A Secure Mechanism for Address Block Allocation and Distribution

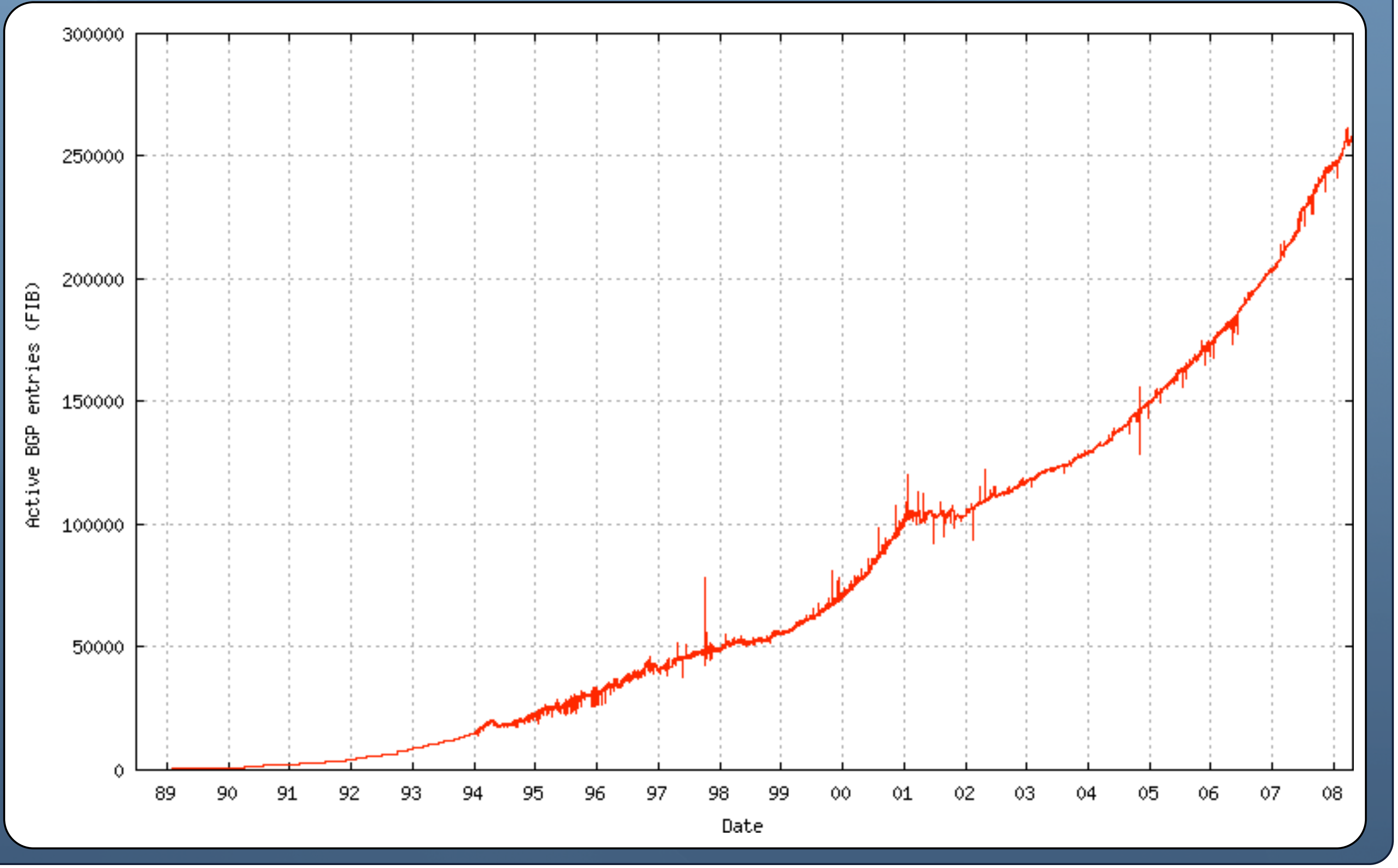
Damien LEROY, Olivier BONAVENTURE

Université catholique de Louvain (UCL) - Belgium
IP Networking Lab - http://inl.info.ucl.ac.be

IFIP Networking 2008 - May 5-9, 2008

Introduction

Growth of BGP routing tables



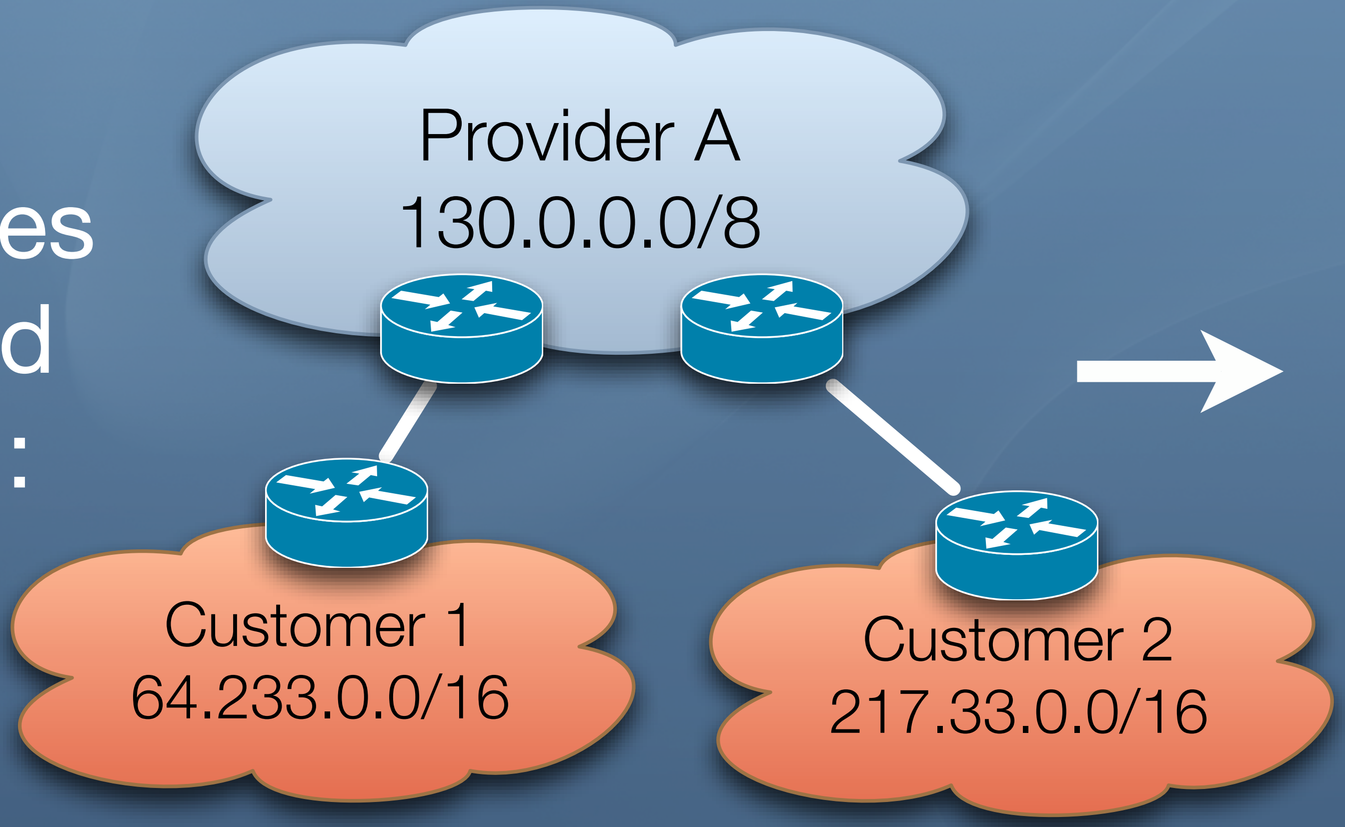
Source : http://bgp.potaroo.net/

Introduction

Growth of BGP routing tables

- Why ?

>200k prefixes are allocated in this way :



→ 3 entries in BGP routing tables

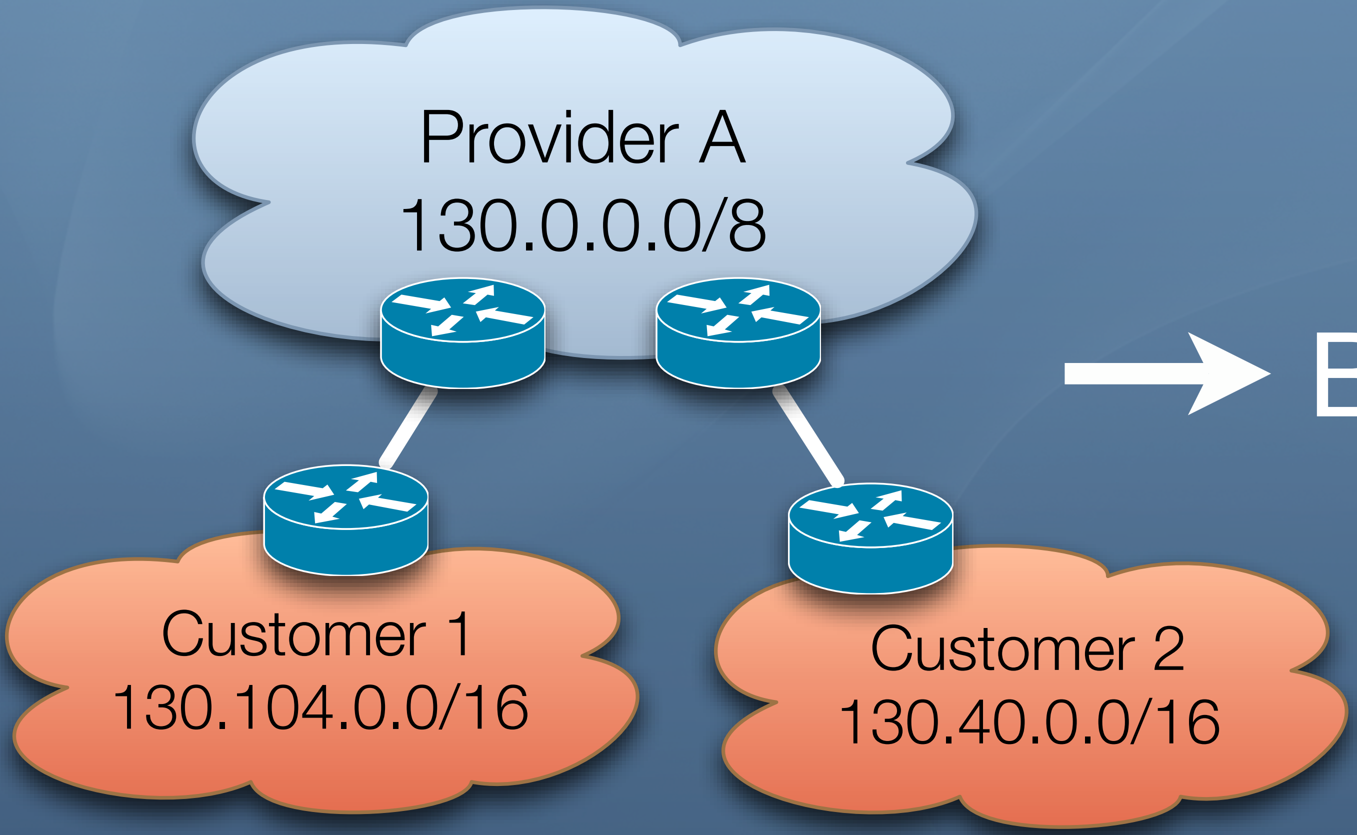
Provider Independent (PI) prefixes

Introduction

Growth of BGP routing tables

- Why ?

