**Требования к оформлению домашней контрольной работе (ДКР).**

(ДКР)должна быть грамотно написана и правильно оформлена.

Текст работы должен быть набран в редакторе Microsoft Word (v.10 – v.19)

***Титульный лист в приложении***.

(ДКР)выполняется на белой бумаге формата А4 (210×297 мм) компьютерного набора и последующей печати без режима экономии тонера и чернил. Текст должен иметь четкие очертания всех символов. Печать должна быть без смазывания и непрочитанных мест, помарок и исправлений.

Нумерация страниц проводится внизу, по центру страницы, арабскими цифрами.

Текст: шрифт Times New Roman, размер основного текста – 14, размер заголовков – 16, поля: слева – 3,5 см, сверху – 2,5 см, справа – 2 см, внизу – 2 см, абзацный отступ – 1,25. Основной текст (ДКР)печатается 1,5 междустрочным интервалом компьютерного набора. Выравнивание текста устанавливается «По левому краю».

Графическое изображение и условные обозначения элементов схем должны приводиться в соответствии с ГОСТом. Название рисунка приводится над рисунком. Номера рисунков должны быть порядковыми и ставятся под рисунком.

**В конце выполнения работы следует привести список литературы, которая использовалась для выполнения данной работы, поставить дату выполнения работы и разборчиво подпись.**

Проверенные преподавателем работы сохраняется студентом до экзамена и предъявляется на экзамене со всеми необходимыми исправлениями и дополнениями, согласно рецензии преподавателя. Без зачетной контрольной работы студент не допускается к сдаче экзамена.

**Введение.**

**Информационная безопасность предприятия.**

Для каждого современного предприятия, компании или организации одной из самых главных задач является именно обеспечение информационной безопасности. Когда предприятие стабильно защищает свою информационную систему, оно создает надежную и безопасную среду для своей деятельности. Повреждение, утечка, неимение и кража информации — это всегда убытки для каждой компании. Например, могут появиться убытки от плохой репутации компании, от отсутствия клиентов, от затрат на возобновление стабильной работы или от потери важной информации, которой располагала данная компания.

На данный момент сформулировано три базовых задачи, которые должна обеспечивать информационная безопасность:

* **Целостность данных** — защита от сбоев, ведущих к потере информации, а также защита от незаконного создания или уничтожения данных. Примером нарушения целостности данных является повреждение бухгалтерских баз, в дальнейшем это повлечет за собой последствия, которые определенно станут негативными для компании.
* **Конфиденциальность информации** — незаконное разглашение, утечка, повреждение информации;
* **Доступность информации для всех пользователей** — отказ в обслуживании или услугах, которые могут быть вызваны вирусной активностью или действиями злоумышленников.

Нарушение одного из этих аспектов может привести к невозможности нормальной работы предприятия. На наличие любого из нарушений могут повлиять и внутренние, и внешние угрозы. Учитывая сегодняшнее развитие информационного общества, можно сделать вывод о тенденции к росту количества угроз безопасности.

Полноценная информационная безопасность компаний предполагает постоянный контроль всех существенных событий и состояний, которые влияют на надежность защиты информации. Причем, защита обязана осуществляться постоянно и охватывать весь жизненный цикл данных, то есть от ее поступления или создания до уничтожения или утраты важности и актуальности.

Основными факторами, оказывающими влияние на защиту информации и данных на предприятии, являются:

* Приумножение сотрудничества компании с партнерами;
* Автоматизация бизнес-процессов;
* Тенденция к росту объемов информации предприятия, которая передается по доступным каналам связи;
* Тенденция к росту компьютерных преступлений.

Информационная защита предприятия определяется целым сочетанием предпринимаемых мер, которые направлены на безопасность важной информации. Эти меры можно разделить на две группы:

* Организационные меры;
* Технические меры.

Организационные меры заключаются в формальных процедурах и правилах работы с важной информацией, информационными сервисами и средствами защиты. Технические меры включают в себя использование программных средств контроля доступа, мониторинг утечек и краж информации, антивирусную защиту, защиту от электромагнитных излучений и т. д.

Задачи систем информационной безопасности компании многогранны. К примеру, это обеспечение надежного хранения данных на различных носителях; защита информации, передаваемой по каналам связи; ограничение доступа к некоторым данным; создание резервных копий и другое.

Полноценное обеспечение информационной безопасности компании реально только при правильном подходе к защите данных. В системе информационной безопасности нужно учитывать все актуальные на сегодняшний день угрозы и уязвимости.

**IP телефония**

До недавнего времени сети с коммутацией каналов (телефонные сети) и сети с коммутацией пакетов (IP-сети) существовали практически независимо друг от друга и использовались для различных целей. Телефонные сети использовались только для передачи голосовой информации, а IP-сети - для передачи данных.

IP-телефония - это технология, которая связывает два абсолютно разных мира - мир телефонии и мир интернет посредством устройства, называемого шлюз или gateway. Шлюз представляет собой устройство, в которое с одной стороны включаются телефонные линии, а с другой стороны - IP-сеть (например, Интернет).

**Что такое IP протокол?**

Протокол IP осуществляет передачу информации от узла к узлу сети в виде дискретных блоков - пакетов. При этом IP не несет ответственности за надежность доставки информации, целостность или сохранение порядка потока пакетов и, таким образом, не решает с необходимым для приложений качеством задачу передачи информации. Эту задачу решают два других протокола – **TCP** (Transfer Control Protocol, протокол управления передачей данных) и **UDP** (User Datagram Protocol, дейтаграммный протокол передачи данных) – которые используют процедуры протокола IP для передачи информации, добавляя к ним свою дополнительную функциональность.

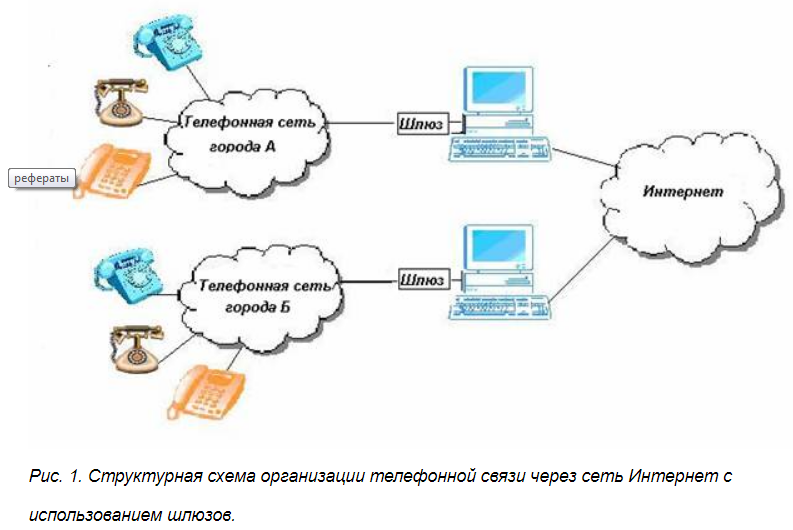
**Варианты построения IP-телефонных систем.**

Известны и практически реализуются две базовые схемы IP-телефонии.

