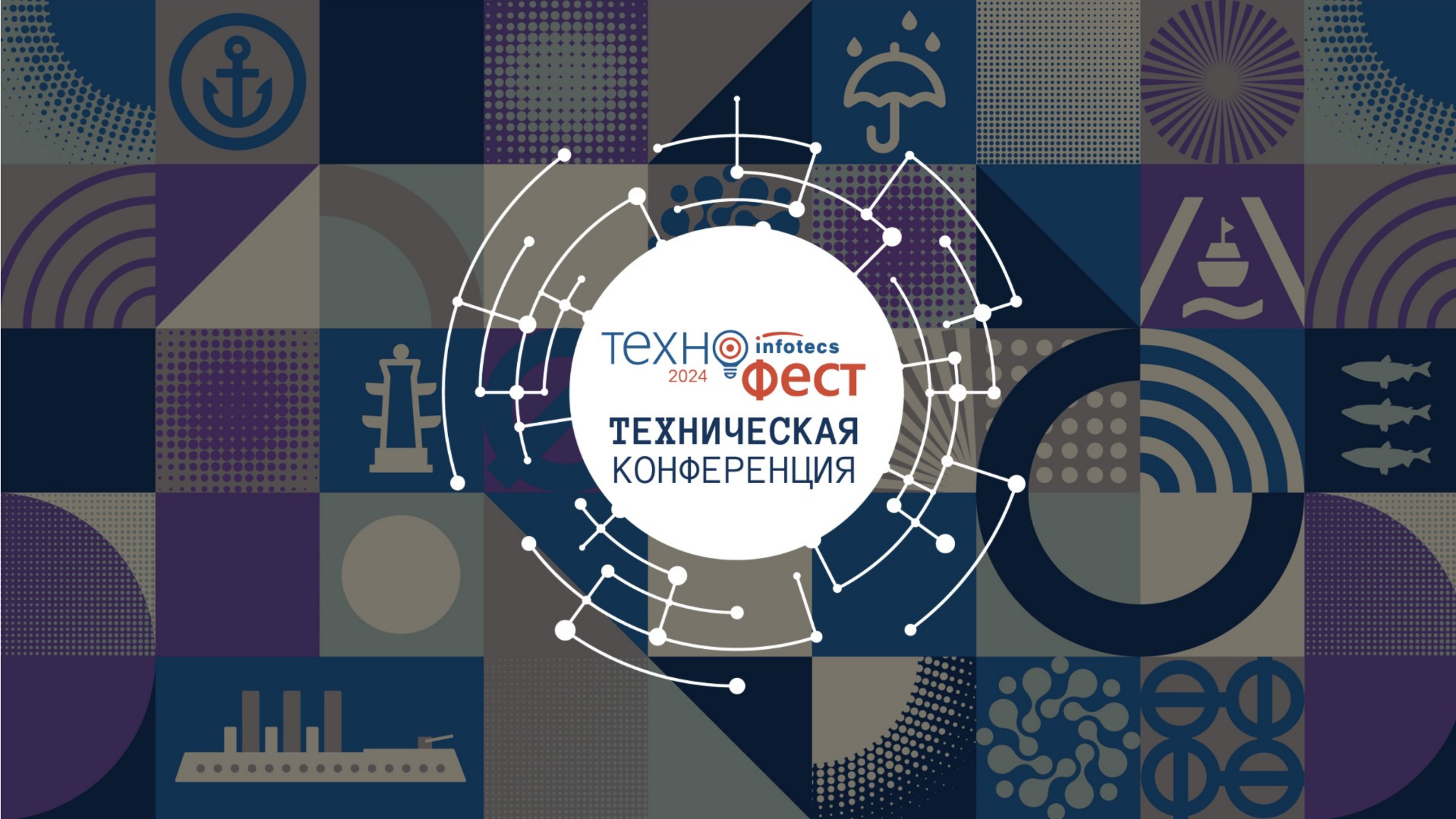

ТЕХНО
2024
infotecs
ФЕСТ
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

TS Solution

2024

Настройка кластера ViPNet Coordinator HW с технологией L2OverIP

Михаил Карлин

Ведущий специалист по защите информации

VIPNET COORDINATOR

- **ViPNet Coordinator HW** – это шлюз безопасности, предназначеннsый для построения виртуальной сети ViPNet и обеспечения безопасной передачи данных между её защищенными сегментами, а также фильтрации IP-трафика.

- Благодаря функциям криптографической защиты данных, межсетевого экранирования, а также наличию встроенных сетевых сервисов ПАК ViPNetCoordinator HW 4 является оптимальным средством защиты компьютерных сетей организаций от несанкционированного доступа к ее ресурсам при передаче информации по открытым каналам связи.

