Информационная безопасность
Методы защиты информации

Информационная безопасность – это защищенность информации от любых действий, в результате которых информация может быть искажена или утеряна, а пользователям информации нанесен недопустимый ущерб. Информационная безопасность – это процесс, обеспечивающий доступность, целостность и конфиденциальность ин формации. В связи с целями и задачами, которые мы ставим перед собой в виртуальном пространстве, для трех названных аспектов информационной безопасности необходимы различные способы защиты информации.

Защита информации – комплекс мер, направленных на обеспечение информационной безопасности. На практике защита информации объясняется как поддержка целостности, доступности и сохранности информации, которая используется для ввода, сохранения, редактирования и передачи данных. В результате защиты информации должны быть обеспечены следующие условия.

Результат защиты информации

Доступность информации нарушается, когда компьютер выходит из строя или web-сайт не отвечает на запросы пользователей в результате массовой атаки вредоносных программ через Интернет.

Нарушение целостности информации – это кража или искажение информации. Например, изменение содержания писем электронной почты и других цифровых документов. **Конфиденциальность информации** нарушается, когда информация становится известной тем людям, которые не должны ее знать, что может повлечь за собой распространение секретной информации.

Основные угрозы доступности информации

К ним можно отнести внутренний отказ информационной системы и выход поддерживающей инфраструктуры из строя.

К внутренним отказам информационной системы относятся:
• нарушение правил передачи (случайно или намеренно);
• выход системы из строя (чрезмерное количество запросов, редактируемой информации и т.д.);
• вредоносное программное обеспечение;
• выход аппаратного и программного обеспечения из строя;
• повреждение информации.

Основные угрозы целостности информации

Есть два вида угроз целостности информации: статические и динамические. К угрозам статической целостности информации относятся введение неправильной информации и изменение информации. К угрозам динамической целостности информации. Конфиденциальность информации делится на предметную и служебную.

Служебная информация не относится к определенной предметной сфере (например, пароли пользователей). Самая главная угроза, от которой сложно защититься, – это превышение должностных полномочий информации относятся повтор данных, введение дополнительной информации и кража информации.

Методы защиты информации

Обеспечение и поддержка информационной безопасности включают комплекс технических, программных и организационных мер.

К техническим мерам защиты информации можно отнести системы видеонаблюдения и сигнализации, а также другие средства предотвращения и блокировки всех возможных способов распространения информации.

Программные меры защиты информации обеспечивают возможность установки паролей на доступ к определенным данным, шифрование текста, временное удаление файлов и защиту от вредоносных программ.

К организационным мерам защиты информации относятся политика безопасности организаций и такое расположение каналов связи, которое затруднило бы доступ к ним. Главная опасность, которую могут нанести вредоносные программы – уничтожение информации или уничтожение ключа доступа к секретной информации. Чтобы это предотвратить, необходимо создать резервные копии важной информации. Если не предпринять мер резервного копирования, то можно потерять важные файлы без возможности их восстановления. Создать резервную копию несложно: для этого есть множество способов.

Создание резервных копий на внешнем накопителе

С помощью внешнего накопителя USB можно создать резервную копию сразу на этом устройстве, используя комбинированные функции резервного копирования. Для Windows 8 и 10 применяется функция История файлов (File History). В ОС Windows 7 используется Резервное копирование Windows, а в Mac-устройствах – функция Time Machine. Для этого нужно активировать функцию резервного копирования и часто подключать внешний накопитель к компьютеру.

Преимущества: большая скорость.

Недостатки: если внешний накопитель потеряется либо повредится, то уничтожится и вся скопированная информация.

Если вы хотите быть уверены в безопасности своих файлов, то можете сделать резервное копирование с помощью таких серверов, как Backblaze, Carbonite и Mozy. Эти программы автоматически создают копии файлов в фоновом режиме. Если ваши файлы исчезнут, их можно восстановить в любое время.

