BUILDING AND RUNNING

A SUCCESSFUL WISP

with a very low budget

Lagos, Nigeria *28th november 2017*

SPADHAUSEN
internet provider

Dott. Elia Spadoni
Network Administrator

ABOUT ME

- **Worked in the IT industry and Small ISPs since 2002 as CTO**
- **Founder of Spadhausen ISP, in 2008**
- **My company is member of RIPE as LIR**
- **MikroTik certified since 2016**

Microsoft CERTIFIED Professional

ePMP CERTIFIED Cambium Networks

UBIQUITI Broadband Wireless Admin UBWA

MikroTik MTCNA | MikroTik MTCRE | MikroTik MTCTCE | MikroTik MTCWE | MikroTik MTCINE

Dott. Elia Spadoni
Network Administrator

COMPANY PROFILE

Spadhausen Internet Provider was established in 2008

Since 2011 we began offering WISP service, high speed broadband access using wireless technologies to overcome the digital divide in our region.
Our area of operations covers a large rural territory and a lot of small towns, where big telcos don't upgrade infrastructures because of the low density of users.

We provide full support to our users without any call-centers, and are very close to them in any way! We are in a small town where people can find us easily, away from the big city!

Dott. Elia Spadoni
Network Administrator

COMPANY'S TIMELINE

2008 : Foundation as one-man consulting firm

2011 : Start WISP operation

2013 : 1° employee and about 230 customers

2017 : Over 2700+ customers and 13 employee

We are growing at about 85 wireless users per month

WIRELESS COVERAGE MAY 2017

100%

of the depicted areas

1000 km²

Lagos, Nigeria

28th november 2017

SPADHAUSEN
internet provider

Dott. Elia Spadoni
Network Administrator

PRESENTATION AGENDA

1. Key facts for anyone wants to begin a small WISP
2. Choosing the right network topology
3. Mantaining the network and the customers
    a. Traffic management and limiting (queues)
    b. Basic firewall rules
4. What do we use

SPADHAUSEN
internet provider

Dott. Elia Spadoni
Network Administrator

KEY FATCS FOR ANYONE WANTS TO BEGIN A SMALL WISP

1. Great ideas, rarely have financial coverage
2. You want (someday) to earn something
3. Start from a weak spot in the available services
4. Be able to offer a service or a way that is missing
5. Have a precise TARGET
6. Know what you have required for your services
7. Keep it simple and optimize everything

Dott. Elia Spadoni
Network Administrator

CHOOSING THE RIGHT NETWORK TOPOLOGY

We assume that we have a single access to internet, through a BORDER ROUTER at the edge of the network.

We start with a single tower, that can be easily expanded through the development of your network backbone (that we represent with a cloud), that can be formed by static/dynamic routing between our nodes.

We do NAT from the border router towards our customers.

Dott. Elia Spadoni
Network Administrator

CHOOSING THE RIGHT NETWORK TOPOLOGY

PPPoE

PRO

Require «ppp» package in RouterOS
May use an external Radius Server
Centrally managed users, with all their attributes
If someone doesnt have the credentials, he CAN'T use your network!
Combination username/password and you are ready to go
Bandwidth can be centrally managed via radius attributes to each PPP users

