***МАШИНОСТРОЕНИЕ И МАШИНОВЕДЕНИЕ***
***05.02.22 – Организация производства***

УДК 004.056.52
DOI: 10.26467/2079-0619-2019-22-6-100-111

# ИЗОЛЯЦИЯ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ ПРЕДПРИЯТИЯ С ИСПОЛЬЗОВАНИЕМ ВИРТУАЛИЗАЦИИ СЕРВЕРОВ

**А.К. БЛАГОРАЗУМОВ[1], И.Г. КИРПИЧЕВ[2], Д.В. ПЕТРОВ[3]**
*[1]Государственный научно-исследовательский институт гражданской авиации, г. Москва, Россия*
*[2]Московский государственный технический университет гражданской авиации, г. Москва, Россия*
*[3]ПАО «Научно-производственное предприятие «Аэросила», г. Ступино, Россия*

Режимные предприятия имеют локальные вычислительные сети (ЛВС), в которых хранятся и циркулируют данные, утечка которых вовне недопустима. В то же время ни одно современное предприятие не может полноценно функционировать без ЛВС, имеющей доступ в Интернет и объединяющей компьютеры отдела продаж, технической службы поддержки и сервер электронной почты. В целях обеспечения информационной безопасности эти две ЛВС изолируются друг от друга физически – исключением любых связывающих их кабелей. Предприятия, на которых к безотказности работы серверного оборудования предъявляются повышенные требования, используют виртуализацию серверов, требующую подключения физических серверов к дисковому хранилищу файловых образов виртуальных серверов. Если высоконадежные серверы необходимы только в одной из двух независимых ЛВС предприятия, то затраты на создание такого серверного кластера обоснованы и окупаемы. Но когда предприятие сталкивается с необходимостью установить в другой ЛВС один, хоть и малопроизводительный, но высоконадежный сервер, то возникает проблема: требуемую надежность может обеспечить только серверный кластер с дорогостоящими компонентами, но для решения возлагаемых на новый сервер задач вычислительная мощность кластера окажется многократно завышенной, и его построение окажется крайне затратным и экономически необоснованным. В то же время необходимые для нового сервера вычислительные мощности могут быть безболезненно позаимствованы у уже имеющегося серверного кластера предприятия путем добавления в него нового виртуального сервера, и это не потребует никаких материальных затрат. Однако для этого необходимо обеспечить изоляцию нового виртуального сервера от ЛВС, к которой подключены те физические серверы, на которых планируется разместить виртуальный сервер. В статье исследуются методы конфигурирования ЛВС, обеспечивающие изоляцию виртуальных и физических серверов на сетевом уровне, позволяющие решить эту задачу. Также рассматривается случай, когда требуется обеспечить передачу файлов между двумя компьютерами, находящимися в разных, изолированных друг от друга ЛВС, и предлагается соответствующее решение.

**Ключевые слова:** локальные вычислительные сети, ЛВС, виртуализация, Hyper-V, VirtualBox.

## ВВЕДЕНИЕ

В настоящее время практически ни одно предприятие, производственные процессы которого зависят от безотказности функционирования серверного оборудования, не может обойтись без ИТ-инфраструктуры, основанной на виртуализации серверов. Суть виртуализации заключается в том, что на одном физическом сервере, называемом хостом (или хост-сервере), выполняется параллельно несколько операционных систем (ОС) с приложениями, называемых гостевыми виртуальными машинами (или виртуальными серверами), причем эти ОС могут быть разных типов (Windows, Linux, macOS и т. п.). Виртуализации свойственно множество преимуществ:

- надежность – выход из строя физического сервера не повлечет простоя служб и приложений на время его ремонта (или подготовки нового сервера с установкой на него ОС и всех необходимых приложений), поскольку образы виртуальных машин могут

быть в считанные минуты запущены на других хостах (при соответствующей настройке виртуальные машины переносятся и запускаются автоматически);

- эффективность использования ресурсов – оперативную и дисковую память хоста можно перераспределять между виртуальными машинами, а сами виртуальные машины можно распределять по хостам для балансировки загрузки последних;
- легкость наращивания ресурсов – после исчерпания возможности аппаратной модернизации физических серверов можно добавить новый сервер, перенеся на него часть виртуальных машин с одновременным выделением последним дополнительных ресурсов;
- простота резервного копирования – образ виртуальной машины хранится в единственном файле, копирование которого при остановленной виртуальной машине гарантирует полноту и консистентность копии.

Наиболее полно реализует все преимущества виртуализации архитектура серверного кластера, состоящего из нескольких серверов и одного дискового хранилища, в которых дублируются контроллеры и кабели, соединяющие контроллеры хранилища и серверов. Высоконадежное дисковое хранилище, в свою очередь, строится на объединенных в отказоустойчивый дисковый массив (RAID) двухпортовых (имеющих продублированные контроллеры) жестких дисках. Пример реализации такой архитектуры описан в [1]. За полученную таким образом высокую отказоустойчивость приходится расплачиваться очень высокой стоимостью аппаратных средств.

Из соображений безопасности локальную вычислительную сеть (ЛВС) предприятия часто разделяют на два полностью изолированных друг от друга сегмента:

- сегмент с доступом в интернет, содержащий веб-сервер, сервер электронной почты, рабочие станции менеджеров по продажам, инженеров технической поддержки и т. п.;
- внутренний сегмент, содержащий ПО автоматизации бухгалтерии, отдела кадров; внутренний документооборот, конструкторское ПО, архив документов ДСП.

Чтобы полностью исключить утечки секретной информации вследствие хакерских атак и ошибок в настройке межсетевых экранов, на режимных предприятиях изоляция сетей обеспечивается радикальным путем: исключением любых кабелей между двумя сегментами ЛВС предприятия.