In a smart world :



→ 1 entry in BGP routing tables

Provider Aggregatable (PA) prefixes

Motivations

Growth of BGP routing tables in DFZ

Motivations

Growth of BGP routing tables in DFZ

↓

Only PA addresses should be used

Motivations

Growth of BGP routing tables in DFZ

↓

Only PA addresses should be used

↓

Renumbering in a whole network must work

Motivations

Growth of BGP routing tables in DFZ

↓

Only PA addresses should be used

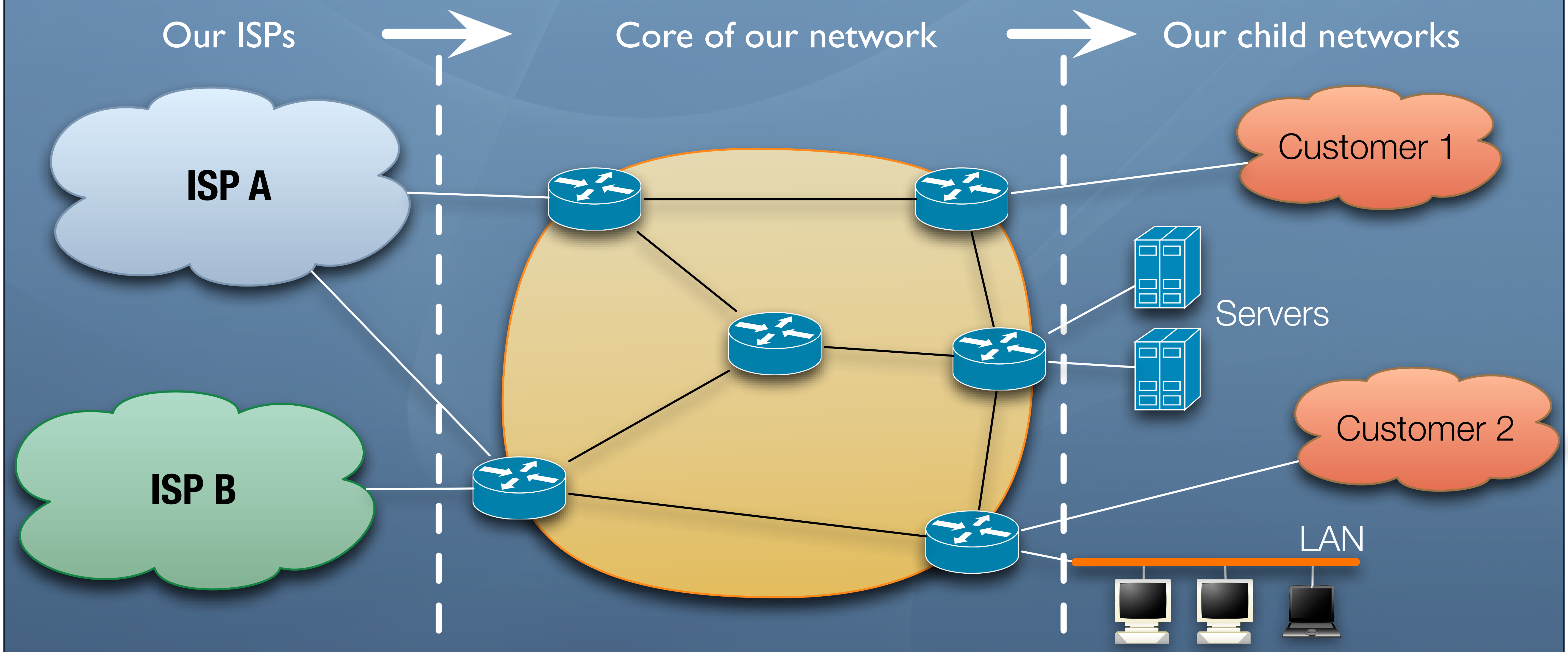
↓

Renumbering in a whole network must work

↓

We need a mechanism to do it automatically

Network Topology



Requirements

Requirements

- High utilization ratio of address space

Requirements

- High utilization ratio of address space
- Independence from routing protocols

Requirements

- High utilization ratio of address space
- Independence from routing protocols
- Security

Requirements

- High utilization ratio of address space
- Independence from routing protocols
- Security
- Roles

Requirements

- High utilization ratio of address space
- Independence from routing protocols
- Security
- Roles
- Prefix coloring

Requirements

Roles

- Group hosts by role in prefixes, e.g. :
  - local users,
  - servers,
  - business customer networks
- Permit a better <u>aggregation</u> (in access control rules)

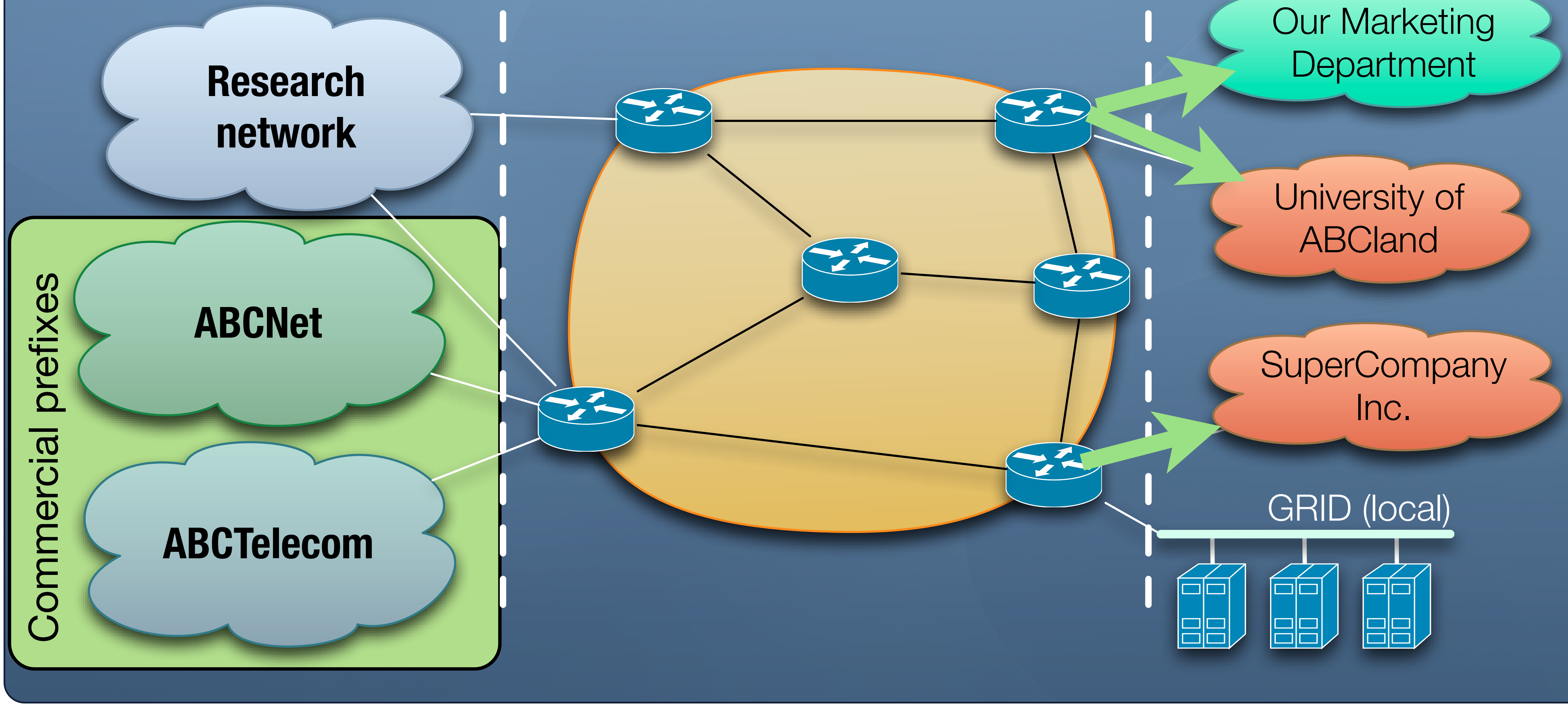
Requirements

Prefix coloring

- Each prefix received has a “color”, e.g. :
  - Research network prefix
  - Commercial network prefix
- Each child network is associated with a set of colors
- Colors are used for prefix assignment

