Kapitel 19

Virtual Router Redundancy Protocol

Router fallen manchmal aus. Und dann erfüllen sie ihre fundamentalste Aufgabe nicht mehr, die darin besteht, Netzwerke zu verbinden.
Und Router fallen genauso gerne aus wie andere elektronische Geräte. Das ist eine akzeptierte Tatsache und aus diesem Grund haben High-End–Router zusätzliche Netzteile, Lüfter, CPUs oder Uplinks. In den unteren Preissegmenten hilft man sich meist damit, dass mehrere Router als Gruppe (engl. Cluster) zum Einsatz kommen. Dann entsteht ein Cluster für Hochverfügbarkeit und Ausfallschutz.
Innerhalb der Router-Gruppe einigen sich die Geräte darauf, dass *ein* Router die Arbeit verrichtet und der andere zuschaut und beobachtet. Die Beobachtungen des passiven Routers sind wichtig, denn dieser übernimmt die Geschäfte, sobald er bemerkt, dass sein Partner hinüber ist.

Grundlagen

Technisch läuft das in geordneten Bahnen ab, denn alle Router der *Redundanz-Gruppe* müssen sich an das gemeinsame Protokoll halten. VyOS und EdgeOS unterstützen das *Virtual Router Redundancy Protocol* (VRRP) nach RFC 3768.
Sobald VRRP auf einem Router eingerichtet ist, horcht dieser an seinen Netzwerkinterfaces auf Lebenszeichen anderer VRRP-Router. Der erste Rou-

ter der Gruppe macht sich selber zum Master und sendet Lebenszeichen im Sekundentakt ins Netz. Der zweite Router derselben Gruppe empfängt diese Keepalives und bleibt im Backup-Modus: nichts tun und warten.
Sobald der Backup-Router drei Herzschläge lang nichts von seinem Meister hört, muss er von einer Havarie ausgehen und macht sich selber zum Master. Dann beginnt die Arbeit, denn er muss alle Aufgaben vom ehemaligen Chef übernehmen. Und das so schnell wie möglich, damit das Tagesgeschäft normal weitergehen kann.

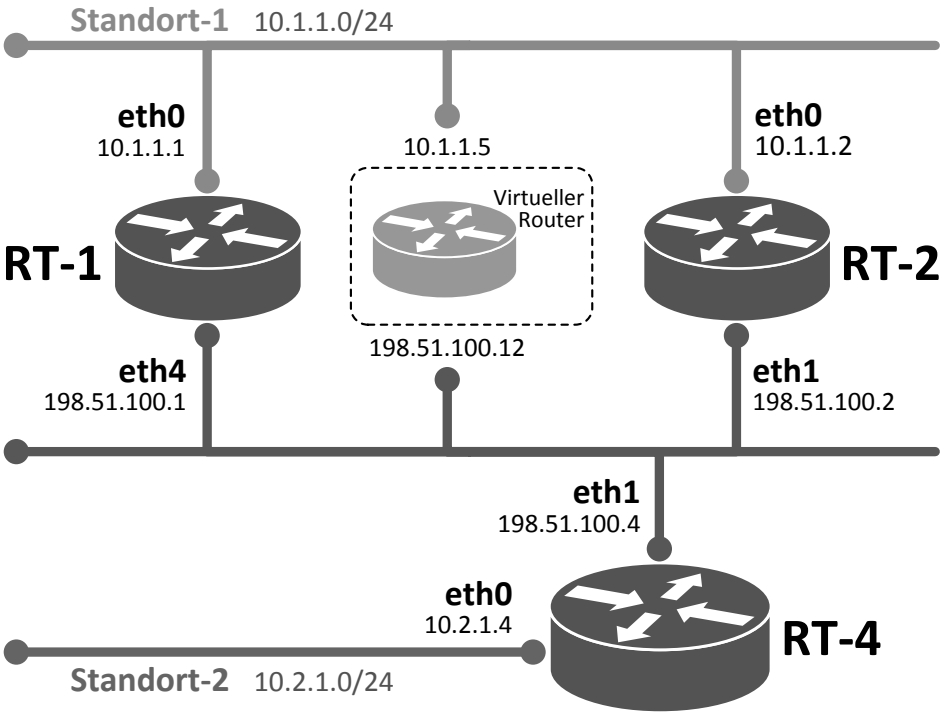

Abbildung 19.1: Laboraufbau für VRRP

Wer erzählt jetzt den anderen Geräten im Netz, dass ein neuer Router am Start ist? Niemand, denn dieser neue Router übernimmt auch die IPv4- und MAC-Adresse der Redundanzgruppe. Für die anderen Teilnehmer im Netz hat sich (außer einer kurzen Unterbrechung) nichts verändert.
Die Lebenszeichen, Heartbeats oder Keepalives, sind IPv4-Pakete an die