ViPNet Coordinator HW 50

ViPNet Coordinator HW 100

ViPNet Coordinator HW 1000

ViPNet Coordinator HW 2000

ViPNet Coordinator HW 5000

ОСНОВНЫЕ ФУНКЦИИ VIPNET COORDINATOR

- **Сервер IP-адресов** - обеспечивает взаимодействие защищенных узлов ViPNet. Сообщает сетевым узлам информацию об адресах и параметрах доступа других узлов.

  Принцип работы сервера IP-адресов:

  - При появлении новой информации о клиенте, координатор рассылает ее на связанные клиенты и координаторы
  - При появлении новой информации о клиентах других координаторов, координатор рассылает эту информацию на свои клиенты, которые связаны с клиентами другого координатора
  - Отсылает информацию о состоянии клиентов на шлюзовой координатор другой сети ViPNet

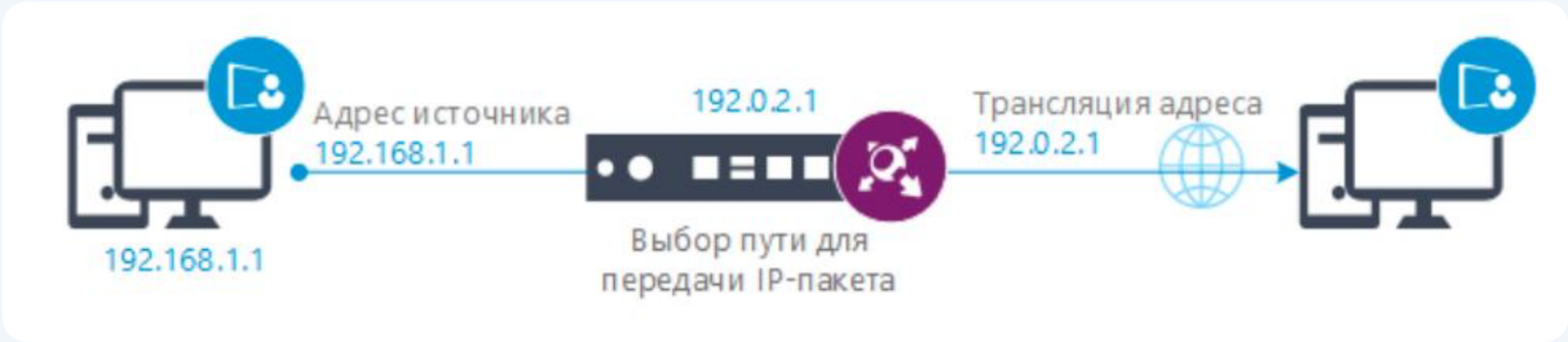
- **Транспортный сервер MFTP**. Обеспечивает доставку на сетевые узлы управляющих сообщений, обновлений справочников, ключей и программного обеспечения из ViPNet ЦУС или Prime, а также обмен прикладными транспортными конвертами между узлами

- **Защищенный интернет-шлюз**. Обеспечивает раздельный доступ защищенных узлов в интернет и к ресурсам защищенной сети ViPNet

- **Межсетевой экран**. Фильтрует IP-трафик на основе заданных правил; транслирует адреса (NAT) для открытого IP-трафика

ОСНОВНЫЕ ФУНКЦИИ VIPNET COORDINATOR

Маршрутизатор VPN-пакетов. Обеспечивает маршрутизацию транзитного защищенного IP-трафика, проходящего через координатор на другие защищенные узлы.



Маршрутизация защищенного трафика осуществляется на основании идентификаторов защищенных узлов, содержащихся в открытой части IP-пакетов, которая защищена от подделки, и на основании защищенного протокола динамической маршрутизации трафика. Одновременно с этим для защищенного трафика выполняется трансляция сетевых адресов (NAT).

ОСНОВНЫЕ ФУНКЦИИ VIPNET COORDINATOR

Сервер соединений - обеспечивает соединение клиентов и координаторов друг с другом.

Для каждого сетевого узла (клиента и координатора) можно назначить свой сервер соединений. По умолчанию сервером соединений для клиента служит координатор, выполняющий функцию **сервера IP-адресов**.

