МАОУ «Средняя общеобразовательная школа р.п. Пинеровка Балашовского района»

LAN – это ЛКС.
Адресация узлов компьютерных сетей

Исследовательская работа

Выполнил Бузанов Денис,
ученик 10 класса

Учитель-консультант
Пичугин Виталий Владимирович

2019-2020 учебный год

План

Введение

Широкое распространение в современном мире средств компьютерной техники предполагает обеспечение взаимосвязи между отдельными компьютерами, гаджетами, периферийными устройствами. При объединении узлов в сеть необходимо решать проблему их адресации.

Исследовательская работа в рамках проекта «LAN – это ЛКС» посвящена исследованию адресации узлов компьютерной сети. Анализ ситуации с распространением компьютерных сетей и перспектив их модернизации позволяет сделать вывод, что тема исследования актуальна в наше время, потому что компьютерные сети очень востребованы в современном обществе, технике, производстве.

Цель работы – исследовать и проанализировать существующее адресное пространство и создать модель сегмента школьной ЛКС.

Среди задач – ответы на предметные вопросы проекта:

Что является узлом сети? Что является физическим адресом узла сети?

Что является логическим адресом узла сети?

Для каких целей используется адресация в сети?

Для чего используют широковещательный адрес?

Какие технические и программные средства фиксируют адрес узла в сети?

Для чего используют маску подсети?

Объект исследования – компьютерные сети.

Предмет исследования – адресация узлов компьютерных сетей.

Используемые методы: изучение и обобщение, анализ информации, сравнение и сопоставление, классификация, моделирование.

На этапе моделирования возникает необходимость изучения компьютерного приложения NetEmul. Приложение NetEmul предоставляет возможность построить наглядную имитационную модель сегмента школьной компьютерной сети.

Исследовательская работа имеет существенную практическую значимость, поскольку приобретённые знания позволяют настраивать локальные компьютерные сети, конструировать локальные сети для решения конкретных задач. При настройке протокола TCP/IP на компьютере с операционной системой MS Windows в параметрах настройки TCP/IP должны быть указаны IP-адрес, маска подсети. Чтобы настроить протокол TCP/IP правильно, необходимо понимать, каким образом сетевые протоколы TCP/IP адресуются и подразделяются на сети и подсети.

I. Физические и логические основы адресации узлов сети

Компьютерная сеть – это совокупность компьютеров, периферийных устройств, соединенных между собой согласно установленным правилам и принципам. Сеть может быть локальной и глобальной, состоять из двух и более узлов. Максимальное количество компьютеров в сети не ограничивается.

Локальная компьютерная сеть (ЛКС, англ. Local Area Network – LAN) – это относительно небольшая сеть компьютеров, имеющих непосредственное соединение между собой. Как правило, такая сеть покрывает небольшую территорию (кабинет, здание, несколько близко расположенных зданий). Устройства в такой сети могут обмениваться информацией, передавать команды и данные.

Интернет (англ. Internet) – это глобальная компьютерная сеть, в состав которой входят национальные, региональные и локальные сети, раскинувшаяся в масштабах всего Земного шара. Компьютеры, которые постоянно подключены к сети Интернет и находятся в постоянно включенном состоянии, называются серверами-хостами. Современный Интернет состоит из миллионов узловых компьютеров, обслуживающих сотни миллионов пользователей

Узел сети – это часть компьютерной сети или устройство, соединенное с другими участниками (узлами) данной сети. Это может быть как компьютер, так и специальный коммутатор или маршрутизатор.

Физический адрес (Hardware Address) узла сети – определяется используемой сетевой технологией. В технологии локальных сетей в качестве физического адреса узла используется так называемый MAC-адрес (англ. Media Access Control – управление доступом к среде) сетевого адаптера компьютера или порта маршрутизатора. MAC-адрес – это уникальный идентификатор интерфейса. Стандартом Ethernet предусмотрено использование уникального значения MAC-адреса, состоящего из шести байт информации, для каждого сетевого устройства. Каждый байт принято записывать в шестнадцатеричной системе счисления и отделять двоеточием, например,

00000000 00011110 10001100 00100110 10100001 11001000 – MAC-адрес,

00:1E:8C:26:A1:C8 – запись этого MAC-адреса.

Уникальность физических адресов достигается за счёт обращения производителей сетевых карт к контролирующему органу, именуемому IEEE Registration Authority, который, свою очередь, выделяет им пул адресов (больше 16 миллионов значений) для назначения новым устройствам. По трём старшим байтам MAC-адреса можно определить производителя. Существуют таблицы, позволяющие определить производителя по MAC-адресу.

Логический адрес – уникальный в рамках сегмента IP-адрес. Этот адрес обычно назначается администратором во время конфигурирования компьютеров и маршрутизаторов сети. При этом в случае, если узел одновременно входит в несколько IP-сетей, то он должен иметь несколько IP-адресов (по числу сетевых связей). Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение. Кроме того, IP-адреса не зависят от локальных физических MAC-адресов и организованы иерархически.

IP-адрес представляет собой 32-разрядный двоичный номер, который уникально идентифицирует узел (компьютер или устройство, например, принтер или маршрутизатор) в сети TCP/IP. Пример IP-адреса: 11000000010100011110111000010 0. Это число для человека трудно запомнить, трудно обрабатывать, поэтому обычно его делят на четыре секции (октеты) из восьми двоичных цифр и представляют десятичными разрядами, разделенных точками, например, 192.168.123.132.

