

「サーバ屋がガチネットワーク
やってみたらこんな感じだった」

おがわ たかし

#ssmjp

2015/8/27 JANOG LT Night

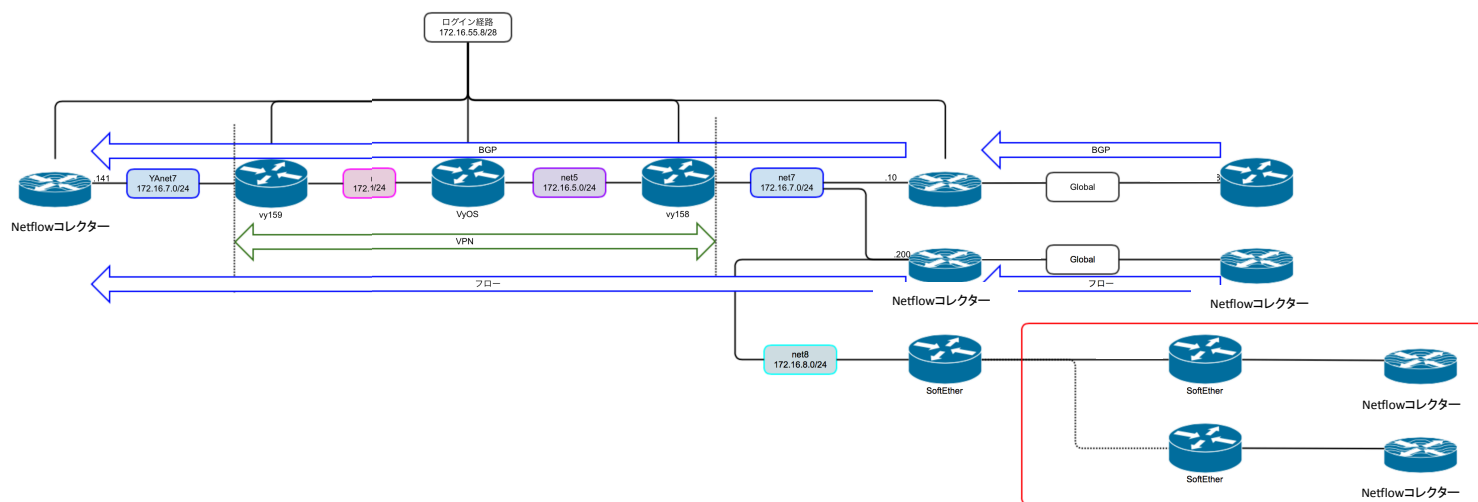
自己紹介



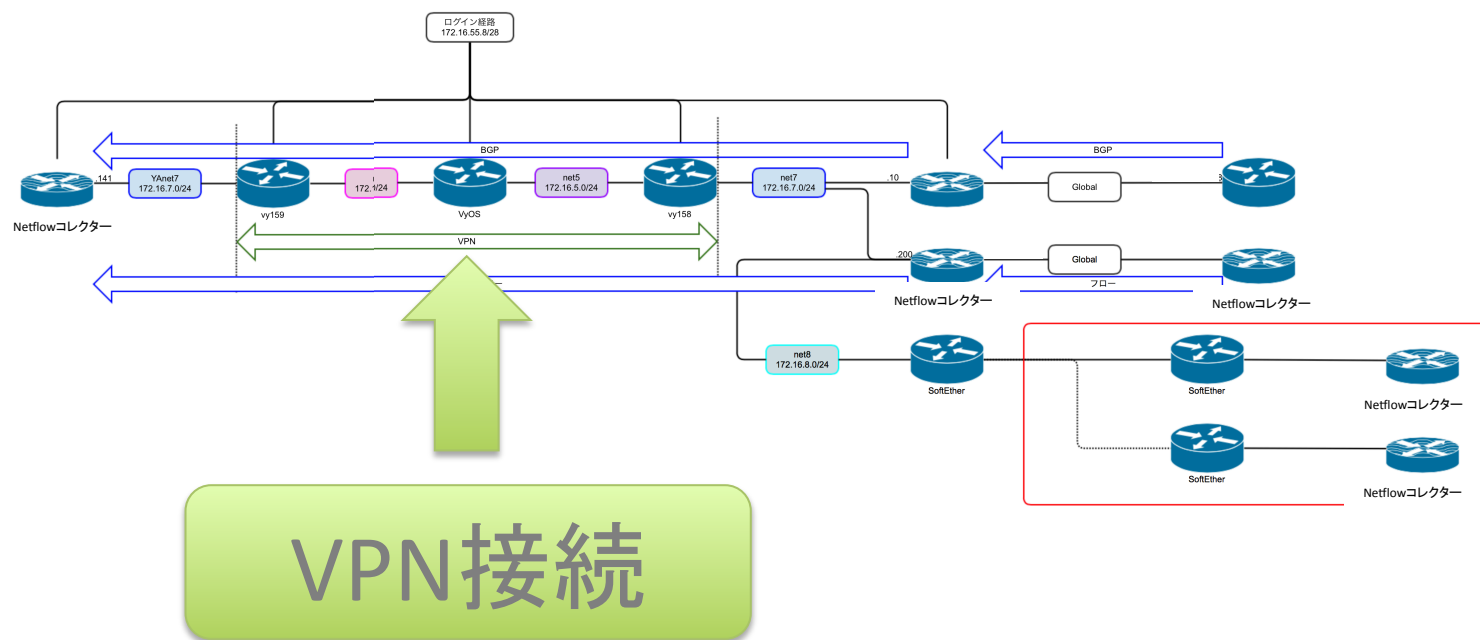
- TW : @yakumo3
- FB : おがわたかし
- 所属 : #ssmjp(主宰)
- 装輪整備手 / Cプログラマ /
セキュリティエンジニア /
インフラエンジニア
- 好きなMSはLM314V25

