LANCASTER
UNIVERSITY
Computing
Department

Network Virtualization

Prof. Laurent Mathy

Lancaster University, UK

Overview

- Definitions
- Network virtualization technologies
  - VLANs
  - VPNs
    - Route filtering
    - Tunneling
    - Logical routers
  - Virtual routers
  - Programmable virtual routers

overview

- Virtual networks
  - Motivations
  - Principles
  - Architecture
  - Migration
- Server virtualization
  - Full-virtualization
  - Paravirtualization
  - Container-based virtualization
- Building vrouters

Definitions

- Network [New Oxford American Dictionary]
  - a group or system of interconnected people or things
    - a number of interconnected computers, machines, or operations
- I prefer
  - A group of interconnected entities that communicate through some predefined method

Definitions

- So a network is, in our case, a set of (interconnected) devices that can communicate with each other by using some protocols

Definitions

- Virtualization [New Oxford American Dictionary]
  - The act of virtualizing
- Virtualize
  - convert (something) to a computer-generated simulation of reality
- Virtual [New Oxford American Dictionary]
  - (Computing) not physically existing as such but made by software to appear to do so

Definitions

- These are very general definitions
  - A PDF file can be said to be a virtual document
  - My Mii is a virtual Me
  - Mr Potato Head is a virtual character (in the movie "Toy Story")
  - Mr Potato Head is not a virtual character (in toy shop)
  - A program addressing space is virtual
  - A harddrive partition is virtual
  - TCP connection to Google is virtual

Definitions

- We are kind of in trouble, let's try something else
- Virtual [New Hacker's Dictionary]
  - [via the technical term `virtual memory', prob. from the term `virtual image' in optics] 1. Common alternative to logical; often used to refer to the artificial objects (like addressable virtual memory larger than physical memory) simulated by a computer system as a convenient way to manage access to shared resources. 2. Simulated; performing the functions of something that isn't really there. An imaginative child's doll may be a virtual playmate. Oppose real.

Definitions

- Definition 1 helps
  - A virtual object is simulated and shares resources (with other virtual objects, presumably)
  - Virtual networks will share a common infrastructure
  - Virtual resource constructed as logical partitioning of underlying common shared resource
    - As opposed to separate dedicated physical resource

Definitions

- Notice how the shared resource could be virtual
  - virtual resources can be further virtualized
  - “recursion” is possible
- The Internet already has many virtual links
  - Many L2 links in internet are build as leased links across shared common transmission bearer service (often telephone company)
    - These L2 links are virtual, but from L3 perspective the Internet is a separate network
      - Layering changes the perspective!

Definition

- The sharing is done for cost reasons, mainly
- From the client perspective, the virtual resource should have some form of isolation from other virtual resources
  - It is that “level” of isolation that is central to the different approaches to virtualization
    - What is being isolated and to what extend

Network virtualization Technologies

- We present a (brief) overview of (some) network virtualization technologies
  - While all of these fall under the umbrella term "network virtualization", the goal is to fix ideas as to
    - What is virtualized
    - The type of isolation provided

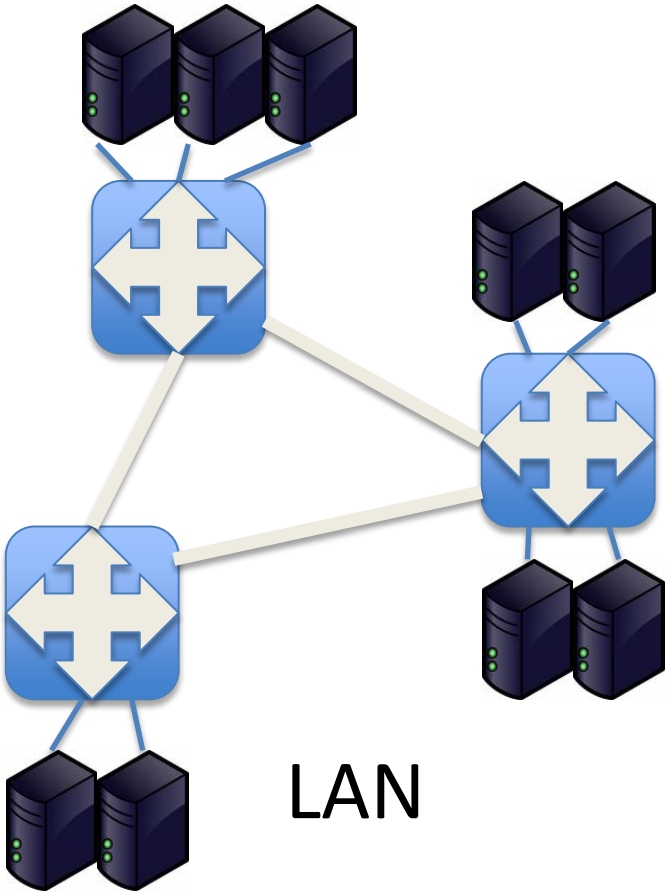
Overview

- Definitions
- Network virtualization technologies
  - VLANs
  - VPNs
    - Route filtering
    - Tunneling
    - Logical routers
  - Virtual routers
  - Programmable virtual routers

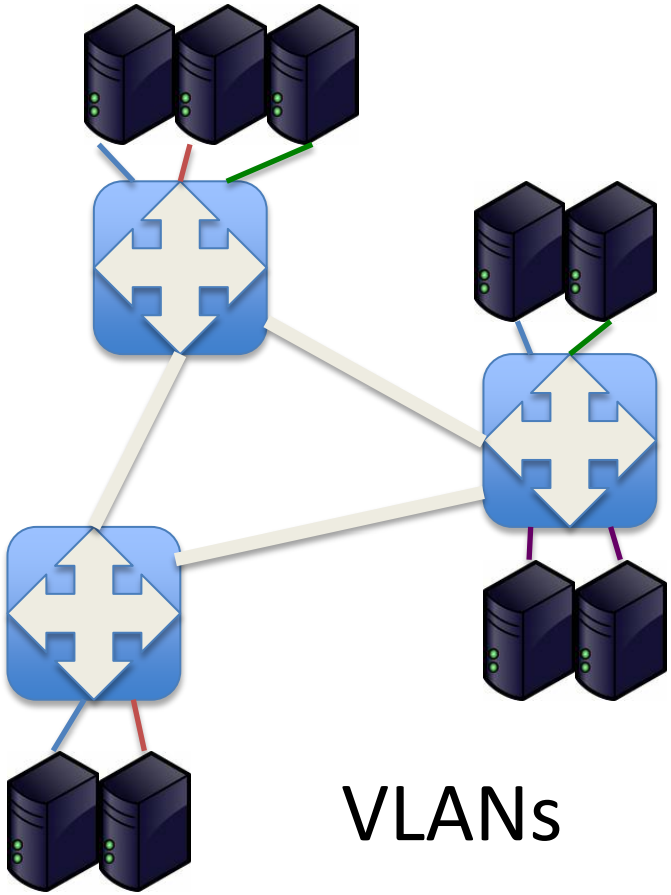
Virtual LAN

- Layer 2 virtualization technology
- Virtualizes physical LANs
  - Creates groups of hosts that communicate as if on same broadcast domain, regardless of physical location
  - A VLAN behaves as a physical LAN

Virtual LAN

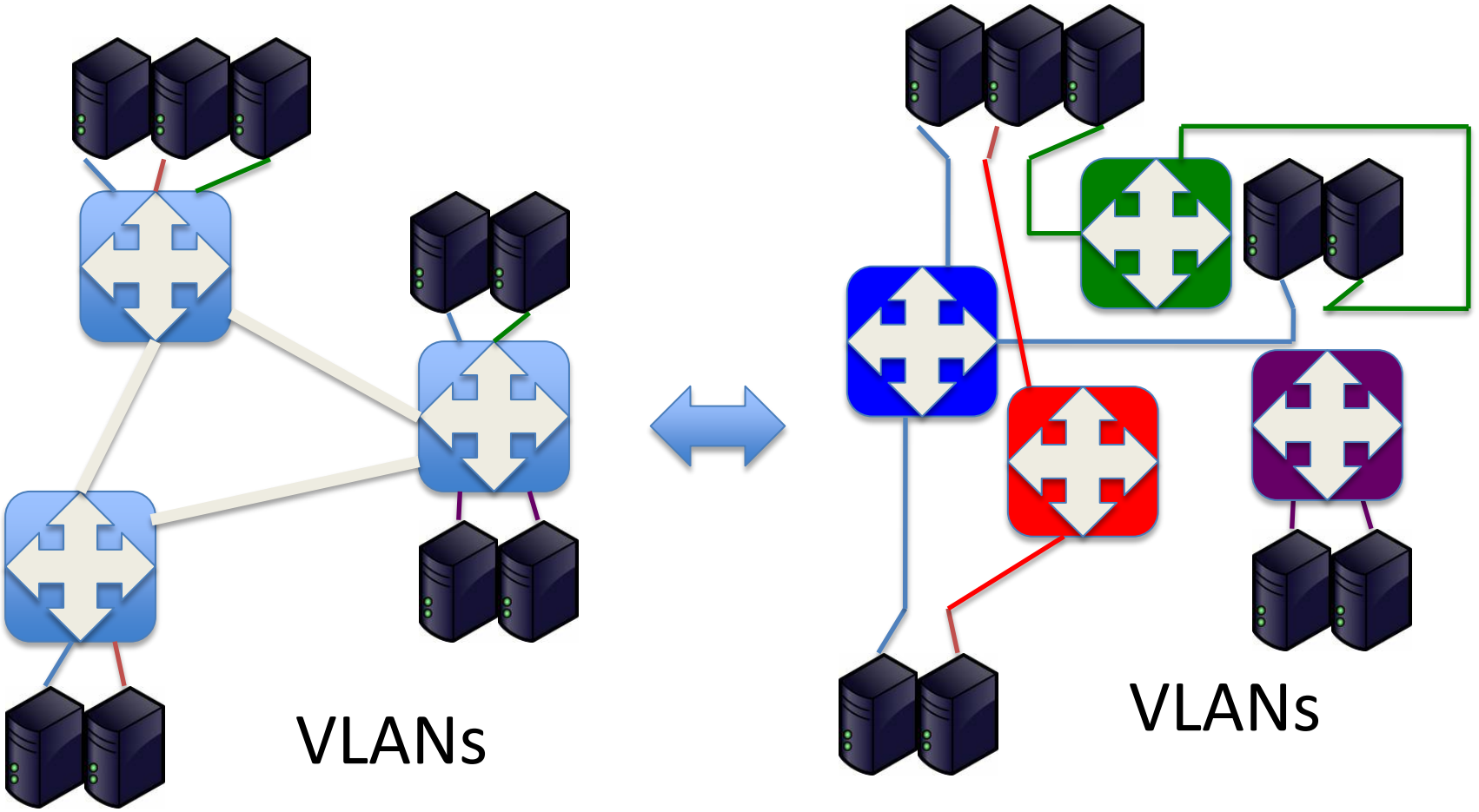


LAN



VLANs

Virtual LAN



Virtual LAN

- Virtualization realized by frame colouring
  - 4-byte tag added to Ethernet frame
  - Colouring usually done on a port-by-port basis
- Isolation of “broadcast domain”
  - Traffic isolation at layer 2
    - E.g. blue LAN isolated from red LAN