Использование таких сервисов, как Dropbox, Google Диск, Microsoft OneDrive, эффективнее использования внешних накопителей. Если возникнет какая-либо проблема, копии файлов сохранятся в облачном хранилище.

Еще одна мера защиты информации – **шифрование**, то есть специальное кодирование. Шифрование применяют при перемещении секретной информации через незащищенные каналы связи. Шифровать можно тексты, фотографии, аудиофайлы, базы данных и любую другую информацию. Методами шифрования и расшифровки данных занимается наука с 4-тысячелетней историей – криптография. Она состоит из двух разделов: криптографии и криптоанализа. **Криптография** – наука о методах шифрования информации.

Криптоанализ – наука о методах и способах расшифровки зашифрованной информации.

Ключ – параметр алгоритма шифрования. Зная ключ, можно скрыть и открыть сообщение. Все системы шифрования делятся на две группы: симметричные и асимметричные. То, что шифр симметричный, означает, что при зашифровке и расшифровке сообщения используется один и тот же ключ. При асимметричном шифровании два ключа связаны между собой. Открытый ключ доступен для всех, кто хочет отправить вам сообщение. Второй ключ – закрытый – хранится в секрете и известен только вам.

Криптографическая стойкость шифра – способность криптографического алгоритма противостоять попыткам его расшифровать. Стойкость алгоритма – стойким считается алгоритм, требующий проделать множество вычислений большого объема для его расшифровки, при этом после расшифровки скрытая информация теряет свою актуальность.

Методы идентификации личности

Существует 2 ступени входа в систему и ввода личных данных: идентификация и аутентификация.

Идентификация – это ввод личных данных пользователя, известных только ему.

Аутентификация – прием и проверка сервером личных данных пользователя. Иногда вместо указанного способа используется и простое регистрационное слово. Процесс регистрации прост. Форму регистрации можно просмотреть в любой социальной сети.

- Регистрация – пользователь вводит адрес электронной почты, номер телефона и пароль. Эти данные не должны повторяться в системе, поэтому для одного лица регистрация более одного аккаунта не допускается.
- Идентификация – ввод данных, указанных при регистрации, в данном случае это электронная почта или номер телефона.
- Аутентификация – после нажатия на кнопку «Вход» страница связывается с сервером, идет проверка наличия и правильности введенных логина или пароля. Если все верно, откроется страница социальной сети.

Существует несколько видов идентификации пользователя, которые отличаются друг от друга уровнем защиты и областью применения.

Защита с помощью пароля. Пользователь знает ключ, или пароль, который известен только ему. Сюда можно отнести и идентификацию через смс-уведомления. При вводе имени и пароля пользователя сервер сравнивает введенные данные с сохраненными данными. В случае полной идентичности введенных данных появляется возможность войти в систему. Различают два вида паролей: динамические и постоянные. **Постоянные** пароли изменяются только по требованию пользователя, а **динамические** – по определенным параметрам. Например, если пользователь забудет пароль, сервер может предложить ему динамический пароль для входа в систему. В работе некоторых фирм или организаций используется **метод проверки с помощью специальных предметов:** карточек, специальных браслетов, флеш-накопителей. При взаимодействии этих устройств с системой сервер проверяет их и либо пропускает, либо останавливает пользователя.

Биометрическая проверка включает в себя методы сканирования отпечатков пальцев, радужной оболочки глаза, формы лица и др. Современные средства могут различать даже мимику лица человека. Это одна из самых надежных, но дорогих систем безопасности.

Использование конфиденциальной информации.

