Diverting the Network Complexity

IETF 86 NCRG, Orlando

March 2013

Sheng Jiang

Content

- **Direction of diverting network complexity**
- Practice scenario 1 – self-managed network
- Practice scenario 2 – semantic prefix

Increasing Complexity of Network Devices and Operations

Network devices become complicated

More new features and functionalities on network Devices

- The code size of routers increases continually
- The configurations size of routers is also increasing
- Diversified network management requirements are growing, beyond the reachability of routing
- There are interference among network operations

Network scale is increasing

The network is larger and larger

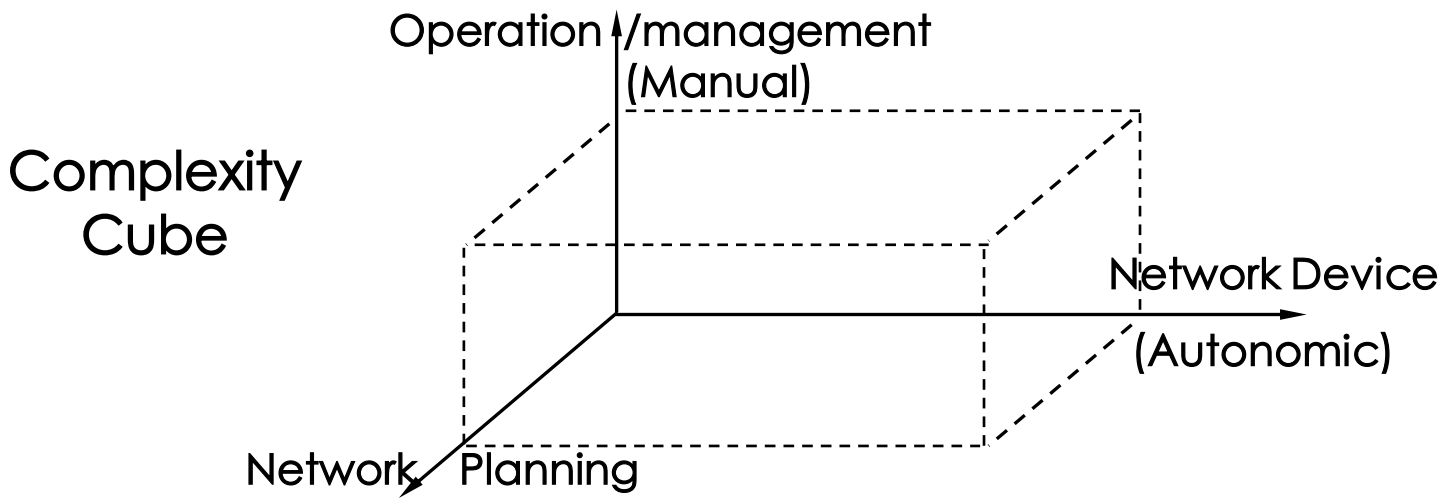
- User number is increase though it is close to the limit
- Traffics per user is exploding with enriched applications
- Intelligent devices are starting to connect to the Internet
- The number of network devices increase
- The coordination among devices are was not well supported

The exploding increasing of Internet is the reason

Requirement of Reducing Human Management

- **Current reality**
  - **Networks keeping changing dynamically; configurations on devices changes frequently**
  - **Configurations relies on the decision and intelligence of human operators**
  - **More than 95% network errors are created human mis-configuring or mis-operating**
  - **Fault location also depends on human diagnosis**
  - **The complex of network require coordination of multiple devices, which are typically managed by different operating personnel**
  - **That different aspects/elemtns of networks intervene each other makes network management even more complex**
- **Human operation is the centre and the bottleneck**
  - **The more complex, the more opportunities for human error, also longer response time, higher cost**