Virtual LAN

- Why?
  - Decoupling of physical/geographical position and LAN assignment
  - Improved security by traffic segregation
    - Interconnection through routers (L3)
  - Better bandwidth utilization
  - Flexibility at low cost

Overview

- Definitions
- Network virtualization technologies
  - VLANs
  - VPNs
    - Route filtering
    - Tunneling
    - Logical routers
  - Virtual routers
  - Programmable virtual routers

VPN

- Virtual Private Network
  - Private [New Oxford American Dictionary]
    - belonging to or for the use of one particular person or group of people [or things] only
  - Devices not participating in the private network are not aware of it and cannot access the private content
    - A VLAN is a layer 2 virtual private network
    - There are very many different types of VPNs and VPN technology
      - At all layers of communication

VPN

- VPN is an umbrella term
  - Encompasses so many different techniques, technologies and terms that you can easily get very confused
    - All with various merit
  - Your definitions are as good anybody else's!

- All VPNs provide traffic isolation
- With appropriate mechanisms, also bandwidth isolation
  - Scheduling
  - QoS mechanisms

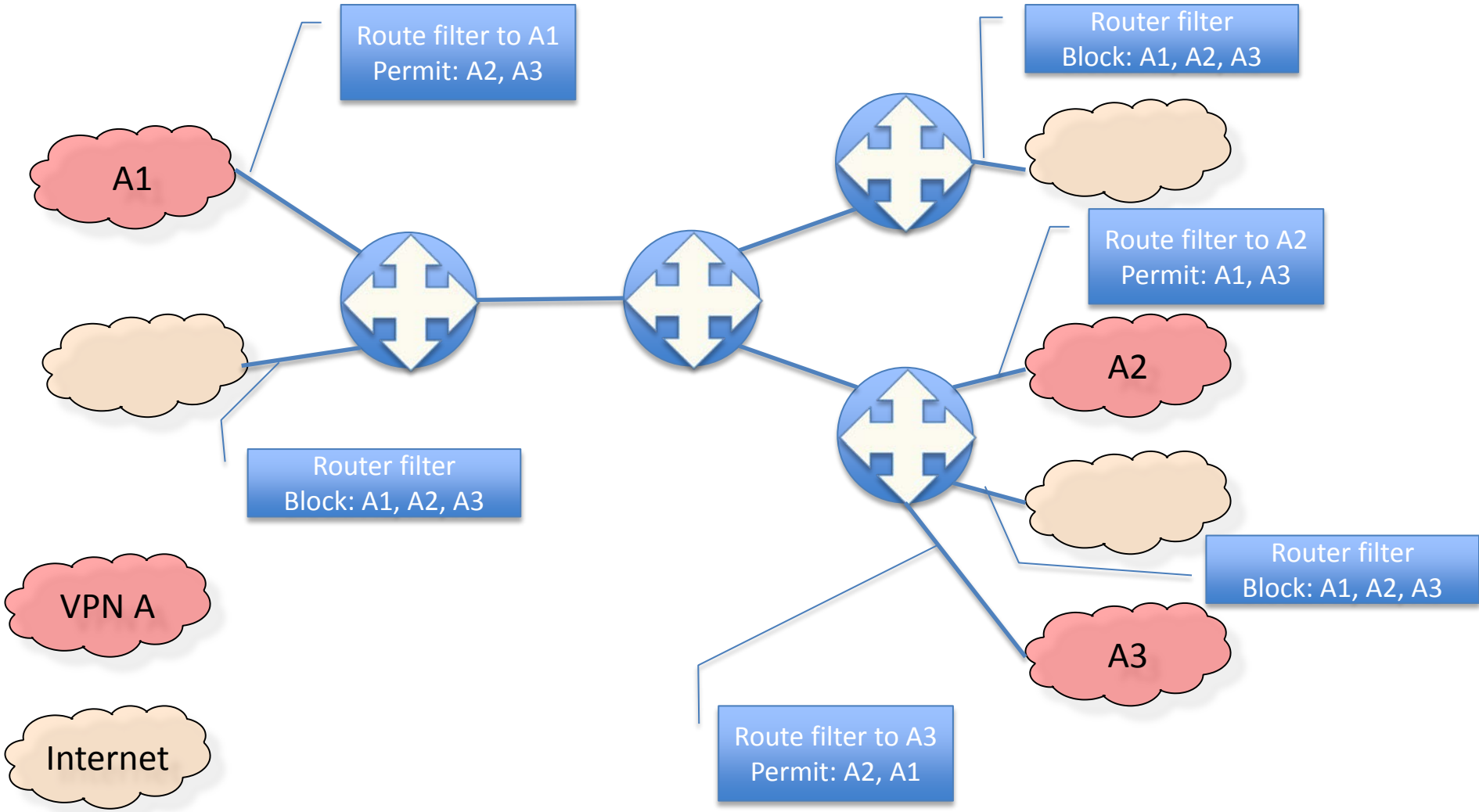
Overview

- Definitions
- Network virtualization technologies
  - VLANs
  - VPNs
    - Route filtering
    - Tunneling
    - Logical routers
  - Virtual routers
  - Programmable virtual routers

VPN – route filtering

- Route filtering
  - Controls route propagation so that
    - Networks within a VPN receive route advertisements for other networks in the same VPN
    - Networks not in same VPN do not receive those advertisement

VPN – route filtering



Overview

- Definitions
- Network virtualization technologies
  - VLANs
  - VPNs
    - Route filtering
    - Tunneling
    - Logical routers
  - Virtual routers
  - Programmable virtual routers

VPN - tunneling

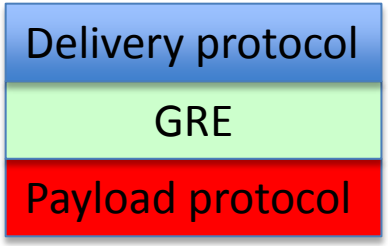
- A tunnel is a method of sending data by encapsulating the data and its protocol information within a different transmission unit
  - Virtual link
  - A very common way to build VPNs
  - Tunnels can be constructed at various layers

VPN - Tunneling

- Layer 2
  - Point-to-point = “pseudo-wire”, “virtual private wire”
    - Logical link created across switching cloud
    - MPLS, L2TP, PPTP, PPP, etc
  - Point-to-multipoint = “virtual private LAN”
    - Interconnection of remote LAN segments across switching cloud
      - VLAN is particular case where LAN segments and switching cloud both Ethernet
      - MPLS, etc

VPN - tunneling

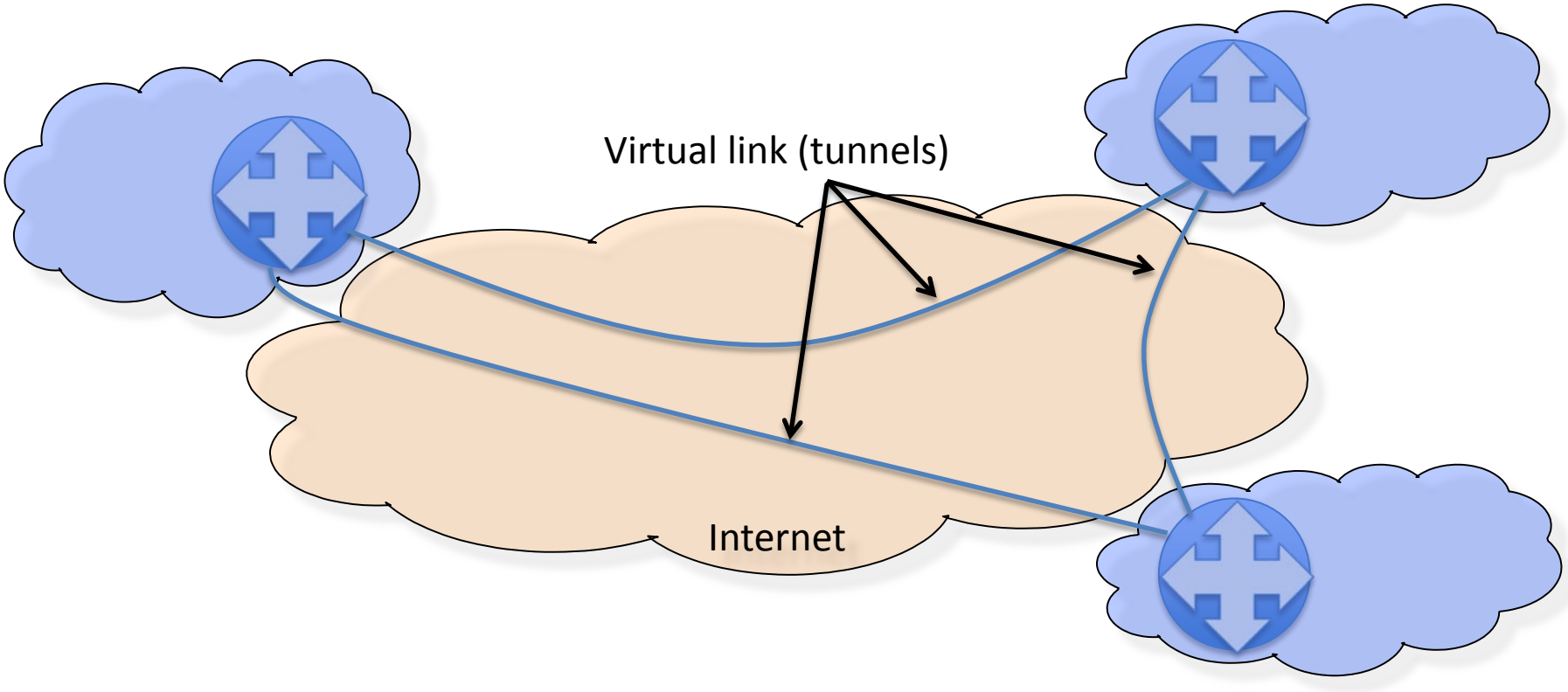
- Layer 3
  - IP-in-IP
  - Generic Routing Encapsulation (GRE)
    - Lightweight “any protocol over any protocol”



