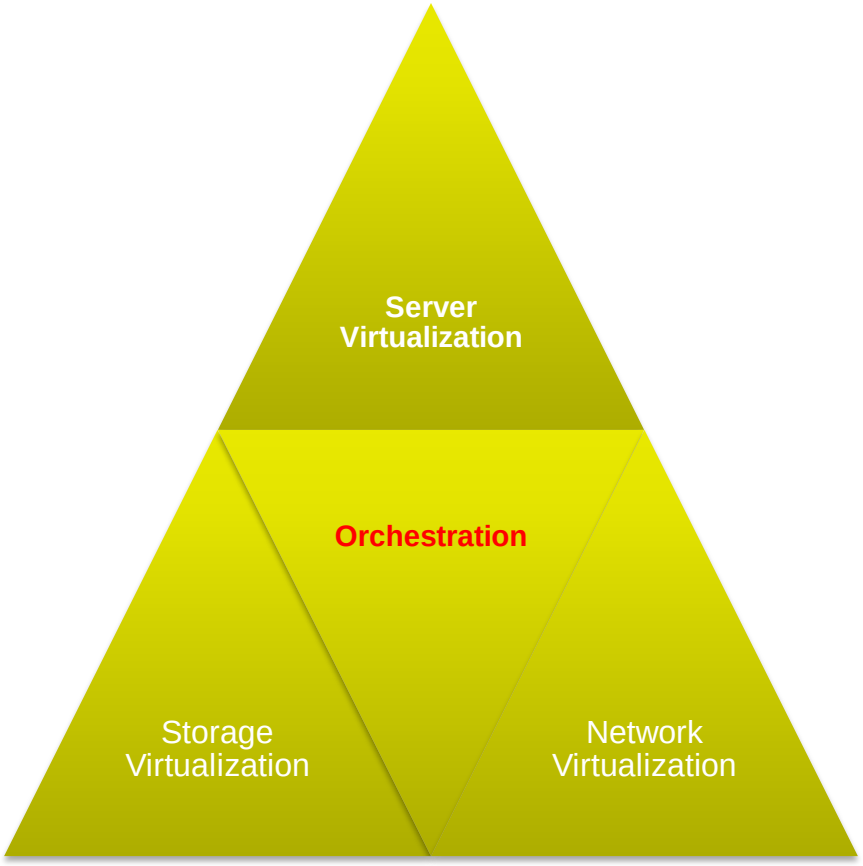
SIC

Serviços e Infraestruturas de Alto Desempenho

Network Virtualization

Image Credits: http://infosecninja.blogspot.pt

SIC &
the 3 vertices of datacenter virtualization…



Today's menu special: Network Virtualization
- The 2nd vertex of Datacenter Virtualization

Network Virtualization

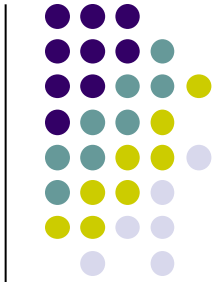
What is Network virtualization?

"*The process of combining hardware and software network resources and network functionality into a single, software-based administrative entity, a virtual network. Network virtualization involves platform virtualization, often combined with resource virtualization.*

Network virtualization is categorized as ***either external virtualization****, combining many networks or parts of networks into a virtual unit,* ***or internal virtualization****, providing network-like functionality to software containers on a single network server*"

[Wikipedia]

Network Virtualization

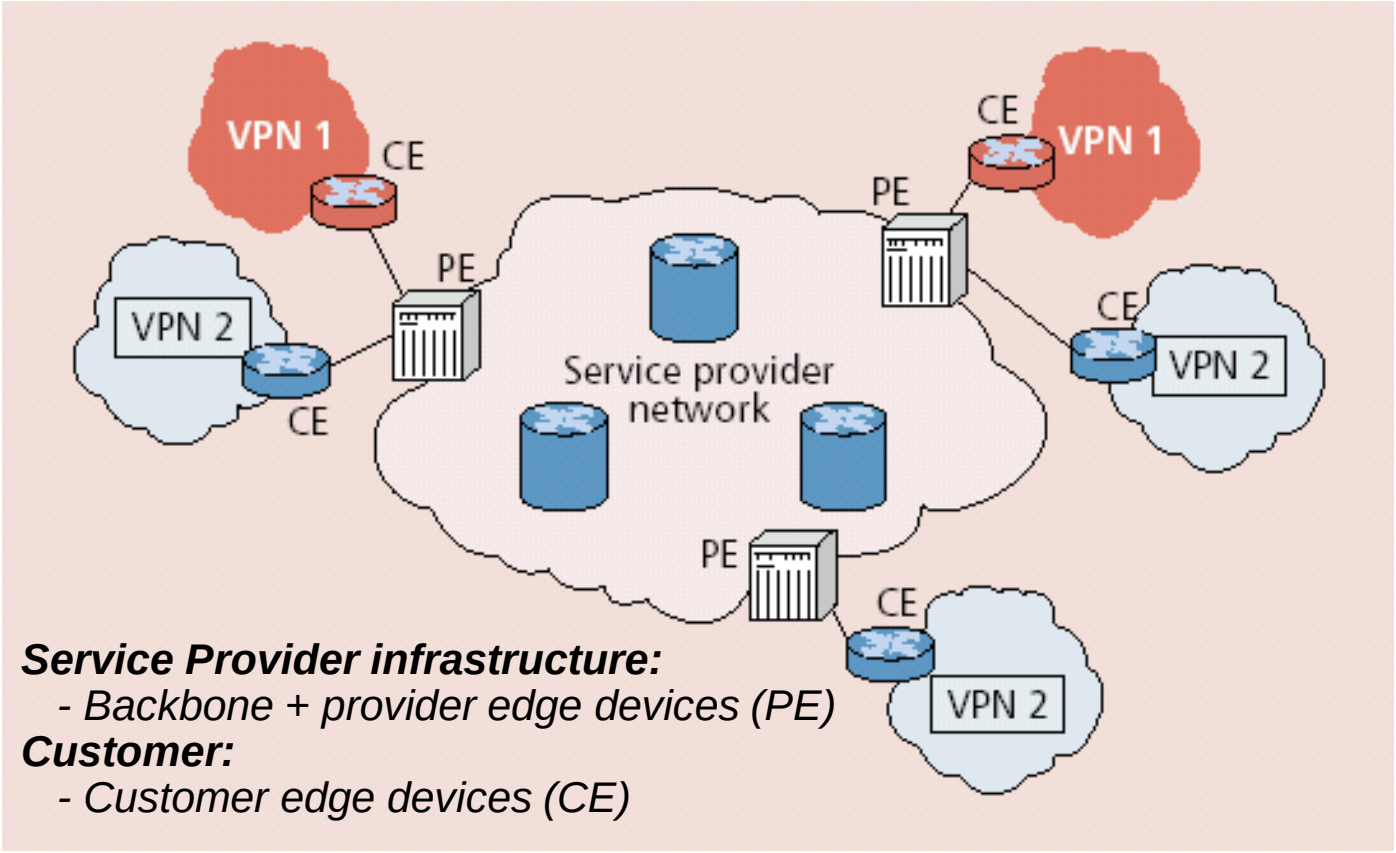


A few familiar examples of external network virtualization:

- Virtual Private Networks (VPNs)
- Virtual Local Area Networks (VLANs)

Virtual Private Network (VPN)

Networks are perceived as being private networks by customers using them but built over shared infrastructure owned by service provider



Service Provider infrastructure:

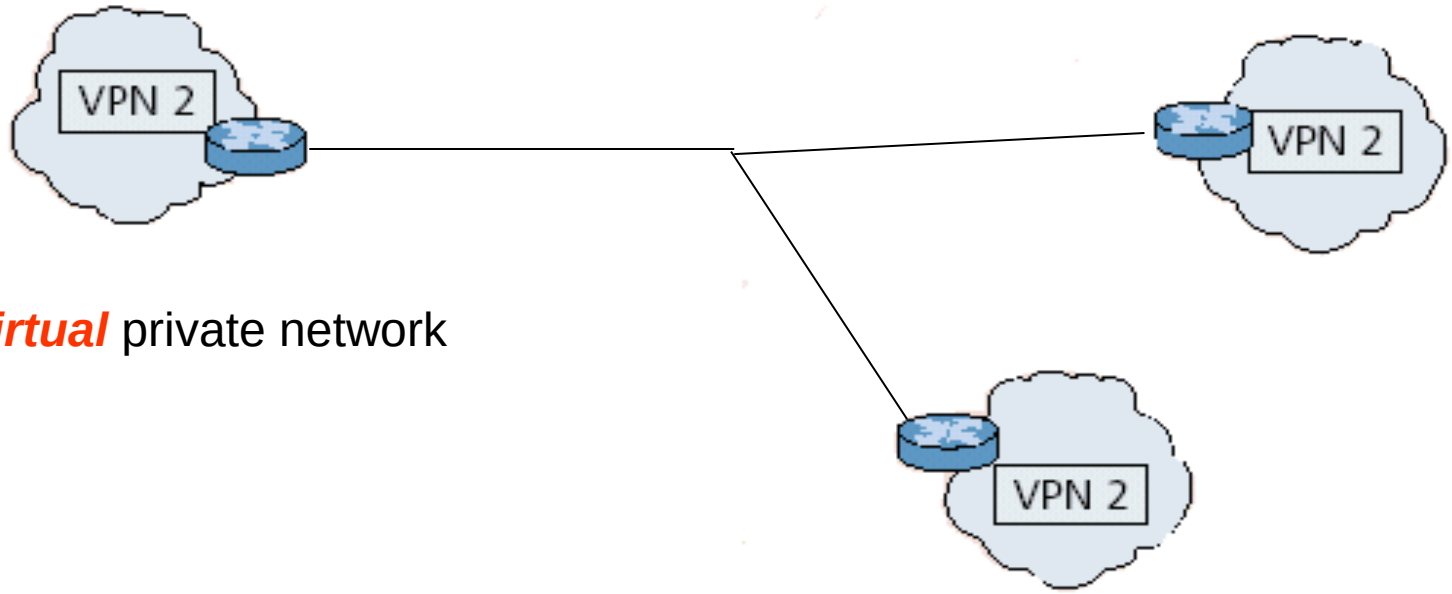
- Backbone + provider edge devices (PE)

Customer:

- Customer edge devices (CE)

