Seguridad Proactiva con Mikrotik y TeamCymru

MUM ECUADOR 2019

Autor: Andrés Genovez Tobar

MTCTCE / MTCRE / MTCSE / TRAINER

EMAIL: agenovez@noctelecom.net

Web: https://www.noctelecom.net

Trayectoria

- NOCTELECOM
  - Servicios de Infraestructura de Internet
  - Consultoría y Capacitación

Agradecimiento

Dedicatoria

Publico Objetivo

- Administran Infraestructura de Redes (Diseño y Acceso)
- Disponen de un número ASN Público o desean adquirir uno (Numero de sistema autónomo)

Objetivo

- Cómo configurar una o más sesiones eBGP y evitar ataques de manera proactiva:
  - Conocer que es BGP y cómo funciona.
  - Cómo puedo asegurarlo.
  - Conocer el proyecto TEAM CYMRU.
    - Cómo hacer Peer con esta entidad.

https://noctelecom.net/mum2019/

AGENDA

- 20 min Charla
  - ¿ Que es BGP?
    - ASN (Numero de Sistema Autónomo)
  - Acerca de seguridad
  - “Team Cymru”
  - UTRS (Servicio de eliminación de trafico no deseado) de “Team Cymru”
- 10 min Cómo podemos Implementarlo?

BGP

- Border Gateway Procotol
- Ruteo Dinámico y vector distancia
- EGP (Protocolo de Pasarela Exterior)
- Puerto TCP/179
- iBGP (internal BGP session)
- eBGP (external BGP session)
- Lo que une a Internet

ASN

- ASN (Numero de Sistema Autónomo)
- ¿Para qué es necesario?
- Público o Privado
  - 16 bit: 23457 – 64534 o 32 bit: 131072 – 4199999999 (4200 mill.)
  - 16 bit: 64512 – 65534 o 32 bit: 4200000000 - 4294967294
- ¿Dónde se consigo?
- Internet Assigned Numbers Authority (IANA)
- RIRs (Regional Internet Registry)
- LACNIC (Centro de Información de Redes de Latinoamérica y el Caribe)
- IPv4 Exhausto

Acerca de Seguridad

- ¿De quien es la responsabilidad?
- Hacer la tarea.
- Aseguramiento de nuestros routers Mikrotik.
- Entrenamiento de seguridad.
- Bloqueo de trafico malicioso.

Team Cymru

- https://www.team-cymru.com/
- 1998
- ¿Quién y por qué?
- Partnership (Alianza entre ISPs)
  - BOGONs
  - Inteligencia de amenazas

UTRS

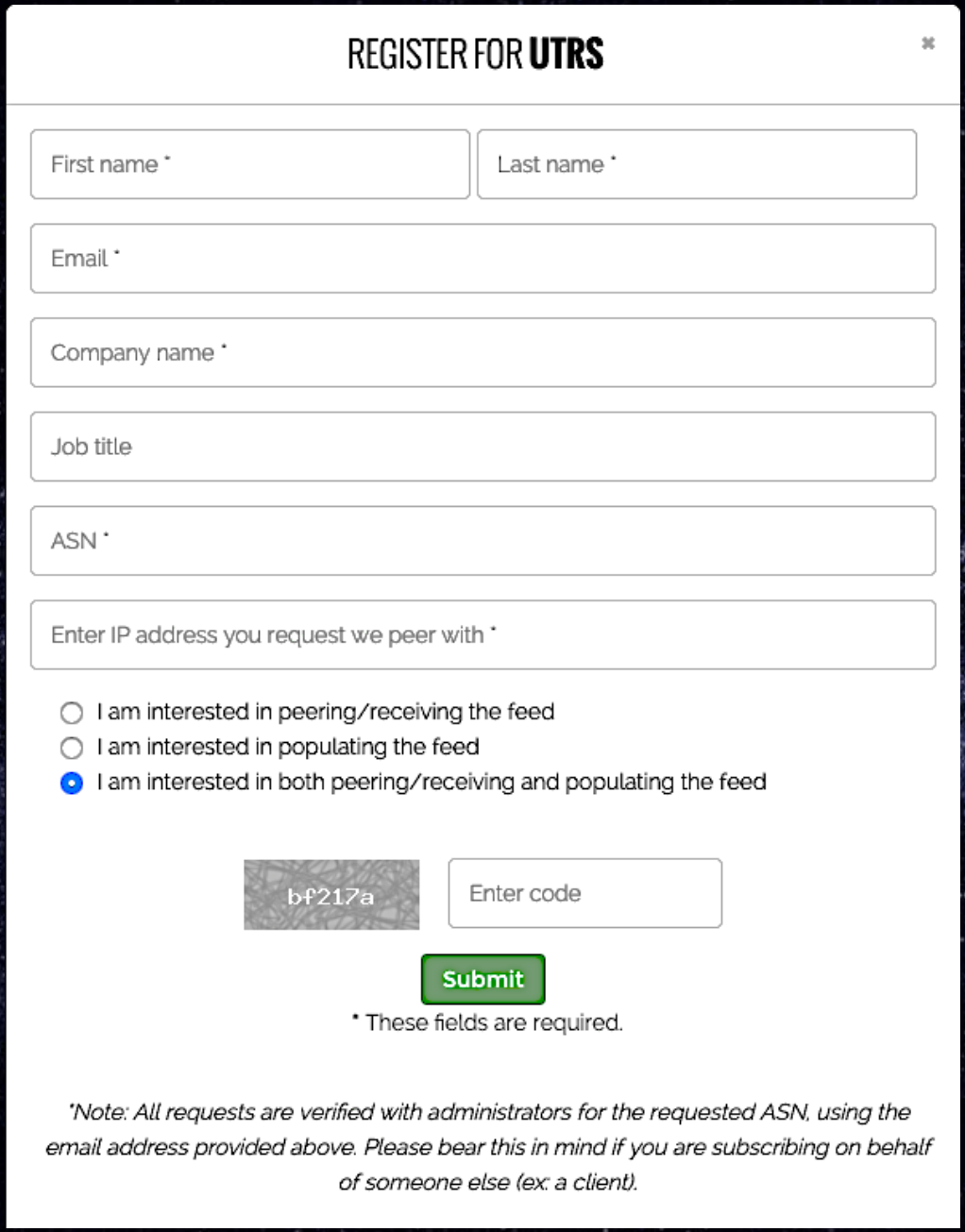
- UTRS (Eliminación de Trafico no Deseado)
- Sesión eBGP
- Ataques DDOS (Ataque de denegación de servicio distribuido)
  - Botnets

UTRS Implementación

- ¿Qué se necesita?
- Configurar una sesión eBGP
  - Seguridad de BGP
  - Configuración del Peer
  - Filtros BGP

