Тема 2.

Текущий контроль по Лекции 5.

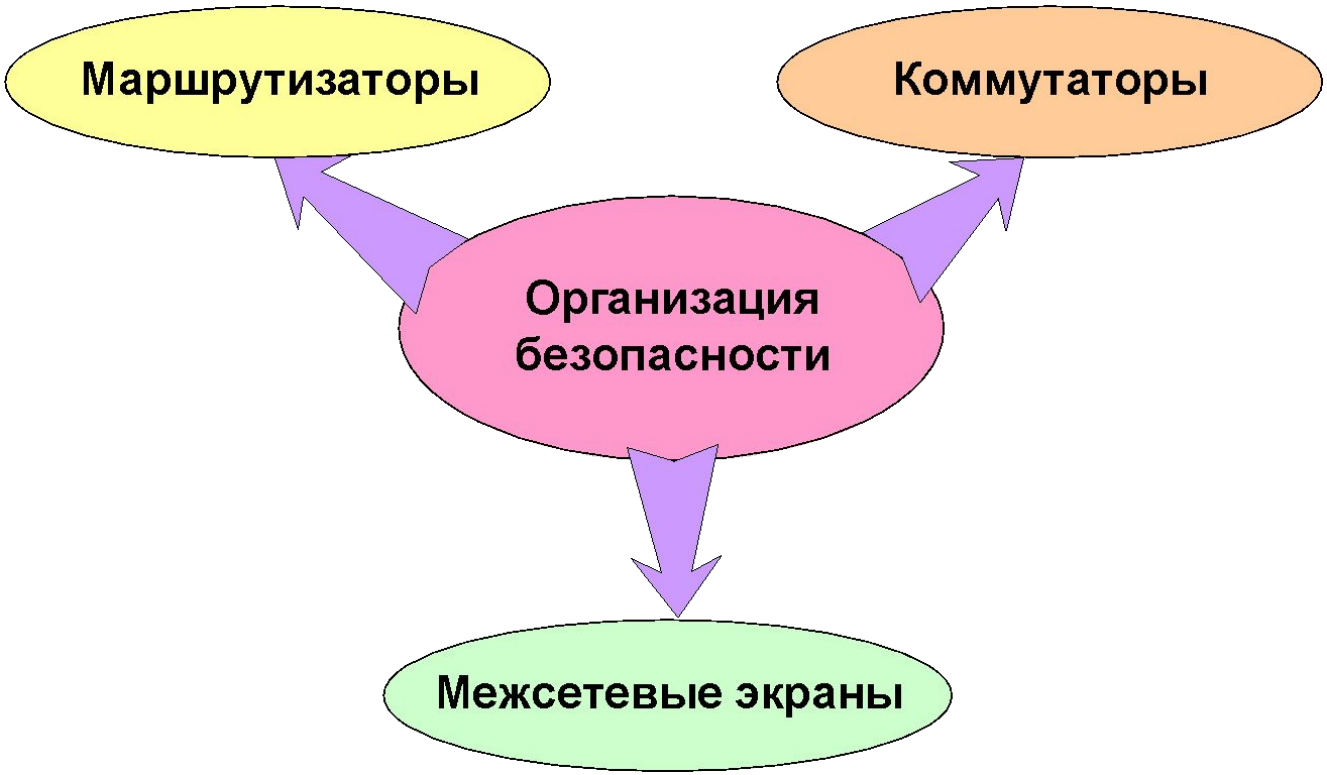
Канальний уровень. Технология Ethernet

20 , 4

1. Представление канального и физического уровней в виде набора подуровней?
2. Что такое NEXT?
3. Состав пакета Ethernet любо известного Вам варианта?
4. Состав пакета IP?
5. Состав пакета эхо-запроса ICMP?
7. Защифруйте последовательность 1110010101000000111111111 в NZR,DiffManchester, MLT-3 коды.
8. Какие варианты посылки прописаны в ICMP?
9. HDLC – что это? Состав пакета?
10. PPP – что это? Состав пакета?

Сетевой уровень. Вопросы обеспечения безопасности и маршрутизации

Лекция 6. Вопросы безопасности в сети.