IP-адрес состоит из двух частей. Первая левая часть IP-адреса обозначает адрес сети, последняя часть – адрес узла. Если рассмотреть IP-адрес 192.168.123.132 и разбить его на эти две части, то получится следующее: 192.168.123.0 – адрес сети, 0.0.0.132 – адрес узла.

Чтобы выделять эти части IP-адреса используют маску подсети. В протоколе TCP/IP части IP-адреса, используемые в качестве адреса сети и узла, не зафиксированы, следовательно, указанные выше адреса сети и узла невозможно определить без наличия дополнительных сведений. Данные сведения можно получить из другого 32-разрядного номера под названием «маска подсети». В этом примере маской подсети является 255.255.255.0. Значение этого номера понятно, если знать, что число 255 в двоичном обозначении соответствует десятичному числу 11111111; таким образом, маской подсети является номер:

11111111.11111111.11111111.0000000

Расположив IP-адрес и маску подсети «в столбик» для побитного умножения, можно выделить составляющие сети и узла:

11000000.10101000.01111011.10000100 – IP-адрес (192.168.123.132)
11111111.11111111.11111111.00000000 – маска (255.255.255.0)

Первые 24 разряда (число единиц в маске подсети) распознаются как адрес сети, а последние 8 разрядов (число оставшихся нолей в маске подсети) – адрес узла. Таким образом, получаем следующее:

11000000.10101000.01111011.00000000 – адрес сети (192.168.123.0)
00000000.00000000.00000000.10000100 – адрес узла (000.000.000.132)

Все десятичные маски подсети преобразовываются в двоичные числа, представленные единицами слева и нолями справа. Вот ещё некоторые распространенные маски подсети:

1111111.11111111.1111111.11000000 – маска 255.255.255.192
1111111.11111111.1111111.11100000 – маска 255.255.255.224

Для указания маски иногда используют, так называемый, префикс. Префикс маски – это короткая запись сетевой маски, определяет количество бит порции сети.

Рассмотрим формальную запись IP-адреса компьютера 192.168.105.21/24. Приписка /24 означает, что в маске левые первые 24 бита – единицы, т.е. префикс 24 соответствует маске 255.255.255.0, и, следовательно, адрес сети легко определить: 192.168.105.0.

Интернет-адреса распределяются организацией InterNIC, которая администрирует Интернет. Эти IP-адреса распределены по классам. Наиболее распространены классы A, B и C. Классы D и E существуют, но обычно не используются конечными пользователями. Каждый из классов адресов имеет свою маску подсети по умолчанию. Определить класс IP-адреса можно по его первому октету.

Сети класса A по умолчанию используют маску подсети 255.0.0.0 и имеют значения от 0 до 127 в первом октете. Адрес 10.52.36.11 является адресом класса A. Первым октетом является число 10, входящее в диапазон от 1 до 126 включительно.

Сети класса B по умолчанию используют маску подсети 255.255.0.0 и имеют в первом октете значение от 128 до 191. Адрес 172.16.52.63 является адресом класса B. Первым октетом является число 172, входящее в диапазон от 128 до 191 включительно.

Сети класса C по умолчанию используют маску подсети 255.255.255.0 и имеют в первом октете значение от 192 до 223. Адрес 192.168.123.132 является адресом класса C. В первом октете число 192, которое находится между 192 и 223 включительно.

В некоторых случаях значение маски подсети по умолчанию не соответствует потребностям организации из-за физической топологии сети или потому, что количество сетей (или узлов) не соответствует ограничениям маски подсети по умолчанию. Поэтому можно распределить сети с помощью масок подсети.

TCP/IP-сеть класса A, B или C может быть ещё разбита на подсети системным администратором. Образование подсетей может быть необходимо при согласовании логической структуры адреса Интернета (абстрактный мир IP-адресов и подсетей) с физическими сетями, используемыми в реальном мире.

Системный администратор, выделивший блок IP-адресов, возможно, администрирует сети, организованные не соответствующим для них образом. Например, имеется глобальная сеть с 150 узлами в трёх сетях (в разных городах), соединенных маршрутизатором TCP/IP. У каждой из этих трёх сетей 50 узлов. Выделим для примера сеть класса C 192.168.123.0 (на самом деле этот адрес из серии, не размещенной в глобальной сети). Это значит, что адреса с 192.168.123.1 по 192.168.123.254 можно использовать для этих 150 узлов.

Два адреса, которые нельзя использовать в данном примере, – 192.168.123.0 и 192.168.123.255, так как двоичные адреса с составляющей узла из одних единиц и нолей недопустимы. Адрес с 0 недопустим, поскольку он используется для определения сети без указания узла. Адрес с числом 255 (в двоичном обозначении адрес узла, состоящий из одних единиц) используется для доставки сообщения на каждый узел сети. Следует просто запомнить,

что первый и последний адрес в любой сети и подсети не может быть присвоен отдельному узлу.

Теперь осталось дать IP-адреса 254 узлам. Это несложно, если все 150 компьютеров являются частью одной сети. Однако в данном примере 150 компьютеров работают в трёх отдельных физических сетях. Вместо запроса на большее количество адресных блоков для каждой сети сеть разбивается на подсети, что позволяет использовать один блок адресов в нескольких физических сетях.

В данном случае сеть разбивается на четыре подсети с помощью маски подсети, которая увеличивает адрес сети и уменьшает возможный диапазон адресов узлов. Другими словами, мы «одалживаем» несколько разрядов, обычно используемых для адреса узла, и используем их для составляющей сети в адресе. Маска подсети 255.255.255.192 позволяет создать четыре сети с 62 узлами в каждой. Это возможно, поскольку в двоичном обозначении 255.255.255.192 – то же самое, что и 11111111.11111111.11111111.11000000. Первые две цифры последнего октета становятся адресами сети, поэтому появляются дополнительные сети 00000000 (0), 01000000 (64), 10000000 (128) и 11000000 (192). В этих четырёх сетях последние шесть двоичных цифр IP-адреса можно использовать в качестве адресов узлов. Часто номер 255.255.255.192 используют в качестве маски подсети.