SPADHAUSEN
internet provider

Dott. Elia Spadoni
Network Administrator

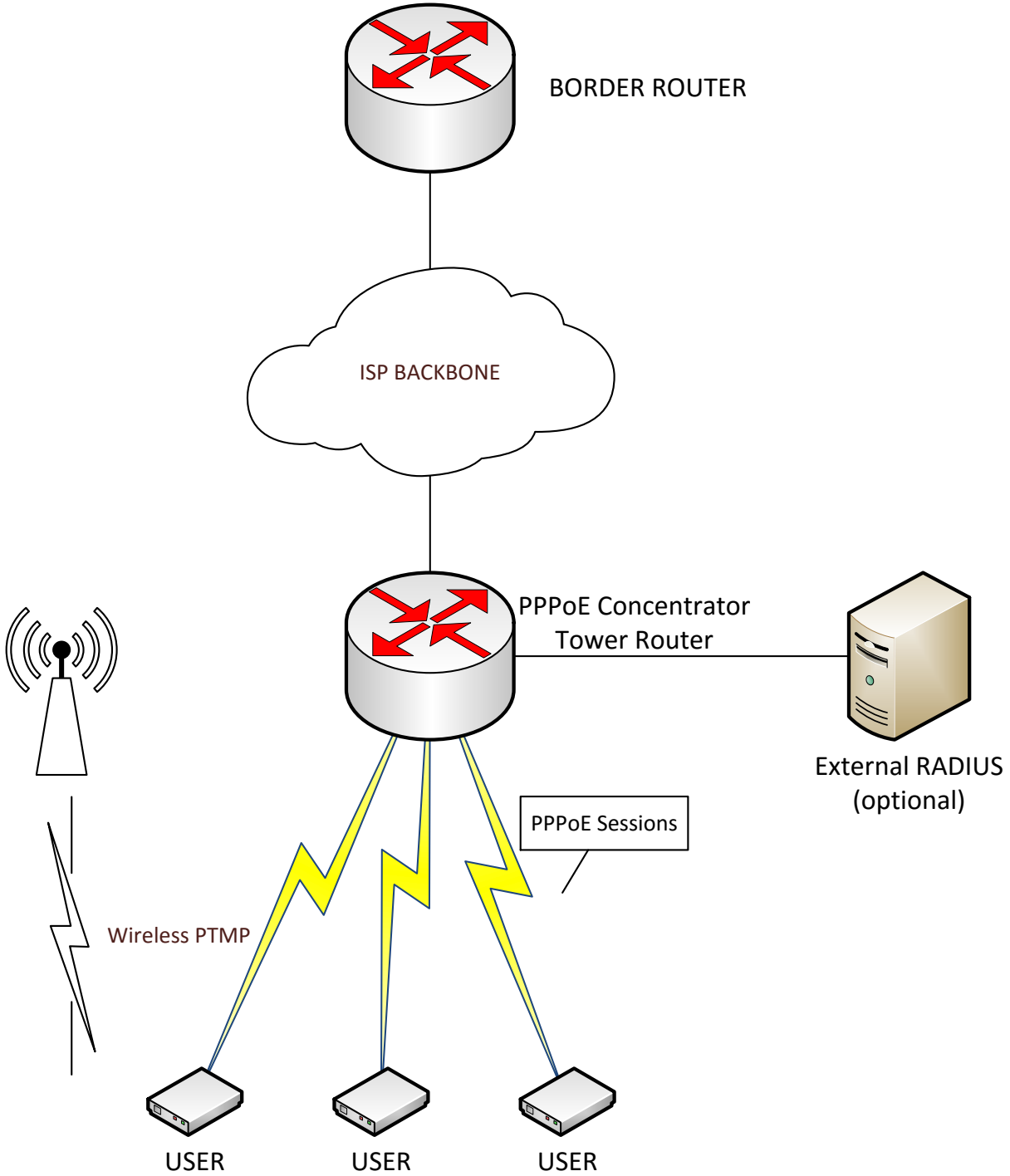
CHOOSING THE RIGHT NETWORK TOPOLOGY

PPPoE

cons

Added complexity of the network, need an auth server (as Radius)
If your wireless devices can do QoS over L2, with PPPoE is not possibile
If the Radius Server or PPPoE Concentrator goes offline, you are offline
You could need a separate server for Radius
MTU issues with protocols with larger MTU
If your wireless network has packet loss, PPP session can drop!
PPPoE is done in software, so you need a strong central router

Dott. Elia Spadoni
Network Administrator


BORDER ROUTER
ISP BACKBONE
PPPoE Concentrator
Tower Router
External RADIUS
(optional)
PPPoE Sessions
Wireless PTMP
USER
USER
USER