Лекция 6. Вопросы безопасности в сети.

1. Маршрутизаторы

Лекция 6. Вопросы безопасности в сети.

Методы защиты маршрутизатора и сети возможностями маршрутизатора:

Контроль доступа:

+ ограничение времени доступа к м. в режиме управления;

+ защита паролем всех возможных подключений к роутеру (telnet/rlogin/SSH/LAT/X.29/V.120/reserveTelnet (удаленный доступ через сеть));

+для управляющих VTY устанавливается разрешенный протокол доступа и ограничивается дозволенные IP-адреса;

+ применение access-list для управления через http;

+ ведение логов – записей о подключенных пользователей (AAA loging);

+ формирование посылок данных об изменениях в системном статусе.

Лекция 6. Вопросы безопасности в сети.

Методы защиты маршрутизатора и сети возможностями маршрутизатора:

Защита IP-маршрутизации:

+ Anti-spoofing – защита от подменных IP-адресов на границах сети;
+ ACL – для запрета пакетов от тех адресов, с которых они прийти не могут, например из интернет пакеты с внутренними адресами;
+ RPF checks – проверка каждого пакета (на симметричность пути) – применяется на границе внутренней сети (в internet core);
+ Controlling Directed Broadcast – против smurf атаки – контроль пакетов, отправляемых на адрес broadcast подсети: пакет посылается как unicast, пока не дойдет до подсети;
+ Фильтрация ICMP redirect во входящем трафике м.;
+ Применение аутентификации при динамической маршрутизации – защита подмены маршрутизации.

Лекция 6. Вопросы безопасности в сети.

Методы защиты маршрутизатора и сети возможностями маршрутизатора:

Защита от шторма:

+ Возможности защиты от транзитного шторма – использование QoS – WFQ (weighted fair queueing), CAR (commited access rate), GTS (generalized traffic shaping)$
+ контроль режима работы – выбор таймера режима работы м. (например, на приём)

Лекция 6. Вопросы безопасности в сети.