1. Для пользователей персональных компьютеров: данная схема связана с организацией телефонных переговоров между пользователями персональных компьютеров, оснащенных мультимедийным оборудованием и (или) специальными программными (программно-аппаратными) средствами, обеспечивающим ведение дуплексных телефонных переговоров, необходимый сервис и контроль. Пользовательские компьютеры могут входить в состав локальной сети, иметь персональный IP-адрес.

2. Для пользователей телефонной сети: Данная схема предусматривает использование специальных многофункциональных устройств - шлюзов. Шлюз предназначен для преобразования аналоговых речевых и служебных сигналов в цифровую последовательность, организации из этой последовательности пакетов глобальной сети Интернет и передачи их в сеть, прием пакетов и восстановление цифровой последовательности - цифровых речевых и служебных сигналов и их преобразование в аналоговую форму, а так же решение большого перечня задач ,связанных с организацией интерфейсов, генерированием и детектированием сигналов абонентской сигнализации, управлением режимами телефонных переговоров и многое другое.

Однако главные задачи шлюза - обеспечение качественного дуплексного телефонного общения абонентов в режиме пакетной передачи и коммутации цифровых сигналов.



**Удаленные атаки на распределенные вычислительные системы**

Основной особенностью любой распределенной системы является то, что ее

компоненты распределены в пространстве и связь между ними физически

осуществляется при помощи сетевых соединений и программно при помощи

механизма сообщений. При этом все управляющие сообщения и данные,

пересылаемые между объектами распределенной ВС, передаются по сетевым

соединениям в виде пакетов обмена. Эта особенность является основной для

удаленных атак на инфраструктуру и протоколы IP-сетей.

**ЗАДАНИЕ**

**МДК 02.01. Технология монтажа и обслуживания компьютерных сетей.**

**Вводная.**

Организация купила блок публичных адресов класса С (*Варианты 1- 28*).

Немаловажной причиной разделения сети на подсети является обеспечение определённого уровня безопасности.

**Для этого** **необходимо выполнить следующие задачи:**

**Задача 1.** Выполнить расчет подсетей по варианту задания из таблицы:

|  |  |  |  |
| --- | --- | --- | --- |
| **Вариант/**  **(кол-во подсетей)** | **Сеть класса С** | **Вариант/**  **(кол-во подсетей)** | **Сеть класса С** |
| **1 (6)** | 223.68.10.0 | **15 (4)** | 200.50.14.0 |
| **2 (5)** | 195.8.25.0 | **16 (5)** | 194.12.130.0 |
| **3 (6)** | 222.240.36.0 | **17 (5)** | 193.18.1.0 |
| **4 (5)** | 193.158.15.0 | **18 (4)** | 201.191.55.0 |
| **5 (6)** | 220.195.1.0 | **19 (4)** | 215.16.13.0 |
| **6 (5)** | 192.200.70.0 | **20 (4)** | 211.165.100.0 |
| **7 (5)** | 195.186.38.0 | **21 (4)** | 205.42.3.0 |
| **8 (4)** | 200.50.14.0 | **22 (6)** | 223.68.10.0 |
| **9 (5)** | 194.12.130.0 | **23 (5)** | 195.8.25.0 |
| **10 (5)** | 193.18.1.0 | **24 (6)** | 222.240.36.0 |
| **11 (4)** | 201.191.55.0 | **25 (5)** | 193.158.15.0 |
| **12 (4)** | 215.16.13.0 | **26 (6)** | 220.195.1.0 |
| **13 (4)** | 211.165.100.0 | **27 (5)** | 192.200.70.0 |
| **14 (4)** | 205.42.3.0 | **28 (5)** | 195.186.38.0 |

Каждая сеть разделена на подсети по варианту, соединенные маршрутизаторами.

**Задача 2.** Выполнить формирование сети в программе NetEmul или Cisco Packet Tracer. Сделать скриншот сети согласно варианту.

***Дальнейшие задания выполняются только для одной (любой) подсети!***

**Задача 3.** Определить IP-адреса подсети, маску подсети.

**Задача 4.** Определить диапазон адресов в каждой подсети.

**Задача 5.** Вычислить широковещательные адреса каждой подсети.

**Задача 6.** Вычислить максимально возможное количество узлов в одной подсети.

**МДК 3.1. Технология применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи.**

**Задача 1.** Нарисовать одну локальную подсеть из работы МДК 02.01 в программе

NetEmul или Cisco Packet Tracer, согласно варианту.

**Задача 2.** Установить сервер в подсети (сделать скриншоты используя программу

Oracle VM VirtualBox).

**Задача 3.** Установить антивирусную программу (Антивирус, файрволл) на сервер. (сделать скриншоты)

**Методические указания**

**1. Пример применения маски для выделения номера сети и узла из некоторого IP адреса и маски:**

Пусть задан IP адрес: 210.56.78.212. Если техника масок не применяется, то номер сети 210.56.78.0, узел номер 212. Теперь сопоставим с этим адресом маску 255.255.255.224.

**Другая форма записи IP и маски - 210.56.78.212/27**

Что теперь номер сети, а что номер узла? На этот вопрос можно ответить, лишь записав и адрес, и маску в двоичной форме:

**Адрес: 11010010.00111000.01001110.11010100**

**Маска: 11111111.11111111.11111111.11100000**

маски класса С (в данном случае говорят «длиннее на три бита») Дальше мы можем записать номер узла и номер сети. Первые 27 бит записанного IP адреса – номер сети, в которой находится узел, остальные 5 бит – номер самого узла (хост). Запишем номер сети, для этого все биты, отвечающие за номер узла положим равными нулю:

Умножим наш IP адрес компьютера на сетевую маску получим:

**Адрес: 11010010.00111000.01001110.110|10100**

**Маска: 11111111.11111111.11111111.111|00000**

**Сеть: 11010010.00111000.01001110.110|00000**

Теперь осталось лишь перевести номер сети в привычную точечно-десятичную форму: 210.56.78.192.

**Проанализируем полученную сеть:**

Номер сети:

• 210.56.78.192.

