



Access Concentrators

Optimizing Availability and Performance



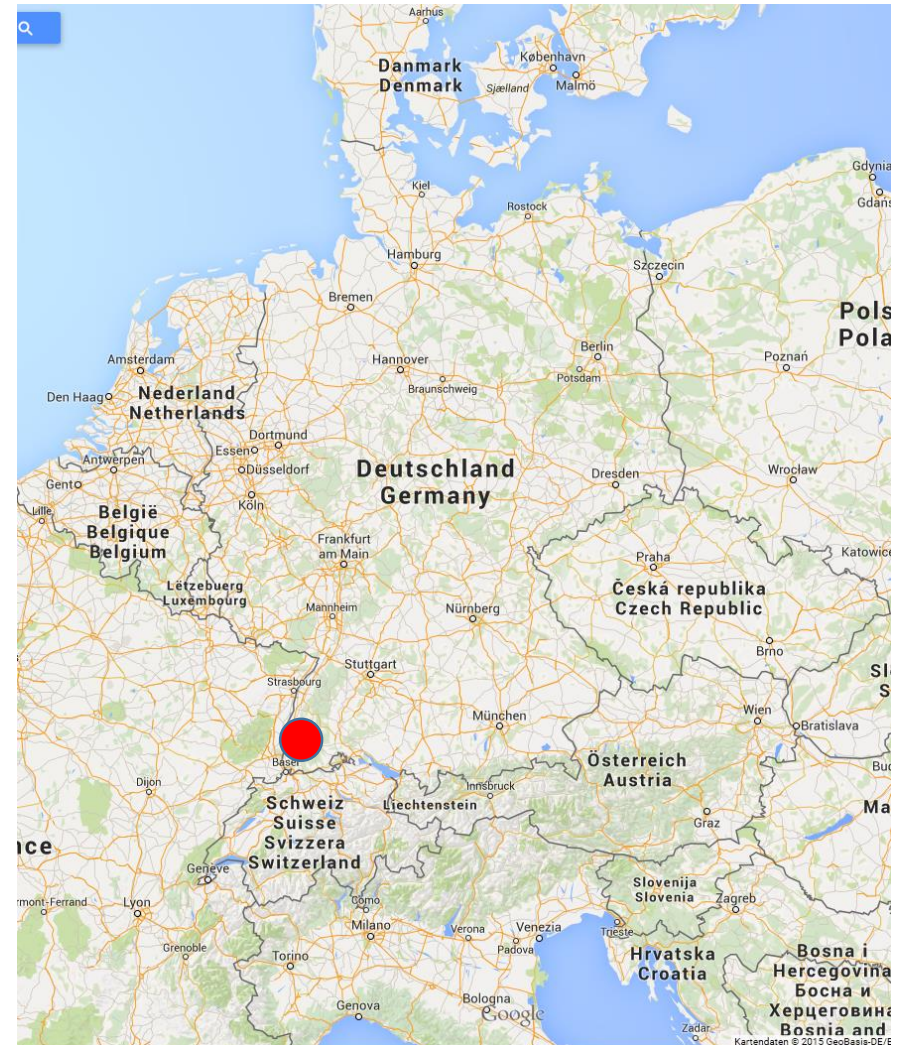
FMS Internetservice GmbH

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

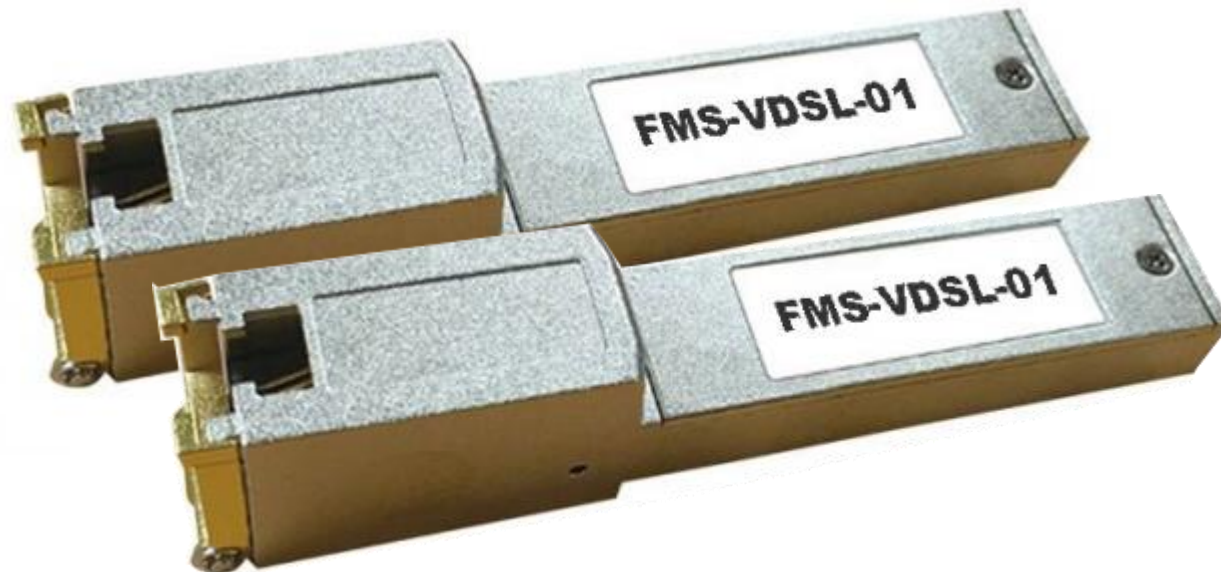




Distributor Table

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

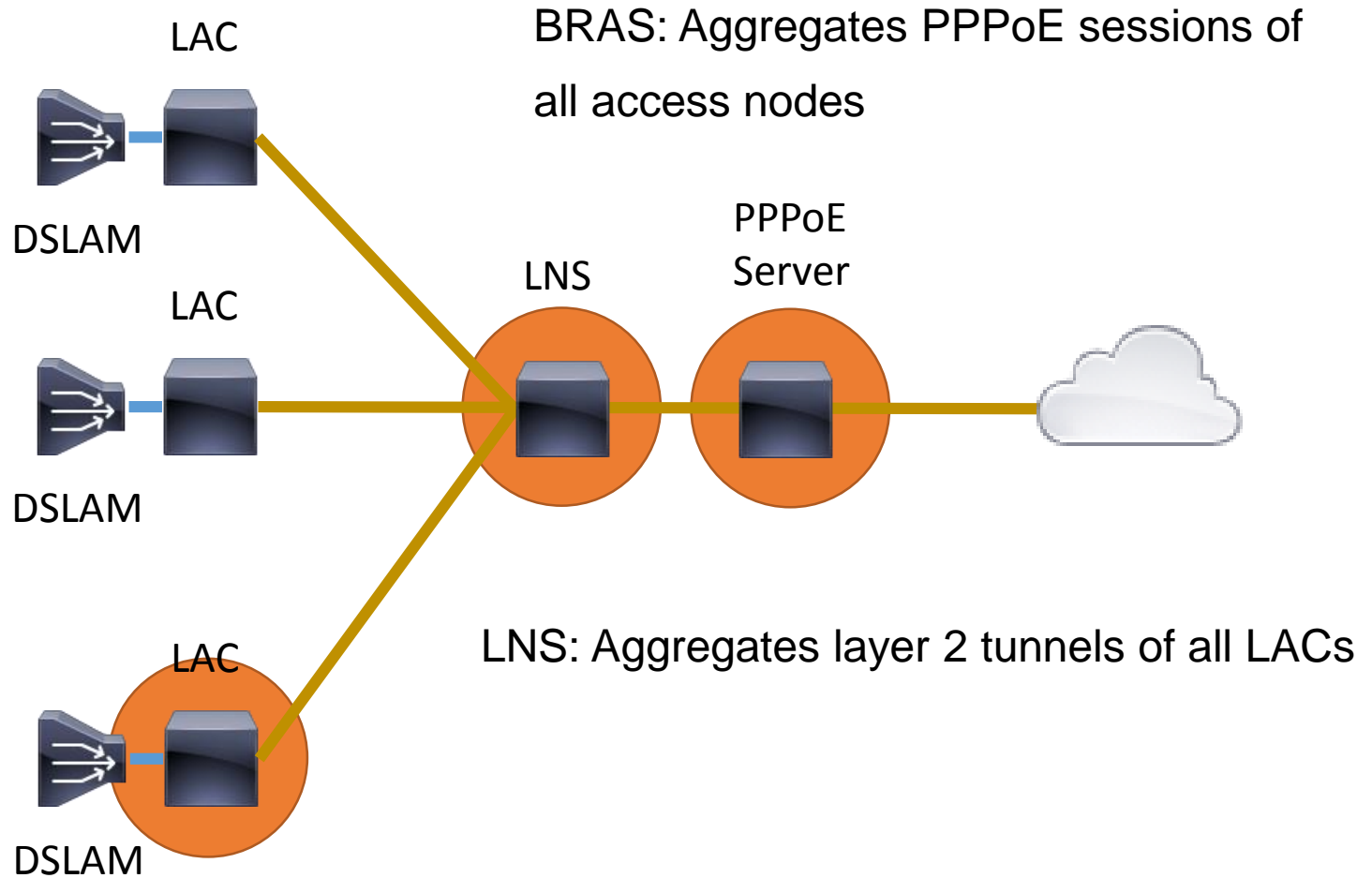
- Remote access concentrator
 - Used in dial up networks
 - ISDN / POTS

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

- VPN Server
- BRAS (PPPoE Server)