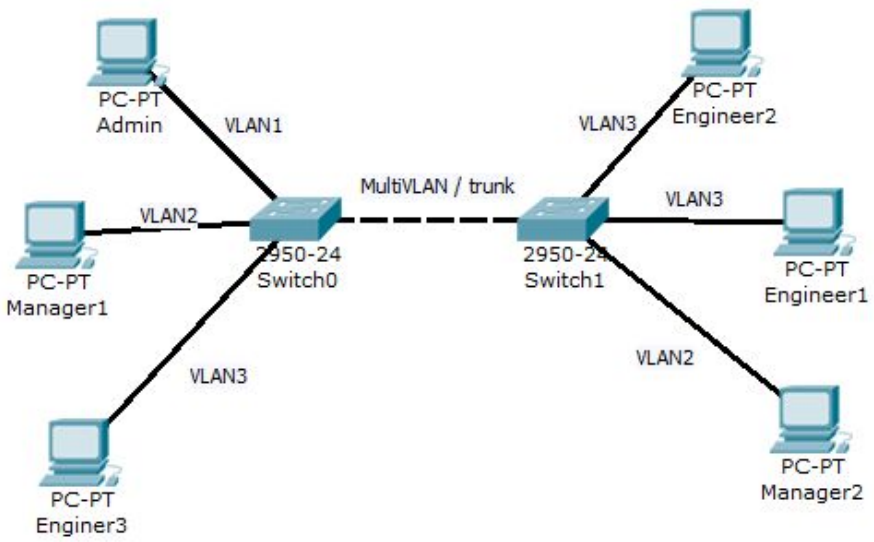
2. Коммутаторы

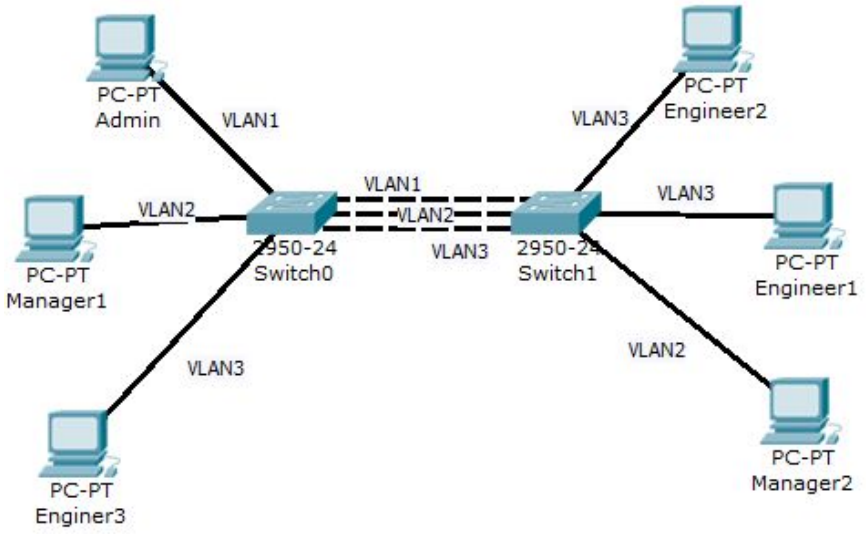
Коммутаторы . Виртуальные сети

Принцип построения:

VLAN – virtual local area network. Может быть построены:

+ по признаку порта (метод группировки портов)
+ по MAC адресу физических устройств в сети;
+ по идентификатору пользователя UserID;
+ по IP адресу.





Коммутаторы . Виртуальные сети

IEEE 802.1Q:

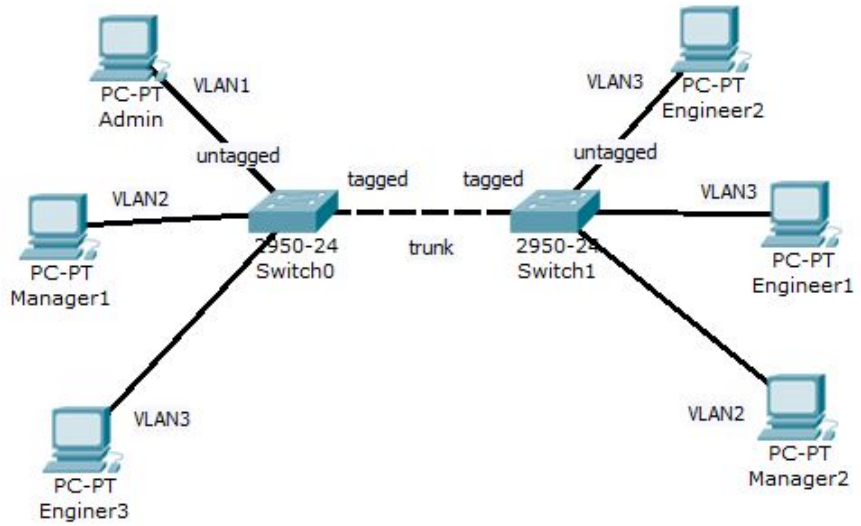
VLAN с маркированными кадрами (тегами).

Процессы: * tagging (маркировка кадра);

* untagging (извлечение тега).

Виды портов:

* tagged – для соединения сетевых устройств (транк);
* untagged – для подключения оконечных устройств (линия доступа).



Коммутаторы . Виртуальные сети

IEEE 802.1Q:

VLAN с маркированными кадрами (тегами –идентификаторами VLAN).

Принцип работы:

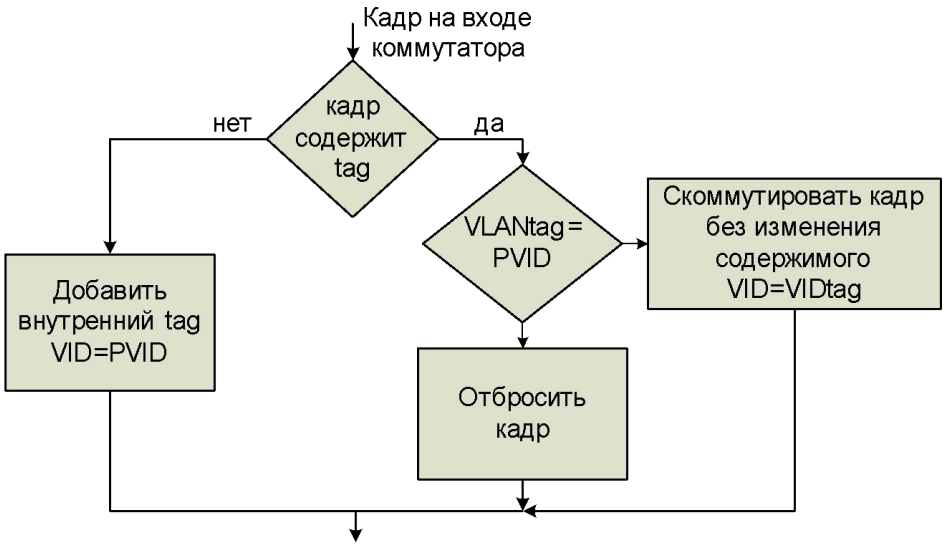
1) Каждый порт коммутатора имеет идентификатор порта VLAN (PVLAN);
Switch имеет внутреннюю таблицу соответствия порт-VLAN.

2) PVLAN используется для внутренней коммутации вне зависимости пришел ли на вход кадр с тегом или без тега.

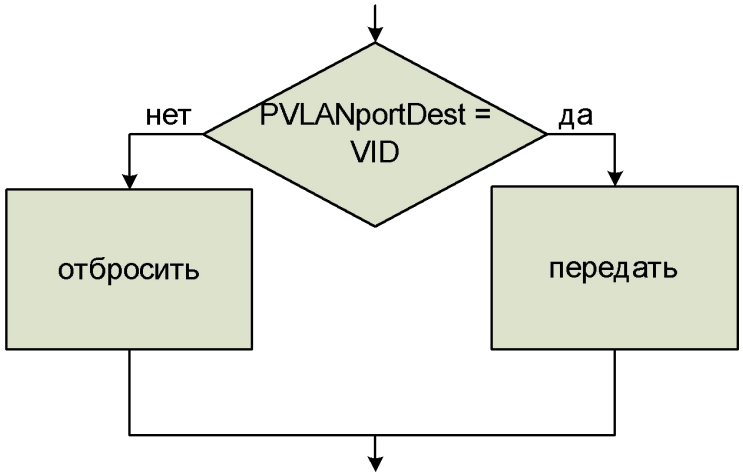
3) Приходящий кадр обрабатывается по 3 правилам:
ingress rules (п. входящего трафика),
forwarding rules (п. продвижения между портами),
egress rules (п. исходящего трафика)

Коммутаторы . Виртуальные сети

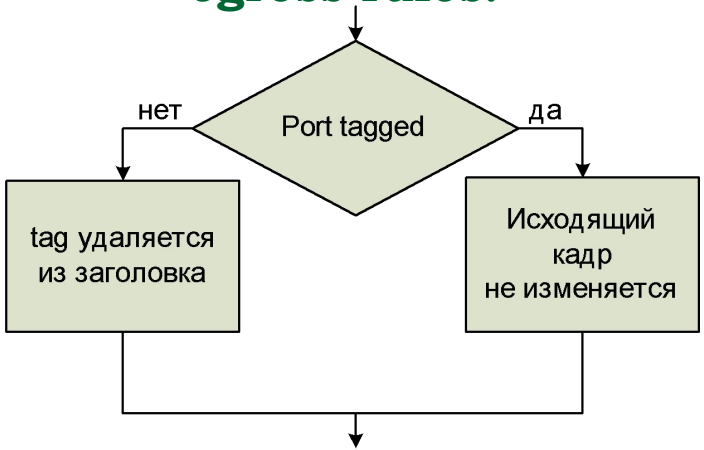
Ingress rules:

