Automatisation for global BGP tunnel

How to use tools that are not made for the job

support@freetransit.ch
02 480 933 93

Pystyy vetää oy

Who

- Also known as juustoperse

- Migrated to finland in 2020

- Online since 2014 with 58299, then 41666, 41051

What is this talk about

- Research and Education Network

- Our Tunnel Network

Freetransit

- Webplatform for sponsoring of
  - IP Transit (via Tunnels or IXPs)
  - IPv6 Blocks
  - ASN

    Sponsoring is not meant to be cost free, but at cost. Sponsoring ORG is a LIR that ""subresells"" the RIR Resources

Tunnel Setup

- Ticket Request

- Check Authority (Spoofing)

- Check best Tunnel node

- Check prefixes to be announced + are they legit?

- Setup BGP Session

- Documentation

- Support

- Fix mistakes

Pystyy vetää oy

Issues

- We are growing

- VYOS as basis system (config generation from one source for different targes, daemons and interfaces)

- Somtimes needs a reboot

- Recently upgraded to 1.3.2 before rebooting (well, why not)

- Broke. Route Leaks

Pystyy vetää oy

New Platform

- Thinned Debian. No SystemD. Boots in 5 seconds

- Script to pull config from ixpmanager

- Setup tunnels by hand, rest by ixpmanager

- Filter updates (new prefixes/NLRI) get accepted automatically from proper sources

Pystyy vetää oy

What's IXPmanager

- Orchestration for IXPs

- Standard tool

- Opensource

- Can be templated

Pystyy vetää oy

IXPmanager

- Change Template: Instead of RR peer, be regular eBGP Peer.

- Add some local Routings

- Filtering: Mark learned routes towards upstream

- IXP Peerings: No Manual work on routers

Pystyy vetää oy

Member Information ▾ **Peering** ▾ **Documentation** ▾ **Statistics** ▾ **Support** **Staff Link** ▾

Jump to member... ▾   **My Account** ▾

Search for... ❓

Members / Create

Documentation

IXP MEMBER ACTIONS

Members

Member Logos

Tags

Interfaces / Ports

Patch Panels

Users

Contacts

Colocated Equipment

IXP ADMIN ACTIONS

Console Servers

Core Bundles

Document Store

Facilities

Infrastructures

IP Addresses

IRRDB Configuration

MAC Addresses

Racks

Prepopulate this form from PeeringDB by entering the network ASN here:

58299   **Populate**   **Help**

Member Details

Name	Openfactory GmbH
Type	Choose Type ▾
Short Name	openfactor
Corporate Website	https://openfactory.net
Date Joined	10/19/2022 📅
Date Left	mm/dd/yyyy 📅
Status	Choose Status ▾
MD5 Support	Choose MD5 Support ▾
Abbreviated Name	Openfactory GmbH

Peering Details

AS Number	58299
Max Prefixes	3000
Email	peering@example.com
IPv4 Peering Macro	AS58299:AS-ALL
IPv6 Peering Macro	AS-ACME-V6-EXAMPLE
Peering Policy	Choose a Peering Policy ▾
IRRDB Source	Choose a IRRDB Source ✕ ▾

☑ **Active Peering Matrix**

Search for...   ❓

Router / List

Documentation   +

Show [10 ⇅] entries

Search: [_____]

Handle ⇅	Name ⇅	Vlan ⇅	Protocol ⇅	Type ⇅	Router ⇅	Peering IP ⇅	ASN ⇅	Actions ⇅
⊕ r1-klo-v4	r1-klo-v4	**KlotenTransit**	IPv4	RS	82.197.169.75	82.197.169.75	41051	📄 👁 ✏ 🗑
⊕ r1-klo-v6	r1-klo-v6	**KlotenTransit**	IPv6	RS	82.197.169.75	2001:67c:2648:82::75	41051	📄 👁 ✏ 🗑
⊕ r3-fra-v4	r3-fra-v4	**fratransit**	IPv4	RS	5.226.149.45	5.226.149.45	41051	📄 👁 ✏ 🗑
⊕ r3-fra-v6	r3-fra-v6	**fratransit**	IPv6	RS	5.226.149.45	2a00:6340:1000:2024::2	41051	📄 👁 ✏ 🗑

Showing 1 to 4 of 4 entries

Previous   **1**   Next

Search for... ?

