

# *Access Point Fault Tolerance with VirtualAP, netwatch and scripts*

*Name: Armando Ventura  
Portugal*

*Email: [armando@semcabo.pt](mailto:armando@semcabo.pt)*

*MUM – Portugal - 2016*

# Acerca de mim

- Licenciatura, Mestrado e Doutorando na área de Engenharia Informática
- Fundador em 2004 da Empresa SEMCABO, a qual se tornou ISP em Portugal em 2007 (**ICP-ANACOM Nº17/2007**)  
<http://www.sem cabo.pt>  
armando@semcabo.pt
- Investigador no Laboratório **UBINET- Segurança Informática e Cibercrime (Local: Beja)**  
<http://ubinet.ipbeja.pt>  
ajventura@ubinet.ipbeja.pt
- Professor na Escola Superior de Tecnologias e Gestão de Beja do Instituto Politécnico de Beja desde 2004  
Área de Engenharia Informática / Segurança Informática  
Cursos: Licenciatura em Engenharia Informática  
Mestrado em Engenharia de Segurança Informática  
Disciplinas: Redes de Computadores 1 e 2  
Administração de Sistemas  
Linguagens de Programação Dinâmicas  
<http://www.ipbeja.pt>  
ajventura@ipbeja.pt

# Acerca de mim

- Certificações Mikrotik
  - MTCNA (MikroTik Certified Network Associate)
  - MTCRE (MikroTik Certified Routing Engineer)
  - MTCWE (MikroTik Certified Wireless Engineer)
  - MTCTCE (MikroTik Certified Traffic Control Engineer)
- Certified Trainer MIKROTIK nas certificações: MTCNA, MTCRE, MTCWE e MTCTCE

Próximo curso 2em1 MTCNA e MTCWE - Dia 6 de Junho de 2016  
Local: Algarve

INSCRIÇÕES em <http://mikrotik.sem cabo.pt> ou <http://www.sem cabo.pt>  
para informações

# Acerca da Empresa “SEMCABO”

- Escritórios em Sines
- ISP desde 2007
- Datacenter em Sines e Lisboa
- Atividades:
  - Sistemas Wireless com gestão centralizada de utilizadores
  - Cloud
  - Servidores (Hosting, Housing, Colocation)
  - Serviço de Email Empresarial
  - Ligações dedicadas Wireless ou Fibra
  - Switching, Networking e Internetworking
  - Datacenter
  - Fiber to Room GPON (Fibra para Hóteis)
  - StrongAP (Comunicações Unificadas)
  - Etc...

Clientes: Nacionais e Internacionais, Setor Privado e Setor Público

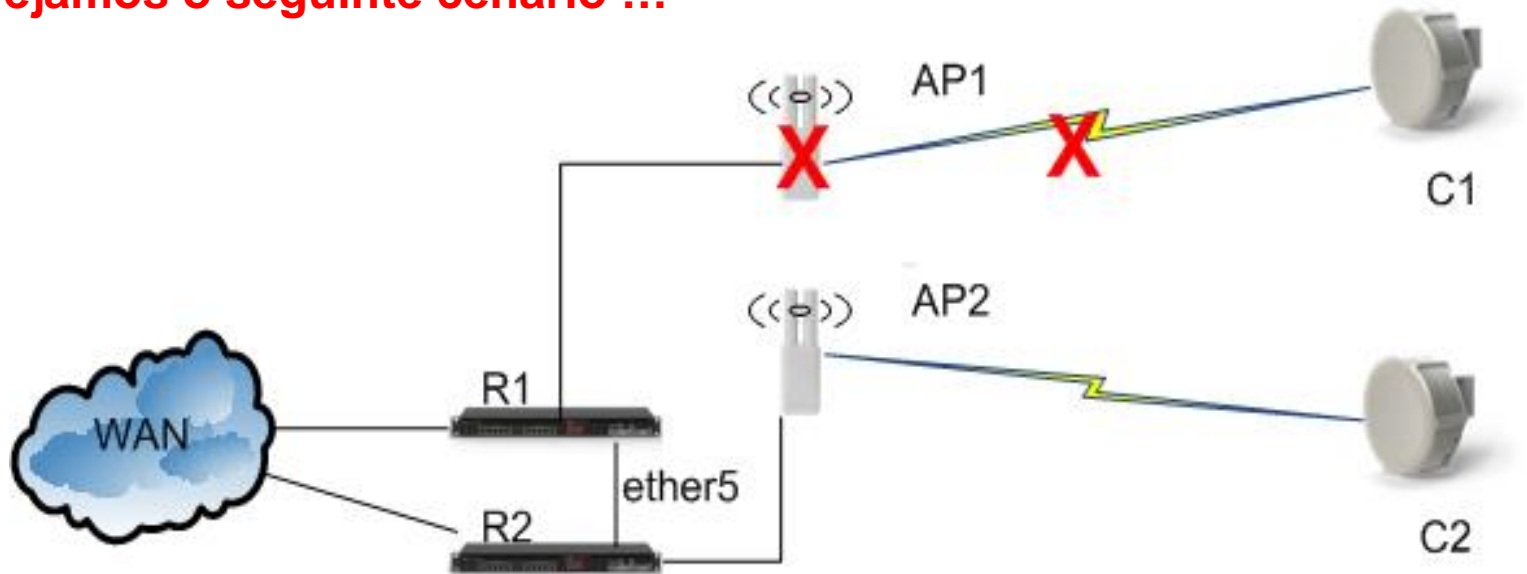
# Objetivo da apresentação

- Exemplificar a implementação de tolerância a falhas em redes wireless, concretamente nos Access Points.

