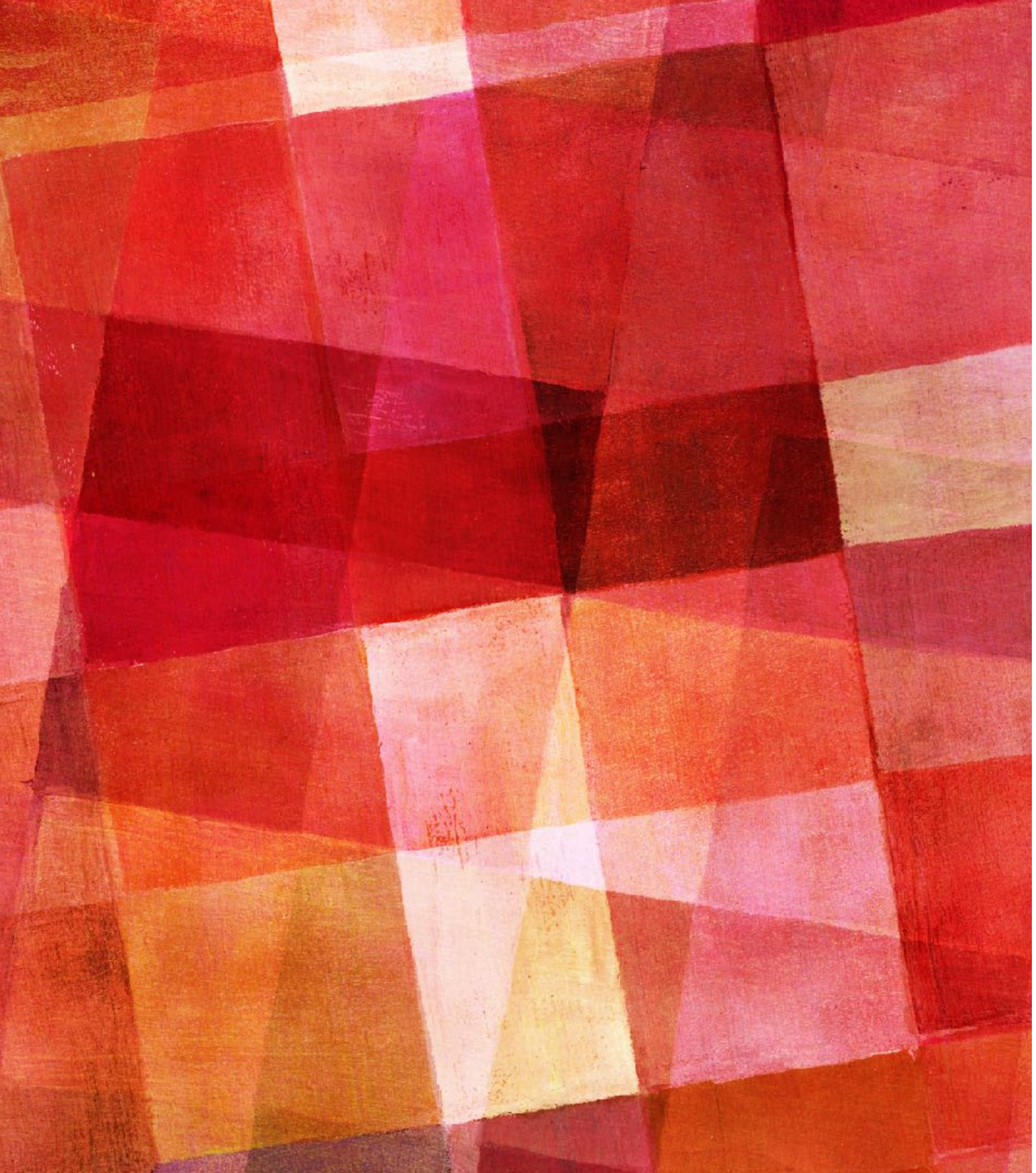
DOCUMENTING YOUR NETWORK IN 3 SIMPLE STEPS