При этом не возникает проблем, если высоконадежные серверы либо требуются только в одном из двух сегментов сети, либо если в каждом сегменте сети необходимо наличие достаточного количества серверов, чтобы оправдать большие расходы на построение сразу двух независимых серверных кластеров.

Гораздо сложней оказывается ситуация, когда в одном сегменте сети присутствие серверного кластера полностью оправдано, а в другом сегменте требуется установить лишь единичный сервер, обладающий, однако, высокой надежностью, обеспечить которую может только виртуализация на дорогостоящем кластере.

Для оптимального разрешения этой ситуации авторами было проведено исследование возможности выноса во второй сегмент сети единичных виртуальных серверов, физически размещаемых в кластере первого сегмента сети. Также исследована проблема передачи файлов между компьютерами, находящимися в изолированных подсетях, встающая при необходимости обеспечения обмена данными между информационной системой предприятия и информационными системами клиентов предприятия, и предложены комплексные решения этих проблем.

## РАЗДЕЛЕНИЕ СЕТЕЙ ВИРТУАЛЬНЫХ МАШИН НА ПРИМЕРЕ HYPER-V

Microsoft Hyper-V — это система аппаратной виртуализации, позиционируемая как промышленное решение для параллельной работы нескольких ОС на одном хост-сервере без потери производительности. Она основана на гипервизоре – программном обеспечении нижнего

уровня, напрямую взаимодействующем с аппаратными ресурсами и распределяющего их между гостевыми ОС, а также обеспечивающем изоляцию ОС друг от друга[1].

Популярности Hyper-V способствует ее бесплатность и высокая надежность – авторы этой статьи с 2011 года эксплуатируют в дата-центре Информационно-аналитического центра ФГУП ГосНИИ ГА отказоустойчивый кластер на основе Hyper-V [1] с гостевыми машинами на Windows Server 2018; Windows 7, 8 ,10; Ubuntu Server и Debian Linux, и за восемь лет не сталкивались с какими-либо проблемами.

Система Hyper-V может быть развернута на хост-сервере в двух вариантах:

1) как отдельная система с интерфейсом командной строки, позволяющим произвести первоначальную настройку. Для последующего конфигурирования и администрирования требуется сторонний компьютер с ОС Windows и графической оболочкой;

2) как роль Windows Server 2008 (и более старших версий) или Windows 8 (и более старших версий, семейств Pro и Enterprise).

В статье описаны настройки и приведены снимки экрана Hyper-V, интегрированной в Windows Server 2008 и Windows 10. В этих версиях Hyper-V поддерживает три варианта подключения виртуальной машины к сети [2]:

1) внешняя сеть (External network);
2) внутренняя сеть (Internal network);
3) частная сеть (Private network).

Из перечисленных вариантов для решения поставленной задачи интересен только первый (*внешняя сеть*), поскольку *внутренняя сеть* предназначена для соединения виртуальных машин с хостом и не предусматривает подключения с физическими сетями, а *частная сеть* только связывает между собой виртуальные машины, изолируя их от хоста и физических сетей.

При выборе варианта *внешняя сеть* к физическому сетевому адаптеру хоста подключается драйвер, называемый виртуальным коммутатором [2], а в виртуальные машины и в управляющую операционную систему хоста устанавливаются виртуальные сетевые адаптеры, подключаемые к этому виртуальному коммутатору. С помощью стандартных интерфейсов ОС виртуальным сетевым адаптерам хоста и гостевых машин можно присвоить индивидуальные IP-адреса, маски подсетей и адреса шлюзов так, что эти адаптеры смогут работать в различных подсетях. При этом один порт физического сетевого адаптера хоста может по одному кабелю передавать TCP/IP-пакеты логически изолированных подсетей.

С выходом Windows Server 2012 в Hyper-V была добавлена поддержка технологии виртуализации сетей *Hyper-V Network Virtualization* (HNV) [3], обеспечивающей инкапсуляции сетевых пакетов виртуальных машин в сетевые пакеты хоста. Подобно технологии VPN (англ. *Virtual Private Network* – виртуальная частная сеть), HNV логически отделяет подсети виртуальных машин от подсетей хост-серверов. Это позволяет не только объединять в общую сеть виртуальные машины, физически размещаемые в разных дата-центрах, но и совершать динамическую миграцию работающей виртуальной машины из одного дата-центра в другой.

В Windows Server 2012 R2 технология виртуализации сетей была расширена возможностью передачи широковещательного (broadcast) и группового (multicast) трафика [4], позволившей использовать в виртуальных сетях серверы DHCP (англ. *Dynamic Host Configuration Protocol* – протокол динамической настройки узла), в результате чего виртуальная сеть своей функциональностью перестала уступать физической сети.

[1] Hyper-V – Википедия [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Hyper-V (дата обращения: 03.03.2019).

Однако чем сложнее становится технология, тем больше потенциальных уязвимостей можно создать некорректной настройкой сети, если не знать в совершенстве тонкости настройки всего оборудования, задействованного при виртуализации сети. К тому же ряд инструментов, например свободно распространяемый корпорацией Microsoft программный анализатор сети *Microsoft Message Analyzer*[2], позволяет в случае получения потенциальными взломщиками доступа к узлу физической сети получить также доступ к трафику виртуальной сети [4].