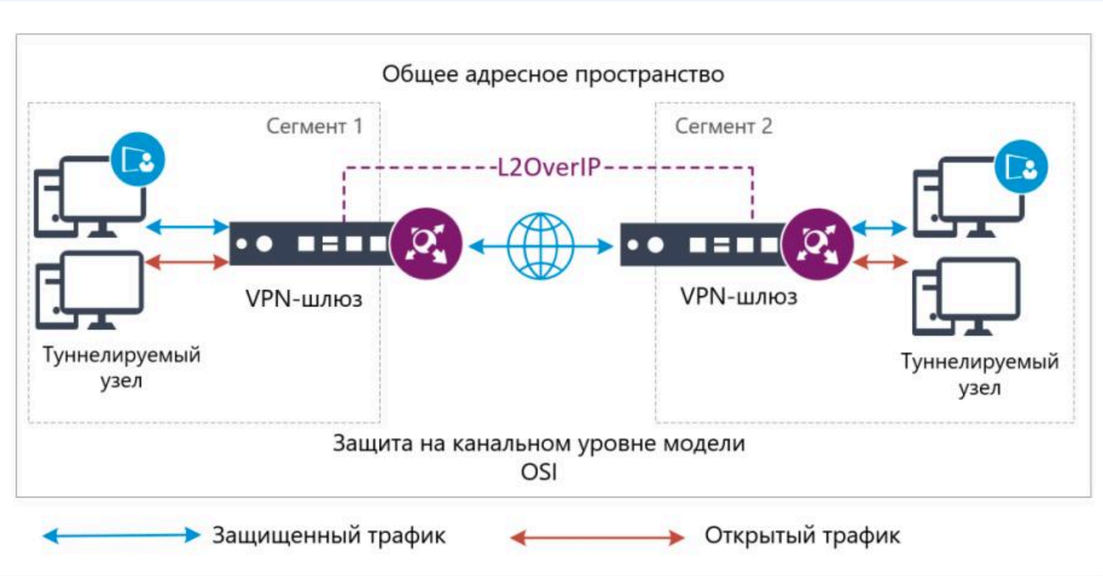
Когда удаленный клиент не может получить доступ к сети ViPNet по протоколу UDP (интернет-провайдер блокирует протокол UDP), он автоматически устанавливает связь через TCP-туннель своего **сервера соединений**. На сервере полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узлы назначения по протоколу UDP.

ОСНОВНЫЕ ФУНКЦИИ VIPNET COORDINATOR

VPN-шлюз

Координатор защищает соединения между узлами сети, которые обмениваются информацией через публичные сети. Для защиты соединения используется туннелирование. Координатор может выполнять туннелирование на сетевом (L3) или канальном (L2) уровнях модели OSI

Туннелирование на канальном уровне, или L2OverIP, позволяет организовать защищенное соединение между узлами удаленных друг от друга сегментов сети так, что они находятся в одном широковещательном домене. На узлах сегментов сети, связанных через L2OverIP, используется адресное пространство в пределах одной IP-подсети



НАЗНАЧЕНИЕ СИСТЕМЫ ЗАЩИТЫ ОТ СБОЕВ

Система защиты от сбоев предназначена для контроля работоспособности ПО ViPNetCoordinator HW и создания отказоустойчивого решения на базе двух ViPNetCoordinator HW. Система может работать в одиночном режиме или в режиме кластера горячего резервирования. Параметры работы системы защиты от сбоев задаются в файле failover.ini.

Работа системы защиты от сбоев в одиночном режиме

По умолчанию система защиты от сбоев работает в одиночном режиме и обеспечивает:

- Контроль собственной работоспособности
- Контроль работоспособности запущенных служб и драйверов ViPNetCoordinator HW, ведение статистики использования системных ресурсов
- Контроль сбоев при обработке IP-пакетов драйвером ViPNet

В состав системы защиты от сбоев входят watchdog-драйвер itcswd и служба failoverd. При загрузке системы сначала запускается watchdog-драйвер, а затем служба failoverd, которая запускает остальные службы и драйверы. Watchdog-драйвер itcswd и служба failoverd работают в фоновом режиме.

