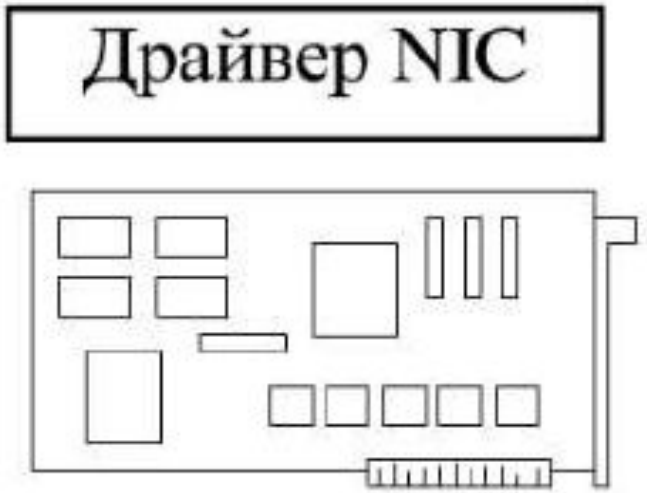
Безопасность в локальной сети

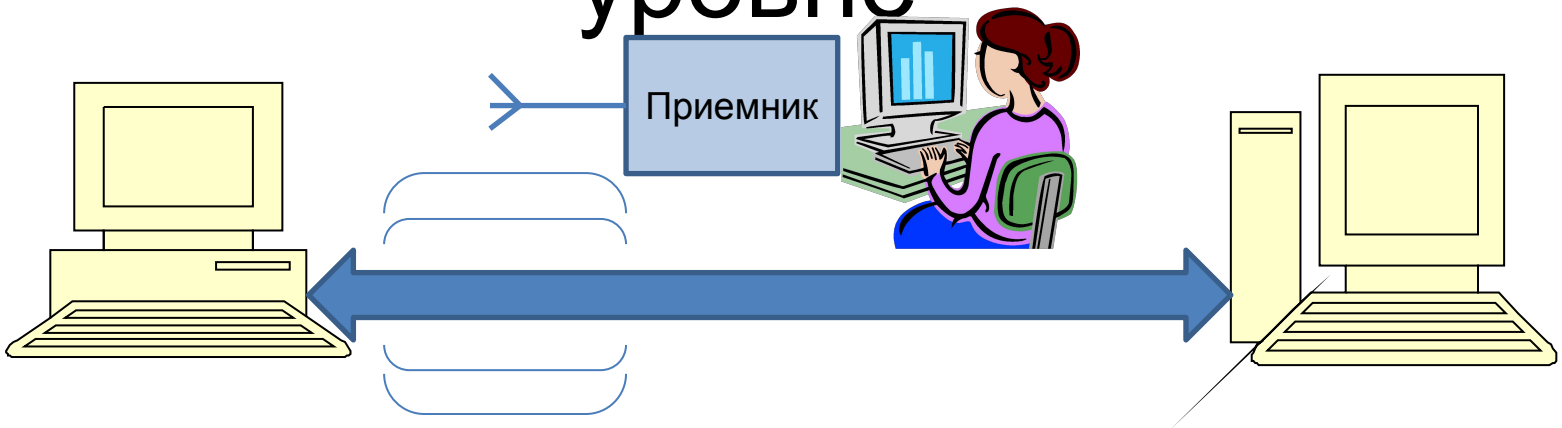
Физический и канальный уровень в модели OSI



Функции физического уровня

- Физический уровень описывает способы передачи бит данных через физические среды линий связи, соединяющие сетевые устройства.
- На этом уровне описываются параметры сигналов, такие как амплитуда, частота, фаза, используемая модуляция, манипуляция.
- Решаются вопросы связанные с синхронизацией, избавлением от помех, скорости передачи данных.

Безопасность на физическом уровне



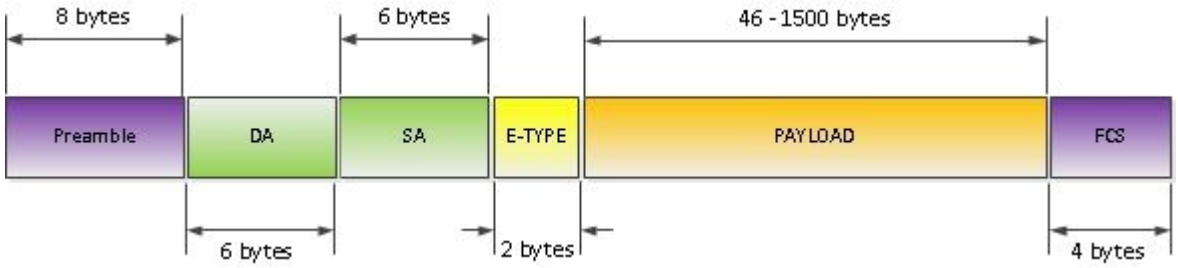
- Экранирование кабеля
- Заземление кабельной системы
- Экранирование помещений, где размещено сетевое оборудование
- Использование оптоволоконных линий
- Управление зоной покрытия (для беспроводных сетей)

Функции канального уровня

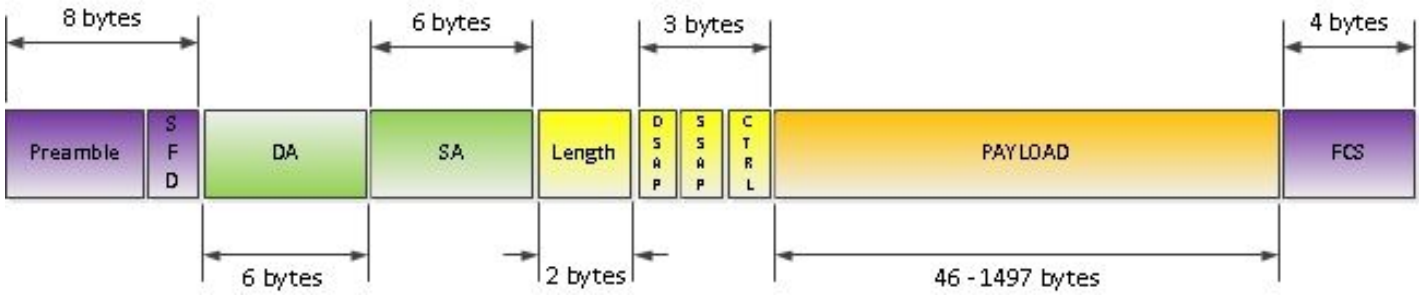
- Передача данных узлам, находящимся в том же сегменте локальной сети.
- Обнаружение и исправление ошибок, возникших на физическом уровне.
- Контроль доступа к разделяемой среде передачи