# Descrivendo o problema

Quem nunca ouviu falar de redes com tolerância a falhas?

**Vejamos o seguinte cenário !!!**



**O que acontece se não providenciarmos tolerância a falha no AP1 e ele falhar?**

**Equipamentos ligados a ele falham!!! Clientes/utilizadores ficam sem rede/Internet.**

**Ficamos com grandes problemas até trocarmos o AP1!!!**

# Formulando a solução...

- Antes de focar diretamente na solução dos Access Points, não esquecer algumas questões relevantes para garantir um bom funcionamento numa rede como:
  - Utilizar energia através de UPS, baterias ou geradores
  - Instalar os equipamentos com ligação a terra e surge protectores
  - Cabo exterior blindado com fio drain
  - Ligar uma rede a dois ou mais ISPs utilizando PCC ou peering BGP
  - Utilizar routing dinâmico com RIP, OSPF ou BGP
  - Utilizar switching com STP/RSTP e MPLS
  - Etc...

# Formulando a solução...

O RouterOS tem uma série de possibilidades para providenciar tolerância a falhas de uma forma geral, com recurso a protocolos standard e features específicas para wireless como:

- routing dinâmico com RIP, OSPF ou BGP
- switching com STP/RSTP e MPLS
- VRRP (Virtual Redundante Router Protocol)
- e Feature Wireless (Connect-List)

**MAS SERÁ** que todos protocolos standard mencionados resolvem o cenário apresentado anteriormente?

**Resposta: NÃO**



# Formulando a solução...

Utilizando a feature “***connect-list***” do roteiros!!!

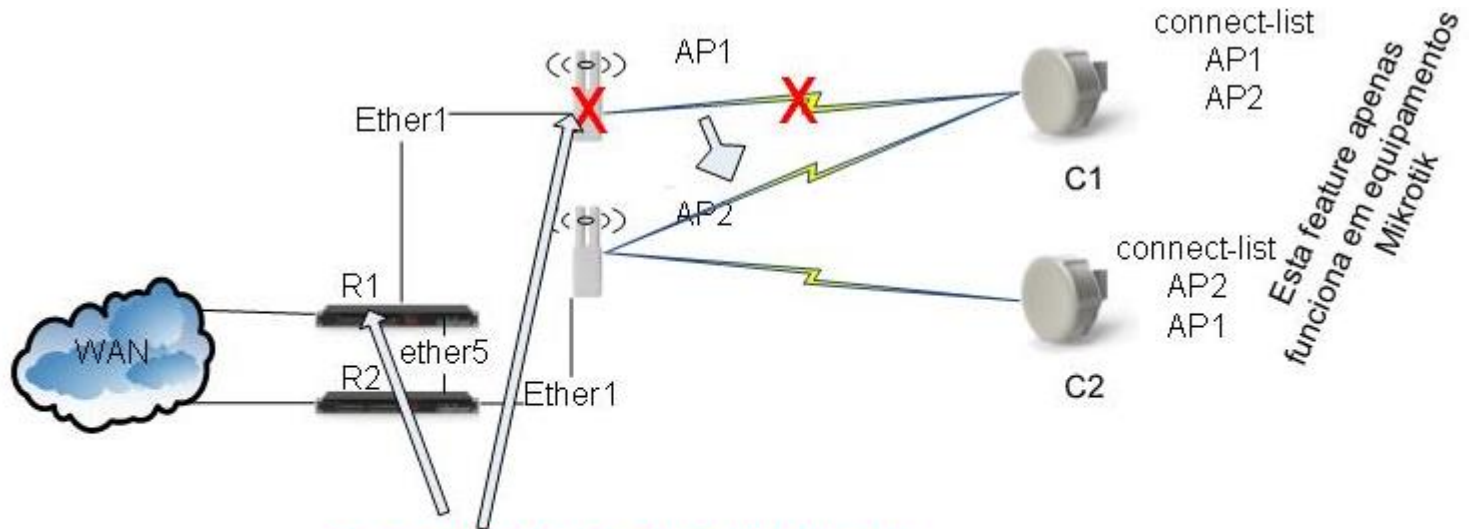
Funciona se a avaria for exclusivamente no rádio do access point, e se este deixar de emitir sinal wifi, os clientes irão se conectar a outro access point que tenha na sua lista sequencial de connect-list.

Vejam os esta solução “não ideal” como funciona.

# Formulando a solução...

(funciona apenas se o rádio do Access Point deixar de emitir sinal...)  
**Solução não ideal...**

Podemos usar “connect-list” para permitir que o cliente “C1” se conecte ao AP2 quando o emissor do AP1 falha



**E se ether1 falhar? ou R1 falhar?  
e SSID AP1 continuar a emitir sinal?  
os clientes continuam conectados ao AP1 e não terão  
rede, problemas!!!**

# Formulando a solução... “connect-list”

(funciona apenas se o rádio do Access Point deixar de emitir sinal...)

