Internet Resource Management

IRINN OPM 2

20 November 2014

APNIC

Srinivas Chendi
Abhishek Mishra
Ruby Rani
Chandra Prakash

APNIC

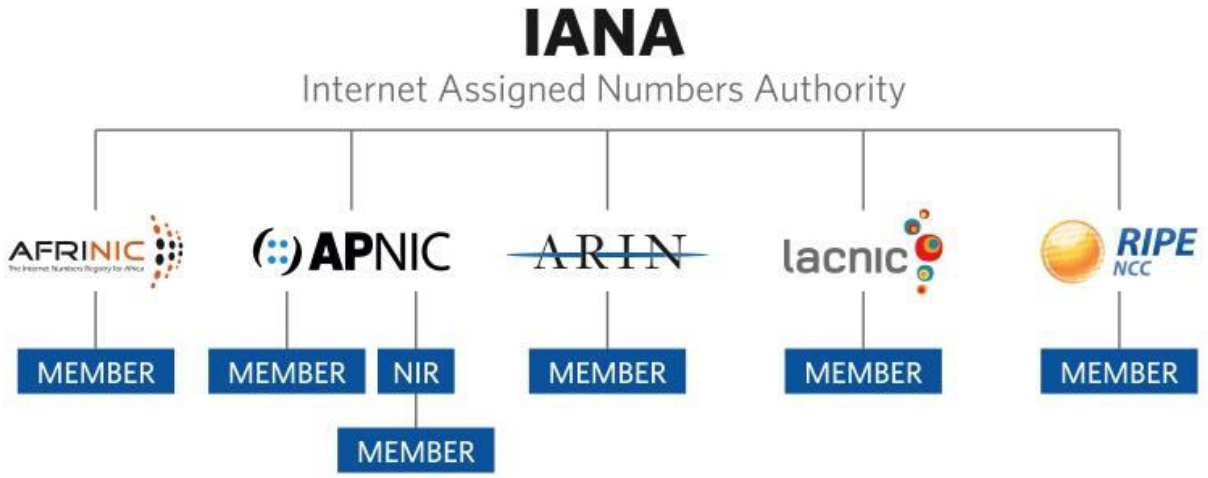
Agenda

- Internet Registry Structure
- Policy Development Process
- Internet Registry Policies
- Resource Registration (Whois)
- Autonomous System Numbers
- Reverse DNS

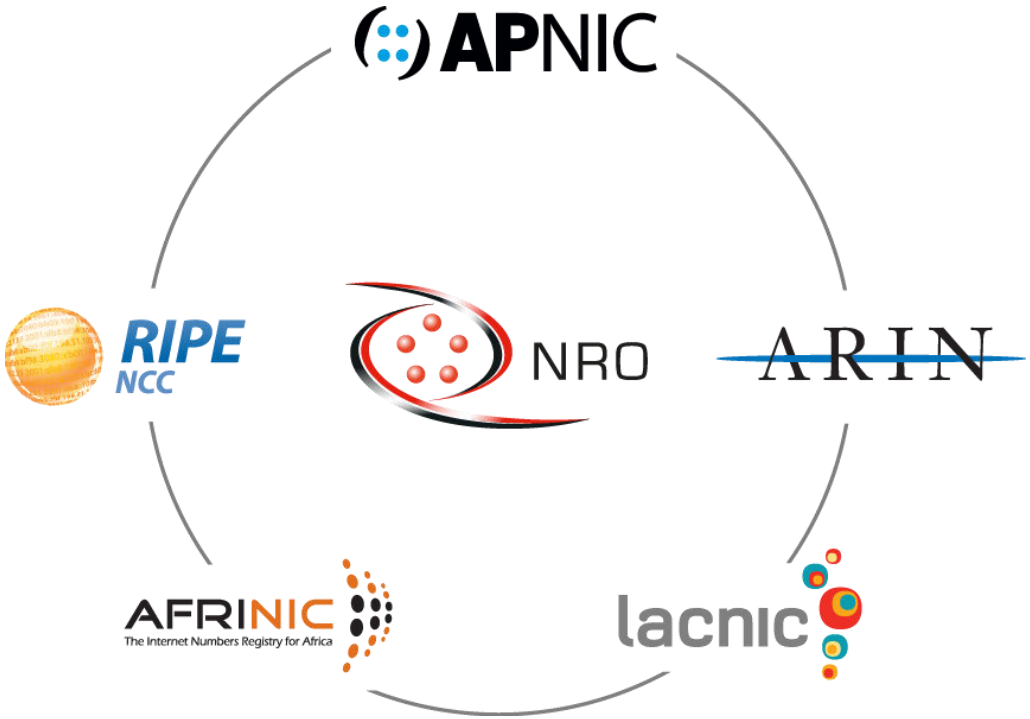
Agenda

- **Internet Registry Structure**
- **Policy Development Process**
- Internet Registry Policies
- Resource Registration (Whois)
- Autonomous System Numbers
- Reverse DNS

Internet Registry Structure



Global Policy Coordination

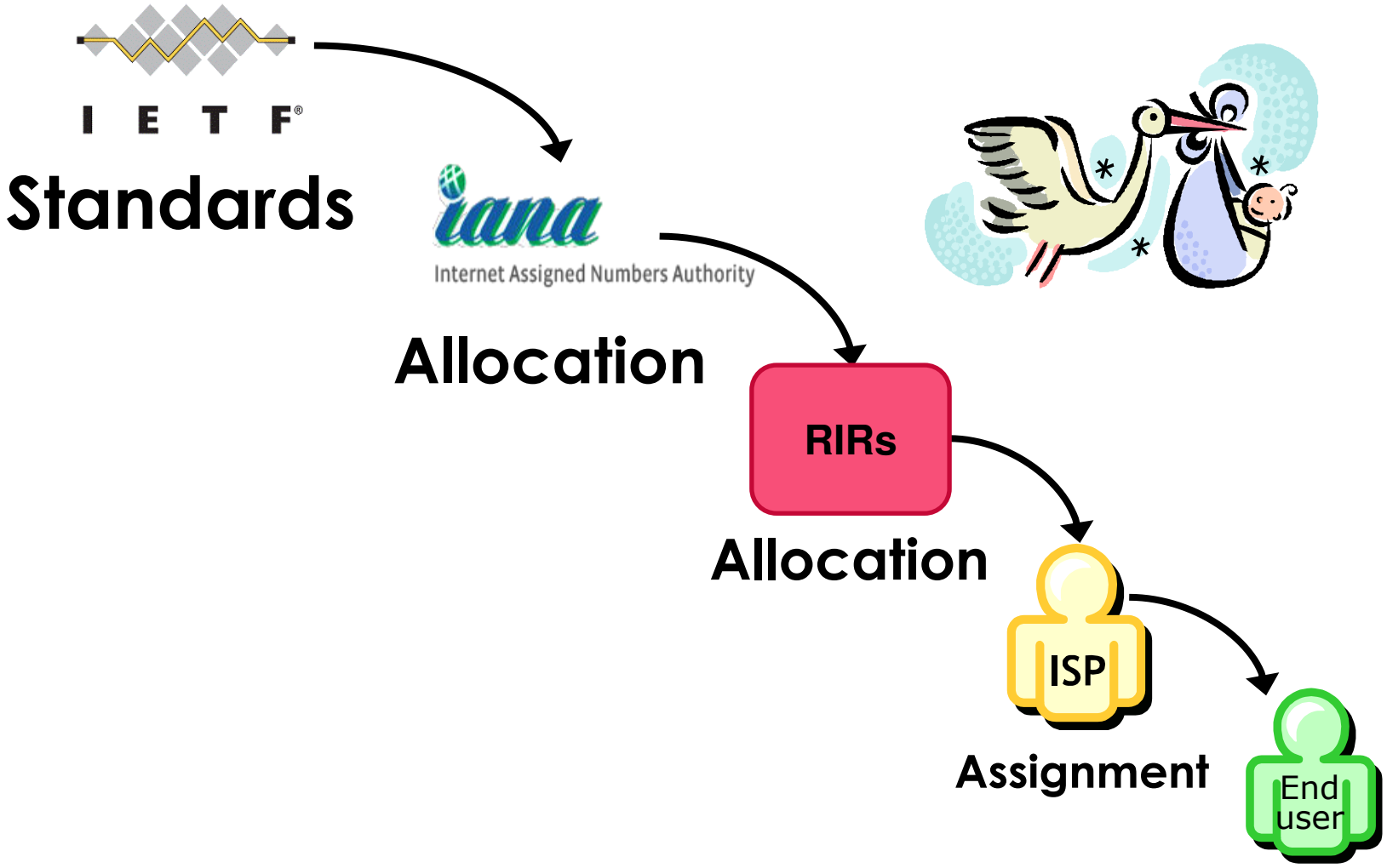


- The main aims of the NRO are to:
  - Protect the unallocated Internet number resource pool
  - Promote and protect the bottom-up policy development process
  - Act as a focal point for Internet community input into the RIR system