Multicast-Adresse 224.0.0.18. In diesen Paketen steht die virtuelle IPv4-Adresse, die sich alle VRRP-Router teilen. Außerdem hat jede Redundanzgruppe eine eigene Nummer, damit mehrere VRRP-Gruppen im selben Netzsegment aktiv sein können.

Labor

Das Demo-Lab stellt drei Router, von denen zwei (RT-1 und RT-2) zusammen ein VRRP-Cluster bilden. Abbildung 19.1 zeigt den Aufbau als Netzdiagramm.
Alle Teilnehmer von Standort-1 nutzen als Standardgateway weder die IPv4-Adresse von RT-1, noch die von RT-2, sondern die *zusätzliche* Adresse 10.1.1.5, die der VRRP-Gruppe gehört. Das ist die LAN-Seite der Geräte – auf der WAN-Seite bilden die Router neben ihren bekannten IP-Adressen ebenfalls eine zusätzliche VRRP-Adresse. Damit der Ausfallschutz funktioniert, muss das VRRP-Cluster aus beiden Richtungen über die virtuellen Adressen angesprochen werden.
Auf der WAN-Seite verbindet Router RT-4 das VRRP-Pärchen mit seinem Standort-2, welcher Ziel des Netzverkehrs von Standort-1 wird.

VRRP-Gruppe

VyOS wird mit einer kurzen Anweisung zum VRRP-Router. In diesem Befehl stecken das eigene Interface, eine beliebige Gruppennummer und die virtuelle Adresse. Mit den Kommandos

```
edit interfaces ethernet
set eth0 vrrp vrrp-group 1 virtual-address 10.1.1.5
set eth4 vrrp vrrp-group 7 virtual-address 198.51.100.12
exit
```

und einem anschließenden `commit` beginnt RT-1 mit dem Aussenden von Heartbeats auf seinen LAN- und WAN-Schnittstellen. Für RT-2 sind die Befehle identisch, bis auf den Namen des WAN-Adapters.
Wenige Sekunden danach haben sich die beiden VRRP-Kandidaten darauf geeinigt, wer der Chef ist und wer der Assistent. In diesem Beispiel hat RT-2 gewonnen und fühlt sich in der Masterrolle:

```
vyos@RT-2:~$ show vrrp
                              RFC         Addr   Last         Sync
Interface    Group  State     Compliant   Owner  Transition   Group
---------    -----  -----     ---------   -----  ----------   -----
eth0         1      MASTER    no          no     5m27s        <none>
eth1         7      MASTER    no          no     5m27s        <none>
```

Bei Router RT-1 sieht die Ausgabe ganz ähnlich aus, nur bei *State* sollte BACKUP stehen.

```
vyos@RT-1:~$ show vrrp
                              RFC         Addr   Last         Sync
Interface    Group  State     Compliant   Owner  Transition   Group
---------    -----  -----     ---------   -----  ----------   -----
eth0         1      BACKUP    no          no     5m35s        <none>
eth4         7      BACKUP    no          no     5m35s        <none>
```

Falls dort ebenfalls MASTER angegeben ist, sind beide Router in der Masterposition und streiten sich um die virtuelle IP-Adresse. Dieser Zustand darf im normalen Betrieb nicht vorkommen, da es auf Clientseite meist zu Programmabbrüchen führt.
Beide Router werden zum MASTER, wenn sie die Lebenszeichen des anderen *nicht* hören. Die Fehlersuche beginnt bei der Kommunikation der Router untereinander mithilfe von `ping` auf die physikalische IPv4-Adresse.

