УДК: 004.9

ОСНОВНЫЕ ПРОТОКОЛЫ ДЛЯ ФУНКЦИОНИРОВАНИЯ ЛОКАЛЬНЫХ СЕТЕЙ.

Симонова Е.С[1]. Золотухин М.С[1].

[1]Брянский государственный университет им. академика И.Г. Петровского Брянск, Россия.

Рассматривается понятие локальной и глобальной сети. Также выделены ключевые протоколы для успешного функционирования локальных сетей. Рассмотрены протоколы Nat, DHCP, RIP, DNS, их работа, преимущества и недостатки.

Ключевые слова: локальные сети, nat, dhcp, dns, vlan.

THE MAIN PROTOCOLS FOR THE FUNCTIONING OF THE LOCAL NETWORK

Simonova E. S[1]. Zolotukhin M.S.[1]

[1]Bryansk State University named after Academician Ivan Georgiyevich Petrovsky Bryansk, Russia.

The concept of local and global networks is considered. Key protocols for the successful functioning of local networks are also highlighted. The protocols Nat, DHCP, RIP, DNS, their work, advantages and disadvantages are considered.

Keywords: local networks, nat, dhcp, dns, vlan.

В начале XX века социолог Георг Герберт Мид (George Herbert Mead), изучая влияние языка на людей, пришел к выводу о том, что человеческий интеллект в первую очередь развился благодаря языку. Язык помогает нам находить смысл в окружающей реальности и истолковывать ее детали. В сетях аналогичную роль выполняют сетевые протоколы, которые позволяют разнообразным системам находить общую среду для взаимодействия.

Понятие локальной сети. **Сеть —** группа компьютеров, соединенных друг с другом, с помощью специального оборудования, обеспечивающего обмен информацией между ними. Соединение между двумя компьютерами может быть непосредственным (*двухточечное соединение*) или с использованием дополнительных узлов связи.

Существует несколько типов сетей, и локальная сеть — лишь одна из них. Локальная сеть представляет собой, по сути, сеть, используемую в одном здании или отдельном помещении, таком как квартира, для обеспечения взаимодействия используемых в них компьютеров и программ. Локальные сети, расположенные в разных зданиях, могут быть соединены между собой с помощью спутниковых каналов связи или волоконно-оптических сетей, что позволяет создать глобальную сеть, т.е. сеть, включающую в себя несколько локальных сетей.

Интернет является еще одним примером сети, которая уже давно стала всемирной и всеобъемлющей, включающей в себя сотни тысяч различных сетей и сотни миллионов компьютеров. Независимо от того, как вы получаете доступ к Интернету, с помощью модема, локального или глобального соединения, каждый пользователь Интернета является фактически сетевым пользователем. Для работы в Интернете используются самые разнообразные программы, такие как обозреватели Интернета, клиенты FTP, программы для работы с электронной почтой и многие другие.

Компьютер, который подключен к сети, называется рабочей станцией (*Workstation*). Как правило, с этим компьютером работает человек. В сети присутствуют и такие компьютеры, на которых никто не работает. Они используются в качестве управляющих центров в сети и как накопители информации. Такие компьютеры называют серверами, Если компьютеры расположены сравнительно недалеко друг от друга и соединены с помощью высокоскоростных сетевых адаптеров то такие сети называются локальными. При использовании локальной сети компьютеры, как правило, расположены в пределах одной комнаты, здания или в нескольких близко расположенных домах.
Для объединения компьютеров или целых локальных сетей, которые расположены на значительном расстоянии друг от друга, используются модемы, а также выделенные, или спутниковые каналы связи. Такие сети носят название глобальные. Обычно скорость передачи данных в таких сетях значительно ниже, чем в локальных. Кроме оборудования, для успешного функционирования локальной сети необходимы протоколы.

В основном протоколы локальных сетей имеют такие же свойства, как и другие коммуникационные протоколы, однако некоторые из них были разработаны давно, при создании первых сетей, которые работали медленно, были ненадежными и более подверженными электромагнитным и радиопомехам. Поэтому для современных коммуникаций некоторые протоколы не вполне пригодны. К недостаткам таких протоколов относится слабая защита от ошибок или избыточный сетевой трафик. Кроме того, определенные протоколы были созданы для небольших локальных сетей и задолго до появления современных корпоративных сетей с развитыми средствами маршрутизации.

Протоколы локальных сетей должны иметь следующие основные характеристики:

- обеспечивать надежность сетевых каналов;
- обладать высоким быстродействием;
- обрабатывать исходные и целевые адреса узлов;
- соответствовать сетевым стандартам, в особенности – стандарту IEEE 802.

Рассмотрим некоторые протоколы локальной сети.

DHCP (Dynamic Host Configuration Protocol - протокол динамической конфигурации узла) - это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Для этого компьютер обращается к специальному серверу, называемому сервером DHCP. Сетевой администратор может задать диапазон адресов, распределяемых среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве крупных (и не очень) сетей TCP/IP.