Кадры Ethernet

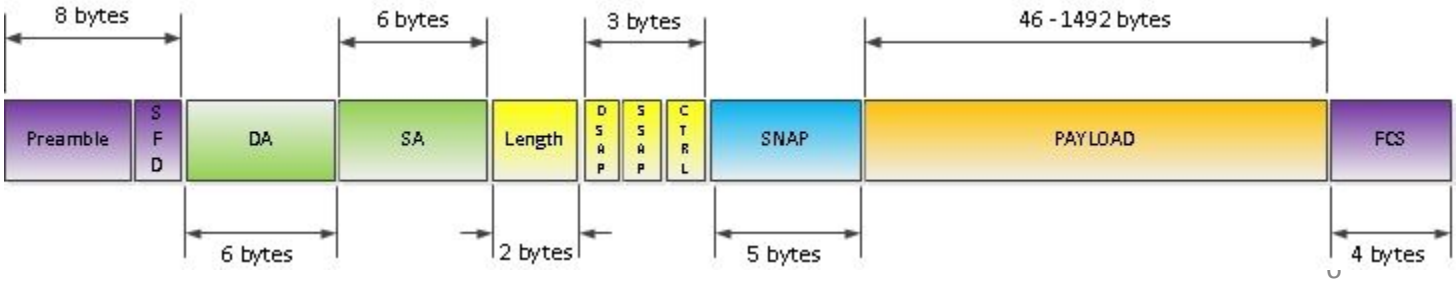
Ethernet II



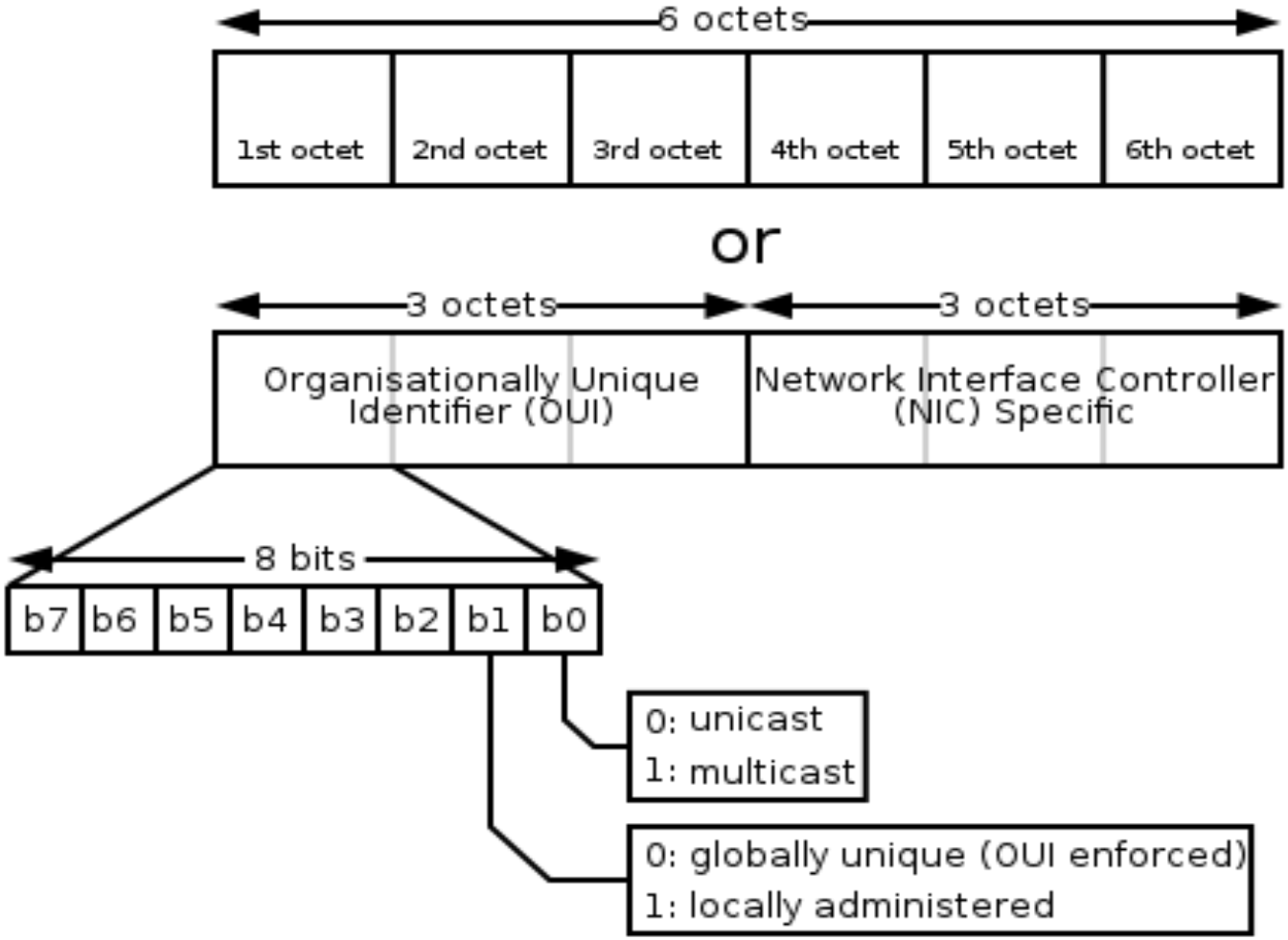
IEEE 802.2 LLC



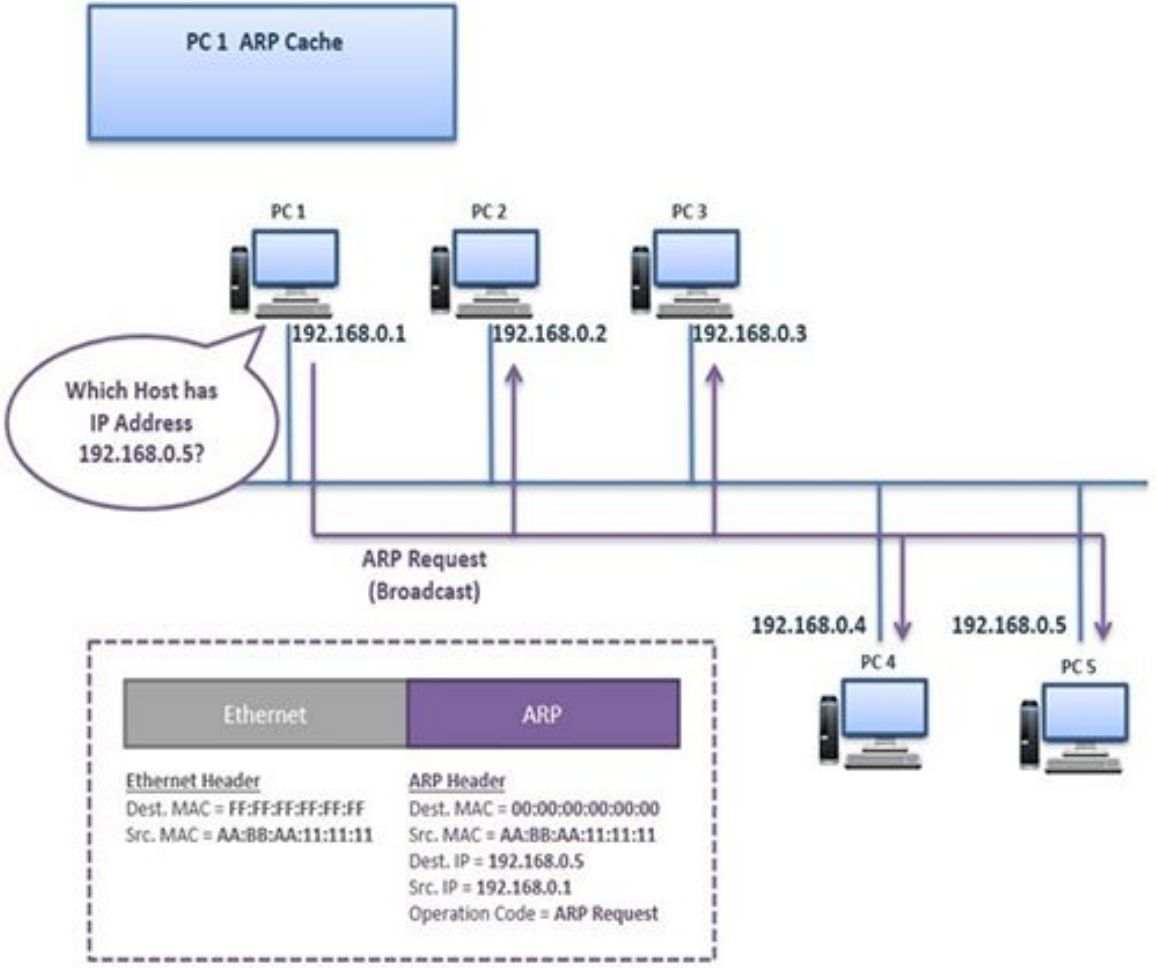
IEEE 802.2 SNAP



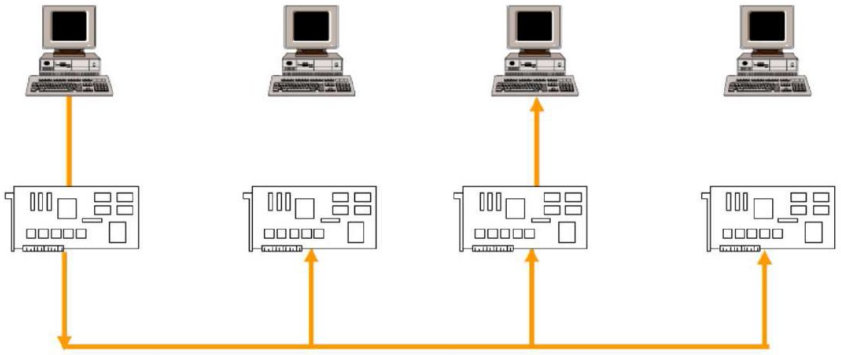