UTRS Implementación

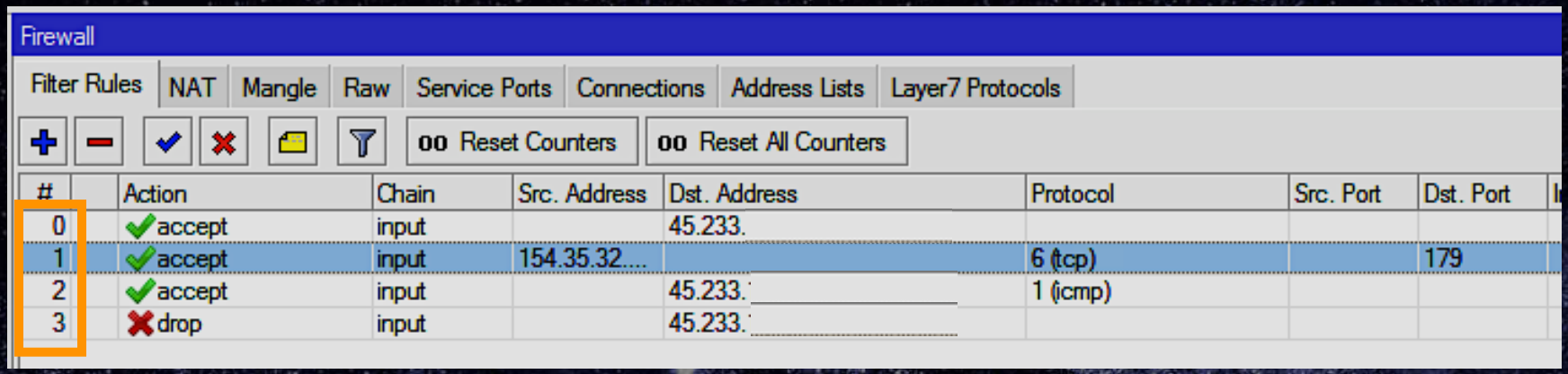
- https://www.team-cymru.com/utrs.html


REGISTER FOR UTRS
First name *
Last name *
Email *
Company name *
Job title
ASN *
Enter IP address you request we peer with *
I am interested in peering/receiving the feed
I am interested in populating the feed
I am interested in both peering/receiving and populating the feed
bf217a
Enter code
Submit
* These fields are required.
*Note: All requests are verified with administrators for the requested ASN, using the email address provided above. Please bear this in mind if you are subscribing on behalf of someone else (ex: a client).

UTRS Implementación

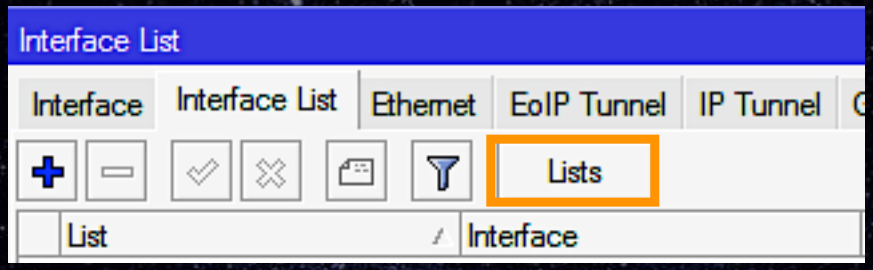
- 0. Seguridad

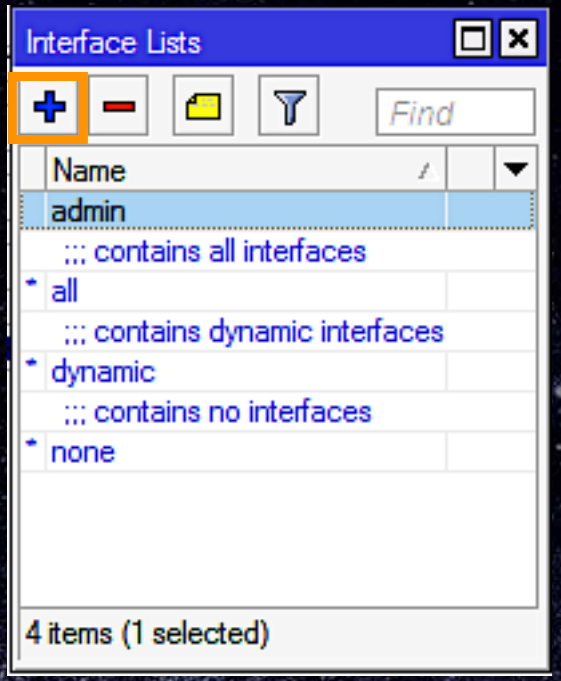
Seguridad L3

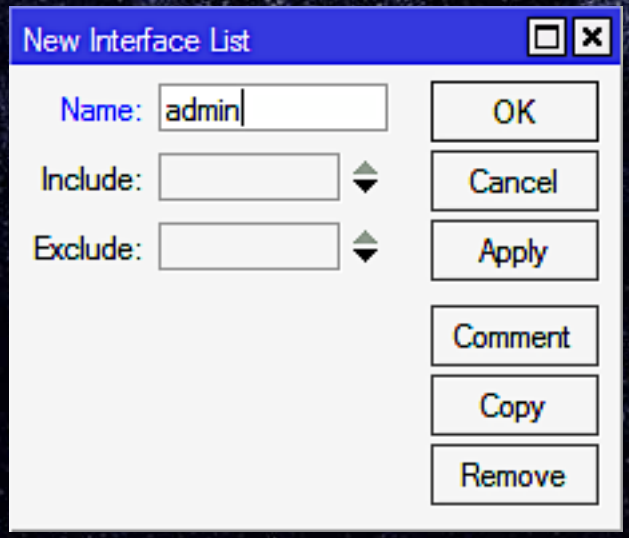


/ip firewall filter
add action=accept chain=input connection-state=established,related dst-address=[CAMBIAR POR SU IP PUBLICA]
add action=accept chain=input dst-port=179 protocol=tcp src-address=[CAMBIAR POR LA IP ASIGNADA POR TEAM CYMRU]
add action=accept chain=input dst-address=[CAMBIAR POR SU IP PUBLICA] protocol=icmp
add action=drop chain=input dst-address=[CAMBIAR POR SU IP PUBLICA]

