Access Concentrators

Optimizing Availability and Performance

FMS Internetservice GmbH

Company Profile

FMS Internetservice GmbH

- Value Added Distributor
  - Distribution
  - Training
  - Consulting
  - Support

- Founded 1997
- 11 employees
- Southern Germany

Get in Touch

- Phone: +49 761 2926500
- Email: sales@fmsweb.de
- Shop: https://www.mikrotik-shop.de

- MikroTik Mirror: http://www.mikrotik-software.de
- Twitter: https://twitter.com/fmsweb_de
- Website: http://www.fmsweb.de
- Wiki: http://wiki.fmsweb.de
- Presentations: http://wiki.fmsweb.de/wiki/MUM-Presentations
- Facebook: https://www.facebook.com/fmsinternetservice

Training Center

- Official MikroTik trainings
- All certification levels
- First German speaking partner
- Two trainers
- Own training facility
- Inquiries: sales@fmsweb.de
- Schedule for 2018: click
- Sebastian Inacker: TR11
- Patrik Schaub: TR23

Services

- Consulting
- Deployment
- Support
- Training
- Support Contract

- Smal to large enterprise customers
- Internet Service Provider
  - Stadtwerke

Examples

- National & global VPNs with hundreds of sites

- ISP backbone and access networks

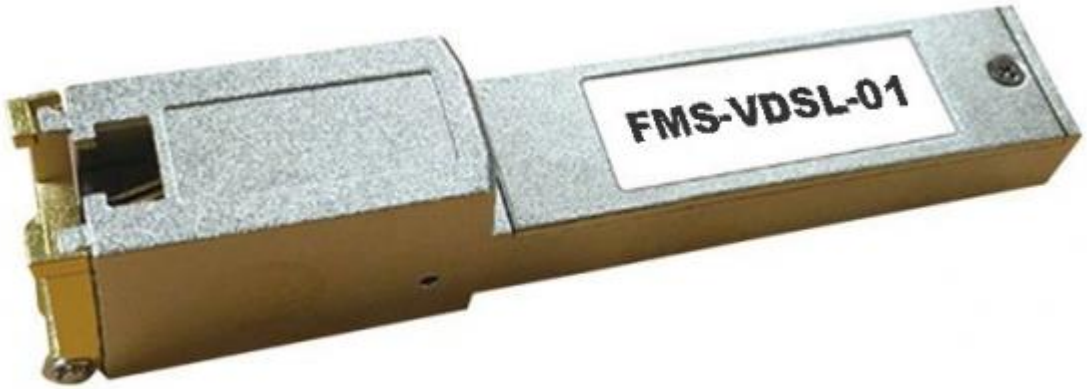
- Sicherheitskonzepte, TAL Contract, RIPE LIR

Distributor Table

Distributor Table

VDSL2 SFP Modules

- Transparent DSL modem for MikroTik
- Vectoring support
- Shop: click



Distributor Table

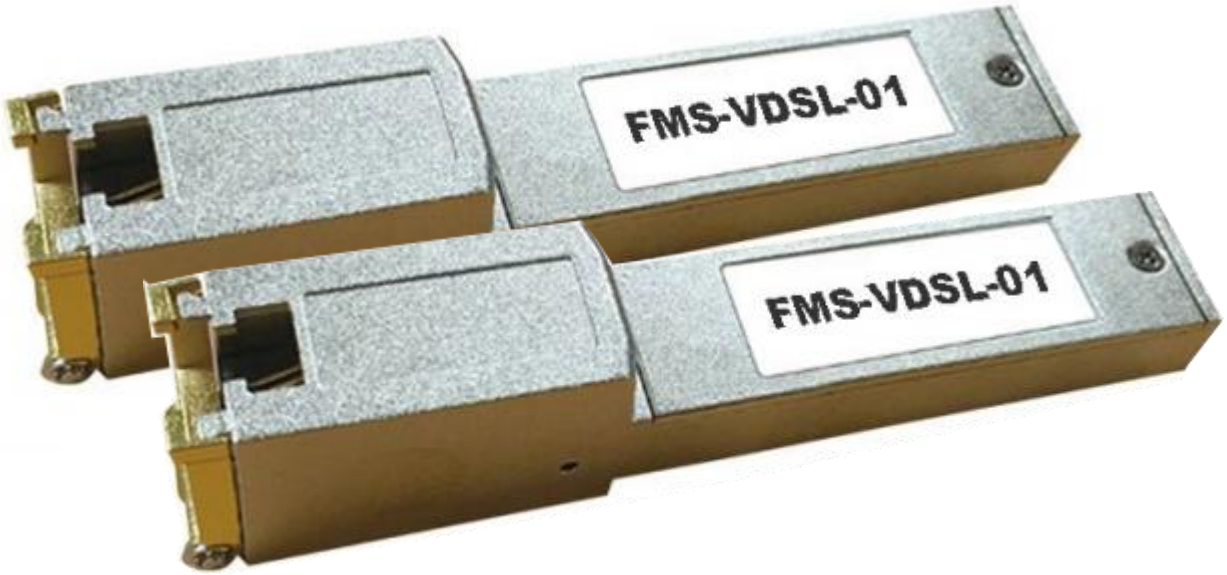
Spectrum Analysers and Signal Generators

- 2,4 & 5GHz
- 60 GHz – e.g. site surveys for 802.11ad

Distributor Table

Live Demonstrations:

- Long range Ethernet with MikroTik for 300m
- Shop: click



Distributor Table

Do you need towers or masts? Contact sales@fmsweb.de

Introduction

Access Concentrators

Concentrator

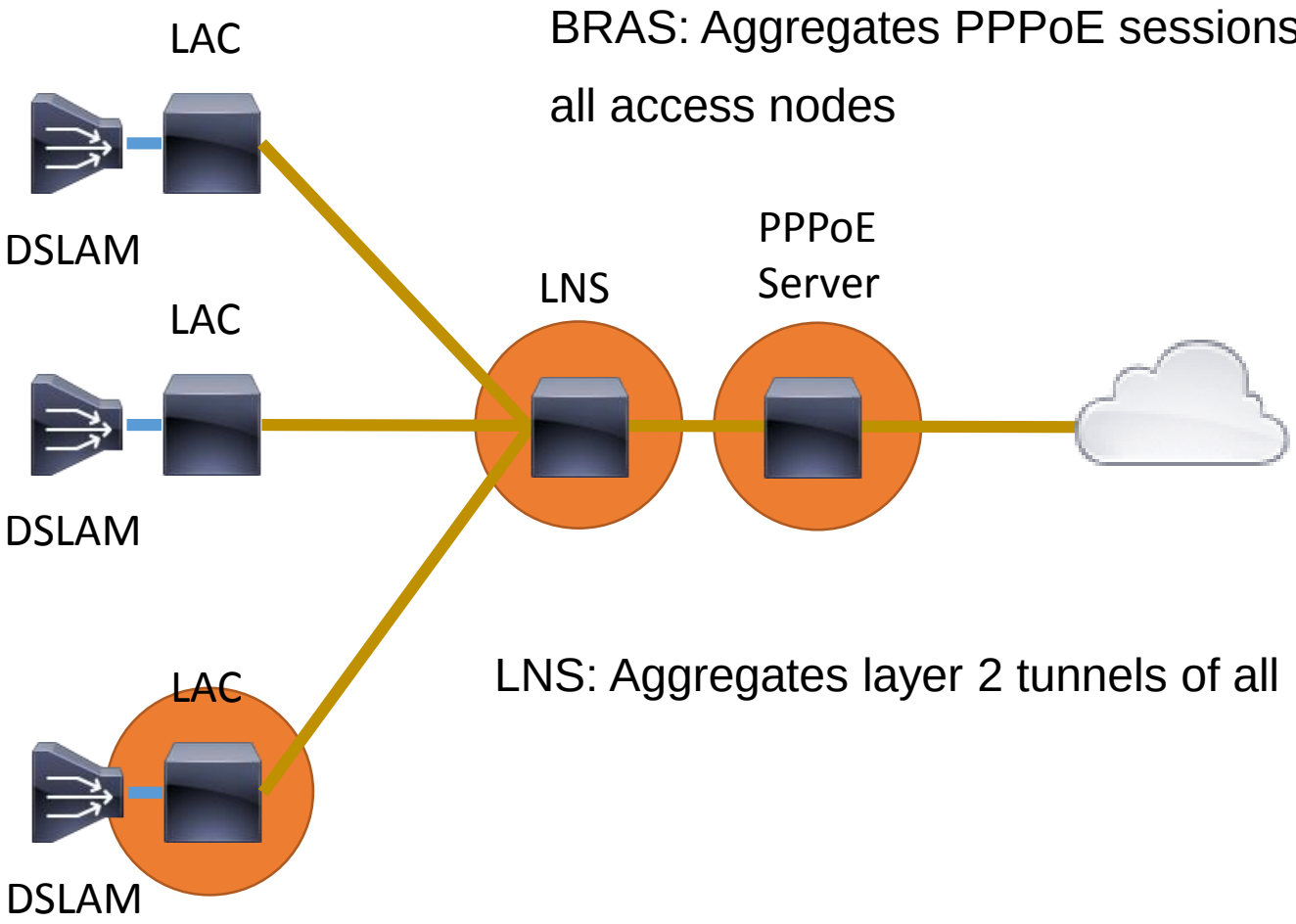
- Endpoint for multiple connections
- Traffic aggregation
- Entry point to another logical network area

  (e.g. gateway to an IP segment)

Types

- Remote access concentrator
  - Used in dial up networks
  - ISDN / POTS
- LAC/LNS
  - E.g. used in broadband networks
  - Aggregate and forward PPPoE traffic
- VPN Server
- BRAS (PPPoE Server)

Multiple Access Concentrators



BRAS: Aggregates PPPoE sessions of all access nodes

LNS: Aggregates layer 2 tunnels of all LACs

LAC: Aggregates users of one access node

Considerations for running ACs

- Services a lot of users
- Failure is critical
- Central single point of failure

- High demand of system resources
  - Network throughput (PPPoE)
  - CPU usage (VPN encryption, PPPoE)

Considerations for running ACs

Critical single point of failure

- Redundancy / fail over

High demand of system resources

- Load balancing

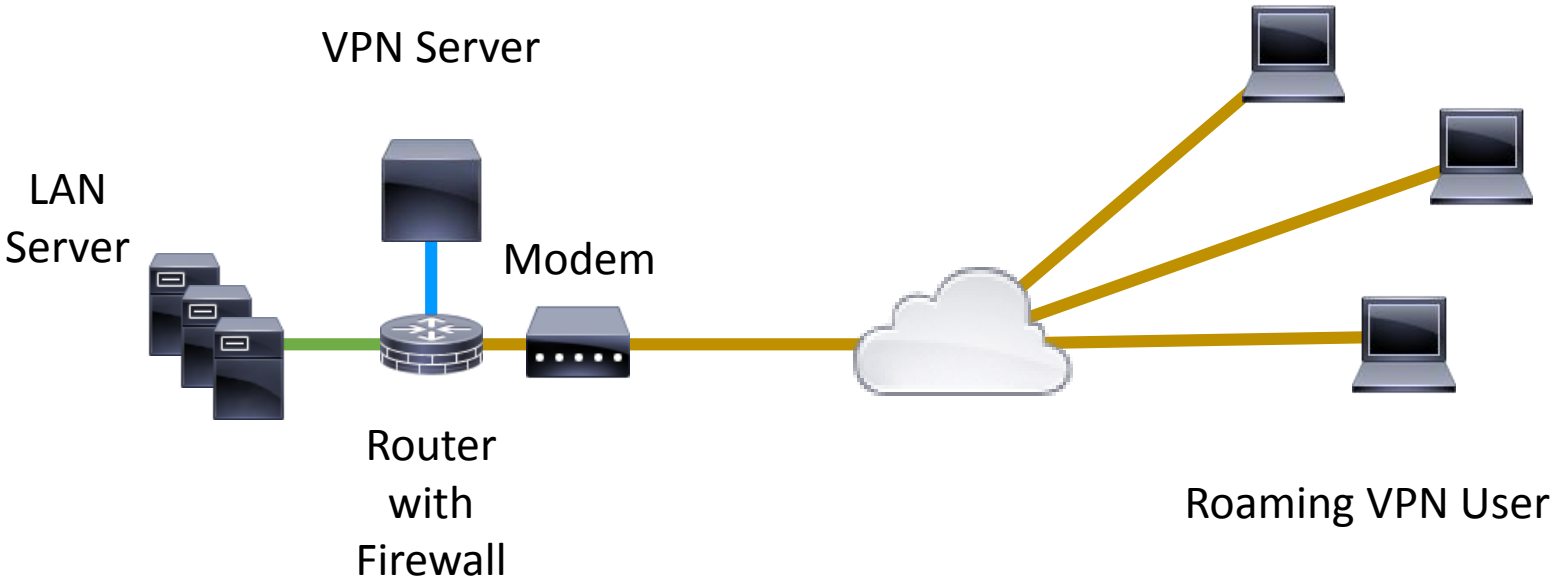
Best Approach

- Load balancing with fail over

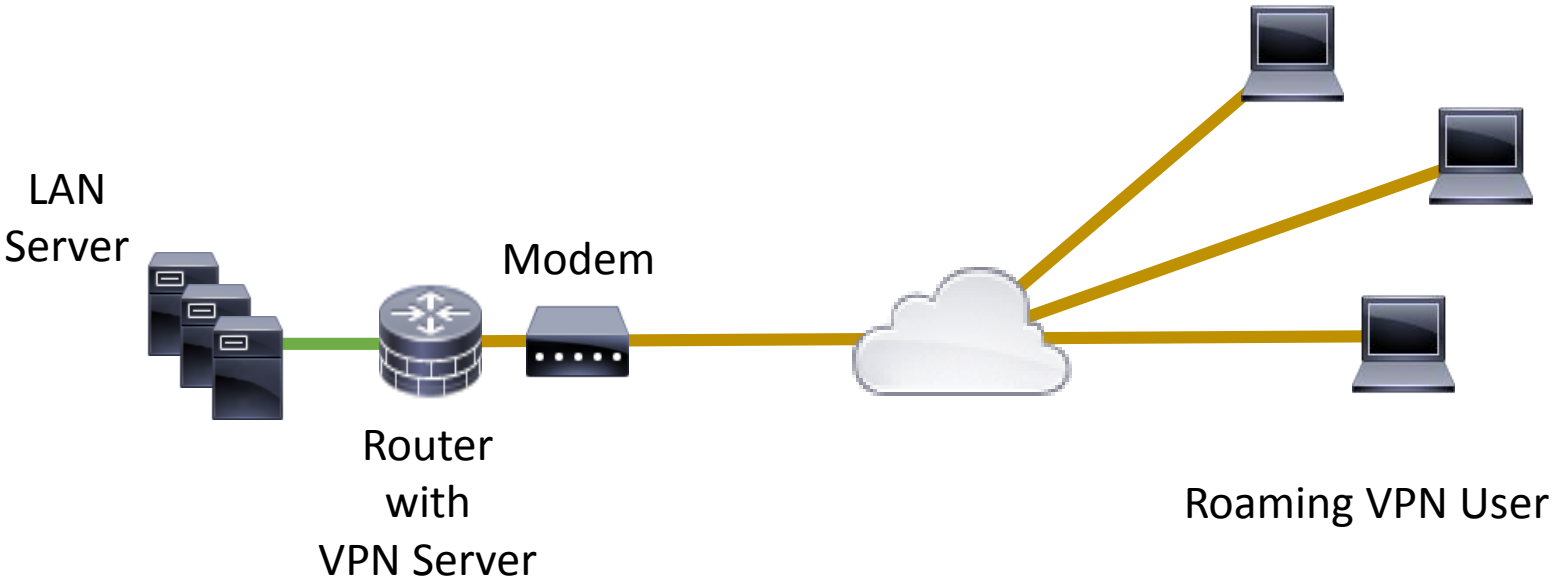
Enterprise Networks

VPN Access Concentrators

Enterprise VPN with DMZ



Enterprise VPN without DMZ



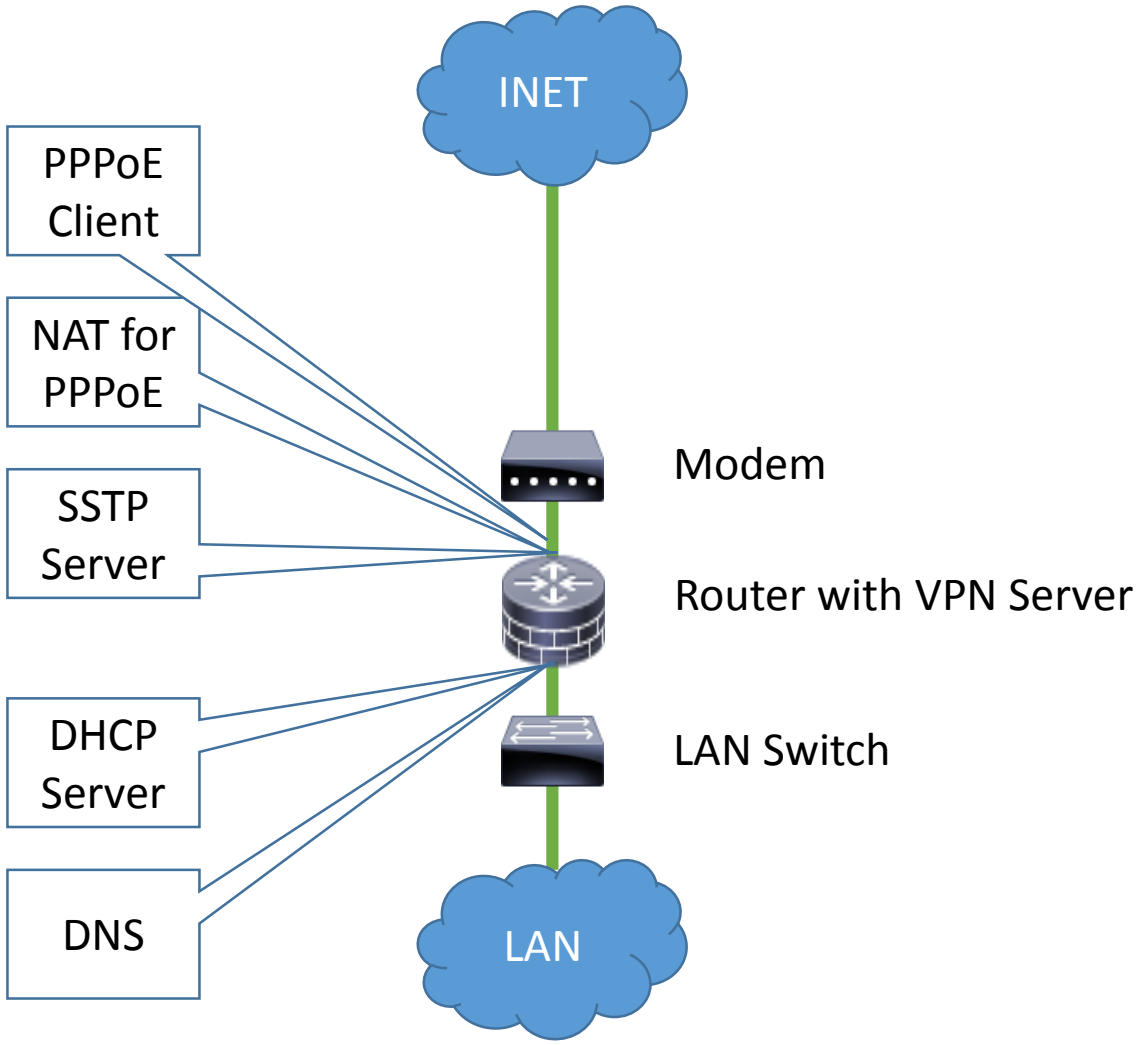
Single points of failure:

- VPN server
- broadband line

Broadband VPN Gateway

Assumptions:

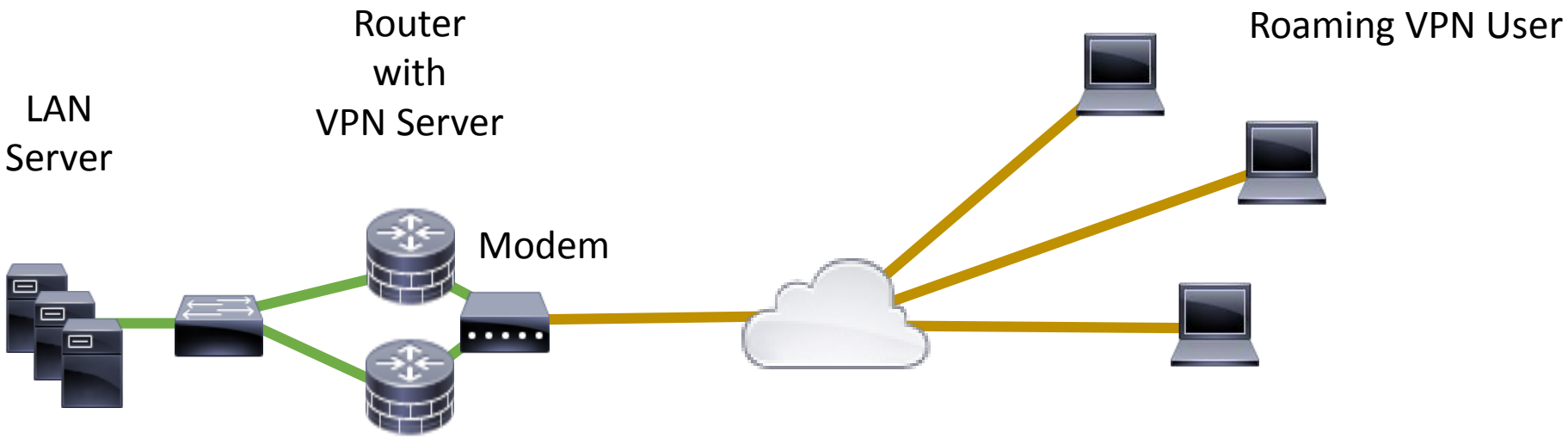
- Basic setup present
- Not discussed unless special considerations necessarry



Enterprise VPN

Hardware Redundancy

Hardware Redundancy



- Switching between the PPPoE clients
- Selecting Default Gateway for the LAN
- Two DHCP servers
- Dynamic public IP address for VPN server
- LAN cable / port failure

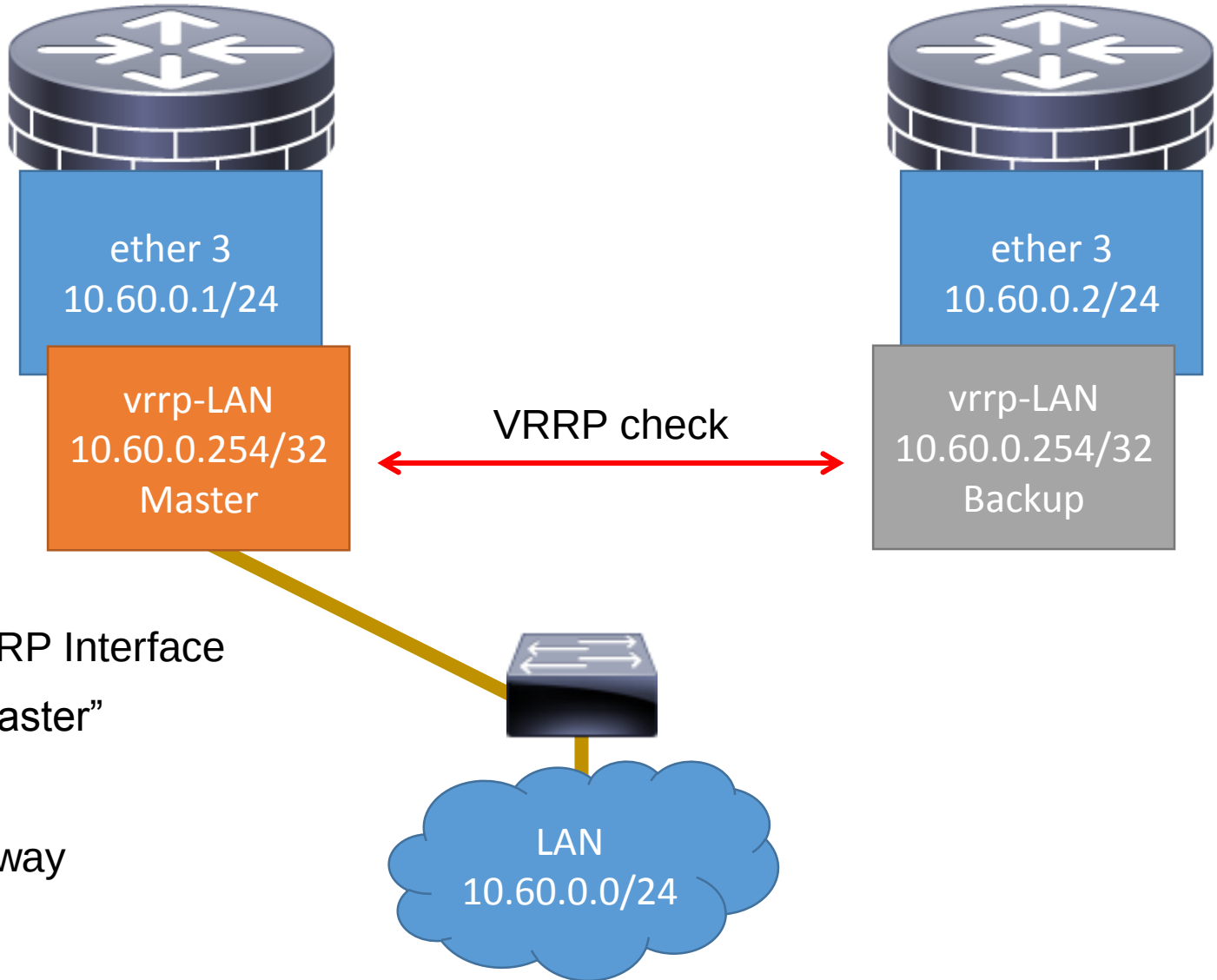
Redundant Default Gateway

- LAN devices will not support dynamic routing
- Default Gateway IP cannot change
- Both Gateways have to share the same IP

- VRRP
- Virtual Router Redundancy Protocol

- Master and Backup router (interface) share IP

Redundant Default Gateway



Only one VRRP Interface

“Runnning Master”

Default Gateway

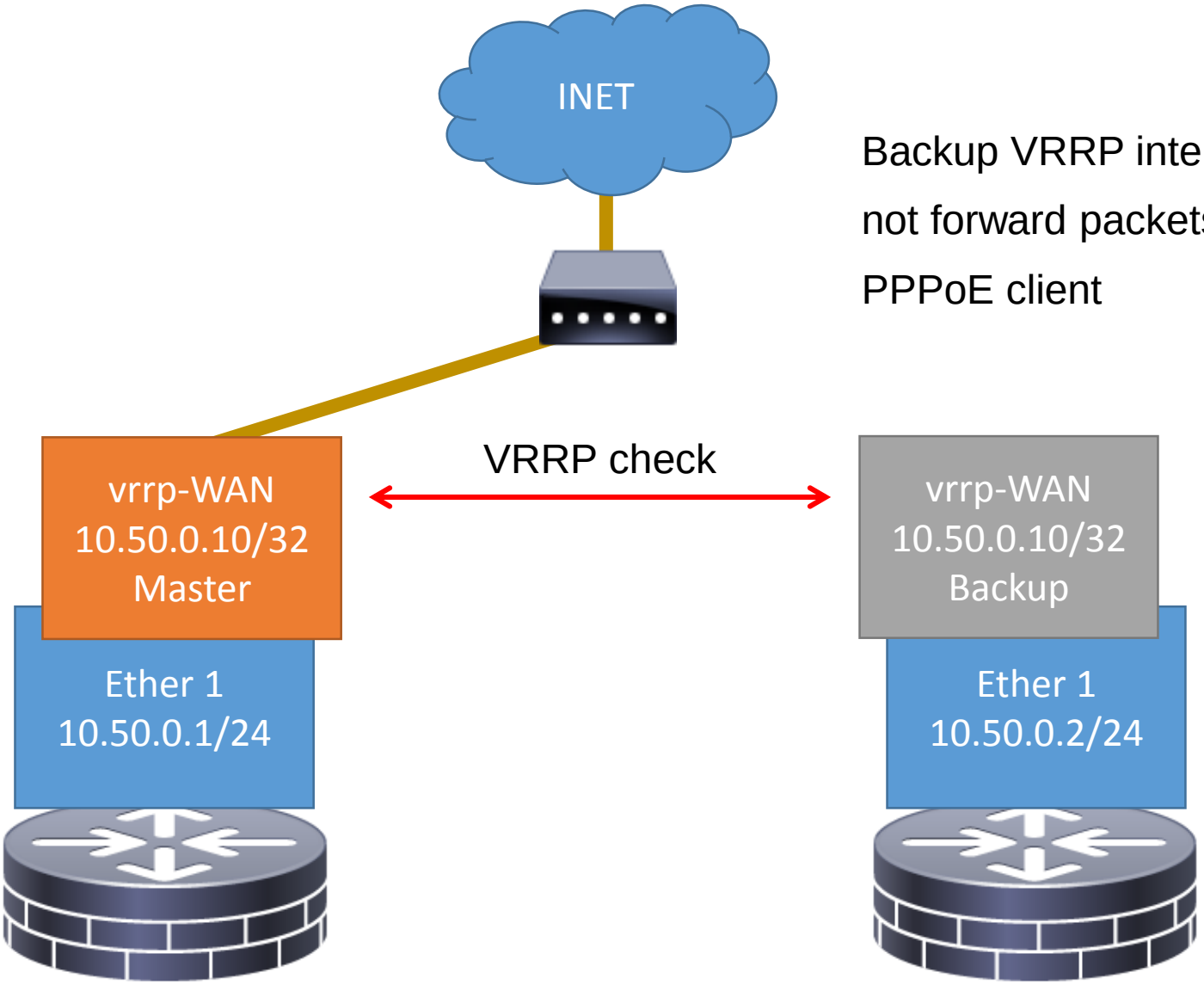
10.60.0.254

Switching PPPoE Client

- Usually ISP will not support multiple sessions
- Routers have to decide where PPPoE shall connect

- VRRP can be (miss)used
- Run pppoe-client on vrrp interface
- Backup interface will not be running
- PPPoE-client will not connect

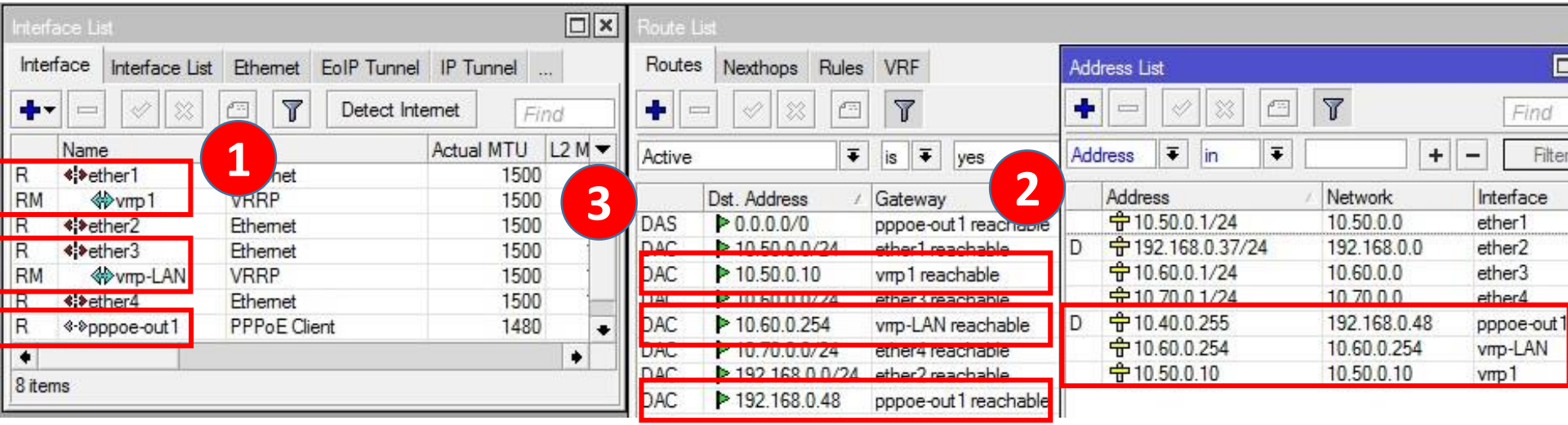
Redundant PPPoE Client



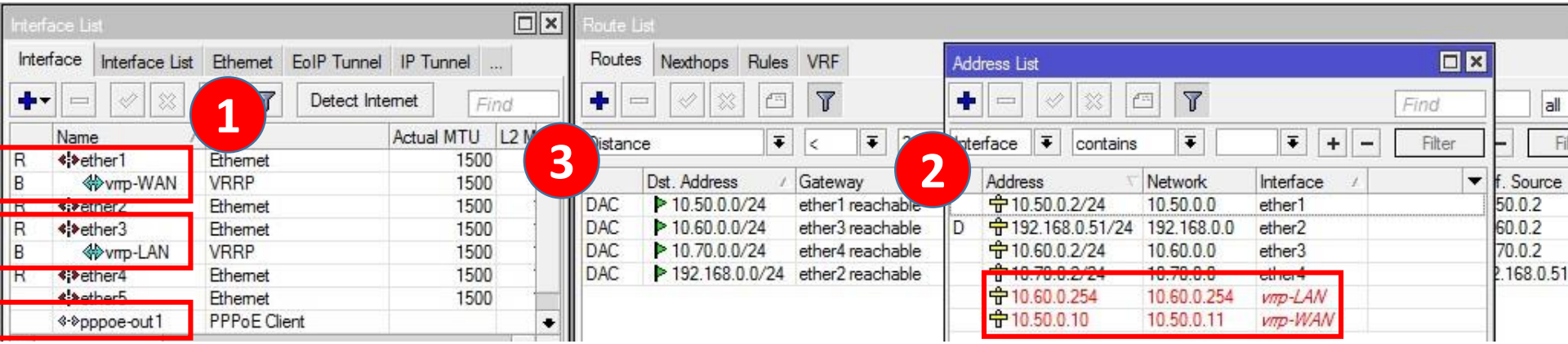
Backup VRRP interface will not forward packets of the PPPoE client