CHOOSING THE RIGHT NETWORK TOPOLOGY

Routed network

PRO

Works based on static or dynamic routing (OSPF)
No tunnels, no ip manipulation involved
Need a subnet for each tower
Pure ip packet as in a ethernet network, DHCP or static IP assigned
Every tower, or router can be an indipendent entity

Lagos, Nigeria *28th november 2017*

SPADHAUSEN
internet provider

Dott. Elia Spadoni
Network Administrator

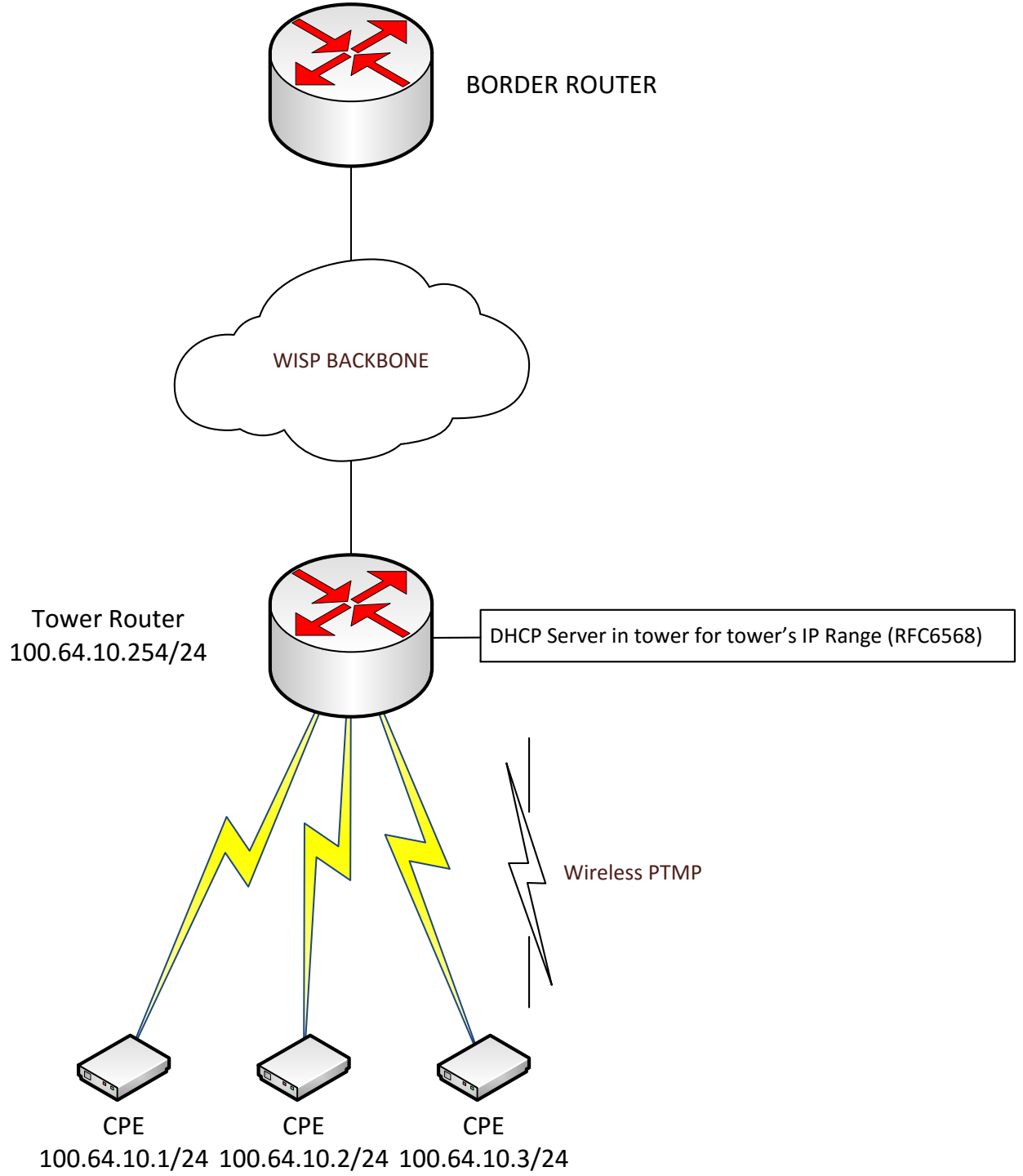
CHOOSING THE RIGHT NETWORK TOPOLOGY

routed network

cons

No central management possibile (as PPPoE)
Every user have an IP, dinamically or statically assigned
Need to know how routing works
You can use queues to statically (per IP) limit the traffic

Dott. Elia Spadoni
Network Administrator