Адресация на канальном уровне



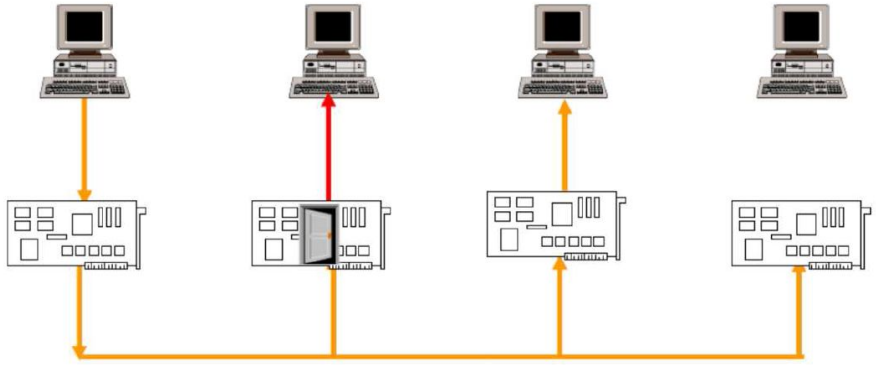
Связь физической и логической адресации - протокол ARP



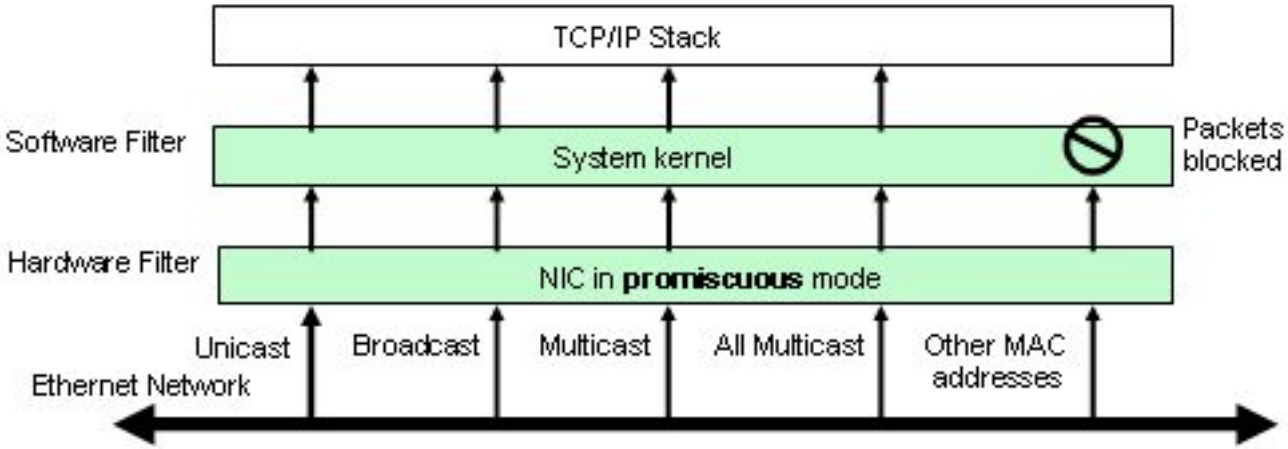
Селективный и неразборчивый режимы работы сетевого адаптера



