СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Р.Р. Фаткиева

Основы построения защищенных компьютерных сетей

Протокол IP

СПбГЭТУ «ЛЭТИ», 2021 г.

3.2 Стек протоколов TCP/IP

Стек TCP/IP имеет четырехуровневую структуру и является самым распространенным средством организации составных компьютерных сетей, из-за следующих свойств (рис. 3.2):

- большинство современных сетей передают основную часть своего трафика с помощью протокола TCP/IP;
- большинство современных операционных систем поддерживают стек TCP/IP для получения доступа к сети Internet;
- гибкая технология для соединения разнородных систем на транспортном и прикладном уровнях;
- устойчивая масштабируемая межплатформенная среда для приложений клиент-сервер.

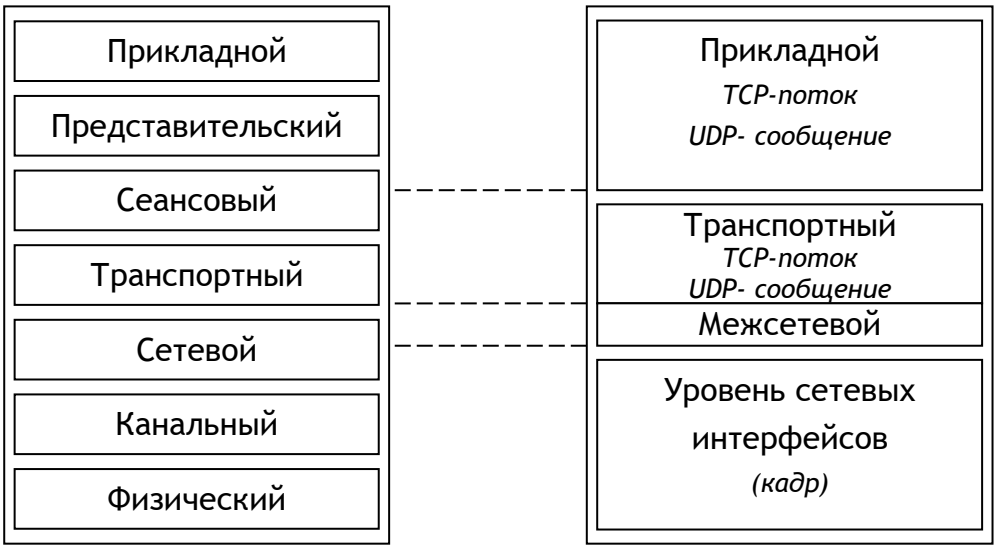

Рис. 3.2

Прикладной уровень объединяет приложения, построенные в архитектуре клиент-сервер. К ним относят Telnet, FTP, DNS, SNMP, HTTP. Для пересылки данных через сеть приложение обращается к транспортному уровню.

Транспортный уровень. На данном уровне функционируют два протокола TCP и UDP. Протокол TCP является надежным протоколом с установлением соединения, который осуществляет:

- деление потока данных, полученных от вышележащего уровня на части–сегменты, и передачу межсетевому уровню IP;
- обеспечение надежной передачи сегментов в сети (установление, поддержка и закрытие соединения);
- обеспечение обратной сборки сегментов в поток.

Протокол UDP обеспечивает передачу прикладных пакетов датаграммным способом и является ненадежным протоколом без установления соединения. Используется как экономичное средство связи уровня межсетевого взаимодействия с прикладным процессами если:

- накладные расходы на установления сеанса и проверки успешной доставки являются выше расходов на повторную передачу;
- приложение использующее протокол UDP обеспечивает установление соединения и проверку доставки пакетов.

Межсетевой уровень. Реализует концепцию коммутации пакетов в режиме без установления соединения. Основными протоколами этого уровня являются дейтаграммный протокол IP и протоколы маршрутизации (RIP, OSPF–, BGP и др.). Протокол IP осуществляет:

- дополнение сегментов, полученных от транспортного уровня, заголовком, содержащим уникальным 32-битным идентификатором (IP–адресом) получателя и отправителя и служебной информацией и передачу дейтограммы на уровень доступа к сети;
- определение маршрута дейтограммы;
- получение дейтограммы и проверку IP-адреса назначении. При соответствии принимающему узлу, производиться сборка дейтограмм и передача транспортному уровню. При несоответствии IP-модулем принимается решение о передаче данной дейтограммы по месту назначения, определив маршрут следования, или уничтожении дейтограммы (например, истечение времени жизни) с отправкой источнику сообщение об ошибки с помощью протокола ICMP.