Задача надежной изоляции подсетей виртуальной машины и хоста значительно упрощается, если один из физических сетевых адаптеров хоста напрямую привязать к виртуальной машине, задав требуемую конфигурацию сетевых протоколов и соединив разъем адаптера кабелем с коммутатором требуемой ЛВС. При таком подключении не потребуется перенастраивать коммутаторы и маршрутизатор, добавляя в них поддержку дополнительных технологий типа VPN и VLAN (англ. *Virtual Local Area Network* – виртуальная локальная компьютерная сеть, представляющая собой группу хостов, взаимодействующих так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения).

Как правило, даже серверы начального уровня поставляются с двумя адаптерами, но если все адаптеры сервера уже задействованы в системе, то дополнительный несложно установить как плату расширения. Hyper-V поддерживает до 12 сетевых адаптеров на каждую виртуальную машину [5], поэтому со стороны программного обеспечения ограничений на количество адаптеров быть не должно.

На рис. 1 изображена схема сети предприятия, в которой виртуальный сервер, имеющий IP-адрес из диапазона адресов внешней (имеющей доступ в интернет через маршрутизатор) подсети ЛВС-1, физически размещен на хост-сервере внутренней (изолированной от интернета) подсети ЛВС-2.

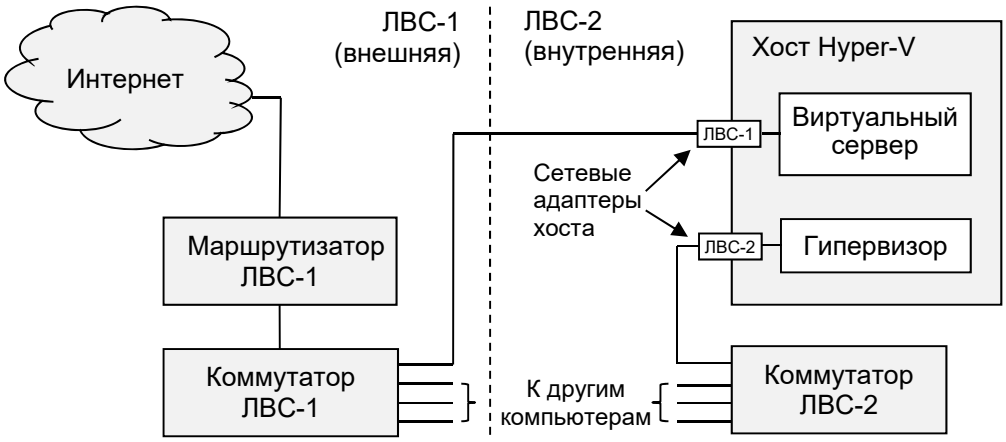


**Рис. 1.** Топология сети с виртуальным сервером Hyper-V
**Fig. 1.** Hyper-V virtual server network topology

В современных версиях Hyper-V виртуальные машины подключаются к сети через *виртуальные коммутаторы*, которые, в свою очередь, связываются гипервизором с физическими сетевыми адаптерами. Изображенную на рис. 1 архитектуру можно реализовать с помощью Hyper-V, выбрав режим *внешняя сеть* и создав виртуальный коммутатор согласно инструкции [6] с помощью интерфейса диспетчера виртуальных коммутаторов (рис. 2).

[2] Microsoft Message Analizer Operating Guide [Электронный ресурс]. URL: https://docs.microsoft.com/en-us/message-analyzer/microsoft-message-analyzer-operating-guide (дата обращения: 03.03.2019).

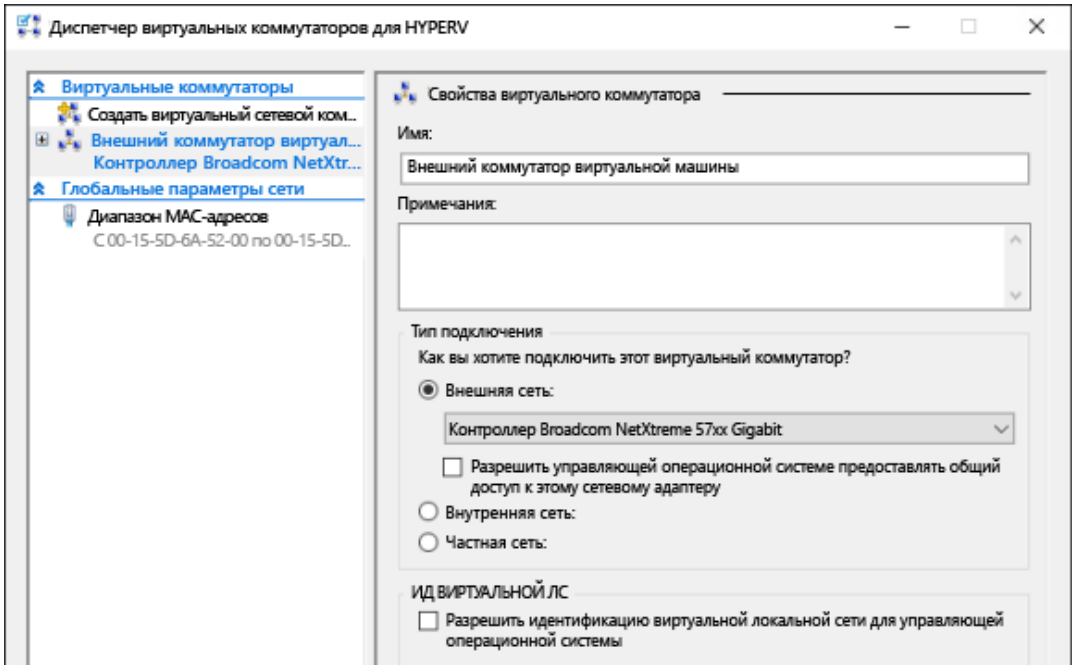


**Рис. 2.** Диспетчер виртуальных коммутаторов Hyper-V
**Fig. 2.** Hyper-V virtual switch manager

Условием для изоляции подсети виртуальной машины от подсети хоста является снятие флага «Разрешить управляющей ОС предоставлять доступ к этому сетевому адаптеру» (рис. 2).