    - Very often implements ethernet-over-IP
  - IPSEC
  - etc

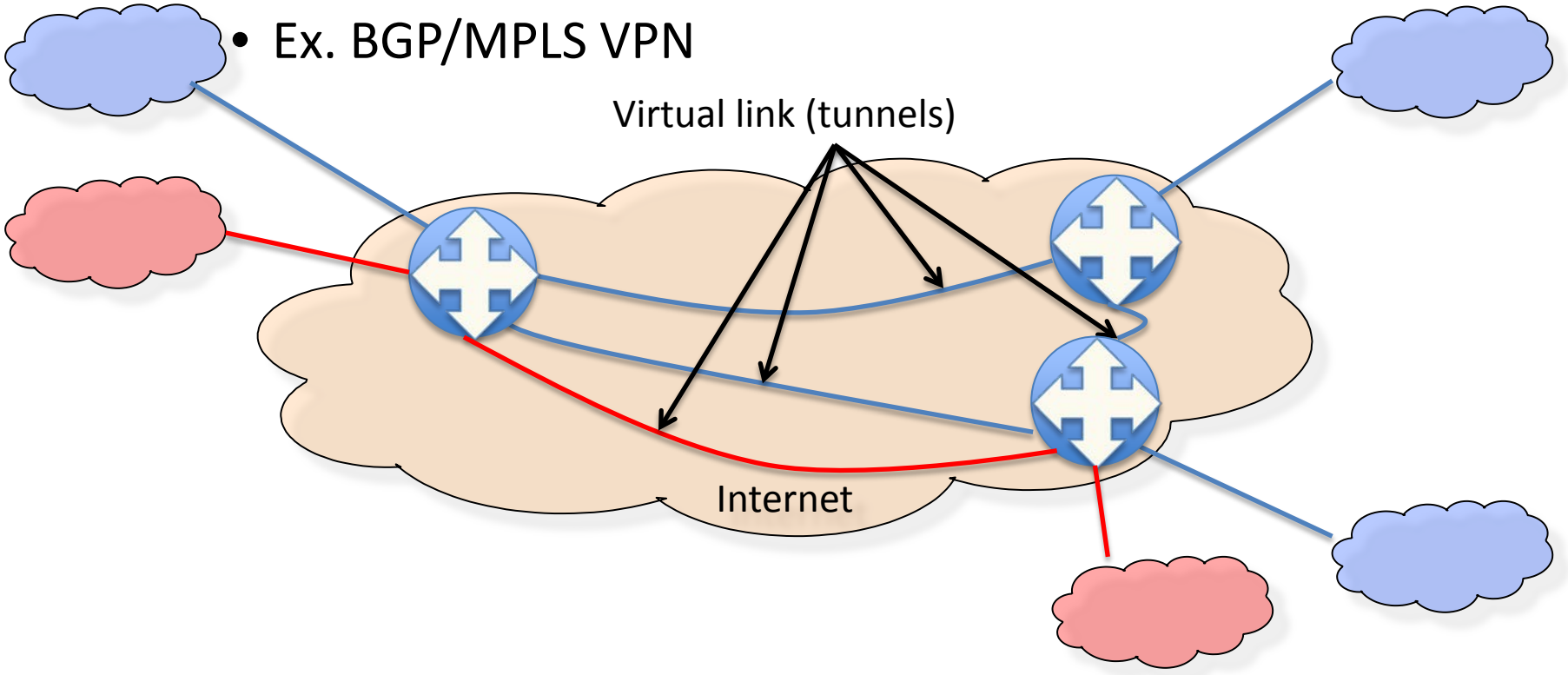
VPN - tunneling

- Customer model (CE-based)



VPN - Tunneling

- Provider model (PE-based)
  - Provider-provisioned VPN (PPVPN)
    - Ex. BGP/MPLS VPN



VPN - tunneling

- Isolation
  - Traffic
  - Bandwidth
  - Addressing and routing
    - Each VPN can use own addressing space and routing
      - Oppose to Route filtering was single addressing/routing
      - In PPVPN, each VPN requires own routing/forwarding
        - » Own instance of routing protocol
        - » Own instance of forwarding table
        - » Own instance of filtering/classification

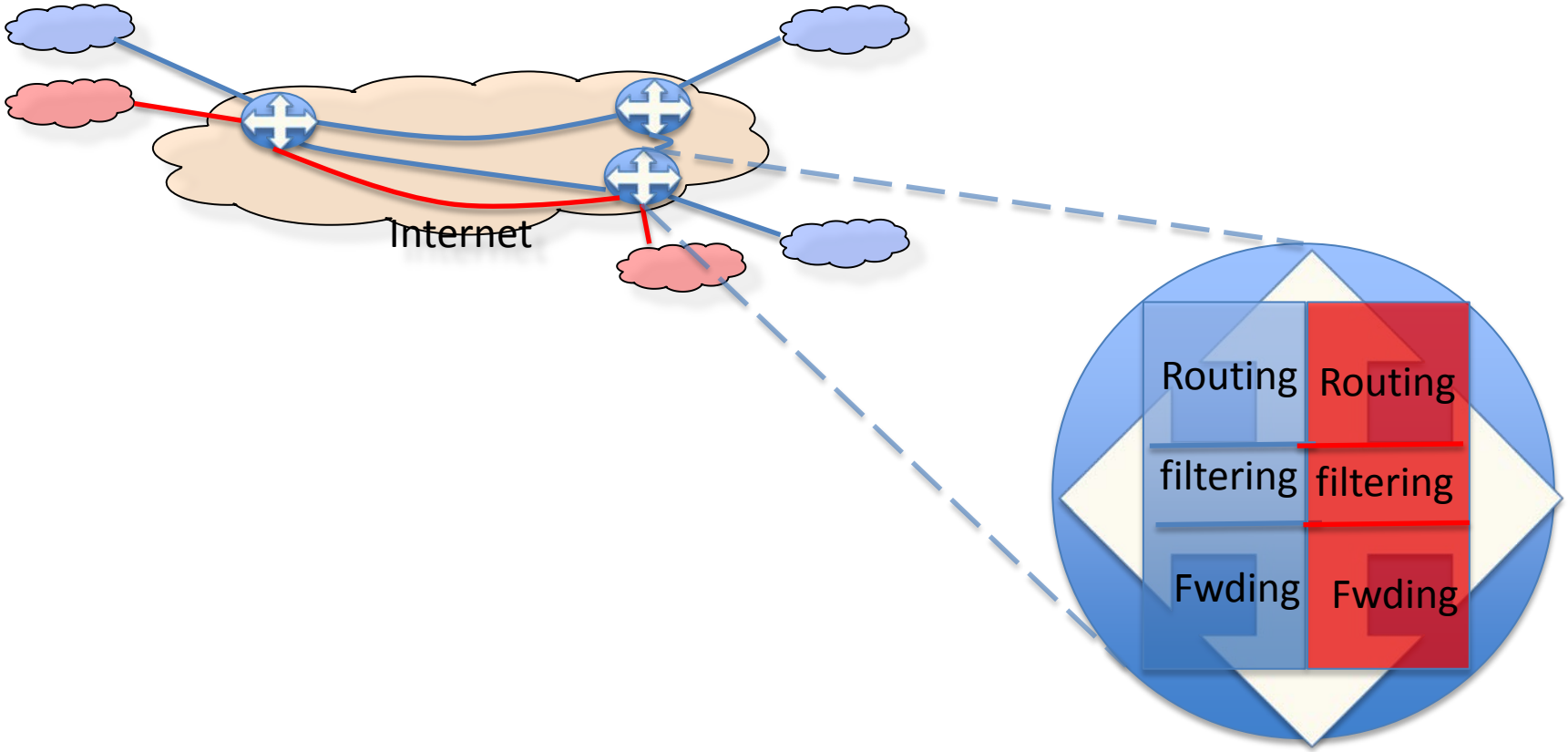
        => Logical router

Overview

- Definitions
- Network virtualization technologies
  - VLANs
  - VPNs
    - Route filtering
    - Tunneling
    - Logical routers
  - Virtual routers
  - Programmable virtual routers