Уровень сетевых интерфейсов. Обеспечивает интеграцию в составную сеть других сетей, поддержкой популярных стандартов физического и

канального уровней: Ethernet, Token Ring, FDDI и др. К функциям данного уровня относят:

- отображение IP-адресов в физические адреса (например, в MAC-адреса);
- инкапсуляция IP-дейтаграмм в кадры для передачи по физическому каналу связи и извлечение дейтаграмм из кадров;
- определение метода доступа к среде передачи (маркерный доступ, множественный доступ с обнаружение коллизий);
- кодирование данных;
- пересылка и прием кадров.

3.3 Протокол IP

Основу транспортных средств стека TCP/IP составляют протоколы межсетевого и транспортного уровней, определяющие маршрут, передачу данных от отправителя к получателям, а также, гарантируют надежность доставки пакетов. Прикладной уровень стека поддерживает интерфейс с пользователем и приложением, а уровень сетевых интерфейсов — интерфейс с технологиями составляющих сетей.

Назначение протокола IP — протокола межсетевого взаимодействия (Internet Protocol, IP) —передача пакетов между сетями. Протокол IP относится к протоколам без установления соединения и обрабатывает каждый пакет как независимую единицу, не имеющую связи с другими пакетами.

К функциям IP- протокола относят:

- передачу пакетов по сети;
- динамическую фрагментацию пакетов при передаче между сетями с различными значениями поля данных кадров;
- перенос между сетями различных типов адресной информации в унифицированной форме.

Структура IP-пакета. Единицей данных, передаваемых по протоколу IP является дейтограмма, состоящая из заголовка и поля данных. Наибольший интерес представляет заголовок дейтограммы, длинной 20 байт и состоящий из следующих полей (рис 3.3):

Рис. 3.3

Поле версии-занимает 4 бита. Содержит номер версии IP-протокола и указывает программе получателю по какой версии IP-протокола следует декодировать остальные поля. Если программа не работает с данной версией протокола, то дейтограмма уничтожается.

Длина заголовка занимает 4 бита. Указывает полную длину IP-заголовка, измеренного в 32-битных словах. В дейтограмме начало поля данных никак не указывается, поэтому возникает необходимость знать где заканчивается заголовок и начинается поле данных.

Тип обслуживания (Тип сервиса) занимает 1 байт. Определяет приоритет дейтограммы и желаемый тип маршрутизации. По установленным флагам. Первые 3 бита занимает поле приоритета дейтограммы, значение которого от 0 (самый низкий) до 7 (высокий), чем оно выше, тем быстрее будет доставлена дейтограмма.

Приоритет PR		Задержка D	Пропускная способность T	Надежность R	Стоимость
0	2	3			7

Поле приоритета: *000-обычно*; *001-срочно*; *010-немедленно*; *011-мгновенно*; *100-мгновенно*; *110межсетевое управление*; *111-управление сетью*.

Установленный флаг в поле:

- *задержка*- указывает промежуточному узлу на выбор маршрута с минимальной задержкой;

- *пропускная способность*- указывает промежуточному узлу на выбор маршрута максимальной пропускной способностью;
- *надежность* - указывает промежуточному узлу на выбор маршрута с максимальной надежностью;
- *стоимость*- указывает промежуточному узлу на выбор маршрута с минимальной стоимостью.

*Длина дейтограммы з*анимает 2 байта. Содержит информацию об общей длине дейтограммы, максимальная длина которой составляет 65535 байт. При передаче по сети которой выбирается с учетом максимальной длины кадра протокола нижнего уровня, несущего IP- дейтограмму (например, в Ethernet 1500 байт). По данному полю протокол нижнего уровня принимающего узла устанавливает полный размер дейтограммы, разбитой на фрагменты.

Поле идентификатора занимает 2 байта. Содержит уникальный идентификатор, присвоенный передающим узлом и позволяющий осуществить правильную сборку фрагментов дейтограммы. При фрагментации дейтограммы каждый фрагмент получает один и тот же идентификатор.

Поле флагов занимает 3 бита и состоит из флагов.

0	DF	MF

Установленный флаг DF запрещает фрагментацию. Если промежуточный узел не может отправить дейтограмму без фрагментации, то дейтограмма уничтожается, а отправителю возвращается сообщение об ошибке.

Установленный флаг MF сообщает, что дейтограмма фрагментирована. Последний фрагмент передается с MF=0. Флаг MF используется с полем смещения.

Поле смещения занимает 13 бит, указывается в единицах кратных 8 байтам. Содержит смещение фрагмента относительно начала исходной дейтограммы. Используется при сборке/разборке фрагментов при передаче их между сетями с различными размерами кадров.