**Количество узлов в этой сети:**

• Судя по количеству нулей в маске, для нумерации узлов остается 5 бит, следовательно, в этой сети 25 узлов, т.е. 32. Но, адрес, в котором все биты, отвечающие за номер узла равны «0», является номером сети и не может быть назначен узлу, а адрес, в котором все биты, отвечающие за номер узла равны «1» является широковещательным адресом в данную сеть и так же не может быть назначен узлу. Таким образом, в данной сети **2^х=25–2=30, т.е. 30 узлов, где х - колличество бит нулей хостовой части IP.**

**Найдем адрес первого узла в этой сети.** В этом случае, биты, отвечающие за номер узла должны принять минимальное значение, но не все быть равны нулям. Т.е. последние пять бит адреса должны принять значение 00001, и тогда адрес первого узла в этой сети выглядит следующим образом:

**Сеть: 11010010.00111000.01001110.110|00000**

**Маска: 11111111.11111111.11111111.111|00000**

**Узел: 11010010.00111000.01001110.110|00001**

Переводим его в точечно-десятичную запись: 210.56.78.193

**Найдем теперь самый большой номер узла**. В этом случае, биты адреса, отвечающие за номер узла должны быть все кроме последнего равны «1» (иначе получится широковещательный адрес сети).

**Сеть: 11010010.00111000.01001110.110|00000**

**Маска: 11111111.11111111.11111111.111|00000**

**Узел: 11010010.00111000.01001110.110|11110**

Переводим его в точечно-десятичную запись: 210.56.78.222

**Наконец найдем** **широковещательный (broadcast)** адрес сети, установив все биты IP

адреса, отвечающие за номер равными «1»:

**Сеть: 11010010.00111000.01001110.110|00000**

**Маска: 11111111.11111111.11111111.111|00000**

**Br-t: 11010010.00111000.01001110.110|11111**

Переводим его в точечно-десятичную запись: 210.56.78.223

**Итого, имеем:**

* Узел с IP адресом **(Address)** - 210.56.78.212;
* Битовая маска **(Bitmask )** – 24;
* Маска **(Netmask)** - 255.255.255.224;
* Инверсия маски (**Wildcard**)- 0.0.0.31;
* Этот узел находится в сети **(Network)** - 210.56.78.192;
* Класс **С**
* Широковещательный адрес сети **(Broadcast)** - 210.56.78.223;
* Первый узел **(HostMin)** - 210.56.78.193;
* Последний узел **(HostMax)** - 210.56.78.222
* Всего в сети **(Hosts/Net)** - 30 узлов;

**Наш узел в серединке 210.56.78.212**

**2. Деление сети на подсети. Расчет масок и подсетей.**

**Причины разбиения на подсети.**

Ранее при развёртывании сети организации часто подключали все компьютеры и другие сетевые устройства к одной IР-сети. Всем устройствам в организации назначались IР-адреса с одинаковой сетевой частью. Конфигурация такого типа называется плоской архитектурой сети. В небольшой сети с небольшим количеством устройств плоская архитектура не представляет проблемы. Однако по мере расширения сети с такой конфигурацией могут возникнуть серьёзные трудности.



Подумайте о том, как в сети Ethernet устройства выполняют поиск необходимых служб и устройств с помощью широковещательной рассылки. Как вы помните, широковещательное сообщение доставляется всем узлам данной сети. Протокол DHCP — пример сетевой службы, которая зависит от широковещательной рассылки. Устройства отправляют по сети широковещательные запросы, чтобы определить местонахождение DHCP-сервера. В крупной сети из-за этого может создаваться значительный трафик, который замедлит общую работу сети. Кроме того, поскольку широковещательная рассылка выполняется по всем устройствам, им необходимо принять и обработать трафик, что приводит к повышению требований к обработке.

**Если устройство должно обработать значительный объём широковещательных рассылок, это может даже привести к замедлению работы устройства. По этой причине более крупные сети необходимо разделить на более мелкие подсети, предназначенные для небольших групп устройств и служб.**

***Процесс сегментации сети путём разделения её на несколько более мелких сетей называется разбиением на подсети.*** ***Эти более мелкие сети называются подсетями.***

Сетевые администраторы могут группировать устройства и службы в подсети по их географическому местоположению (например, 3-й этаж здания), организационному подразделению (например, отдел продаж) или по типу устройств (принтеры, серверы, глобальная сеть и т.п.) или по другому значимому для сети принципу. Разбиение на подсети может снизить общую нагрузку на сеть и повысить её производительность.

***Примечание.***

***Подсеть аналогична сети, и оба этих термина можно использовать как синонимы. Большинство сетей сами являются подсетями более крупных блоков адресов.***

**Разбиение домена широковещания.**

***Первая причина разбиения сети на подсети заключается в том, чтобы не получить огромный broadcast домен.***

В современных IPv4 сетях широковещательный (*broadcast*) трафик является необходимым злом. Например, при помощи широковещательных запросов работает протокол *ARP*, операционная система Windows постоянно что-то рассылает в сеть, чтобы обнаружить другие компьютеры и т.п. Если мы подключим в одну сеть 65 тысяч устройств, то получится, что каждый квант времени кто-то что-то да отправит широковещательного. Такая сеть совершенно не сможет работать, потому что все будут заняты получением широковещательных пакетов. Если мы разобьём такую сеть, например, на 256 сетей в каждой из которых 254 хоста, то мы получим 256 отдельных небольших broadcast доменов, в каждом из которых действует сравнительно небольшое (254) количество источников широковещательного трафика. Такие сети уже смогут работать нормально.

***Второй немаловажной причиной разделения сети на подсети является обеспечение определённого уровня безопасности.***

Дело в том, что в пределах локальной сети у нас сравнительно мало возможностей обеспечения контроля за трафиком. Мы можем, конечно, контролировать на коммутаторах MAC адреса, можем довольно много чего настроить на конечных устройствах (например, сложные правила файрвола на компьютерах).

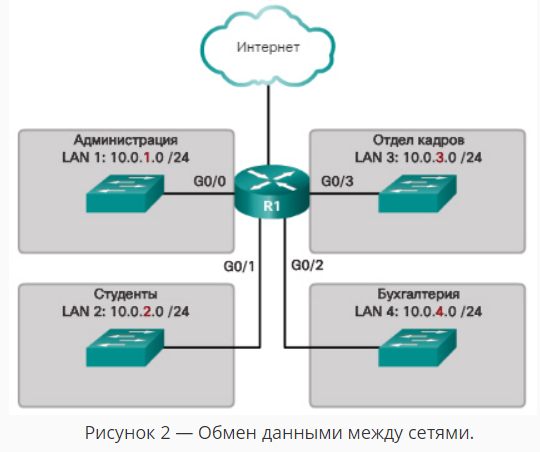
Но лучше всего этим заниматься централизованно при переходе трафика из одной сети в другую. На маршрутизаторе настраивается централизованная фильтрация, можно даже настроить Firewall на маршрутизаторе.

