Building scalable and reliable WISP and city carrier networks based on RouterOS Ver. 3

A secure, stable, scalable, manageable end-to-end solution for all network sizes and services.

menschen.computer.netzwerke
meconet
consulting . distribution . service

menschen.computer.netzwerke

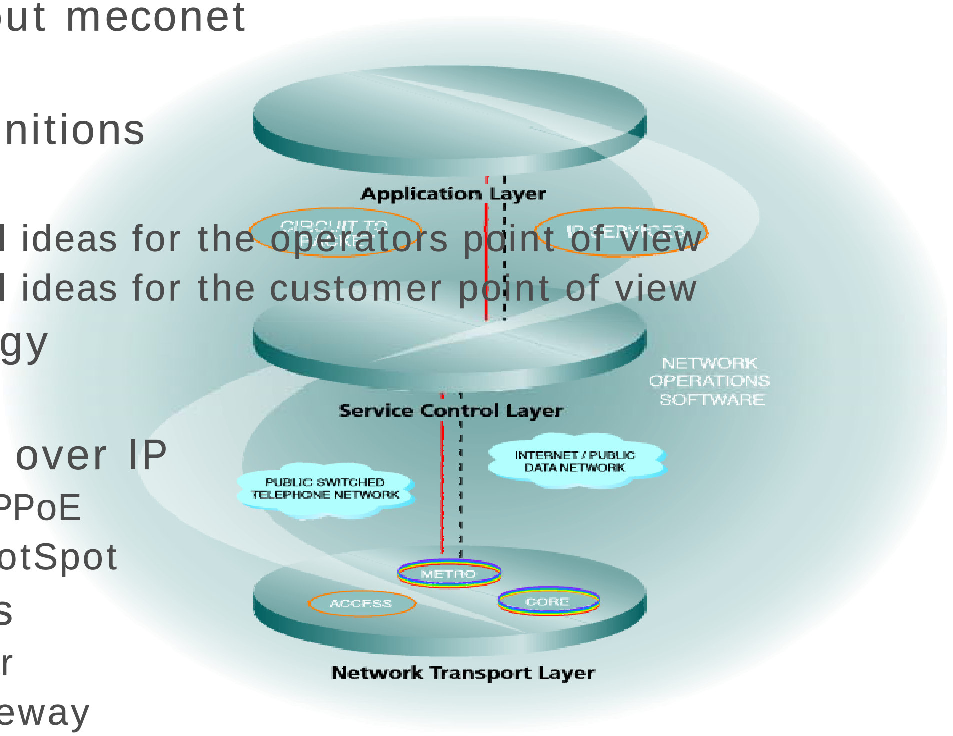
Bottenbacher Str. 78
57223 Kreuztal

Tel: +49.2732.55856-0
Fax: +49.2732.55856-111

www.meconet.de
info@meconet.de

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Table of contents
  - Some facts about meconet
  - Summary
  - Conceptual definitions
  - Basics
    - Fundamental ideas for the operators point of view
    - Fundamental ideas for the customer point of view
  - Network topology
  - IP structure
  - EoIP - ethernet over IP
    - Tunnel for PPPoE
    - Tunnel for HotSpot
  - Central services
    - PPPoE Server
    - HotSpot Gateway
  - The CPE
    - as L(ike)-DSL modem
    - ss (NAT-) router


Application Layer
NETWORK OPERATIONS SOFTWARE
Service Control Layer
INTERNET / PUBLIC DATA NETWORK
PUBLIC SWITCHED TELEPHONE NETWORK
METRO
ACCESS
CORE
Network Transport Layer

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Some facts about meconet
  - Founded in 1996 as local/regional ISP and networking project company with strange skills in RAS, ATM, DSL, security and managed services based on TCP/IP in enterprise and carrier environments.
  - Starting own wireless ISP services in 1998/1999.
  - More than 100 wireless Clients in 2002.
  - Working with MikroTik RouterOS since end of 2002, productive since 2003.
  - Starting distribution business in 2004 with MikroTik and some other wireless vendors like Mars Antennas, Joymax, PC-Engines and modas.
  - New computer center in Siegen with 2 * 155MBit/sec. (STM-1) in 2005, our complete own backbone reached more than 150 Kilometers using wireless links and leased lines. All routers are MikroTik RouterOS based at this time.
  - Some more distribution contracts with Aaronia, Huber+Suhner, MTI and SMARTEQ.
  - At the end of 2005 we stop the whole ISP Business because Deutsche Telekom covered our complete region with DSL and the prices for internet connectivity goes down. At the end nearly 1.000 wireless clients.
  - Since 2006 our business focus is consulting, distribution and services all around wireless data transmission especially for outdoor use and professional VoIP services all over Europe.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Summary

  Demonstration of network topology and network design for Wireless ISPs (WISP) and city carriers – *how to build secure, stable, scalable and reliable networks based on MikroTik RouterOS which fit the needs of any kind of network size and service.*

  The idea behind our *end-to-end solution* is to bring up a network design which have the same behavior for the operator and also for the customer like a network of the most big west European DSL carrier.

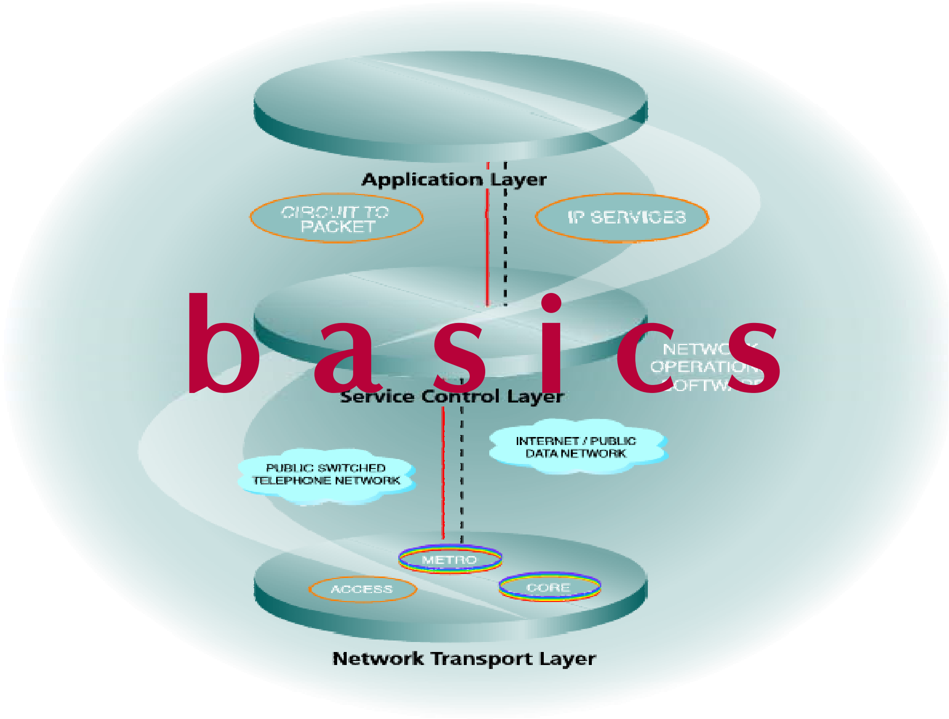
  The defined goal is to have a network which have the same behavior like a DSL network so the customer can use all standard hardware components like DSL router in this environment for the connection to the internet.

  The needed configuration steps in the network for the operator will be described in this presentation.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Some definitions used in this concept
  - **Backbone** – High speed connections in the operator network. All access points of the operator will be connected by the backbone and aggregate the traffic to the central computer center. Pure Backbone Systems have no connectivity to CPEs.
  - **CAP** – Customer Access Point, an access point which is connected on one side with the backbone and will provide access for customer on the other side (backbone edge device).
  - **CO** – Central Office or computer center of the network operator
  - **COE** – Central Office Equipment, is the equipment which is placed in the CO. Like access concentrator, RADIUS-, DNS-, Email-, NM-Server, ...
  - **CPE** - Customer Premises Equipment, is the equipment which is needed to connect the customer to the operators network.
  - **PtP –** Point to Point links described a dedicated point to point connection between e. g. two (wireless) routers. We use this term implicit with dedicated wlan interfaces on each router for such a link.
  - **PtMP –** Point to MultiPoint links aggregate more than one remote link on one interface at a central (wireless) router.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3



b a s i c s

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Why all this complexity?
  - Fundamental ideas for the operators point of view
    - Reliability & stability and bandwidth management
      - The backbone can be a fully routed and fully meshed, thus makes it failsafe. This redundancy works also if we want to use PPPoE (Point to Point over Ethernet) as layer2 protocol later on for customer connections across the backbone.
      - PPPoE is a standard used by the most big west European network operators. It’s available on all modern operation systems and also on various DSL router on the market.
      - PPPoE comes with integrated technologies for bandwidth management in a very simple way to use.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Why all this complexity?
  - Fundamental ideas for the operators point of view
    - IP management
      - IP addresses should be hold on a central system, not in various subnets all over the network on different CAPs. So it's much easier to manage the IP space and the operator don't loose addresses for all the small subnets.
      - IP addresses and subnets should come in an easy way to the customer. To minimize the administrative work, without writing huge routing tables on each backbone device.
      - The IP management must be possible on demand, dynamically customizable.
      - PPPoE comes with integrated technologies for IP management in a very simple way to use.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Why all this complexity?
  - Fundamental ideas for the operators point of view
    - Security
      - Highest protection for the backbone against attacks from customer or internet users, because all customer traffic will go thru tunnels across the backbone, no plain IP.
      - The backbone have no default route to the internet and from the IP point of view it’s a closed system based on RFC1918 IP addresses. No possible way from the backbone to the internet or to the customer networks.
      - Inside the backbones exist only IP traffic from the own administrators, all customer traffic will be tunneled thru a PPPoE tunnel.
      - The backbone can have any IP based connection, e. g. cable, wireless PtP, wireless PtMP, leased line, VPN or other and can be scaled in any way and direction.
      - The whole backbone – regardless of size and medium - is hidden for all customer.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

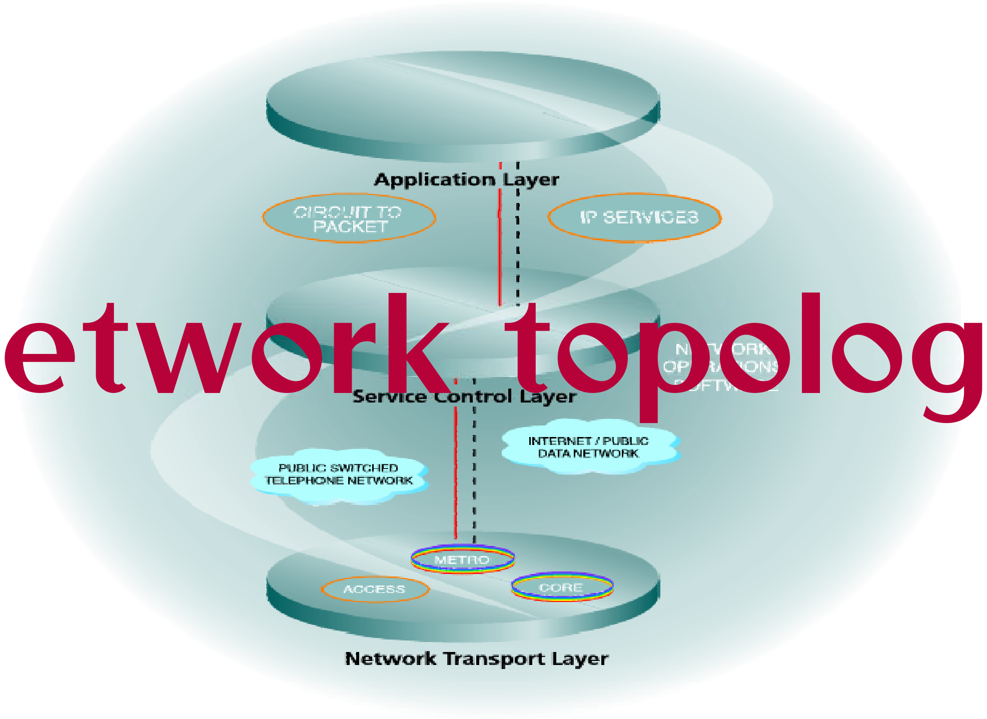
- Why all this complexity?
  - Fundamental ideas for the operators point of view
    - Security & customer connection
      - Simple and effective protection of the CAPs, because only PPPoE traffic from the CPEs must go thru them.
      - Well defined transition point at customer side (L-DSL modem = ***L****ike* a DSL modem) which is managed by the network operator. So this reduce the time to a minimum for configuration and troubleshooting.
      - The customer can use any kind of available DSL CPE equipment on the market. Support for this can be found in various forms in the internet. Reduction of customer support because they are not using hundreds of different CPEs.
      - The network operator can configure a pure L-DSL modem or also a complete DSL NAT router for the customer, using the same hardware. Reduction of equipment and price, increase the customer satisfaction.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Why all this complexity?
  - Fundamental ideas for the customer point of view
    - The network of the (wireless) operator will work like a network from a DSL carrier, so the customer can use any DSL equipment he prefer, from cheap and simple up to high end routers and firewalls.
    - The customer get the best protection against other customers using standard filters and additional IP NAT.
    - The customer can get dynamic or static IP addresses or subnets on demand.
    - The customer can get nearly any bandwidth on demand.