Selective mode



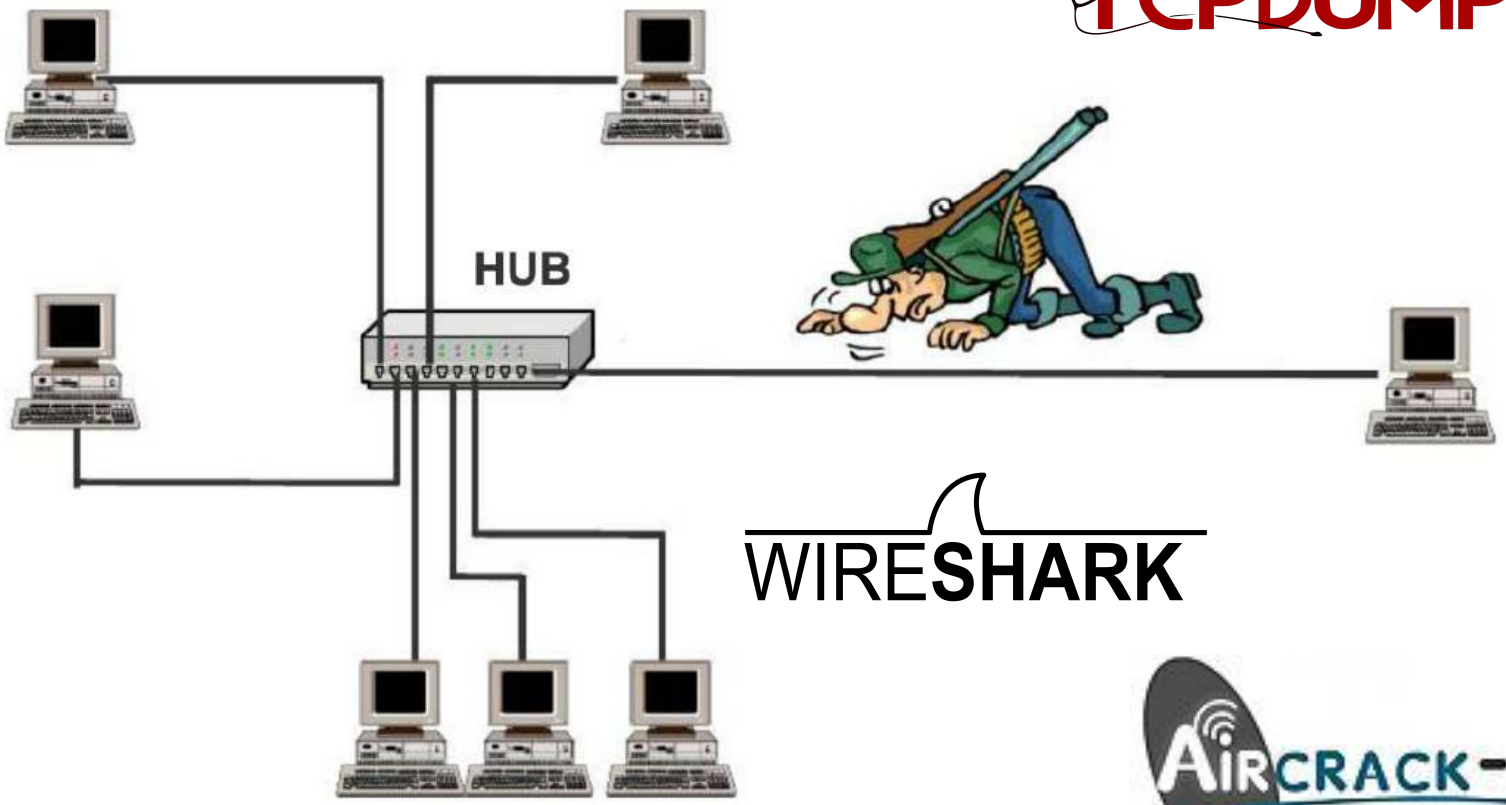
Promiscuous mode



Снифферы и их применение

Сниффер - программа или устройство для перехвата и анализа сетевого трафика
(своего и/или чужого).

