Provisioning and Operation of Virtual Networks

KIVS 2011 Workshop on Network Virtualization

Sebastian Meier
sebastian.meier@ikr.uni-stuttgart.de
10.03.2011

Universität Stuttgart
Institute of Communication Networks
and Computer Engineering (IKR)
Prof. Dr.-Ing. Andreas Kirstädter

Outline

What is Network Virtualization?

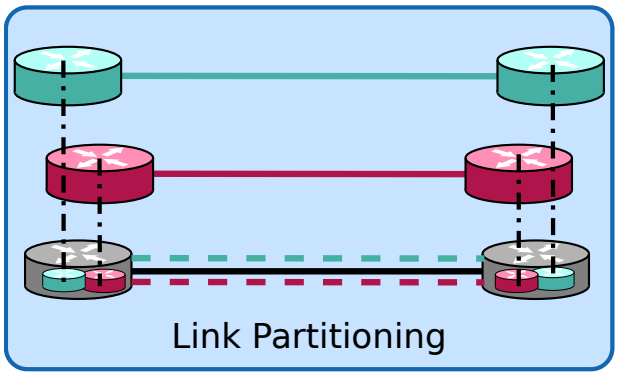
Network Virtualization

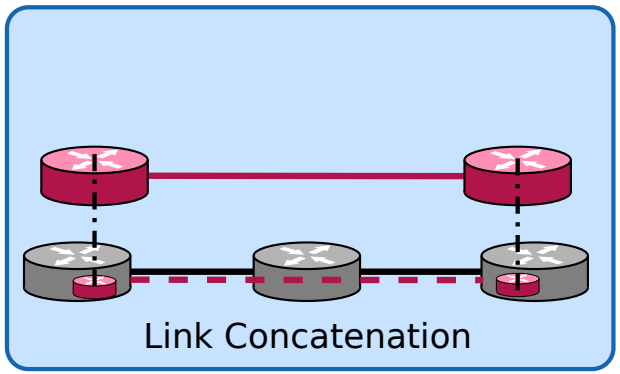
Network	Nodes + Links
Virtual Network	Virtual Nodes + Virtual Links

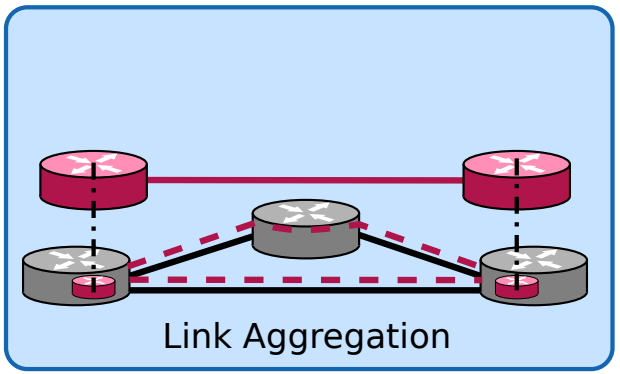
Our View on Virtual Links

- May abstract from physical topology and characteristics
- Can share physical resources with other virtual links

Examples for Virtual Links







What is Network Virtualization?

Network Virtualization

Network	Nodes + Links
Virtual Network	Virtual Nodes + Virtual Links

Views on Virtual Nodes

- Network centric view — virtual node performs routing and switching
- IT centric view — virtual node provides computing or storage resources