Where to divert network complexity



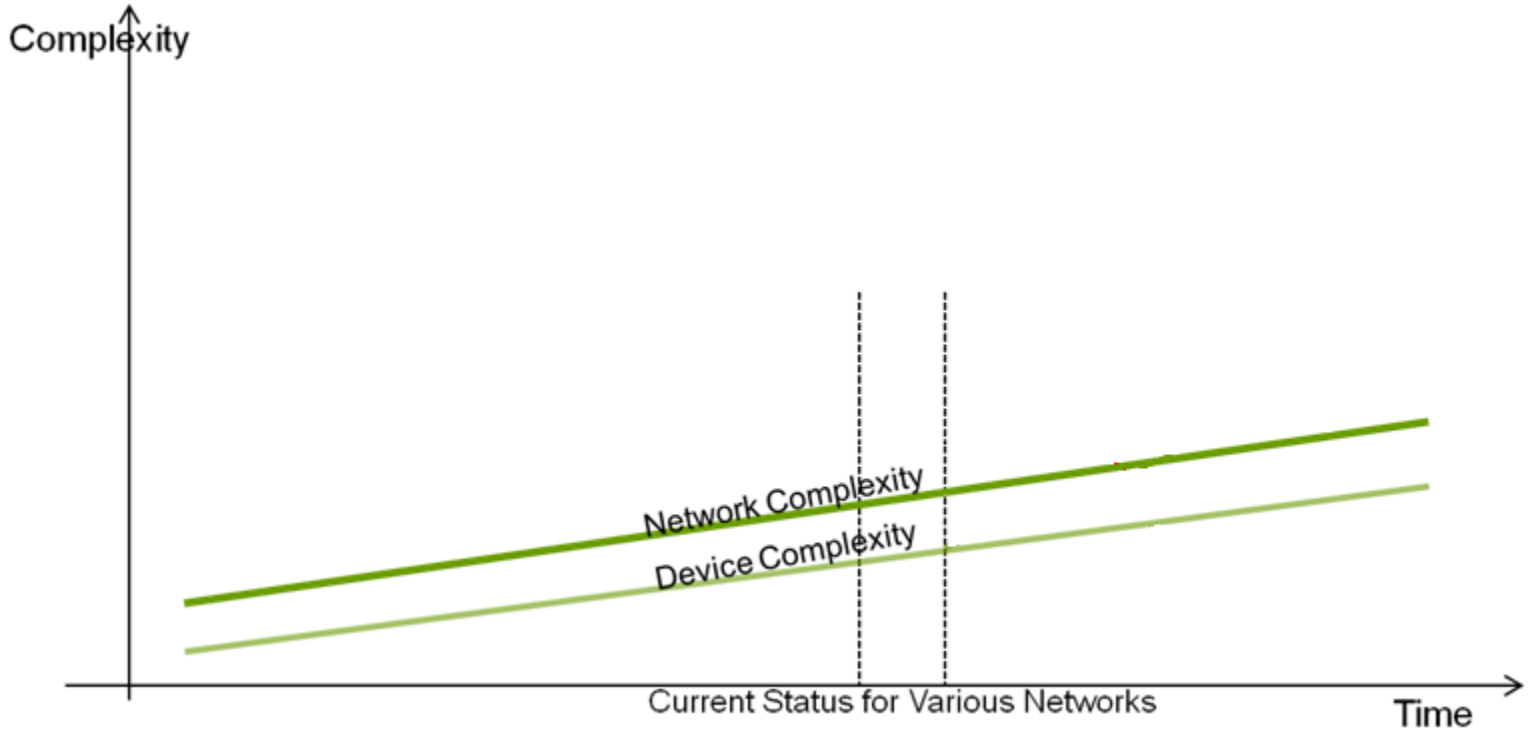
Using Cube to modelling network complexity is first mentioned by http://conferences.sigcomm.org/co-next/2009/workshops/rearch/papers/Behringer.pdf

- **Complexity can be diverted among network elements**
- **The total network complexity is the volume of three dimensions: complexity of operation/management, complexity of network device, and complexity of network planning**
- **The objective network is the easiest manageable by network operators**
- **The cost : Operation > device > network planning**