Таким образом, использование маски подсети 255.255.255.192 преобразует сеть 192.168.123.0 в четыре сети: 192.168.123.0, 192.168.123.64, 192.168.123.128 и 192.168.123.192. Эти четыре сети будут иметь следующие действующие адреса узлов: 192.168.123.1-62, 192.168.123.65-126, 192.168.123.129-190, 192.168.123.193-254

Двоичные адреса узлов с одними только единицами и нолями недействительны, поэтому нельзя использовать адреса со следующими десятичными числами в последнем октете: 0, 63, 64, 127, 128, 191, 192 или 255.

Особого внимания требуют два адреса узлов: 192.168.123.71 и 192.168.123.133. Если использовать по умолчанию маску подсети класса C 255.255.255.0, оба адреса будут в сети 192.168.123.0. Однако, если использовать маску подсети 255.255.255.192, они окажутся в разных сетях: 192.168.123.71 – в сети 192.168.123.64, в то время как 192.168.123.133 – в сети 192.168.123.128.

Для того чтобы отправить данные ко всем устройствам в сети, используется широковещательный адрес (Broadcast Address). Широковещательные IP-адреса заканчиваются двоичными единицами во всей хостовой части адреса.

Широковещательный адрес – условный (не присвоенный никакому устройству в сети) адрес, который используется для передачи широковещательных пакетов в компьютерных сетях.

Впервые технология использования широковещательных адресов в IP-сетях была предложена в 1982 году Робертом Гурвицем и Робертом Хинденом.

Различают несколько видов широковещательных адресов.

Например, используется широковещательный MAC-адрес FF:FF:FF:FF:FF:FF для передачи служебных команд.

Используются так же широковещательные адреса, вид которых зависит от протокола. Так, в IP-сетях широковещательные адреса формируются следующим образом: к адресу подсети прибавляется побитовая инверсия маски подсети (то есть все биты адреса подсети, соответствующие нулям в маске, устанавливаются в «1»). Например, если адрес сети равен 192.168.0.0, маска подсети 255.255.255.0, то широковещательный адрес будет 192.168.0.255.

11000000.10101000.00000000.00000000 – адрес сети (192.168.0.0)
00000000.00000000.00000000.11111111 – побитовая инверсия маски (0.0.0.255)
11000000.10101000.00000000.11111111 – широковещательный адрес 192.168.0.255

Различают следующие применения широковещательных адресов.

В локальном сегменте IP-сети используется для передачи широковещательных пакетов всем устройствам. Все устройства в сети должны интерпретировать широковещательный адрес как свой собственный.

В удалённом сегменте IP-сети иногда используется для передачи широковещательных пакетов за пределы локального сегмента сети. Работает аналогично адресу в локальном сегменте IP-сети, пакет маршрутизируется как обычный, пока не попадает на шлюз, подключённый к подсети, в которой адрес получателя является широковещательным.

Не существует адреса, который бы в рамках всего Интернета интерпретировался бы как широковещательный.

Классы сетей можно свести в таблицу:

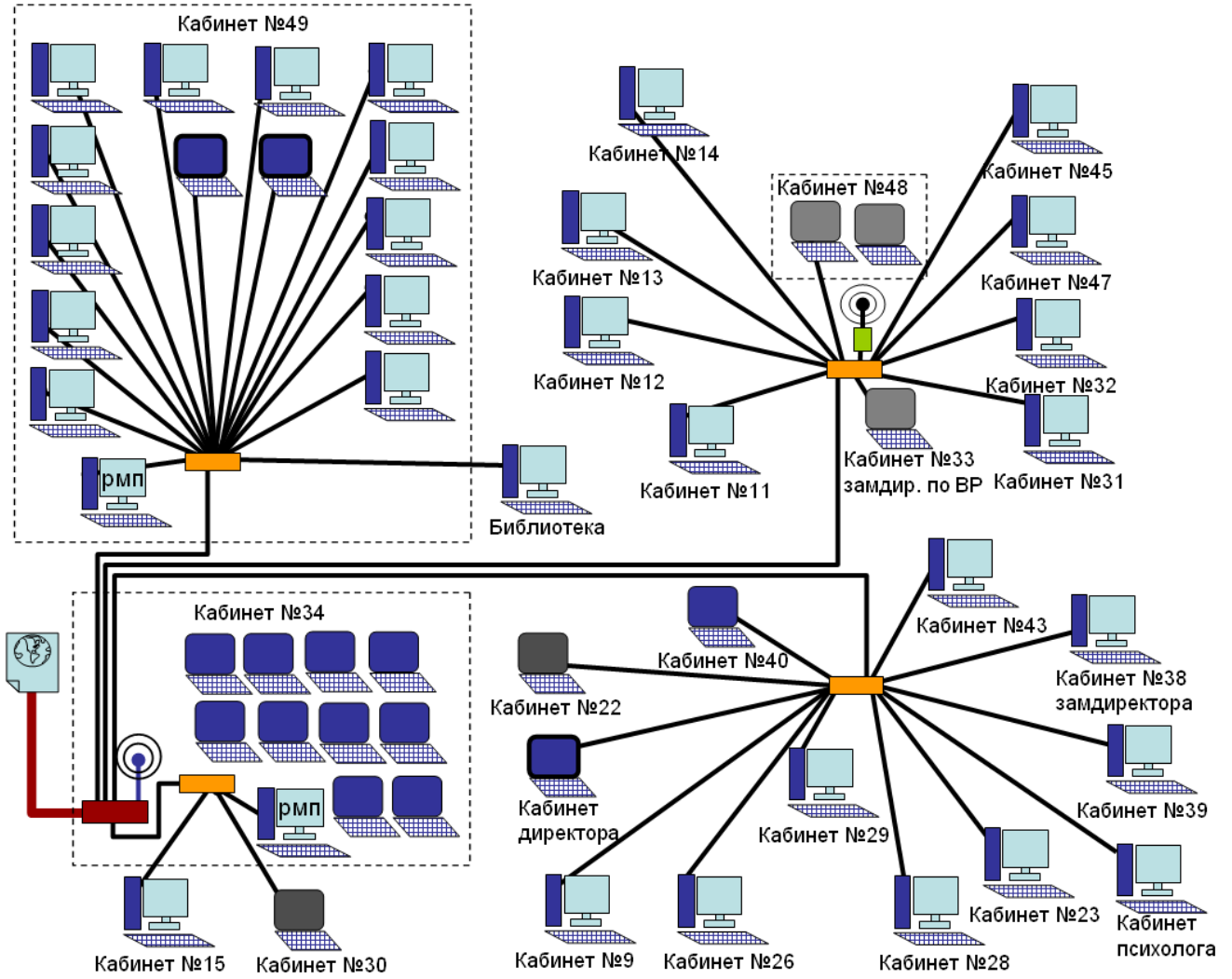
Класс	Первые биты	C – сеть, X – хост	Количество адресов сетей	Количество возможных адресов хостов	Маска сети	Начальный адрес	Конечный адрес
A	0	C.X.X.X	128	16777214	255.0.0.0	1.0.0.0	126.255.255.255
B	10	C.C.X.X	16384	65534	255.255.0.0	128.0.0.0	191.255.255.255
C	110	C.C.C.X	2097152	254	255.255.255.0	192.0.0.0	223.255.255.255
D	1110	Зарезервировано				224.0.0.0	239.255.255.255
E	1111	Зарезервировано				240.0.0.0	247.255.255.255

Таблица масок подсети:

Маска подсети	Двоичная маска	Префикс	Количество адресов
255.255.255.255	11111111.11111111.11111111.11111111	/32	1
255.255.255.254	11111111.11111111.11111111.1111111**0**	/31	2
255.255.255.252	11111111.11111111.11111111.111111**00**	/30	4
255.255.255.248	11111111.11111111.11111111.11111**000**	/29	8
255.255.255.240	11111111.11111111.11111111.1111**0000**	/28	16
255.255.255.224	11111111.11111111.11111111.111**00000**	/27	32
255.255.255.192	11111111.11111111.11111111.11**000000**	/26	64
255.255.255.128	11111111.11111111.11111111.1**0000000**	/25	128
255.255.255.0	11111111.11111111.11111111.**00000000**	/24	256
255.255.254.0	11111111.11111111.1111111**0**.00000000	/23	512
255.255.252.0	11111111.11111111.111111**00**.00000000	/22	1024
255.255.248.0	11111111.11111111.11111**000**.00000000	/21	2048
255.255.240.0	11111111.11111111.1111**0000**.00000000	/20	4096
255.255.224.0	11111111.11111111.111**00000**.00000000	/19	8192
255.255.192.0	11111111.11111111.11**000000**.00000000	/18	16384
255.255.128.0	11111111.11111111.1**0000000**.00000000	/17	32768
255.255.0.0	11111111.11111111.**00000000**.00000000	/16	65536
255.254.0.0	11111111.1111111**0**.00000000.00000000	/15	131072
255.252.0.0	11111111.111111**00**.00000000.00000000	/14	262144
255.248.0.0	11111111.11111**000**.00000000.00000000	/13	524288
255.240.0.0	11111111.1111**0000**.00000000.00000000	/12	1048576
255.224.0.0	11111111.111**00000**.00000000.00000000	/11	2097152
255.192.0.0	11111111.11**000000**.00000000.00000000	/10	4194304
55.128.0.0	11111111.1**0000000**.00000000.00000000	/9	8388608
255.0.0.0	11111111.**00000000**.00000000.00000000	/8	16777216
254.0.0.0	1111111**0**.00000000.00000000.00000000	/7	33554432
252.0.0.0	111111**00**.00000000.00000000.00000000	/6	67108864
248.0.0.0	11111**000**.00000000.00000000.00000000	/5	134217728
240.0.0.0	1111**0000**.00000000.00000000.00000000	/4	268435456
224.0.0.0	111**00000**.00000000.00000000.00000000	/3	536870912
192.0.0.0	11**000000**.00000000.00000000.00000000	/2	1073741824
128.0.0.0	1**0000000**.00000000.00000000.00000000	/1	2147483648

II. Адресное пространство школьной локальной компьютерной сети

Школьная локальная компьютерная сеть является одноранговой и объединяет 52 компьютера. Имеются технические возможности расширения сети. Сеть построена на основе ADSL-модема-роутера с wi-fi DSL-2750U (каб.34), коммутатора Acorp Ethernet Switch 16port (каб.34), коммутатора D-Link DES-1024A (каб.49), коммутатора D-Link DES-1016A (каб.29), коммутатора D-Link DES-1016A (каб.33), wi-fi-точки доступа D-Link DAP-1155 (каб.33). Большая часть компьютеров подключена к сети по электрическому проводу «витая пара», ноутбуки в кабинете 34 и в кабинете 48 включаются в сеть по запароленному каналу wi-fi, зона wi-fi покрывает примерно половину площади школьного здания (вблизи кабинетов 33 и 34).