Sobald sich MASTER und BACKUP geeinigt haben, kann die Ende-zu-Ende–Verbindung von Client CL-1 durch die Router zu Client CL-2 mit `traceroute` anschaulich geprüft werden. Denn `traceroute` ermittelt, welchen Weg ein Paket durchs Netz nimmt und zeigt in der folgenden Ausgabe, dass RT-1 für die Weiterleitung zuständig ist.

```
root@cl-1 ~> traceroute -I 10.2.1.25
traceroute to 10.2.1.25 (10.2.1.25), 30 hops max, 60 byte packets
 1  rt-2-eth0 (10.1.1.2)  0.434 ms  0.397 ms  0.363 ms
 2  rt-4-eth1 (198.51.100.4)  0.976 ms  0.945 ms  0.925 ms
 3  cl-2 (10.2.1.25)  1.950 ms  1.678 ms  1.677 ms
```

Nachdem dieser Normalzustand herrscht, passiert ein erster simulierter Routerausfall. Der Masterrouter RT-2 erfährt einen plötzlichen Stromausfall oder die virtuelle Maschine wird gestoppt.
Was passiert? RT-1 empfängt keine Lebenszeichen mehr und ernennt sich nach wenigen Sekunden zum Meister. Dasselbe `traceroute`–Kommando auf Client CL-1 zeigt nur den geänderten Pfad durch RT-1 bis zum Ziel.

```
root@cl-1 ~> traceroute -I 10.2.1.25
traceroute to 10.2.1.25 (10.2.1.25), 30 hops max, 60 byte packets
 1  rt-1-eth0 (10.1.1.1)  2.404 ms  2.374 ms  2.348 ms
 2  rt-4-eth1 (198.51.100.4)  2.977 ms  2.958 ms  2.928 ms
 3  cl-2 (10.2.1.25)  3.601 ms  3.679 ms  3.665 ms
```

Zustandslos

Wenn kein Traffic im Netz ist, bemerkt auch kein Client den Ausfall von Router RT-2. Aber was passiert bei einem Dateitransfer?
Wie sich ein unterbrochener Transfer verhält, hängt ganz von der Anwendung und den Timeouts ab. Ein beispielhafter Webdownload von CL-1, der auf CL-2 als http-Server zugreift, kommt während des Ausfalls ins Stocken, läuft aber nach circa fünf Sekunden weiter.

```
root@cl-1 ~> wget http://10.2.1.25/vyos-1.1.7-amd64.iso
```

Im Moment ist die Konfiguration der Laborgeräte noch ziemlich weltfremd, da alle Router jeden Traffic uneingeschränkt weiterreichen und zustandslos arbeiten. In Unternehmensnetzen gibt es jede Menge Hindernisse, wie Adressumsetzung (NAT) oder Firewallregeln, die sich den Zustand jeder Verbindung merken.

Firewall und NAT

Ein Router mit Kontakt zum Internet hat normalerweise einen Paketfilter an Bord. Höchstwahrscheinlich ist auch noch NAT dabei, um von privaten Adressen in öffentliche zu übersetzen.

```
1 set firewall name WAN-in default-action drop
2 set firewall state-policy related action accept
3 set interfaces ethernet eth1 firewall in name WAN-in
4
5 set nat source rule 1 source address 10.1.1.0/24
6 set nat source rule 1 outbound-interface eth1
7 set nat source rule 1 translation address 198.51.100.12
```

Listing 19.1: Firewall-Regelwerk mit NAT im Router RT-2

Um das Labornetz etwas realitätsnaher zu gestalten, erhalten die VRRP-Router ein kleines Firewallregelwerk und eine Adressumsetzung vom internen Netz 10.1.1.0/24 in die passende öffentliche IPv4-Adresse. Beispiel 19.1 zeigt die VyOS-Konfiguration von Router RT-2.

Falls die Kapitel zur Firewall (8) oder NAT (10) zu lange zurückliegen, gibts eine kleine Auffrischung:
Die ersten drei Zeilen bilden eine Firewallpolicy für das WAN-Interface *eth1*, welches jede ausgehende Verbindung erlaubt und jede neue eingehende Verbindung blockiert. Die Adressumsetzung beginnt in Zeile 5 mit der Quelle 10.1.1.0/24, welche einfach in die WAN–IP-Adresse der VRRP-Gruppe (Zeilen 6 und 7) übersetzt wird.
Für RT-1 ist die Konfiguration identisch, bis auf den Namen der WAN-Schnittstelle.