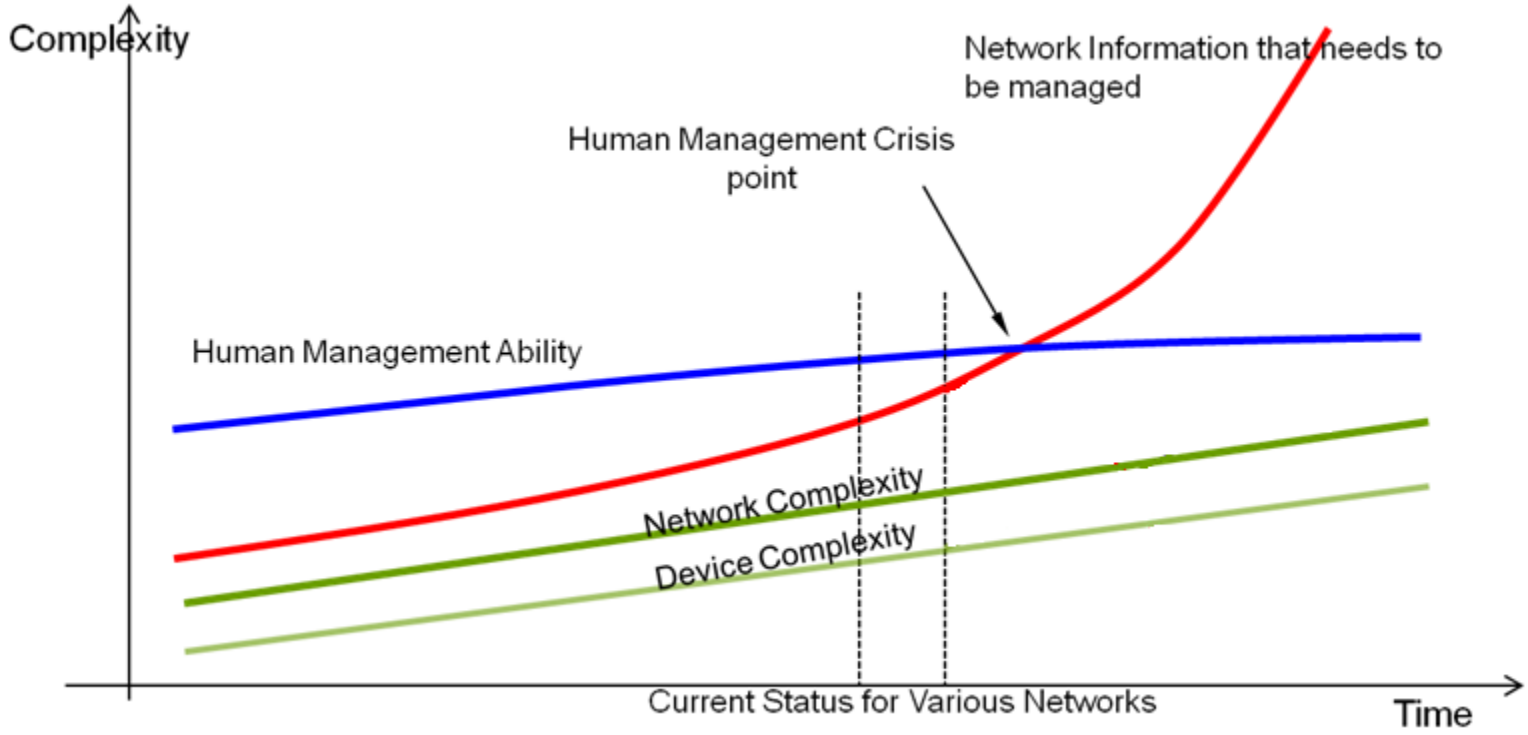
Content

- Direction of diverting network complexity
- **Practice scenario 1 – self-managed network**
- Practice scenario 2 – semantic prefix

