

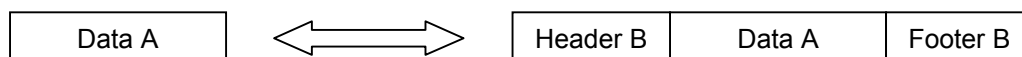
Введение в архитектуру маршрутизаторов NSG

1. Иерархическая архитектура протоколов в устройствах NSG

Продукты компании NSG, относящиеся к сериям NPS-7e, NSG-500, NX-300 и NSG-800 — мультипротокольные маршрутизаторы и коммутаторы для сетей с коммутацией пакетов, обеспечивающие маршрутизацию пакетов IP, коммутацию пакетов Frame Relay и X.25, статическую коммутацию различных видов трафика, и многочисленные виды инкапсуляции трафика между этими и другими протоколами. Для организации потоков трафика в устройствах используется ряд промежуточных объектов, передающих пакеты от физических интерфейсов к модулям коммутации и маршрутизации и обратно. Иерархическая архитектура протоколов, используемая в продуктах NSG, представлена на рис. 1. Она основана на многоуровневой модели, аналогичной модели OSI, и представляет собой комбинацию протокольных стеков TCP/IP, X.25 и Frame Relay. На рисунке использованы следующие обозначения:

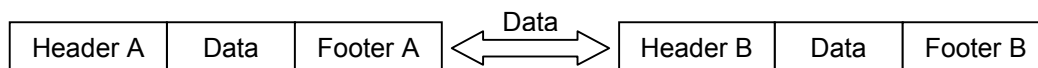
A — B Передача данных между объектами A и B без дополнительных преобразований.

A → B Инкапсуляция трафика A в пакеты протокола B. При передаче данных от объекта A к объекту B к пакетам A присоединяются заголовок и окончание, предписанные протоколом B; если трафик A представляет собой неструктурированный поток, или размер пакетов A несовместим с форматом B, то предварительно производится его разбиение или переразбиение на протокольные блоки данных (PDU) формата B. При передаче данных от объекта B к объекту A производится обратное преобразование, т.е. удаление заголовка и окончания пакета B.



A ↔ B

Преобразователь протоколов (шлюз) трафика между форматами пакетов A и B. При передаче данных от объекта A к объекту B из пакетов A извлекаются протокольные блоки данных (PDU), к которым присоединяются заголовок и окончание формата B. При передаче данных от объекта B к объекту A производится обратное преобразование. В общем случае длины PDU обоих пакетов могут не совпадать; это означает, что данные, извлеченные из одного пакета, сегментируются, объединяются или переразбиваются на блоки, соответствующие формату другого пакета.



В простейшем случае трафик, поступающий на физические интерфейсы, последовательно передается с низших уровней протокольной иерархии на высшие, по пути освобождаясь от заголовков и окончаний нижних уровней — вплоть до уровня, на котором происходит его коммутация или маршрутизация. Основные задачи данных устройств решаются, как правило, на третьем уровне: IP-маршрутизация, коммутация X.25, статическая IP-коммутация. Для этой цели используются таблицы коммутации, статической и динамической маршрутизации. Однако часть задач может решаться и на других уровнях. Например, коммутация служб Telnet с последовательным портом, к которому подключено асинхронное устройство, производится на прикладном уровне, а коммутация Frame Relay — на канальном. После коммутации или маршрутизации трафик передается по иерархической лестнице в обратном направлении, "сверху вниз", по пути претерпевая инкапсуляцию в пакеты нижних уровней.

Сетевой администратор может определять различные пути передачи трафика между объектами одного или разных протокольных стеков, одного или различных уровней, в частности:

- Инкапсуляцию в пакеты протокола нижележащего уровня, "родного" для данного стека (например, пакетов IP в пакеты Ethernet).
- Инкапсуляцию в пакеты протокола того же или нижележащего уровня, относящегося к другому стеку (например, пакетов X.25 в пакеты Frame Relay).
- Передачу пакетов на верхний уровень другого протокольного стека, где они рассматриваются в качестве пользовательских данных и последовательно обрабатываются всеми уровнями данного стека (например, пакетов IP в сеть X.25).

Именно для этой цели предназначены различные вспомогательные объекты, и этим объясняется определенная сложность самих устройств и многовариантность их конфигурирования. Поэтому в данной части руководства основное внимание уделено протокольной архитектуре устройств, объясняющей многие особенности их настройки и эксплуатации.

1.1. Прикладной уровень

Простейшим типом данных, передаваемых внутри устройства, является неструктурированный поток байтов. В общем случае это может быть и структурированный поток, если заголовки и окончания кадров рассматриваются с точки зрения последующих преобразований как обычные данные.

Для передачи по сетям с пакетной коммутацией пользовательский трафик должен быть, в первую очередь, разделен на пакеты. В сетях X.25 для этой цели используется процедура сборки-разборки пакетов (Packet Assembler/Disassembler, PAD), определенная протоколами X.3/X.28/X.29. Далее пользовательские пакеты направляются на третий уровень стека X.25.

В сетях IP аналогичное преобразование выполняется службами Telnet. Однако в этом случае задача допускает больше вариантов, которые реализуются при помощи дополнительных объектов — *станций*.

ОПРЕДЕЛЕНИЕ Станция — вспомогательный программный модуль, предназначенный для объединения и перенаправления потоков данных, с выполнением дополнительной инкапсуляции или без нее.

К серверу Telnet подключаются несколько станций, каждая из которых имеет один из двух типов:

ASYNС Прозрачным образом передает данные между сервером Telnet и другими асинхронными объектами. Таким объектом может быть асинхронный порт RS-232 или Frame Relay-станция типа ASYNС.

PAD Работает как шлюз между сетями IP и X.25. При передаче из сети IP в сеть X.25 данные извлекаются из пакетов Telnet, собираются в неструктурированный поток внутри станции, а затем разбиваются на пакеты X.25. При передаче из сети X.25 в сеть IP выполняется обратное преобразование.

Выбор станции может производиться по номерам портов TCP, если они определены в процессе конфигурации уникальными для каждой станции (или для групп однородных станций).

Клиент Telnet предназначен для более ограниченной задачи, а именно, для обслуживания пользователей сети X.25. По этой причине он не использует станции и всегда выполняет преобразование данных из пакетов X.25 в Telnet и обратно.

Помимо служб Telnet, на прикладном уровне стека TCP/IP выполняется еще ряд задач, генерирующих пакеты соответствующих прикладных протоколов. (Например, Web-сервер, предназначенный для управления устройством с помощью Web-браузера, генерирует пакеты протокола HTTP.) Все эти пакеты передаются на транспортный и сетевой уровень стека TCP/IP.

На прикладном уровне стека X.25 функционируют четыре служебных процесса: Manager, Traffic Generator, Echo Port и трассировщик портов. (В документации NSG они прежде именовались "логическими портами", однако ныне этот термин используется в другом смысле.) Их пакеты попадают непосредственно на третий уровень X.25. Manager обеспечивает управление устройством в режиме командной строки; остальные три процесса служат для отладки сети.

1.2. Сетевой уровень

Третий уровень протокольной архитектуры NSG формально соответствует пакетному уровню стека X.25, транспортному уровню и уровню межсетевому взаимодействию в стеке TCP/IP, транспортному и сетевому уровням в модели OSI.

Пакеты прикладных протоколов TCP/IP на этом уровне пакуются сначала в пакеты TCP, UDP либо ICMP, а затем — в пакеты IP. Именно на этом уровне производится основная обработка IP-трафика — маршрутизация, трансляция сетевых адресов, фильтрация и учет пакетов. Далее пакеты IP направляются на IP-интерфейсы маршрутизатора, инкапсулирующие их в различные протоколы канального уровня.

Начиная с версии 8.0.0b, IP-интерфейсам любого типа могут назначаться, помимо основного IP-адреса, вторичные адреса (*aliases*). Таким образом, в рамках одной физической сети можно создать несколько логических подсетей с непересекающимися диапазонами IP-адресов.