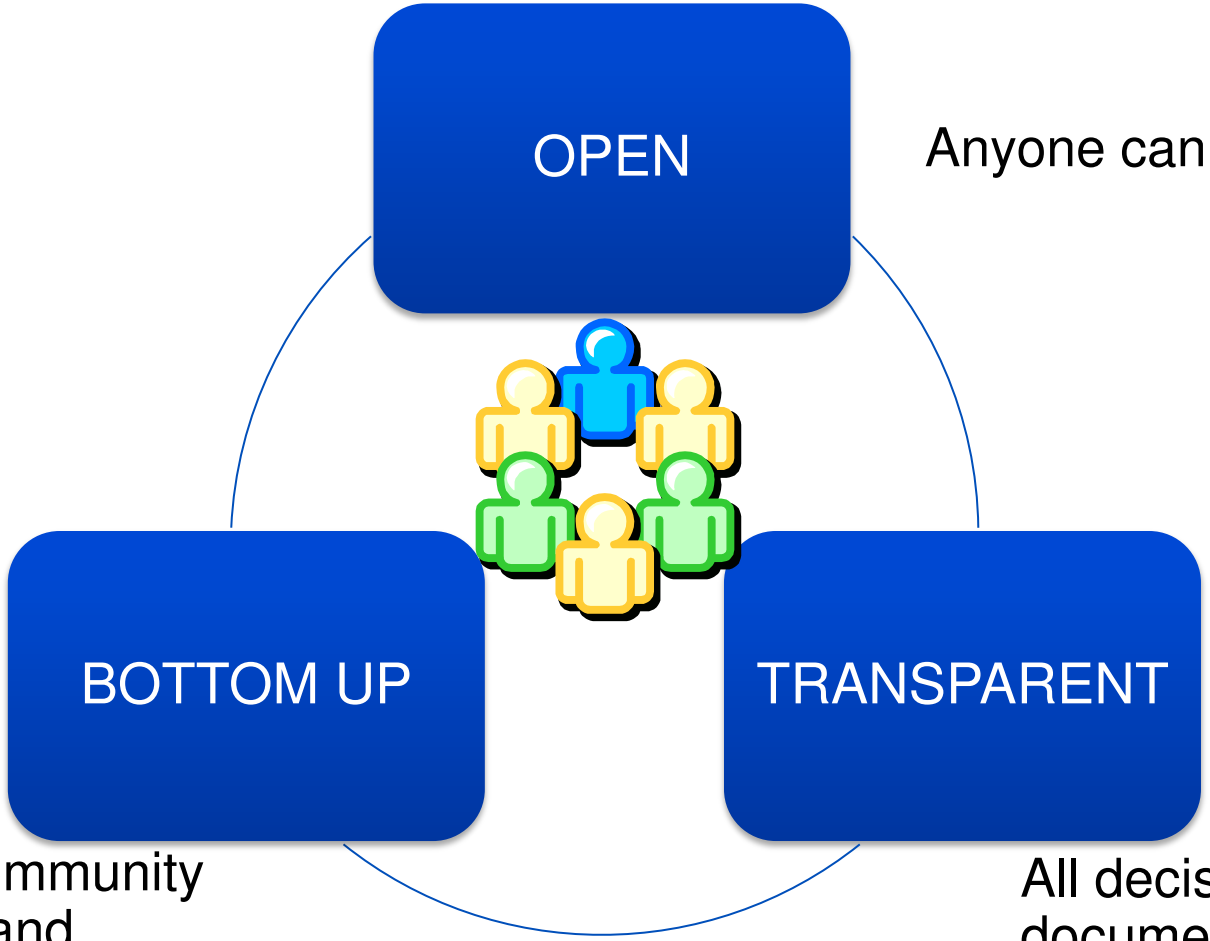
Global Policy Coordination

- The main function of ASO:
  - receives global policies and policy process details from the NRO
  - forwards global policies and policy process details to ICANN board

Where do IP Addresses come from?



Policy Development Process

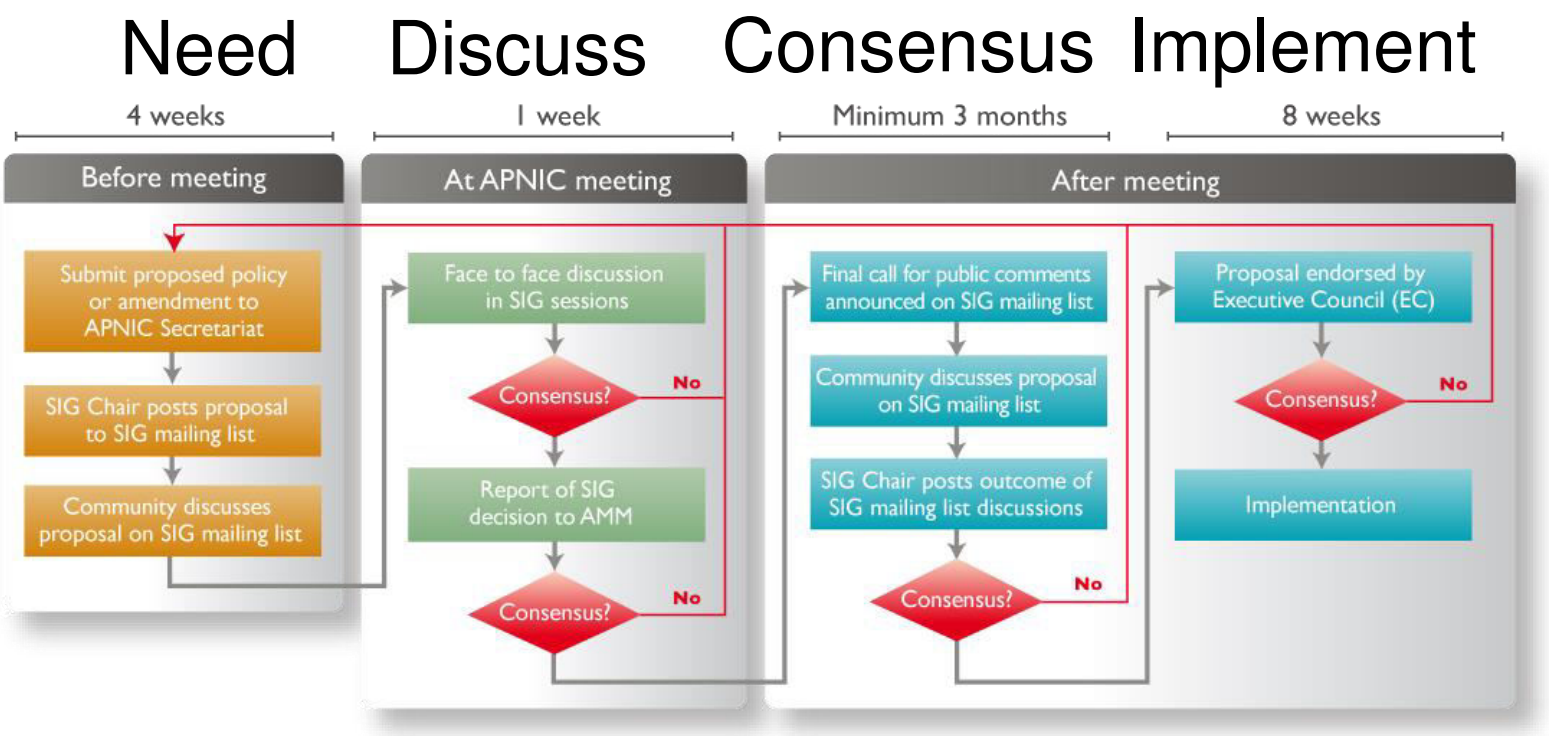


Anyone can participate

Internet community proposes and approves policy

All decisions & policies documented & freely available to anyone

Policy Development Process



You can participate!

More information about policy development can be found at:

http://www.apnic.net/policy

How to Make Your Voice Heard

- Contribute on the public mailing lists
  - http://www.apnic.net/mailing-lists
  - Attend APNIC conferences
  - Or send a representative
  - Watch the webcast (video streaming) from the conference web site
  - Read live transcripts from APNIC web site
  - And express your opinion via the Jabber chat
- Provide your feedback
  - Training or community outreach events

