we SYSTEMS

CloudStack Networking in Action

Inspiration, Practical Tips and Sharing Experience

Stephan Bienek
@StepBee

weSystems Portfolio

Computing

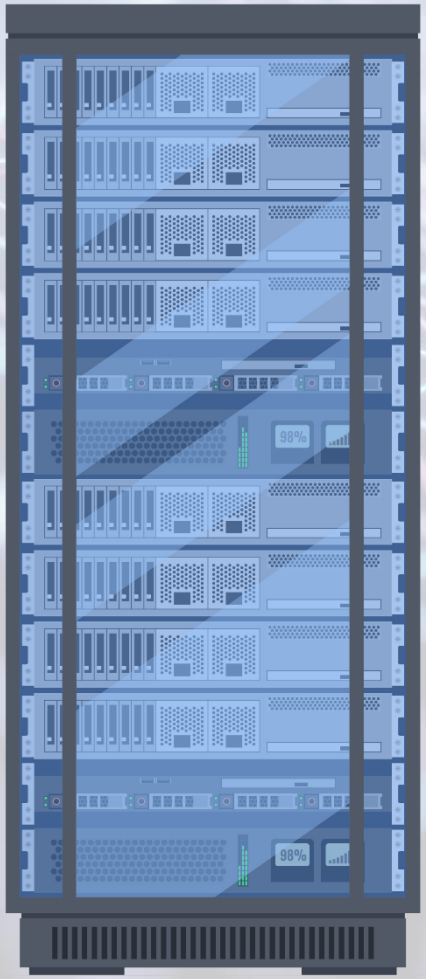
Cloud Services · Dedicated Hosting · Colocation · On-prem & hybrid IT Infrastructures · Data Center Services

Storage & Backup

High Performance Storage · Intel DAOS · Performance Storage · Backup · Ceph Cluster Management

Managed IT Services

Managed Hardware · Managed OS · Managed Firewalls · Managed Ceph · Monitoring as a Service · Container aaS



Network & Connectivity

Internet Services · BGP · Ethernet Services · Wide Area Network · Cloud Connect · Location networking

Cloud Voice

Global Cloud Telephony (VoIP) · SIP Trunks · Phone numbers · Contact Center · Cloud SBC · VVN Platform · Voice Migration

Professional Services

Strategic & technical Consulting · Project Management · Implementation · Support · Workshops · Managed Services

CloudStack Networking

Network Types

Isolated
- Usually non-routed Subnet (IPv4)
- commonly including Virtual Router
- commonly including Network Functions

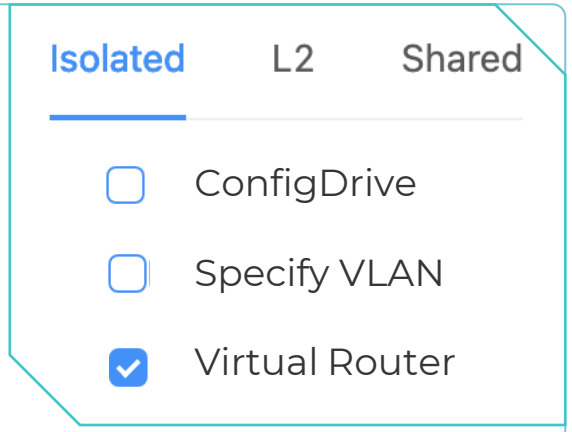
L2 (Layer 2)
- Communication with resources outside of CloudStack

Shared
- Networks across multiple organizational units

Network Offerings

Templates for Networks
- Defining Bandwidth
- Specify available network functions
- Ability to specify VLAN/VNI during creation
- Limit availability to specific Domains
- Define System offering for Virtual Router