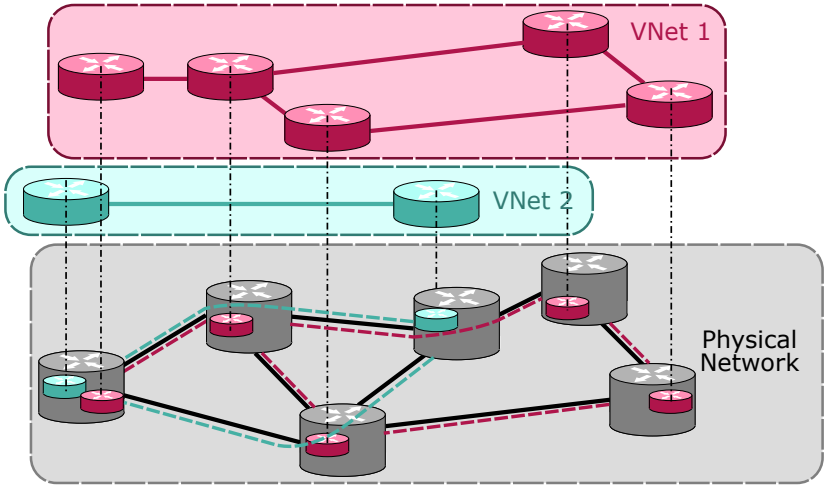
Both views have to be well understood

- Identify similarities and differences
- Identify common mechanisms and interfaces for provisioning and management

What offers Network Virtualization?

Abstraction

- From physical topology
- From technology in physical layer



Isolation

- Own address space, protocol stack, routing
- QoS guarantees (e.g. delay, bandwidth, ...)

Cost Efficiency

- "On-Demand" provisioning of virtual networks
- Consolidation, e.g. multiple virtual servers on shared physical server

  → Economy of scale

What offers Network Virtualization?

New Role Model (Based on 4WARD Role Model)

- Traditionally Internet Service Provider (ISP) owns and operates the network
- Virtualization separates network operation from infrastructure administration

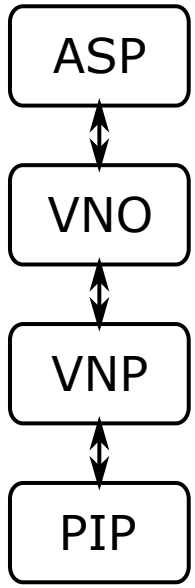
ISP

Virtual Network Operator (VNO)

- Administrates enabler services (e.g. Routing, DNS)
- Controls and monitors virtual network

Phyical Infrastructure Provider (PIP)

- Owns physical infrastructure
- Offers virtual resources hosted by physical resources
- May specialize on certain resource types



- Mapping of virtual network to resources of PIPs is difficult
  → Additional Role: Virtual Network Provider (VNP)
- New services might require expert knowledge for operation
  → Additional Role: Application Service Provider (ASP)

Role Interaction

Virtual Network Provisioning

- Focus on creation of virtual network
- Negotiation between VNO, VNP and PIP
- Requires interfaces to request, interconnect and manage virtual resources

→ Addressed by a couple of projects

Our focus: Operation of Carrier Grade Virtual Networks

- Adjustment of existing virtual networks
- Optimization of mapping between virtual and physical resources
- Error handling
- Proactive network adjustments

→ Reuse and refine existing provisioning interfaces

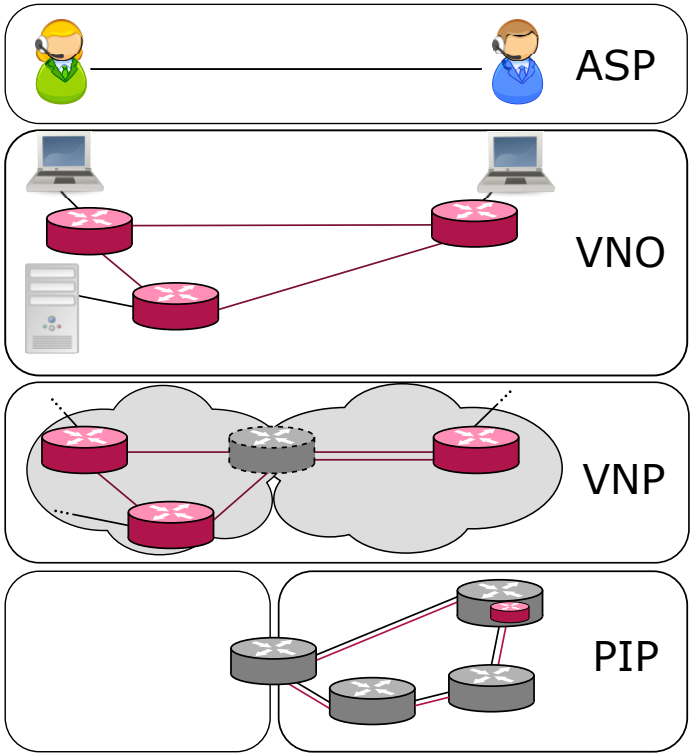
→ Define additional role interactions and interfaces if required

Virtual Network Operation

Indirection and Abstraction

- Each role may introduce abstractions
- Each role may have its own view
- Virtual Network Operation requires interaction between different roles

→ Mapping of abstract views is required



Example on Different Views

ASP users, end-to-end delay, buffer fill levels, ...