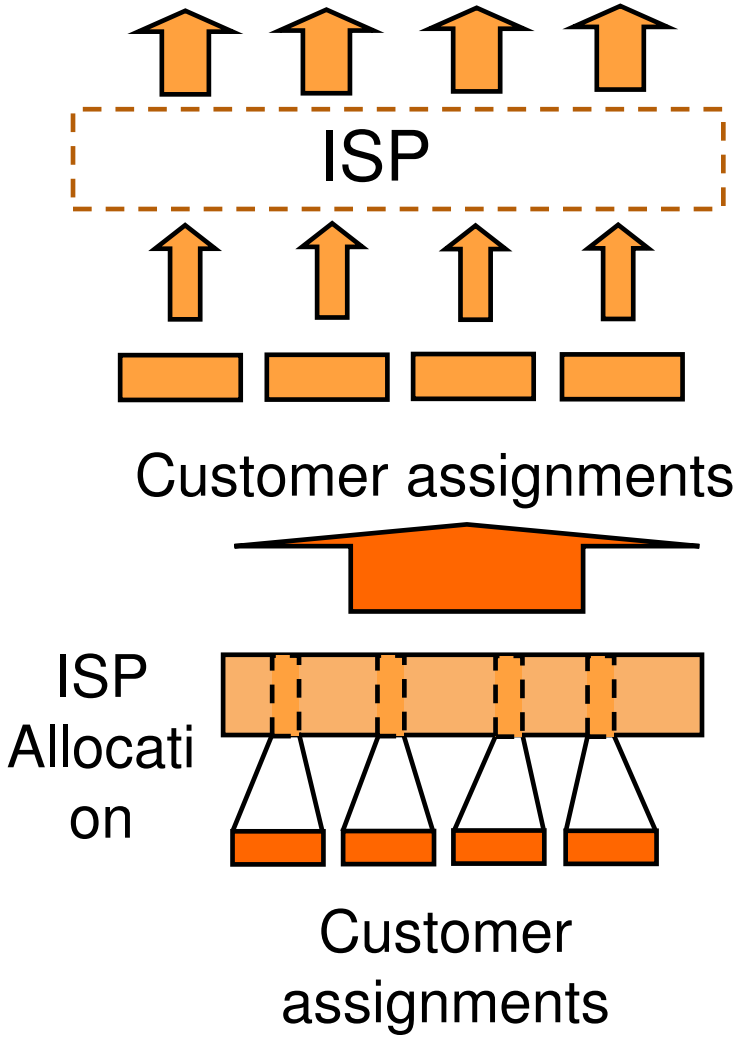
Questions

Agenda

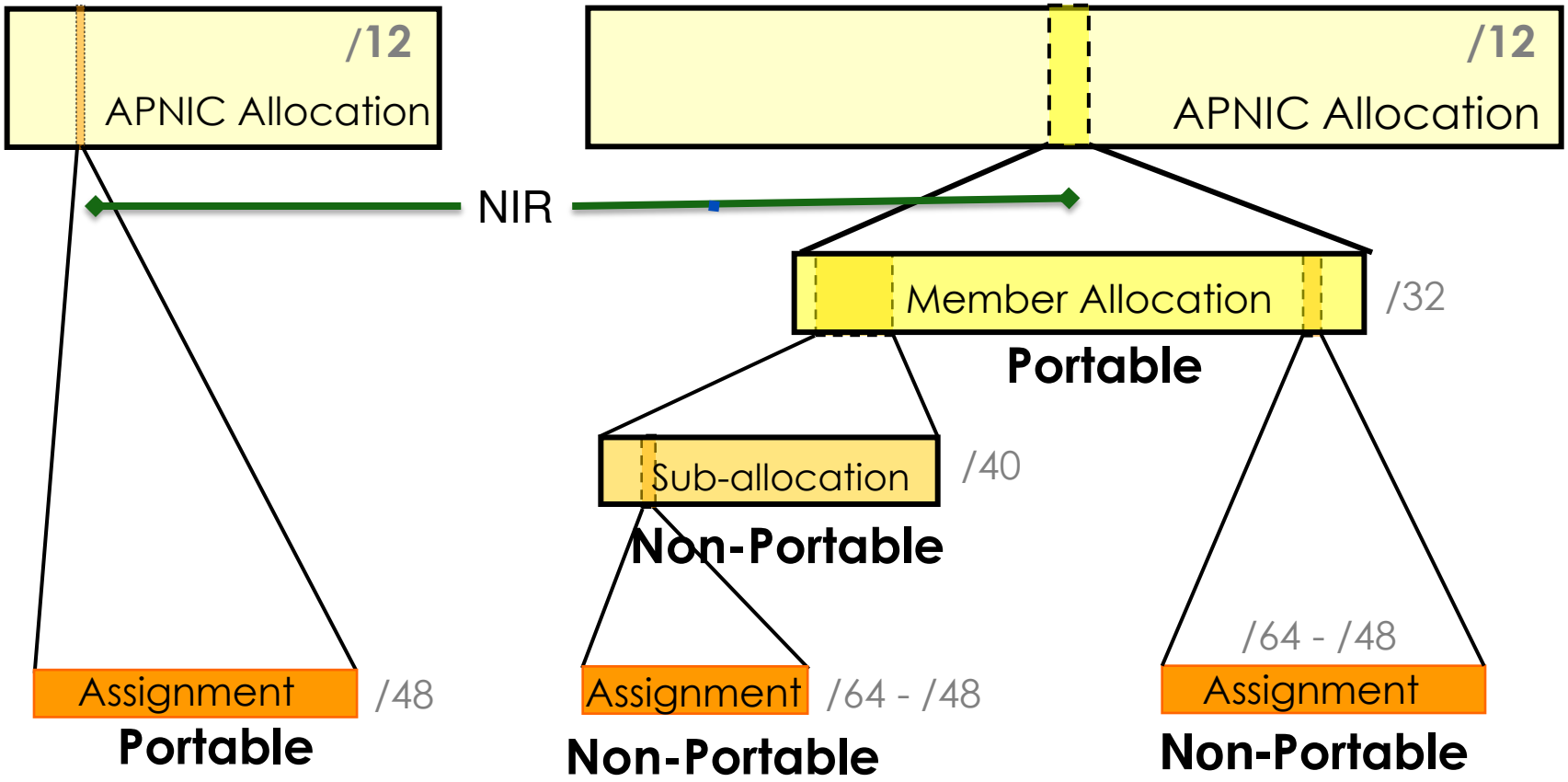
- Internet Registry Structure
- Policy Development Process
- **Internet Registry Policies**
- Resource Registration (Whois)
- Autonomous System Numbers
- Reverse DNS

Portable and Non-Portable

- Portable Assignments
  - Customer addresses independent from ISP
  - Keeps addresses when changing ISP
  - Bad for size of routing tables
  - Bad for QoS: routes may be filtered, flap-dampened
- Non-portable Assignments
  - Customer uses ISP's address space
  - Must renumber if changing ISP
  - Only way to effectively scale the Internet
- Portable allocations
  - Allocations made by APNIC/NIRs



Address Management Hierarchy



Describes "portability" of the address space

Internet Resource Management Objectives

Conservation
- Efficient use of resources
- Based on demonstrated need

Aggregation
- Limit routing table growth
- Support provider-based routing

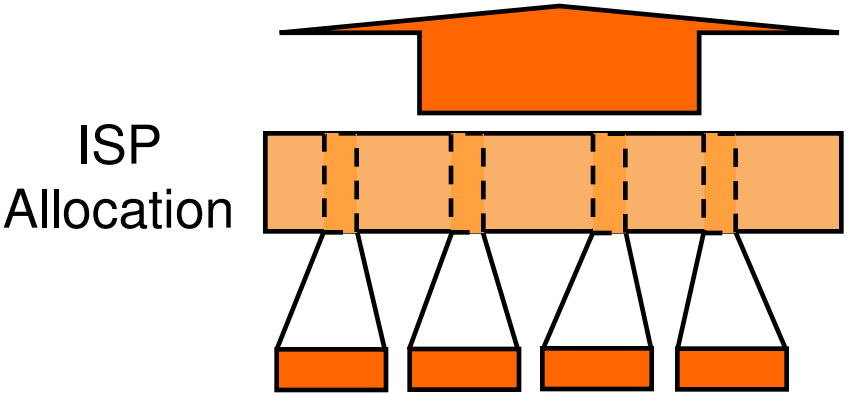
Registration
- Ensure uniqueness
- Facilitate trouble shooting

Uniqueness, fairness and consistency

Aggregation and Portability

Aggregation

BGP Announcement (1)

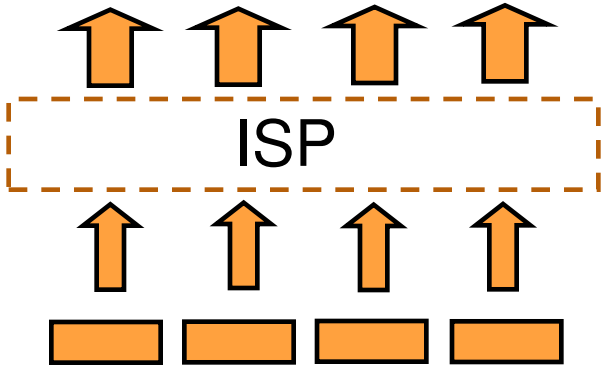


Customer assignments

(non-portable assignments)

No aggregation

BGP Announcements (4)

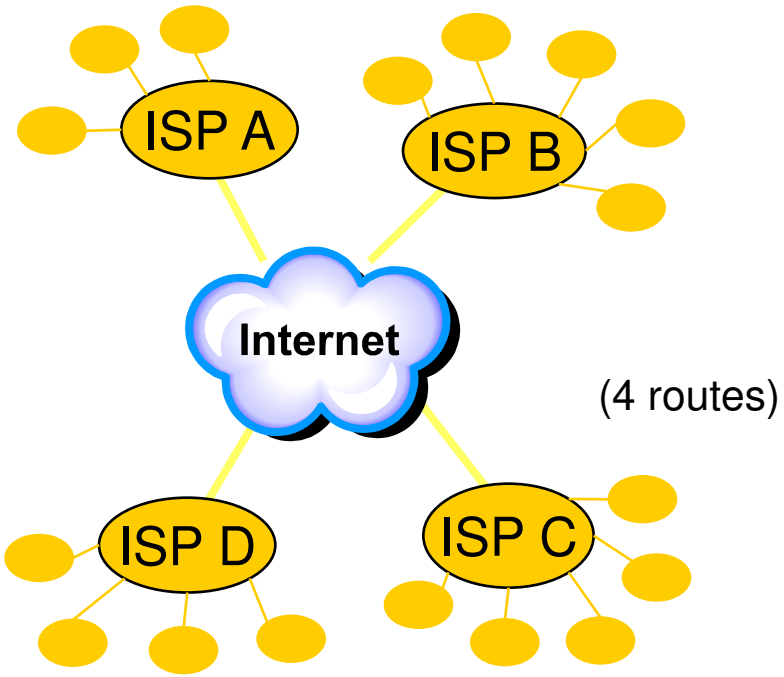


Customer assignments

(portable assignments)