BORDER ROUTER
WISP BACKBONE
Tower Router
100.64.10.254/24
DHCP Server in tower for tower's IP Range (RFC6568)
Wireless PTMP
CPE
100.64.10.1/24
CPE
100.64.10.2/24
CPE
100.64.10.3/24

MANTAINING THE NETWORK AND THE USERS

Traffic control. With these feature named «queues» you can easily limit traffic in your network

We use SIMPLE QUEUES and PARENT QUEUE

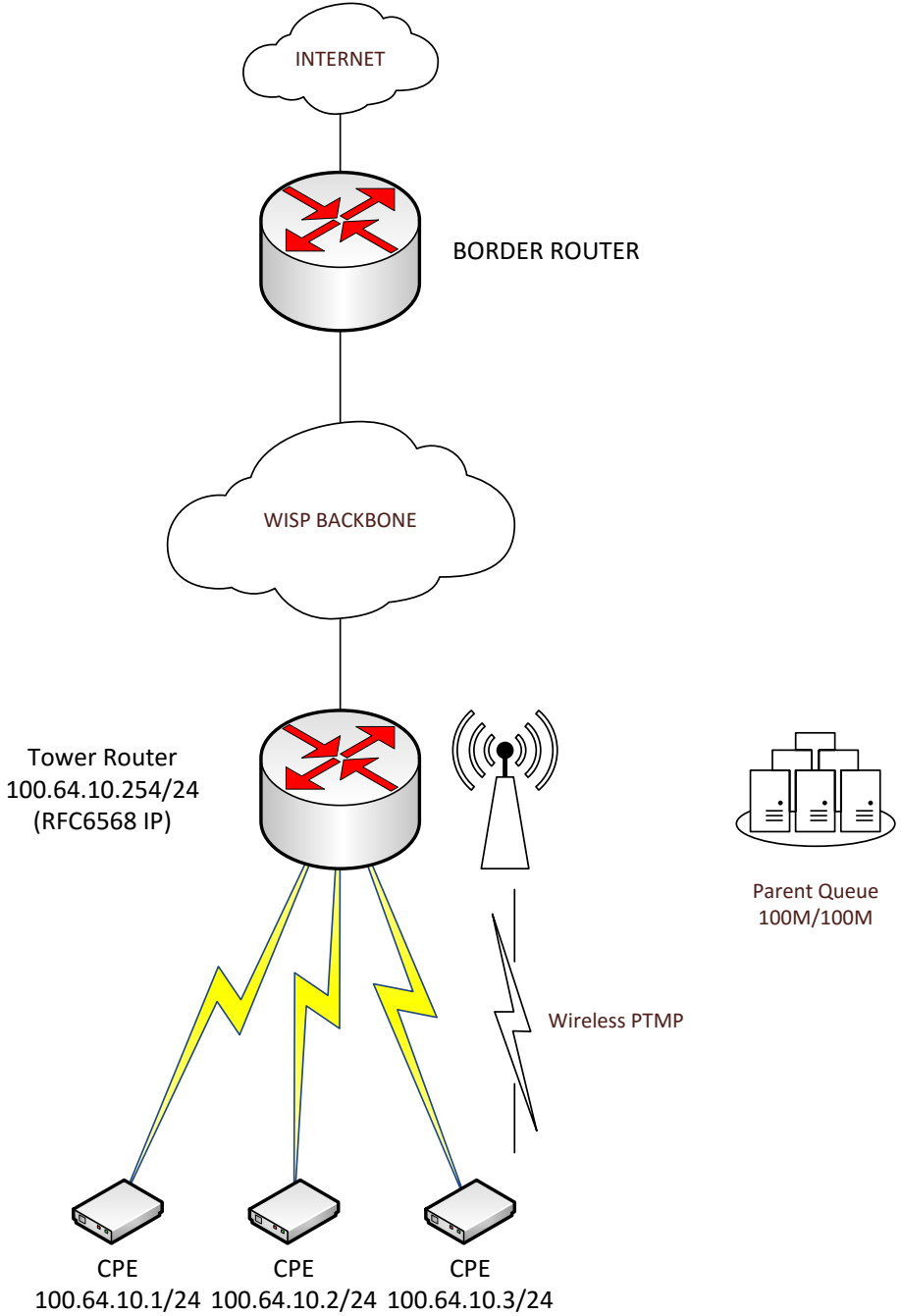
For each tower you have, you have to DEFINE a specific capacity (bandwidth available) You set MAX download and MAX upload available.

```
/queue simple
add max-limit=100M/100M name=TOWER_1 queue=default/default target=100.64.10.0/24

/queue simple
add limit-at=256k/2M max-limit=2M/10M name=user1 parent=TOWER_1 queue=default/default target=100.64.10.1
```

