта:

```
switchport mode trunk
```

Настройка подынтерфейсов маршрутизатора для работы с тегированным (802.1Q) трафиком:

```
interface <тип> <номер>.<номер подынтерфейса>
  encapsulation dot1q <номер VLAN>
```

Создание именованного списка контроля доступа:

```
ip access-list standard <имя ACL>

  [<порядковый номер>] {permit|deny}
          {any|<адрес> <wildcard-маска>|host <адрес>}
```

Применение списка контроля доступа к сетевому интерфейсу:

```
ip access-group <имя ACL> {in|out}
```

Применение списка контроля доступа к VTY:

```
access-class <имя ACL> in
```