Jetzt müssen die Router genau Buch führen: Welches (Antwort-)Paket muss die Firewall akzeptieren und welche IP mit welchem Port wird wie übersetzt.
Beim Ausfall vom Master-VRRP–Router wird ein Datentransfer von CL-1 nach CL-2 erst stocken und nach dem Schwenk auf den Backup-Router abbrechen. Die Ursache liegt in den Firewall- und NAT-Tabellen vom Backup-Router. Denn diese sind leer.

Zustandstabellen

Eine Zustandstabelle ist grundsätzlich eine feine Sache: Sie listet alle bestehenden Verbindungen, die durch den Router fließen. Paketfilter und Adressumsetzer schauen für jedes Paket in diese Tabelle, um zu erfahren, ob das Paket zu einer bestehenden Verbindung gehört und weiter behandelt werden darf.
Bei *einem* Router ist das eine Verbesserung der Sicherheit. Bei mehreren Routern besteht das Problem, dass jeder Router seine eigene Tabelle pflegt. Bei VRRP hat der Master-Router eine volle Tabelle und die Tabelle des Backup-Routers ist leer, denn er hat noch keine einzige Verbindung gesehen.

Synchronisation der Tabellen

VyOS löst das Problem mit den unterschiedlichen Tabelleninhalten durch eine Synchronisations-Gruppe und dem Connection-Tracking-Sync. Damit teilt der VRRP-Master sein Wissen über die Zustandstabelle mit dem Backuprouter. In kurzen Abständen sendet der Master-Router Änderungen seiner Tabelle an eine frei wählbare Multicast-Adresse, sodass die Backup-Router ihre lokalen Tabellen entsprechend ergänzen können. Das Ziel ist, dass alle Router im VRRP-Cluster denselben Inhalt in ihren Firewall- und NAT-Tabellen haben.
Falls für die Synchronisation ein eigenes Netzsegment zur Verfügung steht, umso besser. Denn der Abgleich zwischen den Routern muss in Echtzeit passieren. Eine zehn Sekunden alte Firewalltabelle hilft nicht viel bei Verbindungen, die innerhalb der letzten neun Sekunden abgebaut wurden.
Am Beispiel von Router RT-2 spendieren wir dem VRRP-Setup eine Sync-Gruppe mit dem unscheinbaren Namen *CG-1*:

```
set interfaces ethernet eth0 vrrp vrrp-group 1 sync-group CG-1
set interfaces ethernet eth1 vrrp vrrp-group 7 sync-group CG-1
set service conntrack-sync failover-mechanism vrrp sync-group CG-1
set service conntrack-sync interface eth2
set service conntrack-sync mcast-group 239.22.6.1
```

Der Austausch von Tabelleninhalten passiert über das Interface *eth2*, welches eine direkte, aber unabhängige Verbindung zwischen RT-1 und RT-2 darstellt. Die Multicast-Adresse ist beliebig. Der Bereich für administrative Zwecke ohne vorherige Registrierung ist 239.0.0.0/8 und daraus stammt die willkürlich gewählte 239.22.6.1.

Zur Kontrolle: Mit `show vrrp` ist die Spalte *Sync Group* nun mit der eben konfigurierten Gruppe belegt.

```
vyos@RT-2:~$ show vrrp
                                RFC         Addr   Last         Sync
Interface    Group  State       Compliant   Owner  Transition   Group
---------    -----  -----       ---------   -----  ----------   -----
eth0         1      MASTER      no          no     5m4s         CG-1
eth1         7      MASTER      no          no     5m4s         CG-1
```

Jetzt lernen die VRRP-Router gegenseitig ihre Tabelleninhalte. Für VRRP würde es ausreichen, wenn nur der Backup-Router vom Master lernt, aber

Sync-Gruppen sind universell einsetzbar, sodass eine Limitierung der Richtung nicht vorgesehen ist.
VyOS unterscheidet zwischen eigenen Verbindungen und fremden Verbindungen. Fremde Verbindungen stehen im externen Cache und wurden anhand der Sync-Gruppe erlernt. Die eigenen Verbindungen stehen im internen Cache.
Folglich wandert der Inhalt vom internen Cache von RT-1 in den externen Cache von RT-2 und umgekehrt. Der Datentransfer aus dem Beispiel von CL-1 (10.1.1.25) zu CL-2 (10.2.1.25) läuft im Normalfall durch RT-2 und steht dort im internen Cache:

```
vyos@RT-2:~$ show conntrack-sync internal-cache|match 10.1.1.25
|10.1.1.25|:40455            |10.2.1.25|:80               tcp [6]
```