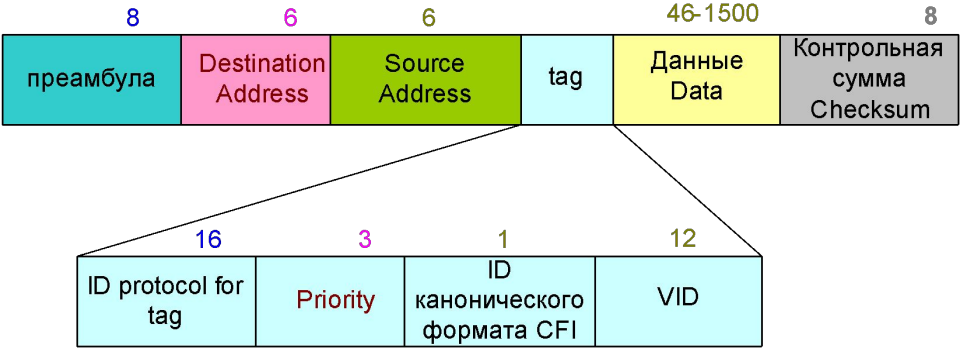


Forwarding rules:



egress rules:





Коммутаторы . Виртуальные сети. VTP

VTP (Vlan trunking protocol):

Протокол для удаленного администрирования VLAN (создание, изменение и удаление VLAN, передача информация о vlane).

Режимы работы коммутатора:

1) Server

+ создание и удаление удаленно с помощью командной строки;

+ генерирование сообщения-объявления VTP и передает другим Switch;

+ обновление базы при получении информации от других Switches в режиме Server;

+ сохраняет настройки в файле vlan.dat

2) Client

+ без создания/изменения VLAN;

+ передает обновление от других;

+ синхронизирует свою базу при получении информации; сохраняет лог.

3) Transparent

+ создает VLAN только для своих подключений; не генерирует обновления, передает трафик.

Коммутаторы . Виртуальные сети. IPSec

спецификация:

Security Association – соединение, предоставляющее службы безопасности передаваемого через него трафика.

Все участники SA хранят режим, протокол, алгоритмы и ключи SA. 1 направление - 1 SA – 1 протокол и режим, поэтому при необходимости одновременного использования аутентифицирующего заголовка AH и инкапсуляцию зашифрованных данных ESP необходимо применять 2 SA.

Политика безопасности – база данных политики безопасности: отбросить пакет, не обрабатывать пакет с помощью IPSec, обрабатывать пакет с помощью IPSec (по полям пакета).

Лекция 6
Вопросы безопасности в сети

3. Межсетевые экраны

Межсетевой экран (***firewall***) – устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением разрешенных данных.

Уровень в модели OSI: L3 – L7.

Принцип работы: определяется набором правил передачи трафика, причем это не процесс маршрутизации, а средство защиты, исключения. Межсетевой экран может быть реализован аппаратно или на основе ПО (в виде вычислительного устройства с стандартной ОС), имеет несколько интерфейсов (по одному на сеть). По умолчанию межсетевой экран закрыт и для передачи требуется явное разрешение. Настраивается по службам, по IP-адресам (Source/Destination), по идентификаторам пользователя.

Виды: * прикладного уровня МЭ (прокси-экран)

устанавливается на входе и скрывает внутренную адресацию, содержит модули для каждого протокола

* пакетной фильтрации МЭ

высокоскоротной, анализирует поступающие пакеты на соответствие правилам и передает непосредственно получателю.

* комбинированные МЭ

Лекция 6
Вопросы безопасности в сети

Межсетевые экраны . Назначение:

Защита сетей разных масштабов как основные или сегментные шлюзы с функциями мульти-протокольного VPN-концентратора; позволяют одновременно с маршрутизацией выполнять задачи:

- управление полосой пропускания для пользователей и приложений,
- мониторинг сетевых ресурсов,
- поддержка защищенных каналов связи с удаленными офисами и сотрудниками,
- предотвращение атак, вторжений и проникновения вирусов и спама,
- фильтрация содержимого,
- отказоустойчивое резервирование связи и распределения нагрузки между выделенными каналами связи провайдеров.