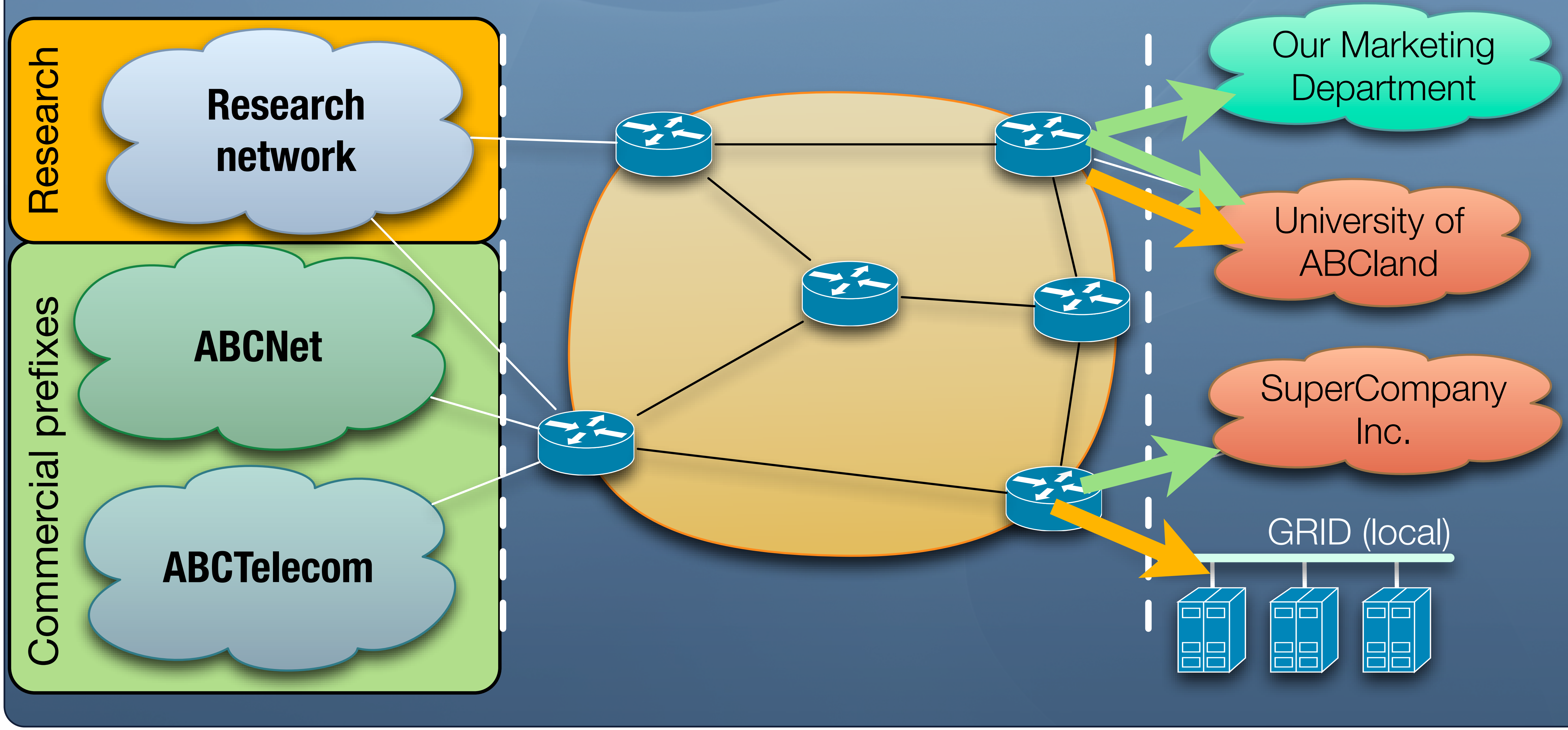
Requirements

Prefix coloring

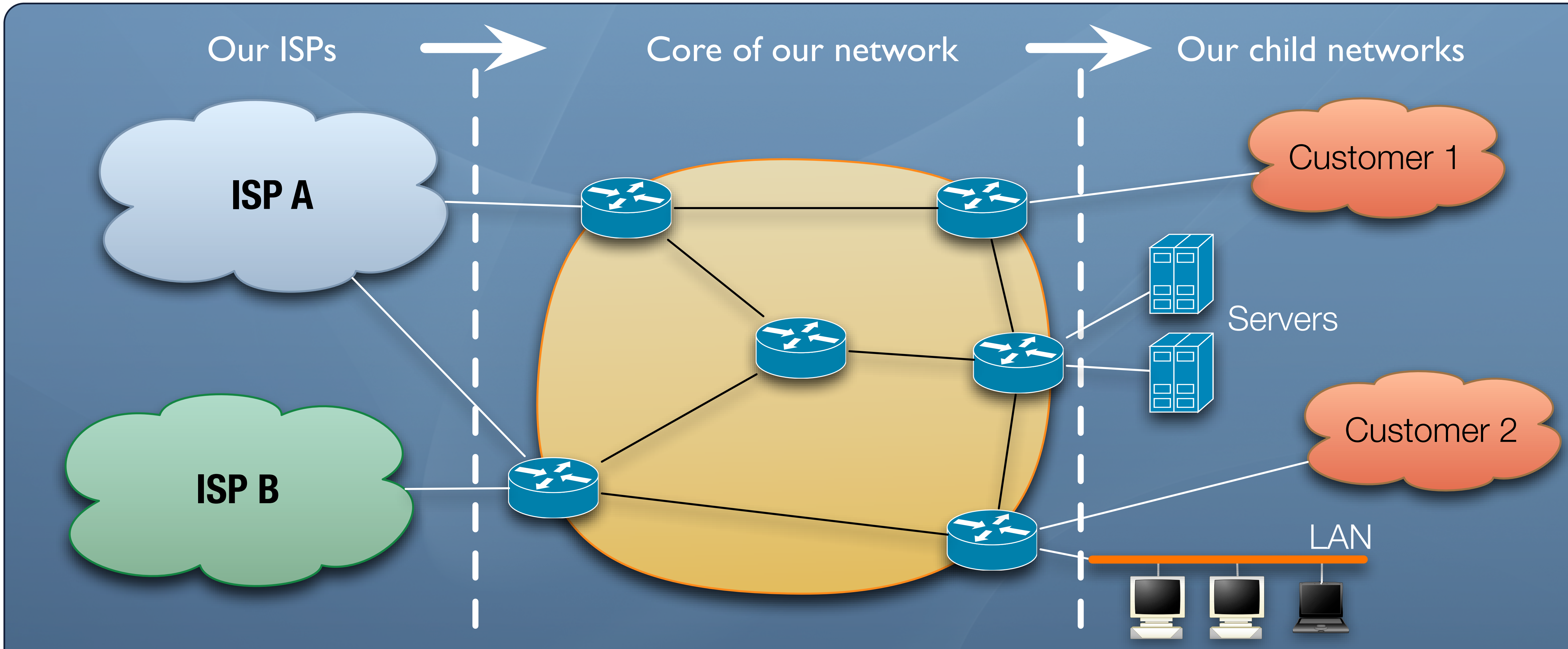


Requirements

Prefix coloring



Parts of the Addresses



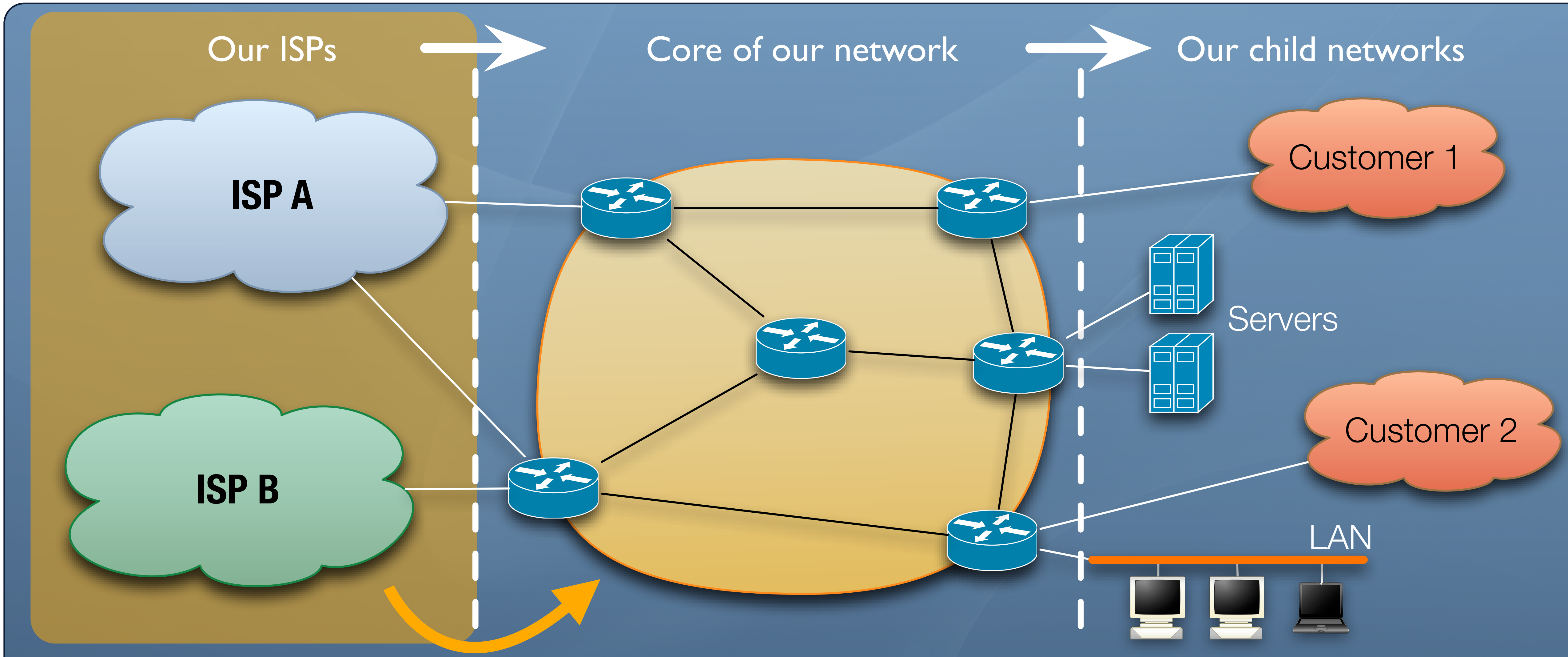
`2001:6a8:3080:20e1:217:f2ff:fe34:51ee`

PREFIX
48 bits

SID
16 bits

IID
64 bits

Parts of the Addresses

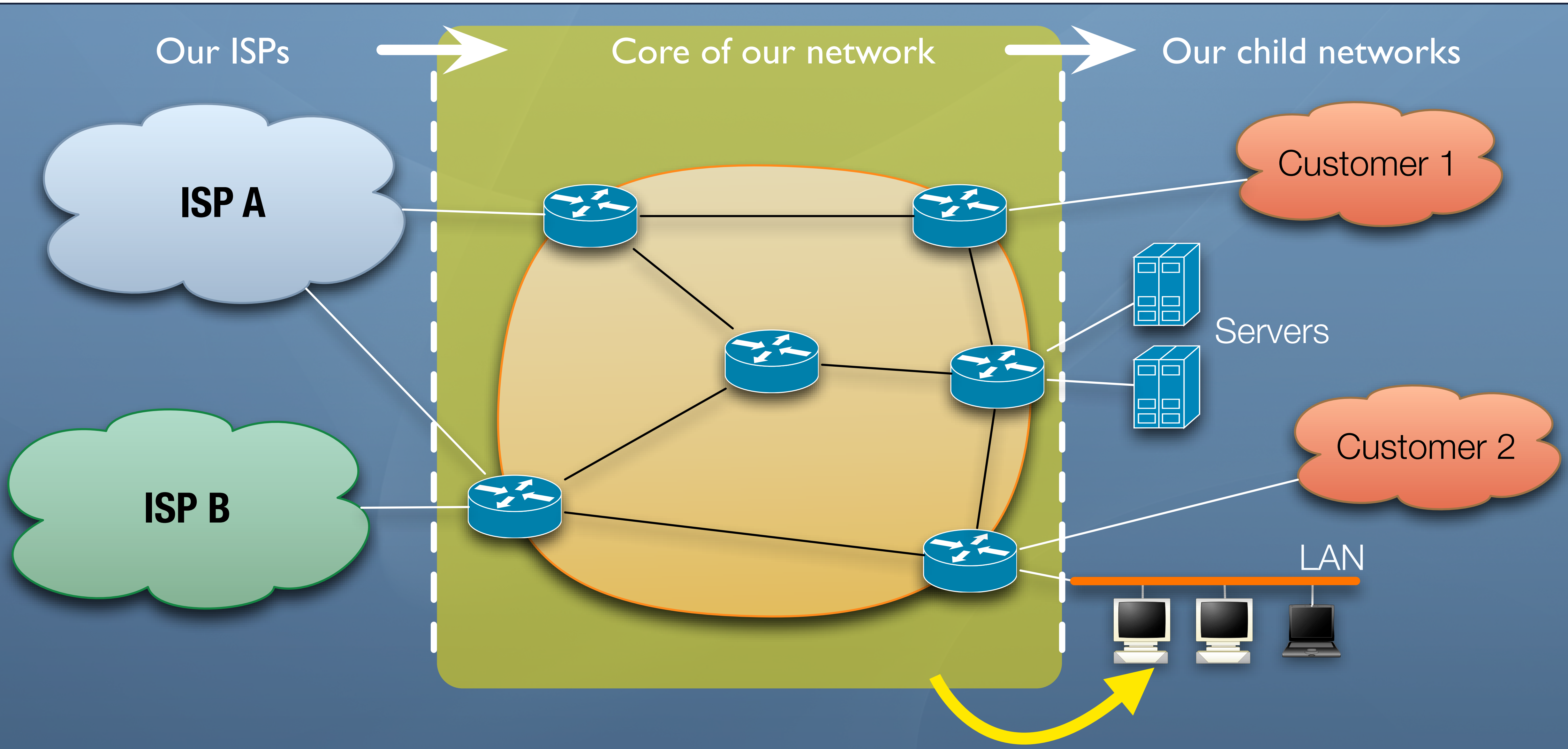


2001:6a8:3080:20e1:217:f2ff:fe34:51ee

$\underbrace{\texttt{2001:6a8:3080}}_{}$

PREFIX
8-64 bits

Parts of the Addresses



Our ISPs

Core of our network

Our child networks

ISP A

ISP B

Customer 1

Servers

Customer 2

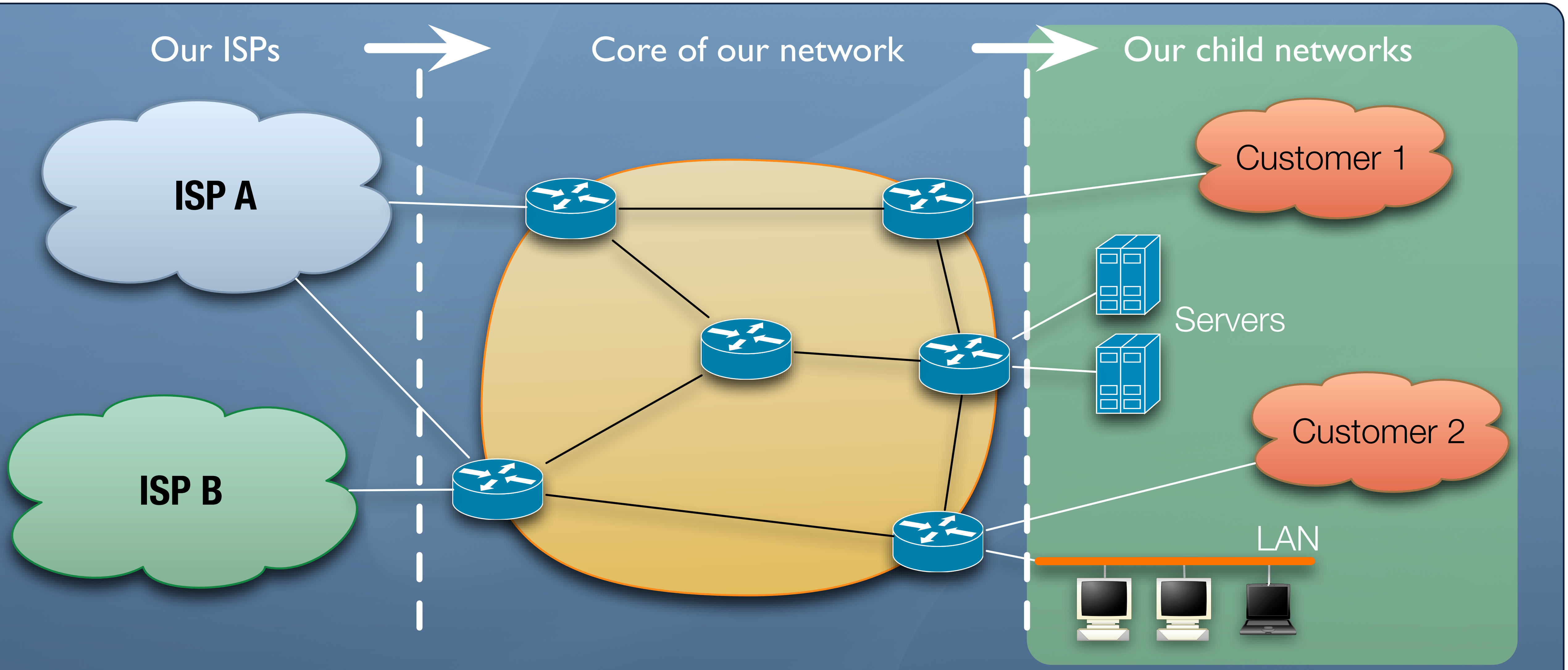
LAN

2001:6a8:3080:20e1:217:f2ff:fe34:51ee

Allocated SID

1-56 bits

Parts of the Addresses

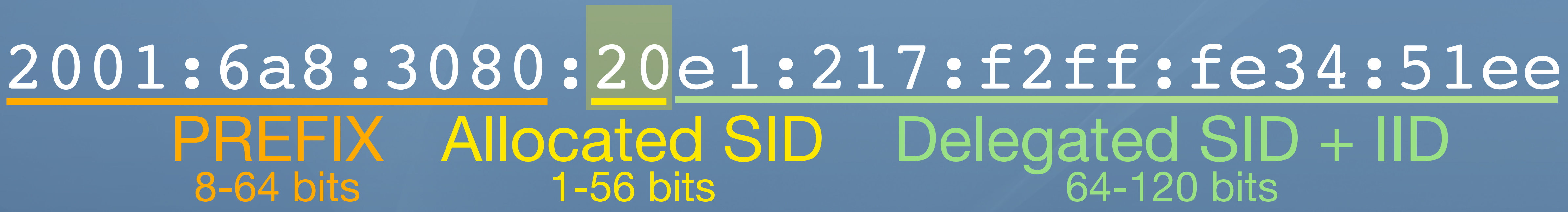