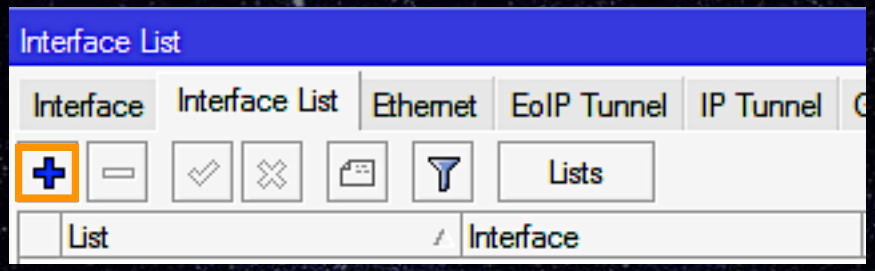
Seguridad L2

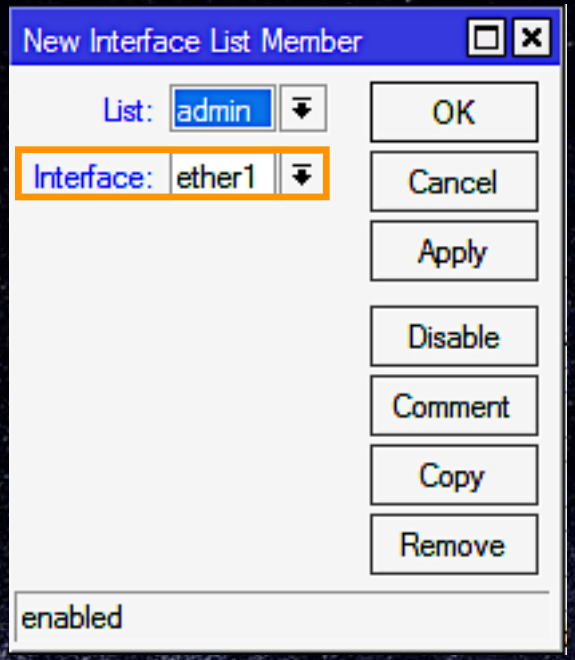


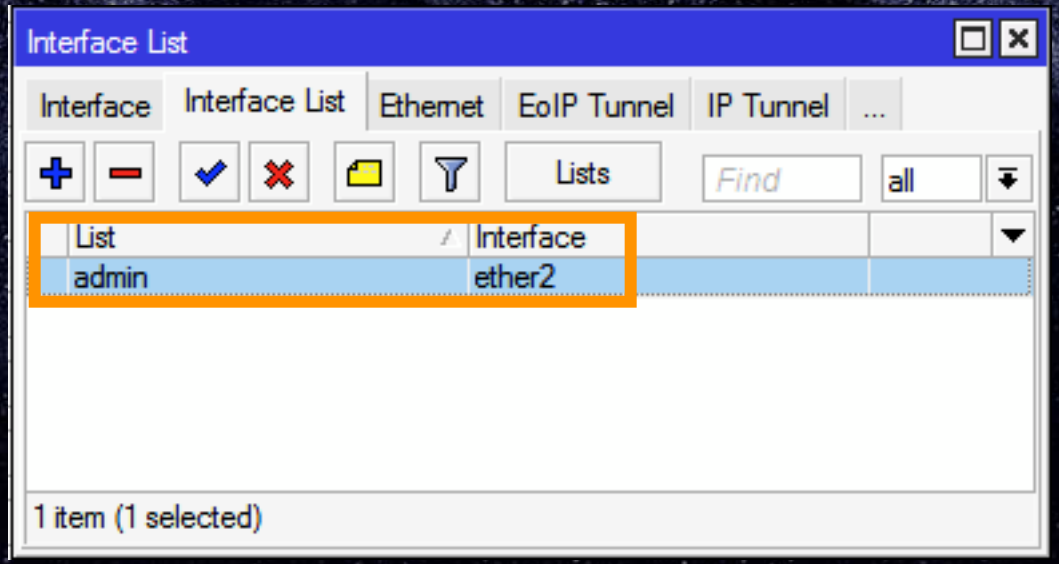




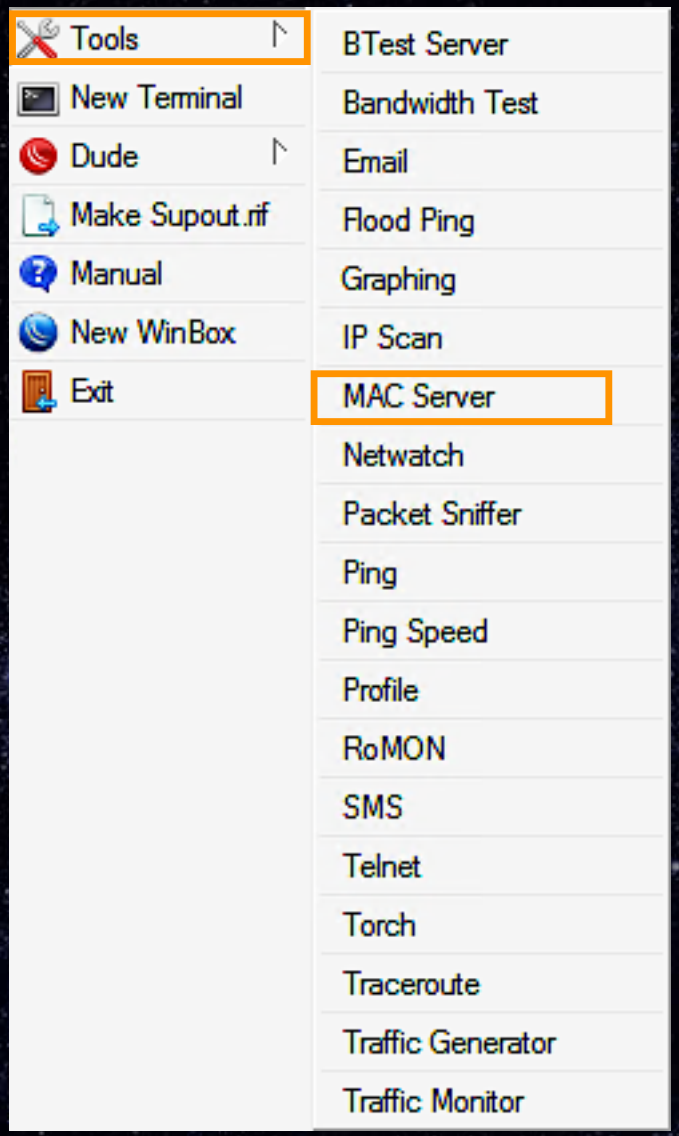
Seguridad L2

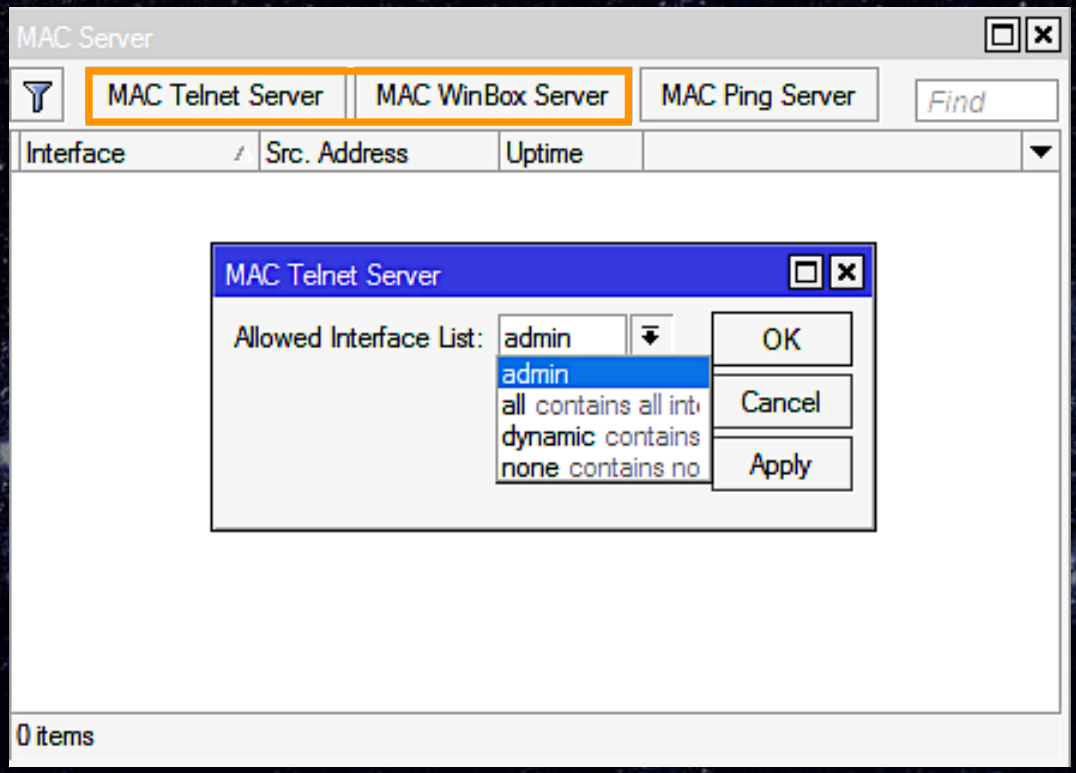