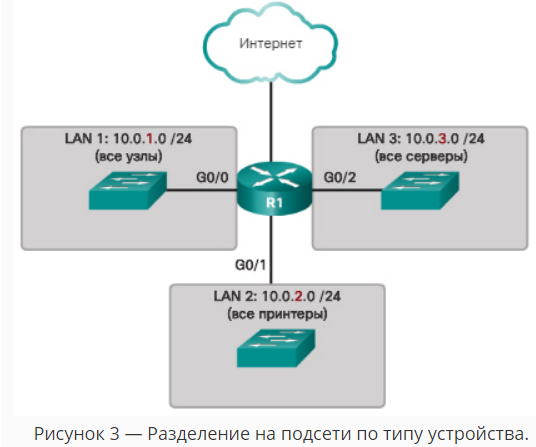
Существует несколько способов использования подсетей для управления сетевыми устройствами. Сетевые администраторы могут группировать устройства в подсети по следующим принципам.

* Местоположение, например, по этажам здания (рисунок 1)
* Подразделение (рисунок 2)
* Тип устройства (рисунок 3)
* Любой другой значимый для сети принцип.

Обратите внимание, что на каждом рисунке для подсетей используется более длинный префикс, обозначающий сеть.



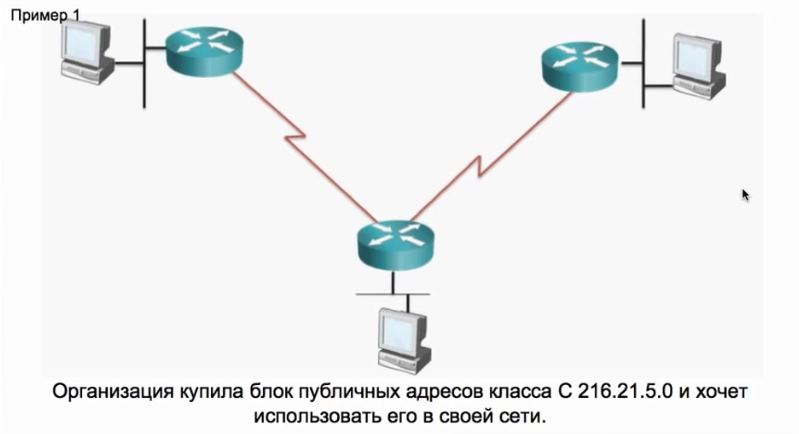




***Понимание принципа разделения сети на подсети — главный навык, которым должен обладать каждый сетевой администратор.***

**I часть.**

**Деление сети на подсети.**



**Вопрос:** ***Сколько на рисунке подсетей?***

**Пример 1. Разделить сеть на 5 подсетей.**

**Маска класса С**

**Дано:** 216.21.5.0/24

255.255.255.0

1. **Узнаем количество сетей которое нам нужно, и переводим это число в двоичный вид.**

1024 512 256 128 64 32 16 8 4 2 1

5s = 0 0 0 0 0 0 0 0 1 0 1

Необходимо вычислить общее колличество бит для определения подсетей.

1 0 1 - **3 бита**

1. **Резервируем нужное колличество бит в маске, ищем инкремент.**

255.255.255.0 – 11111111.11111111.11111111.00000000

Необходимо зарезервировать необходимое колличество бит в маске.

Резервируем колличество подсетей, добавляем в хостовую часть 3 бита едениц.

11111111.11111111.11111111.11100000 – 255.255.255.224 = /27

Сетевая часть Хостовая часть

***Вариант: К префиксу исходной маски (24) добавляем 3. Получаем / 27***

**Поиск Инкремента**

***increment of growth — инкремент нарастания***

**Инкремент** это число, с помощью которого можно подсчитать подсети.

Определяется последняя еденица в маске, и определяется десятичное число, соответствующее весам двоичной комбинации.

1024 512 256 128 64 32 16 8 4 2 1

11111111.11111111.11111111.11100000

Инкремент равен 32.

1. **Используем инкремент для поиска сетевого диапазона.**

1 сеть: 216.21.5.0 - 216.21.5.31 1-30 хостов

2 сеть: 216.21.5.32 - 216.21.5.63 33-62 хостов

3 сеть: 216.21.5.64 - 216.21.5.95 65-94 хостов

4 сеть: 216.21.5.96 - 216.21.5.127 97-126 хостов

5 сеть: 216.21.5.128 – 216.21.5.159 129-158 хостов

Можем использовать 1-30 хостов.

***Мы не можем использовать сетевой и широковещательный адреса***

216.21.5.0 - сетевой адрес

216.21.5.31 - широковещательный адрес

**Пример 2. Разделить сеть на 50 подсетей. Маска класса С**

**Дано:** 195.5.20.0/24

255.255.255.0

1. **Узнаем количество сетей которое нам нужно, и переводим это число в двоичный вид.**

1024 512 256 128 64 32 16 8 4 2 1

50s = 0 0 0 0 0 1 1 0 0 1 0

Необходимо вычислить общее колличество бит для определения подсетей.

1 1 0 0 1 0 - **6 бит**

**2. Резервируем нужное колличество бит в маске, ищем инкремент.**

255.255.255.0 – 11111111.11111111.11111111.00000000

Необходимо зарезервировать необходимое колличество бит в маске.

Резервируем колличество подсетей, добавляем в хостовую часть 6 бит едениц.

11111111.11111111.11111111.11111100 – 255.255.255.252 = /30

Сетевая часть Хостовая часть

***Вариант: К префиксу исходной маски (24) добавляем 6. Получаем / 30***

**Поиск Инкремента**

Определяется последняя еденица в маске, и определяется десятичное число, соответствующее весам двоичной комбинации.

1024 512 256 128 64 32 16 8 4 2 1

11111111.11111111.11111111.111111 0 0

Инкремент равен 4.

**3. Используем инкремент для поиска сетевого диапазона.**

**1 сеть:** 195.5.20.0 - 195.5.20.3 **4 сеть:** 195.5.20.12 - 195.5.20.15

**2 сеть:** 195.5.20.4 - 195.5.20.7 **5 сеть:** 195.5.20.16 - 195.5.20.19

**3 сеть:** 195.5.20.8 - 195.5.20.11 **и. т. д.**

**Пример 3. Разделить сеть на 100 подсетей. Маска класса B.**

**Дано:** 150.5.0.0/16

255.255.0.0

1. **Узнаем количество сетей которое нам нужно, и переводим это число в двоичный вид.**

1024 512 256 128 64 32 16 8 4 2 1

100s = 0 0 0 0 1 1 0 0 1 0 0

Необходимо вычислить общее колличество бит для определения подсетей.

1 1 0 0 1 0 0 - **7 бит**

**2. Резервируем нужное колличество бит в маске, ищем инкремент.**

255.255.0.0 – 11111111.11111111.00000000.00000000

Необходимо зарезервировать необходимое колличество бит в маске.

Резервируем колличество подсетей, добавляем в хостовую часть 7 бит едениц.