Multiple Access Concentrators



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

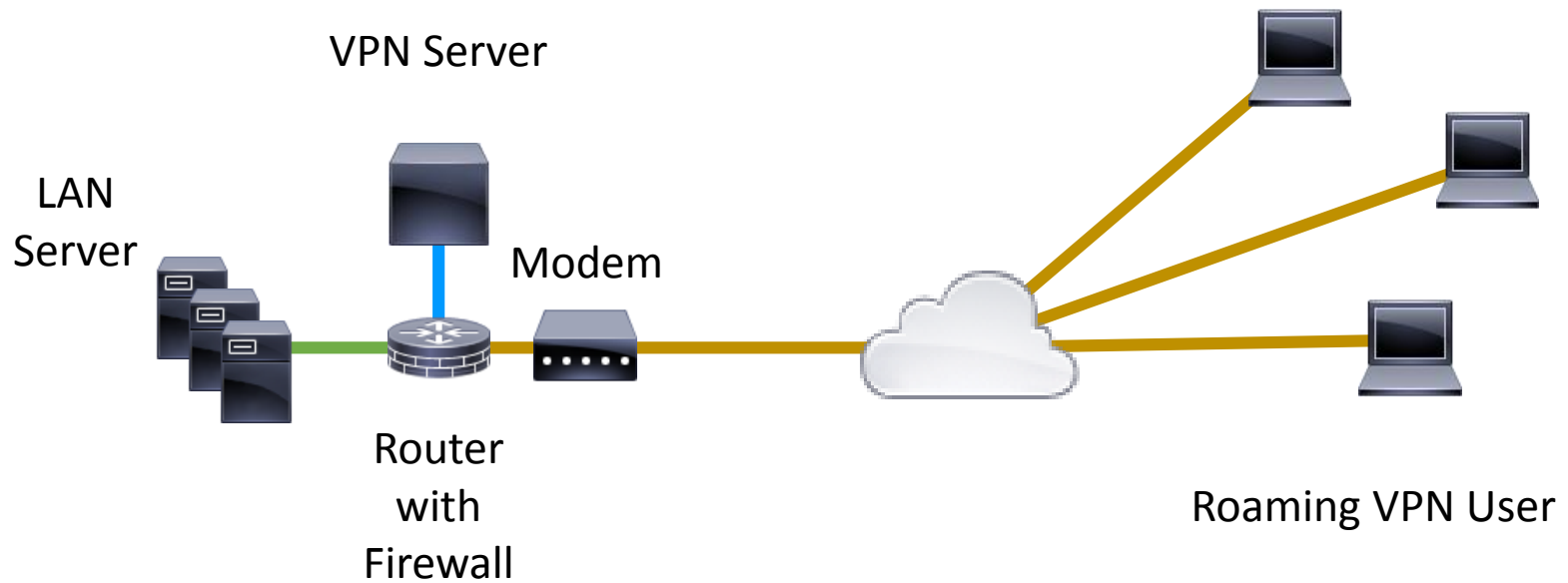


Enterprise Networks

VPN Access Concentrators

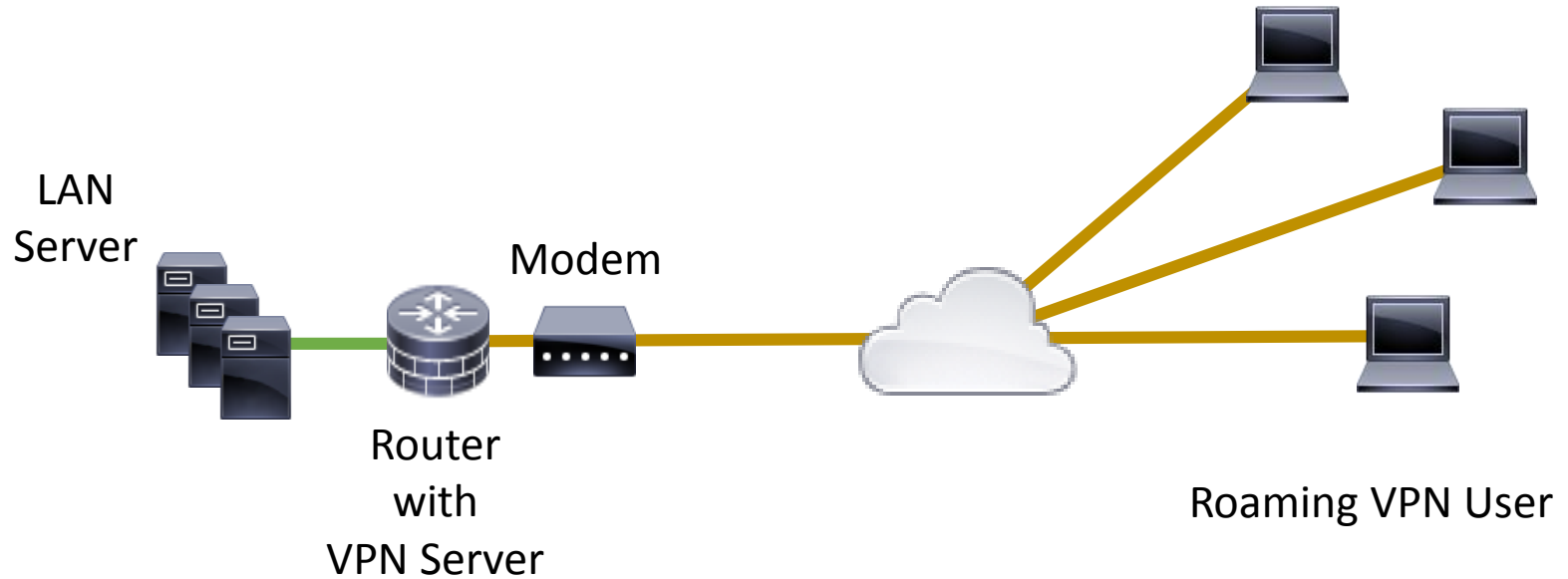


Enterprise VPN with DMZ





Enterprise VPN without DMZ



Single points of failure:

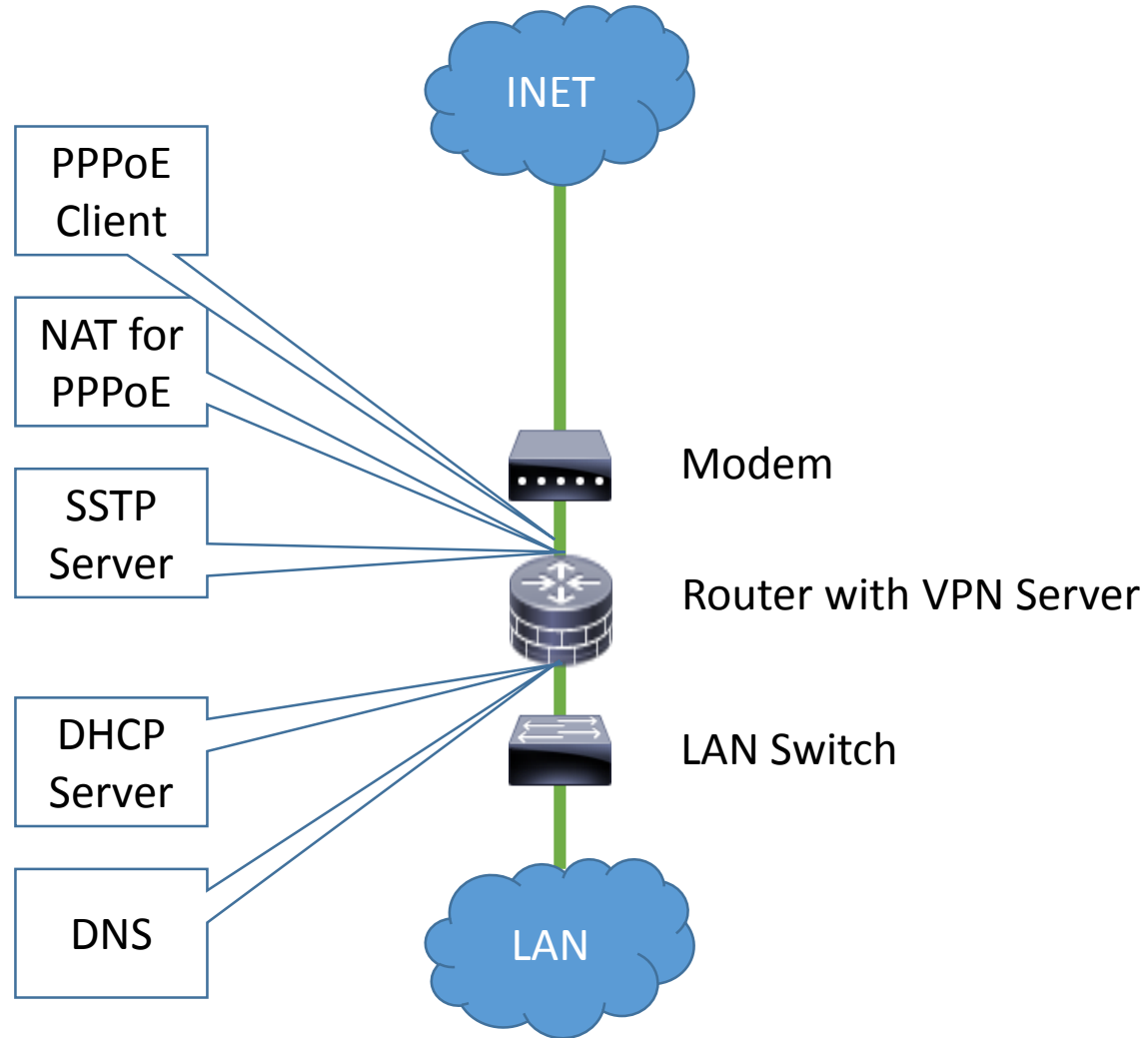
- VPN server
- broadband line



Broadband VPN Gateway

Assumptions:

- Basic setup present
- Not discussed unless special considerations necessary



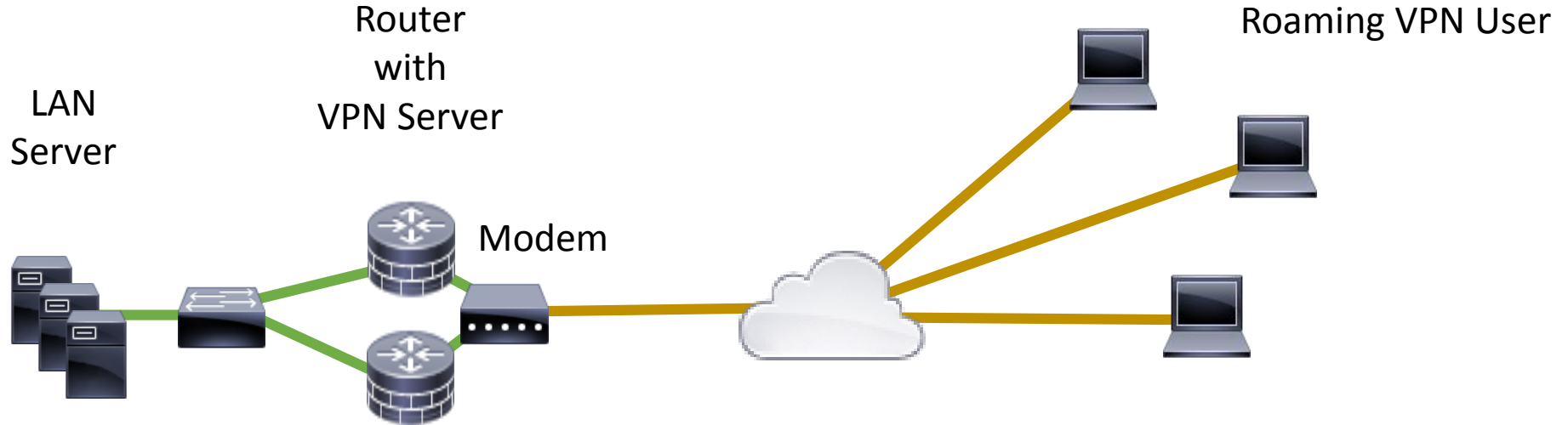


Enterprise VPN

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

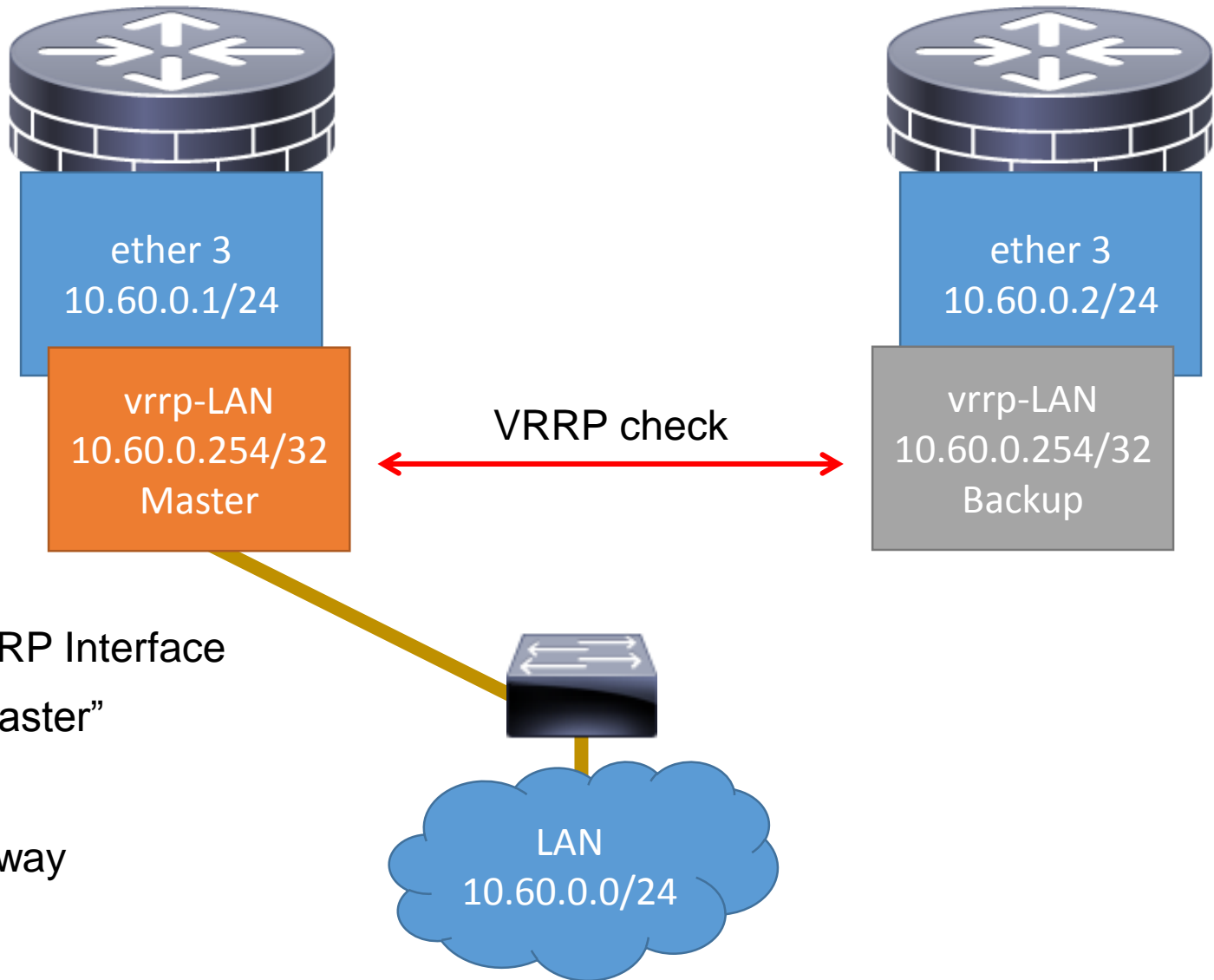
- LAN devices will not support dynamic routing
- Default Gateway IP cannot change
- Both Gateways have to share the same IP