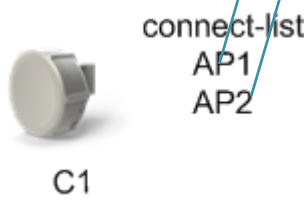
wireless

Wireless Tables

Interfaces Nstreme Dual Access List Registration **Connect List** Security Profiles

Find

| # | Interface | MAC Address       | Connect | SSID | Signal Str... | Security ... |
|---|-----------|-------------------|---------|------|---------------|--------------|
| 0 | wlan1     | D4:CA:6D:4C:A2:FB | yes     | AP1  | -120..120     | default      |
| 1 | wlan1     | D4:CA:6D:52:64:55 | yes     | AP2  | -120..120     | default      |



connect-list  
AP1  
AP2

Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme ...

Mode: station

Band: 2GHz-B/G/N

Channel Width: 20MHz

Frequency: 2412 MHz

SSID: [arrow pointing to SSID field]

Scan List: default

Wireless Protocol: unspecified

Security Profile: default

Bridge Mode: enabled

Default AP Tx Rate: [ ] bps

Default Client Tx Rate: [ ] bps

Default Authenticate

Default Forward

Hide SSID

OK  
Cancel  
Apply  
Disable  
Comment  
Torch  
Scan...  
Freq. Usage...  
Align...  
Sniff...  
Snooper...  
Reset Configuration  
Advanced Mode

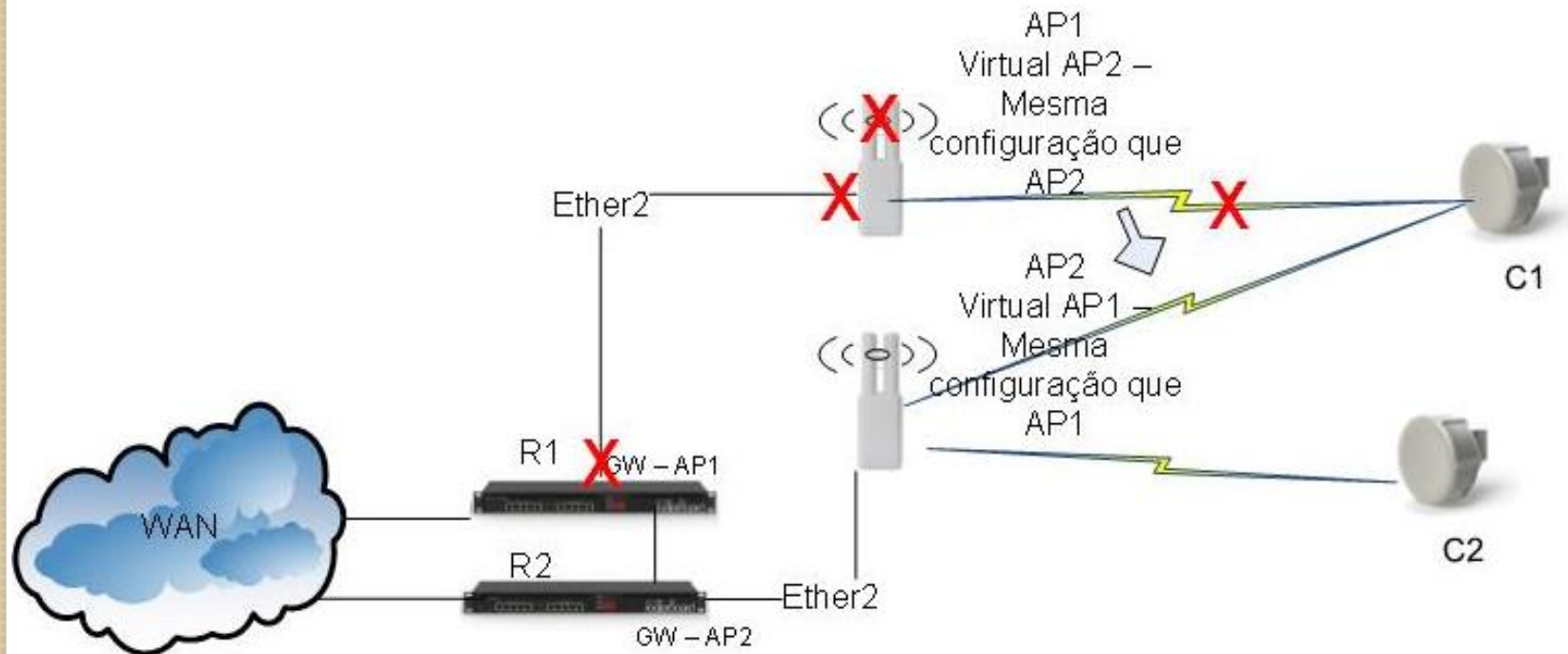
não esquecer  
SSID none  
Default Authenticate no

