IEN 178 April 1981

ADDRESSING PROBLEMS IN MULTI-NETWORK SYSTEMS

Проблемы адресации в многосетевых системах

Carl A. Sunshine

University of Southern California

Information Sciences Institute

4676 Admiralty Way

Marina del Rey, CA 90291

Оригинал

Аннотация

Чтобы пользователи из разных сетей могли взаимодействовать друг с другом, важно разработать мощные и практичные способы и средства именования, адресации и маршрутизации. Начали применяться базовые процедуры для многосетевых систем находящихся под управлением одной организации, но предстоит решить ещё множество более сложных задач. В этой публикации рассмотрено несколько более сложных проблем, включая расширяемость, множественную адресацию, разделение сетей, мобильные хосты, общий доступ, локальные соединения сайта, маршрутизацию через шлюзы и преодоление различий между разнородными системами.

Примечание. С этим документом связаны три рисунка, которые можно запросить у автора, отправив ему сообщение по адресу <SUNSHINE@ISIF>[1].

Введение

Соединения между множеством компьютерных систем позволяют взаимодействовать все более широкому кругу пользователей и приложений. Базовый набор задач, которые требуется решить для организации такого взаимодействия, включает обеспечение достаточно общих и удобных процедур именования, адресации и маршрутизации. Решение этих задач осложняется различным устройством соединяемых систем и их работой под независимым управлением.

Имеющиеся многосетевые системы достаточно малы (не более десятков сетей) и в основном созданы и управляются одной организацией. Здесь такие сети называются однородными или гомогенными. Базовые соединения между сетями поддерживаются на основе простых иерархических процедур адресации и маршрутизации, единообразно применяемых в системах [1,4,10,13]. Организация соединений между многосетевыми системами (неоднородные или гетерогенные сети) только начинается и происходит в основном на основе специализированных решений.

Таким образом, хотя некоторые базовые задачи уже решены, возникают проблемы следующего уровня (имеющиеся методы непрактичны для систем с сотнями и тысячами сетей), включающие поддержку более сложных функций, таких как многодомность (множественная адресация), разделение сетей, мобильные хосты, общий доступ и преодоление различий разнотипных систем.

В этой публикации описано несколько интересных проблем и возможные решения с акцентом на постановку задач и определение возможных решений, а не на подробностях или формализации отдельной проблемы. Во многих случаях будет ясно, что нужны дополнительные исследования для прояснения проблем или поиска и оценки лучших решений.

Иерархические методы

Базовым подходом к адресации и маршрутизации в больших системах являются иерархические методы, которые могут применяться на различных уровнях (например, в сети или между сетями). Здесь представлен краткий обзор базовых принципов, обеспечивающих основу для решения множества других задач.

По мере роста числа абонентов или «хостов» в одной сети возникает потребность установки множества коммутаторов, каждый из которых обслуживает часть хостов. Эти коммутаторы должны поддерживать таблицы маршрутов, которые указывают наиболее подходящий канал (набор каналов) для связи с адресатом. Таблицы применяются для пересылки входящих пакетов в направлении получателя. В сетях на основе дейтаграмм решение о маршрутизации принимается на основе конечного получателя для каждого пакета, тогда как сети на основе виртуальных устройств (соединений) требуют маршрутного решения лишь для начального пакета вызова (последующие пакеты пересылаются по фиксированным маршрутам, хранящимся в других таблицах.

Если бы каждый коммутатор сохранял маршрутную информацию отдельно для каждого получателя, таблицы маршрутизации были бы очень большими. Стандартным подходом служит иерархическая адресация, где каждому хосту назначается определённый порт в конкретном коммутаторе и адрес принимает форму <коммутатор, порт>. После этого маршрутизацию также можно организовать иерархически, отправляя все пакеты, предназначенные для данного коммутатора, по одному маршруту с игнорированием «младшей» части адреса (порт). Поэтому каждому

[1]Адрес был действителен в момент публикации документа, но утратил актуальность. *Прим. перев.*

коммутатору нужно поддерживать лишь таблицу маршрутов к другим коммутаторам, что существенно снижает число разных пунктов назначения и, следовательно, маршрутных записей.

Отметим, что иерархическая маршрутизация является одним из основных мотивов введения иерархических адресов, но эти два метода не обязательно применяются совместно, как будет показано ниже. Другой причиной использования иерархических адресов является упрощение распределения полномочий по назначению адресов в больших системах [14].

