

First Hop Redundancy

Die Verfügbarkeit eines Default-Gateway ist ein MUSS für Hosts innerhalb eines Netzwerkes.

Ohne Kenntnis eines Default GW kann der Host nicht mit Zielen ausserhalb seines logischen Segments kommunizieren.

Die Konfiguration eines Default-Gateway auf einem (LAN)-Host, d.h. die Festlegung des Next-Hop für Datenverkehr in entfernte Netzwerke erfolgt i.d.R. durch

- statische Konfiguration oder
- über DHCP.

Problematik:

Da auf einem Host nur ein Default-GW angegeben werden kann, ist das Default-GW – ohne adäquate Gegenmaßnahmen – ein single-point-of-failure für alle Hosts innerhalb des LAN Segments. Fällt das Default-GW aus, können die Hosts entfernte Ziele nicht mehr erreichen.

Daher ist es sinnvoll, Maßnahmen zu ergreifen, um diesen single-point-of-failure zu beseitigen.

Generell existieren dazu 2 unterschiedliche Methoden:

- **Dynamic Router Discovery**
Funktionalitäten auf Hosts, die es diesen ermöglichen das Default-GW aktiv zu ermitteln.

Die unterschiedlichen Möglichkeiten für eine Dynamic Router Discovery haben jedoch alle ihre eigenen Nachteile und sind nicht empfehlenswert.

Überblick: Methoden für die Dynamic Router Discovery

- **Proxy ARP**
- **Routing Protocol**
- **IRDP** – ICMP Router Discovery Protocol (RFC 1256)
- **FHRPs – First Hop Redundancy Protocols**
Funktionalitäten auf Router bzw. Multilayer Switches, die – transparent – für Hosts eine sofortige, verlustfreie Kommunikation über ein redundantes "standby" Default-GW ermöglichen, wenn das eigentliche Default-GW ausfällt.

Grundsätzlich empfehlenswert zur Vermeidung der single-point-of-failure Default-GW Problematik.

Überblick: Default Gateway Redundancy Features

- **HSRP** – Hot Standby Routing Protocol
→ Cisco proprietär .. aber beschrieben in RFC 2281
 - optimiert für 2 Router, keine Lastverteilung
- **VRRP** – Virtual Router Redundancy Protocol
→ offener Standard - RFC 2338
 - optimiert für 2 Router, keine Lastverteilung
- **GLBP** – Gateway Load Balancing Protocol
→ Cisco proprietär
 - für multiple Router, default Lastverteilung zwischen den Routern

Dynamic Router Discovery – Methoden für Hosts

Es gibt unterschiedliche Möglichkeiten, wie ein Host das Default-GW selbst ermitteln kann, die allerdings verschiedene Nachteile (administrativen Aufwand, Overhead im Netzwerk) haben:

- **Proxy ARP** (RFC 1027)

Host stellen eine ARP Anfrage zu einem entfernten Ziel, eine entsprechend konfigurierter Router antwortet stellvertretend (proxy) für den entfernten Host mit seiner eigenen MAC Adresse, wenn er einen Pfad zum Zielhost in seiner Routing Tabelle hat.

Der Host hat also mehrere Einträge in seiner ARP Tabelle, die zu unterschiedlichen remote IP Adressen führen aber auf die gleiche Dst-MAC Adresse (die des Routers) gemappt sind.

Fällt nun der entsprechende Router aus, wird Datenverkehr zu den bekannten Zielen selbst dann gedroppt, wenn es einen zweiten, redundanten Router gibt, da nur für unbekannte Ziele "neue" ARP Anfragen gestellt werden (die der redundante Router dann beantworten würde).

Proxy ARP hat eine Reihe weiterer Nachteile: schwieriges Troubleshooting, unsichere Funktionalität. Proxy ARP ist eigentlich eine Funktion aus "grauer" Ethernet Vorzeit, wo VLANs noch keine Bedeutung hatten, da Proxy ARP eine physikalische Ethernet-Verbindung von Geräten unterschiedlicher logischer Netzwerke (z.B. an einen Hub oder Switch) ermöglichte.
Nicht empfehlenswert.

- **Routing Protocol**

Durch Aktivierung eines Routing Protocols auf dem Host, erhält der Host alle notwendigen Routing Informationen und erzeugt seine eigene Routing Tabelle aus diesen Informationen.

Diese Methode benötigt und verwendet – vermeidbar – Ressourcen im Netzwerk und auf den Hosts.
Nicht empfehlenswert.

- **IRDP** – ICMP Router Discovery Protocol (RFC 1256)

Auf dem Host läuft ein IRDP Client und auf den Routern ist IRDP ebenfalls aktiviert. IRDP ist eine Erweiterung von ICMP, die einen Mechanismus zur Ermittlung eines Default-GWs für Hosts zur Verfügung stellt.

IRDP Router senden in bestimmten Intervallen IRDP Multicast Nachrichten an IRDP Clients und teilen so ihre Verfügbarkeit für eine bestimmte lifetime mit. Nach Ablauf der lifetime erwarten die Host eine neue IRDP Nachricht von einem Router.

Die Verwendung von IRDP ist wenig gebräuchlich und erschwert das Troubleshooting.
Nicht empfehlenswert.

HSRP – Hot Standby Routing Protocol

HSRP ist eine Cisco proprietäres Protokoll, das in Cisco Netzwerken weit verbreitet ist. Mittlerweile ist HSRP von der IETF jedoch auch als Standard übernommen: RFC 2281.

Mit HSRP verwalten mehrere (i.d.R. zwei), redundante Router innerhalb eines gleichen logischen IP Netzwerks eine einzelne virtuelle IP Adresse (und eine passende virtuelle MAC Adresse), die das Default-GW für die Hosts innerhalb des Netzwerks repräsentiert.

HSRP groups und Router roles

Alle HSRP Router gehören zu einer, mittels ID gekennzeichneten, **HSRP standby group** mit folgenden Einheiten (**roles**):

- es existiert genau ein **active** Router
leitet Datenverkehr, die an die virtuelle IP Adresse gerichtet ist weiter

- Die **HSRP priority** (0-255, default: 100) eines Routers legt die role des Routers fest
 - **höchste HSRP priority** (IP Adresse) → **active** Router
.. wenn gleich
 - **höchste IP Adresse** auf dem Routed Interface

- es existiert genau ein **standby** Router
ist der Backup-Router, der im Falle eines Ausfalls des active Routers die Rolle des active Router übernimmt, d.h. die Weiterleitung des Datenverkehrs übernimmt.

- Optional: zusätzliche HSRP **member** Router
Router, die zur entsprechenden HSRP Gruppe gehören, aber weder active noch standby sind – sondern im **listen** state - aber in diese HSRP states wechseln können, falls das entsprechende Gerät ausgefallen ist.

Active und Standby Router bilden einen **virtual** Router.