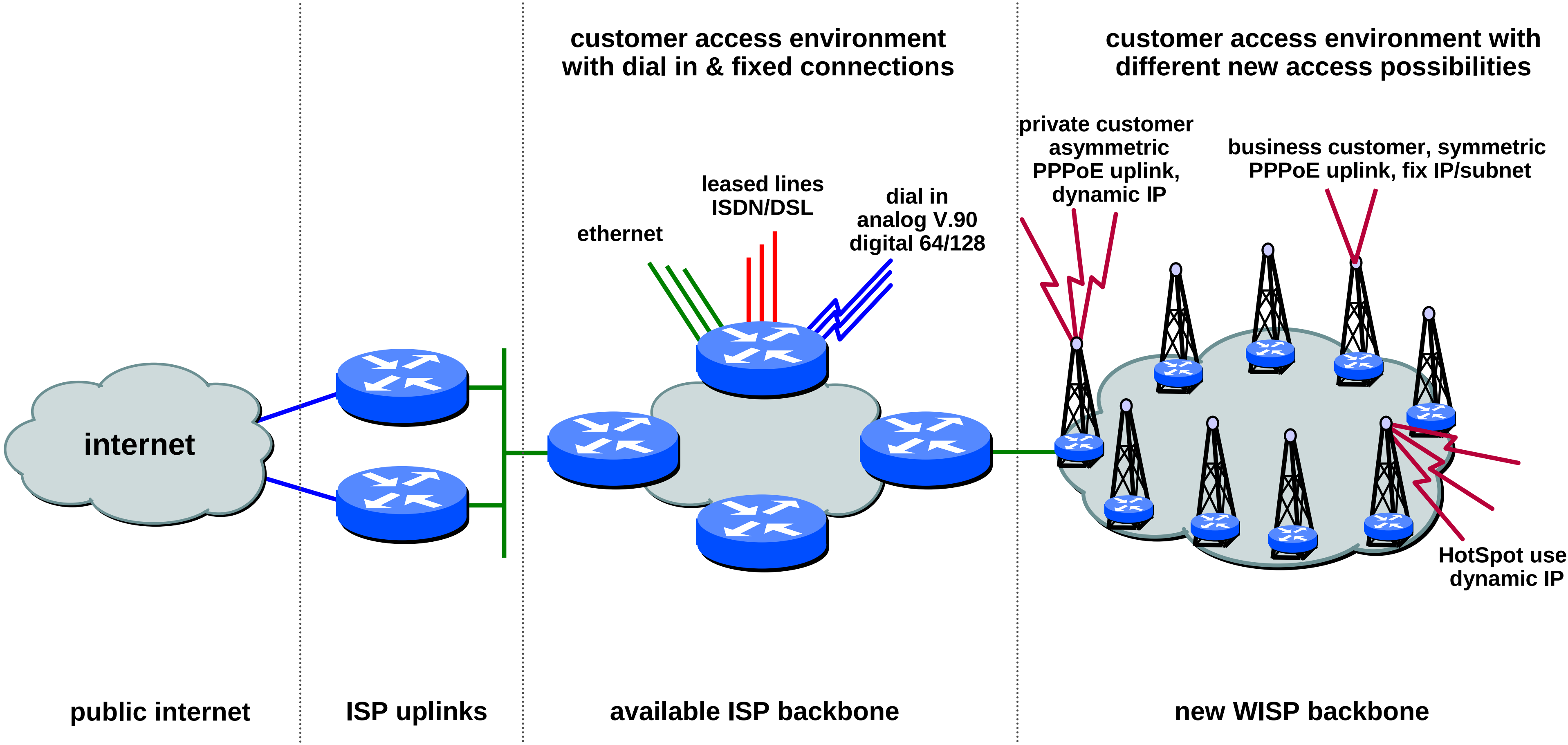
Building scalable and reliable WISP and city carrier networks based on RouterOS 3

network topology



Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Schematic network design

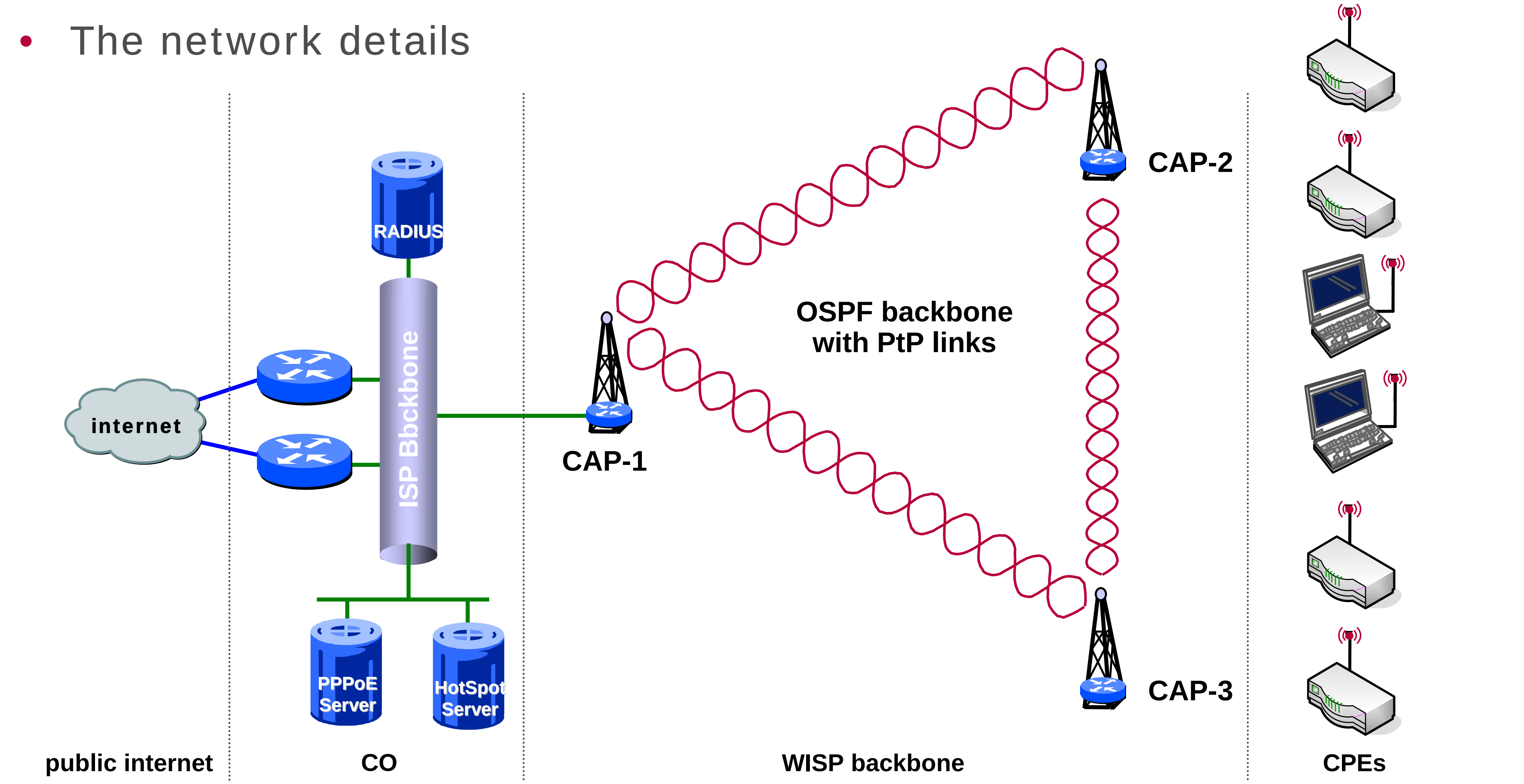

customer access environment with dial in & fixed connections
customer access environment with different new access possibilities
private customer asymmetric PPPoE uplink, dynamic IP
business customer, symmetric PPPoE uplink, fix IP/subnet
leased lines ISDN/DSL
dial in analog V.90 digital 64/128
ethernet
internet
HotSpot user dynamic IP
public internet
ISP uplinks
available ISP backbone
new WISP backbone

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Basic requirements for the network design
  - Must work with nearly each existing network infrastructure which can be found at the operators side.
  - Should be an enhancement for the existing network infrastructure with a new access area for connecting new customer to the network.
  - The only network protocol is IP, whereas it doesn’t matter what kind of physical links are used in the network.

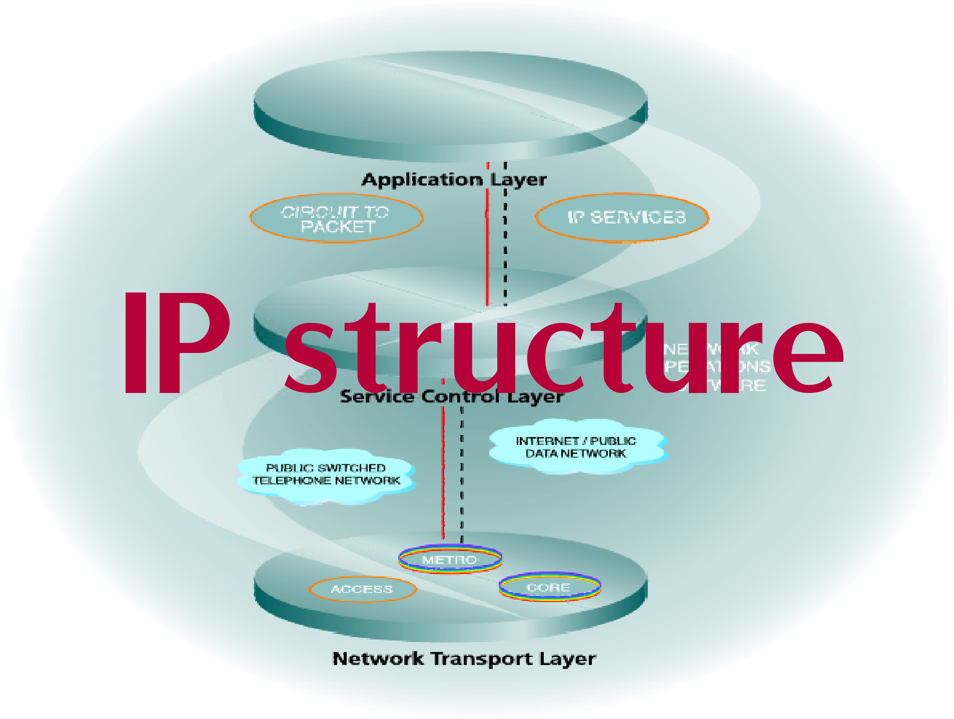
Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- The network details



Building scalable and reliable WISP and city carrier networks based on RouterOS 3

IP structure



Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – IP structure

  - Internet
    - We need a default route to the internet on the central access concentrators (for PPPoE and HotSpot) and really nowhere else in the backbone.

