NOKIA Bell Labs

Enforcing user's constraints in dynamic software-defined network of devices

APNOMS 2017 – Seoul, Korea

- P. Peloso, M. Boussard, D.T. Bui

- 28/09/2017

Outline

- Concept of SD-LANs
- Sharing policies
- DSL definition
- Handling algorithms
- Validation

Starting point: Intuitively organize connected life of users [securely]

Eg Organizing the connected home

SD-LANs to organize connected life locally

Cross-places SD-LANs to have interworking of remote devices (e.g. work from home, share media with friends)

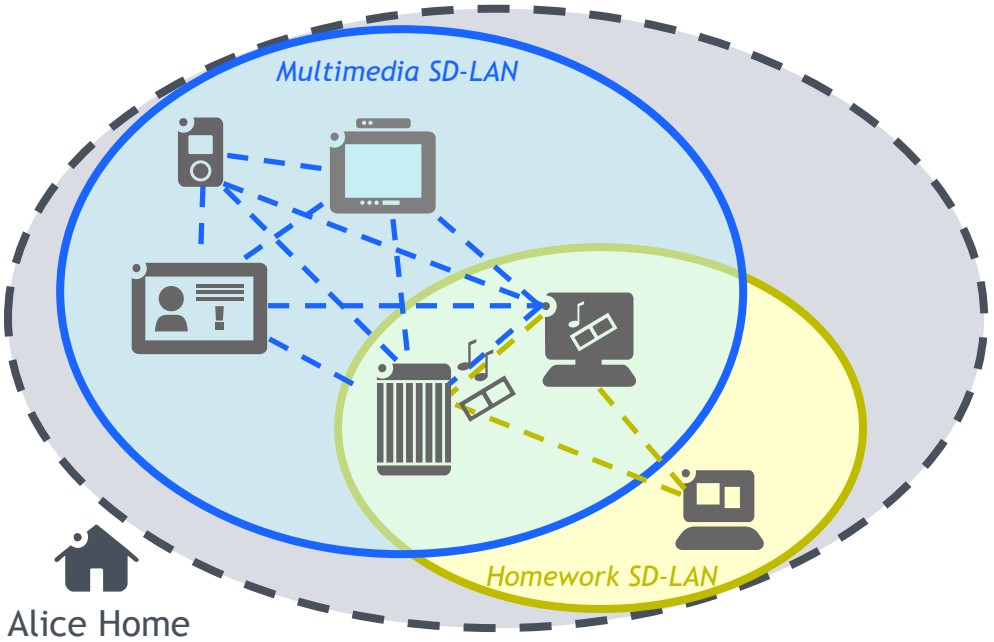
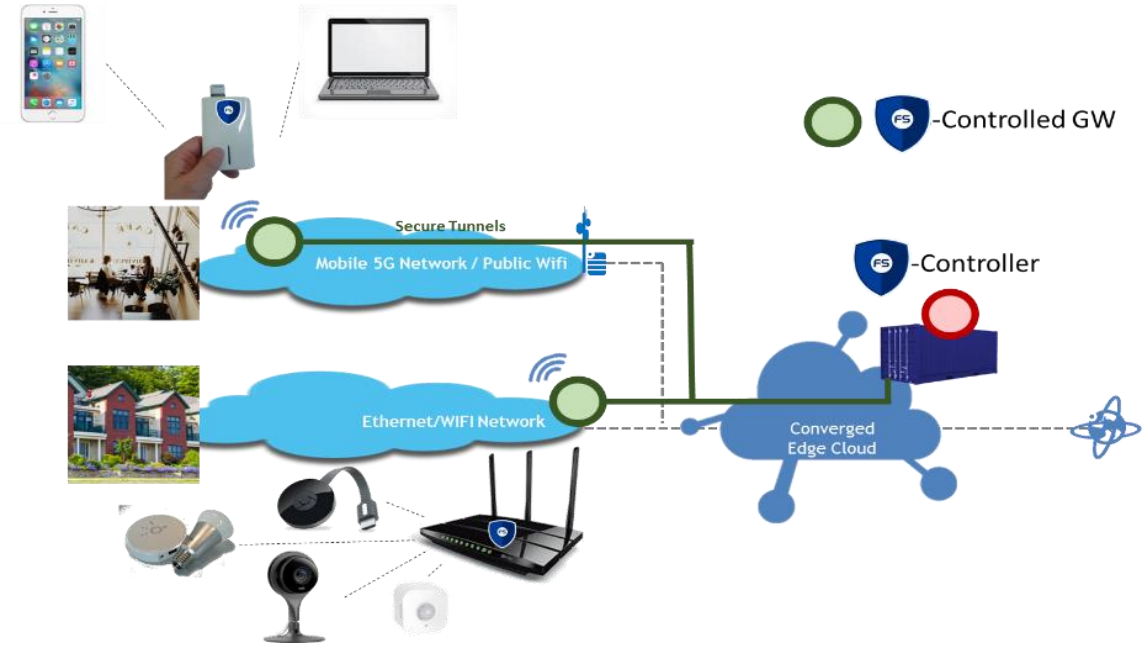