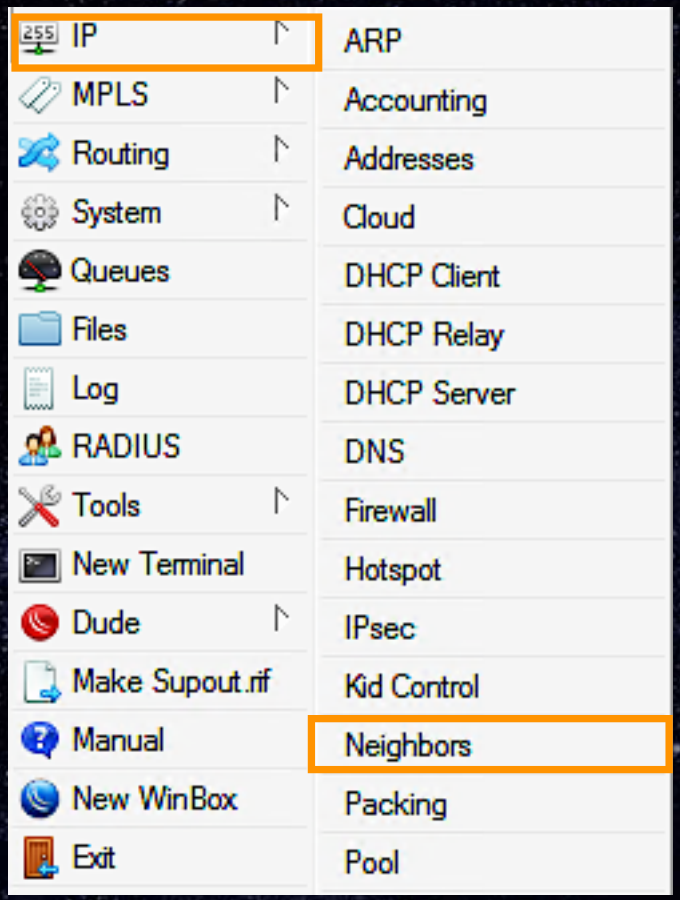


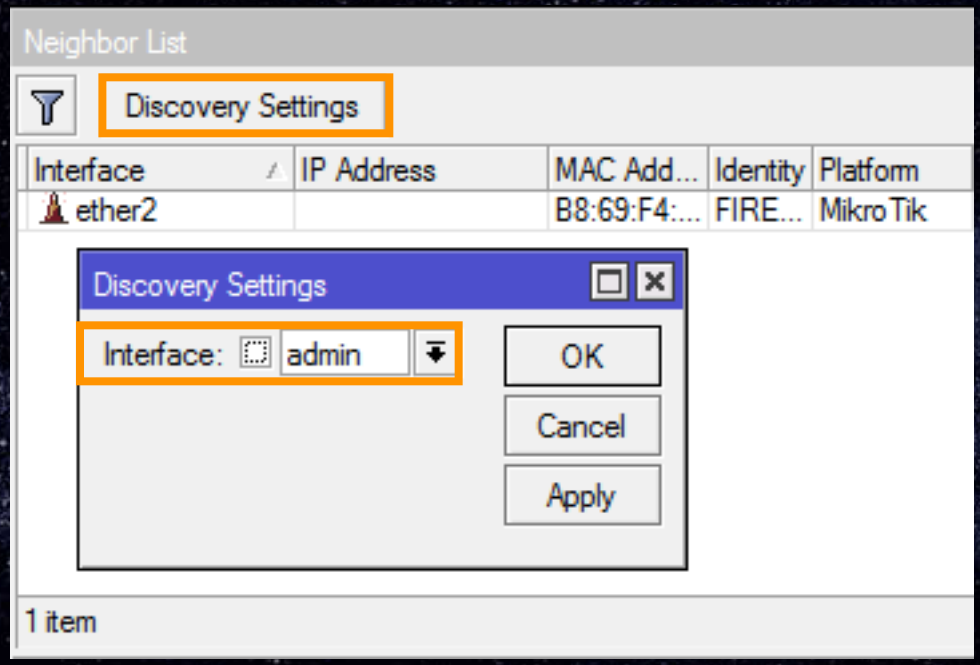
Seguridad L2



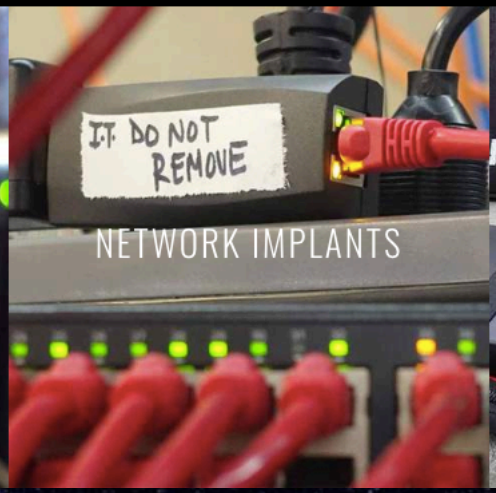


Seguridad L2





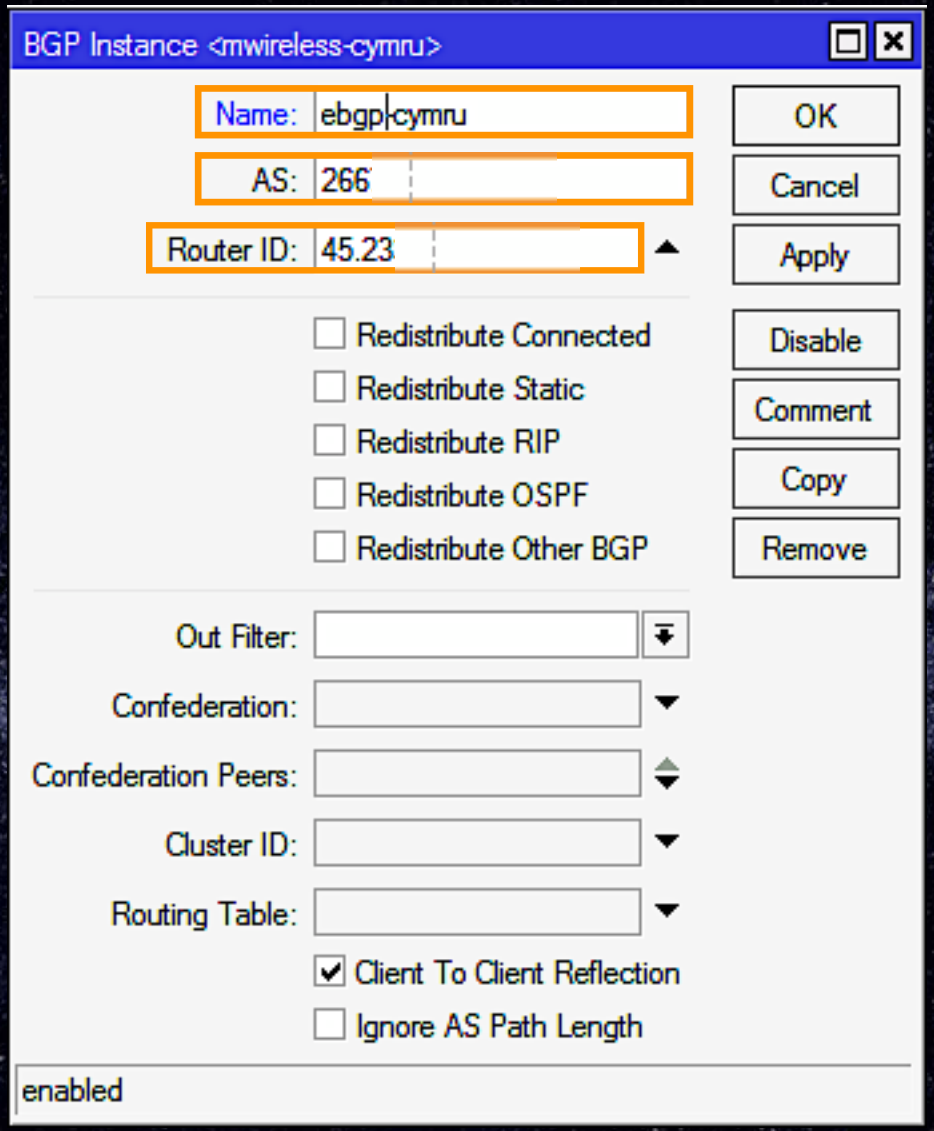
Seguridad L0



Fuente: https://shop.hak5.org