VPN – logical routers

- Also known as “virtual routers”
  - But I “reserve” that term

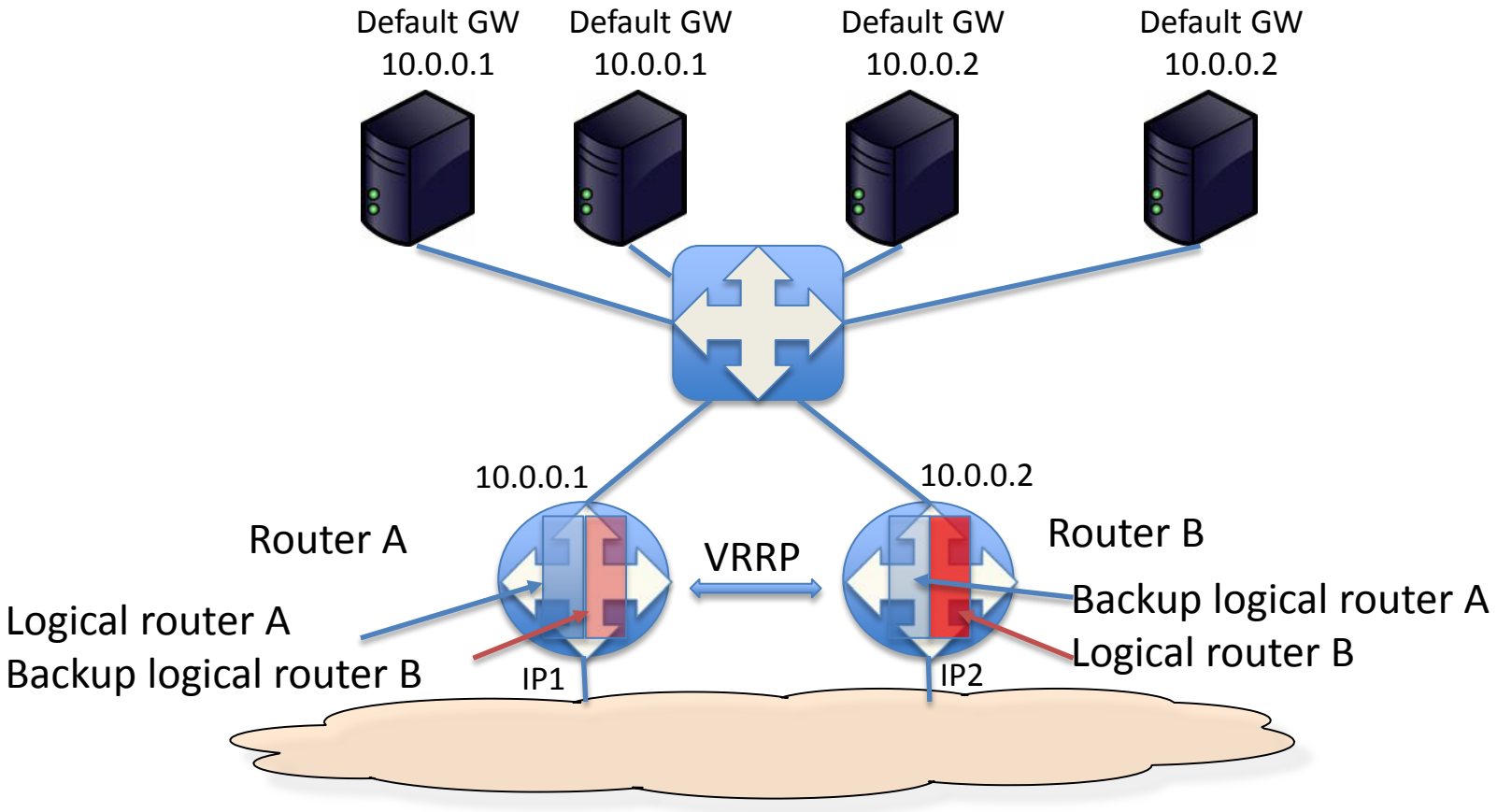


VPN – logical routers

- Scaling limited by amount of high-speed memory used for caching forwarding and filtering data structures
  - Such memory accounts for large portion of cost
- Results in limited number of logical routers
- Research question
  - How to split memory between logical routers?
  - Better memory usage efficiency
    - Combine/overlap data structures into single one

Logical routers - VRRP

- Virtual Router Redundancy Protocol
  - It is really about logical routers



Overview

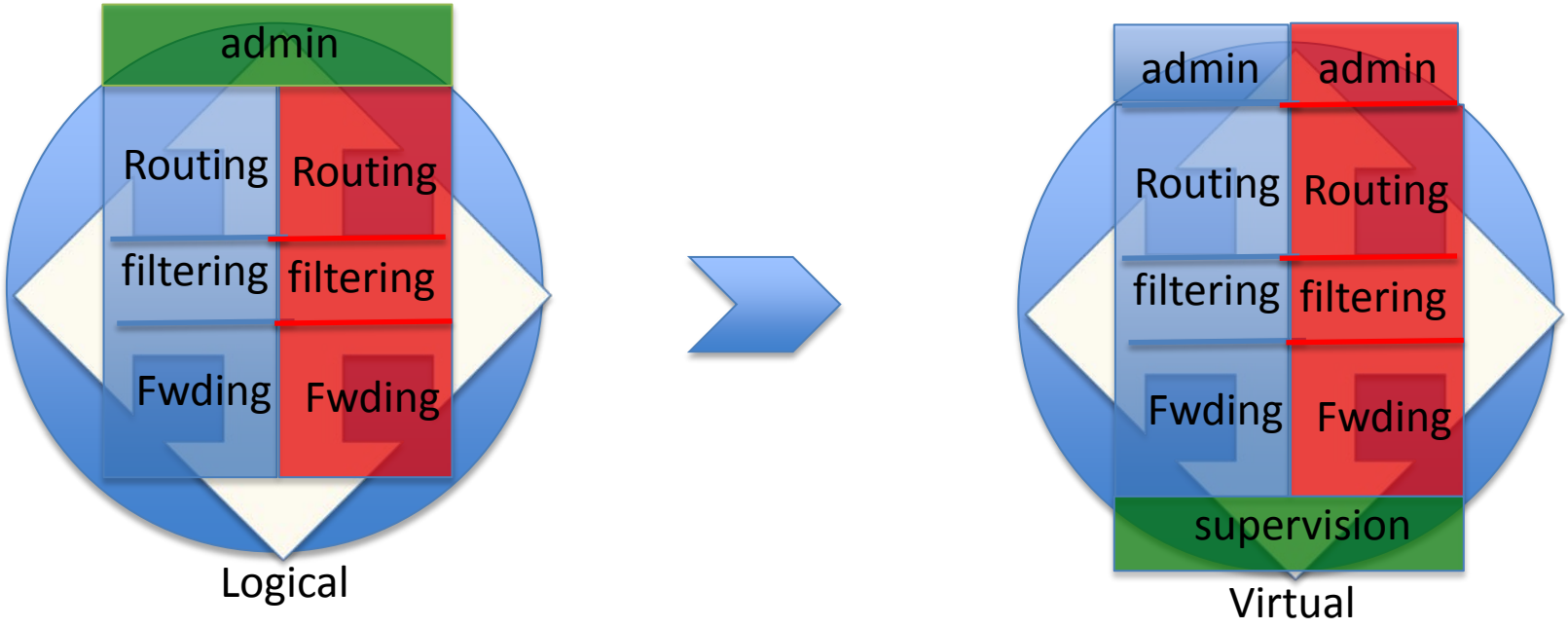
- Definitions
- Network virtualization technologies
  - VLANs
  - VPNs
    - Route filtering
    - Tunneling
    - Logical routers
  - Virtual routers
  - Programmable virtual routers

Virtual Routers

- Logical routers provide traffic, bandwidth, addressing and routing isolation through replicated data structures
- But the router is still under the authority of a single administrator
- If we want our very own logical router, and manage it ourselves, we need something else

Virtual routers

- A virtual router is sliced so to provide isolation of administration/management
  - In addition to isolation of traffic, bandwidth, addressing and routing



Overview

- Definitions
- Network virtualization technologies
  - VLANs
  - VPNs
    - Route filtering
    - Tunneling
    - Logical routers
  - Virtual routers
  - Programmable virtual routers

Virtual Programmable Routers

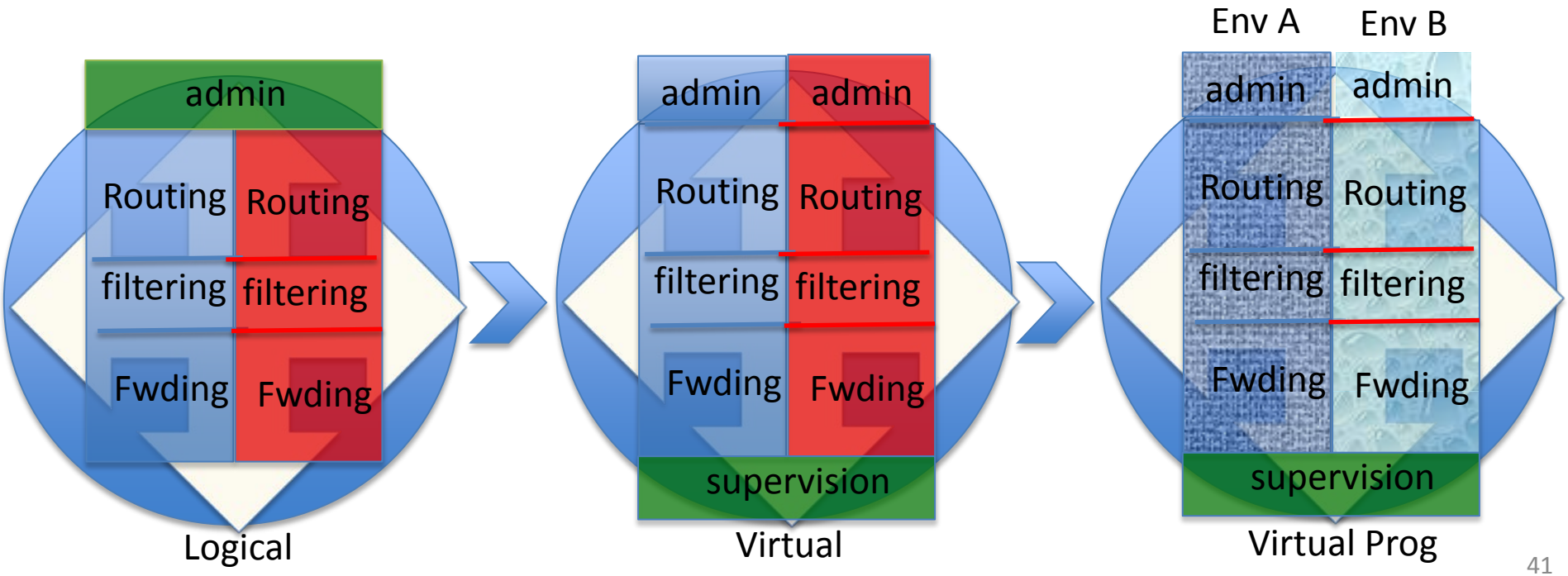
- So far, all routers ran the same stack
  - (Logical and) virtual routers have separate data structures
- The next "step" is to run different stacks

$\Rightarrow$ Virtual Programmable Routers

  - Also commonly known as "virtual routers"
    - How confusing!
      - This shouldn't be surprising, as historically, computer scientists have had serious issues with language and imagination for new terms