Der virtual Router ist kein real existierender Router, sondern wird durch die virtual IP address und der virtual MAC address repräsentiert, und stellt so das einzige, "virtuelle" Default-GW für die Hosts dar.

Der active Router leitet Datenverkehr, der an den virtual Router (an die virtuelle MAC Adresse) adresse) gesendet wird, weiter.

- Die **virtual IP adress** wird administrativ festgelegt.
- Die **virtual MAC address** wird wie folgt gebildet:
Beispiel: bei Verwendung der HSRP group ID von (dezimal) 42
Virtual MAC Address: → 0000.0c**07.ac**2a

24 Bit OUI	→ 0000.0c
16 Bit HSRP Well-Known Tag	→ 07.ac
8 Bit HSRP group ID (42)	→ 2a

HSRP Kommunikation und Stati

Die Kommunikation zwischen den unterschiedlichen HSRP Routern innerhalb einer standby group erfolgt durch **HSRP hello** Nachrichten (**UDP** Port **1985**, Multicast **224.0.0.2**):

- active und standby Router
→ senden in regelmäßigen Abständen, geregelt durch die verwendete **hello interval time** (default: **3 Sek.**), HSRP Nachrichten, um andere Router innerhalb der standby group über ihren Rolle und ihren Status zu unterrichten
- member (listen) Router
→ senden nicht, sondern empfangen HSRP hellos nur (monitoring)

Wenn HSRP hellos für die Dauer der **dead interval time** (default: 10 Sek.) vom active Router ausbleiben, übernimmt der standby Router die Rolle des active Router und somit die Funktion des virtual Router.

Deshalb ist die Ausfallzeit des Default-GW abhängig von der dead interval time.

HSRP definiert 6 unterschiedliche **HSRP states** für HSRP Router.

- **Disabled**: HSRP nicht funktional
- **Initial** (transitory): HSRP ist nicht funktional.
Nach Konfigurationsänderungen oder IF down/up.
→ Senden von Hellos
- **Learn** (transitory): Warten auf HSRP hello Nachrichten
→ (noch) kein Empfang von HSRP hellos
- **Listen**: Status von HSRP member Routern
→ Empfangen von hellos
- **Speak** (transitory): Status jedes HSRP group Router während der (Neu)-Festlegung der HSRP roles (election of active and/or standby). Bidirektionale Kommunikation
→ Senden/Empfangen von HSRP hellos
- **Standby**: Status des HSRP standby Router
→ Senden/Empfangen von HSRP hellos
- **Active**: Status des HSRP active Router
→ Senden/Empfangen von HSRP hellos

Konfiguration HSRP

Aktivierung von HSRP

Angabe der group ID (1-255) und der virtual IP address im SubConfiguration Mode des IF.

Die HSRP Group ID ist nur lokal auf einem Interface gültig, d.h. auf unterschiedlichen Schnittstellen können identische Group-IDs verwendet werden. Es ist jedoch empfehlenswert, die Group ID an die entsprechende VLAN ID anzupassen.

```
(config-if)# standby group-id ip virtual-ip-address
```

Optional, aber empfehlenswert: Festlegung der HSRP Priorität (**default: 100**) zur Manipulation der Router roles (active, standby, member) → höchste gewinnt.

```
(config-if)# standby group-id priority priority
```

Optional, aber empfehlenswert: **HSRP Preempt**

Sollte ein ausgefallener, ehemalige active Router im Netzwerk wieder verfügbar werden, übernimmt er nicht automatisch wieder die Rolle des active Router (trotz höherer Priorität). Dieses Verhalten kann jedoch mit der Konfiguration von HSRP preempt geändert werden, d.h. es wird in jedem Fall der Router mit der höchsten Priorität zum active Router.

Die Konfiguration einer Verzögerung (z.B. nach Reboot) ist sinnvoll, um anderen Protokollen z.B. Routing Protokollen Konvergenzzeit einzuräumen ..

```
(config-if)# standby [ group-id ] preempt [ delay [ minimum sec ] [ reload sec ]]
```

Optional: Veränderung der HSRP Timer Werte

Innerhalb von HSRP hellos werden die, lokal veränderten, Timer Werte an andere Router übertragen.

ACHTUNG: die Reduzierung der Timer bewirkt zwar ein schnelleres Bermerken eines Ausfalls, bewirkt jedoch auch eine häufigeres Senden von Hellos.

```
(config-if)# standby group-id timers [ msec ] hello-time [ msec ] hold-time
```

Optional aber empfehlenswert: **Authentication**

Die HSRP Kommunikation kann authentifiziert erfolgen, mittels:

- Clear-text authentication (max. 8 Zeichen)
- MD5 authentication (max. 64 Zeichen.. ähnlich einer HMAC Funktion)

Dabei wird eine identisch konfiguriertes Passwort in HSRP Nachrichten mitgesendet.

- Das Passwort kann direkt im standby Kommando konfiguriert werden.
- Es kann jedoch auch ein vorher konfiguriertes Key-Chain verwendet werden.

```
(config-if)# standby group-id authentication password
```

.. oder

```
(config-if)# standby group-id authentication md5 key-string password
```

.. oder

```
(config)# key chain chain-name
```

```
(config-keychain)# key key-number
```

```
(config-keychain-key)# key-string password
```

```
(config-if)# standby group-id authentication md5 key-chain chain-name
```

HSRP Interface Tracking

Es kann u.U. nützlich sein, dass eine active Router seine active role verliert, wenn eine bestimmte Verbindung auf dem Router ausgefallen ist.

Wenn z.B. die Verbindung des active Routers zum "Rest des Netzwerks" ausfällt, der standby Router aber noch über Konnektivität verfügt, sollte dieser Router von den Hosts im LAN nicht mehr als Default-GW verwendet werden.

Bei HSRP Tracking wird der Status eines IF überprüft.

Das Tracking kann

- direkt im standby Kommando konfiguriert werden: Wenn das IF in den Status "down" wechselt, wird die Priorität um den angegebenen Wert (oder **default: 10**) vermindert und die Sendung von HSRP hellos (für einen Zeitraum) eingestellt, oder
- Alternativ kann jedoch auch ein vorher konfiguierter track verwendet werden,
 - der Schnittellen überwacht
 - ip routing: überprüft OSI 3 Funktionalität der Schnittstelle
 - line-protocol: überprüft OSI 2 Funktionalität der Schnittstelle
 - oder das Vorhandensein von Routen innerhalb der Routing Tabelle
 - oder IP SLA Tracking, wie z.B. ein ping an eine "wichtige" IP Adresse

Einfaches Tracking

```
(config-if)# standby group-id track if-id [ decrement-value ]
```

Interface Tracking mit Track Object

- L3 Funktionalität (ip routing)
- L2 Funktionalität (line-protocol)

```
(config)# track track-id interface if-id { ip routing | line-protocol }
```

IP Route Tracking mit Track Object

```
(config)# track track-id ip route Net-ID/Length reachability
```

IP SLA Tracking

```
(config)# ip sla sla-nr
(config-ip-sla)# icmp-echo dst-IP
(config-ip-sla-echo)# frequency sekunden
```

```
(config)# track track-id ip sla sla-nr reachability
```

Referenzierung des Track Objects für HSRP

```
(config-if)# standby group-id track track-id [ decrement value ]
```

Troubleshooting

```
# show standby
# show standby brief
# show standby if-type if-number
# show standby delay
# show track
# debug standby terse
```

Load Balancing mit HSRP

Die Default GW Adresse der Hosts eines einzelnen LAN oder VLAN zeigt auf die HSRP virtual IP address.