НАЗНАЧЕНИЕ СИСТЕМЫ ЗАЩИТЫ ОТ СБОЕВ

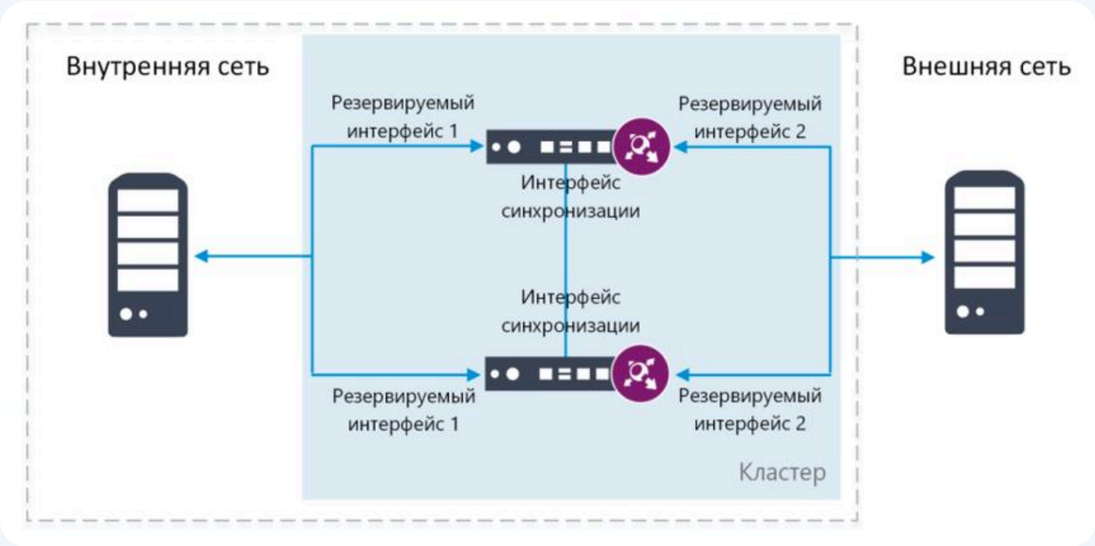
Работа системы защиты от сбоев в режиме кластера горячего резервирования

Система защиты от сбоев позволяет объединить два ViPNetCoordinator HW с одинаковой аппаратной платформой в кластер горячего резервирования. Кластер состоит из двух узлов:

- Активный узел — выполняет функции координатора ViPNet
- Пассивный узел — находится в режиме ожидания

В случае нарушения работоспособности активного узла, пассивный узел переключается в активный режим и выполняет функции сбойного узла, а сбойный узел переходит в пассивный режим

Наличие канала передачи данных между узлами кластера позволяет пассивному узлу содержать актуальные конфигурационные файлы, журналы, справочники и ключи на момент переключения в активный режим. Для этого активный узел кластера периодически передает указанные данные на пассивный узел



АЛГОРИТМ ПРОВЕРКИ РАБОТОСПОСОБНОСТИ КЛАСТЕРА

Алгоритм проверки работоспособности активного узла кластера:

1. Пассивный узел периодически проверяет присутствие в сети интерфейсов с IP-адресами активного узла кластера. Для этого используются ARP-запросы в режиме Duplicateaddressdetection. Если нет возможности обеспечить прохождение запросов за указанное время, увеличьте время ожидания ответа на ARP-запрос (параметр timeout)

2. Если ни один из резервируемых интерфейсов активного узла не отвечает на запросы, счетчик сбоев увеличивается на единицу. Если хотя бы один интерфейс ответил на запрос, счетчик сбоев сбрасывается

3. При достижении счетчиком порогового значения активный узел считается неработоспособным, и пассивный узел переходит в активный режим

Алгоритм проверки работоспособности интерфейсов активного узла кластера:

1. Активный узел периодически анализирует IP-трафик, проходящий через каждый из своих резервируемых интерфейсов

2. Если за определенный период времени не зафиксировано ни одного отправленного и принятого IP-пакета, выполняется дополнительная проверка — через каждый интерфейс посылаются эхо-запросы заданным объектам сети (например, маршрутизаторам)

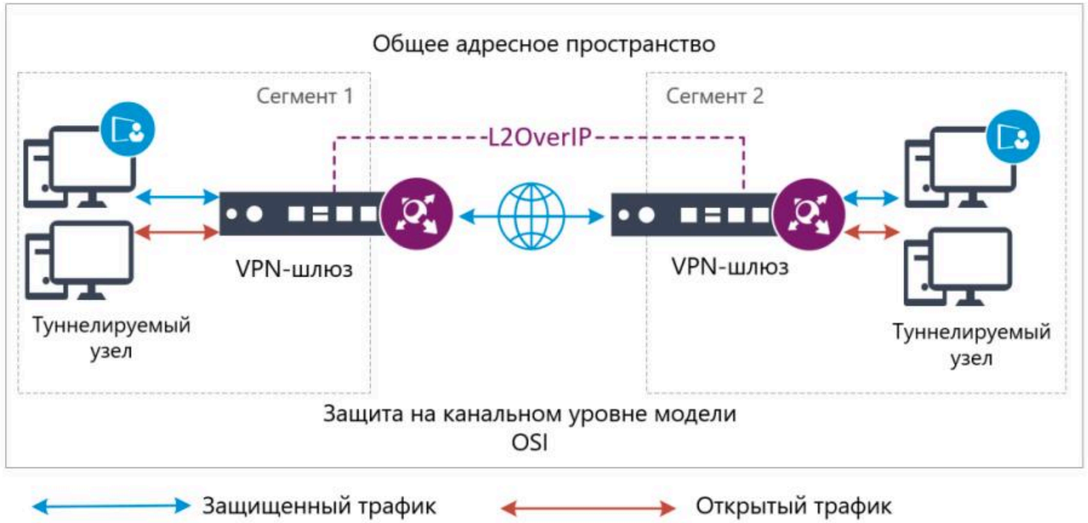
3. При отсутствии ответов на эхо-запросы, счетчик отказов для соответствующего интерфейса увеличивается на единицу. Если получен хотя бы один ответ или зафиксирован трафик на интерфейсе, счетчик сбрасывается