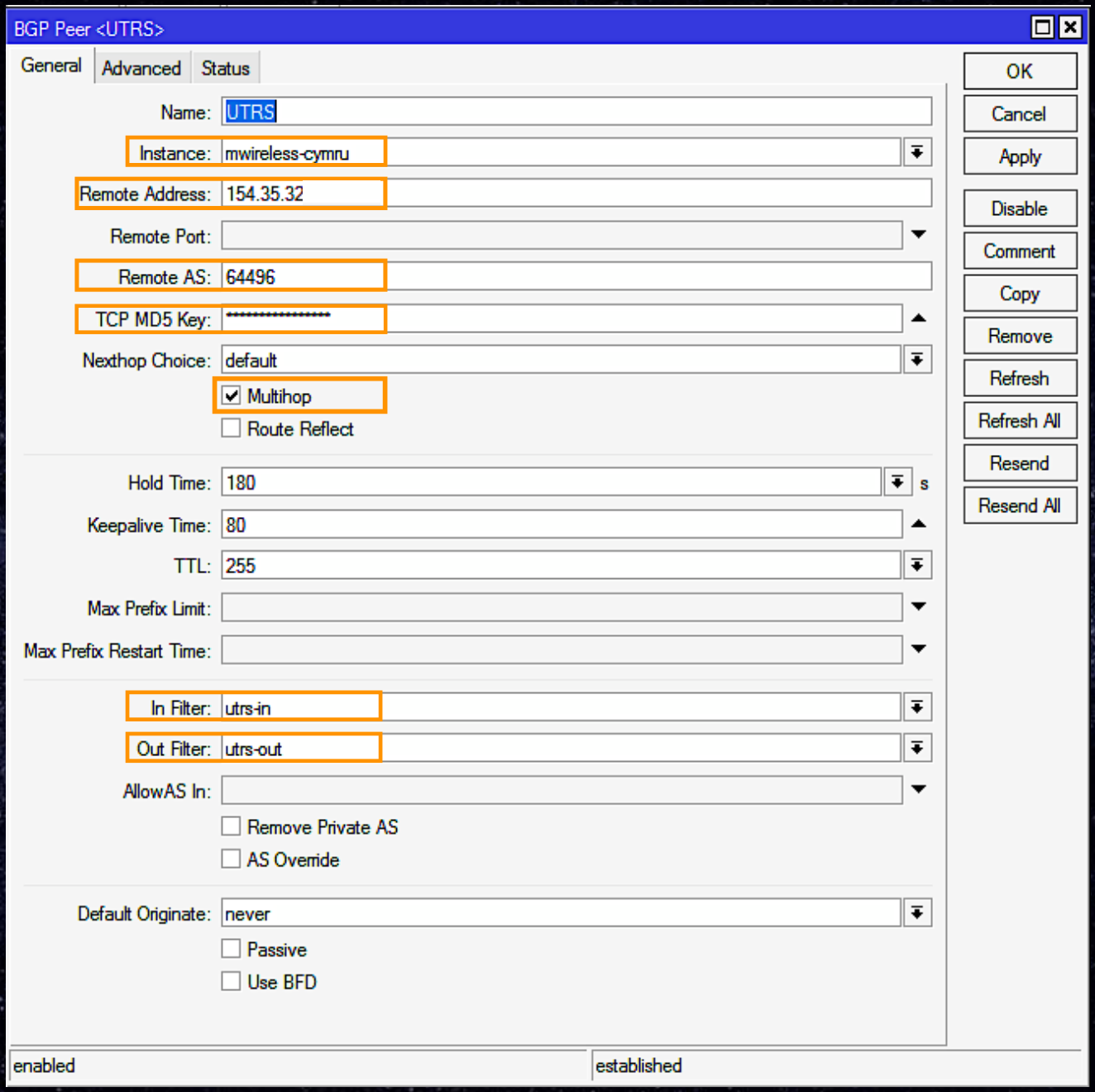
UTRS Implementación

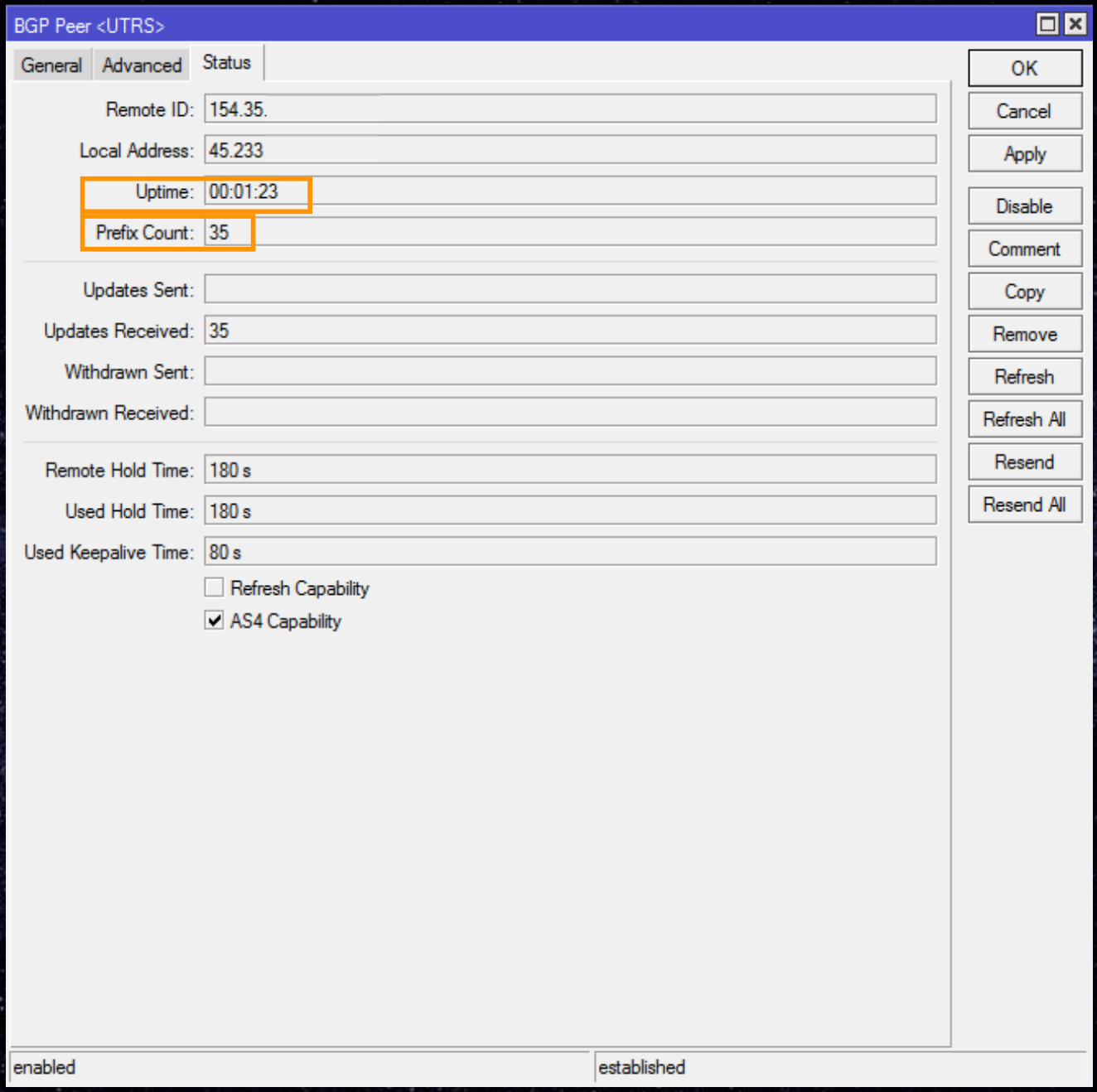
- 1. Configurar Instancia


BGP Instance <mwireless-cymru>
Name: ebgp-cymru
AS: 266
Router ID: 45.23
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Redistribute Connected
Redistribute Static
Redistribute RIP
Redistribute OSPF
Redistribute Other BGP
Out Filter:
Confederation:
Confederation Peers:
Cluster ID:
Routing Table:
Client To Client Reflection
Ignore AS Path Length
enabled