В первых версиях Hyper-V (Windows Server 2008) настройка сети была организована иначе. Менеджер виртуальных сетей позволял создать виртуальную сеть (Virtual Network) и назначить ее выбранному сетевому адаптеру (рис. 3) посредством привязки к нему протокола *Microsoft Virtual Network Switch Protocol* (рис. 4). Полностью отвязать сетевой адаптер от хоста можно посредством снятия всех галочек напротив сетевых протоколов и служб в интерфейсе свойств сетевого адаптера (рис. 4).

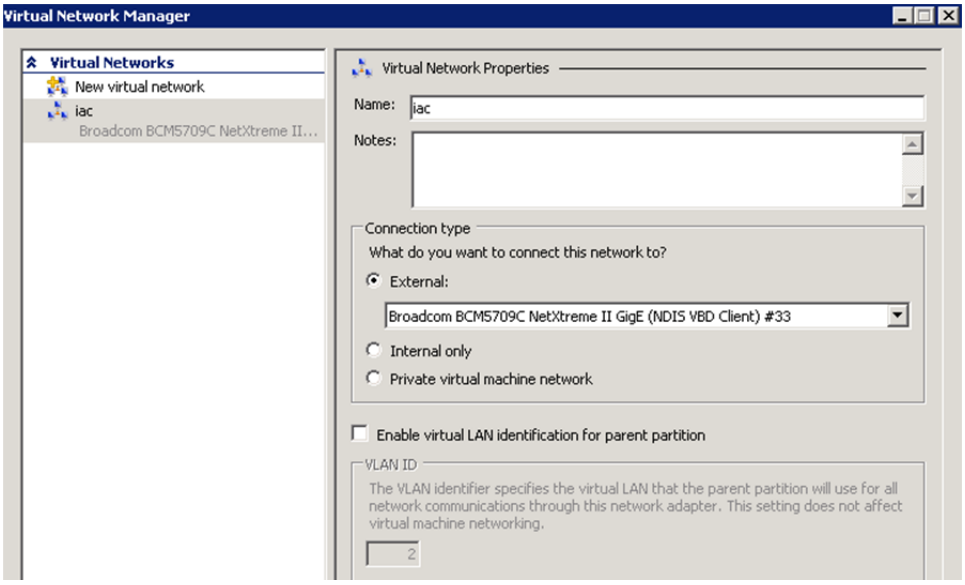


**Рис. 3.** Менеджер виртуальных сетей Windows Server 2008
**Fig. 3.** Virtual network manager of Windows Server 2008

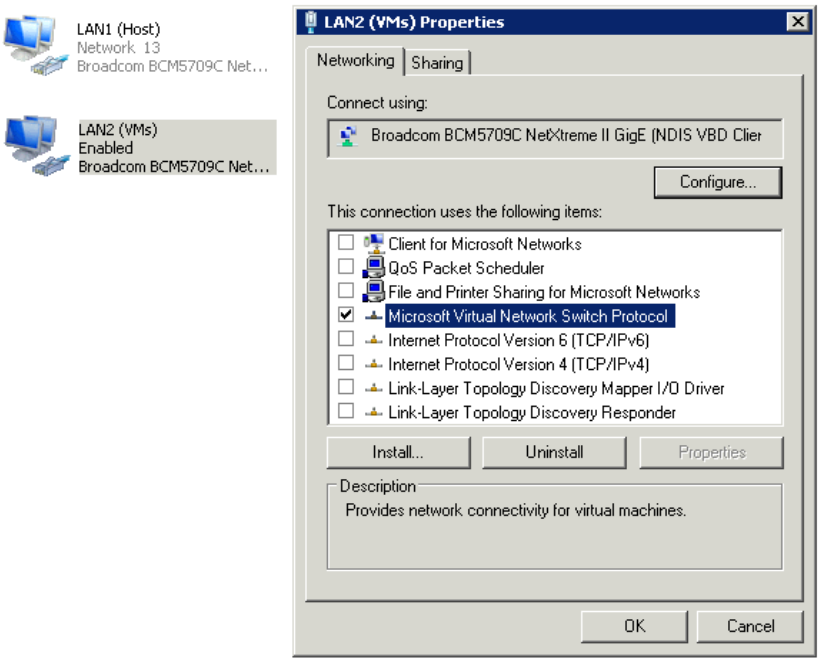


**Рис. 4.** Привязка протоколов и служб к сетевому адаптеру в Windows Server 2008
**Fig. 4.** Binding of protocols and services to a network adapter in Windows Server 2008

## ПЕРЕДАЧА ФАЙЛОВ МЕЖДУ ХОСТОМ И ВИРТУАЛЬНОЙ МАШИНОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СЕТИ

На предприятиях, имеющих разделение сети на два изолированных сегмента, может возникнуть необходимость передачи данных между внешним миром и сервером, расположенным во внутренней, изолированной от интернета сети. Такой случай возможен, если информационная система предприятия, развернутая на сервере внутренней сети, не может функционировать без данных, регулярно предоставляемых информационными системами клиентов предприятия.

С помощью криптографических средств можно обеспечить достаточную надежность идентификации отправителя и получателя, а также защитить передаваемые данные от перехвата и подмены. В частности, авторами статьи была разработана система автоматизированной передачи данных по защищенному каналу между несколькими информационными системами [7]. Однако в рассматриваемой архитектуре сети предприятия проблематична передача данных между внешней и внутренней ЛВС при условии соблюдения требования изоляции ЛВС на сетевом уровне.