You create a queue for «user1» with a specific bandwith profile

With the limit-at you set a sort of MCR (minimum committed rate), and using priority you can give bandwith first to specific users (1 top, 8 low)



/queue simple add max-limit=100M/100M name=TOWER_1 queue=default/default target=100.64.10.0/24
/queue simple add limit-at=256k/2M max-limit=2M/10M name=user1 parent=TOWER_1 queue=default/default target=100.64.10.1

MANTAINING THE NETWORK AND THE USERS

You can limit the EGRESS traffic, not INGRESS.

If you limit at the top edge of the network, then ad the lower part of it, you have the simplest (but effective) traffic control, that is very easy to manage, so your backbone let pass only the exact amount of traffic for each user connectivity.

There are ways to manage traffic that are better (more articolate), but not so easy to mantain if you are new to this business,

With the simple queues you are able to easily manage the bandwidth, without complex systems of traffic and packet markings.

Dott. Elia Spadoni
Network Administrator

MANTAINING THE NETWORK AND THE USERS

Protect your users

In RouterOS you have a powerful firewall that can protect your users and devices

You have two directions to filter

INGRESS at the edge of the network

Protect from external attacks (DNS amplifications, SSH bruteforces, worms)

EGRESS near the access level

Filter what goes out to the internet from your network (NetBIOS broadcast or queries, worms, etc)

IP FIREWALL FILTER is your RouterOS section

MANTAINING THE NETWORK AND THE USERS

INGRESS RULES

SSH Bruteforce Prevention

Source: https://wiki.mikrotik.com/wiki/Bruteforce_login_prevention

```
add chain=input comment="Regole in entrata specifiche sul router" protocol=icmp
add chain=input connection-state=established,related
add action=drop chain=input connection-state=invalid

add action=reject chain=forward comment= "INBOUND" dst-address=xxxxx dst-port=22,53,80,135-139,445,593,1433-1434,4444 in-
interface=WAN_INTERFACE protocol=tcp reject-with=icmp-admin-prohibited
add action=reject chain=forward dst-address=xxxxx dst-port=161,135-139,445,593,1433-1434,1900 protocol=udp reject-with=icmp-
admin-prohibited
```