Virtual Programmable Routers

- Run potentially completely different environments (control – data planes)
  - Different protocols, implementations, etc



overview

- Virtual networks
  - Motivations
  - Principles
  - Architecture
  - Migration
- Server virtualization
  - Full-virtualization
  - Paravirtualization
  - Container-based virtualization
- Building vrouters

Virtual networks - motivations

- Traditionally, ISPs have provided both
  - (Physical) Communication infrastructure
  - Communication services (network protocol deployment and service provisioning)
  - To have a presence, ISP must deploy material at geographical location

Virtual networks - motivations

- This state of affairs leads to resistance to new service deployment
  - To achieve large-scale deployment, an ISP must
    - Either deploy infrastructure world-wide (expensive)
      - And hope to gain customers
    - Or rely on cooperation from other ISPs (to do the same), to provide service end-to-end
  - Add to this that communication service is a critical revenue stream

=> “Ossification” of the network

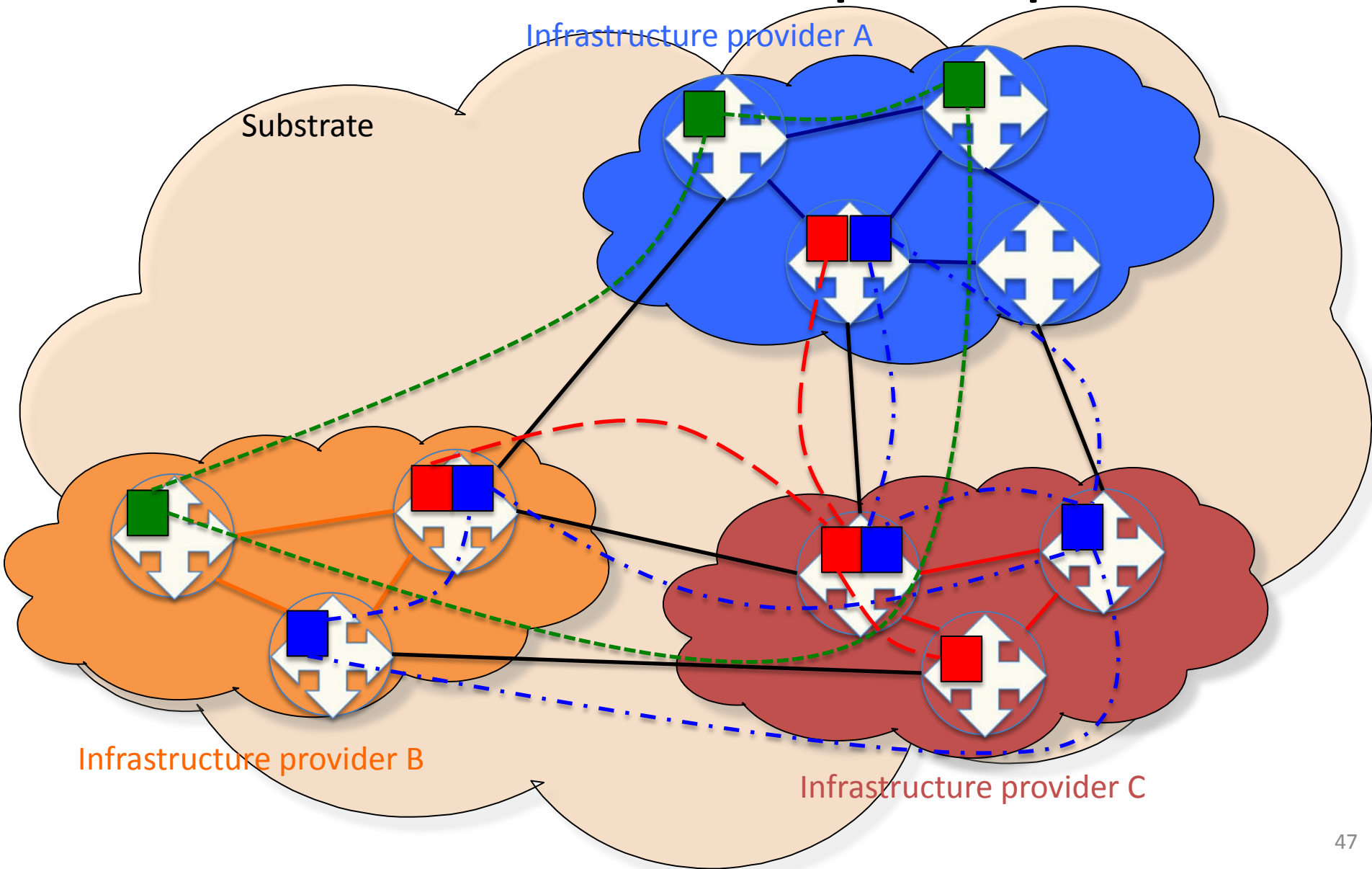
overview

- Virtual networks
  - Motivations
  - Principles
  - Architecture
  - Migration
- Server virtualization
  - Full-virtualization
  - Paravirtualization
  - Container-based virtualization
- Building vrouters

Virtual networks - principles

- Overall principle: decoupling of infrastructure substrate and communication services
  - Several networks deployed as virtual networks over a common physical infrastructure
  - Central to all proposals
    - Cabo, GENI, Cabernet, 4WARD
- virtual networks = VPN + virtual routers

Virtual networks - principles

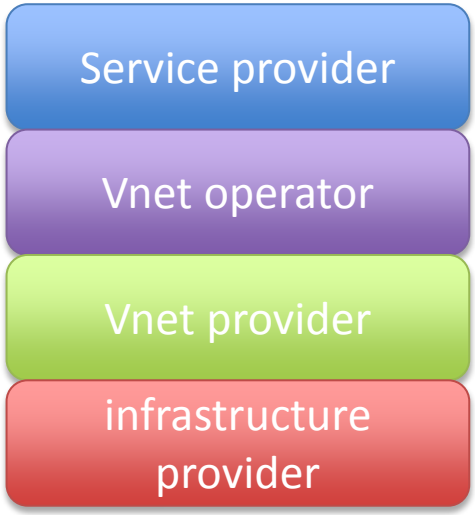


overview

- Virtual networks
  - Motivations
  - Principles
  - Architecture
  - Migration
- Server virtualization
  - Full-virtualization
  - Paravirtualization
  - Container-based virtualization
- Building vrouters

Virtual networks - architecture

- We describe 4WARD
  - The most “fine grained”
  - The others are similar
    - “merged” layers

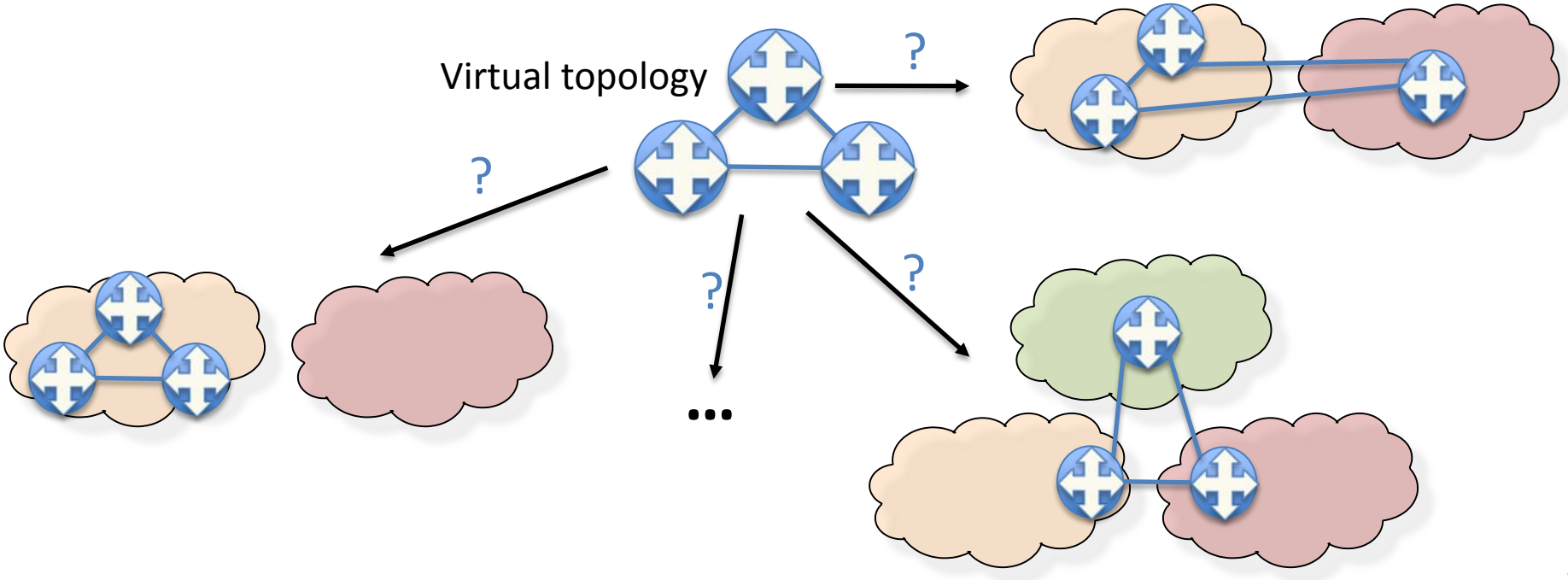


Virtual networks - architecture

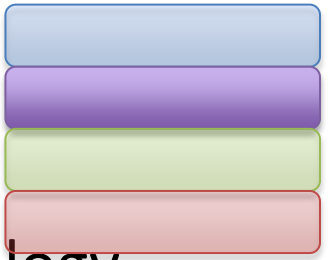
- Physical Infrastructure Provider (PIP)
  - Own and manage (some) physical infrastructure
    - Routers, switches, links, etc.
  - Wholesale of raw bit pipes
  - Wholesale of processing “cycles”
  - Main goal
    - Optimize mapping of requests for part of virtual network onto physical resources

Virtual networks - architecture

- Virtual Network Provider (VNP)
  - Assembles resources from one or more PIPs into a virtual topology
  - A resource broker



Virtual networks - architecture



- Virtual Network Operator (VNO)
  - Installs and manages VNET over virtual topology
    - Virtual topologies is either “empty” slices or unconfigured routers
      - Installs (if necessary) and configures “router images”
  - Realizes a tailored network service
  - Could use several VNPs and “stitch” several virtual topologies together
    - Requires notion of “half-link” in virtual topologies
  - This is an outsource outpost