2001:6a8:3080:20e1:217:f2ff:fe34:51ee

Delegated SID + IID
64-120 bits

Parts of the Addresses

- Our job : Choose and distribute the **Allocated SID**



2001:6a8:3080:20e1:217:f2ff:fe34:51ee

PREFIX
8-64 bits

Allocated SID
1-56 bits

Delegated SID + IID
64-120 bits

- Allocated SID size can be different according to the child network :
  - A LAN needs a /64
  - A customer network may need a /56

Address Block Distribution Protocol

Main characteristics

- Router-only protocol
- Distributed
- Hop-by-hop and flooding communication
- Routers choose address blocks and allocate their child networks in them

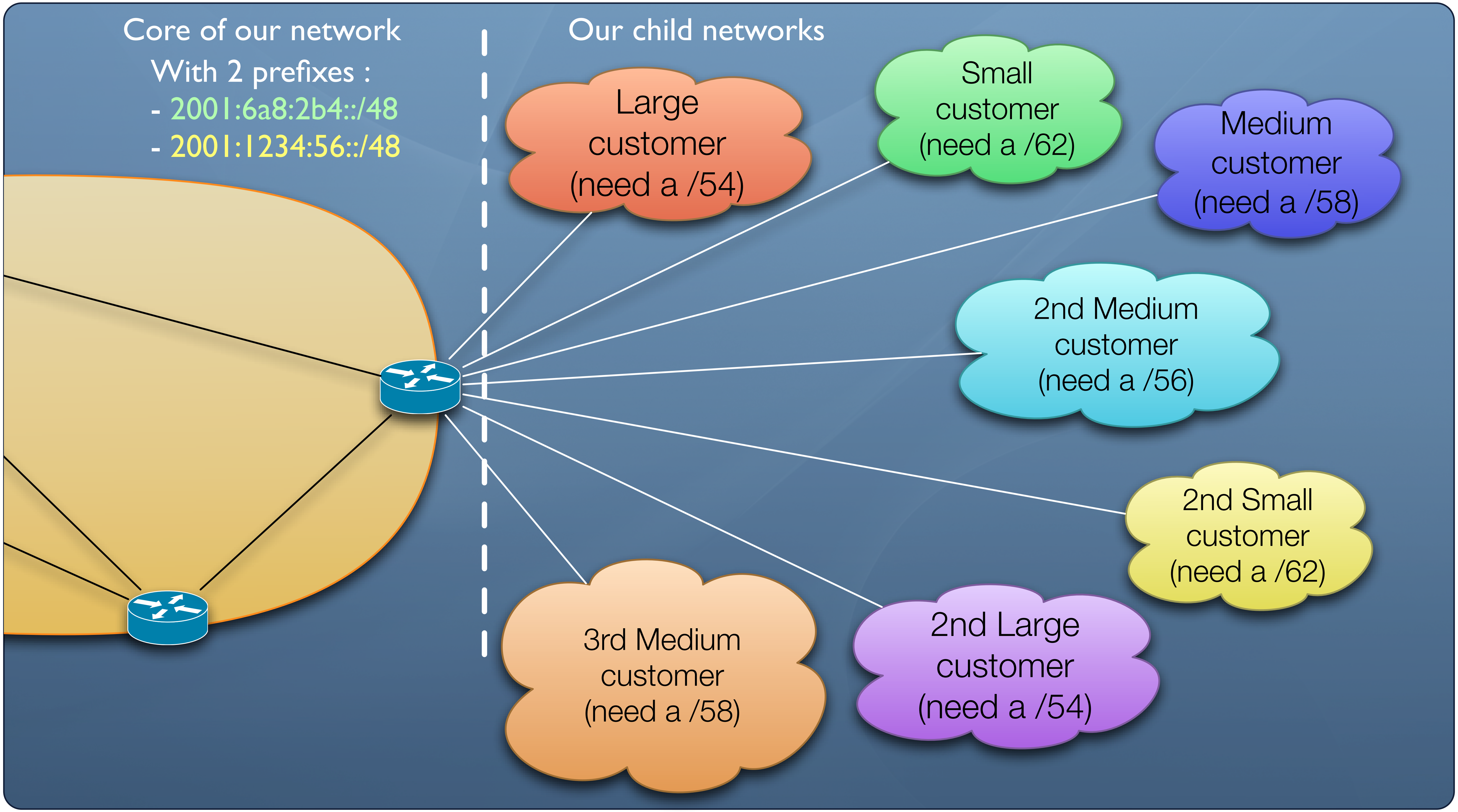
Address Block Distribution Protocol

Core of our network

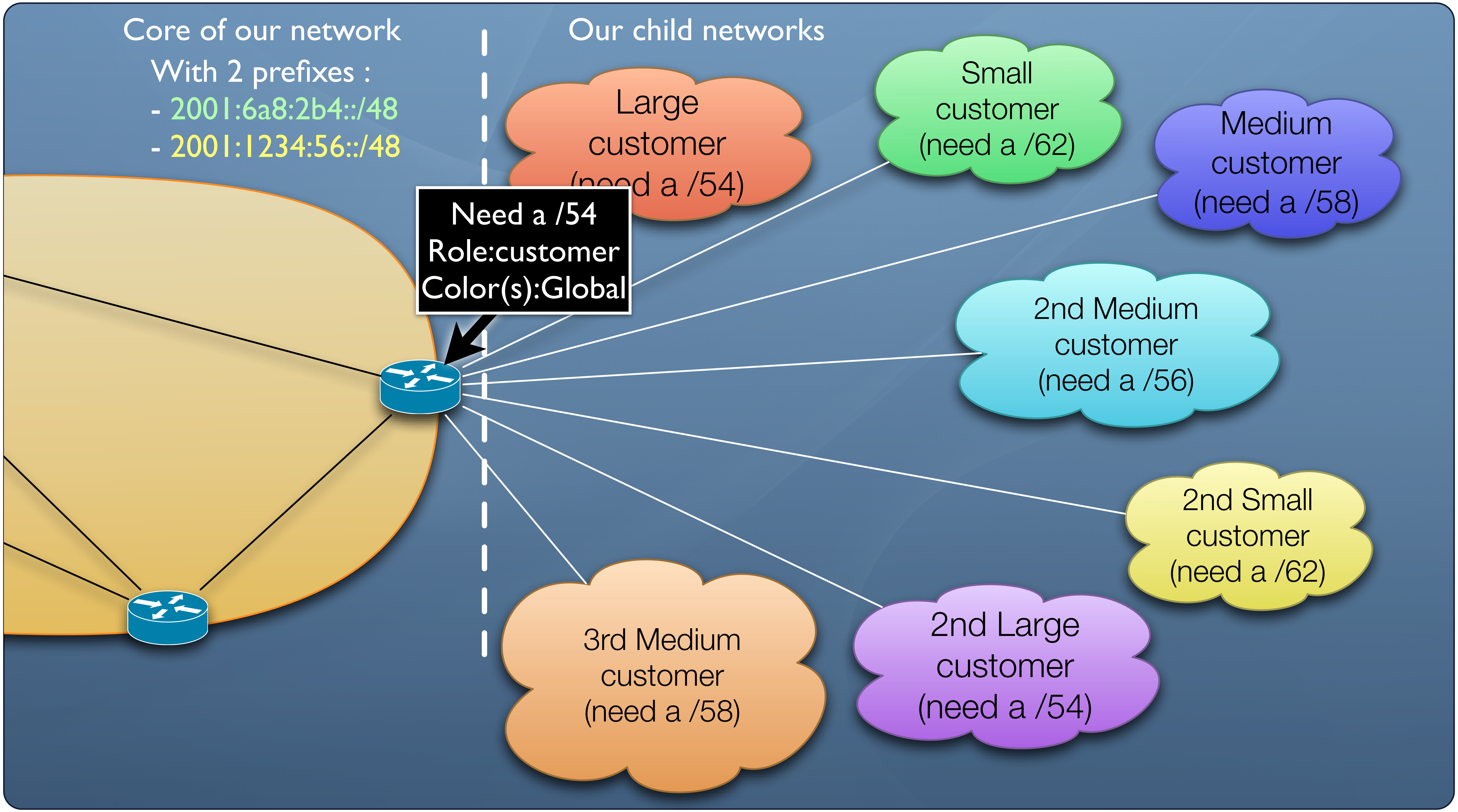
With 2 prefixes :