サーバ屋がガチネットワークをやる経緯

なんかこんな絵が降ってきた。

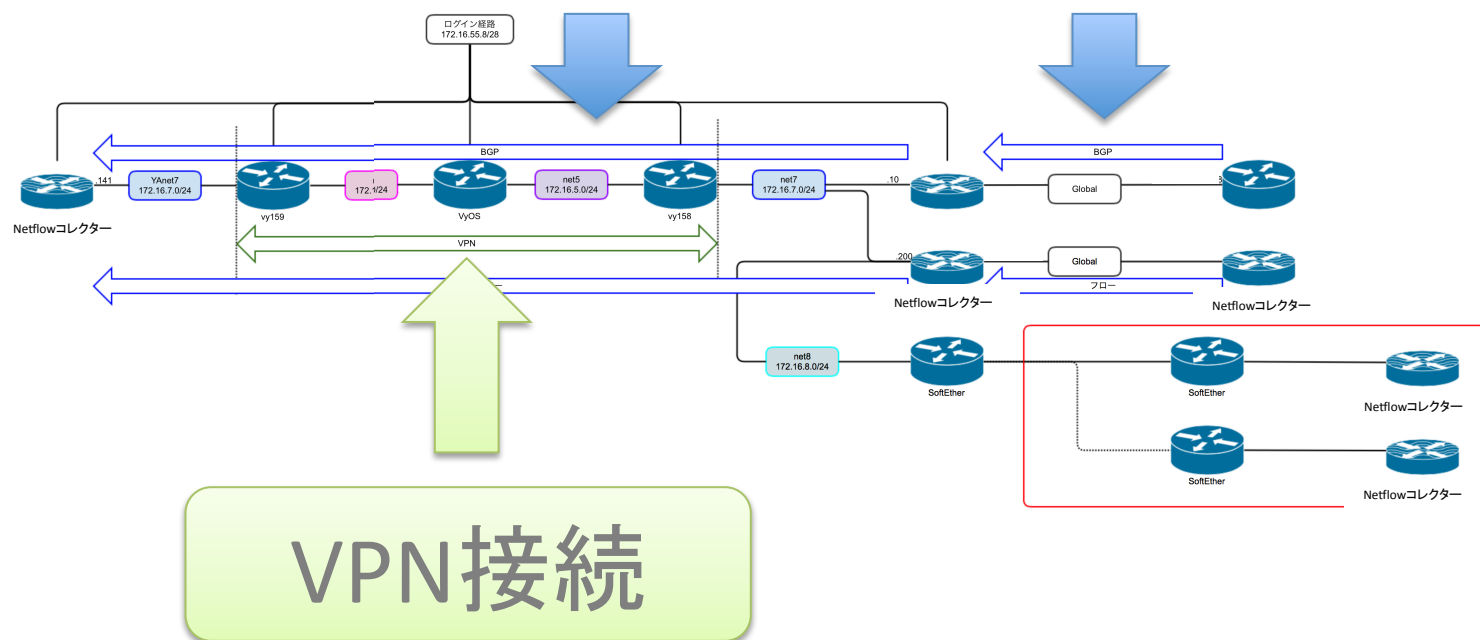


やること



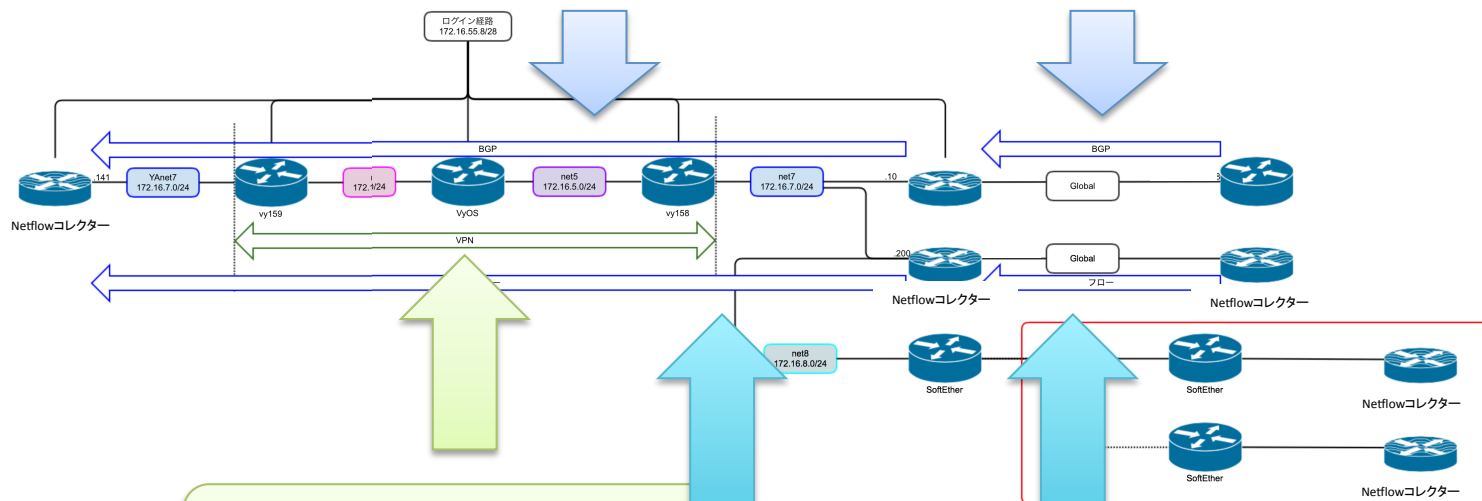
やること

BGP接続*2



やること

BGP接続*2

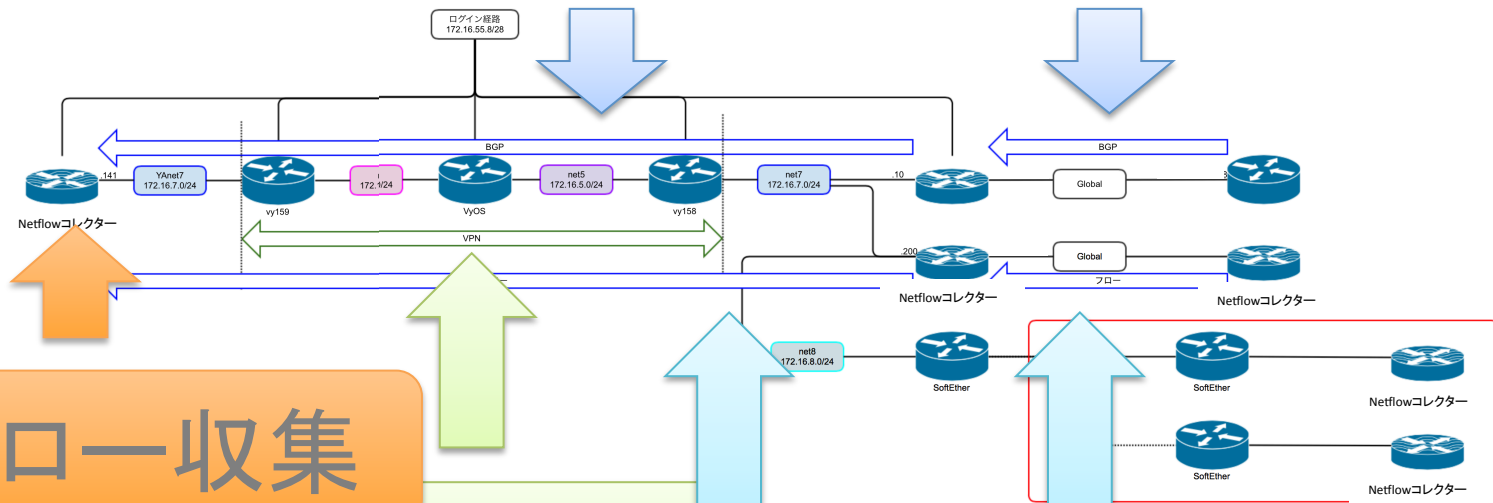


VPN接続

フロー転送*2

やること

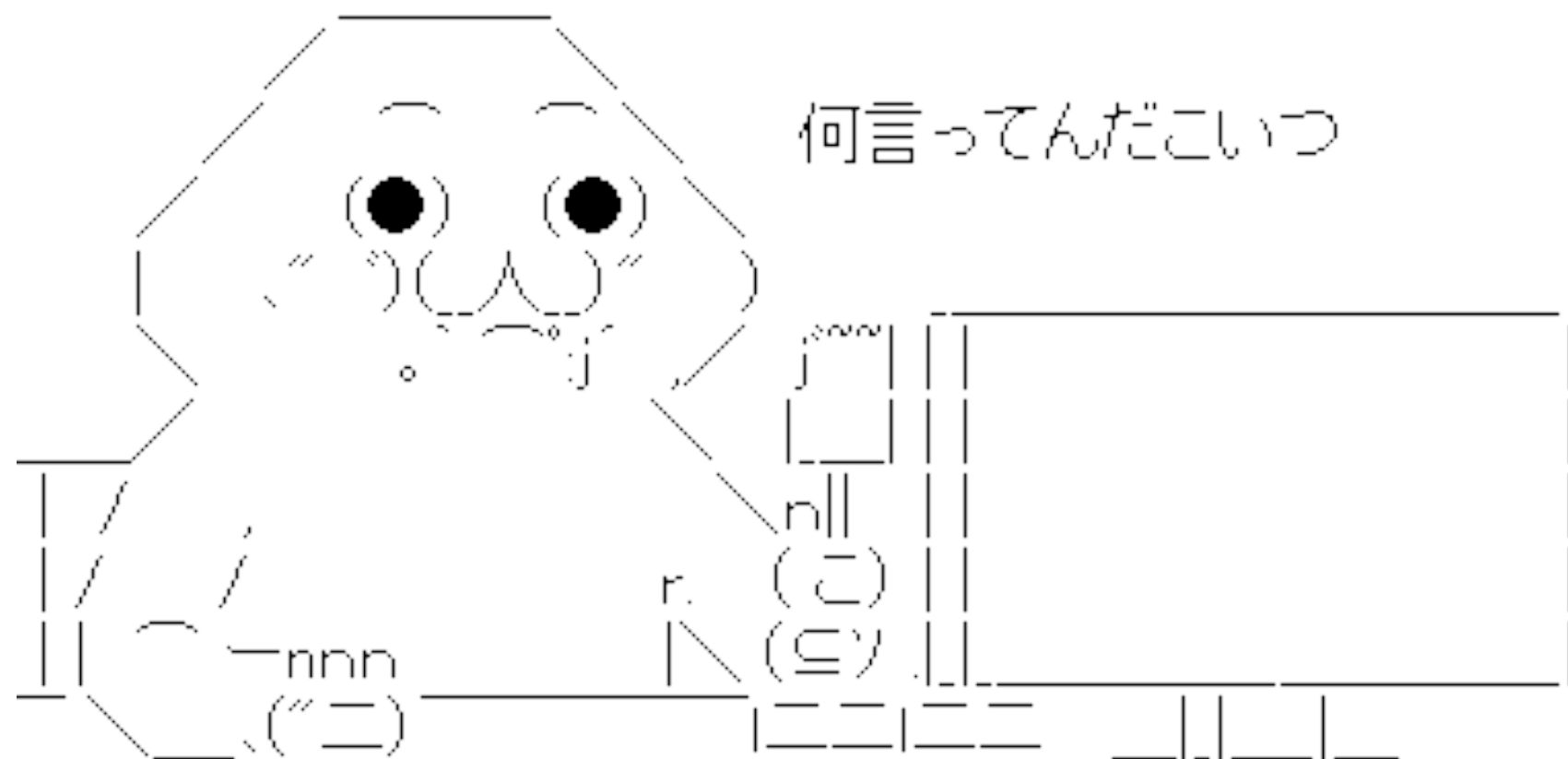
BGP接続*2



フロー収集

VPN接続

フロー転送*2



とは言えないので

実現の方法を検討

- VPNはVyOSで張れそう
- BGPはJuniperとVyOSで張って、それをVPN越しで飛ばそう
- フローはVPNさえ張れれば行けるんじゃないか？

- VyOSでVPNは簡単でした。
- ググると情報も結構豊富



約 17,400 件 (0.49 秒)

BGPってなんだ？



詳解
新世代ルータOS

はじめての JUNOS

S t a r t i n g J U N O S

ISBN4-8222-1280-7 日経BP社

「はじめての」
とは書いてあるけど、
「初心者への」
とは書いてなかった！

設定入力の方法が出るのが
P85、それまではずっと
アーキテクチャの話

- 泣きながらP224からのBGPの章を読む
- 知らない用語が山盛り出て来る
(と言うか知ってる単語の方が少ない)

不幸中の幸い

- バックボーンチームが隣にいた
- BGPオペレーターだらけ
- アドバイスを貰いながら何とか設定できた

罫

ないしょ

BGP router identifier 64626 local AS number 64626
IPv4 Unicast - max multipaths: ebgp 255 ibgp 1
RIB entries 1005143, using 92 MiB of memory
Peers 3, using 13 KiB of memory

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
	4	65001	105527	4639839	0	0	0	3d08h10m	Active
ないしょ	4	64626	24963	2150871	0	0	0	3d22h32m	0
	4	64600	3120202	263575	0	0	0	04w2d17h	547825