Da immer nur der active HSRP Router die virtuelle IP Adresse verwaltet, kann auch immer nur ein Pfad (über den active router) aus dem Netzwerk führen – obwohl eigentlich 2 Pfade bereitstehen.

Um beide Pfade zu verwenden, wenn Host aus dem LAN in remote Netzwerke kommunizieren kann **Load Balancing** zwischen den zwei HSRP Routern verwendet werden.

- Es werden **zwei Gruppen** mit jeweils einer eigenen virtuellen IP für ein LAN konfiguriert – es existieren also 2 virtuelle Gateways für ein LAN.
 - Ein HSRP Router wird active router für die erste Gruppe und standby router für die zweite Gruppe.
 - der andere HSRP Router wird (entgegengesetzt) standby router für die erste Gruppe und active router für die zweite Gruppe.
- Dann wird eine Hälfte der Hosts innerhalb des LANs mit der virtuellen IP der ersten HSRP Gruppe konfiguriert und die zweite Hälfte der Hosts mit der virtuelle IP der zweiten HSRP Gruppe konfiguriert.
- Wenn ein HSRP Router ausfällt übernimmt der andere den Datenverkehr für beide virtuellen IP Adressen.

Nachteil: Unterschiedliche – nicht dynamische – Gateway Konfiguration notwendig auf den Hosts im LAN.

Dsw1	Dsw2
<pre>! interface Vlan1 ip address 192.168.1.250 255.255.255.0 standby 1 ip 192.168.1.1 standby 1 priority 110 standby 1 preempt standby 1 track FastEthernet1/0 20 ! standby 2 ip 192.168.1.2 standby 2 preempt standby 2 track FastEthernet1/0 !</pre>	<pre>! interface Vlan1 ip address 192.168.1.251 255.255.255.0 standby 1 ip 192.168.1.1 standby 1 preempt standby 1 track FastEthernet1/0 ! standby 2 ip 192.168.1.2 standby 2 priority 110 standby 2 preempt standby 2 track FastEthernet1/0 20 !</pre>

Wenn **mehrere VLANs** verwendet werden, ist es empfehlenswert folgende Einstellungen für redundante Gateways (Multilayer Switch) durchzuführen

- Layer 2: für eine Hälfte der VLANs ist ein Multilayer Switch die Root Bridge, für die zweite Hälfte der andere
- Layer 3: für eine Hälfte der VLANs ist ein Multilayer Switch der active router, für die zweite Hälfte der andere.

TIPPs:

- Pakete, die aus remote Netzwerken zurückkommen, können mgl. beide Pfade nehmen, d.h. die Pakete müssen nicht über den active Router zurück ins LAN kommen.
- Es können bis zu 255 HSRP Gruppen konfiguriert werden.

HSRP Version 2

HSRP Version 2 ist für IPv6 und IPv4 konzipiert.

Die virtuelle MAC von HSRPv2 hat sich geändert: **0000.0c9f.f<group-ID>**

Die standby group ID kann im Bereich von **0 bis 4095** angegeben werden, da nun 12 Bit für die Group ID reserviert sind

Wichtigste Unterschiede zw. HSRPv1 und HSRPv2

	HSRPv1	HSRPv2
virtual MAC	0000.0c07.ac<group-ID>	0000.0c9f.f<group-ID>
group ID	0-255	0-4095
Multicast	224.0.0.2	224.0.0.102 ff02::66

Konfiguration

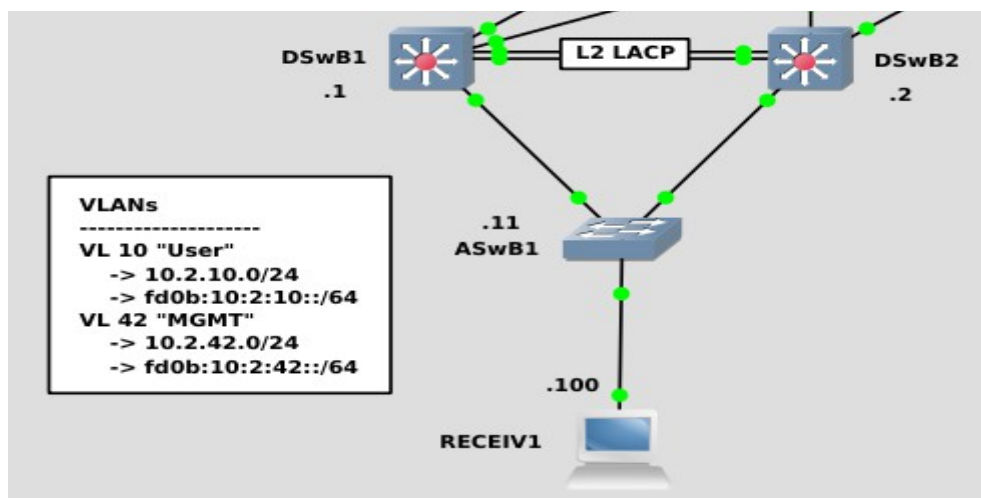
Auf Version 2 einstellen - falls möglich immer empfohlen

```
(config)# interface IF-ID
(config-if)# standby version 2
```

Weitere Einstellungen - mit Ausnahme der virtual IP - entsprechen den Einstellung von HSRPv1 für IPv4. Die virtual IP kann via „autoconfig“ (empfohlen) oder manuell zugewiesen werden

```
(config-if)# standby group-ID ipv6 autoconfig
(config-if)# standby group-ID priority wert
(config-if)# standby group-ID preempt
(config-if)# standby group-ID authentication md5 key-chain key-chain-name
(config-if)# standby group-ID track track-ID decrement wert
```