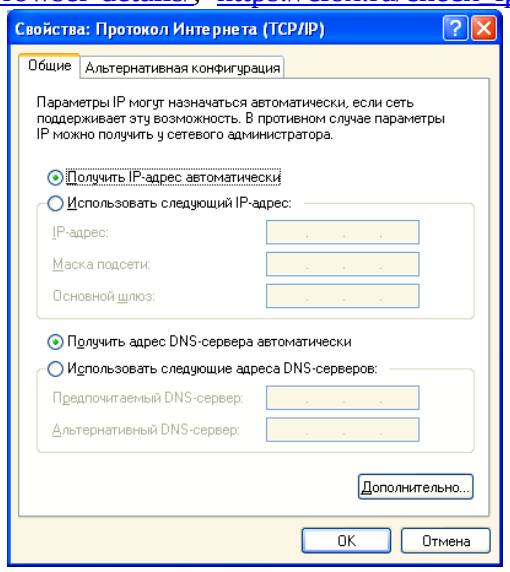
В сети различают локальные (внутренние, серые) и глобальные (внешние, белые, публичные) IP-адреса. В локальной сети внутренний IP-адрес компьютера может назначаться двумя способами:

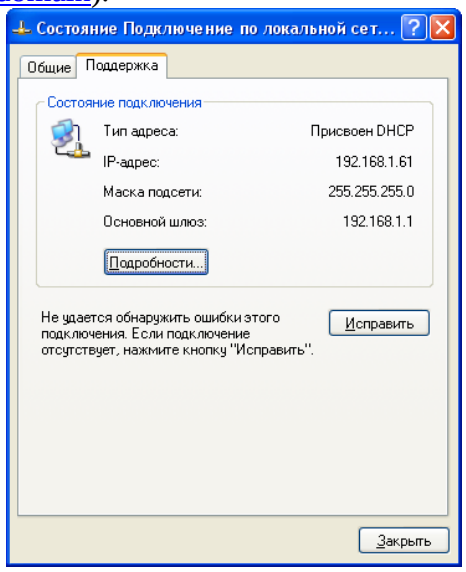
- автоматически Windows, с помощью DHCP (Dynamic Host Configuration Protocol);
- вручную.

Внешний IP-адрес динамически задается провайдером, внутренние IP-адреса узлов в школьной сети устанавливаются автоматически. При этом выбор диапазона адресов зависит от настроек роутера DSL-2750U в кабинете 34. Так, в небольших сетях обычно используют диапазоны адресов 192.168.0.1–192.168.0.254 или 192.168.1.1–192.168.1.254, при которых можно подключать до 254 узлов-клиентов.

Чтобы узнать IP-адрес компьютера можно воспользоваться средствами операционной системы (например, в режиме командной строки командой ipconfig) или на

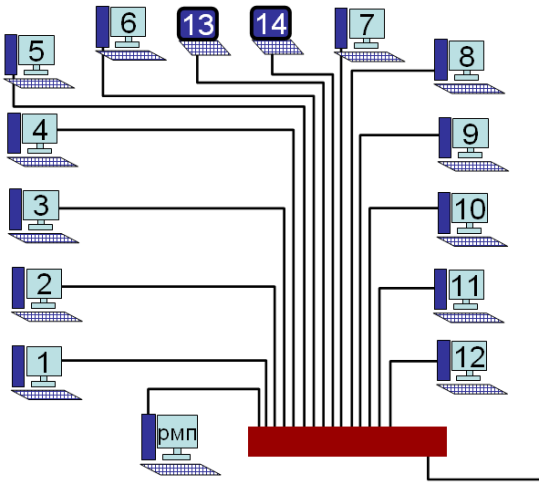
специализированных сайтах (например, https://2ip.ru/, https://whatleaks.com/ru/, https://pr-cy.ru/browser-details/, https://ciox.ru/check_ip_of_domain).





Для подключения локального компьютера к Интернету используется технология NAT (Network Address Translation), которая внедрена на всех современных маршрутизаторах, в том числе реализована на школьном роутере DSL-2750U в кабинете 34. Она преобразует локальный IP-адрес устройства в публичный, т.е. тот, который используется в сети Интернет. Глобальный публичный IP-адрес должен быть уникальным: он статично или динамически (как в школе) присваивается провайдером только одному подключенному к мировой сети узлу.

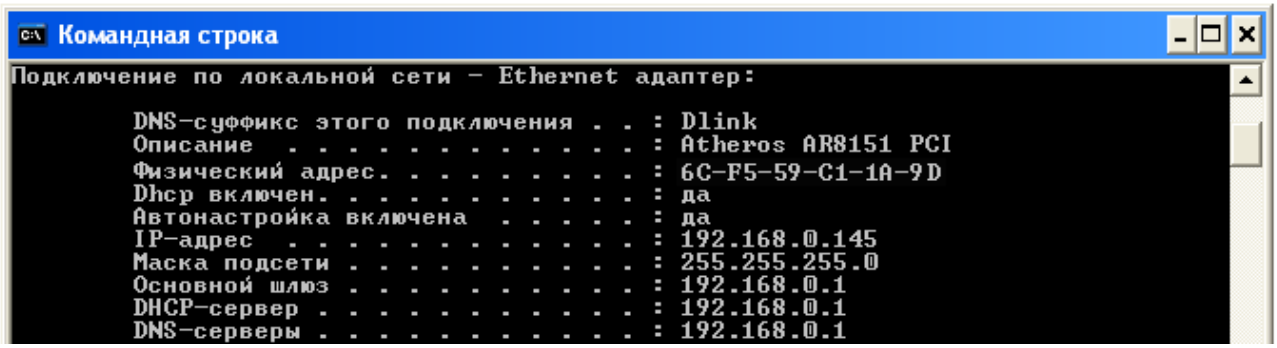
Рассмотрим сегмент локальной сети в школьном кабинете 49.