- 2001:6a8:2b4::/48
- 2001:1234:56::/48

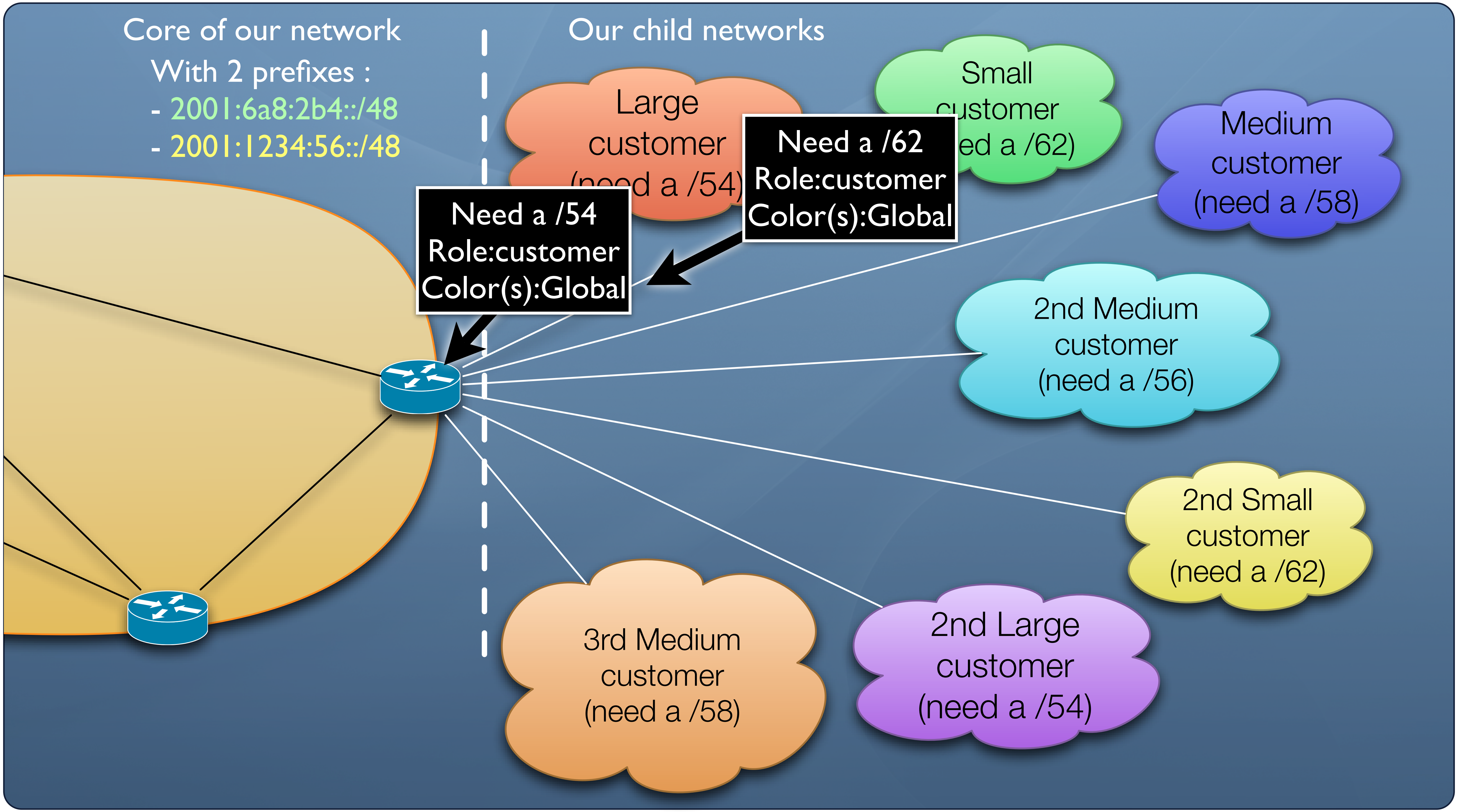
Our child networks


Large customer (need a /54)
Small customer (need a /62)
Medium customer (need a /58)
2nd Medium customer (need a /56)
2nd Small customer (need a /62)
2nd Large customer (need a /54)
3rd Medium customer (need a /58)

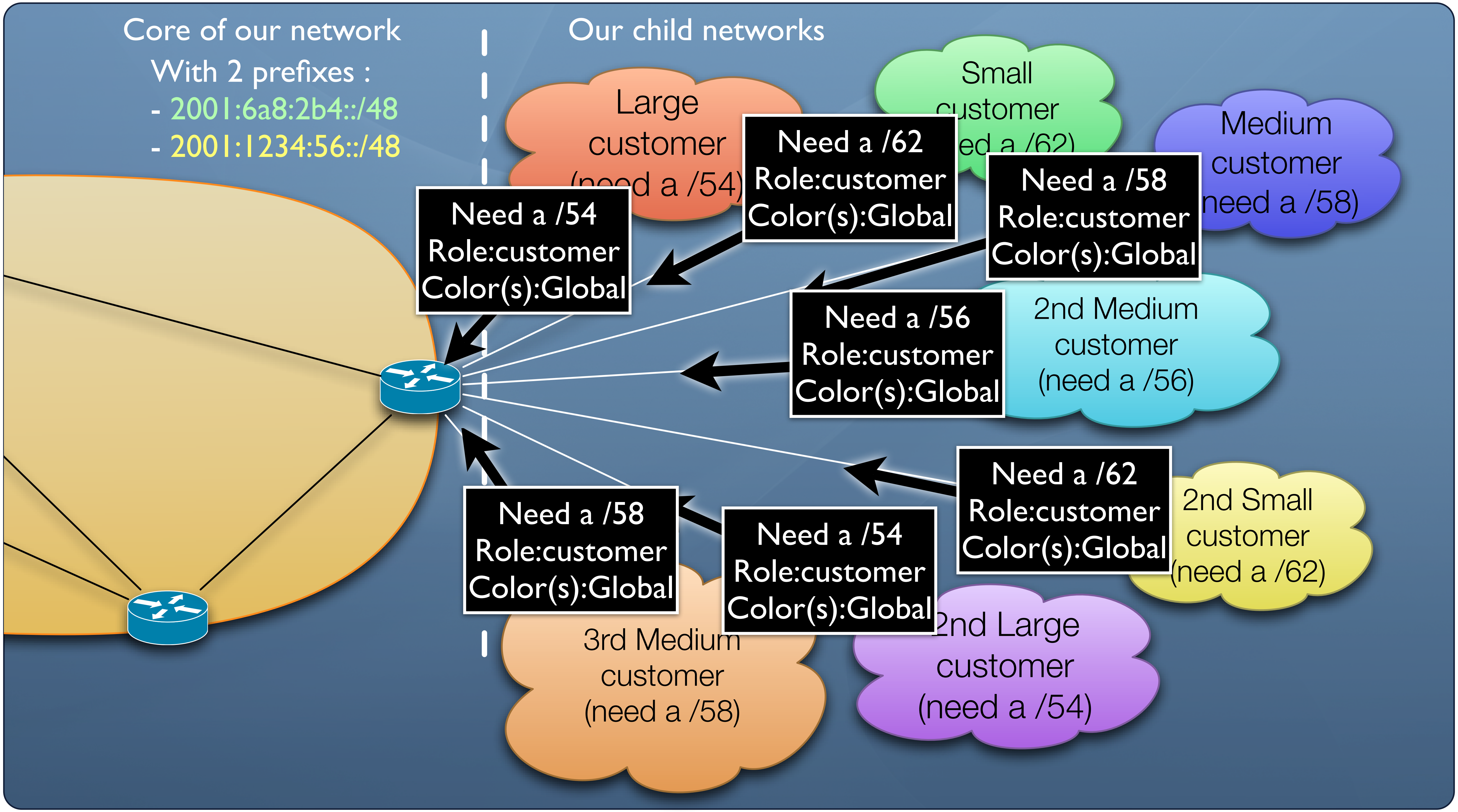
Address Block Distribution Protocol


Core of our network
With 2 prefixes :
- 2001:6a8:2b4::/48
- 2001:1234:56::/48
Our child networks
Large customer (need a /54)
Small customer (need a /62)
Medium customer (need a /58)
Need a /54
Role:customer
Color(s):Global
2nd Medium customer (need a /56)
2nd Small customer (need a /62)
3rd Medium customer (need a /58)
2nd Large customer (need a /54)

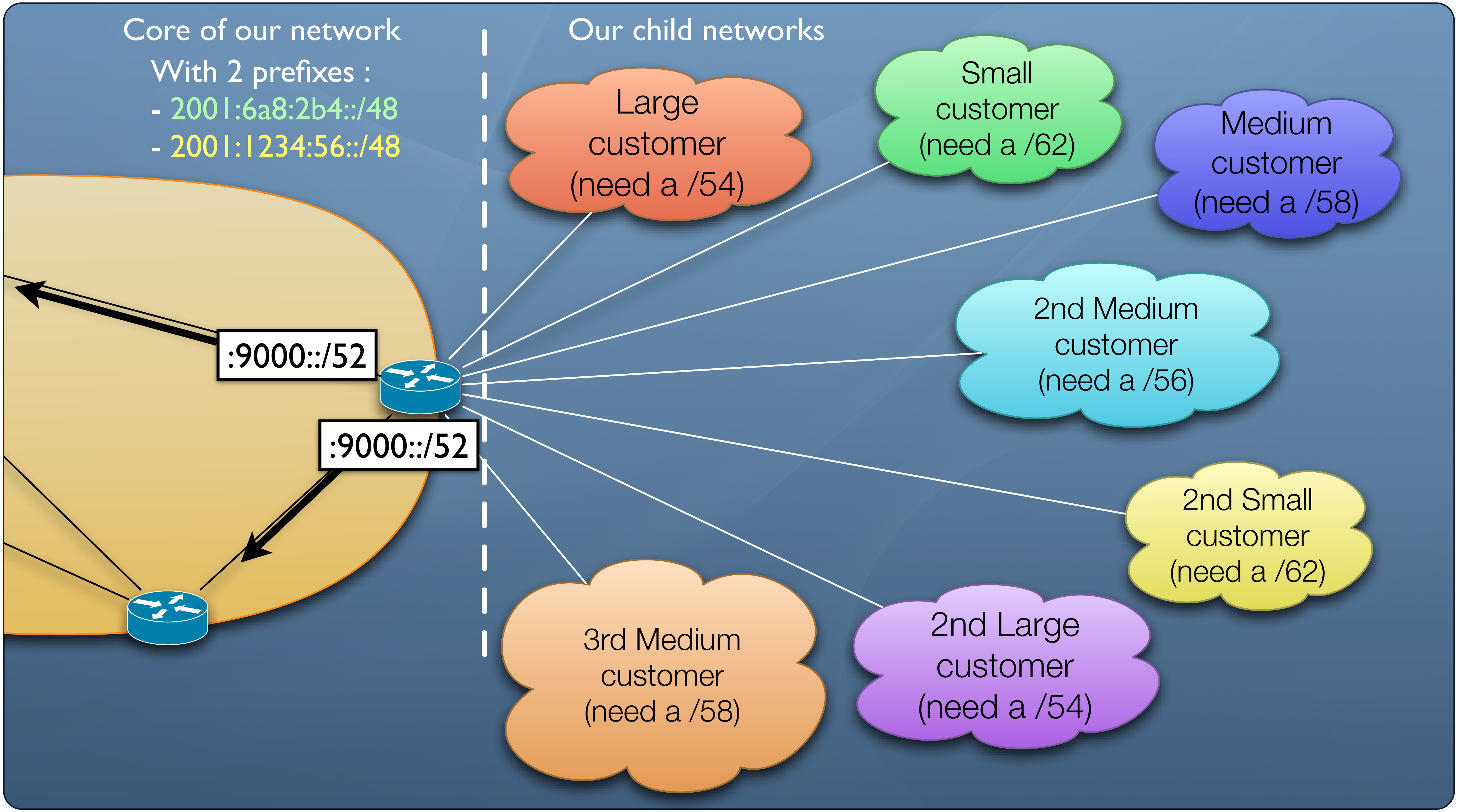
Address Block Distribution Protocol


Core of our network
With 2 prefixes :
- 2001:6a8:2b4::/48
- 2001:1234:56::/48
Our child networks
Large customer (need a /54)
Small customer (need a /62)
Medium customer (need a /58)
Need a /62
Role:customer
Color(s):Global
Need a /54
Role:customer
Color(s):Global
2nd Medium customer (need a /56)
2nd Small customer (need a /62)
3rd Medium customer (need a /58)
2nd Large customer (need a /54)

