СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Р.Р. Фаткиева

Основы построения защищенных компьютерных сетей

Сетевые протоколы передачи информации. Модель OSI

СПбГЭТУ «ЛЭТИ», 2021 г.

3 СЕТЕВЫЕ ПРОТОКОЛЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

3.1 Эталонная модель взаимодействия открытых систем (ISO OSI). Уровни и протоколы

Стремление создания единой, универсальной и открытой к изменениям структуры привело к тому, что Международная организация по стандартизации (ISO-International Standard Organization) предложила концепцию архитектуры открытых систем, в соответствии с которой, распределенная информационно-вычислительная среда делится на ряд логических уровней, распложенных друг над другом, и называемых уровнями.

Общие свойства открытых систем рассматриваются в совокупности, как взаимосвязанные, и реализуются в комплексе:

- расширяемость/масштабируемость - extensibility/scalability,
- мобильность (переносимость) - portability,
- интероперабельность (способность к взаимодействию с другими системами)- interoperability,
- дружественность к пользователю, в том числе легкая управляемость -driveability.

Использование подхода открытых систем обеспечивает следующие преимущества:

- устранение избыточности программных кодов благодаря стандартизации программных интерфейсов или повторному использованию программ (reusability).
- процесс постепенного развития функций систем позволяет осуществлять замену отдельных компонентов без перестройки всей системы;
- условия соблюдения поставщиком соответствующих стандартов открытых систем дает независимость от поставщиков аппаратных или программных средств;
- возможность использования информационных ресурсов других систем

- возможность совместного использования прикладных программ, реализованных в разных ОС.

Использование подхода открытых систем, описанного выше нашло применение в стандартной модели взаимодействия открытых систем ISO/OSI, разработанной в начале 1980-х годов. Модель OSI определяет различные уровни взаимодействия систем, а также функции, выполняемые каждым уровнем. Часть открытой системы, реализующая некоторую функцию и входящая в состав того или иного уровня, называется объектом. Набор правил взаимодействия объектов одного и того же N-го уровня называется N-протоколом. Связь между объектами соседних уровней определяется интерфейсом. Всего выделено семь уровней: физический (Physical), канальный (Data Link), сетевой (Network), транспортный (Transport), сеансовый (Session), представительный (Presentation), прикладной (Application).

При обмене данными через каналы связи приложение обращается с запросом к прикладному уровню, на основании которого программное обеспечение прикладного уровня формирует сообщение стандартного формата, состоящего из заголовка и поля данных. Заголовок содержит служебную информацию, которую необходимо передать через сеть прикладному уровню машины-адресата, чтобы сообщить ему, какую работу надо выполнить. Поле данных сообщения может быть пустым содержать данные или служебную информацию. Затем прикладной уровень направляет сообщение представительному уровню, который на основании информации, полученной из заголовка прикладного уровня, выполняет требуемые действия и добавляет к сообщению собственную служебную информацию — заголовок представительного уровня, в котором содержатся указания для протокола представительного уровня машины-адресата. Полученное в результате сообщение передается вниз сеансовому уровню, который в свою очередь добавляет свой заголовок, и т. д. Данная операция называется инкапсуляция данных верхнего уровня в пакет нижнего уровня (см. Рис 3.1). Наконец, достигается нижний физический уровень, который, собственно, и передает сообщение в сеть. При этом устройства сети не анализируют сообщения, но

иногда записывают в ее заголовок адреса пройденных машин и другую информацию.

Выйдя из подсети сообщение переходит от шлюза к шлюзу. Каждый шлюз, через который проходит сообщение, вычисляет контрольную сумму и сравнивает полученное значение с тем, которое записано в конце сообщения. При совпадении сообщение передается подсети данного шлюза или следующему шлюзу, в противном случае сообщение уничтожается как поврежденное, а машине отправителю передается сообщение об ошибке. Когда сообщение с первым фрагментом приходит к компьютеру -адресату, в нем запускается программа уровня межсетевого взаимодействия, называемая таймером сборки. Если все пакеты сообщения поступили на машину адресат, то сообщение последовательно перемещается вверх с уровня на уровень.