- VRRP
- Virtual Router Redundancy Protocol

- Master and Backup router (interface) share IP



Redundant Default Gateway



Only one VRRP Interface
"Running Master"

Default Gateway
10.60.0.254



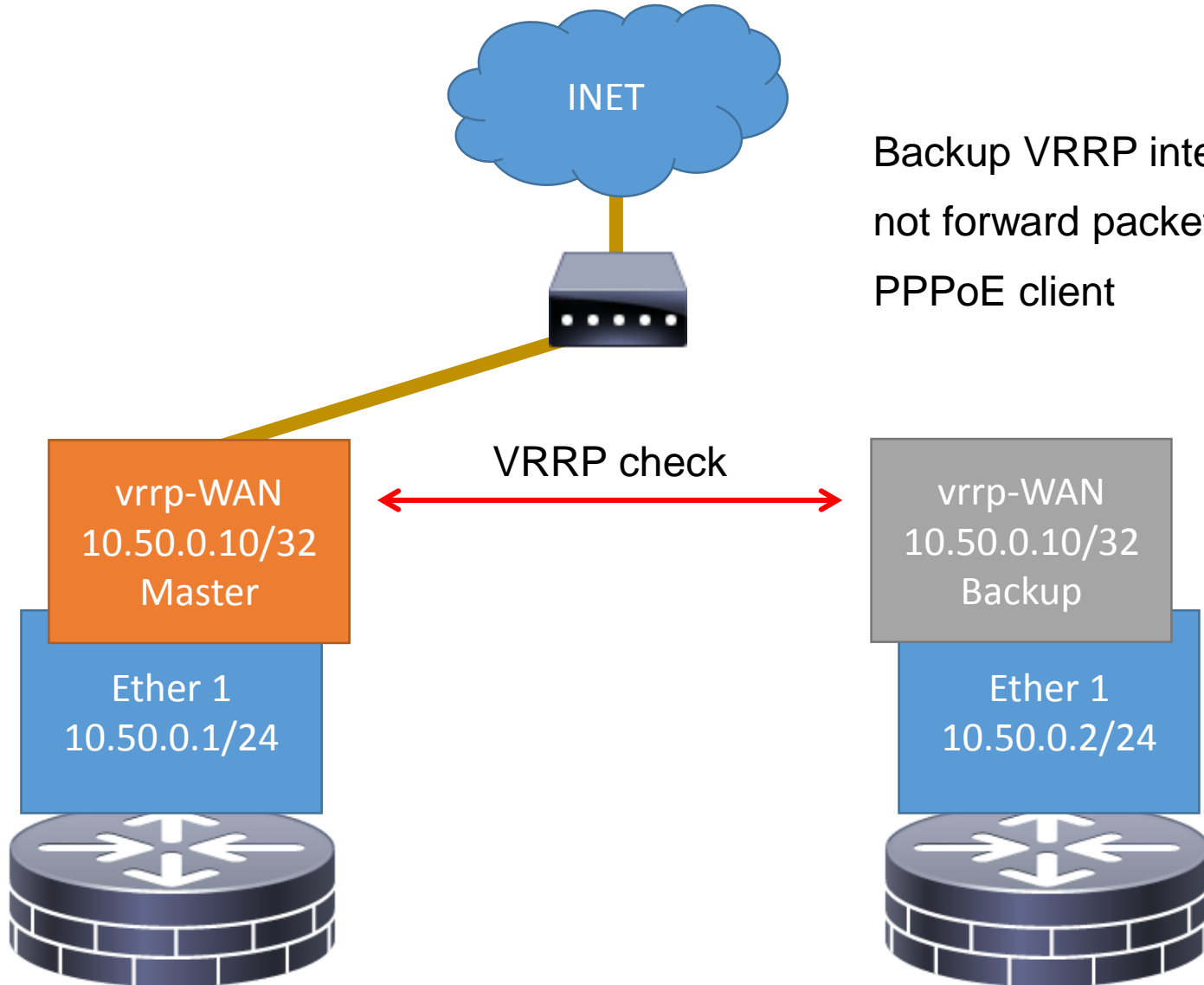
Switching PPPoE Client

- 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

Interface List

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

Route List

Routes	Nexthops	Rules	VRF
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	10.50.0.0/24	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

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

Route List

Routes	Nexthops	Rules	VRF
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 interface. The top window, titled "Address List", shows a table of IP addresses and their associated interfaces. The bottom window, titled "Interface <vmp-LAN>", shows the configuration for the VRRP group on the vmp-LAN interface.

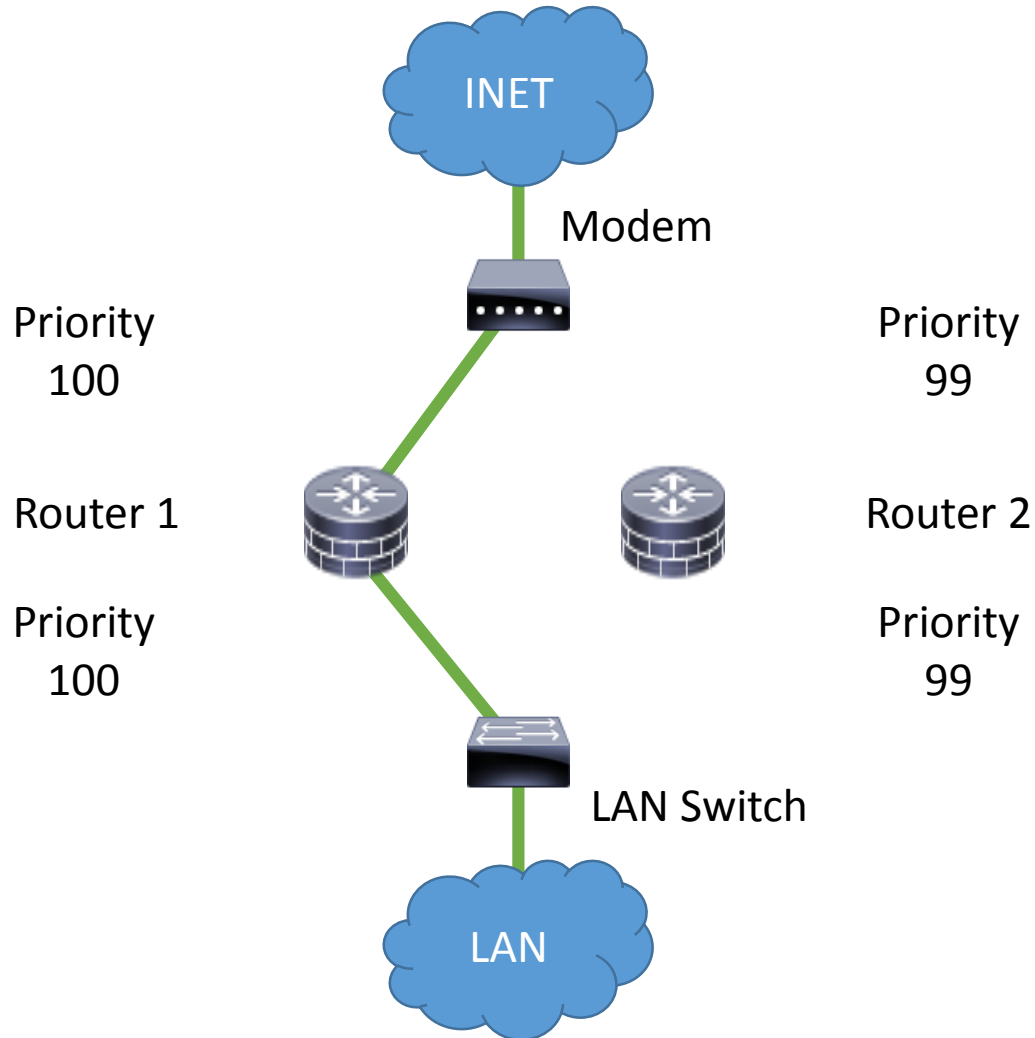
	Address	Network	Interface
D	10.40.0.255	192.168.0.48	pppoe-out1
	10.50.0.1/24	10.50.0.0	ether1
	10.50.0.10	10.50.0.10	vmp1
	10.60.0.1/24	10.60.0.0	ether3
	10.60.0.254	10.60.0.254	vmp-LAN
	10.70.0.1/24	10.70.0.0	ether4
D	192.168.0.37/24	192.168.0.0	ether2

The "Interface <vmp-LAN>" window shows the following configuration:

- Interface: ether3
- VRID: 20
- Priority: 100
- Interval: 1.00 s
- Preemption Mode
- Authentication: none
- Password: (empty)
- Version: 3
- V3 Protocol: IPv4