Total number of neighbors 3

State/PfxRcd
Active

罣

ないしょ

```
BGP router identifier ないしょ local AS number 64626
IPv4 Unicast - max multipaths: ebgp 255 ibgp 1
RIB entries 1005143, using 92 MiB of memory
Peers 3, using 13 KiB of memory
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
ないしょ	4	65001	105527	4639839	0	0	0	3d08h10m	Active
	4	64626	24963	2150871	0	0	0	3d22h32m	0
	4	64600	3120202	263575	0	0	0	04w2d17h	547825

Total number of neighbors 3

~~State/PfxRcd
Active~~



547825

学び

- 「はじめての」と銘打ってあっても業界初めての人は対象じゃない可能性がある。
- 困ったら聞ける環境大事

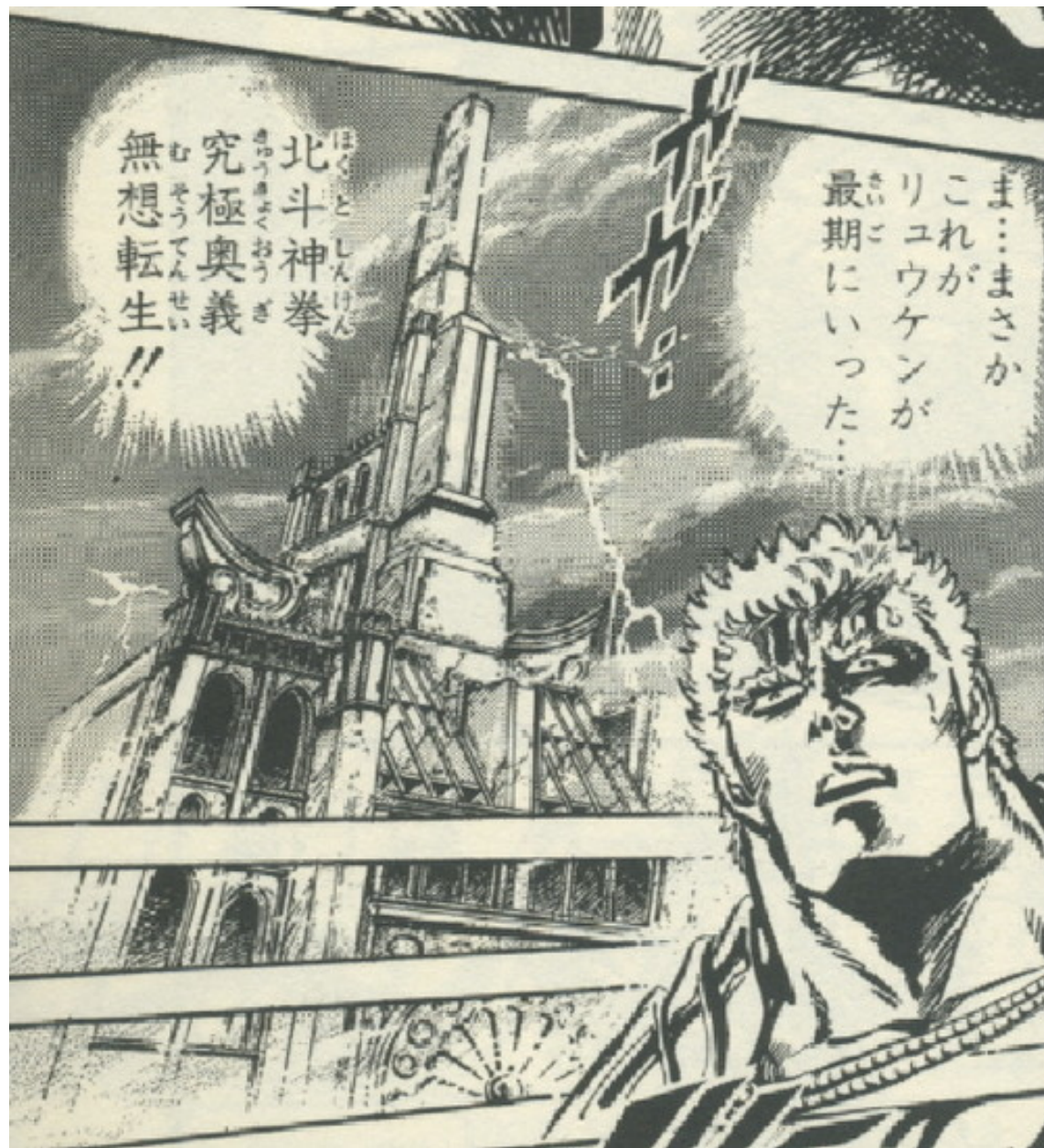
残るはフロー転送

フロー？

僕が知ってるフロー

フロー (英: Flow) とは、人間がそのときしていることに、完全に浸り、精力的に集中している感覚に特徴づけられ、完全にのめり込んでいて、その過程が活発さにおいて成功しているような活動における、精神的な状態をいう。ZONE、ピークエクスペリエンスとも呼ばれる。