Aggregation and Portability

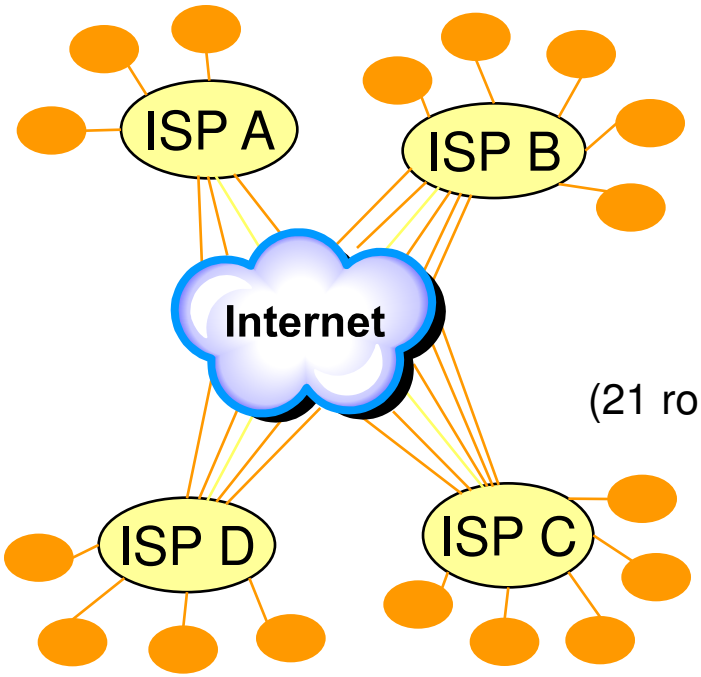
Aggregation



(4 routes)

(non-portable assignments)

No aggregation

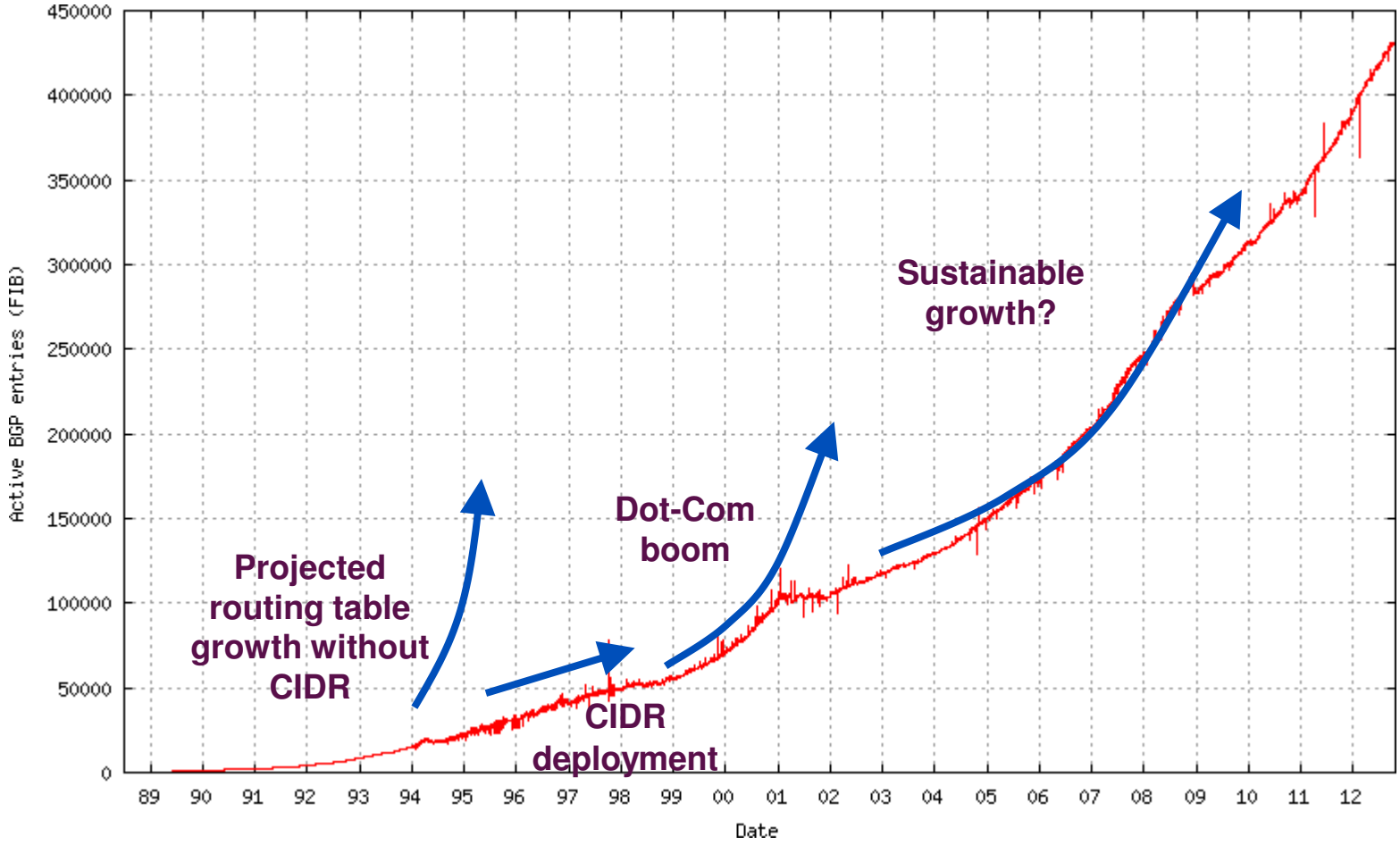


(21 routes)

(portable assignments)

Growth of the Global Routing Table

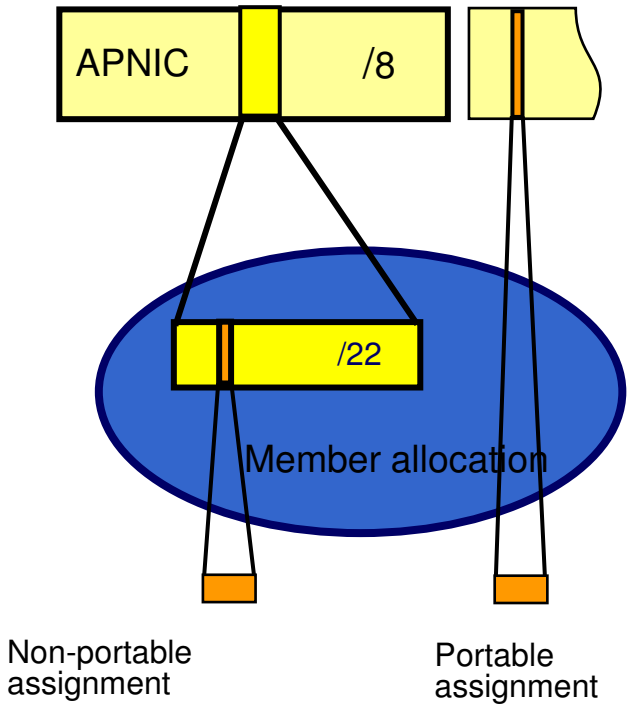
487889 prefixes
As of 27 Dec 2013



Source: http://www.cidr-report.org/as2.0/

IPv4 Allocation Policies

- APNIC IPv4 allocation size per account holder
  - Minimum /24
  - Maximum /22
- According to current allocation from the final /8 block
  - Allocation is based on demonstrated need



IPv6 Allocation Policies

- Initial allocation criteria
  - minimum of /32 IPv6 block
  - larger than /32 may be justified
- Without existing IPv4 space
  - Must meet initial allocation criteria
- Subsequent allocation
  - Based on HD ratio (0.94)
  - Doubles the allocated address space

IPv6 Assignment Policies

- Assignment address space size
  - Minimum of /64 (only 1 subnet)
  - Normal maximum of /48
  - Initial allocation larger than /32 may be justified
- Assignment of multiple /48s to a single end site
  - Documentation must be provided
  - Will be reviewed at the RIR/NIR level
- Assignment to operator's infrastructure
  - /48 per PoP as the service infrastructure of an IPv6 service operator

Questions

Agenda

- Internet Registry Structure
- Policy Development Process
- Internet Registry Policies
- **Resource Registration (Whois)**
- Autonomous System Numbers
- Reverse DNS

Resource Registration

- As part of your membership agreement, all Members are required to register their resources in the whois database
  - Members must keep records up to date
  - Whenever there is a change in contacts
  - When new resources are received
  - When resources are sub-allocated or assigned

What is the Whois Database?