На третий уровень стека X.25 поступают пользовательские пакеты X.25 от портов и Telnet-станций типа PAD, а также от других источников: Telnet-клиента, прикладных процессов X.25, IP-интерфейсов типа PPP и X.25, Frame Relay-станций типа FRX, сервера X.25-over-X.25 (ХоХ). Они инкапсулируются в пакеты третьего уровня X.25 и направляются в коммутатор. Далее эти пакеты могут быть переданы:

- Канальному уровню X.25.
- Третьему уровню стека TCP/IP для инкапсуляции в пакеты TCP (технология X.25-over-TCP/IP, ХОТ).
- Станциям ХоХ. Эти станции возвращают их на третий уровень стека X.25 в качестве данных для повторной инкапсуляции. Это фирменная технология, совместимая только с продуктами NSG.

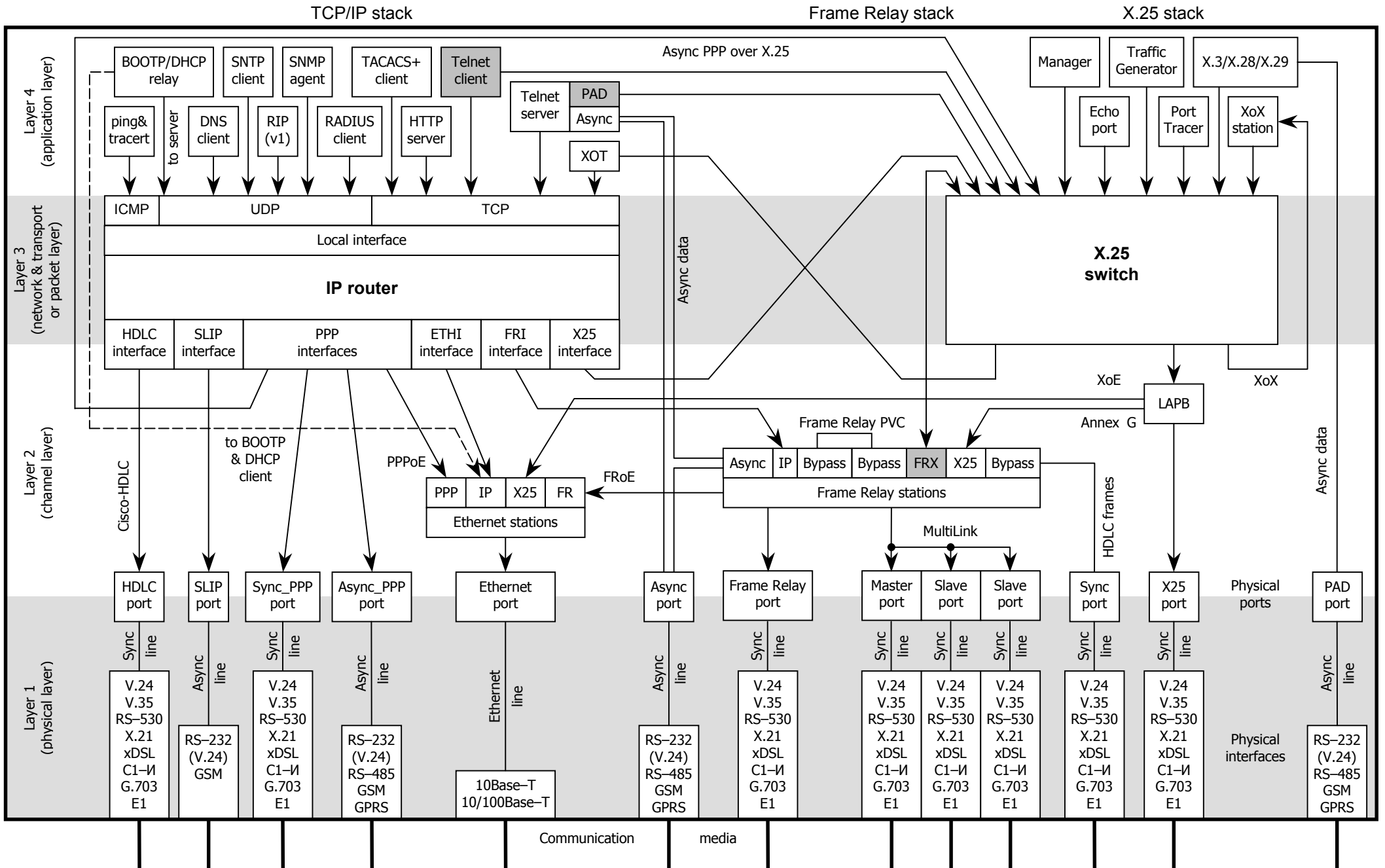


Рис. 1. ИЕРАРХИЧЕСКАЯ АРХИТЕКТУРА ПРОТОКОЛОВ В УСТРОЙСТВАХ NSG

1.3. Канальный уровень TCP/IP

На канальном уровне стека TCP/IP определен обширный набор объектов, позволяющих осуществить различные типы инкапсуляции. К ним относятся IP-интерфейсы, Ethernet-станции и физические порты.

ОПРЕДЕЛЕНИЕ IP-интерфейс — программный модуль, предназначенный для инкапсуляции пакетов IP в протоколы канального уровня либо в пользовательские пакеты X.25.

ОПРЕДЕЛЕНИЕ Физический порт — программно-аппаратный модуль, предназначенный для инкапсуляции данных канального уровня в данные физического уровня.

Для физических портов определяется протокол канального уровня, который используется вышестоящими программными объектами. В документации NSG он также называется *первичным протоколом* порта. Каждый порт идентифицируется уникальным номером (от 0 до максимального для данной модели), который используется при конфигурации самого порта и связывании его с другими программными объектами.

Каждый IP-интерфейс относится к одному из следующих типов:

PPP	Инкапсулирует пакеты IP в пакеты PPP и передает их одному из следующих объектов: — Физическому порту типа SYNC_PPP — Физическому порту типа ASYNC_PPP — Ethernet-станции типа PPP — Третьему уровню стека X.25 (в виде пользовательских пакетов).
SLIP	Инкапсулирует пакеты IP в пакеты SLIP и передает их физическому порту типа SLIP.
HDLC	Инкапсулирует пакеты IP в пакеты Cisco-HDLC и передает их физическому порту типа HDLC.
ETHI	Инкапсулирует пакеты IP в пакеты Ethernet и передает их Ethernet-станции типа IP.
FRI	Инкапсулирует пакеты IP в кадры Frame Relay и передает их Frame Relay-станции типа IP.
X25	Инкапсулирует пакеты IP в пользовательские пакеты X.25 и передает их на третий уровень стека X.25.

Помимо этого, в IP-маршрутизаторе определен формальный объект, называемый *локальным интерфейсом*. Он используется для конфигурации общих параметров, относящихся ко всему маршрутизатору.

Каждый IP-интерфейс типа SLIP, HDLC, ETHI или FRI в процессе настройки должен быть связан с одним и только одним портом или станцией соответствующего типа. Каждому IP-интерфейсу типа X25 соответствует один логический канал X.25, который может быть установлен либо динамически (при помощи коммутатора X.25), либо статически (при помощи постоянных виртуальных соединений). Интерфейс типа PPP может быть связан с фиксированным портом, либо динамически связываться с портом, Ethernet-станцией или логическим каналом X.25.

Каждый физический порт типа SYNC_PPP, ASYNC_PPP, SLIP или HDLC обслуживает один и только один IP-интерфейс соответствующего типа.

1.4. Канальный уровень Ethernet

Функции канального уровня Ethernet реализованы в устройствах NSG в виде виртуальных объектов — станций. Помимо традиционного IP-трафика, эти станции позволяют передавать по сети Ethernet трафик PPP (стандартная инкапсуляция PPPoE), а также, что является особенностью продуктов NSG, трафик X.25 и Frame Relay. Для этих целей определены, соответственно, четыре типа Ethernet-станций:

IP	Передают трафик IP. Каждый IP-интерфейс типа ETHI должен быть привязан к одной из станций этого типа. Станция типа IP может обслуживать только один IP-интерфейс.
PPP	Реализуют функции сервера PPP-over-Ethernet (PPPoE). Станции позволяют удаленным клиентам PPPoE подключаться к IP-интерфейсам маршрутизатора типа PPP. Основное назначение этой технологии состоит в аутентификации клиентов средствами протокола PPP, т.е. PAP или CHAP. Станция типа PPP использует по одному IP-интерфейсу типа PPP для каждого подключенного клиента.
X25	Передают по сети Ethernet трафик второго уровня X.25, упакованный в пакеты протокола LAPB. По своим функциям каждая такая станция аналогична синхронному порту X.25, однако средой передачи для нее является не синхронное физическое соединение WAN, а логическое соединение "точка-точка" через сеть Ethernet со станцией на другом устройстве NSG.
FR	Передают по сети Ethernet трафик Frame Relay. Как и Ethernet-станции типа X25, станции этого типа, с точки зрения вышестоящих протоколов, аналогичны физическим синхронным портам WAN (в данном случае — типа Frame Relay). Подробнее о технологиях XoE и FRoE см. ниже.