  - CO
    - the COE should use public IPs – private with NAT is also possible – also we define the public address pools for the customers here.

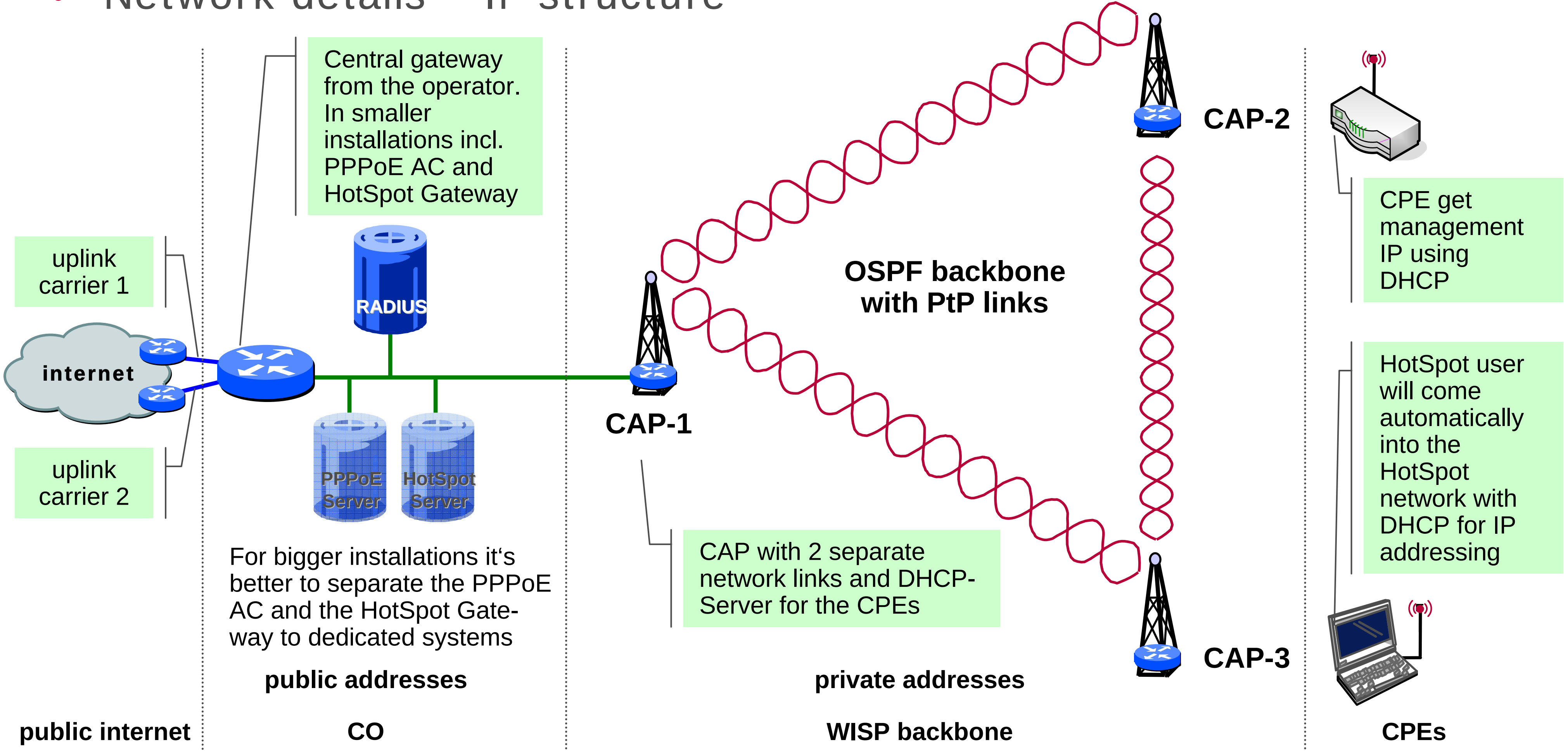
  - Backbone
    - The backbone use RFC1918 networks like 10.x.y.0/8. We will give each CAP one complete C-Net in form of 10.x.y.z/24.
    - For the needed transfer networks between the routers we use /29 networks, so you have enough addresses for 2 router on each side and VRRP.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – IP structure
  - CAP
    - Every CAP need a local loop interface if you plan redundant links. We use the first IP for that.
      - CAP-1 – 10.0.1.1/30
      - CAP-2 – 10.0.2.1/30
      - CAP-3 – 10.0.3.1/30
    - Every CAP use the network 10.0.x.128/25 at his access interfaces, the CAP himself uses the first IP (10.0.x.129/25).
    - Just use the addresses 10.0.x.130 - .254 for a DHCP Pool on the CAP to advise the management IP address for the connected CPEs. You can also use static IP addressing on the CPEs.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – IP structure



Central gateway from the operator. In smaller installations incl. PPPoE AC and HotSpot Gateway

uplink carrier 1

uplink carrier 2

For bigger installations it's better to separate the PPPoE AC and the HotSpot Gateway to dedicated systems

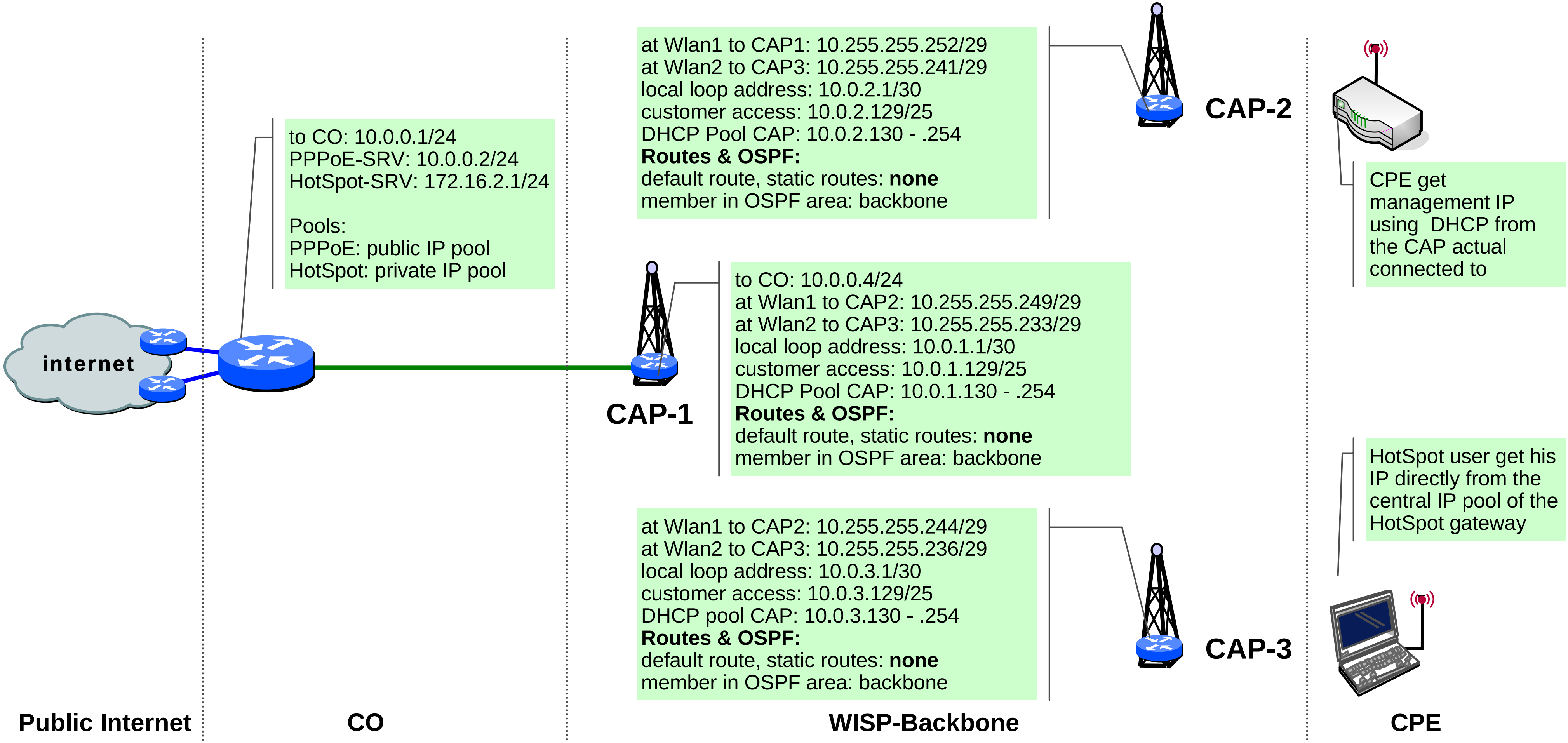
CAP with 2 separate network links and DHCP-Server for the CPEs

CPE get management IP using DHCP

HotSpot user will come automatically into the HotSpot network with DHCP for IP addressing

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – IP structure



to CO: 10.0.0.1/24
PPPoE-SRV: 10.0.0.2/24
HotSpot-SRV: 172.16.2.1/24

Pools:
PPPoE: public IP pool
HotSpot: private IP pool

at Wlan1 to CAP1: 10.255.255.252/29
at Wlan2 to CAP3: 10.255.255.241/29
local loop address: 10.0.2.1/30
customer access: 10.0.2.129/25
DHCP Pool CAP: 10.0.2.130 - .254
Routes & OSPF:
default route, static routes: **none**
member in OSPF area: backbone

to CO: 10.0.0.4/24
at Wlan1 to CAP2: 10.255.255.249/29
at Wlan2 to CAP3: 10.255.255.233/29
local loop address: 10.0.1.1/30
customer access: 10.0.1.129/25
DHCP Pool CAP: 10.0.1.130 - .254
Routes & OSPF:
default route, static routes: **none**
member in OSPF area: backbone

at Wlan1 to CAP2: 10.255.255.244/29
at Wlan2 to CAP3: 10.255.255.236/29
local loop address: 10.0.3.1/30
customer access: 10.0.3.129/25
DHCP pool CAP: 10.0.3.130 - .254
Routes & OSPF:
default route, static routes: **none**
member in OSPF area: backbone

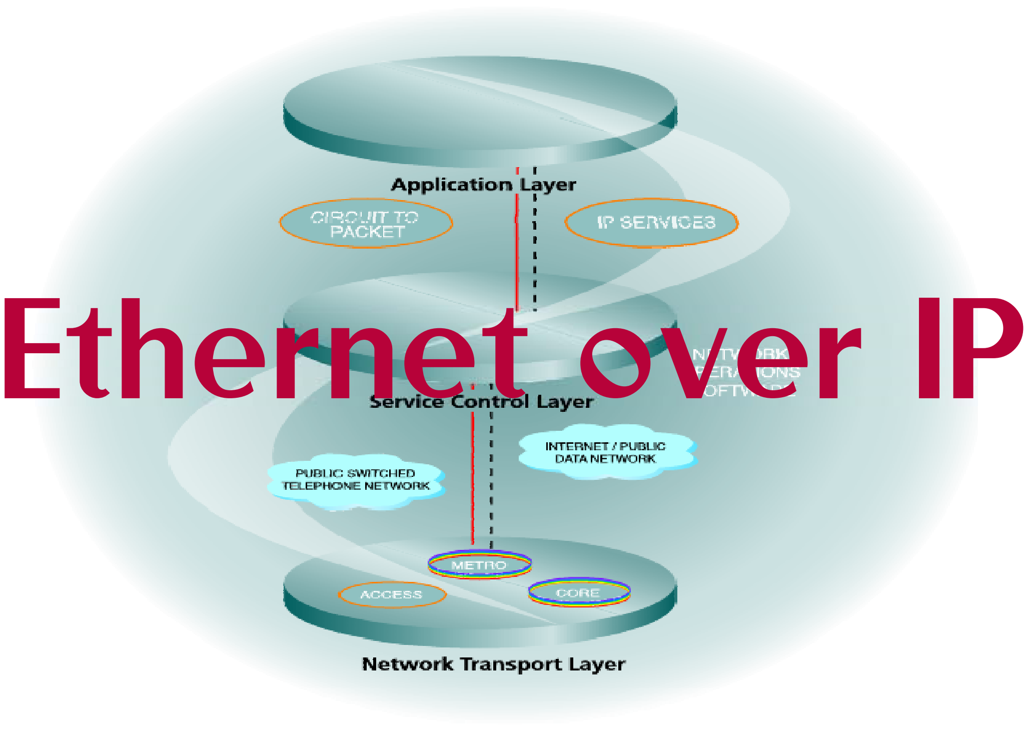
CPE get management IP using DHCP from the CAP actual connected to

HotSpot user get his IP directly from the central IP pool of the HotSpot gateway

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – IP structure
  - Using OSPF in the backbone, and have at least two different uplinks per CAP, you will get a dynamically routed backbone. So if a Link - or a CAP - goes down, OSPF will recalculate the routing and the backbone will be still running and available for the other CAPs and therefore also usable for the connected customer.
  - OSPF works with any kind of IP link - like leased lines, wireless, VPN and others.
  - The local loop interface is an interface which never goes down so long the system is up and running. Also an IP address bound to this interface is also up and running. You can't use e. g. a wlan interface for that, because you will loose IP connectivity if this interface lost his link.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3



Ethernet over IP

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – needed tunnel for PPPoE

  - How can we bring layer2 traffic – PPPoE is a layer2 protocol – from the customer thru the whole layer3 backbone to the central PPPoE access concentrator or the HotSpot gateway?