UTRS Implementación

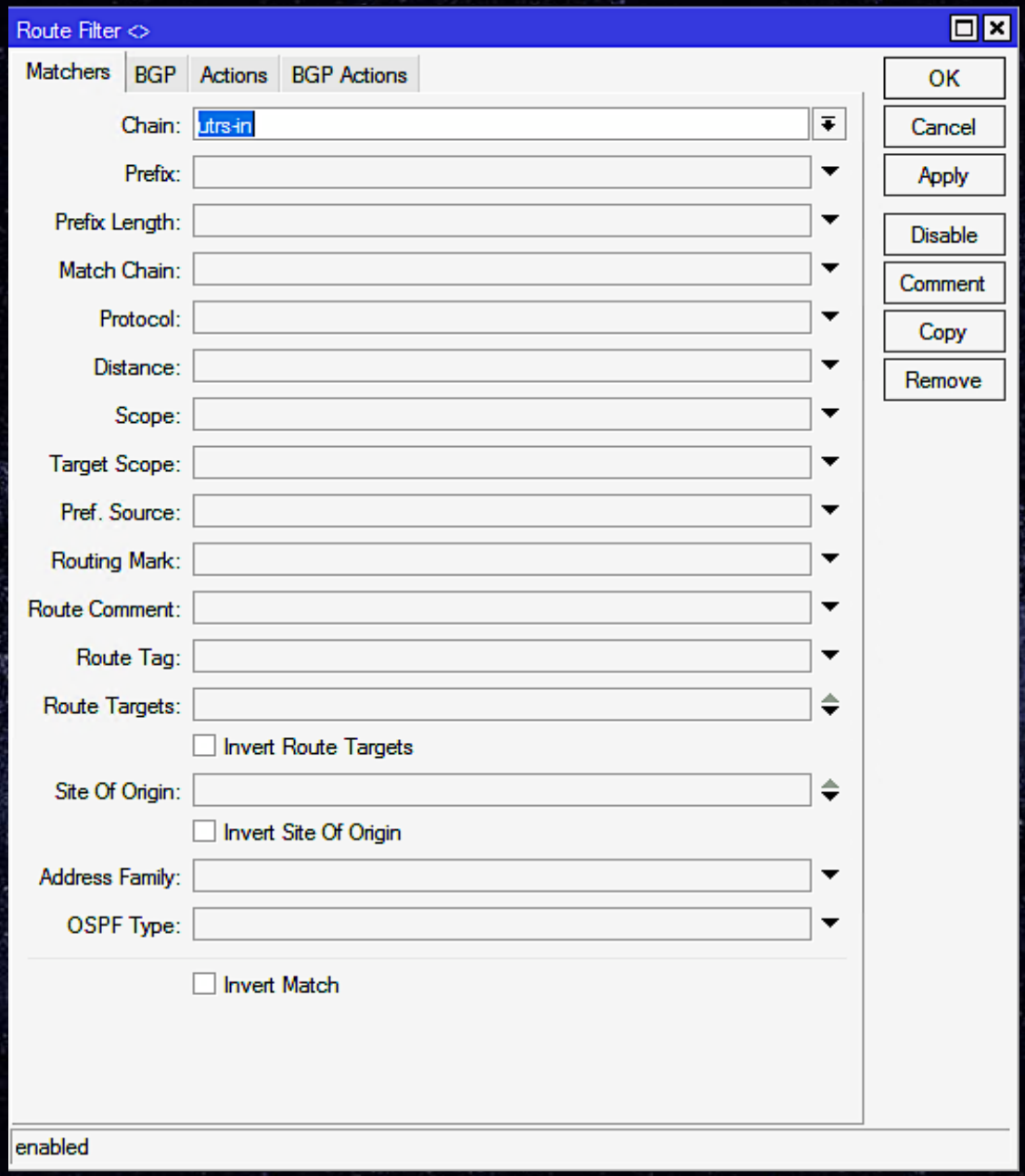
- 2. Configurar Peer

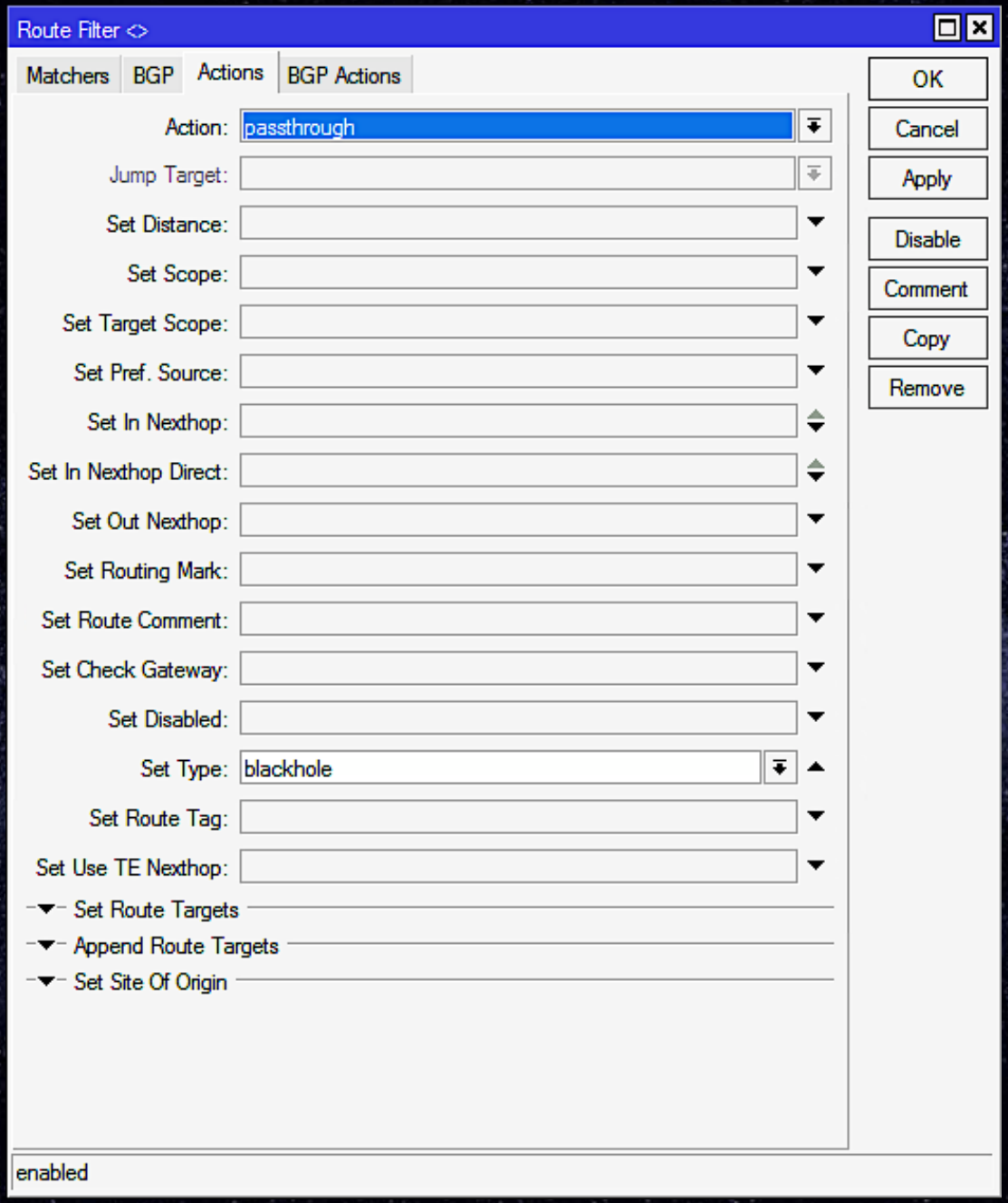

BGP Peer <UTRS>
General
Advanced
Status
Name: UTRS
Instance: mwireless-cymru
Remote Address: 154.35.32
Remote Port:
Remote AS: 64496
TCP MD5 Key: ••••••••••••••••
Nexthop Choice: default
Multihop
Route Reflect
Hold Time: 180 s
Keepalive Time: 80
TTL: 255
Max Prefix Limit:
Max Prefix Restart Time:
In Filter: utrs-in
Out Filter: utrs-out
AllowAS In:
Remove Private AS
AS Override
Default Originate: never
Passive
Use BFD
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Refresh
Refresh All
Resend
Resend All
enabled
established


BGP Peer <UTRS>
General
Advanced
Status
Remote ID: 154.35.
Local Address: 45.233
Uptime: 00:01:23
Prefix Count: 35
Updates Sent:
Updates Received: 35
Withdrawn Sent:
Withdrawn Received:
Remote Hold Time: 180 s
Used Hold Time: 180 s
Used Keepalive Time: 80 s
Refresh Capability
AS4 Capability
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Refresh
Refresh All
Resend
Resend All
enabled
established