for saner & healthier network administrators

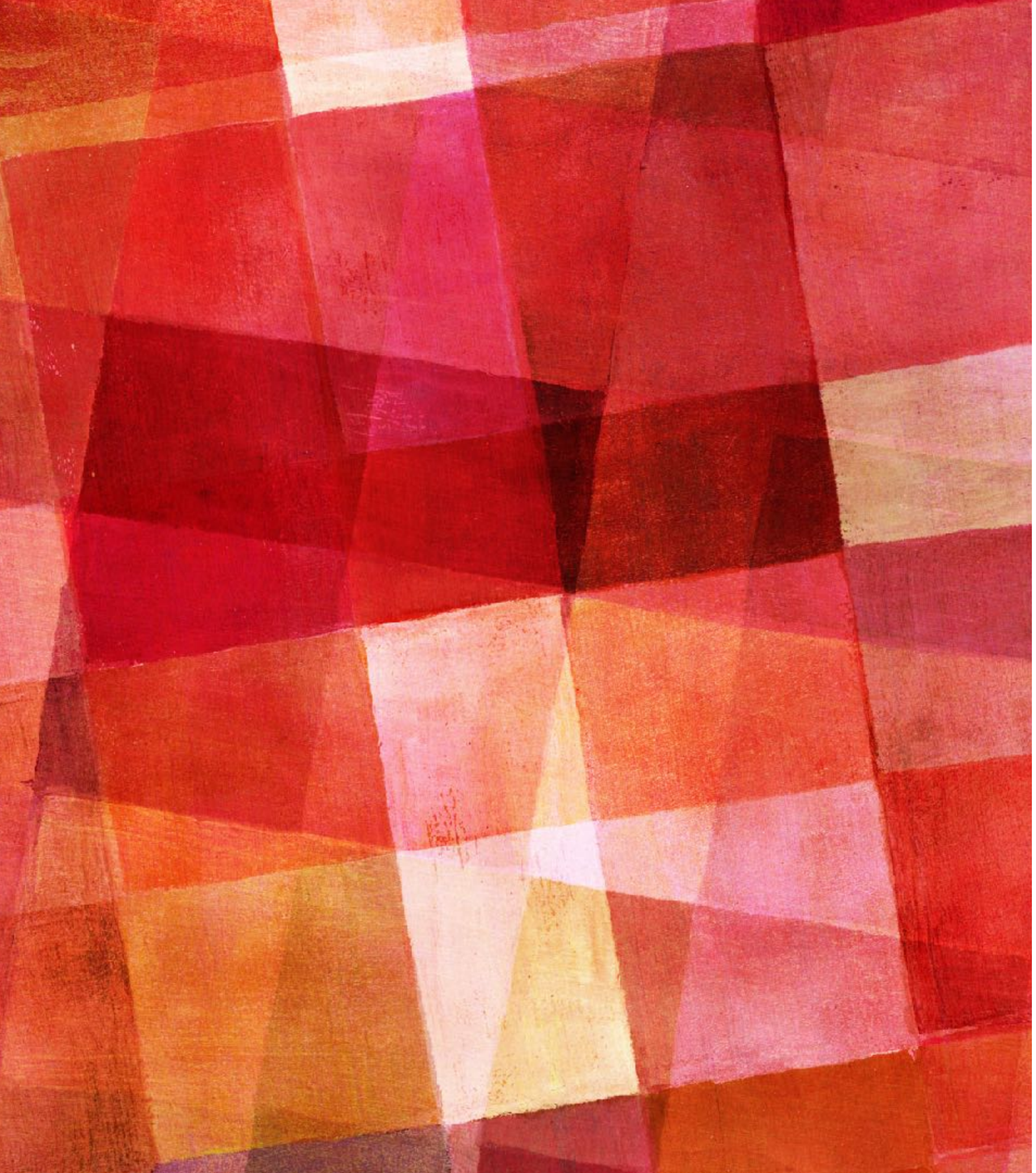
WHOAMI

- Affan Basalamah
- IT Development Manager
- Institut Teknologi Bandung (itb.ac.id)
- @affanzbasalamah



SANE & HEALTHY SYSADMIN ARE GOOD

- They perform well in the workplaces in weekdays
- Your family loves you
- And also your employer
- OTOH, insane & unhealthy sysadmins are toxic in workplaces
  - BOFH (Bast*rd operator from hell) is not good for workplaces
  - Not getting things done



THREE STEPS

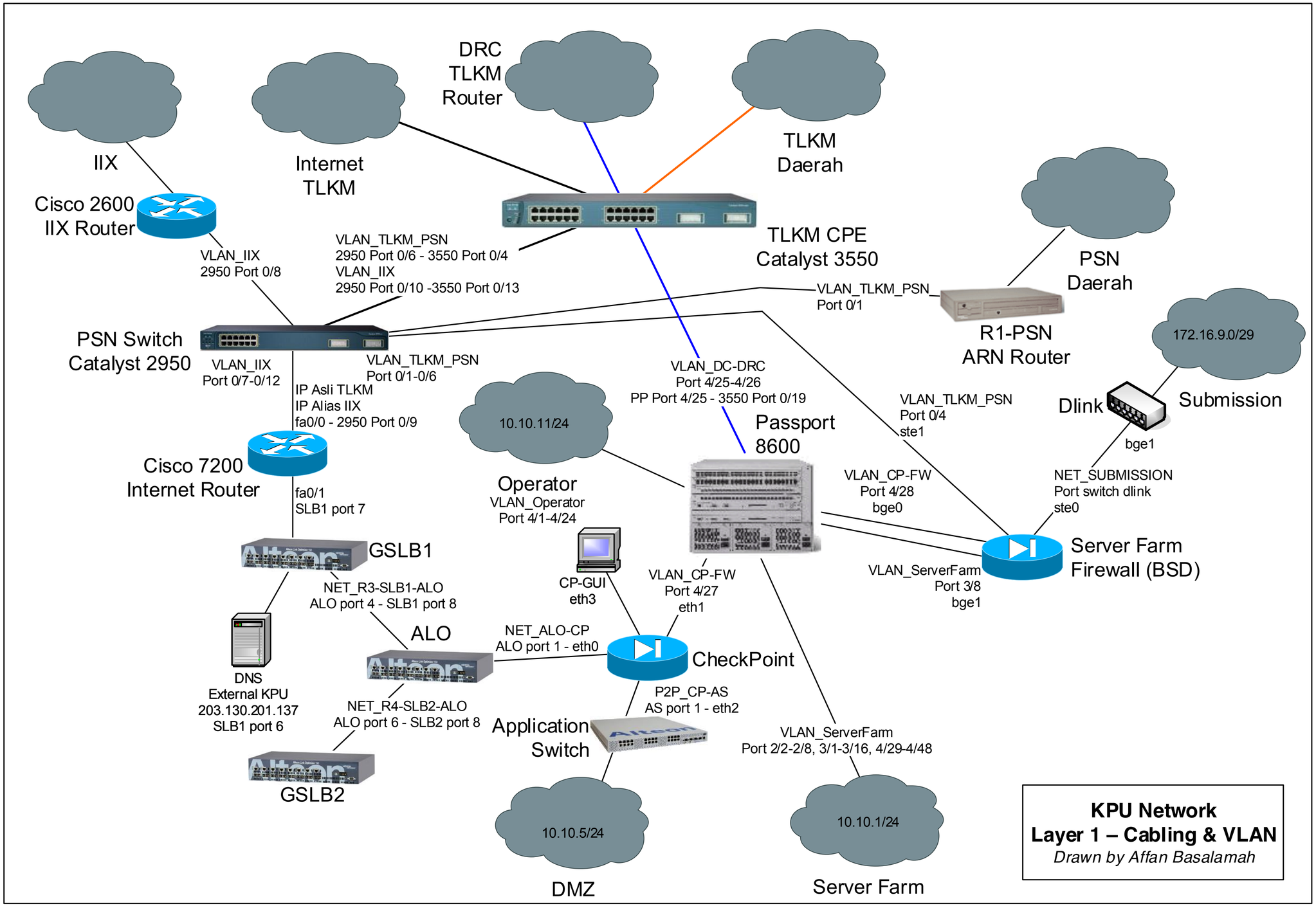
1. Drawing your network
2. Backup your network config
3. Use IP address management tools