    The solution is quite simple and straight forward. It's based on MikroTiks EoIP (Ethernet over IP) protocol.

    EoIP uses GRE for a transparent ethernet tunnel across any kind of layer3 IP network. It creates a virtual ethernet interface which can be used like any physical ethernet interface in a MikroTik system.

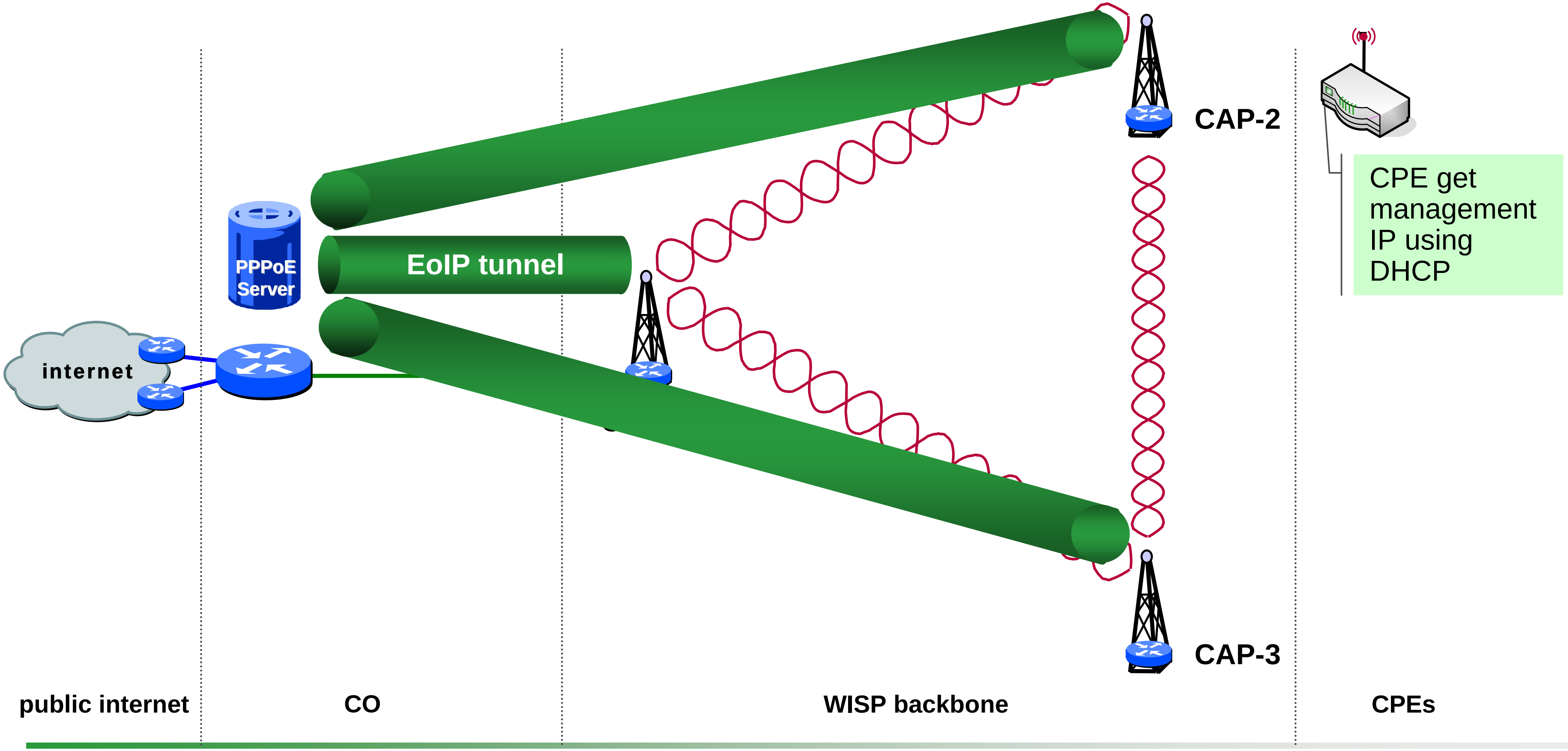
    So you have the possibility to bring any kind of layer2 traffic in a point to point (tunnel) over a routed network.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – needed tunnel for PPPoE
  - Some important notes using EoIP tunnel
    - EoIP tunnel are not bi-directional. So they have to be configured on both endpoints at a time to the corresponding peer. Both need the same tunnel ID which need to be unique in the whole system.
    - The interface on the remote system which will be the destination for the EoIP tunnel can not be used in a bridge group together with the EoIP tunnel.
    - The MAC address for all EoIP interfaces must be assigned per hand during configuration and must be in the range of 00:00:5E:80:00:00 to 00:00:5E:FF:FF:FF. EoIP tunnel will work also with other MACs, but than sometimes indefinably errors will occur.
    - the MTU should be 1500 byte so no fragmentation of ethernet packets must be done if they pass the tunnel.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

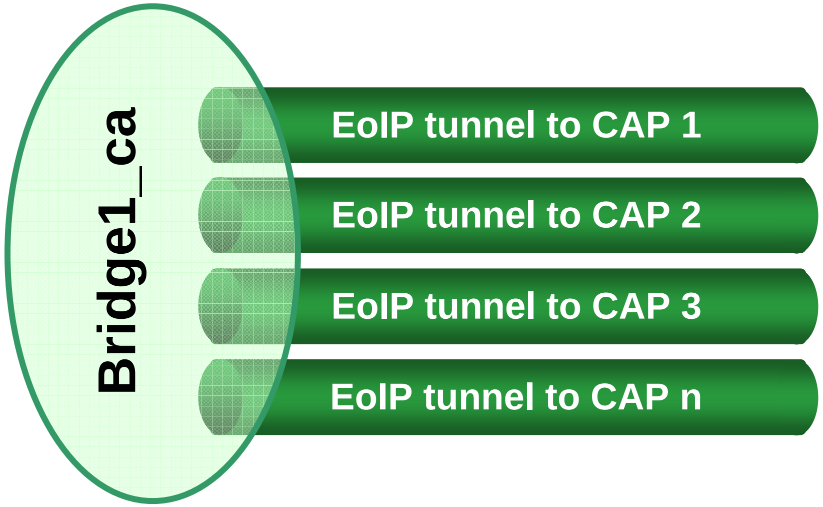
- Network details – needed tunnel for PPPoE



CPE get management IP using DHCP

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – needed tunnel for PPPoE
  - Deep detail at the central AC (Access Concentrator)



```
[admin@inet-gw] > interface bridge print
Flags: X - disabled, R - running
 0  R name="bridge1_ca" mtu=1500 arp=enabled
      mac-address=00:00:5E:80:00:00
      protocol-mode=none priority=0x8000 auto-mac=yes
      admin-mac=00:00:00:00:00:00 max-message-age=20s
      forward-delay=15s transmit-hold-count=6 ageing-time=5m

[admin@inet-gw] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic
 #    INTERFACE          BRIDGE     PRIORITY PATH-COST
 0    eoip-tunnel_AP1_ca bridge1_ca 0x80          10
 1    eoip-tunnel_AP2_ca bridge1_ca 0x80          10
 2    eoip-tunnel_AP3_ca bridge1_ca 0x80          10
```

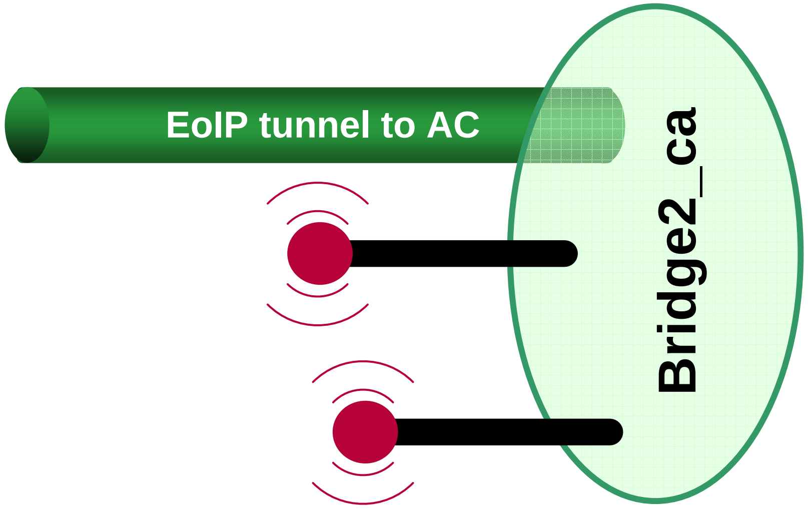
Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – needed tunnel for PPPoE
  - Deep detail at the central AC (Access Concentrator)
    - From the AC configure one EoIP tunnel directly to each CAP
      - IP address of CAP as tunnel peer: local loop address
    - At the AC configure all local EoIP tunnel interfaces in one bridge, on this Bridge must the central PPPoE Server be installed.
    - To secure the AC, just configure bridge filter passing only the needed PPPoE traffic (protocol 0x8863 [PPPoE discovery] & 0x8864 [PPPoE session]) thru the bridge to the AC. All offer traffic can be dropped here.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – needed tunnel for PPPoE
  - Deep detail at the CAP (access point for customer)

```
[admin@CAP-1] > interface bridge print
Flags: X - disabled, R - running
 1  R name="bridge2_ca" mtu=1500 arp=enabled
      mac-address=00:00:5E:80:00:01
      protocol-mode=none priority=0x8000 auto-mac=yes
      admin-mac=00:00:00:00:00:00 max-message-age=20s
      forward-delay=15s transmit-hold-count=6 ageing-time=5m


Flags: X - disabled, I - inactive, D - dynamic
 #    INTERFACE            BRIDGE       PRIORITY PATH-COST
 0    eoip-tunnel_AP1_ca  bridge2_ca    0x80          10
 1    wlan3                bridge2_ca    0x80          10
```



Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – needed tunnel for PPPoE
  - Deep detail at the CAP (access point for customer)
    - From each CAP configure one EoIP tunnel directly to the central AC
      - IP address of AC as tunnel peer: Lan IP of AC in the CO
    - At the CAP configure the EoIP tunnel interface and all interfaces responsible for customer access in one bridge. This interfaces can have different physics like ethernet and wlan.
    - To secure the CAP, just configure filter which allow only needed PPPoE traffic from the CPEs thru the CAP. Don’t forget filter for you own administrative traffic to the CAP and thru the CAP to the CPEs.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – needed tunnel for HotSpot services

