

МЕТОДЫ РАСПРЕДЕЛЕНИЯ АДРЕСНОГО РЕСУРСА В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

И.В. Жигалов, С.А. Падишин, С.А. Панихидников

В статье рассмотрены способы распределения адресного ресурса и построения телекоммуникационной сети в условиях перемещения должностных лиц между местами выполнения служебных обязанностей.

Ключевые слова: методы распределения адресного ресурса, настройка сети, перемещение рабочих мест, DHCP, VPN, PPPoE, доступность рабочих мест в сети.

DISTRIBUTION METHODS OF VARIOUS ADDRESS WITHIN TELECOMMUNICATION NETWORK CONFIGURATIONS

Padishin S., Panihidnikov S., Zhigalow I.

The article describes distribution choices of various address and telecommunication network configurations based on the persons traveling in between job locations.

Keywords: distribution Methods of various addresses, network settings, allocation of job placements, DHCP, VPN, PPPoE, availability of job placements within network.

В современных условиях развития телекоммуникационных сетей специального назначения четко обозначилась проблема необходимости оперативной перенастройки телекоммуникационных сетей, перераспределения адресного ресурса в процессе топологического и логического перемещения элементов сети и абонентов сетей связи специального назначения.

При топологическом перемещении абонента сети на новое место для подключения его к информационному ресурсу сети необходимо выполнить две основные операции: идентифицировать абонента и обеспечить доступ к необходимым сведениям.

Рассмотрим этап идентификации абонента сети, который будет заключаться в том, что его необходимо ввести в адресное пространство нового узла связи телекоммуникационной сети.

Основным показателем, при этом, считается время подключения терминального устройства абонента к сети.

Существуют следующие методы и порядок распределения адресного пространства в телекоммуникационных сетях специального назначения [1]:

- статический метод (жесткое закрепление IP-адресов за сетевыми элементами);
- динамический метод (DHCP-протокол);
- смешанный метод.

Рассмотрим достоинства и недостатки каждого из методов.

- 1) Статический метод распределения адресного пространства.

Данный метод применяется в сетях, где необходима повышенная надежность сети в стационарных условиях и не допускает быстрого изменения конфигурации сети.

Достоинства: повышенная стабильность работы в сети при наличии помех, многочисленных обрывах и потерях связи с серверами динамического распределения адресного пространства, работающих по DHCP-протоколу.

Недостатки: отсутствие динамической перестройки сети. Для проведения перестройки необходима согласованная работа достаточного количества системных администраторов.

Для перестройки всей сети со статическим назначением сетевых настроек, в подавляющем большинстве необходим физический доступ к оборудованию, со всеми вытекающими отсюда последствиями – увеличение сроков перестройки, наличие всех учетных данных (логинов/паролей) ко всему перечню оборудования, необходимость «ногами» пройти по всем точкам установки оборудования, что в определённых условиях порой невозможно.

2) Динамический метод.

Данный метод основан на автоматизации настроек сети. К его достоинствам можно отнести:

- централизованное быстрое изменение настроек сети (включая маршрутизацию, адресацию доменных имен и остальные настройки сети, поддерживаемые DHCP-протоколом (более 40 настроек);

- возможность проведения плановых работ по настройке DHCP-серверов заблаговременно с большим запасом по времени и высоким качеством проведенных работ;

- привлечение минимального количества личного состава для проведения данных работ, как следствие этого повышение качества выполняемых работ за счет повышения профессиональной подготовки.

К недостаткам динамического метода распределения сети можно отнести:

- существенное понижение безопасности сети по причине возможности получения всего спектра настроек после подключения к сети и элементарной подделки mac-адреса оборудования;

- невозможность выявления подобного подключения стандартными методами;

- невозможность подключения оборудования к сети при потере связи с DHCP-сервером.

3) Смешанный метод.

Для повышения устойчивости сети и при невозможности удаления из цепи настройки системного администратора, статические IP-адреса необходимо назначать для ключевого «пограничного» оборудования отвечающего за прохождение трафика на магистралях и обеспечивающих критически важные функции сети. При этом, для повышения устойчивости для этого оборудования необходимо иметь на DHCP-серверах учетные записи с полным комплектом

настроек на случай их сброса «пограничным» оборудованием. Вариант построения подобного сегмента представлен на рис. 1.