Easy Quick Start



Purpose

- Quick start for customers
- No specific network/VNF Know-How required

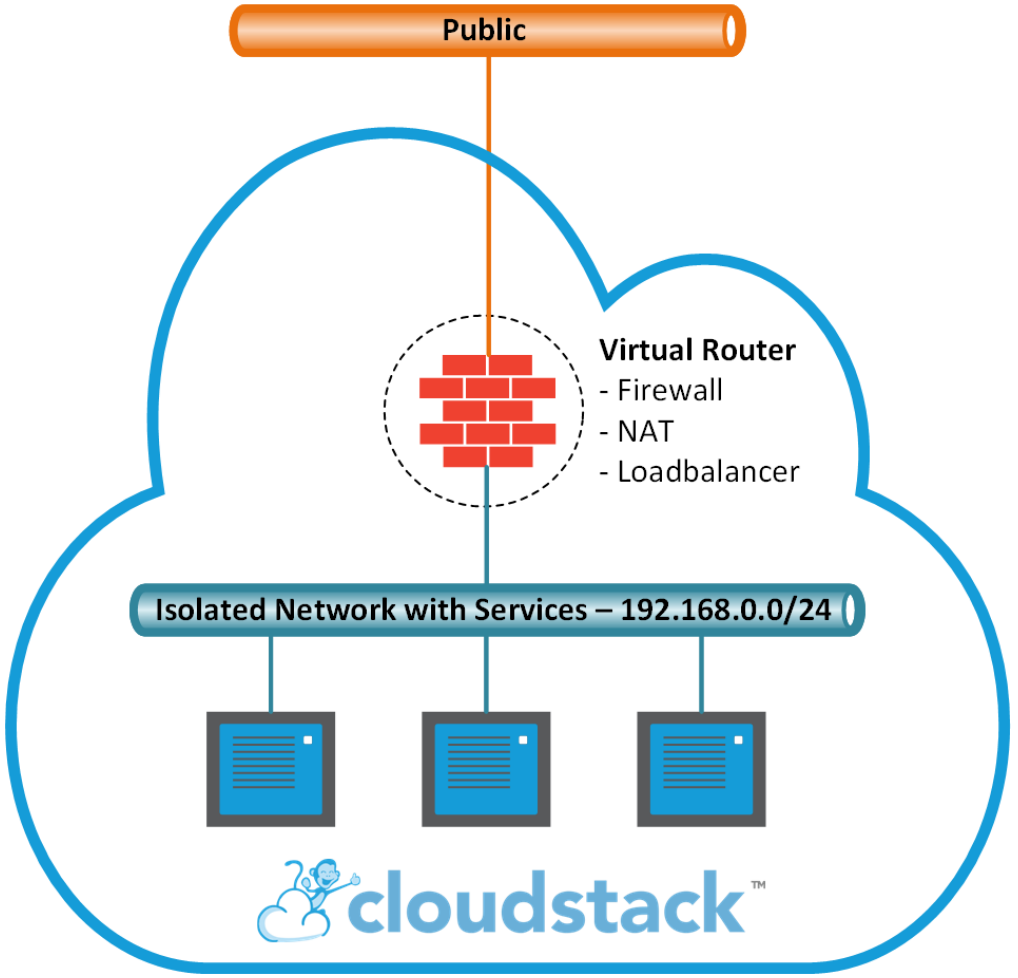
Virtual Router

- Integrated Firewall - Layer 3 Packet Filter, basic functionality
- Integrated Loadbalancer - Basic Loadbalancing functionality
- Integrated (Client-)VPN for secure platform access
- automated Public IP assignment
- Source NAT and Destination NAT

API / WebUI integrated

- one API to manage virtual machines and firewall / loadbalancer rule

Easy Quick Start



CKS Kubernetes Cluster with CSI

Purpose

- Network and Loadbalancer/Ingress integration with CloudStack
- Routed access to external resources like Storage for use with CSI