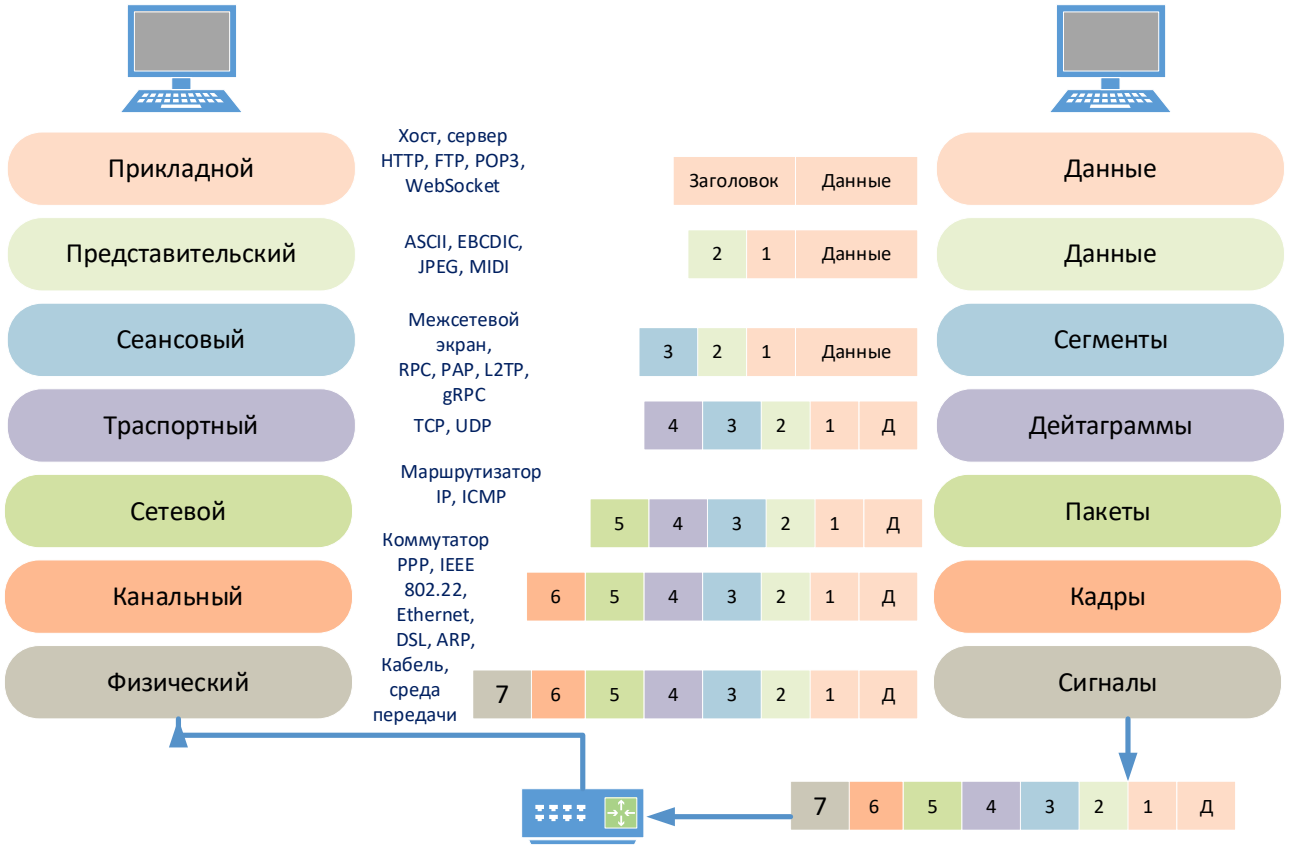

Рис. 3.1

Каждый уровень анализирует и обрабатывает заголовок своего уровня, выполняя соответствующие данному уровню функции, а затем удаляет этот заголовок и передает сообщение вышележащему уровню. Рассмотрим каждый из уровней подробнее.