Пропуск сетевых пакетов между ЛВС чреват тем, что потенциальные взломщики могут сгенерировать такие пакеты, которые могут:

- помочь злоумышленникам определить топологию внутренней сети;
- использовать уязвимости типа переполнения буфера;
- нести в себе команды, интерпретируемые и исполняемые сетевыми устройствами;
- нести в себе несанкционированно извлекаемые из внутренней сети данные.

Поскольку рассматриваемые информационные системы должны обмениваться исключительно файлами (а не командами), то решить задачу их безопасной передачи между сегментами сети можно, отказавшись от сетевых пакетов в качестве носителей данных и передавая непосредственно файлы через внутреннюю шину системы виртуализации.

Возможность двухсторонней передачи файлов между виртуальными машинами и хостом реализована для систем виртуализации, ориентированных на рабочие станции (настольные компьютеры, ноутбуки). В промышленных системах виртуализации такие решения не востребованы, поскольку гостевым виртуальным машинам нет необходимости обмениваться файлами с хостом, и такой обмен нарушил бы концепцию разграничения доступа к файлам с контролем учетных записей пользователей и списков доступа прав файлов, особенно если виртуальная машина и хост работают на разных платформах (Windows, Linux). Поэтому в промышленных решениях виртуализации передача файлов базируется на встроенных в операционные системы сетевых протоколах прикладного уровня для удаленного доступа к файлам:

- CIFS (Common Internet File System);
- SMB (Server Message Block);
- NFS (Network File System).

Справедливости ради, следует отметить, что Hyper-V способна передавать файлы с хоста внутрь виртуальной машины, используя сервисы интеграции Linux (англ. Linux Integration Services, LIS) [8], но невозможность передачи файлов из виртуальной машины на хост не позволяет решить поставленную задачу.

Передача и обработка данных, описанная в [7], выполняется автоматизированно, без участия операторов, гарантируя, что обменные файлы никогда не будут переданы на выполнение командному интерпретатору. Содержимое полученных обменных файлов будет рассматриваться обрабатывающими программами исключительно как структурированные данные, извлекаемые из файла по заранее предопределенным шаблонам. Даже если в обменный файл попадет тело вируса, то оно не будет извлечено, так как не будет соответствовать шаблону. При таких условиях отсутствие контроля прав доступа для файлов, передаваемых между виртуальными машинами и хостом, не является критичным для безопасности информационной системы.

Таким образом, обмен данными с другими информационными системами можно реализовать, если вынести в отдельную виртуальную машину сервер, принимающий и передающий данные через интернет по криптозащищенным каналам, и соединить его с сервером информационной системы на файловом уровне с помощью шины системы виртуализации.

Поскольку такой сервер будет наделен весьма ограниченным набором функций, он может быть реализован на компактной сборке Linux без графической оболочки, что делает сервер нетребовательным к ресурсам, позволяя запускать его в любых системах виртуализации, поддерживающих передачу файлов между хостом и виртуальными машинами, в том числе в системах, основанных на эмуляторах. ПО виртуализации, относящееся к классу эмуляторов, работает поверх существующей ОС компьютера-хоста и предоставляет ресурсы компьютера в пользование гостевым виртуальным машинам. Несмотря на то что скорость работы гостевых ОС может незначительно снижаться по сравнению с виртуализацией на базе гипервизора, эмуляция позволяет более гибко настраивать различные методы предоставления ресурсов хоста гостевым ОС, в том числе создать общую для разных ОС файловую папку.

К системам виртуализации, поддерживающим обмен файлами через общую папку, относятся VMware Workstation [9] и Oracle VM VirtualBox[3]. Первая является платной (лицензия стоит порядка $300), а вторая – бесплатная в версии, функциональности которой хватает для решения поставленной задачи, поэтому ниже будет рассмотрено использование виртуальной машины VirtualBox для организации файлового шлюза между хостом и гостевой машиной с одновременной изоляцией сетей, к которым эти машины подключены.

[3] VirtualBox – Википедия. [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/VirtualBox (дата обращения: 03.03.2019).

## ИЗОЛЯЦИЯ СЕТЕЙ И ПЕРЕДАЧА ФАЙЛОВ НА ПРИМЕРЕ VIRTUALBOX

Отличительной способностью ПО VirtualBox является его полная кроссплатформенность – в роли гостевой и хостовой ОС могут выступать практически все распространенные ОС в любой комбинации. VirtualBox имеет развитые средства конфигурирования (настраивать виртуальные машины и управлять ими можно как через графическую оболочку, так и утилитами командной строки) и предоставляет пять вариантов сопряжения подсетей гостевой и хостовой ОС [10], а также общую папку (англ. *Shared Folder*) для совместного доступа к файлам.

На рис. 5 изображена схема сети предприятия с использованием VirtualBox для размещения виртуального сервера, обменивающегося файлами через интернет с другими информационными системами по алгоритму [7], а также обменивающегося файлами через общую папку с сервером информационной системы предприятия, находящимся во внутреннем изолированном сегменте сети.

Из пяти вариантов настроек сети [10] изоляцию подсетей гостевой и хостовой ОС обеспечивает режим *Сетевой мост* (Bridged Networking). В случае использования Windows в качестве ОС хоста, VirtualBox создает в системе виртуальный сетевой адаптер и связывает его с физическим адаптером привязкой драйвера *VirtualBox NDIS6 Bridged Networking Driver* к виртуальному и физическому адаптерам (рис. 6).