При конфигурировании Ethernet-станции она должна быть связана с портом Ethernet. Каждый порт Ethernet может обслуживать не более чем одну станцию типа IP, одну станцию типа PPP и несколько станций типа X25 и/или FR одновременно. Все эти станции имеют один MAC-адрес.

1.5. Канальный уровень X.25

Пакеты, выходящие из коммутатора X.25 на канальный уровень, могут быть переданы следующим объектам:

- Физическому порту типа X25
- Ethernet-станции типа X25; этот вид инкапсуляции называется X.25-over-Ethernet (XoE) и поддерживается только устройствами NSG.
- Frame Relay-станции типа X25; этот вид инкапсуляции определен спецификацией ANSI T1.617a Annex_G и совместим с продукцией других производителей.

Во всех этих случаях пакеты третьего уровня X.25 предварительно инкапсулируются в кадры LAPB. Таким образом, логические каналы X.25 прокладываются либо по физическим соединениям сети X.25, либо поверх транспортной сети Ethernet или Frame Relay. С точки зрения сетевой архитектуры X.25, оба типа станций полностью эквивалентны физическим портам.

1.6. Канальный уровень Frame Relay

Протокольный стек Frame Relay, как и Ethernet, представлен станциями. Каждая станция служит входом в определенный виртуальный канал (Data Link Channel). Канал определяется номером физического порта (типа Frame Relay) и идентификатором DLC (DLCI) на этом порту. Каждая станция относится к одному из следующих типов:

- | | |
|--------|---|
| IP | Передает по виртуальному каналу IP-пакеты, которые могут рассматриваться процессами IP-маршрутизации. Станция этого типа является транспортной средой для соответствующего IP-интерфейса. |
| ASYNC | Используется для передачи асинхронного потока данных по виртуальному каналу Frame Relay. Станции этого типа должны быть скомутированы (посредством PVC) с другим асинхронным объектом — портом, станцией Telnet или Frame Relay типа ASYNC. |
| BYPASS | Передает весь трафик, содержащийся в кадрах Frame Relay, прозрачным образом. Используется для коммутации (посредством PVC) двух виртуальных каналов Frame Relay. Кроме того, станции этого типа могут быть скомутированы с портом типа SYNC, через который передаются данные, инкапсулированные в кадры HDLC. |
| X25 | Устанавливает соединение X.25 через сеть Frame Relay (ANSI T1.617a Annex G). |
| FRX | Передает по виртуальному каналу Frame Relay данные, полученные из логического канала X.25, и наоборот. Это фирменная технология, совместимая только с продуктами NSG. |

Каждая станция Frame Relay при конфигурировании должна быть связана с одним и только одним портом Frame Relay, либо с Ethernet-станцией типа FR. Таким образом, транспортом для нее может быть либо физическое соединение WAN, либо логическое соединение "точка-точка" между двумя станциями через сеть Ethernet. Инкапсуляция Frame Relay-over-Ethernet (FRoE), как и X.25-over-Ethernet, является фирменной разработкой NSG. Физический порт или Ethernet-станция типа FR может обслуживать одну или несколько станций Frame Relay одинакового или различных типов.

Каждая станция типа IP, ASYNC, BYPASS или FRX передает один и только один поток данных. Станция типа X25 может содержать несколько логических каналов X.25, передаваемых по одному виртуальному каналу Frame Relay.

Несколько физических портов Frame Relay могут быть объединены на канальном уровне в одно целое при помощи фирменной технологии NSG MultiLink Frame Relay. Такой подход позволяет обеспечить требуемую скорость и надежность за счет количества параллельных линий связи в тех случаях, когда это не удается сделать из-за их качества.

1.7. Физический уровень

ОПРЕДЕЛЕНИЕ Физический порт — программно-аппаратный модуль, предназначенный для инкапсуляции данных канального уровня в данные физического уровня.

ОПРЕДЕЛЕНИЕ Физический интерфейс — аппаратный модуль, преобразующий данные физического уровня в формат, используемый внешней средой передачи.

Каждый физический порт оснащен физическим интерфейсом и представлен одним разъемом на корпусе устройства. Внешней средой передачи, в зависимости от типа интерфейса, может быть многожильный кабель для последовательных интерфейсов, одно- или двухпарный медный кабель, либо витая пара UTP5/STP1.

Таким образом, каждый порт характеризуется, с одной стороны, протоколом канального уровня, а с другой — типом используемого физического интерфейса. Те и другие могут быть разделены на три существенно разные группы:

Асинхронные	Предполагают передачу информации в старт-стопном режиме и включают порты следующих типов: ASYNC, ASYNC_PPP, SLIP, PAD. В качестве физического интерфейса используется V.24 (RS-232) либо RS-485.
Синхронные	Предполагают передачу информации в бит-синхронном режиме и включают порты следующих типов: SYNC_PPP, HDLC, Frame Relay, X25, SYNC, LOOPBACK. В качестве физических интерфейсов могут использоваться синхронные интерфейсы DTE/DCE (V.24, V.35, RS-530, X.21), модемные интерфейсы xDSL, интерфейсы систем цифровой иерархии G.703 и G.703.1. Особым случаем являются физические интерфейсы, способные передавать несколько независимых каналов данных — такие как E1. Каждый такой канал оканчивается собственным суб-интерфейсом. Со стороны канального уровня он представлен логическим портом WAN. Такой порт, с точки зрения вышестоящих протоколов, эквивалентен физическому и может иметь любой из вышеперечисленных синхронных типов. Создание суб-интерфейсов и их коммутация с логическими портами представляет собой отдельную задачу, решаемую на аппаратном уровне (см. ниже).
Ethernet	Предполагают широкополосную среду передачи Ethernet. Порт может иметь только тип Ethernet (ETH), физические интерфейсы — Ethernet 10Base-T и 10/100Base-T для витой медной пары категории 5.

В рамках сложившейся терминологии и синтаксиса команд NSG тип порта обозначается, как правило, по названию протокола канального уровня. В пределах одной группы любой тип порта может сочетаться с любым физическим интерфейсом. Канальные протоколы и физические интерфейсы из разных групп несовместимы (за исключением протокола PPP и физических интерфейсов V.24, которые могут использоваться как в синхронном, так и в асинхронном режиме).

Большинство физических интерфейсов в устройствах NSG выполнено в виде сменных аппаратных модулей; синхронные порты поддерживают, при установке соответствующих интерфейсных модулей, также и асинхронный режим, а также, в ряде устройств, режим Ethernet. Поэтому такие порты часто называются в документации NSG *универсальными портами* WAN или WAN/LAN. Не универсальными являются только порты с фиксированными интерфейсами определенных типов: RS-232 (с разъемами RJ-45 либо DBH-62), Ethernet, E1, а также консольный порт.

Выделенный *консольный порт* предназначен для управления устройством в режиме асинхронного терминала. С аппаратной и программной точек зрения, он представляет собой обычный асинхронный порт RS-232 типа PAD и отличается от остальных портов тем, что скомутирован с программным модулем Manager при включении устройства: в нормальном режиме работы — по умолчанию, при выполнении процедуры "холодный старт" — всегда.

Консольный порт может использоваться и для обмена данными, а управление при этом возможно при помощи удаленного PAD, клиента Telnet, Web-интерфейса или SNMP. Однако, в зависимости от модели устройства, он может иметь определенные аппаратные и программные ограничения (отсутствие сигнальных линий, поддержки других асинхронных протоколов, попеременная работа с одним из основных интерфейсов).

1.8. Многоканальные физические интерфейсы

Определенные типы физических интерфейсов, использующие технологию мультиплексирования по времени (TDM) или ATM, способны поддерживать несколько независимых потоков трафика (каналов). Так, для интерфейса E1 можно организовать до 31 независимого канала данных по 64 Кбит/с, если каждому из них назначить отдельный канальный интервал (таймслот) или группу канальных интервалов. В системах xDSL с инкапсуляцией трафика в ячейки ATM (в настоящее время устройствами NSG не поддерживается) можно создать на одном физическом соединении несколько виртуальных каналов ATM (Virtual Connection Circuit, VCC) с одинаковыми или различными характеристиками. (См. рис. 2.)