4. При достижении счетчиком порогового значения интерфейс считается неработоспособным, и активный узел переключается в пассивный режим, а пассивный узел становится активным

ТЕХНОЛОГИЯ L2OVERIP

Технология L2OverIP предполагает взаимодействие между узлами нескольких удаленных сегментов сети через ViPNet Coordinator HW, которые установлены на границе этих сегментов. В основе технологии лежит перехват на канальном уровне модели OSI Ethernet-кадров, отправленных из одного сегмента сети в другой. ViPNet Coordinator HW осуществляет перехват Ethernet-кадров, отправленных из его сегмента сети в другой, их упаковку в IP-пакеты специального формата и передачу этих IP-пакетов другому ViPNet Coordinator HW по защищенному каналу. ViPNet Coordinator HW, получивший IP-пакеты специального формата, извлекает из них исходные кадры и передает получателям в своем сегменте.

При использовании L2OverIP ViPNet Coordinator HW работает как виртуальный сетевой коммутатор. Каждому сегменту сети назначается свой номер порта, который задается в настройках L2OverIP. Порт, заданный для собственного сегмента сети, называется локальным. Порты, заданные на ViPNet Coordinator HW в других сегментах, называются удаленными. Трафик самого ViPNet Coordinator HW всегда относится к порту с номером 0.



НАСТРОЙКА КЛАСТЕРА VIPNET COORDINATOR

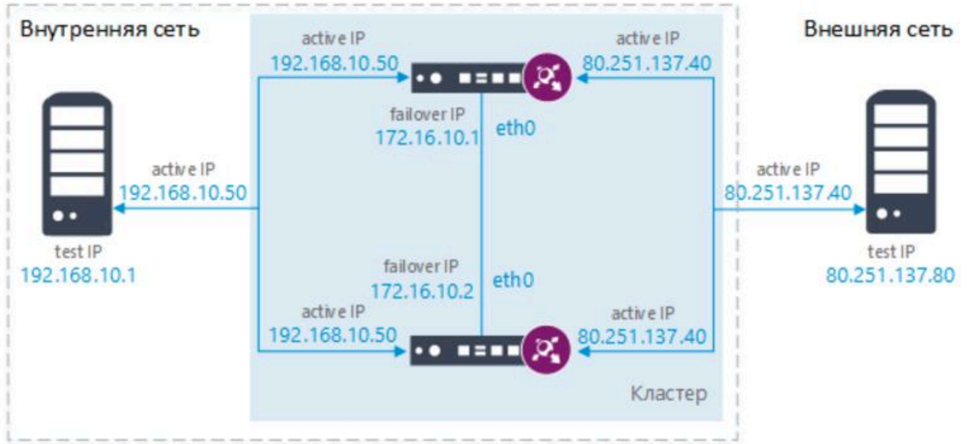
Перед развертыванием кластера горячего резервирования требуется:

1. Убедиться, что оба ViPNetCoordinator HW имеют одинаковую аппаратную платформу и версию ПО. Кластер на базе ViPNetCoordinator VA - оба узла должны иметь одинаковые количество процессоров, ОЗУ и сетевых интерфейсов
2. Отключить от локальной сети оба ViPNetCoordinator HW, которые будут входить в состав кластера. Это позволит избежать проблем в работе локальной сети и рассылке справочно-ключевой информации в сети ViPNet
3. Установить на оба ViPNetCoordinator HW одинаковые справочники и ключи одним из следующих способов:
   - Установите один дистрибутив ключей (файл *.dst) на оба ViPNetCoordinator HW
   - Перенесите справочники и ключи с одного ViPNet Coordinator HW на другой (файл *.vbe)
4. Если вы разворачиваете кластер на исполнениях HW50 или HW100, то убедитесь, что для них в ViPNet ЦУС или Prime задана роль (функция) Failover100
5. Выбрать сетевые интерфейсы, которые будут использоваться в качестве резервируемых интерфейсов. Вы также можете использовать виртуальные или VLAN интерфейсы
6. Убедиться, что в настройках резервируемых интерфейсов заданы статические IP-адреса, установлен класс access, и данные интерфейсы включены
7. На каждом ViPNet Coordinator HW выбрать сетевой интерфейс, который будет использоваться в качестве интерфейса синхронизации, соедините и настройте их. IP-адреса интерфейсов синхронизации должны принадлежать одной сети
8. Выбрать один или несколько стабильных объектов сети (например, маршрутизатор), которые будут использоваться для проверки работоспособности интерфейсов активного узла кластера