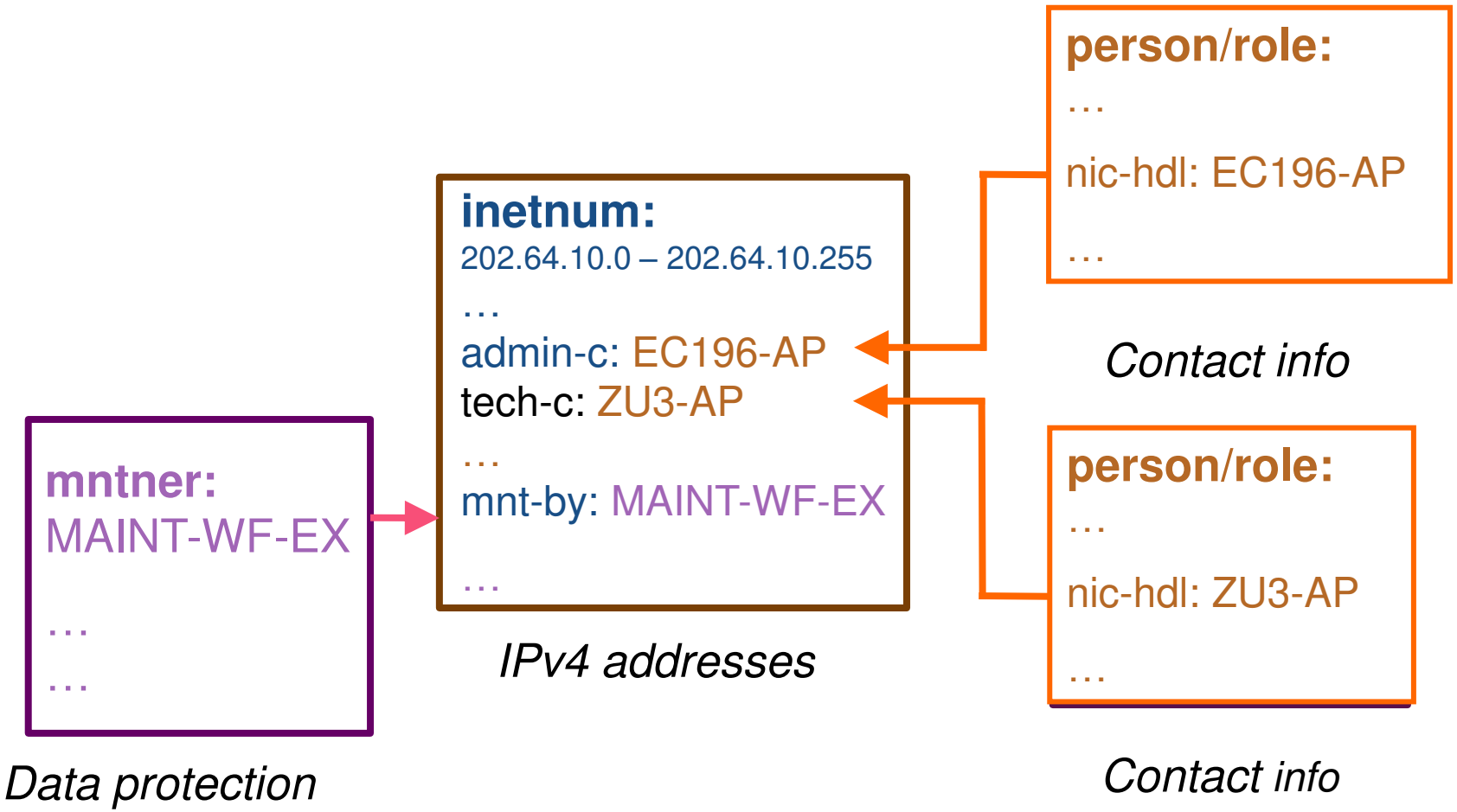
- Public network management database
  - Operated by Internet Registries
- Public data only (For private data, please see “Privacy of customer assignment” module)
  - Tracks network resources
    - IP addresses, ASNs, Reverse Domains, Routing policies
- Records administrative information
  - Contact information (persons/roles)
  - Authorization

Object Types

OBJECT	PURPOSE
person	contact persons
role	contact groups/roles
inetnum	IPv4 addresses
Inet6num	IPv6 addresses
aut-num	Autonomous System number
domain	reverse domains
route	prefixes being announced
mntner	(maintainer) data protection
mnt-irt	Incident Response Team

http://www.apnic.net/db/

Inter-Related Objects



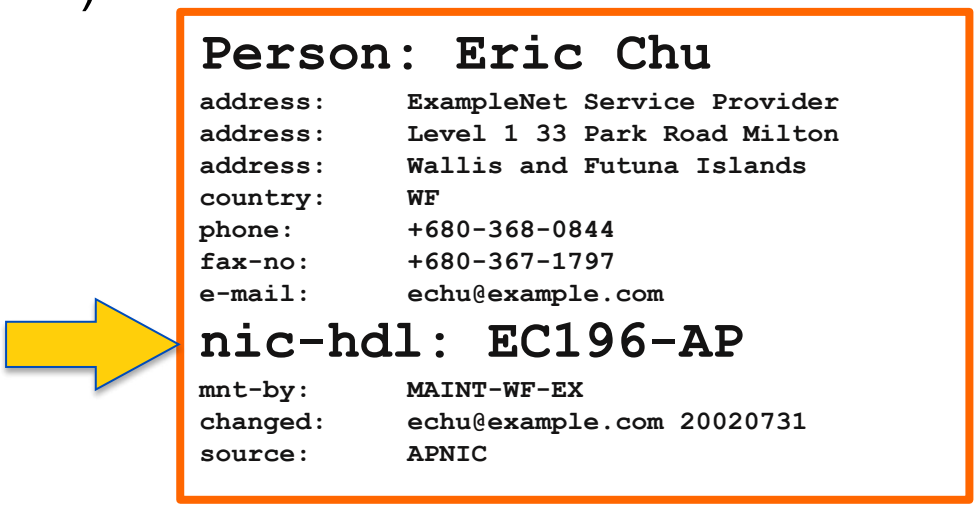
* Please note that the following slides refer back to this one.

Person Object

- Represents a contact person for an organization
  - Every Member must have at least one contact person registered
  - Large organizations often have several contacts for different purposes
- Is referenced in other objects
- Has a nic-hdl
  - Eg. EC17-AP

What is a ‘nic-hdl’?

- Unique identifier for a person or role
- Represents a person or role object
- Referenced in objects for contact details
  - (inetnum, aut-num, domain…)
  - format: <XXXX-AP>
    - Eg: EC196-AP



Role Object

- Represents a group of contact persons for an organization
  - Eases administration
- Also has a nic-hdl
  - Eg. HM20-AP
- used instead of a Person Object as a reference in other objects
  - This means only a single replacement is required instead of many

Replacing Contacts in the DB - Using Person Objects

E. Chu is leaving my organization. A. Nagali is replacing him.

1. Create a Person Object for new contact (***E. Chu***)

2. Find all objects containing old contact (***E. Chu***)

3. Update all objects, replacing old contact (EC196-AP) with new contact (AN3-AP)

4. Delete old contact's (EC196-AP) Person Object

inetnum:
202.0.10.0
...
AN3-AP

inetnum:
202.0.12.127
...
AN3-AP

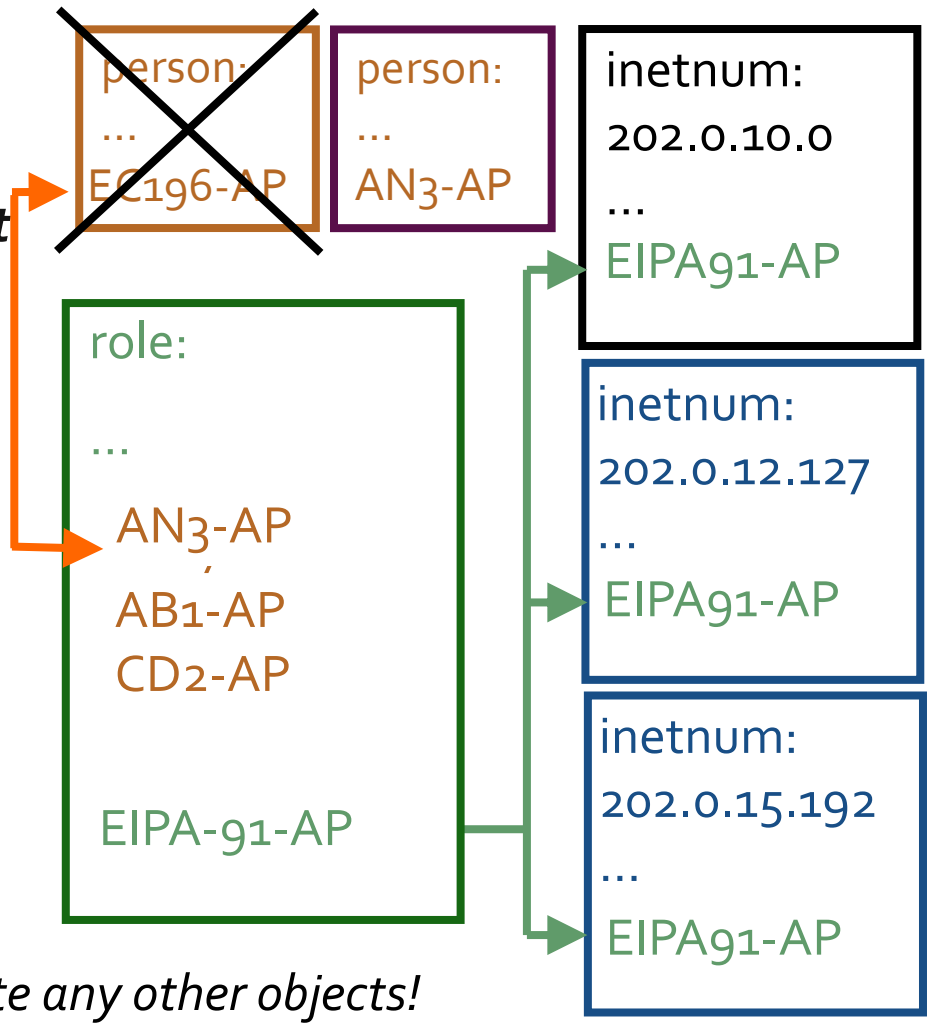
inetnum:
202.0.15.192
...
AN3-AP

Replacing Contacts in the DB – Using a Role Object

E. Chu is leaving my organization.
A. Nagali is replacing him.

My Role Object contains all contact info, that is referenced in all my objects.

1. Create a Person Object for new contact (A. Nagali)
2. Replace old contact (EC196-AP) with new contact (AN3-AP) in Role Object
3. Delete old contact's Person Object.



No need to update any other objects!

What is a Maintainer?