Все многоканальные интерфейсы — как TDM, так и ATM — реализуют, в более или менее полном объеме, коммутацию канальных интервалов E1 или ячеек ATM. Эта коммутация производится средствами самого интерфейсного модуля и аппаратного коммутатора; она никак не связана с протоколами вышестоящих уровней и не занимает ресурсов центрального процессора. Поэтому с точки зрения общей архитектуры устройства можно считать, что она относится исключительно к физическому уровню. Коммутатор может, в зависимости от конструкции конкретного устройства, располагаться на плате интерфейсного модуля, на материнской плате, или представлять собой отдельный модуль.

Коммутатор выделяет из общего потока физического уровня индивидуальные каналы, называемые также *суб-интерфейсами*. Для интерфейса E1 такой суб-интерфейс представляет собой совокупность заданных канальных интервалов (таймслотов); для интерфейса ATM — определенное виртуальное соединение ATM. Некоторые производители используют также термин "виртуальный порт WAN".

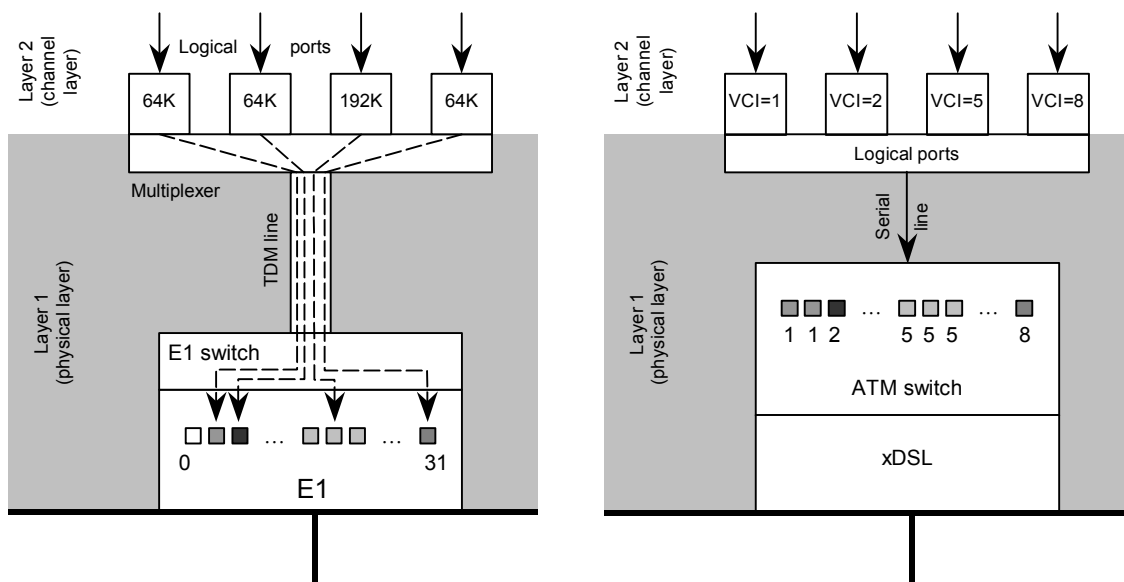


Рис. 2. Многоканальные интерфейсы E1 и ATM-over-xDSL

Если интерфейс использует для передачи данных только один суб-интерфейс (а остальной трафик игнорирует), то канальном уровне он представлен обычным физическим портом. Если же интерфейс истинно многоканальный, т.е. обрабатывает несколько независимых каналов данных, то на канальном уровне эти потоки представлены *логическими портами WAN*. Для объектов канального и вышестоящих уровней каждый такой порт полностью эквивалентен физическому. Но если физический порт однозначно связан с определенным физическим интерфейсом (одноканальным) или единственным суб-интерфейсом многоканального интерфейса, то логический порт соединяется с некоторым суб-интерфейсом в процессе настройки. Это вторая задача, решаемая коммутатором.

В общем случае, в зависимости от возможностей аппаратного коммутатора, может производиться произвольная коммутация трафика между несколькими физическими и логическими портами и несколькими суб-интерфейсами одного или разных физических интерфейсов — при условии, что они совместимы по типу трафика и быстродействию. Например, часть канальных интервалов интерфейса E1 может передаваться непосредственно в другой интерфейс E1, часть — на интерфейсы N×64 Кбит/с (V.35, G.703.1 и/или IDSL), часть — на логические порты для последующей программной обработки (рис. 3).

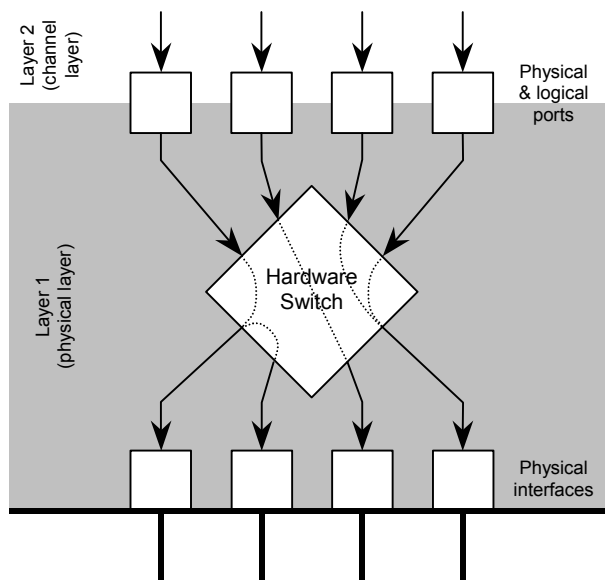


Рис. 3. Подсистема физического уровня с аппаратной коммутацией (общий случай)

Важная особенность коммутации на физическом уровне состоит в том, что она не зависит от трафика вышестоящих уровней и не связана с теми или иными протоколами, например, Frame Relay или X.25. Любые потоки данных, которые могут быть переданы в физический или логический порт, могут быть объединены на выходе одного физического интерфейса. Кроме того, технология TDM и, для определенных типов трафика, технология ATM обеспечивают гарантированную полосу пропускания для каждого логического порта.

Для интерфейсов, позволяющих выбирать число каналов данных и их внутреннюю структуру, в документации NSG используется термин *настраиваемые физические интерфейсы*.

2. Функциональная организация устройств NSG

С функциональной точки зрения, основными компонентами программного обеспечения NSG являются IP-маршрутизатор и коммутатор пакетов X.25. Каждый из них обслуживает свой тип трафика и имеет свой набор портов, станций и прикладных процессов. Подсистемы взаимодействуют друг с другом в той части работ, которая относится к передаче пакетов IP, PPP и трафика Telnet по сети X.25, а также пакетов X.25 по сети TCP/IP.

Кроме того, между различными программными модулями могут быть сконфигурированы постоянные виртуальные соединения (PVC). Коммутация с помощью PVC является основным инструментом для работы в сетях Frame Relay и в технологических системах с асинхронными последовательными интерфейсами.

Функциональная схема устройств NSG представлена на рис. 4. Она тесно связана с иерархической схемой, приведенной на рис. 1. Образно выражаясь, если рис. 1 показывает архитектуру устройств при виде «сбоку», то рис. 4 — это вид «в плане». Физический уровень не показан, чтобы не усложнять картину.

IP-маршрутизатор обеспечивает передачу пакетов IP как между своими интерфейсами, так и между прикладными процессами IP. При этом он может осуществлять трансляцию IP-адресов (NAT), фильтрацию пакетов и учет трафика по IP-адресам.

Коммутатор X.25 устанавливает *коммутируемые виртуальные каналы (SVC)* между следующими объектами:

- Портами и Telnet-станциями типа PAD
- Telnet-клиентом
- IP-интерфейсами типа PPP
- IP-интерфейсами типа X25
- Портами типа X25, станциями Ethernet и Frame Relay типа X25
- Служебными процессами: Manager, Echo Port, Traffic Generator, трассировщик портов
- Frame Relay-станциями типа FRX
- Соединениями X.25-over-TCP/IP (ХОТ)
- Станциями ХоХ
- Сервером (совокупностью станций) ХоХ

Обмен трафиком может осуществляться между любыми двумя из вышеперечисленных объектов, хотя отдельные частные случаи не представляют практического интереса. Исключениями являются следующие ситуации:

- IP-интерфейс типа PPP, Telnet-клиент и системные прикладные процессы Manager, Echo Port, Traffic Generator, трассировщик портов не могут инициировать установление SVC к другим объектам;
- IP-интерфейсы типа X25 не могут устанавливать соединения с вышеперечисленными "пассивными" объектами, а также с объектами типа PAD (физическими портами, Telnet-станциями).