Этот подход можно распространить на многосетевые системы, добавив ещё один уровень в иерархию адресов, чтобы получить формат <сеть, коммутатор, порт>. При иерархической маршрутизации пакеты сначала направляются в сеть получателя с игнорированием остальных частей адреса, затем маршрутизируются в этой сети, как описано выше. Эта форма иерархической адресации была принята для сетей общего пользования с коммутацией пакетов в документе CCITT Recommendation X.121 и похоже, что большинство сетей общего пользования планируют применять иерархическую маршрутизацию [13,19].

За уменьшение размера таблиц при использовании иерархической маршрутизации приходится платить тем, что маршруты не всегда могут быть оптимальными. При наличии двух путей в удалённую сеть (что часто встречается на практике) один может оказаться лучше для одних хостов сети, второй - для других. Однако нет возможности определить это из локальной таблицы маршрутизации, содержащей единственную запись для всей удалённой сети. Ещё более серьёзные последствия строгого применения иерархической маршрутизации рассмотрены ниже.

Для предотвращения указанных проблем можно принимать решения на основе большего числа адресов там, где это желательно [5,14]. Например, таблицу межсетевой маршрутизации можно дополнить записями для отдельных коммутаторов, получающих большой объем трафика в удалённой сети, сохранив для всех прочих коммутаторов этой сети общую запись. Это ведёт к селективному росту таблиц маршрутизации и требует поддержки операций поиска в таблицах по части адреса переменного размера с разным уровнем детализации.

Разделение сетей

Сеть считается разделённой (partitioned) при выходе из строя коммутаторов и/или каналов, в результате которого в сети возникает две или более группы хостов, не способных взаимодействовать между собой. В изолированной сети проблема не может быть решена, пока не будут выполнены работы, обеспечивающие восстановление связности. Но если разделённая сеть является частью многосетевой системы, могут быть пути через другие сети, позволяющие соединить части разделённой сети. К сожалению эти пути не могут использоваться при строгой процедуре иерархической маршрутизации, описанной выше. Даже при передаче «локального» пакета коммутатором в соседнюю сеть этот пакет скорей всего вернётся из неё в ту же часть разделённой сети.

Это указывает дополнительную сложность. Трафик в удалённой сети, предназначенный для разделённой сети, будет маршрутизироваться в ту или иную часть без учёта коммутации внутри разделённой сети (напомним, что другие сети видят лишь один «лучший» путь в эту сеть, рассматриваемую как целое). Для некоторых адресатов пакеты будут приходить не в тот раздел, а эти получатели будет недоступны для внутрисетевых маршрутов, что ведёт к их недоступности из удалённых сетей [14,16].

Одним из решением этой проблемы является настройка системы с обеспечением достаточной отказоустойчивости, в которой разделение происходит редко, и принимать в этих редких случаях проблемы с доставкой как должное. Это может оказаться приемлемым для коммерческих сетей где загрузка и отключения достаточно предсказуемы.

В военных системах, где предполагаются многочисленные повреждения, желательно иметь средства принудительного использования любых доступных соединений [3]. Один из подходов заключается в рассмотрении числа сетей как динамического параметра и превращении разделённой сети в две сети, каждая из которых может быть явным адресатом. Это требует более сложных методов обновления представлений каждой сети об общей топологии и распространения информации о разделе одной сети во все другие сети [8]. Другой подход заключается в возврате специального сообщения об ошибке, вынуждающего выбрать другую точку входа в «отвалившуюся» сеть. Этот метод «резервирования с переключением» (backup-and-try-alternate) реализован для организации вызовов в Telenet [19].

Маршрутизация по «быстрому пути»

Использование разных внешних маршрутов между парой точек, расположенных в одной области, может быть желательно не только в случаях аварий с разделением сети. Если две сети охватывают одну территорию, например, наземная сеть с промежуточной буферизацией (store-and-forward) и широковещательная спутниковая сеть, для некоторых типов трафика производительность может быть повышена при выходе из наземной сети вблизи источника и возврате в неё вблизи получателя. Например, передача файлов в этом варианте может ускоряться.

Для достижения этого снова требуется отойти от иерархической маршрутизации. Либо маршрутизация на уровне сетей должна различать адресатов, доступных напрямую в этой сети и адресатов, доступных с использованием внешних путей, либо маршрутизация внутри сети должна видеть пути через другие сети как особый случай доступных изнутри каналов [9]. Однако в последнем случае требуется внедрение информации о состоянии внешних путей в процедуры поддержки состояний внутренних каналов, что может оказаться «грязным» делом.