Credits: Jim Kurose & Keith Ross

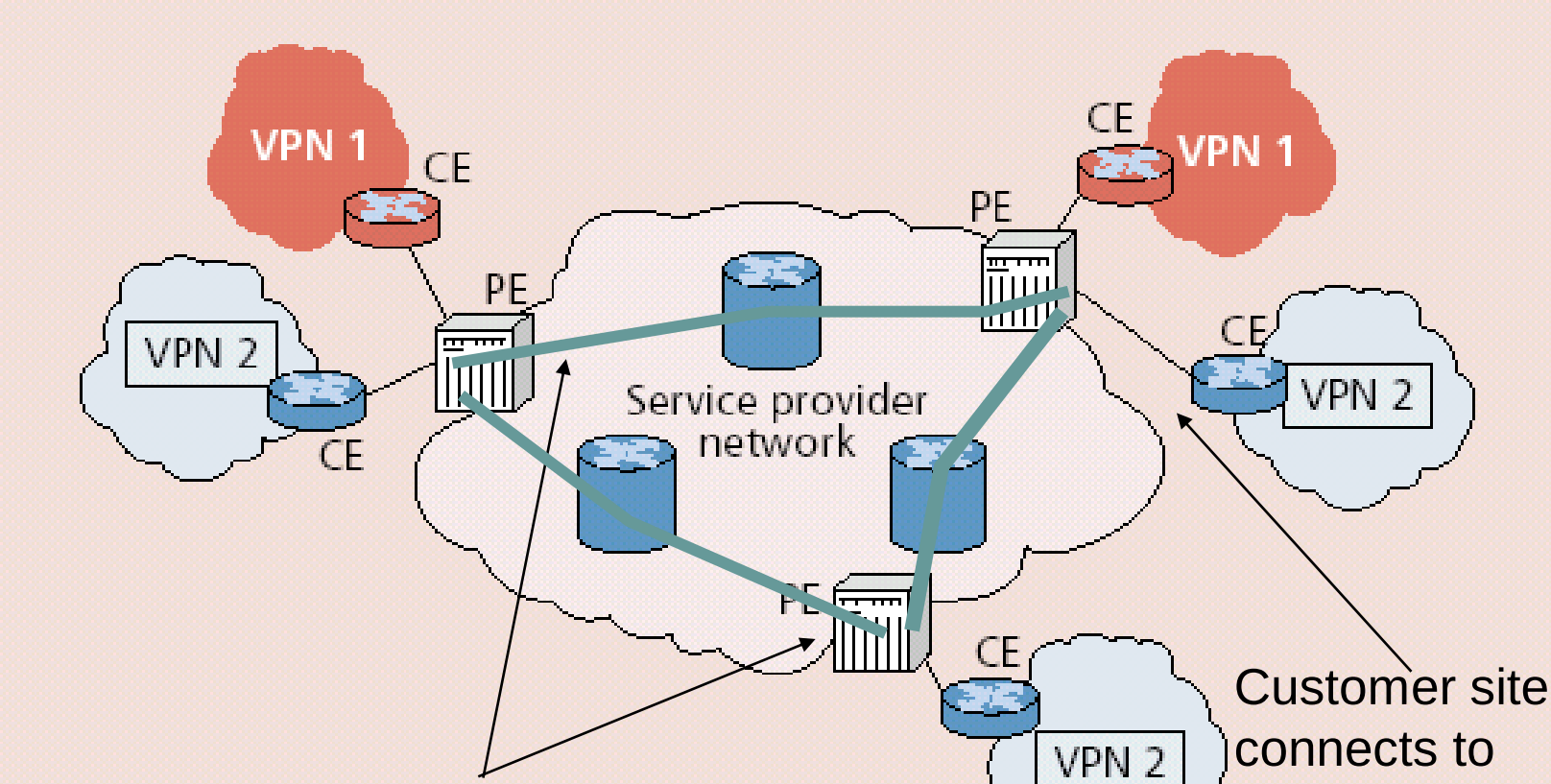
VPN's – Logical View



virtual private network

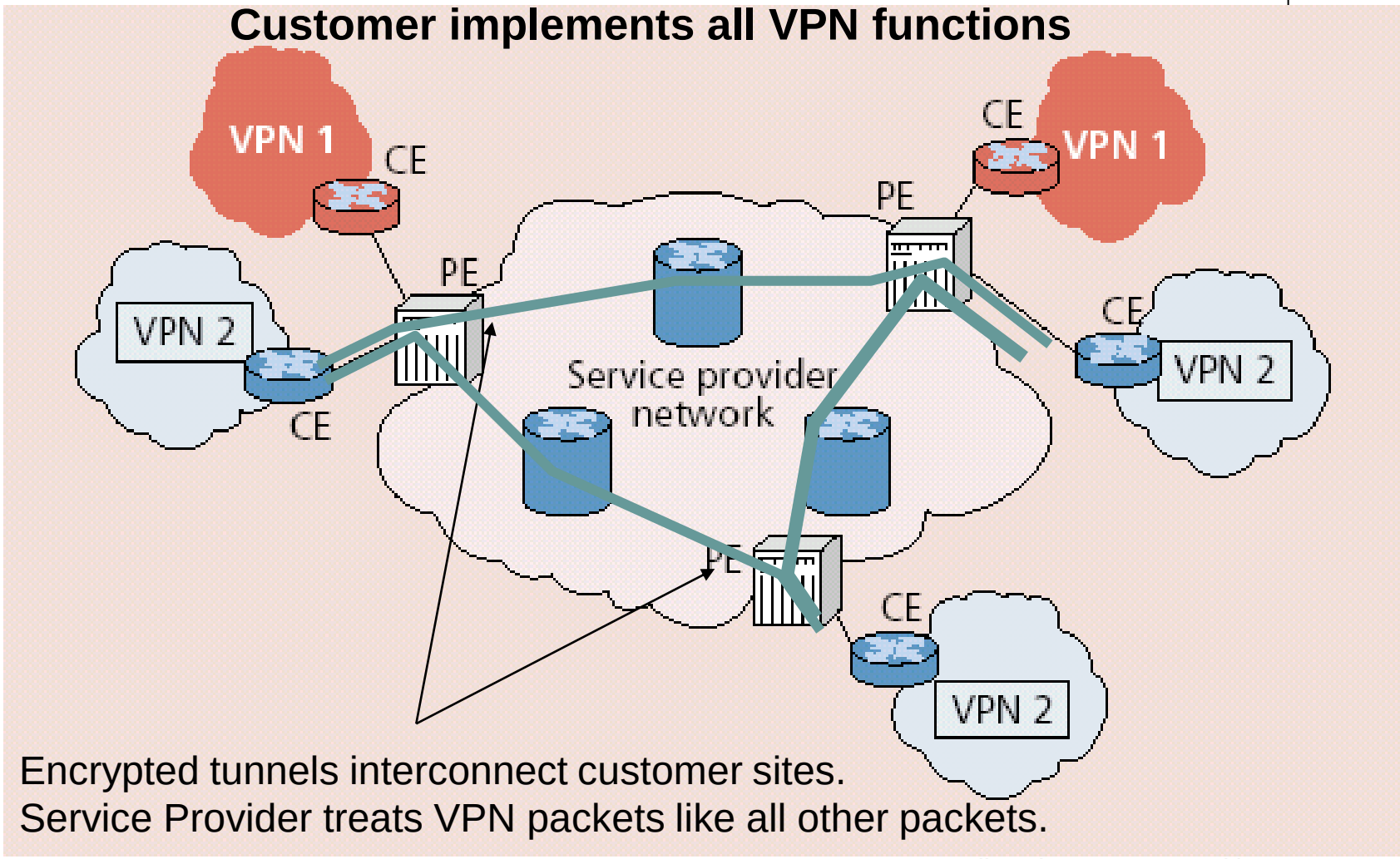
Credits: Jim Kurose & Keith Ross

Alternative A: Leased-line VPN



Credits: Jim Kurose & Keith Ross

Alternative B: Customer-provisioned VPN



Encrypted tunnels interconnect customer sites.
Service Provider treats VPN packets like all other packets.