Лекция 6
Вопросы безопасности в сети

Межсетевые экраны . Функции безопасности и VPN:

Функции безопасности:

*Для безопасности VLAN применяются правила IPSec, L2TP (over IPSec), SSL;

*применяется проверка безопасности endpoints (End Point Secirity);

*политика управления доступом (по критериям: ip-адрес / порт/ пользова-тель / время);

*блокировка URL из заданного списка и по ключевым словам;

*блокировка JAVA-апплетов, cookies, ActiveX;

*применяются процедуры предотвращения DoS/DDoS атаки и определение аномального трафика (сканирование портов, лавины);

*защита от дефектных пакетов; определение аномалий в протоколах HTTP/ICMP/TCP/UDP;

Безопасность VPN:

*применение маршрутизированных туннелей IPSec VPN

*аутентификация в туннеле процедурами: MDS,SHA-1, SHA-2;

*управление ключами: вручную, IKE; *PKI:PKCS #7, #10, #12;

*регистрация сертификатов: CMP, SCEP;

*алгоритм упреждающей смены ключей (PFS);

*применение аутентифицирующего заголовка (AH);

*инкапсуляция зашифрованных данных (ESP);

*поддержка NAT поверх IPSec и NAT Traversal;

*DPD (dead peer detection); * reverse Proxy.

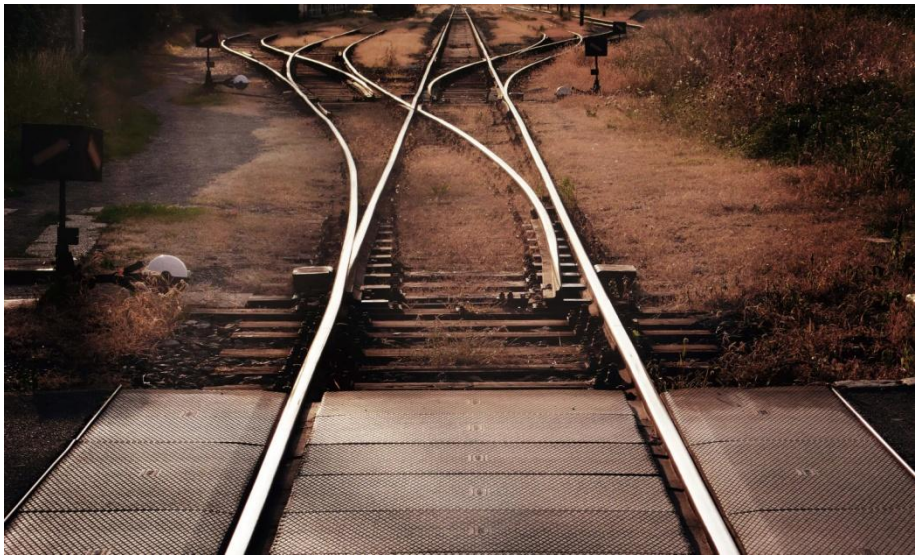
Лекция 6
Вопросы безопасности в сети

Межсетевые экраны . Авторизация:

Функции авторизации пользователя:

*применение алгоритмов RADIUS, LDAP, MS Active Directory и др.;
*поддержка двухфакторной аутентификации (OTP);
*политика правил на основе пользователей или групп.

Лекция 3.
Маршрутизация в сети.



Маршрутизатор (***router***) – мощное вычислительное УК, с одним или несколькими специализированными процессорами (часто построенными по RISC архитектуре); специализированный компьютер с высокоскоростной шиной/шинами (с пропускной способностью в среднем 600-2000 Мбит/с), со специализированной ОС. Обеспечивает выбор оптимального маршрута, а также некоторые дополнительные высокоуровневые функции.

Уровень в модели OSI: L3, L4 (…).

Принцип работы: для каждого приходящего фрейма (пакета) осуществляется выбор наилучшего маршрута в сети путём вычисления сложного алгоритма состояния связей для определения оптимальный путь на графе сети (протоколы OSPF, NLSP, IS-IS).