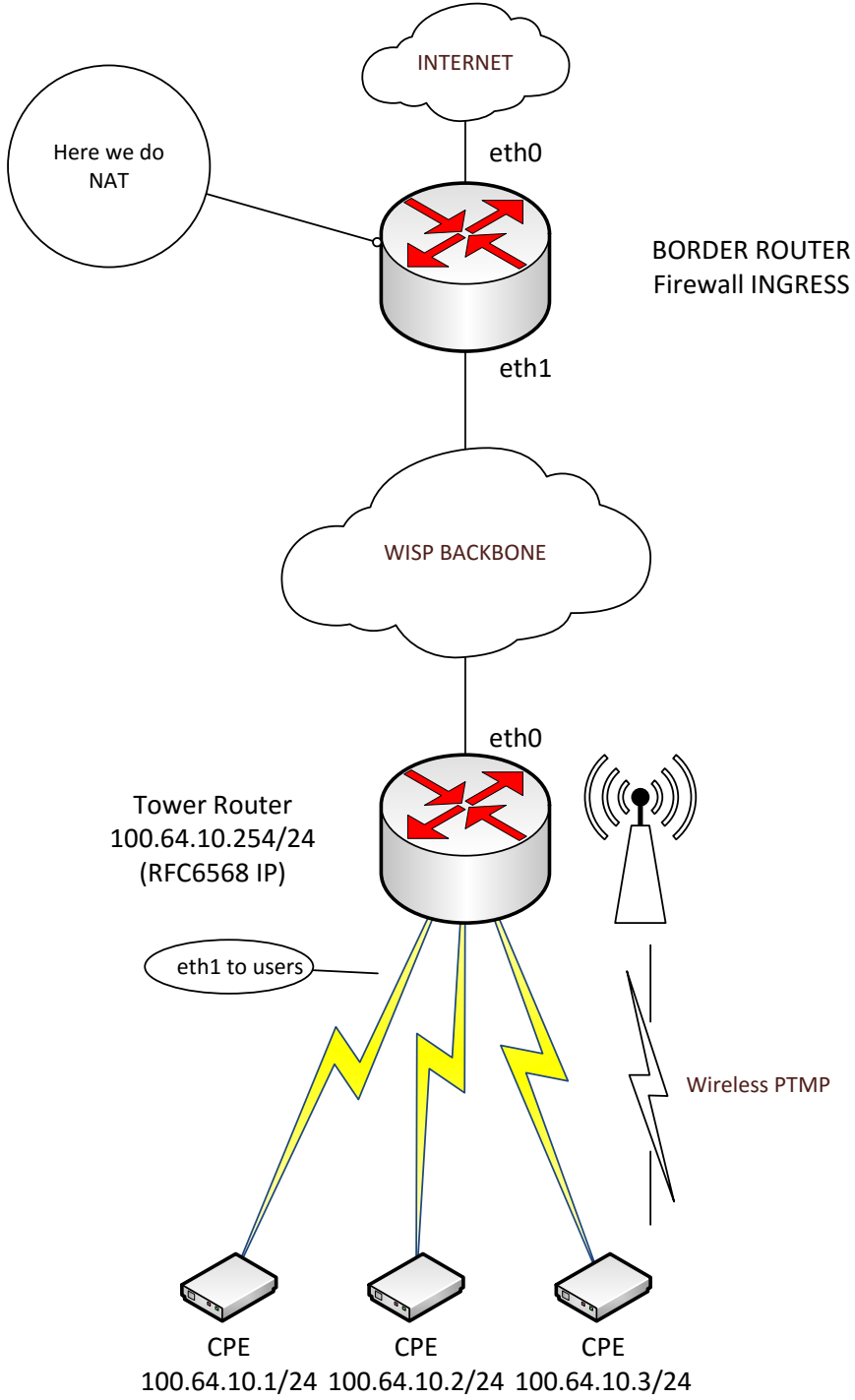
With these rules, you can protect the management ports (22,80) for the CPE of the users.
You can protect DNS, SNMP, NetBIOS ingress, SQL and uPnP.