Некоторые из вышеперечисленных объектов (например, порт типа PAD) могут содержать только один логический канал X.25, другие — несколько каналов. Коммутация, строго говоря, осуществляется не между объектами, а между каналами. Для одноканальных объектов эти понятия тождественны. Как частный случай, два канала одного объекта (например, порта типа X25) могут быть скомутированы друг на друга.

В процессе установки соединения коммутатор может, одновременно с маршрутизацией пакетов CALL, выполнять их фильтрацию и подстановку (трансляцию) сетевых адресов. В таблице маршрутизации выводов могут быть предусмотрены резервные маршруты, используемые, если соединение не может быть установлено по основному маршруту.

ПРИМЕЧАНИЕ Хотя для сетей X.25 основной процедурой является коммутация (передача пакетов по установленным логическим каналам), следует помнить, что на этапе установления соединения осуществляется не коммутация, а маршрутизация пакета CALL, т.е. определение дальнейшего маршрута, по которому следует послать этот пакет.

Коммутация при помощи *постоянных виртуальных каналов (PVC)* может осуществляться между любыми парами объектов с однотипным форматом данных, а именно:

- Между следующими объектами X.25:
 - Портами и Telnet-станциями типа PAD (кроме соединений с IP-интерфейсами типа X25)
 - Портами типа X25, станциями Ethernet и Frame Relay типа X25
 - IP-интерфейсами типа X25 (кроме соединений с портами и Telnet-станциями типа PAD)
 - Frame Relay-станциями типа FRX
 - Тремя служебными процессами: Manager, Echo Port, Traffic Generator (кроме соединений друг с другом)
- Между любыми двумя портами, станциями Telnet и/или Frame Relay типа ASYNC
- Между любыми двумя станциями Frame Relay типа BYPASS и/или портами типа SYNC

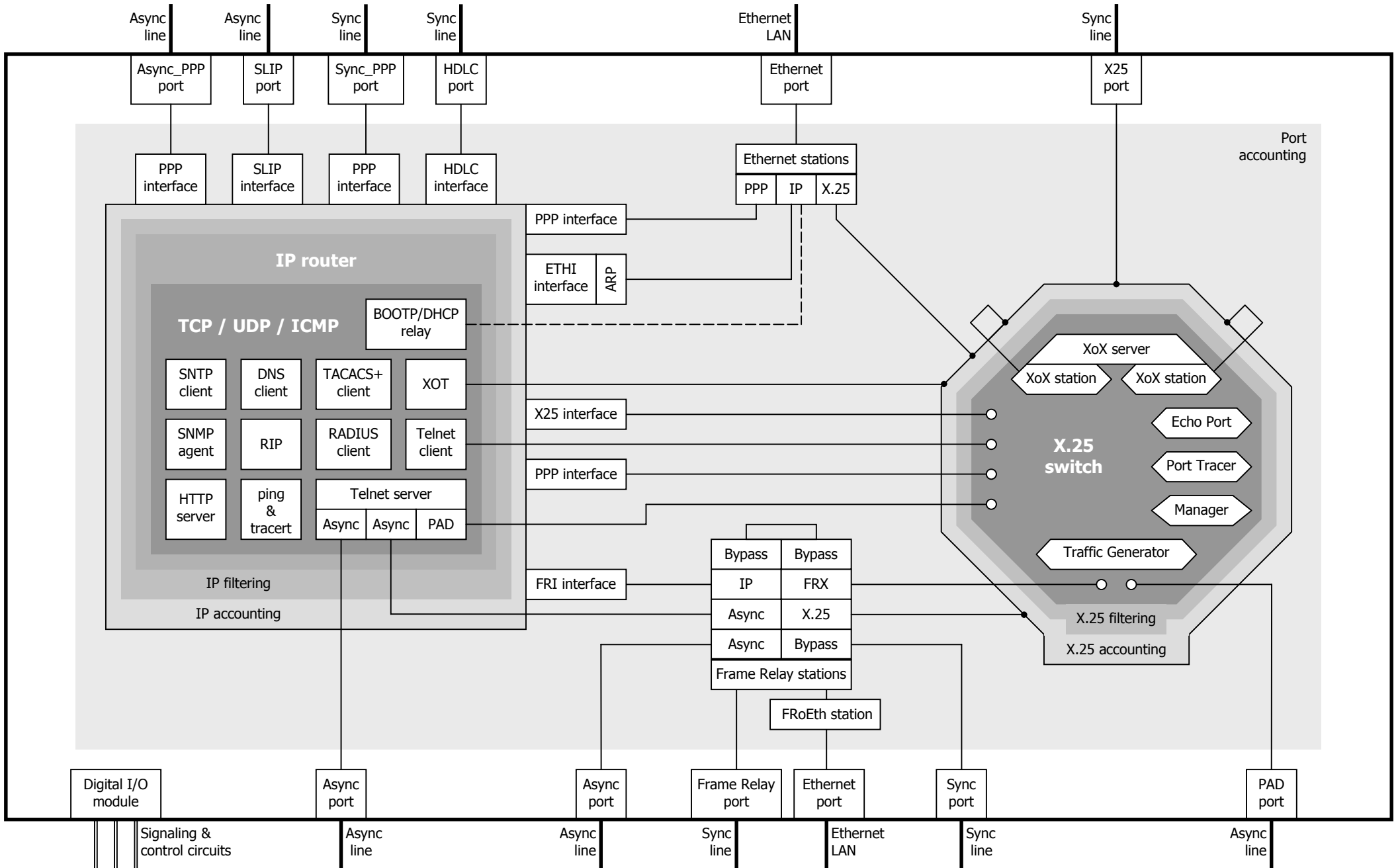


Рис. 4. Функциональные модули и подсистемы

Как IP-маршрутизатор, так и коммутатор X.25 окружены «оболочками» сбора статистики и фильтрации пакетов, а всё программное ядро канального, сетевого и прикладного уровней — аналогичной «оболочкой» для сбора статистики по портам. Они обрабатывают весь входящий и исходящий трафик в следующем порядке:

1. Учитываются все пакеты, входящие в физические и логические порты;
2. Учитываются все пакеты X.25, входящие в коммутатор из различных источников;
3. Все входящие пакеты IP и вызовы X.25 фильтруются при помощи заданного набора фильтров;
4. Производится маршрутизация пакетов IP, коммутация пакетов X.25 или передача пакетов X.25 по PVC;
5. Фильтруются все исходящие пакеты IP и вызовы X.25;
6. Учитываются все исходящие пакеты IP и X.25;
7. Учитываются все пакеты, исходящие через физические и логические порты.

Процедура фильтрации IP-пакетов допускает, помимо обычных действий «разрешить/запретить», еще и третий вариант — переслать пакет, попадающий под действие фильтра, на заданный интерфейс. Подробнее об этом варианте *статической IP-коммутации* см. ниже. При мультипротокольной обработке трафик фильтруется и обрабатывается как подсистемой IP, так и подсистемой X.25, в зависимости от используемых протоколов.

Служба ARP позволяет устанавливать фиксированные соответствия между IP- и MAC-адресами, а также удалять как статические, так и динамические записи из таблицы ARP. При отправке IP-пакетов по сети Ethernet статические записи имеют приоритет над динамическими. Возможен режим Proxu ARP, при котором в ответ на запрос ARP посылается MAC-адрес интерфейса маршрутизатора.

Ретранслятор BOOTP/DHCP принимает запросы от клиентов, находящихся в локальной сети Ethernet, и передает их серверу, доступному через IP-сеть. Ответы сервера возвращаются клиентам.

Клиент DNS позволяет устанавливать соответствия между символическими именами хостов IP-сети и их адресами, необходимые для работы локальных служб: выполнения процедур *ping*, *traceroute* и т.п. Помимо этого, заданные адреса серверов DNS могут передаваться удаленным клиентам PPP в процессе установления PPP-соединения.