НАСТРОЙКА КЛАСТЕРА VIPNET COORDINATOR

Для развертывания кластера выполните следующие действия на каждом из ViPNet Coordinator HW:

1. Завершите работу службы системы защиты от сбоев: **hostname# failover stop**
2. Откройте файл failover.ini для редактирования: **hostname# failoverconfigedit**
3. При необходимости измените другие параметры секции [sendconfig] и [network] файла failover.ini.
4. Сохраните изменения и закройте редактор.



Настройка на первом узле	Настройка на втором узле
[channel] device = eth1 activeip = 192.168.10.50/24 testip = 192.168.10.1 testdevice = eth1 ident = internal checkonlyidle = yes	[channel] device = eth1 activeip = 192.168.10.50/24 testip = 192.168.10.1 testdevice = eth1 ident = internal checkonlyidle = yes
[channel] device = eth2 activeip = 80.251.137.40/24 testip = 80.251.137.80 testdevice = eth2 ident = external checkonlyidle = yes usevirtualmac = yes	[channel] device = eth2 activeip = 80.251.137.40/24 testip = 80.251.137.80 testdevice = eth2 ident = external checkonlyidle = yes usevirtualmac = yes
[misc] syncconnections = yes	[misc] syncconnections = yes
[network] checktime = 10 timeout = 2 activeretries = 3 channelretries = 3 synctime = 5 fastdown = yes virtualmacprefix = 39	[network] checktime = 10 timeout = 2 activeretries = 3 channelretries = 3 synctime = 5 fastdown = yes virtualmacprefix = 39
[sendconfig] device = eth0 activeip = 172.16.10.2 **(соответствует failover IP второго узла)**	[sendconfig] device = eth0 activeip = 172.16.10.1 **(соответствует failover IP первого узла)**

НАСТРОЙКА КЛАСТЕРА VIPNET COORDINATOR

5 Переведите систему защиты от сбоев в режим кластера горячего резервирования:
hostname# failover config mode cluster

6 Подключите оба ViPNet Coordinator HW к локальной сети

7 Проверьте связь с каждым IP-адресом, заданным в параметре testip секции [channel] файла failover.ini:
hostname# inet ping

8 Запустите систему защиты от сбоев:
hostname# failover start {active | passive}

Если активный узел кластера уже запущен, перед запуском службы на втором узле кластера, сначала проверьте доступность активного узла:

hostname# failover show active-mac-address

В случае успешной проверки будет выведен список активных сетевых интерфейсов кластера

Так же командой **failover show info** можно посмотреть состояние кластера и работоспособности демонов ViPNet Coordinator HW

Кластер ViPNet Coordinator HW настроен

```
HW5000-Q2-192804bd-N2# failover show active-mac-address
Address check is in progress ...
Interface       IP-address      MAC-address
bond0           10.100.252.250  00:E0:ED:E6:C9:4A
HW5000-Q2-192804bd-N2#
```

```
HW5000-Q2-192804bd-N1# failover show info
Running failover info
Versions: ViPNet 4.5.2 (237), daemon 1.5 (1)
Workstation configured for ID 192804BD (SPb-Sm3-HW5000)
The workstation works in a cluster mode of protection against failures
Workstation time (utc: 1715604074) Mon May 13 15:41:14 2024

                    * local             * remote
failover mode       * active            * passive
failover uptime     * 17d  3:06         * 6d 19:35
total cpu           * 4%                * 0%
total memory        * 65834776 Kb       * 65912364 Kb
available memory    * 64342432 Kb       * 64452500 Kb
failover state      * works             * works
failover cpu        * 0%                * 0%
iplir state         * works             * works
iplir cpu           * 0%                * 0%
mftp state          * works             * works
mftp cpu            * 0%                * 0%
webgui state        * works             * stopped
webgui cpu          * 0%                * 0%
HW5000-Q2-192804bd-N1#
```

