

GTER 46



GTER 46 | GTS 32

IPv6

Problemas e Soluções na Identificação de
usuários usando RouterOS



NETWORK
EDUCATION

Quem somos?



Quem Somos?

Saiba um pouco mais sobre os instrutores da Network Education!



Uesley Corrêa

INSTRUTOR



Rinaldo Vaz

INSTRUTOR



Elizandro Pacheco

INSTRUTOR



Leonardo Furtado

INSTRUTOR



Patrick Brandão

INSTRUTOR



Rudson Costa

INSTRUTOR

E eu?



Co-Fundador e Instrutor na **Network Education**, escola de treinamento para profissionais de ISP's com mais

de 5 mil alunos no Brasil e exterior.

Vice-presidente do **BPF (Brasil Peering Forum)**, um grupo de profissionais que trabalham para o desenvolvimento da Internet Brasileira.

CEO da **Telecom Consultoría, Entrenamiento y Servicios**, uma empresa Paraguaia que leva conhecimento, tecnologia, melhores práticas e desenvolvimento para os ISP's no Paraguay. Construiu e administra o IX-CDE, primeiro IX privado do Paraguay.



TELECOM
Consultoría, Entrenamiento y Servicios



Brasil Peering Forum



Motivação

Numa pesquisa independente feita pela Network Education, aproximadamente 20% dos ASN's que possuem alocação IPv6 e não entregam IPv6 ao seu assinante o fazem por falta de suporte do RouterOS nos logs de Túnel e PD do PPPoE. E isso é altamente preocupante haja visto que estamos avançados no esgotamento do IPv4 e na necessidade crescente de implementação de IPv6.



Problema

De acordo com o MCI (Marco Civil da Internet), é obrigatória a identificação do usuário de um determinado recurso de numeração (IPv4 ou IPv6). Num assunto bem amplo, o CGNAT / Radius tem algumas formas de fazer essa identificação em IPv4. Mas e no IPv6?



FreeRadius

O FreeRadius desde a versão 3 já passou a suportar armazenamento de endereços IPv6 em suas tabelas. Com alguns ajustes na tabela Radacct também é possível armazenar o prefixo que foi entregue tanto para o Delegate quanto para o Framed em IPv6. Só que aí há um problema: o RouterOS não retorna no accounting as informações referentes ao IPv6 (coisa que outras aplicações de PPPoE Server já o fazem).