В случае если компьютер имеет единственный сетевой адаптер, то ему присваивается сразу два MAC-адреса (от англ. *Media Access Control* – уникальный идентификатор, присваиваемый каждой единице активного оборудования в сетях Ethernet), благодаря чему физический адаптер представляется в сети как два независимых устройства, каждому из которых можно предоставить собственный IP-адрес с индивидуальными масками подсети, адресами шлюза и адресами DNS-серверов.

Если такой компьютер подключен к сети через коммутатор, не фильтрующий сетевые пакеты по IP-адресам, то одним физическим кабелем можно подключить хост и виртуальную машину сразу к двум сегментам сети.

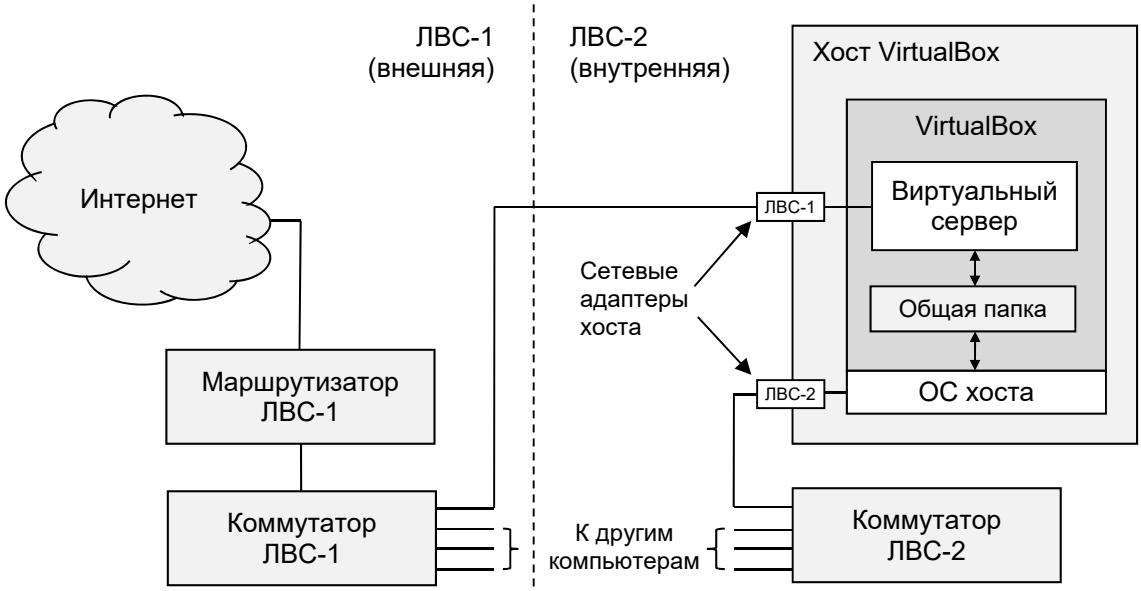


**Рис. 5.** Разделение сетей посредством VirtualBox
**Fig. 5.** Network separation using VirtualBox

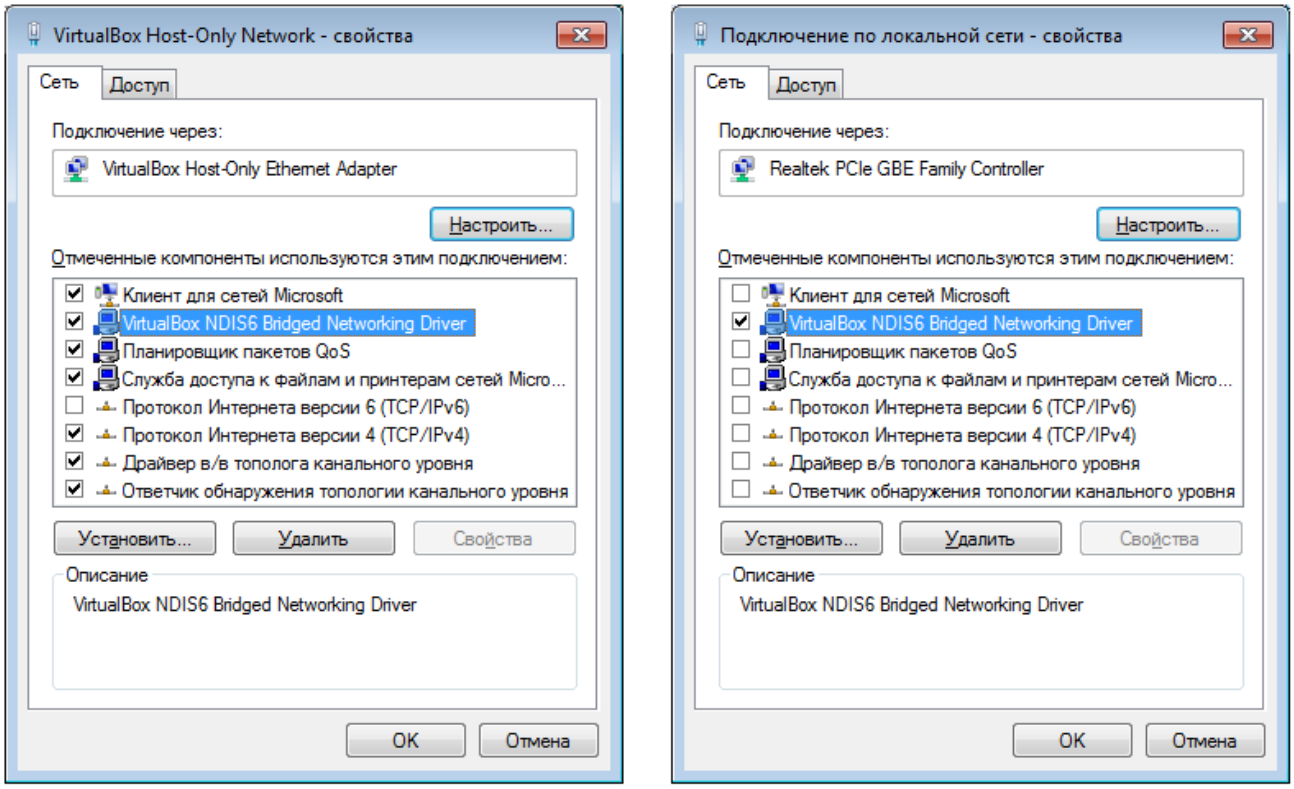


**Рис. 6.** Привязка протоколов и служб к сетевым адаптерам VirtualBox
**Fig. 6.** Binding of protocols and services to network adapters of VirtualBox

Однако, как и в случае рассмотренного выше метода подключения к сети виртуальных машин Hyper-V, нам интересен вариант с использованием двух сетевых адаптеров. Как показали натурные испытания, проведенные авторами статьи, VirtualBox позволяет полностью изолировать виртуальную машину от подсети хоста, если в настройках одного из двух сетевых адаптеров отключить привязку к нему всех протоколов и служб, за исключением *VirtualBox NDIS6 Bridged Networking Driver*.

Таким образом, VirtualBox позволяет обеспечить как изоляцию виртуального сервера на сетевом уровне, так и связывание на уровне файловой системы подключенного к интернету виртуального сервера сервиса обмена файлами с основным сервером информационной системы, расположенной во внутренней сети предприятия.

## ЗАКЛЮЧЕНИЕ

Вышеописанное решение задачи размещения связанных серверов в изолированных подсетях не является единственно возможным – тот же результат можно получить и другими способами, например с помощью использования технологий маркирования сетевых пакетов (VLAN) или их инкапсуляции (GRE, VPN). Но такие решения требуют настройки всего сетевого оборудования высококвалифицированными специалистами по сетям.

Предлагаемое же в статье решение с использованием дополнительного сетевого адаптера и кабеля не требует от подключающего сервер инженера навыков и знаний, выходящих за рамки уже используемых в сети предприятия технологий, поэтому новый сервер может быть подключен к сети штатным персоналом предприятия, что особо актуально для режимных предприятий, в которых привлечение сторонних специалистов весьма проблематично.