В этом сегменте 15 компьютеров, объединенные в группу KVT49. Подключение по проводной электрической линии «витая пара». В кабинете помещён коммутатор D-Link DES-1024A 10/100.

Для определения публичного IP-адреса компьютера использован запрос Яндекса.

Для определения MAC-адреса компьютера использована команда ipconfig /all в командной строке. После ввода команды ipconfig /all получаем подробную информацию обо всех подключениях на компьютере.



Для того чтобы узнать MAC-адрес, определяем физический адрес нужного подключения. Используя ipconfig /all нужно быть внимательным, поскольку эта команда выводит информацию сразу обо всех подключениях, у каждого из которых есть свой MAC-адрес. Для того чтобы не запутаться, можно ориентироваться на название сетевой карты, оно указано в поле «Описание».

Рабочее место	MAC-адрес компьютера (сетевой карты)	IP-адрес локальный (на момент исследования)	IP-адрес публичный
РМП	1C:6F:65:57:52:69	192.168.1.61	88.137.129.234
РМУ01	00:14:85:D5:32:60	192.168.1.112	88.137.129.234
РМУ02	00:14:85:D5:21:5F	192.168.1.135	88.137.129.234
РМУ03	00:14:85:D5:32:A6	192.168.1.182	88.137.129.234
РМУ04	00:14:85:D5:1E:61	192.168.1.173	88.137.129.234
РМУ05	00:08:A1:9D:4E:6A	192.168.1.122	88.137.129.234
РМУ06	00:14:85:D5:32:5C	192.168.1.108	88.137.129.234
РМУ07	00:14:85:D5:32:59	192.168.1.106	88.137.129.234
РМУ08	00:14:85:D5:25:C7	192.168.1.33	88.137.129.234
РМУ09	00:14:85:D5:21:60	192.168.1.136	88.137.129.234
РМУ10	00:14:85:D5:21:45	192.168.1.109	88.137.129.234
РМУ11	00:80:48:1A:3B:17	192.168.1.174	88.137.129.234
РМУ12	00:15:58:06:BD:A1	192.168.1.1	88.137.129.234
РМУ13	00:15:C5:66:93:08	192.168.1.71	88.137.129.234
РМУ14	00:15:C5:6B:AF:64	192.168.1.246	88.137.129.234

Проанализировав внутренние IP-адреса легко понять, что в кабинете развернута локальная сеть класса С (т.к. первые двоичные биты 110), которая «видна» из сети класса А как узел с IP-адресом 88.137.129.234.

Перейдём к моделированию.

Существуют два основных подхода к моделированию вычислительных сетей: аналитическое моделирование с использованием элементов теории массового обслуживания и имитационное моделирование. Выбор имитационной модели обусловлен необходимостью детального моделирования протекающих в вычислительной сети процессов, не имеющих эффективного выражения в аналитической форме.

К основным достоинствам имитационного моделирования, положенного в основу исследования, можно отнести возможность детального исследования процессов, протекающих в вычислительных сетях, и представляющих наибольший интерес с точки зрения оптимизации действующих и проектируемых вычислительных сетей. К таким процессам можно отнести: взаимодействие сетевых прикладных программ, работу сетевых протоколов и коммуникационного оборудования. Полученная в результате моделирования информация о функционировании элементов вычислительной сети может быть использована при проведении анализа и решении задачи оптимизации.

Суть моделирования работы ЛВС заключается в построении модели компьютерной сети из набора объектов, представляющих те или иные её элементы и проведения имитационного моделирования процессов обмена информацией между в объектами, моделирующих работу

сетевого программного обеспечения. Построение модели осуществляется путём установления связей между объектами и определением начальных состояний объектов.

Имитация процессов обмена информацией между объектами моделируемой сети осуществляется путём последовательной обработки событий объектами модели. Каждое событие отражает течение тех или иных процессов в элементах моделируемой сети.

Для построения информационной модели воспользуемся программой NetEmul (netemul-1.0, http://netemul.sourceforge.net/).

Программа предоставляет возможность визуализации происходящих в сети процессов связанных с передачей служебной и пользовательской информации.

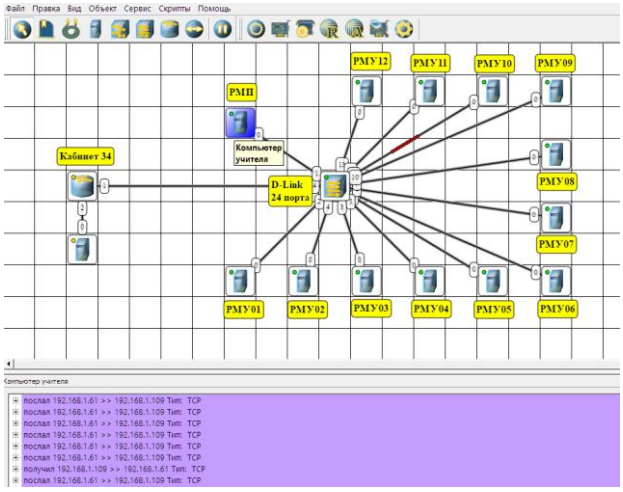
Интерфейс программы интуитивно понятен. Программа NetEmul располагает гибкой системой помощи и лаконичным руководством пользователя, также стандартным подходом в реализации всех пользовательских действий, для поддерживаемых операционных систем.