Множество адресов

Абонент может организовать несколько соединений с системой связи для повышения надёжности или производительности. В простейшем случае несколько независимых физических линий может поддерживаться как один логический канал для повышения надёжности и производительности или снижения стоимости (с учётом тарифов операторов связи). Было разработано несколько процедур множественных подключений, например, Transpac и X.75. Абонент по-прежнему имеет один адрес и никаких сложностей не возникает.

Для защиты от отказов узлов и линий можно подключать линии к разным коммутаторам. В этом случае у абонента будет два (или более) адреса. Разные адреса могут возникать на любом уровне иерархии (например, два адреса в сети или подключение к двум сетям). Несколько линий могут также обеспечить рост производительности за счёт прямого соединения с часто используемыми областями системы для исключения дополнительных этапов пересылки через сеть.

Для достижения этих преимуществ требуется возможность использовать оба адреса и выбирать из них оптимальный. Это можно реализовать явным выбором отправителем одного адреса, но для этого отправитель должен знать о наличии нескольких адресов у данного получателя, чтобы выбрать из них лучший и переключаться на другой в случае отказа. Эту задачу, очевидно тяжёлую, можно решить с помощью удалённой службы каталогов и маршрутизации.

Другим вариантом может быть явное указание в пакете нескольких адресов, позволяющее каждому коммутатору выбирать из них лучший маршрут к каждому адресу. Это увеличивает размер пакетов и нагрузку на маршрутизацию.

Вместо включения нескольких адресов пакет может содержать имя (логический адрес) получателя [14], предоставляя коммутаторам возможность поиска и выбора лучшего адреса в каждой точке. Это упростит пакет, но внесёт дополнительные требования к обработке в коммутаторах.

Таким образом, имеется набор решений с ростом нагрузки на отправителя или сеть в результате использования нескольких адресов. В сетях на основе дейтаграмм сложная обработка адресов в каждом пакете может оказаться непрактичной, поэтому может оказаться целесообразным выбирать адрес у отправителя. В сетях на основе виртуальных соединений большая часть работы может выполняться в сети при организации соединения. Некоторые сети общего пользования уже предоставляют средства организации соединений с переадресацией в случае недоступности или занятости адреса.

Проблемы наблюдаются как на стороне источника, так и у получателя. Для использования преимуществ наличия нескольких адресов получатель должен быть готов принимать трафик по любому из этих адресов. В сетях с виртуальными соединениями весь трафик для данного вызова должен проходить по одной линии, поэтому в случае отказа во время соединения переключение на другой адрес невозможно. Соединение должно быть сброшено с возможностью потери данных и запросом нового соединения.

Даже в сетях на основе дейтаграмм протоколы высоких уровней чувствительны к адресам локального и удалённого хоста [3]. Адес отправителя служит для демультиплексирования входящих пакетов в нужно «соединение» и получение пакета с другого адреса приведёт к тому, что он не будет должным образом распознан. Для предотвращения этой проблемы можно использовать (одно) имя отправителя в таблицах соединений, но это имя потребуется включать в пакет. Другим решением может быть хранение нескольких удалённых адресов в таблице соединений, чтобы пакет с любого из этих адресов обрабатывался корректно. Эти адреса могут быть представлены в процессе организации соединения и могут применяться для передачи трафика при отказе основного адреса.

Мобильные хосты

Мобильные хосты представляют собой особый случай проблемы множества адресов. Тот или иной уровень «мобильности» присущ технически каждому хосту, поскольку хост может время от времени менять свой адрес в результате изменения конфигурации сети, переноса в другое место или изменения топологии сети. Поэтому поддерживаются базы данных с привязкой имён хостов к их текущим адресам, размещаемые локально или на удалённых серверах.

Однако проблема смены адресов существенно меняется для хостов, которые часто меняют точку подключения к сети даже в процессе работы организованных ранее соединений. Разработаны специальные процедуры динамической маршрутизации и адресации для наземных мобильных хостов, взаимодействующих через радиоканалы в рамках одной сети [6]. По мере роста дальности такой связи технология может быть перенесена в самолёты и следует ожидать выхода за границы одной сети.