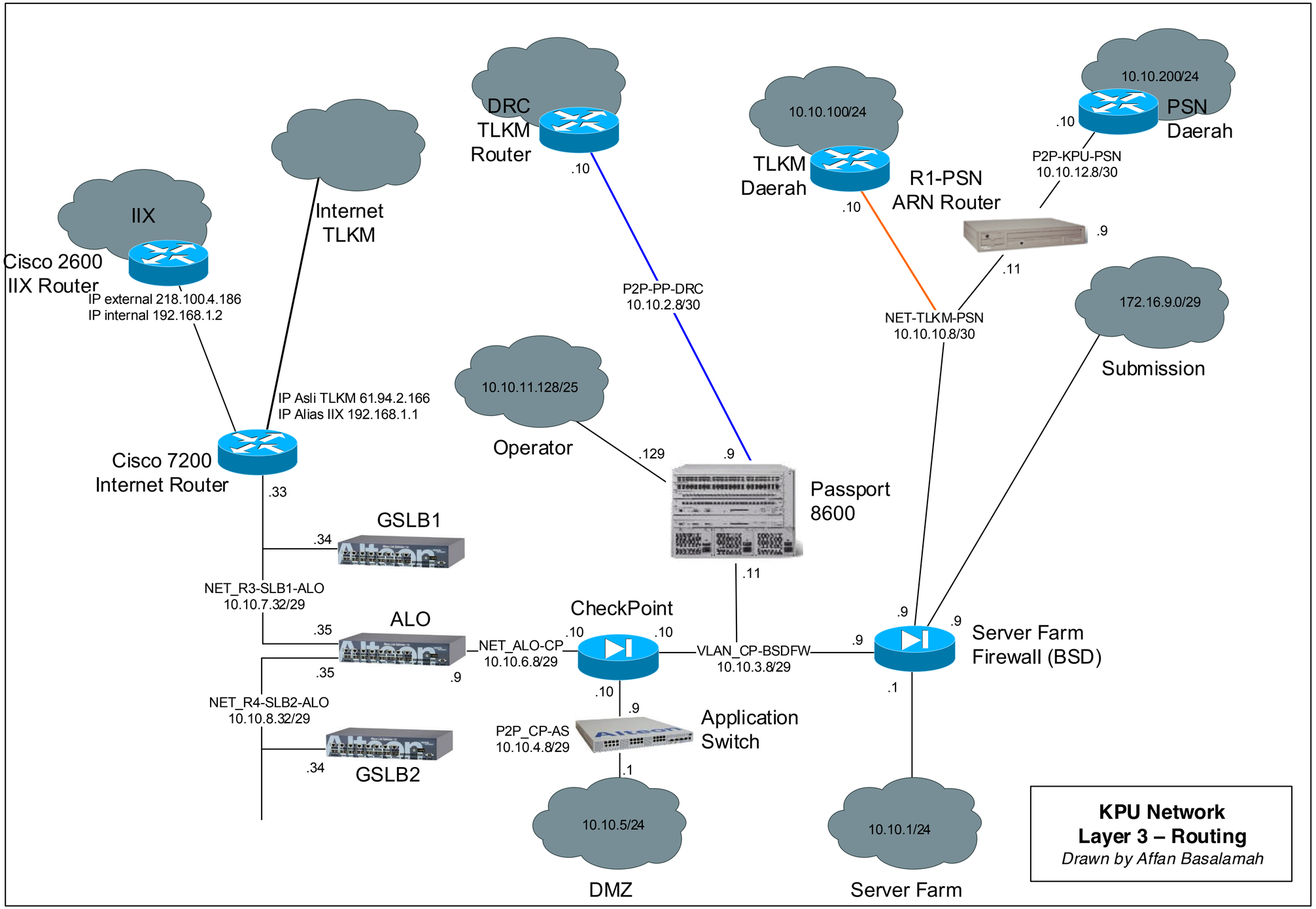
1ST – DRAWING YOUR NETWORK

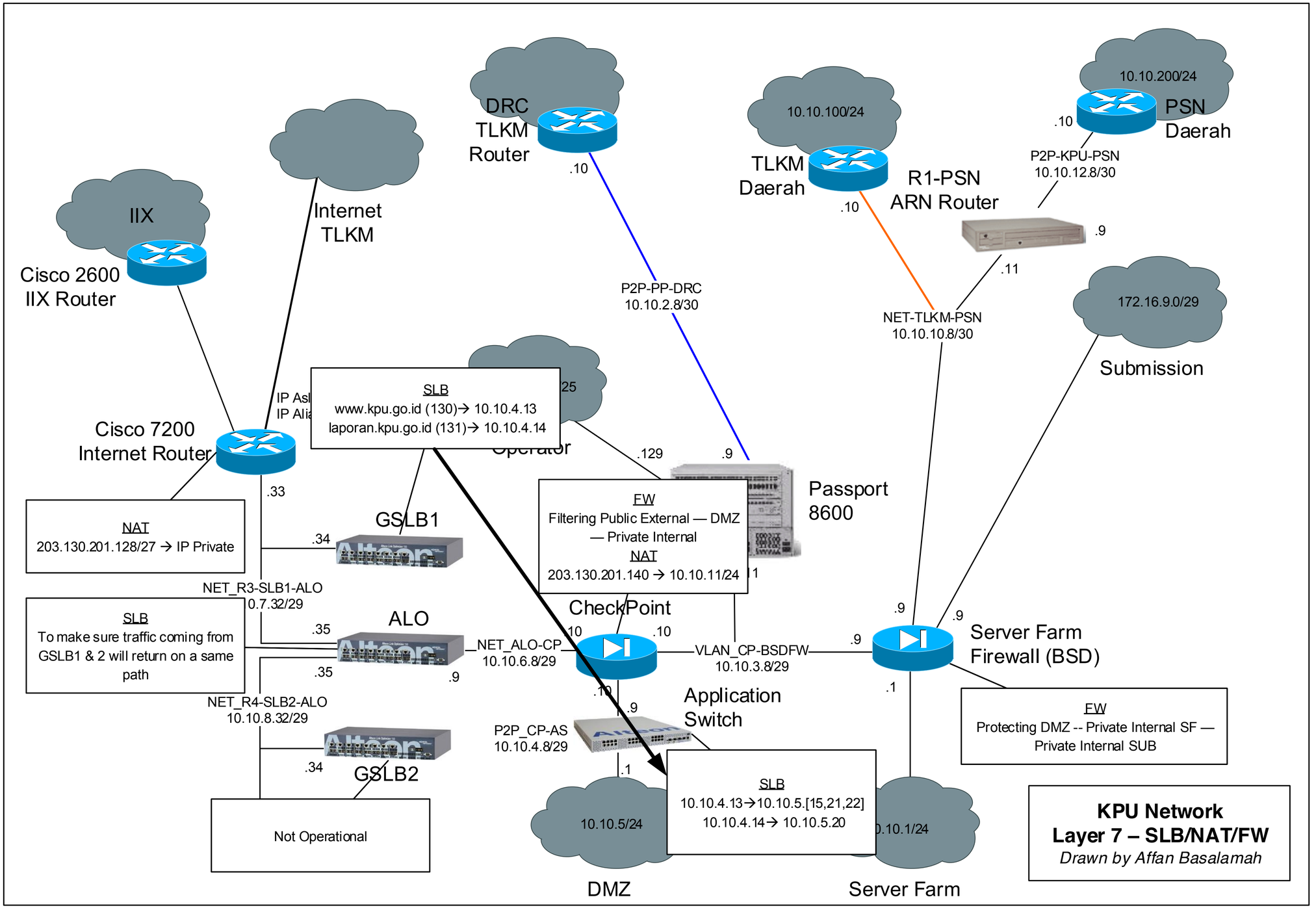
- **Lots of tools:**
  - Microsoft Visio (no macOS version yet, only Visio Viewer on iPad)
  - EDrawMax or OmniGraffle for macOS
  - Network Notepad (free version, commercial version available)
- **Starts with the basics:**
  - Layer 1 and layer 2 diagram
  - Layer 3 diagram
  - Layer 4 to layer 7 diagram
- **Put them at accessible websites/private wiki**
  - Or better, put them on Cacti with Weathermap plugin!