VRRP Overview

MASTER

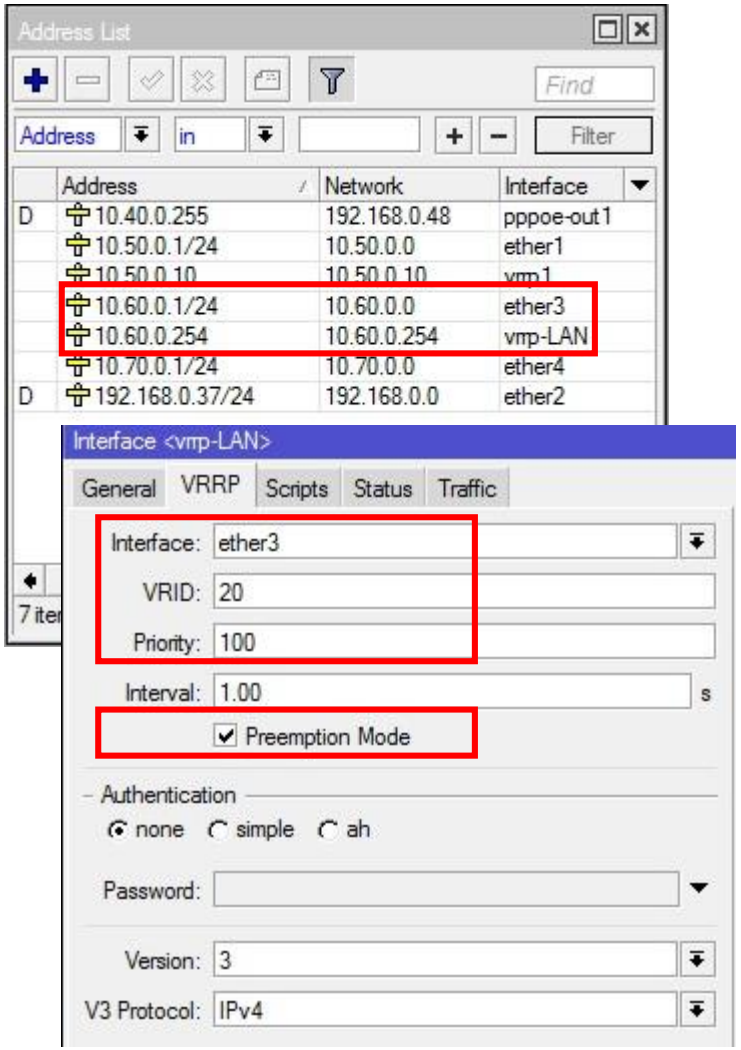


BACKUP

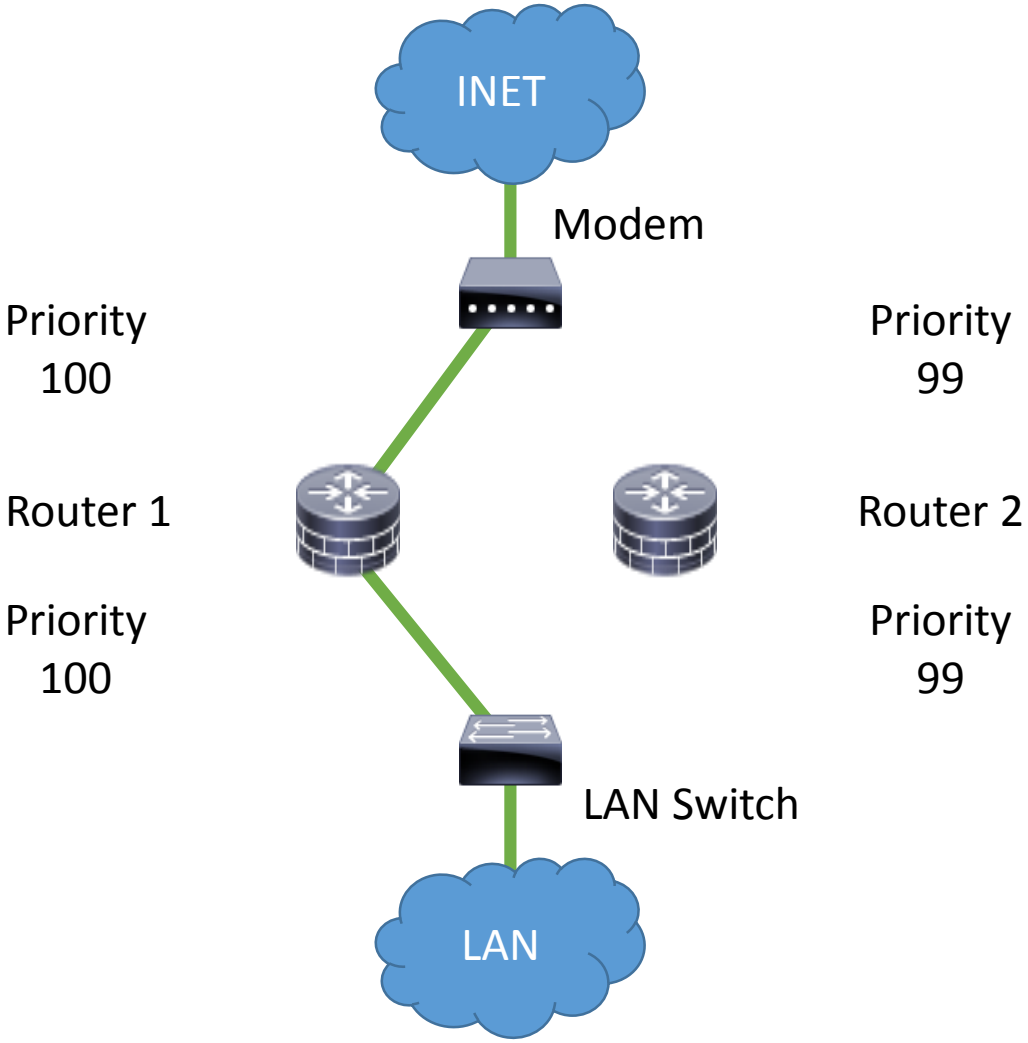


VRRP Configuration

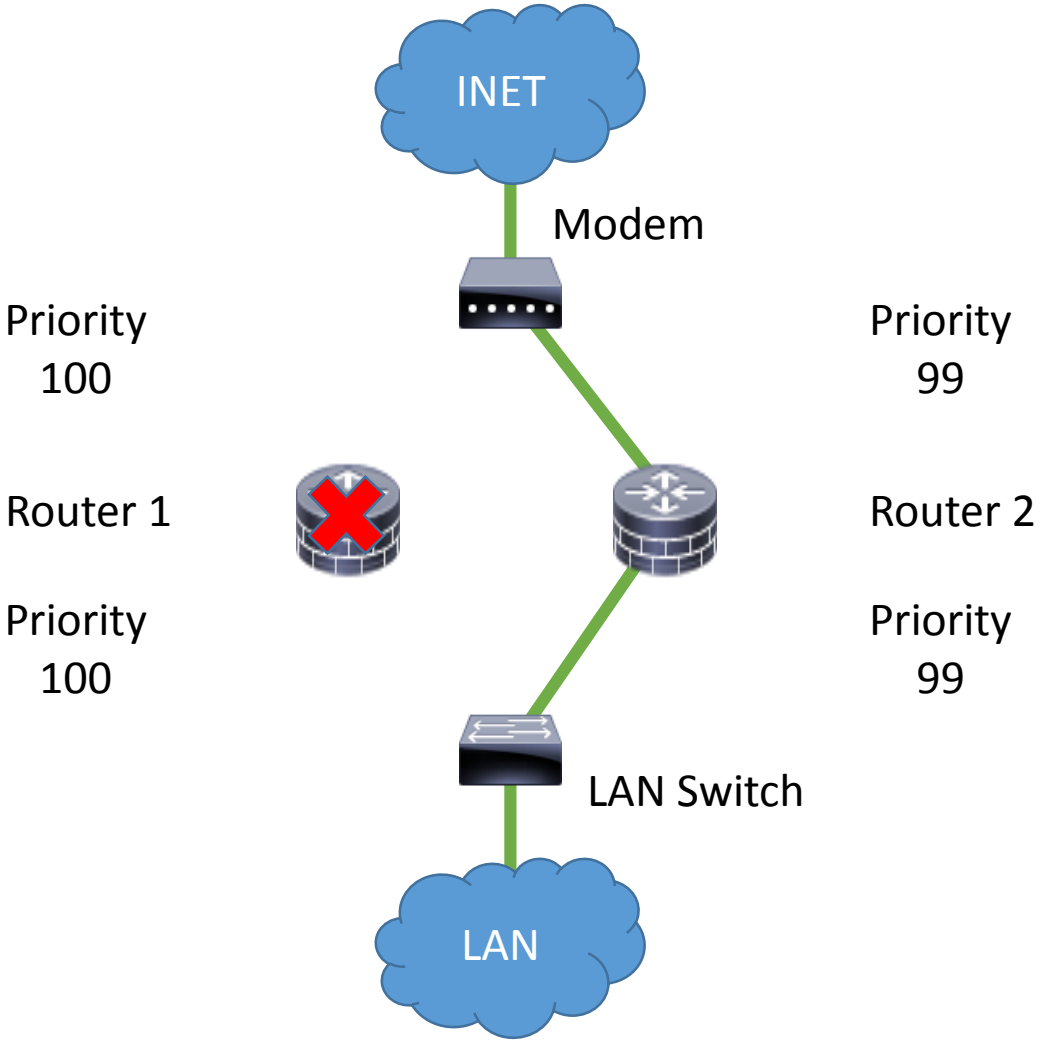
- Physical interface IP
- VRRP interface IP
- Parent interface
- VRID
- Priority
- Preemption Mode



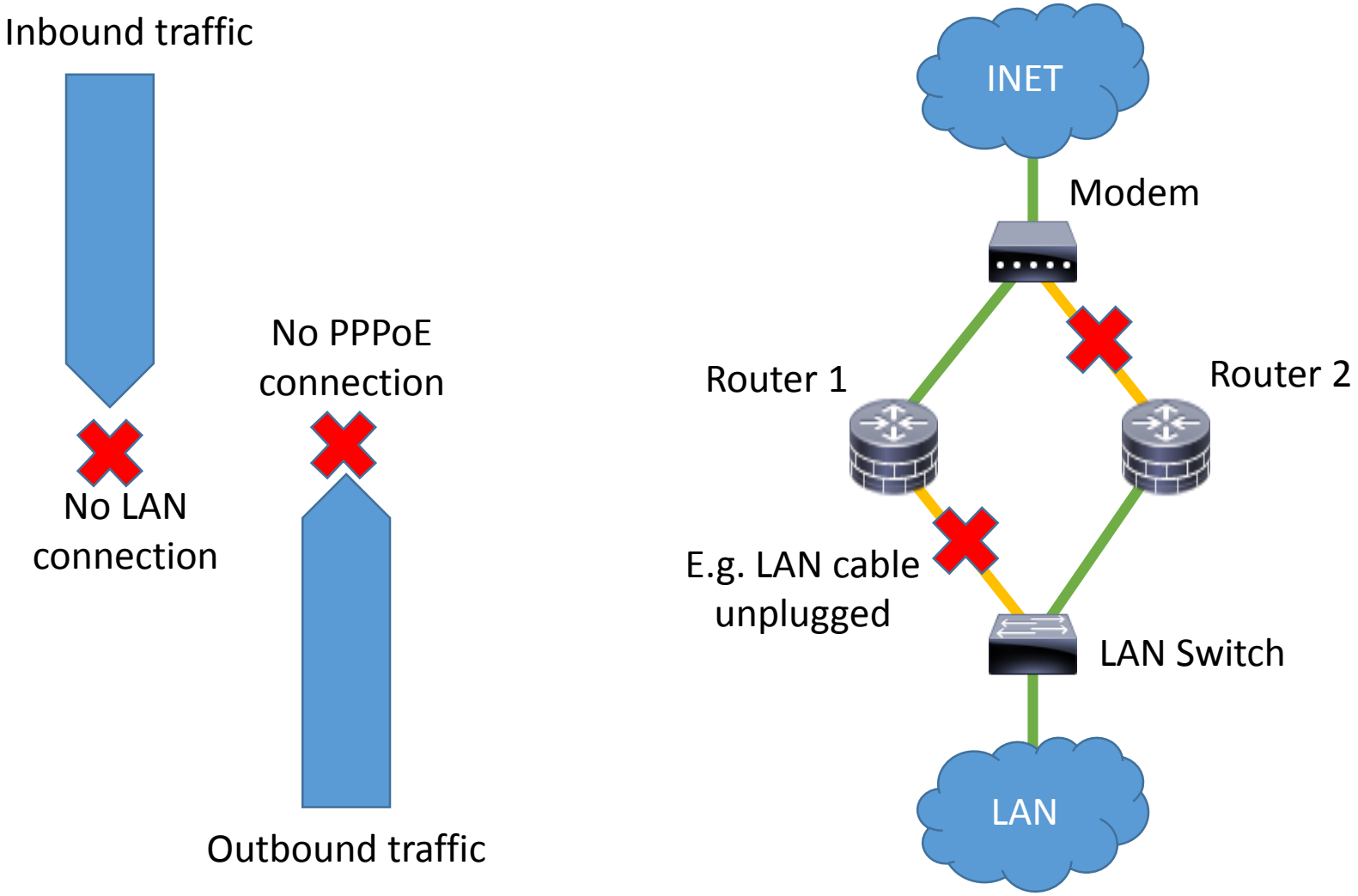
Router 1 VRRP Master



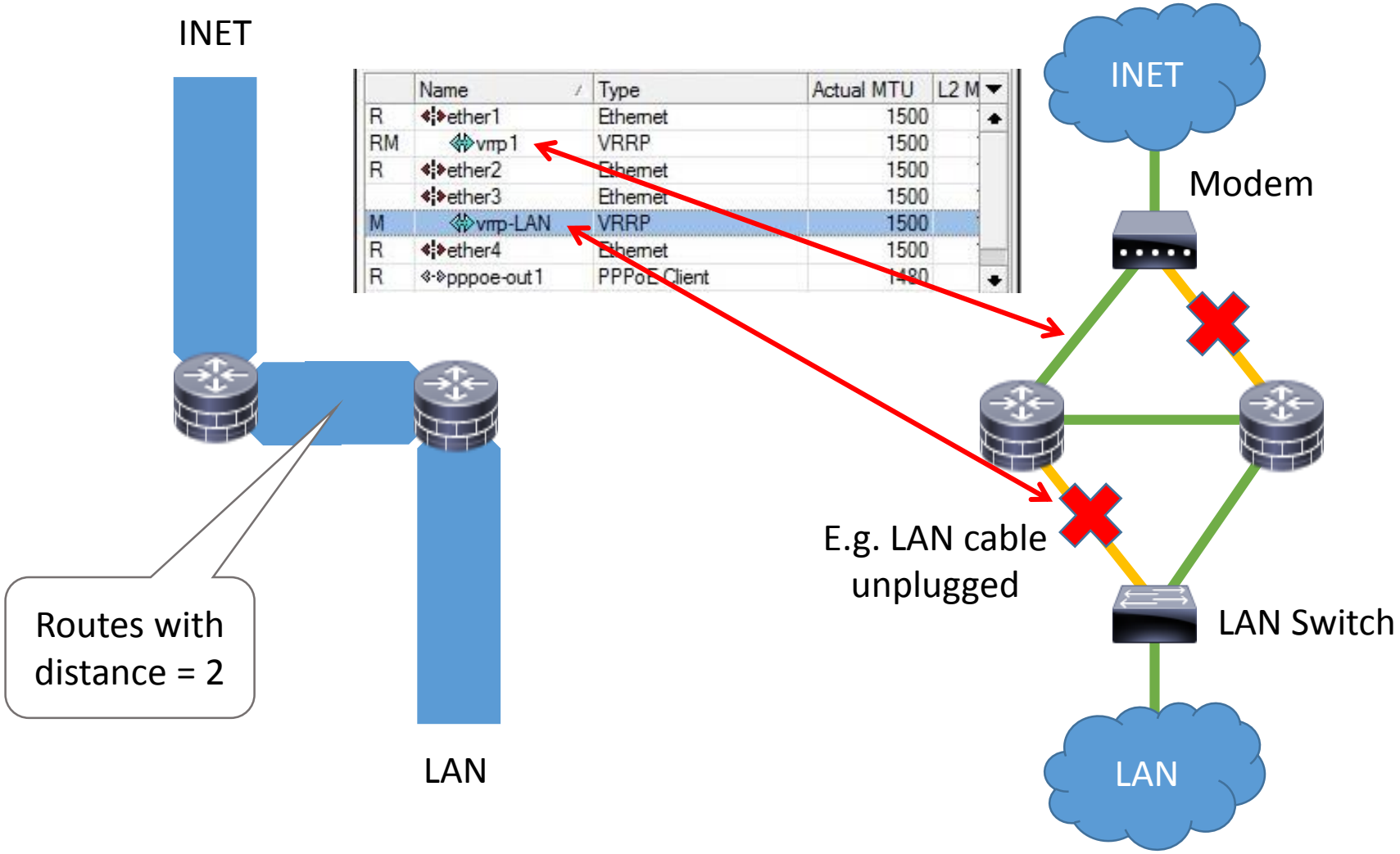
Router 2 VRRP Master



Asymmetric VRRP



Asymmetric VRRP



Routing ether4 Crosslink

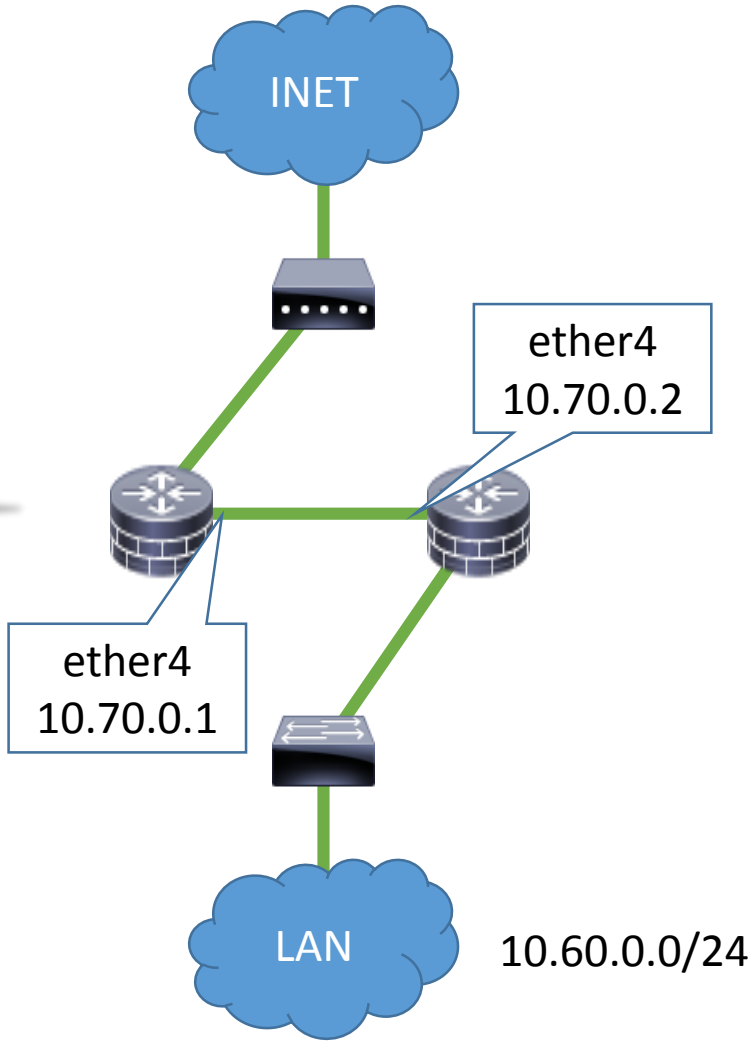
Route List

Routes | Nexthops | Rules | VRF

Find | all

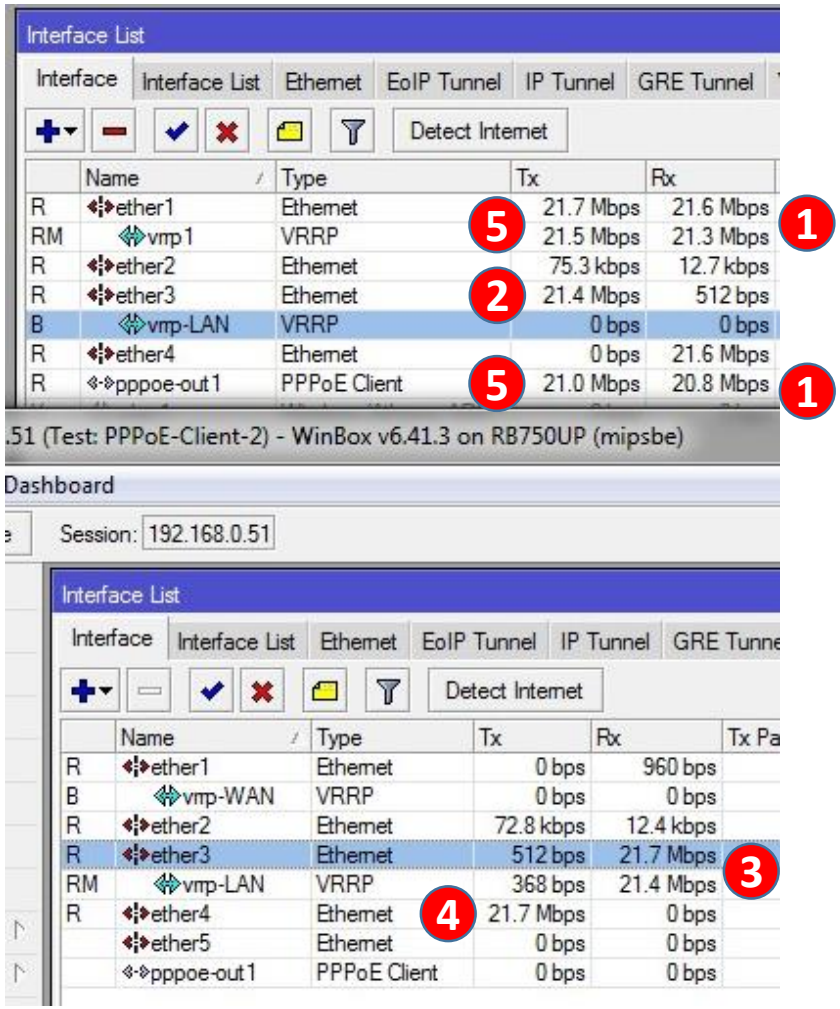
	Dst. Address	Gateway	Distance
S	0.0.0.0/0	10.70.0.2 reachable ether4	2
DAS	0.0.0.0/0	pppoe-out1 reachable	1
DAC	10.50.0.0/24	ether1 reachable	0
DAC	10.50.0.10	vrrp1 reachable	0
AS	10.60.0.0/24	10.70.0.2 reachable ether4	2
DC	10.60.0.0/24	ether3 unreachable	255
DC	10.60.0.254	vrrp-LAN unreachable	255
DAC	10.70.0.0/24	ether4 reachable	0
DAC	192.168.0.0/24	ether2 reachable	0
DAC	192.168.0.48	pppoe-out1 reachable	0