11111111.11111111.11111110.00000000 – 255.255.254.0 = /23

Сетевая часть Хостовая часть

***Вариант: К префиксу исходной маски (16) добавляем 7. Получаем / 23***

**Поиск Инкремента**

Определяется последняя еденица в маске, и определяется десятичное число, соответствующее весам двоичной комбинации.

1024 512 256 128 64 32 16 8 4 2 1

11111111.11111111.1 1 1 1 1 1 1 0.00000000

Инкремент равен 2.

***Правила сложения.***

По аналогии 19+1 =20 

**3. Используем инкремент для поиска сетевого диапазона.**

**1 сеть:** 150.5.0.0 - 150.5.1.255

**2 сеть:** 150.5.2.0 – 150.5.3.255

**3 сеть:** 150.5.4.0 – 150.5.5.255

**4 сеть:** 150.5.6.0 - 150.5.7.255

**5 сеть:** 150.5.8.0 - 150.5.9.255

**и. т. д.**

**Пример 4. Разделить сеть на 1000 подсетей. Маска класса A.**

**Дано:** 10.0.0.0/8

255.0.0.0

1. **Узнаем количество сетей которое нам нужно, и переводим это число в двоичный вид.**

1024 512 256 128 64 32 16 8 4 2 1

1000s = 0 1 1 1 1 1 0 1 0 0 0

Необходимо вычислить общее колличество бит для определения подсетей.

1 1 1 1 1 0 1 0 0 0 - **10 бит**

**2. Резервируем нужное колличество бит в маске, ищем инкремент.**

255.0.0.0 – 11111111.00000000.00000000.00000000

Необходимо зарезервировать необходимое колличество бит в маске.

Резервируем колличество подсетей, добавляем в хостовую часть 10 бит едениц.

11111111.11111111.11000000.00000000– 255.255.192.0 = /18

Сетевая часть Хостовая часть

***Вариант: К префиксу исходной маски (8) добавляем 10. Получаем / 18***

**Поиск Инкремента**

Определяется последняя еденица в маске, и определяется десятичное число, соответствующее весам двоичной комбинации.

1024 512 256 128 64 32 16 8 4 2 1

11111111.11111111.1 1 0 0 0 0 0 0.00000000

Инкремент равен 64.

***Правила сложения.***

По аналогии 19+1 =20 

**3. Используем инкремент для поиска сетевого диапазона.**

**1 сеть:** 10.0.0.0 – 10.0.63.255

**2 сеть:** 10.0.64.0 – 10.0.127.255

**3 сеть:** 10.0.128.0 – 10.0.191.255

**4 сеть:** 10.0.192.0 – 10.0.255.255

**и. т. д.**

10.0.0.0 – сеть **(Network)**

255.255.192.0 - Битовая маска **(Bitmask )** – 18

10.0.63.255 – широковещательный адрес **(Broadcast)**

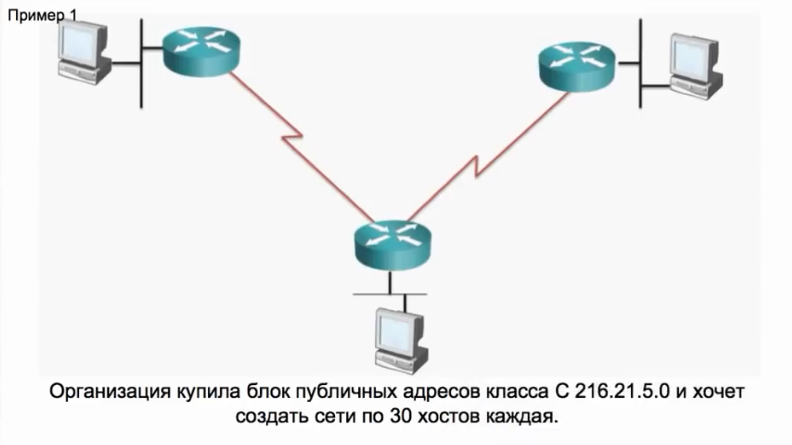
10.0.0.1 – первый хост **(HostMin)**

10.0.63.254 – последний хост **(HostMax)**

2^X-2 = 2^14 – 2 = 16384 хоста - Всего в сети **(Hosts/Net)**

**II часть**

**Обратная задача:**



**Пример 1. Создать сеть по 30 (host) хостов каждая.**

**Маска класса С**

**Дано:** 216.21.5.0/24

255.255.255.0

1. **Узнаем количество хостов которое нам нужно, и переводим это число в двоичный вид.**

1024 512 256 128 64 32 16 8 4 2 1

30h = 0 0 0 0 0 0 1 1 1 1 0

Необходимо вычислить общее колличество бит для определения подсетей.

1 1 1 1 0 - **5 бит**

1. **Резервируем нужное колличество бит в маске, ищем инкремент.**

255.255.255.0 – 11111111.11111111.11111111.00000000

Необходимо зарезервировать необходимое колличество бит в маске.

Резервируем колличество подсетей, добавляем в хостовую часть справа 5 бит нулей.

11111111.11111111.11111111.11100000 – 255.255.255.224 = /27

Сетевая часть Хостовая часть

***Вариант: К префиксу исходной маски (24) добавляем 3. Получаем / 27***

**Поиск Инкремента**

***increment of growth — инкремент нарастания***

**Инкремент** это число, с помощью которого можно подсчитать подсети.

Определяется последняя еденица в маске, и определяется десятичное число, соответствующее весам двоичной комбинации.

1024 512 256 128 64 32 16 8 4 2 1

11111111.11111111.11111111.111 0 0 0 0 0

Инкремент равен 32.

1. **Используем инкремент для поиска сетевого диапазона.**

1 сеть: 216.21.5.0 - 216.21.5.31 1-32 хостов

2 сеть: 216.21.5.32 - 216.21.5.63 33-62 хостов

3 сеть: 216.21.5.64 - 216.21.5.95 65-94 хостов

4 сеть: 216.21.5.96 - 216.21.5.127 97-126 хостов

5 сеть: 216.21.5.128 – 216.21.5.159 129-158 хостов

Можем использовать 1-30 хостов.

***Мы не можем использовать сетевой и широковещательный адреса***

216.21.5.0 - сетевой адрес

216.21.5.31 - широковещательный адрес

**Пример 2. Создать сеть по 50 (host) хостов каждая. Маска класса С**

**Дано:** 195.5.20.0/24

255.255.255.0

1. **Узнаем количество хостов которое нам нужно, и переводим это число в двоичный вид.**

1024 512 256 128 64 32 16 8 4 2 1

50h = 0 0 0 0 0 1 1 0 0 1 0

Необходимо вычислить общее колличество бит для определения подсетей.

1 1 0 0 1 0 - **6 бит**

**2. Резервируем нужное колличество бит в маске, ищем инкремент.**

255.255.255.0 – 11111111.11111111.11111111.00000000

Необходимо зарезервировать необходимое колличество бит в маске.