IXP MEMBER ACTIONS

Members

Interfaces / Ports

Patch Panels

Users

Contacts

Colocated Equipment

IXP ADMIN ACTIONS

Console Servers

Core Bundles

Document Store

Facilities

Infrastructures

IP Addresses

IRRDB Configuration

MAC Addresses

Racks

Routers

Switches

Switches

Documentation Show Active Only List Mode: Default ▾ +

Show 20 ⬍ entries

Search: _____

Name ⇅	Rack ⇅	Vendor ⇅	Infrastructure ⇅	Active ⇅	Poll ⇅	Model ⇅	IPv4 Address ⇅	Actions
r1-klo	Marktgasse7 Rack Rechts	Linux	Kloten	Yes	Yes	Unknown	82.197.169.75	👁 ✏ 🗑 ▾
r3-fra	Meerfarbig	Linux	Frankfurt	Yes	No	VM	5.226.149.45	👁 ✏ 🗑 ▾

Showing 1 to 2 of 2 entries

Previous 1 Next

❓ This section of **IXP Manager** allows you to add, edit and generally manage your switches. You can add new switches via the ✚ button on the top right.

See the official documentation for more information.

Switch Ports / Create Switch Port

Search for...   ❓

IXP MEMBER ACTIONS

Members

Interfaces / Ports

Patch Panels

Users

Contacts

Colocated Equipment

IXP ADMIN ACTIONS

Console Servers

Core Bundles

Document Store

Facilities

Infrastructures

IP Addresses

IRRDB Configuration

MAC Addresses

Racks

Routers

Switches

⚠ **Use of this method is strongly discouraged!**

While it is possible to add switches and ports without SNMP polling, this is strongly discouraged as SNMP polling will ensure that IXP Manager will pull the correct information from the switch.

Remember also that any information entered here that is updated by an SNMP poll from IXP Manager will be overwritten by that poll.

Switch	r3-fra ▾
Type	Peering ▾
Number of First Port	1337
Number of Ports	1
Name in printf Format	tun%d

Generate   Help

Create   Cancel

Search for... ❓

IXP MEMBER ACTIONS

Members

Interfaces / Ports

Patch Panels

Users

Contacts

Colocated Equipment

IXP ADMIN ACTIONS

Console Servers

Core Bundles

Document Store

Facilities

Infrastructures

IP Addresses

    IPv4 Addresses

    IPv6 Addresses

IRRDB Configuration

MAC Addresses

Racks

IPv4 Addresses

+

VLAN	fratransit ▾	Switch to IPv6 + 🗑

Show 50 ⬍ entries

Search:

IP Address ↑↓	Member ↑↓	Hostname ↑↓	Action ↑↓
169.254.1.26	UPP Microcomponent	as42394.r2-fra-de.node.freetransit.ch	👁 🗑
169.254.1.58	Cyprea	as147039.r2-fra-de.node.freetransit.ch.	👁 🗑
185.1.147.106	Level 86	as212483.foxixp.org	👁 🗑
185.1.147.120	Muilties Network	as205329.fogixp.org	👁 🗑
185.1.166.64	DevStorage	as210633.locix.online	👁 🗑
185.1.166.84	Shinra Electric Power Company	as212068.locix.online.	👁 🗑
185.1.166.151	IT-Service David Froehlich	as39083.locix.online	👁 🗑
185.1.166.212	GeFökoM e.V.	as12817.fra.locix.online.	👁 🗑
185.1.166.237	Christian Elsen	as213151.fra.locix.online.	👁 🗑