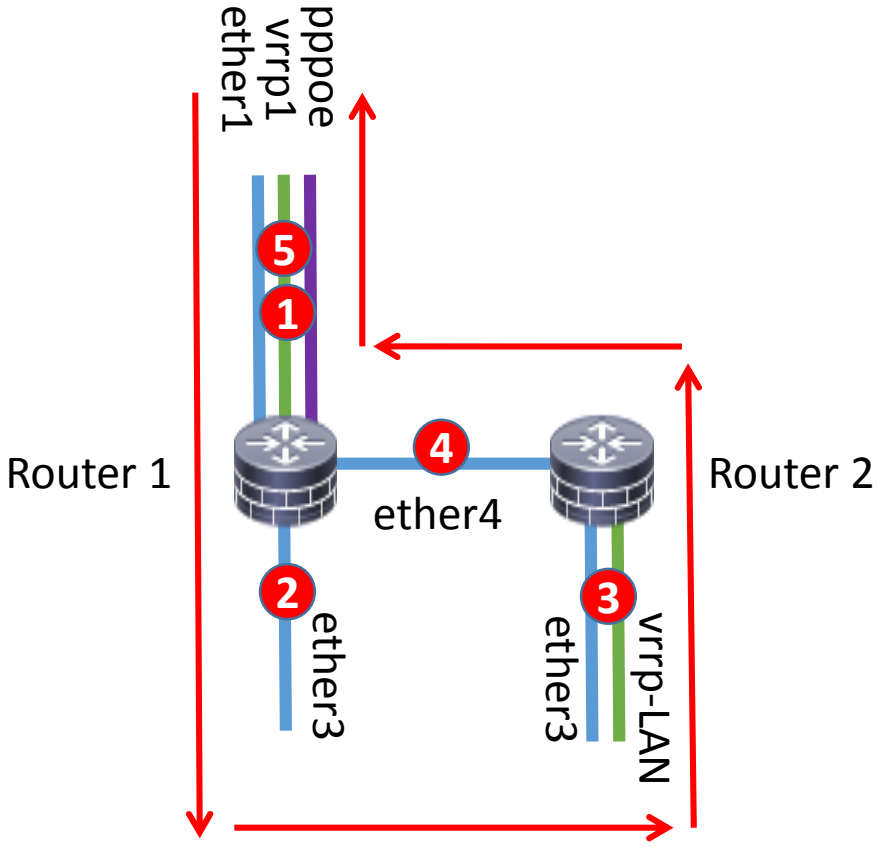
10 items (1 selected)



Cable replugged but no Preemption

20Mbps bidirectional BW test



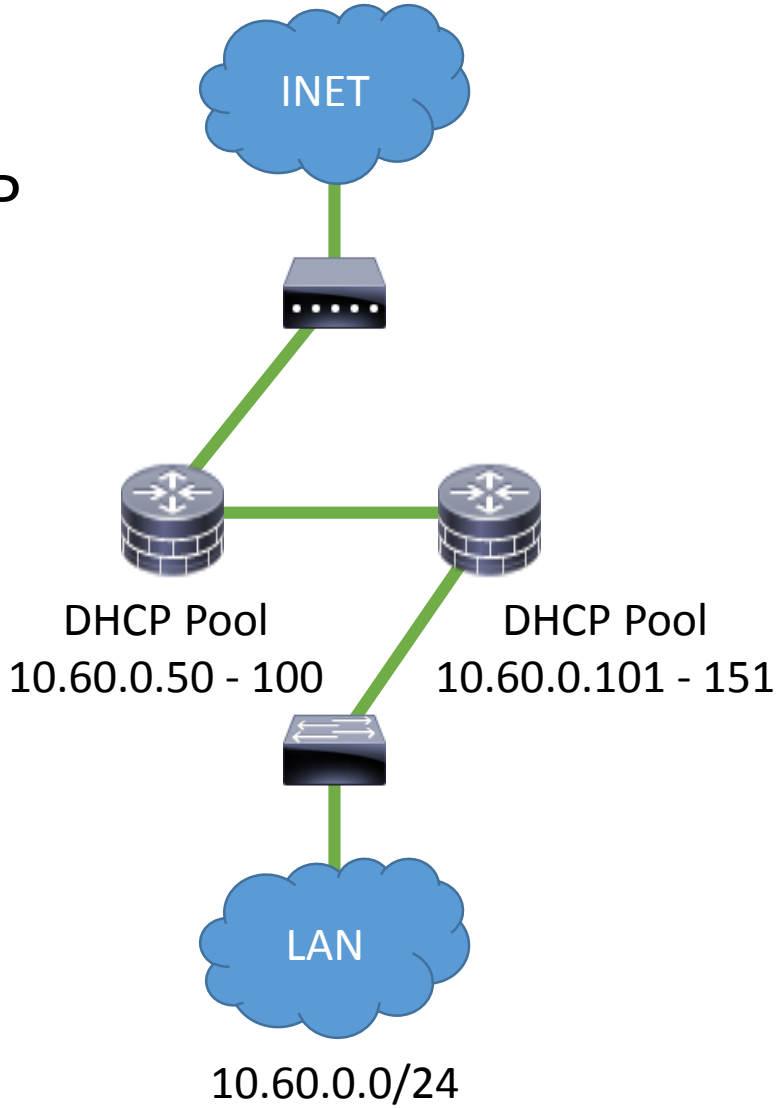


DHCP Server

- DHCP on both routers
- DHCP server changes with VRRP
- DHCP on backup is inactive
- Avoid handing out IPs twice

- Split LAN IP pool
- Optionally save static range

- Clients will survive router change
- Can continue to use old lease



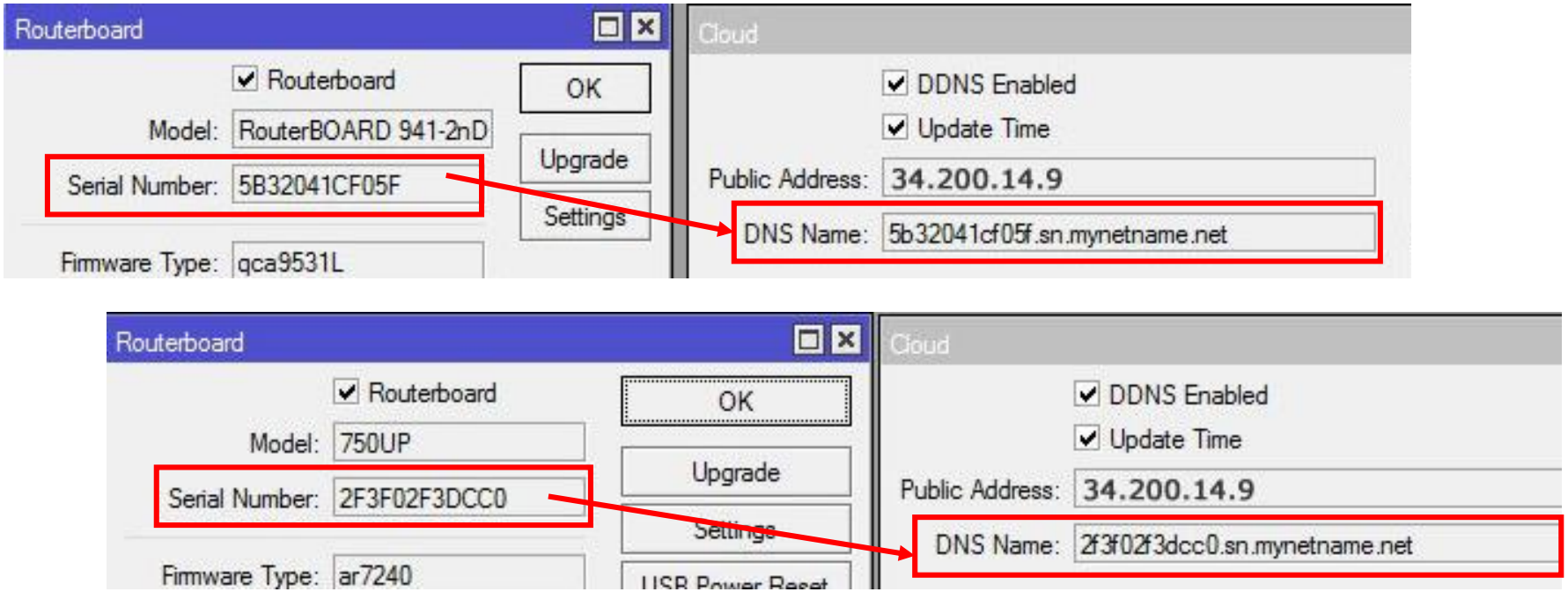
Dynamic Public IP / DynDNS

- VPN clients need public IP of VPN server
- Public IP not static with broadband line

- Use FQDN instead of IP
- Update DNS once IP changes

- RouterOS DynDNS feature
- /ip cloud
- Will not do the job

/ip cloud



- Automatic FQDN from serial number
- No common FQDN for both routers possible

DynDNS

- Many different services available
- ChangeIP (uses /tools dns-update)
- Other approaches use /tools fetch
- See WIKI for scripts

https://wiki.mikrotik.com/wiki/Dynamic_DNS_Update_Script_for_ChangeIP.com

- Different versions for NAT and public IP

  to understand if update necessary
- NAT version writes to disk

- Use encrypted transport

DynDNS

https://wiki.mikrotik.com/wiki/Dynamic_DNS_Update_Script_for_ChangeIP.com

```
:global ddnsuser "YourChangeIPUserID"
:global ddnspass "PASSWORD"
:global ddnshost "MyRouterHostname.example.org"
:global ddnsinterface "ether1"

:global ddnsip [ /ip address get [/ip address find interface=$ddnsinterface] address ]
:global ddnslastip

:if ([:len [/interface find name=$ddnsinterface]] = 0 ) do={ :log info "DDNS: No interface named
$ddnsinterface, please check configuration." }

:if ([ :typeof $ddnslastip ] = "nothing" ) do={ :global ddnslastip 0.0.0.0/0 }

:if ([ :typeof $ddnsip ] = "nothing" ) do={

:log info ("DDNS: No ip address present on " . $ddnsinterface . ", please check.")

} else={

  :if ($ddnsip != $ddnslastip) do={

    :log info "DDNS: Sending UPDATE!"
    :log info [ :put [/tool dns-update name=$ddnshost address=[:pick $ddnsip 0 [:find $ddnsip "/"] ] key-
name=$ddnsuser key=$ddnspass ] ]
    :global ddnslastip $ddnsip

  } else={

    :log info "DDNS: No changes necessary."
  }
}
```

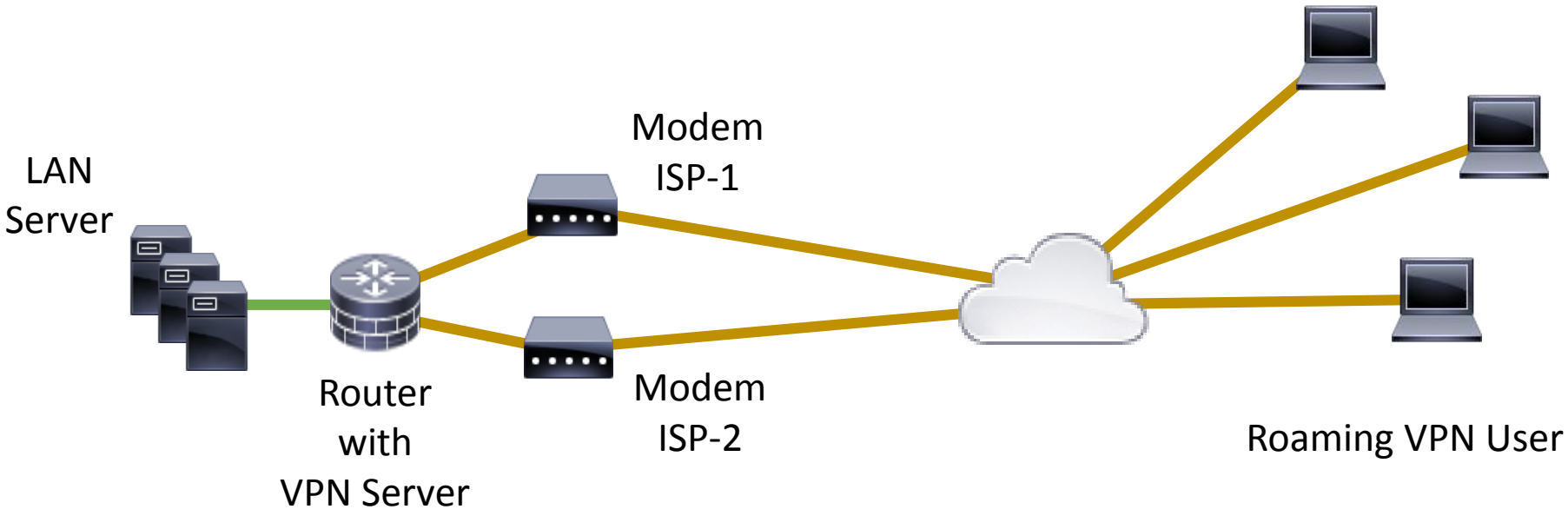
Hardware Redundancy Running

- Done
  - Switching between the PPPoE clients
  - Selecting Default Gateway for the LAN
  - Two DHCP servers
  - Dynamic public IP address for VPN server
  - LAN cable / port failure
- Optionally to do:
  - VPN user accounts
  - Static DHCP leases, static DNS entries
  - Export / import between routers can be scripted

Enterprise VPN

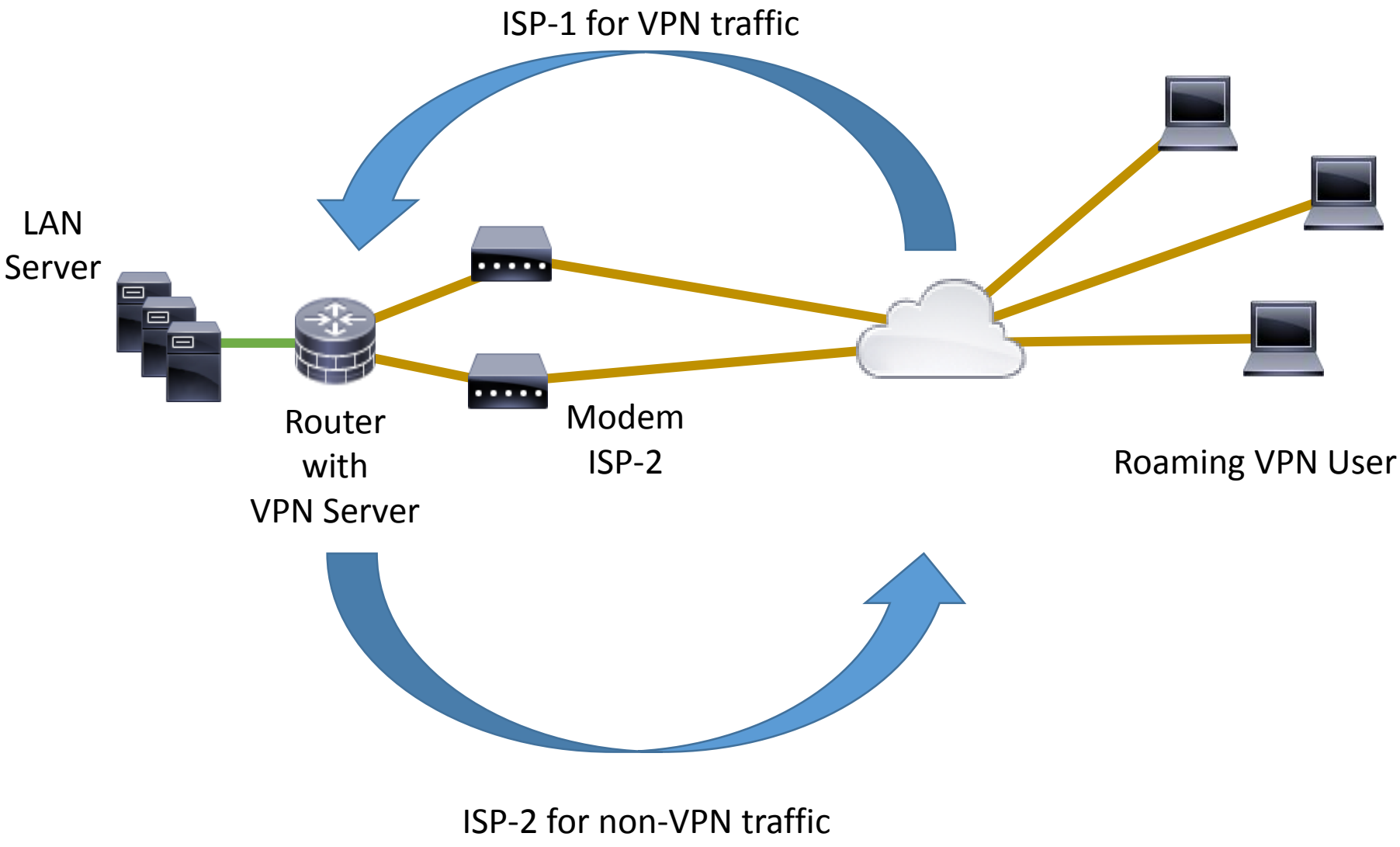
Redundant Access Lines

Overview



- two DSL lines (PPPoE)
- Dynamic public IPs

Overview


ISP-1 for VPN traffic
LAN
Server
Router
with
VPN Server
Modem
ISP-2
Roaming VPN User
ISP-2 for non-VPN traffic