Network Complexity leads to Self-management

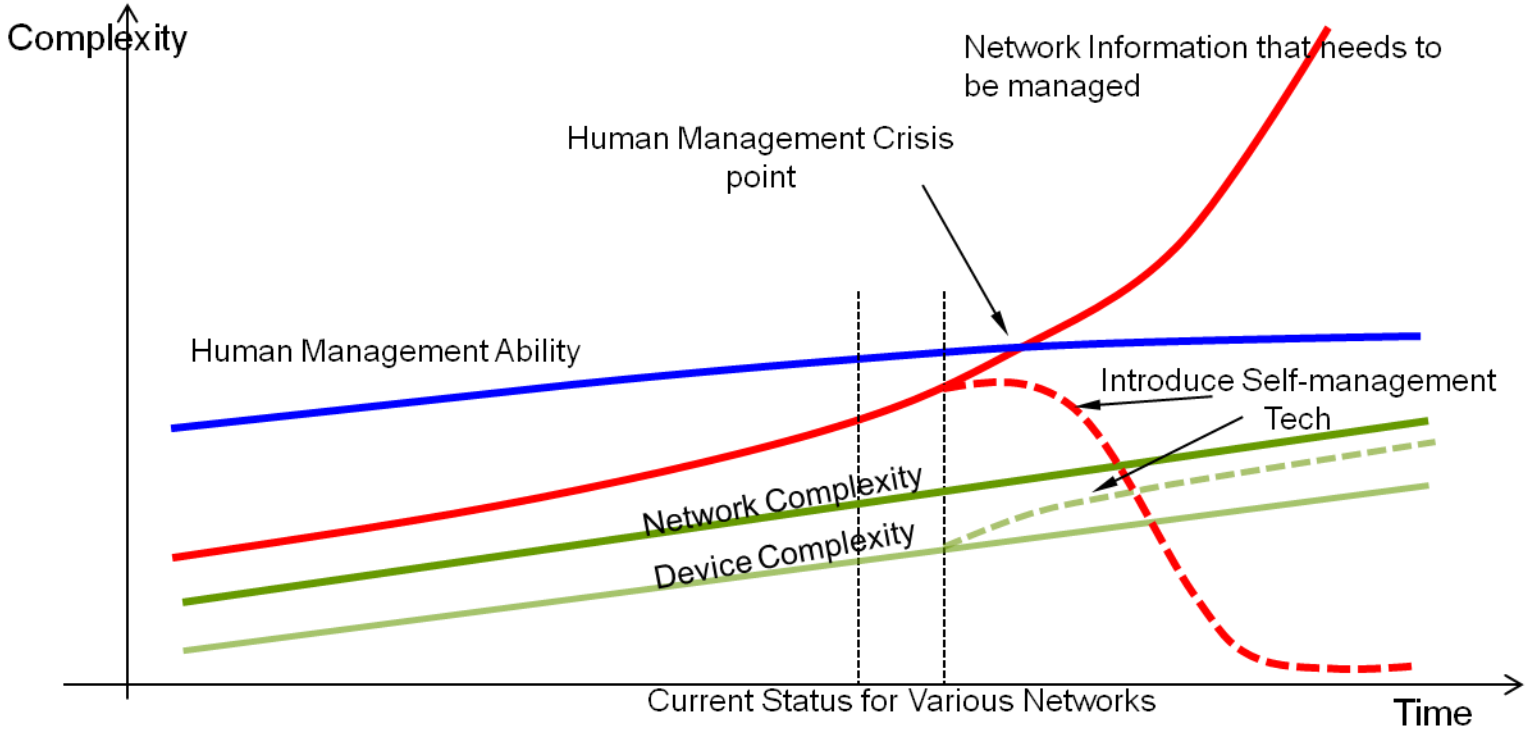


Network Complexity leads to Self-management



- **With more requirements of managing network and traffic in more details, the element for network management become more smaller. The management model nowadays could not manage the future networks anymore (including SDN). The crisis point become more nearer**