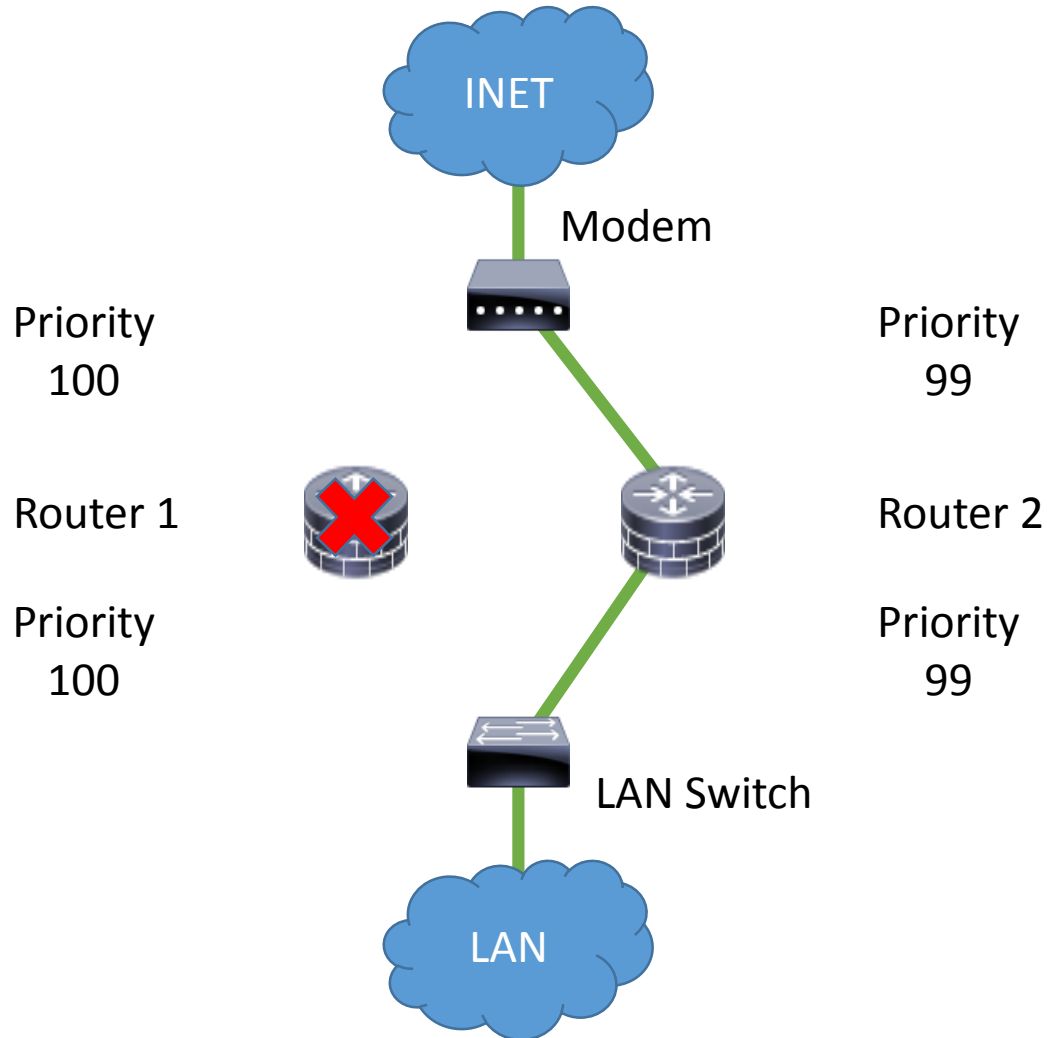


Router 1 VRRP Master





Router 2 VRRP Master





Asymmetric VRRP

Inbound traffic

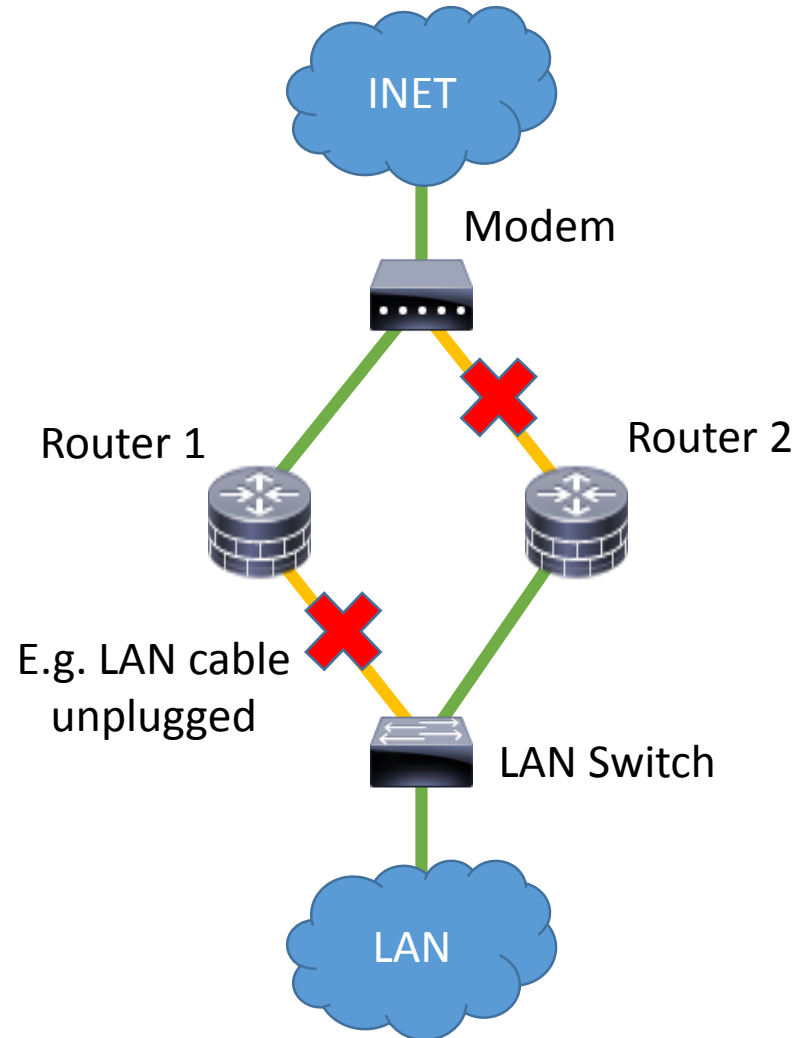


No LAN connection

No PPPoE connection



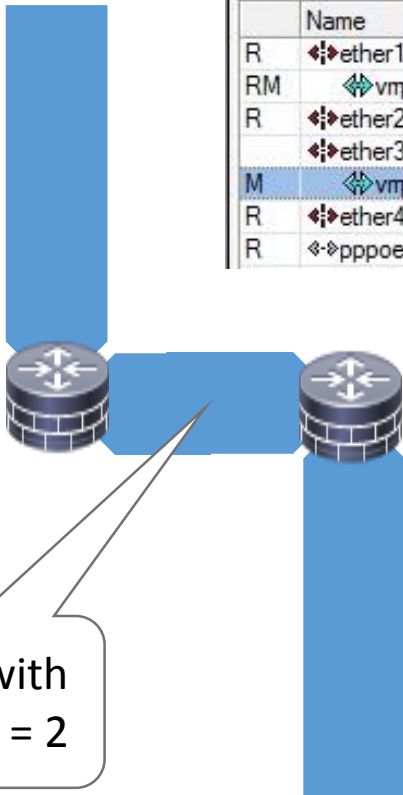
Outbound traffic





Asymmetric VRRP

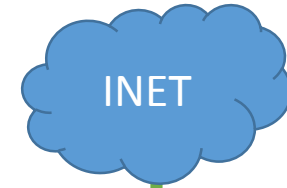
INET



Routes with distance = 2

LAN

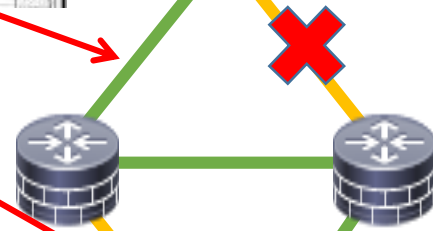
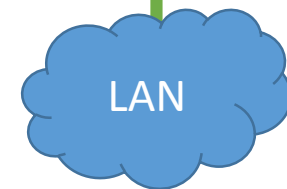
	Name	Type	Actual MTU	L2 M
R	ether1	Ethernet	1500	
RM	vmp1	VRRP	1500	
R	ether2	Ethernet	1500	
R	ether3	Ethernet	1500	
M	vmp-LAN	VRRP	1500	
R	ether4	Ethernet	1500	
R	pppoe-out1	PPPoE Client	1480	



Modem

E.g. LAN cable unplugged

LAN Switch





Routing ether4 Crosslink

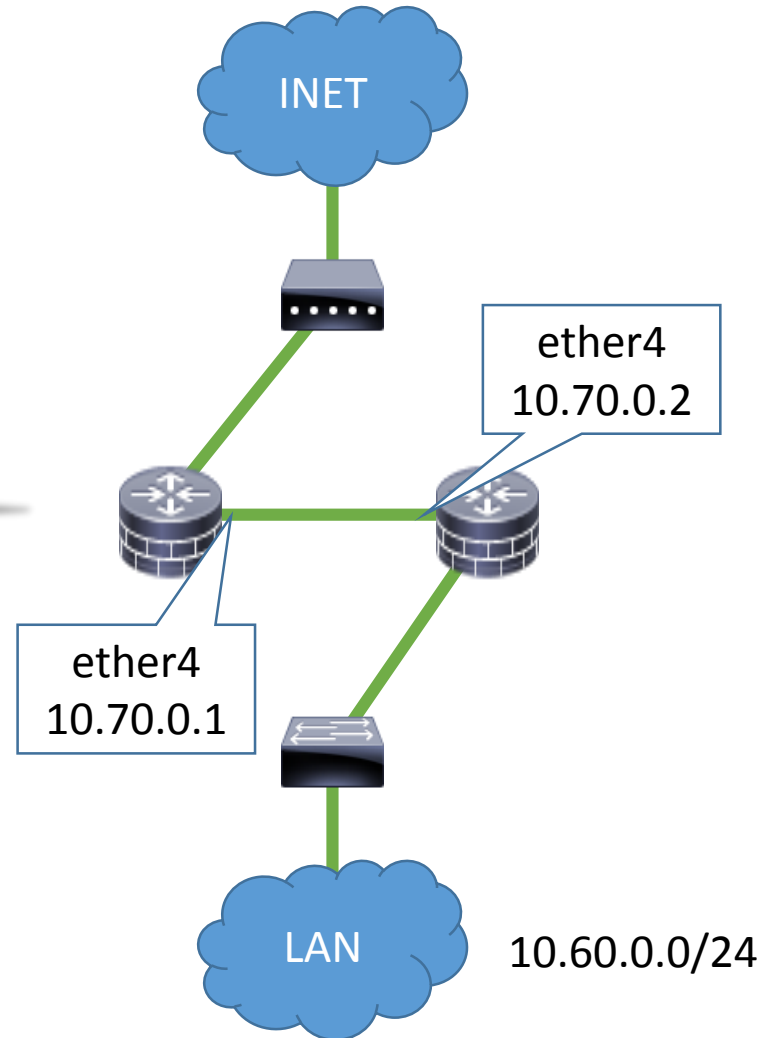
Route List

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)



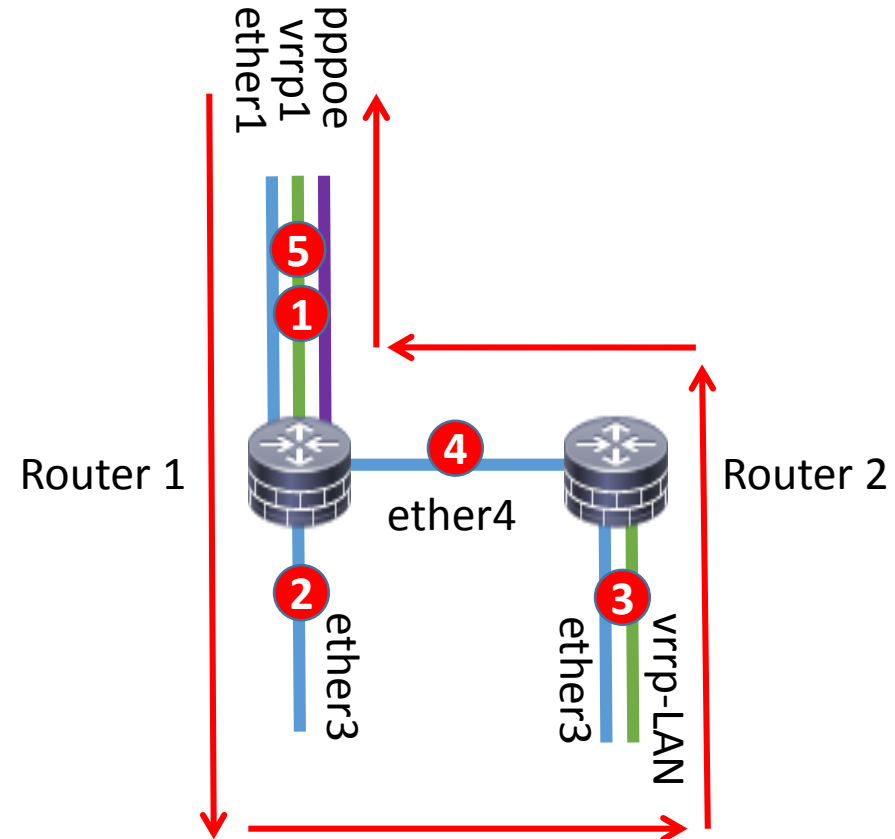


Cable replugged but no Preemption

20Mbps bidirectional BW test

The screenshot shows two instances of the WinBox 'Interface List' window. The top window shows Router 1's interface statistics, and the bottom window shows Router 2's interface statistics. Red circles with numbers 1 through 5 highlight specific data points in both windows.