Virtual networks - architecture

- Service provider
  - Uses the virtual network to provide services
    - Virtual ISP
    - Value-added, custom service
      - Application provider

Virtual networks - architecture

- The 4 layers are in the control plane only
  - The “only extra overhead” in the data plane is the virtualization technology overhead
- Users can connect as virtual machines through VPN access techniques
  - If a end-host connects to several Vnets without the isolation of virtual machines, then end-host can become an inter-vnet interconnection point.
-

Virtual networks – config language

- Request and configuration language is needed and still is an open research question
  - You need topology description with potentially "qualified" constraints
    - Location (router in Strasbourg)
    - Protocol spec (running IPv6)
    - Environment description
      - General system (CISCO, linux, etc)
      - Or very specific (IOS version x, linux kernel 2.x with Y patch z.z, etc)

overview

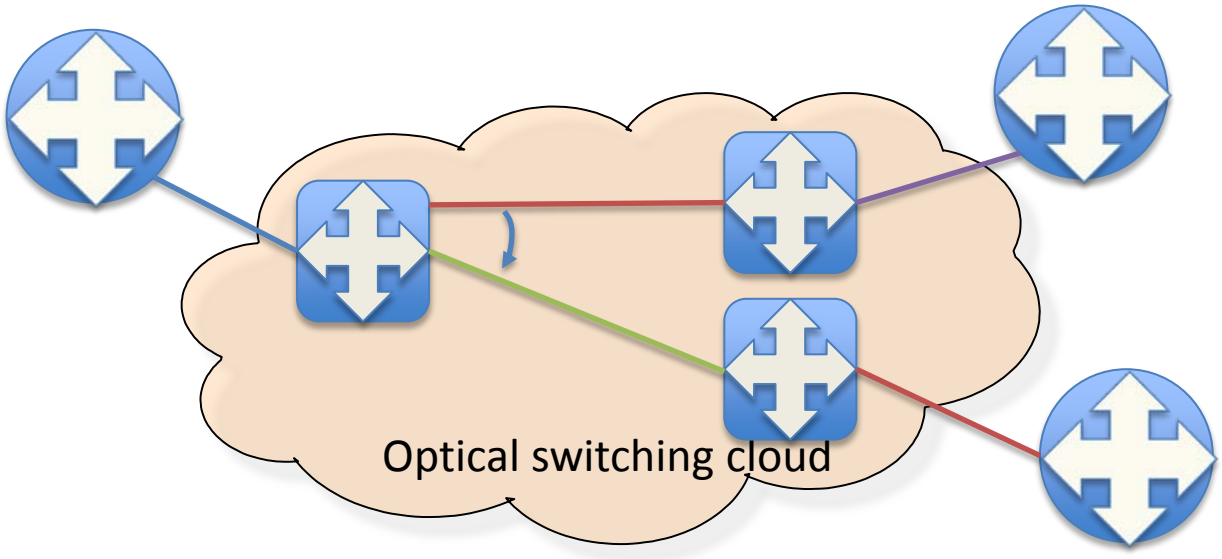
- Virtual networks
  - Motivations
  - Principles
  - Architecture
  - Migration
- Server virtualization
  - Full-virtualization
  - Paravirtualization
  - Container-based virtualization
- Building vrouters

Virtual networks – migration

- A natural consequence of the decoupling of the communication service and the physical platform
- Need to migrate 2 things
  - Virtual links
  - The virtual router per se

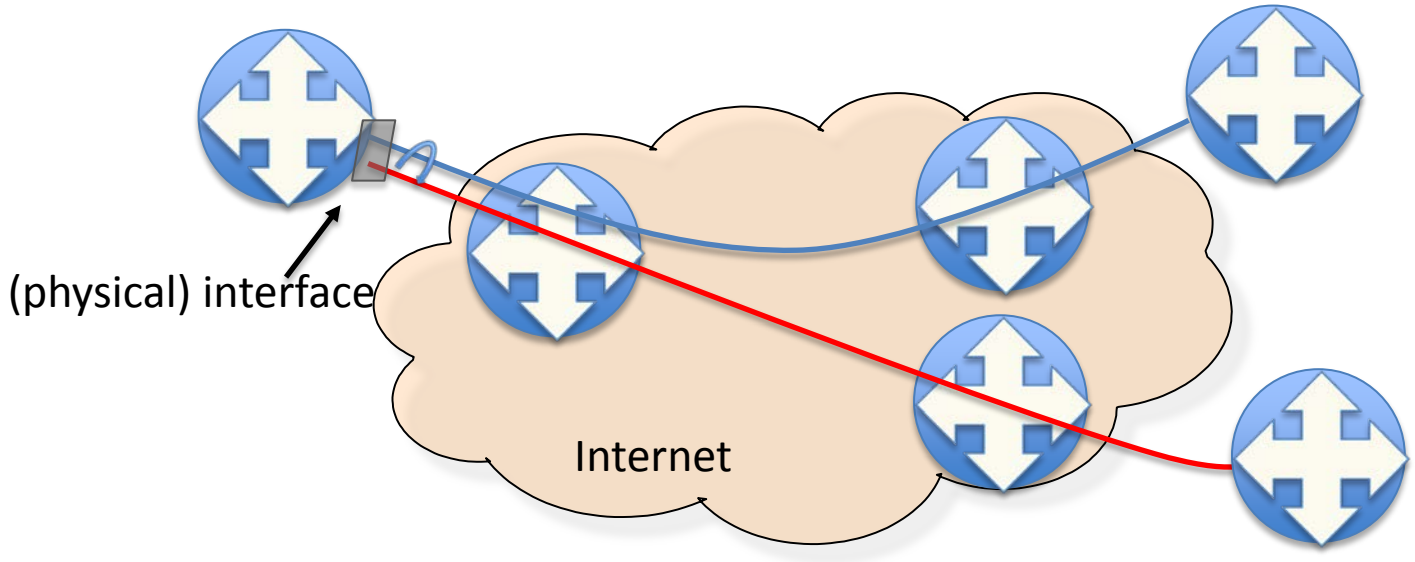
Virtual networks – vlink migration

- Link switched through transport network (e.g. optical network)



Virtual networks – vlink migration

- Packet-aware transport network (e.g. pseudo-wire)



Virtual networks – vrouter migration

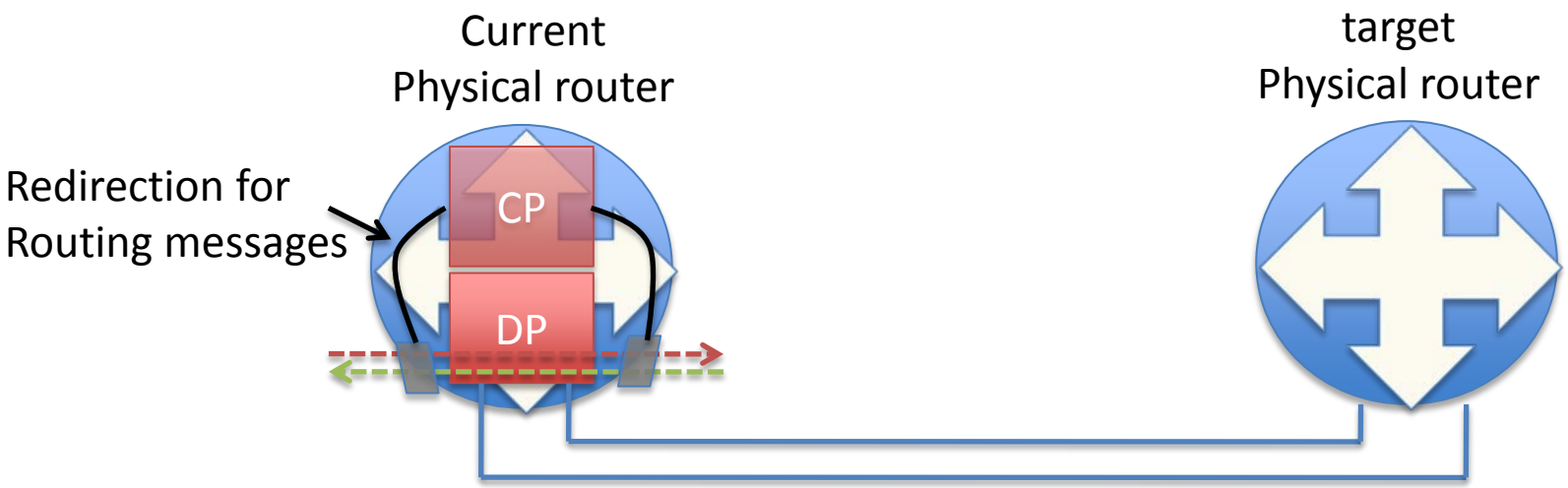
- At best, must migrate configs and state from both control and data plane
- At worst, must migrate binaries, configs and state.
- Either way, their will be some delay and some disruption
  - Critical for data plane (a lot of packets will be lost)
  - Issue for control protocols
    - routing protocols would retransmit, etc.
    - too many/too long and will reconverge

Virtual networks – vrouter migration

- VROOM solution
  - Principle implemented by data-plane hypervisor
    - Separation of control and data-planes
    - Dynamic interface binding
- 5-step process to minimize disruption