VNO addresses, routing settings, link utilization, ...

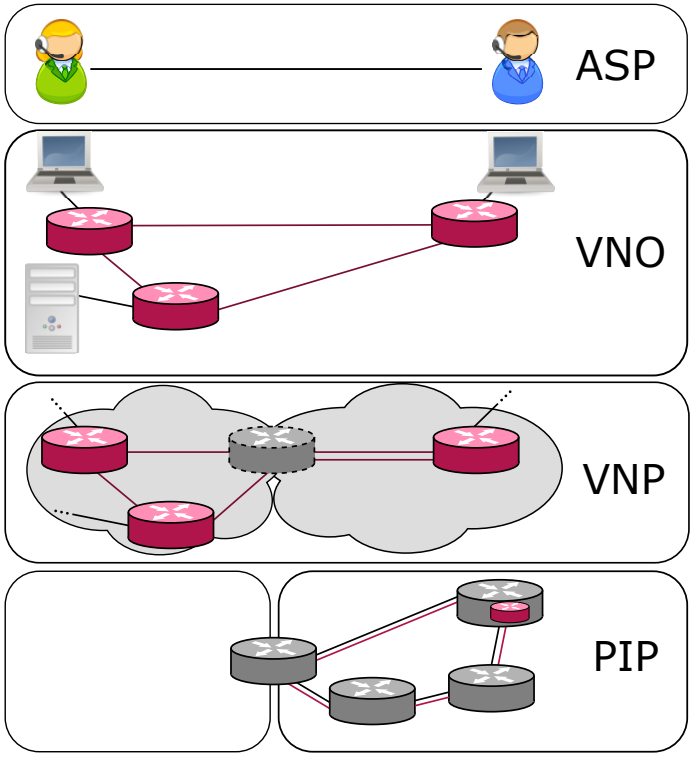
VNP composition of virtual network

PIP mapping of virtual to physical resources,
detailed information on physical resources in own domain

Mapping of different abstract views is challenging

Virtual Network Operation

Example for Mapping of Abstract Views



- Identification of entities
  - ASP users (user clients), servers
  - VNO IP addresses

  → Mapping required
- Identification of (mis)behaviour
  - ASP
    - observes a symptom (e.g. video buffer low)
    - may only guess cause (e.g. insufficient bandwidth)
  - VNO
    - observes underlying cause (e.g. fully loaded link)
    - must be able to relate cause to a symptom
      (e.g. a fully loaded link may be fine for some services, but a problem for others)

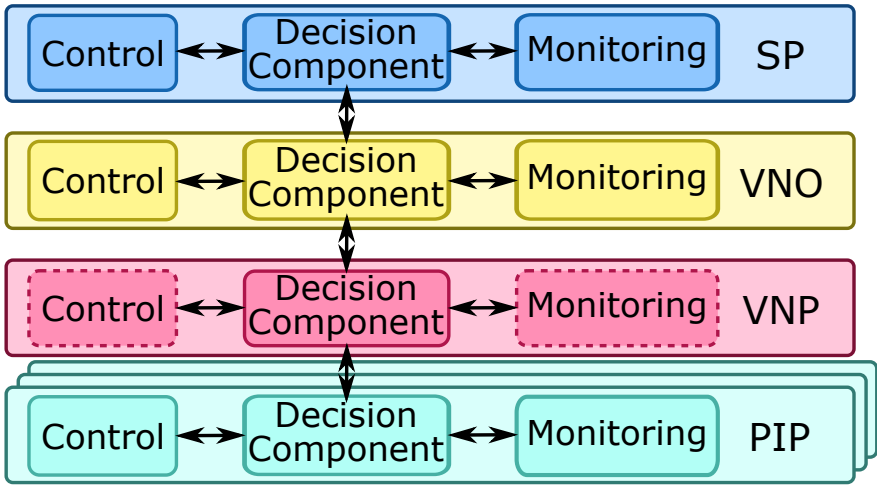
→ Typical and problematic characteristics have to be known across roles

