Network Monitoring and Management

Where and How to get IP Addresses

Quick recap and some terminologies

(from wikipedia)

NAT – Network Address Translation

- process of modifying IP address information in IP packet headers while in transit across a traffic routing device

IP Address– Internet Protocol Address

- numerical label assigned to each device (e.g., computer, printer) participating in a computer network

ASN – Autonomous System Number

- an identifier (number) for a collection of IP networks and routers under the control of one entity

RIR – Regional Internet Registry

- is an organization that manages the allocation and registration of Internet number resources within a particular region of the world

LIR – Local Internet Registry

- is an organization that has been allocated a block of IP addresses by a regional Internet registry (RIR), and that assigns most parts of this block to its own customers

Why get IPs in the first place?

- Independence and mobility – you are free to choose your own upstreams and can change when and if necessary
- Identity – you can manage your own IPs and everyone will know that they are yours (with WHOIS). Can get an ASN as well and be identified as an NREN
- Redundancy and uptime – with your own IPs, its easier to get and control multiple upstreams (multi-homing), you can have redundancy between two links and hence improved uptime

What about NAT?

- Many types of NAT – one to one, one to many, port address translation, etc
- Mostly used when public IPs are at a minimum but IPv6 is now available
- NAT also:
  - Breaks some protocols (FTP, SIP)
  - Could get tricky to scale up
  - No end to end connectivity
  - Complicates configs - port forwarding, bi-nat, FTP passive and active

IP and DNS?

Yes they go together!

- A record – Address record
- AAAA – Quad A record (IPv6)
- PTR – aka reverse record
- MX – Mail Exchanger
- CNAME – Canonical Name aka alias record
- NS – Name Server record
- TXT – for Sender Policy Framework (SPF record)
- Many others (SOA, SRV, TKEY, TSIG, etc)

- When you get IPs, you should understand the main DNS records

NREN assigned or Individually/per University acquired IPs?

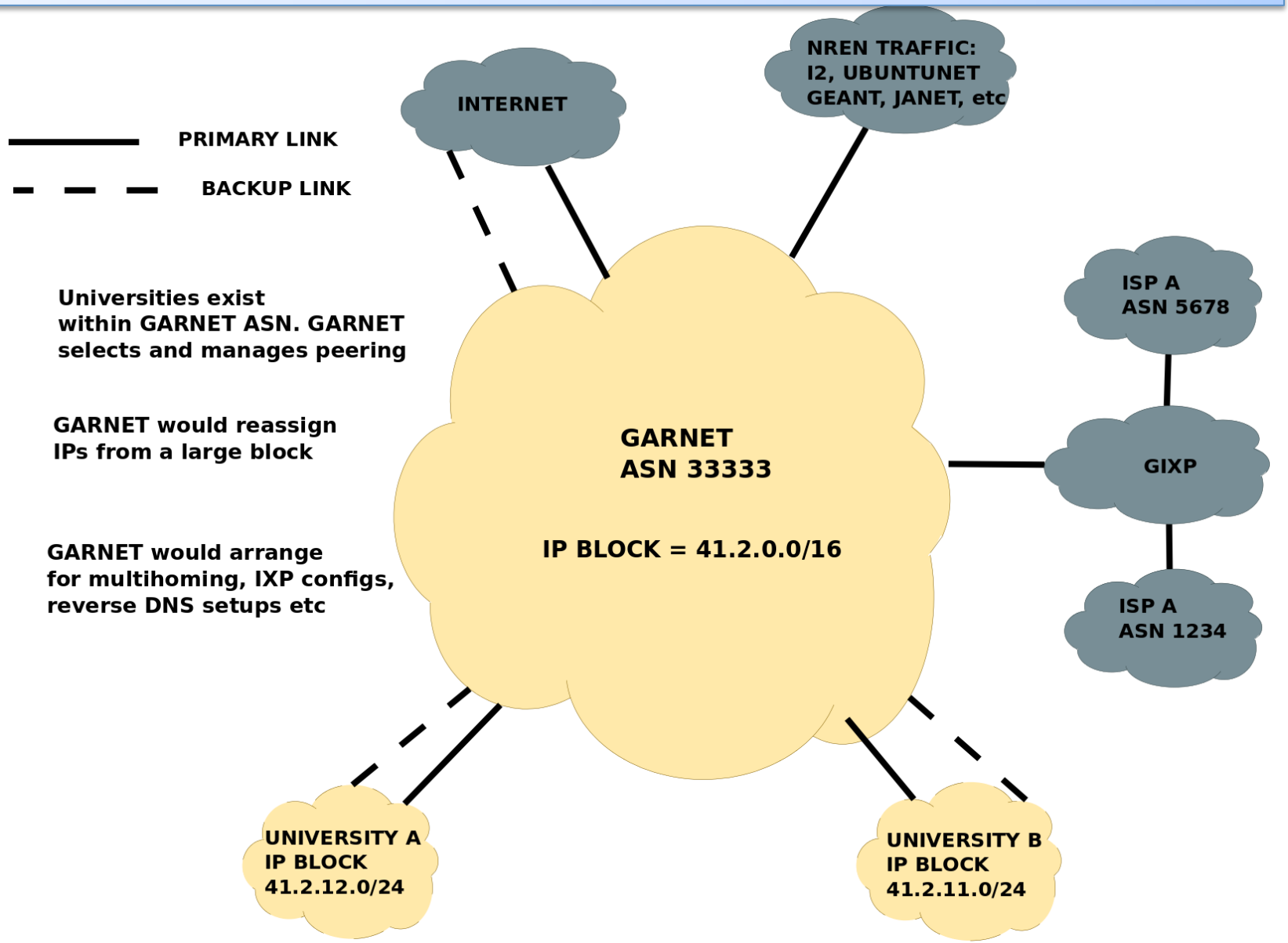
Both models will work :)