- Protects other objects in the APNIC Whois Database:
- Multiple levels of maintainers exist in a hierarchical manner
- Applied to any object created directly below that maintainer object
- Why do we need Maintainer?
  - to prevent unauthorized persons from changing the details in the Whois DB
  - As parts of a block are sub-allocated or assigned, another layer of maintainers is often created to allow the new users to protect their (sub)set of addresses

Database Protection
Maintainer Object

```
mntner:         MAINT-AU-APNICTRAINING
descr:          APNIC Training
country:        AU
admin-c:        AA196-AP
tech-c:         AA196-AP
auth:           MD5-PW $1$FUrnj.4g$sIyzbkZj2XJoDanL/ndXN0
mnt-by:         MAINT-AU-APNICTRAINING
upd-to:         amante@apnic.net
referral-by:    APNIC-HM
changed:        hm-changed@apnic.net 20080424
changed:        hm-changed@apnic.net 20090325
changed:        hm-changed@apnic.net 20090403
changed:        hm-changed@apnic.net 20090702
changed:        hm-changed@apnic.net 20091111
changed:        hm-changed@apnic.net 20091217
changed:        hm-changed@apnic.net 20100528
source:         APNIC
```

Questions

Agenda

- Internet Registry Structure
- Policy Development Process
- Internet Registry Policies
- Resource Registration (Whois)
- **Autonomous System Numbers**
- Reverse DNS

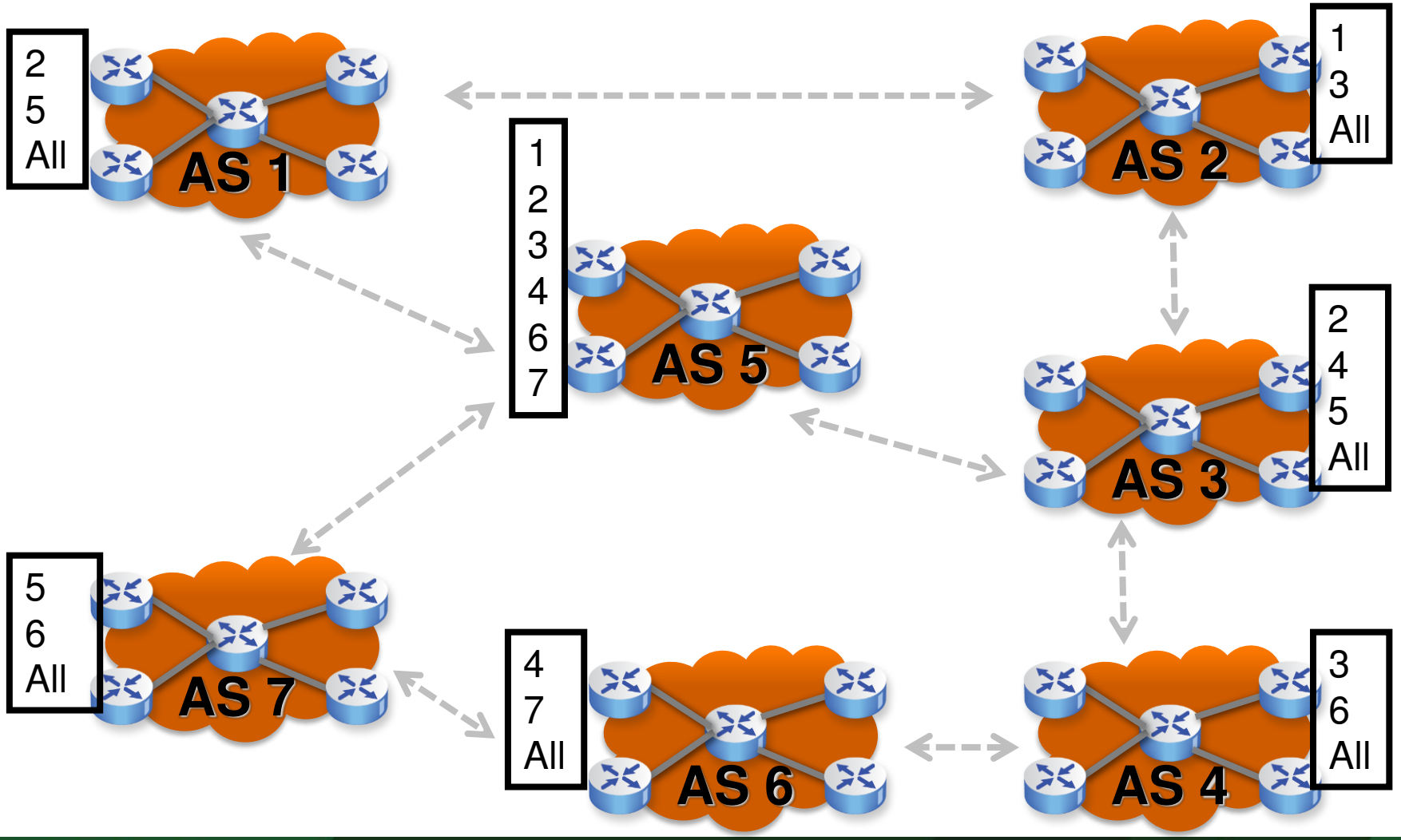
What is an Autonomous System Number?

- Autonomous System Numbers (ASNs) are globally unique identifiers for IP networks
- ASNs are allocated to each Autonomous System (AS) for use in BGP routing
- AS numbers are important because the ASN uniquely identifies each network on the Internet

What Is an Autonomous System?

- Group of Internet Protocol-based networks with the same routing policy
- Usually under single ownership, trust or administrative control
- The AS is used both in the exchange of exterior routing information (between neighboring ASes) and as an identifier of the AS itself

How Do Autonomous Systems Work?



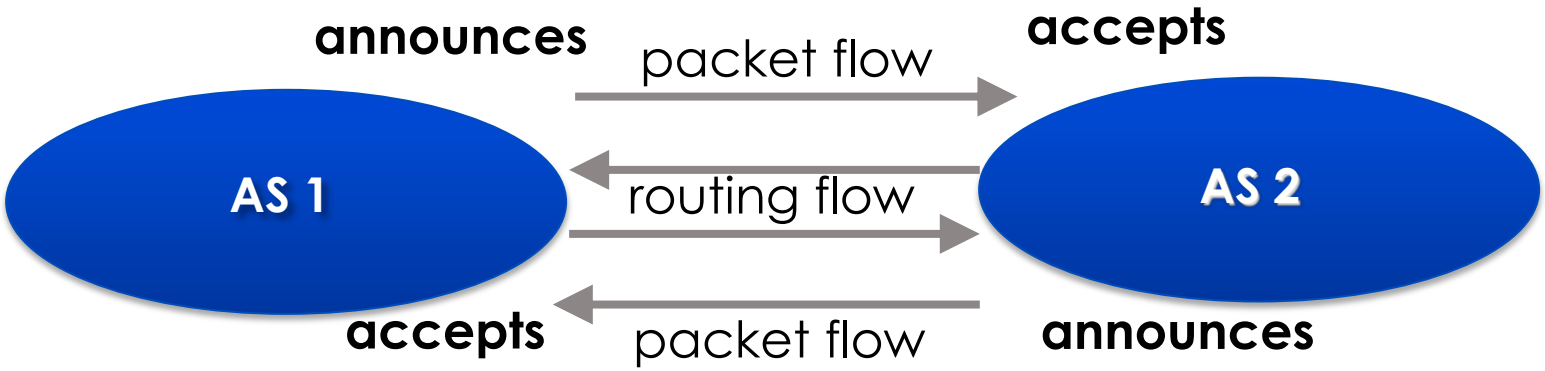
When Do I Need An ASN?

- An ASN is needed if you have a
  - Multi-homed network to different providers AND
  - Routing policy different to external peers

  - * For more information please refer to RFC1930: Guidelines for creation, selection and registration of an Autonomous System

Representation of Routing Policy

- Routing and packet flows

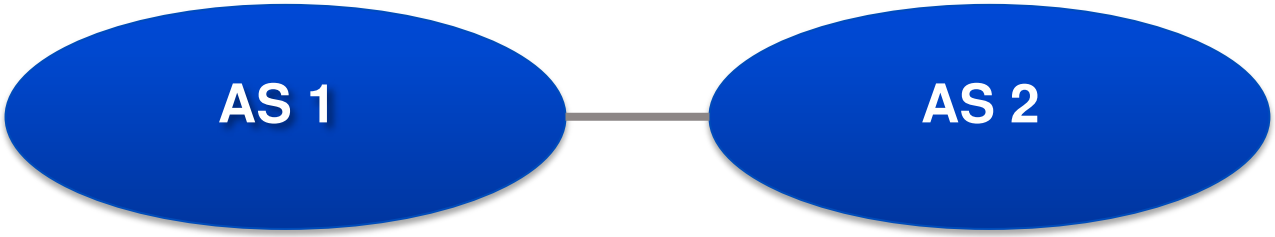


For AS1 and AS2 networks to communicate

- AS1 must announce to AS2
- AS2 must accept from AS1
- AS2 must announce to AS1
- AS1 must accept from AS2

