



Access Concentrators

Optimizing Availability and Performance



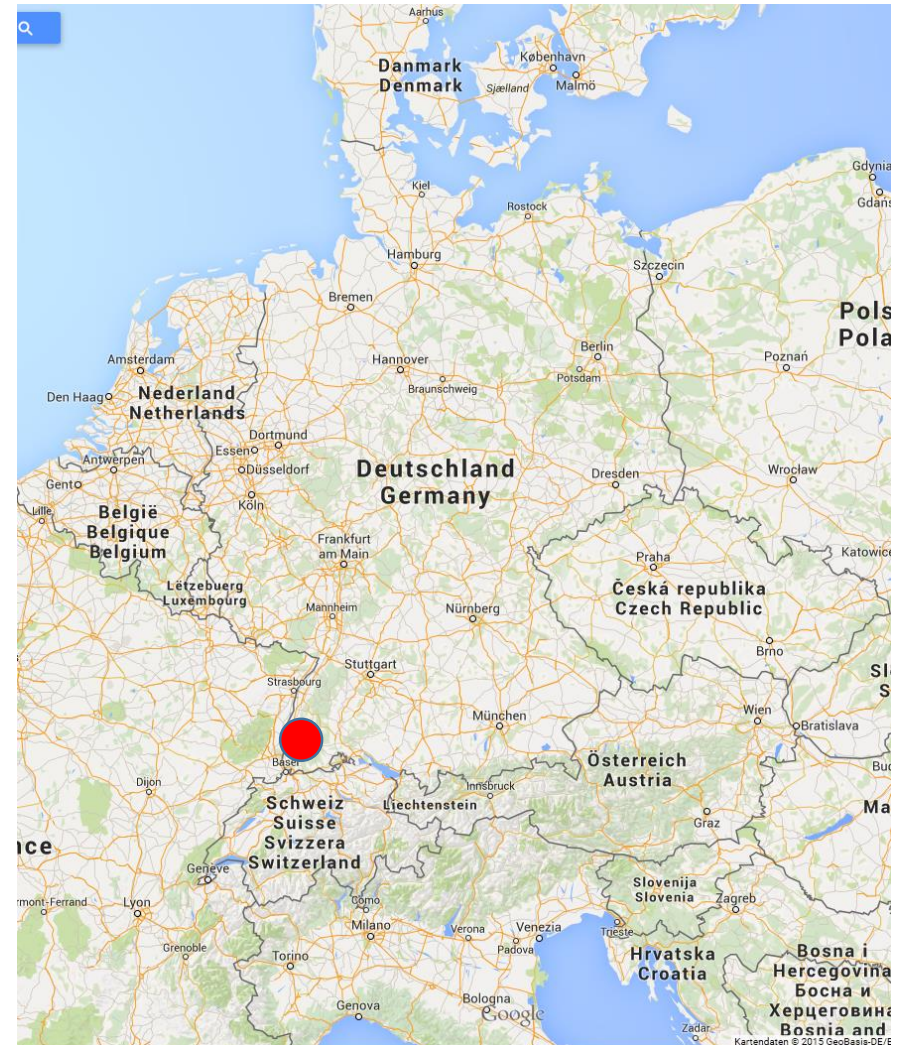
FMS Internetservice GmbH

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
- Small 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



NOKIA

Siklu

MikroTik



MARS ANTENNAS & RF SYSTEMS LTD.





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

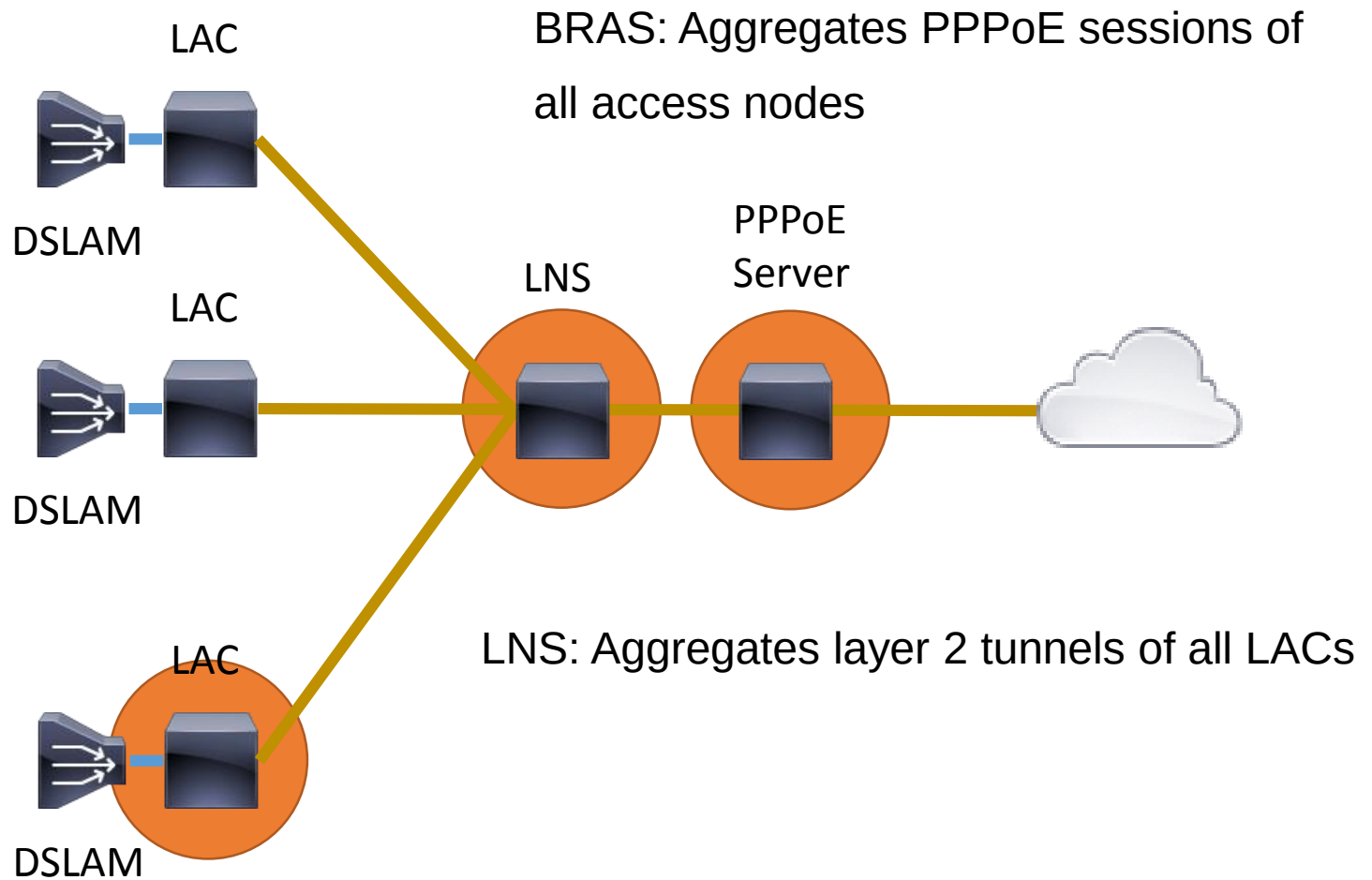
- Remote access concentrator
 - Used in dial up networks
 - ISDN / POTS

- LAC/LNS
 - E.g. used in broadband networks
 - Aggregate and forward PPPoE traffic

- VPN Server
- BRAS (PPPoE Server)



Multiple Access Concentrators





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

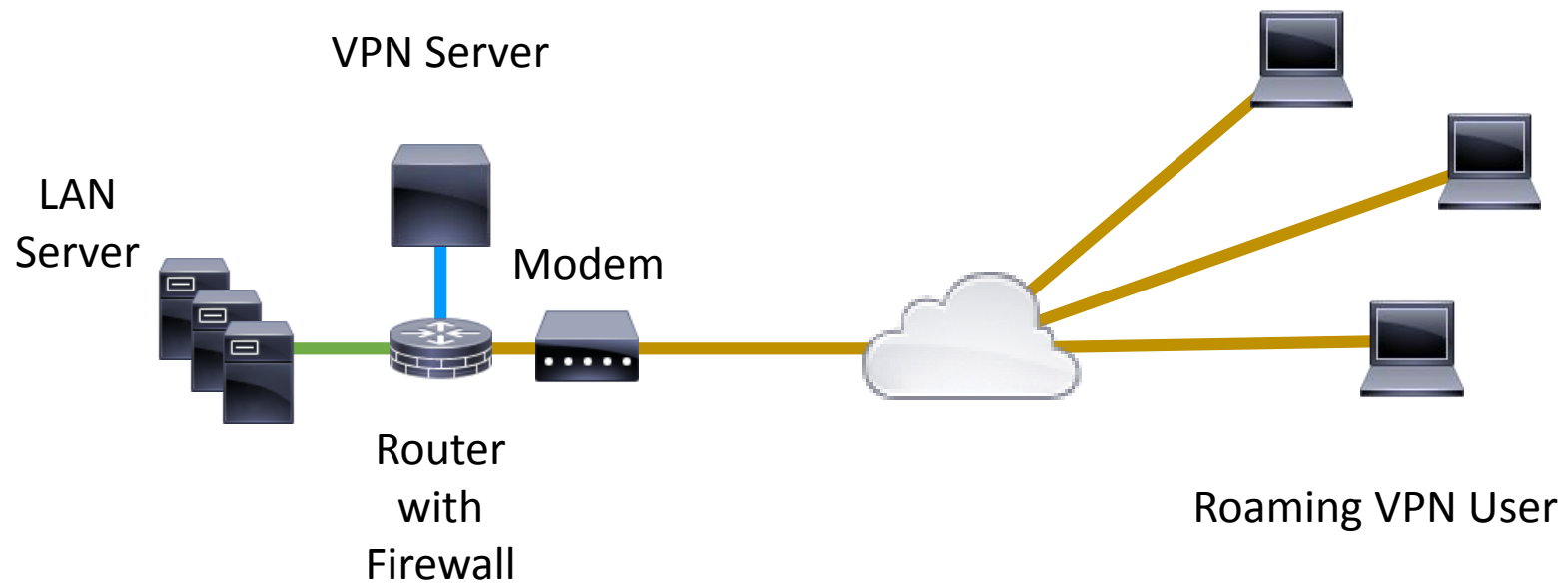


Enterprise Networks

VPN Access Concentrators

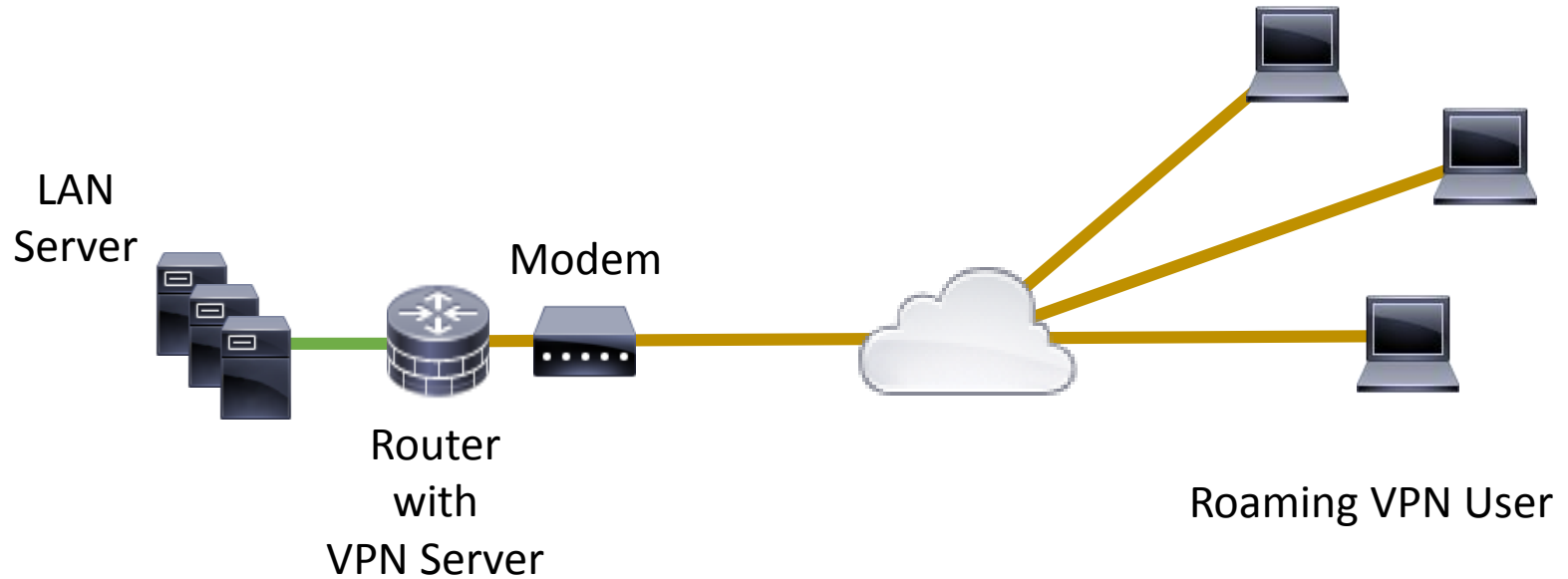


Enterprise VPN with DMZ





Enterprise VPN without DMZ



Single points of failure:

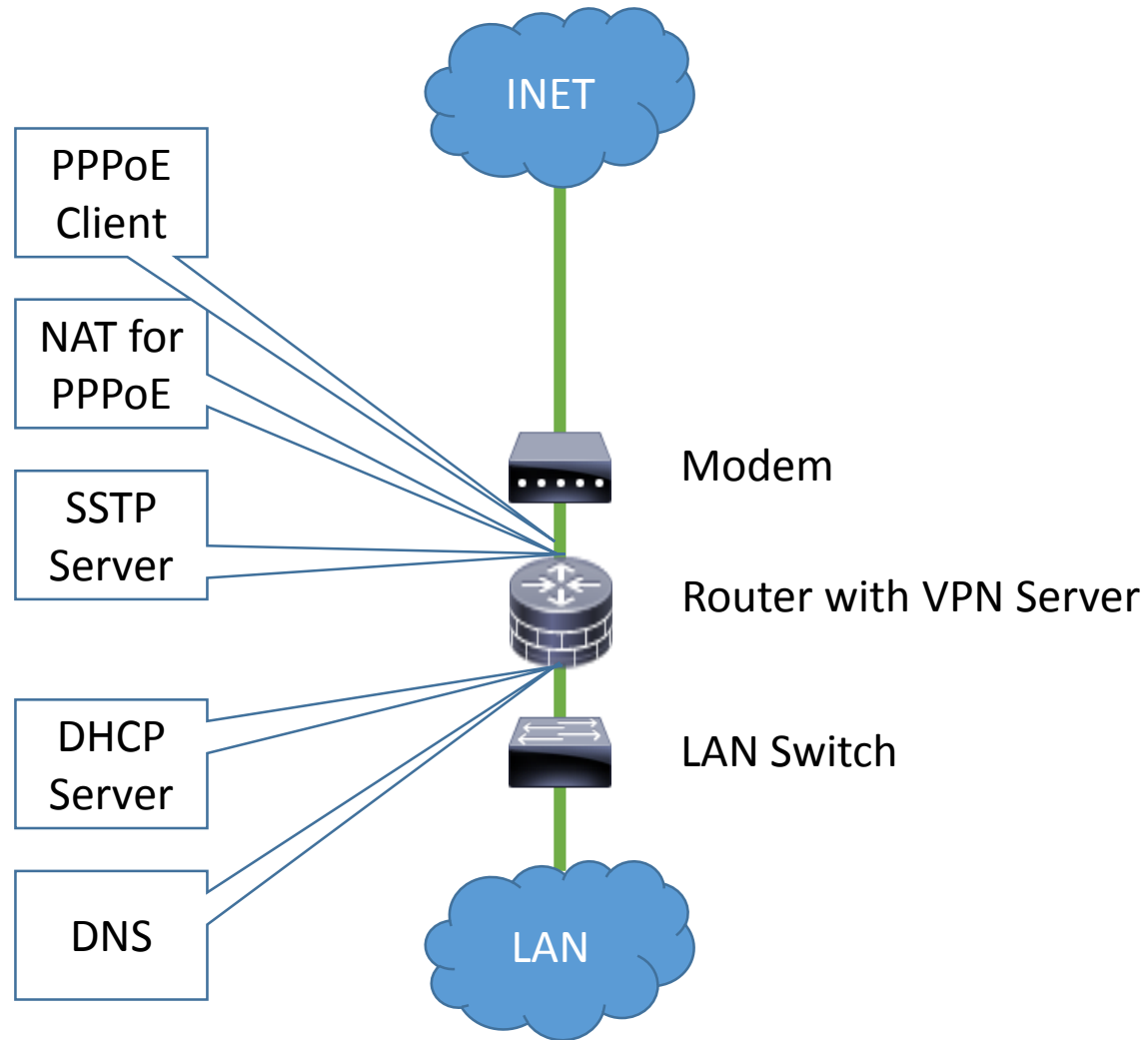
- VPN server
- broadband line



Broadband VPN Gateway

Assumptions:

- Basic setup present
- Not discussed unless special considerations necessary



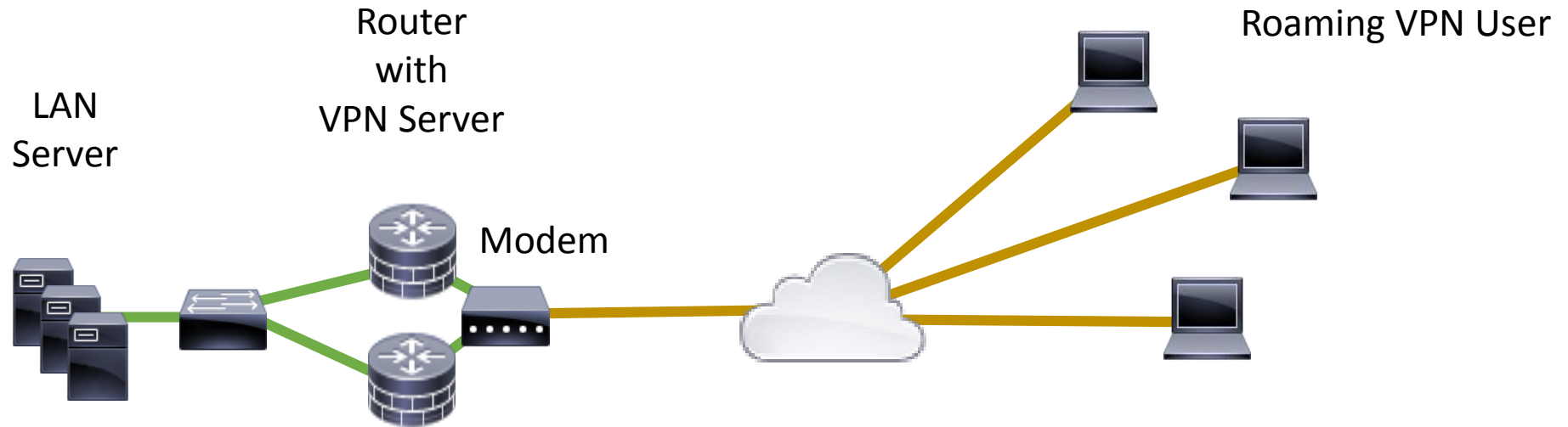


Enterprise VPN

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

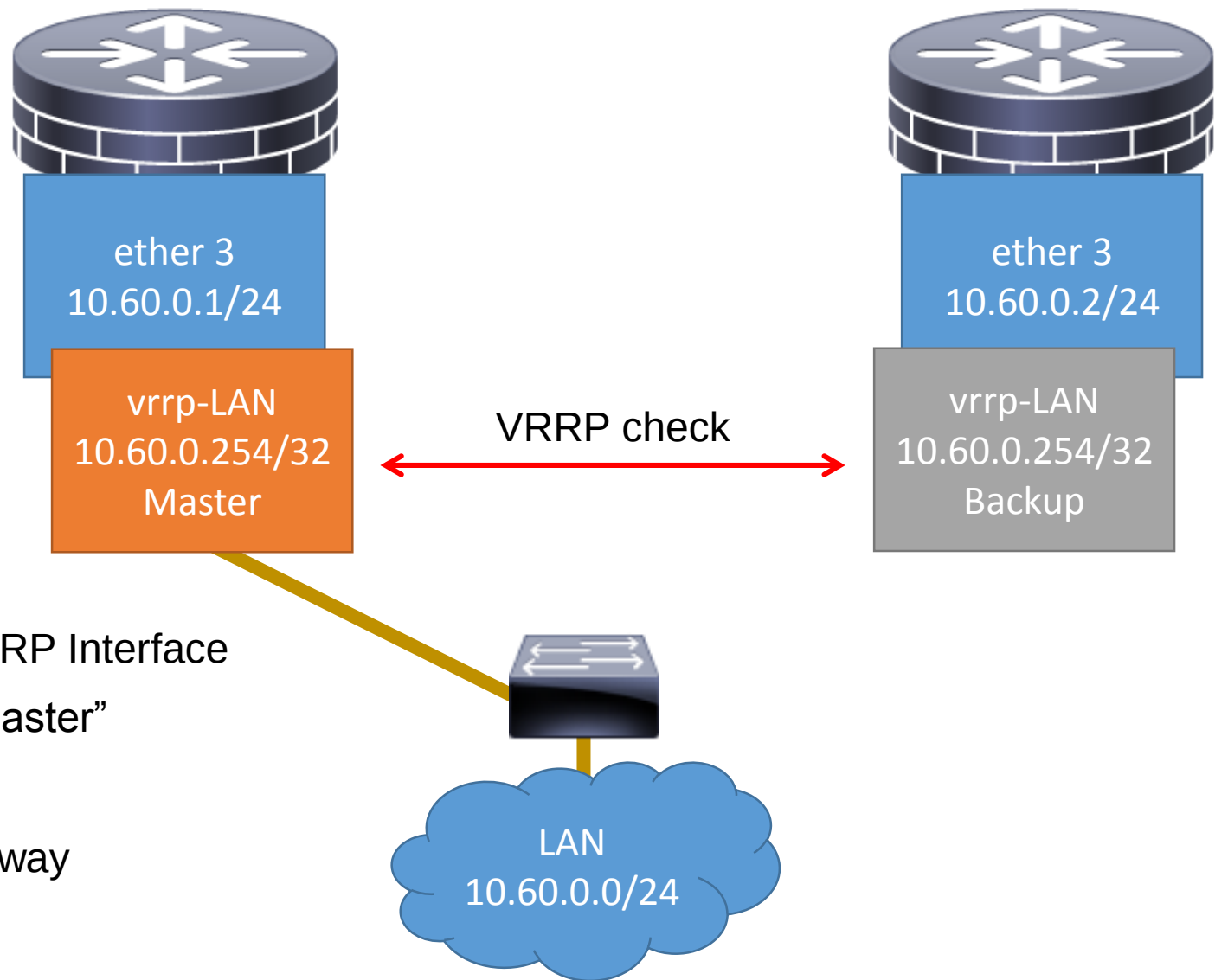
- LAN devices will not support dynamic routing
- Default Gateway IP cannot change
- Both Gateways have to share the same IP