Клиент SNTP (Simple Network Time Protocol) обеспечивает синхронизацию системного времени устройства с сетевым временем. В качестве эталона могут использоваться до четырех серверов SNTP.

Подсистема аутентификации и авторизации состоит из стандартных клиентов RADIUS, TACACS+ и модуля локальной аутентификации. Помимо аутентификации, она позволяет автоматически конфигурировать асинхронные порты для работы в режиме PAD или PPP согласно заданной таблице пользователей. Для сеансов PPP могут быть использованы протоколы аутентификации PAP и CHAP, причем в обоих случаях устройства NSG могут выступать как в качестве сервера, так и в качестве клиента. Аутентификация производится независимо от транспортной среды, использованной для передачи трафика PPP — будь то синхронное или асинхронное соединение WAN, сеть X.25 или локальная сеть Ethernet. Одновременно с аутентификацией пользователю PPP может быть назначен IP-адрес, а также включены фильтры.

Входящие и исходящие соединения могут устанавливаться вручную, автоматически при включении питания, или по требованию (т.е. при наличии данных для передачи по этому соединению).

В подсистему управления и диагностики входят модули Manager, Echo Port, Traffic Generator, трассировщик портов, Web-сервер и клиент SNMP. Доступ к модулю Manager может осуществляться через консольный порт, сервер Telnet, сеть X.25 либо Frame Relay.

Специфическое место в общей архитектуре устройства занимают модули дискретного ввода-вывода (DIO). Они не предназначены для передачи данных, а только замыкают внешние электрические цепи по командам от процессов управления, либо передают в эти процессы информацию о состоянии внешних цепей.

3. Фирменные технологии и методы NSG

Наряду с общеизвестными технологиями, которые определены соответствующими международными стандартами и поддерживаются аппаратурой многих производителей, в продуктах NSG реализован ряд фирменных решений и технологий. Они поддерживаются только устройствами NSG и могут применяться при наличии таких устройств на обеих сторонах соединения.

3.1. MultiLink Frame Relay

Технология MultiLink Frame Relay позволяет объединить несколько физических портов Frame Relay в одно целое на канальном уровне. В этом случае один из портов назначается ведущим (Master), остальные — ведомыми (Slave). Для вышестоящих объектов (станций) доступен только ведущий порт, но формальное быстродействие этого порта равно суммарному по всем объединенным портам; именно с этим портом должны быть связаны все станции, использующие данную группу каналов связи. Кроме того, при отказе одного из физических каналов передача продолжается по параллельным каналам и соединение не разрывается, пока действует хотя бы один канал. Максимальное число портов, объединенных в одну группу, программно не ограничено.

Порты могут иметь как одинаковое, так и различное быстродействие. Балансировка нагрузки производится автоматически по принципу равной длины очередей: чем быстрее порт отправляет данные в линию, тем быстрее планировщик очередей ставит в его очередь новые пакеты. Таким образом, если используемые каналы имеют различное быстродействие и/или различный процент ошибок, то суммарный объем трафика распределяется между ними приблизительно пропорционально фактической пропускной способности.

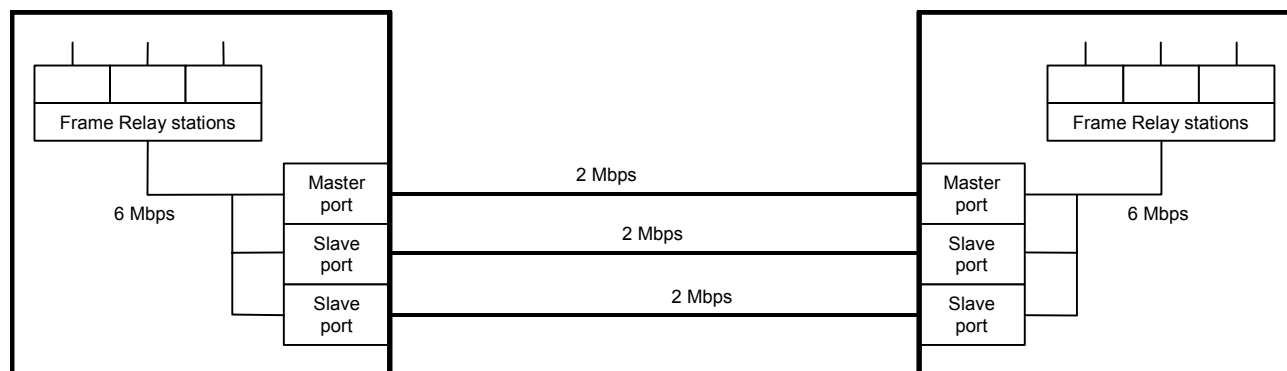


Рис. 5. Многоканальное соединение Frame Relay

Типичные применения технологии Frame Relay MultiLink включают:

- Высокоскоростное объединение локальных сетей на дальностях порядка нескольких километров. Применение многоканальных соединений позволяет заполнить эту нишу, специфическую для России и многих развивающихся стран. Она занимает промежуточное место между решениями VDSL (в т.ч. 4-проводными), практическая применимость которых сильно ограничена из-за малой дальности, и SDSL, SHDSL, быстродействие которых не всегда оказывается достаточным.

Это удобное решение для кампусных сетей, в особенности, для соединения офисов (например, центрального офиса и склада), расположенных на территориях промышленных предприятий и НИИ, которые были построены еще в советское время. Как правило, такие площадки обладают весьма густой и доступной, но низкокачественной кабельной инфраструктурой, изначально предназначенной для внутренней телефонной сети, а высокий уровень электромагнитного шума от работающего силового оборудования снижает дальность и быстродействие соединений еще более. Применение нескольких параллельных линий в этом случае оказывается самым простым и эффективным решением.

- Использование низкоскоростных каналов связи, например, физических междугородных телефонных линий, до сих пор сохранившихся в регионах России и стран СНГ. Объединение нескольких аналоговых (!) соединений на основе синхронных модемов позволяет на выходе предложить пользователю современную услугу цифровой сети со скоростью 64 Кбит/с или более.
- Инверсное мультиплексирование каналов цифровой иерархии — задача, актуальная не только для развивающихся стран, но и для территорий с развитой коммуникационной инфраструктурой. Объединение нескольких каналов с быстродействием 2 Мбит/с позволяет заполнить весьма существенный технологический и экономический разрыв между услугами E1 и E3 (точнее, между каналами G.703 со скоростью 2 и 34 Мбит/с), из которых первая оказывается недостаточной, а вторая — чрезмерно дорогостоящей. В силу быстрого увеличения доступности и снижения стоимости каналов E1, такое решение становится все более актуальным для корпоративных пользователей во многих странах мира.

3.2. X.25-over-Ethernet и Frame Relay-over-Ethernet

Технологии X.25-over-Ethernet (XoE) и Frame Relay-over-Ethernet позволяют трафик сетей X.25 и Frame Relay, соответственно, между двумя или более устройствами NSG по локальной сети Ethernet. Для этой цели на каждом устройстве создаются Ethernet-станции типа X25 или FR, соответственно; в конфигурации каждой станции указывается MAC-адрес парной к ней станции на удаленном устройстве. Логическое соединение между этими станциями полностью эквивалентно, с точки зрения протоколов X.25 и Frame Relay, физическому соединению “точка-точка”, а сами эти станции — физическим портам. Пример использования технологии XoE приведен на рис. 6. На всех локальных устройствах создано по одной станции, а на устройстве, подключенном к глобальной сети — парные станции для каждого из остальных устройств.