Kurz nach Verbindungsaufbau lernt RT-1 diese Information und listet sie in seinem externen Cache:

```
vyos@RT-1:~$ show conntrack-sync external-cache|match 10.1.1.25
|10.1.1.25|:40455            |10.2.1.25|:80               tcp [6]
```

Wenn jetzt wieder ein unerwartetes Ereignis den Master-Router RT-2 zur Strecke bringt, übernimmt RT-1 die VRRP-Rolle und das Routing der Verbindungen. Der Failover-Prozess dauert ein paar Sekunden, aber dann läuft der Datentransfer von CL-1 zur CL-2 weiter und steht im internen Cache von RT-1. Der Wechsel von externem zu internem Cache passiert, weil die Session nach dem Failover zu RT-1 gehört.

```
vyos@RT-1:~$ show conntrack-sync internal-cache|match 10.1.1.25
|10.1.1.25|:40458            |10.2.1.25|:80               tcp [6]
```

Best Practice

Asymmetrisches Routing

Wenn ein Paket auf dem Hinweg zum Server einen anderen Pfad nimmt als auf dem Rückweg, ist das Routing asymmetrisch. Theoretisch ist das kein Problem, aber in der Praxis verhindern zustandsorientierte Firewalls, NAT-Gateways oder IDS-Systeme eine erfolgreiche Verbindung.

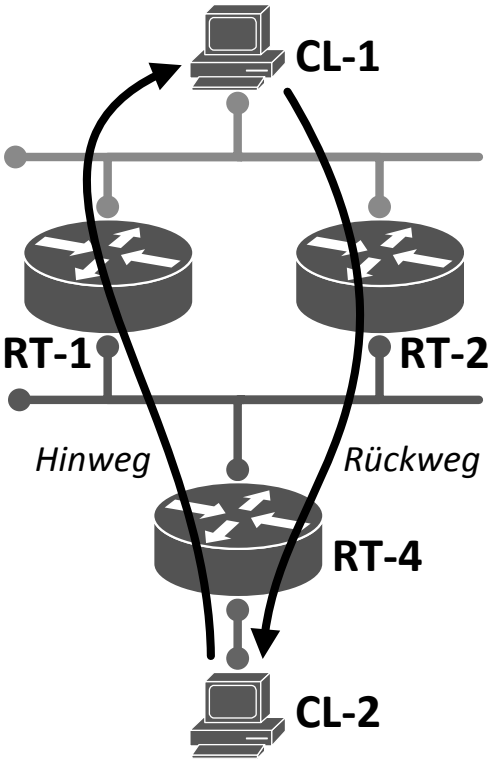

Abbildung 19.2: VRRP kann asymmetrisches Routing hervorrufen

Mit VRRP passiert sehr leicht ein asymmetrisches Routing. Diese Asymmetrie entsteht sogar im Labornetz, wenn RT-1 Master für die LAN-Seite ist und RT-2 Master für die WAN-Seite ist.
In Abbildung 19.2 sendet Client CL-1 Netzpakete an sein Defaultgateway, welches von RT-2 angenommen wird. Über RT-4 gelangt das Paket an sein Ziel CL-2. Der Weg zurück beginnt bei RT-4. Dieser Router sendet weiter an die VRRP-Adresse und wird von RT-1 beantwortet. RT-1 weiß von dieser Verbindung nichts, weil es das erste Paket gar nicht gesehen hat, welches über RT-2 geroutet wurde. Wenn RT-1 als „dummer“ Router agiert, leitet er die Pakete weiter zu CL-1 und alles ist gut. Falls RT-1 aber *stateful* arbeitet, wird er alle unbekannten Pakete verwerfen. Dann verhindert asymmetrisches Routing die erfolgreiche Kommunikation von CL-1 und CL-2.

VyOS kann den VRRP-Routern eine Priorität mitgeben, sodass *ein* Router für alle VRRP-Gruppen Master wird. Damit ist und bleibt das Routing symmetrisch. Die Einrichtung von Prioritäten ist weiter unten beschrieben.