## СПИСОК ЛИТЕРАТУРЫ

1. **Кирпичев И.Г., Благоразумов А.К.** Защита данных Информационно-аналитической системы мониторинга летной годности воздушных судов // Научный вестник ГосНИИ ГА. 2012. № 2. С. 37–43.
2. **УваровА.С.** Настраиваем сеть в HyperV. [Электронный ресурс].«Интерфейс» Технический блог.URL: https://interface31.ru/tech_it/2014/01/nastraivaem-set--v-hyper-v.html (дата обращения 03.03.2019).
3. **Шаповал А.** Виртуализация сети в Hyper-V. Концепция. [Электронный ресурс]. URL: https://habr.com/company/microsoft/blog/173159/ (дата обращения:03.03.2019).
4. **Шаповал А.** Виртуализация сети в Hyper-V. Что нового в WindowsServer 2012 R2? [Электронный ресурс]. URL: https://habr.com/company/microsoft/blog/209684/ (дата обращения: 17.10.2018).
5. **Хабаров Д.** Понимание виртуальных сетей в MicrosoftHyper-V–MicrosoftTechNet [Электронный ресурс]. URL: https://blogs.technet.microsoft.com/ru_forum_support/2010/09/10/microsoft-hype/ (дата обращения: 03.03.2019).
6. **Cooley S.** Создание виртуальной сети – MicrosoftDocs [Электронный ресурс]. URL: https://docs.microsoft.com/ru-ru/virtualization/hyper-v-on-windows/quick-start/connect-to-network (дата обращения: 03.03.2019).
7. **Благоразумов А.К., Кирпичев И.Г.** Автоматизация информационного обмена в Информационно-аналитической системе мониторинга лётной годности воздушных судов // Научный вестник МГТУ ГА. 2011. №163. С. 204–209.
8. **Siron E.** 4 Ways to Transfer Files to a Linux Hyper-V Guest. [Электронныйресурс]. URL: https://www.altaro.com/hyper-v/transfer-files-linux-hyper-v-guest/ (дата обращения: 03.03.2019).
9. **Семин И.** Как создать общую папку между физическим компьютером и виртуальной машиной на VMwarework station 11. [Электронный ресурс]. URL: http://pyatilistnik.org/kak-sozdat-obshhuyu-papku-mezhdu-fizicheskim-kompyuterom-i-virtualnoy-mashinoy-na-vmware-workstation-11/ (дата обращения:03.03.2019).
10. **Smeets M.** VirtualBox networking explained. [Электронный ресурс]. URL: https://technology.amis.nl/2018/07/27/virtualbox-networking-explained (дата обращения: 03.03.2019).

## СВЕДЕНИЯ ОБ АВТОРАХ

**Благоразумов Андрей Кириллович,** начальник группы Информационно-аналитического центра, ФГУП «Государственный научно-исследовательский институт гражданской авиации», blagorazumov@mlgvs.ru.

**Кирпичев Игорь Геннадьевич,** доктор технических наук, профессор кафедры технической эксплуатации летательных аппаратов и авиадвигателей МГТУ ГА, i.kirpichev@mstuca.aero.