- 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

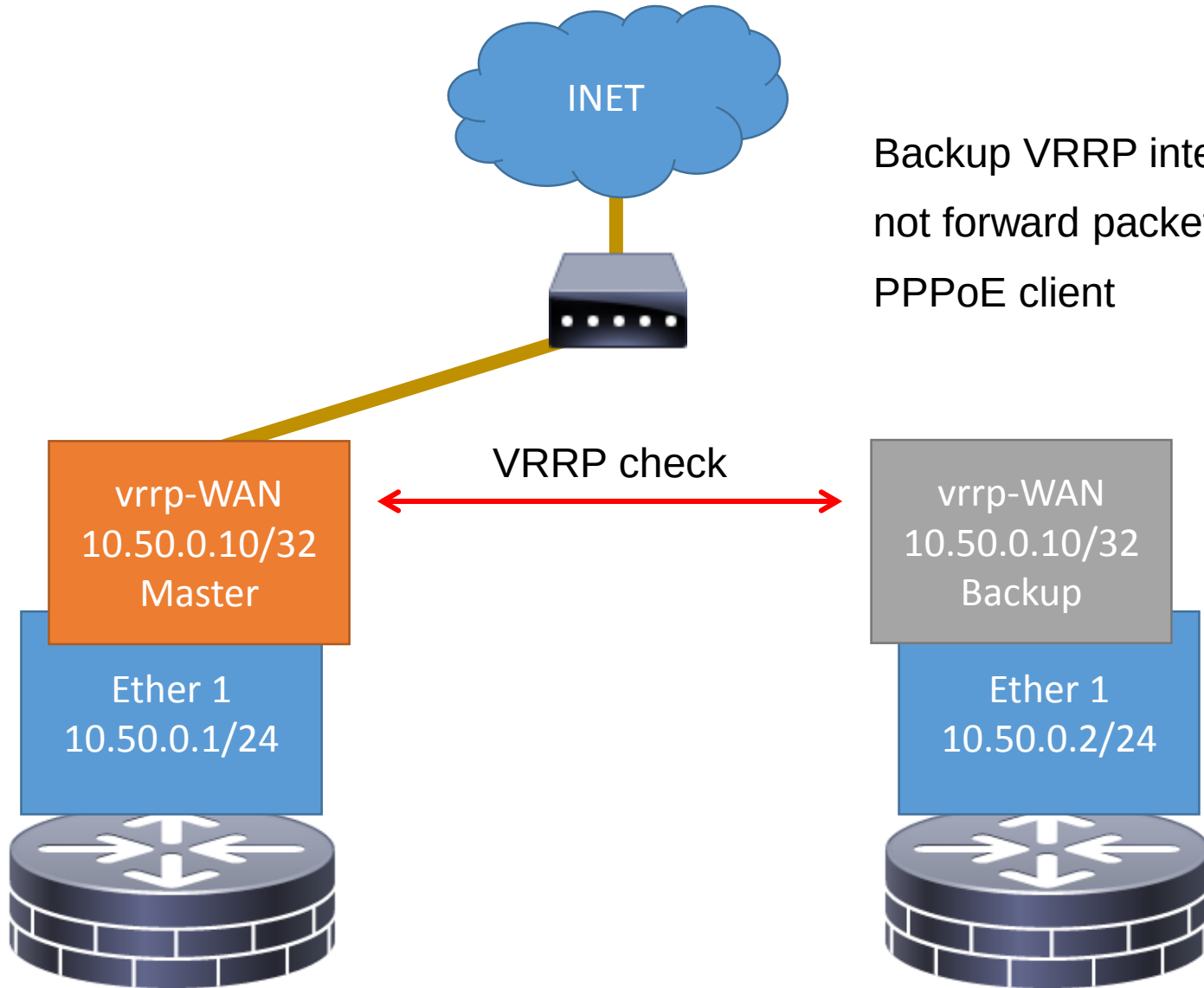


Switching PPPoE Client

- 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





VRRP Overview

MASTER

Interface List

Interface	Name	Actual MTU	L2 M
R	ether1	1500	
RM	vmp1	1500	
R	ether2	1500	
R	ether3	1500	
RM	vmp-LAN	1500	
R	ether4	1500	
R	pppoe-out1	1480	

8 items

Route List

Routes	Nextops	Rules	VRF
Active			
DAS	0.0.0.0/0	pppoe-out1 reachable	
DAC	10.50.0.0/24	ether1 reachable	
DAC	10.50.0.10	vmp1 reachable	
DAC	10.60.0.0/24	ether3 reachable	
DAC	10.60.0.254	vmp-LAN reachable	
DAC	10.70.0.0/24	ether4 reachable	
DAC	192.168.0.0/24	ether2 reachable	
DAC	192.168.0.48	pppoe-out1 reachable	

Address List

Address	Network	Interface
10.50.0.1/24	10.50.0.0	ether1
192.168.0.37/24	192.168.0.0	ether2
10.60.0.1/24	10.60.0.0	ether3
10.70.0.1/24	10.70.0.0	ether4
10.40.0.255	192.168.0.48	pppoe-out1
10.60.0.254	10.60.0.254	vmp-LAN
10.50.0.10	10.50.0.10	vmp1

BACKUP

Interface List

Interface	Name	Actual MTU	L2 M
R	ether1	1500	
B	vmp-WAN	1500	
R	ether2	1500	
R	ether3	1500	
B	vmp-LAN	1500	
R	ether4	1500	
R	ether5	1500	
R	pppoe-out1		

Route List

Routes	Nextops	Rules	VRF
Distance			
DAC	10.50.0.0/24	ether1 reachable	
DAC	10.60.0.0/24	ether3 reachable	
DAC	10.70.0.0/24	ether4 reachable	
DAC	192.168.0.0/24	ether2 reachable	

Address List

Address	Network	Interface
10.50.0.2/24	10.50.0.0	ether1
192.168.0.51/24	192.168.0.0	ether2
10.60.0.2/24	10.60.0.0	ether3
10.70.0.2/24	10.70.0.0	ether4
10.60.0.254	10.60.0.254	vmp-LAN
10.50.0.10	10.50.0.11	vmp-WAN



VRRP Configuration

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

The screenshot displays two windows from a network configuration tool. The top window, titled 'Address List', contains a table with the following data:

	Address	Network	Interface
D	10.40.0.255	192.168.0.48	pppoe-out1
	10.50.0.1/24	10.50.0.0	ether1
	10.50.0.10	10.50.0.10	vmp1
	10.60.0.1/24	10.60.0.0	ether3
	10.60.0.254	10.60.0.254	vmp-LAN
	10.70.0.1/24	10.70.0.0	ether4
D	192.168.0.37/24	192.168.0.0	ether2

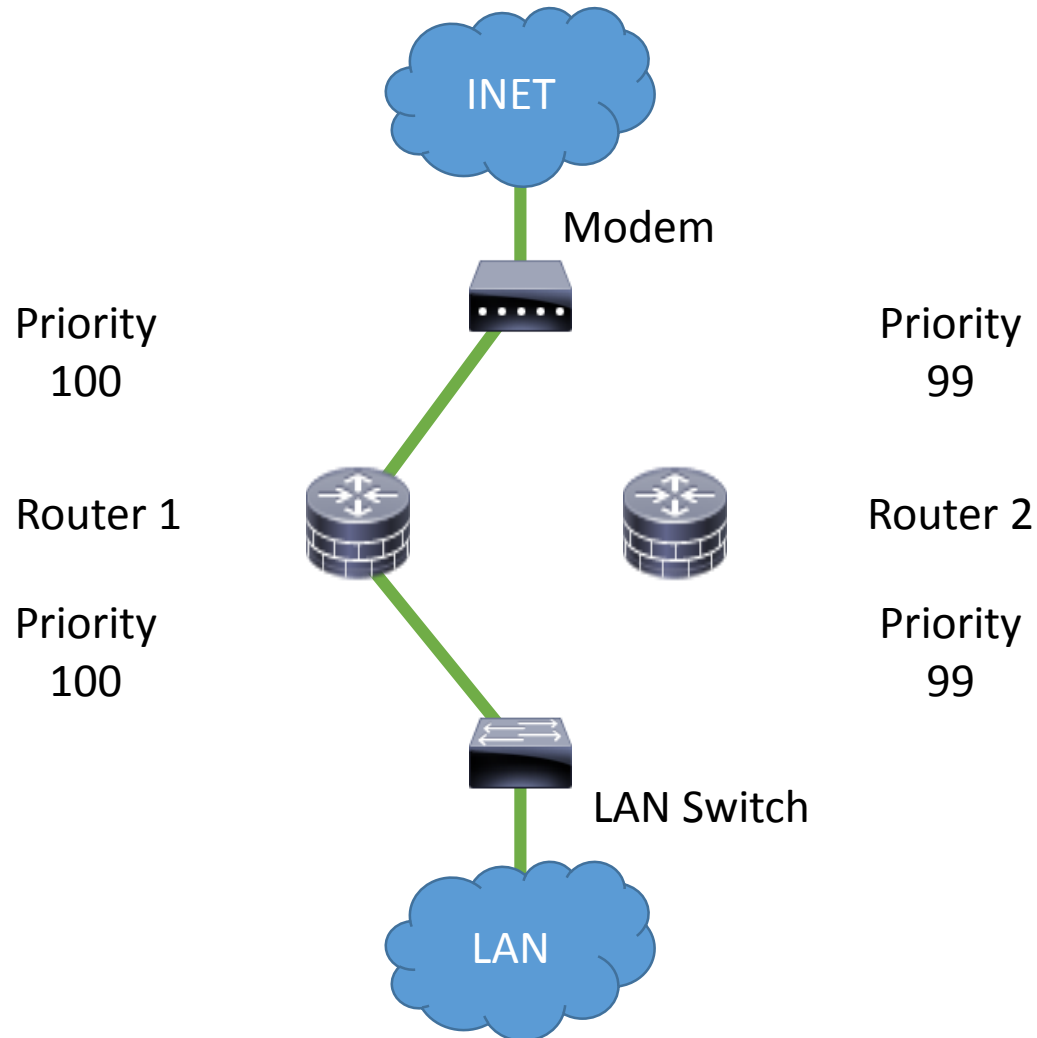
The bottom window, titled 'Interface <vmp-LAN>', shows the configuration for the VRRP group. The 'VRRP' tab is selected. The following fields are highlighted with red boxes:

- Interface: ether3
- VRID: 20
- Priority: 100
- Interval: 1.00 s
- ☒ Preemption Mode

Below these fields, the 'Authentication' section shows 'none' selected, and the 'Version' is set to 3. The 'V3 Protocol' is set to IPv4.