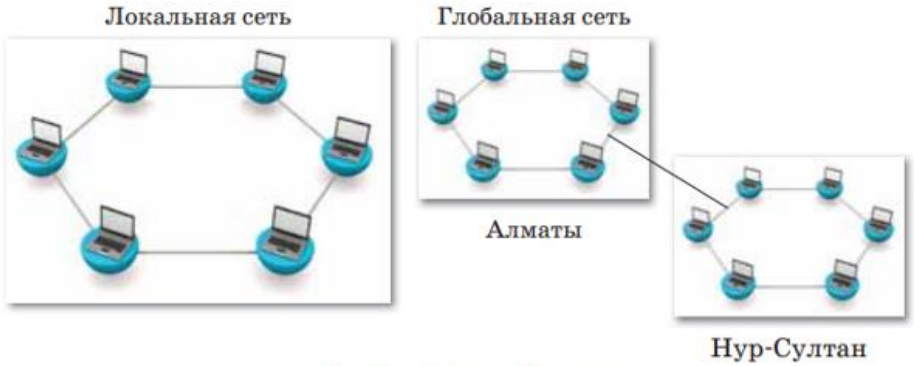
Этот способ чаще всего применяется для защиты программного обеспечения. При его использовании проверяется кэш браузера, установленного на персональном компьютере, места расположения и другие параметры. Знание о понятиях регистрации, идентификации и аутентификации дает возможность правильно применять их по назначению. А это, в свою очередь, способствует сохранению безопасности всех интернет-пользователей.

Принципы работы компьютерных сетей

1. Компьютерные сети
2. IP-адреса
3. Домен. Частные виртуальные сети
4. Пример расчета количества хостов и подсетей на основе IP-адреса и маски

Компьютерная сеть – это совокупность компьютеров, объединенных каналами связи и обеспеченных коммуникационным оборудованием и программным обеспечением для совместного использования данных и оборудования. Важной характеристикой любой компьютерной сети является широта территории, которую она охватывает. Широта охвата определятся взаимной удаленностью компьютеров, составляющих сеть и, следовательно, влияет на технологические решения, выбираемые при построении сети.

Классически выделяются два типа сетей: локальные и глобальные.



Локальная и глобальная сети

К локальным сетям (Local Area Network, LAN) обычно относят сети, компьютеры которых сосредоточены на относительно небольших территориях (как правило, в радиусе до 1–2 км). Классическим примером локальной сети является сеть одного предприятия, расположенного в одном или нескольких рядом стоящих зданиях. Глобальные сети (Wide Area Network, WAN) – это сети, предназначенные для объединения отдельных компьютеров и локальных сетей, расположенных на значительном удалении (сотни и тысячи километров) друг от друга.

Независимо от используемых на каждом компьютере приложений, все машины сети делятся на два класса – серверы и рабочие станции. Сервером называют компьютер, предоставляющий свои ресурсы (например, диски) другим компьютерам сети, т.е. серверы предоставляют свои ресурсы рабочим станциям. Рабочая станция, или клиент, использует ресурсы сервера. Рабочие станции имеют доступ к сетевым ресурсам, но своих ресурсов в общее пользование не предоставляют.

Основные аппаратными компоненты:

• Абонентские системы (компьютеры (рабочие станции, или клиенты, и серверы), принтеры, сканеры и др.).
• Сетевое оборудование (сетевые адаптеры, концентраторы, мосты, маршрутизаторы и др.).

• Коммуникационные каналы (кабели, разъемы, устройства передачи и приема данных в беспроводных технологиях). Основные программные компоненты:
• сетевые операционные системы – Windows NT, WindowsNT Server, Windows for Workgroups, LANtastic, NetWare, Unix, Linux и др.
• сетевые программные обеспечения – клиент сети, сетевые адаптеры, протоколы, служба дистанционного доступа.
Сетевые компоненты компьютерных сетей являются основными составляющими сети. Каждый из них важен и выполняет разные функции для оптимизации связи между компьютерами сети.