→ Characteristics have to be specified by overlying role

Control and Monitoring Patterns

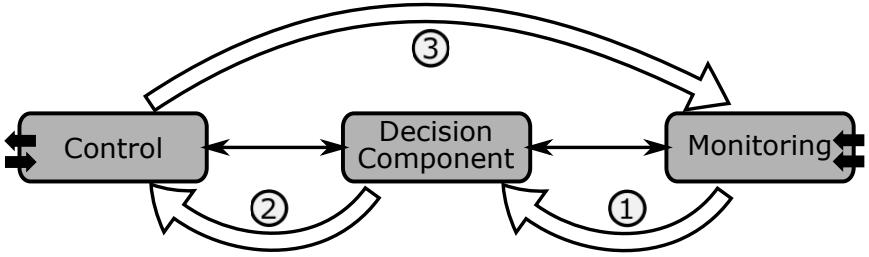
Horizontal Control Loops

- Monitoring supervises functionality provided by role
- Decision component (DC)
  - is informed by monitoring of current state
  - decides whether adjustments are required
  - decides whether adjustment can be done within role
- Control carries out adjustments



Example for Horizontal Control Loop in PIP

- Monitoring detects increasing bit error rate on interface of physical node
- DC decides to relocate virtual paths using affected interface
- Control triggers signaling to relocate virtual paths



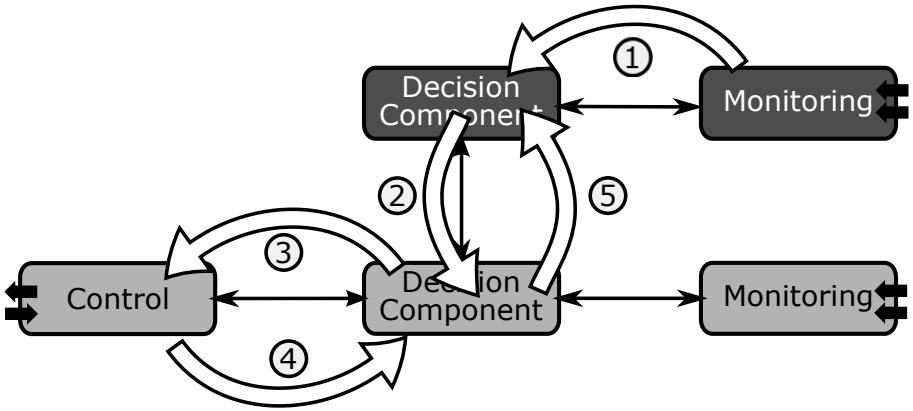
Control and Monitoring Patterns

Vertical Control Loops

- Vertical Control loops are used for interaction between adjacent role
- For example, interactions might be necessary for
  - problem escalation
  - proactive adjustments
- DC is responsible for mapping between different views when interacting

Example for Vertical Control Loop between ASP and VNO

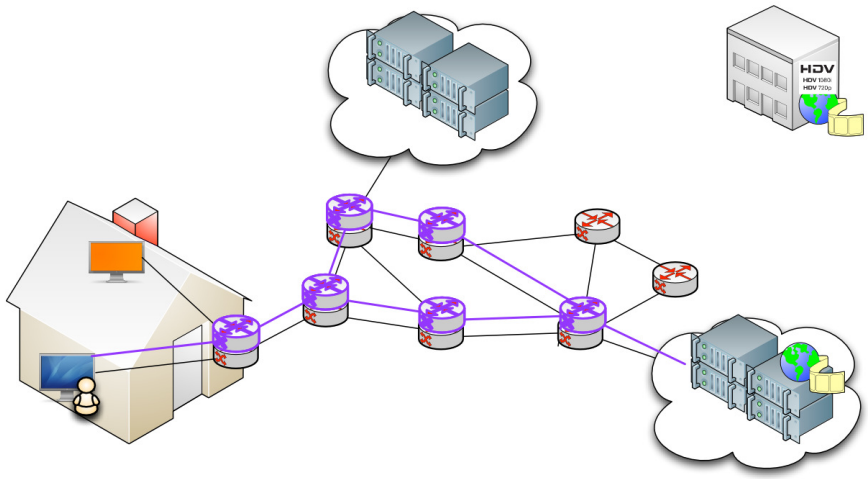
1. Monitoring in ASP detects high end-to-end delay
2. DC of ASP reports problem to DC of VNO
3. DC of VNO tries to solve problem by route optimization
4. Control is triggered to adjust routing
5. Result is reported to ASP's DC