Split Subnet

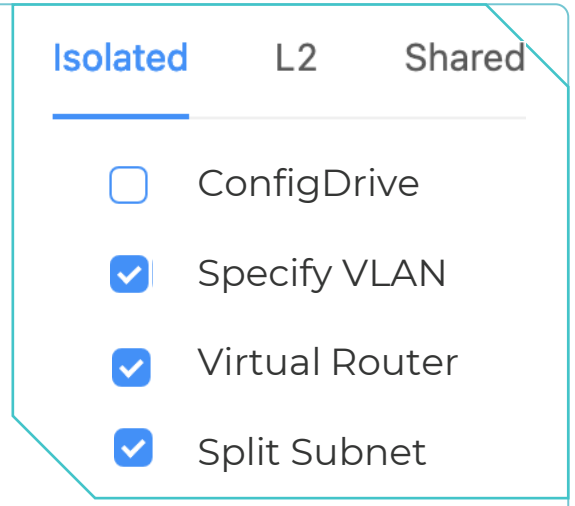
- Shrink Isolated Subnet managed IPs from /24 to /25
- first /25 managed by Virtual Router for DHCP, NAT, Loadbalancing
- second /25 for resources outside of CloudStack like external Router

Specify VLAN

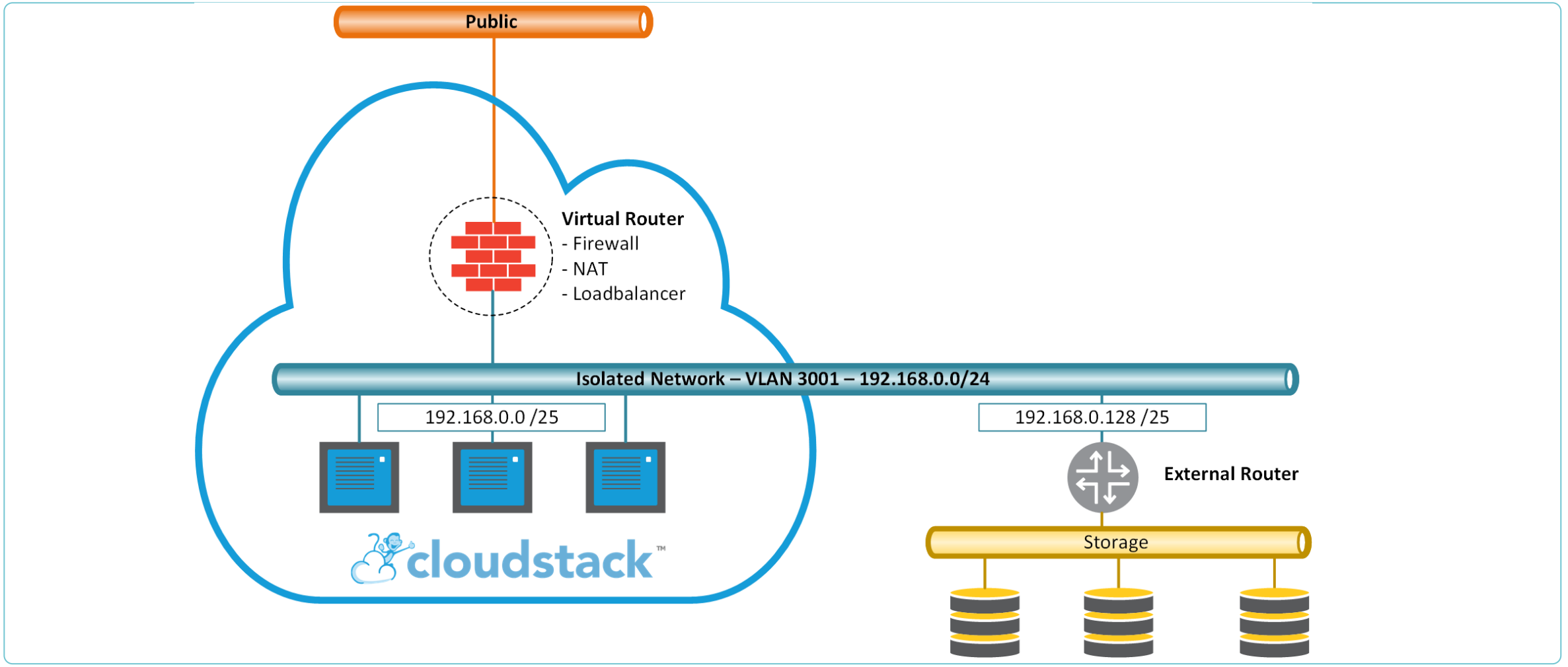
- configure fixed VLAN ID
- presented to router outside of CloudStack
- low latency and high bandwidth routing of packets to/from storage