**Петров Дмитрий Владимирович,** ведущий инженер-программист, ПАО «Научно-производственное предприятие «Аэросила», petrovbox@gmail.com.

# ISOLATION OF CORPORATE LOCAL AREA NETWORKS USING SERVER VIRTUALIZATION

**Andrey K. Blagorazumov[1], Igor G. Kirpichev[2], Dmitry V. Petrov[3]**
[1]*The State Scientific Research Institute of Civil Aviation, Moscow, Russia*
[2]*Moscow State Technical University of Civil Aviation, Moscow, Russia*
[3]*PJSC Scientific Production Enterprise "Aerosila", Stupino, Russia*

## ABSTRACT

Secure enterprises have Local Area Networks (LANs) that store and process sensitive data that should not be accessed from outside. At the same time, no modern enterprise can successfully function without a LAN which provides the Internet access for the computers of the sales department, technical support service and E-mail server. In order to ensure information security, these two network segments are usually physically isolated from each other by means of exception of any cable interconnections. Enterprises with high demands for server uptime use server virtualization, which requires connecting physical servers to disk storage of virtual server image files. When highly reliable servers are needed only in one of two independent corporate network segments, the cost of creating such a server cluster is reasonable and fast paying off. But when a company encounters the need to place a small but highly reliable server into another network segment, the following problem arises: only server cluster with expensive components can provide the required reliability, but to solve the tasks assigned to the new server, the cluster computing capacity would be too high, and deploying of a cluster would be extremely costly and economically unjustified. On the other hand, the required computing capacity for a new server would be taken from the existing server cluster by creating a new virtual server without any expenses. However, in such case it is necessary to ensure isolation of the new virtual server from the network segment the physical hosts servers are connected to. The article examines the methods of configuring the LAN that allow to isolate virtual and physical servers at the network level. The authors also consider the episode when it is necessary to transfer files between the two computers located in the LAN segments isolated from each other and gives the appropriate solution.

**Key words:** local area network, LAN, virtualization, Hyper V, VirtualBox.

## REFERENCES

1. **Kirpichev, I.G. and Blagorazumov, A.K**. (2012). *Protection of data in the information analysis system for aircraft airworthiness monitoring.* Scientific Herald of the State Research Institute of Civil Aviation, 2012, no.2, pp. 37–43. (in Russian)
2. **Uvarov, A.S.** *Nastraivaem set v Hyper-V* [Configuring the network in Hyper-V]. Available at: https://interface31.ru/tech_it/2014/01/nastraivaem-set--v-hyper-v.html (accessed 03.03.2019). (in Russian)
3. **Shapoval, A.** *Virtualizatsiya seti v Hyper-V. Kontseptsiya* [Network virtualization in Hyper-V. The Concept]. Available at: https://habr.com/company/microsoft/blog/173159/ (accessed 03.03.2019). (in Russian)
4. **Shapoval, A.** *Virtualizatsiyaseti v Hyper-V. Chto novogo v Windows Server 2012 R2?* [Network Virtualization in Hyper-V. What's new in Windows Server 2012 R2?]. Available at: https://habr.com/company/microsoft/blog/209684/ (accessed 03.03.2019). (in Russian)
5. **Khabarov, D.** *Ponimanie virtualnykh setey v Microsoft Hyper-V Microsoft Tech Net* [Understanding of Microsoft Hyper-V Virtual Networks Microsoft Tech Net]. Available at: https://blogs.technet.microsoft.com/ru_forum_support/2010/09/10/microsoft-hype/ (accessed 03.03.2019). (in Russian)
6. **Cooley, S.** Create a virtual network – Microsoft Docs. Available at: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/connect-to-network (accessed 03.03.2019).
7. **Blagorazumov, A.K. and Kirpichev, I.G.** (2011). *Automation of Data Exchange in the Information Analysis System for Aircraft Airworthiness Monitoring.* Nauchnyi Vestnik MGTU GA, no.163, pp. 204–209. (in Russian)

**8. Siron, E.** 4 ways to transfer files to a Linux hyper v guest. Available at: https://www.altaro.com/hyper-v/transfer-files-linux-hyper-v-guest/ (accessed 03.03.2019).

**9. Semin, I.** *Kak sozdat obshchuyu papku mezhdu fizicheskim kompyuterom I virtualnoi mashinoi na V Mware workstation 1.* [How to create a shared folder between a physical computer and a virtual machine on VMware workstation 11]. Available at: http://pyatilistnik.org/kak-sozdat-obshhuyu-papku-mezhdu-fizicheskim-kompyuterom-i-virtualnoy-mashinoy-na-vmware-workstation-11/ (accessed 03.03.2019). (in Russian)

**10. Smeets, M.** Virtual Box networking explained. Available at: https://technology.amis.nl/2018/07/27/virtualbox-networking-explained (accessed 03.03.2019).

## INFORMATION ABOUT THE AUTHORS

**Andrey K. Blagorazumov,** Head of Group of the Information Analysis Center of The State Scientific Research Institute of Civil Aviation, blagorazumov@mlgvs.ru.

**Igor G. Kirpichev,** Doctor of Technical Sciences, Professor of Technical Operation of Aircraft and Engines Chair, Moscow State Technical University of Civil Aviation, i.kirpichev@mstuca.aero.

**Dmitry V. Petrov,** Senior Software Engineer, PJSC Scientific Production Enterprise "Aerosila", petrovbox@gmail.com.

| | | | |
|---|---|---|---|
| Поступила в редакцию | 24.03.2019 | Received | 24.03.2019 |
| Принята в печать | 14.11.2019 | Accepted for publication | 14.11.2019 |