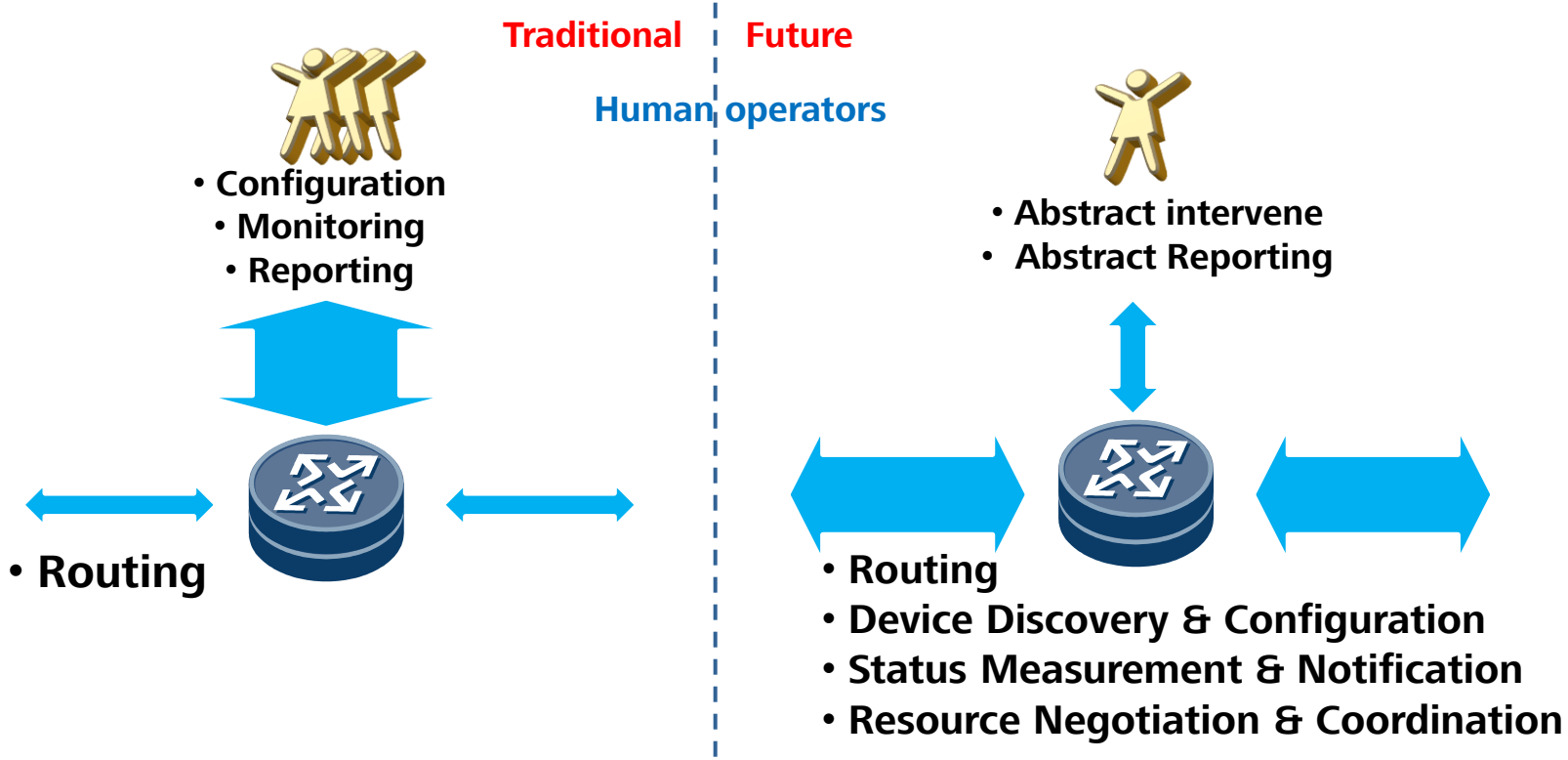
Network Complexity leads to Self-management



- **With more requirements of managing network and traffic in more details, the element for network management become more smaller. The management model nowadays could not manage the future networks anymore (including SDN). The crisis point become more nearer**
- **A more flexible, extensible and self-management system is urgent needed**
- **The completely automation of network could simplify the human management, reduce the human error and the cost of network maintenance**