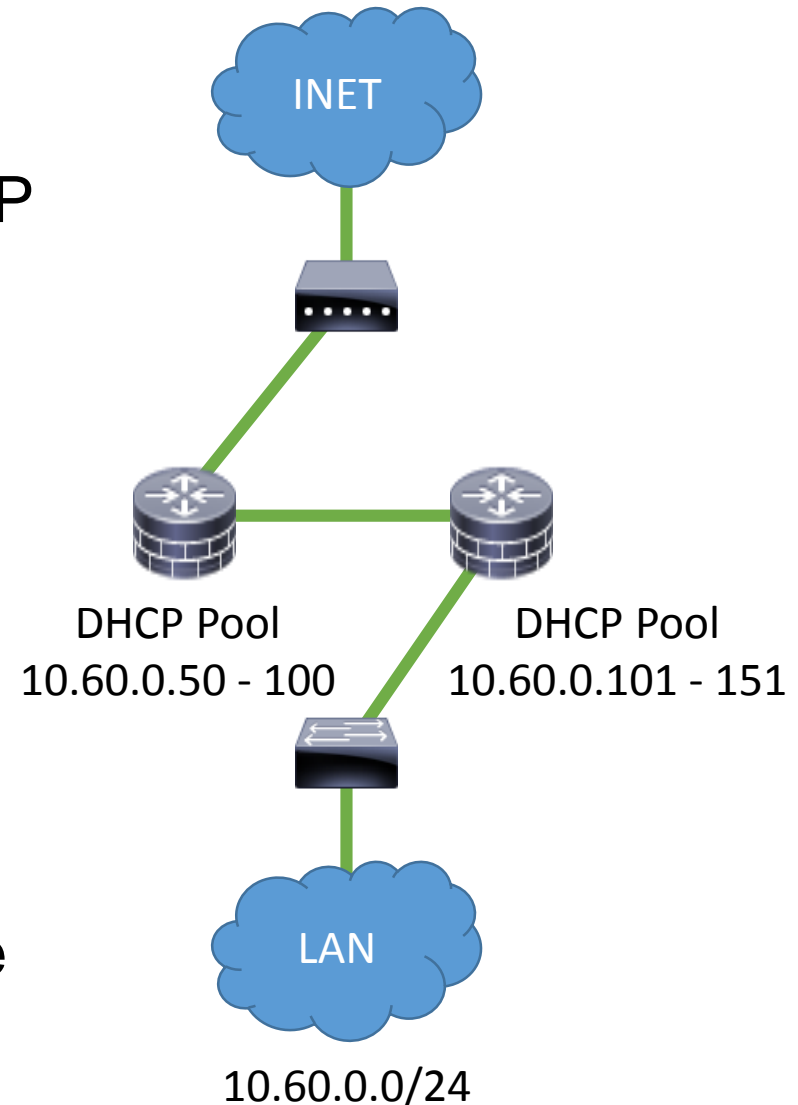
Router	Name	Type	Tx	Rx	Highlight
1	ether1	Ethernet	21.7 Mbps	21.6 Mbps	5
1	vmp1	VRRP	21.5 Mbps	21.3 Mbps	1
1	ether2	Ethernet	75.3 kbps	12.7 kbps	2
1	ether3	Ethernet	21.4 Mbps	512 bps	2
1	vmp-LAN	VRRP	0 bps	0 bps	1
1	ether4	Ethernet	0 bps	21.6 Mbps	1
1	pppoe-out1	PPPoE Client	21.0 Mbps	20.8 Mbps	5
2	ether1	Ethernet	0 bps	960 bps	
2	vmp-WAN	VRRP	0 bps	0 bps	
2	ether2	Ethernet	72.8 kbps	12.4 kbps	
2	ether3-LAN	Ethernet	512 bps	21.7 Mbps	3
2	vmp-LAN	VRRP	368 bps	21.4 Mbps	4
2	ether4	Ethernet	21.7 Mbps	0 bps	
2	ether5	Ethernet	0 bps	0 bps	
2	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

USB Power Reset

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 ddnspass "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=$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

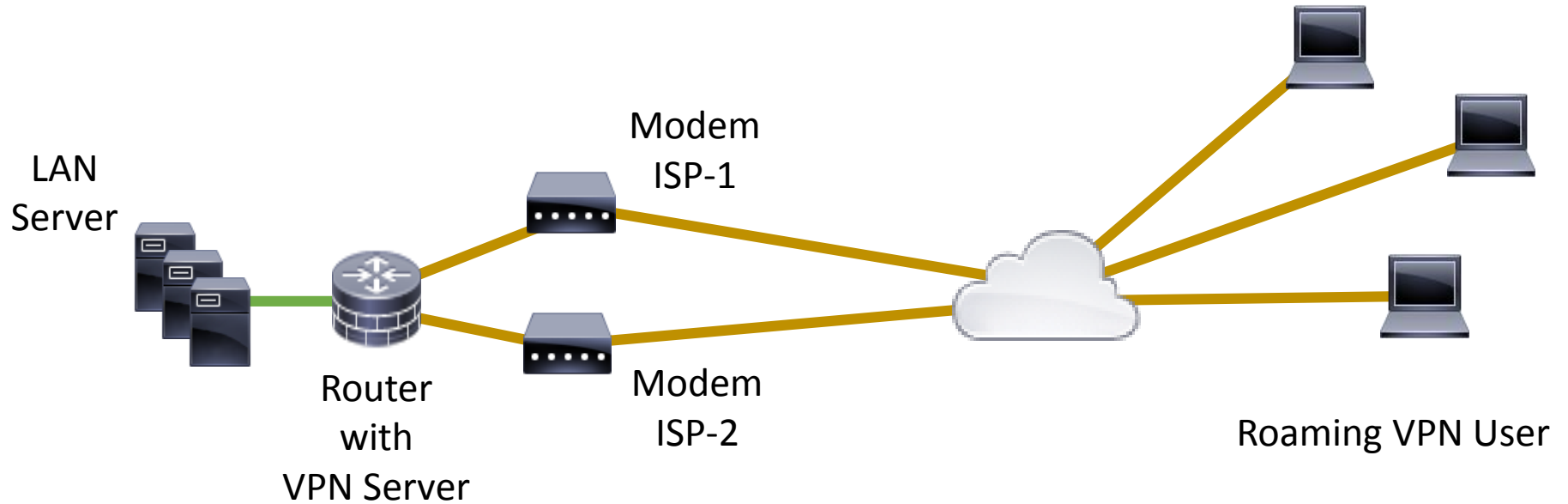


Enterprise VPN

Redundant Access Lines



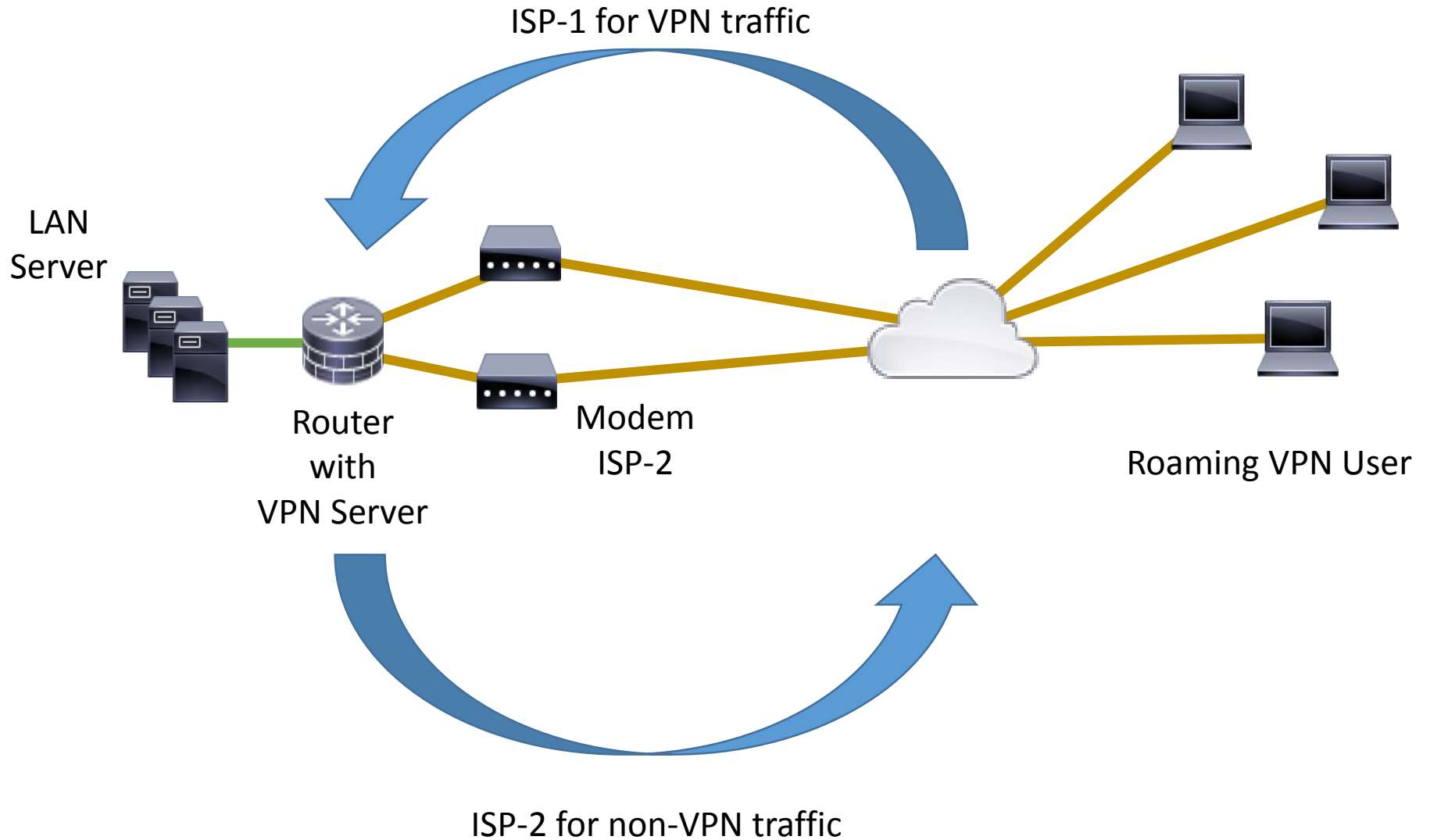
Overview



- two DSL lines (PPPoE)
- Dynamic public IPs



Overview





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

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

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



Failover ISP2 -> ISP1

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

PPP configuration window showing a table of entries:

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

Route List window showing a table of routes:

	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)	

The screenshot displays four configuration windows for Mangle Rules in Mikrotik WinBox. The top-left window is for rule <8.8.8.8> with fields: Chain: output, Dst. Address: 8.8.8.8, Protocol: 1 (icmp). The top-right window is for rule <8.8.8.8> with fields: Action: mark routing, New Routing Mark: ISP-1-Only. The bottom-left window is for rule <8.8.4.4> with fields: Chain: output, Dst. Address: 8.8.4.4, Protocol: 1 (icmp). The bottom-right window is for rule <8.8.4.4> with fields: Action: mark routing, New Routing Mark: ISP-2-Only, and Passthrough checked.