Illustration of implemented solution

Open-Flow in-house controller to config OVSs on edges



D. T. Bui, L. Ciavaglia, R. Douville, M. Le Pallec, N. Le Sauze, L. Noirie, S. Papillon, P. Peloso, F. Santoro M. Boussard, "Software-Defined LANs for Interconnected Smart Environments," in *27th International Teletraffic Congress (ITC 27)*, Ghent, Belgium, September 8, 2015.

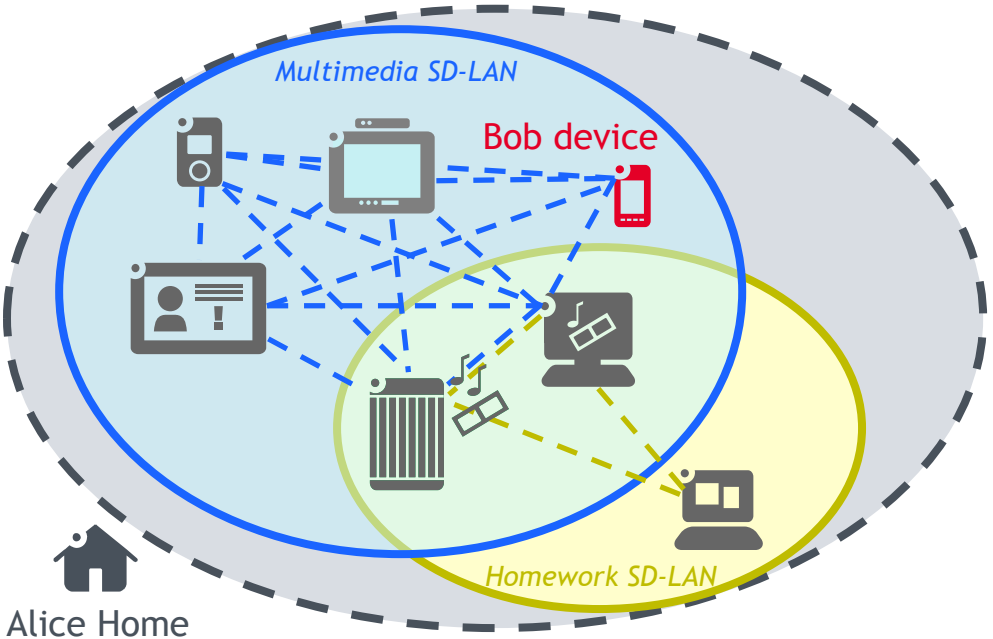
The root of the problem comes from user sharing their connected devices,

Each stakeholder having his own will

Building trust trough the concept of sharing policies

Human being expressed constraint:

This multimedia server cannot be used in a SD-LAN containing Resources not belonging to my home



Requirements regarding such policies

Machine readable rules

Hence need to compose a model and a language

Implicit needs to be made explicit

Permanently enforced rules

Hence, Written once, Evaluated often

Need to be evaluated under different circumstances

Cope with SD-LAN specificities

SD-LANs are bags of Resources, with evolving content

Do not endanger stability

No loops,

No conflicts

Then we'll take inspiration from PBNM where policies take the form of:

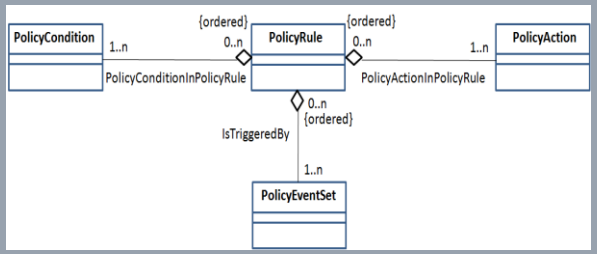
IF [Condition]

THEN EXECUTE [Action]

Need tailoring to address our use-cases

Defining a DSL for sharing policies,

And its model, specializing PBNM



Getting to understand the rules

Analyzing the example:

This multimedia server cannot be used in a SD-LAN containing Resources not belonging to my home

A subject to which the rule is defined

An action to apply to

This multimedia server must be excluded from SD-LANs containing Resources not belonging to my home

A set on which the condition is checked

Hence, gives

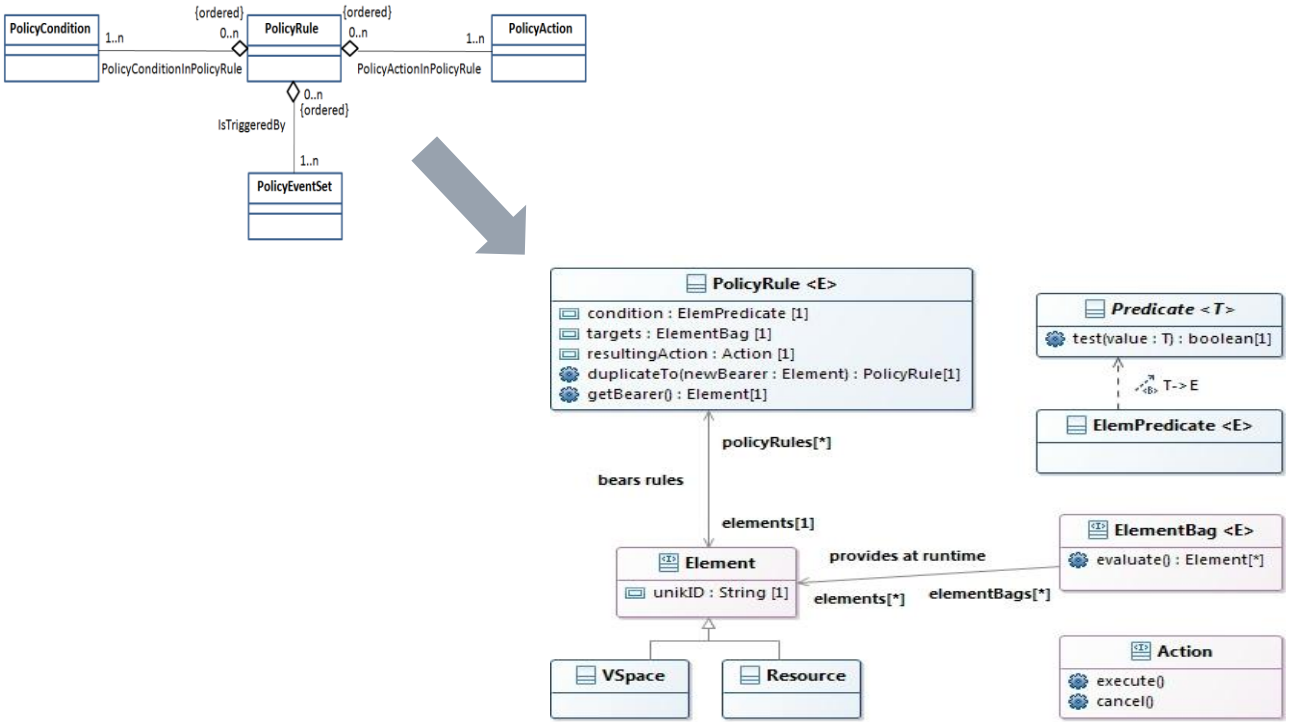
Sharing Policy attached to a Subject (SD-LANs or Resources):

