Wireless solutions
for M2M world

Обеспечение доступа к внутрисетевым службам средствами PortForwarding

RUH, RUH2, RUH2b, RUH3, RCA

Содержание

Таблицы

Рисунки

1. Введение

1.1. Описание документа

Данный документ является частью пакета инструкций по применению роутера iRZ и содержит примеры конфигурации по обеспечению доступа к внутрисетевым службам средствами Port forwarding на базе роутеров iRZ. Данный документ не содержит всей информации по работе с роутером.

Версия документа		**Дата публикации**	
1.0		2013-03-22	
Подготовлено:	Афанасьев Д.С., Головин В.Н.	**Проверено:**	Павлов Д.С.

1.2. Обзор пакета инструкций

Вся документация на русском языке по продукции iRZ доступна на официальном сайте группы компаний «Радиофид» (www.radiofid.ru) в разделе «Поддержка».

Содержание «Пакета инструкций по обслуживанию роутера iRZ»:

- Руководство по эксплуатации роутера iRZ;
- Описание средств управления и мониторинга роутера iRZ;
- Диагностика и методы устранения неисправностей роутера iRZ;
- Руководство по настройке роутера iRZ с помощью USB-накопителя;
- Примеры рабочих конфигураций роутера iRZ:
  - Создание виртуальных сетей и туннелей средствами OpenVPN;
  - Удалённый доступ к COM-порту роутера;
  - Защита передаваемых данных средствами IPSec;
  - DynDNS и обход ограничений внешнего динамического IP-адреса;
  - Объединение сетей с помощью GRE-туннелей;
  - Отказоустойчивость уровня сети средствами VRRP;
  - **Обеспечение доступа к внутрисетевым службам средствами Port Forwarding;**
  - Защита локальной сети и сервисов средствами встроенного Firewall;
- Технические условия (ТУ);
- Протокол температурных испытаний;
- Декларация о соответствии.

1.3. Предупреждение

Отклонение от рекомендованных параметров и настроек может привести к непредсказуемым последствиям и значительным издержкам, как в процессе пуско-наладки вычислительного комплекса, так и во время эксплуатации production-версии вычислительного комплекса в «боевых» условиях.

Внимание! Прежде чем вносить любые изменения в настройки оборудования, устанавливаемого на объекты, настоятельно рекомендуется проверить работоспособность всех параметров новой конфигурации на тестовом стенде. Так же, не следует ограничиваться синтетическими тестами, а максимально реалистично воспроизвести условия, в которых будет эксплуатироваться оборудование.

2. Конфигурация «Доступ к службе устройства локальной сети»

Данная конфигурация призвана обеспечить доступ к сетевой службе (далее – «*локальной службе*») одного из узлов, находящегося в рамках локальной сети, обслуживаемой роутером, имеющим доступ в Интернет.

Обязательным условием работоспособности данной конфигурации является наличие у роутера **фиксированного**, либо **динамического внешнего IP-адреса** в Интернет. В случае, если планируется, что роутер iRZ будет получать доступ к всемирной сети через сотового оператора, а доступ к локальной службе будет осуществляться устройством, подключённым к Интернет так же через оператора сотовой связи, то настоятельно рекомендуется ознакомиться с блоком «Предупреждение», следующим далее.

Предупреждение: Для Северо-Западного региона России характерна невозможность установления связи между роутерами, когда на обоих устройствах используются SIM-карты одного и того же оператора сотовой связи – «Мегафон» или «МТС» (независимо от используемого тарифа и подключённых услуг, в т.ч. «Фиксированный IP-адрес» у «Мегафон», или «Реальный IP» у «МТС»). Поэтому перед заключением договора на предоставление телематических услуг с оператором, рекомендуется провести ряд тестов на возможность осуществления связи между устройствами, использующими SIM-карты данного оператора.

Данное ограничение недействительно для случаев использования выделенного APN.