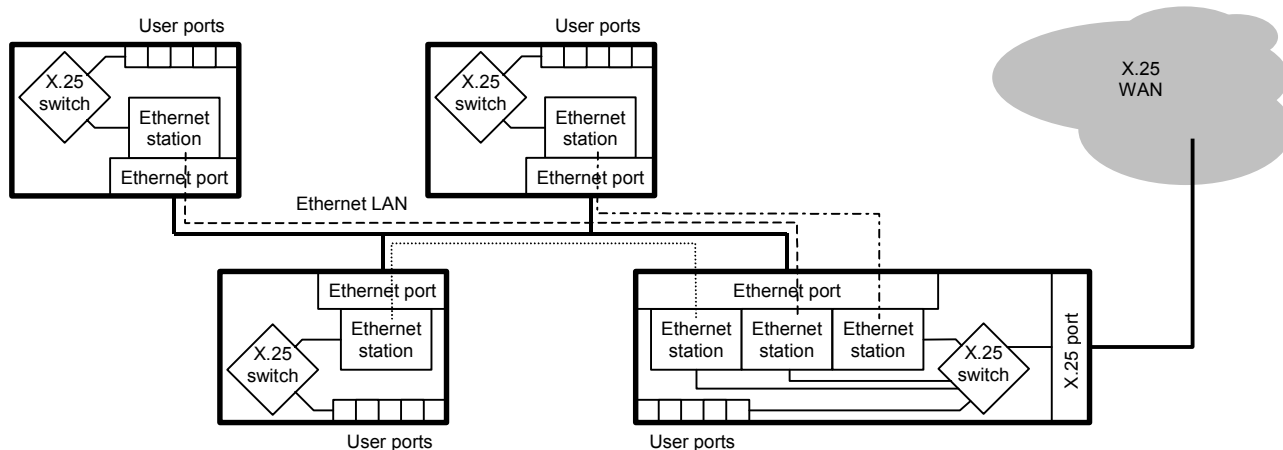


Рис. 6. Многопортовый узел доступа X.25-over-Ethernet

Использование этих технологий позволяет решить ряд практических задач, в частности:

- Каскадировать устройства NSG, используя в качестве шины локальную сеть Ethernet, для увеличения числа портов при массовом подключении терминального оборудования (см. рис. 6). При этом достигается значительная экономия дорогостоящих портов коммутатора: если при традиционном последовательном подключении требуется 2 порта на каждое дополнительное устройство, то при использовании XoE — один.
- Аналогичным образом каскадировать устройства NSG для построения многопортовых узлов коммутации пакетов. Схема такого узла, составленного из пяти устройств NX-300/7WL и насчитывающего, в общей сложности, 35 портов WAN, приведена на рис. 7. Сеть Frame Relay-over-Ethernet между коммутаторами имеет полносвязную топологию, т.е. каждое устройство соединено с каждым. (Любопытно заметить, что при этом сама сеть Ethernet 10Base-T имеет логическую топологию "шина" и физическую топологию "звезда".)

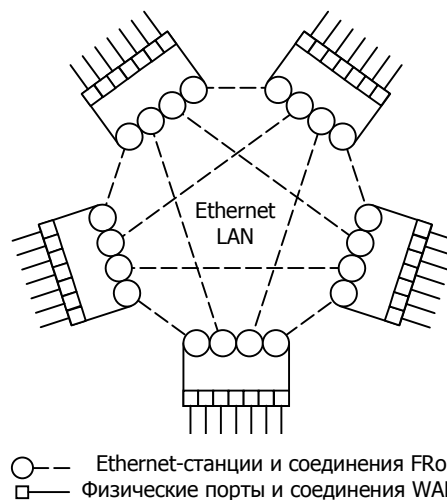


Рис. 7. Узел коммутации Frame Relay на 35 портов

- Создавать распределенные системы, например, размещать сеть банкоматов и POS-терминалов в пределах крупного здания или комплекса зданий (супермаркета, делового центра, аэропорта и т.п.). Использование транспорта Ethernet позволяет создавать системы диаметром до нескольких сотен метров, что в большинстве случаев нереально при использовании обычных последовательных интерфейсов (V.35, X.21, RS-530 и т.п.); с другой стороны, оно оказывается значительно дешевле выделенных модемных интерфейсов. Кроме того, прокладка кабельной сети Ethernet с практической точки зрения существенно проще, удобнее и дешевле, чем многожильных кабелей для последовательных интерфейсов.
- Транслировать трафик сетей X.25 и Frame Relay через городские сети Ethernet (радио, волоконно-оптические и т.п.) и широкополосные системы местного доступа (ADSL/SDSL/SHDSL, кабельные модемы, оптические мосты прямой видимости и т.п.) — в общем случае, через любое оборудование, оснащенное портами Ethernet.

ПРИМЕЧАНИЕ При передаче трафика Frame Relay необходимо учитывать, что длина пакетов Frame Relay может оказаться больше, чем максимальная длина пакета Ethernet. Чтобы избежать ошибок при передаче, следует ограничить длину пакетов Frame Relay на конечных узлах сети (при помощи параметра MTU или иного, в зависимости от характера трафика).

3.3. X.25-over-X.25

В качестве транспорта для сети X.25 может выступать сама сеть X.25. Для этой цели пакеты третьего уровня снова инкапсулируются, в качестве пользовательских данных, в пакеты третьего, а затем второго уровня. Это преобразование осуществляется станциями XoX. Соединение между двумя станциями XoX является *туннелем*, внутри которого может существовать одно или несколько вложенных соединений, которые передают пользовательские данные (или, в свою очередь, также могут являться туннелями). Такой подход позволяет решить несколько прикладных задач:

- Разрывать туннели между станциями при отсутствии трафика и восстанавливать их по требованию, не разрывая при этом вложенные логические соединения между узлами корпоративной сети. Это может обеспечить значительную экономию средств, если в качестве транспортной сети используется сеть X.25 общего пользования, а время фактического обмена данными (например, между банкоматом и процессинговым центром) невелико.
- Передавать трафик нескольких логических соединений по одному физическому соединению, не способному поддерживать более одного логического соединения (например, по асинхронной линии в режиме PAD–AntiPAD).
- Устанавливать большее число логических соединений, чем непосредственно допускается данной линией X.25.

Каждая станция может обслуживать несколько логических каналов; максимальное число каналов и станций программно не ограничено, но должно быть указано при настройке службы XoX. Для каждой станции устанавливается X.121 адрес парной к ней станции. Логическое соединение с этой станцией является особенным, поскольку именно внутри него прокладываются все остальные соединения. По отношению ко всем другим логическим каналам XoX-станция полностью эквивалентна порту X.25.

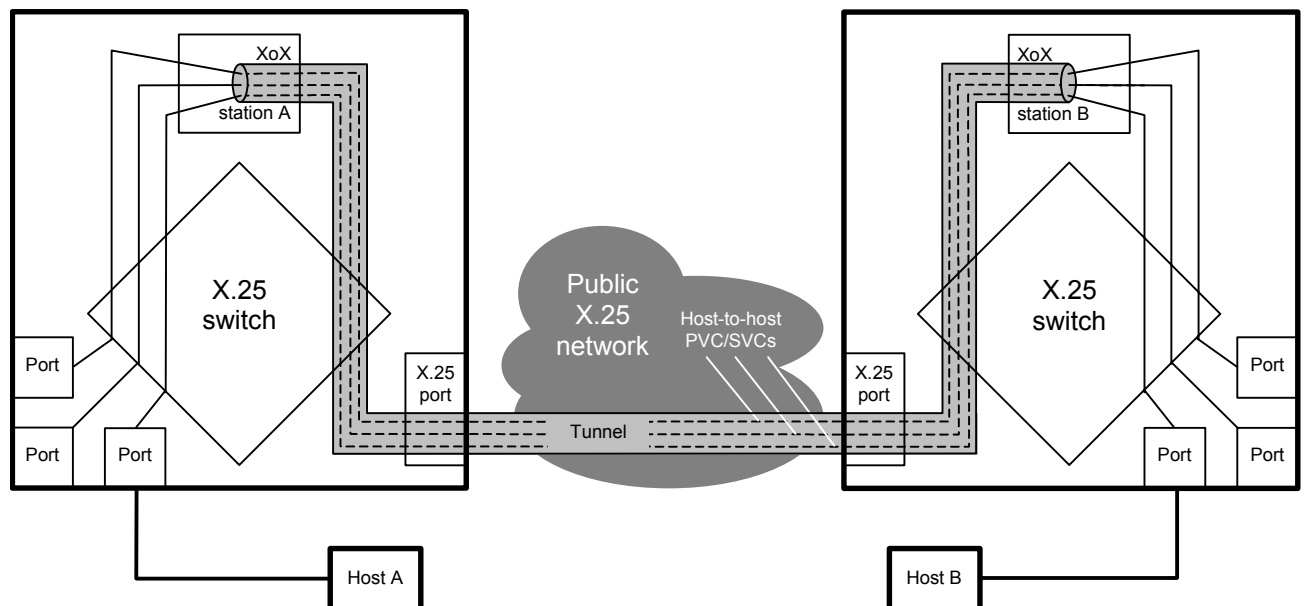


Рис. 8. Технология X.25-over-X.25

Пример применения технологии XoX приведен на рис. 8. Логическое соединение между хостами А и В (например, банкоматом и процессинговым центром) проходит внутри туннеля, установленного между двумя станциями XoX (на рисунке показан серым цветом). Последний проходит через сеть X.25 общего пользования с высокой повременной оплатой. Трафик между хостами невелик, однако специфика их программного обеспечения требует, чтобы соединение между ними поддерживалось постоянно.