Одним из методов «отслеживания» мобильных хостов может служить поддержка специальной базы данных с текущим местоположением хостов (возможно дублирование базы для надёжности), как это делается в отдельных пакетных радиосетях (на «станциях»). Мобильные хосты по мере необходимости обновляют записи в этой базе, а пользователи, которым нужны соединения с мобильными хостами, могут запросить адрес в базе данных, как в обычной службе каталогов. Однако они должны быть готовы к получению частых обновлений о смене адреса от самого мобильного хоста, дополнительных точек ретрансляции или базы данных. Описание этой схемы представлено в работе [18].

В предположении, что трафик доходит до получателей, они должны быть «нечувствительны» к конкретному адресу отправителя, как было отмечено выше, поскольку этот адрес будет меняться у мобильных хостов. Однако в этом случае нет фиксированного набора возможных адресов для указания в процессе организации соединения, поэтому пакеты должны, вероятно, включать уникальный идентификатор (имя) отправителя и его текущий адрес. Для надёжности может быть целесообразно включение с пакет имени получателя на случай, что оно теряет привязку к ранее доступному адресу.

Мобильные хосты могут иметь несколько адресов одновременно или менять адрес со временем (например, самолёт может быть подключён к двум радиосетям). Это усугубляет проблемы и усложняет их решение.

Общий доступ в сеть

Проблема, обратная по отношению к хосту с множеством линий, возникает при использовании одной линии доступа несколькими хостами. Это может оказаться желательным при ограниченном числе физических интерфейсов или портов в сети, а также при использовании линии дальней связи несколькими близко расположенными абонентами. Сети общего доступа предоставляют многоточечные интерфейсы для терминального трафика (X.28), но не для пакетов (X.25). Для пакетных устройств альтернативой фиксированному (следовательно, неэффективному) мультиплексору с частотным или временным разделением является тот или иной «интеллектуальный» мультиплексор, работающий на уровне пакетов протокола доступа в сеть.

Широковещательные сеть (например, Ethernet и кольцевые сети) обеспечивают такую возможность по своей природе, поскольку каждый интерфейс «слышит» весь трафик. Интерфейс отвечает за восприятие соответствующего трафика и в некоторых случаях может настраиваться на захват трафика для нескольких адресов.

Другим подходом служит использование протоколов вышележащего уровня для обеспечения мультиплексирования. Протокол доступа Arpanet (Host-IMP) не поддерживает разделяемые интерфейсы а ограничение в 4 интерфейса на хосте для исходных IMP в некоторых случаях стало проблемой. Протокол Internet (IP) является следующим уровнем над конкретными протоколами доступа в сеть в иерархии ARPA [10,11]. Размер адреса IP достаточно велик для

поддержки нескольких «логических» хостов на одном физическом порту хоста Arpanet. заголовок Host-IMP указывает один физический адрес хоста для всех таких пакетов, а модуль вышележащего уровня IP у адресата демультиплексирует пакеты нужному логическому хосту. Разработано независимое устройство для реализации этой функции на базе оборудования PDP-11/03. Этот «расширитель портов» эффективно превращает каждый порт IMP в 4-8 портов для остов, использующих протокол IP [7].

Сравнение сетей и шлюзов в качестве узла коммутации

В большинстве моделей иерархической маршрутизации сети рассматриваются как «супер-коммутаторы», похожие на обычные узлы коммутации в сети. Такое представление было бы верным, если бы в каждой сети присутствовал один коммутирующий межсетевой трафик узел для маршрутизации входящего из других сетей трафика с пересылкой его в другую сеть или на локальный хост. На рисунке X[1] показа пример небольшой многосетевой системы и таблица маршрутизации в одной сети (коммутаторе). Таблица указывает стоимость числом интервалов межсетевой пересылки (internet hop) и лучшую из соседних сетей для доступа в каждую из сетей системы.

В целях эффективности функция межсетевой коммутации обычно распределена между процессорами, называемыми шлюзами (gateway) и обслуживающими каждый межсетевой канал. Вместо передачи через сеть в ту или иную центральную точку межсетевой трафик можно маршрутизировать напрямую в точке входа на лучшую точку выхода (другой шлюз или целевой хост). На рисунке Y показана та же система с помеченными межсетевыми каналами и таблицей маршрутизации шлюза, размещённого на входном канале. Поскольку шлюз должен отправлять пакеты через свою сеть в конкретный выходной канал, в таблице маршрутизации указано имя следующего канала а не сети.