*Физический уровень (Physical layer). О*существляет кодирование данных и представление их в виде сигналов для передачи по физическим каналам связи (коаксиальный кабель, витая пара, оптоволоконный кабель). Имея дело с входящими сообщениями физический уровень осуществляет обратный процесс, превращая сигналы в биты.

Преамбула	Признак начала данных	Данные	Признак конца данных

Канальный уровень (Data Link layer) осуществляет проверку доступности среды передачи, направление пакетов данных, поступающих от протоколов верхних уровней, узлу назначения, адрес которого указывает протокол верхнего уровня физическому уровню и реализацию механизмов обнаружения и коррекции ошибок, предотвращает перегрузку сети (приостановкой трафика).

MAC-адрес получателя	MAC-адрес отправителя	Длина и тип данных	Данные	Контрольная сумма

Сетевой уровень (Network layer). Осуществляет фрагментацию (сборку) передаваемых транспортным уровнем данных, маршрутизацию и продвижение пакета по составной сети. На основании сетевого адреса

Сетевой адрес отправителя	Сетевой адрес получателя	Длина, тип и номер пакета	Контрольная сумма	Служебная информация	Данные

Транспортный уровень (Transport layer). Обеспечивает приложениям или верхним уровням стека — прикладному и сеансовому — передачу данных с той степенью надежности, которая им требуется:

- разбивку сообщения сеансового уровня на пакеты, их нумерация;
- буферизация принимаемых пакетов;
- упорядочивание прибывающих пакетов;
- адресация прикладных процессов;
- управление потоком.

В то время, как задачей сетевого уровня является передача данных между произвольными узлами сети, задача транспортного уровня заключается в передаче данных между любыми прикладными процессами, выполняющимися на любых узлах сети. Действительно после того, как пакет средствами протокола IP доставлен в компьютер-получатель, данные

необходимо направить конкретному процессу-получателю. Каждый компьютер может выполнять несколько процессов, более того, прикладной процесс тоже может иметь несколько точек входа, выступающих в качестве адреса назначения для пакетов данных.

Вид приложения отправителя	Вид приложения получателя	Длина, тип и номер пакета	Контрольная сумма	Служебная информация	Данные

Пакеты, поступающие на транспортный уровень, организуются операционной системой в виде множества очередей к точкам входа различных прикладных процессов. В терминологии TCP/IP такие системные очереди называются портами. Таким образом, адресом назначения, который используется на транспортном уровне, является идентификатор (номер) порта прикладного сервиса. Номер порта, задаваемый транспортным уровнем, в совокупности с номером сети и номером компьютера, задаваемыми сетевым уровнем, однозначно определяют прикладной процесс в сети.

Сеансовый уровень (Session layer). Устанавливает, поддерживает, завершает текущее соединение между отправителем и получателем.

При обрыве связи позволяют вставлять контрольные точки в длинные передачи, для возможности начала соединения с последней контрольной точкой, а не сначала.

1. установление способа обмена сообщениями (дуплексный или полудуплексный);
2. синхронизация обмена сообщениями;

Представительный уровень (Presentation layer) Уровень представления — согласовывает представление (синтаксис) данных при взаимодействии двух прикладных процессов:

-преобразование данных из внешнего формата во внутренний;

-шифрование и расшифровка данных.

Прикладной уровень (Application layer) — это в действительности просто набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организуют совместную работу,

например с помощью протокола электронной почты. Единица данных, которой оперирует прикладной уровень, обычно называется сообщением (message).

Прикладной уровень — набор всех сетевых сервисов, которые предоставляет система конечному пользователю:

-идентификация, проверка прав доступа;

-принт- и файл-сервис, почта, удаленный доступ...