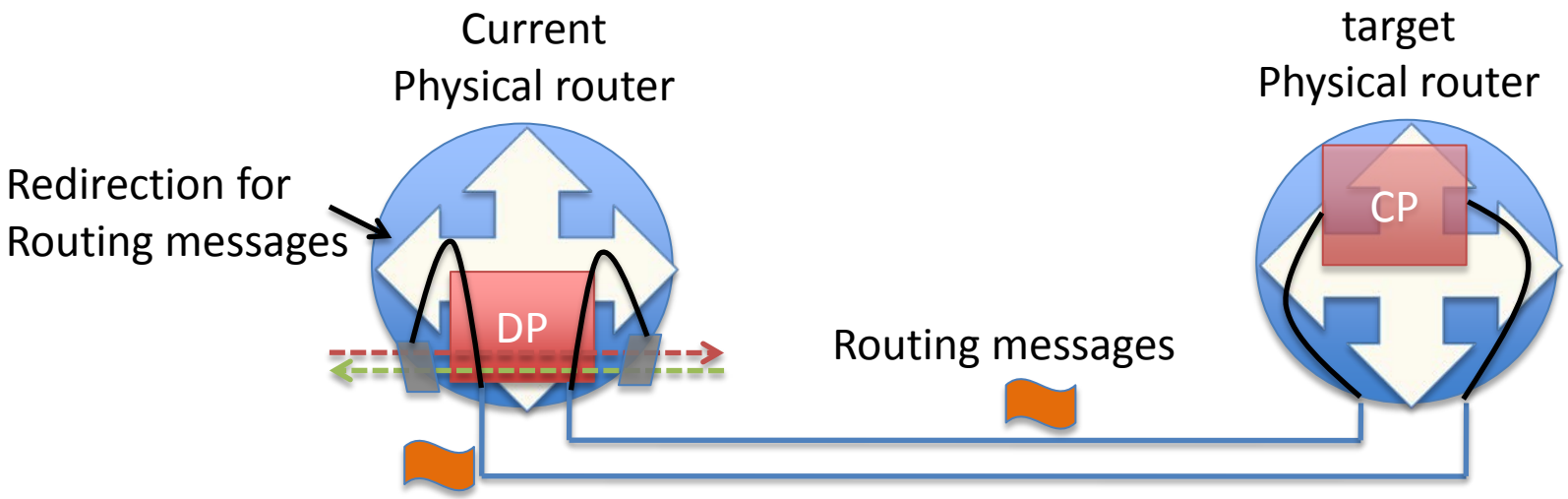
Virtual networks – vrouter migration

- Step 1: Tunnel set-up



Virtual networks – vrouter migration

- Step 2: control plane migration
  1. Router-image copy (code + configs)
  2. Memory copy
     1. Pre-copy
     2. Stall-and-copy of modified (control plane downtime)
  3. On completion, redirect routing messages (both sides)

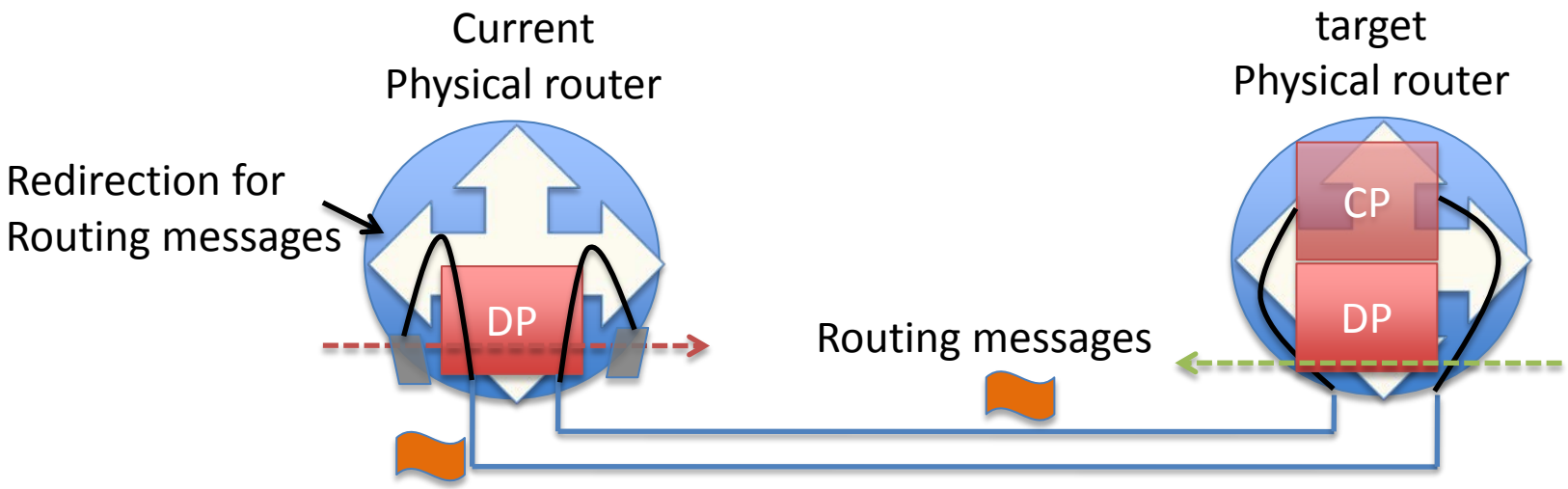


Virtual networks – vrouter migration

- Step 3: data-plane cloning
  - Moving data-plane state is wasteful
  - All we need is already in the control plane
    - Re-generate
  - This is not instantaneous
    - Installing a FIB entry can typically take a few hundred microseconds
    - Installing full BGP RIB (~250K entries) cat take about 20 seconds
- Control plane acts as remote control plane for original data plane

Virtual networks – vrouter migration

- Step 4: link migration
  - Once new data plane has been cloned, we have 2 functioning data planes
  - Start migrating links to new data-plane asynchronously



Virtual networks – vrouter migration

- Step 5: remove old data-plane and redirection tunnels
  - Once all links have been migrated, we are done

overview

- Virtual networks
  - Motivations
  - Principles
  - Architecture
  - Migration
- Server virtualization
  - Full-virtualization
  - Paravirtualization
  - Container-based virtualization
- Building vrouters

Server virtualization

- Isolation of administration and performance
- System virtualization
  - 2 main techniques
    - Full virtualization
    - Paravirtualization
  - Hardware assists
- OS virtualization
  - Container-based virtualization

Server virtualization

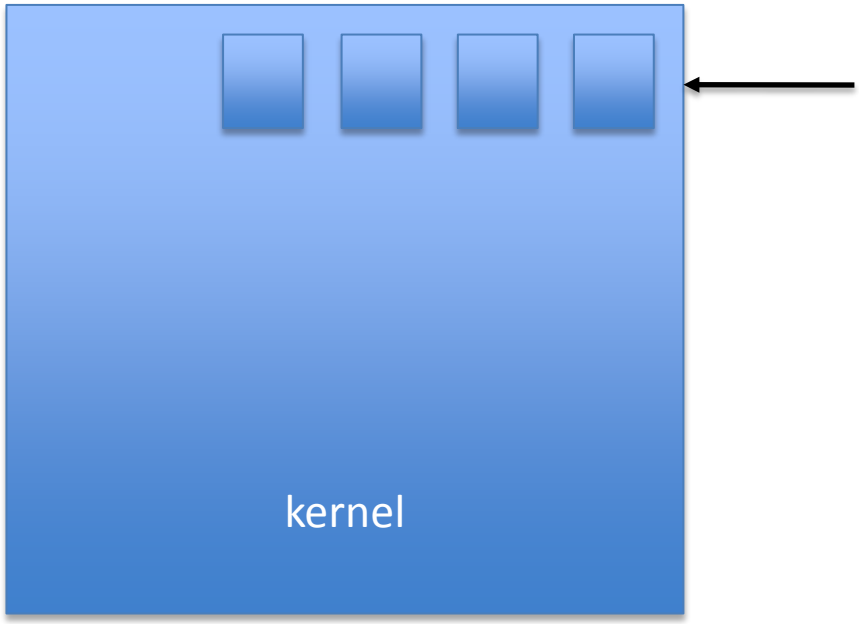
- Full virtualization
  - Complete simulation of underlying hardware in software
  - Must intercept and simulate privileged operations
    - Effects of any instruction must be kept to that specific machine
      - If it does, executed in HW; if not, trapped into software
  - Example: VMWare workstation, fusion

Server virtualization

- Paravirtualization
  - Simulation of underlying hardware
  - Software interface presented to virtual machines is slightly different from hardware interface
    - Goal is to change syscalls that are much more difficult to run than in native mode
      - Better performance as run closer to hardware
    - Guest operating system must be modified
  - Example: Xen, VMWare server, etc.

Server virtualization

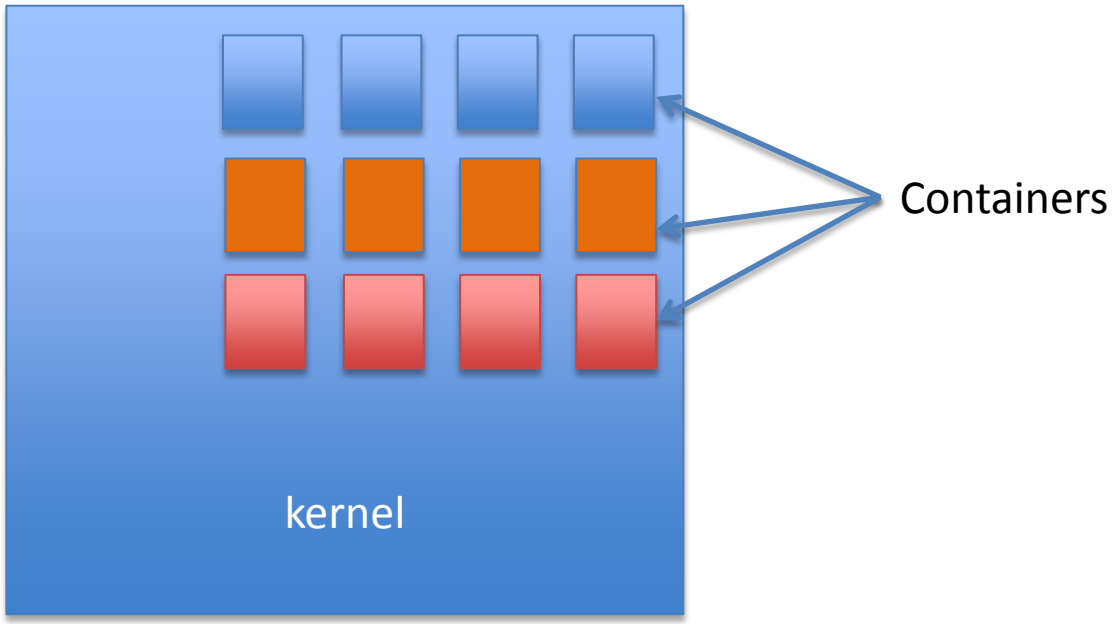
- Container-based OS virtualization



Kernel data structures
(process tables, file descriptors,
connection blocks, etc)

Server virtualization

- Container-based OS virtualization



- Very lightweight
  - But less flexibility (kernel is fixed)