DRAWING YOUR NETWORK

- **Layer 1 and layer 2 diagram**
  - ***Physical connectivities***: cables, WiFi channel, ports, unmanaged NE,
  - Physical identities: MAC address
- **Layer 3 diagram**
  - ***Logical connectivities***: subnet, VLAN
  - Physical identities: IP[v4,v6] address, loopback address
- **Layer 4 to layer 7 diagram**
  - ***End-to-end connectivities***: middleboxes (NAT, Firewall, VPN, ADC, etc.)
  - Network function other than connectivity: address translation, packet filter, load balancer, secure tunnel, etc.


IIX
Internet
TLKM
DRC
TLKM
Router
TLKM
Daerah
Cisco 2600
IIX Router
VLAN_IIX
2950 Port 0/8
VLAN_TLKM_PSN
2950 Port 0/6 - 3550 Port 0/4
VLAN_IIX
2950 Port 0/10 -3550 Port 0/13
TLKM CPE
Catalyst 3550
PSN
Daerah
VLAN_TLKM_PSN
Port 0/1
R1-PSN
ARN Router
172.16.9.0/29
PSN Switch
Catalyst 2950
VLAN_IIX
Port 0/7-0/12
VLAN_TLKM_PSN
Port 0/1-0/6
VLAN_DC-DRC
Port 4/25-4/26
PP Port 4/25 - 3550 Port 0/19
VLAN_TLKM_PSN
Port 0/4
ste1
Dlink
Submission
bge1
IP Asli TLKM
IP Alias IIX
fa0/0 - 2950 Port 0/9
10.10.11/24
Passport
8600
Cisco 7200
Internet Router
fa0/1
SLB1 port 7
Operator
VLAN_Operator
Port 4/1-4/24
VLAN_CP-FW
Port 4/28
bge0
NET_SUBMISSION
Port switch dlink
ste0
GSLB1
CP-GUI
eth3
VLAN_CP-FW
Port 4/27
eth1
Server Farm
Firewall (BSD)
VLAN_ServerFarm
Port 3/8
bge1
NET_R3-SLB1-ALO
ALO port 4 - SLB1 port 8
ALO
NET_ALO-CP
ALO port 1 - eth0
CheckPoint
DNS
External KPU
203.130.201.137
SLB1 port 6
P2P_CP-AS
AS port 1 - eth2
NET_R4-SLB2-ALO
ALO port 6 - SLB2 port 8
Application
Switch
VLAN_ServerFarm
Port 2/2-2/8, 3/1-3/16, 4/29-4/48
GSLB2
10.10.5/24
10.10.1/24
DMZ
Server Farm
KPU Network
Layer 1 – Cabling & VLAN
Drawn by Affan Basalamah


IIX
Cisco 2600
IIX Router
IP external 218.100.4.186
IP internal 192.168.1.2
Internet
TLKM
IP Asli TLKM 61.94.2.166
IP Alias IIX 192.168.1.1
Cisco 7200
Internet Router
.33
GSLB1
.34
NET_R3-SLB1-ALO
10.10.7.32/29
ALO
.35
.35
.9
NET_R4-SLB2-ALO
10.10.8.32/29
.34
GSLB2
DRC
TLKM
Router
.10
P2P-PP-DRC
10.10.2.8/30
10.10.11.128/25
Operator
.129
.9
Passport
8600
.11
CheckPoint
.10
.10
NET_ALO-CP
10.10.6.8/29
VLAN_CP-BSDFW
10.10.3.8/29
.10
.9
P2P_CP-AS
10.10.4.8/29
Application
Switch
.1
10.10.5/24
DMZ
10.10.100/24
TLKM
Daerah
.10
R1-PSN
ARN Router
NET-TLKM-PSN
10.10.10.8/30
10.10.200/24
.10
PSN
Daerah
P2P-KPU-PSN
10.10.12.8/30
.9
.11
172.16.9.0/29
Submission
.9
.9
.9
.1
Server Farm
Firewall (BSD)
10.10.1/24
Server Farm
KPU Network
Layer 3 – Routing
Drawn by Affan Basalamah


DRC
TLKM
Router
.10
10.10.100/24
TLKM
Daerah
.10
10.10.200/24
PSN
Daerah
.10
P2P-KPU-PSN
10.10.12.8/30
R1-PSN
ARN Router
.9
.11
IIX
Cisco 2600
IIX Router
Internet
TLKM
P2P-PP-DRC
10.10.2.8/30
NET-TLKM-PSN
10.10.10.8/30
172.16.9.0/29
Submission
SLB
www.kpu.go.id (130)→ 10.10.4.13
laporan.kpu.go.id (131)→ 10.10.4.14
Cisco 7200
Internet Router
.33
.129
.9
Passport
8600
FW
Filtering Public External — DMZ
— Private Internal
NAT
203.130.201.140 → 10.10.11/24
NAT
203.130.201.128/27 → IP Private
.34
GSLB1
NET_R3-SLB1-ALO
10.10.7.32/29
SLB
To make sure traffic coming from
GSLB1 & 2 will return on a same
path
.35
ALO
.35
.9
NET_ALO-CP
10.10.6.8/29
.10
.10
CheckPoint
VLAN_CP-BSDFW
10.10.3.8/29
.9
.9
.9
Server Farm
Firewall (BSD)
.1
.10
.9
Application
Switch
NET_R4-SLB2-ALO
10.10.8.32/29
P2P_CP-AS
10.10.4.8/29
FW
Protecting DMZ -- Private Internal SF —
Private Internal SUB
.34
GSLB2
.1
SLB
10.10.4.13→10.10.5.[15,21,22]
10.10.4.14→ 10.10.5.20
10.10.5/24
10.10.1/24
Not Operational
DMZ
Server Farm
KPU Network
Layer 7 – SLB/NAT/FW
Drawn by Affan Basalamah