# Formulando a solução...

(yes reliability!!! i am relaxed with this solution, I WANT TEST AND IMPLEMENT IT)

dois Access Points a funcionar em conjunto utilizando as funcionalidades de **VirtualAP**, **netwatch** e **scripts**

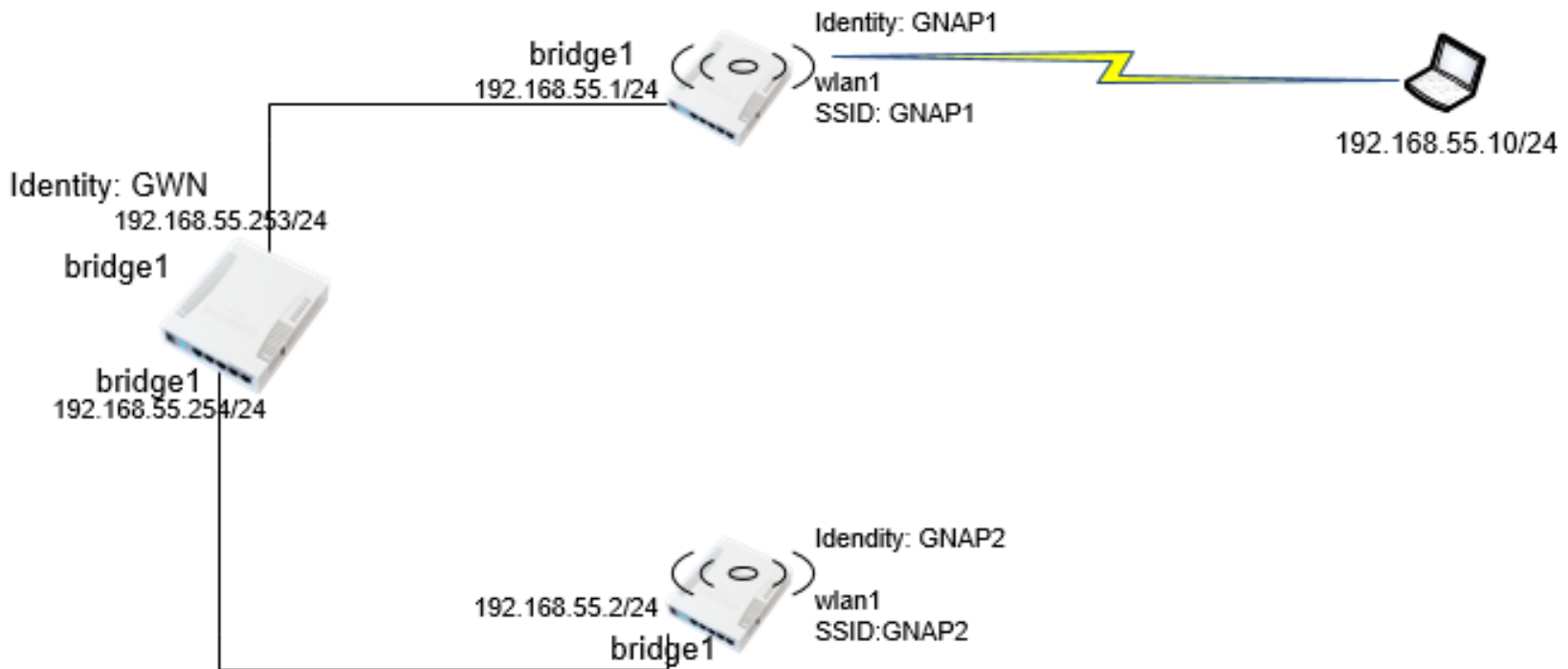
Se ethernet ou Gateway do AP1 falhar, no AP2 será ativado um Virtual AP que contém a mesma configuração do Access Point AP1