Ниже (на рис. 2.1) представлена схема работы функции Port Forwarding:

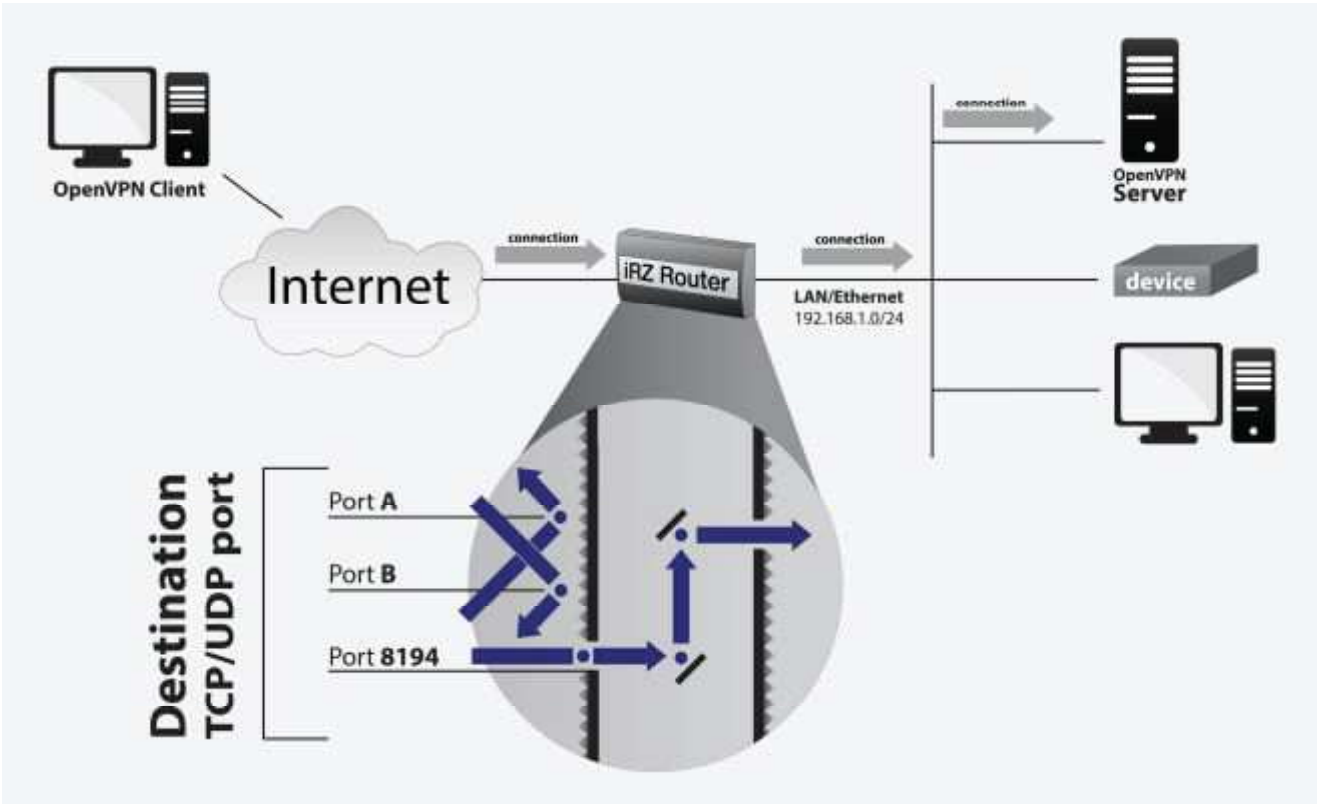

Рис. 2.1. Схема работы Port Forwarding

2.1. Подготовка к настройке

Процесс проектирования и развертывания данной конфигурации состоит из следующих этапов:

- определение характеристик и параметров функционирования локальной службы;
- настройка Интернет-подключения на роутере;
- предоставление на роутере доступа извне к службе узла локальной сети;
- проверка работоспособности конфигурации.

Описание процесса проектирования развёртываемой сети, а так же настройки Интернет-подключения на роутерах выходит за рамки данного документа. Для получения рекомендаций по проектированию следует обратиться к документу «**Руководство по развёртыванию решений на базе роутера iRZ**». Описание настройки Интернет-подключения на роутерах представлено в документе «**Руководство по эксплуатации роутеров iRZ**» (см. разд. «Интернет соединение по GSM-каналу»).

Далее описан процесс предоставления доступа к серверу OpenVPN, находящемуся в переделах локальной сети, обслуживаемой роутером iRZ и не доступному, изначально, для подключений, со стороны сети Интернет.