Маршрутизатор, коммутатор, концентратор

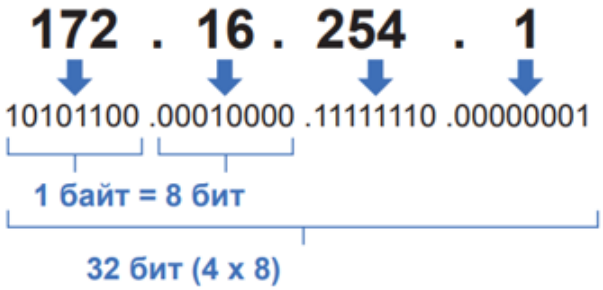
В отличие от коммутаторов и маршрутизаторов, концентраторы (hub) – самые дешевые и простые устройства сети. С помощью концентраторов осуществляется обмен данными между компьютерами сети. Все данные, которые поступают в один порт концентратора, пересылаются на все другие порты. Следовательно, все компьютеры, подсоединенные к одному концентратору, «видят» друг друга в сети. Работа коммутатора (switch) во многом схожа с функционированием концентратора, но он делает ее более эффективно. Каждый пакет данных (фрагмент Ethernet), передаваемый в сети, имеет MAC-адреса источника и адресата. Коммутатор способен «запоминать» адрес каждого компьютера, подключенного к его портам, и действовать как регулировщик – передавать данные только на компьютер адресата и ни на какие другие.

Маршрутизатор (router) – интеллектуальное («умное») устройство, связывающее две или более сети для доставки пакетов. По сравнению с коммутаторами, маршрутизаторы медленны и относительно дорогостоящи. Они выполняют такие функции, как быстрое определение изменений в сети и проверка содержимого сообщений, причем правила доставки могут изменяться в зависимости от содержания сообщений.

Принципы работы компьютерных сетей. IP-адрес

IP-адрес (англ. Internet Protocol Address) – уникальный сетевой адрес, необходимый для нахождения, получения и передачи информации от одного узла к другому.

Под узлом понимается любое устройство (мобильный телефон, компьютер, принтер, концентратор, коммутатор, маршрутизатор и т.п.), имеющее доступ к сети. IP-адрес присваивается устройству вне зависимости от величины сети, к которой он подключен – это может быть как глобальный доступ в Интернет, так и локальная сеть, состоящая из нескольких устройств.



Пример IP-адреса

Октет – каждый разряд IP-адреса, состоящий из 1 байта. IP-адрес может быть представлен в формате IPv4 или IPv6. IPv4 – интернет-протокол, использующий 32-битные адреса.

Пример такого IP-адреса: 123.45.67.89. Главная проблема этого протокола – ограниченность возможных адресов. Несмотря на то, что их более четырех миллиардов (4 294 967 296), этого не хватает для всех устройств, выходящих в сеть.

В 1996 году была представлена шестая версия IP-протокола, которая должна была решить проблемы предыдущей, четвертой, версии. Длина адреса, используемая в IPv6, составляет уже 128 бит. Пример такого IP-адреса: 21DA:00D3: 0000:2F3B:02AA: 00FF:FE28:9C5A.

Существует два вида IP-адресов:

1. Внутренние IP-адреса (частный, локальный, «серый»).

2. Внешние IP-адреса (публичный, глобальный, «белый»). Внутренние (частные) IP-адреса не используются в сети Интернет. К внутренним относятся адреса, используемые в локальных сетях. Доступ к внутреннему IP-адресу можно получить лишь в пределах локальной подсети.

К частным относятся IP-адреса, значения которых лежат в следующих диапазонах:

• 10.0.0.0 – 10.255.255.255

• 172.16.0.0 – 172.31.255.255

• 192.168.0.0 – 192.168.255.255

IP-адреса присваиваются провайдерами.

Провайдер (от англ. internet service provider, сокр. ISP – поставщик интернет-услуг) – компания, которая предоставляет возможность доступа к сети Интернет и другие связанные с Интернетом услуги. Внешние (публичные) IP-адреса используются в сети Интернет. Публичным IP-адресом называется IP-адрес, под которым вас видят устройства в Интернете, и он является уникальным во всей сети Интернет. Доступ к устройству с публичным IP-адресом можно получить из любой точки глобальной сети. К примеру, IP-адреса компьютеров, присоединенных к сети класса, – внутренние, а IP-адрес сетевого компонента, который дает этим компьютерам доступ в Интернет – внешний, т.е. он присваивается для передачи запросов компьютеров серверу.