Netwatch / Routing Tables

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

Route List

Routes | Nexthops | Rules | VRF

Find: ISP-1-Only

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

2 items out of 10

Route List

Routes | Nexthops | Rules | VRF

Find: ISP-2-Only

	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	Conne
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)

Interface: pppoe-out 1

Entry Timeout: 00:00:03 s

Collect

- Src. Address
- Dst. Address
- MAC Protocol
- Protocol
- DSCP
- Src. Address6
- Dst. Address6
- Port
- VLAN Id

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

#	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	

The top screenshot shows the 'NAT Rule' dialog in the 'General' tab. The 'Chain' dropdown is set to 'srcnat'. The 'Src. Address' and 'Dst. Address' fields are empty. Buttons for 'OK', 'Cancel', 'Apply', and 'Disable' are visible.

The bottom screenshot shows the 'NAT Rule' dialog in the 'Advanced' tab. The 'Action' dropdown is set to 'masquerade'. The 'Routing Mark' dropdown is set to 'ISP-1-Only'. Other fields like 'Any. Port', 'In. Interface', 'Out. Interface', 'In. Interface List', 'Out. Interface List', 'Packet Mark', and 'Connection Mark' are empty. Buttons for 'OK', 'Cancel', 'Reset Counters', and 'Reset All Counters' are visible.



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

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

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



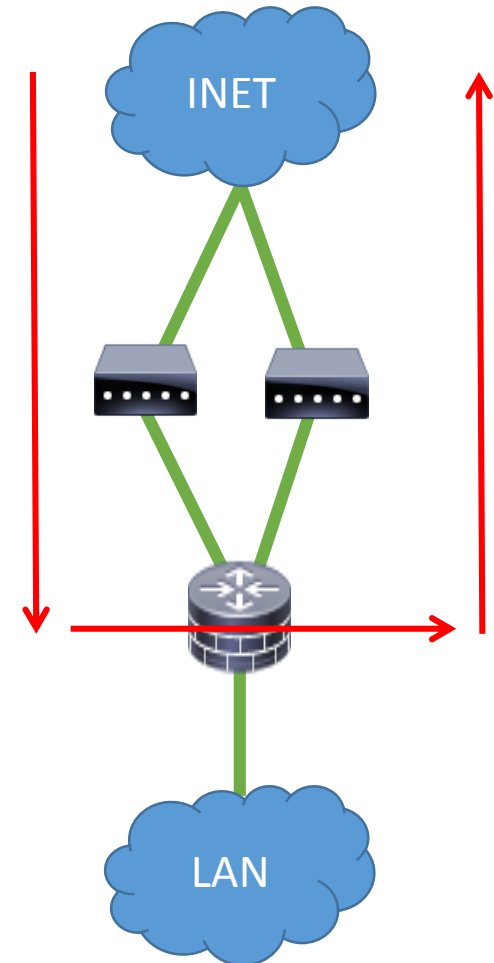
Outbound SSTP Packets

While both ISP are operational:

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

Inbound:
ChangelIP

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:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State: invalid established related new untracked

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

OK

Cancel

Apply

Disable

Comment



Routing Mark for SSTP Connections

The image displays two screenshots of the Mikrotik WinBox Mangle Rule configuration interface. The top screenshot shows the 'Chain' field set to 'output'. The bottom screenshot shows the 'Action' set to 'mark routing', 'New Routing Mark' set to 'ISP-1-Only', and 'Connection Mark' set to 'connectionmark-sstp'. Red boxes highlight these specific fields.

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

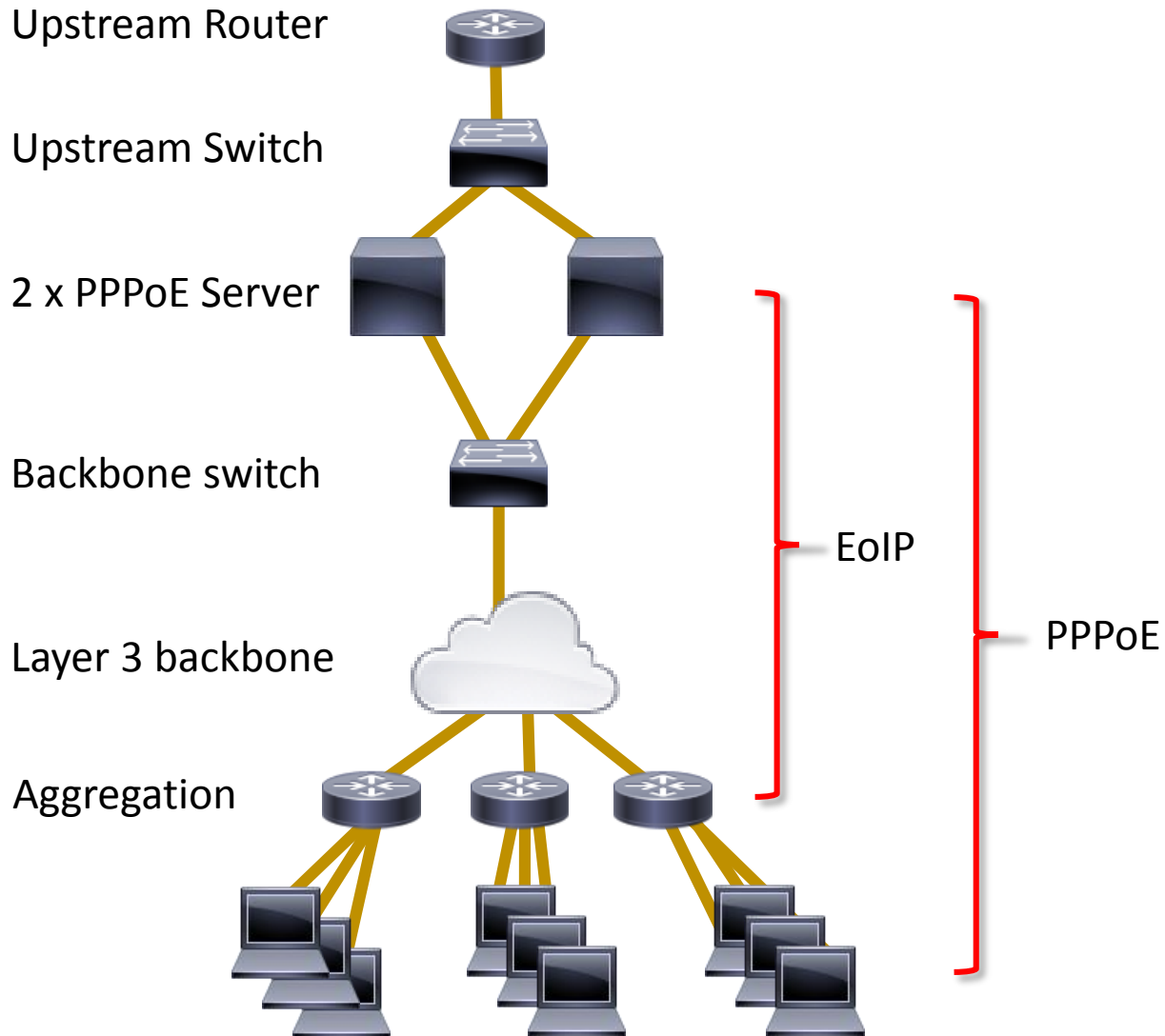


PPPoE Access Concentrator

EoIP Approach



Overview

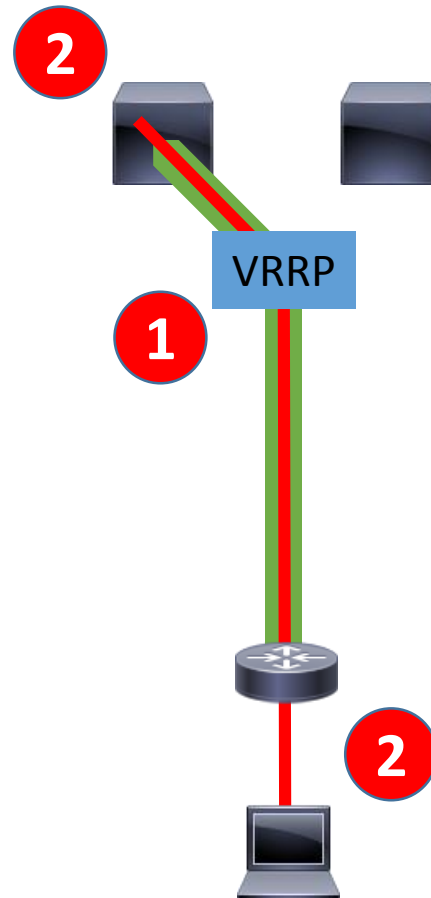




Failover (Backbone)

1 EoIP Tunnel
endpoint = VRRP
IP address

2 Multiple PPPoE
tunnels through
each EoIP tunnel

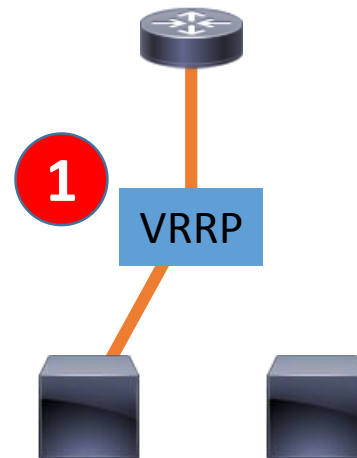




Failover (Upstream)

1

Upstream ISP will route networks to external VRRP IP





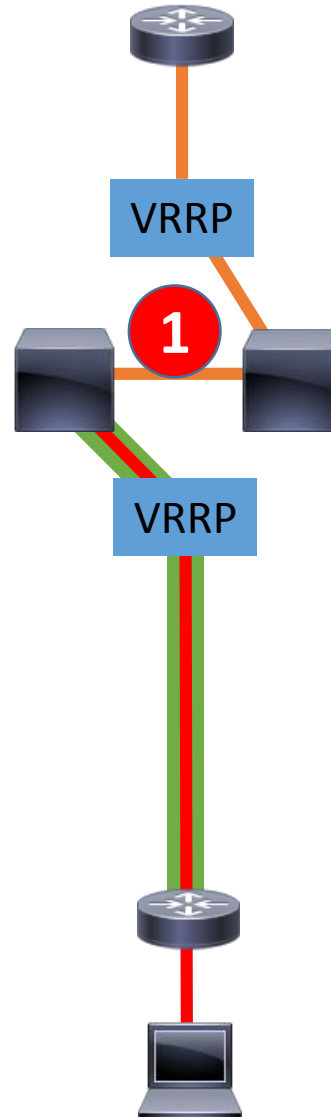
Asymmetric VRRP / Radius

BRAS:

- failover
- No loadbalancing

RADIUS

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



1

Crosslink with static routes *

* See first VPN setup

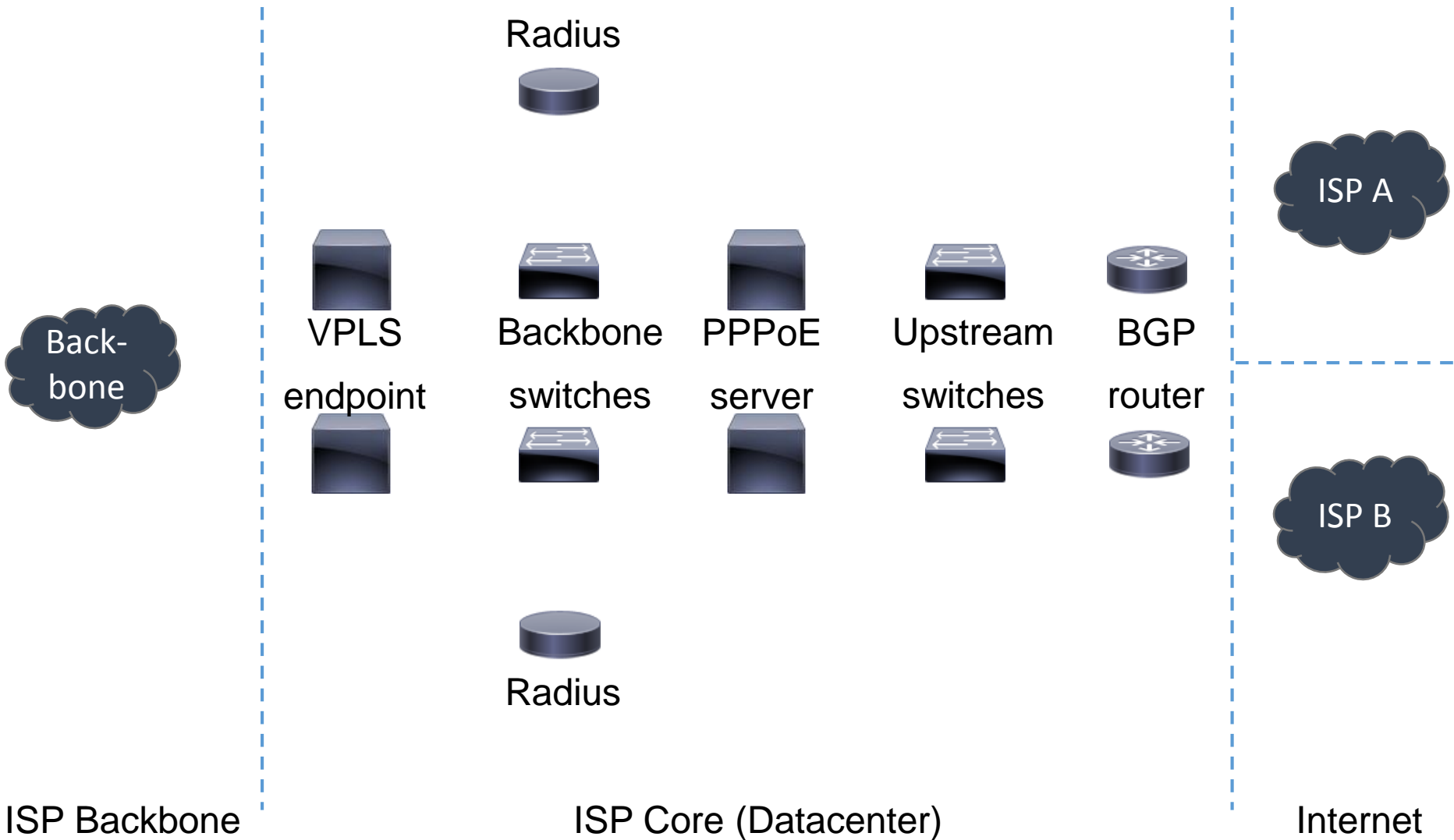


PPPoE Access Concentrator

VPLS Approach

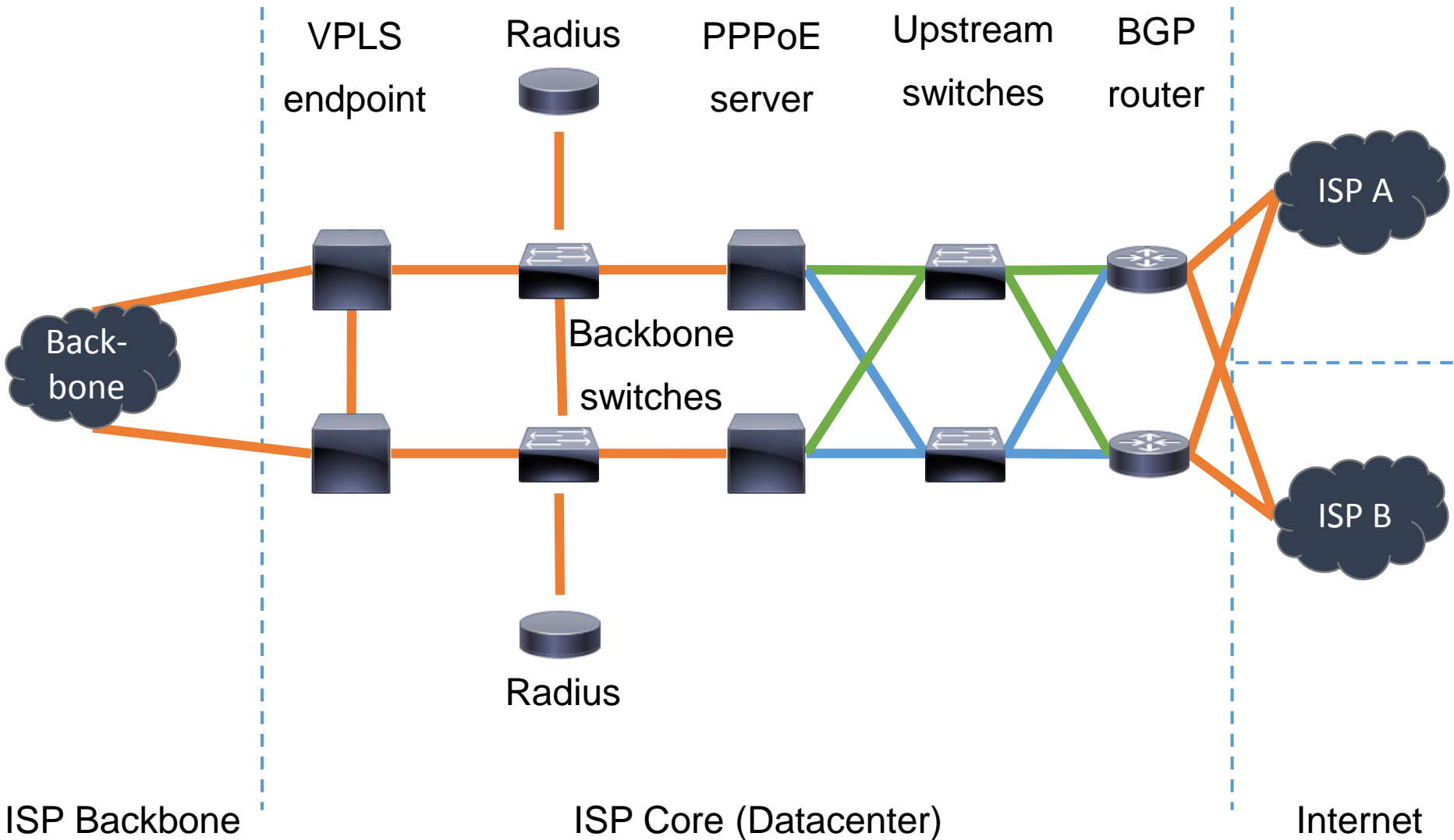


High Available ISP Network





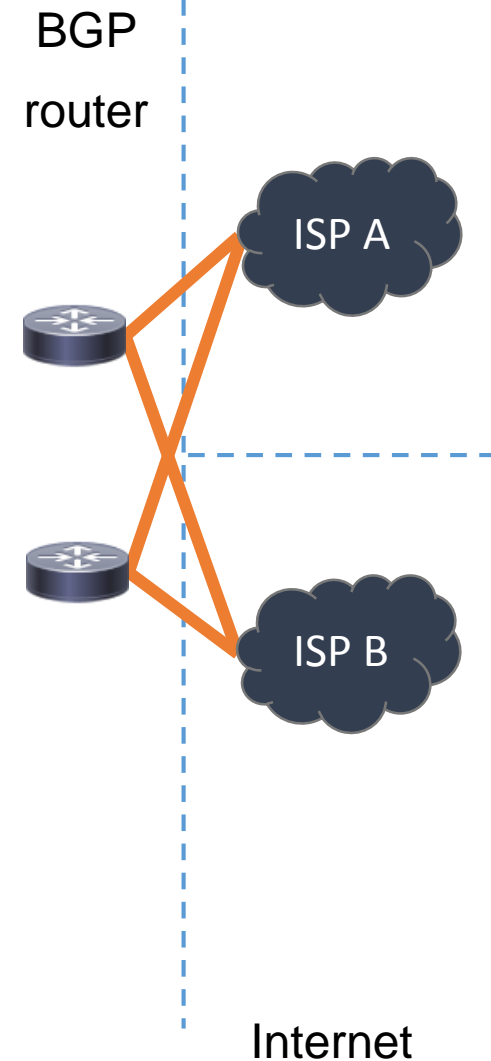
High Available ISP Network





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
- router

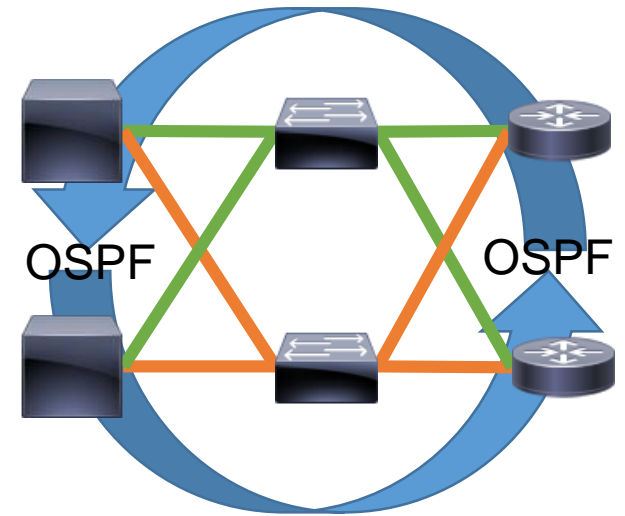




Routing

- 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



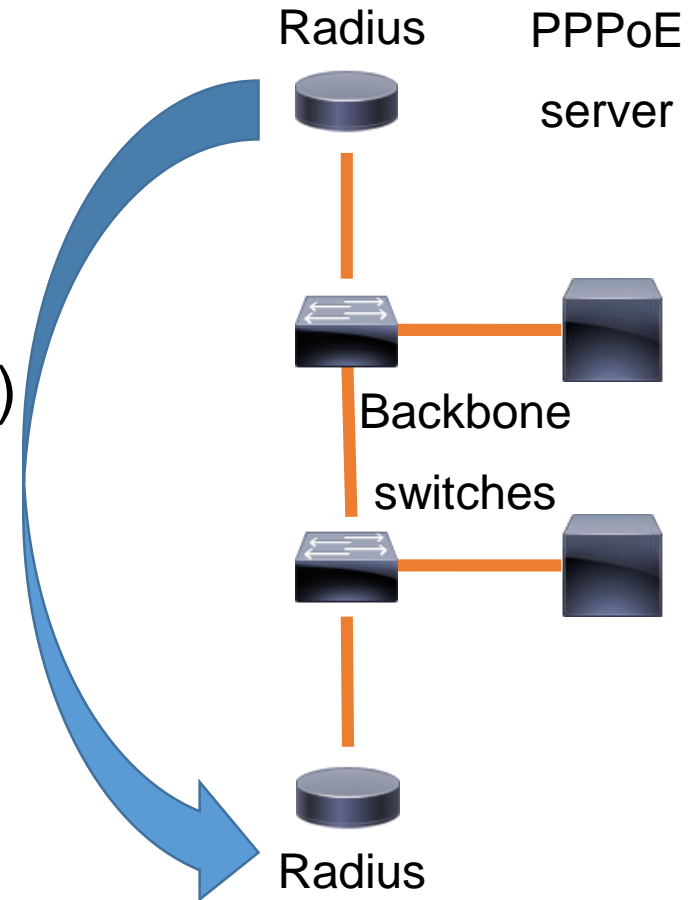


Redundant Radius Server

- 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

HotSpot Network Manager Dashboard

System Dashboard

Admin | Data | Search

- General Options
- System Settings
- Currency and Payment Systems
- External Authentications Settings
- Static Routes
- Radius Federation (Out)
- Radius Federation (In)
- System Log
- User Traffic Log
- Documentation
- Updates