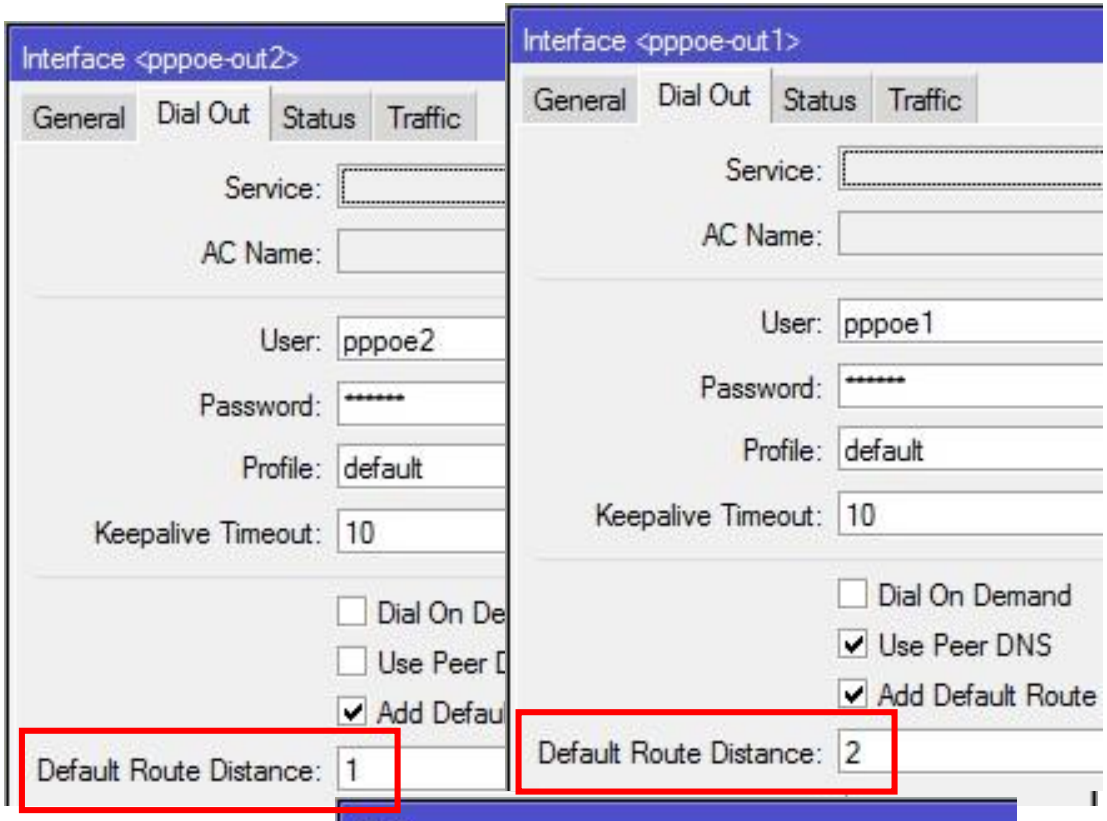
Goals

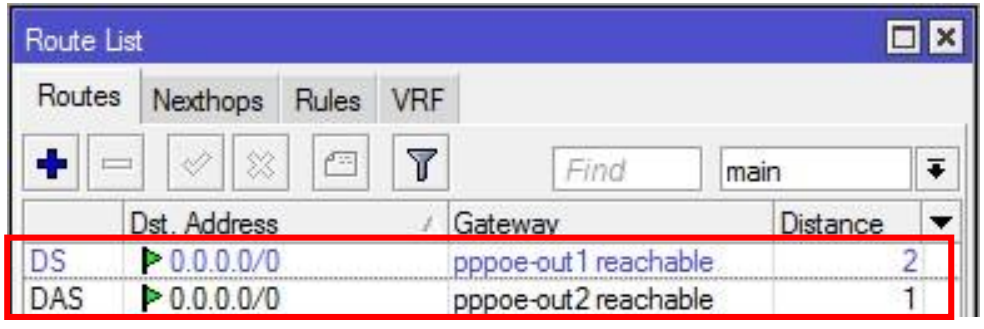
- Redundant internet access
- Advanced line checks
- Inbound VPN with dynamic IPs
- “Application” based load-balancing

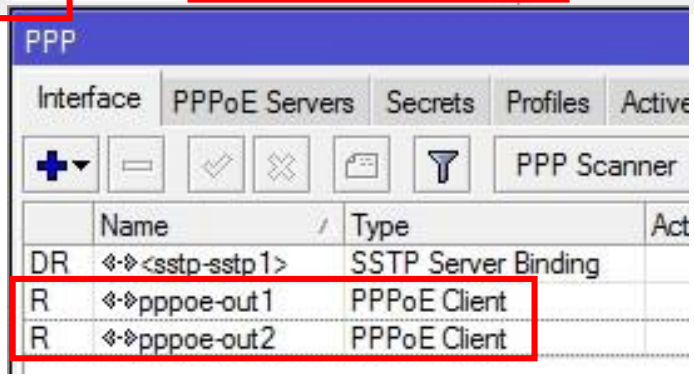
- During normal operation:
  - ISP 1 for VPNs
  - ISP 2 for local (non VPN) traffic

Route Distance

- Two pppoe-clients
- Different default route distance
- Traffic will use ISP2

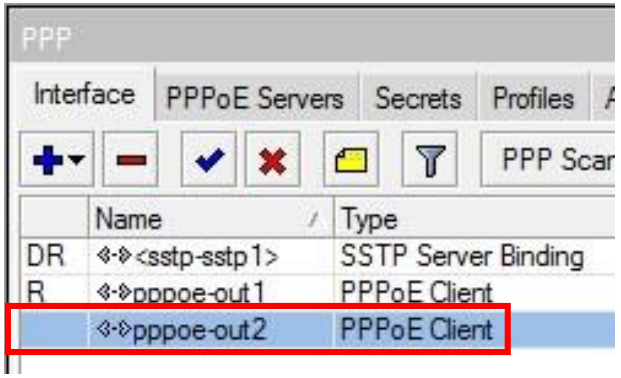


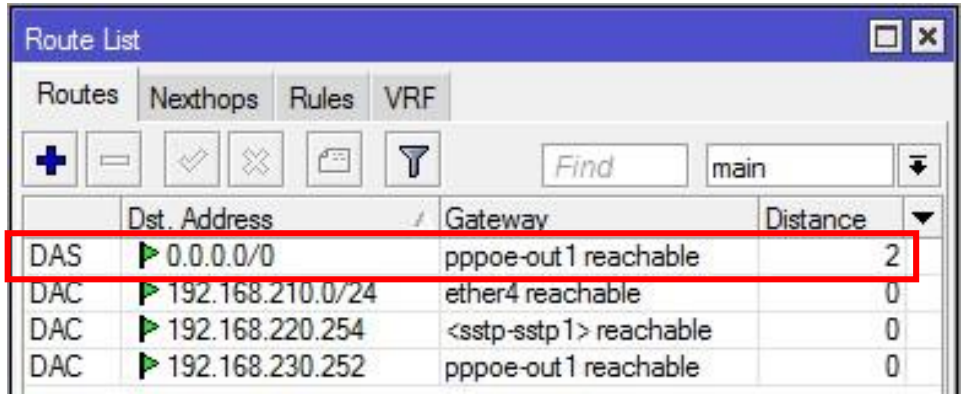




Failover ISP2 -> ISP1

- ISP2 PPPoE connection fails
- ISP2 Default Route disappear
- ISP1 Default Route is active





ISP Check

- Problem in ISP2 network not detected
- Router wouldn’t swap to ISP1
- Router offline, although connectivity available
- Common CheckGateway approach not useful

- Solution: Netwatch
- Any host can be checked

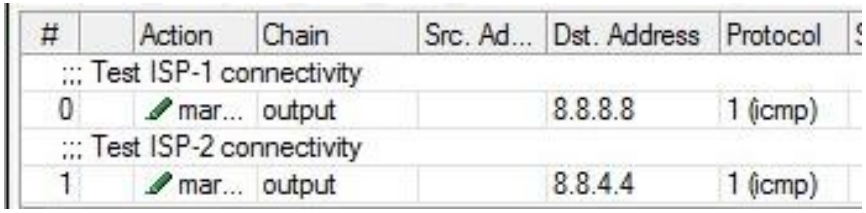
- Force check to use dedicated line
- Real availability of both ISP can be checked

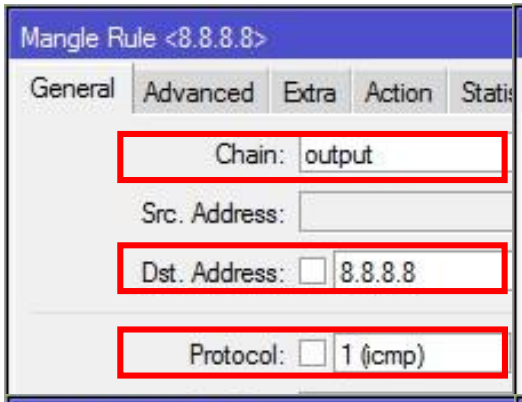
Netwatch

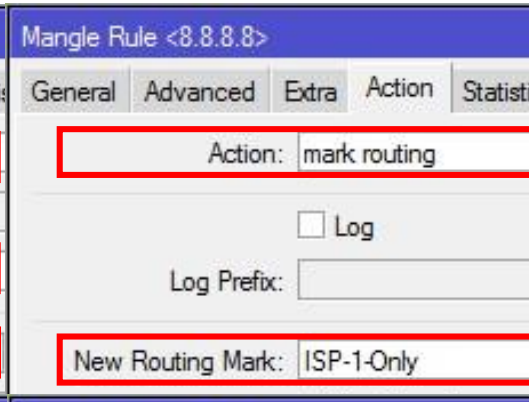
- Example targets: 8.8.8.8 for ISP1 8.8.4.4 for ISP2
- Forcing routing by static route?
- /ip route add distance=1 dst-address=8.8.8.8/32 gateway=pppoe-out1
- Target fully unusable if line fails -> bad

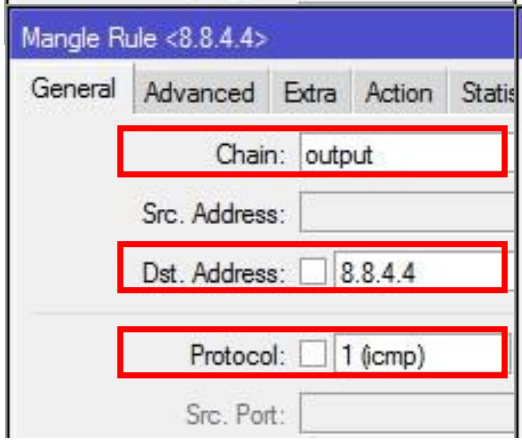
Netwatch / Mangle Rules

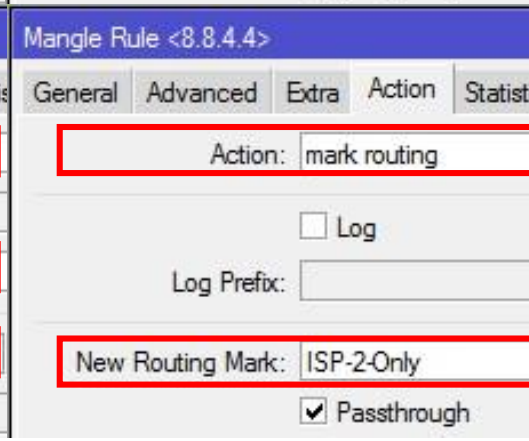
- Best approach: Mangle + 2 extra routing tables
- Limited to ICMP in output chain
- Rest of network not affected
- Local DNS not affected





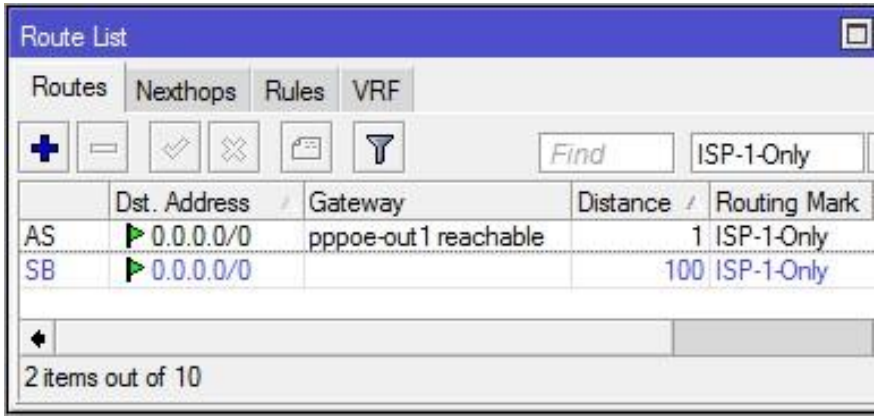


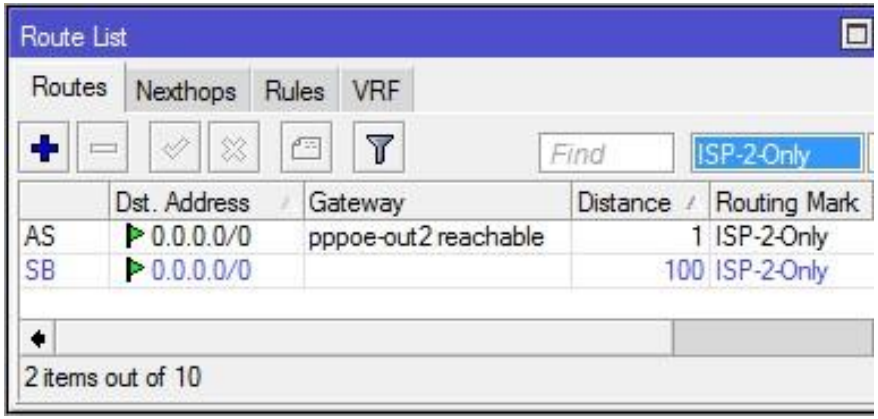




Netwatch / Routing Tables

- Alternative default routes
- Main table used if additional default route inactive
- Additional routing tables need blackhole routes with higher distance





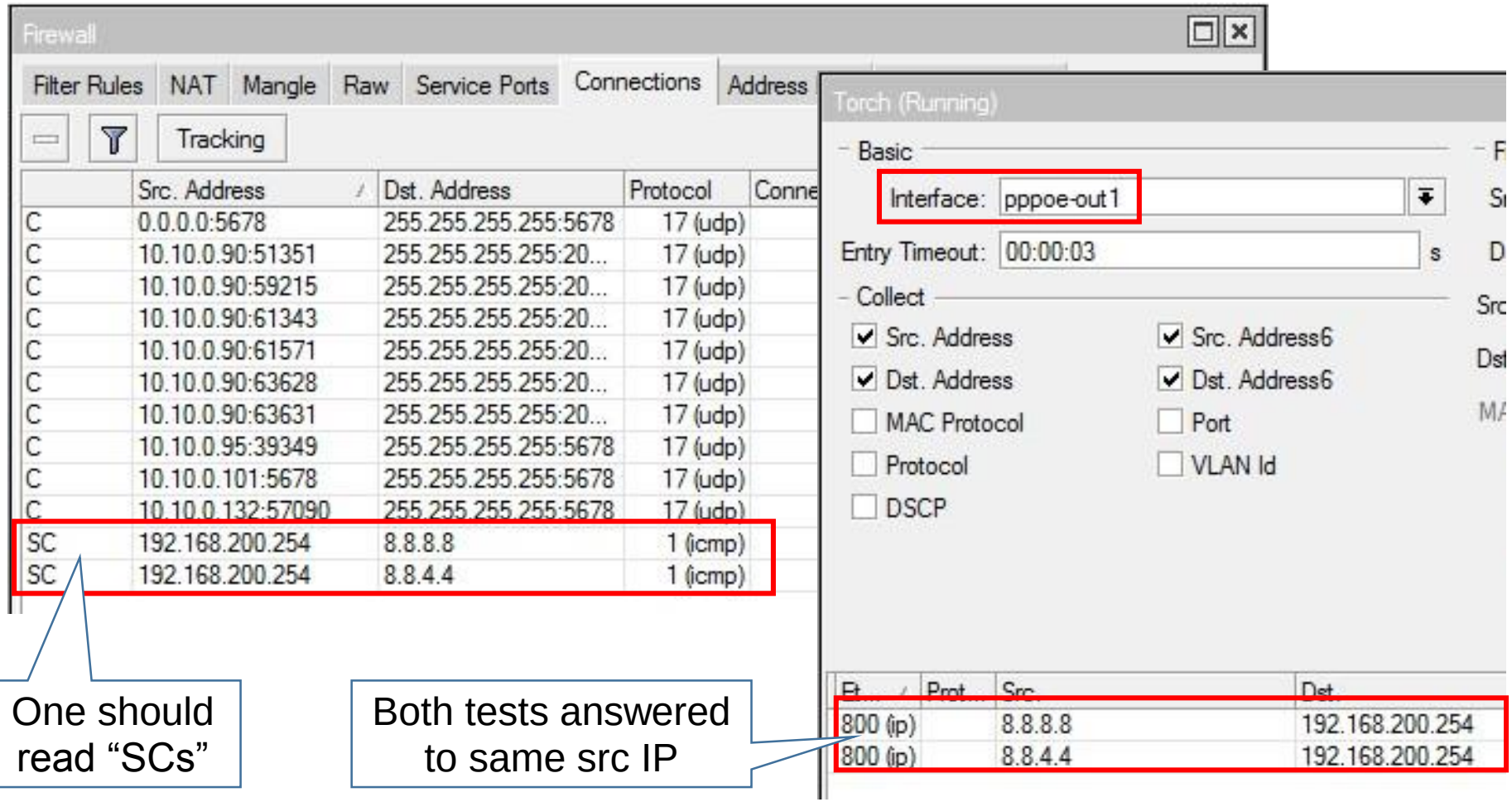
Netwatch / Malformed Packets

- Test pings to 8.8.8.8 / 8.8.4.4
- Use correct ISP

- Problem when switching ISP
- -> Switching active main default route
- -> Using different src IP
- -> SRC NAT necessary for other connection