TCPDUMP & LIBPCAP



WIRESHARK

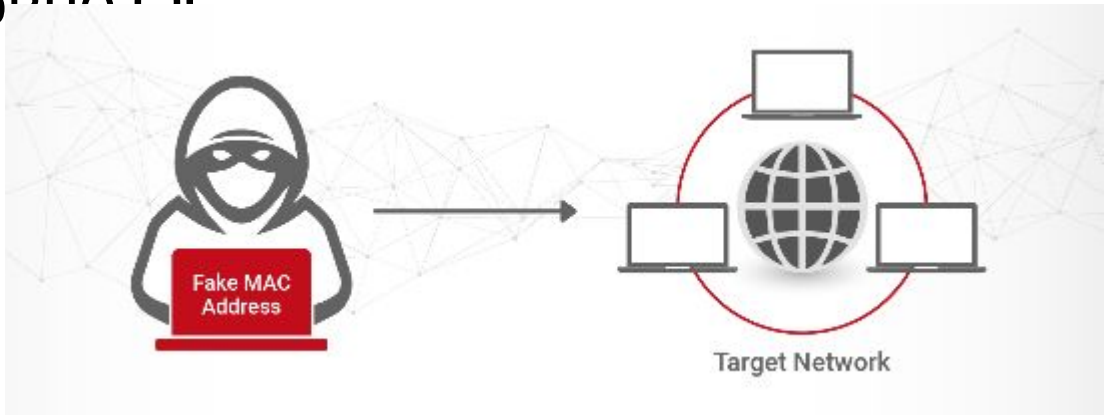
AIRCRACK-NG

Меры защиты от снифферов

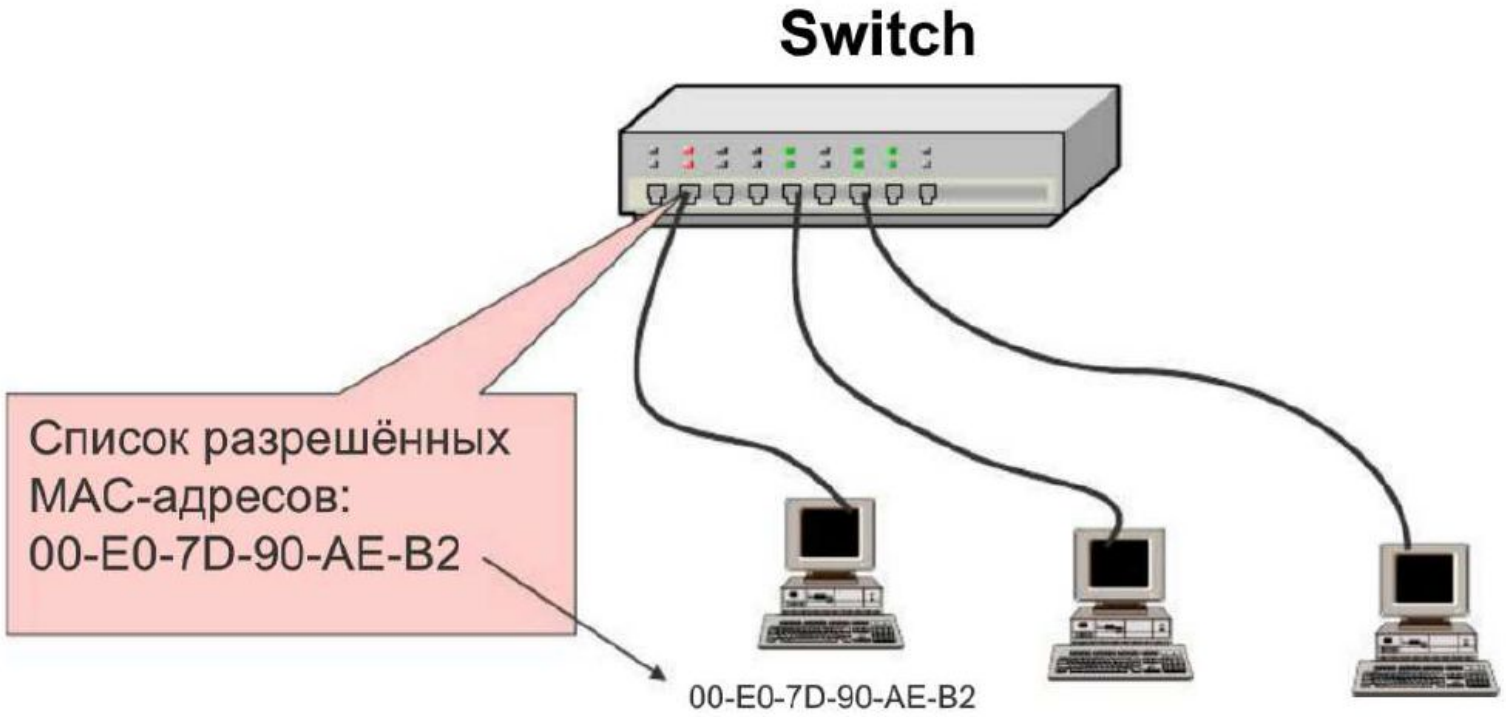
- Криптографические методы
- Сегментирование сети
- Обнаружение несанкционированных анализаторов трафика
  - Анализ задержек
  - Ping со случайным destination MAC
  - Сниффер кэширует данные ARP от всех хостов (обычный хост сначала отправит ARP запрос)

MAC-spoofing

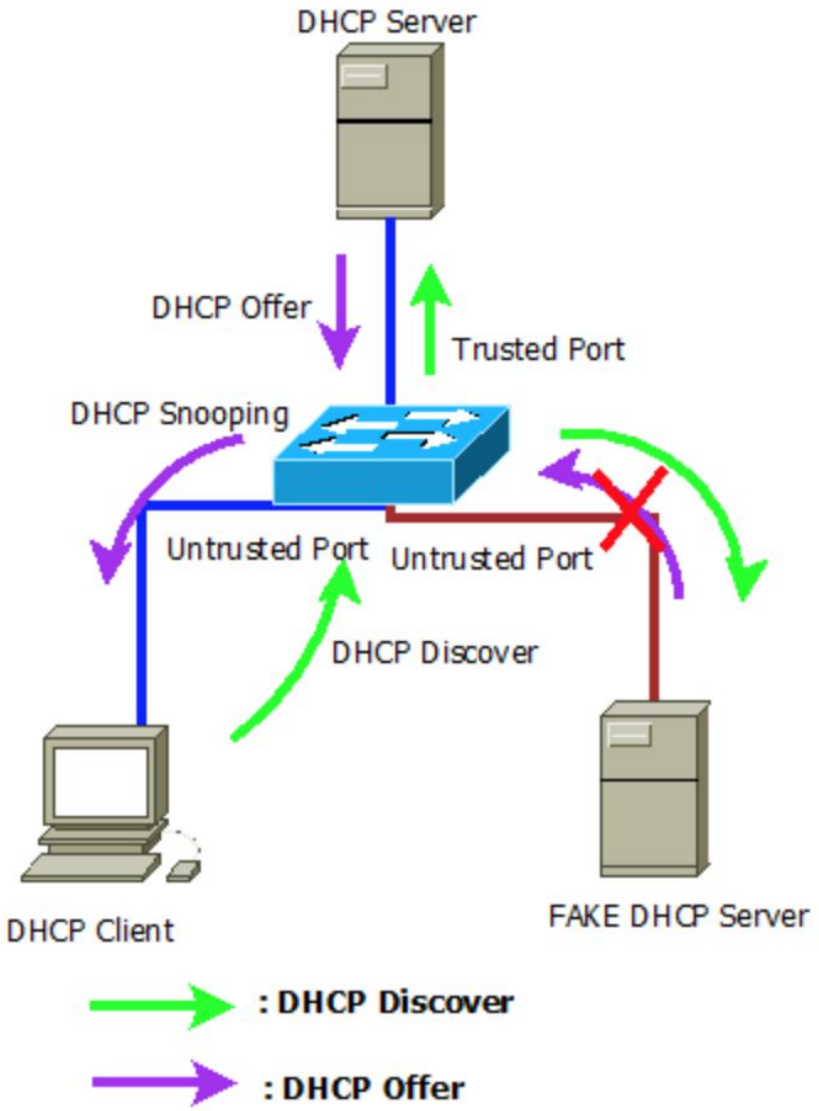
- MAC-адрес является основным идентификатором узла на канальном уровне. Атака может быть реализована через подмену MAC-адреса:
  - На физическом уровне
  - В момент считывания в память ОС
  - На уров[illegible] ОС