2ND – BACKUP YOUR NETWORK CONFIG

- But first, let's centralize network authentication first
  - Get small Linux/BSD server
  - Make sure your NE can use Tacacs+ or Radius login authentication
  - Install loopback IP on your NE
  - Use SSH, disable Telnet
- **RANCID** (*Really Awesome New Cisco Config Differ*) http://www.shrubbery.net/rancid/
  - Simple Expect script that can periodically save your router config on CVS repo
  - If there's a difference in last config, it can email you the diff
  - Most router supported: Cisco IOS/XE, JunOS, IronWare, HP, etc.

RIGHT NOW THERE'S OXIDIZE

- RANCID ➟ **Oxidize** https://github.com/ytti/oxidized
- If there's a difference in last config, it can email you the diff
- Support lots of NE: Cisco IOS/XE/XR, JunOS, IronWare, etc.
  - Even Mikrotik router!
- CVS and Git repo supported
- Hooks: after backup & config diff, it can send message to AWS SNS and Slack channel

versions / Diff version 36 - 35 for Node `Labtek5.NOC-Labtek5-GTW.brocade`

Date of version: 24-06-17 at 05:03:47 PM

Number of lines changed: added 15 removed 15

Version 37 (15 days 11 hours ago)

Get Diffs!

Version 35 (40 days 20 hours ago)

```
diff --git a/Labtek5.NOC-Labtek5-GTW.brocade b/Labtek5.NOC-Labtek5-GTW.brocade
index 484b942..da46176 100644
--- a/Labtek5.NOC-Labtek5-GTW.brocade
@@ -2202,8 +2202,8 @@ interface ve 8
  ip ospf area 0
  ip address 167.205.48.1/26
  ip policy route-map pbr-mx
- ip helper-address 167.205.23.74
  ip helper-address 167.205.62.54

 !
 interface ve 9
  port-name Router_radar
@@ -2315,31 +2315,31 @@ interface ve 26
  ip ospf area 0
  ip address 167.205.48.193/27
  ip policy route-map pbr-mx
- ip helper-address 167.205.23.74
  ip helper-address 167.205.62.54

 !
 interface ve 27
  port-name SITH
  ip ospf area 0
  ip address 167.205.38.65/26
```

Version 36 (30 days 17 hours ago)

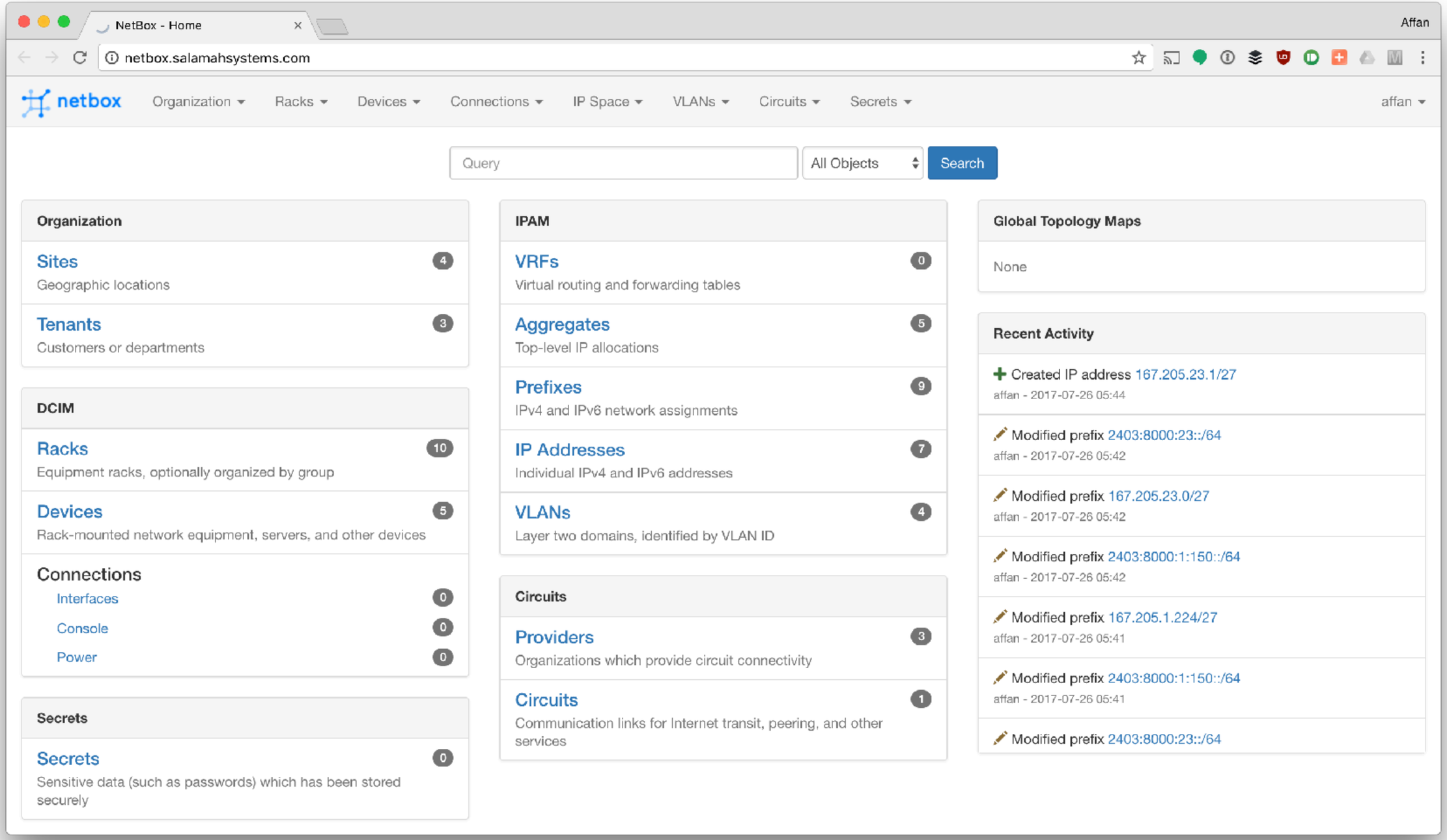
```
diff --git a/Labtek5.NOC-Labtek5-GTW.brocade b/Labtek5.NOC-Labtek5-GTW.brocade
index 484b942..da46176 100644
+++ b/Labtek5.NOC-Labtek5-GTW.brocade
@@ -2202,8 +2202,8 @@ interface ve 8
  ip ospf area 0
  ip address 167.205.48.1/26
  ip policy route-map pbr-mx

  ip helper-address 167.205.62.54
+ ip helper-address 167.205.23.74
 !
 interface ve 9
  port-name Router_radar
@@ -2315,31 +2315,31 @@ interface ve 26
  ip ospf area 0
  ip address 167.205.48.193/27
  ip policy route-map pbr-mx

  ip helper-address 167.205.62.54
+ ip helper-address 167.205.23.74
 !
 interface ve 27
  port-name SITH
  ip ospf area 0
  ip address 167.205.38.65/26
```