Server virtualization

- Virtual machines usually use virtual (software) network interfaces
  - With own MAC address
- Use of soft-switch to interconnect virtual and physical interfaces
  - This is usually very slow

overview

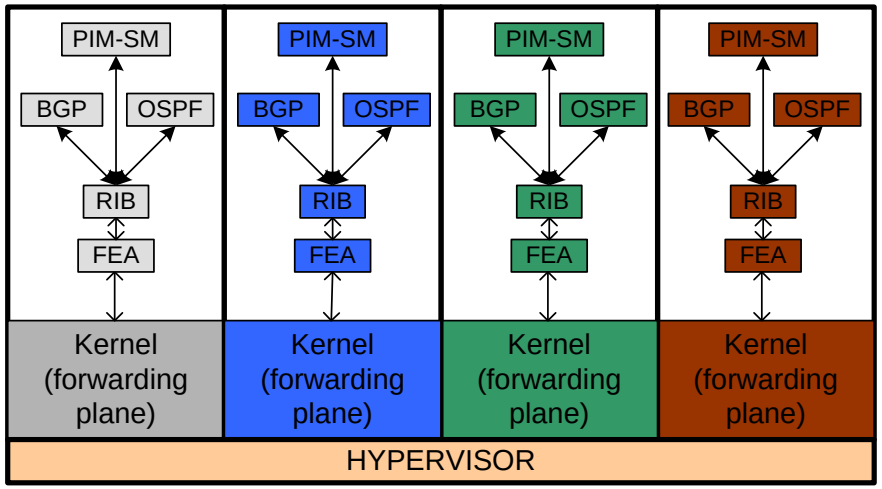
- Virtual networks
  - Motivations
  - Principles
  - Architecture
  - Migration
- Server virtualization
  - Full-virtualization
  - Paravirtualization
  - Container-based virtualization
- Building vrouters

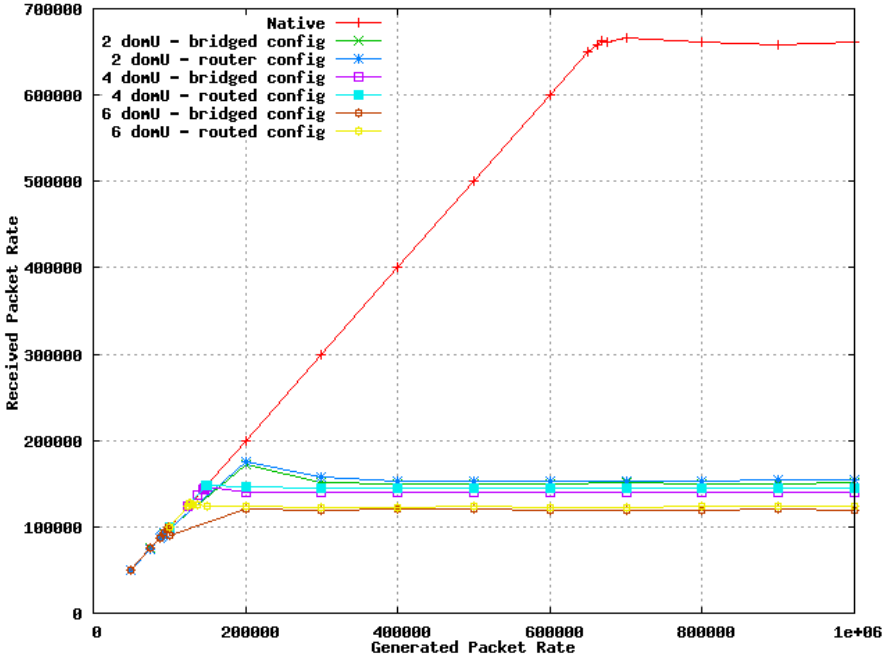
Building vrouters

- Trellis uses container-based virtualization to build virtual routers on PCs
  - This is mostly non-programmable IP vrouters
    - Could program in kernel
  - Uses modified soft-switch to improve performance
    - Essentially introduction of direct link between virtual and physical interfaces

Building vrouters

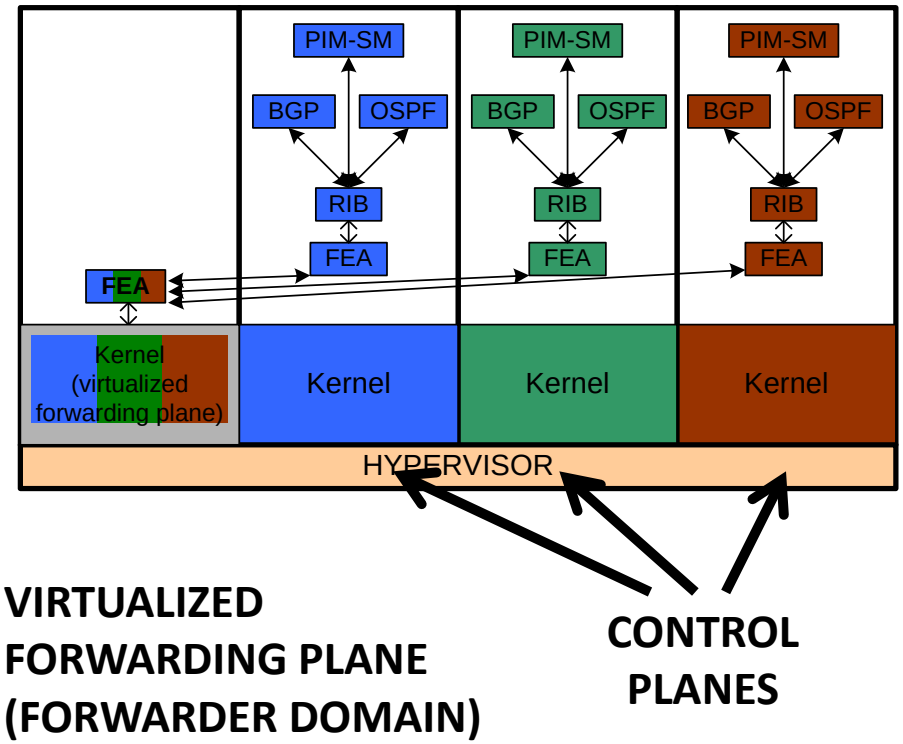
- Programmable vrouter using off-the-shelf server virtualization





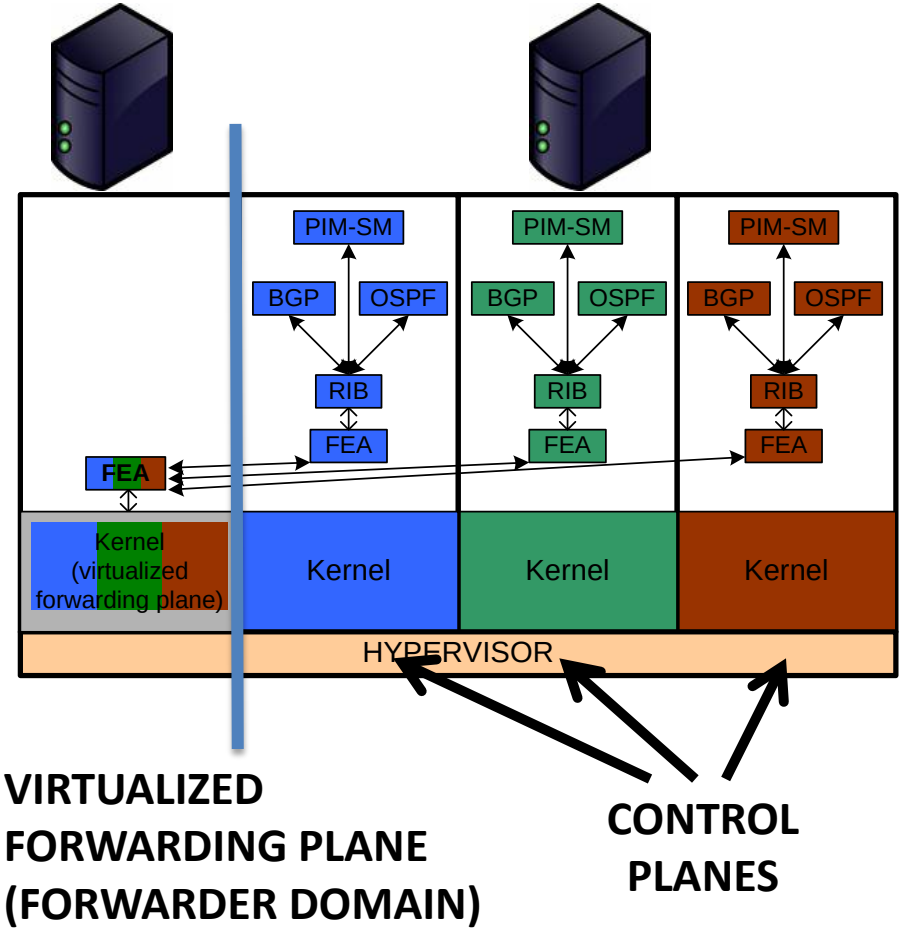
Building vrouters

- (programmable) Vrouter project



Building vrouters

- (programmable) Vrouter project



Building vrouters

- (programmable) Vrouter project
  - Forwarding path built using Click in kernel mode
    - Modular router system
      - Fully programmable above Ethernet
    - Using forwarding path merging techniques
  - Optimized for multi-core systems
    - Memory latency is bottleneck
      - Plenty of surplus CPU cycles in many cores
    - High performance (~ 10 small Mpps)

Building vrouters

- All software based virtual routers benefit from NIC hardware assist to implement fairness
  - Virtual Machines Device Queues
    - Hardware queues associated with (virtual) MAC addresses
    - Traffic classification/isolation on NIC

Building vrouters

- Programmable NP-based vrouters
  - Supercharging PlanetLab
    - Split data-path between NP and servers
  - NPR
    - NP hosts a pipeline, made up of “classic” modules and plug-ins
      - Plug-in are programmable in C

Closing remarks

- Virtualization is ubiquitous in networking
  - Reduces costs, increases flexibility
- Offered some “taxonomy” of network virtualization based on isolation
- Virtual networks of programmable virtual routers are an enabler for the future Internet
  - Concurrent deployment of existing and new protocols
  - Shadow networks for testing/debugging
  - Many more applications
    - A very hot research topic

objects