# Formulando a solução ideal com base num laboratório...

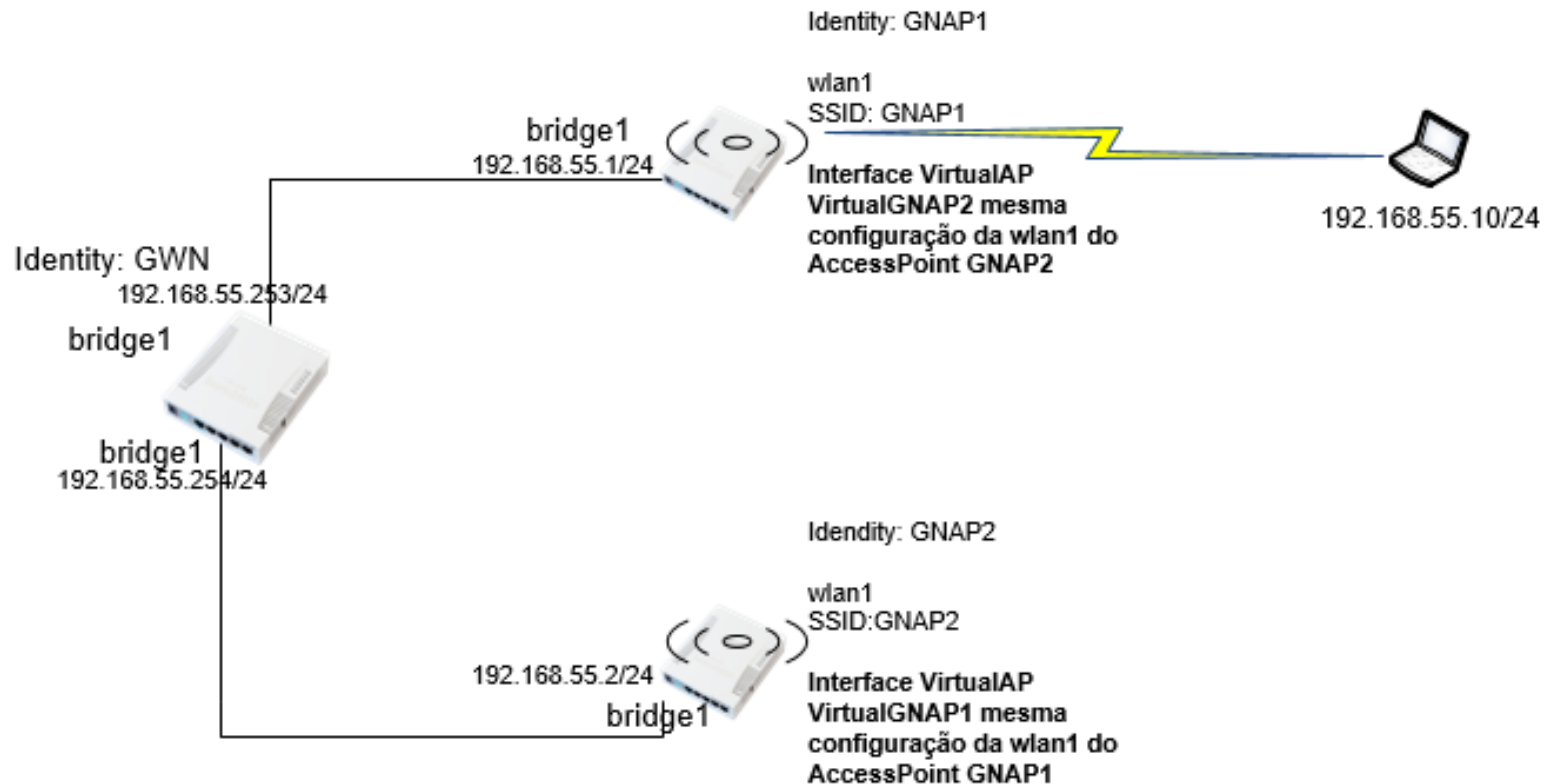
## Ponto inicial - Rede sem tolerância a falhas...

1 Gateway e 2 Access Points



# VirtualAP interface

Após a criação dos Virtuais APs ficamos com o seguinte cenário

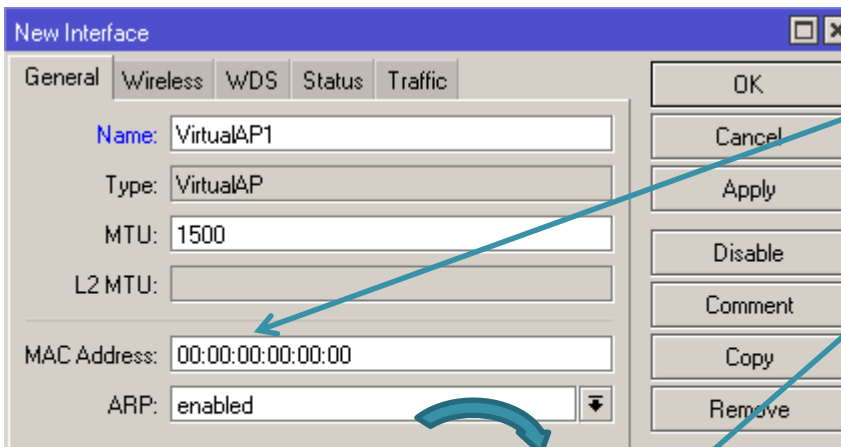
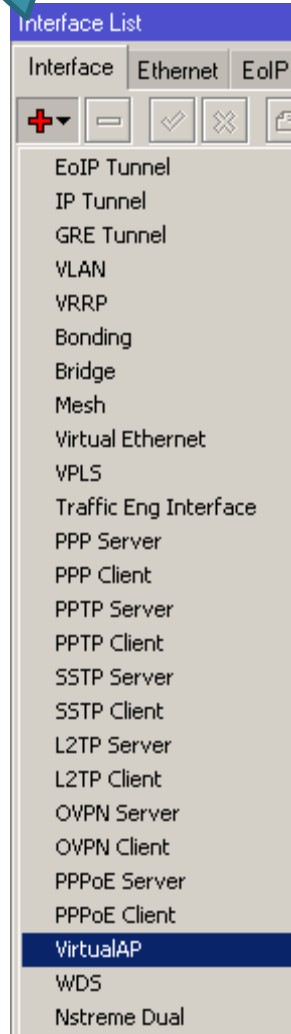


Vamos ver como criar os APs Virtuais...