- RouterOS doesn’t always do so correctly

Netwatch / Malformed Packets

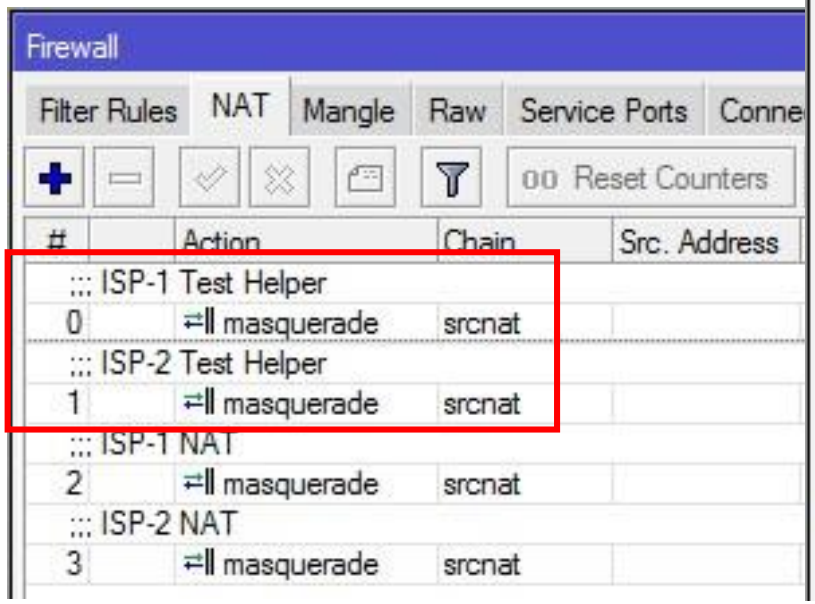


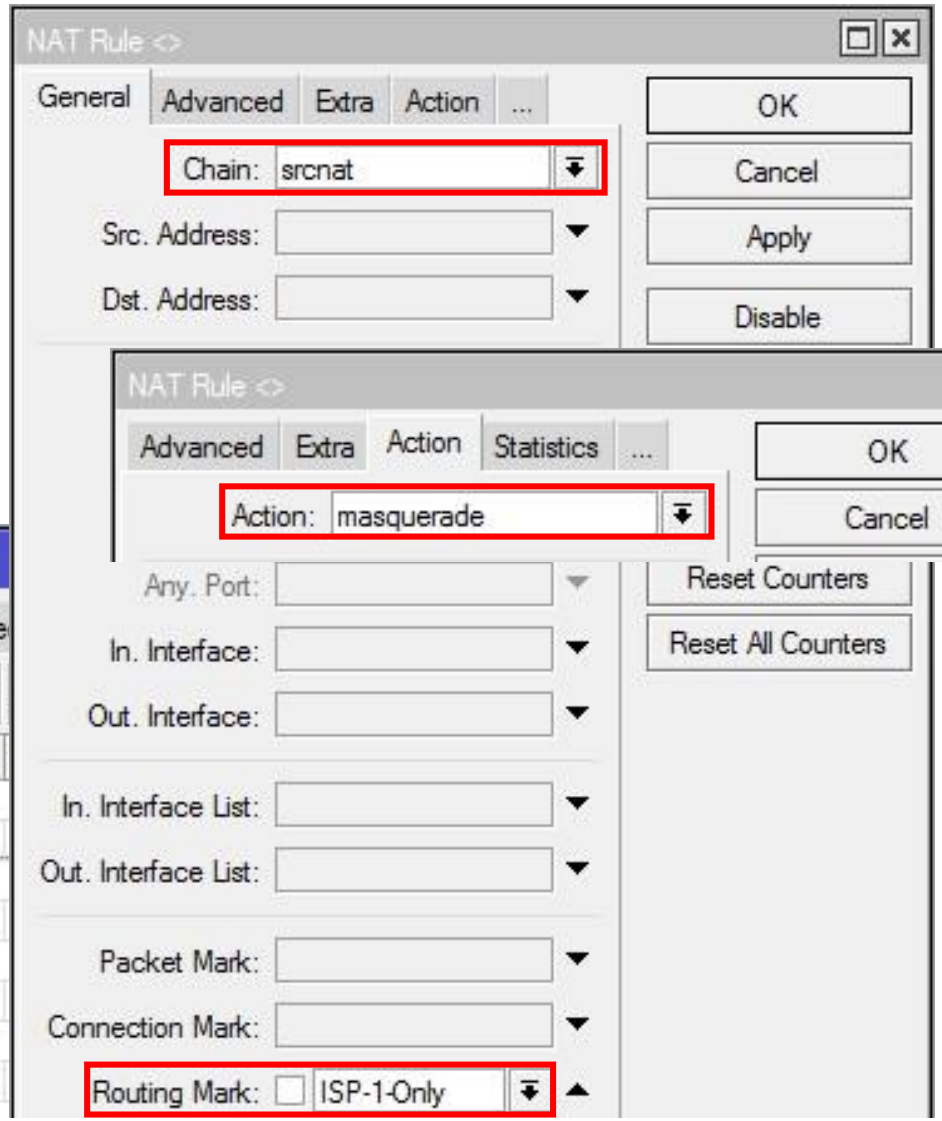
One should read “SCs”

Both tests answered to same src IP

Netwatch / Malformed Packets

- Solution: Two additional NAT rules
- Matching according to routing markers





Netwatch / Scripts

- Create Netwatch test for ISP-2
- Set Up/Down Scripts

Down:

:log info "PPPoE-2 not working"

/interface pppoe-client set pppoe-out2 default-route-distance=3

Up:

:log info "PPPoE-2 working again"

/interface pppoe-client set pppoe-out2 default-route-distance=1

Netwatch / Scripts

Problem:

- Connection tracking gets stuck if timeout not reached
- Delay and connection tracking reset in script

Add to up and down script:

:delay 2

/ip firewall connection remove [find]

Inbound SSTP ISP selection

- ChangeIP script controls public IP
- FQDN shall point to preferred ISP

- Modify ChangeIP script
- Update IP independent from outgoing interface
- Use interface from global variable instead

:if ([:typeof $ddnsinterface] = "nothing") do={ :global ddnsinterface "pppoe-out1" }

ChangeIP Script

```
:global ddnsuser „foo@fmsweb.de"
:global ddnspass „12345678"
:global ddnshost „mum2018.ns01.info"
:global ddnsinterface

:if ([ :typeof $ddnsinterface ] = "nothing" ) do={ :global ddnsinterface "pppoe-out1" }
:global ddnsip [ /ip address get [/ip address find interface=$ddnsinterface] address ]
:global ddnslastip
:if ([:len [/interface find name=$ddnsinterface]] = 0 ) do={ :log info "DDNS: No interface named $ddnsinterface, please check configuration." }
:if ([ :typeof $ddnslastip ] = "nothing" ) do={ :global ddnslastip 0.0.0.0/0 }

:if ([ :typeof $ddnsip ] = "nothing" ) do={
:log info ("DDNS: No ip address present on " . $ddnsinterface . ", please check.")
} else={
  :if ($ddnsip != $ddnslastip) do={
    :log info ("DDNS: Sending UPDATE for interface " . $ddnsinterface . ".")
    :log info [ :put [/tool dns-update name=$ddnshost address=[:pick $ddnsip 0 [:find $ddnsip "/"] ] key-name=$ddnsuser key=$ddnspass ] ]
    :global ddnslastip $ddnsip
  } else={
    :log info ("DDNS: No changes necessary. (Interface: " . $ddnsinterface . ")")
  }
}
```

Inbound SSTP ISP selection

- Create Netwatch for ISP-1
- Set variable from up/down scripts

Up:

```
:log info "PPPoE-1 working again"
:global ddnsinterface "pppoe-out1"
/system script run ChangeIP
```

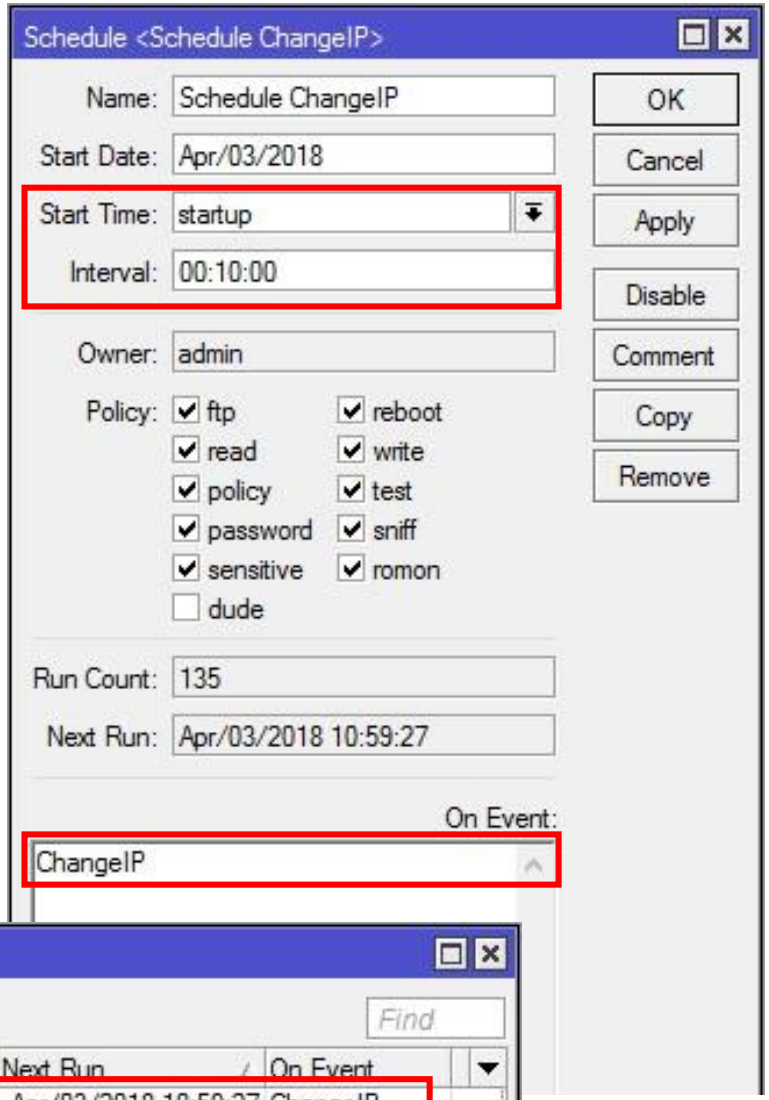
Down:

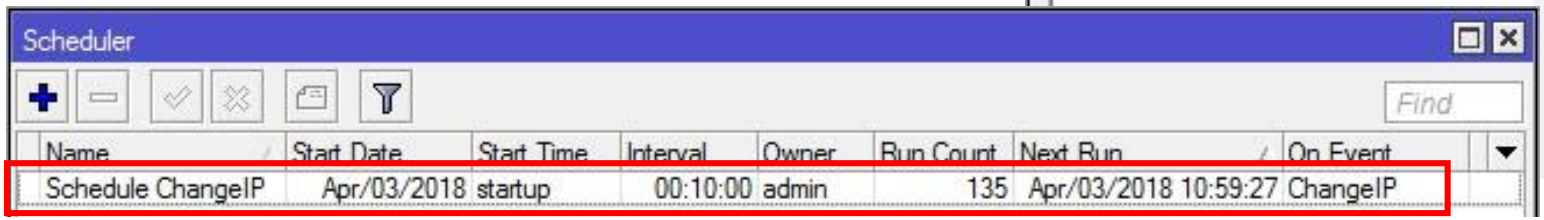
```
:log info "PPPoE-1 not working"
:global ddnsinterface "pppoe-out2"
/system script run ChangeIP
```

Inbound SSTP ISP selection

- Inbound SSTP will use ISP-1 if online
- Will fallback to ISP-2

- Add Scheduler to cover changes of dynamic IP
- Run at startup

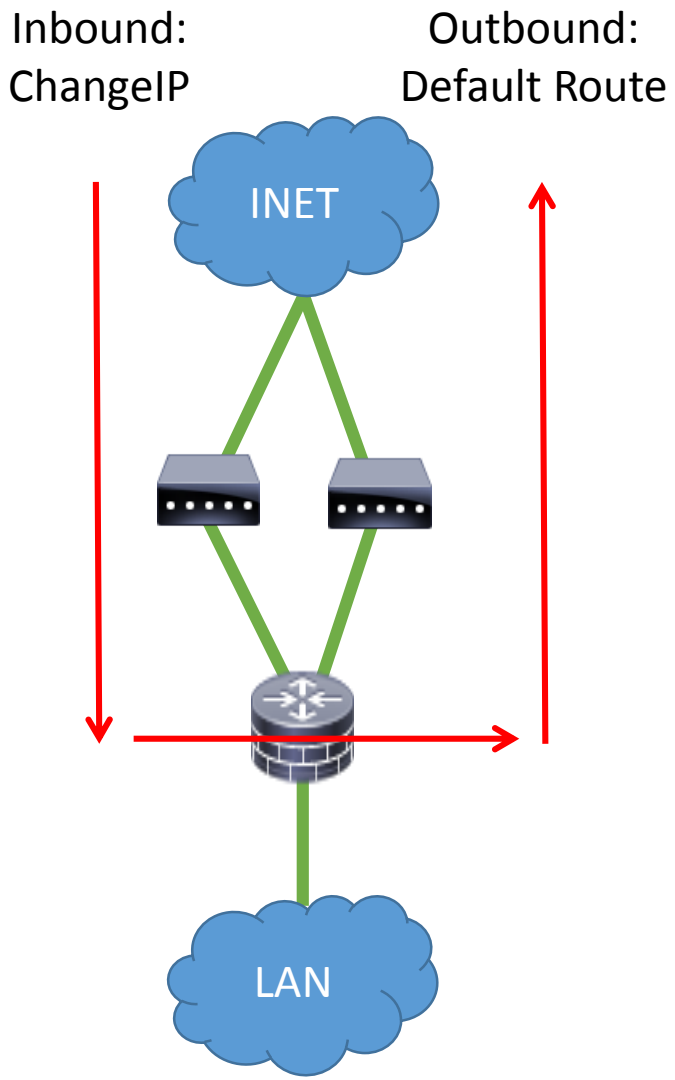




Outbound SSTP Packets

While both ISP are operational:

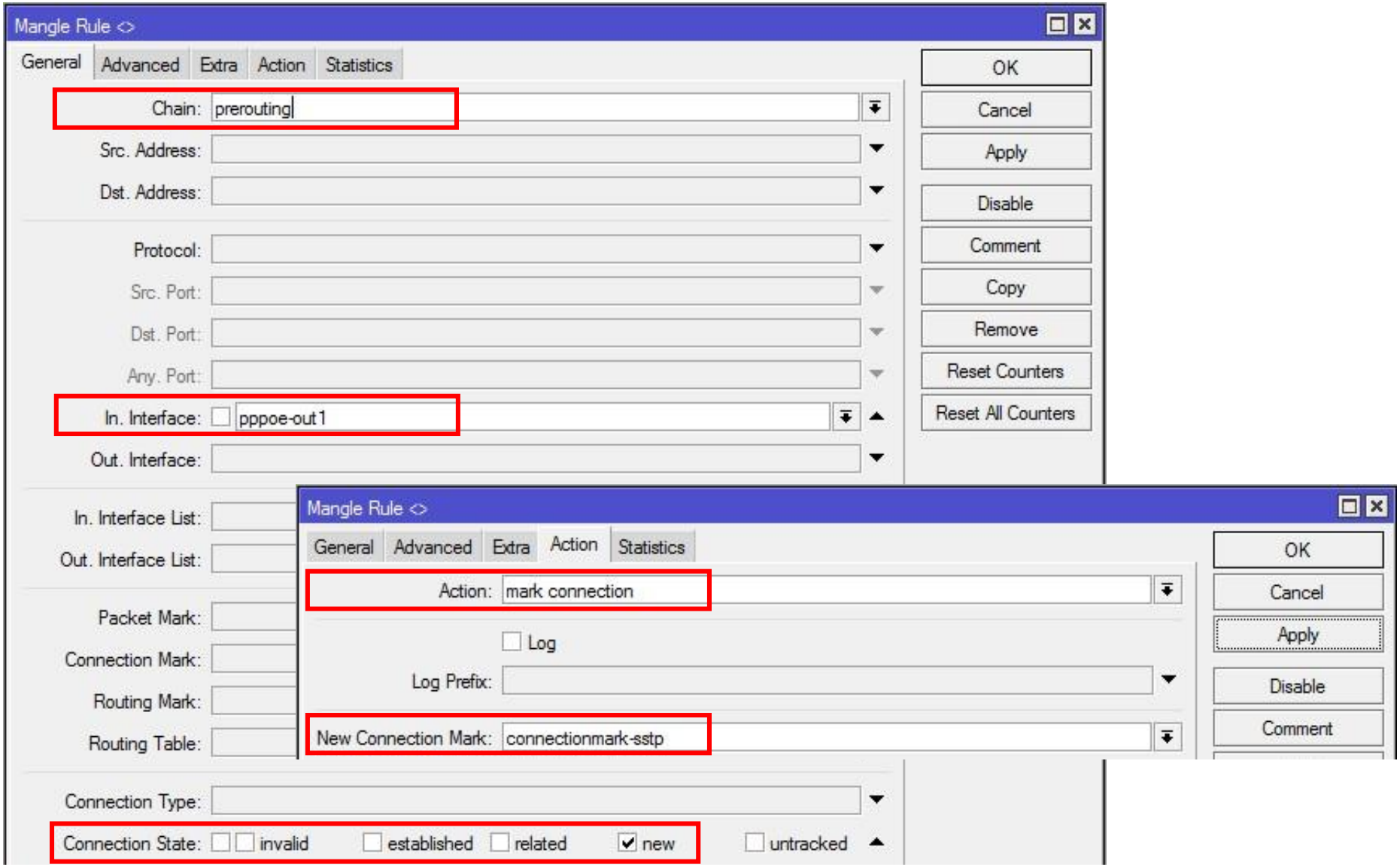
- Inbound SSTP packets on ISP-1
- Outbound on ISP-2 (Default route)



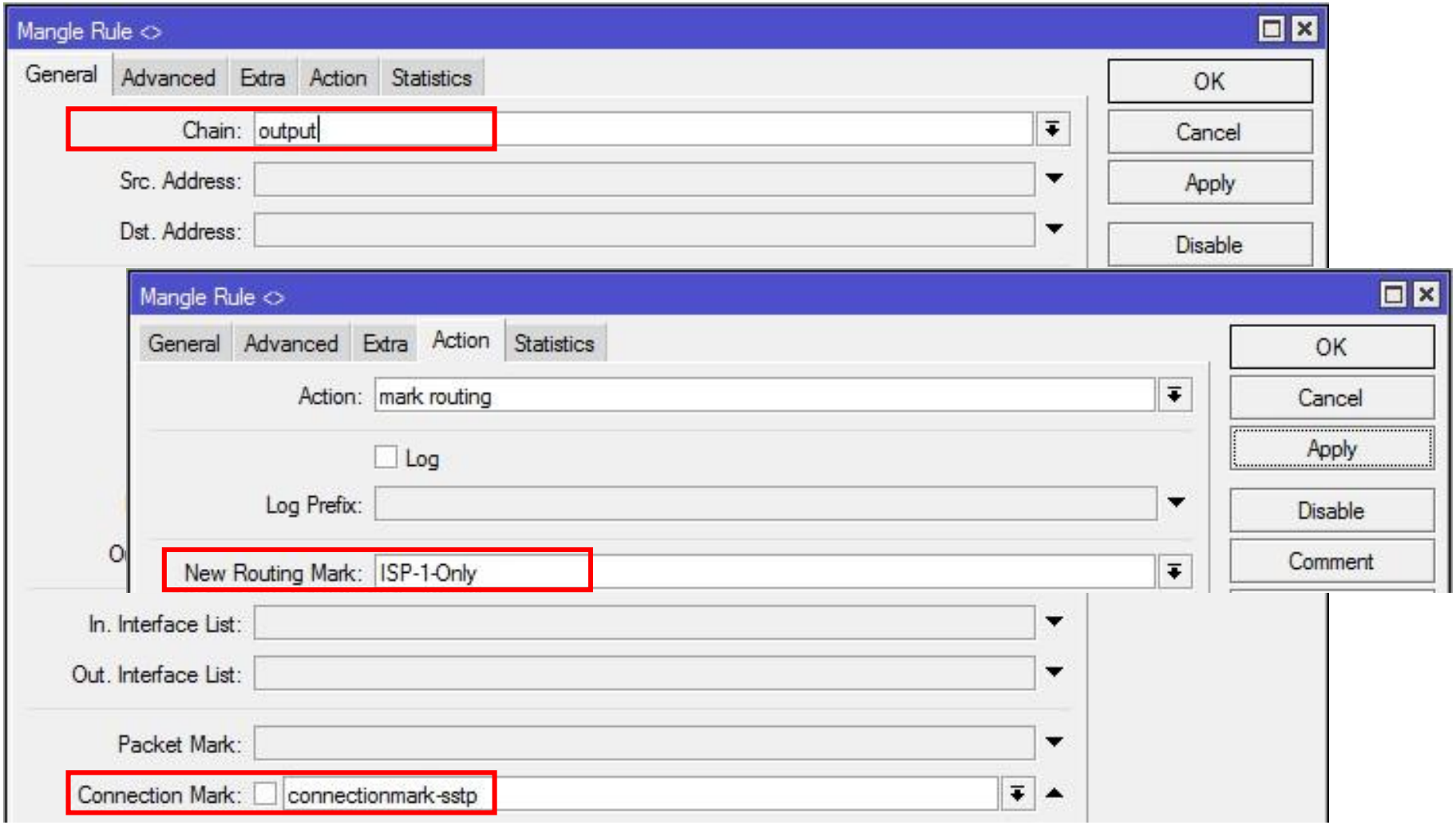
Outbound SSTP Packets

- Use two mangle rules to send outbound packets on inbound interface:
- Set connection mark for new connections
- Set routing mark for above connection mark