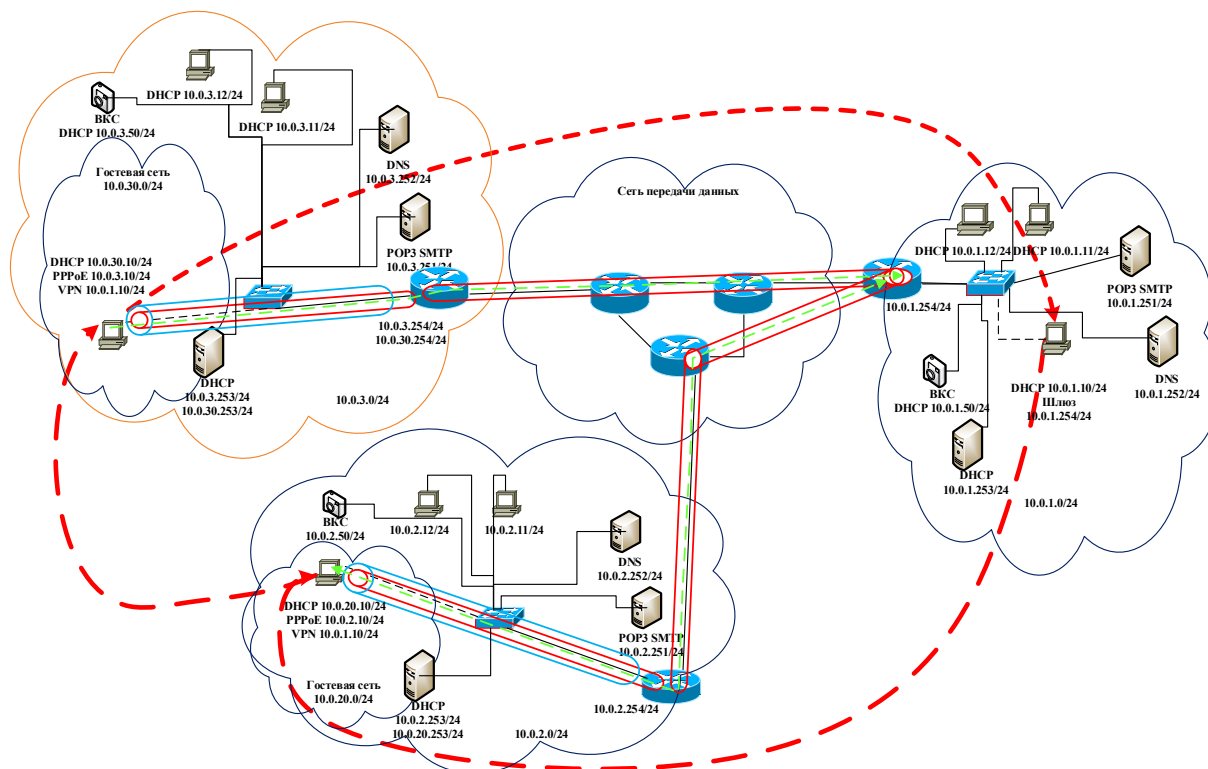


Рис. 1. Организация адресного пространства комбинированным способом

Динамические адреса целесообразно назначать для оборудования внутри узла с максимальным сроком аренды. Причины максимального срока – это время, за которое возможно устранить неисправность в случае ее возникновения в цепи клиент-DHCP-сервер. Также необходимо рассматривать возможность для подключения в сеть оборудования приданных сил или для других задач. Для этого на DHCP-сервере необходимо создать «гостевой» диапазон с предоставлением возможности создания VPN-канала в «домашнюю» сеть через сеть VPN-взаимодействия.

VPN сеть взаимодействия – это сеть создаваемая поверх транспортной сети для обеспечения взаимодействия удаленных автоматизированных рабочих мест с сетями в которых эти автоматизированные рабочие места (АРМ) постоянно функционируют в обычное время. «Гостевой» диапазон – диапазон IP-адресов, который выделяется неизвестным устройствам автоматически с целью скрыть истинные настройки сети подключённого сегмента.