Schnelleres Failover

Andere Redundanzprotokolle für Gateway-Failover erreichen Umschaltzeiten von unter einer Sekunde. Das Intervall für die Keepalives liegt dann im Bereich von wenigen Hundert Millisekunden mit einem Timeout von einer knappen Sekunde.
Dieser Luxus ist bei VRRP nicht möglich. Die vorgegebene Dauer zwischen zwei Herzschlag-Paketen ist gleichzeitig der Minimalwert: eine Sekunde. Höhere Werte lassen sich konfigurieren, aber der Timeout ist stets die dreifache Dauer. Per Voreinstellung sind das etwa 3–4 Sekunden.
Ein flotteres Umschalten ist mit VRRP nicht machbar. Failover im Millisekundenbereich erreicht VyOS mit dem *cluster*–Kommando, das in Kapitel 20 untersucht wird.

Besondere Protokolle

Protokolle mit separater Datenverbindung brechen selbst bei Verwendung der Sync-Gruppe ab. Denn Router können die zusätzliche Verbindung, wie sie bei FTP, SIP oder NFS Teil des Konzepts ist, nicht als solche erkennen. VyOS bietet selbst dafür Unterstützung und verwaltet diese Verbindungen in der erweiterten Tabelle *expect*. Allerdings müssen die Protokolle erst für den Tabellenabgleich aktiviert werden. Der Befehl

```
set service conntrack-sync expect-sync all
```

nimmt alle verfügbaren Protokolle in die Synchronisation auf. Unterstützt werden FTP, H.323, NFS, SIP und SQLnet.

Wahl zum Master

Grundsätzlich gewinnt der VRRP-Router mit der höchsten Priorität. Wenn beide Kandidaten die voreingestellte Priorität von 100 haben, gewinnt der Router mit der größeren IP-Adresse. Aus diesem Grund wird auch stets RT-2 der Master, weil seine IPv4 10.1.1.2 numerisch größer ist, als die von seinem

Gegenkandidaten RT-1 mit 10.1.1.1. Auf der WAN-Seite ist das genauso. Wenn RT-1 der bevorzugte Router sein soll, weil beispielsweise die Hardware leistungsstärker oder neuer ist, kann in RT-1 mit

```
set interfaces ethernet set eth0 vrrp vrrp-group 1 priority 200
```

die Wahl ganz schnell manipuliert werden. Als Folge schwenkt die Masterrolle von RT-2 zu RT-1.

Lastverteilung

Bei VRRP ist immer nur *ein* Router der aktive Master. Eine Verteilung der Netzlast auf mehrere Geräte ist im Protokoll mit Tricks möglich.

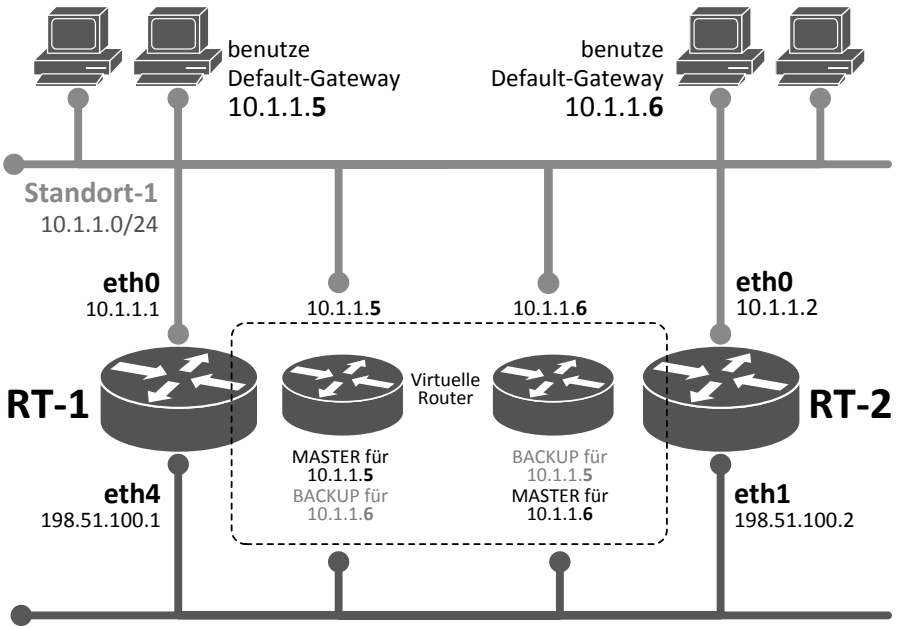

Abbildung 19.3: Lastverteilung mit VRRP

Für eine „Lastverteilung des kleinen Mannes“ (Abbildung 19.3) bekommen die Router eine weitere VRRP-Gruppe pro Interface. In dieser neuen Gruppe ist genau der Router Master, der in der ersten Gruppe Backup ist.