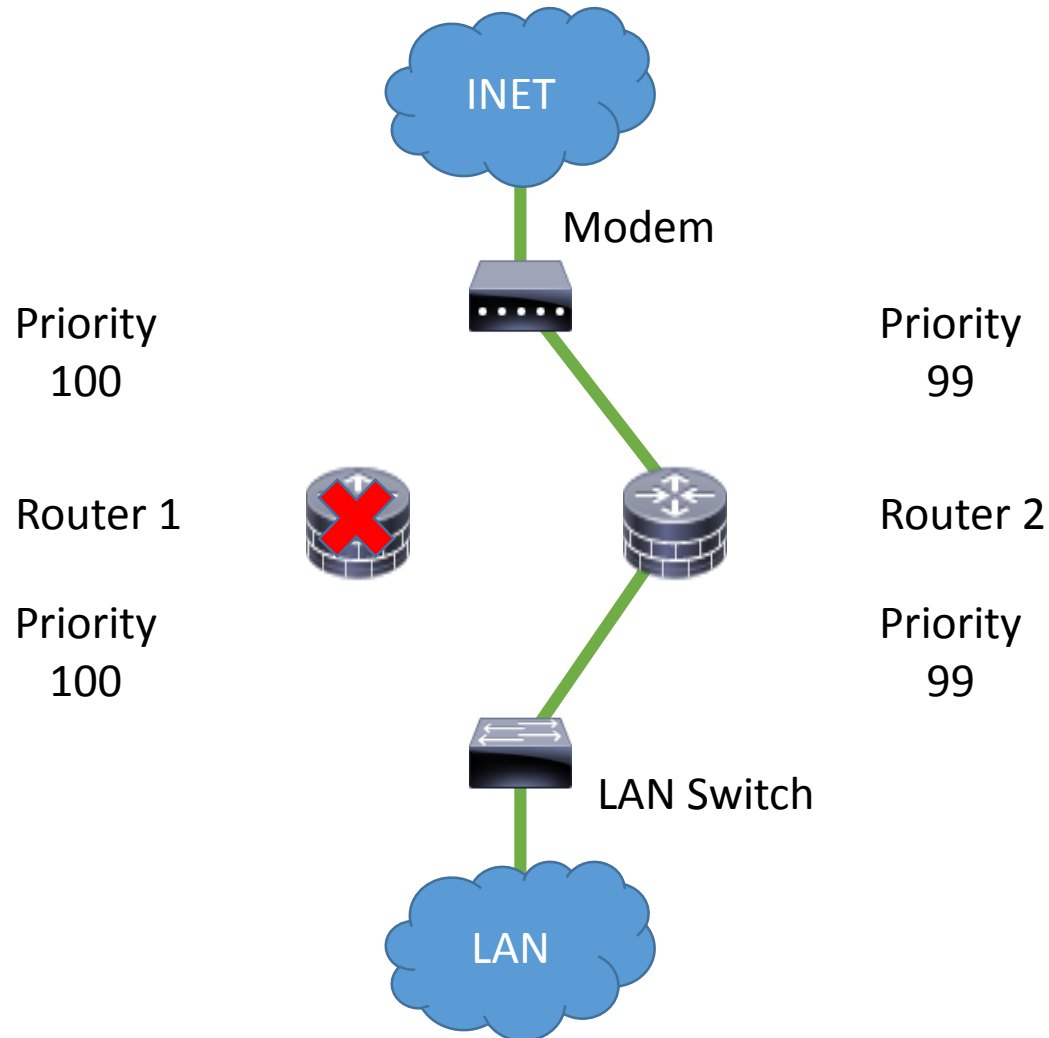


Router 1 VRRP Master





Router 2 VRRP Master





Asymmetric VRRP

Inbound traffic

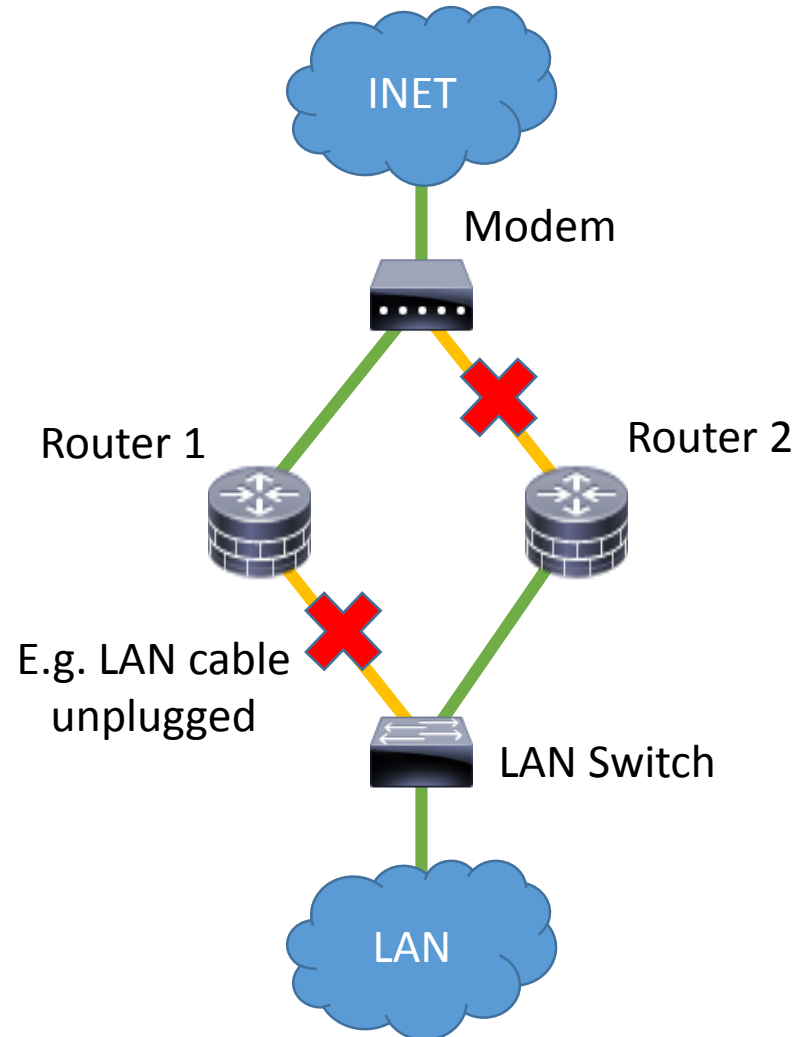


No LAN
connection

No PPPoE
connection



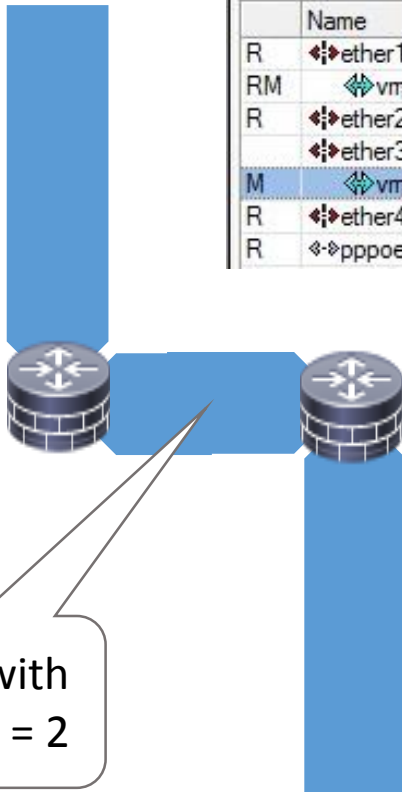
Outbound traffic





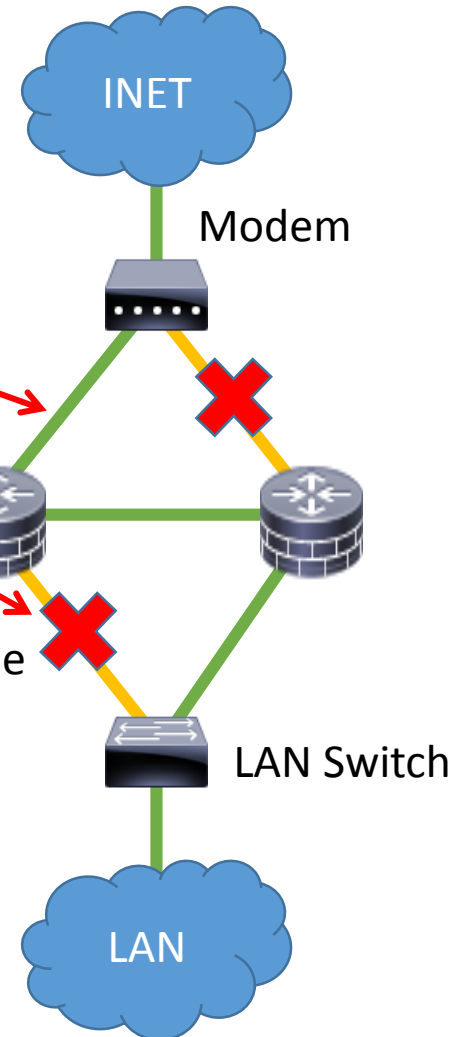
Asymmetric VRRP

INET



LAN

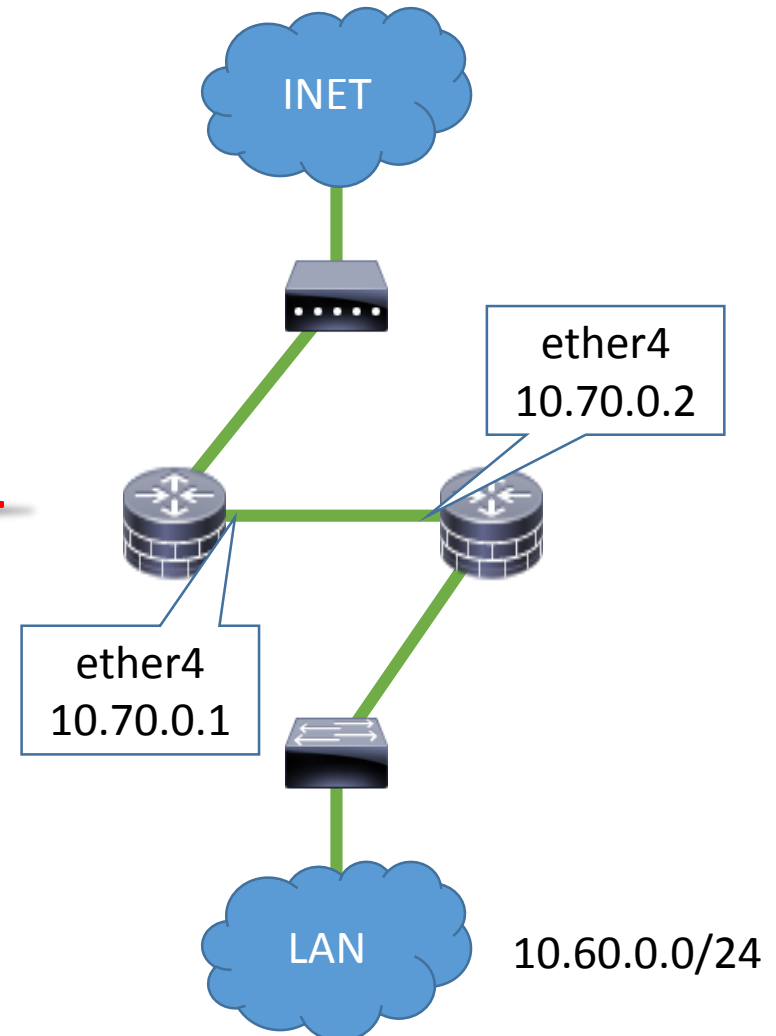
	Name	Type	Actual MTU	L2 M
R	ether1	Ethernet	1500	
RM	vrrp1	VRRP	1500	
R	ether2	Ethernet	1500	
R	ether3	Ethernet	1500	
M	vrrp-LAN	VRRP	1500	
R	ether4	Ethernet	1500	
R	pppoe-out1	PPPoE Client	1480	





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	vmp1 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	vmp-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

Interface List

Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel
+	-	✓	✗	📁	🔍
Detect Internet					
Name	Type	Tx	Rx		
R ether1	Ethernet	21.7 Mbps	21.6 Mbps	1	
RM vmp1	VRRP	21.5 Mbps	21.3 Mbps		
R ether2	Ethernet	75.3 kbps	12.7 kbps		
R ether3	Ethernet	21.4 Mbps	512 bps	2	
B vmp-LAN	VRRP	0 bps	0 bps		
R ether4	Ethernet	0 bps	21.6 Mbps		
R pppoe-out1	PPPoE Client	21.0 Mbps	20.8 Mbps	5	1

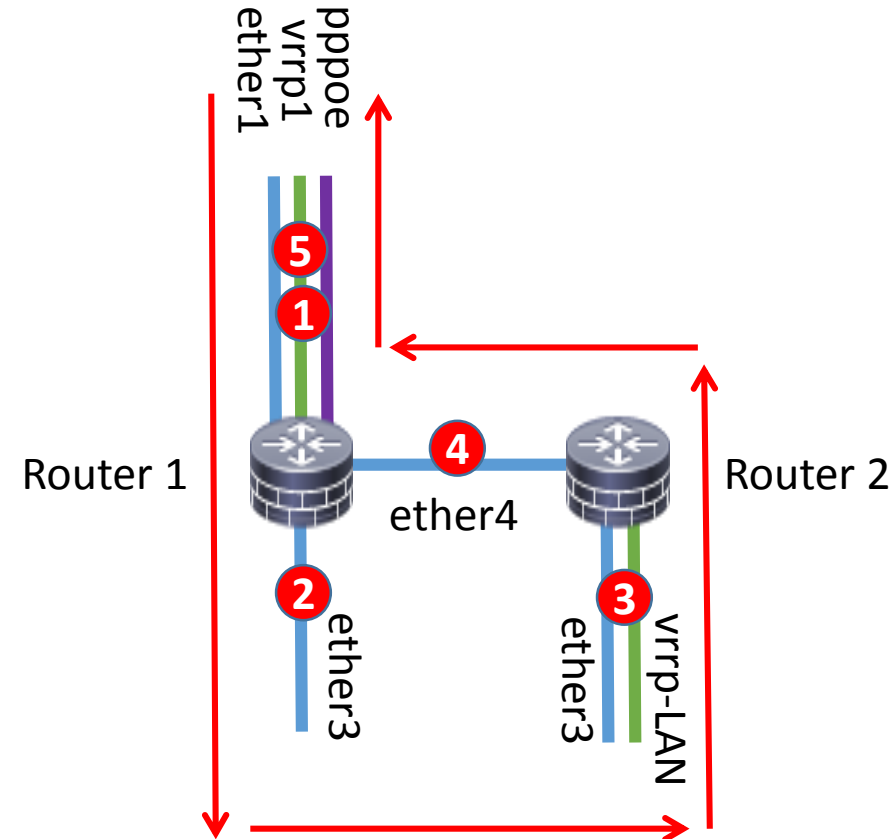
.51 (Test: PPPoE-Client-2) - WinBox v6.41.3 on RB750UP (mipsbe)