Kubernetes DeamonSet

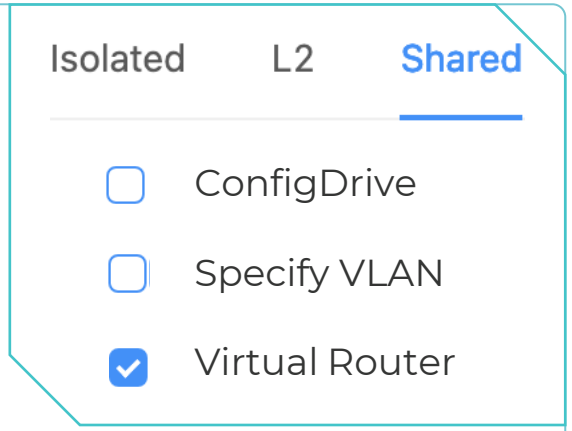
- DeamonSet to deploy host-routes to each worker node to reach storage via external gateway



CKS Kubernetes Cluster with CSI



Shared Network across Domains / Org Units



Purpose

- Connecting resources split into organizational units for example departments
- one joined network for data exchange between customers platforms

Virtual Router for multiple Org Units

- DHCP
- User Data
- DNS

Network Permissions

- Granular sharing control within the same Domain
- Across Domains - Shared Networks are still required

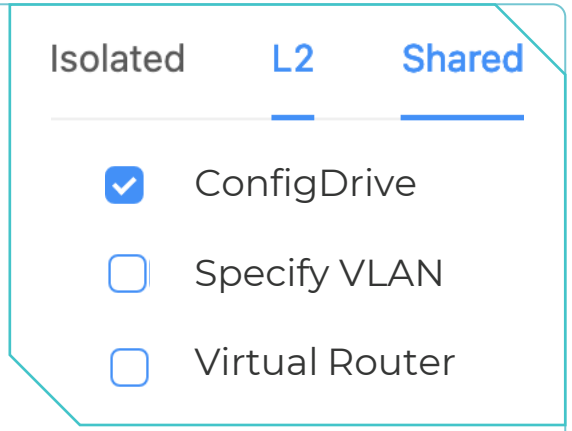
Public IP Access for Virtual Machines

- Risky in Advanced Zones without Security Groups, requires fixed MAC-IP entries on Routers

Backend Networks without functions

Purpose

- Backend network to connect different application tiers without any network functions



ConfigDrive

- UserData without Virtual Router to preconfigure VMs

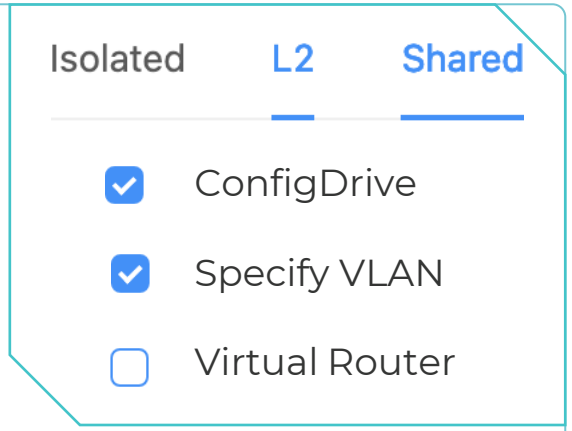
Without specify VLAN

- Let CloudStack manage the VLAN assignment
- not exposed to external routers for isolation within CloudStack