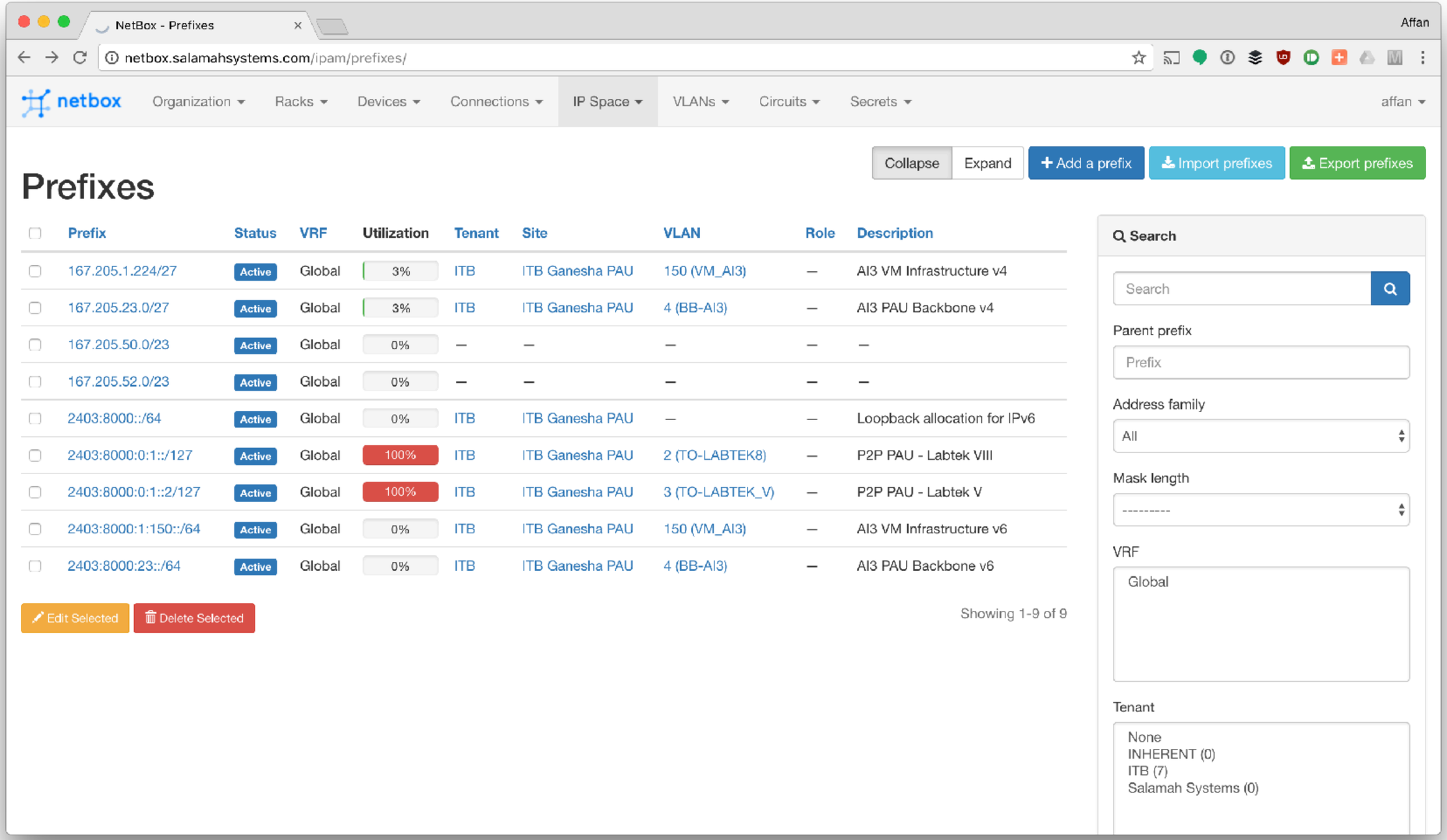
3RD – USE IP ADDRESS MANAGEMENT TOOLS (IPAM)

- You use MS Excel to record your IP address assignment, right? Please don't lie!
- Recording your IPv4 assignment is easy right? Try IPv6!
- Deploying IPv6 network forces you to use IPAM
- Which tools you use?
  - Commercial: from ManageEngine, SolarWinds, etc.
  - Opensource: Netbox, phpIPAM, GestioIP, Netdot, etc.
  - I choose Netbox https://github.com/digitalocean/netbox