Credits: Jim Kurose & Keith Ross

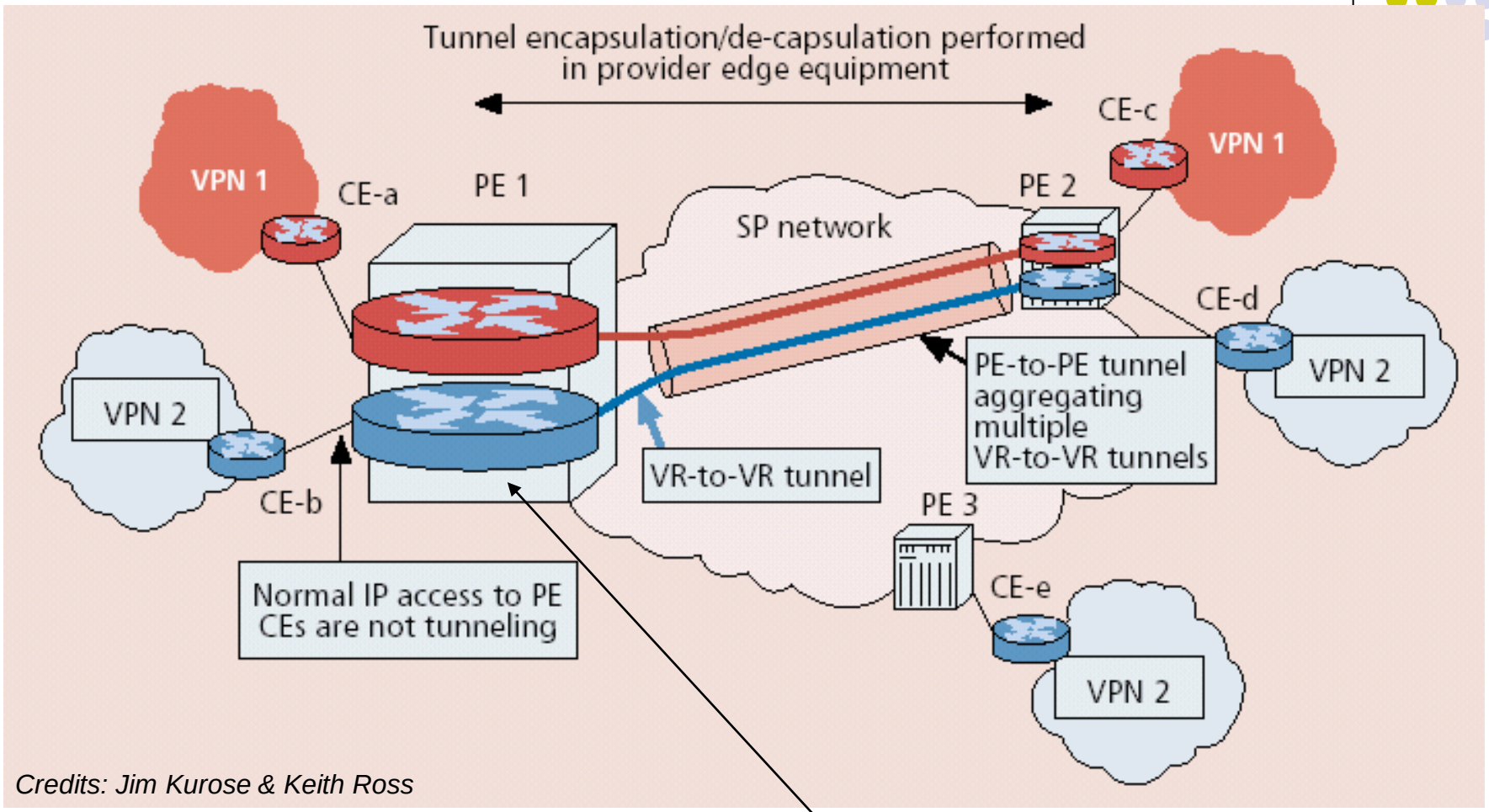
Drawbacks

- **Leased-line VPN (alternative A):**
  configuration costs, maintenance by the Service Provider
  (long time to deploy - weeks, much manpower, higher costs)
- **CPE-based VPN (alternative B):**
  customer needs expertise, no SLA support
  (but still a nice, quick, cost-effective solution for many situations)

Third Option: network-based VPN

- Customer's routers connect to Service Provider routers
- Service Provider routers maintain separate (independent) IP contexts for each VPN
  - Sites can use private addressing
  - Traffic from one VPN can not be injected into another *(at least in principle)*

Alternative C: Network-based Layer 3 VPN

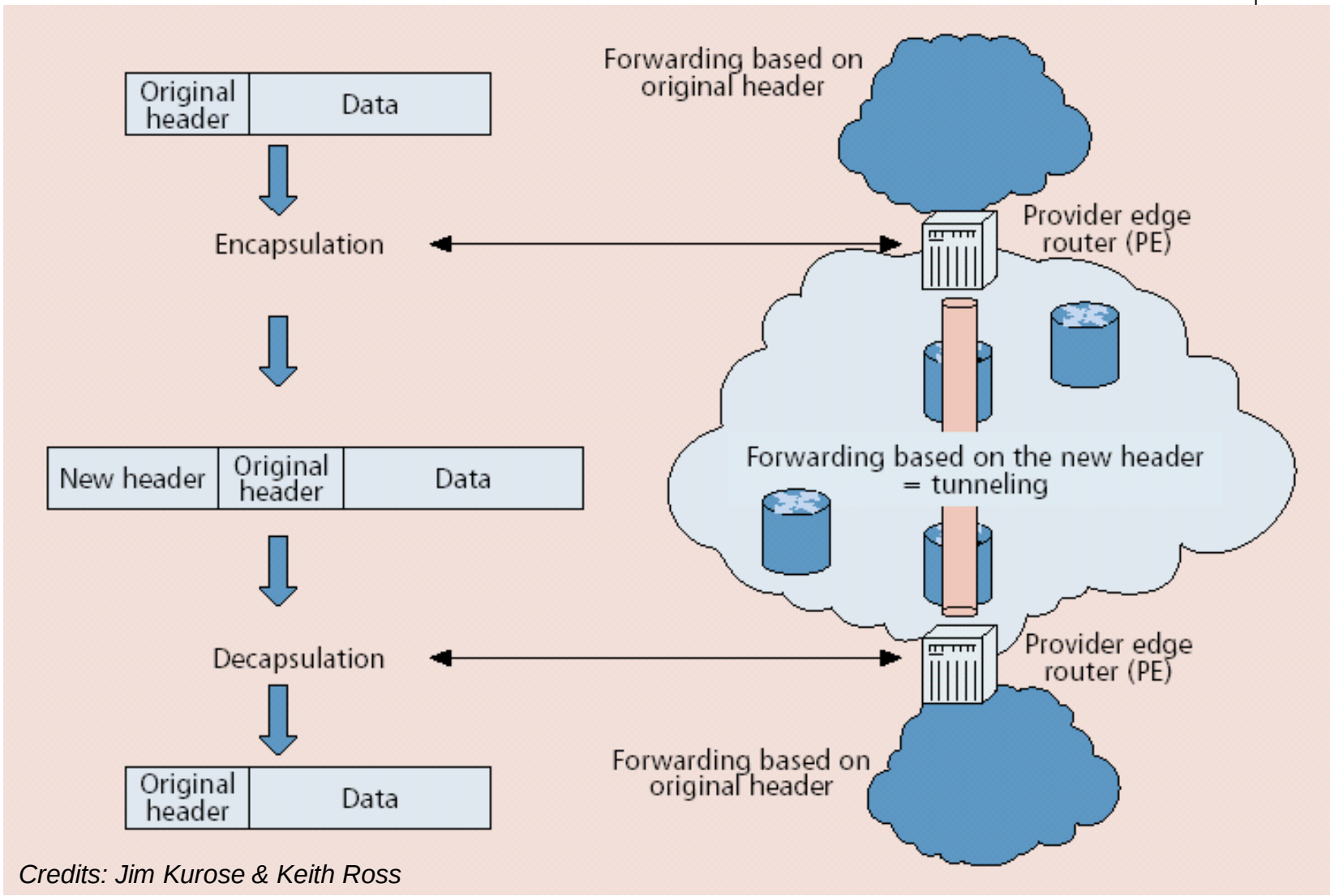


Credits: Jim Kurose & Keith Ross

Multiple virtual routers
in single provider edge device

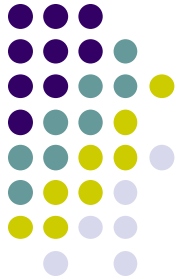
Don't worry if you don't understand all the acronyms!