NREN assigned

If NREN gets the IPs and allocates them to the Universities it will make routing easier for all

- NREN would select & manage upstreams, multi-homing
- NREN would be a one stop shop
- Focus would be on in-country links – two redundant paths to the Universities from NREN pops
- NREN would manage peerings and exchange point configs
- NREN would be the BGP experts
- NREN would be the IP + DNS experts
- Universities would be ‘tied in’ to the NREN

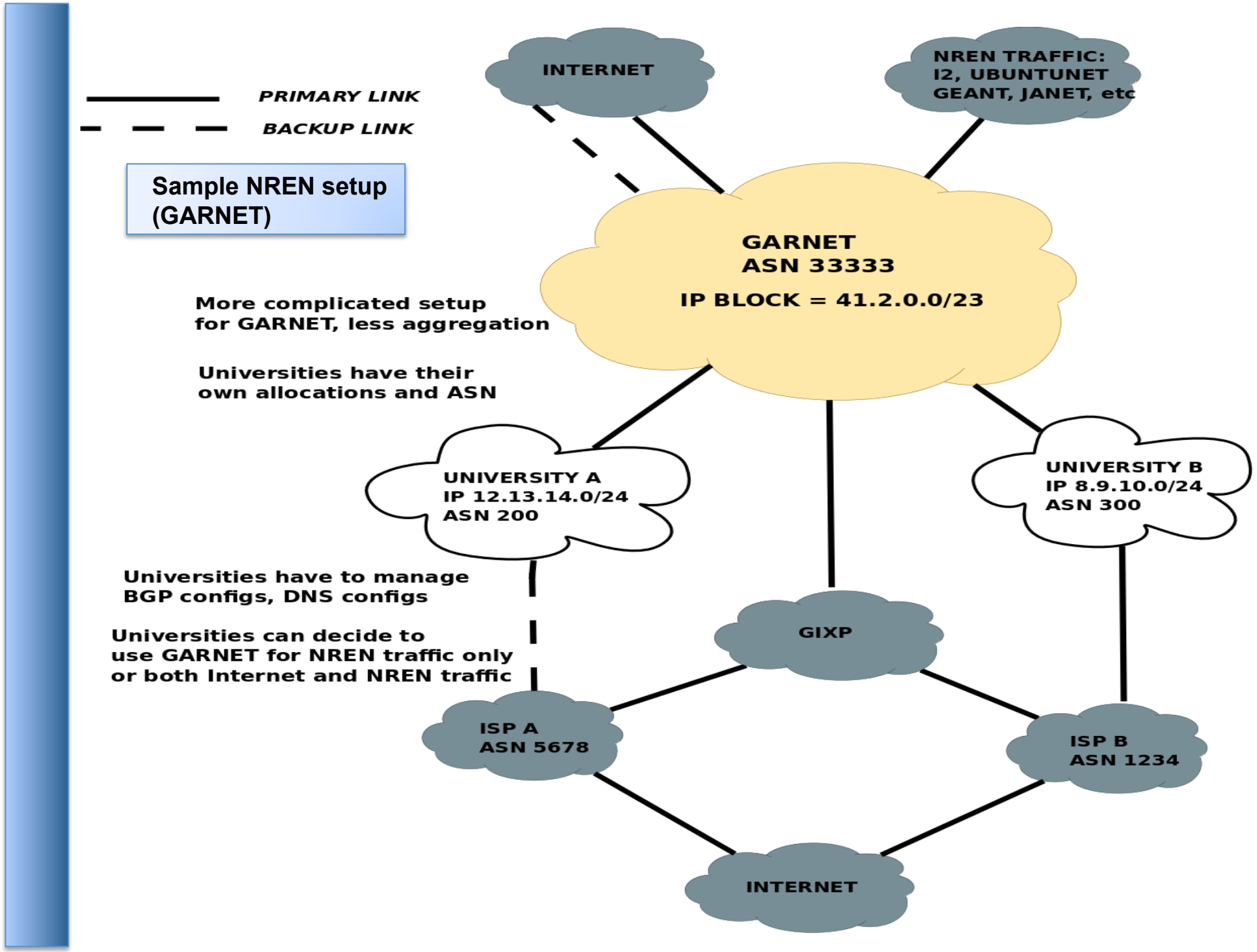
Sample NREN setup (GARNET)