HSRPv2 Konfigurationsbeispiel



DSwB1	DSwB2
→ VLAN 10: active, → VLAN 42: standby → MD5 Authentication mit Key Chain → IP SLA Trackauf remote IP 10.10.10.10 inkl. preemption	→ VLAN 10: standby, → VLAN 42: active → MD5 Authentication mit Key Chain → IP SLA Trackauf remote IP 10.10.10.10 inkl. preemption
<pre> ! ip sla 10 icmp-echo 10.10.10.10 frequency 5 ip sla schedule 10 start now life forever ! track 10 ip sla 10 reachability ! key chain SBK key 7 key-string geheim ! int vlan 10 ip address 10.2.10.1 255.255.255.0 ipv6 address fe80::db1 link-local ipv6 address fd0b:10:2:10::1/64 standby version 2 standby 410 ip 10.2.10.254 standby 410 priority 110 standby 410 preempt standby 410 authentication md5 key-chain SBK standby 410 track 10 decrement 20 standby 610 ipv6 autoconfig standby 610 priority 110 standby 610 preempt standby 610 authentication md5 key-chain SBK standby 610 track 10 decrement 20 ! int vlan 42 ip address 10.2.42.1 255.255.255.0 ipv6 address fe80::db2 link-local ipv6 address fd0b:10:2:42::2/64 standby version 2 standby 442 ip 10.2.42.254 standby 442 priority 110 standby 442 preempt standby 442 authentication md5 key-chain SBK standby 442 track 10 decrement 20 standby 642 ipv6 autoconfig standby 642 priority 110 standby 642 preempt standby 642 authentication md5 key-chain SBK standby 642 track 10 decrement 20 ! </pre>	<pre> ! ip sla 10 icmp-echo 10.10.10.10 frequency 5 ip sla schedule 10 start now life forever ! track 10 ip sla 10 reachability ! key chain SBK key 7 key-string geheim ! int vlan 10 ip address 10.2.10.1 255.255.255.0 ipv6 address fe80::db1 link-local ipv6 address fd0b:10:2:10::1/64 standby version 2 standby 410 ip 10.2.10.254 standby 410 preempt standby 410 authentication md5 key-chain SBK standby 610 ipv6 autoconfig standby 610 preempt standby 610 authentication md5 key-chain SBK ! int vlan 42 ip address 10.2.42.1 255.255.255.0 ipv6 address fe80::db2 link-local ipv6 address fd0b:10:2:42::2/64 standby version 2 standby 442 ip 10.2.42.254 standby 442 priority 110 standby 442 preempt standby 442 authentication md5 key-chain SBK standby 442 track 10 decrement 20 standby 642 ipv6 autoconfig standby 642 priority 110 standby 642 preempt standby 642 authentication md5 key-chain SBK standby 642 track 10 decrement 20 ! </pre>

VRRP – Virtual Router Redundancy Protocol

VRRP ist ein offener Standard (RFC 2338).

VRRP existiert bereits in 3 Versionen:

- VRRPv1
- VRRPv2
- VRRPv3 für IPv4/IPv6

Wie bei Ciscos proprietärem HSRP, wird bei VRRP ein virtueller Router (IP und MAC) aus einer Gruppe von redundanten Routern bereitgestellt.

Unterschiede:

- Bei VRR existieren nur 3 Router Arten:
 - **master** Router
entspricht dem HSRP active Router
 - **backup** Router
entspricht HSRP standby und member Routern
 - **virtual** Router
entspricht HSRP virtual Router
- Virtual Router Addressing
 - Die **IP Adresse des virtuellen Routers** kann ..
 - .. anders als bei HSRP, auch eine, von einem VRRP Router **verwendete IP Adresse** sein. In diesem Fall ist der Router auch automatisch master Router – die Priorität wird auf 255 (max.) erhöht und kann nicht verändert werden .. z.B. durch Tracking!
 - .. oder; wie bei HSRP, **administrativ festgelegt** werden. Wenn der Router master Router werden soll, ist zusätzlich die höchste Priorität zu konfigurieren.
 - Die **virtual MAC address** setzt sich wie folgt zusammen:
0000.5e00.{lfdNR}{VR-ID}.
Beispiel:
lfdNR (laufende Nummer) → master *01*, backup *02*;
vrrp group ID → 42 (0x**2a**)
MAC Adresse des master: 0000.5e00.**012a**
MAC Adresse des backup: 0000.5e00.**022a**
- Timer Bezeichnungen und Werte
 - **advertisement-interval** → default: **1 sek.**
 - **master-down-interval** → (immer) **3 x advertisement-interval**
- Preemption
 - im Gegensatz zu HSRP ist bei VRRP **preemption default aktiviert**
- Load Sharing über multiple VRRP Groups wird unterstützt
- Kommunikation
 - Bei VRRP **sendet nur der master router Nachrichten** in das Netzwerk (**IP Protocol 112, 224.0.0.18**)
 - Die TTL für VRRP packets muss 255 betragen.

Konfiguration VRRP

Aktivierung mit Angabe der VRRP-ID (VRRP Gruppennummer) und einer virtual Router IP.

Es ist empfehlenswert nicht die IP Adresses auf einem physikalischen Interface des Routers als virtuelle GW IP zu verwenden, da z.B. dann das Tracking nicht möglich ist.
Die virtuelle IP sollte immer administrativ bestimmt werden.

```
(config-if)# vrrp vrrp-group-id ip virtual-router-ip
```

Manuelle Festlegung der **Priorität** (default 100).
.. zur administrative Bestimmung des master Routers.

```
(config-if)# vrrp vrrp-group-id priority priority
```

Authentication

VRRP unterstützt plain text und md5 authentication

Plain Text Authentication

```
(config-if)# vrrp vrrp-group-id authentication text password
```

MD5 Authentication mit key-string

```
(config-if)# vrrp vrrp-group-id authentication md5 key-string password
```

MD5 Authentication mit key-chain

```
(config)# key chain key-chain-name  
(config-keychain)# key key-number  
(config-keychain-key)# key-string password
```

```
(config-if)# vrrp vrrp-group-id authentication md5 key-chain key-chain-name
```

Preemption ist default aktiv – kann mit no deaktiviert werden (nicht empfehlenswert).
Preemption

- bedeutet, dass ein Router IMMER seine seine Rolle als master einfordert.
Bsp.:
 - fällt der master aus, wird der backup zum master
 - ist der ehemalige master wieder erreichbar, fordert er seine ehemalige Rolle vom augenblicklichen master wieder ein, und wird wieder zum master.
 - mit delay kann für die „Rück-Übernahme“ eine Verzögerungszeit eingestellt werden
.. machmal sinnvoll beim Tracking

```
(config-if)# [no] vrrp vrrp-group-id preempt [ delay seconds ]
```

Troubleshooting

```
# show vrrp  
# show vrrp brief  
# show vrrp interface if-type if-nr
```

VRRP Tracking

Optional: VRRP Tracking

Es kann u.U. nützlich sein, dass eine master Router seine aktive Rolle verliert, wenn eine andere Verbindung des Routers ausgefallen ist, als die Verbindung in das LAN.

Zum Beispiel wenn die ISP Verbindung des master Routers ausfällt (der backup Router aber noch über Konnektivität ins Internet verfügt), sollte dieser Router von den Hosts im LAN nicht mehr als Default-GW verwendet werden.