Tunneling



Credits: Jim Kurose & Keith Ross

VPNs – Advantages



- Privacy
- Security
- Works well with mobility
  (looks like you are always at your office)
- Reduced costs compared with leased lines
  - Ability to share at lower layers, even though logically separate, means lower cost
  - Exploit multiple paths, redundancy, fault-recovery in lower layers
  - Need isolation mechanisms to ensure proper resource sharing
- Abstraction and manageability: all machines with addresses that are “in” are trusted no matter where they are

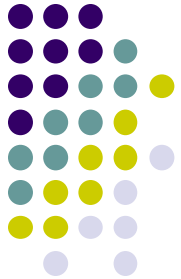
VPNs – A whole world on its own…

- Client VPNs vs. Lan-to-Lan VPNs
- Layer 2 VPNs vs. Layer 3 VPNs
- Encrypted vs. non-encrypted VPNs
- Pseudowire concept (PW), applies to many technologies
- Ethernet over IP tunneling (3378)
- BGP/MPLS PPVPN (RFC 2547)
- L2TP (Layer 2 tunneling protocol, RFC 2661)

...

(outside the scope of SIC)

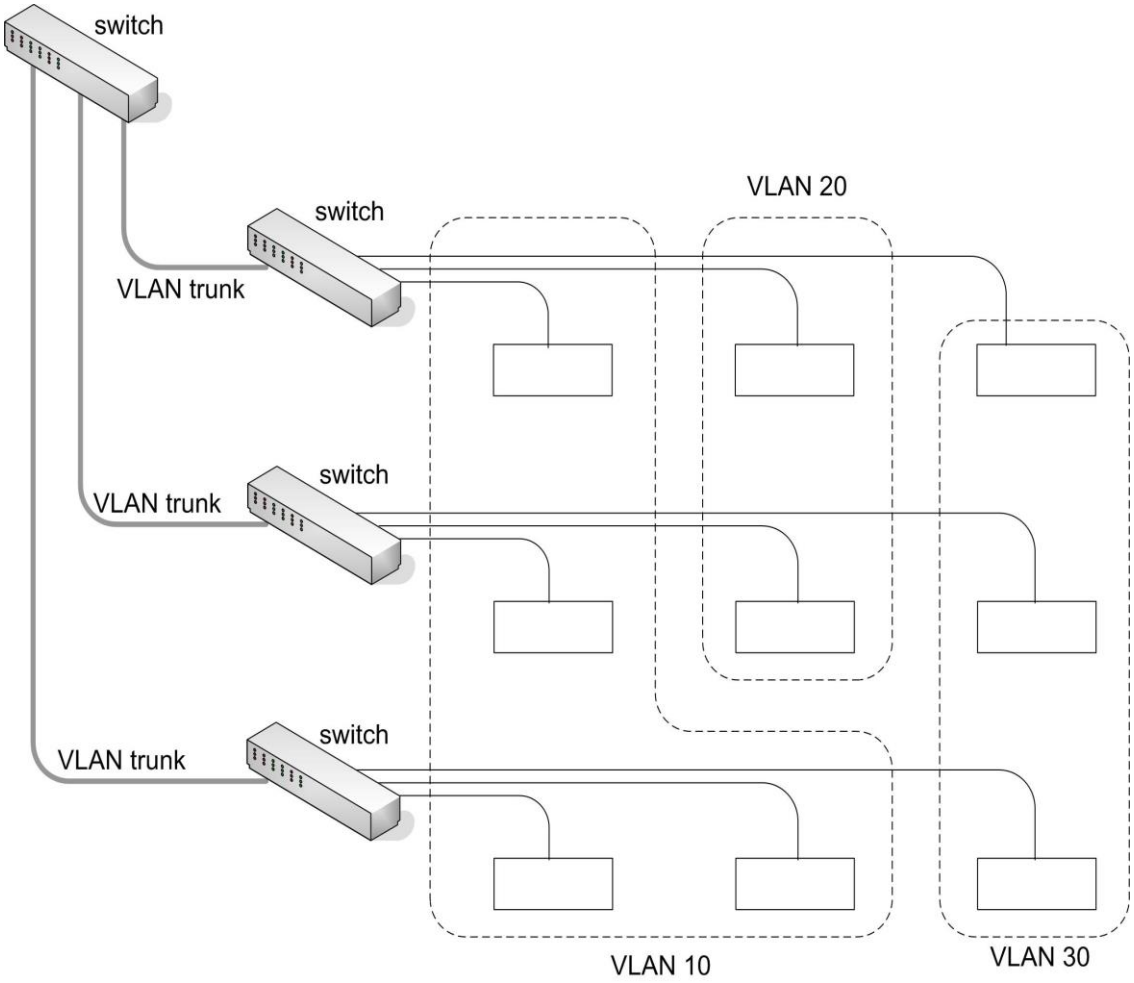