Предупреждение: Обязательные требования, несоблюдение которых сделает невозможным нормальную работу функции **Port Forwarding**:

- роутер iRZ и устройство/узел, на котором находится локальная служба должны иметь IP-адреса, находящиеся в одном адресном пространстве, либо должны быть как минимум доступны друг для друга (в случае использования опции “Send all remaining incoming packets to default server”);
- для обеспечения возможности прохождения трафика в обоих направлениях между клиентом службы и самой службой на участке “Роутер iRZ ←→ Локальная Служба” необходимо, чтобы на узле, на котором запущена локальная служба, в качестве значения параметра настроек сети «роутер по-умолчанию» должен был бы быть указан IP-адрес роутера iRZ.

Примечание: К процессу применения данной конфигурации следует приступать, когда служба, доступ к которой планируется предоставить уже проверена на работоспособность и надёжность функционирования.

ВНИМАНИЕ! Предоставление доступа к локальной службе со стороны Интернет может стать причиной несанкционированного доступа к ней третьих лиц. Прежде чем выполнять настройку функции **Port Forwarding** настоятельно рекомендуется убедиться в том, что версия используемого в работе локальной службы ПО актуальна и не имеет уязвимостей.

Так же, в случае, если локальная служба является web-интерфейсом, либо консольным интерфейсом управления какого-либо устройства настоятельно рекомендуется убедиться в том, что реквизиты доступа к этому устройству сменены. В случае, если реквизиты доступа, установленные на локальном устройстве по-умолчанию не были изменены – велик риск получения несанкционированного доступа к самому устройству, а также к локальным сетям, к которым оно подключено и любым другим узлам этой сети.

2.2. Определение характеристик и параметров локальной службы

Прежде чем выполнять настройку доступа к службе на роутере необходимо определить номер TCP/UDP порта и IP-адрес узла, на которых она функционирует. Эту информацию можно уточнить у администратора сети компании-заказчика.

Замечание: В случае если во внутреннюю сеть требуется перенаправить служебные пакеты ICMP-трафика, используемые, как правило, для проверки доступности узла, номер порта уточнять не требуется.

Примечание: В приложении 1 документа «**Защита локальной сети средствами встроенного сетевого экрана**» приведена таблица (табл. 1) соответствия номеров портов наиболее распространённым службам, используемым в локальных и глобальных вычислительных сетях. Руководствуясь данной таблицей можно уточнить номер порта локальной службы, доступ к которой необходимо разрешить.

В приложении 1 данного документа приведена (табл. 2) выдержка из таблицы 1, которая упомянута в примечании, содержащая сокращённый список служб, использование которых в рамках современных технических решений наиболее вероятно.

2.3. Предоставление доступа к службе

Предоставление доступа к локальной службе осуществляется на странице web-интерфейса роутера **Configuration → Port Forwarding**.

В данном примере будет рассмотрен простой вариант конфигурации роутера, позволяющий обеспечить доступ к серверу OpenVPN со стороны сети Интернет, при условии, что роутер будет иметь внешний IP адрес, а так же будет задействована служба клиента DynDNS, позволяющая всегда иметь информацию о текущем IP-адресе роутера.

Далее приведена таблица 1 с описанием параметров конфигурации функции Port Forwarding и значениями в данной конфигурации, а так же приведён пример конфигурации клиента OpenVPN (фрагмент файла настроек, листинг 1), обращающегося к серверу OpenVPN через роутер iRZ.

Таблица 1. Конфигурация функции Port Forwarding

Название параметра	Значение в данной конфигурации	Описание
Public Port	**8194**	TCP/UDP-порт, к которому должен будет подключаться клиент службы со стороны Интернет
Private Port	**1194**	локальный TCP/UDP-порт, который используется службой в локальной сети фактически
Type	**TCP/UDP**	тип порта
Server IP Address	**192.168.1.100**	IP-адрес узла локальной сети, на котором запущена служба

Предупреждение: В целях безопасности, для параметра **Public Port** рекомендуется использовать значение, отличное от номера порта, используемого локальной службой по-умолчанию. Это снизит риск возможных попыток сканирования на предмет уязвимости службы со стороны Интернет потенциальными злоумышленниками.
Из табл. 1 видно, что несмотря на то, что служба OpenVPN использует TCP-порт **1194** доступ к ней извне можно получить, только подключившись к порту **8194** роутера.