Протокол DHCP предоставляет три способа распределения IP-адресов:

- Ручное распределение. При этом способе сетевой администратор сопоставляет аппаратному адресу (обычно MAC-адресу) каждого клиентского компьютера определённый IP-адрес. Фактически, данный способ распределения адресов отличается от ручной настройки каждого компьютера лишь тем, что сведения об адресах хранятся централизованно (на сервере DHCP), и потому их проще изменять при необходимости.
- Автоматическое распределение. При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определённого администратором диапазона.
- Динамическое распределение. Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок. Это называется арендой адреса. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым).

Некоторые реализации службы DHCP способны автоматически обновлять записи DNS, соответствующие клиентским компьютерам, при выделении им новых адресов. Это производится при помощи протокола обновления DNS, описанного в RFC 2136.

DNS (англ. Domain Name System - система доменных имён) - распределённая система (распределённая база данных), способная по запросу, содержащему доменное имя хоста (компьютера или другого сетевого устройства), сообщить IP адрес или (в зависимости от запроса) другую информацию. DNS работает в сетях TCP/IP. Как частный случай, DNS может хранить и обрабатывать и обратные запросы, определения имени хоста по его IP адресу - IP адрес по определённому правилу преобразуется в доменное имя, и посылается запрос на информацию типа "PTR".

DNS обладает следующими характеристиками:

- Распределённость хранения информации. Каждый узел сети в обязательном порядке должен хранить только те данные, которые входят в его зону ответственности и (возможно) адреса корневых DNS-серверов.
- Кеширование информации. Узел может хранить некоторое количество данных не из своей зоны ответственности для уменьшения нагрузки на сеть.
- Иерархическая структура, в которой все узлы объединены в дерево, и каждый узел может или самостоятельно определять работу нижестоящих узлов, или делегировать (передавать) их другим узлам.
- Резервирование. За хранение и обслуживание своих узлов (зон) отвечают (обычно) несколько серверов, разделённые как физически, так и логически, что обеспечивает сохранность данных и продолжение работы даже в случае сбоя одного из узлов.

Протокол RIP (Routing Information Protocol) - протокол маршрутизации, который позволяет маршрутизаторам динамически обновлять маршрутную информацию (направление и дальность в хопах), получая ее от соседних маршрутизаторов.

RIP - дистанционно-векторный протокол, который оперирует хопами в качестве метрики маршрутизации. Максимальное количество хопов, разрешенное в RIP - 15 (метрика 16 означает «бесконечно большую метрику»). Каждый RIP-маршрутизатор по умолчанию вещает в сеть свою полную таблицу маршрутизации раз в 30 секунд, генерируя довольно много трафика на низкоскоростных линиях связи. RIP работает на прикладном уровне стека TCP/IP, используя UDP порт 520.

OSPF (Open Shortest Path First) - протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути Алгоритм Дейкстры (Dijkstra's algorithm).

OSPF предлагает решение следующих задач:

- Увеличение скорости сходимости (в сравнении с протоколом RIP2, т.к. нет необходимости выжидания многократных таймаутов по 30с);
- Поддержка сетевых масок переменной длины (VLSM);
- Достижимость сети (быстро обнаруживаются отказавшие маршрутизаторы, и топология сети изменяется сооответствующим образом);
- Оптимальное использование пропускной способности (т.к строится минимальный остовный граф по алгоритму Дейкстры);
- Метод выбора пути.

Описание работы протокола

1. Маршрутизаторы обмениваются hello-пакетами через все интерфейсы, на которых активирован OSPF. Маршрутизаторы, разделяющие общий канал передачи данных, становятся соседями, когда они приходят к договоренности об определенных параметрах, указанных в их hello-пакетах.

2. На следующем этапе работы протокола маршрутизаторы будут пытаться перейти в состояние соседства с маршрутизаторами, находящимися с ним в пределах прямой связи (на расстоянии одного хопа). Переход в состояние соседства определяется типом маршрутизаторов, обменивающихся hello-пакетами, и типом сети, по которой передаются hello-пакеты. OSPF определяет несколько типов сетей и несколько типов маршрутизаторов. Пара маршрутизаторов, находящихся в состоянии соседства, синхронизирует между собой базу данных состояния каналов.

3. Каждый маршрутизатор посылает объявление о состоянии канала маршрутизаторам, с которыми он находится в состоянии соседства.

4. Каждый маршрутизатор, получивший объявление от соседа, записывает передаваемую в нём информацию в базу данных состояния каналов маршрутизатора и рассылает копию объявления всем другим своим соседям.

5. Рассылая объявления через зону, все маршрутизаторы строят идентичную базу данных состояния каналов маршрутизатора.

6. Когда база данных построена, каждый маршрутизатор использует алгоритм «кратчайший путь первым» для вычисления графа без петель, который будет описывать кратчайший путь к каждому известному пункту назначения с собой в качестве корня. Этот граф - это дерево кратчайшего пути.

7. Каждый маршрутизатор строит таблицу маршрутизации из своего дерева кратчайшего пути.

VLAN (Virtual Local Area Network) - виртуальная локальная вычислительная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям, группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств.

Регламентирующий стандарт: IEEE 802.1

Стандарт IEEE 802.1 определяет один протокольный блок данных (PDU), который носит название SDE (Secure Data Exchange) PDU. Заголовок пакета IEEE 802.1 имеет внутреннюю и внешнюю секции.