VLAN – Virtual Local Area Networks



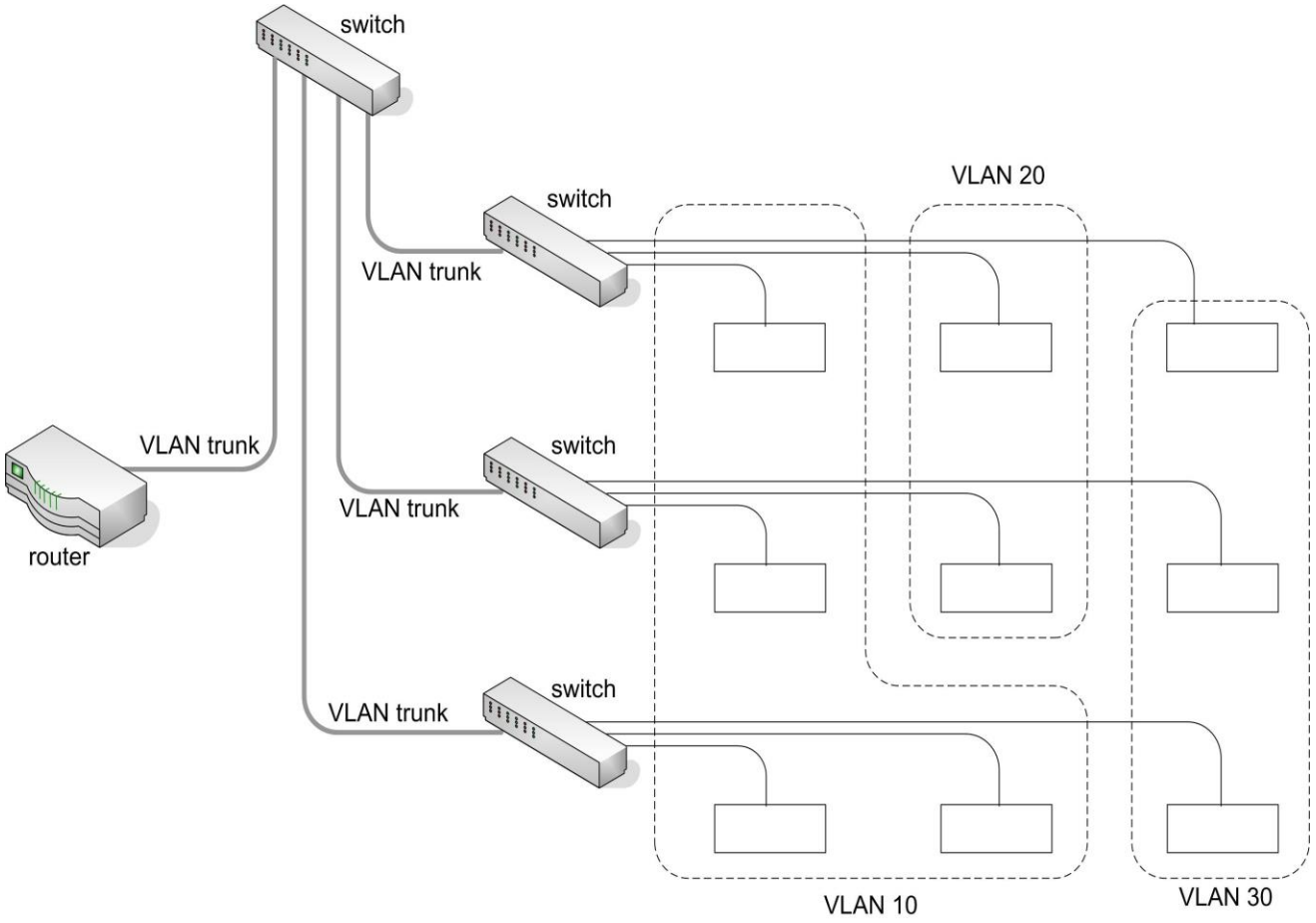
Standardized concept (**IEEE 802.1q**)

- Allows defining groups of network nodes (servers, PCs, printers) that communicate between themselves as if they were on an isolated network
- Multiple logic (isolated) networks in a single physical network
- Traffic between VLANs typically passes by routers and/or firewalls, where access control policies can be enforced

An example of VLAN



Traffic a between VLANs



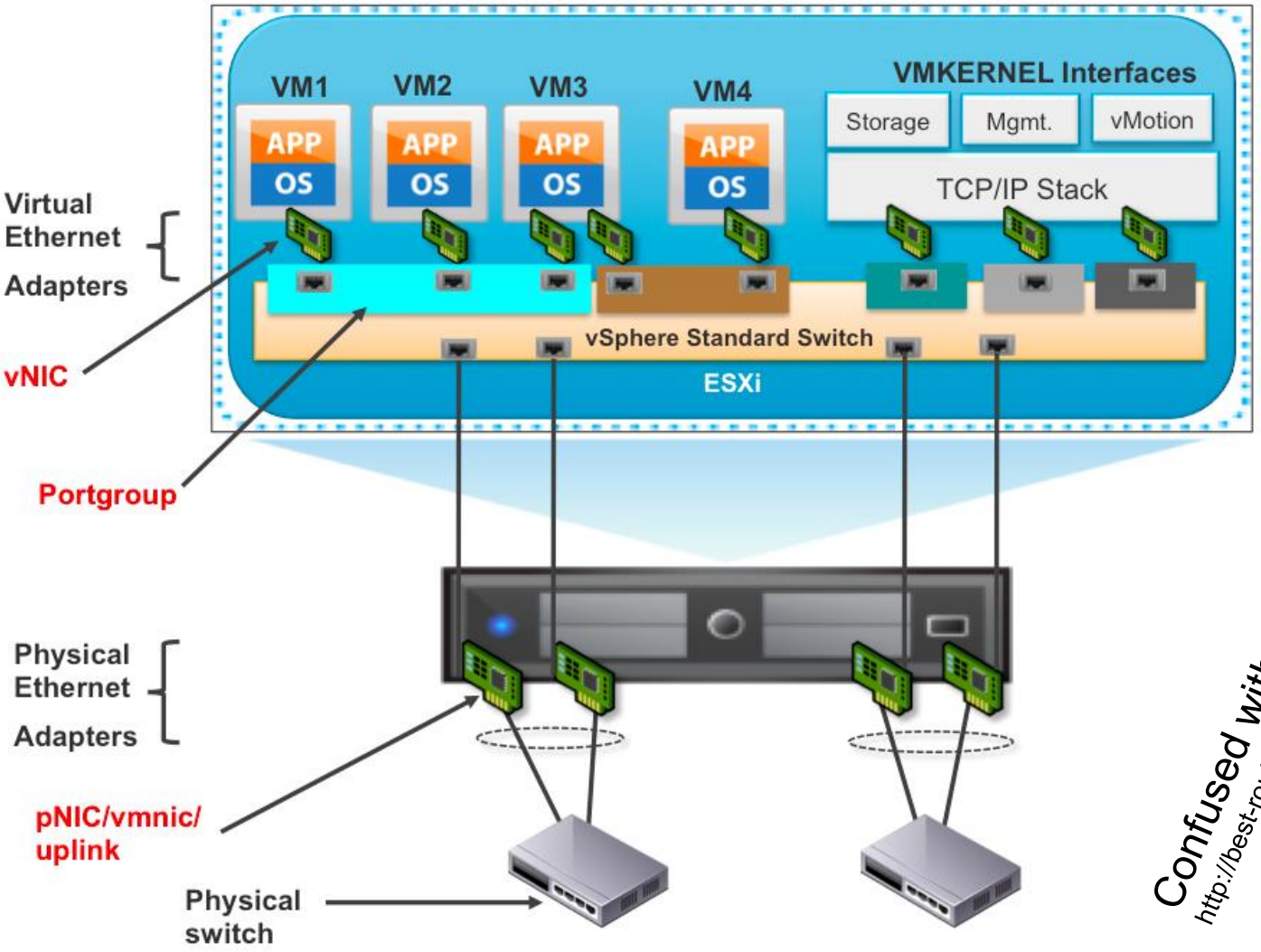
How to assign packets to VLAN's

- Port-based VLANs
- MAC address-based VLANs
- Tag-based VLANs
- Protocol-based VLANs (e.g., based on IP address)
- Dynamic, e.g., based on 802.1x authentication

- Frame headers are encapsulated or modified to reflect a VLAN ID before the frame is sent over the link between switches (**VLAN trunks**, **VLAN tagging**).
- Before forwarding to the destination device, the frame header is changed back to the original format.