IP-адреса также бывают статическими и динамическими.

Статический (постоянный, неизменный) IP-адрес задается в настройках устройства либо назначается провайдером. Он не может быть присвоен другому устройству и не меняется с течением времени. **Динамический** (непостоянный, изменяемый) также назначается провайдером, однако только на ограниченный срок.

У компьютеров сети кроме IP-адресов также имеется **маска**, которая необходима для определения границ (диапазона) подсети, т.е. определяет, какая часть IP-адреса сетевого узла относится к адресу самой сети, а какая часть – к адресу узла в этой сети. Таким образом, маска подсети отделяет адрес подсети от адреса конечного устройства, которое находится в этой сети.

К примеру, 192.168.11.10/21:

11000000.10101000.00001011.0000101011111111.11111111.11111000.00000000

11000000.10101000.00001000.00000000 = 192.168.8.0

Адрес 192.168.8.0, полученный в результате логического умножения, называется адресом подсети.

По формуле Хартли можно вычислить общее количество информации, которое находится в сообщении общей длиной N.

Решение: Количество информации в интернет-адресе I = 32 бит, тогда N – общее количество интернет-адресов: $N = 2^i = 232 = 4\ 294\ 967\ 296$. Вывод: 32-разрядный интернет-адрес позволит подключить более 4 миллиардов компьютеров к Интернету.

Домен. Частные виртуальные сети

Компьютерные сети и информационная безопасность

Домен – символьное имя, разделенное точкой. Система доменных имен является иерархической структурой: домены верхнего уровня – домены второго уровня – домены третьего уровня. Домены верхнего уровня бывают двух типов: географические и административные. Каждой стране мира присвоен свой географический домен с двухбуквенным кодированием, например: kz – Казахстан, ru – Россия, uk – Великобритания, fr – Франция.

Обычно домен определяет страну, в которой находится компьютер, который, следовательно, является частью национальной сети. Национальный домен верхнего уровня для Казахстана.kz впервые был зарегистрирован 19 сентября 1994 года. Административные домены отмечаются тремя или более буквами. Каждая компания использует их для регистрации своих доменов второго уровня. Например, сайт компании Microsoft зарегистрирован в домене административного верхнего уровня, как .com.

Доменное имя интернет-сервера состоит (справа налево) из имени домена верхнего уровня, имени домена второго уровня и имени самого компьютера. Например, имя основного сервера компании Microsoft – www.microsoft.com, а имя сервера института – iit.metodist.ru.

Каждый компьютер, подключенный к Интернету имеет интернет-адрес, но может не иметь своего доменного имени. Обычно его не имеют компьютеры, подключенные к Интернету через телефонную линию.

Протокол – стандарт для предоставления, модификации и передачи информации в компьютерной сети. Другими словами, протокол – это определенный сетевой язык. Когда разные глобальные сети работали автономно, они «разговаривали на разных языках». Чтобы их объединить, было необходимо разработать общий сетевой язык. Таким языком стал протокол TCP/IP.

Термин TCP/IP состоит из двух протоколов:

• TCP (Transmission Control Protocol) – транспортный протокол;

• IP (Internet Protocol) – протокол маршрутизации.

На основе протокола TCP/IP были реализованы другие прикладные интернет-протоколы, которые являются основой сервиса сетей. Этот протокол поддерживает программные и аппаратные устройства сетей.

Он стандартизирует следующие процессы:

• разделение данных на пакеты (части);

• адресацию пакетов и их доставку в пункт назначения по указанным маршрутам;

• сбор пакетов в исходный тип данных.

Частная виртуальная сеть (VPN – Virtual Private Network) – это технология, позволяющая создать защищенную (закрытую от внешнего доступа) связь логической сети поверх частной или публичной при наличии высокоскоростного Интернета.