Representation of Routing Policy

Basic concept

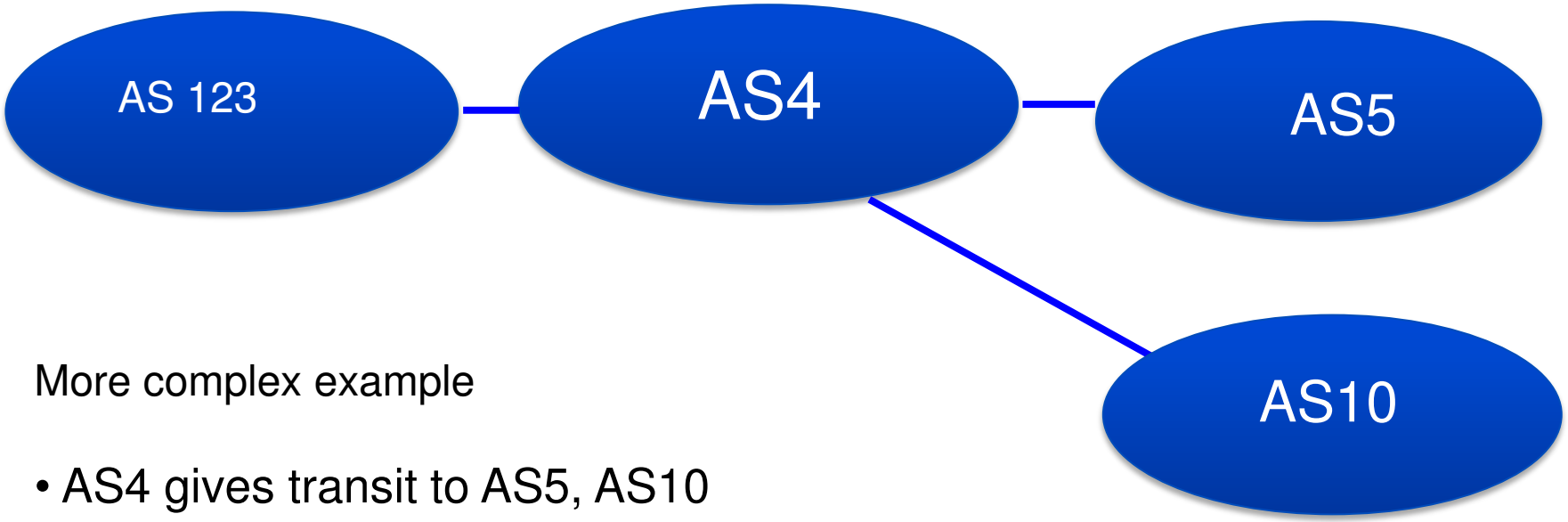


"action pref" - the lower the value,
the more preferred the route

aut-num: AS1
…
import: from AS2
action pref=100;
accept AS2
export: to AS2 announce AS1

aut-num: AS2
…
import: from AS1
action pref=100;
accept AS1
export: to AS1 announce AS2

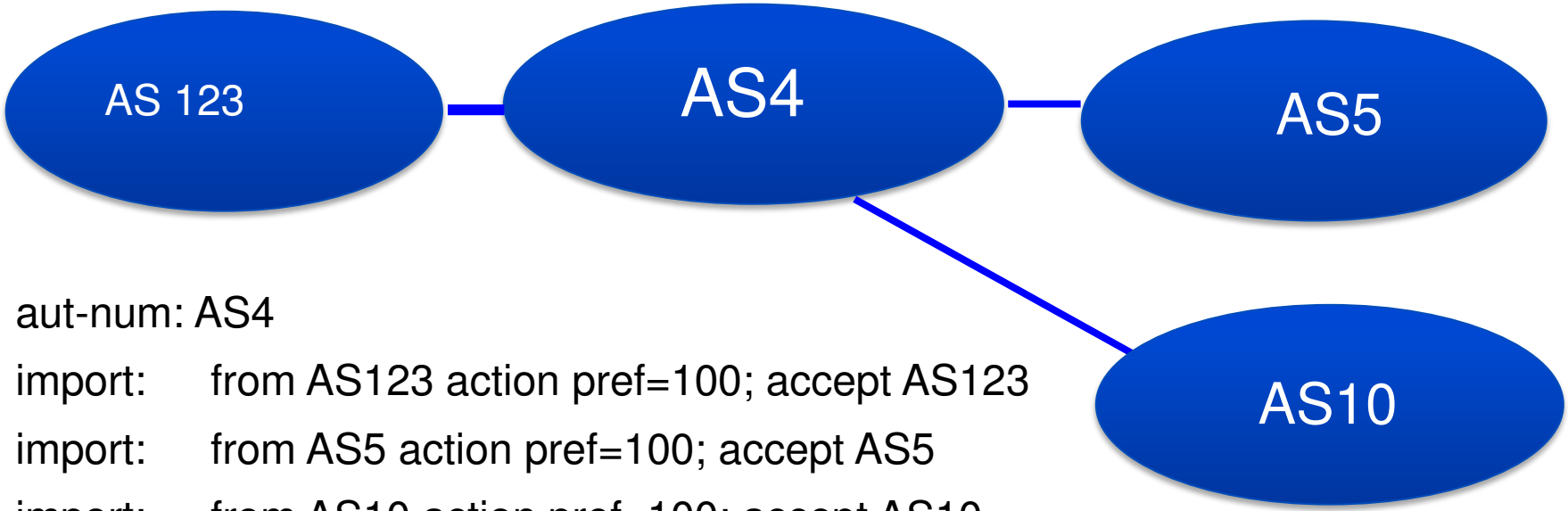
Representation of Routing Policy



More complex example

- AS4 gives transit to AS5, AS10
- AS4 gives local routes to AS123

Representation of Routing Policy



aut-num: AS4
import: from AS123 action pref=100; accept AS123
import: from AS5 action pref=100; accept AS5
import: from AS10 action pref=100; accept AS10
export: to AS123 announce AS4
export: to AS5 announce AS4 AS10
export: to AS10 announce AS4 AS5 ← Not a path

Aut-num Object Example

```
aut-num:    AS4777
as-name:    APNIC-NSPIXP2-AS
Descr:      Asia Pacific Network Information Centre
descr:      AS for NSPIXP2, remote facilities site
import:     from AS2500 action pref=100; accept ANY
import:     from AS2524 action pref=100; accept ANY
import:     from AS2514 action pref=100; accept ANY
export:     to AS2500 announce AS4777
export:     to AS2524 announce AS4777
export:     to AS2514 announce AS4777
default:    to AS2500 action pref=100; networks ANY
admin-c:    PW35-AP
tech-c:     NO4-AP
remarks:    Filtering prefixes longer than /24
mnt-by:     MAINT-APNIC-AP
changed:    paulg@apnic.net 19981028
source:     APNIC
```

POLICY RPSL

Questions

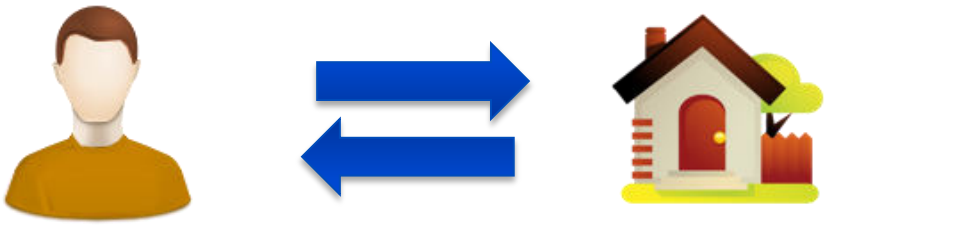
Agenda

- Internet Registry Structure
- Policy Development Process
- Internet Registry Policies
- Resource Registration (Whois)
- Autonomous System Numbers
- **Reverse DNS**

What is ‘Reverse DNS’?

- ‘Forward DNS’ maps names to numbers
  - svc00.apnic.net ➔202.12.28.131

- ‘Reverse DNS’ maps numbers to names
  - 202.12.28.131 ➔ svc00.apnic.net



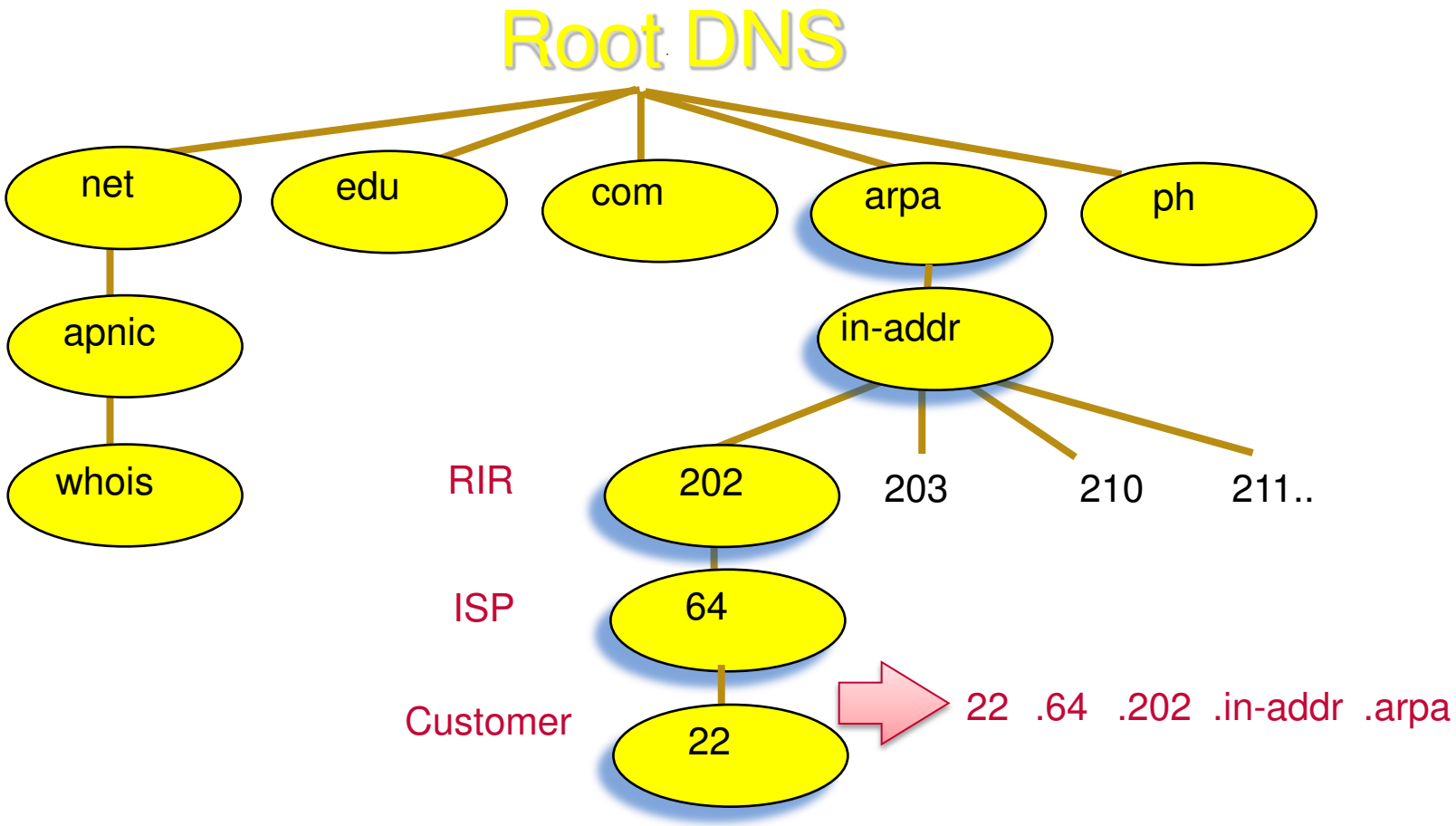
Person (Host) Address (IPv4/IPv6)