Address Block Distribution Protocol


Core of our network
With 2 prefixes :
- 2001:6a8:2b4::/48
- 2001:1234:56::/48
Our child networks
Large customer (need a /54)
Small customer (need a /62)
Medium customer (need a /58)
2nd Medium customer (need a /56)
2nd Small customer (need a /62)
2nd Large customer (need a /54)
3rd Medium customer (need a /58)
Need a /54 Role:customer Color(s):Global
Need a /62 Role:customer Color(s):Global
Need a /58 Role:customer Color(s):Global
Need a /56 Role:customer Color(s):Global
Need a /62 Role:customer Color(s):Global
Need a /58 Role:customer Color(s):Global
Need a /54 Role:customer Color(s):Global

Address Block Distribution Protocol


Core of our network
With 2 prefixes :
- 2001:6a8:2b4::/48
- 2001:1234:56::/48
Our child networks
Large customer (need a /54)
Small customer (need a /62)
Medium customer (need a /58)
2nd Medium customer (need a /56)
2nd Small customer (need a /62)
3rd Medium customer (need a /58)
2nd Large customer (need a /54)
:9000::/52
:9000::/52

Address Block Distribution

Depth : 52

Depth : 53

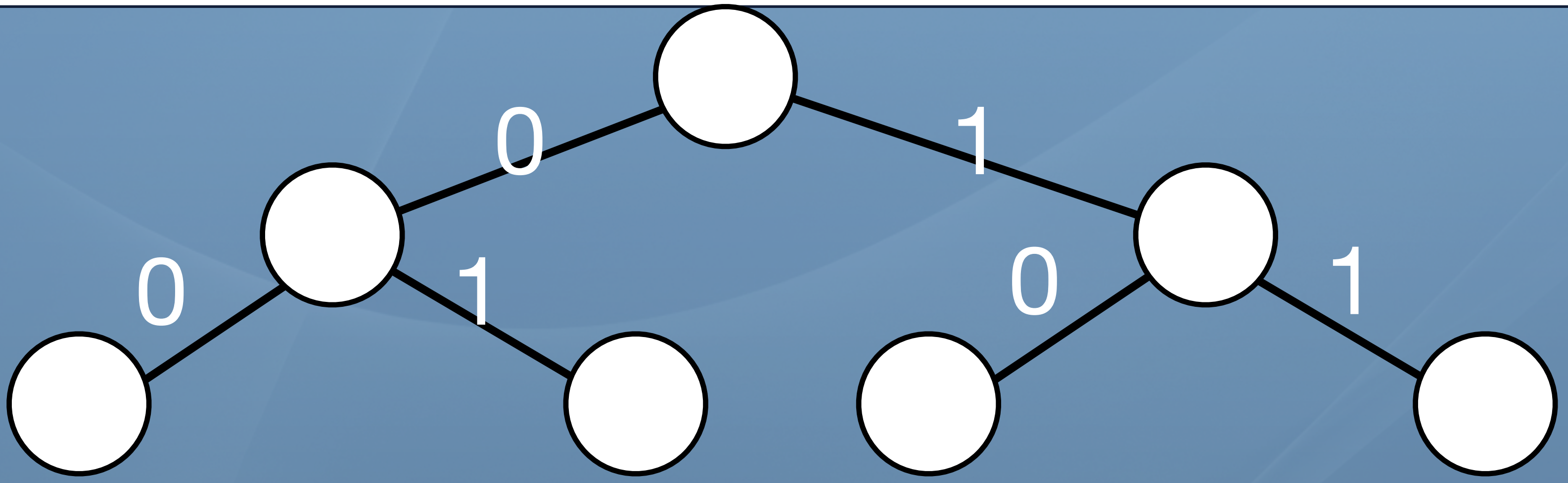
Depth : 54

Depth : 55

Depth : 56

Depth : 57

Depth : 58



Large customer (need a /54)

2nd Large customer (need a /54)

2nd Medium customer (need a /56)

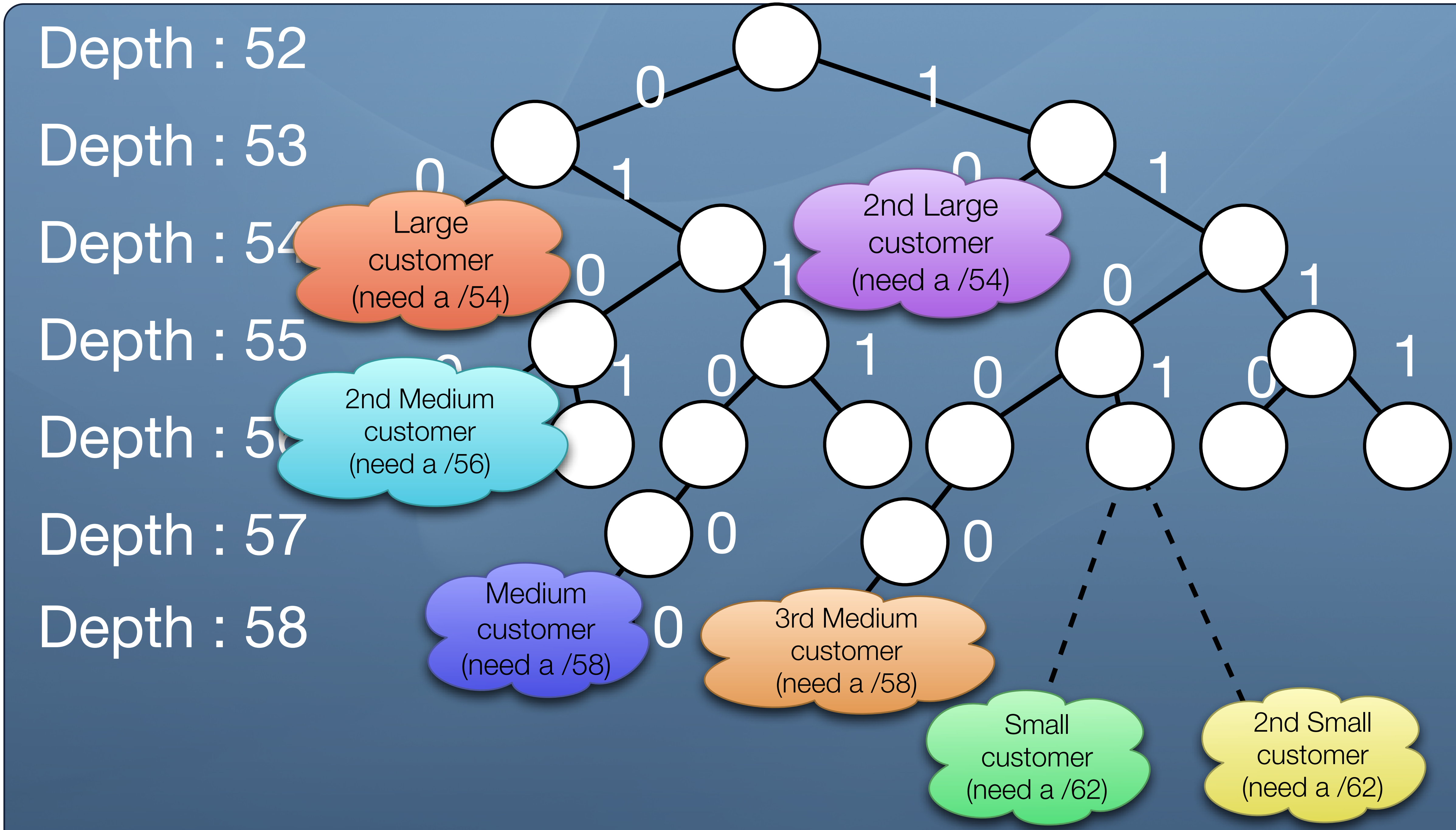
Medium customer (need a /58)

3rd Medium customer (need a /58)

Small customer (need a /62)

2nd Small customer (need a /62)

Address Block Distribution



Depth : 52

Depth : 53

Depth : 54

Depth : 55

Depth : 56

Depth : 57

Depth : 58

Large customer (need a /54)

2nd Large customer (need a /54)

2nd Medium customer (need a /56)

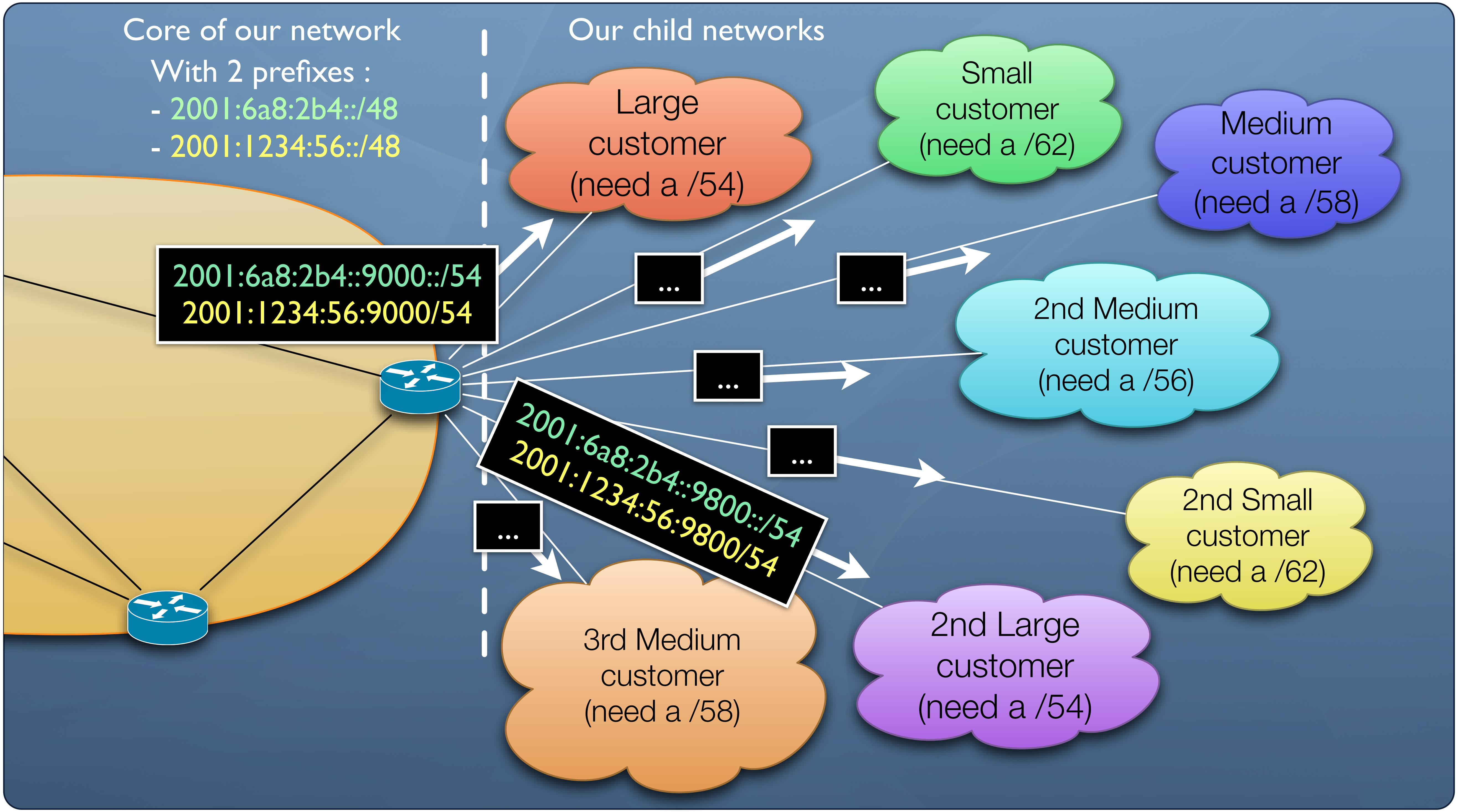
Medium customer (need a /58)