Dashboard

Session: 192.168.0.51

Interface List

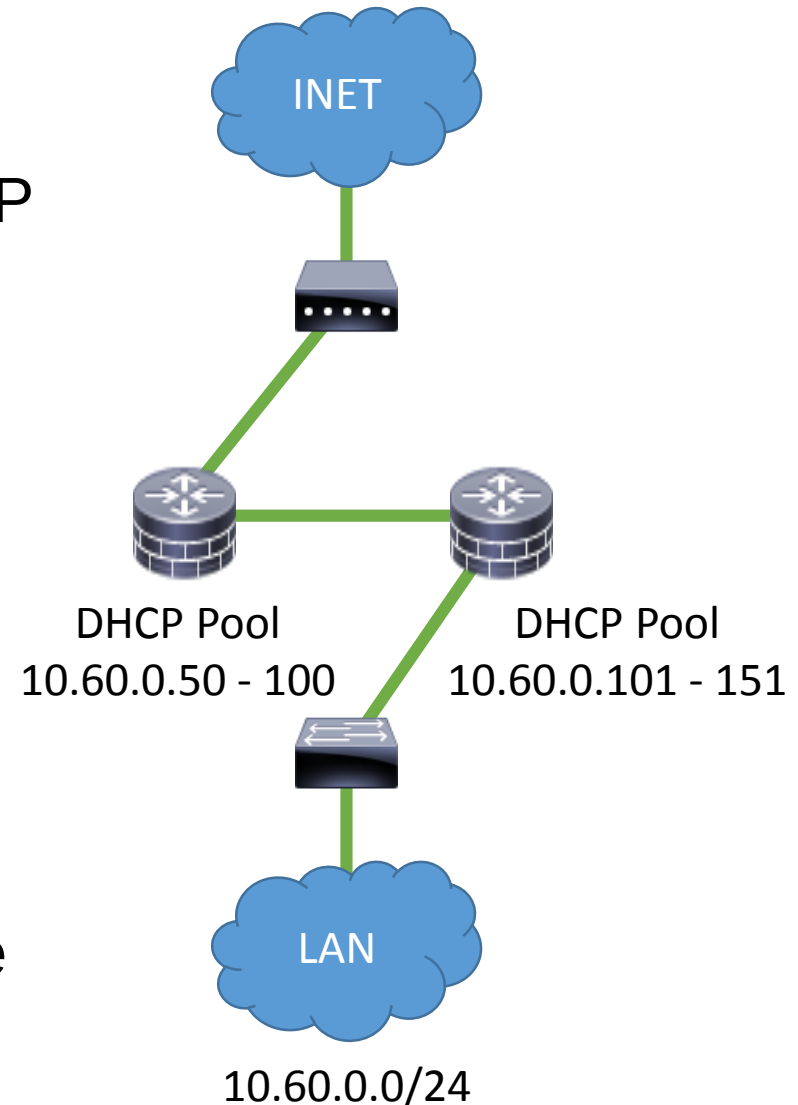
Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel
+	-	✓	✗	📁	🔍
Detect Internet					
Name	Type	Tx	Rx	Tx Pa	
R ether1	Ethernet	0 bps	960 bps		
B vmp-WAN	VRRP	0 bps	0 bps		
R ether2	Ethernet	72.8 kbps	12.4 kbps		
R ether3	Ethernet	512 bps	21.7 Mbps	3	
RM vmp-LAN	VRRP	368 bps	21.4 Mbps	4	
R ether4	Ethernet	21.7 Mbps	0 bps		
ether5	Ethernet	0 bps	0 bps		
pppoe-out1	PPPoE Client	0 bps	0 bps		





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

Routerboard

☒ Routerboard

Model: RouterBOARD 941-2nD

Serial Number: 5B32041CF05F

Firmware Type: qca9531L

OK

Upgrade

Settings

Cloud

☒ DDNS Enabled

☒ Update Time

Public Address: 34.200.14.9

DNS Name: 5b32041cf05f.sn.mynetname.net

Routerboard

☒ Routerboard

Model: 750UP

Serial Number: 2F3F02F3DCC0

Firmware Type: ar7240

OK

Upgrade

Settings

Cloud

☒ DDNS Enabled

☒ Update Time

Public Address: 34.200.14.9

DNS Name: 2f3f02f3dcc0.sn.mynetname.net

- 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 ddns�ass "PASSWORD"
:global ddns�host "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=$ddns�host address=[ :pick $ddnsip 0 [ :find $ddnsip "/" ] ] key-
name=$ddnsuser key=$ddns�ass ] ]
        :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

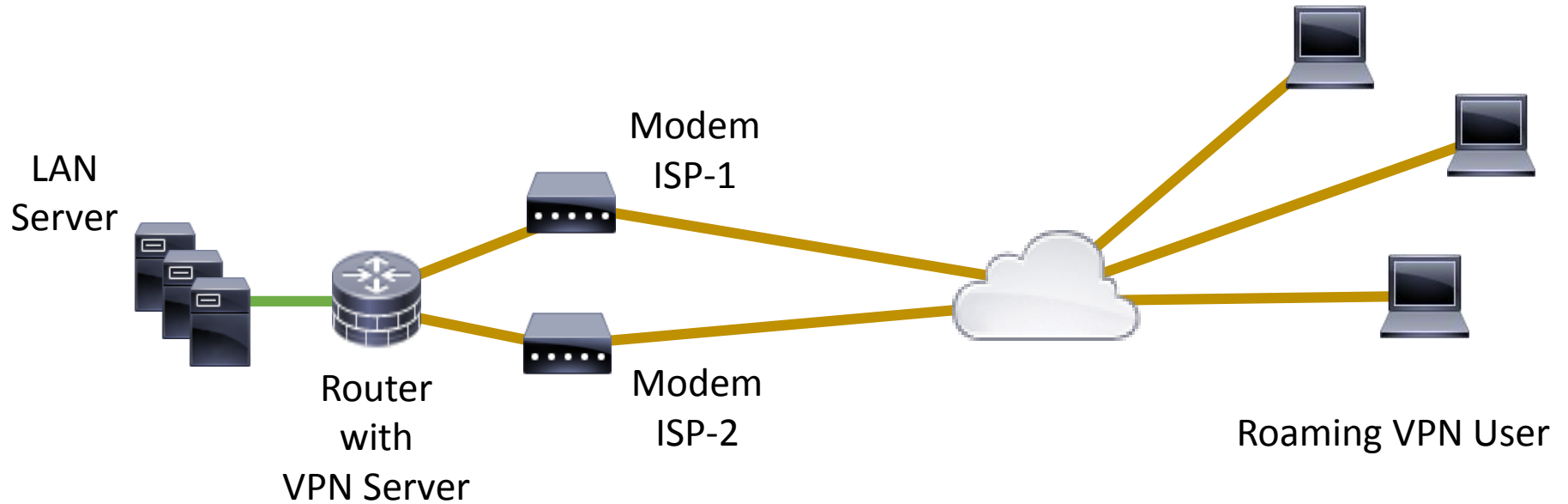


Enterprise VPN

Redundant Access Lines



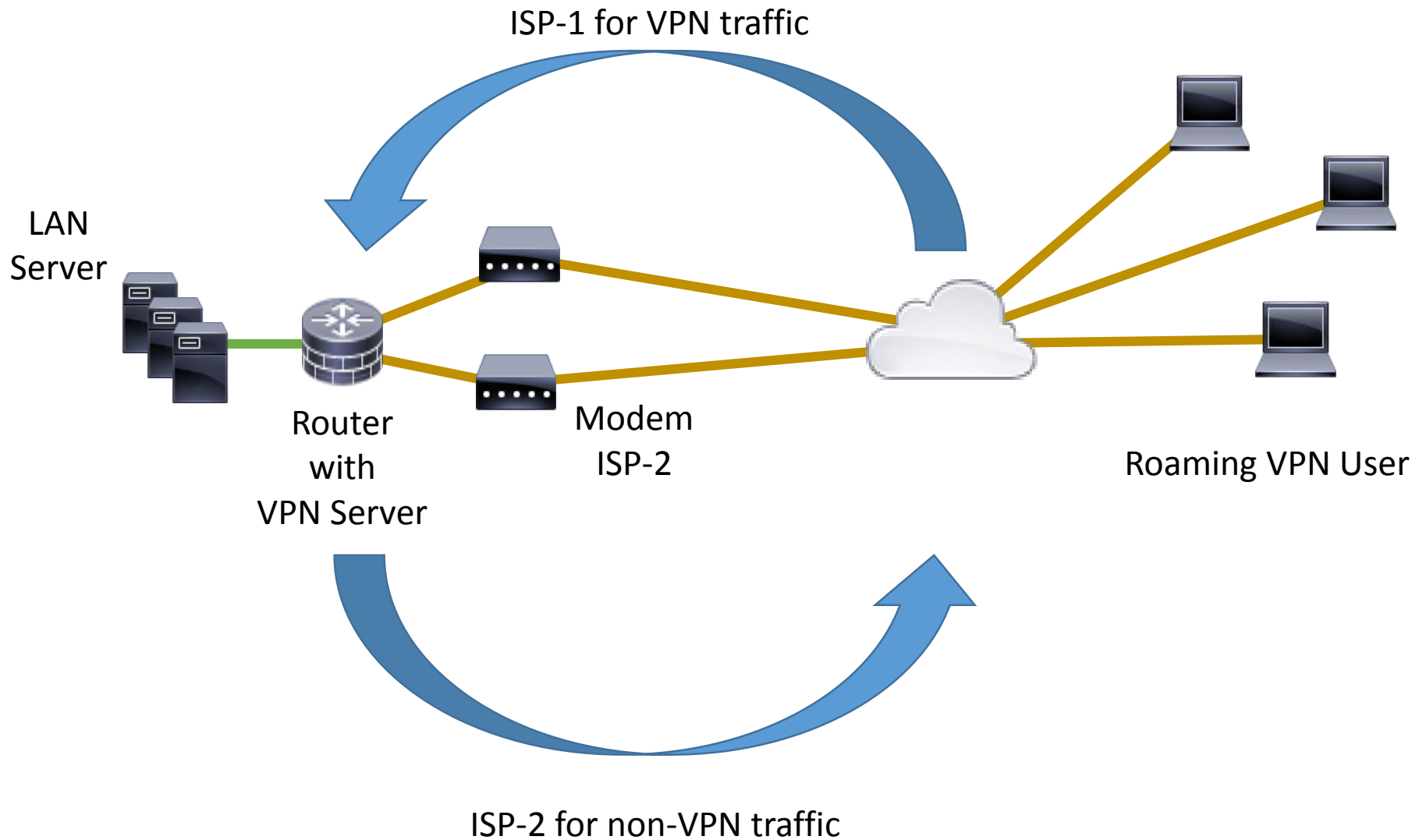
Overview



- two DSL lines (PPPoE)
- Dynamic public IPs



Overview





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

Interface <pppoe-out2>

General Dial Out Status Traffic

Service:

AC Name:

User: pppoe2

Password:

Profile: default

Keepalive Timeout: 10

☐ Dial On Demand

☐ Use Peer DNS

☒ Add Default Route

Default Route Distance: 1

Interface <pppoe-out1>

General Dial Out Status Traffic

Service:

AC Name:

User: pppoe1

Password:

Profile: default

Keepalive Timeout: 10

☐ Dial On Demand

☒ Use Peer DNS

☒ Add Default Route

Default Route Distance: 2

Route List

Routes Nexthops Rules VRF

Find main

	Dst. Address	Gateway	Distance
DS	0.0.0.0/0	pppoe-out1 reachable	2
DAS	0.0.0.0/0	pppoe-out2 reachable	1

PPP

Interface PPPoE Servers Secrets Profiles Active

PPP Scanner

	Name	Type	Act
DR	<sstp-sstp 1>	SSTP Server Binding	
R	pppoe-out1	PPPoE Client	
R	pppoe-out2	PPPoE Client	



Failover ISP2 -> ISP1

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

	Name	Type
DR	<sstp-sstp1>	SSTP Server Binding
R	<pppoe-out1>	PPPoE Client
	<pppoe-out2>	PPPoE Client

	Dst. Address	Gateway	Distance
DAS	0.0.0.0/0	pppoe-out1 reachable	2
DAC	192.168.210.0/24	ether4 reachable	0
DAC	192.168.220.254	<sstp-sstp1> reachable	0
DAC	192.168.230.252	pppoe-out1 reachable	0



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

#	Action	Chain	Src. Ad...	Dst. Address	Protocol	S
... Test ISP-1 connectivity						
0	mar...	output		8.8.8.8	1 (icmp)	
... Test ISP-2 connectivity						
1	mar...	output		8.8.4.4	1 (icmp)	

Mangle Rule <8.8.8.8>						Mangle Rule <8.8.8.8>					
General	Advanced	Extra	Action	Statist		General	Advanced	Extra	Action	Statist	
Chain: output						Action: mark routing					
Src. Address:						☐ Log					
Dst. Address: 8.8.8.8						Log Prefix:					
Protocol: 1 (icmp)						New Routing Mark: ISP-1-Only					

Mangle Rule <8.8.4.4>						Mangle Rule <8.8.4.4>					
General	Advanced	Extra	Action	Statist		General	Advanced	Extra	Action	Statist	
Chain: output						Action: mark routing					
Src. Address:						☐ Log					
Dst. Address: 8.8.4.4						Log Prefix:					
Protocol: 1 (icmp)						New Routing Mark: ISP-2-Only					
Src. Port:						☒ Passthrough					



Netwatch / Routing Tables

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

	Dst. Address	Gateway	Distance	Routing Mark
AS	0.0.0.0/0	pppoe-out1 reachable	1	ISP-1-Only
SB	0.0.0.0/0		100	ISP-1-Only

2 items out of 10

	Dst. Address	Gateway	Distance	Routing Mark
AS	0.0.0.0/0	pppoe-out2 reachable	1	ISP-2-Only
SB	0.0.0.0/0		100	ISP-2-Only