Следующим шагом является добавление одного шлюза, размещаемого «в середине» каждого межсетевого канала, вместо установки по одному процессору в каждой сети. Шлюзы идентифицируют свои межсетевые каналы. В такой конфигурации более реально задавать стоимость числом интервалов пересылки, а не межсетевых соединений. Поэтому каждый шлюз поддерживает сведения о дистанции (число интервалов) между шлюзами и лучший следующий шлюз для каждого адресата. В этой модели более реалистично считать шлюзы узлами коммутации, а сети - соединительными каналами между ними. По сути, это двойник предыдущей модели, показанный на рисунке Z. Однако получателями в таблице маршрутизации являются сети, а не шлюзы, что делает эту схему любопытным гибридом. В результате неясно, как применить маршрутизацию по состоянию канала (link state), используемую внутри отдельной сети (например, Arpanet) к этой многосетевой системой со шлюзами в качестве узлов коммутации.

Соединения внутри сайта

Многие сайты начинались с одного хоста, подключённого к сети дальней связи. По мере развития к коммутаторам сетей дальней связи подключались напрямую дополнительные хосты сайта. Поскольку число таких хостов росло, могли возникать проблемы связанные с дороговизной или неэффективностью использования процедур доступа в сеть. Привлекательными стали «расширители портов» и интеллектуальные мультиплексоры, упомянутые выше.

Это решало проблему подключения к сети, но локальный трафик также возрастал и в какой-то момент мог превзойти по объёму трафик с удалёнными сайтами. Сетевой коммутатор обслуживает большой объем трафика, который никуда не идёт дальше через сеть. В некоторых случаях расширители портов обеспечивали локальную коммутацию, формируя рудиментарную локальную сеть.

Для более эффективной обработки локального трафика может оказаться желательным организация явной локальной сети. При этом возникает вопрос - нужно ли остальной части многосетевой системы «знать» об этой сети и подключать такую сеть (через один или несколько полноценных шлюзов) или оставить её «невидимой» на межсетевом уровне с представлением хостов локальной как подключённых напрямую к сети дальней связи. В первом случае локальные хосты получают «межсетевой» адрес в явной локальной сети, а во втором используют адреса сети дальней связи.

Модель с явной локальной сетью имеет некоторые преимущества за счёт явной идентификации группы хостов сайта как сети. Если сайт подключён к нескольким внешним сетям, механизмы межсетевой маршрутизации будут автоматически выбирать лучший путь к локальным хостам, которые имеют один адрес (в своей локальной сети.

Однако такое участие может вызывать проблемы на межсетевом уровне. По мере роста числа сайтов с локальными сетями будут расти таблицы маршрутизации и объем обновлений, которые должны распространяться по всей межсетевой системе. Если рост продолжается на сайте и там появляется несколько локальных сетей, соединённых «локальными» шлюзами, возникает вопрос о передаче сведений об этих локальных сетях и их топологии в межсетевую систему (internet). В какой-то момент рассмотрение локальных сетей как дальних или магистральных станет невозможным.

Модель с «невидимой» локальной сетью позволяет избежать проблем, связанных ростом числа сетей на межсетевом уровне. Многие расширители портов или локальные системы распределения могут выполнять функции коммутации, освобождая коммутатор сети дальней связи от обработки локального трафика. Однако сайты, соединённые с несколькими сетями, будут иметь множество адресов на своих хостах (по одному адресу для каждой сети, к которой хост представляется подключённым напрямую) и это вызывает сложности, рассмотренные выше (см. Множество адресов).

Эффективный компромисс для решения этих проблем не найден. Добавление уровня в иерархию адресов может дать временное решение, но оно тоже с течением времени столкнётся со сложностями. Это решение предполагает использование переменного числа уровней иерархии в системе с добавлением уровней по мере усложнения той или иной области. Однако это требует жёсткого упорядочения уровней и, следовательно, маршрутизации, тогда как в реальности представления «выше-ниже» для уровней могут зависеть от точки зрения пользователя. Требуются дальнейшие исследования процессов роста многосетевых систем (internet) с поддержкой в них эффективных процедур адресации и маршрутизации.

Множество доменов

В большей части предшествующего обсуждения предполагалось наличие единого «домена» с согласованными процедурами адресации и маршрутизации. В реальном мире наблюдается наличие и рост нескольких крупных доменов

[1]См. примечание в начале заметки.