Provide Public IPv4 & IPv6 to VMs

Purpose

- Public IPs for VMs providing network functions like Routers and FWs
- IPv6 IPs / Subnets
  - /64 IPv6 Transfer Subnet
  - /48 IPv6 Routed Subnet to customers gateway VM
- direct Internet access without NAT



Specify VLAN

- configure fixed VLAN ID on external Router
- configure Gateway IP of public Subnet on external Router
- Cloudstack Virtual Machines using Public IP without NAT

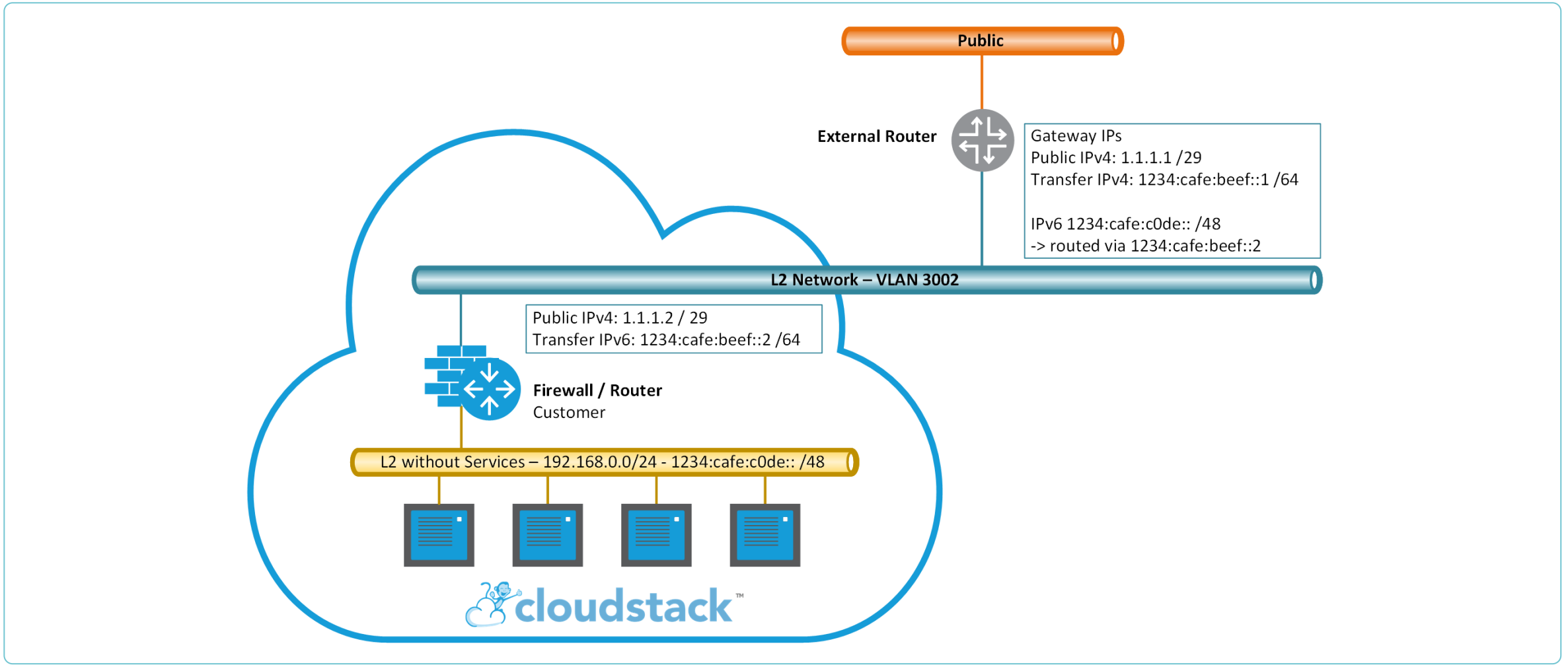
ConfigDrive

- UserData without Virtual Router to preconfigure VMs

Without Virtual Router

- No DHCP or NAT with external Routers

Provide Public IPv4 & IPv6 to VMs



Geo-redundant platforms across DCs / Zones

Purpose

- Build geo-redundant platforms across multiple DCs / zones, increase availability
- connect VMs in different zones

Specify VLAN

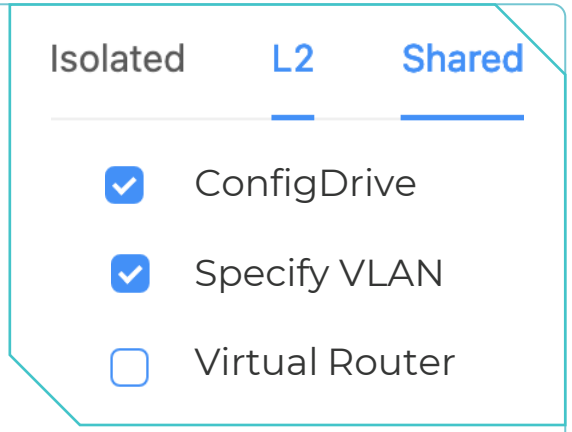
- Routed
  - configure fixed VLAN ID on external Router
  - configure Gateway IP of network on external Routers
- Stretched VLAN
  - VXLAN based backbone – configure fixed VLAN/VNI on external switch
  - stretch VLAN across Datacenters