Кроме визуализации функционирования сети, следует отметить отличную возможность более детального рассмотрения её работы с помощью отображаемой статистики и службы для гибкой трассировки происходящих событий, для каждого сетевого устройства. Как правило, в небольших сетях отсутствуют аппаратные сетевые компоненты, которые могут предоставить пользователю статистику, управление, и вызывать события на различные ситуации работы сети. Таким образом, NetEmul лучшим образом может подходить для использования его в качестве пособия, иллюстрирующего и моделирующего передачу данных в локальных сетях.

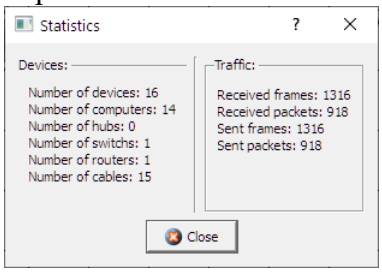
Подготовительная работа заключалась в оформлении модели: нанесение узлов, заполнение таблиц интерфейсов в соответствии с данными, полученными на этапе изучения сегмента школьной локальной сети.

Для настройки IP-адреса интерфейса открываем окно «Интерфейсы». Выставляем IP-адреса и маски подсети в соответствующих строках каждого интерфейса. После нажатия на кнопку «Ок», можем наблюдать, как индикатор поменял цвет с желтого на зеленый и от устройства, которому сейчас дали адрес, побежал кадр ARP-протокола. Это нужно для того, чтобы выявить, нет ли в сети повторения адресов. Если адреса совпали (ситуацию смоделируем специально), то появится информативное сообщение, после которого можно самостоятельно разрешить эту ситуацию для корректной работы сети.

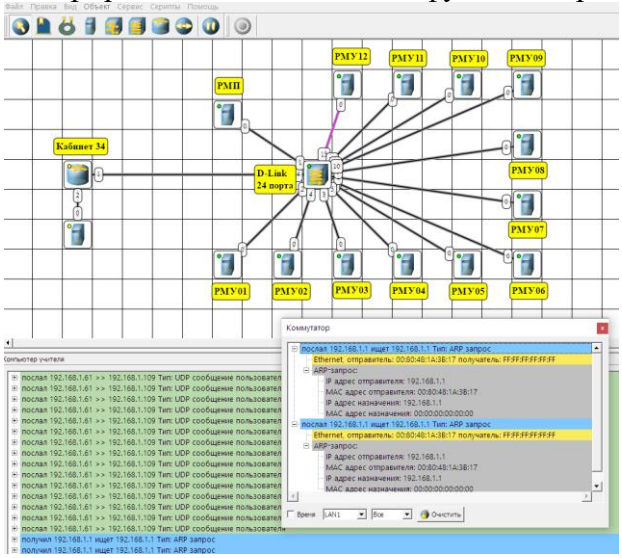
После того, как расставлены все IP-адреса конечным узлам, появляется в принципе работающая подсеть.



Программная оболочка позволяет посмотреть статистику сети в каждый момент времени:

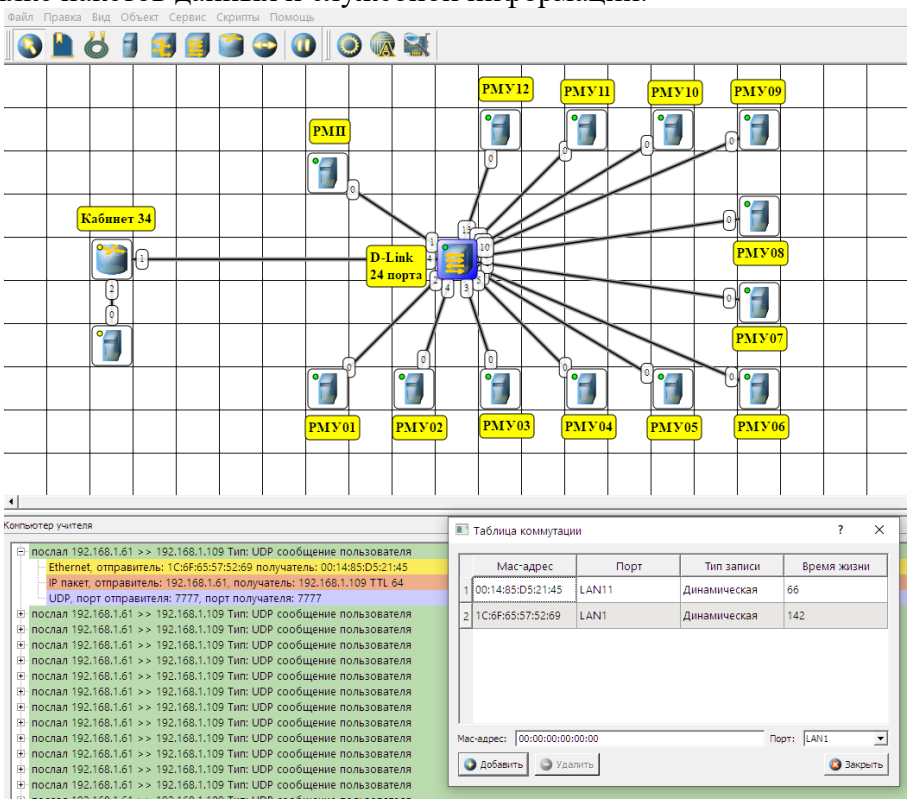


Смоделирована ситуация совпадения IP-адресов двух компьютеров и продемонстрирована невозможность функционирования сети в этом случае.