FreeRADIUS

The world's most popular RADIUS Server



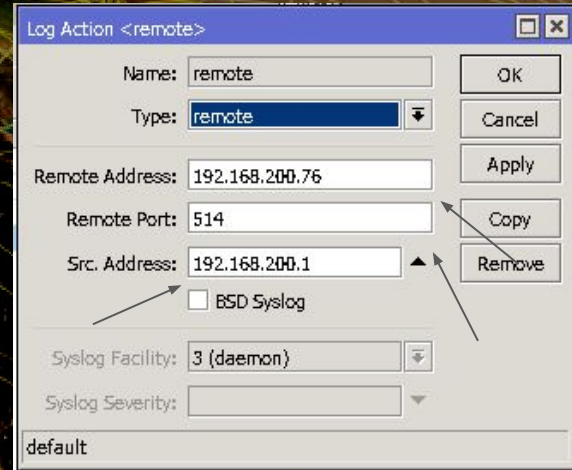
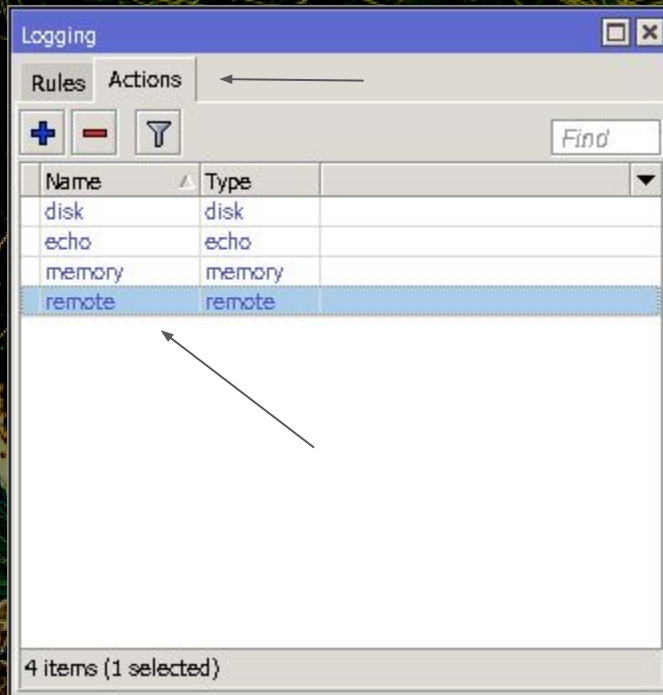
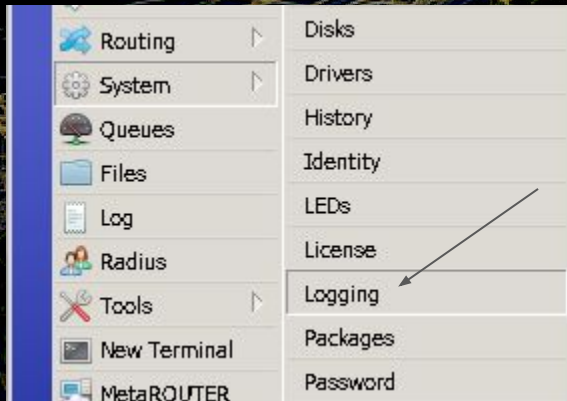
Qual seria a alternativa a momento?

A momento, há a possibilidade de utilizar alguma solução de Syslog (Syslog-NG, Graylog ou alguma outra) para armazenar isso e configurar o Mikrotik para enviar esses log's ao servidor. Basicamente na configuração padrão, o Syslog grava em arquivo ou banco tudo o que é enviado na porta do daemon.

syslog-ng



No RouterOS:



No RouterOS:

Logging

Rules Actions

+ - ✓ ✗ ⏏ Find

Topics	Prefix	Action
* critical		echo
* warning		memory
radvd		memory
* info		memory
* error		memory
dhcp		memory
radvd		remote
dhcp		remote

8 items

New Log Rule

Topics:

Prefix:

Action:

OK Cancel Apply Disable Copy Remove

enabled

New Log Rule

Topics:

Prefix:

Action:

OK Cancel Apply Disable Copy Remove

enabled



No Syslog-NG:

```
source concentrador01 {  
    udp(  
        ip(192.168.200.76)  
        port(514)  
    );  
};
```

```
#####
```

```
# Destinations
```

```
#####
```

```
#destination concentradores
```

```
destination concentrador01_file { file("/var/log/concentrador01.log"); };
```

```
filter f_pd_concentrador01 { host(192.168.200.1) and not message("skip Router Advertisement") and not message("received prefix"); };
```

```
#####
```

```
# Log paths
```

```
#####
```

```
#concentradores
```

```
log { source(concentrador01); filter(f_pd_concentrador01); destination(concentrador01_file); };
```