Резервируем колличество подсетей, добавляем в хостовую часть справа 6 бит нулей.

11111111.11111111.11111111.11000000 – 255.255.255.192 = /26

Сетевая часть Хостовая часть

***Вариант: К префиксу исходной маски (24) добавляем 2. Получаем / 26***

**Поиск Инкремента**

Определяется последняя еденица в маске, и определяется десятичное число, соответствующее весам двоичной комбинации.

1024 512 256 128 64 32 16 8 4 2 1

11111111.11111111.11111111.11 0 0 0 0 0 0

Инкремент равен 64.

**3. Используем инкремент для поиска сетевого диапазона.**

**1 сеть:** 195.5.20.0 - 195.5.20.63

**2 сеть:** 195.5.20.64 - 195.5.20.127

**3 сеть:** 195.5.20.128 - 195.5.20.191

**4 сеть:** 195.5.20.192 - 195.5.20.255

**5 сеть:** 195.5.21.0 - 195.5.21.63

**и. т. д.**

Можем использовать 2^X-2 = 2^6 – 2 = 62 хоста - **(Hosts/Net)**

***Мы не можем использовать сетевой и широковещательный адреса***

195.5.20.0 - сетевой адрес

195.5.20.63 - широковещательный адрес

**Пример 3. Создать сеть по 500 (host) хостов каждая. Маска класса B.**

**Дано:** 150.5.0.0/16

255.255.0.0

1. **Узнаем количество хостов которое нам нужно, и переводим это число в двоичный вид.**

1024 512 256 128 64 32 16 8 4 2 1

500h = 0 0 1 1 1 1 1 0 1 0 0

Необходимо вычислить общее колличество бит для определения подсетей.

1 1 1 1 1 0 1 0 0- **9 бит**

**2. Резервируем нужное колличество бит в маске, ищем инкремент.**

255.255.0.0 – 11111111.11111111.00000000.00000000

Необходимо зарезервировать необходимое колличество бит в маске.

Резервируем колличество подсетей, добавляем в хостовую часть справа 9 бит нулей.

11111111.11111111.11111110.00000000 – 255.255.254.0 = /23

Сетевая часть Хостовая часть

***Вариант: К префиксу исходной маски (16) добавляем 7. Получаем / 23***

**Поиск Инкремента**

Определяется последняя еденица в маске, и определяется десятичное число, соответствующее весам двоичной комбинации.

1024 512 256 128 64 32 16 8 4 2 1

11111111.11111111.1 1 1 1 1 1 1 0.00000000

Инкремент равен 2.

***Правила сложения.***

По аналогии 19+1 =20 

**3. Используем инкремент для поиска сетевого диапазона.**

**1 сеть:** 150.5.0.0 - 150.5.1.255

**2 сеть:** 150.5.2.0 – 150.5.3.255

**3 сеть:** 150.5.4.0 – 150.5.5.255

**4 сеть:** 150.5.6.0 - 150.5.7.255

**5 сеть:** 150.5.8.0 - 150.5.9.255

**и. т. д.**

**Пример 4. Создать сеть по 100 (host) хостов каждая.Маска класса A.**

**Дано:** 10.0.0.0/8

255.0.0.0

1. **Узнаем количество хостов которое нам нужно, и переводим это число в двоичный вид.**

1024 512 256 128 64 32 16 8 4 2 1

100s = 0 0 0 0 1 1 0 0 1 0 0

Необходимо вычислить общее колличество бит для определения подсетей.

1 1 0 0 1 0 0 - **7 бит**

**2. Резервируем нужное колличество бит в маске, ищем инкремент.**

255.0.0.0 – 11111111.00000000.00000000.00000000

Необходимо зарезервировать необходимое колличество бит в маске.

Резервируем колличество подсетей, добавляем в хостовую часть справа 7 бит нулей.

11111111.11111111.11111111.10000000– 255.255.255.128 = /25

Сетевая часть Хостовая часть

***Вариант: К префиксу исходной маски (8) добавляем 17. Получаем / 25***

**Поиск Инкремента**

Определяется последняя еденица в маске, и определяется десятичное число, соответствующее весам двоичной комбинации.

1024 512 256 128 64 32 16 8 4 2 1

11111111.11111111.11111111.1 0 0 0 0 0 0 0

Инкремент равен 128.