Bei VRRP Tracking wird der Status eines IF überprüft.

Wenn das angegebene IF in den Status "down" wechselt, wird die Priorität um den angegebenen Wert (decrement) oder **10** (default decrement) vermindert.

```
(config-if)# vrrp group-id track IF-ID [ decrement ]
```

Tracking Objects

Erweiterte Tracking Möglichkeiten stehen durch modulare Konfiguration eines Tracking Objekts mit eindeutiger ID (Track Nr) zur Verfügung, das dann von HSRP verwendet wird, wie z.B.

Interface Tracking → OSI 2 Funktion, OSI 3 Funktion

```
(config)# track track-nr interface IF-ID [line-protocol | ip routing]
```

IP Route Tracking → Vorhandensein einer Route in der Routing Tabelle

```
(config)# track track-nr ip route net-id/länge reachability
```

IP SLA Tracking → z.B. Erreichbarkeit einer IP durch regelmäßiges Senden von ping Paketen

1. Anlegen einer SLA Operation (ip sla sla-nr)
- .. Senden von ping Paketen (icmp-echo) .. default: alle 5 Sekunden (frequency)
2. Starten der SLA Operation (ip sla schedule): für immer (life) sofort (start-time)
3. Anlegen des Tracks

```
(config)# ip sla sla-nr
(config-ip-sla)# icmp-echo dst-IP [ source-ip src-IP | source-interface IF-ID ]
(config-ip-sla-echo)# frequency sekunden
```

```
(config)# ip sla schedule sla-nr life forever start-time now
```

```
(config)# track track-nr ip sla sla-nr [state | reachability]
```

Tracking Object mit VRRP verwenden

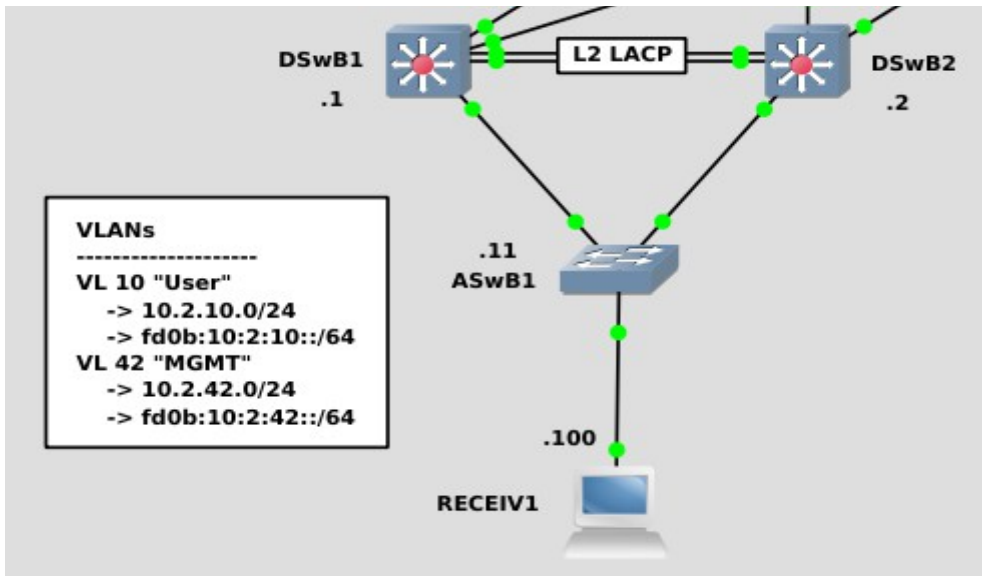
→ den angelegten Track mit Hilfe der Track-Nummer für HSRP nutzen. Default decrement: 10

```
(config-if)# vrrp group-nr track track-nr [decrement wert]
```

Troubleshooting

```
# show track [track-nr]
# show vrrp [group-nr]
```

VRRP Konfigurationsbeispiel



DSwB1	DSwB2
→ VLAN 10: MASTER, → VLAN 42: BACKUP → MD5 Autentication mit Key Chain → IP SLA Trackauf remote IP 10.10.10.10 inkl. preemption	→ VLAN 10: BACKUP, → VLAN 42: MASTER → MD5 Authentication mit Key Chain → IP SLA Trackauf remote IP 10.10.10.10 inkl. preemption
<pre> ! ip sla 10 icmp-echo 10.10.10.10 frequency 5 ip sla schedule 10 start now life forever ! track 10 ip sla 10 reachability ! key chain SBK key 7 key-string geheim ! int vlan 10 ip address 10.2.10.1 255.255.255.0 vrrp 10 ip 10.2.10.254 vrrp 10 priority 110 vrrp 10 authentication md5 key-chain SBK vrrp 10 track 10 decrement 20 ! int vlan 42 ip address 10.2.42.1 255.255.255.0 vrrp 42 ip 10.2.42.254 vrrp 42 priority 110 vrrp 42 authentication md5 key-chain SBK ! </pre>	<pre> ! ip sla 10 icmp-echo 10.10.10.10 frequency 5 ip sla schedule 10 start now life forever ! track 10 ip sla 10 reachability ! key chain SBK key 7 key-string geheim ! int vlan 10 ip address 10.2.10.1 255.255.255.0 vrrp 10 ip 10.2.10.254 vrrp 10 authentication md5 key-chain SBK ! int vlan 42 ip address 10.2.42.1 255.255.255.0 vrrp 42 ip 10.2.42.254 vrrp 42 priority 110 vrrp 42 authentication md5 key-chain SBK vrrp 42 track 10 decrement 20 ! </pre>

VRRPv3

.. unterstützt IPv4 und IPv6 mit address-family Konfiguration.

Ansonsten sind Funktionalitäten nahezu identische mit VRRPv2 - ausser das Authentication NICHT unterstützt wird.

Wichtigste Unterschiede zw. VRRPv2 und VRRPv3

	VRRPv2	VRRPv3
Authentication	MD5 und PlainText	nicht möglich
Multicast	224.0.0.18	224.0.0.18 ff02::12

Konfiguration

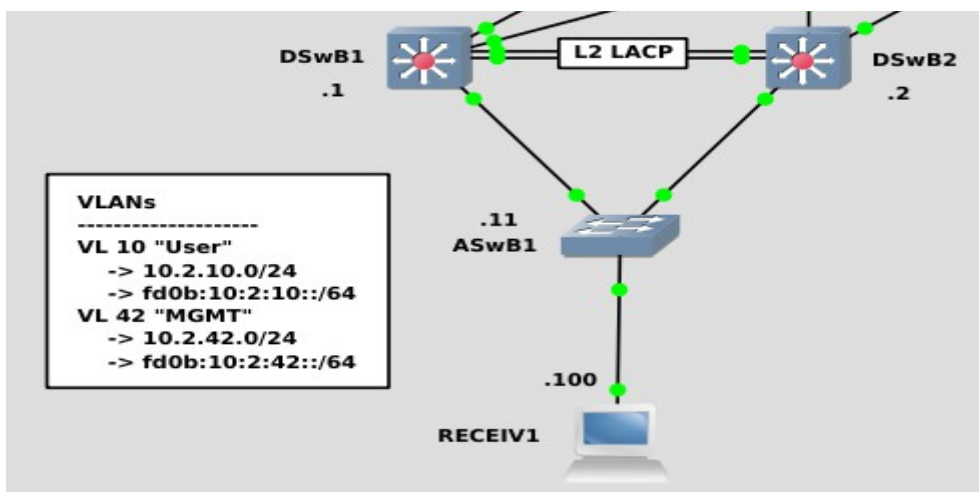
VRRP Version 3 aktivieren

```
(config)# vrp version vrrp v3
```