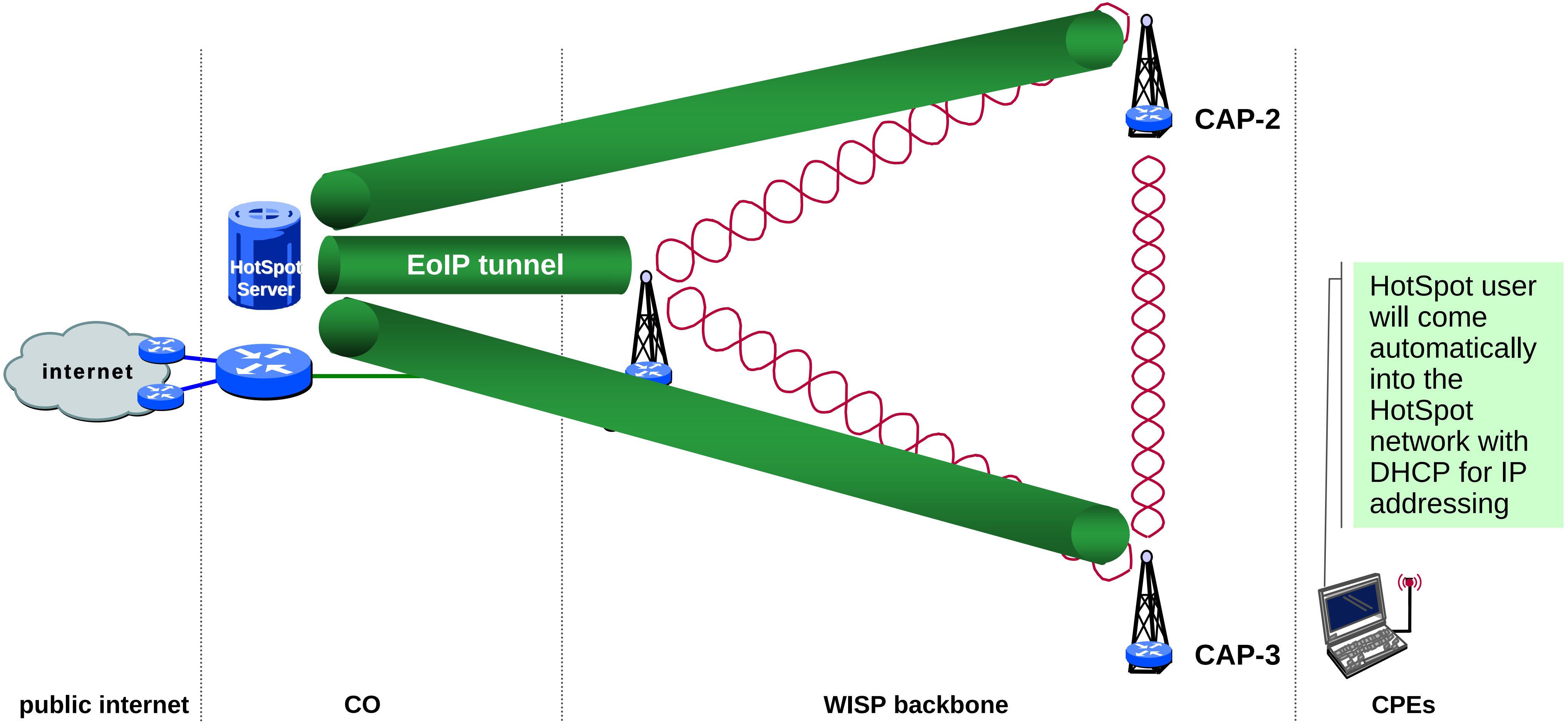
  - With very few configurations can also a separate HotSpot network infrastructure parallel be used on the same backbone. So the operator have some extra benefit from the same network installation.

  - Additional costs per CAP are only one wlan interface, cable, surge arrestor and a 2.4 GHz antenna (if you use 2.4GHz for your fixed client access, a virtual AP can be enough). In bigger networks a separate HotSpot gateway is needed, in smaller installation the central HotSpot gateway can run also on the PPPoE AC.

  - The configuration is analog to the PPPoE configuration, one EoIP tunnel from each HotSpot interface to the central HotSpot gateway, *but* separated from the EoIP tunnel used for PPPoE connections.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

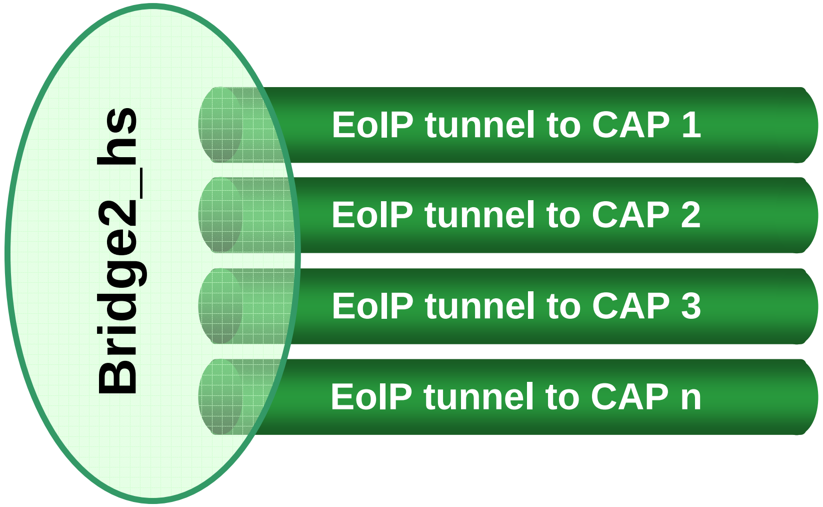
- Network details – needed tunnel for HotSpot services



HotSpot user will come automatically into the HotSpot network with DHCP for IP addressing

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – needed tunnel for HotSpot services
  - Deep detail at the central HotSpot-Gateway



```
[admin@inet-gw] > interface bridge print
Flags: X - disabled, R - running
  1  R name="bridge2_hs" mtu=1500 arp=enabled
       mac-address=00:00:5E:80:00:06
       protocol-mode=none priority=0x8000 auto-mac=yes
       admin-mac=00:00:00:00:00:00 max-message-age=20s
       forward-delay=15s
       transmit-hold-count=6 ageing-time=5m

[admin@inet-gw] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic
 #    INTERFACE          BRIDGE     PRIORITY PATH-COST
 3    eoip-tunnel_AP1_hs bridge2_hs 0x80          10
 4    eoip-tunnel_AP2_hs bridge2_hs 0x80          10
 5    eoip-tunnel_AP3_hs bridge2_hs 0x80          10
```

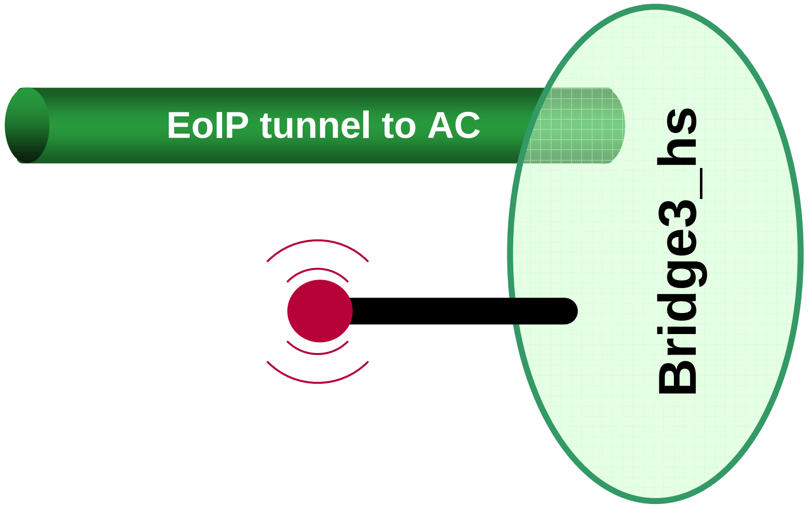
Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – needed tunnel for HotSpot services
    - Deep detail at the central HotSpot-Gateway
        - From the HotSpot Gateway configure one EoIP tunnel directly to each CAP
            - IP address of CAP as tunnel peer: local loop address
        - At the HotSpot Gateway configure all local EoIP tunnel interfaces in one bridge, on this Bridge must the central HotSpot Server be installed.
        - Use filter if you want no direct IP connectivity between your HotSpot user and also for other restrictions for this kind of user.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – needed tunnel for HotSpot services
  - Deep detail at the CAP (access point for customer)

```
[admin@CAP-1] > interface bridge print
Flags: X - disabled, R - running
 2  R name="bridge3_hs" mtu=1500 arp=enabled
      mac-address=00:00:5E:80:00:07
      protocol-mode=none priority=0x8000 auto-mac=yes
      admin-mac=00:00:00:00:00:00 max-message-age=20s
      forward-delay=15s transmit-hold-count=6 ageing-time=5m


Flags: X - disabled, I - inactive, D - dynamic
 #    INTERFACE           BRIDGE      PRIORITY PATH-COST
 2    eoip-tunnel_AP1_hs  bridge3_hs  0x80        10
 3    wlan4               bridge3_hs  0x80        10
```

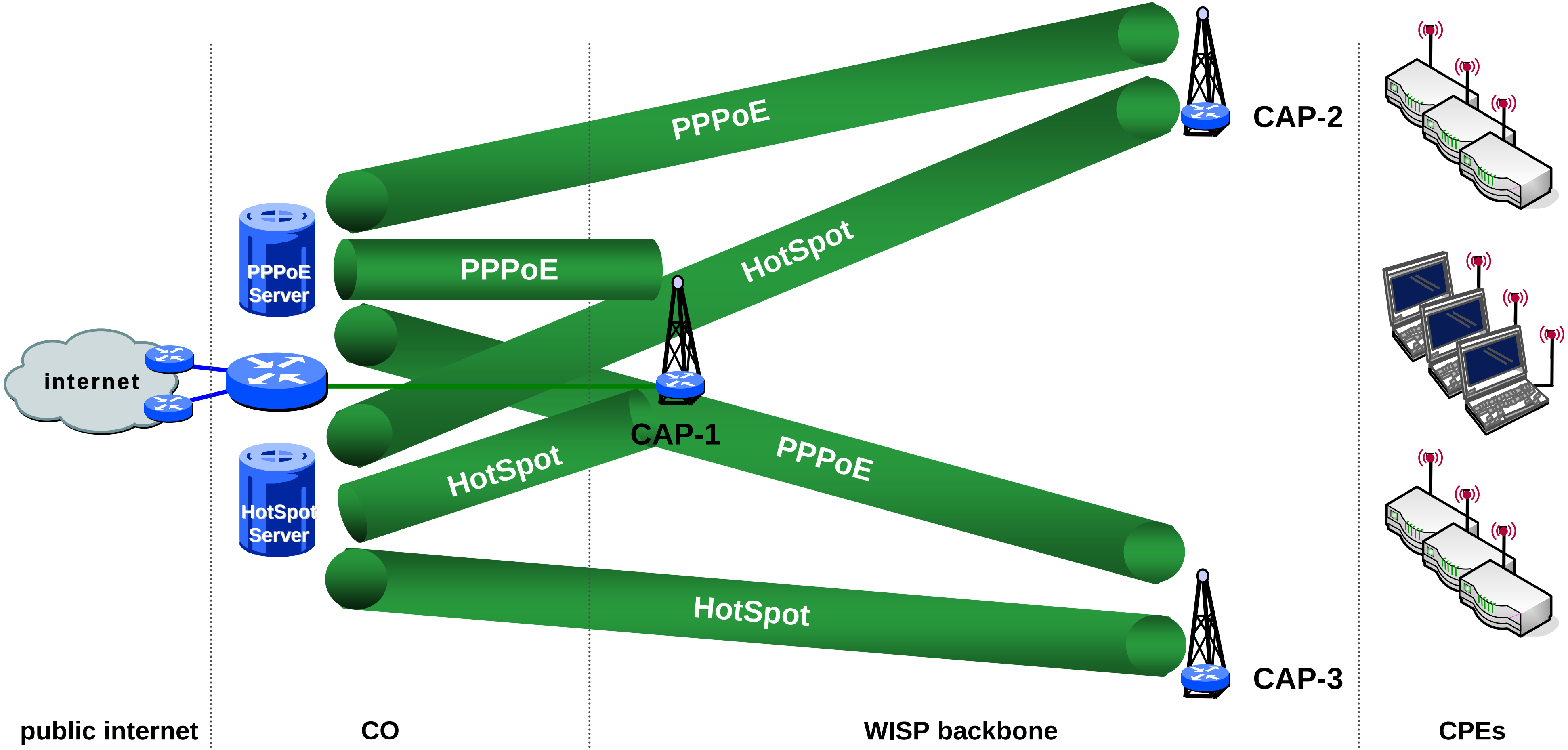


Building scalable and reliable WISP and city carrier networks based on RouterOS 3