MANTAINING THE NETWORK AND THE USERS

EGRESS RULES

```
add action=reject chain=forward comment="OUTBOUND" dst-port=135,139,445,593,4444 in-interface=ether11 protocol=tcp reject-
with=icmp-admin-prohibited
add action=reject chain=forward dst-port=69,137-139,593,1900 in-interface=TO_MY_BACKBONE protocol=udp reject-with=icmp-
admin-prohibited
```


Dott. Elia Spadoni
Network Administrator


INTERNET
Here we do NAT
eth0
BORDER ROUTER
Firewall INGRESS
eth1
WISP BACKBONE
eth0
Tower Router
100.64.10.254/24
(RFC6568 IP)
eth1 to users
Wireless PTMP
CPE
100.64.10.1/24
CPE
100.64.10.2/24
CPE
100.64.10.3/24

MANTAINING THE NETWORK AND THE USERS

We have a single internet access, and have a pool of public IP addresses.

We decide to do NAT 1-1

```
ip firewall nat
add action=src-nat chain=srcnat out-interface=eth0 src-address=100.64.10.1 to-addresses=1.1.1.1
add action=dst-nat chain=dstnat dst-address=1.1.1.1 in-interface=eth0 to-addresses=100.64.10.1



Then we do a nat overload for the IP that we don’t want to directly map 1-1

add action=src-nat chain=srcnat comment="NAT for everyone" out-interface=eth0 src-address=100.64.10.0/24 to-addresses=1.1.1.254

We decide to NAT all the 100.64.10.0/24 network to wan public ip 1.1.1.254
```

We can also route this IP to the tower and give them directly to our users.

Dott. Elia Spadoni
Network Administrator

WHAT DO WE USE TO RUN OUR NETWORK

TOWER

1xTower Router (Routerboard)
POE Switch for APs (or use the POE-out in some cases)

CPE

Wireless STA in NAT/Router Mode
Wireless AP at customer's home

Dott. Elia Spadoni
Network Administrator

WHAT DO WE USE TO RUN OUR NETWORK

Know your hardware very well!
You will find a lot of routerboards that can do your task

How to choose the right routerboard

What amount of traffic does the router needs to operate? – Check your datasheet CPU/RAM

Know your hardware limit – Study the block diagram

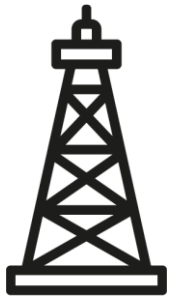
Need many ports? – Do you need the onboard switch?

Dott. Elia Spadoni
Network Administrator

WE DO WE USE TO RUN OUR NETWORK

Small sized tower

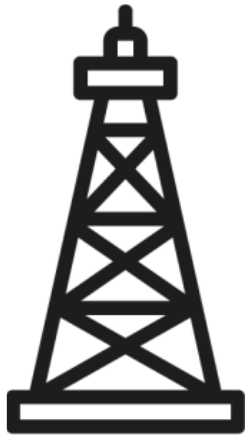
~40 users/queues



Routerboard Hex lite
or similar 1xCPU

Medium sized tower

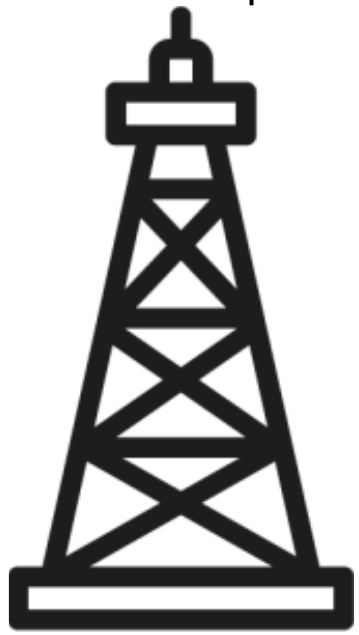
~100 users/queues



Routerboard Hex/RB3011

Large sized tower

>100 users/queues



RB1100AHx2; CCR1009

SPADHAUSEN
internet provider

Dott. Elia Spadoni
Network Administrator

THANK YOU

TO CONTACT ME

LinkedIn
admin@spadhausen.com
www.spadhausen.com