Листинг 1. Пример фрагмента файла настроек клиента OpenVPN в данной конфигурации

```
..
proto tcp
remote irz-server.no-ip.com 8194
..
```

2.4. Проверка работоспособности конфигурации

Для проверки работоспособности данной конфигурации требуется выполнить следующие действия:

1. Открыть командную строку ОС Windows на компьютере, имеющего доступ к сети Интернет, но не подключённого к настраиваемому роутеру;
   («Пуск» → «Выполнить» → ввести «cmd» → [Enter])
2. Ввести команду «telnet [внешний IP-адрес роутера] [номер внешнего порта]»;
   (в этом примере: telnet X.X.X.X 8194)
3. В случае если в течение небольшого периода (от нескольких секунд до минуты) окно консоли очистилось – подключение к локальной службе через роутер прошло успешно.

Рекомендация: В случае если по каким-то причинам этого не произошло, рекомендуется обратиться к разделу «Разрешение проблем в ходе эксплуатации функции Port Forwarding» документа «**Диагностика и методы устранения неисправностей роутера iRZ**» в целях сокращения времени поиска и устранения возможных неисправностей.

2.5. Частные случаи использования функции Port Forwarding

Опция Send all remaining incoming packets to default server / Default Server IP Address

В ряде случаев может возникнуть необходимость предоставить доступ к локальной службе в условиях, которые предполагают использования в схеме сети зону DMZ (демилитаризованную зону). Данная опция призвана реализовать эту схему.

Для этого необходимо поставить галочку напротив надписи «Send all incoming packets to default server», а затем указать IP-адрес узла, который будет принимать все подключения, не попадающие под правила, определённые в 10-строчной таблице перенаправления портов блока «**Port Forwarding**» на странице **Configuration → Port Forwarding**. Механизм работы данной функции представлен на рис. 2.2.