A condition that triggers the rule

IF [Condition] APPLIES TO [Set of targets (either SD-LANs or Resources)]

THEN EXECUTE [Action]

Conclusions in terms of DSL model
Specialized PBNM policies Model into…



Conclusions in terms of DSL model
Specializations

1. Policy Event trigger

   Always is: When a Resource enters a SD-LAN (following a control action)

2. Policy Repository

   Borne by the SD-LAN agent or the Resource Agent => Hence highly distributed policies

   From there comes the handling and transformation algorithms

3. ElementBag

   In our model the element that ensures Written Once – Evaluated Often

   Conditions and Actions rely on ElementBags to achieve the above

4. Multi-tenants context

   Rules may be provided in an inconsistent manner

   Inherent problem is conflicts => Solution resides in avoiding conflicts / cascade **by design**

   1.Stackable actions – not contradictory

   2.Separation between rule conditions space and rule actions space

5. System relying on a split between composition and connectivity

   Each is a logical layer

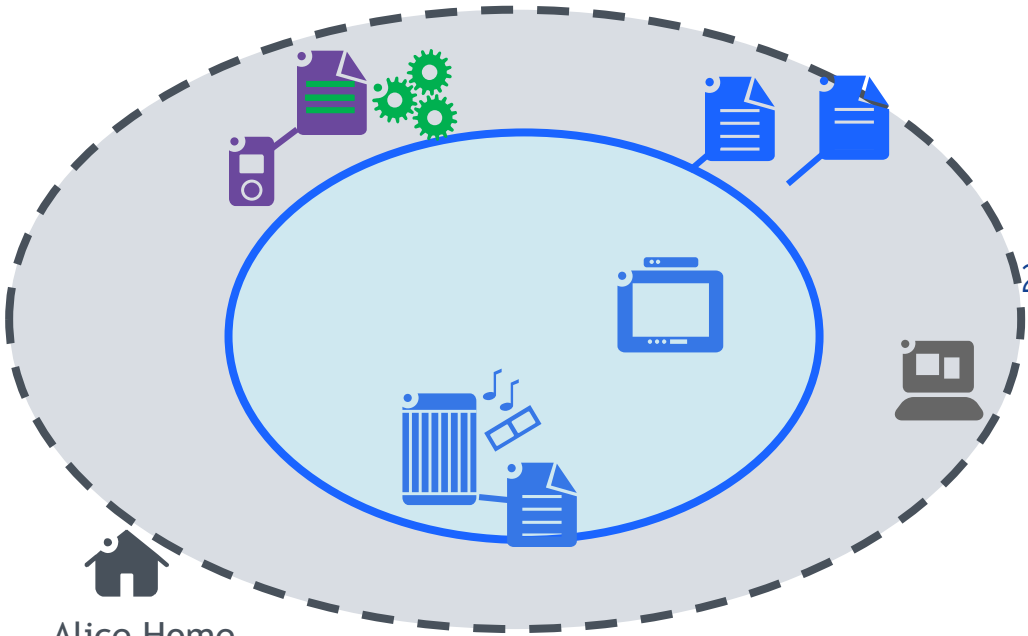
   - Rule conditions tested on the composition layer
   - Rules actions executed on the connectivity layer