Individually/per University acquired IPs?

If Individually acquired, each University would acquire its own IP block and maybe separate ASNs

- Universities would be able to connect to another upstream as redundancy to NREN if necessary
- Configs slightly more complicated
- Each University would have to register and manage their own IPs, would have to understand BGP fully
- Each University would have to understand DNS properly
- More work for NREN in terms of configs


PRIMARY LINK
BACKUP LINK
Sample NREN setup (GARNET)
INTERNET
NREN TRAFFIC: I2, UBUNTUNET GEANT, JANET, etc
GARNET
ASN 33333
IP BLOCK = 41.2.0.0/23
More complicated setup for GARNET, less aggregation
Universities have their own allocations and ASN
UNIVERSITY A
IP 12.13.14.0/24
ASN 200
UNIVERSITY B
IP 8.9.10.0/24
ASN 300
Universities have to manage BGP configs, DNS configs
Universities can decide to use GARNET for NREN traffic only or both Internet and NREN traffic
GIXP
ISP A
ASN 5678
ISP B
ASN 1234
INTERNET

How many IPs should I get?

- Depends on your infrastructure, your needs and policy
  - Public IP for every University desktop PC? Good, easy to trace defective/compromised machines
  - How many public machines do you have and how fast is your network growing?
- A /24 allocation means 254 use-able public IPs
- For NREN, a large allocation at least a /16 to distribute to the members
- Some upstreams only do BGP with you if you have a minimum /24 BGP advertisement
- IPv6 - NREN as a LIR could get a /32 = 2^96 (many IPs!)
  - Universities could get /48 = 2^80 (still very many)

Where do I get IPs from?

- Africa's RIR is Afrinic (http://afrinic.net). Its mission
  - *"To serve the African community by providing professional and efficient management of Internet Number Resources, supporting Internet technology usage and development, and promoting a participative and multi-stakeholder approach to Internet self governance."* (http://afrinic.net/about.htm)
- Head offices are in Mauritius
- Everything is on-line based
  - Membership registration
  - IP Address management – Reverse records, allocation requests
  - Many other functions – billing, voting etc

How do I get the IPs?

- You first must be an Afrinic member and sign up. You can choose from two types of members:
  - LIR – Local Internet Registry ie ISP (NREN in this case) can re-assign IPs to others
  - End User – the Universities (not re-assigning IPs to another entity)
- http://my.afrinic.net/registration
- Members benefit by:
  - Can get IPs and ASNs
  - Can get training on IPv4, whois, IPv6 and DNSSEC
- Once registered, you will be creating objects in the database which reflect various types of information:
  - Domain – forward or reverse DNS
  - Role – administrative or technical
  - Many others (auto-num, as-set etc)