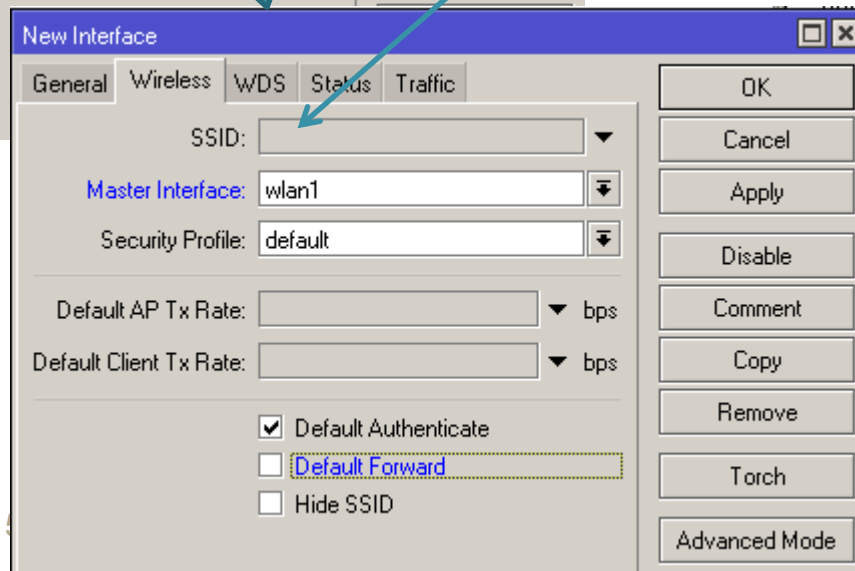
# VirtualAP interface

Virtual Access Point interface é usado para adicionar um AP virtual, pode ter endereços IP, SSID, endereço MAC e encriptação, etc

interfaces



definir mac address



definir SSID

# VirtualAP interface

Identity: GNAPl

wlan1  
SSID: GNAPl

Interface VirtualAP  
VirtualGNAP2 mesma  
configuração da wlan1 do  
AP GNAPl

Interface <VirtualAP1>

General Wireless WDS Status Traffic

Name: VirtualGNAP2

Type: VirtualAP

MTU: 1500

L2 MTU:

MAC Address:

ARP: enabled

OK Cancel Apply Disable Comment Copy Remove Torch Advanced Mode

mesmo mac address da wlan1 do GNAPl

Interface <VirtualAP2>

General Wireless WDS Status Traffic

SSID: GNAP2

Master Interface: wlan7

Security Profile: default

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

OK Cancel Apply Enable Comment Copy Remove Torch Advanced Mode

mesma SSID da wlan1 do GNAPl

Identity: GNAP2

wlan1  
SSID:GNAP2

Interface VirtualAP  
VirtualGNAP1 mesma  
configuração da wlan1 do  
AccessPoint GNAP1

Interface <VirtualAP1>

General Wireless WDS Status Traffic

Name: VirtualGNAP1

Type: VirtualAP

MTU: 1500

L2 MTU:

MAC Address:

ARP: enabled

OK Cancel Apply Disable Comment Copy Remove Torch Advanced Mode

mesmo mac address da wlan1 do GNAP1

Interface <VirtualAP2>

General Wireless WDS Status Traffic

SSID: GNAP1

Master Interface: wlan7

Security Profile: default

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

OK Cancel Apply Enable Comment Copy Remove Torch Advanced Mode

mesmo SSID da wlan1 do GNAP1



# netwatch feature

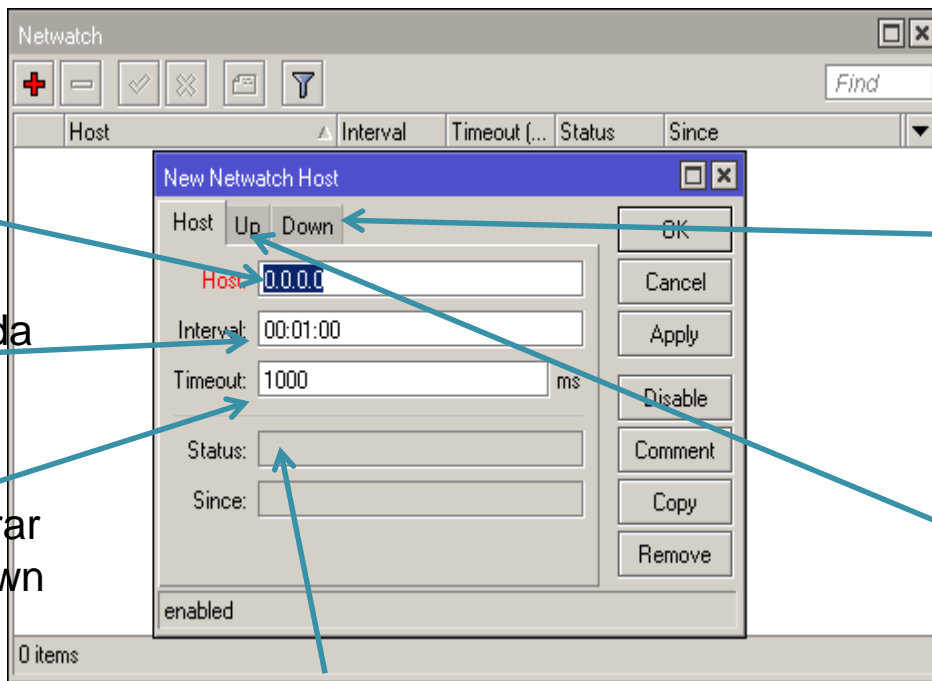
Netwatch monitoriza o status dos equipamentos de rede através do envio de pacotes ICMP “pings”