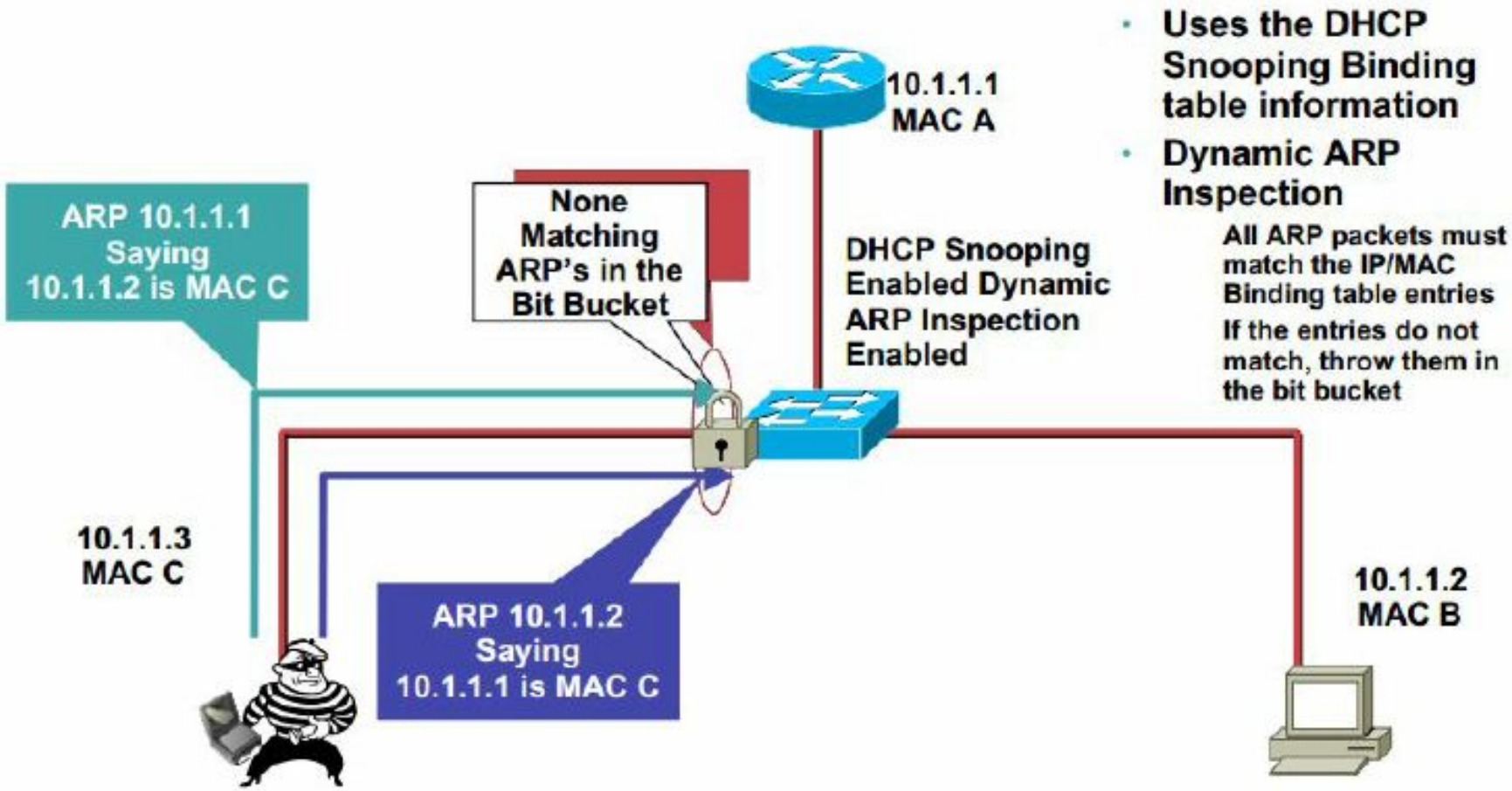
Port security



DHCP Snooping

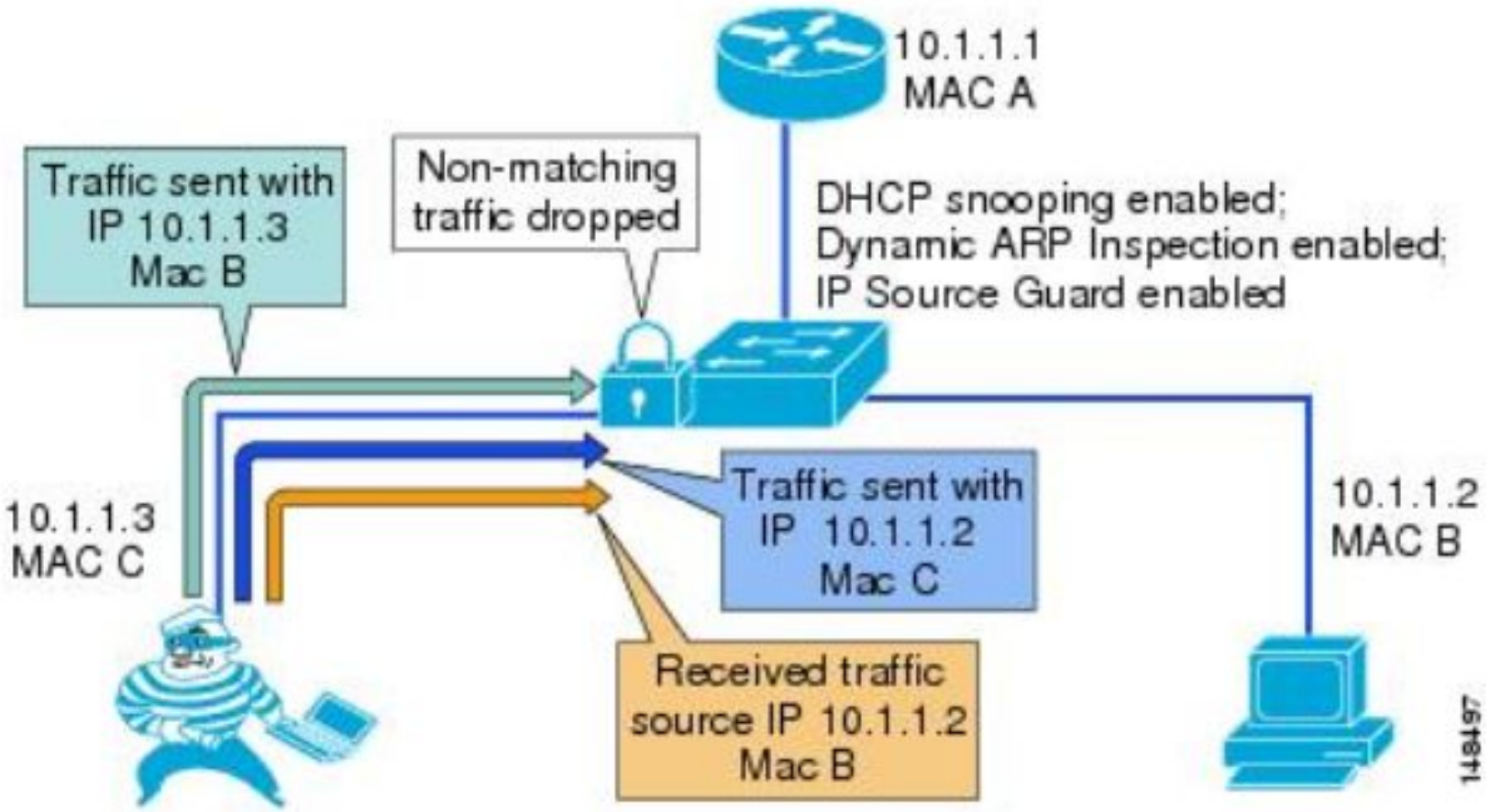


Dynamic ARP inspection



- Uses the DHCP Snooping Binding table information
- Dynamic ARP Inspection
  - All ARP packets must match the IP/MAC Binding table entries
  - If the entries do not match, throw them in the bit bucket