Registration at Afrinic

- You will need a “nic-handle” which is a unique identifier. Also known as a person object or “nic-hnl”
- Used to identify the contact person responsible for a specific object
- Can be created by sending an email to auto-dbm@afrinic.net in the following format:

person:	*[mandatory] [single] [lookup key]*
address:	*[mandatory] [multiple] [ ]*
phone:	*[mandatory] [multiple] [ ]*
fax-no:	*[optional] [multiple] [ ]*
e-mail:	*[mandatory] [multiple] [lookup key]*
nic-hdl:	*[mandatory] [single] [primary/lookup key]*
remarks:	*[optional] [multiple] [ ]*
notify:	*[optional] [multiple] [inverse key]*
mnt-by:	*[optional] [multiple] [inverse key]*
changed:	*[mandatory] [multiple] [ ]*
source:	*[mandatory] [single] [ ]*

WHOIS

- is a query and response protocol
- widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information.
- The protocol stores and delivers database content in a human-readable format.[1] The WHOIS protocol is documented in RFC 3912. (WikiPedia)
- Most registries have *whois* servers. Afrinic: *http://whois.afrinic.net*

Sample Nic Handle

```
$ whois  -h whois.afrinic.net kc1-afrinic
```

% This is the AfriNIC Whois server.

% Note: this output has been filtered.

% Information related to 'KC1-AFRINIC'

person:	Kevin Chege
address:	P.O. Box 30244 00100, Nairobi, Kenya
phone:	+254206750435
e-mail:	noc@kenet.or.ke
nic-hdl:	KC1-AFRINIC
remarks:	Kenya Education Network
source:	AFRINIC # Filtered

Sample inetnum object

```
$ whois -h whois.afrinic.net 41.204.160.22
```

% This is the AfriNIC Whois server.
% Note: this output has been filtered.
% Information related to '41.204.160.0 - 41.204.160.255'

inetnum:	41.204.160.0 - 41.204.160.255
netname:	KENET-NBI-POP
descr:	KENET-NBI-POP
country:	KE
admin-c:	KC1-AFRINIC
tech-c:	KNT1-AFRINIC
status:	ASSIGNED PA
mnt-by:	KENET
source:	AFRINIC # Filtered
parent:	41.204.160.0 - 41.204.163.255

Sample domain object

```
$ whois -h whois.afrinic.net 164.204.41.in-addr.arpa
```

% This is the AfriNIC Whois server.
% Note: this output has been filtered.
% Information related to '164.204.41.in-addr.arpa'

domain: 164.204.41.in-addr.arpa
descr: Kenya Education Network
admin-c: KC1-AFRINIC
zone-c: KC1-AFRINIC
tech-c: KC1-AFRINIC
nserver: ns1.kenet.or.ke
nserver: ns2.kenet.or.ke
nserver: ns3.kenet.or.ke
source: AFRINIC # Filtered
mnt-by: kenet-mnt

Route Registries

- A centralized database that contains routing information, e.g., prefixes, AS_PATH's, ASN's, e.t.c
- RIPE and RADB operate route registries. AFRINIC does not operate a route registry - *http://www.afrinic.net/fr/library/membership-documents/215-creating-route-object-*
- ISPs publish their routing policies using RPSL - Routing Policy Specification Language. In particular, route objects
- When dealing with your upstreams as an NREN you will need to create route objects at RIPE/RADb
- Route objects allow others (in particular your upstreams) to automatically configure their routers based on the information you publish at the Registry, eg your ASN and the IP blocks you are advertising

Route Registries cont'd

- This improves efficiency for your upstream and you (the NREN) because you can edit the registry and not have to seek your upstream to make changes to his router for IP Prefix advertisement to be effected in the future
- In a way, your upstream is allowing you to indirectly configure his router. Upstreams configure their filters automatically based on the info you publish
- You will be entering route information for your prefixes similar to below:
  - *route: 192.168.1.0/22*
    descr: NREN Block
    objectorigin: AS1234
    country: TZ
    notify: xyz@example.
    netmnt-routes: MAINTROUTE-TZ-EXAMPLE
    mnt-by: MAINT-TZ-EXAMPLE
    changed: changed@ripe.net 20121011
    source: RIPE
    password: xxxxxx

References and where to get more info

- http://www.afrinic.net/faq.htm
- http://www.afrinic.net/about.htm
- http://www.afrinic.net/docs/db/afsup-obj200502.htm
- http://ripe.net
- http://www.afrinic.net/rs/eligibility.htm
- http://www.radb.net/tutorials/how1.php
- http://www.apnic.net/apnic-info/whois_search/using-whois/guide/creating-route-objects
- Google and WikiPedia are your friends!

Questions

?