Виды маршрутизаторов:

м. магистральные (backbone router): для построения центральной сети из множества LAN в разных территориальных локациях; обработка 10^5-10^6 пакетов в секунду, большое кол-во интерфейсов;

м. региональные: для соединения региональных отделений с центральной сетью; менее скоростной, меньше портов;

м. удаленных офисов: *для соединения LAN удаленного офиса к центральной сети через глобальную связь*; может содержать несколько интерфейсов (FastEthernet/GigEthernet, выделенная линия);

м. локальных сетей (коммутатор L3): для разделения крупных локальных сетей на подсети, основная особенность – высокоскоростная маршрутизация, отсутствие низкоскоростных портов.

Лекция 6
Маршрутизация в сети

Маршрутизация – процесс выбора определенного оптимального набора узлов в сети, через которые происходит соединения между двумя узлами сети (источником и получателем)

Или же

Маршрутизация – процесс передачи пакетов какого-либо протокола при помощи специального протокола маршрутизации, при котором может осуществляться выбор оптимального набора узлов в сети, через которые происходит соединение между двумя узлами сети (источником и получателем).

Оптимальность маршрута: определяется взвешенной суммой времен доставки сообщения между узлами на маршрутном пути при фиксированном значении вероятности его доставки.

Административное расстояние – мера достоверности, подсказка для выбора из нескольких оптимальных маршрутов от разных протоколов, которые включены на устройстве. Чем меньше, тем лучше

Метрика – вычисляется на основании одного или нескольких параметров: задержка (зависит от пропускной способности промежуточных линий, размера очереди в портах, загрузки сети и физического расстояния); ширина полосы пропускания канала; загрузка (средняя); надежность (относительное количество ошибок в канале); количество переходов; стоимость (составное значение, назначает администратор).

Таблица маршрутизации

Механизм получения маршрута	Получатель (сеть, узел)	Административное расстояние	Метрика маршрута	Адрес интерфейса м. на расстоянии пересылки (via)	Время присутствия маршрута	Выходной интерфейс маршрутизатора
C - direct		Connected - 0		192.168.5.11	0:00:00	Serial0
S - static	192.168.1.0	Static -1	5514496			GigEthernet0/1
I - IGRP	10.80.1.64	EIGRP - 5				FastEthernet 1/2
D - EIGRP	(с маской)	BGP - 20				
B-DGP		EGRP - 90				
E-EGP		IGRP - 100				
i - IS-IS		OSPF - 110				
…		RIP - 120				
…		…				

Выбор:
метрика
префикс
админ. расстояние

Статическая маршрутизация – назначается (прописывается) администратором сети, не физическое соединение, строка в таблице, в которой указывается IP адрес следующего соседнего маршрутизатора или выходной интерфейс.

Применение:

Небольшие сети, старое оборудование, администратор трудоголик-параноик, резервирование динамических маршрутов, служебный трафик не желателен

Плавающая статическая маршрутизация:

Статический маршрут выбирается из таблицы маршрутизации только в том случае, если динамический маршрут недоступен.

Маршрутизация по умолчанию:

Можно настроить маршрутизатор так, чтобы весь поток или часть его отправлять по специальному маршруту по умолчанию. Все специальные случаи при этом должны быть прописаны, поскольку в первую очередь проверяются они.

Динамическая маршрутизация – протокол назначается администратором на каждом маршрутизаторе. Маршрутизаторы обмениваются между собой информацией. При изменении топологии происходит адаптация маршрутных таблиц. Позволяет применять механизм балансировки нагрузки по нескольким маршрутам. Маршрутизатор может быть настроен на несколько протоколов.

Скорость подстройки:

Определяется временем общения удаленных маршрутизаторов

Внутренний протокол:

IGP – interior gateway protocol: RIP, EIGRP, OSPF.

Внешний протокол:

EGP – exterior gateway protocol: протокол внешнего шлюза, BGP.

Классовые-безклассовые:

Содержат или не содержат информацию о подсетях.

Известные производители сетевого оборудования:

Производитель	Страна
Cisco Systems	США
ZyXEL	Тайвань
Juniper networks	США
TP-link	Китай
NETGEAR	США
D-Link	Тайвань
MicroTik	Латвия
ASUS	Тайвань
Huawei	Китай