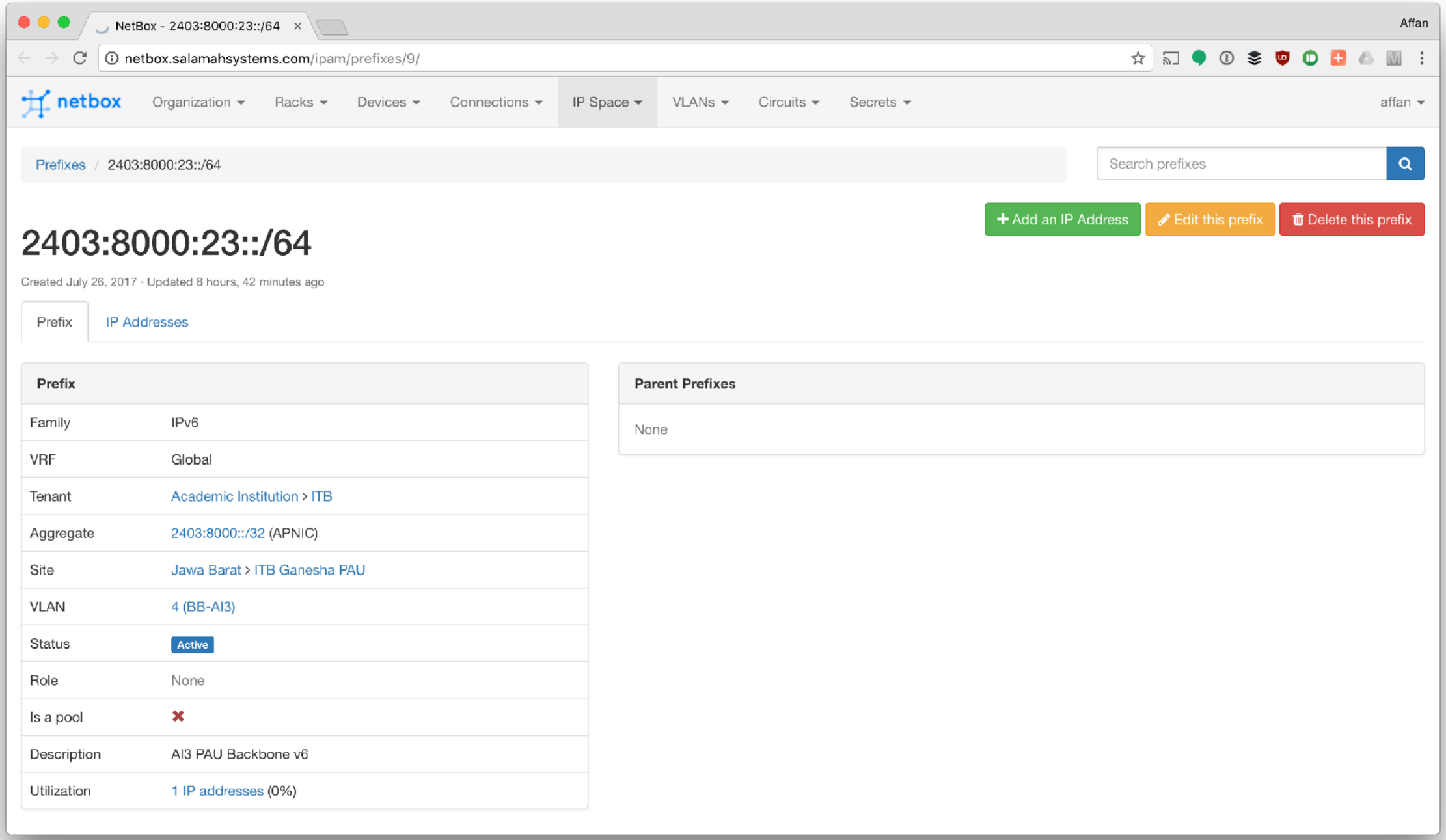
NETBOX FOR DOCUMENTING YOUR NETWORK

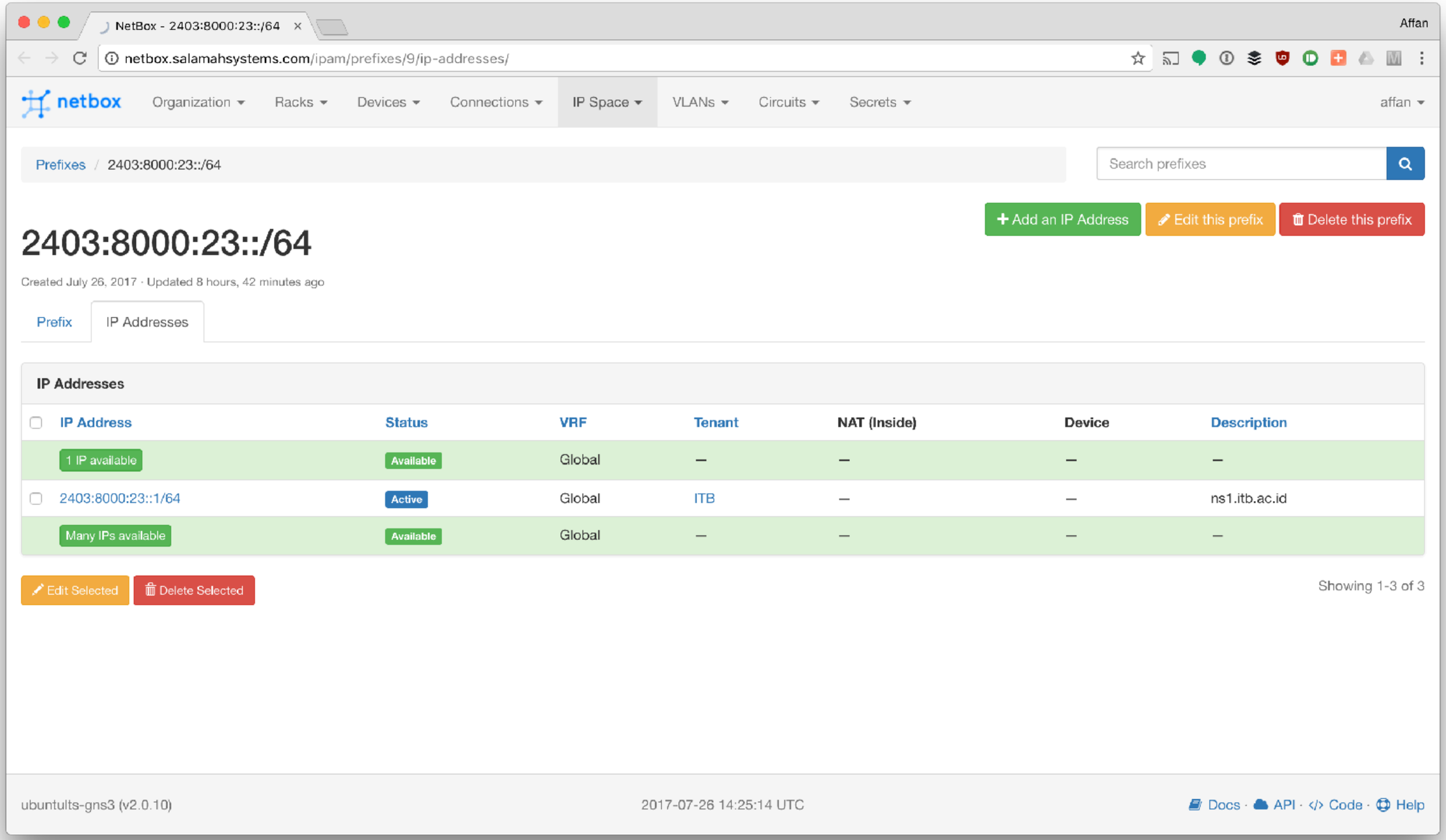
- Not only IPAM, but DCIM at the same time
- Documenting your datacenter also
- IPv4 prefix, IPv6 prefix, on global network or VRF
- Which devices, sits on which rack, in which room, connecting to which link?