UTRS Implementación

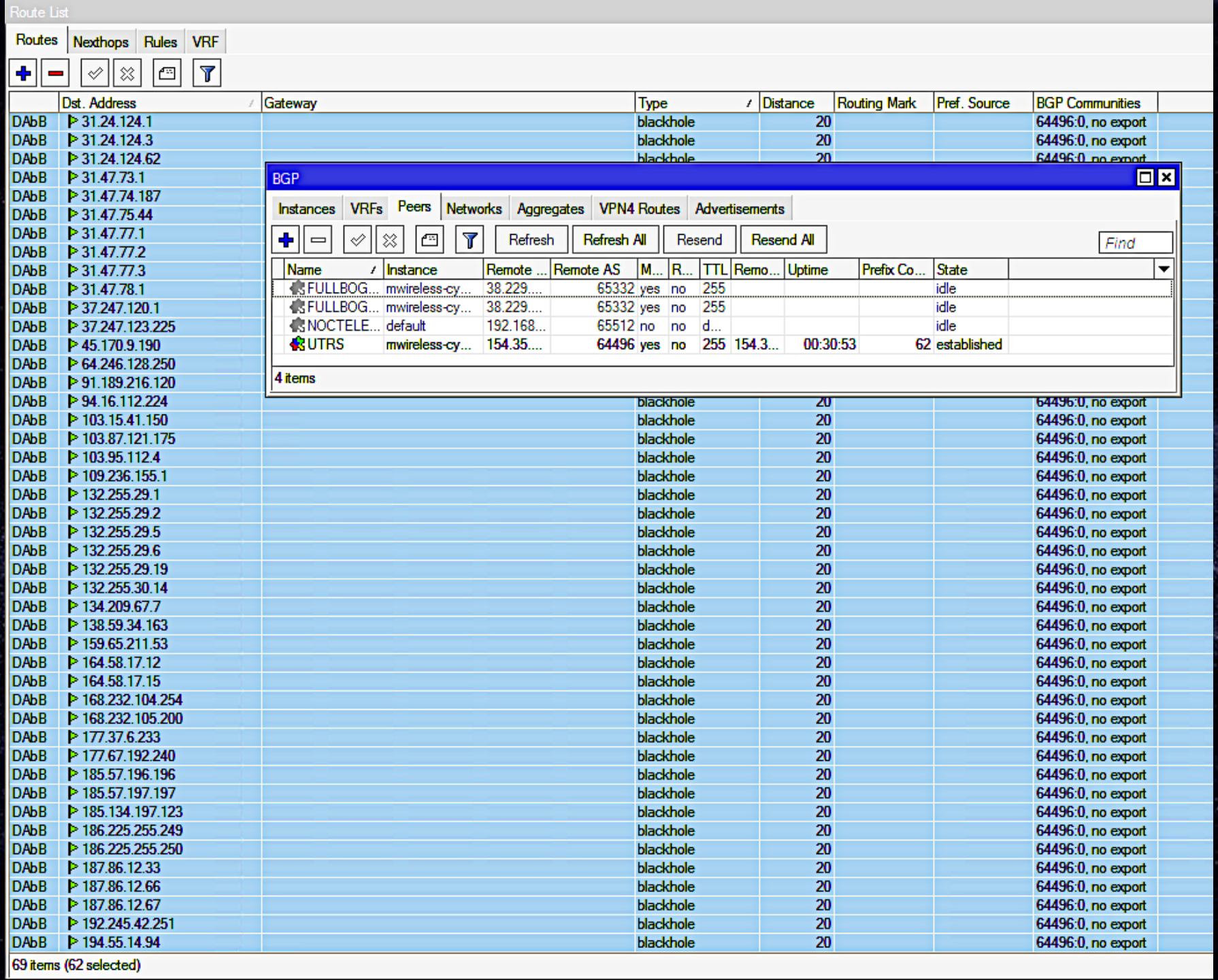
- 3. Configurar Filtro


Route Filter <>
Matchers
BGP
Actions
BGP Actions
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Chain:
utrs-in
Prefix:
Prefix Length:
Match Chain:
Protocol:
Distance:
Scope:
Target Scope:
Pref. Source:
Routing Mark:
Route Comment:
Route Tag:
Route Targets:
Invert Route Targets
Site Of Origin:
Invert Site Of Origin
Address Family:
OSPF Type:
Invert Match
enabled


Route Filter <>
Matchers
BGP
Actions
BGP Actions
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Action: passthrough
Jump Target:
Set Distance:
Set Scope:
Set Target Scope:
Set Pref. Source:
Set In Nexthop:
Set In Nexthop Direct:
Set Out Nexthop:
Set Routing Mark:
Set Route Comment:
Set Check Gateway:
Set Disabled:
Set Type: blackhole
Set Route Tag:
Set Use TE Nexthop:
Set Route Targets
Append Route Targets
Set Site Of Origin
enabled

UTRS Implementación

- 4. Resultados:
  - Se obtuvieron 62 prefijos
  - Los 62 prefijos están como “blackhole”


Route List
Routes
Nexthops
Rules
VRF
Dst. Address
Gateway
Type
Distance
Routing Mark
Pref. Source
BGP Communities
DAbB 31.24.124.1 blackhole 20 64496:0, no export
DAbB 31.24.124.3 blackhole 20 64496:0, no export
DAbB 31.24.124.62 blackhole 20 64496:0, no export
DAbB 31.47.73.1
DAbB 31.47.74.187
DAbB 31.47.75.44
DAbB 31.47.77.1
DAbB 31.47.77.2
DAbB 31.47.77.3
DAbB 31.47.78.1
DAbB 37.247.120.1
DAbB 37.247.123.225
DAbB 45.170.9.190
DAbB 64.246.128.250
DAbB 91.189.216.120
DAbB 94.16.112.224 blackhole 20 64496:0, no export
DAbB 103.15.41.150 blackhole 20 64496:0, no export
DAbB 103.87.121.175 blackhole 20 64496:0, no export
DAbB 103.95.112.4 blackhole 20 64496:0, no export
DAbB 109.236.155.1 blackhole 20 64496:0, no export
DAbB 132.255.29.1 blackhole 20 64496:0, no export
DAbB 132.255.29.2 blackhole 20 64496:0, no export
DAbB 132.255.29.5 blackhole 20 64496:0, no export
DAbB 132.255.29.6 blackhole 20 64496:0, no export
DAbB 132.255.29.19 blackhole 20 64496:0, no export
DAbB 132.255.30.14 blackhole 20 64496:0, no export
DAbB 134.209.67.7 blackhole 20 64496:0, no export
DAbB 138.59.34.163 blackhole 20 64496:0, no export
DAbB 159.65.211.53 blackhole 20 64496:0, no export
DAbB 164.58.17.12 blackhole 20 64496:0, no export
DAbB 164.58.17.15 blackhole 20 64496:0, no export
DAbB 168.232.104.254 blackhole 20 64496:0, no export
DAbB 168.232.105.200 blackhole 20 64496:0, no export
DAbB 177.37.6.233 blackhole 20 64496:0, no export
DAbB 177.67.192.240 blackhole 20 64496:0, no export
DAbB 185.57.196.196 blackhole 20 64496:0, no export
DAbB 185.57.197.197 blackhole 20 64496:0, no export
DAbB 185.134.197.123 blackhole 20 64496:0, no export
DAbB 186.225.255.249 blackhole 20 64496:0, no export
DAbB 186.225.255.250 blackhole 20 64496:0, no export
DAbB 187.86.12.33 blackhole 20 64496:0, no export
DAbB 187.86.12.66 blackhole 20 64496:0, no export
DAbB 187.86.12.67 blackhole 20 64496:0, no export
DAbB 192.245.42.251 blackhole 20 64496:0, no export
DAbB 194.55.14.94 blackhole 20 64496:0, no export
69 items (62 selected)
BGP
Instances
VRFs
Peers
Networks
Aggregates
VPN4 Routes
Advertisements
Refresh
Refresh All
Resend
Resend All
Find
Name
Instance
Remote ...
Remote AS
M...
R...
TTL
Remo...
Uptime
Prefix Co...
State
FULLBOG... mwireless-cy... 38.229.... 65332 yes no 255 idle
FULLBOG... mwireless-cy... 38.229.... 65332 yes no 255 idle
NOCTELE... default 192.168... 65512 no no d... idle
UTRS mwireless-cy... 154.35.... 64496 yes no 255 154.3... 00:30:53 62 established
4 items

Conclusiones

- ¿Qué tomar en Cuenta?
- ¿Dónde encuentro ejemplos?
  - https://noctelecom.net/mum2019/

Referencias

- UTRS: https://www.team-cymru.com/utrs.html
- LACNIC: https://www.lacnic.net/
- CAMPUS LACNIC: https://campus.lacnic.net/
- Sistema Autónomo (Definición): https://es.wikipedia.org/wiki/Sistema_aut%C3%B3nomo

PREGUNTAS

Muchas Gracias