Demonstrator Implementation

Demo Scenario: Video Streaming Service

- Focus
  - Application and network operation
  - Interaction between application and network
- Simplifications
  - role model (combine ASP+VNO, VNP+PIP)
  - single domain scenario



- Application
  HD Video streaming using scalable video codec
- Network
  IPv4 Network operated via Generalized Multi-Protocol Label Switching (GMPLS)

GMPLS Control Plane

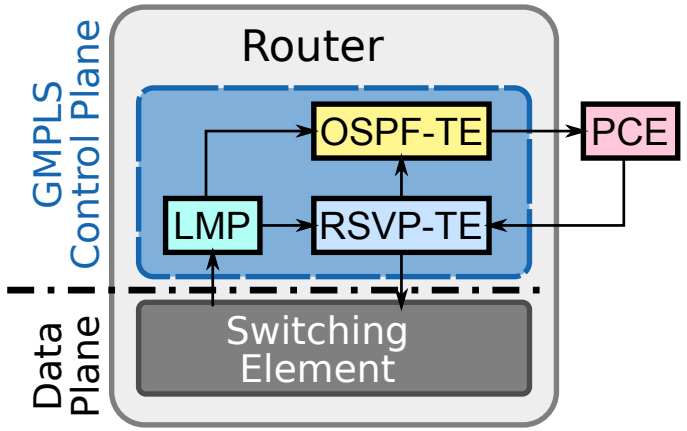
Overview

Motivation for Control Plane Usage

- Complexity of today's and future networks calls for control plane assisted management
- Dynamic modifications to virtual networks require automation to some extent

Generalized Multi-Protocol Label Switching (GMPLS)

- Technology independent framework for network control
- Relies on protocols standardized by IETF



GMPLS Components

- LMP (Link Management Protocol)
  Discovers adjacencies on data and control plane
- OSPF-TE (Open Shortest Path First)
  Disseminates network topology and traffic engineering information
- PCE (Path Computation Element)
  Performs constraint based path computation
- RSVP-TE (Resource Reservation Protocol)
  Signals path requests and configures switching elements

GMPLS Control Plane

Virtualization Extensions

Why GMPLS?

- Components are well standardized and quite matured
- Supports computation, and signaling of Label Switched Paths (LSP)

→ LSP is quite similar to a virtual link!

→ Reuse existing parts, extend missing components for network virtualization

Towards a Virtualization Enabled GMPLS Control Plane

- Open source GMPLS implementation required for extension
  - No up-to-date implementation for signaling protocol RSVP-TE
  - No implementation for path computation element (PCE)
- We implement missing components based on RFCs
- Status of the implementation
  - RSVP-TE is almost complete
  - PCE implementation started last month

The COMCON Consortium

COMCON – COntrol and Monitoring of COexisting Networks

- Consortium of G-Lab Phase 2
- 5 partners from industry and academia

Excerpt of Current Topics

• DOCOMO	Mapping of reference architecture on Next Mobile Network
• Infosim	Definition of monitoring architecture for virtual networks
• NSN	Analysis of combined resource management and control of IT and network resources
• Universität Stuttgart	Fixed core network control plane
• Universität Würzburg	Monitoring for multi-path scalable video codec transmission

Conclusion and Outlook

Conclusion

- Indirection and abstraction is a major challenge for operation of virtual networks
- In error cases even simple problems might be difficult to resolve
- Typical and problematic characteristics have to be known across roles

Outlook

- Implement Demonstrator for simple scenario
- Extend GMPLS for network virtualization
- Evaluate interaction between different roles for selected scenarios