Изучены принципы функционирования коммутатора.

Особого внимания потребовала таблица коммутации, формируемая коммутатором при пересылке пакетов данных и служебной информации.



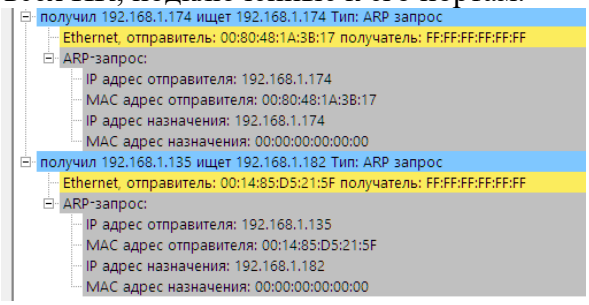
Чтобы понять, как работает коммутатор, смоделирована ситуация отправки данных с РМУ02 на РМУ03.

Таблица коммутации (ТК) описывает, к какому именно порту коммутатора, какие ПК подключены. Применяется алгоритм обратного обучения, чтобы узнать MAC-адреса компьютеров, подключённых к его портам. Алгоритм прозрачного моста применяется после заполнения таблицы коммутации, для передачи данных.

В простом виде таблица коммутации состоит из 4-х столбцов. Столбец №1 это MAC-адрес ПК, 2-ой – это порт коммутатора, 3-ий – тип записи, 4-ый – время жизни.

Имея возможность сбрасывать в модели записи в таблице коммутации, можно проследить алгоритм обратного обучения. Чтобы узнать, как коммутатор узнает MAC-адреса компьютеров, которые подключены к его портам, применяется алгоритм обратного обучения.

Например, есть коммутатор, у него 24 порта. Его только что включили и не знает ничего про ПК, подключенные к нему. Ячейки в таблице коммутации пока пустые, коммутатор принимает все кадры, которые приходят на его порты, и проводит анализ заголовка канального уровня. Из заголовка он извлекает адрес отправителя. Коммутатор определяет, что к порту №3 подключен ПК с таким же MAC-адресом. И, следовательно, записывает этот MAC-адрес в ТК. И так далее, пока вся таблица коммутации не заполнится, а коммутатор не будет знать MAC-адреса всех ПК, подключенные к его портам.



Заключение

В рамках проекта «LAN – это ЛКС» проведено исследование адресации узлов компьютерной сети, подтверждена актуальность темы «Адресация узлов компьютерной сети», потому что компьютерные сети очень востребованы в современном обществе, технике, производстве.

Объектом исследования выступили компьютерные сети, предмет исследования – адресация узлов компьютерных сетей.

Цель работы достигнута: проведён анализ адресного пространства и создана имитационная модель сегмента школьной ЛКС.

Получены ответы на предметные вопросы проекта:

Что является узлом сети? Что является физическим адресом узла сети?

Что является логическим адресом узла сети?

Для каких целей используется адресация в сети?

Для чего используют широковещательный адрес?

Какие технические и программные средства фиксируют адрес узла в сети?

Для чего используют маску подсети?

На разных этапах исследовательской работы были использованы различные методы: изучение и обобщение, анализ информации, сравнение и сопоставление, классификация, моделирование. На этапе моделирования было изучено приложение NetEmul, которое дало возможность построить наглядную имитационную модель сегмента школьной компьютерной сети. Построенная модель дала возможность провести серию экспериментов.

Исследовательская работа имеет существенную практическую значимость, поскольку приобретённые знания позволяют настраивать локальные компьютерные сети, конструировать локальные сети для решения конкретных задач. Полученные в процессе моделирования данные возможно использовать для анализа работы сети при решении задач оптимизации и рационального проектирования локальных вычислительных сетей.

Использованные источники

1. Куроуз Д.Ф., Росс К.В. Компьютерные сети. Настольная книга системного администратора. – М.:Эксмо, 2016.

2. Понятие TCP/IP-адресации и основные сведения о подсетях [Электронный ресурс] − Режим доступа: https://support.microsoft.com/ru-ru/help/164015, свободный. − Загл. с экрана.

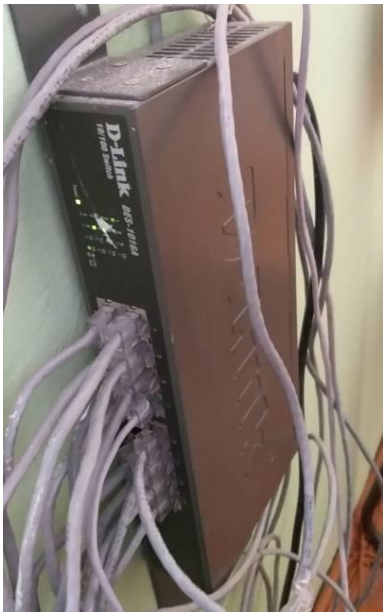
3. Твой Сетевичек: всё о локальных сетях и сетевом оборудовании [Электронный ресурс] − Режим доступа: https://tvoi-setevichok.ru/lokalnaya-set, свободный. − Загл. с экрана.

4. Угринович Н.Д. Информатика и ИКТ. Базовый курс: Учебник для 9 класса / Н.Д.Угринович. – М.: БИНОМ. Лаборатория знаний, 2015.

Приложения


D-Link


D-Link
10/100 Switch
DES-1024A


D-Link


16-Port 10/100M
Nway Switch
acorp


D-Link