***Правила сложения.***

По аналогии 19+1 =20 

**3. Используем инкремент для поиска сетевого диапазона.**

**1 сеть:** 10.0.0.0 – 10.0.0.127

**2 сеть:** 10.0.0.128 – 10.0.0.255

**3 сеть:** 10.0.1.0 – 10.0.1.127

**4 сеть:** 10.0.1.128 – 10.0.1.255

**5 сеть:** 10.0.2.0 – 10.0.2.127

**6 сеть:** 10.0.2.128 – 10.0.2.255

**7 сеть:** 10.0.3.0 – 10.0.3.127

**8 сеть:** 10.0.3.128 – 10.0.3.255

**9 сеть:** 10.0.4.0 – 10.0.4.127

**10 сеть:** 10.0.4.128 – 10.0.4.255

**11 сеть:** 10.0.5.0 -

**и. т. д.**

10.0.0.0 – сеть **(Network)**

255.255.255.128 - Битовая маска **(Bitmask )** – 25

10.0.0.127 – широковещательный адрес **(Broadcast)**

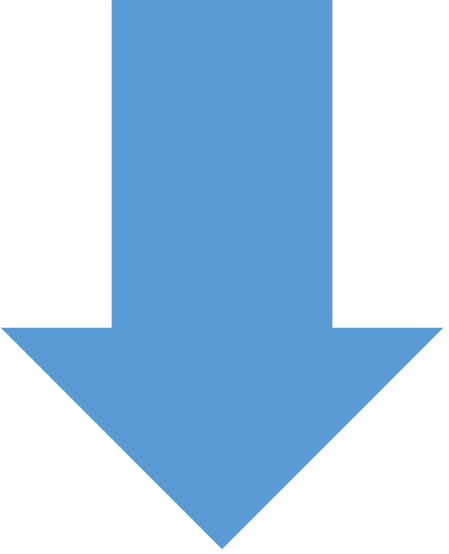
10.0.0.1 – первый хост **(HostMin)**

10.0.0.126 – последний хост **(HostMax)**

2^X-2 = 2^7 – 2 = 128-2=126 хостов - Всего в сети **(Hosts/Net)**

2^17 = 131072 - Колличество сетей

**Шпаргалка**

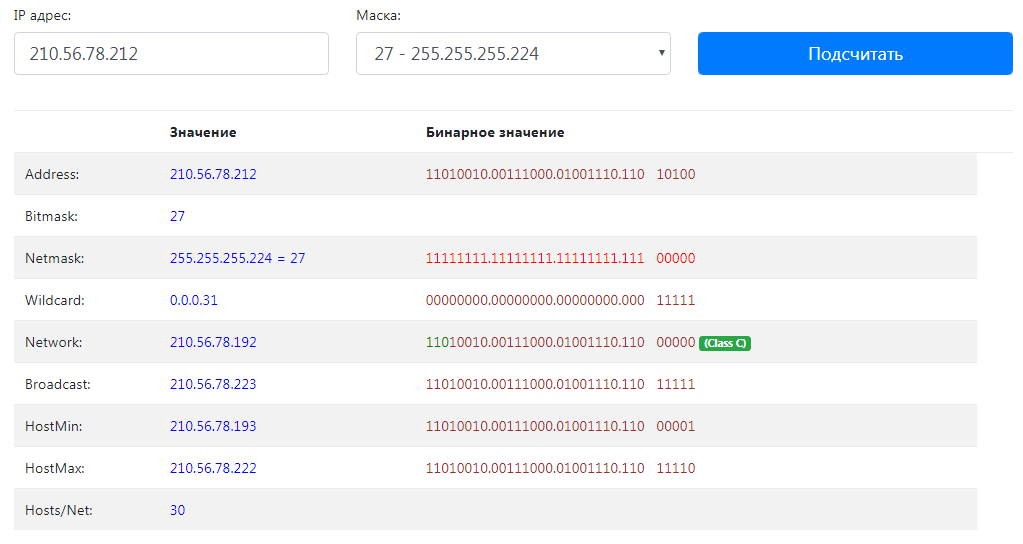


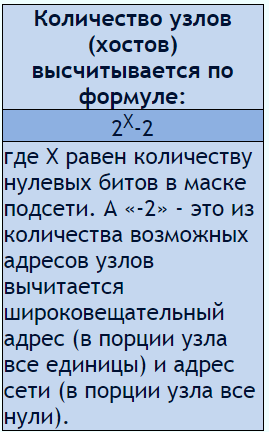
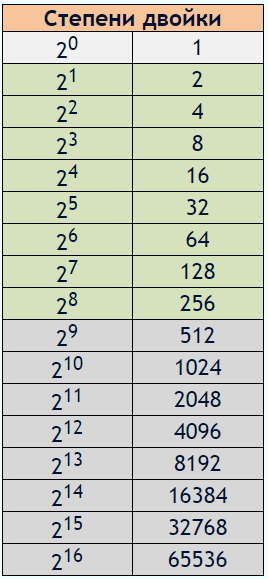
**Шпаргалка**

IP калькулятор : <https://ipcalc.co/> <http://wb0.ru/ipcalc.php>

Перевод чисел: <https://matworld.ru/calculator/perevod-chisel.php>

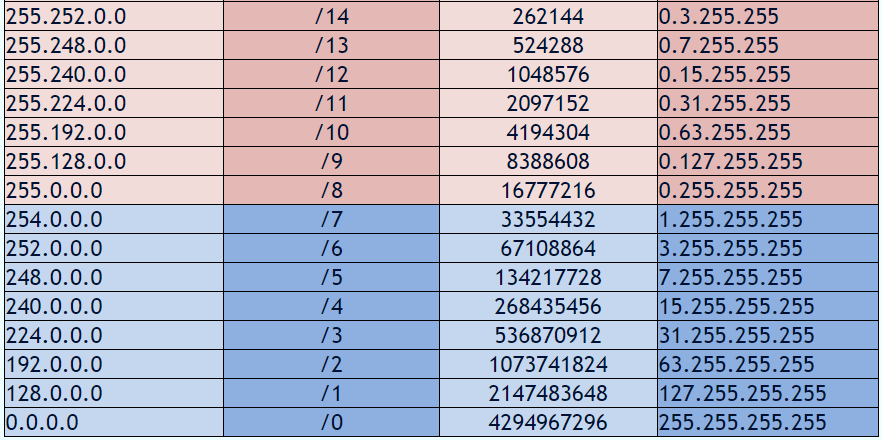
Решение:

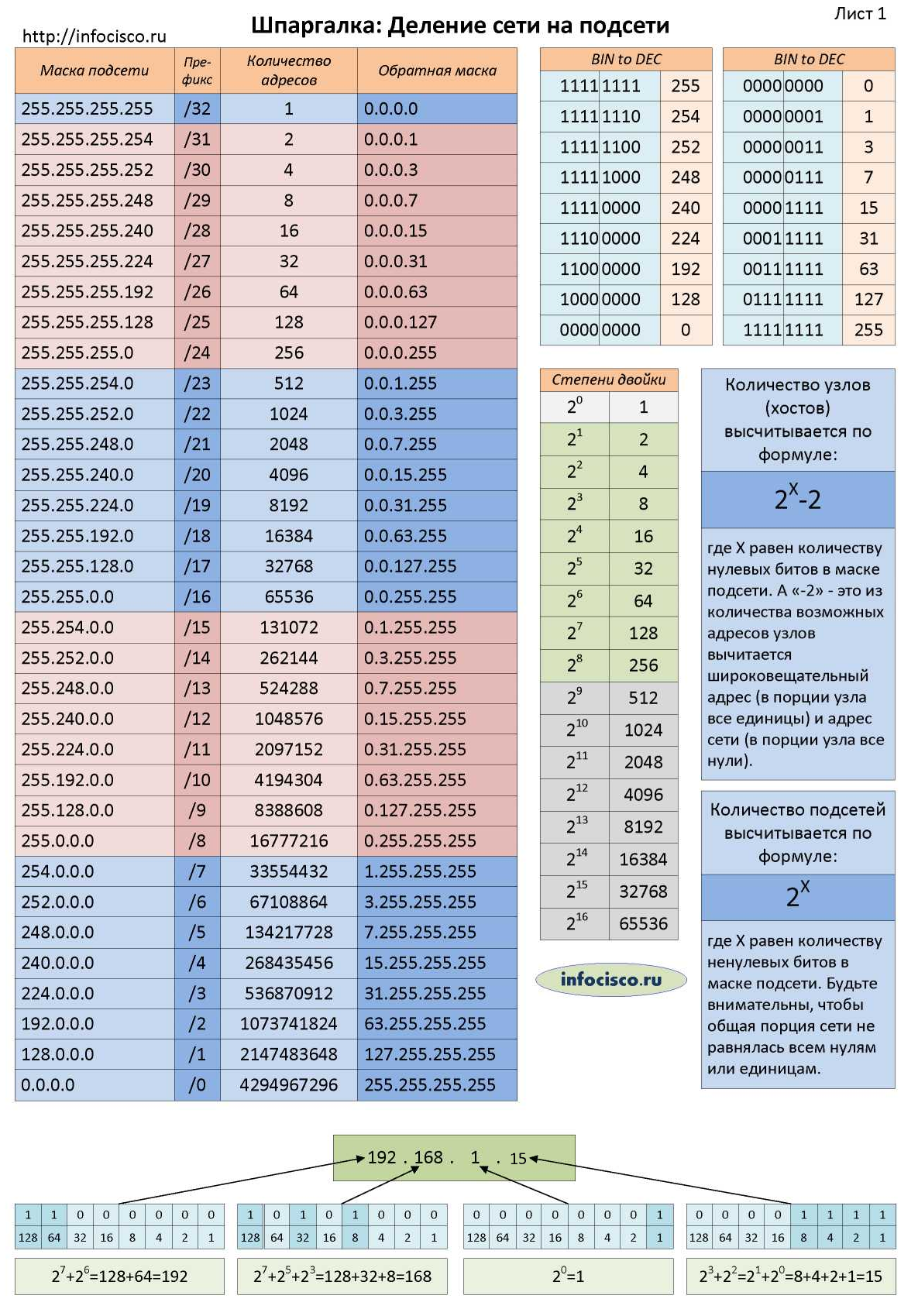


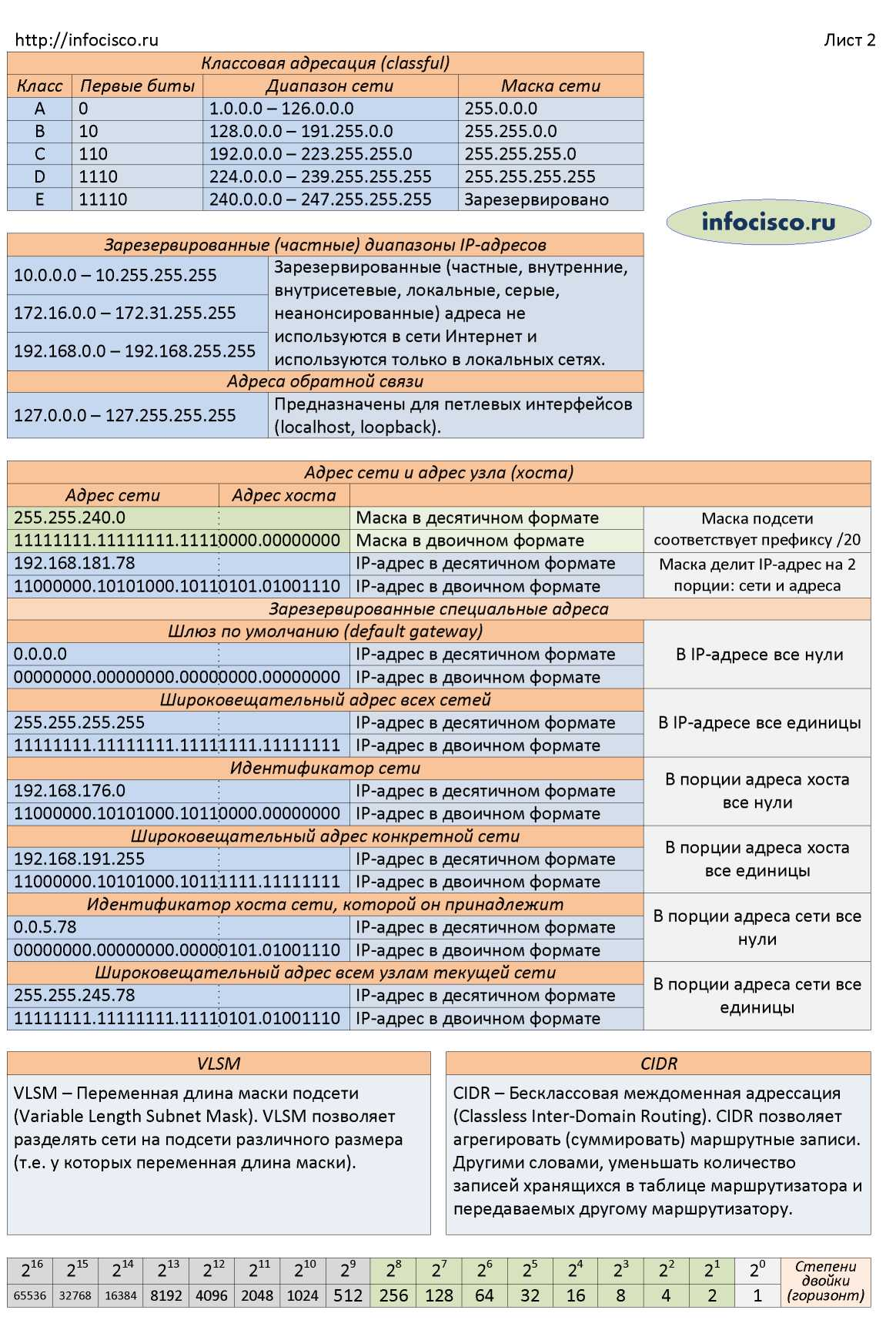
  











**Литература.**

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер,2016.
2. <https://www.intuit.ru> Курс «Работа в программе Cisco Packet Tracer»
3. [www.intuit.ru](http://www.intuit.ru) 6 Курс «Безопасность информационных систем»
4. [www.intuit.ru](http://www.intuit.ru) 2 Курс «Основы информационной безопасности»
5. <https://www.intuit.ru/studies/courses/3688/930/info> Курс «Компьютерные сети»

ПРИЛОЖЕНИЕ

**Федеральное агентство связи**

Колледж телекоммуникаций

ордена Трудового Красного Знамени

федерального государственного бюджетного

образовательного учреждения высшего образования

«Московский технический университет связи и информатики»

**(КТ МТУСИ)**

**ДОМАШНЯЯ КОНТРОЛЬНАЯ РАБОТА**

По специальности № 11.02.09

«Многоканальные телекоммуникационные системы»

(заочная форма обучения)

**МДК 02.01.** **Технология монтажа и обслуживания компьютерных сетей.**

Студент\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

Курс Группа / МЗ-219 /

Шифр /\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Оценка /\_\_\_\_\_\_\_\_\_\_\_\_\_/ Дата /\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

Преподаватель:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Пазий С. И. /

Регистрация:

Москва 2021 г.

**Федеральное агентство связи**

Колледж телекоммуникаций

ордена Трудового Красного Знамени

федерального государственного бюджетного

образовательного учреждения высшего образования

«Московский технический университет связи и информатики»

**(КТ МТУСИ)**

**ДОМАШНЯЯ КОНТРОЛЬНАЯ РАБОТА**

По специальности № 11.02.09

«Многоканальные телекоммуникационные системы»

(заочная форма обучения)

**ПМ.03 Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи**

**МДК 3.1.** Технология применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи.

Студент\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

Курс Группа / МЗ-219 /

Шифр /\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Оценка /\_\_\_\_\_\_\_\_\_\_\_\_\_/ Дата /\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

Преподаватель:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Пазий С. И. /

Регистрация:

Москва 2021 г.