Частная виртуальная сеть

Доступ в Интернет. Чаще всего применяется провайдерами городских сетей, но этот способ также весьма распространен и в сетях предприятий. Основным достоинством использования VPN является более высокий уровень безопасности, так как доступ в локальную сеть и Интернет осуществляется через две разные сети, что позволяет задать для них разные уровни безопасности. При классическом решении – раздача Интернета в корпоративной сети – выдержать разные уровни безопасности для локального и интернет-трафика практически не представляется возможным.

Доступ в корпоративную сеть извне (а также объединение сетей филиалов в единую сеть). Это то, для чего и задумывался VPN: организация безопасной работы в единой

корпоративной сети для клиентов, находящихся вне предприятия. Широко используется для объединения территориально удаленных друг от друга подразделений, обеспечения доступа в сеть для сотрудников, находящихся в командировке или на отдыхе, дает возможность работать из дома.

Объединение сегментов корпоративной сети. Зачастую сеть предприятия состоит из нескольких сегментов с различными уровнями безопасности и доверия. В этом случае для взаимодействия между сегментами можно использовать VPN, ведь это гораздо более безопасное решение, нежели простое объединение сетей.

Пример расчета количества хостов и подсетей на основе IP-адреса и маски

IP-адреса используются для идентификации устройств в сети. Для взаимодействия с другими устройствами по сети IP-адрес должен быть назначен каждому сетевому устройству (в том числе компьютерам, серверам, маршрутизаторам, принтерам и т.д.). Такие устройства в сети называют хостами.
С помощью маски подсети определяется максимально возможное число хостов в конкретной сети. Помимо этого, маски подсети позволяют разделить одну сеть на несколько подсетей.

Знакомство с IP-адресами

Одна часть IP-адреса представляет собой номер сети, другая – идентификатор хоста. Точно так же, как у разных домов на одной улице в адресе присутствует одно и то же название улицы, у хостов в сети в адресе имеется общий номер сети. И точно так же, как у различных домов имеется собственный номер дома, у каждого хоста в сети имеется собственный уникальный идентификационный номер – идентификатор хоста. Номер сети используется маршрутизаторами (роутерами, интернет-центрами) для передачи пакетов в нужные сети, тогда как идентификатор хоста определяет конкретное устройство в этой сети, которому должны быть доставлены пакеты.

Структура

IP-адрес состоит из четырех частей, записанных в виде десятичных чисел с точками (например, 192.168.1.1). Каждую из этих четырех частей называют октетом. Октет представляет собой восемь двоичных цифр (например, 11000000, или 192 в десятичном виде).
Таким образом, каждый октет может принимать в двоичном виде значения от 00000000 до 11111111, или от 0 до 255 в десятичном виде.
На следующем рисунке показан пример IP-адреса, в котором первые три октета (192.168.1) представляют собой номер сети, а четвертый октет (16) – идентификатор хоста.

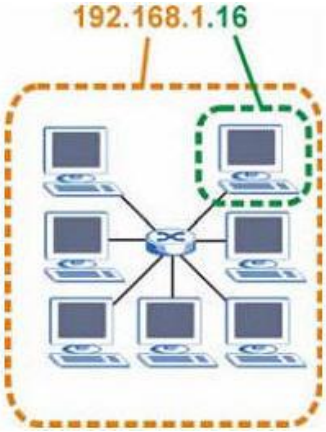


Рисунок 1. Номер сети и идентификатор хоста

Количество двоичных цифр в IP-адресе, которые приходятся на номер сети, и количество цифр в адресе, приходящееся на идентификатор хоста, могут быть различными в зависимости от маски подсети.

Частные IP-адреса

У каждого хоста в сети Интернет должен быть уникальный адрес. Если ваши сети изолированы от Интернета (например, связывают два филиала), для хостов без проблем можно использовать любые IP-адреса. Однако, уполномоченной организацией по распределению нумерации в сети Интернет (IANA) специально для частных сетей зарезервированы следующие три блока IP-адресов:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

IP-адреса указанных частный подсетей иногда называют "серыми". IP-адреса можно получить через IANA, у своего провайдера услуг Интернет или самостоятельно назначить из диапазона адресов для частных сетей.