Исходя из вышеизложенного достоинствами смешанного метода можно считать:

- гибкое распределение адресного пространства на узле связи;
- повышение безопасности сети за счет мониторинга сети с применением DHCP-серверов, которые выдают сетевые настройки «чужому оборудованию» непригодные для использования и применения;

- возможность создания VPN-каналов, контроля их активности и возможности ограничения по пропускной способности;
- сохранение логической структуры узла при изменении топологии сети;
- упрощение эксплуатации сети персоналом с низким уровнем подготовки.

Недостатками смешанного метода является необходимость администрирования сети высококвалифицированным персоналом в подготовительный период.

Для подключения внутри узла связи рабочих мест и элементов, изначально не стоящих в составе узла связи и не прописанных на DHCP сервере необходимо выделить «гостевой» диапазон IP-адресов автоматического подключения.

При получении дополнительных маршрутов «гостевым» устройствам маршруты раздаются автоматически вместе с получением IP-адреса на DHCP-сервере. Дальнейшие действия пользователя при подключении АРМ будут заключаться в активации PPPoE-соединения.

В дальнейшем через PPPoE-соединение для получения ресурсов сети постоянной приписки целесообразна активация VPN-тоннеля в сеть постоянной приписки.

При этом IP-адрес, получаемый клиентом при VPN-подключении, должен совпадать с адресом, получаемым при локальном подключении клиента в сеть постоянной приписки.

Положительными сторонами такого построения сети специального назначения являются:

- повышается безопасность;
- более равномерно распределяется нагрузка по маршрутизаторам, смещаясь от центра к периферии сети;
- подавляющая часть настройки сети по времени смещается на подготовительный период, при этом во время перемещения должностных лиц на новый узел связи работа системного администратора сводится к выдаче логинов и паролей PPPoE-соединения и мониторингу сети, а при необходимости к выделению постоянного IP-адреса с полным комплектом настроек и маршрутов;
- у конечных пользователей, аппаратных и узлов отпадает необходимость в перестройке оборудования в ходе переключений, или эти работы сведены к минимальным настройкам типа активации VPN-соединения.

К отрицательным сторонам данного построения сети можно отнести:

- доработка структуры существующей сети;
- необходимость наличия подготовленного личного состава для предварительной настройки сети.

В тоже время, проведя анализ имеющихся возможностей телекоммуникационного оборудования, на наш взгляд, возможно выделить еще один метод – Организация адресного пространства при закреплении нескольких IP-адресов за одним АРМ и подключением VPN-соединения. Пример построения сегмента данной сети показан на рис. 2.