tools

ip address do equipamento a monitorar

tempo entre cada Icmp “ping”

tempo para considerar um equipamento down

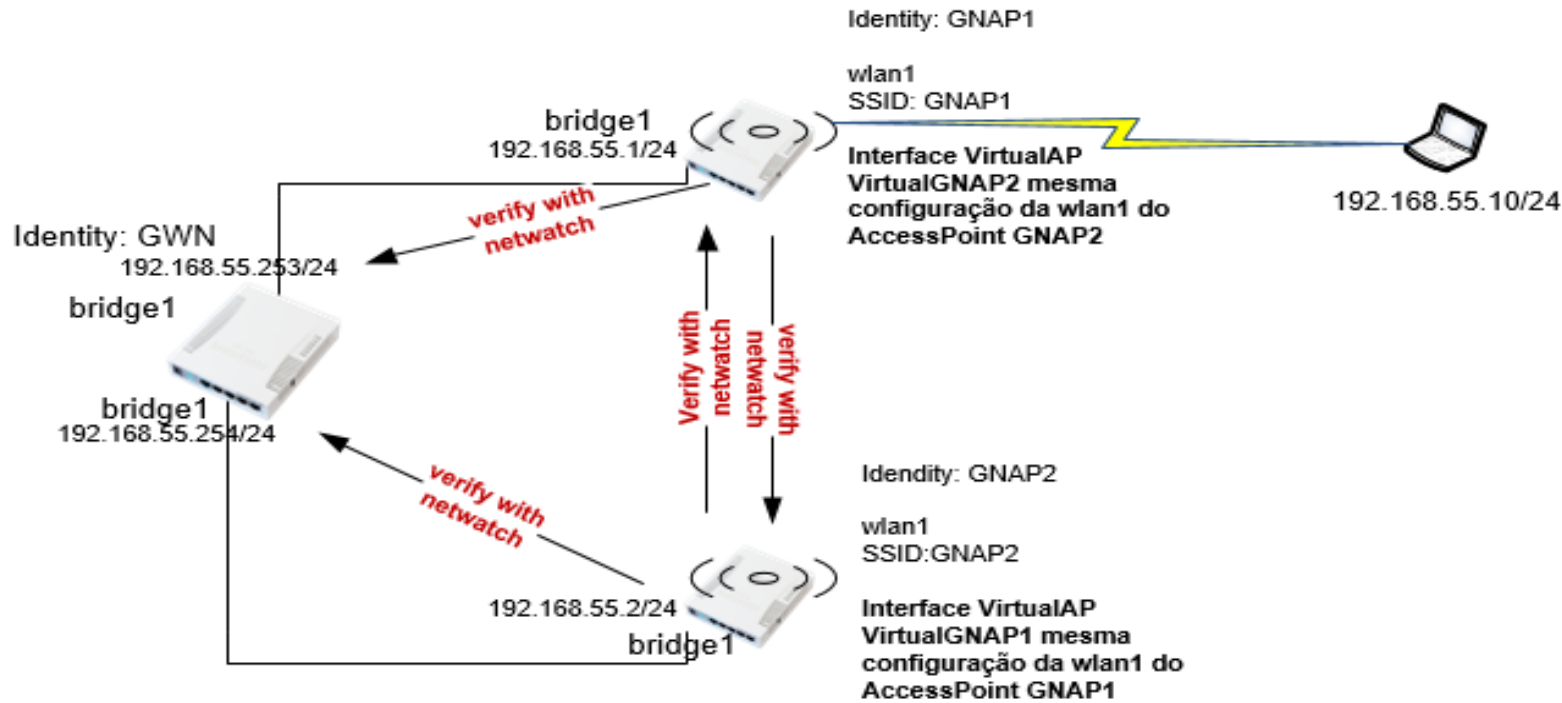


current status: up ou down

Console de script que é executado **uma vez** quando o status de um equipamento muda para **down**

Console de script que é executado **uma vez** quando o status de um equipamento muda para **up**

**Aviso:** Netwatch executa scripts como usuário \*sys, portanto qualquer variável global definida no script de netwatch não será legível pelo agendador ou outros usuários  
(Última consulta em 15 de Maio de 2016 (<http://wiki.mikrotik.com/wiki/Manual:Tools/Netwatch>))



## Utilização do netwatch no Access Point GNAP1

- ✓ if i can reach the GWN (script up - **interface enable wlan1**)  
(script down - **interface disable wlan1**)
- ✓ if i can reach the GNAP2 (script up - **interface disable VirtualGNAP2**)  
(script down - **interface enable VirtualGNAP2**)

## Utilização do netwatch no Access Point GNAP2

- ✓ if i can reach the GWN (script up - **interface enable Wlan1**)  
(script down - **interface disable wlan1**)
- ✓ if i can reach the GNAP1 (script up - **interface disable VirtualGNAP1**)  
(script down - **interface enable VirtualGNAP1**)

# Scripts

O RouterOS tem uma linguagem de scripting que permite o desenvolvimento de scripts para tarefas de manutenção e outras funcionalidades.