NetBox - Home
Affan
netbox.salamahsystems.com
netbox
Organization
Racks
Devices
Connections
IP Space
VLANs
Circuits
Secrets
affan
Query
All Objects
Search
Organization
Sites
Geographic locations
4
Tenants
Customers or departments
3
DCIM
Racks
Equipment racks, optionally organized by group
10
Devices
Rack-mounted network equipment, servers, and other devices
5
Connections
Interfaces
0
Console
0
Power
0
Secrets
Secrets
Sensitive data (such as passwords) which has been stored securely
0
IPAM
VRFs
Virtual routing and forwarding tables
0
Aggregates
Top-level IP allocations
5
Prefixes
IPv4 and IPv6 network assignments
9
IP Addresses
Individual IPv4 and IPv6 addresses
7
VLANs
Layer two domains, identified by VLAN ID
4
Circuits
Providers
Organizations which provide circuit connectivity
3
Circuits
Communication links for Internet transit, peering, and other services
1
Global Topology Maps
None
Recent Activity
Created IP address 167.205.23.1/27
affan - 2017-07-26 05:44
Modified prefix 2403:8000:23::/64
affan - 2017-07-26 05:42
Modified prefix 167.205.23.0/27
affan - 2017-07-26 05:42
Modified prefix 2403:8000:1:150::/64
affan - 2017-07-26 05:42
Modified prefix 167.205.1.224/27
affan - 2017-07-26 05:41
Modified prefix 2403:8000:1:150::/64
affan - 2017-07-26 05:41
Modified prefix 2403:8000:23::/64


NetBox - Prefixes
Affan
netbox.salamahsystems.com/ipam/prefixes/
netbox
Organization
Racks
Devices
Connections
IP Space
VLANs
Circuits
Secrets
affan
Collapse
Expand
+ Add a prefix
Import prefixes
Export prefixes
Prefixes
Prefix
Status
VRF
Utilization
Tenant
Site
VLAN
Role
Description
167.205.1.224/27 Active Global 3% ITB ITB Ganesha PAU 150 (VM_AI3) — AI3 VM Infrastructure v4
167.205.23.0/27 Active Global 3% ITB ITB Ganesha PAU 4 (BB-AI3) — AI3 PAU Backbone v4
167.205.50.0/23 Active Global 0% — — — — —
167.205.52.0/23 Active Global 0% — — — — —
2403:8000::/64 Active Global 0% ITB ITB Ganesha PAU — — Loopback allocation for IPv6
2403:8000:0:1::/127 Active Global 100% ITB ITB Ganesha PAU 2 (TO-LABTEK8) — P2P PAU - Labtek VIII
2403:8000:0:1::2/127 Active Global 100% ITB ITB Ganesha PAU 3 (TO-LABTEK_V) — P2P PAU - Labtek V
2403:8000:1:150::/64 Active Global 0% ITB ITB Ganesha PAU 150 (VM_AI3) — AI3 VM Infrastructure v6
2403:8000:23::/64 Active Global 0% ITB ITB Ganesha PAU 4 (BB-AI3) — AI3 PAU Backbone v6
Edit Selected
Delete Selected
Showing 1-9 of 9
Search
Search
Parent prefix
Prefix
Address family
All
Mask length

VRF
Global
Tenant
None
INHERENT (0)
ITB (7)
Salamah Systems (0)


NetBox - 2403:8000:23::/64
Affan
netbox.salamahsystems.com/ipam/prefixes/9/
netbox
Organization
Racks
Devices
Connections
IP Space
VLANs
Circuits
Secrets
affan
Prefixes / 2403:8000:23::/64
Search prefixes
+ Add an IP Address
Edit this prefix
Delete this prefix
2403:8000:23::/64
Created July 26, 2017 · Updated 8 hours, 42 minutes ago
Prefix
IP Addresses
Prefix
Family IPv6
VRF Global
Tenant Academic Institution > ITB
Aggregate 2403:8000::/32 (APNIC)
Site Jawa Barat > ITB Ganesha PAU
VLAN 4 (BB-AI3)
Status Active
Role None
Is a pool
Description AI3 PAU Backbone v6
Utilization 1 IP addresses (0%)
Parent Prefixes
None


NetBox - 2403:8000:23::/64
Affan
netbox.salamahsystems.com/ipam/prefixes/9/ip-addresses/
netbox
Organization
Racks
Devices
Connections
IP Space
VLANs
Circuits
Secrets
affan
Prefixes / 2403:8000:23::/64
Search prefixes
+ Add an IP Address
Edit this prefix
Delete this prefix
2403:8000:23::/64
Created July 26, 2017 · Updated 8 hours, 42 minutes ago
Prefix
IP Addresses
IP Addresses
IP Address
Status
VRF
Tenant
NAT (Inside)
Device
Description
1 IP available
Available
Global
—
—
—
—
2403:8000:23::1/64
Active
Global
ITB
—
—
ns1.itb.ac.id
Many IPs available
Available
Global
—
—
—
—
Edit Selected
Delete Selected
Showing 1-3 of 3
ubuntults-gns3 (v2.0.10)
2017-07-26 14:25:14 UTC
Docs · API · Code · Help

RESULTS THAT'S GOOD FOR YOUR SANITY AND HEALTH

- You have single knowledge of physical & logical resources of your network
- You know how your network looks like
- You know when the config changes, something is about to happen (or not)
- And that's good for your sanity and health
  - You can enjoy weekend
  - Your family loves you (for not working in the weekend)
  - Your employer also loves you for performing better in weekdays

AND THAT'S IT!

Any Questions?