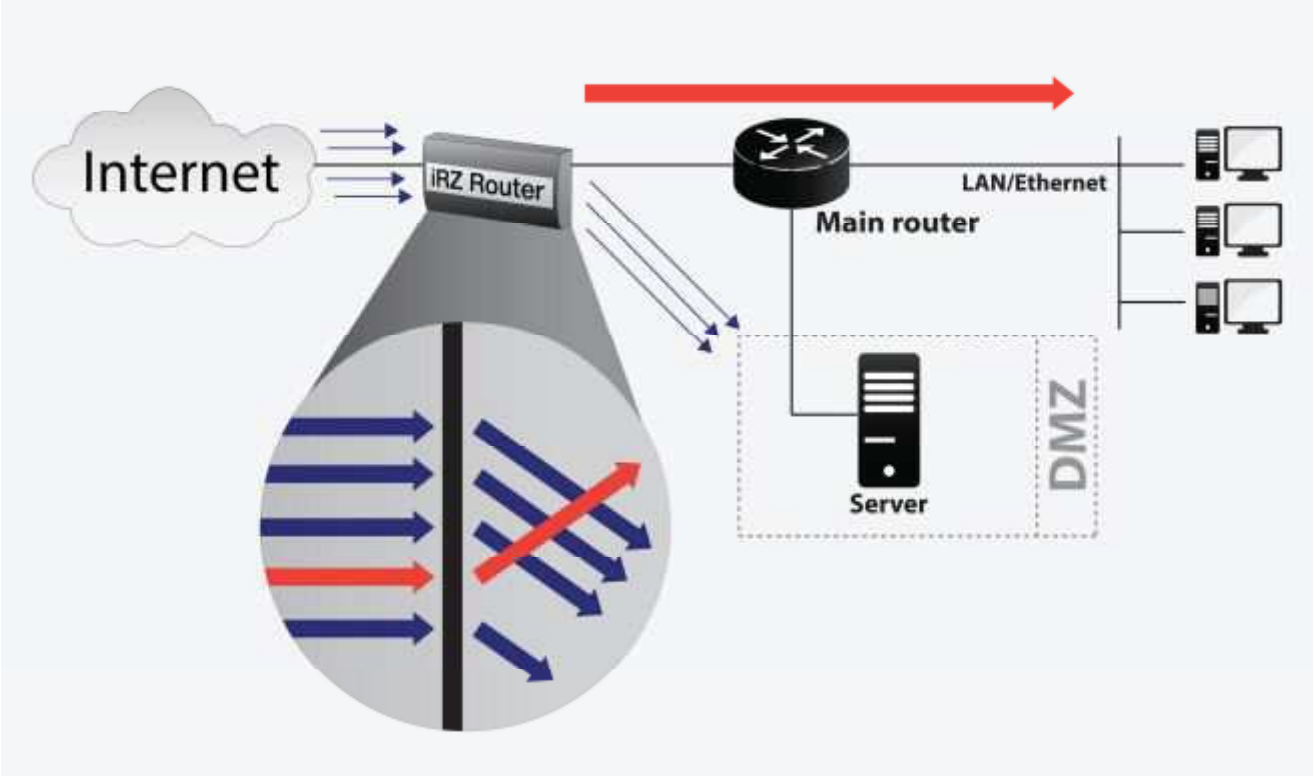

Рис. 2.2. Использование функции Port Forwarding

Опция Enable UPnP/NAT-PMP

Данная опция позволяет снять ограничения NAT, не позволяющие установить узлам в сети Интернет связь с узлами в локальной сети. Однако, задействовать этот механизм (при условии, что опция включена) могут только узлы локальной сети, проявив инициативу в обращении к роутеру с запросом о его внешнем IP-адресе и о предоставлении разрешений для подключения к ним со стороны Интернет по указанным портам. Это позволяет, в большинстве случаев, улучшить характеристики канала связи (пропускная способность, надёжность, время отклика) для программного обеспечения, работающего в пиринговых децентрализованных сетях (торрент-клиенты, Skype и социальные сети, использующие схему доставки контента посредством **p2p**).

Опция Do not masquerade outgoing traffic (use with caution)

Данная опция призвана изменить поведение механизма трансляции адресов, сохраняя в пакетах, отправленных узлом локальной сети, обслуживаемой роутером, служебную информацию, содержащую IP-адрес отправителя.

Эта функция может быть полезна в решениях, где предполагается использование проводного подключения к Интернет, либо взаимодействия роутера с частными арендованными компанией-заказчиком локальными сетями оператора сотовой связи.

3. Приложение 1

Таблица 2 содержит список служб, которые, как правило используются в тех или иных современных технических проектах. Например, удалённый офис/филиал, каналы защищённой связи, удалённый доступ к интерфейсу управления устройством/сервером, обмен файлами и создание общих ресурсов в сети с географически разнесёнными точками, автоматизированный сбор информации и мониторинг, системы организации аудио- и видеоконференций и общения, и пр.

Таблица 2. Краткий список номеров портов наиболее часто используемых сетевых служб

Название службы *(в алфав. порядке)*	**Тип соединения** *(TCP/UDP)*	**№ порта(ов)**	**Краткое описание назначения**
Citrix (ICA)	TCP	**1494**	Сервис удалённого управления компьютером
DameWare NT	TCP	**6129**	Сервис удалённого управления компьютером
DNS	UDP	**53**	Служба разрешения доменных имён
DHCP	UDP	**67/68**	Автонастройка IP-адреса
DynDNS	TCP	**→ → →**	*(по-умолчанию – HTTP)*
FTP	TCP	**21**	Служба обмена файлами в сети
FTP-DATA	TCP	**20**	Служба обмена файлами в сети
HTTP	TCP	**80**	Web-интерфейс устройства
HTTPS	TCP	**443**	Web-интерфейс устройства
ICQ	TCP	**5190**	Служба обмена мгновенными сообщениями
IPSec (ISAKMP)	UDP	**500**	Средство защиты данных в рамках сети
IPSec (NAT-T)	UDP	**4500**	Средство защиты данных в рамках сети
Microsoft sharing	TCP	**137/138/139/445**	Общий доступ к файлам и каталогам Windows
OpenVPN	TCP/UDP	**1194**	Сервис туннелинга и защиты данных в сети
RAdmin	TCP	**4899**	Сервис удалённого управления компьютером
RDP	TCP	**3389**	Сервис удалённого управления компьютером
POP3	TCP	**110**	Сервис получения электронной почты
PPtP	TCP	**1723**	Сервис туннелинга и защиты данных в сети
RTMP	TCP/UDP	**1935/80**	Сервис передачи медиапотока (конференции)
SIP	TCP/UDP	**5060**	IP-телефония (Интернет-телефония)
SIP-TLS	TCP	**5061**	Защищённая IP-телефония (over TLS)
Skype	TCP/UDP	**> 1024, 80**	Аудио/видео конференции, служба обмена мгновенными сообщениями
SMTP	TCP	**25**	Сервис отправки электронной почты
SNMP	TCP/UDP	**161**	Сервис управления сетевыми устройствами
SSH	TCP	**22**	Удалённая консоль управления (защищенная)
Telnet	TCP	**23**	Удалённая консоль управления устройством
VNC (RealVNC)	TCP	**5900/5800/6000**	Сервис удалённого управления компьютером