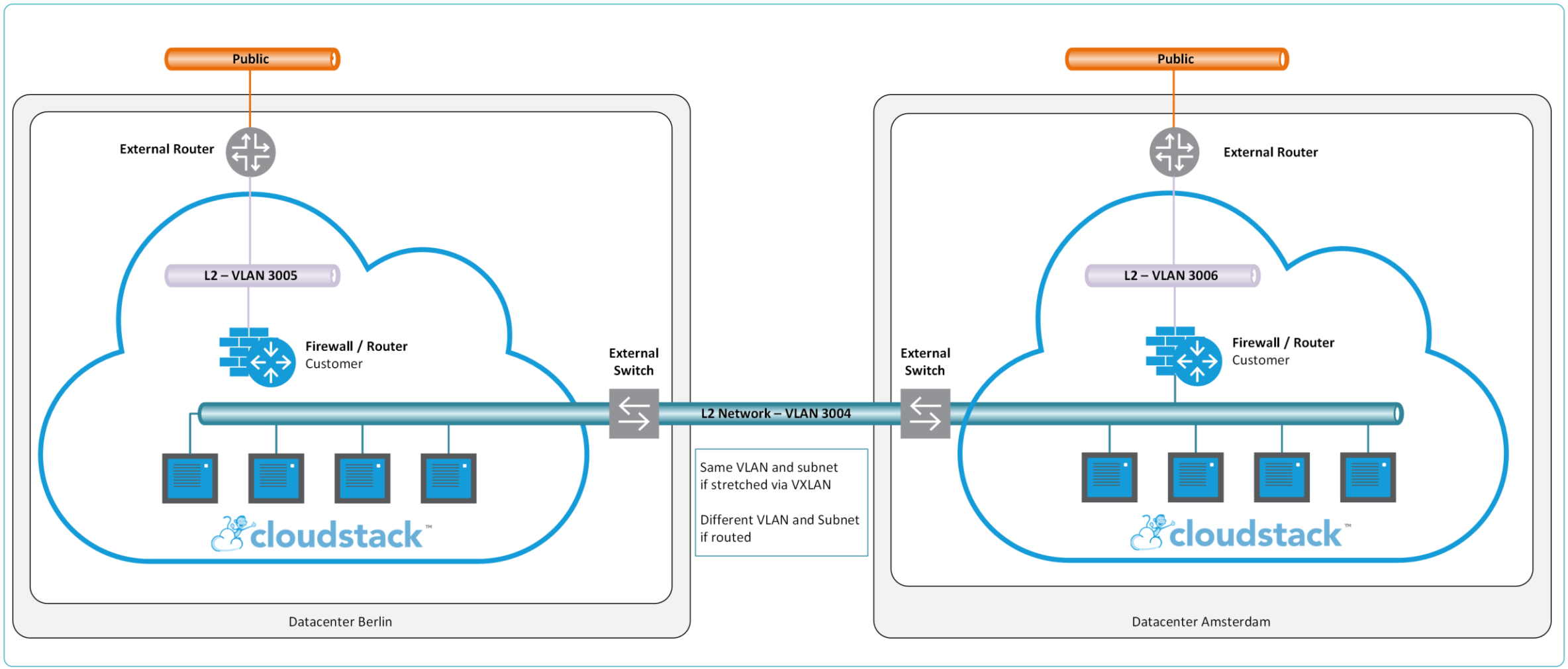
ConfigDrive

- UserData without Virtual Router to preconfigure VMs

Without Virtual Router

- No DHCP or NAT with external Routers




Public
External Router
L2 – VLAN 3005
Firewall / Router
Customer
External
Switch
L2 Network – VLAN 3004
Same VLAN and subnet
if stretched via VXLAN
Different VLAN and Subnet
if routed
Public
External Router
L2 – VLAN 3006
Firewall / Router
Customer
External
Switch
cloudstack
cloudstack
Datacenter Berlin
Datacenter Amsterdam

Hybrid Platforms

Purpose

- Build hybrid platforms – VMs and physical servers
- Combine physical and virtual resources to one platform

Specify VLAN

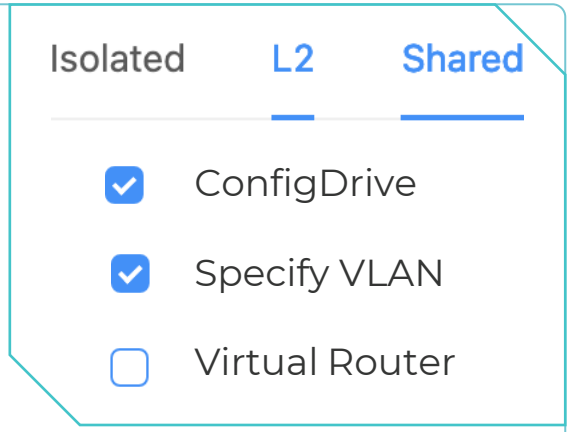
- Routed
  - configure fixed VLAN ID on external Router
  - configure Gateway IP of network on external Routers
- Stretched VLAN
  - VXLAN based backbone – configure fixed VLAN/VNI on external switch
  - stretch VLAN across the DCs

ConfigDrive

- UserData without Virtual Router to preconfigure VMs

Without Virtual Router

- No DHCP or NAT with external Routers



Cloudstack Networks - Outlook

IPv6 via Static Routing – in a dynamic way

- Dynamic deployment of IPv6 routes to external Routers
- Trigger on CloudStack Network creation Events
- Deploy routes to external Routers via BGP using custom script and ExaBGP

Routed Mode – Static and Dynamic Routing

- potentially more integrated way of
  - assigning Public IPs to VMs
  - communication with external resources
- Pre-configured, CloudStack integrated, dynamic routing

Stephan Bienek
Head of Hosting

s.bienek@wesystems.ag
+49 89 24410-861
+49 160 2000 581

@StepBee

we SYSTEMS

www.wesystems.de