The image shows a screenshot of the RouterOS 'New Script' dialog box. The dialog is titled 'New Script' and has a blue header. It contains several fields and options:

- Name:** A text field containing 'script1'. A blue arrow points to this field with the label 'nome do script'.
- Owner:** An empty text field.
- Policy:** A section with two columns of checkboxes, all of which are checked:
  - reboot, write, test, sniff
  - read, policy, password, sensitive
- Last Time Started:** An empty text field.
- Run Count:** A text field containing '0'.
- Source:** A large empty text area for entering the script code. A blue arrow points to this area with the label 'Código fonte do script'.

On the right side of the dialog, there are several buttons: 'OK', 'Cancel', 'Apply', 'Copy', 'Remove', and 'Run Script'. The 'OK' button is highlighted with a blue arrow.

At the top left of the dialog, there is a blue callout box with the word 'system' and an arrow pointing to the 'Scripts' tab in the 'Script List' window above it.

# Scheduler

O scheduler pode acionar a execução do script num determinado momento, após um intervalo de tempo ou ambos

system

Scheduler

Name Start Date Start Time Interval

New Schedule

Name:  OK

Start Date:  Cancel

Start Time:  Apply

Interval:  Disable

On Event:

Owner:

Policy

reboot  read

write  policy

test  password

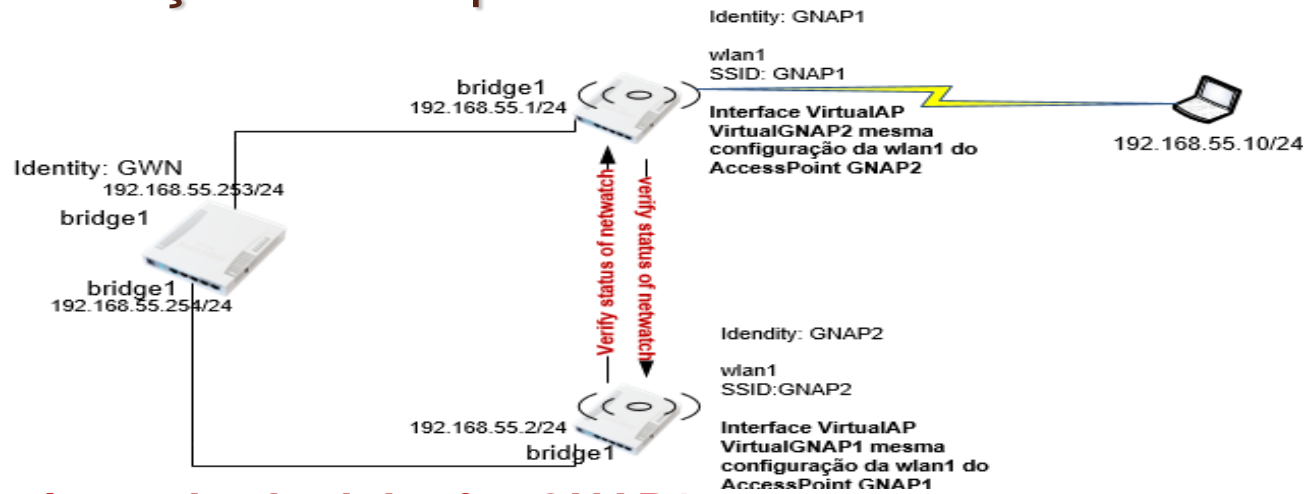
sniff  sensitive

Run Count:

Next Run:

Introduzir o nome do script aqui para ser executado no scheduler

# Implementação de script e scheduler



## Using script and scheduler for GNAP1

- ✓ if GATEWAY netwatch status is down and VIRTUALGNAP2 netwatch status is down turn off wlan1 and virtualGNAP2

### Script code name=faultTolerance

```
:if (([/tool netwatch get 1 status ] = "down") && [/tool netwatch get 0 status ] \="down") do={/interface wireless disable numbers=0,1 ;
```

```
/system scheduler add name=APfaultTolerance on-event=faultTolerance start-time=startup interval=2
```

## Using script and scheduler for GNAP2

- ✓ if GATEWAY netwatch status is down and VIRTUALGNAP1 netwatch status is down turn off wlan1 and virtualGNAP1

### Script code name=faultTolerance

```
:if (([/tool netwatch get 1 status ] = "down") && [/tool netwatch get 0 status ] \="down") do={/interface wireless disable numbers=0,1 ;
```

```
/system scheduler add name=APfaultTolerance on-event=faultTolerance start-time=startup interval=2
```

# NOTA FINAL

**NV2 não permite VirtualAP,  
utilizar Access Points Físicos em  
vez de Aps virtuais.**



# Final

## Obrigado...

## Questões?

## Contatos:

**[armando@semcabo.pt](mailto:armando@semcabo.pt)**

**[www.semcabo.pt](http://www.semcabo.pt)**