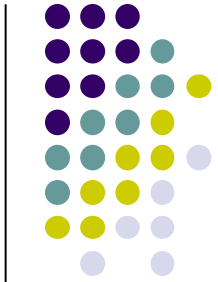
Internal Network Virtualization

- Software-based emulation of physical networks (routers, switches, firewalls, NIC's…)



Confused with pNIC, vmnic, vNIC and portgroups?
http://best-route.blogspot.com/2014/03/network-adapter-nic-vic-vnic-vmnic-niv.html

vNICs

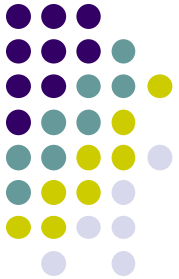


Virtualized Network Interface Cards

- Paravirtualized and/or emulators of real physical NIC
  (still remember the implications of paravirtualization?)

- In the VMWARE ecosystem:
  - vNICs are layer 2 devices
  - Each has its own MAC address(es) and uni/multi/broadcast filters
  - General purpose vNICs…
  - …and specialized vNICs
    (management, vMotion – live migration, iSCSI, and NFS)

Virtual Switch (vSwitch)

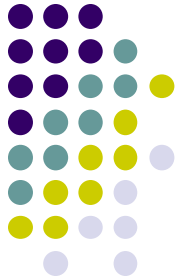


Similar to physical switches, despite minor differences
(e.g., no need to have a spanning tree protocol)

- In the VMWARE ecosystem the ESX Virtual Switch includes:
  - Layer 2 switching engine
  - Support for VLAN (tagging, stripping)
  - Layer 2 security

- Want to have a look outside VMware's world?
  - Take a look at http://openvswitch.org

Virtual Ports, Uplink Ports, Port Groups



Virtual Ports Connect the virtual switch to vNICs (VMs)

- In the VMware ecosystem the ESX Virtual Switch includes:
  - Layer 2 switching engine
  - Support for VLAN (tagging, stripping)
  - Layer 2 security mechanisms

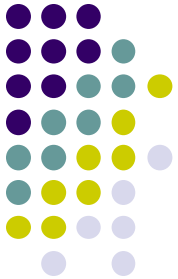
Uplink Ports connect virtual switches to physical switches (uplinks)

- Each vSwitch can be associated with several physical ports

Port Groups define sets of ports with similar configurations:

- VLAN ID's and policies, L2 security options, traffic shaping
- Typically ports in the same group share the same VLAN IDs but there may be more than one port group for each VLAN

VLAN Tagging in VMware



Virtual switch tagging (VST mode):

- One port group for each VLAN
  (more or less similar, though not equal, to “port-based VLAN”)
- vSwitch tags packets incoming/outgoing to physical switches to use “VLAN Trunks” in the uplinks

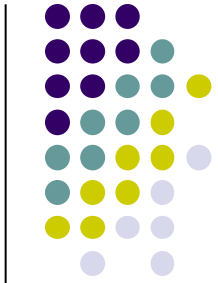
Virtual machine guest tagging (VGT mode):

- Each VM “tags” its packets according to the assigned VLANs
- VLAN trunks are possible between vSwitches and VMs

External switch tagging (EST mode):

- No tagging (and no VLAN trunks) by VM or vSwitch
  (requires one separate uplink per VLAN)

NIC teaming, LB and failover



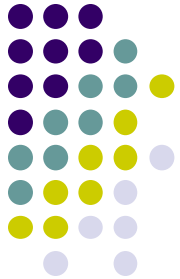
If multiple physical ports are associated with the same port group NIC teaming provides support for:

- **Load Balancing**, including multiple policies:
  - Route based on the originating virtual switch port ID
    (each virtual port always uses the same physical uplink port)
  - Route based on source MAC hash
  - Route based on source IP hash
    (useful when a server has a single vPort but multiple IPs – why?)

    https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2006129
- **Failover mechanisms**, for instance:
  - Link-status only
    (based on link status, does not react to configuration errors)
  - Beacon probing – send beacon probes to detect physical and/or configuration errors.

More reading at http://www.vmware.com/files/pdf/virtual_networking_concepts.pdf

Is the vSwitch tied to a single server box?



Yes and No!

VMware standard (a.k.a. standalone) vSwitch (recalling today's class…)