Einstellungen auf dem Interface

```
(config)# interface IF-ID
(config-if)# vrrp vrrp-ID address-family { ipv4 | ipv6 }
(config-if-vrrp)# priority wert
(config-if-vrrp)# address { IPv4 | IPv6 } primary
(config-if-vrrp)# track track-ID decrement wert
(config-if-vrrp)# exit-vrrp
```

VRRPv3 Konfigurationsbeispiel



DSwB1	DSwB2
→ VLAN 10: MASTER, → VLAN 42: BACKUP → MD5 Authentication mit Key Chain → IP SLA Trackauf remote IP 10.10.10.10 inkl. preemption	→ VLAN 10: BACKUP, → VLAN 42: MASTER → MD5 Authentication mit Key Chain → IP SLA Trackauf remote IP 10.10.10.10 inkl. preemption
<pre> ! ip sla 10 icmp-echo 10.10.10.10 frequency 5 ip sla schedule 10 start now life forever ! track 10 ip sla 10 reachability ! fhrp version vrrp v3 ! int vlan 10 ip address 10.2.10.1 255.255.255.0 ipv6 address fe80::db1 link-local ipv6 address fd0b:10:2:10::1/64 vrrp 10 address-family ipv4 priority 110 address 10.2.10.254 primary track 10 decrement 20 exit-vrrp vrrp 10 address-family ipv6 priority 110 address FE80::254 primary track 10 decrement 20 exit-vrrp ! int vlan 42 ip address 10.2.42.1 255.255.255.0 ipv6 address fe80::db2 link-local ipv6 address fd0b:10:2:42::2/64 vrrp 42 address-family ipv4 priority 110 address 10.2.42.254 primary track 10 decrement 20 exit-vrrp vrrp 42 address-family ipv6 priority 110 address FE80::254 primary track 10 decrement 20 exit-vrrp ! </pre>	<pre> ! ip sla 10 icmp-echo 10.10.10.10 frequency 5 ip sla schedule 10 start now life forever ! track 10 ip sla 10 reachability ! fhrp version vrrp v3 ! int vlan 10 ip address 10.2.10.1 255.255.255.0 ipv6 address fe80::db1 link-local ipv6 address fd0b:10:2:10::1/64 vrrp 10 address-family ipv4 address 10.2.10.254 primary exit-vrrp vrrp 10 address-family ipv6 address FE80::254 primary exit-vrrp ! int vlan 42 ip address 10.2.42.1 255.255.255.0 ipv6 address fe80::db2 link-local ipv6 address fd0b:10:2:42::2/64 vrrp 42 address-family ipv4 priority 110 address 10.2.42.254 primary track 10 decrement 20 exit-vrrp vrrp 42 address-family ipv6 priority 110 address FE80::254 primary track 10 decrement 20 exit-vrrp ! </pre>

TRICKY: IPv6 First Hop Redundanz via NDP RA und EEM Tracking

IPv6 First Hop Redundancy mit Tracking ohne FHRP

primary/secondary GW via ND Router Advertisements

- Konfiguration für „primary“ Router
 - ND router-preference → high
- Konfiguration für „secondary“ Router
 - keine - default ND router-preference → medium

EEM für Tracking auf „primary“ Router

- Track down
 - ND router-preference set to low: „secondary“ Router übernimmt GW (medium)
- Track up
 - ND router-preference set to high: „primary“ Router übernimmt GW

Die Konfigurationsänderung via EEM bewirkt sofortiges Senden eines RA, und damit einen direkten Wechsel des Default GW's auf den Endgeräten.

Beispielkonfiguration „primary“ Router

→ mit IP SLA Tracking

```

!
ip sla 1
 icmp-echo 172.16.0.9 source-interface loopback 0
 frequency 5
ip sla schedule 10 start now life forever
!
track 1 ip sla 1 reachability
!
int fa 0/0
 descr -> LAN
 ip address 10.1.9.1 255.255.255.0
 ipv6 address fe80:88::1 link-local
 ipv6 address 2000:1:8:1::1/64
 ipv6 nd router-preference high
!
event manager applet ND-RPrefLOW
 event track 1 state down
 action 1.0 cli command "enable"
 action 1.1 cli command "conf t"
 action 1.2 cli command "interface fastethernet0/0"
 action 1.3 cli command "ipv6 nd router-preference low"
 action 1.4 cli command "end"
 action 2.0 puts "ND Preference set to LOW"
event manager applet ND-RPrefHIGH
 event track 1 state up
 action 1.0 cli command "enable"
 action 1.1 cli command "conf t"
 action 1.2 cli command "interface fastethernet0/0"
 action 1.3 cli command "ipv6 nd router-preference high"
 action 1.4 cli command "end"
 action 2.0 puts "ND Preference set to HIGH"
!

```


GLBP – Gateway Load Balancing Protocol

Ein Nachteil von HSRP oder VRRP ist, das immer nur genau ein Router als Default-GW verwendet wird – obwohl redundante Pfade vorhanden sind.

Eine Art Load Sharing für HSRP bzw. VRRP ist zwar mit multiplen Gruppen möglich, aber erfordert zusätzlichen administrativen Aufwand bei der Konfiguration der Router und der Hosts im LAN (unterschiedliche Default-GW Adressen).

GLBP ist ein Protokoll, das **Lastverteilung zwischen unterschiedlichen möglichen Default-GWs** im Netzwerk implementiert

Arbeitsweise GLBP

Eine GLBP group kann aus maximal 4 Routern bestehen, die als Default-Gateway arbeiten: sogenannte **AVFs – active virtual forwarders** (weitere Router sind **secondary VFs**).

GLBP verwaltet alle notwendigen Funktionen innerhalb der GLBP Gruppe, durch den "master" Router der Gruppe: **AVG - active virtual gateway** - der natürlich auch eine AVF ist.

Das AVG regelt z.B. die virtuelle MAC Adressierung (in ARP Response) und somit die (default) Lastverteilung (round robin) zwischen den AVFs.