В этом случае при длительном отсутствии активности во всех вложенных логических соединениях туннель между станциями может быть принудительно разорван. Это позволяет сэкономить значительные средства на оплату услуг оператора сети X.25. Конечные узлы при этом не получают никакой информации о разрыве соединения; с их точки зрения, связь поддерживается непрерывно — что и требуется. Если в одном из вложенных соединений возникает какой-либо трафик, например, узел А посылает пакет узлу В, то этот пакет задерживается на небольшое время на станции А; станция восстанавливает туннель до станции В и после этого передает ей пакет; станция В отправляет его по оставшейся части логического соединения между узлами. Если после этого трафик снова становится нулевым на длительное время в ожидании следующей транзакции, туннель между станциями снова может быть разорван.

Совокупность всех станций XoX называется сервером XoX; это вспомогательное понятие, используемое при настройке общих параметров для всех станций и при установлении туннелей.

3.4. Шлюз X.25/Frame Relay

Основное назначение этой технологии — обеспечение связи между хостами, подключенными к сети X.25 и к сети Frame Relay. Из пакетов X.25, приходящих на Frame Relay-станцию типа FRX, удаляются все заголовки второго и третьего уровней, а пользовательские данные инкапсулируются в пакет Frame Relay и передаются адресату по виртуальному соединению Frame Relay. Если пакеты приходят со стороны сети Frame Relay, то станция извлекает из них пользовательские данные и инкапсулирует их в пакет данных X.25. Этот пакет передается по логическому каналу в сети X.25 — либо существующему на данный момент, либо вновь установленному между станцией и заданным узлом.

Как можно видеть, станция типа FRX работает в качестве шлюза между сетями разных типов и является окончательным устройством для каждой из сетей. Как частные случаи, возможен обмен данными между двумя сетями X.25 через сеть Frame Relay или, наоборот, между двумя сетями Frame Relay через сеть X.25. В сочетании с другими возможностями устройств NSG возможны и более сложные решения, например, передача трафика Frame Relay *через* IP-сеть: Frame Relay-to-X.25-over-TCP/IP.

При использовании станций типа FRX необходимо помнить, что механизмы контроля ошибок и обеспечения целостности данных, имеющиеся в сети X.25, за пределами этой сети не действуют и, следовательно, надежность и устойчивость соединения ограничиваются возможностями сети Frame Relay; с другой стороны, быстродействие соединения, как правило, ограничивается сетью X.25. Кроме того, имеются ограничения, связанные с максимальной длиной пакета Frame Relay — 1600 байт.

3.5. Anti-PAD

Режим Anti-PAD предназначен для подключения терминальных устройств, оснащенных встроенными PAD, к сети, которая уже предлагает сервис PAD (и только PAD). Такая задача типична для случая постепенной модернизации или расширения парка терминального оборудования, когда радикальная перестройка сети в соответствии с особенностями новых терминалов невозможна или нецелесообразна, либо для подключения через сеть X.25 общего пользования. Порт, подключенный к устройству, конфигурируется для работы в режиме X.25, а порт, подключенный к сети — в режиме Anti-PAD.

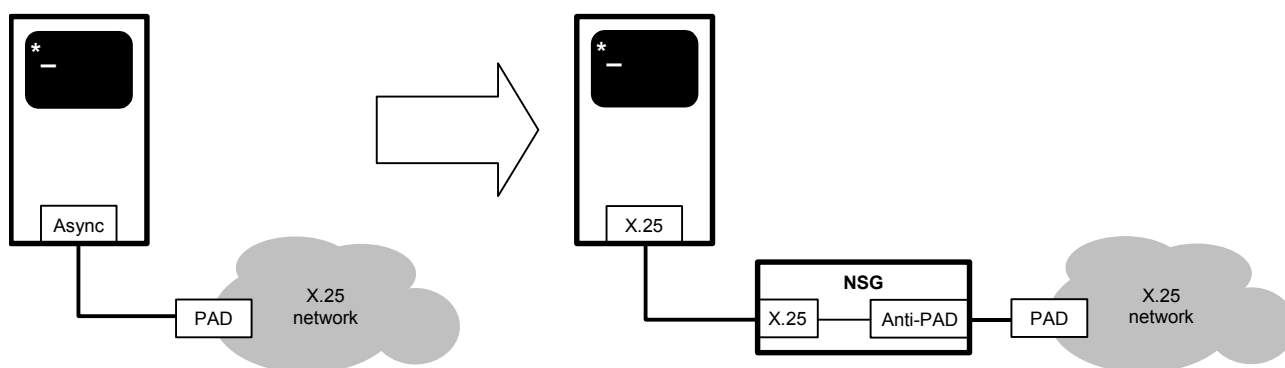


Рис. 9. Применение устройства Anti-PAD при модернизации терминального оборудования

В сочетании с технологией ХоХ этот режим позволяет решить и более сложную задачу, а именно, установить неограниченное число логических соединений X.25 по одной асинхронной линии, работающей в режиме PAD.

3.6. Multi-PAD

Режим Multi-PAD представляет собой расширение возможностей обычного PAD и позволяет передавать в сеть X.25 одновременно несколько неструктурированных потоков данных по одной асинхронной линии связи. Эти потоки разбиваются на пакеты при помощи фирменного протокола, построенного на основе SLIP. Протокол несложен в реализации и открыт для сторонних разработчиков. В заголовке каждого пакета содержится уникальный идентификатор, позволяющий определить, к какому из исходных потоков относится данный пакет. На стороне пользователя такое преобразование осуществляется заказным приложением, разработанным в соответствии с потребностями данного заказчика. На стороне сети устройство NSG разбирает входящий асинхронный трафик на отдельные потоки, преобразует их в пакеты X.25 согласно заданным профилям PAD, и передает в сеть. При этом для каждого из первоначальных потоков устанавливается свой логический канал X.25.

3.7. Статическая IP-коммутация

Термин "IP-коммутация" представляет собой весьма общее понятие, которое использовалось в разное время и разными производителями в различных, не связанных между собой значениях, поэтому следует уточнить его смысл применительно к продукции NSG.

ОПРЕДЕЛЕНИЕ В устройствах NSG и в данной документации статической IP-коммутацией называется пересылка пакетов с одного IP-интерфейса на другой по заданному набору правил.

По существу, статическая IP-коммутация представляет собой расширенный вариант фильтрации пакетов: помимо того, что входящий пакет может быть пропущен или заблокирован, он может быть направлен на заданный интерфейс. Некоторые производители используют для такого алгоритма термин *IP Bridging* или производные от него.

Правила коммутации, как и остальные фильтры, могут включать номер IP-интерфейса, с которого получен пакет, адрес источника и/или назначения, номера портов TCP/UDP и тип пакетов ICMP. Они входят в общую таблицу фильтров и рассматриваются наряду с остальными фильтрами, в порядке убывания приоритета. Таким образом, статическая IP-коммутация может рассматриваться и как вариант статической маршрутизации, осуществляемой не по IP-адресу назначения, а по иным вышеперечисленным критериям.

Правила коммутации являются односторонними, т.е. если установлено правило "пересылать пакеты с интерфейса А на интерфейс В", то оно никак не определяет пересылку пакетов, поступающих с интерфейса В. Для двусторонней коммутации интерфейсов необходимо установить два правила, определяющие передачу пакетов в том и другом направлениях.

Применение статической IP-коммутации, как правило, целесообразно только в том случае, если она определена согласованным образом на всех смежных устройствах сети. Однако в определенных ситуациях она может быть полезна и при использовании на одном устройстве. Например, трафик некоторой приоритетной подсети или хоста может быть направлен по отдельному виртуальному каналу Frame Relay или физическому каналу — более быстродействующему, надежному, или менее загруженному.

© ООО «Эн-Эс-Джи» 2002–2005