2 items out of 10



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

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address

Tracking

	Src. Address	Dst. Address	Protocol	Conn
C	0.0.0.0:5678	255.255.255.255:5678	17 (udp)	
C	10.10.0.90:51351	255.255.255.255:20...	17 (udp)	
C	10.10.0.90:59215	255.255.255.255:20...	17 (udp)	
C	10.10.0.90:61343	255.255.255.255:20...	17 (udp)	
C	10.10.0.90:61571	255.255.255.255:20...	17 (udp)	
C	10.10.0.90:63628	255.255.255.255:20...	17 (udp)	
C	10.10.0.90:63631	255.255.255.255:20...	17 (udp)	
C	10.10.0.95:39349	255.255.255.255:5678	17 (udp)	
C	10.10.0.101:5678	255.255.255.255:5678	17 (udp)	
C	10.10.0.132:57090	255.255.255.255:5678	17 (udp)	
SC	192.168.200.254	8.8.8.8	1 (icmp)	
SC	192.168.200.254	8.8.4.4	1 (icmp)	

Torch (Running)

Basic

Interface: pppoe-out1

Entry Timeout: 00:00:03 s

Collect

☒ Src. Address ☒ Src. Address6

☒ Dst. Address ☒ Dst. Address6

☐ MAC Protocol ☐ Port

☐ Protocol ☐ VLAN Id

☐ DSCP

Et	Prot	Src	Dst
800 (ip)		8.8.8.8	192.168.200.254
800 (ip)		8.8.4.4	192.168.200.254

One should read "SCs"

Both tests answered to same src IP



Netwatch / Malformed Packets

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

Firewall				
Filter Rules NAT Mangle Raw Service Ports Conne				
+ - ✓ ✗ [icon] [icon] [icon] Reset Counters				
#	Action	Chain	Src. Address	
0	ISP-1 Test Helper masquerade	srcnat		
1	ISP-2 Test Helper masquerade	srcnat		
2	ISP-1 NAT masquerade	srcnat		
3	ISP-2 NAT masquerade	srcnat		

NAT Rule <>

General Advanced Extra Action ...

Chain: srcnat

Src. Address:

Dst. Address:

OK

Cancel

Apply

Disable

NAT Rule <>

Advanced Extra Action Statistics ...

Action: masquerade

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark: ☐ ISP-1-Only

Reset Counters

Reset All Counters

OK

Cancel



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

- ChangIP script controls public IP
- FQDN shall point to preferred ISP
- Modify ChangIP script
- Update IP independent from outgoing interface
- Use interface from global variable instead

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



Changelp 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

Schedule <Schedule ChangeIP>

Name: Schedule ChangeIP

Start Date: Apr/03/2018

Start Time: startup

Interval: 00:10:00

Owner: admin

Policy:

- ☒ ftp
- ☒ read
- ☒ policy
- ☒ password
- ☒ sensitive
- ☐ dude
- ☒ reboot
- ☒ write
- ☒ test
- ☒ sniff
- ☒ romon

Run Count: 135

Next Run: Apr/03/2018 10:59:27

On Event: ChangeIP

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

Name	Start Date	Start Time	Interval	Owner	Run Count	Next Run	On Event
Schedule ChangeIP	Apr/03/2018	startup	00:10:00	admin	135	Apr/03/2018 10:59:27	ChangeIP



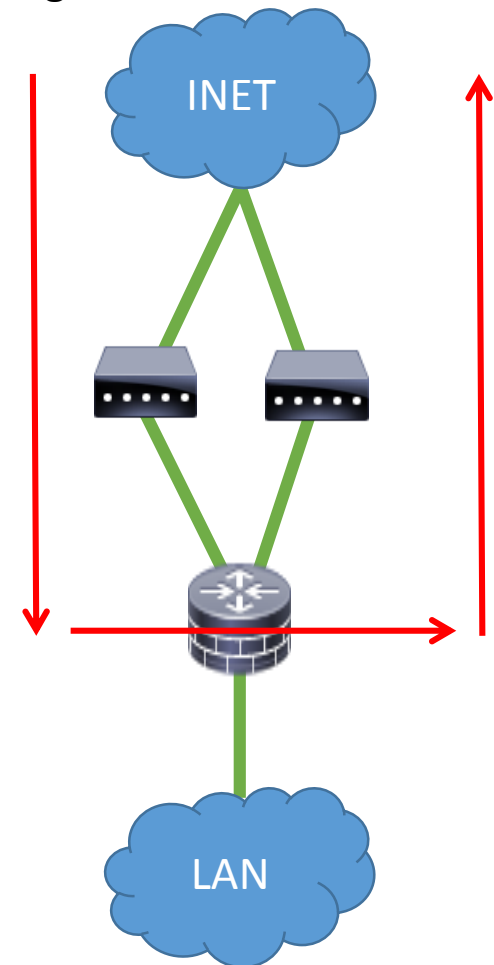
Outbound SSTP Packets

While both ISP are operational:

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

Inbound:
ChangIP

Outbound:
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

Mangle Rule <>

General Advanced Extra Action Statistics

Chain: prerouting

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface: ☐ pppoe-out1

Out. Interface:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Mangle Rule <>

General Advanced Extra Action Statistics

Action: mark connection

☐ Log

Log Prefix:

New Connection Mark: connectionmark-sstp

Connection Type:

Connection State: ☐ invalid ☐ established ☐ related ☒ new ☐ untracked

OK

Cancel

Apply

Disable

Comment



Routing Mark for SSTP Connections

The image displays two screenshots of the Mikrotik WinBox Mangle Rule configuration window, illustrating the steps to configure a routing mark for SSTP connections.

Top Screenshot (Chain Configuration):

- Chain: **output**
- Src. Address: (empty)
- Dst. Address: (empty)

Bottom Screenshot (Action Configuration):

- Action: **mark routing**
- ☐ Log
- Log Prefix: (empty)
- New Routing Mark: **ISP-1-Only**
- In. Interface List: (empty)
- Out. Interface List: (empty)
- Packet Mark: (empty)
- Connection Mark: ☐ **connectionmark-sstp**

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

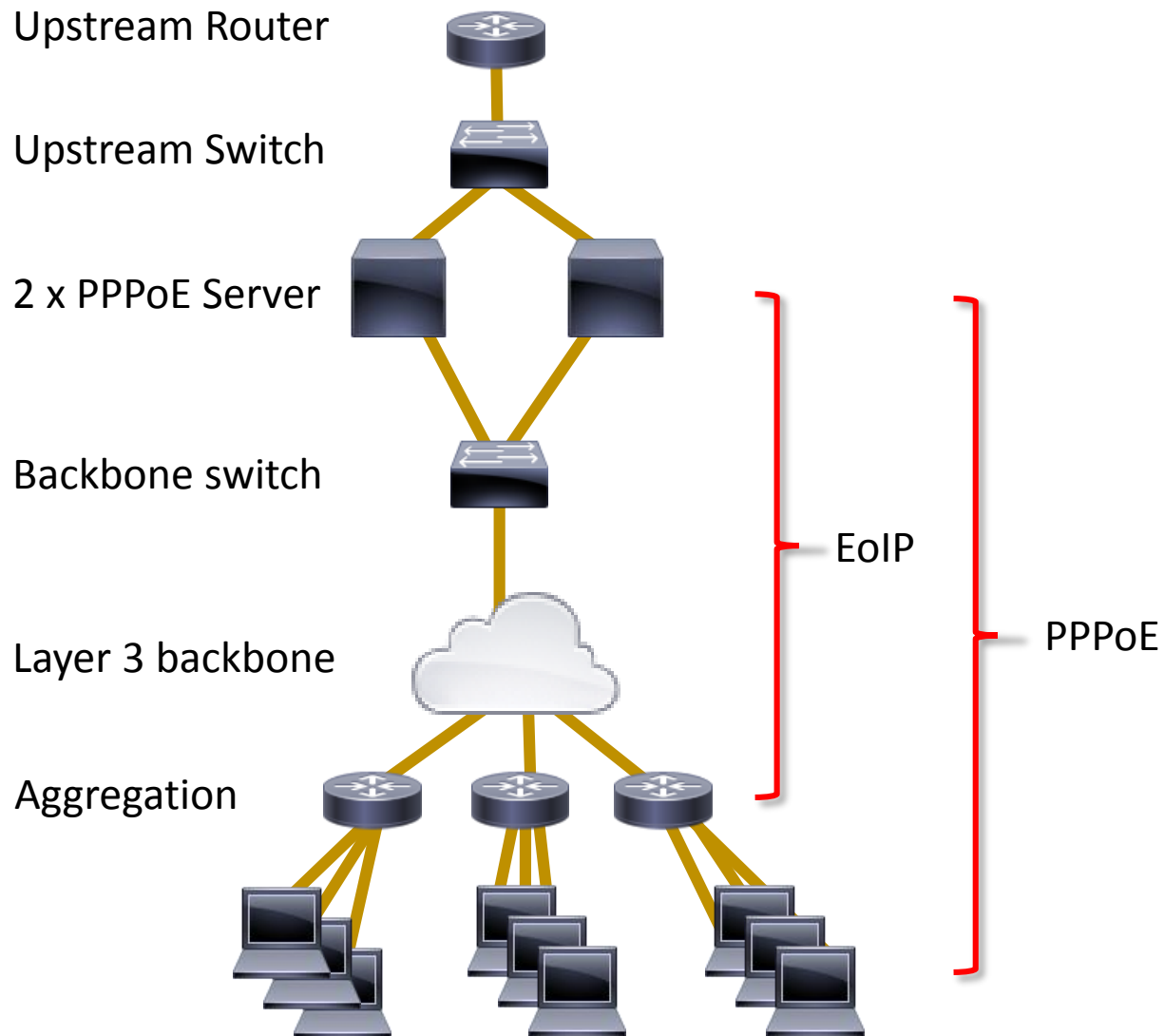


PPPoE Access Concentrator

EoIP Approach



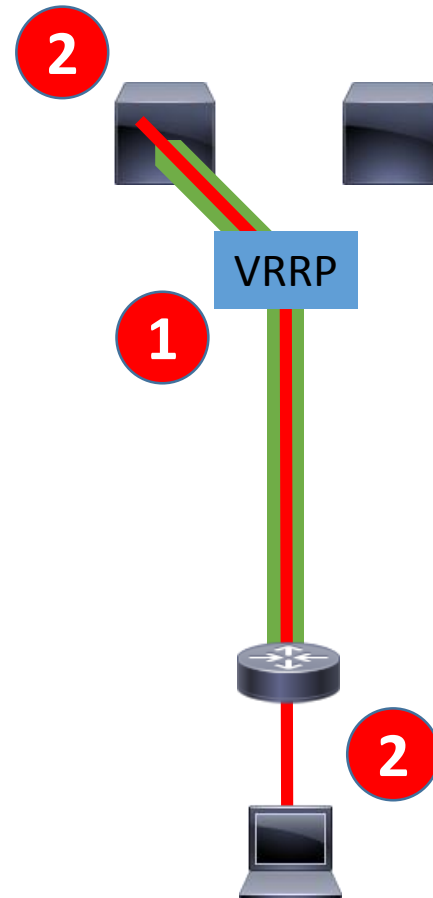
Overview





Failover (Backbone)

- 1** EoIP Tunnel
endpoint = VRRP
IP address
- 2** Multiple PPPoE
tunnels through
each EoIP tunnel

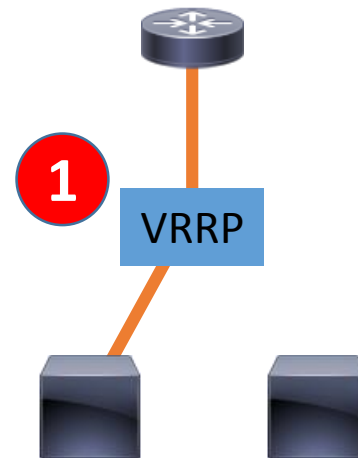




Failover (Upstream)

1

Upstream ISP will route networks to external VRRP IP





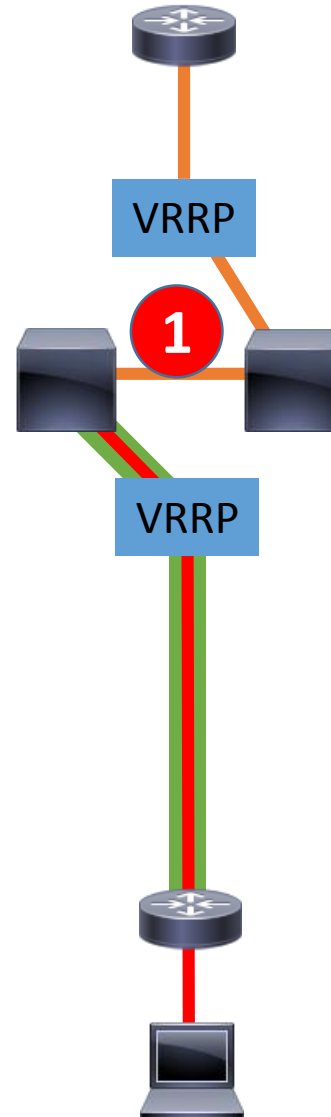
Asymmetric VRRP / Radius

BRAS:

- failover
- No loadbalancing

RADIUS

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



1 Crosslink with static routes *

* See first VPN setup

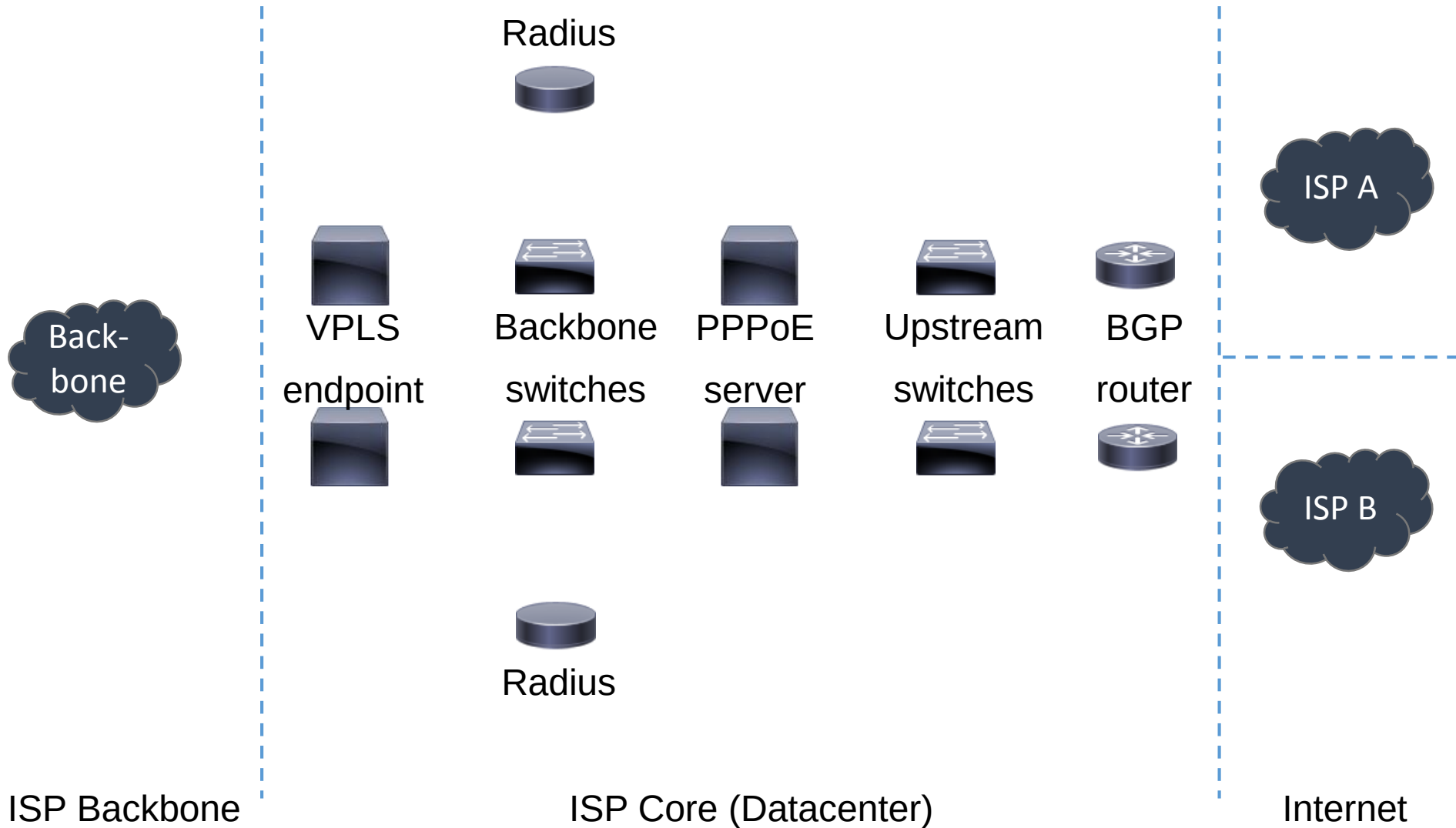


PPPoE Access Concentrator

VPLS Approach

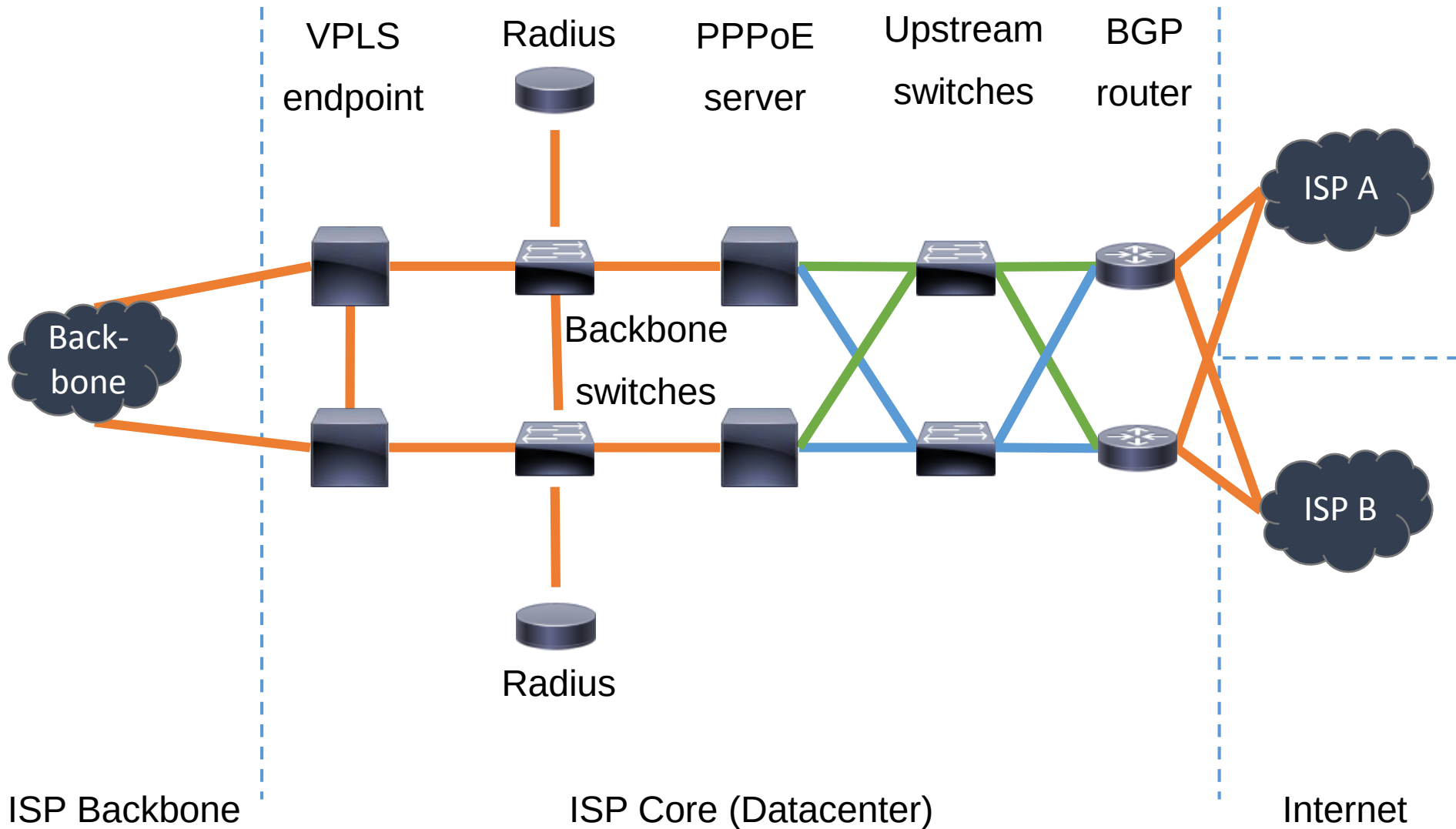


High Available ISP Network





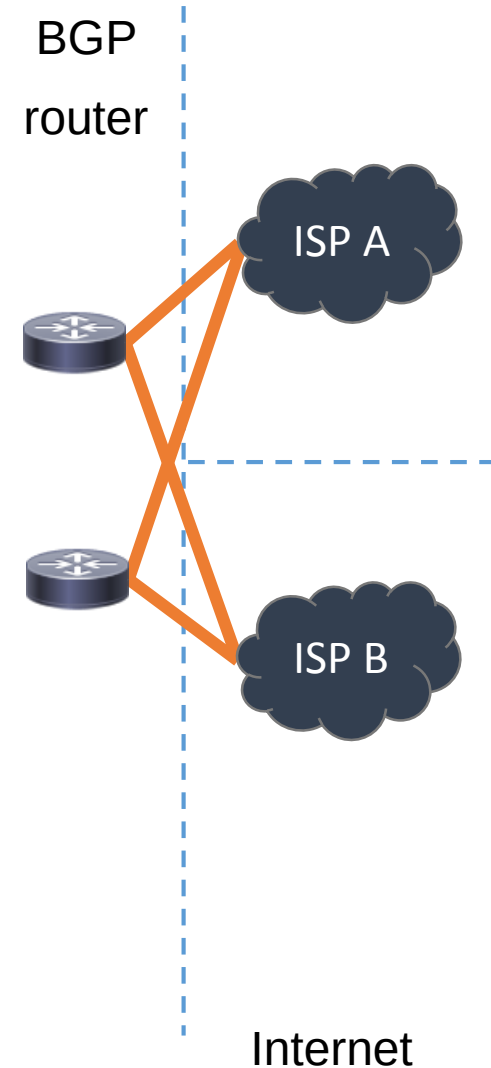
High Available ISP Network





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

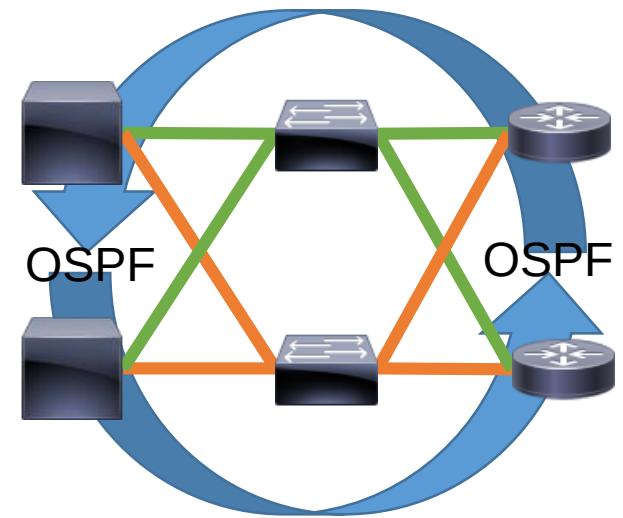




Routing

- 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

PPPoE
server Upstream
switches BGP
router



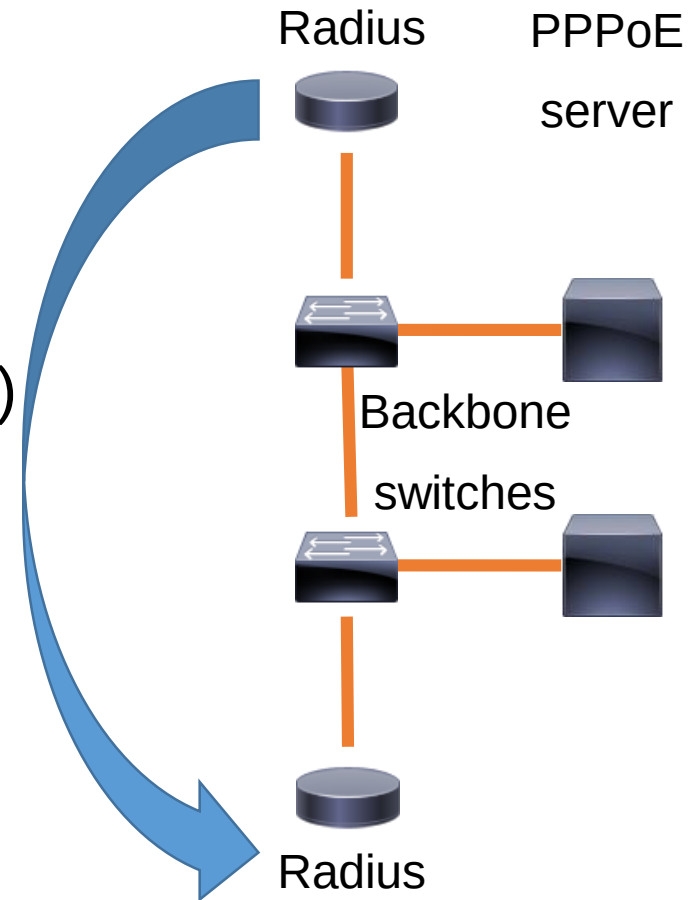


Redundant Radius Server

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

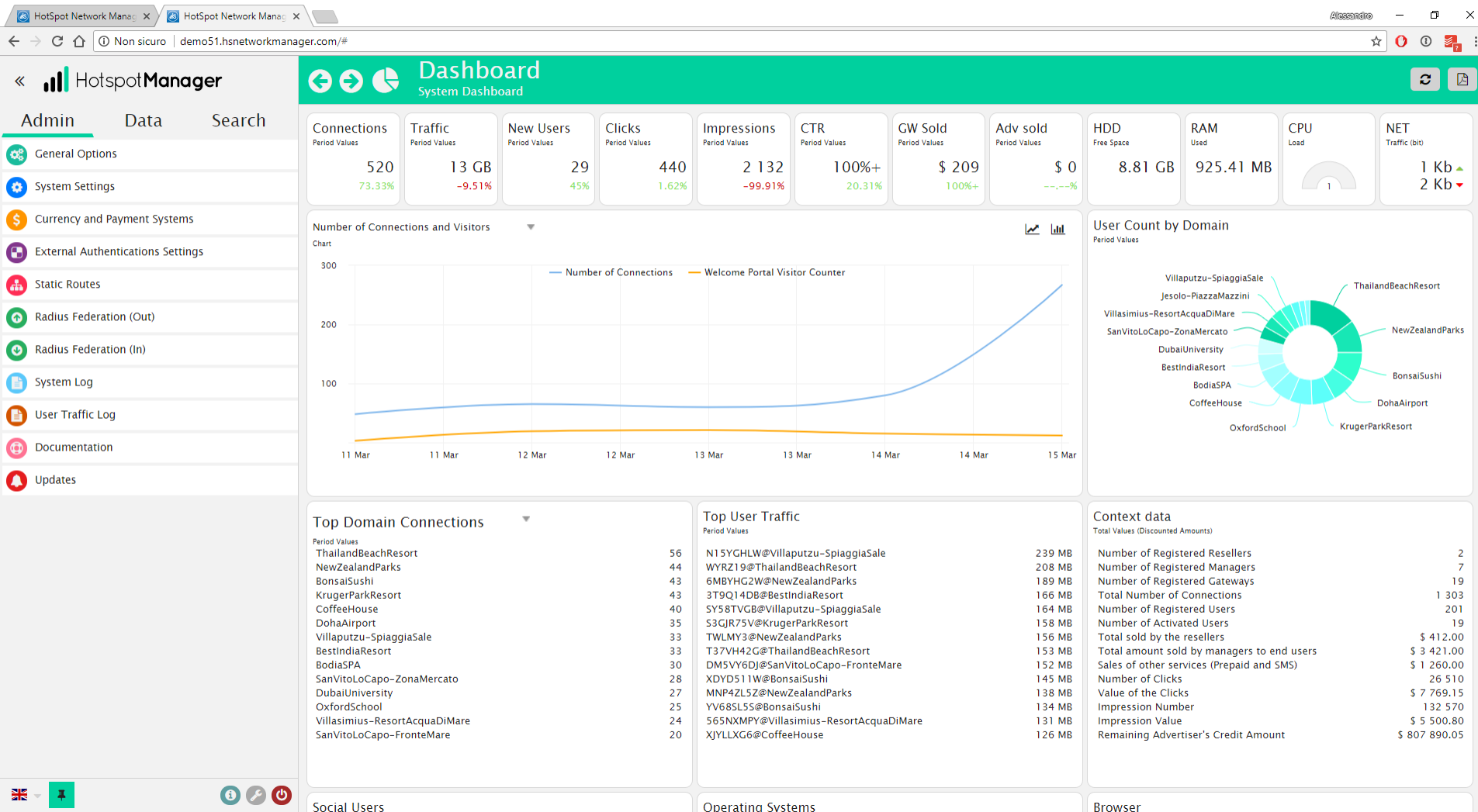
Ready to run alternative:

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