- Wenn ein Host eine ARP Anfrage für die virtual IP stellt ..
.. antwortet (nur) der AVG mit einer MAC Adresse, die er aus seinem aktuellen load-balancing algorithm ermittelt.
- Wenn ein zweiter Host eine ARP Anfrage stellt ..
.. bekommt er vom AVG eine andere MAC Adresse mitgeteilt.

Von GLBP unterstützte load-balancing algorithm

- **Round-robin load-balancing algorithm (default)**
nach ARP: jeder ARP Request wird mit einer anderen MAC Adresse beantwortet
- **Weighted load-balancing algorithm**
nach Einstellung des maximum weight Werts der AVFs
- **Host-dependent load-balancing algorithm**
nach ARP eines gleichen Hosts (gleicher Host → immer gleiche Default GW MAC)

Bestimmung des **AVG**: höchste Priorität, wenn gleich: höchste IP

Bei GLBP ist (AVG) preemption default nicht aktiv.

- Wenn der AVG ausfällt, wird der AVF mit der nächsten, höchsten priority zum AVG.
- Wird der vormals ausgefallenen AVG wieder aktiv, übernimmt er nur dann wieder die Rolle des AVG, wenn **priority preemption** (default: deaktiviert) konfiguriert wurde.

Bestimmung eines **AVF**: höchster weight, wenn gleich: höchste IP.

Bei GLBP ist auch (AVF) preemption default aktiv.

Ein AVG ist immer auch ein AVF.

(AVF) Tracking – Bestimmung der AVF Funktionalität (**weight**)

- Einem AVF kann eine Gewichtung (**maximum weight**) zugeordnet werden, die quasi einer Priorität entspricht und festlegt, ob eine Router AVF wird oder nicht (default maximum weight: 100)
- Der voreingestellte maximum weight Wert kann – bei Ausfall einer Schnittstelle – automatisch reduziert werden (default weight decrement: 10)
- Wenn ein AVF einen konfigurierten **lower weight** Wert unterschreitet, verliert er die Funktion als AVF – wenn er einen konfigurierten **upper weight** Wert überschreitet wird er automatisch wieder zum AVF (default: **weight preemption** aktiv).

Konfiguration GLBP

Aktivierung von GLBP und Festlegung der virtuellen Gateway IP Adresse.

```
(config-if)# glbp glbp-id ip virtual-gateway-ip
```

(AVG) Priorität: Manuelle Konfiguration der Priorität für die Rolle des AVG (default 100)

```
(config-if)# glbp glbp-id priority priority
```

AVG priority preemption → default: deaktiviert

```
(config-if)# glbp glbp-id preempt [ delay minimum seconds ]
```

Load Balancing Verfahren festlegen (default: round-robin)

```
(config-if)# glbp glbp-id load-balancing \  
[ host-dependent | round-robin | weighted ]
```

Timer Manipulation (weniger empfehlenswert)

```
(config-if)# glbp glbp-id timers [ msec ] hello-time [ msec ] hold-time
```

AVF Weighting

zur Bestimmung ob eine Router AVF für eine Gruppe ist oder diese Funktion verliert - anstelle der Priorität (regelt ob ein Router AVG wird) wird eine Gewichtung (**maximum weight**) verwendet. Der maximum weight Wert wird ebenfalls für das **weighted Load-balancing** (falls konfiguriert) verwendet.

- **maximum weight** (default 100) → regelt ob ein Router **AVF** oder **secondary VF** wird bzw. bei weighted Load-balancing, wie oft die virtuelle MAC des AVFs in Antworten des AVGs an Hosts gesendet wird.
- **lower/upper weight** → .. für Tracking: wird der lower weight Wert unterschritten verliert der Router den Status als AVF, wird der upper weight Wert wieder erreicht, wird er wieder zum AVF.

```
(config-if)# glbp glbp-id weighting maximum [ lower lower ] [ upper upper ]
```

AVF Tracking

```
(config)# track object-nr interface if-type if-nr [ line-protocol | ip routing ]  
(config-if)# glbp glbp-id weighting track object-nr [ decrement value ]
```

AVF (weight) preemption → default: aktiv

```
(config-if)# glbp glbp-id forwarder preempt
```

Authentication

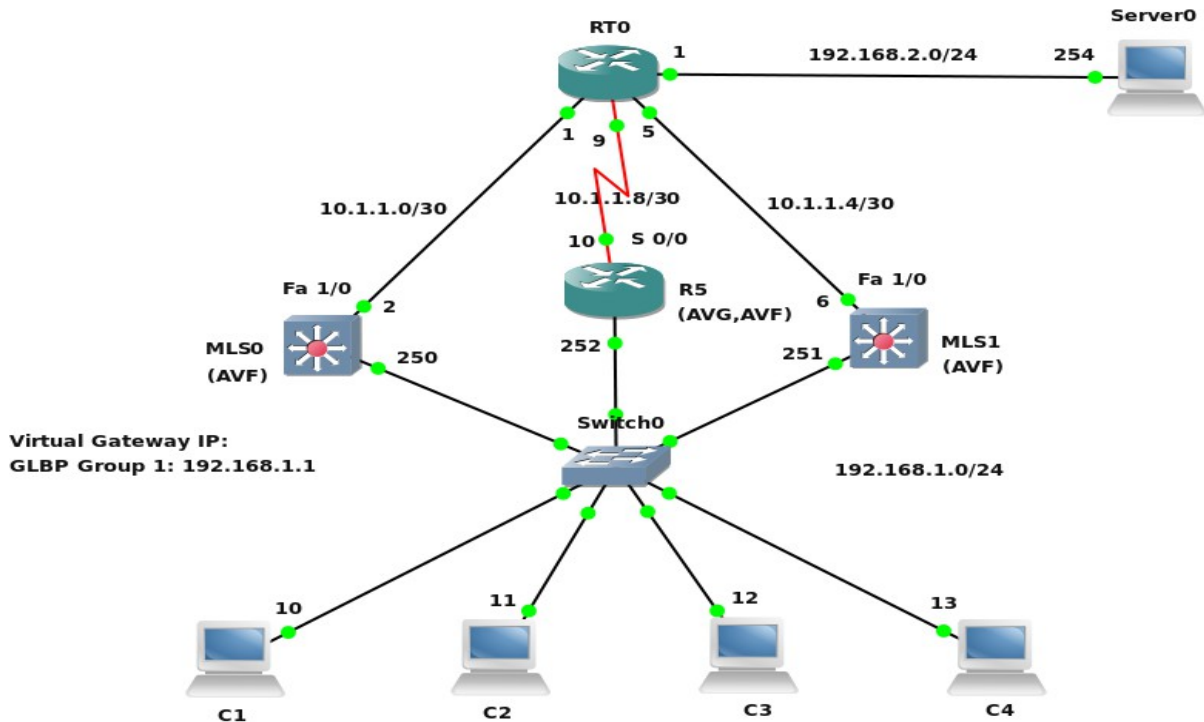
VRRP unterstützt: no, plain text und md5 authentication (auch mit key-chain)

```
(config-if)# glbp glbp-id authentication md5 key-string key
```