Время жизни занимает 8 бит. Содержит время в секундах, отводимое на доставку дейтограмм получателю. Поле заполняется отправителем. Согласно стандарту TCP/IP каждый промежуточный узел сети уменьшает значение поля на 1с. При достижении 0 дейтограмма уничтожается, а отправителю

посылается сообщение об ошибки. Данный механизм предотвращает зацикливание дейтограмм в сети.

Поле протокола занимает 8 бит. Определяет вышестоящий протокол стека, согласно которому должны обрабатываться данные.

Контрольная сумма занимает 2 байта. Вычисляется только по заголовку и изменяется вместе с полем времени жизни на каждом промежуточном узле. Контрольная сумма повышает надежность передачи дейтограмм и если при проверки обнаруживается ошибка, то передавать дейтограмму не имеет смысла, она уничтожается.

Поля IP-адрес отправителя и IP-адрес получателя занимают 32 бита, заполняются при создании дейтограммы и остаются неизменными во время передачи.

Поле Опции состоит из одного или нескольких кодов переменной длины, следующих друг за другом без разделителей и определяют дополнительные функции по обработке IP-дейтограммы. Опция делится на 3 подполя:

Обработка опции прекращается при обнаружении опции *Конец списка опций*. Опция *Нет операции* используется для выравнивания между опциями по границе 32 бита.

Поля заполнителя используется для дополнения заголовка нулями до числа 32 разрядных слов.

Фрагментация IP дейтограмм. Важной особенностью протокола IP является его способность выполнять динамическую фрагментацию пакетов при передаче их между сетями. Это связано ч тем, что разнородные сети имеют различный максимальный размер передаваемых кадров MTU (Maximum Transmission Unit) например, в сетях Ethernet =1536, FDDI 4036. При передаче дейтограммы из среды с большим MTU в среду с меньшим MTU возникает необходимость фрагментации дейтограмм. Для этого модуль IP создает:

1. Несколько новых дейтограмм, при этом данные из исходной дейтограммы делится на число частей, размер которых кроме самой последней кратен 8 байтам. Размер последней равен полученному остатку.
2. В заголовках новых дейтограмм изменяются следующие поля:

- в поле смещения первого фрагмента устанавливается значение 0, в остальных –положение фрагмента относительно исходной дейтограммы;
- в поле общей длины – помещается длина каждой дейтограммы;
- в поле идентификатора – уникальные значения однозначно определяющие все фрагменты исходной дейтограммы, для пары отправитель –получатель;
- в поле флагов –для всех фрагментов кроме последнего флаг MF устанавливается в 1, флаг MF=0 указывает на последний фрагмент дейтограммы
- контрольная сумма
- Длина заголовка

Все остальные поля заголовка исходной дейтограммы копируются в поля заголовка фрагментов.

Для сборки IP модуль протокола получателя буферизирует фрагменты с одинаковым идентификатором, до получения всех фрагментов дейтограммы. При этом у полученных фрагментов уменьшается поле *время жизни* до тех пор, пока не придут недостающие фрагменты. При истечении срока жизни фрагменты дейтограммы уничтожаются. При получении всех фрагментов на основании поля смещения и длины дейтограммы осуществляется сборка дейтограммы.

Примечание: *IP-маршрутизаторы не собирают фрагменты пакетов в более крупные пакеты, даже если такое укрупнение допускается. Это связано с тем, что отдельные фрагменты сообщения могут перемещаться по различным маршрутам, поэтому нет гарантии, что все фрагменты проходят через какой-либо промежуточный маршрутизатор на их пути.*

3.4 Протокол ICMP

Протокол ICMP (Internet Control Message Protocol) –это система правил уведомления об ошибках доставки дейтограмм. Согласно ICMP сообщение об ошибках почти всегда передаются машине отправителю, получив которое отправитель выбирает порядок повторной передачи дейтограммы. Все ICMP-сообщения имеют заголовок, поля: тип, код и контрольная сумма. Поля код и

тип определяют содержание ICMP сообщения, некоторые из которых представлены ниже:

Echo- сообщение типа 0 и 8 используется для тестирования сети между двумя узлами. Для этого тестирующим узлом формируется серия сообщений представленных на рис.