Enforcing the policies,
to achieve stackholders trust

Entrance Algorithm

Executed when a Resource enters a SD-LAN

: List of Rules

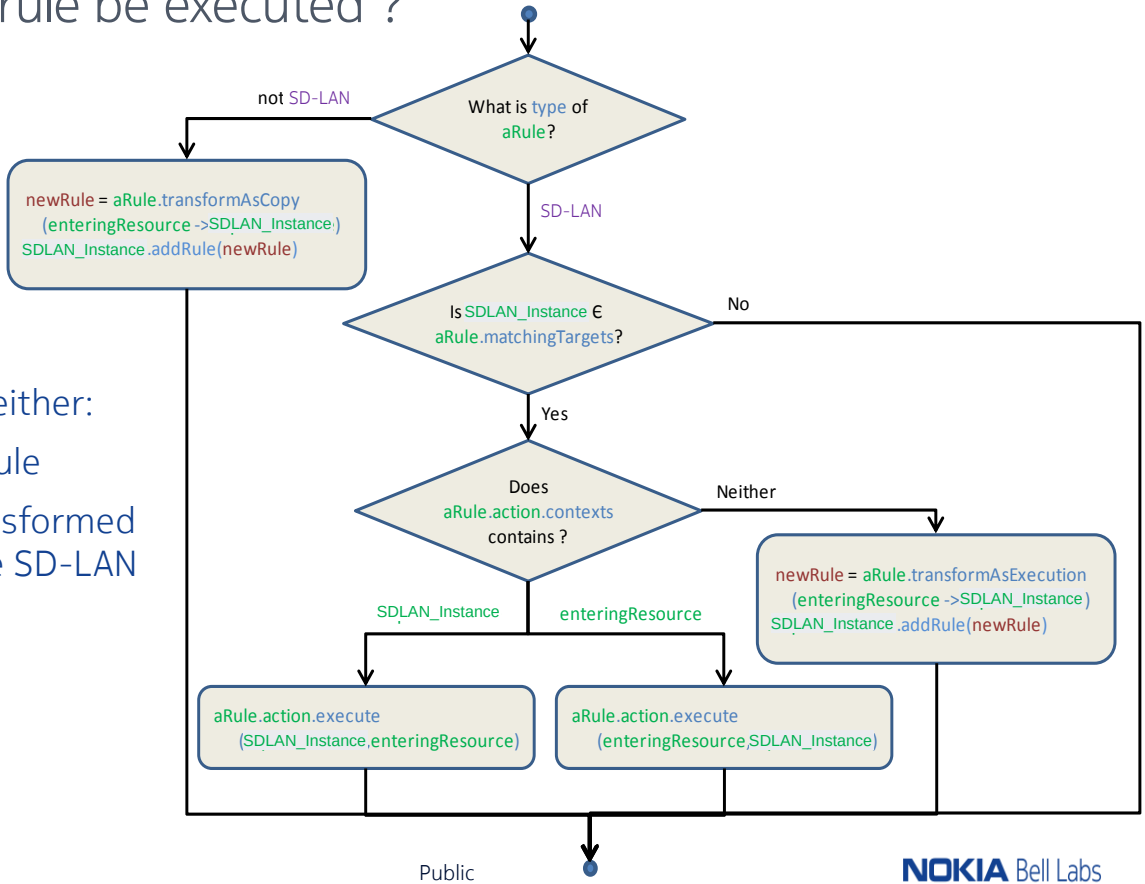


1. Parse all the rules from the Resource, and for each, either:
   - Execute the rule
   - Copy the transformed rule to the SD-LAN
   - Do nothing
2. Parse all the rules from the SD-LAN, and for each, either:
   - Execute the rule
   - Copy the transformed rule to the Resource
   - Do nothing

Rule handling Algorithm
Should a rule be executed ?

Outcomes are either:

- Execute the rule
- Copy the transformed rule to the SD-LAN
- Do nothing



Rule transforming Algorithm
How copying a rule from Resource to SD-LAN

Sharing policy attached to a Resource

IF [Condition] APPLIES TO
[Set of targets (either SD-LANs or Resources)]
THEN EXECUTE [Action]

to

Sharing policy attached to a SD-LAN

IF [Condition] APPLIES TO
[Set of targets (either SD-LANs or Resources)]
THEN EXECUTE [Action]

Basically, Sets of targets are the ones impacted by changes

This multimedia server must be excluded from SD-LANs containing Resources not belonging to my home

to

The rule provider must be excluded from Me if I contain Resources not belonging to the rule provider home