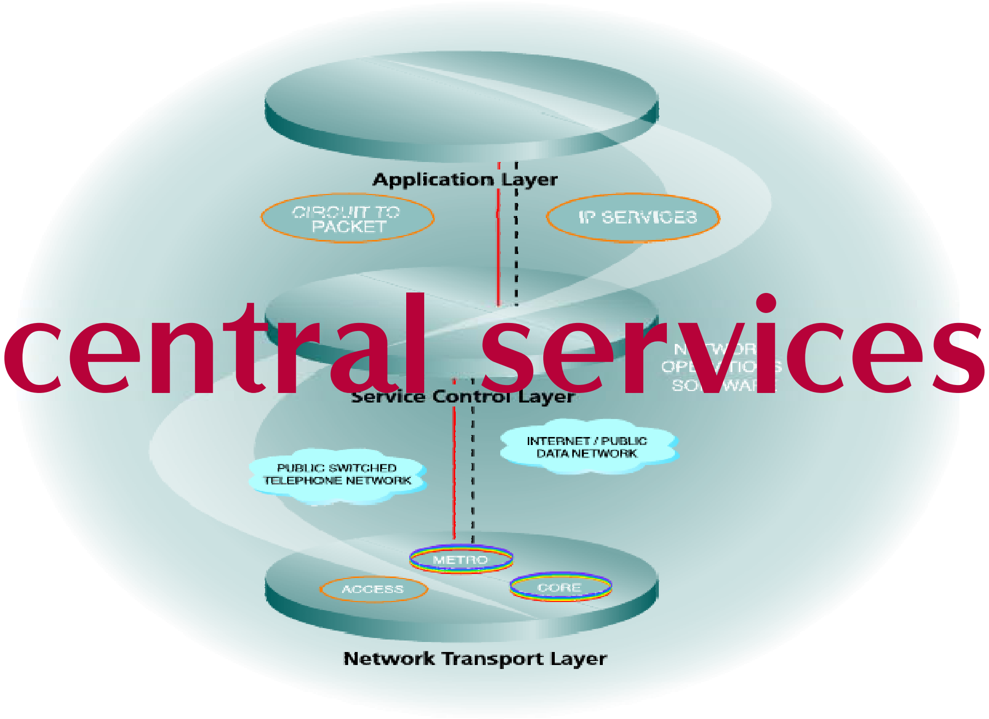
- Network details –needed tunnel for HotSpot services
  - Deep detail at the CAP (access point for customer)
    - From each CAP configure one EoIP tunnel directly to the central HotSpot gateway
      - IP address of HotSpot gateway as tunnel peer: Lan IP of HotSpot gateway in the CO
    - At the CAP configure the EoIP tunnel interface and all interfaces responsible for HotSpot services in one bridge. This interfaces can have different physics like ethernet and wlan.
    - To secure the CAP, just configure filter which allow only wanted traffic from and to the HotSpot gateway thru the CAP. Drop all unneeded access directly to the CAP.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details - all needed EoIP tunnel für PPPoE & HotSpot



Building scalable and reliable WISP and city carrier networks based on RouterOS 3



central services

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – central services
  - If you plan a network with roundabout 100 users, all central services can run on one system, e. g. the gateway to the internet. If you plan networks with more customers we prefer separate systems per service.
  - So scalability is also given in the CO. You can start with one RouterOS (e.g. RB/532 or RB/333) based system and run your internet routing, the PPPoE access concentrator and also the HotSpot gateway on this one machine. If your network grow, just separate the central services. This can be done with a minimum off network downtime.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

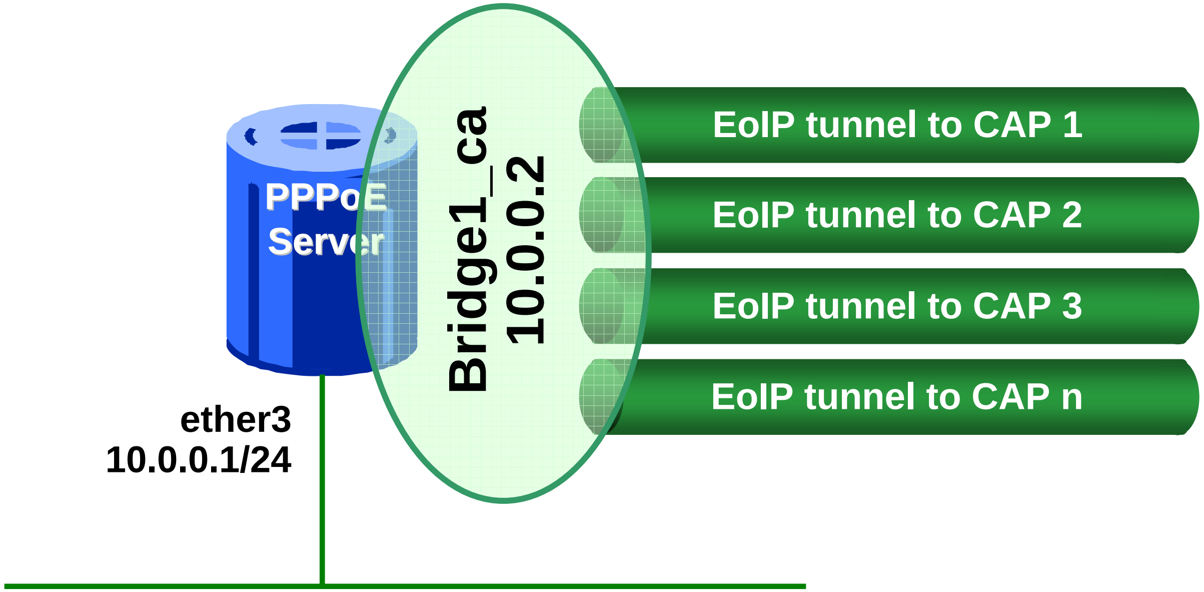
- Network details – central services
  - The PPPoE server
    - Runs on the bridge which have all the EoIP tunnel to the customer access interfaces on the CAPs in the network.
    - Even if PPPoE a layer2 protocol, the access concentrator have to route the packets from and to the customer behind the tunnel. So it‘s better to have different IP networks on the left and the right side of the AC. Otherwise you need proxy ARP, but this should be the last compromise, routing is much better mainly in the case of troubleshooting and understanding the packet flow.

```
[admin@inet-gw] > ip route print detail
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme, B - blackhole, U - unreachable, P - prohibit
 4 ADC  dst-address=172.16.1.252/32 pref-src=10.0.0.2  interface=<pppoe-pppoe-1> distance=0 scope=10
```

Shows the dynamic generated route at the AC, after the login from user “pppoe-1”. The user get his IP address 172.16.1.252 automatically during the PPPoE negotiation.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – central services
  - The PPPoE server



The local IP address of the PPPoE servers will be assigned using the PPPoE server profile.

This IP address should not be in the same subnet like the IP addresses behind the PPPoE tunnel, because this address is used for the routing thru the tunnel to the customer

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – central services
  - The PPPoE server
    - Basic configuration of the PPPoE servers.

```
[admin@inet-gw] > interface pppoe-server server print
Flags: X - disabled
 0   service-name="" interface=bridge1_ca max-mtu=1480 max-mru=1480 mrru=disabled
     authentication=pap,chap,mschap1,mschap2 keepalive-timeout=10 one-session-per-
     host=yes max-sessions=0 default-profile=PPPoE-SRV

[admin@inet-gw] > ppp profile print
Flags: * - default
 1   name="PPPoE-SRV" local-address=10.0.0.2 remote-address=pool_PPPoE
     bridge=bridge1_ca use-compression=no use-vj-compression=no use-encryption=yes
     only-one=yes change-tcp-mss=yes dns-server=192.168.255.1,192.168.255.9
```

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – central services
  - The PPPoE server – bandwidth management
    - Limitations for bandwidth can be placed in profiles. This profiles can be easily mapped to any user in the user configuration.

```
[admin@inet-gw] > ppp profile print
Flags: * - default
 2   name="PPPoE-2Mdown/512kup" local-address=10.0.0.2 remote-address=pool_PPPoE
     bridge=bridge1_ca idle-timeout=30m use-compression=no use-vj-compression=no use-
    encryption=yes only-one=yes change-tcp-mss=yes rate-limit=512k/2M
    dns-server=192.168.255.1,192.168.255.9

[admin@inet-gw] > ppp secret print
Flags: X - disabled
 #   NAME        SERVICE CALLER-ID        PASSWORD         PROFILE              REMOTE-ADDRESS
 0   pppoe-1      pppoe                    pppoe-1           PPPoE-2Mdown/512kup
```

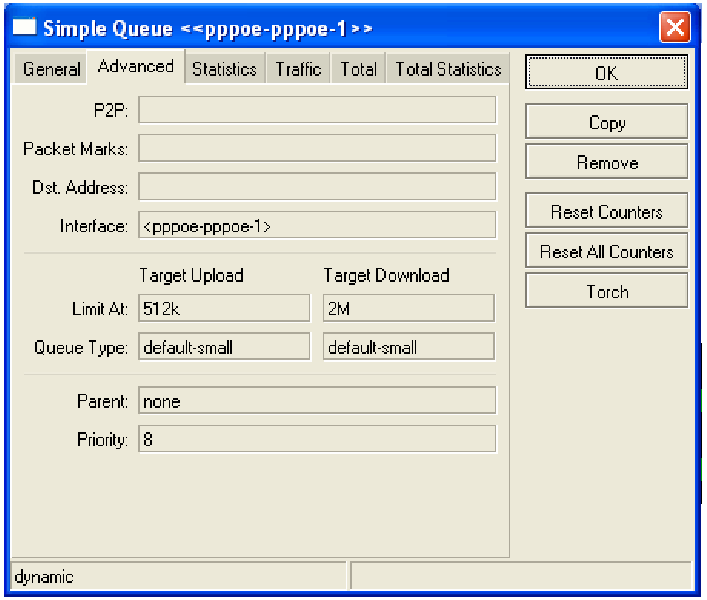
Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – central services
  - Bandwidth management is included in the PPPoE protocol. RouterOS will generate a simple queue with the correct bandwidth settings for each PPPoE user which logs in. Nothing else is necessary for this, you have only to define a tunnel bandwidth in the user configuration.
  - So you have a powerful possibility to control your users link speed, regardless if this should be synchronous or asynchronous. Just define one profile per link speed combination you want to sell and map this to any customer you like.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – central services

  - After the PPPoE login from user “pppoe-1” RouterOS generate the correct simple queue dynamically for this user:



Simple Queue <<pppoe-pppoe-1>>

P2P:

Packet Marks:

Dst. Address:

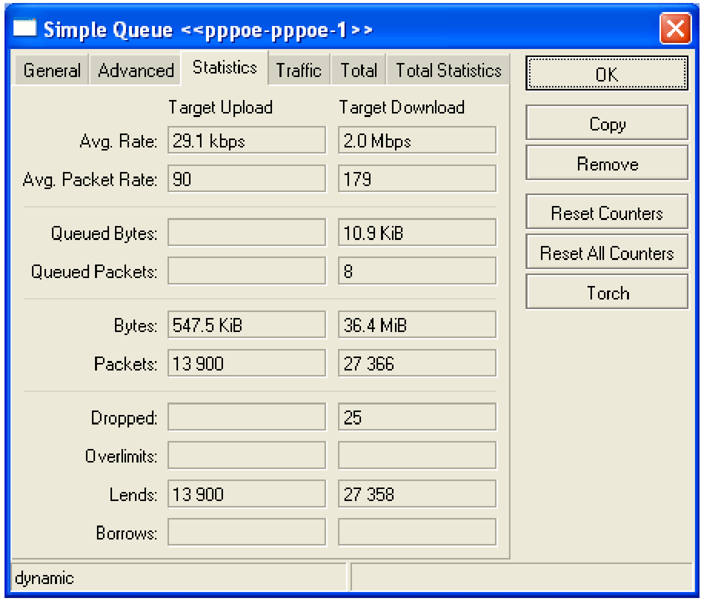
Interface: <pppoe-pppoe-1>

	Target Upload	Target Download
Limit At:	512k	2M
Queue Type:	default-small	default-small

Parent: none

Priority: 8

dynamic



Simple Queue <<pppoe-pppoe-1>>

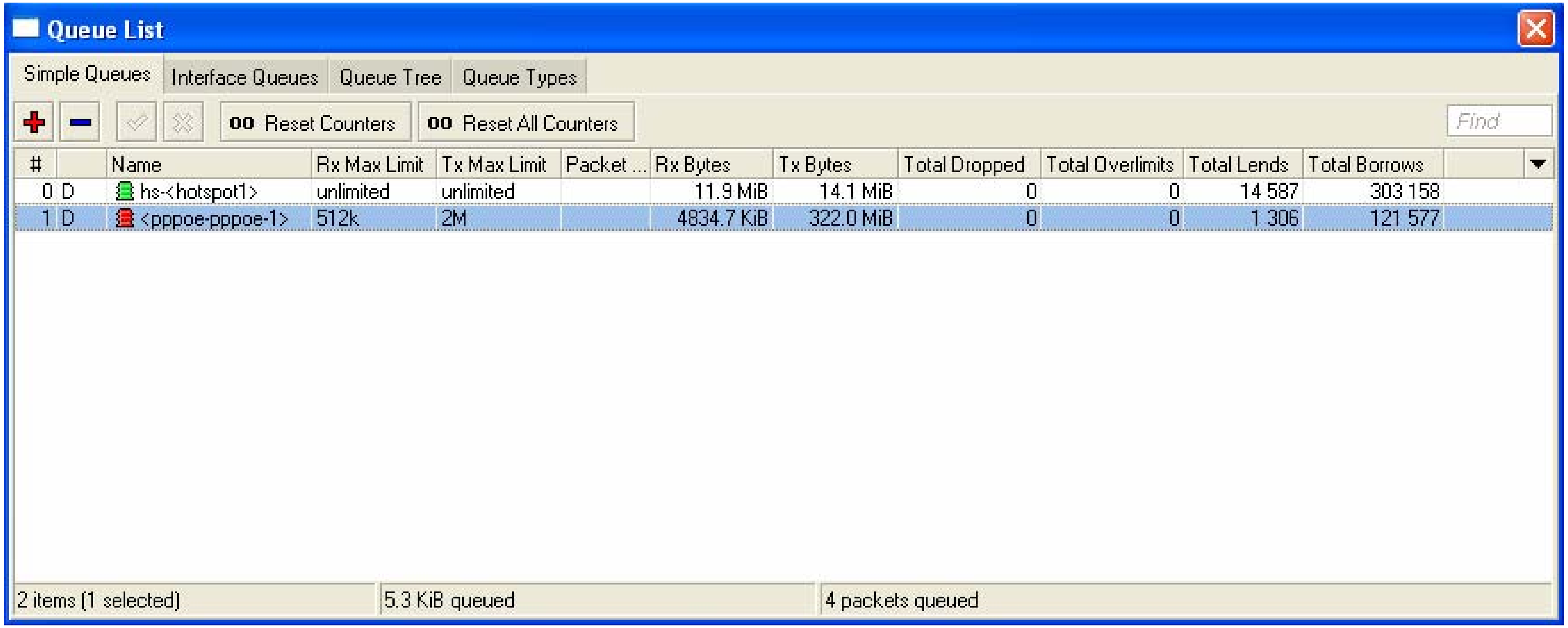
	Target Upload	Target Download
Avg. Rate:	29.1 kbps	2.0 Mbps
Avg. Packet Rate:	90	179
Queued Bytes:		10.9 KiB
Queued Packets:		8
Bytes:	547.5 KiB	36.4 MiB
Packets:	13 900	27 366
Dropped:		25
Overlimits:		
Lends:	13 900	27 358
Borrows:		

dynamic

  - The right picture shows the running queuing during an active download from the user.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – central services
  - The queue overview shows with the red icon that this queue has reached the assigned bandwidth limit.



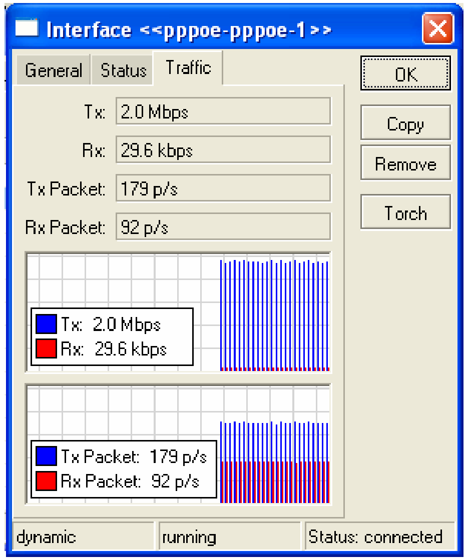
#		Name	Rx Max Limit	Tx Max Limit	Packet ...	Rx Bytes	Tx Bytes	Total Dropped	Total Overlimits	Total Lends	Total Borrows
0	D	🟩 hs-<hotspot1>	unlimited	unlimited		11.9 MiB	14.1 MiB	0	0	14 587	303 158
1	D	🟥 <pppoe-pppoe-1>	512k	2M		4834.7 KiB	322.0 MiB	0	0	1 306	121 577

2 items (1 selected) | 5.3 KiB queued | 4 packets queued

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – central services

  - The interface statistics for this PPPoE interface shows the active bandwidth control in a impressive way. Can it be much more simple to control each users bandwidth on one central system by the operator, as with a simple entry in a profile, or with an additional RADIUS System?



Tx: 2.0 Mbps

Rx: 29.6 kbps

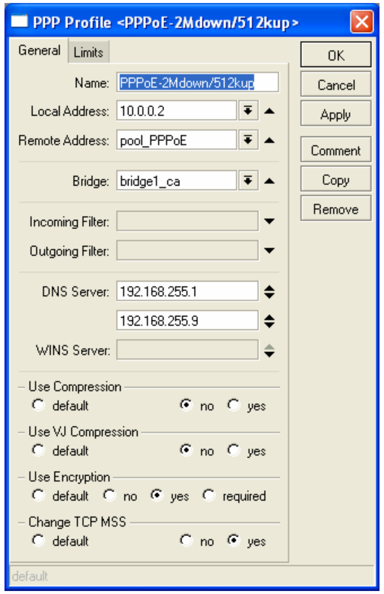
Tx Packet: 179 p/s

Rx Packet: 92 p/s

🟦 Tx: 2.0 Mbps
🟥 Rx: 29.6 kbps

🟦 Tx Packet: 179 p/s
🟥 Rx Packet: 92 p/s

dynamic | running | Status: connected



Name: PPPoE-2Mdown/512kup

Local Address: 10.0.0.2

Remote Address: pool_PPPoE

Bridge: bridge1_ca

Incoming Filter:

Outgoing Filter:

DNS Server: 192.168.255.1
192.168.255.9

WINS Server:

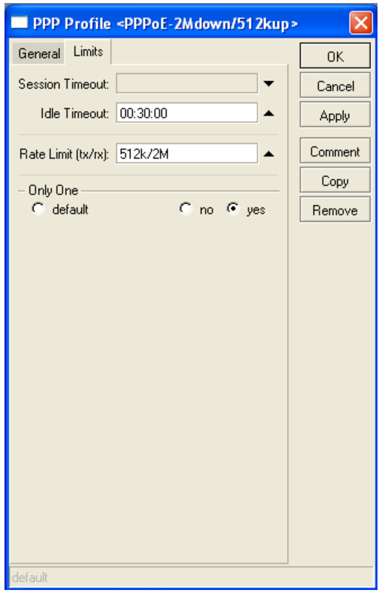
Use Compression: ○ default ● no ○ yes

Use VJ Compression: ○ default ● no ○ yes

Use Encryption: ○ default ○ no ● yes ○ required

Change TCP MSS: ○ default ○ no ● yes

default



Session Timeout:

Idle Timeout: 00:30:00

Rate Limit (tx/rx): 512k/2M

Only One: ○ default ○ no ● yes

default

The declaration of TX and RX rate are interchanged in the Winbox!

Order:
RX / TX from AC view!

(checked up to 3.0RC4)

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – central services
  - The PPPoE server – IP management

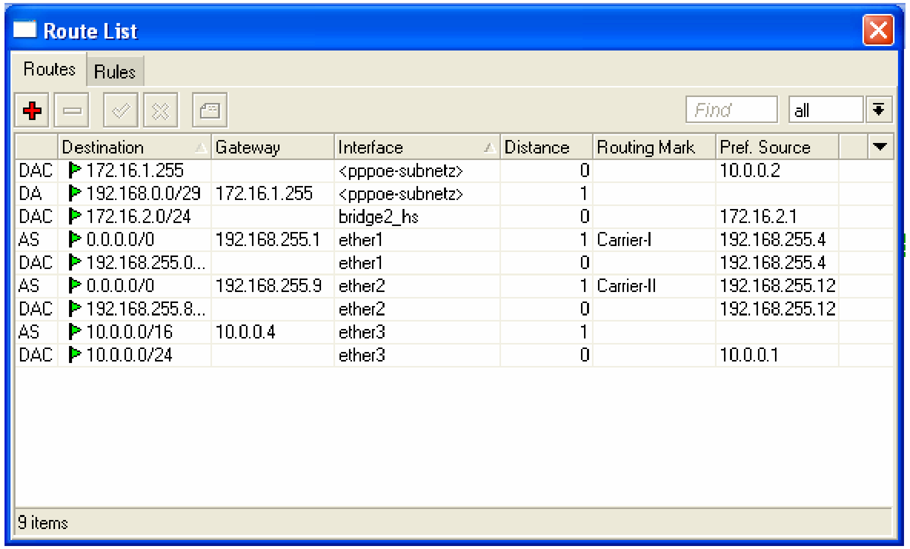
```
[admin@inet-gw] > ppp profile print
Flags: * - default
 2   name="PPPoE-2Mdown/512kup" local-address=10.0.0.2 remote-address=pool_PPPoE
     bridge=bridge1_ca idle-timeout=30m use-compression=no use-vj-compression=no use-
    encryption=yes only-one=yes change-tcp-mss=yes rate-limit=512k/2M
    dns-server=192.168.255.1,192.168.255.9

[admin@inet-gw] > ppp secret print detail
Flags: X - disabled
4   name="subnetz" service=pppoe caller-id="" password="subnetz" profile=PPPoE-2Mdown/512kup
    remote-address=172.16.1.255 routes="192.168.0.0/29" limit-bytes-in=0 limit-bytes-out=0
```

IP subnets can also be easily assigned to customers using the user configuration. Here we route the subnet 192.168.0.0/29 over the remote IP address 172.16.1.255 thru the PPPoE tunnel to the customer.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – central services

  - During the PPPoE login from the user “subnetz”, RouterOS generate the needed two routes on the fly.