Connections Period Values 520 73.33%	Traffic Period Values 13 GB -9.51%	New Users Period Values 29 45%	Clicks Period Values 440 1.62%	Impressions Period Values 2 132 -99.91%	CTR Period Values 100%+ 20.31%	GW Sold Period Values \$ 209 100%+	Adv sold Period Values \$ 0 ---%-%	HDD Free Space 8.81 GB	RAM Used 925.41 MB	CPU Load 1	NET Traffic (bit) 1 Kb 2 Kb
--	--	--	--	---	--	--	--	-------------------------------------	---------------------------------	-------------------------	---

Number of Connections and Visitors

User Count by Domain

Top Domain Connections		Top User Traffic	
Period Values		Period Values	
ThailandBeachResort	56	N15YGLW@Villaputzu-SpiaggiaSale	239 MB
NewZealandParks	44	WYRZ19@ThailandBeachResort	208 MB
BonsaiSushi	43	6MBYHG2W@NewZealandParks	189 MB
KrugerParkResort	43	3T9Q14DB@BestIndiaResort	166 MB
CoffeeHouse	40	SY58TVGB@Villaputzu-SpiaggiaSale	164 MB
DohaAirport	35	S3GJR75V@KrugerParkResort	158 MB
Villaputzu-SpiaggiaSale	33	TWLMY3@NewZealandParks	156 MB
BestIndiaResort	33	T37VH42G@ThailandBeachResort	153 MB
BodiasPA	30	DM5VY6DJ@SanVitoLoCapo-FronteMare	152 MB
SanVitoLoCapo-ZonaMercato	28	XDYD511W@BonsaiSushi	145 MB
DubaiUniversity	27	MNP4ZLSZ@NewZealandParks	138 MB
OxfordSchool	25	YV68SL55@BonsaiSushi	134 MB
Villasimius-ResortAcquaDIMare	24	565NXMPY@Villasimius-ResortAcquaDIMare	131 MB
SanVitoLoCapo-FronteMare	20	XJYLXG6@CoffeeHouse	126 MB

Context data

Total Values (Discounted Amounts)

Number of Registered Resellers	2
Number of Registered Managers	7
Number of Registered Gateways	19
Total Number of Connections	1 303
Number of Registered Users	201
Number of Activated Users	19
Total sold by the resellers	\$ 412.00
Total amount sold by managers to end users	\$ 3 421.00
Sales of other services (Prepaid and SMS)	\$ 1 260.00
Number of Clicks	26 510
Value of the Clicks	\$ 7 769.15
Impression Number	132 570
Impression Value	\$ 5 500.80
Remaining Advertiser's Credit Amount	\$ 807 890.05

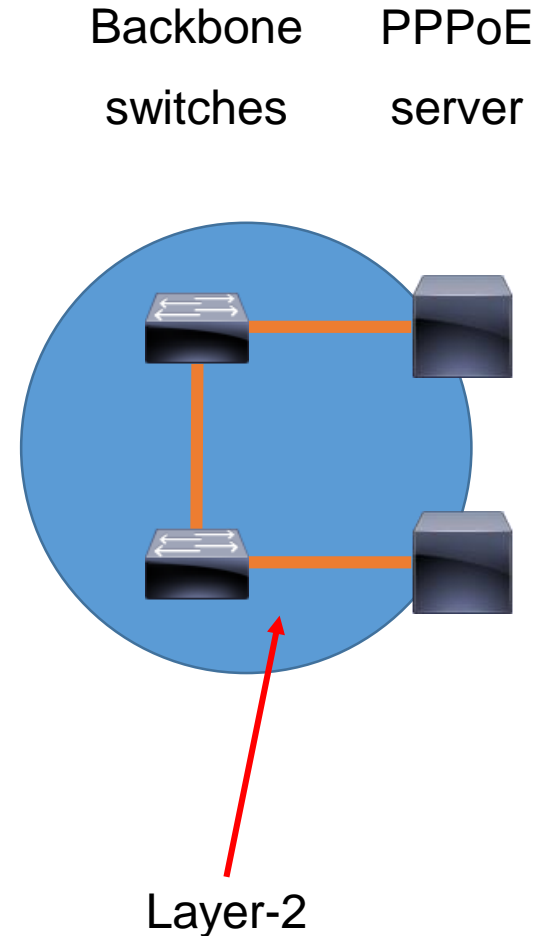
Social Users | Operatina Systems | Browser

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



BRAS Loadbalancing

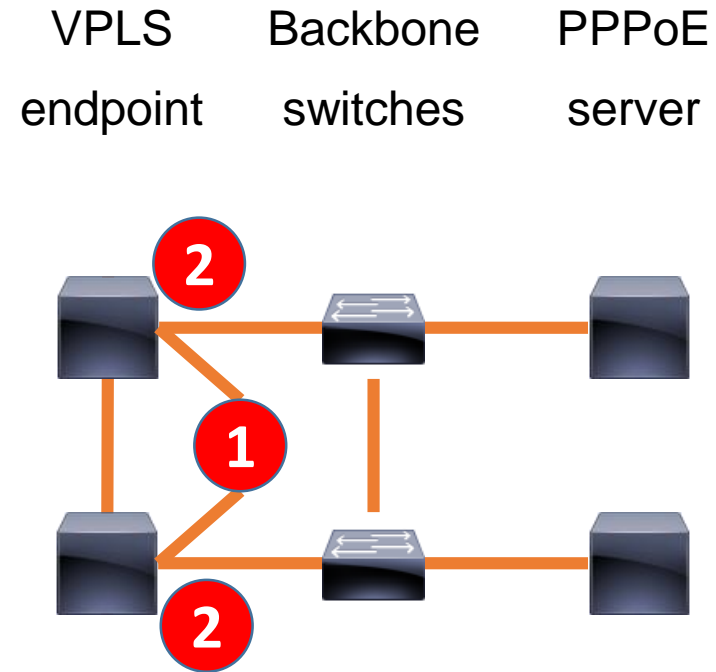
- Multiple BRAS in layer 2 network
- Works out off the box
- First come first serve
- PPPoE sessions will distribute across BRAS
- BRAS loadbalancing and failover





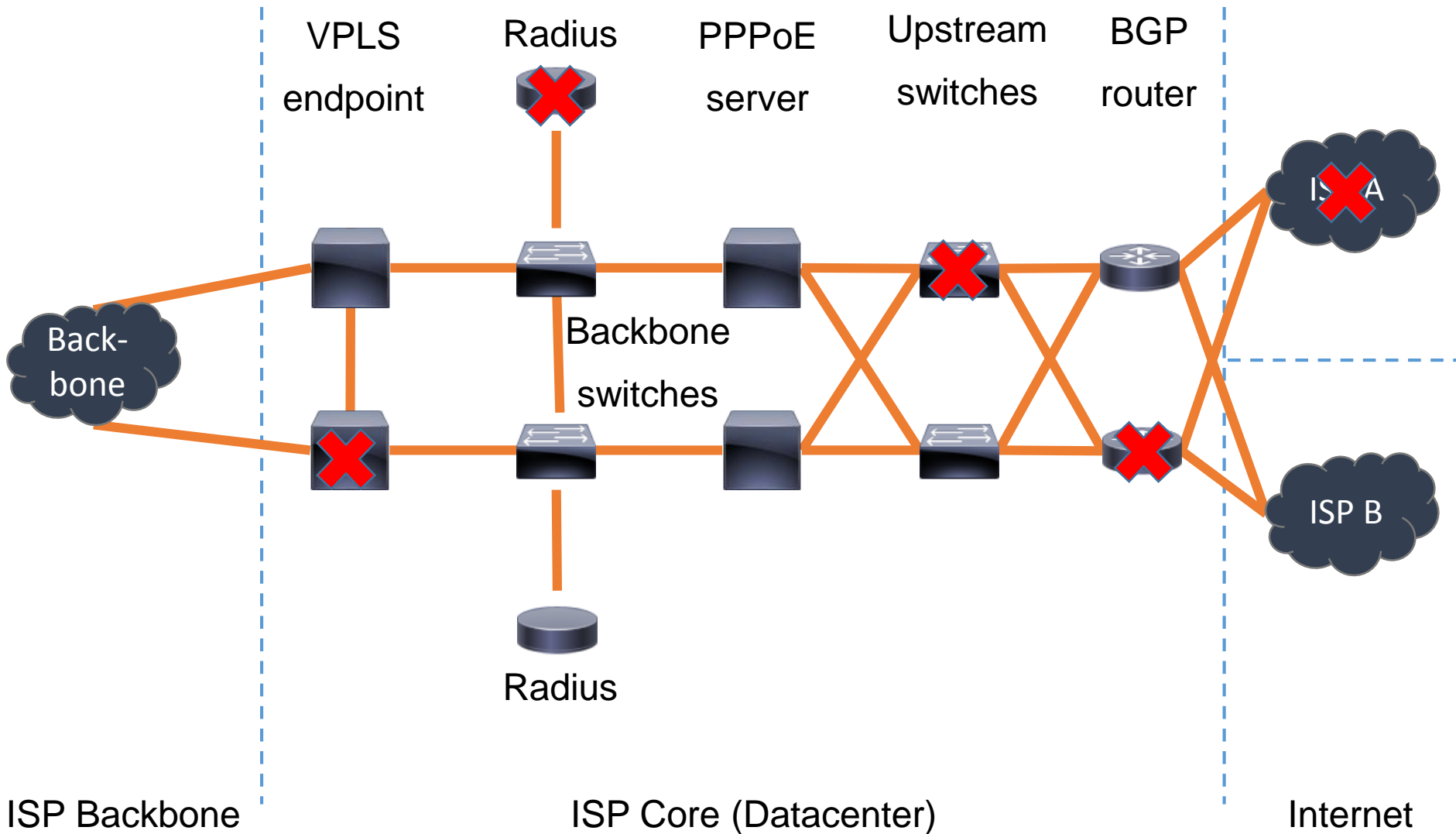
VPLS Concentrator Redundancy

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



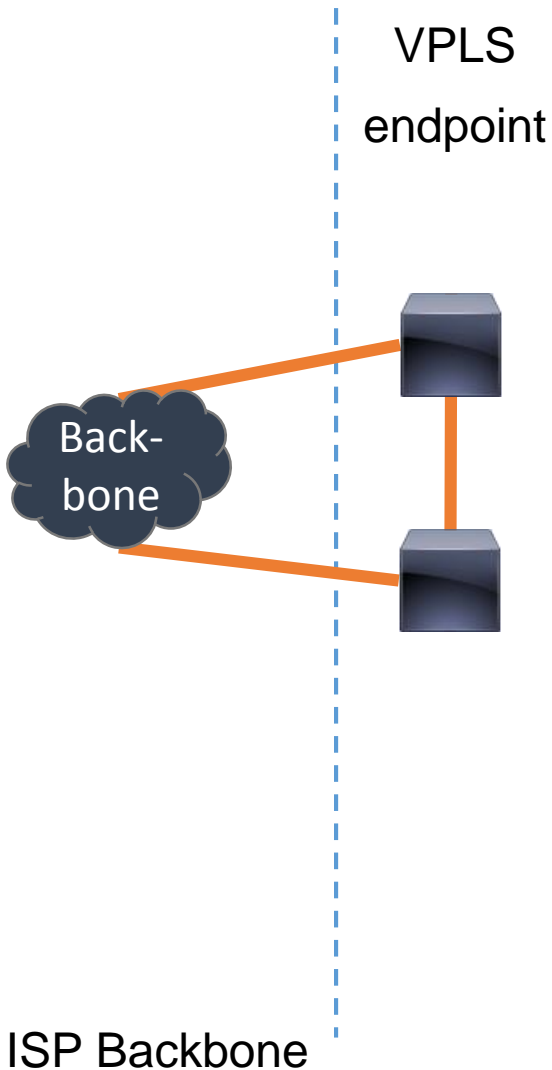


Still Operational with Loadbalancing





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