с разными соглашениями, включающих общедоступные сети, сети мэйнфреймов, сеть министерства обороны (США) и локальные сети. Нереально надеяться, что эти разные группы когда-либо придут к единой схеме адресации, поэтому в обозримом будущем придётся учитывать наличие разнородных доменов.

Один из подходов основан на допущении об использовании одним доменом другого в качестве транспортной среды между своими однородными компонентами. Используемая система появляется просто как один из нескольких типов сред, которые использующая система может применить через соответствующие протоколы доступа. Пакеты использующей системы будут «инкапсулироваться» в пакеты протоколов используемой системы. Два таких домена могут взаимно использовать друг друга иногда даже неограниченно взаимодействовать между собой, используя «взаимную инкапсуляцию» [15]. Для неограниченного взаимодействия между разнородными системами каждая из них должна распознавать хосты другой системы. Имеется два базовых варианта работы через границы доменов — отображение (mapping) и заданная отправителем маршрутизация (source routing).

В варианте с отображением каждый домен предоставляет набор свободных внутренних адресов для сопоставления с адресами в другом домене. Трафик, направленный на такой «псевдо-адрес» маршрутизируется на интерфейс или шлюз в соответствующий внешний домен. В простейшем случае это требует лишь двухстороннего соглашения между доменами, но может быть распространено и на работу через промежуточные домены. Недостаток такого подхода заключается в том, что набор доступных внешних адресов ограничен таблицей сопоставления, которая обычно включает лишь часть адресов удалённого домена. Другой недостаток состоит в том, что один объект имеет разные адреса в каждом домене и каталог имён включает несколько записей для каждого имени (по одной для каждого домена). Основным преимуществом этого подхода является возможность обращения к поддерживаемым именам из удалённого домена как к локальным без дополнительных процедур.

В модели source routing [14,17,5] отправитель задаёт маршрут к адресату, состоящий из последовательности адресов промежуточных междоменных шлюзов вплоть до конечного получателя. Каждый адрес из этого списка интерпретируется в своём домене, где он имеет смысл, и затем удаляется, чтобы в следующем домене применялся понятный ему адрес. При использовании этого метода доступны все адреса удалённого домена, а междоменным шлюзам не нужно поддерживать заранее заданные сопоставления или преобразовывать адреса. Вся работа переносится к отправителю, который должен иметь сведения о топологии и форматах адресов для задания полного маршрута. Это увеличивает размер заголовков в пакете и объем обработки пакетов, поскольку размер заданного отправителем маршрута является переменным. Ещё раз отметим, что «адреса» различаются в разных доменах, но сейчас можно комбинировать эту информацию, - если каталог даёт маршрут для задания отправителем в домен X из домена A, а пользователь из домена B знает маршрут в домен A, он может объединить их в маршрут для домена X из B (хотя он может не быть оптимальным).

Зачастую полезно собрать маршрут возврата в процессе прохождения «прямого» маршрута, заданного отправителем (source route). Это позволяет адресату отвечать. В общем случае маршрут возврата не является простым обращением прямого маршрута. Адес возврата добавляется при входе пакета в каждый домен, а достигнутый адрес получателя удаляется на выходе из каждого домена (см. подробный пример в [17]).

«Независимый» от сети транспортный протокол [2], разработанный в British PSS Users Forum, является первым из тех, которые явно решают проблему нескольких доменов. По сути, предлагается механизм задаваемой отправителем маршрутизации, включая дополнительные средства трансляции явно указанной адресной информации, передаваемой между пользователями как данные. Протокол предполагает процедуру организации маршрута как часть организации соединения, поэтому задаваемый отправителем маршрут требуется передавать лишь в пакете запроса соединения.

В сетях общего пользования также предоставляется ограниченная возможность задания маршрута отправителем в форме поля Call User Data пакетов запроса соединения X.25. Это поле может использоваться целевым устройством DTE как дополнительная адресная информация для последующих шагов в соединении. Этот механизм применялся для соединений между сетями общего пользования в Канаде и США до внедрения иерархической адресации X.121 [12]. Поле Call User Data также начинает применяться в специализированной форме для адресации в различных частных и локальных сетях, соединённых с сетями общего пользования.

Протокол Arpa Internet также поддерживает опцию задаваемой отправителем маршрутизации, но для всех адресов на маршруте предполагается формат IP [11].