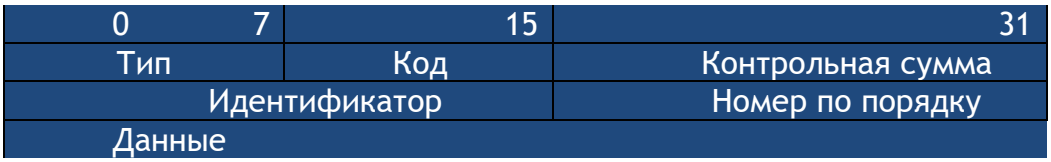

Рис. 3.4

Поля код и тип указывают что данное сообщение является Echo-сообщением, поле номер по порядку определяет порядковый номер данного сообщения, среди серии сообщений, отправленный в данном сеансе. Сам сеанс связи однозначно определяется полем идентификатор. В поле данных содержаться произвольные данные, размер его определяется общей длиной дейтограммы, указанной в длине IP-заголовка.

Приняв Echo-сообщение, получатель:

- изменяет значение поля тип сообщения с 8 на 0;
- меняет местами адрес отправителя и получателя;
- пересчитывает контрольную сумму;
- возвращает сообщение отправителю.

По времени оборота, проценту потерь и последовательности прибытия дейтограмм можно определить качество связи с тестируемым узлом. Однако если сообщение Echo отправлено на широковещательный адрес сети, то отправитель получит ответ со всех узлов, поддерживающих широковещательные сообщения и подключенных к сети. Данное свойство используется злоумышленником для атаки называемой Smurf, при которой от имени атакуемого узла происходит рассылка Echo-сообщений, и если число возвращаемых сообщений велико, то узел не справится с нагрузкой и «захлебнется».

Destination Unreachable (Адресат недоступен). Отправляется маршрутизатором при невозможности доставки дейтограммы в случаях когда:

- возникает необходимость фрагментации дейтограммы, а флаг DF запрещает фрагментацию;
- у маршрутизатора нет маршрута в сеть назначения дейтограммы;

- указанный в дейтограмме протокол вышестоящего уровня не поддерживается получателем;
- правила фильтрации запрещают передачу пакета к месту назначения.

0 7	15	31
Тип	Код	Контрольная сумма
Не используется		
IP- заголовок и первые 64 байта		

Данные сообщения могут использоваться для нарушения связи между отправителем и получателем, путем отправки сообщения Destination Unreachable.

Source Quench сообщение тип 4 о снижении скорости передачи служит для ограничения частоты отправления дейтограммы. При получении сообщения отправитель должен уменьшить скорость или приостановить отправку дейтограмм до тех пор, пока не перестанет получать сообщения такого типа. Однако в большинстве узлов сообщения типа Source Quench не используются, так как возможна фальсификация сообщений злоумышленником с целью помешать отправке данных с атакуемого узла.

Redirect. Сообщение Redirect – переадресовать направляется отправителю промежуточным узлом при наличии маршрута лучшего, чем тот, который был выбран ранее. Например:

1. Узел А, подключенный к маршрутизаторам С1 и С2 отправляет дейтограмму узлу В через маршрутизатор С1.
2. Маршрутизатор С1, получив дейтограмму определяет, что рациональнее доставлять дейтограмму через маршрутизатор С2. Поэтому С1 направляет узлу В полученную дейтограмму, а узлу А – сообщение Redirect, содержащее IP-адрес найденного узла.
3. Узел А, получив сообщение Redirect воспользуется новой маршрутизацией лишь некоторое время, а затем вертеться к предыдущей.

0 7	15	31
Тип	Код	Контрольная сумма
IP-адрес шлюза		
IP- заголовок и первые 64 байта		

Сообщения Redirect может использоваться злоумышленником для навязывания ложного маршрута см. табл.

Router Advertisement/Solicitation используются узлом для получения информации об адресах маршрутизаторов к которым он подключен. Для этого узлом формируется широковещательное сообщение ICMP типа 10 (Router Solicitation). Маршрутизатор, получив данное сообщение посылает узлу ответ-сообщение ICMP типа 9 (Router Advertisement), содержащее адрес одного или нескольких маршрутизаторов и значения их приоритетов.

Сообщение Router Advertisement может использоваться злоумышленником для навязывания атакуемому узлу ложного маршрута или конфигурирования таблиц маршрутизации узла.

Address Mask Request/Reply. Сообщения Address Mask Request Address Mask Reply (17 и 18) используются узлом для получения маски сети, в которой он находится. Для этого узлом генерируется сообщение Address Mask Request, в ответ на которое маршрутизатор отправляет сообщение Address Mask Reply с записанным значением маски той сети откуда пришел запрос (рис 3.5. *Запрос адресной маски*, 3.6 *Отклик на запрос адресной маски*).