Reverse DNS - why bother?

- Service denial
  - That only allow access when fully reverse delegated eg. anonymous ftp
- Diagnostics
  - Assisting in network troubleshooting (ex: traceroute)
- Spam identifications
  - Reverse lookup to confirm the source of the email
  - Failed lookup adds to an email's spam score
- Registration responsibilities

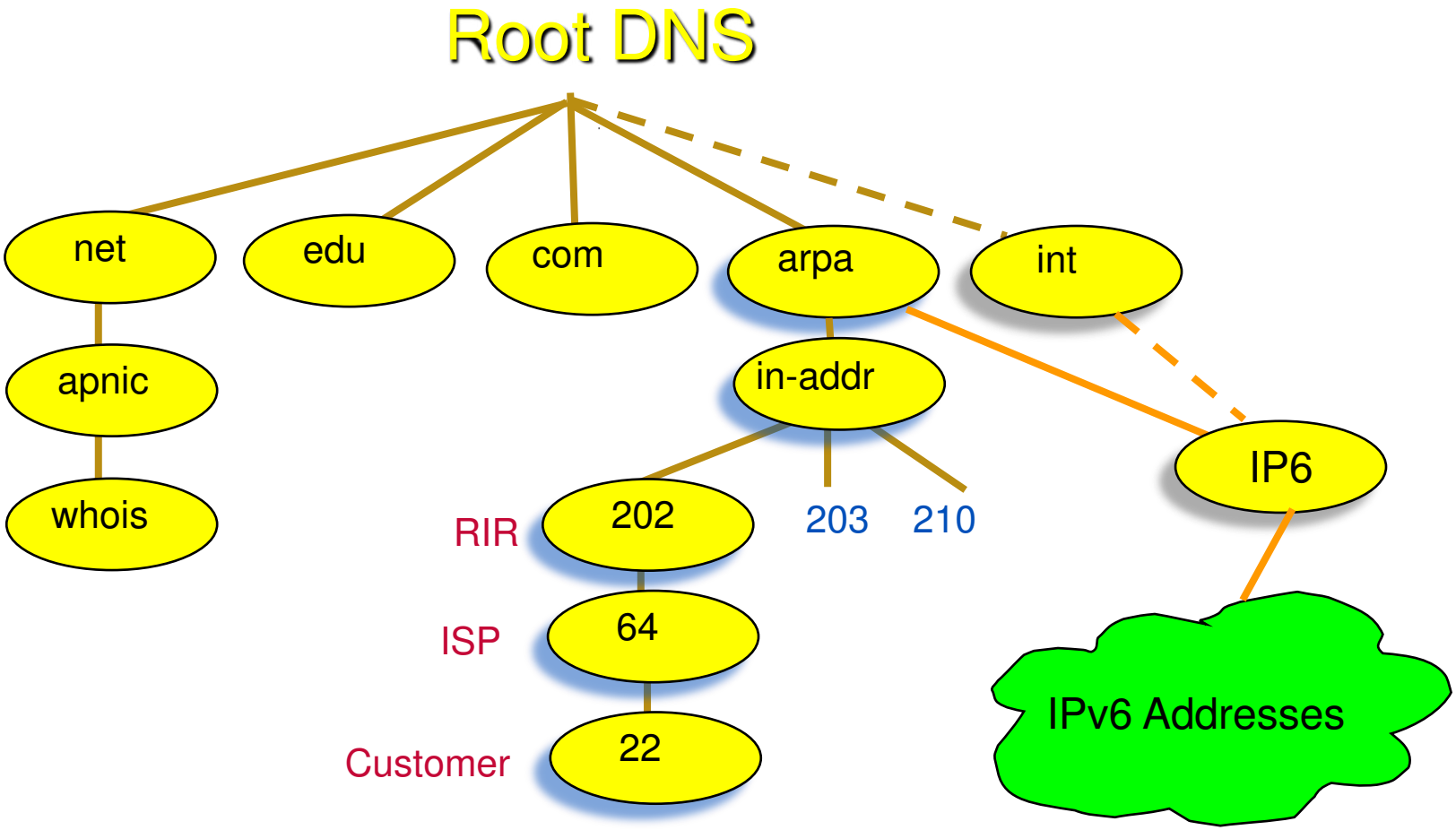
Principles – DNS tree

- *Mapping numbers to names - 'reverse DNS'*



Reverse DNS Tree – with IPv6

RFC 3152



Creating reverse zones

- Same as creating a forward zone file
  - SOA and initial NS records are the same as normal zone
- Main difference
  - need to create additional PTR records
- Can use BIND or other DNS software to create and manage reverse zones
  - Details can be different

Creating reverse zones (continued)

- Files involved
  - Zone files
    - Forward zone file
    - e.g. db.domain.net
  - Reverse zone file
    - e.g. db.192.168.254
  - Configuration files
    - <named.conf>
  - Other
    - Hints files etc.
    - Root.hints

Start of Authority (SOA) record

-

```
<domain.name.>          CLASS   SOA     <hostname.domain.name.>
<mailbox.domain.name> (
                                                <serial-number>
                                                <refresh>
                                                <retry>
                                                <expire>
                                                <negative-caching> )
```

253.253.192.in-addr.arpa.

Pointer (PTR) records

- Create pointer (PTR) records for each IP address

```
131.28.12.202.in-addr.arpa. IN PTR svc00.apnic.net.
```

- or

```
131             IN      PTR             svc00.apnic.net.
```

IPv6 Reverse Lookups – PTR records

- Similar to the IPv4 reverse record

b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.ip6.arpa.

IN PTR test.ip6.example.com.

- Example: reverse name lookup for a host with address 3ffe:8050:201:1860:42::1

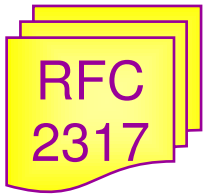
- $ORIGIN 0.6.8.1.1.0.2.0.0.5.0.8.e.f.f.3.ip6.arpa.
- 1.0.0.0.0.0.0.0.0.0.0.0.0.0.2.4.0.0 14400 IN PTR host.example.com.

A reverse zone example

```
$ORIGIN 1.168.192.in-addr.arpa.
@       3600  IN SOA test.company.org. (
                      sys\.admin.company.org.
                      2002021301    ; serial
                      1h            ; refresh
                      30M           ; retry
                      1W            ; expiry
                      3600 )        ; neg. answ. ttl

        NS      ns.company.org.
        NS      ns2.company.org.

1       PTR     gw.company.org.
                router.company.org.

2       PTR     ns.company.org.
;auto generate:  65 PTR host65.company.org
$GENERATE 65-127 $ PTR host$.company.org.
```

Reverse delegation requirements

- /24 Delegations
  - Address blocks should be assigned/allocated
  - At least two name servers
- /16 Delegations
  - Same as /24 delegations
  - APNIC delegates entire zone to member
- < /24 Delegations
  - Read “classless in-addr.arpa delegation”



ISPs Responsibilities

- Be familiar with DNS procedures
- Ensure that addresses are reverse-mapped
- Maintain name servers for allocations
- Minimize pollution of DNS

Reverse Delegation Procedures

- Standard whois database object
- Nameserver/domain set up verified before being submitted to the database
- Protection by maintainer object
  - (current auths: CRYPT-PW, PGP)

Whois domain object

```
domain:     28.12.202.in-addr.arpa
Descr:      in-addr.arpa zone for 28.12.202.in-addr.arpa
admin-c:    NO4-AP
tech-c:     AIC1-AP
zone-c:     NO4-AP
nserver:    cumin.apnic.net
nserver:    tinnie.apnic.net
nserver:    tinnie.arin.net
mnt-by:     MAINT-APNIC-AP
mnt-lower:  MAINT-AP-DNS
changed:    inaddr@apnic.net 20021023
changed:    inaddr@apnic.net 20040109
changed:    hm-changed@apnic.net 20091007
changed:    hm-changed@apnic.net 20111208
source:     APNIC
```

Reverse Zone

Contacts

Name Servers

Maintainers (protection)

Questions

You're Invited!

APRICOT 2015: Fukuoka, Japan,
24 Feb-6 Mar 2015

2015.apricot.net

THANK YOU

Sunny Chendi

sunny@apnic.net

http://www.apnic.net




APNIC