Troubleshooting

```
# show glbp  
# show glbp brief  
# show glbp interface if-type if-number
```

Konfigurationsbeispiel GLBP



MLS0 (backup AVG, AVF)	R5 (AVG, AVF)	MLS1 (AVF)
<pre>! track 1 interface FastEthernet1/0 ip routing ! interface Vlan1 ip address 192.168.1.250 255.255.255.0 duplex full glbp 1 ip 192.168.1.1 glbp 1 priority 110 glbp 1 preempt glbp 1 weighting 110 lower 95 upper 105 glbp 1 authentication md5 key-string geheim glbp 1 weighting track 1 decrement 20 !</pre>	<pre>! track 1 interface Serial1/0 ip routing ! interface FastEthernet0/0 ip address 192.168.1.252 255.255.255.0 duplex full glbp 1 ip 192.168.1.1 glbp 1 priority 120 glbp 1 preempt glbp 1 weighting 110 lower 95 upper 105 glbp 1 authentication md5 key-string geheim glbp 1 weighting track 1 decrement 20 !</pre>	<pre>! track 1 interface FastEthernet1/0 ip routing ! interface Vlan1 ip address 192.168.1.251 255.255.255.0 duplex full glbp 1 ip 192.168.1.1 glbp 1 weighting 110 lower 95 upper 105 glbp 1 authentication md5 key-string geheim glbp 1 weighting track 1 decrement 20 !</pre>

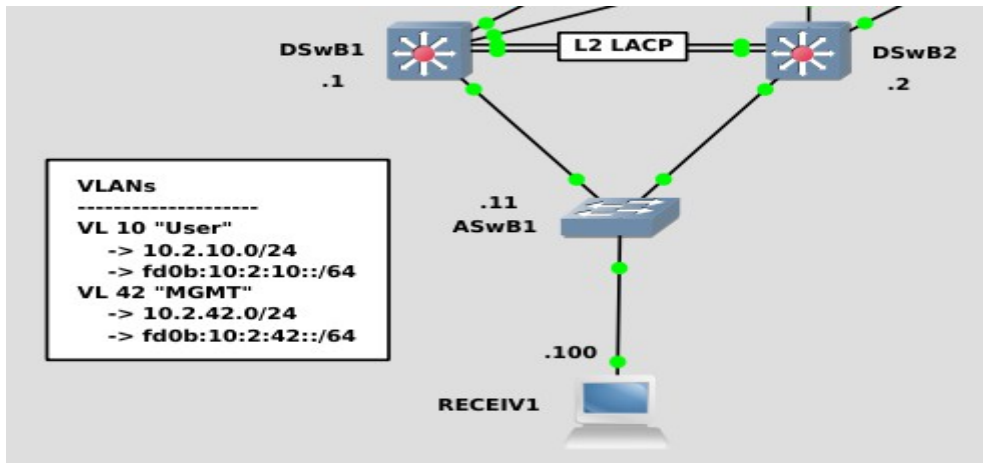
Besonderheiten der Konfiguration:

- Fällt R5 aus, wird MLS0 zum AVG (priority 110) – ist R5 wieder verfügbar übernimmt er wieder die Rolle des AVG (glbp 1 preempt).
- Fallt auf einem der Geräte das überwachte IF aus, reduziert sich die forwarder priority (weight) um 20 auf 90 (110 – 20 = 90). Da 90 kleiner ist als der lower weight (95) ist er nicht mehr aktiver AVF. Wenn die Schnittstelle wieder "up" ist wird er automatisch wieder aktiver AVF (AVF weight preemption ist default aktiv), da der weight Wert dann wieder 110 beträgt und somit größer als der upper weight Wert (105) ist.
HINWEIS: Fällt das überwachte IF auf dem AVG (R5) aus, bleibt R5 der AVG, aber ist kein aktiver AVF mehr.

Konfiguration GLBP für IPv4 und IPv6

Sobald eine IPv6 Adresse auf dem Interface konfiguriert ist, ist GLBP automatisch auch für IPv6 aktiv.

Es wird explizit KEINE virtuelle IPv6 Adresse konfiguriert.



<p>DSwB1 → VLAN 10: AVG, AVF → MD5 Autentication mit Key Chain</p>	<p>DSwB2 → VLAN 10: AVF → MD5 Authentication mit Key Chain</p>
<pre>! interface Vlan10 description -> USER ip address 10.2.10.1 255.255.255.0 ipv6 address FE80::DC1 link-local ipv6 address FD0C:10:2:10::1/64 glbp 10 ip 10.2.10.254 glbp 10 priority 110 glbp 10 preempt !</pre>	<pre>! interface Vlan10 description -> USER ip address 10.2.10.2 255.255.255.0 ipv6 address FE80::DC2 link-local ipv6 address FD0C:10:2:10::2/64 glbp 10 ip 10.2.10.254 glbp 10 preempt !</pre>

Überblick: Eigenschaften HSRPv1, VRRPv2, GLBP

	HSRP	VRRP	GLBP
Bezeichnung	Hot Standby Routing P.	Virtual Router Redundancy P.	Global Load Balancing P.
Protokoll	Cisco .. und RFC 2281	RFC 2338	Cisco
Kommunikation	224.0.0.2 UDP 1985	224.0.0.18 IP 112	224.0.0.102 UDP 3222
Max. Router	2 optimal	2 optimal	4
Router	active router standby router .. und member router	master router backup router .. und virtual router	AVG – active virtual gateway AVF – active virtual forwarder .. und secondary VF
Mehrere Router können gleichzeitig Traffic weiterleiten	Nein	Nein	Ja (bis zu 4)
Load Sharing/ Load Balancing	multiple groups	multiple groups	default: round robin – per ARP Req. optional: weighted – per Load optional: host-dependend – per Host
Interface IP als virtual IP	Nein	Ja → wird dann auto. master	Nein
default Priorität	100	100	AVG priority: 100 AVF weight: 100
max. Priorität	255	255	AVG priority: 255 AVF weight: 255
Virtual MAC	0000.0c07.ac<group-id>	0000.5e00.<IfdNR><group-id>	0007.b400.<groupID><IfdNR>
Timer	Hello: 3 Sekunden Holddown: 10 Sekunden	advertisement-interval: 1 Sekunde master-down-time: 3 * advertisement-interval	Hello: 3 Sekunden Holddown: 10 Sekunden
Preemption	default: deaktiviert	default: aktiviert	AVG priority: default deaktiviert AVF weight: default aktiviert
Tracking	Möglich für Priorität: default decrement 10	Möglich für Priorität: default decrement 10	Möglich für weight (AVF): default decrement 10
Authentication	no auth plain text md5	no auth plain text md5	no auth plain text md5