0 7	15	31
Тип	Код	Контрольная сумма
Идентификатор		Порядковой номер

Рис. 3.5

0 7	15	31
Тип	Код	Контрольная сумма
Идентификатор		Порядковой номер
Адресная маска		

Рис. 3.6

Сообщения Address Mask Request Address Mask Reply могут использоваться злоумышленником незаконно подключенным к сети для определения маски сети, или для навязывания узлу неверной сетевой маски, лишив его тем самым возможности полноценно работать в сети.

3.5 Протокол ARP

Данный протокол предназначен для преобразования IP- адресов в физические адреса (хранящиеся в сетевой плате), называемые также MAC-адресами. Для передачи IP-дейтограммы по физическому каналу связи требуется инкапсулировать дейтограмму в кадр физического уровня с указанием MAC- адреса получателя, так как IP- адрес, включенный в заголовок дейтограммы, не несет информации о физическом адресе устройства. Для

поиска по IP- адресу соответствующего физического адреса используется протокол ARP. Формат сообщения представлен на рис.

Работа протокола ARP осуществляется на основании динамической ARP таблицы по следующему алгоритму:

1. С межсетевого уровня IP дейтограмма вместе с IP адресом поступает к модулю ARP с запросом на разрешение адреса. Если адрес найден то дейтограмма предается в физический канал передачи данных.
2. ARP модулем происходит поиск в ARP-таблице указанного IP адреса.
3. Если запрашиваемый адрес отсутствует, то IP –дейтограмма ставится в очередь, а модуль ARP формирует широковещательный ARP запрос.
4. Все узлы, получившие запрос, сравнивают указанный IP адрес с собственным, в случае совпадения узел отправляет ответ со значением своего физического адреса. Одновременно узел получатель запроса вносит данные об IP-адресе и физическом адресе отправителя в свою ARP- таблицу.
5. На основании полученных данных ARP-модулем корректируется таблица, дейтограмма извлекается из очереди и передается в физический канал передачи данных.

Gratuitous ARP*– особый тип запроса, в котором поля IP- адреса отправителя и IP-адреса получателя содержат адрес одного и того же узла. Широковещательная рассылка такого сообщения информирует об изменении MAC адреса отправившего узла.*

Безопасность. Модуль ARP не хранит состояния, поэтому примет ответ, даже если не посылал запроса. Этим свойством может воспользоваться злоумышленник, который, генерирует ложные ARP- ответы для:

- навязывания узлу ложного или несуществующего маршрутизатора;
- выдачи себя за другой узел;

Таким образом использование сообщений Gratuitous ARP позволяет ввести в заблуждение целую сеть.

Для предотвращения использования ARP- модуля необходимо:

- Использование статической ARP таблицы, в которой MAC- и IP- адреса приведены в однозначное соответствие, а динамическое изменение запрещено. Данную таблицу необходимо использовать на критических узлах сети. И если злоумышленник незаконно присвоит себе IP, то

сможет обмениваться дейтограммами только с узлами, использующими динамические ARP-таблицы.

- Использование программы, прослушивающей сеть и информирующей о замеченных нарушениях (напр. arpwatch).

Список литературы

1. Таненбаум, Эндрю. Компьютерные сети [Текст] : учебное пособие / Э. Таненбаум; [Пер. с англ. В. Шрага], 2003. 991 с. 60
2. Олифер, Виктор Григорьевич. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учеб. пособие для вузов по направлению ”Инфор матика и вычислит. техника” и по специальности ” Вычислит. машины, комплексы, системы и сети”, ”Автоматизир. машины, комплексы, системы и сети”, ” Програм. обеспечение вычислит. техники и автоматизир. систем” / В.Г. Олифер, Н.А. Олифер, 2006. 957 с. 133
3. Борисенко, Константин Алексеевич. Сети и телекоммуникации [Текст] / К. А. Борисенко, 2021. 43 с. 50 4 Дибров, Максим Владимирович. Сети и телекоммуникации. Маршрутизация в IPсетях в 2 ч. Часть 2 [Электронный ресурс] : Учебник и практикум для вузов / Дибров М. В., 2021. 351 с неогр.
4. Дибров, Максим Владимирович. Сети и телекоммуникации. Маршрутизация в IPсетях в 2 ч. Часть 1 [Электронный ресурс] : Учебник и практикум для вузов / Дибров М. В., 2021. 333 с неогр.
5. Шелухин О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие для вузов [Электронный ресурс] / О. И. Шелухин, Д. Ж. Сакалема, А. С. Филинова, 2018. 220 с