Route List

	Destination	Gateway	Interface	Distance	Routing Mark	Pref. Source
DAC	172.16.1.255		<pppoe-subnetz>	0		10.0.0.2
DA	192.168.0.0/29	172.16.1.255	<pppoe-subnetz>	1		
DAC	172.16.2.0/24		bridge2_hs	0		172.16.2.1
AS	0.0.0.0/0	192.168.255.1	ether1	1	Carrier-I	192.168.255.4
DAC	192.168.255.0...		ether1	0		192.168.255.4
AS	0.0.0.0/0	192.168.255.9	ether2	1	Carrier-II	192.168.255.12
DAC	192.168.255.8...		ether2	0		192.168.255.12
AS	10.0.0.0/16	10.0.0.4	ether3	1		
DAC	10.0.0.0/24		ether3	0		10.0.0.1

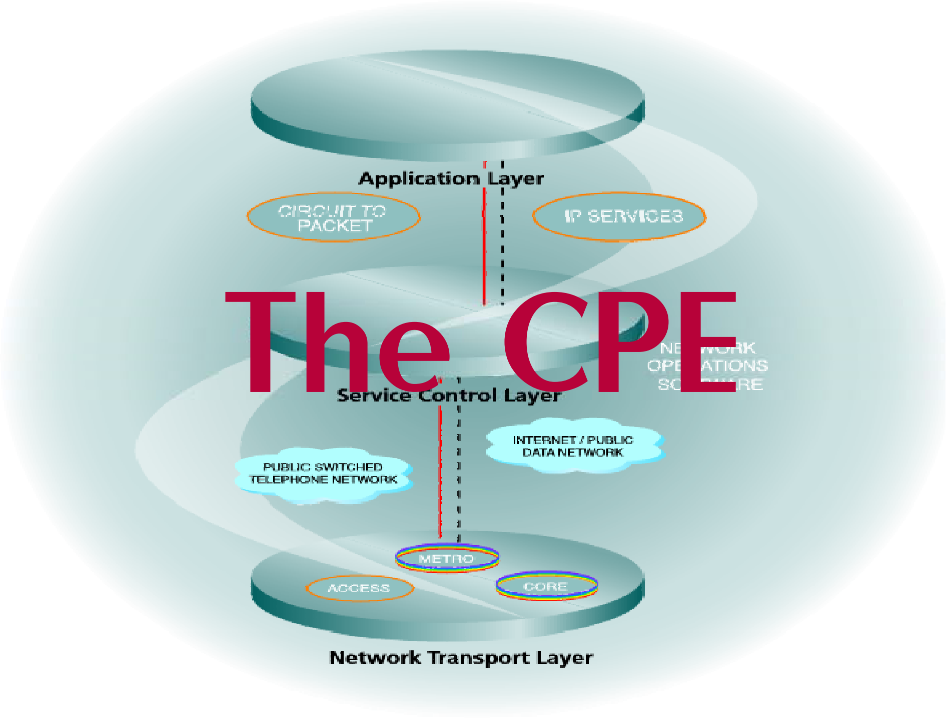
9 items

  - The whole IP management for all customers can be done on one central system. The whole backbone needs no routing information for the assigned customer IP addresses and/or IP (sub) networks.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- Network details – central services
  - The HotSpot server
    - Runs on the bridge which have all the EoIP tunnel to the HotSpot interfaces on the CAPs.
    - The HotSpot network is totally decoupled from the network for the customer which have fixed connections.
    - Can be use NAT IPs or public IPs for the customers. Depending what you want to allow your customers.
    - In this presentation we will not go deeper in the HotSpot configuration and possibilities. This is stuff for an own presentation. We only described how to implement a working HotSpot infrastructure across a routed backbone. Please keep in mind, that in a HotSpot installation a transparent layer2 connectivity between the HotSpot gateway and the HotSpot client is needed. Otherwise fundamental features of a HotSpot wouldn't work.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3



The CPE

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- The CPE
  - The CPE can – using the same Hardware – be used in two different types of configurations:
    - As a L-DSL Modem (**L**ike a **DSL** Modem)
      - In this mode the CPE works *like* a DSL Modem in a DSL infrastructure. This means that the customer can connect any DSL router (better: PPPoE router) or a system with integrated PPPoE client behind the CPE and log into the operators infrastructure using the given credentials.
    - As a router with or without NAT for the customer
      - The operator want to advertise that his customers don't need any own equipment? No problem, all you need for a high end router and firewall is included in RouterOS. Just configure a PPPoE client on the wlan interface and you have a router for that customer. Regardless if you want to use NAT or not, you have all possibilities you need to fit customers requirements. As value added service you can sell managed security services with this RouterOS device without the needs of a second appliance.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- The CPE as L-DSL modem
  - Only a few configuration steps needed. Just put wlan and ethernet interface in one bridge.

```
[admin@client-2] > interface wireless print
Flags: X - disabled, R - running
 0  R name="wlan1" mtu=1500 mac-address=00:12:17:5D:16:89 arp=enabled interface-type=Atheros
      AR5213 mode=station-pseudobridge ssid="www.meconet.de" frequency=5660 band=5ghz scan-
      list=5470-5720 antenna-mode=ant-a wds-mode=disabled wds-default-bridge=none
      wds-ignore-ssid=no default-authentication=yes default-forwarding=yes default-ap-tx-limit=0 default-
      client-tx-limit=0 hide-ssid=no security-profile=WPA2-CA compression=no

[admin@client-2] > interface bridge print
Flags: X - disabled, R - running
 0  R name="bridge1_pppoe" mtu=1500 arp=enabled mac-address=00:0C:42:15:36:4E protocol-
      mode=none priority=0x8000 auto-mac=yes admin-mac=00:00:00:00:00:00 max-message-age=20s
      forward-delay=15s transmit-hold-count=6 ageing-time=5m

[admin@client-2] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic
 #   INTERFACE     BRIDGE        PRIORITY PATH-COST
 0   ether1        bridge1_pppoe 0x80     10
 1   wlan1         bridge1_pppoe 0x80     10
```

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- The CPE as L-DSL modem
  - The management IP address for the administrative tasks will be assigned using the DHCP client on the CPE after the WLAN connect is established. (Can also be configured static).

```
[admin@client-2] > ip dhcp-client print detail
Flags: X - disabled, I - invalid
 0   interface=bridge1_pppoe host-name="client-2" client-id="client-2"
     add-default-route=yes use-peer-ntp=yes status=bound
     address=10.0.3.253/25 gateway=10.0.3.129 dhcp-server=10.0.3.129
     primary-ntp=10.0.0.1 expires-after=39m53s
```

  - Now the customer behind the L-DSL modem can start any PPPoE-Client thru the CPE and the operator had administrative access to the CPE.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- The CPE as L-DSL modem
  - To secure the CPE against customer attacks just use some bridge filter which only allow PPPoE traffic thru the CPE and drop all other from customer side. So the customer is not able to do any session to the CPE.

```
[admin@client-2] > interface bridge filter print
Flags: X - disabled, I - invalid, D - dynamic
 0   ;;; allow PPPoE-Discovery from ether1
     chain=forward out-interface=wlan1 action=accept in-interface=ether1
     mac-protocol=0x8863
 1   ;;; allow PPPoE-Session from ether1
     chain=forward out-interface=wlan1 action=accept in-interface=ether1
     mac-protocol=0x8864
 2   ;;; Block all other from ether1
     chain=forward action=drop in-interface=ether1
 3   ;;; Block all other from ether1
     chain=input action=drop in-interface=ether1
```

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

- The CPE as (NAT) router
  - For this configuration the PPPoE credentials must be configured within the PPPoE client running on the wlan interface of the CPE. After the PPPoE session from the CPE to the AC is established, you can use the CPE as router with or without NAT for customers access to the internet.

```
 0  R name="wlan1" mtu=1500 mac-address=00:12:17:5D:18:61 arp=enabled
      interface-type=Atheros AR5213 radio-name="client-1" mode=station
      ssid="www.meconet.de" frequency-mode=regulatory-domain country=germany antenna-
      gain=15 band=5ghz scan-list=5470-5720 ack-timeout=dynamic tx-power-mode=default
      default-authentication=no default-forwarding=yes proprietary-extensions=post-2.9.25
      security-profile=WPA2-CA

[admin@client-1] > interface pppoe-client print detail
Flags: X - disabled, R - running
 0  R name="pppoe-out1" max-mtu=1480 max-mru=1480 interface=wlan1
      user="router-1" password="router-1" profile=default service-name=""
      ac-name="" add-default-route=yes dial-on-demand=no use-peer-dns=yes
      allow=pap,chap,mschap1,mschap2
```

Building scalable and reliable WISP and city carrier networks based on RouterOS 3

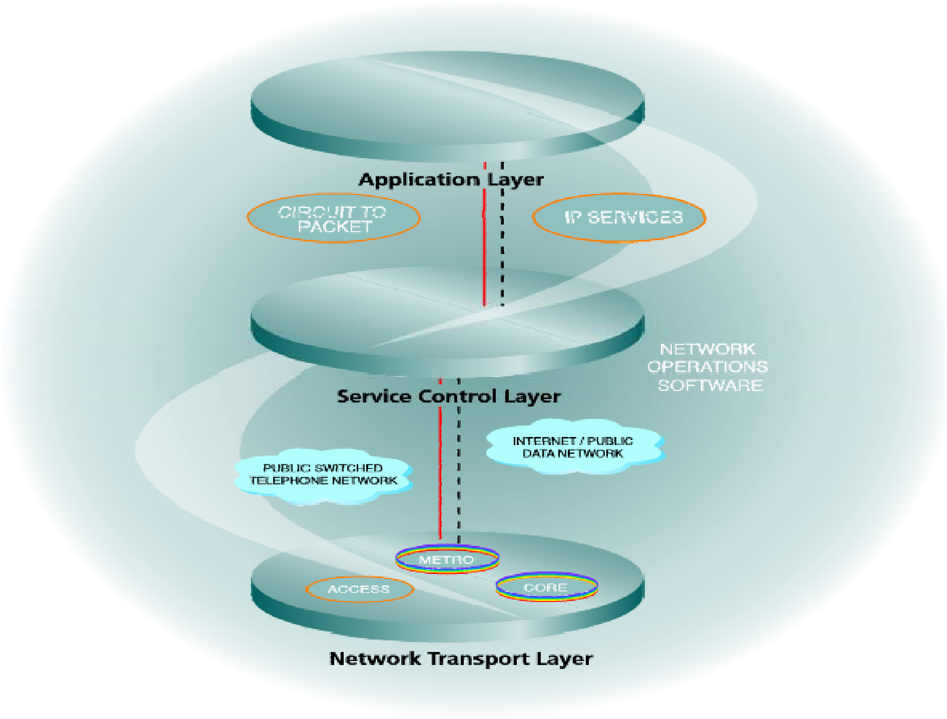
- The CPE as (NAT) router

  - For administrative traffic the CPE needs a static route to the management network.

```
[admin@client-1] > ip route print
Flags: B - blackhole, U - unreachable, P - prohibit, X - disabled, A - active,
D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf
 #       DST-ADDRESS      PREF-SRC       G GATEWAY        DIS INTERFACE
 0  AD    0.0.0.0/0                      r   10.0.0.2       1   pppoe-out1
 1  AS    10.0.0.0/24                    r  10.0.3.129      1   wlan1
 2  ADC  10.0.0.2/32      172.16.1.254                      0   pppoe-out1
 3  ADC  10.0.3.128/25    10.0.3.251                        0   wlan1
 4  ADC  192.168.1.0/24   192.168.1.1                       0   ether1
```

  - For securing the CPE just use input filter to block access from the customer network to the CPE.

Building scalable and reliable WISP and city carrier networks based on RouterOS 3



We thank you for you attention

For advanced information just send an email to info@meconet.de