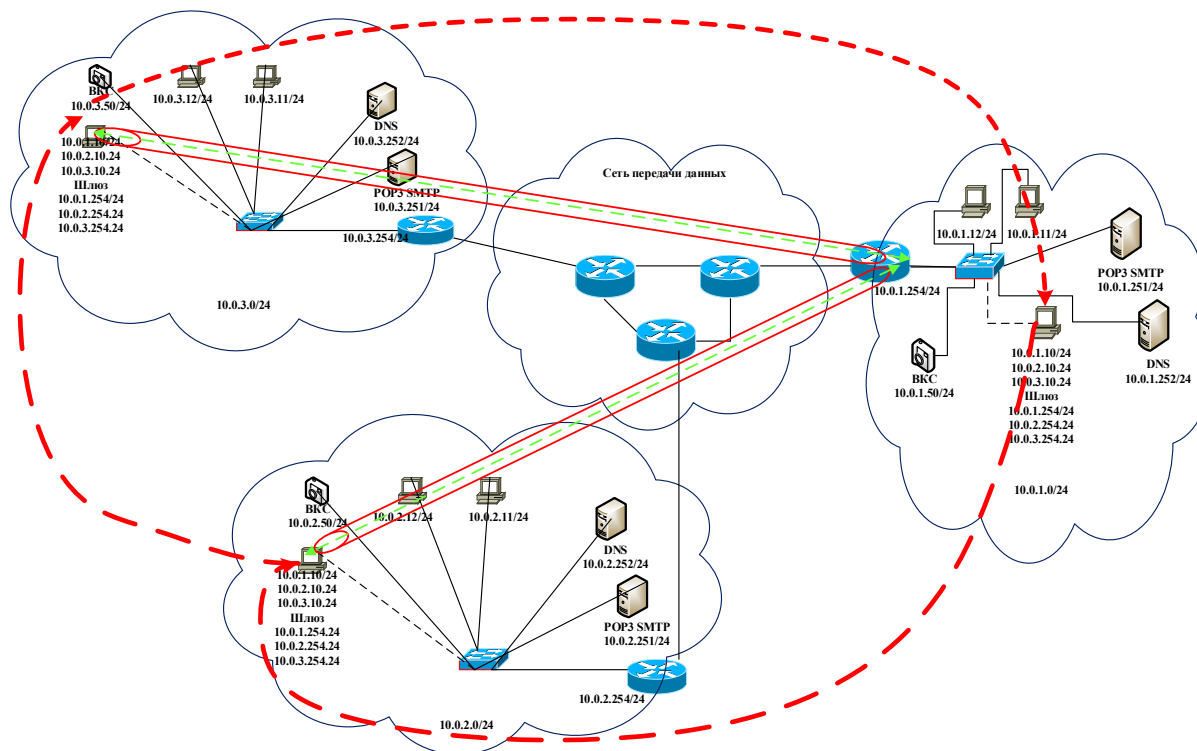


Рис. 2. Организация адресного пространства при закреплении нескольких IP-адресов за одним АРМ и подключением VPN-соединения

Как правило, топологическое и логическое перемещение абонентов сети планируется заранее, поэтому на наш взгляд более оптимально применить другой способ настройки параметров сетевых адаптеров АРМ.

В сетевые адаптеры АРМ вручную задаются основной и несколько дополнительных IP-адресов, шлюзов, DNS-серверов по количеству сетей, в которых предполагается работа АРМ должностного лица. Следующим шагом для обеспечения ресурсов с сети постоянной приписки необходима активация VPN-соединения аналогично описанной в смешанном методе.

На данном этапе существует и требует решения проблема распределения адресного пространства в телекоммуникационных сетях специального назначения. Для ее решения необходим творческий подход и совместная работа групп специалистов, рассредоточенных по объектам телекоммуникации и связи, уточнение существующих руководящих документов, основанных на практике работы системных администраторов в структурно-сложных телекоммуникационных сетях.

Представленные научно-технические предложения позволяют оптимизировать процесс распределения адресного пространства сети и обеспечить выполнение требований по идентификации абонентов сети и предоставления им доступа к информационному ресурсу в условиях топологического и логического изменения структуры телекоммуникационных сетей специального назначения в динамике их функционирования.

Список используемых источников

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. СПб.: ООО «Лидер», 2010. 944 с.

**АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ
УПРАВЛЕНИЯ СВЯЗЬЮ**

В.Г. Иванов, Д.Д. Корякин, С.А. Панихидников

Одним из важнейших путей обеспечения требуемого качества связи в процессе обеспечения управления является повышение эффективности управления связью. С этой целью продолжается развитие и дальнейшее совершенствование автоматизированных систем управления связью (АСУС). В статье рассмотрена обобщенная архитектура управления связью в АСУС, общие принципы функционирования и построения АСУС, предложения по использованию концепции TMN и связанных наборов протоколов, приведен краткий анализ развития АСУС в сетях связи специального назначения.

Ключевые слова: автоматизированные системы управления связью, АСУС, TMN, технологии, система связи, специальные сети

**AUTOMATED CONTROL SYSTEMS FOR COMMUNICATION
OF A SPECIAL PURPOSE**

Ivanov V., Koryakin D., Panihidnikov S.

One of the most important ways to ensure a desired quality of communication in the process control software is to improve the communication control efficiency. To this end, continued development and further improvement of the automated communication management systems (ACMS). The article describes the architecture of a generalized communication control in ADR, the general principles of operation and construction of ACMS, proposals for the use of TMN concept and associated set of protocols is a brief analysis of the development of ACMS in the communication networks of special purpose.

Keywords: automated communication control system, ACMS, TMN, technology, communications, special networking.

Одним из важнейших путей обеспечения требуемого качества связи в процессе обеспечения управления войсками является повышение эффективности управления связью.

АСУС объединений и соединений создаются в соответствии с принципами построения систем управления связью. Эти принципы в полной мере соответствуют принципам построения и функционирования АСУВ, а АСУС объединений и соединений создаются как функциональные подсистемы соответствующих АСУВ, т. е. являются их составными частями. В то же время при создании АСУС учитываются условия выполнения задач управления связью, требования к нему и особенности функционирования системы и войск связи.