Заключение

Здесь отмечен ряд проблем, которые нужно принимать во внимание при выходе за пределы простых методов соединения сетей, применяемых сегодня. Значимость этих проблем только начинает осознаваться. Были предложены некоторые предварительные решения, но практического опыта ещё недостаточно. Предстоит проделать большую работу по прояснению задач, а также разработке и оценке решений.

Благодарности

Многие из представленных здесь концепций обсуждались несколько лет в рамках проекта ARPA Internet. Значительные заслуги в разработке и прояснении идей принадлежат коллегам автора из ISI и других организаций, вовлечённых в проект.

Литература

Примечание. Некоторые из указанных ниже ссылок относятся к категории IEN (Internet Experiment Note), разработанных в рамках проекта ARPA Internet, и не были опубликованы.

[1] D. R. Boggs, J. F. Shoch, E. A. Taft, and R. M. Metcalfe, "Pup: An Internetwork Architecture," IEEE Trans. On Communications 28, 4, April 1980, pp. 612-623[1].

[2] British Post Office PSS User Forum, A Network Independent Transport Service, February 1980.

[1]Доступна по ссылке. *Прим. перев.*

[3] V. G. Cerf, Internet Addressing and Naming in a Tactical Environment, Internet Experiment Note 110, August 1979.

[4] V. G. Cerf and P. T. Kirstein, "Issues in Packet-Network Interconnection," Proc. IEEE 66, 11, November 1978, pp. 1386-1408[2].

[5] D. D. Clark and D. Cohen, A Proposal for Addressing and Routing in the Internet, Internet Experiment Note 46, June 1978.

[6] R. E. Kahn, S. A. Gronemeyer, J. Burchfiel, and R. C. Kunzelman, "Advances in Packet Radio Technology," Proc. IEEE 66, 11, November 1978, pp. 1468-1496.

[7] H. A. Nelson, J. E. Mathis, and J. M. Lieb, The ARPANET IMP Port Expander, SRI Report 1080-140-1, November 1980.

[8] R. Perlman, Flying Packet Radios and Network Partitions, Internet Experiment Note 146, June 1980.

[9] R. Perlman, Utilizing Internet Routes as Expressways Through Slow Nets, Internet Experiment Note 147, June 1980.

[10] J. B. Postel, "Internetwork Protocol Approaches," IEEE Trans. on Communications 28, 4, April 1980, pp. 604-611[3].

[11] J. B. Postel, C. A. Sunshine, and D. Cohen, "The ARPA Internet Protocol," to appear in Computer Networks, 1981.

[12] A. M. Rybczynski, D. F. Weir, and I. M. Cunningham, "Datapac Internetworking for International Services," Proc. 4th Int. Conf. on Computer Communication, September 1978, pp. 47-56.

[13] A. M. Rybczinski, J. D. Palframan, and A. Thomas, "Design of the Datapac X.75 Internetworking Capability," Proc. 5th Int. Conf. on Computer Communication, October 1980, pp. 735-740.

[14] J. F. Shoch, "Inter-Network Naming, Addressing, and Routing," Proc. 17th IEEE Computer Society Int. Conf., September 1978, pp. 72-79[4].

[15] J. F. Shoch, D. Cohen, and E. A. Taft, "Mutual Encapsulation of Internetwork Protocols," to appear in Computer Networks, 1981[5].

[16] C. A. Sunshine, "Interconnection of Computer Networks," Computer Networks 1, 3, January 1977, pp. 175-195.

[17] C. A. Sunshine, "Source Routing in Computer Networks," ACM SIGCOMM Computer Communication Rev. 7, 1, January 1977, pp. 29-33.

[18] C. A. Sunshine and J. B. Postel, Addressing Mobile Hosts in the ARPA Internet Environment, Internet Experiment Note 135, March 1980.

[19] D. F. Weir, J. B. Holmblad, and A. C. Rothberg, "An X.75 Based Network Architecture," Proc. 5th Int. Conf. On Computer Communication, October 1980, pp. 741-750.

Перевод на русский язык

Николай Малых

nmalykh@gmail.com

[2]Статья доступна по ссылке. *Прим. перев.*
[3]Статья доступна по ссылке. *Прим. перев.*
[4]Доступна в IEN 19. *Прим. перев.*
[5]Доступна в IEN 140. *Прим. перев.*