Direction selection

- **Questions to be answered during coming years**
  - **Manual vs. Autonomic**
  - **Protocol vs. Architecture**
  - **Centralization vs. Distribution**



Modified from https://tnc2012.terena.org/core/presentation/47

Content

- Direction of diverting network complexity
- Practice scenario 1 – self-managed network
- **Practice scenario 2 – semantic prefix**

Requirements for Packet Semantic Awareness

Requirements

Network operators (both ISPs and enterprises) desire to be aware of more information about each packet

- so that packets can be treated differently and efficiently
- Packet-level differentiating can enable flow-level and user-level differentiating

Problematic Mechanisms

There are existing semantic mechanisms, but they are passive and indirection

- Deep Packet Inspection
- DiffServ Remark, etc.

- Many information is not expressed explicitly. Hence, it is difficult and costly for network operators to identify

Why IPv6 Prefix for Semantics

IPv6, with a large address space, allows semantics to be embedded into addresses

Routers can easily apply relevant operations accordingly

Untrusted choices:

interface identifier,

extension header, diffServ field, etc.

- Prefix is almost the only thing network operators can trust in IP packets
  - it is delegated by the network and the network can detect any undesired modifications, then filter the packet
  - if one get the destination address wrong, the packet would not reach; it get the source address wrong, the return packet would not arrive
  - It surely allows enterprise semantics to be able to traverse ISP networks

The Embedded Semantics

Too much embedded semantics is dangerous

- The more semantics embedded into prefix, the more complicated management could be. Also there are technical gaps to be filled
- It tries to push the problem to host OS and applications, but they are not ready to take it

Only most useful semantics can be embedded in the prefix

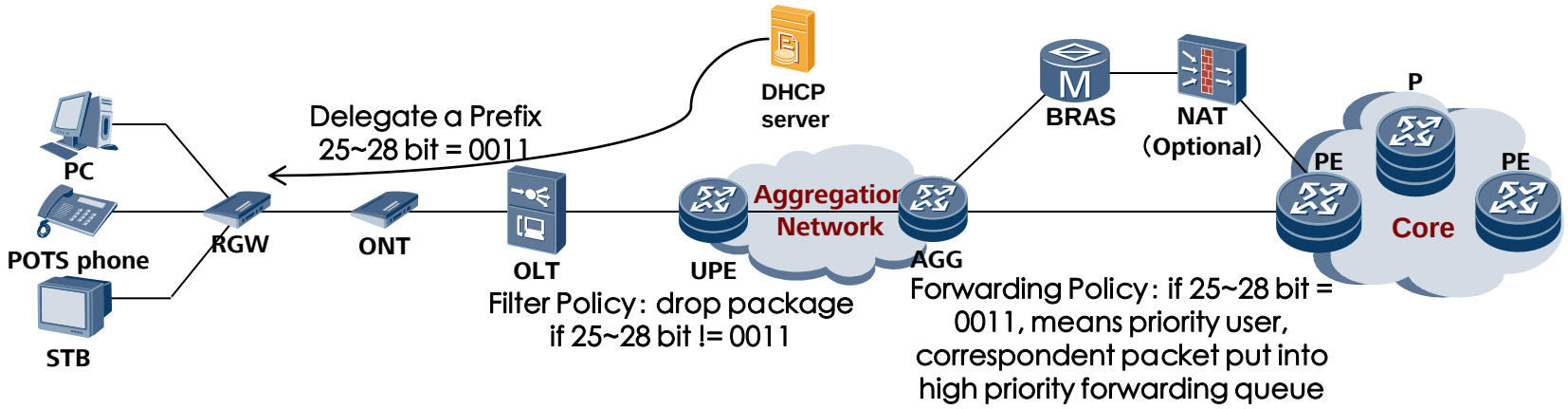
- it could be manageable if the semantics have been carefully restricted
- When used, all of semantic should be restricted in a highly abstracted way