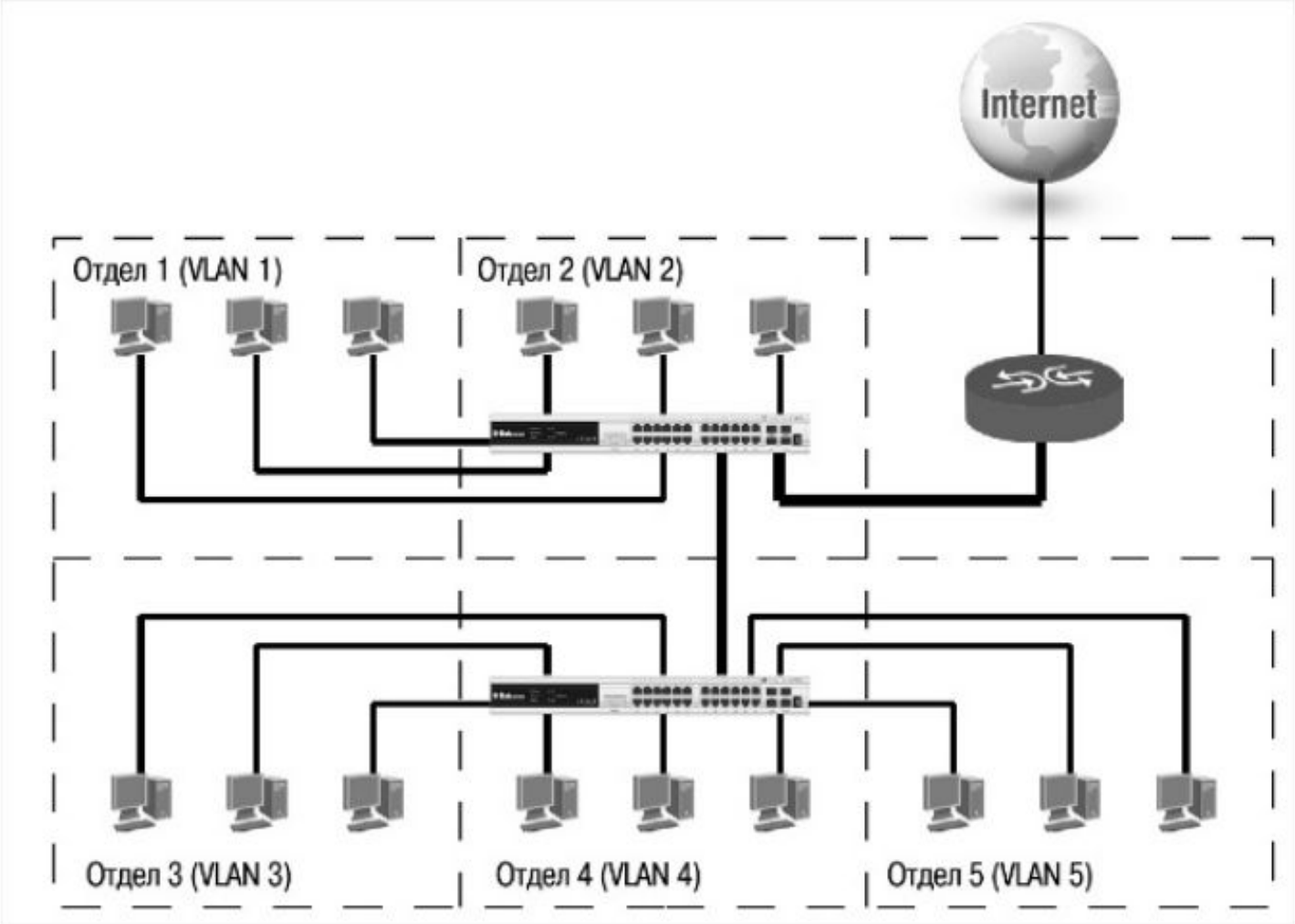
IP Source Guard



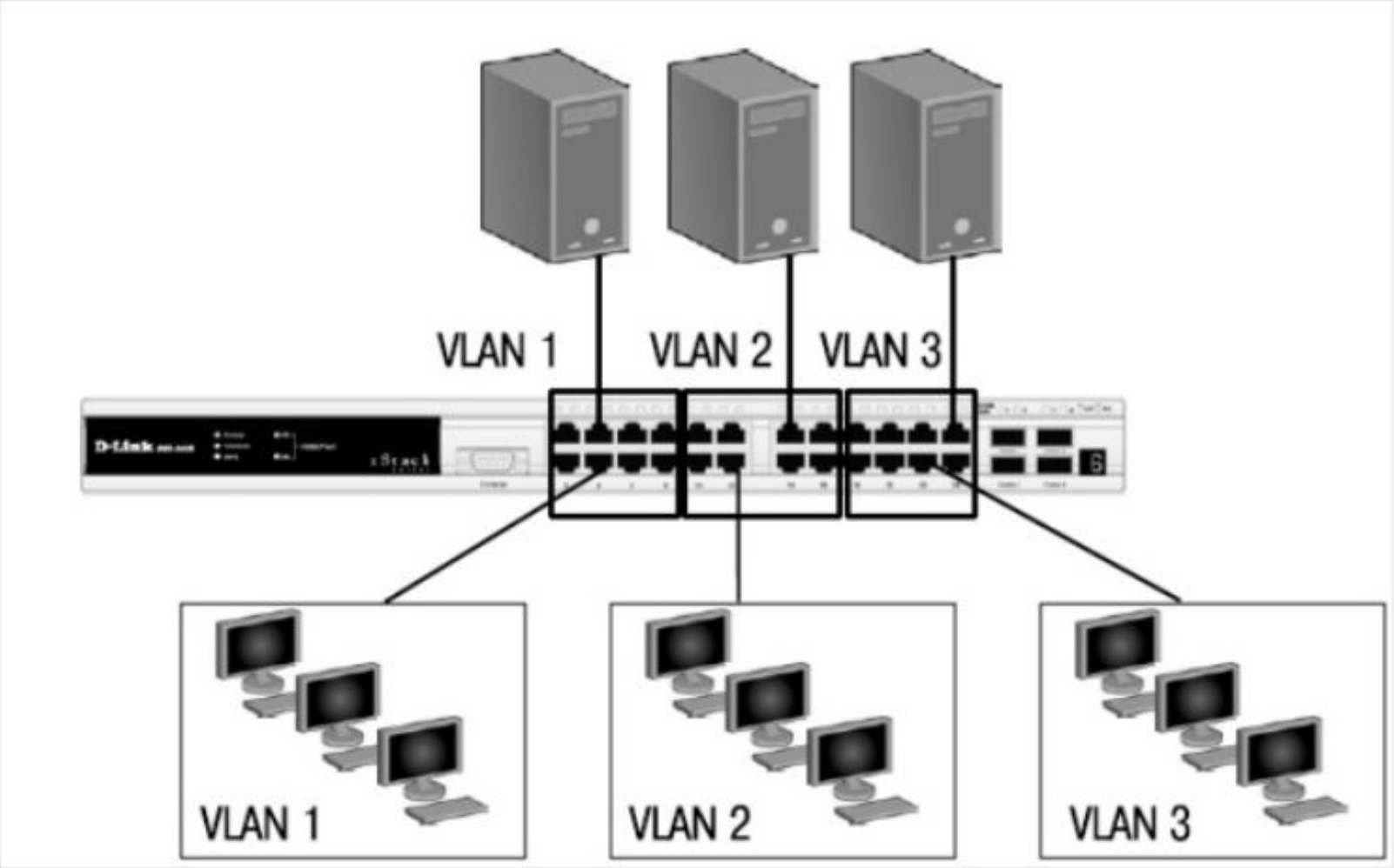
Виртуальные локальные сети

- **Виртуальной локальной сетью (VLAN)** называется логическая *группа* узлов сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов сет
- Передача кадров между разными виртуальными сетями на основании MAC-адреса невозможна независимо от типа адреса: уникального, группового или широковещательного.
  - гибкость внедрения;
  - *VLAN* обеспечивают возможность контроля широковещательных сообщений, что увеличивает полосу пропускания;
  - *VLAN* позволяют повысить безопасность сети, посредством политики взаимодействия пользователей из разных виртуальных сетей.