Существует очень много различных служб прикладного уровня. Приведем в качестве примера хотя бы несколько наиболее распространенных реализаций файловых служб: NCP в операционной системе Novell NetWare, SMB в Microsoft Windows NT, NFS, FTP и TFTP, входящие в стек TCP/IP.

Таблица 1

Уровень	Функции	Возможные нарушения	Способы устранения нарушений
Физический	- синхронизация; - модуляция; - кодирование информации; - формирование электрических сигналов: - передача битов по каналам связи.	1. Перехват данных с помощью несанкционированного физического подключение к сети; 2. Прослушивание сети; 3. Наличие коллизий и ошибок. 4. Электромагнитные наводки	1.-2. Шифрование данных; 1.-2. Использование интеллектуальных концентраторов для назначения MAC-адресов, имеющих доступ к сети; 3. Автосегментация-способность изолировать работающие порты, создающие помехи, ошибки или имеющих недопустимый для данной сети MAC-адрес. 4.Кодирование информации 5. Заземление линий передач данных.
Канальный	- установление и расторжение соединения; - управление соединением физических каналов передачи данных. - расщепление соединения на несколько физических; - сериализация; - обнаружение и исправление ошибок; - управление потоком		
Сетевой	Функции сетевого уровня:	1. Фальсификация IP-адреса; 2. Сканирование сети	1. Межконцевое шифрование (VPN);

	- выбор наилучшего маршрута передачи данных; - организация сетевых соединений; - согласование разных протоколов канального уровня; - сегментирование и блокирование; - обнаружение и исправление ошибок; - сериализация; - управление потоком; - передача срочных данных;	3. Атаки на протоколы маршрутизации; 4. Использование туннелирования для передачи трафика в обход системы фильтрации пакетов	2. Использование механизмов аутентификации (партнеров взаимодействия, ЦП, привязка к сетевым адресам); 3. Использование средств обнаружения атак (IDS) 4. Использозвание механизмов управление доступом (в.т. ч. МЭ, фильтрация трафика)
Транспортный	- отображения транспортного адреса на сетевой адрес; - мультиплексирование и расщепление транспортных соединений на сетевые соединения; - установление и расторжение транспортных соединений; - управление потоком на отдельных соединениях; - обнаружение ошибок и управление качеством сервиса; - исправление ошибок; - сегментирование, блокирование и сцепление;	Сканирование портов	1. Использование механизмов аутентификации (привязка к портам);

	- передача срочных блоков данных.		
Сеансовый	Функции сеансового уровня: ○ установлению и расторжению сеансового соединения; ○ обмен нормальными и срочными данными; ○ управлению взаимодействием; ○ синхронизации сеанса; ○ восстановлению сеанса;	Принуждение к ускоренной передаче данных	1. увеличение окна передачи данных после получения подтверждения 2. VPN сеансового уровня; 3. Регистрация событий, 4. Трансляция внутренних сетевых адресов
Представления данных	Функции представительного уровня - запрос на установление сеанса; - передача данных; - согласование и пересогласование выбора синтаксиса; - преобразование синтаксиса, включая преобразование данных, форматирование и специальные преобразования (сжатие, шифрование/дешифрование)	Подбор паролей, ключей	1.Использование механизмов идентификации и аутентификации; 2. Криптографическое преобразование данных
Прикладной	Предоставление услуг на уровне конечного пользователя: почта, регистрация и т.д.	1.Подбор паролей, ключей, атаки типа маскарад; 2.Вирусные, спам- атаки 3.Атаки отказ в обслуживании	1. Криптографическое преобразование; 2. Использование механизмов идентификации и

		4. Атаки направленные на «уязвимости» в программном обеспечении	аутентификации; Использование средств обнаружения атак (IDS) 3. Использование механизмов управление доступом (в.т. ч. МЭ, фильтрация трафика) 4. Контроль за участниками взаимодействия; 5. Антивирусная защита; Системное администрирование (в т.ч., анализ log-файлов, установка заплат на ОС и т.д)

Литература

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 IP-сетях 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