Туннелирование

Туннелирование (от англ. *tunnelling* — «прокладка туннеля») в компьютерных сетях — это процесс, в ходе которого создаётся логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов.

Туннелирование представляет собой метод построения сетей, при котором один сетевой протокол инкапсулируется в другой. От обычных многоуровневых сетевых моделей (таких как OSI или TCP/IP) туннелирование отличается тем, что инкапсулируемый протокол относится к тому же или более низкому уровню, чем используемый в качестве туннеля.

Суть туннелирования состоит в том, чтобы «упаковать» передаваемую порцию данных, вместе со служебными полями, в область полезной нагрузки пакета несущего протокола. Туннелирование может применяться на сетевом и на прикладном уровнях. Комбинация туннелирования и шифрования позволяет реализовать закрытые виртуальные частные сети (VPN). Туннелирование обычно применяется для согласования транспортных протоколов либо для создания защищённого соединения между узлами сет.

Типы протаколов

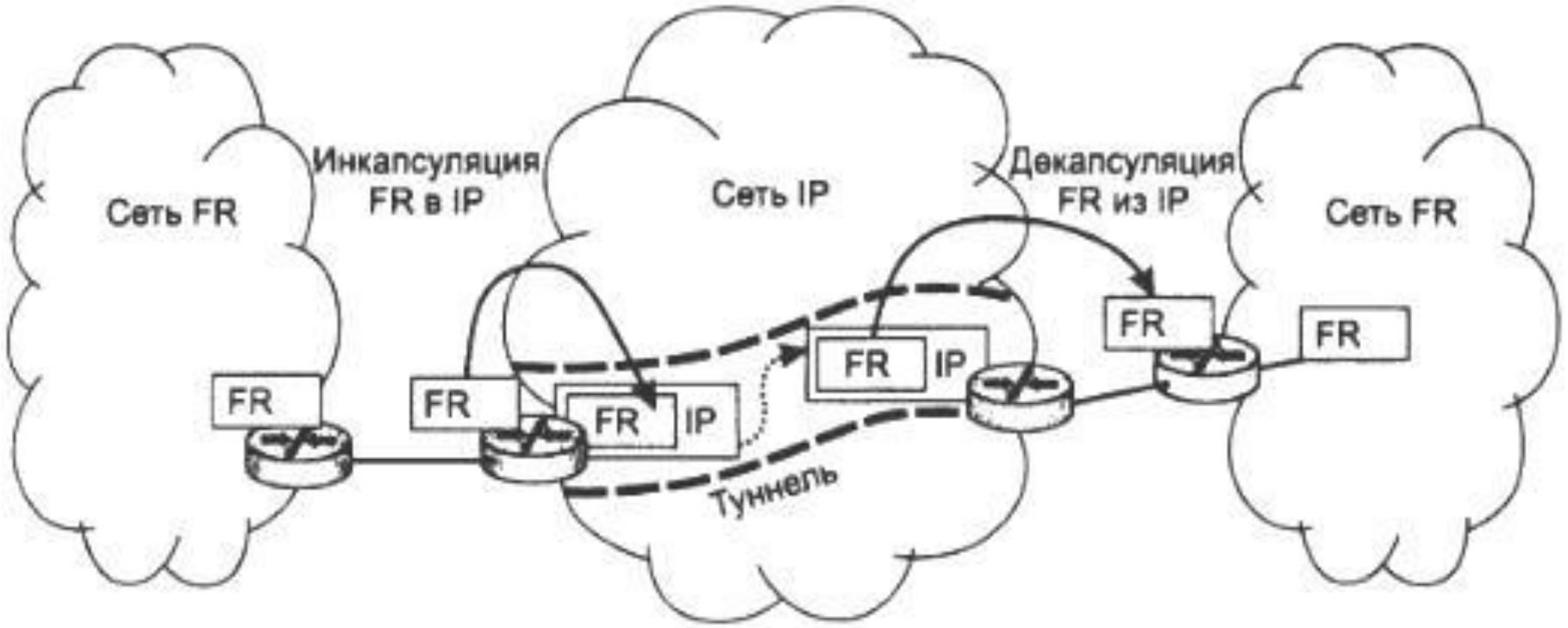
В процессе инкапсуляции (туннелирования) принимают участие следующие типы протоколов:

1) транспортируемый протокол;

2) несущий протокол;

3) протокол инкапсуляции.

Протокол транзитной сети является несущим, а протокол объединяемых сетей — транспортируемым. Пакеты транспортируемого протокола помещаются в поле данных пакетов несущего протокола с помощью протокола инкапсуляции. Пакеты-«пассажиры» не обрабатываются при транспортировке по транзитной сети никаким образом. Инкапсуляцию выполняет пограничное устройство (маршрутизатор или шлюз), которое находится на границе между исходной и транзитной сетями. Извлечение пакетов транспортируемого протокола из несущих пакетов выполняет второе пограничное устройство, расположенное на границе между транзитной сетью и сетью назначения. Пограничные устройства указывают в несущих пакетах свои адреса, а не адреса узлов в сети назначения.



Туннелирование трафика Frame Relay через IP-сеть

Согласование транспортных протоколов

Туннель может быть использован, когда две сети с одной транспортной технологией необходимо соединить через сеть, использующую другую транспортную технологию. При этом пограничные маршрутизаторы, которые подключают объединяемые сети к транзитной, упаковывают пакеты транспортного протокола объединяемых сетей в пакеты транспортного протокола транзитной сети. Второй пограничный маршрутизатор выполняет обратную операцию.

Обычно туннелирование приводит к более простым и быстрым решениям по сравнению с трансляцией, так как решает более частную задачу, не обеспечивая взаимодействия с узлами транзитной сети.

Основные компоненты туннеля

Основными компонентами туннеля являются:

1)инициатор туннеля;

2)маршрутизируемая сеть;

3)туннельный коммутатор;

4)один или несколько туннельных терминаторов.

Инициатор туннеля встраивает пакеты в новый пакет, содержащий наряду с исходными данными новый заголовок с информацией об отправителе и получателе. Несмотря на то, что все передаваемые по туннелю пакеты являются пакетами IP, инкапсулируемые пакеты могут принадлежать к протоколу любого типа, включая пакеты немаршрутизируемых протоколов. Маршрут между инициатором и терминатором туннеля определяет обычная маршрутизируемая сеть IP, которая может быть и сетью, отличной от Internet. Терминатор туннеля выполняет процесс, который является обратным инкапсуляции — он удаляет новые заголовки и направляет каждый исходный пакет в локальный стек протоколов или адресату в локальной сети. Инкапсуляция сама по себе никак не влияет на защищенность пакетов сообщений, передаваемых по туннелю VPN. Но инкапсуляция даёт возможность полной криптографической защиты инкапсулируемых пакетов. Конфиденциальность инкапсулируемых пакетов обеспечивается путём их криптографического закрытия, т. е. зашифровывания, а целостность и подлинность — путём формирования цифровой подписи. Так как существует множество методов криптозащиты данных, необходимо чтобы инициатор и терминатор туннеля использовали одни и те же методы и могли согласовывать друг с другом эту информацию. Более того, для возможности расшифровывания данных и проверки цифровой подписи при приеме инициатор и терминатор туннеля должны поддерживать функции безопасного обмена ключами. Чтобы туннели VPN создавались только между уполномоченными пользователями, конечные стороны взаимодействия требуется аутентифицировать.