3rd Medium customer (need a /58)

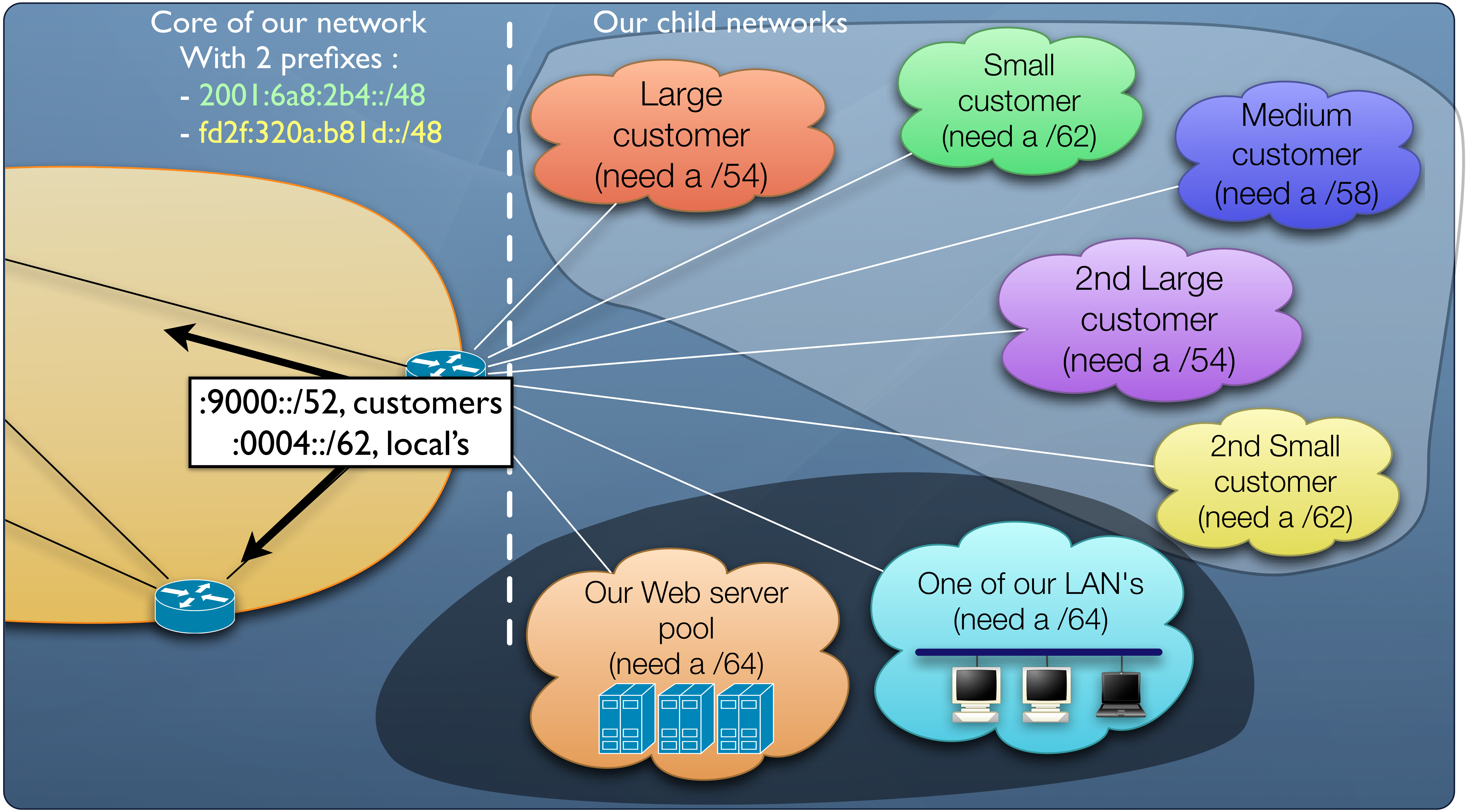
Small customer (need a /62)

2nd Small customer (need a /62)

Address Block Distribution


Core of our network
With 2 prefixes :
- 2001:6a8:2b4::/48
- 2001:1234:56::/48
Our child networks
2001:6a8:2b4::9000::/54
2001:1234:56:9000/54
Large customer (need a /54)
Small customer (need a /62)
Medium customer (need a /58)
...
...
...
...
...
2nd Medium customer (need a /56)
2001:6a8:2b4::9800::/54
2001:1234:56:9800/54
2nd Small customer (need a /62)
3rd Medium customer (need a /58)
2nd Large customer (need a /54)

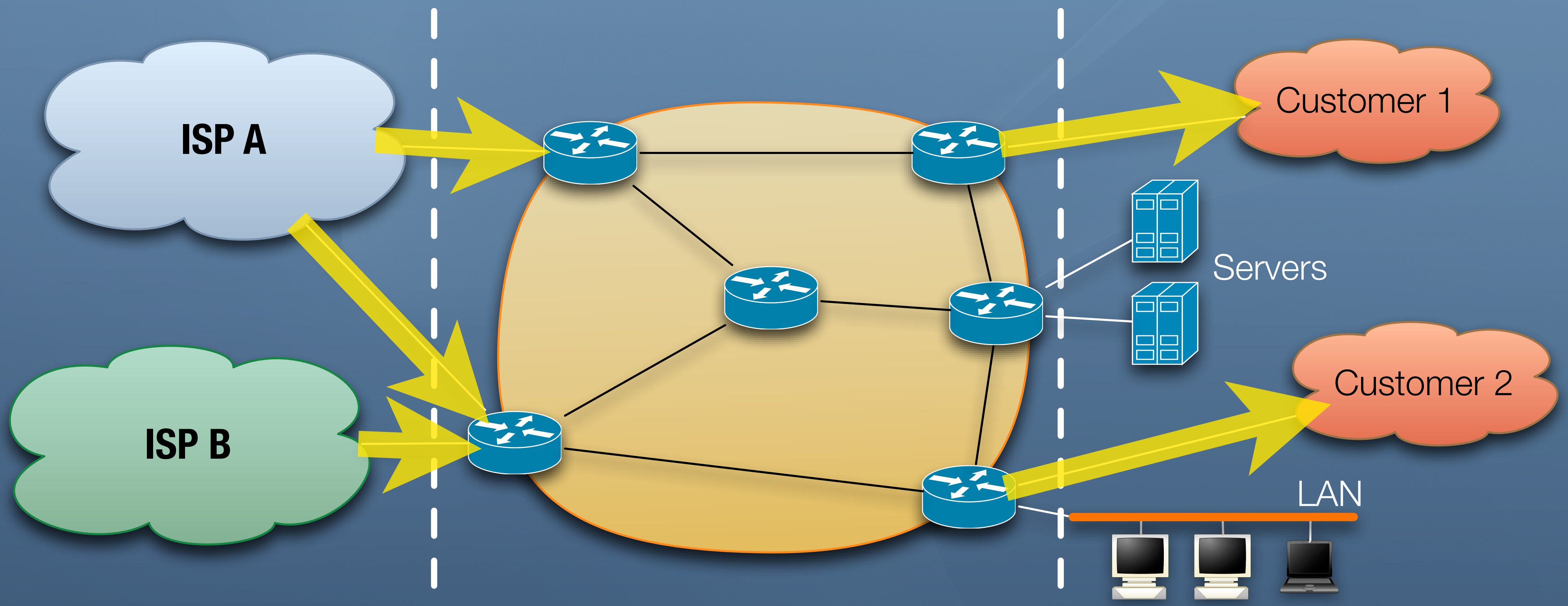
Roles


Core of our network
With 2 prefixes :
- 2001:6a8:2b4::/48
- fd2f:320a:b81d::/48
Our child networks
:9000::/52, customers
:0004::/62, local's
Large customer (need a /54)
Small customer (need a /62)
Medium customer (need a /58)
2nd Large customer (need a /54)
2nd Small customer (need a /62)
Our Web server pool (need a /64)
One of our LAN's (need a /64)

Security

Authentication needed

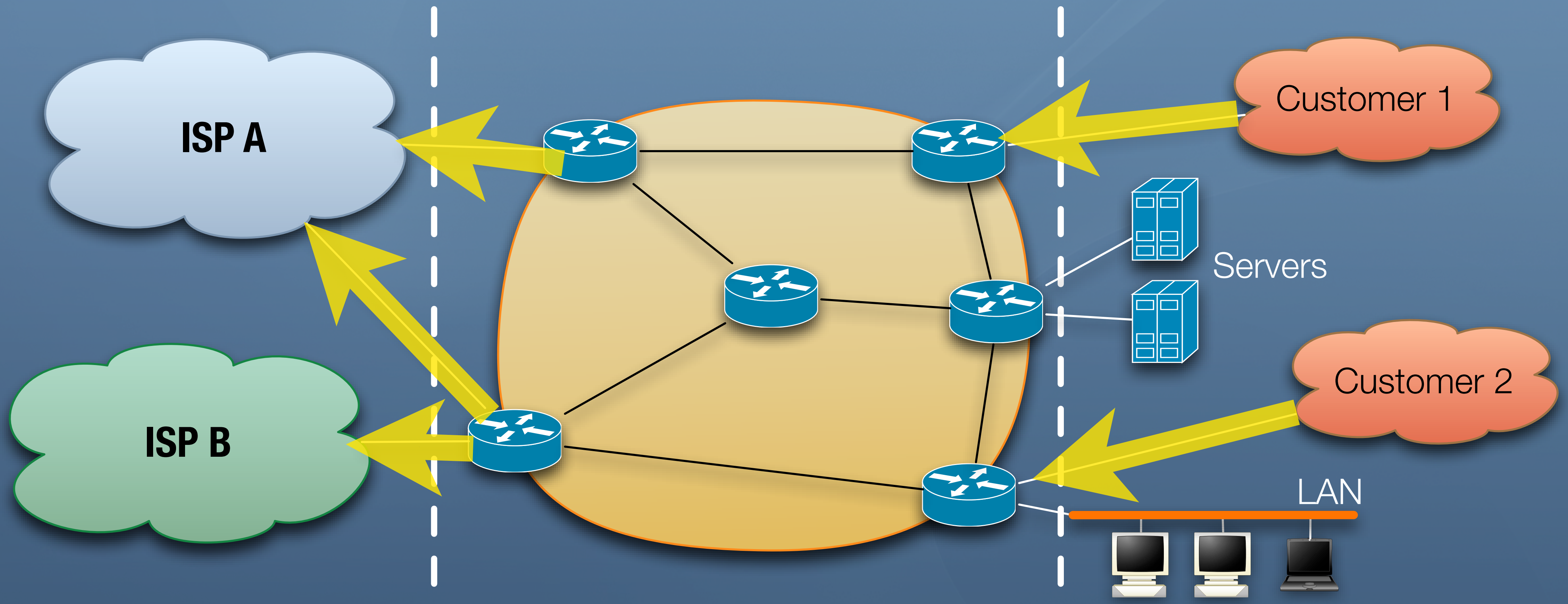
1. Of an ISP to its customers (top-down auth.)