Чистый заголовок включает в себя три субполя. MDF (Management Defined Field) является опционным и содержит информацию о способе обработки PDU. Четырехбайтовое субполе SAID (Security Association Identifier) - идентификатор сетевого объекта (VLAN ID). Субполе 802.1 LSAP (Link Service Access Point) представляет собой код, указывающий принадлежность пакета к протоколу vlan. Предусматривается режим, когда используется только этот заголовок.

Защищенный заголовок копирует себе адрес отправителя из mac-заголовка (MAC - Media Access Control), что повышает надежность.

Поле ICV (Integrity Check Value) - служит для защиты пакета от несанкционированной модификации. Для управления VLAN используется защищенная управляющая база данных SMIB(security management information base).

Наличие VLAN ID (SAID) в пакете выделяет его из общего потока и переправляет на опорную магистраль, через которую и осуществляется доставка конечному адресату. Размер поля DATA определяется физической сетевой средой. Благодаря наличию mac-заголовка VLAN-пакеты обрабатываются как обычные сетевые кадры.

NAT (от англ. Network Address Translation - «преобразование сетевых адресов») - это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

Преобразование адресов методом NAT может производиться почти любым маршрутизирующим устройством - маршрутизатором, сервером доступа, межсетевым экраном. Суть механизма состоит в замене адреса источника (source) при прохождении пакета в одну сторону и обратной замене адреса назначения (destination) в ответном пакете. Наряду с адресами source/destination могут также заменяться номера портов source/destination.

Помимо source NAT (предоставления пользователям локальной сети с внутренними адресами доступа к сети Интернет) часто применяется также destination NAT, когда обращения извне транслируются межсетевым экраном на сервер в локальной сети, имеющий внутренний адрес и потому недоступный извне сети непосредственно (без NAT).

Существует 3 базовых концепции трансляции адресов: статическая (Static Network Address Translation), динамическая (Dynamic Address Translation), маскарадная (NAPT, PAT).

Механизм NAT определён в RFC 1631, RFC 3022.

Преимущества

NAT выполняет две важных функции.

1. Позволяет сэкономить IP-адреса, транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних).

2. Позволяет предотвратить или ограничить обращение снаружи ко внутренним хостам, оставляя возможность обращения изнутри наружу. При инициации соединения изнутри сети создаётся трансляция. Ответные пакеты, поступающие снаружи, соответствуют созданной трансляции и поэтому пропускаются. Если для пакетов, поступающих снаружи, соответствующей трансляции не существует (а она может быть созданной при инициации соединения или статической), они не пропускаются.

Недостатки

1. Не все протоколы могут «преодолеть» NAT. Некоторые не в состоянии работать, если на пути между взаимодействующими хостами есть трансляция адресов. Некоторые межсетевые экраны, осуществляющие трансляцию IP-адресов, могут исправить этот недостаток, соответствующим образом заменяя IP-адреса не только в заголовках IP, но и на более высоких уровнях (например, в командах протокола FTP). См. Application-level gateway.

2. Из-за трансляции адресов «много в один» появляются дополнительные сложности с идентификацией пользователей и необходимость хранить полные логи трансляций.

3. DoS со стороны узла, осуществляющего NAT - если NAT используется для подключения многих пользователей к одному и тому же сервису, это может вызвать иллюзию DoS атаки на сервис (множество успешных и неуспешных попыток). Например, избыточное количество пользователей ICQ за NAT'ом приводит к проблеме подключения некоторых пользователей из-за превышения допустимой скорости коннектов к серверу. Частичным решением проблемы является использование пула адресов (группы адресов), для которых осуществляется трансляция.

4. Сложности в работе с пиринговыми сетями, в которых необходимо не только инициировать исходящие соединения, но также принимать входящие.

Список литературы

1. «Основы информационных технологий, том 1 «Алгоритмы телекоммуникационных сетей» Ю.А. Семенов 2015г. 637с. Бином.ЛБЗ - Интернет-университет информационных технологий-ИНТУИТ

2. «Основы информационных технологий, том 2 «Алгоритмы и протоколы Интернет» Ю.А. Семенов 2016г. 826с. Бином. ЛБЗ - Интернет-университет информационных технологий-ИНТУИТ

3. «Основы информационных технологий, том 3 «Процедуры, диагностика, безопасность» Ю.А. Семенов 2015г. 509с. Бином.ЛБЗ - Интернет-университет информационных технологий - ИНТУИТ

4. «Компьютерные сети. Принципы, технологии, протоколы» Олифер В.Г., Олифер Н. А. 2017 г., 958 Стр. учебник для вузов; Гриф МО РФ; 3-е изд.

5. Материал лекций дисциплины «Информационные сети»

6. Материал с информационного ресурса http://citforum.ru/ (учебное пособие «Телекоммуникационные технологии» http://citforum.ru/nets/semenov/)

7. Материал с информационного ресурса http://citforum.ru/ (статья «Стратегическое планирование сетей масштаба предприятия» http://citforum.ru/nets/spsmp/)