No Syslog-NG:

```
Oct 23 15:49:02 192.168.200.1 dhcp,debug,packet recv server: <pppoe-alex[redacted]com.py> fe80::3 -> ff02::1:2
Oct 23 15:49:02 192.168.200.1 dhcp,debug,packet type: solicit
Oct 23 15:49:02 192.168.200.1 dhcp,debug,packet transaction-id: 2b670b
Oct 23 15:49:02 192.168.200.1 dhcp,debug,packet -> clientid: 00030001 6c3b6bb0 7c54
Oct 23 15:49:02 192.168.200.1 dhcp,debug,packet -> oro: 23
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet -> elapsed_time: 0
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet -> rapid_commit:
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet -> ia_pd:
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet t1: 1800
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet t2: 2880
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet id: 0x3
Oct 23 15:49:03 192.168.200.1 dhcp,debug processing client 6c3b6bb07c54 iapd:0x3
Oct 23 15:49:03 192.168.200.1 dhcp,debug added dynamic binding: 6c3b6bb07c54 2803:a040:c0ca:3a80::/60
Oct 23 15:49:03 192.168.200.1 dhcp,debug offering: 6c3b6bb07c54 2803:[redacted]:c0ca:3a80::/60
Oct 23 15:49:03 192.168.200.1 dhcp,debug rebound: 6c3b6bb07c54 2803:[redacted]:c0ca:3a80::/60
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet send <pppoe-alex[redacted]com.py> -> fe80::3%36699
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet type: reply
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet transaction-id: 2b670b
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet -> clientid: 00030001 6c3b6bb0 7c54
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet -> serverid: 00030001 e48d8c7b 17d4
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet -> rapid_commit:
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet -> ia_pd:
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet t1: 129600
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet t2: 207360
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet id: 0x3
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet -> ia_prefix:
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet prefix: 2803:[redacted]:c0ca:3a80::/60
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet valid time: 259200
Oct 23 15:49:03 192.168.200.1 dhcp,debug,packet pref. time: 233280
Oct 23 15:49:04 192.168.200.1 radvd,debug sending Router Advertisement on <pppoe-alex[redacted]com.py>
Oct 23 15:49:04 192.168.200.1 radvd,debug adding prefix=2803:[redacted]:face:f0c::/64
```



Consumo de recursos

Nesse cenário, um provedor com 1000 assinantes gerou 7MB de log's diários. Esse montante pode ser reduzido com alguns ajustes adicionais.



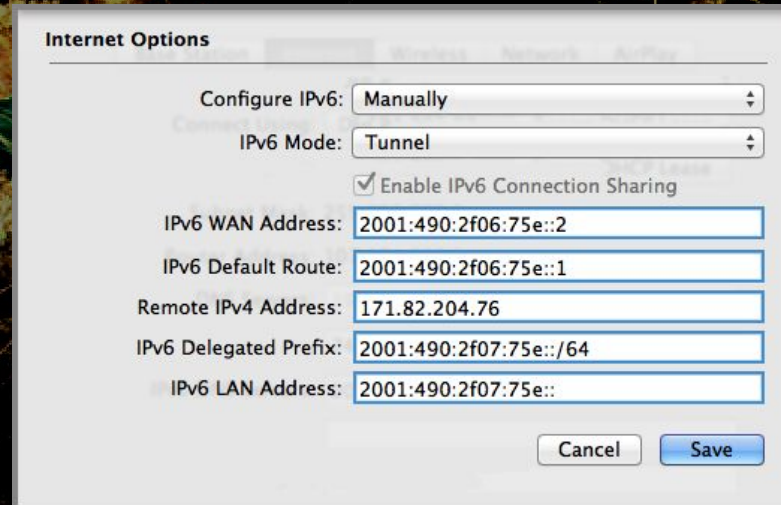
Outros clientes de LOG

A configuração é semelhante em outros clientes de LOG, inclusive os com interface web como Graylog e etc.



Outro problema...

Durante todos esses anos trabalhando com treinamentos e implantações de IPv6, descobrimos uma deficiência presente na maioria das CPE's do mercado no que tange à alocação dinâmica de prefixos IPv6.



The screenshot shows a 'Internet Options' dialog box with the following settings:

- Configure IPv6: Manually
- IPv6 Mode: Tunnel
- ☒ Enable IPv6 Connection Sharing
- IPv6 WAN Address: 2001:490:2f06:75e::2
- IPv6 Default Route: 2001:490:2f06:75e::1
- Remote IPv4 Address: 171.82.204.76
- IPv6 Delegated Prefix: 2001:490:2f07:75e::/64
- IPv6 LAN Address: 2001:490:2f07:75e::

Buttons: Cancel, Save



Outro problema...