HS Network Manager

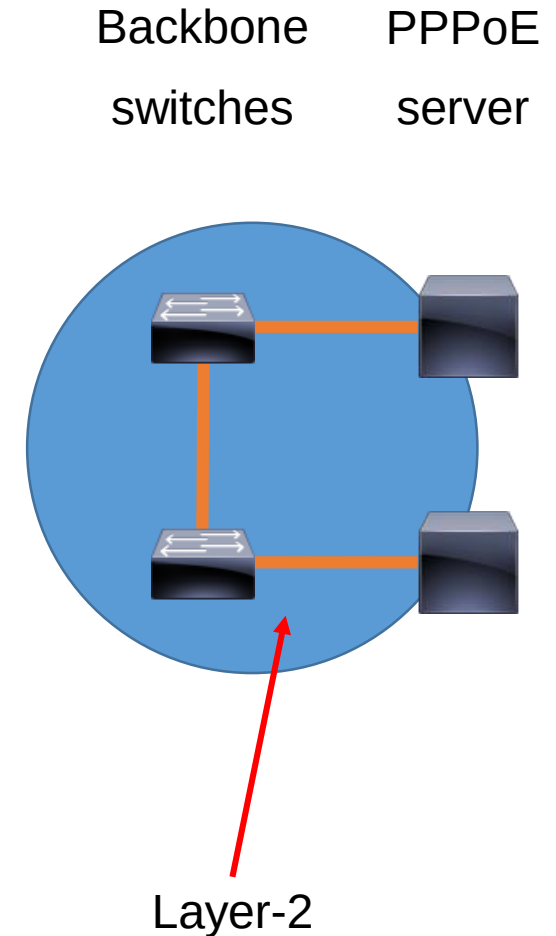


Looking for Captive Portal and PPPoE authentication? Contact sales@fmsweb.de



BRAS Loadbalancing

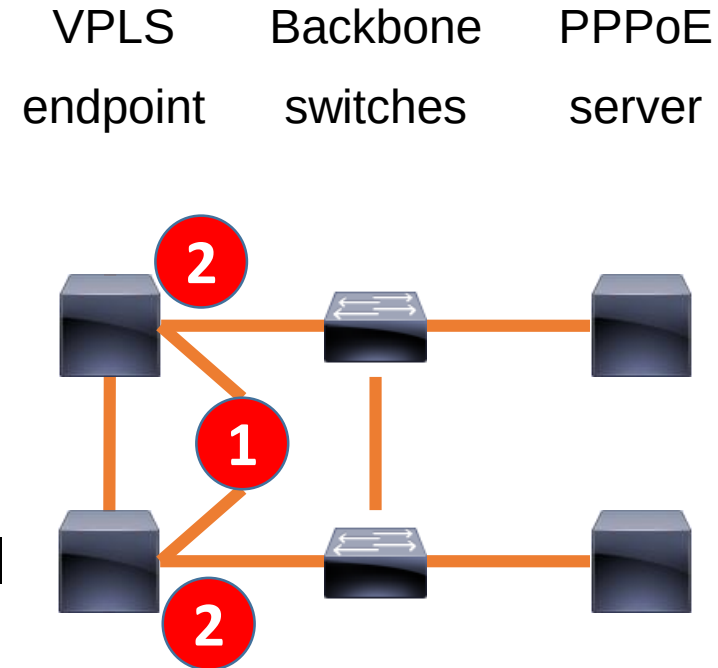
- Multiple BRAS in layer 2 network
- Works out off the box
- First come first serve
- PPPoE sessions will distribute across BRAS
- BRAS loadbalancing and failover





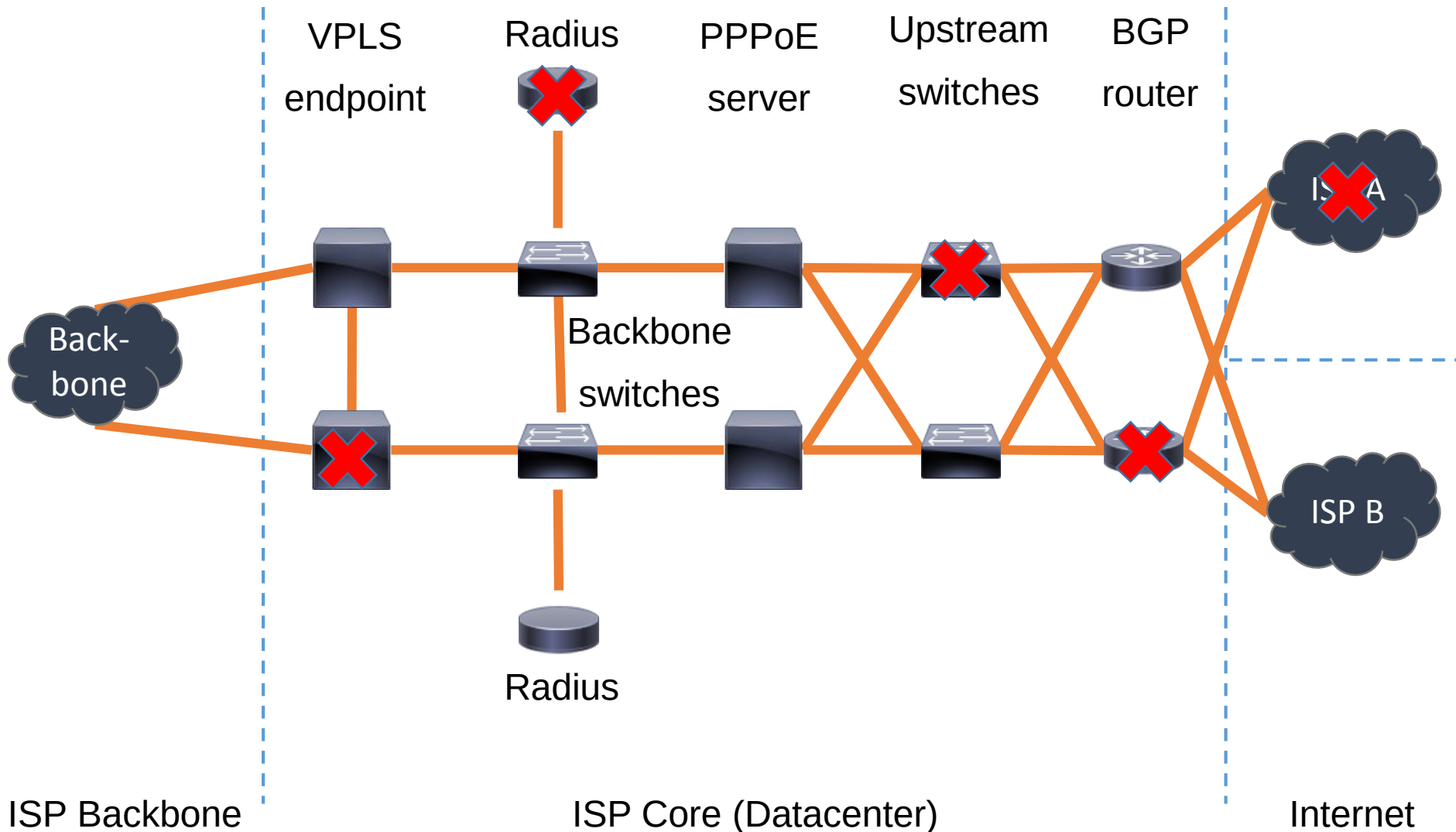
VPLS Concentrator Redundancy

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





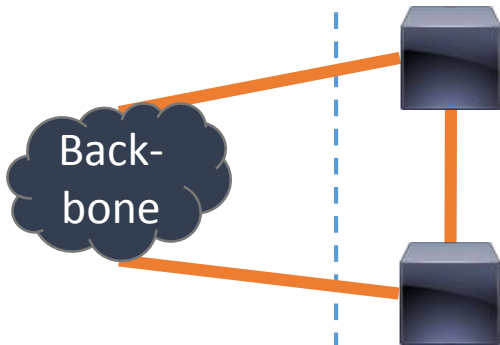
Still Operational with Loadbalancing





Presentation of Sebastian Inacker

VPLS
endpoint



Today 14:15

Presentation of Sebastian Inacker

“Use cases and pitfalls in
MPLS/VPLS networks”

Access all our presentations [here](#).

ISP Backbone



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