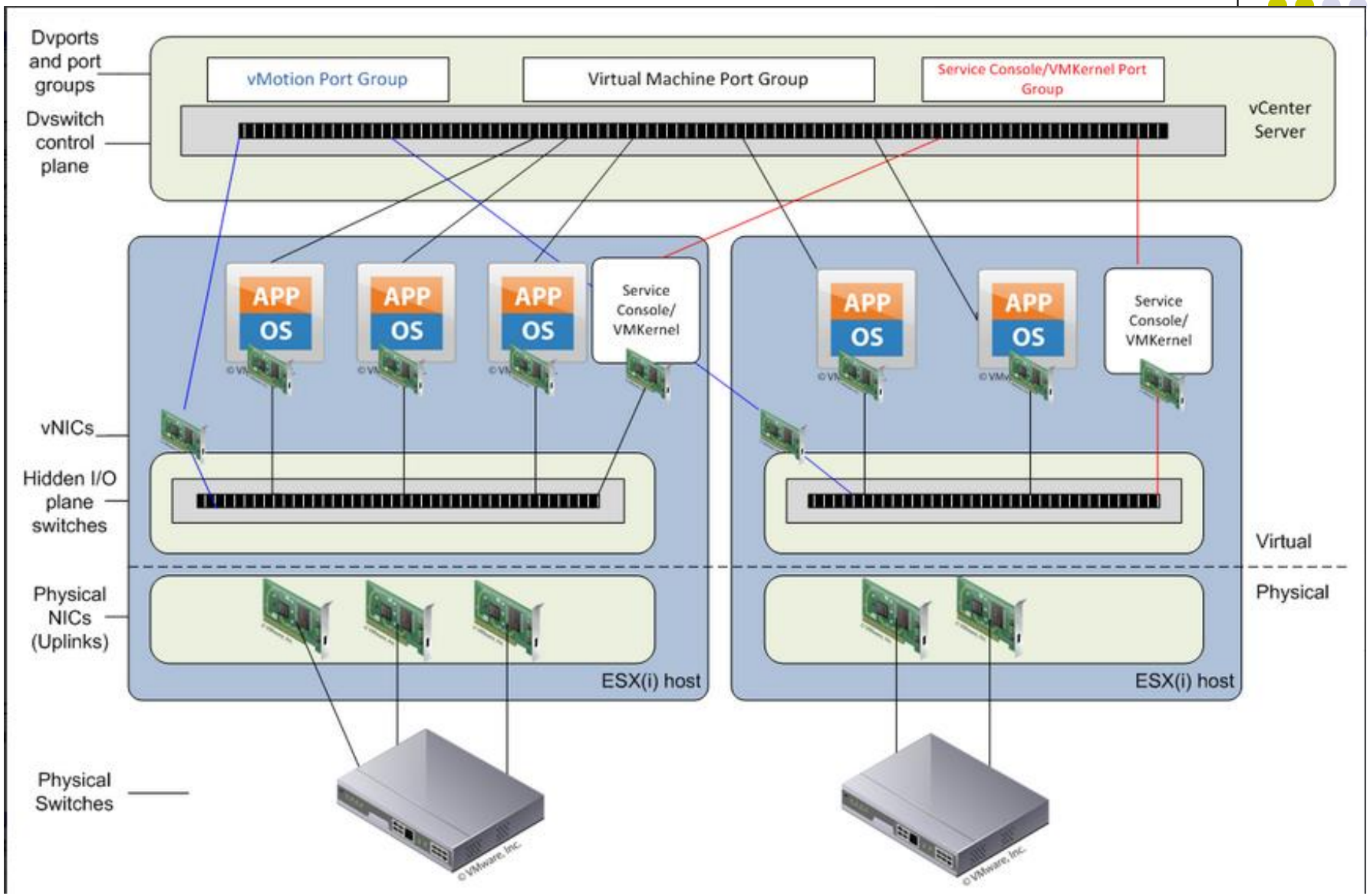
https://www.youtube.com/watch?v=seUXJ6Uy4h8

VMware vNetwork Distributed Switch and vSphere

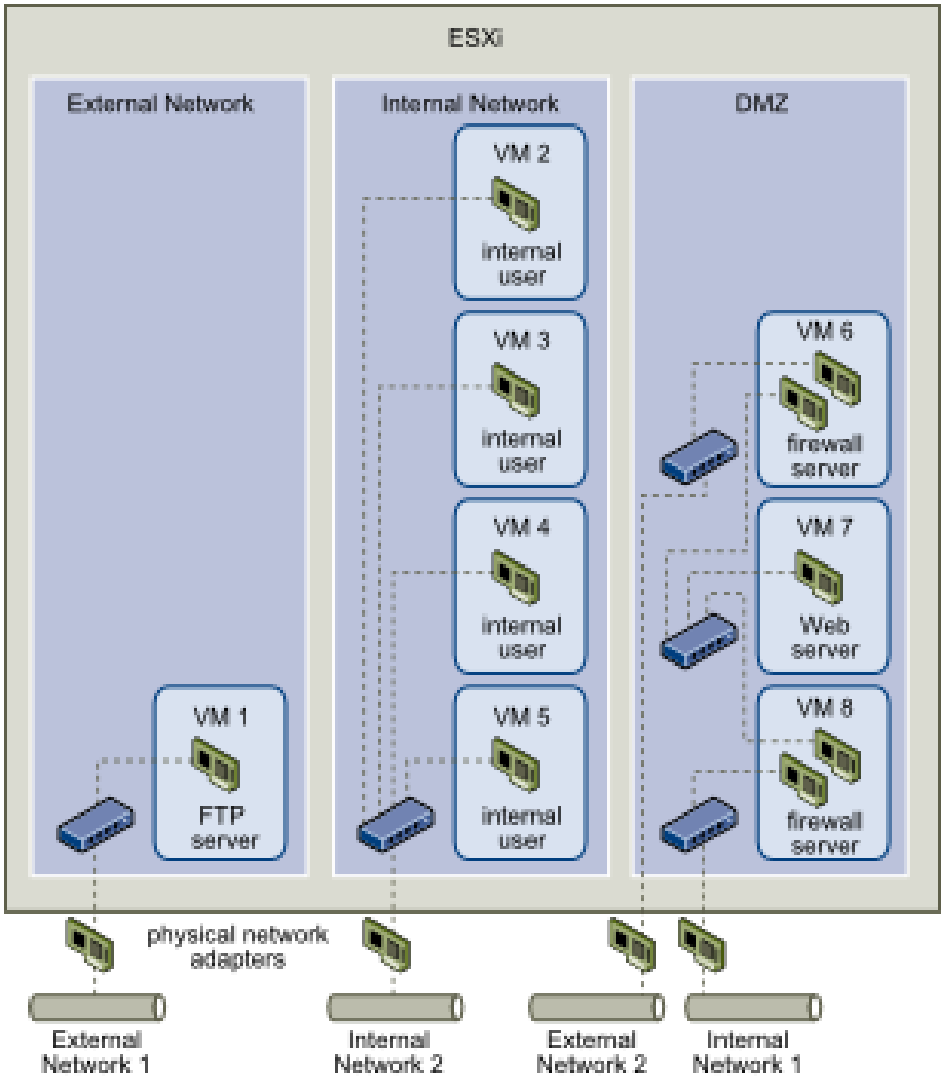
- https://www.youtube.com/watch?v=XZPNvE6PMdM

Distributed vSwitch

data and control planes



A very simplistic example – single vSwitch



Credits & Further Reading

Several slides were inspired by/include content from:

- Slides from Jim Kurose & Keith Ross (introduction to VPN's)
- The various *YouTube* videos provided in the slides
- VMware materials, including:
  - Virtual Networking Concepts
    http://www.vmware.com/files/pdf/virtual_networking_concepts.pdf
  - Virtual Network Design Guide
    https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmw-nsx-network-virtualization-design-guide.pdf
  - Nice presentation with technical content
    https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.networking.doc/GUID-35B40B0B-0C13-43B2-BC85-18C9C91BE2D4.html