Member Information ▾ Peering ▾ Documentation ▾ Statistics ▾ Support Staff Link ▾

Jump to member...   My Account ▾

Search for... ❓

Virtual Interfaces / Create Interface Wizard

IXP MEMBER ACTIONS

Members

Interfaces / Ports

   Physical Interfaces

   Vlan Interfaces

   Sflow Receivers

Patch Panels

Users

Contacts

Colocated Equipment

IXP ADMIN ACTIONS

Console Servers

Core Bundles

Document Store

Facilities

Infrastructures

IP Addresses

IRRDB Configuration

MAC Addresses

Virtual Interface Settings

Member
Choose a member ▾

Vlan
Choose a Vlan ▾

☐ Use 802.1q framing

☐ IPv6 Enabled

☐ IPv4 Enabled

Physical Interface Settings

Switch
Choose a switch ▾

Switch Port
Choose a switch port ▾

Status
Choose a status ▾

Speed
Choose a speed ▾

Duplex
full ▾

General VLAN Settings

Max BGP Prefixes
[   ]

☐ Route Server Client

☑ Apply IRRDB Filtering

☐ IRRDB - Allow More Specifics?

☐ AS112 Client

Create Cancel Help External Documentation ≫

AS-SET

- Definition of your "cone"

- Your upstream and RS should generate filters

- They can be stacked (included)

BROKEN AS-SET

- Recursions

- Misuse: Include upstreams, include large ASN

- Overflow on Hardware resources (ACL)

Pystyy vetää oy

Incident

- We screwed up an ACL and had no more "on exit discard" (default deny) – we lost the last rule on copy paste

- A downstream included their Upstreams

- They leaked that prefix

- We leaked Cloudflare towards Salesforce – and self inflicted DOS

Countermeasures

- Filter more intelligent, detect mistakes
  - Machinelearning
  - AI
  - Static Filters
- Other system (none in use)
- Stop using it

No more acceptance of AS-SET

- Lot more tunnel requests

- Helpful for latency, as resharing tunnels is garbage
  - MTU
  - Scenic Routing
  - Hard debugging
  - More support cases, tho other are the problem

Pystyy vetää oy

Impact with IXPmanager

- Shorter TimeToDeployment

- Automated & Better filter updates

- Documentation built in

- Config Centralized

Pystyy vetää oy

Numbers

~ >>> whois AS41051:AS-PARTICIPANTS|grep members|grep AS|
wc -l

320

~ >>>

ca **0.5%** of the Global IPv6 Table

- Sloppy/Lazyness of Endusers
- Reworking of AMS node

Pystyy vetää oy

Technical

- Neighbor-template.foil.php:
  - rs-client
  - source address routeserveraddress;
  (due to tunnel interfaces)

- Header-foil.php:
  + protocol direct
  + protocol device
  + protocol kernel
  (we do want to write the routes to the operating system, we are actually a router!)

- Footer.foil.php:
  + if/else bird/bird6
  + include "/etc/bird/bird*(6)*.d/*.conf.static";

Pystyy vetää oy

Technical

CONFIG BLOCK PER TUNNEL

auto tun9

iface tun9 inet static

    address 169.254.1.25/30

#netmask 255.255.255.252

    pre-up ip route add 192.0.2.1/32 via 5.226.149.44; ip tunnel add tun9 mode gre local 5.226.149.45 remote 193.33.84.8 ttl 255

    post-down ip route del 192.0.2.1/32; ip tunnel del tun9

iface tun9 inet6 static

    address 2a01:20e:1001:13c::1/64

END CONFIG BLOCK PER TUNNEL

Pystyy vetää oy

Contact

- https://bgp.he.net/AS41051

-

- www.freetransit.ch

- @freetransit_ch

- support@freetransit.ch

Pystyy vetää oy