Mark new SSTP Connections



Routing Mark for SSTP Connections



Make connections use “ISP-1 Only” routing table

Access Line Redundancy Running

- Done
  - Select preferred line for non ISP traffic
  - Implemented advanced line checks
  - Sorted out connection list and NAT issues
  - Dynamic public IP address for VPN server
  - Made SSTP stick to one interface
  - Redundancy for failing lines
- Optionally to do:
  - Combine both setups
  - Achieve hardware and access line redundancy

ISP Networks

Broadband Remote Access Server

Overview

- PPPoE commonly used
- PPPoE server aka BRAS
- Needs layer 2 network

- Many users / tunnels
- Requires high system performance
- Large and frequently changed user database

Challenges

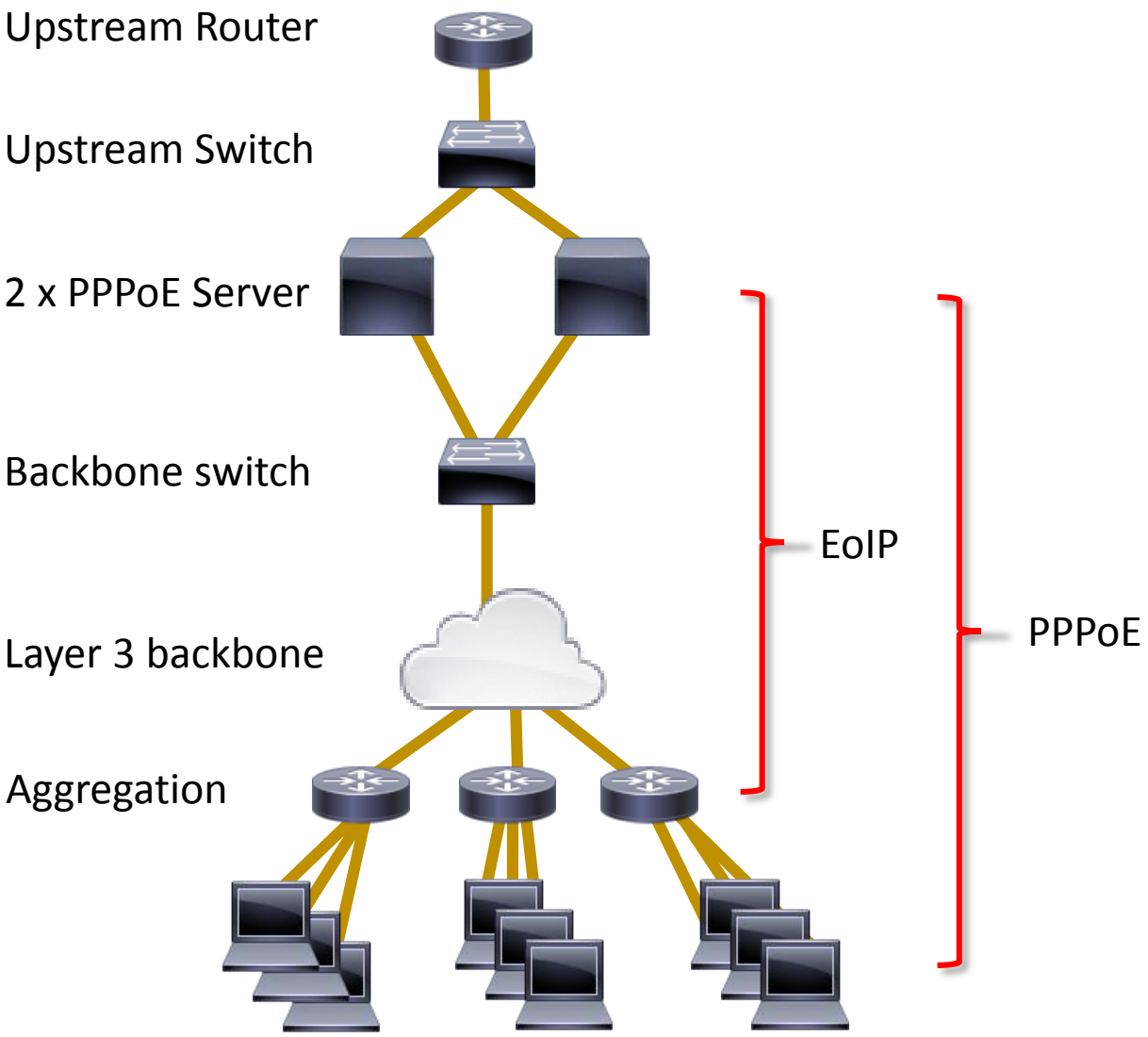
- BRAS redundancy (critical SPoF)
- BRAS loadbalancing (high system performance)
- High available solution for user database

- Virtual layer 2 tunnels
- Redundancy of transport tunnel concentrator

PPPoE Access Concentrator

EoIP Approach

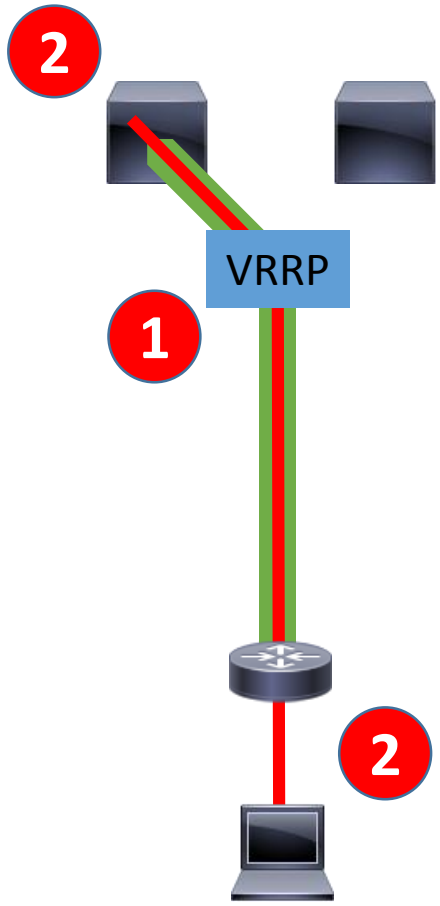
Overview


Upstream Router
Upstream Switch
2 x PPPoE Server
Backbone switch
Layer 3 backbone
Aggregation
EoIP
PPPoE

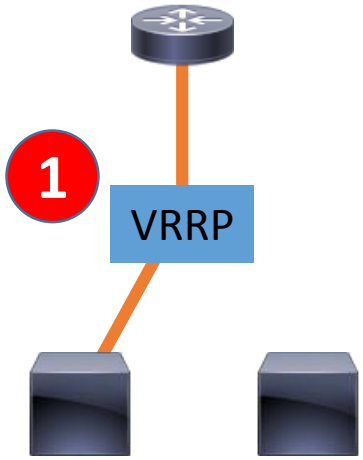
Failover (Backbone)

1. EoIP Tunnel endpoint = VRRP IP address

2. Multiple PPPoE tunnels through each EoIP tunnel



Failover (Upstream)



1 Upstream ISP will route networks to external VRRP IP

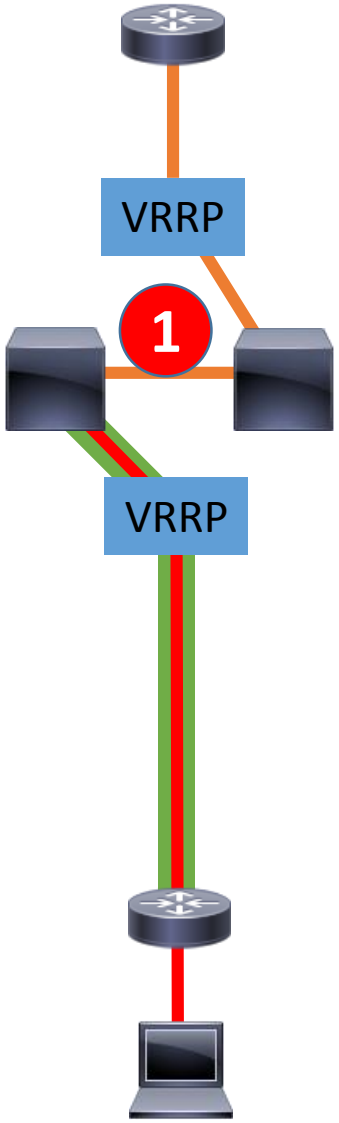
Asymmetric VRRP / Radius

BRAS:

- failover
- No loadbalancing

RADIUS

- E.g. Usermanager
- Script based import / export



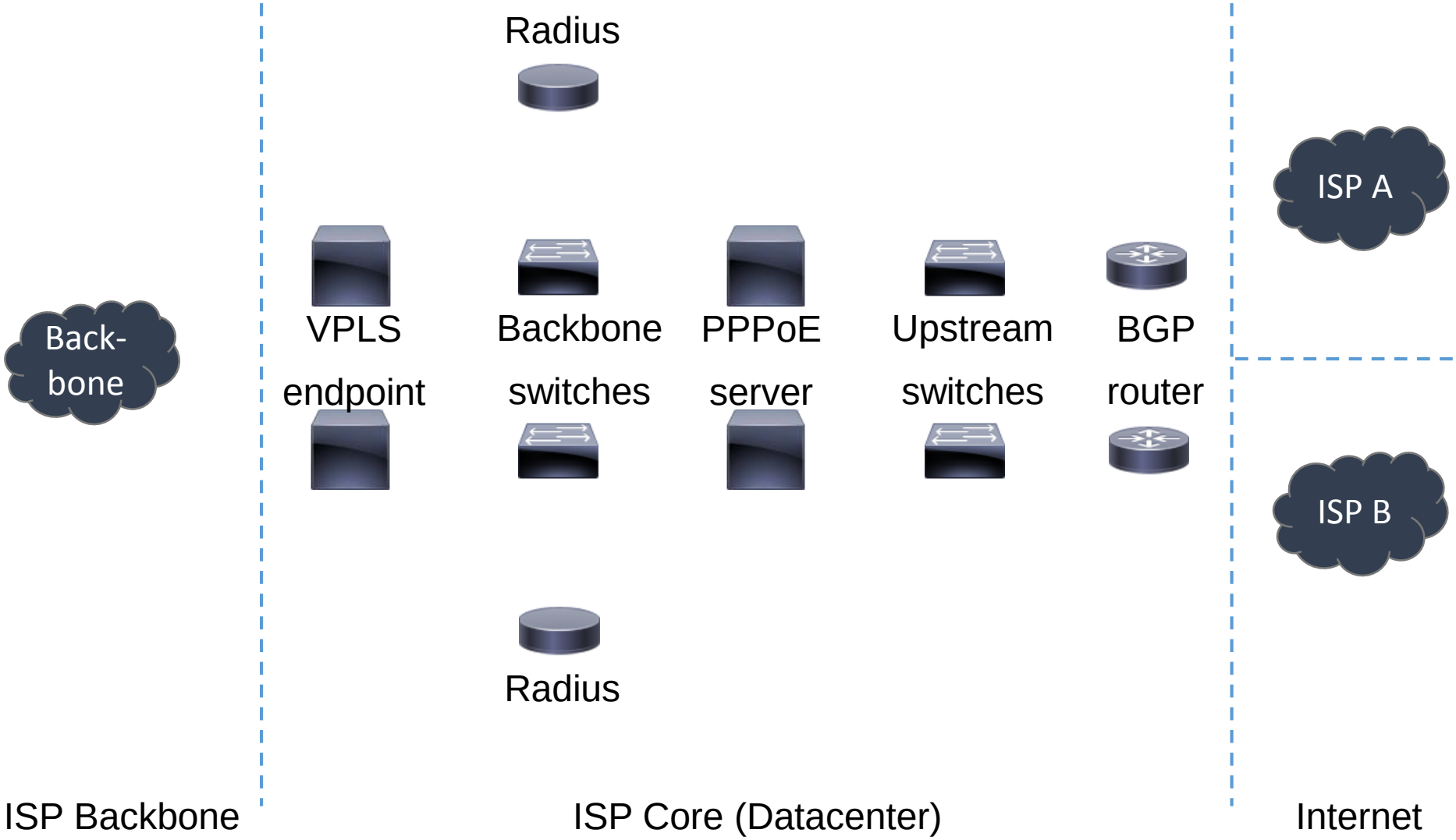
1 Crosslink with static routes *

* See first VPN setup

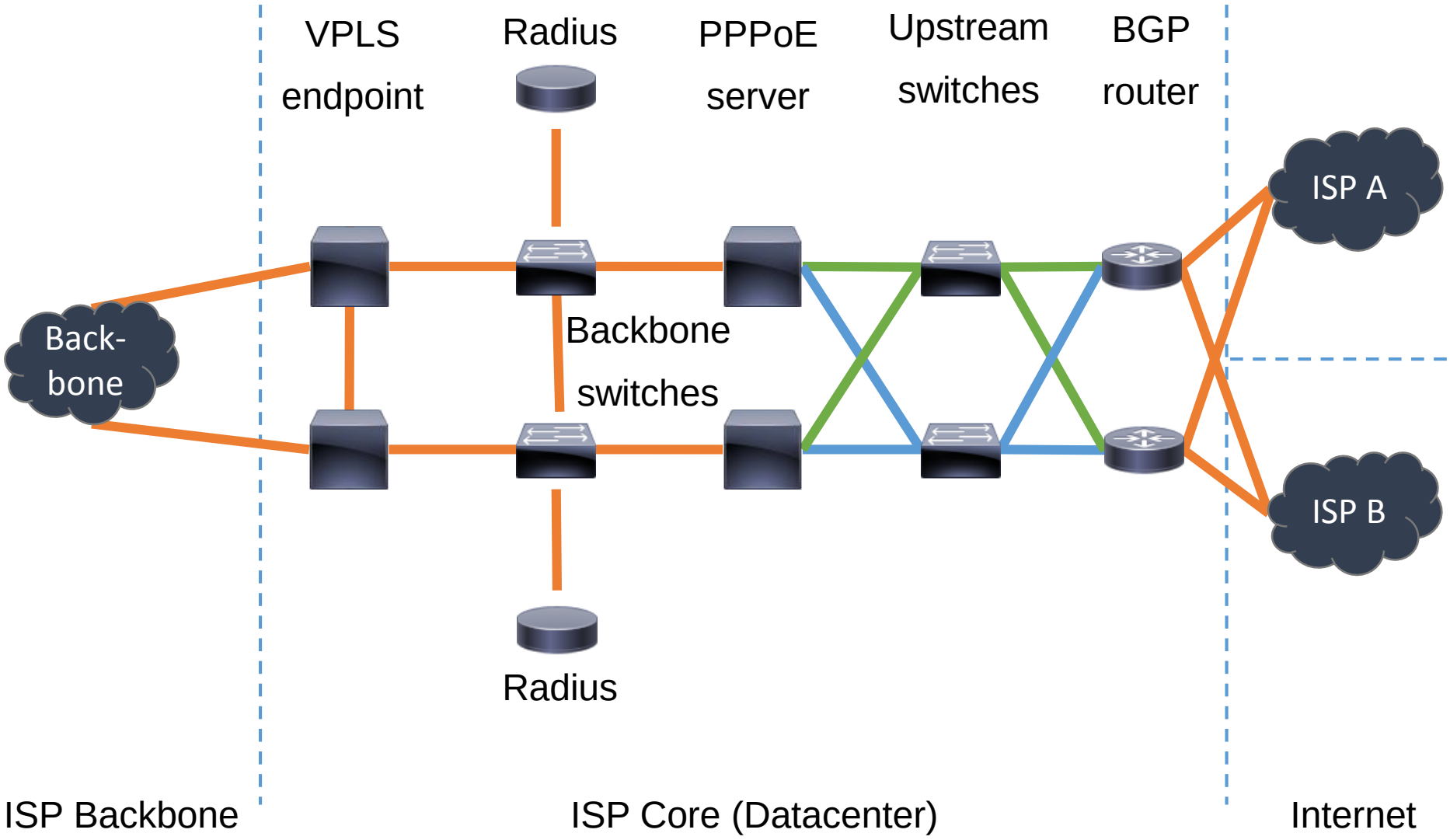
PPPoE Access Concentrator

VPLS Approach

High Available ISP Network



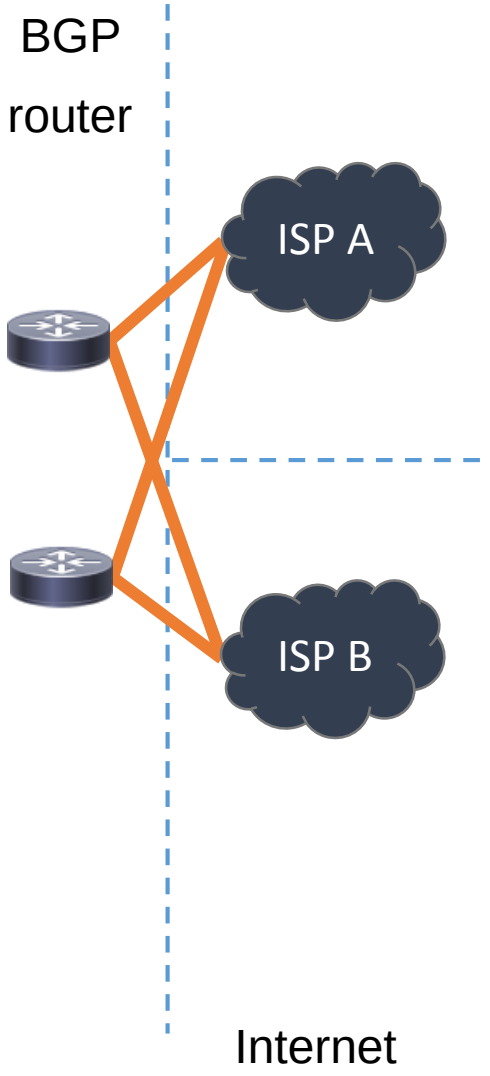
High Available ISP Network



BGP Upstream

- Redundant BGP routers
- Two BGP sessions to each ISP
- Preferred ISP “always” available