Ao haver uma queda no PPPoE da CPE e posterior reconexão, um novo prefixo passa a ser alocado dinamicamente pelo PD para essa conexão. Só que a CPE não solicita esse novo prefixo pelo fato do Lease-Time do DHCPv6 Client ainda estar válido. Esse renew só vai acontecer quando expirar o time do prefixo e a CPE fizer uma nova solicitação. Como lidar com isso?



Alocação Estática de IPv6

Com a alocação estática de IPv6 para usuários finais, podemos matar três problemas de uma só vez:

- 1 - Identificação do usuário sem necessidade de guarda de logs adicionais;
- 2 - Fim das CPE's órfãs de IPv6;
- 3 - Facilidade / possibilidade de alocação de entradas DNS quad-a ou reversos para endereços desse prefixo.



De quem é a ideia??

BCOP IPv6 Prefix Assignment for end-customers, página 19

by Jordi Pallet, Luis Balbinot e outros

<https://ripe74.ripe.net/presentations/39-bcop-ipv6-prefix-v2.pdf>



TELECOM
Consultoria, Entrenamiento y Servicios



Mas como aplicar isso no meu RouterOS???

Isso é simples: no seu radius, você precisa setar na tabela radreply junto ao username do seu cliente o prefixo delegado que ele deve instalar. O atributo do radius a ser utilizado é o Delegated-IPv6-Prefix para Prefix-Delegated e Framed-IPv6-Prefix para prefixos de interconexão. E no caso do cliente suspenso, enviar o pool de bloqueio previamente cadastrado no seu Mikrotik, que usam como parâmetros: Mikrotik-Delegated-IPv6-Pool e Framed-IPv6-Pool.



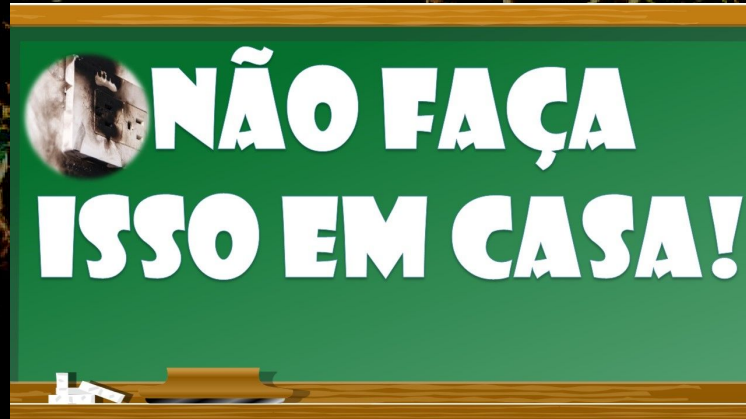
Porém...

Ainda não está 100% essa funcionalidade. O RouterOS já recebe e reconhece os atributos do Radius que entregam o Prefixo Delegado estaticamente porém ainda não consegue entregar isso na conexão do cliente. Em uma tentativa frustrada de fazer isso funcionar, a Mikrotik inclusive quebrou a funcionalidade de Prefix-Delegation nas versões 6.42.x, demorando um tempo até repararem novamente. E isso foi amplamente discutido nessa thread da lista GTER:

<https://eng.registro.br/pipermail/gter/2018-October/075318.html>

Mas há uma luz no fim do túnel!

Uma possibilidade existente é criar pools de Túnel e PD estaticamente para cada cliente em cada concentrador. Com esses pools criados, podem ser utilizados os parâmetros Mikrotik-Delegated-IPv6-Pool e Framed-IPv6-Prefix para entregar os pools estaticamente aos clientes.