Security

Authentication needed

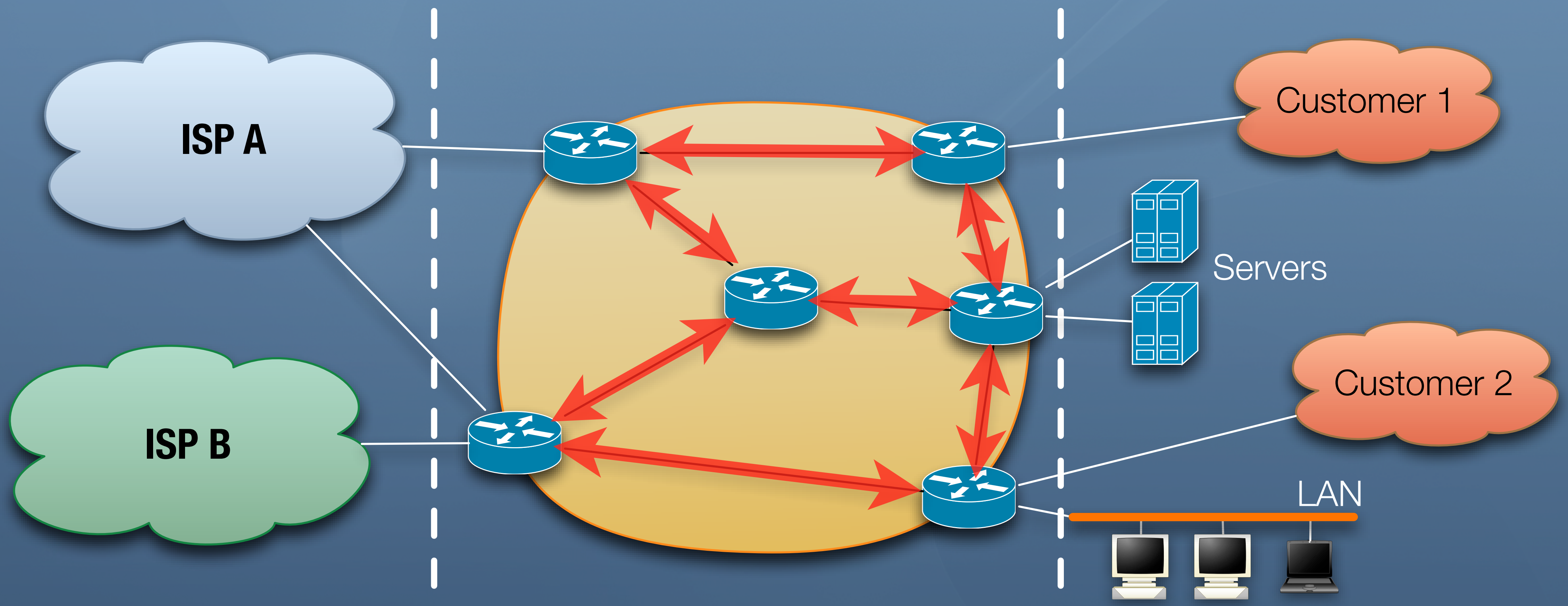
2. Of a customer to its ISP(s) (bottom-up auth.)



Security

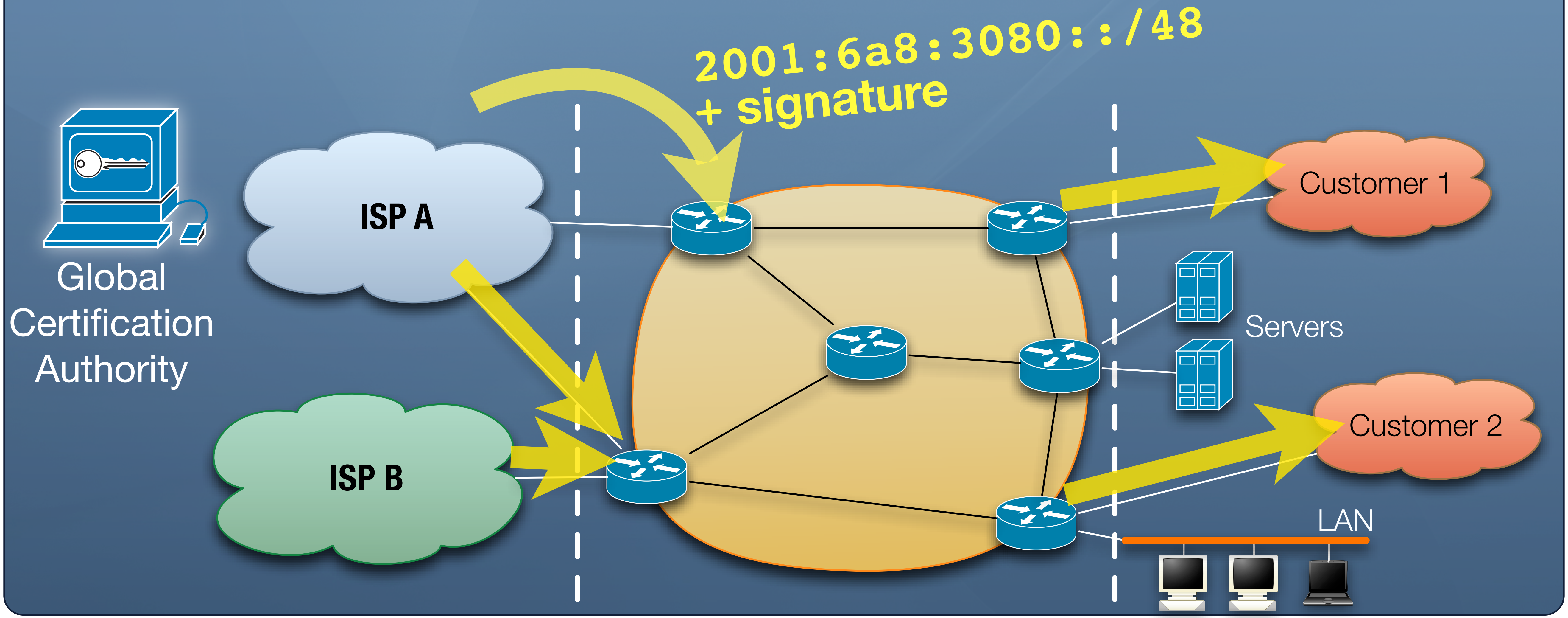
Authentication needed

3. Between routers



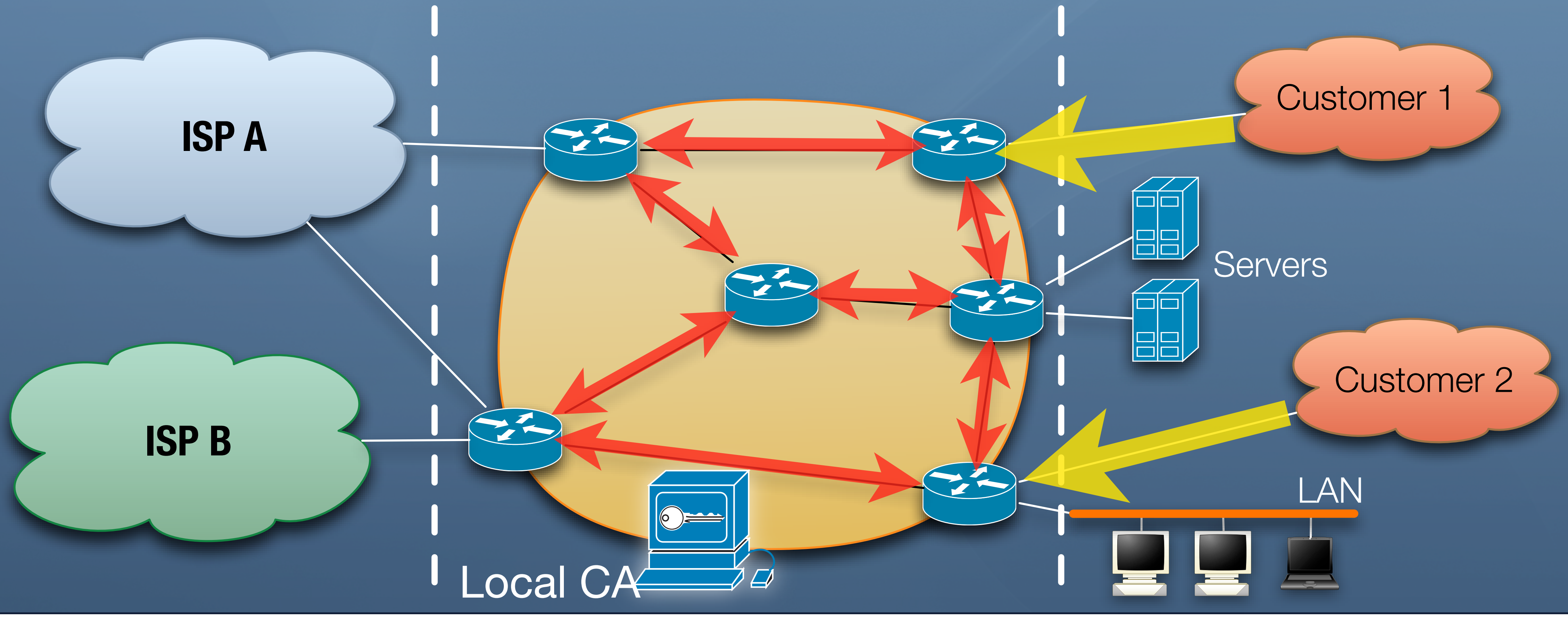
Top-down Authentication

- A **Global** Certification Authority is added
- Using the PKI of SIDR working group at IETF



Bottom-up and Router Authentication

- A **Local** Certification Authority is added
- A certificate is given to each entity defining its permissions



Bottom-up and Router Authentication

Sample certificate information

- Type : router
- Public keys & local CA'sign.

- Type : child network
- Role : customer
- Color(s) : business
- Prefix size needed: 54
- Public keys & local CA'signature

Bottom-up and Router Authentication

Sample certificate information

- Type : router
- Public keys & local CA’sign.

- Type : child network
- Role : customer
- Color(s) : business
- Prefix size needed: 54
- Public keys & local CA’signature

Keys and Certificates can be distributed offline or the first time the entity connects

Evaluations

- Protocol simulator implemented
- Evaluations have been performed
- A prototype in XORP is planned

Conclusion

Contributions

Conclusion

Contributions

- Distributed mechanism for address allocation and distribution

Conclusion

Contributions

- Distributed mechanism for address allocation and distribution
- Targeted at ISP, campus, enterprise networks

Conclusion

Contributions

- Distributed mechanism for address allocation and distribution
- Targeted at ISP, campus, enterprise networks
- Roles permit aggregation

Conclusion

Contributions

- Distributed mechanism for address allocation and distribution
- Targeted at ISP, campus, enterprise networks
- Roles permit aggregation
- Security

Questions ?