НАСТРОЙКА ТЕХНОЛОГИИ L2OVERIP

Чтобы организовать защиту соединения сегментов, на каждом ViPNet Coordinator HW настройте функцию L2OverIP:

1 Укажите сетевой интерфейс, сегмент сети которого будет объединяться с другим сегментом с помощью функции L2OverIP:

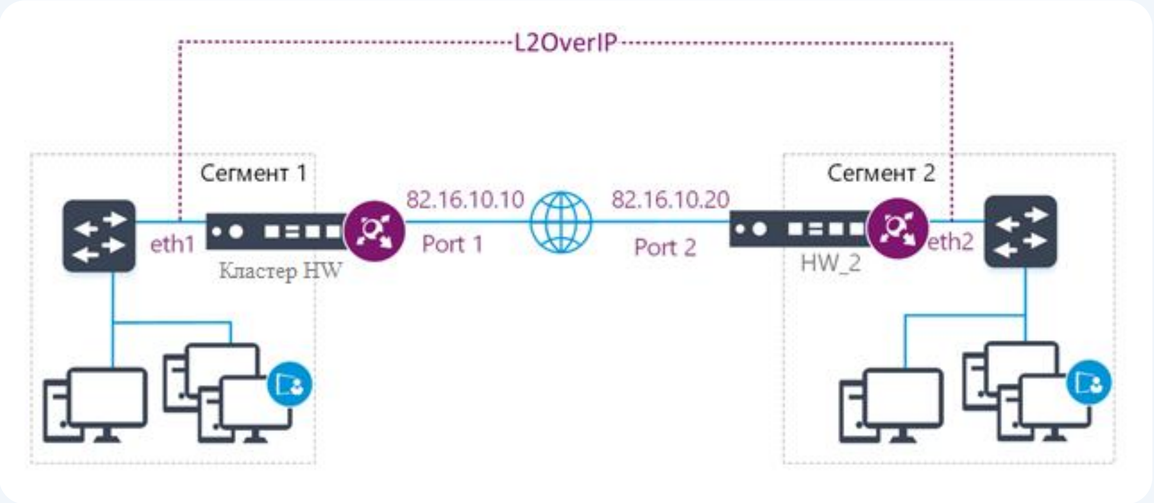
- На Кластере HW:
  hostname# iplir set l2overip interface eth1
- На HW-2:
  hostname# iplir set l2overip interface eth2

2 Задайте параметры локального сегмента сети

- На Кластере HW:
  hostname# iplir set l2overip local-port 1 82.16.10.10
- На HW-2:
  hostname# iplir set l2overip local-port 2 82.16.10.20

3 Задайте параметры удаленного сегмента сети:

- На Кластере HW:
  hostname# iplir set l2overip remote-port 2 82.16.10.20
- На HW-2:
  hostname# iplir set l2overip remote-port 1 82.16.10.10



НАСТРОЙКА ТЕХНОЛОГИИ L2OVERIP

4 Добавьте сетевые фильтры защищенной сети, разрешающие любые соединения по протоколу 97:

hostname# firewall vpn add src @local dst @any proto 97 pass

hostname# firewall vpn add src @any dst @local proto 97 pass

5 Включите функцию L2OverIP:

hostname# iplir set l2overip mode switch

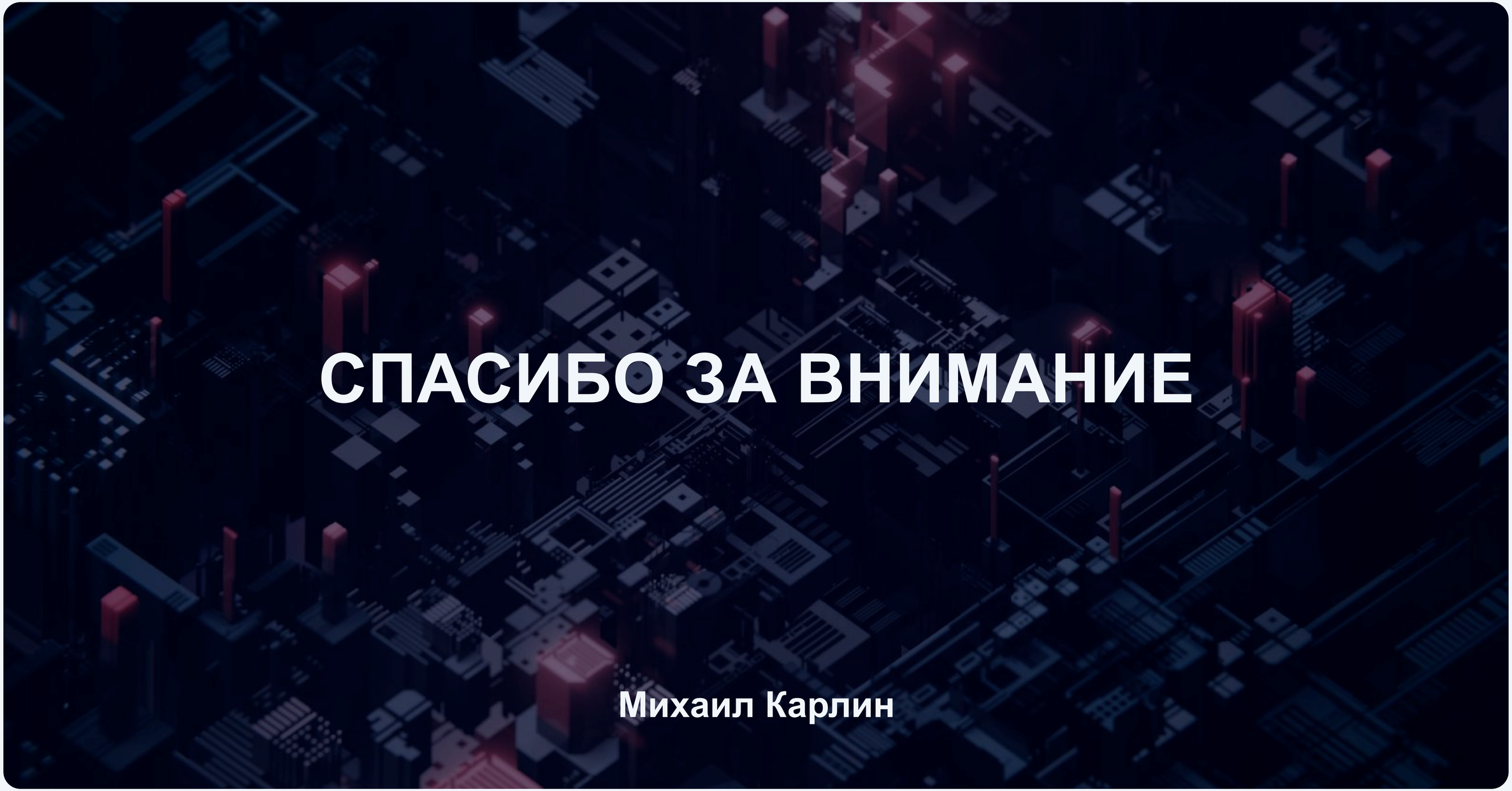
6 Убедитесь в корректности выполненных настроек функции L2OverIP:

hostname# iplir show l2overipconfig

7 После корректной настройки проверьте получение MAC-адресов от удаленного ViPNet Coordinator HW

После настройки и включения функции L2OverIP на всех ViPNet Coordinator HW взаимодействие между узлами удаленных сегментов сети будет защищено на канальном уровне модели OSI.

```
HW5000-Q2-192804bd-N1# iplir show l2overip mac-address-table
Mac address          VLAN  Port     Idle     Flags
-----------------    ----  -----    -----    -----
00:E0:2B:00:00:01     303      1        2
00:E0:2B:00:00:01     300      1        2
5C:F9:DD:E2:00:10       6      1       50
00:A0:98:7C:00:76      64      3      180
1C:1B:0D:CC:00:AC              1        2
1C:1B:0D:CC:00:BE              1        0
1C:1B:0D:CC:00:D5      69      2        4
5C:F9:DD:E2:00:E9       6      1       39
5C:F9:DD:E2:00:ED       6      1        0
5C:F9:DD:E2:00:F9       6      1        4
5C:F9:DD:E2:01:48       6      1        9
78:8C:77:8A:01:60      69      2        2
9C:93:4E:F2:01:64      69      2        6
00:25:AB:6B:01:91     303      1        0
1C:1D:86:94:01:99     303      1        1
1C:1D:86:94:01:99      72      1        0
1C:1D:86:94:01:99     106      1        3
1C:1D:86:94:01:99      64      1        0
1C:1D:86:94:01:99              1       42
1C:1B:0D:CC:01:AB      69      2        0
00:2B:67:74:01:C0      69      2        0
78:8C:77:8A:01:C0      69      2        2
C4:65:16:36:02:11      69      2        0
40:01:C6:B6:02:56      73      2        1
38:22:E2:31:03:04              1        0
```


СПАСИБО ЗА ВНИМАНИЕ
Михаил Карлин