http://ja.wikipedia.org/wiki/%E3%83%95%E3%83%AD%E3%83%BC_%28%E5%BF%83%E7%90%86%E5%AD%A6%29



(ジャンプコミック 北斗の拳より)

紆余曲折ありまして

- 経路上のRouterのフィルターが開いてなかった
経路上のスイッチのVlan設定が入ってなかった
仮想基盤の仕様でL2接続できなかった
L3接続だと思って使ってみたSoftetherはL2接続+L3接続な仕様だったから結局使えなかった
手元の仮想環境でサーバ量産して評価したらローカルIPを使い果たして新たに払いだして設定したら経路上のRouterのフィルターが開いてなかったり経路上のスイッチの

できた

NWを触ってみた感想

- BGPとかネットフローとかネット上に情報が少ない
- 一子相伝的に口伝で伝わる技術継承
 - NWを学びたくてもNWの仕事に付かないと学べない？
- なんでJANOGがあるのか何となく分かった
 - サーバ屋はJANOG的なのが無い

NWを触ってみた感想

- サーバ屋がネットワークに触れてみるなら、VyOSやJUNOS系が良い
- NW装置のノリに慣れるとCISCO系は楽
- NW装置はAnsibleとか相性良さそう
- サーバ屋がNW装置をいじりすぎると、サーバでコマンドを打ってる途中で”？”とか”tab”とか打つので注意

まとめ

- サーバ屋は一度本格的なNWに触れて、NW屋さんとは話すると、よりサーバもNWも楽しくなる
- サーバ屋とNW屋さんは同じチームで働いた方がお互いの業務に良い影響をあたえるんじゃないかと思いました