Dem obigen Beispiel folgend ist RT-1 Master und RT-2 Backup der VRRP-Gruppe 1. In der neuen VRRP-Gruppe 2 ist RT-1 Backup und RT-2 der Master. Während Gruppe 1 die IPv4-Adresse 10.1.1.5 bedient, könnte Gruppe zwei zur Adresse 10.1.1.6 gehören. Der Trick besteht darin, dass die Hälfte der Clients in diesem Netzsegment ihr Standardgateway auf 10.1.1.5 stellen und die andere Hälfte 10.1.1.6 als Gateway nutzen.
Ob ein Router Master oder Backup wird, liegt an seiner Priorität, die über Konfigurationsbefehle voreingestellt wird. Der Ausgangswert ist 100. Die folgenden Kommandos auf RT-1 machen ihn zum Master für Gruppe 1 und zum Backup von Gruppe 2:

```
edit interfaces ethernet
set eth0 vrrp vrrp-group 1 priority 120
set eth0 vrrp vrrp-group 1 virtual-address 10.1.1.5
set eth0 vrrp vrrp-group 2 priority 70
set eth0 vrrp vrrp-group 2 virtual-address 10.1.1.6
```

Genau andersherum wird RT-2 der Backup-Router für Gruppe 1 und der Master von Gruppe 2:

```
edit interfaces ethernet
set eth0 vrrp vrrp-group 1 priority 70
set eth0 vrrp vrrp-group 1 virtual-address 10.1.1.5
set eth0 vrrp vrrp-group 2 priority 120
set eth0 vrrp vrrp-group 2 virtual-address 10.1.1.6
```

Die genauen Zahlen für die Priorität sind nicht entscheidend. Hauptsache ein Router hat einen höheren Wert als der andere.
Damit teilen sich beide Router die Netzlast. Der Anteil jedes Routers ist nicht kontrollierbar: Im besten Fall arbeitet jeder Router genau 50% der Pakete ab, im ungünstigsten Fall erhält RT-1 über 99% aller Verbindungen und RT-2 langweilt sich mit dem verbleibenden Prozent.

Eine echte Lastverteilung über mehrere Leitungen benutzt andere VyOS-Features und beginnt in Kapitel 27.

Sicherheit

In einer VRRP-Gruppe ist jeder Router willkommen. Ein unbekannter neuer Router mit höchster Priorität wird also ohne weitere Prüfung der Gruppenmeister. Ein Angreifer mit VRRP im Gepäck erhält folglich ungefragt allen Netzverkehr zur Durchsicht und Weiterleitung.
So einfach darf es ein Angreifer nicht haben. Daher kommt eine effektive Sicherheitsvorkehrung von VRRP ins Spiel: Authentifizierung. Alle vertrauenswürdigen Teilnehmer einer VRRP-Gruppe erhalten ein Kennwort. Mit diesem Kennwort wird das VRRP-Paket um einen *Authentication Header* (AH) ergänzt, der aus der Protokollfamilie IPsec stammt. Alle Teilnehmer müssen jetzt die Vertrauenswürdigkeit der VRRP-Keepalives überprüfen.
VyOS macht die Konfiguration dieses kryptografisch spannenden Vorhabens denkbar einfach. Denn außer einem Passwort und dem Hinweis auf AH wird nichts weiter benötigt.

```
edit interfaces ethernet eth0 vrrp vrrp-group 1
set authentication password YOGHURT
set authentication type ah
```

Das Passwort und der Authentifizierungstyp müssen auf allen Routern einer VRRP-Gruppe identisch sein. Nach dem folgenden `commit` sendet der Router bereits authentifizierte Pakete und erwartet ebenfalls authentifizierte Pakete. Sobald im Authentication Header etwas nicht stimmt, *muss* der Router das fragwürdige Paket verwerfen.