Маски подсети

Маска подсети используется для определения того, какие биты являются частью номера сети, а какие – частью идентификатора хоста (для этого применяется логическая операция конъюнкции – "И").
Маска подсети включает в себя 32 бита. Если бит в маске подсети равен "1", то соответствующий бит IP-адреса является частью номера сети. Если бит в маске подсети равен "0", то соответствующий бит IP-адреса является частью идентификатора хоста.

Таблица 1. Пример выделения номера сети и идентификатора хоста в IP-адресе

	1-ый октет: (192)	**2-ой октет: (168)**	**3-ий октет: (1)**	**4-ый октет: (2)**
IP-адрес (двоичный)	11000000	10101000	00000001	00000010
Маска подсети (двоичная)	**11111111**	**11111111**	**11111111**	00000000

Номер сети	**11000000**	**10101000**	**00000001**	
Идентификатор хоста				00000010

Маски подсети всегда состоят из серии последовательных единиц, начиная с самого левого бита маски, за которой следует серия последовательных нулей, составляющих в общей сложности 32 бита.

Маску подсети можно определить как количество бит в адресе, представляющих номер сети (количество бит со значением "1"). Например, "8-битной маской" называют маску, в которой 8 бит – единичные, а остальные 24 бита – нулевые. Маски подсети записываются в формате десятичных чисел с точками, как и IP-адреса. В следующих примерах показаны двоичная и десятичная запись 8-битной, 16-битной, 24-битной и 29-битной масок подсети.

Таблица 2. Маски подсети

	Двоичная 1-ый октет:	**Двоичная 2-ой октет:**	**Двоичная 3-ий октет:**	**Двоичная 4-ый октет:**	**Десятичная**
8-битная маска	11111111	00000000	00000000	00000000	255.0.0.0
16-битная маска	11111111	11111111	00000000	00000000	255.255.0.0
24-битная маска	11111111	11111111	11111111	00000000	255.255.255.0
29-битная маска	11111111	11111111	11111111	11111000	255.255.255.248

Размер сети

Количество разрядов в номере сети определяет максимальное количество хостов, которые могут находиться в такой сети. Чем больше бит в номере сети, тем меньше бит остается на идентификатор хоста в адресе.
IP-адрес с идентификатором хоста из всех нулей представляет собой IP-адрес сети (192.168.1.0 с 24-битной маской подсети, например). IP-адрес с идентификатором хоста из всех единиц представляет собой широковещательный адрес данной сети (192.168.1.255 с 24-битной маской подсети, например).
Так как такие два IP-адреса не могут использоваться в качестве идентификаторов отдельных хостов, максимально возможное количество хостов в сети вычисляется следующим образом:

Таблица 3. Максимально возможное число хостов

Маска подсети		**Размер идентификатора хоста**		**Максимальное количество хостов**
8 бит	255.0.0.0	24 бит	$2^{24} – 2$	16777214
16 бит	255.255.0.0	16 бит	$2^{16} – 2$	65534
24 бит	255.255.255.0	8 бит	$2^{8} – 2$	254
29 бит	255.255.255.248	3 бит	$2^{3} – 2$	6

Формат записи

Поскольку маска всегда является последовательностью единиц слева, дополняемой серией нулей до 32 бит, можно просто указывать количество единиц, а не записывать значение каждого октета. Обычно это записывается как "/" после адреса и количество единичных бит в маске.

Например, адрес 192.1.1.0 /25 представляет собой адрес 192.1.1.0 с маской 255.255.255.128. Некоторые возможные маски подсети в обоих форматах показаны в следующей таблице.