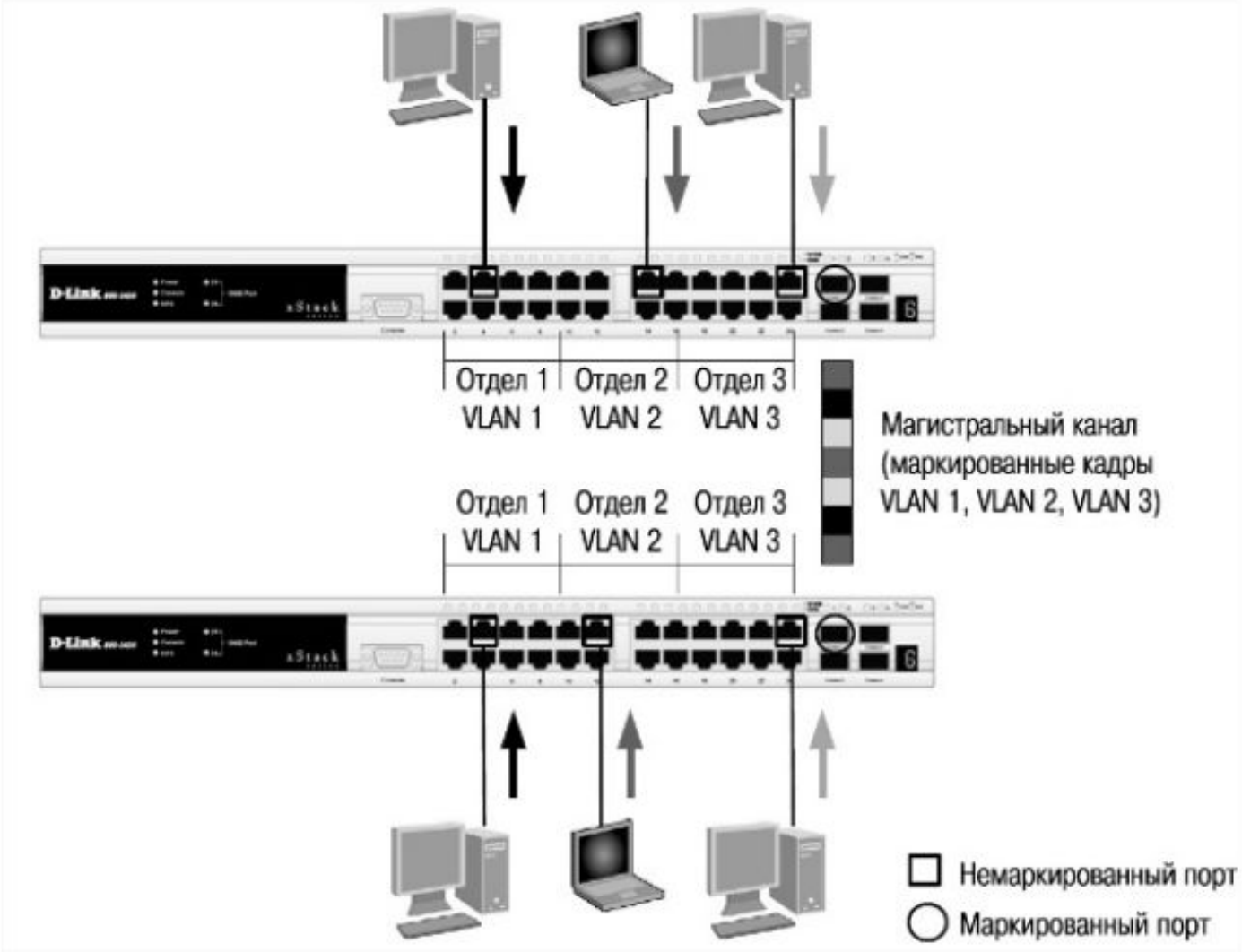
Логическая сегментация сети с использованием VLAN



VLAN на основе портов



VLAN на основе стандарта IEEE 802.1Q



Маркированный кадр

Продвижение кадров VLAN IEEE 802.1Q

Входящий трафик

Исходящий трафик

Виды сетевого оборудования

	Уровень OSI	Применение	Маршрутизация	VLAN	QoS	WAN connect
Концентратор (hub)	1	Многопортовый повторитель	Нет	Нет	Нет	Нет
Коммутатор L2 (L2 switch)	2	Коммутация LAN	Нет	Да	Ограничена	Нет
Коммутатор L3 (L3 switch)	2 и 3	Коммутация и маршрутизация VLAN	В основном, статическая	Да	Да	Нет
Коммутатор L3+ (L3+ switch)	2 и 3	Расширенная маршрутизация	Динамическая	Да	Да	Да
Маршрутизатор	3+	Межсетевое соединение	Динамическая	Да	Да	Да