Different operators have variable requirements for the most meaningful semantics

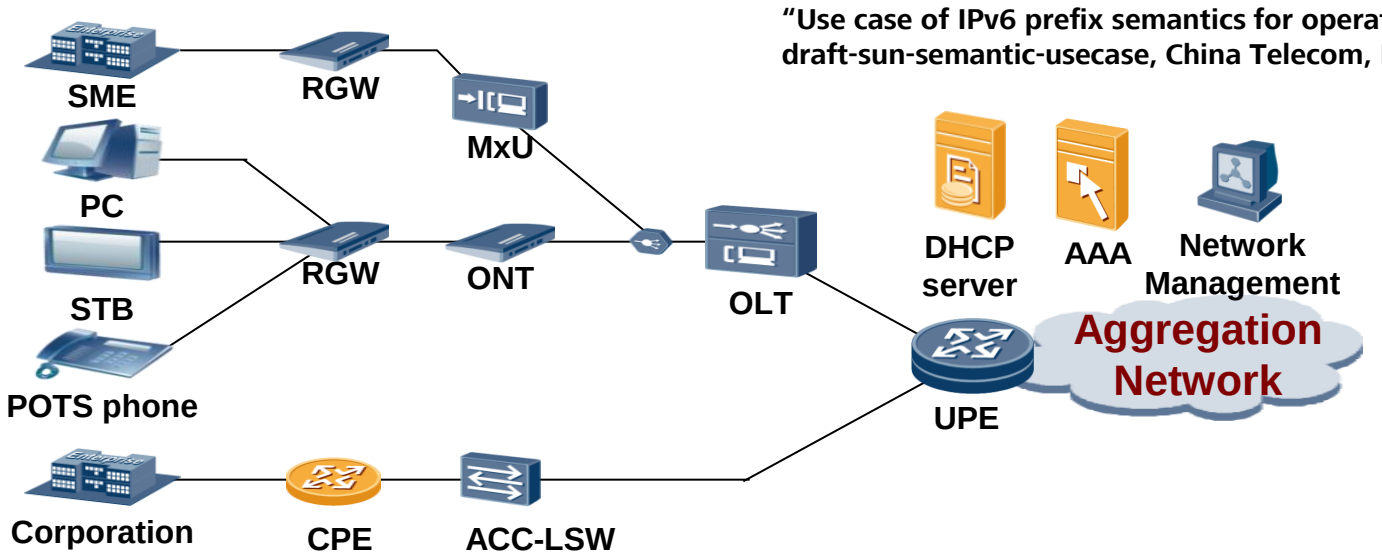
Semantic Prefix Technical Framework

- Network operator delegate prefixes with semantics
- Packets from Hosts have semantic prefix in source addresses
- Filters drop packets for any address spoofing attacks
- Forwarding policies can be easily applied according to semantics
- Security isolation can be naturally based on user/service semantics

A Framework for Semantic IPv6 Prefix and Gap Analysis
draft-jiang-v6ops-semantic-prefix, Huawei, China Telecom, Deutsche Telekom



ISP Use Case (User Type Semantic)



- Users are managed in different classes, such as broadband access subscriber (different priorities), mobile subscriber (different priorities), corporation subscribers, WiFi subscribers, special-secure-request users, etc.
- Each user class has been assigned a certain value in user semantic bits
  - For example, 25~28 bits are used as user semantic bits; 0000~0011 for broadband access subscriber with different priorities, 0100~0111 for mobile subscriber with different priorities, 1000~ 1010 for corporation subscribers, 1100~1110 for WiFi subscribers
- Policies based on distinguished user types can differentiate packets handling

Semantic Prefix Benefits

Depending on embedded semantics, various beneficial scenarios can be expected

1. Simplified measurement and statistics gathering
2. Simplified flow control
3. Service Segregation and User Segregation
4. Policy aggregation
5. Easy dynamic reconfiguration of semantic oriented policy
6. Application-aware routing
7. Easy user behavior management
8. Network resources access rights management
9. Easy virtualization

◆The above list are not all

Acknowledgement: the author was edified by Michael Behringer's previous work

Questions, clarifications?

Thanks!