TELECOM
Consultoria, Entrenamiento y Servicios

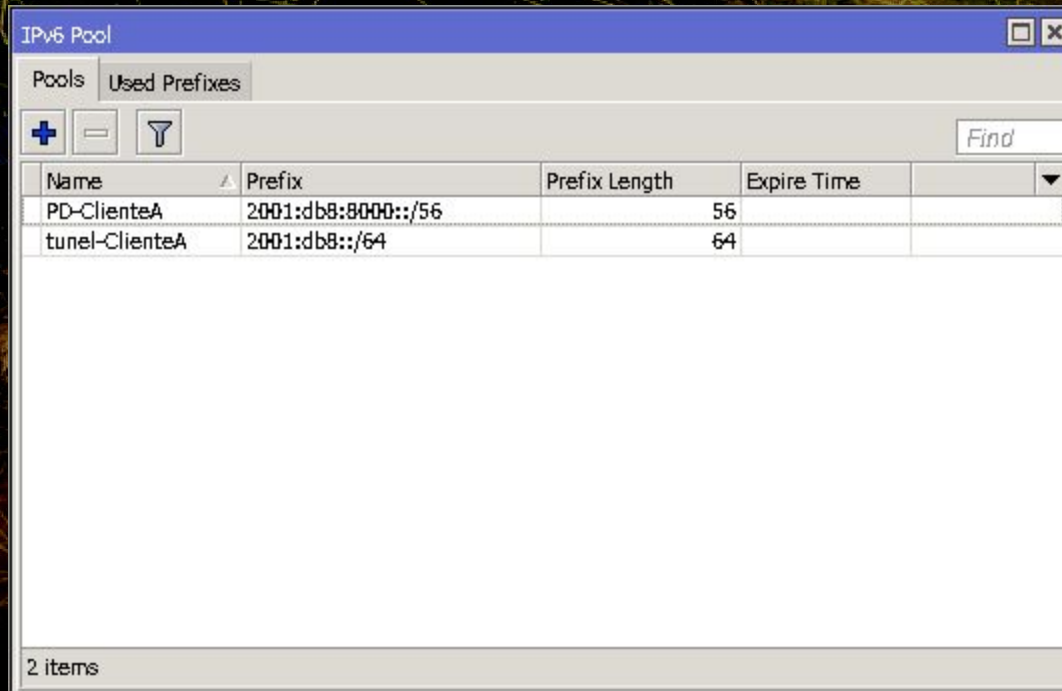


Mas há uma luz no fim do túnel!

Isso dependerá de integração do seu sistema administrativo com os concentradores para esse cadastro via API do RouterOS. Foi testado em laboratório com desempenho satisfatório, porém nunca testado em produção (pelo menos não que fosse amplamente informado).



Mas há uma luz no fim do túnel!



The screenshot shows a window titled "IPv6 Pool" with two tabs: "Pools" and "Used Prefixes". The "Used Prefixes" tab is active. Below the tabs are three buttons: a plus sign (+), a minus sign (-), and a funnel icon. To the right of these buttons is a search box labeled "Find". Below the buttons is a table with the following data:

Name	Prefix	Prefix Length	Expire Time
PD-ClienteA	2001:db8:8000::/56	56	
tunel-ClienteA	2001:db8::/64	64	

At the bottom of the window, it says "2 items".



Considerações:

Verifique com o seu jurídico (especialista em direito de Telecom) como fazer para "validar judicialmente" esse log. Talvez algum termo cartorial onde o cartorário firma que o conteúdo daquele arquivo de log é fiel ao que foi gerado eletronicamente. Importante também é sempre gerar uma cópia do arquivo original para fazer as consultas, não mexendo no arquivo original (pode alterar ponteiros de data / hora de alteração).



Contatos



TELECOM

Consultoria, Entrenamiento y Servicios

<http://facebook.com/telecomtreinamentos>

s

contato@telecomti.net

+595 (982) 725-079

+55 (45) 98809-0457



TELECOM

Consultoria, Entrenamiento y Servicios



NETWORK
EDUCATION

<http://facebook.com/networkeducationbr>

<http://network.education>

treinamentos@network.education



NETWORK
EDUCATION

Dúvidas?



Obrigado!



TELECOM

Consultoria, Entrenamiento y Servicios



NETWORK
EDUCATION



TELECOM

Consultoria, Entrenamiento y Servicios



NETWORK
EDUCATION