Während der Umstellung auf Authentifizierung bzw. während einer Passwortänderung, kann es zu ungewollten Statusänderungen und zu Unterbrechungen für die Netzteilnehmer kommen. Außer natürlich, die Änderung passiert auf allen Routern einer Gruppe zur selben Zeit, z. B. mithilfe des Task-Schedulers aus Kapitel 33.

Kompatibilität

Die verwendete Version von VRRP basiert auf RFC 3768. Allerdings weicht die Implementierung von VyOS im Detail von diesem RFC ab. Wenn nur VyOS-Router mitspielen, macht das keinen Unterschied, da alle Teilnehmer

dieselbe Implementierung haben. Sobald sich Router anderer Hersteller beimischen, muss auf Kompatibilität geachtet werden. Mit dem Konfigurationsbefehl

```
set interfaces ethernet eth0 vrrp vrrp-group 1 rfc3768-compatibility
```

kann VyOS schnell überzeugt werden, ein akzentfreies VRRP nach RFC 3768 zu sprechen. Ob in der Praxis ein gemischtes VRRP-Cluster mit den Routern von Cisco möglich ist, untersucht Kapitel 22.

IP Version 6

VyOS benutzt die VRRP Version 2, welche ausschließlich für IPv4 konzipiert ist. Die Unterstützung für IPv6 kam sechs Jahre später und hat noch nicht seinen Weg in den Programmcode von VyOS gefunden.
Schlimmer noch: Sobald VyOS VRRP-Pakete der neueren Version 3 empfängt, wird jedes Keepalive mit drei Logzeilen gewürdigt:

```
Jun 21 12:20:01 RT-8 Keepalived_vrrp: invalid version. 3 and expect 2
Jun 21 12:20:01 RT-8 Keepalived_vrrp: bogus VRRP packet received on eth0
Jun 21 12:20:01 RT-8 Keepalived_vrrp: VRRP_Instance(vyatta-eth0) Dropping
```

EdgeOS

Im Umfeld von VRRP ist EdgeOS deutlich weiter, denn die IPv6-kompatible Version 3 ist bereits mit von der Partie.
Zurück bei VRRPv2 und IPv4 ist das Zusammenspiel von VyOS und EdgeOS kein Problem, da beide auf derselben Software *Keepalived* basieren. Auch mit der Authentifizierung über IPsec einigen sich beide Router auf ihre Rolle als Master oder Backup.

Leider fehlt bei den EdgeMAX-Routern die Synchronisation der Sessiontabelle. Ein transparentes Failover ist damit nicht möglich. EdgeOS bietet zwar die lokale Sync-Gruppe, aber nicht die Synchronisation der Verbindungsdaten.
Zum besseren Verständnis ist die Abgrenzung dieser Techniken hilfreich: Die Sync-Gruppe sorgt nur dafür, dass sich alle lokalen Interfaces mit VRRP-Fähigkeit gleich verhalten. Fällt *ein* Interface dieses Routers aus, stellt sich

VRRP tot um ein Failover zum Backup-Router zu beginnen. Damit sind alle Interfaces synchron.
Der Zusatz *conntrack-sync* für eine Sync-Gruppe erweitert die Funktionalität um den Abgleich der Sessiontabellen *zwischen* mehreren Routern. Und genau dieses Zusatzpaket zur Tabellensynchronisation fehlt im EdgeOS.

Technischer Hintergrund

VyOS setzt auf die Linuxsoftware *Keepalived* [19] um VRRP anzubieten. Die Entwickler von Keepalived beschäftigen sich seit dem Jahr 2000 mit der Implementierung von VRRP. VyOS nutzt die Keepalived-Version 1.2.2 die sich auf VRRP Version 2 (RFC 3768) beschränkt und damit nur IPv4 beherrscht.
EdgeOS bedient sich ebenfalls bei Keepalived, aber hier ist schon Version 1.2.19 im Einsatz, die VRRP Version 3 (RFC 5798) bietet. Diese Version beschäftigt sich mit IPv6 und damit ist EdgeOS im Bereich VRRP bereits „IPv6-ready“.
Um die Synchronisation der Verbindungsdaten kümmert sich der Linuxdienst *conntrackd*, der aus der *netfilter*-Welt stammt. *conntrackd* beobachtet den lokalen Cache auf Sessioninformationen und informiert seine Partner bei Änderungen. Die Unterscheidung nach internem und externem Cache kommt übrigens von conntrackd.