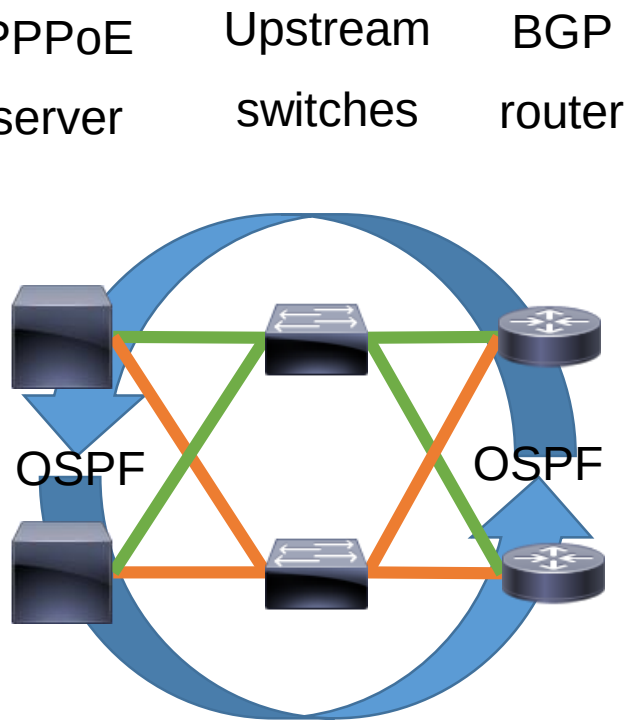
- Prepends to prefer ISP
- E.g. community to choose backup router



Routing

- Default route by OSPF
- BGP router can fail

- PPPoE client routes by OSPF
- /32 address appears on BRAS with client connection
- OSPF will route to correct BRAS

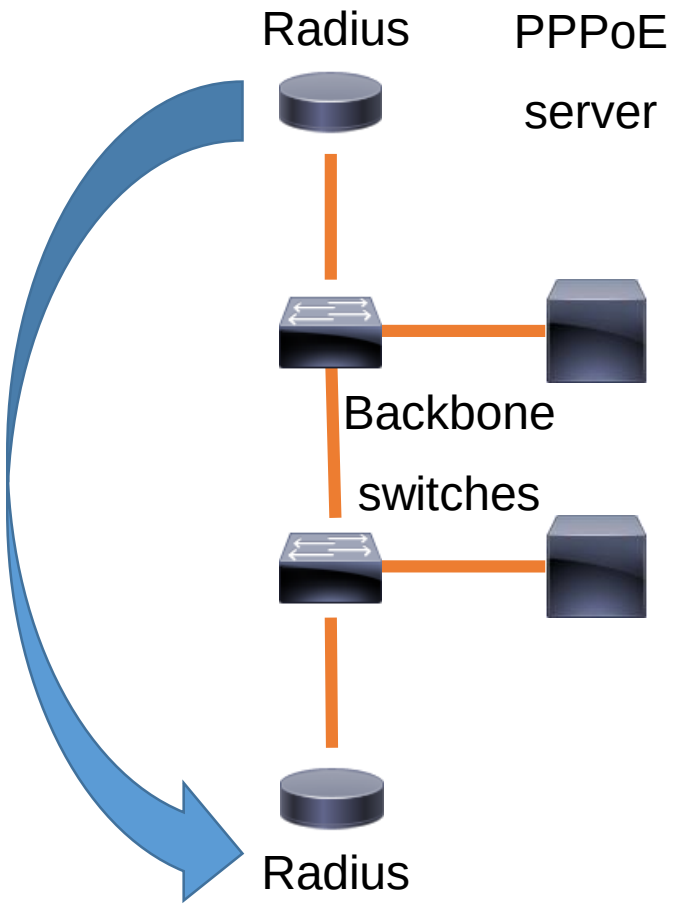


Redundant Radius Server

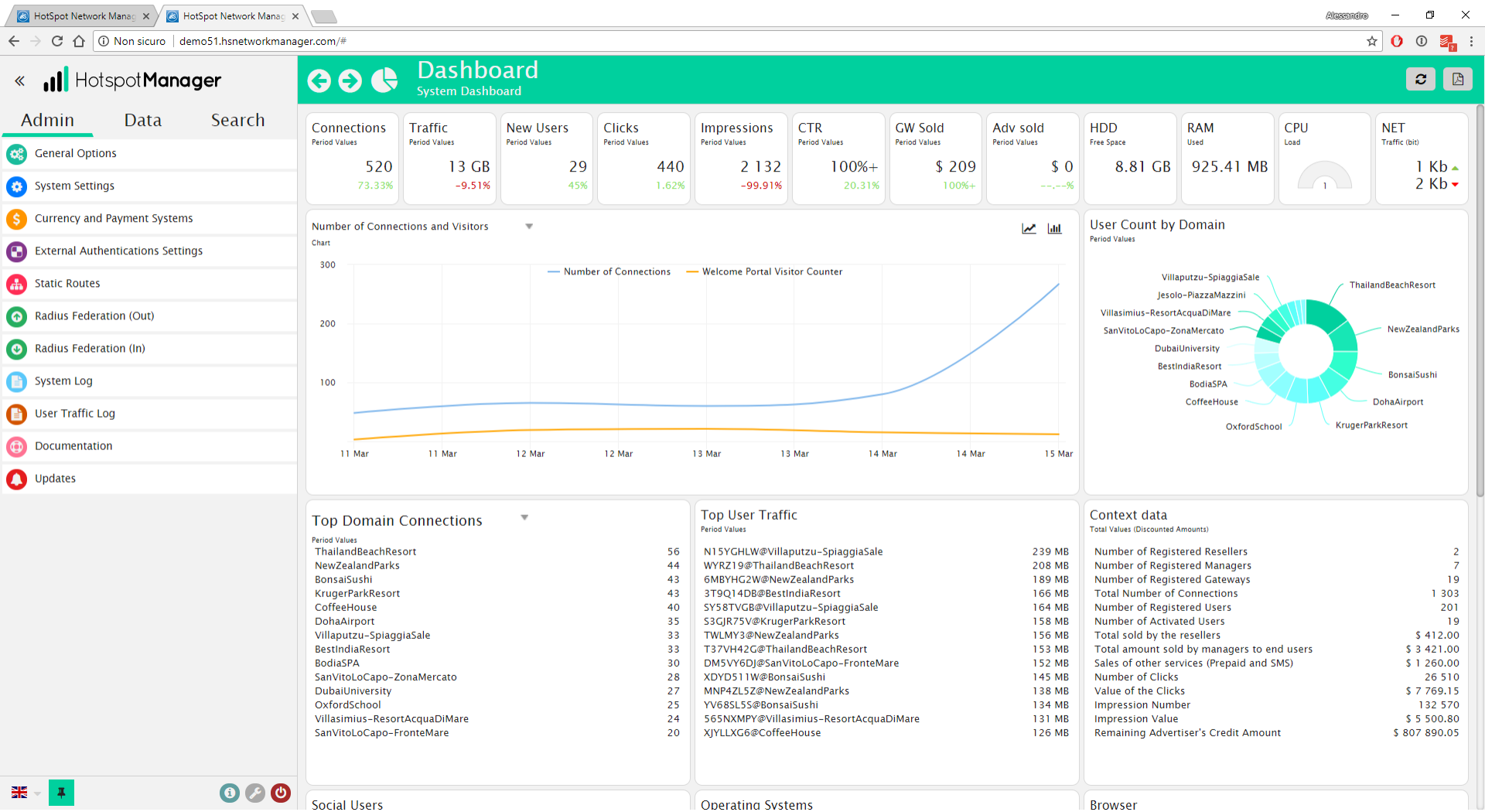
- Two radius server on BRAS
- Replication
- E.g. FreeRADIUS (mysql replication)

Ready to run alternative:

- HSNM (click)
- Integrated replication
- Complex services with Radius federations



HS Network Manager



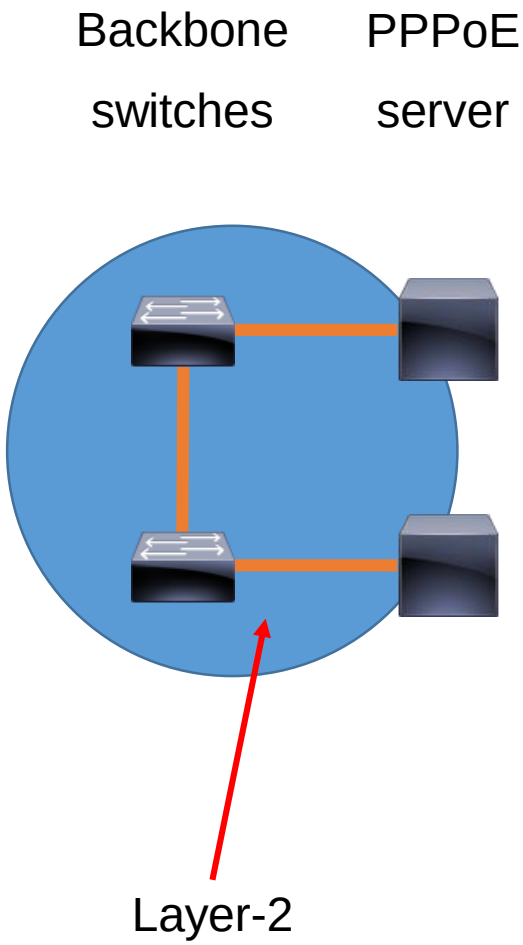
Looking for Captive Portal and PPPoE authentication? Contact sales@fmsweb.de

BRAS Loadbalancing

- Multiple BRAS in layer 2 network
- Works out off the box
- First come first serve

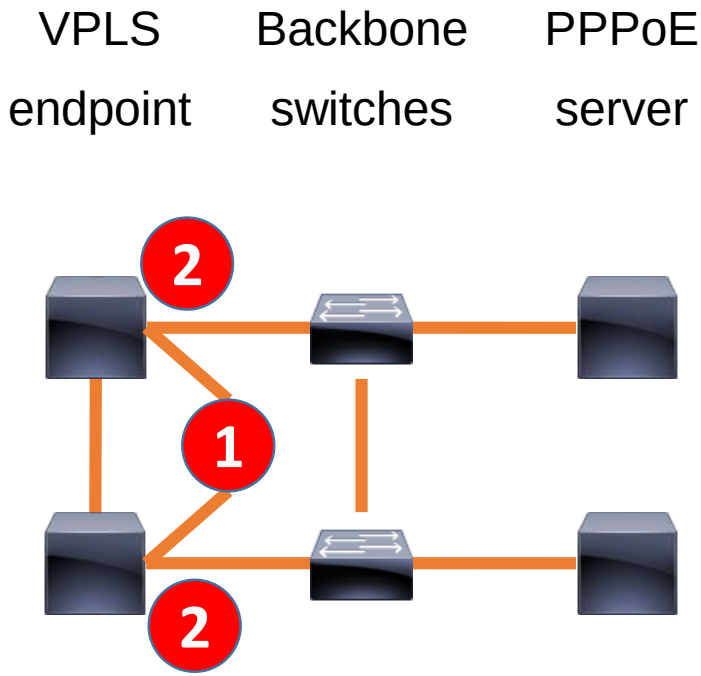
- PPPoE sessions will distribute across BRAS

- BRAS loadbalancing and failover

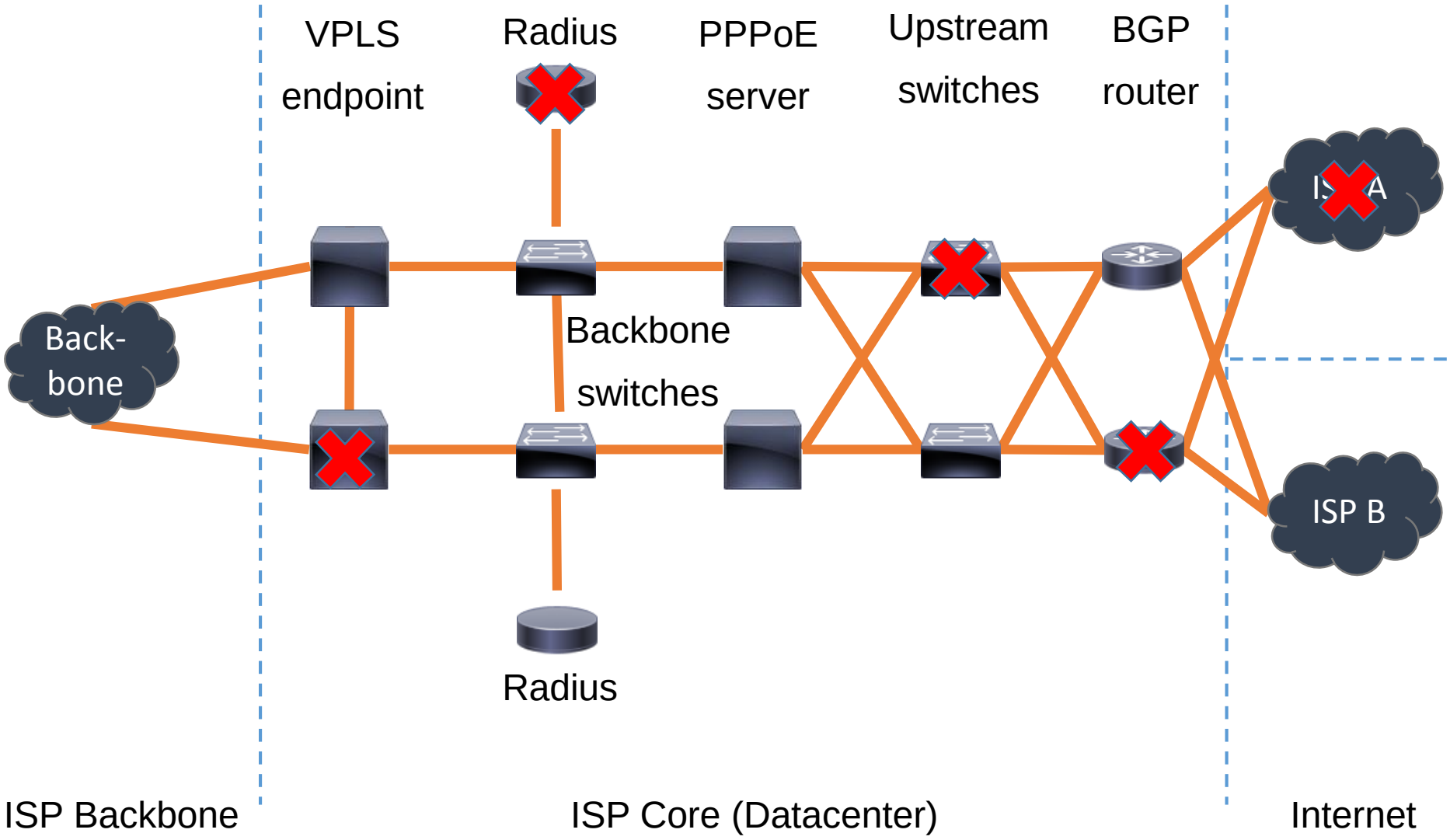


VPLS Concentrator Redundancy

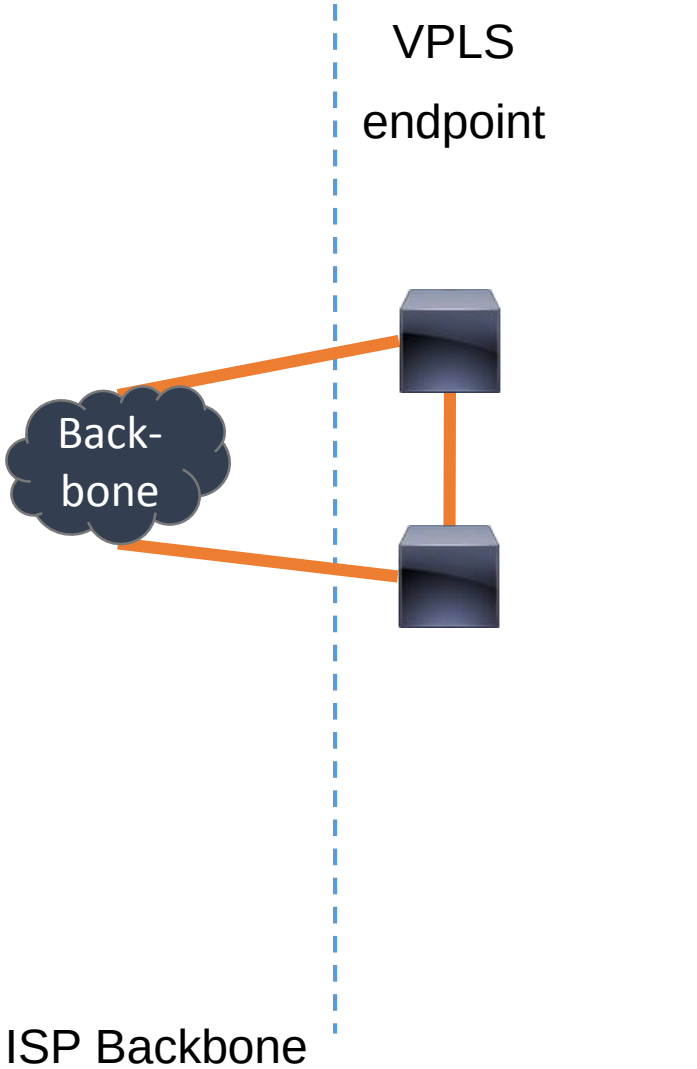
- 1 = VRRP interface
- VRRP IP as VPLS tunnel endpoint
- Achieve redundant VPLS concentrator
- Interface 2 bridged with VPLS tunnel



Still Operational with Loadbalancing



Presentation of Sebastian Inacker



Today 14:15

Presentation of Sebastian Inacker

“Use cases and pitfalls in MPLS/VPLS networks”

Access all our presentations here.

THANK YOU

… and enjoy the Usermeeting

FMS Internetservice GmbH

Phone: +49 761 2926500
Web: www.fmsweb.de
Shop: www.mikrotik-shop.de
Email: sales@fmsweb.de
Twitter: https://twitter.com/fmsweb_de