Таблица 4. Альтернативный формат записи маски подсети

Маска подсети	**Альтернативный формат записи**	**Последний октет (в двоичном виде)**	**Последний октет (в десятичном виде)**
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248

255.255.255.252	/30	1111 1100	252

Формирование подсетей

С помощью подсетей одну сеть можно разделить на несколько. В приведенном ниже примере администратор сети создает две подсети, чтобы изолировать группу серверов от остальных устройств в целях безопасности.
В этом примере сеть компании имеет адрес 192.168.1.0. Первые три октета адреса (192.168.1) представляют собой номер сети, а оставшийся октет – идентификатор хоста, что позволяет использовать в сети максимум $2^8 – 2 = 254$ хостов.
Сеть компании до ее деления на подсети показана на следующем рисунке.

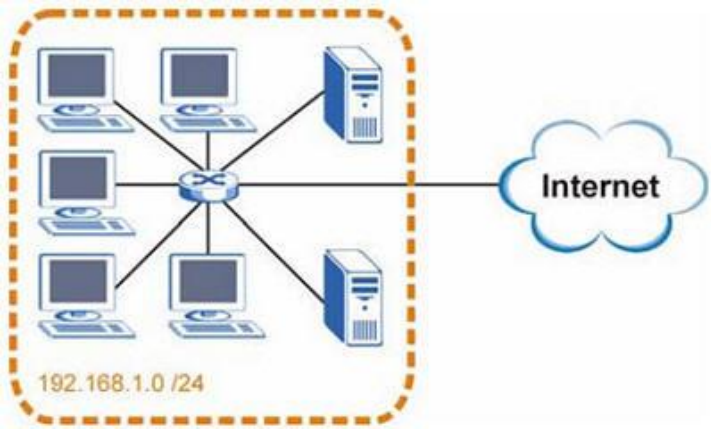
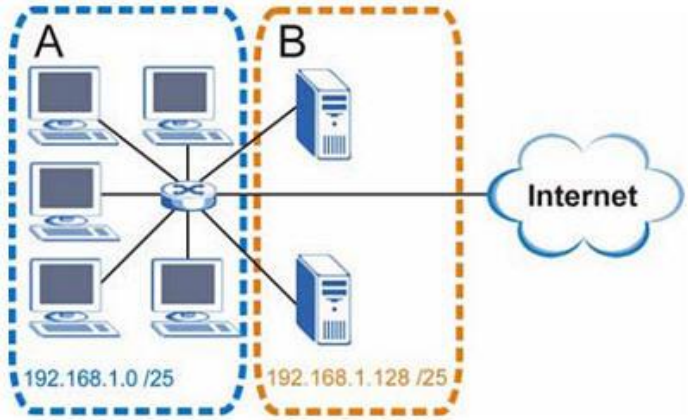


Рисунок 2. Пример формирования подсетей: до разделения на подсети

Чтобы разделить сеть 192.168.1.0 на две отдельные подсети, можно "позаимствовать" один бит из идентификатора хоста. В этом случае маска подсети станет 25-битной (255.255.255.128 или /25).

"Одолженный" бит идентификатора хоста может быть либо нулем, либо единицей, что дает нам две подсети: 192.168.1.0 /25 и 192.168.1.128 /25.
Сеть компании после ее деления на подсети показана на следующем рисунке. Теперь она включает в себя две подсети, **A** и **B**.



>Рисунок 3. Пример формирования подсетей: после деления на подсети

В 25-битной подсети на идентификатор хоста выделяется 7 бит, поэтому в каждой подсети может быть максимум $2^7 – 2 = 126$ хостов (идентификатор хоста из всех нулей – это сама подсеть, а из всех единиц – широковещательный адрес для подсети). Адрес 192.168.1.0 с маской 255.255.255.128 является адресом подсети **A**, а 192.168.1.127 с маской 255.255.255.128 является ее широковещательным адресом. Таким образом, наименьший IP-адрес, который может быть закреплен за действительным хостом в подсети **A** – это 192.168.1.1, а наибольший – 192.168.1.126.
Аналогичным образом диапазон идентификаторов хоста для подсети **B** составляет от 192.168.1.129 до 192.168.1.254.