Relies on transformation algorithm

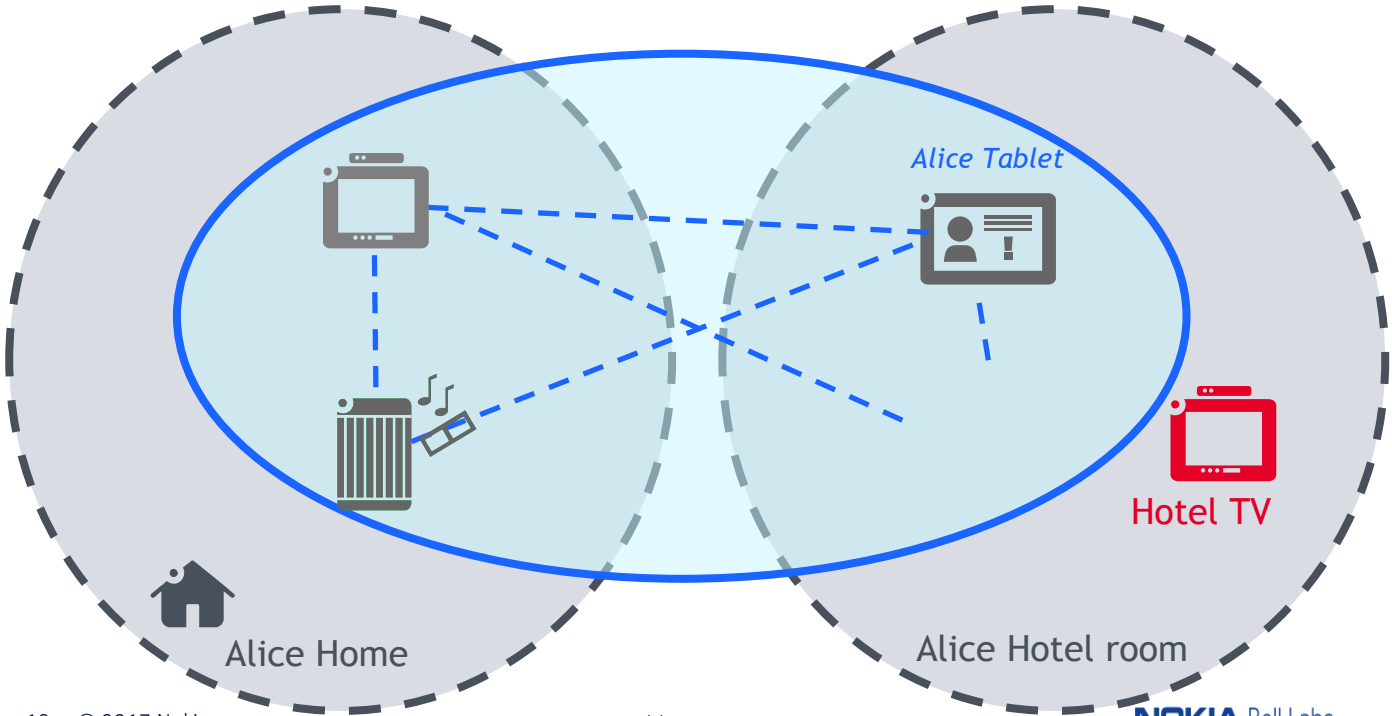
Validation,

Through test bed result in a 2 places scenario

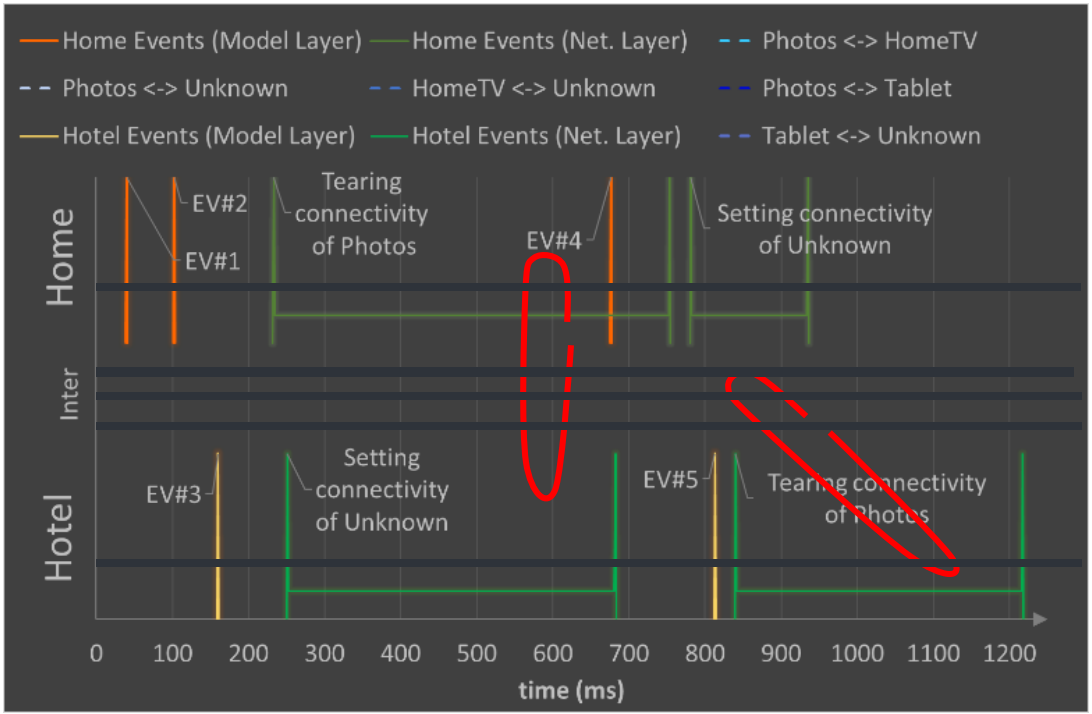
Evaluation of policy in a multi-place scenario

Human being expressed constraint:

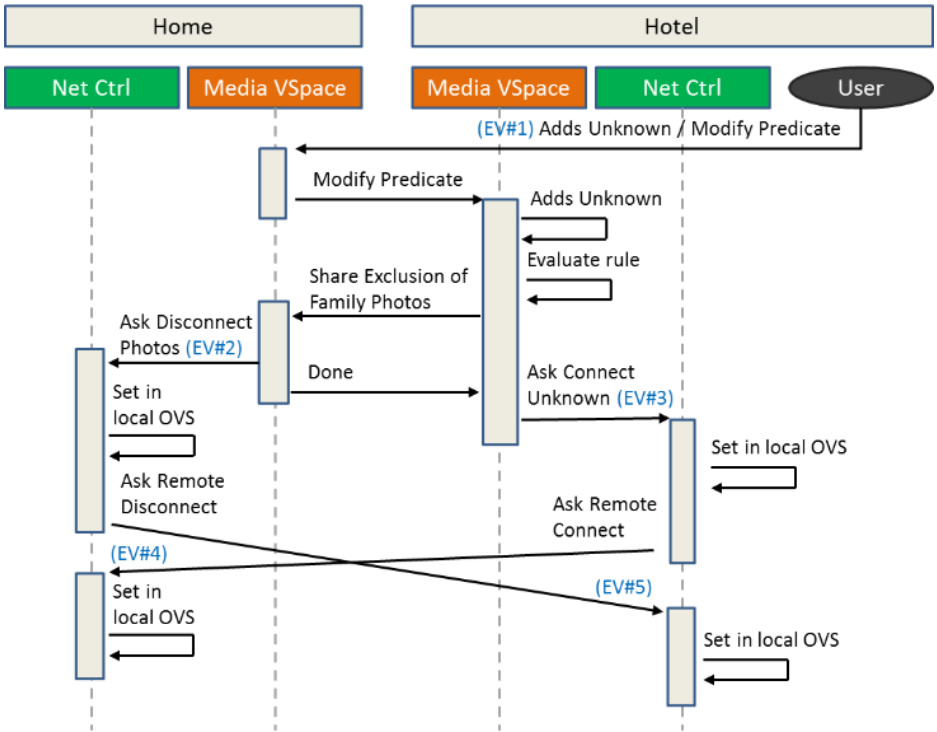
This photo server cannot be used in a SD-LAN containing Resources not belonging to my home



Test results for a dual locations SD-LAN



Test results for a dual locations SD-LAN
Corresponding Sequence Diagram



Conclusions

Provided

- Policy definition language/model for safe sharing of devices in multi-tenants contexts
- Algorithms to handle these policies

Embedded and demonstrated

- Through our test-bed facility

Next steps

- Validate on bigger setup

NOKIA