

# Hybrid Networks Security

## L2/L3 integration and its security implications

Nicolas Fischbach - Director, Network Architecture

**colt**

smarter / faster / further



RIPE#61 // Nov'10

© 2010 Colt Technology Services Group Limited. All rights reserved.

*The information delivery  
platform for European business*

# Agenda

- 1** Ethernet and IP Services Comparison
- 2** Why Hybrid Networking ?
- 3** Hybrid Networking Solution
- 4** Security
- 5** Questions

# Benefits of Carrier Ethernet and IP Services

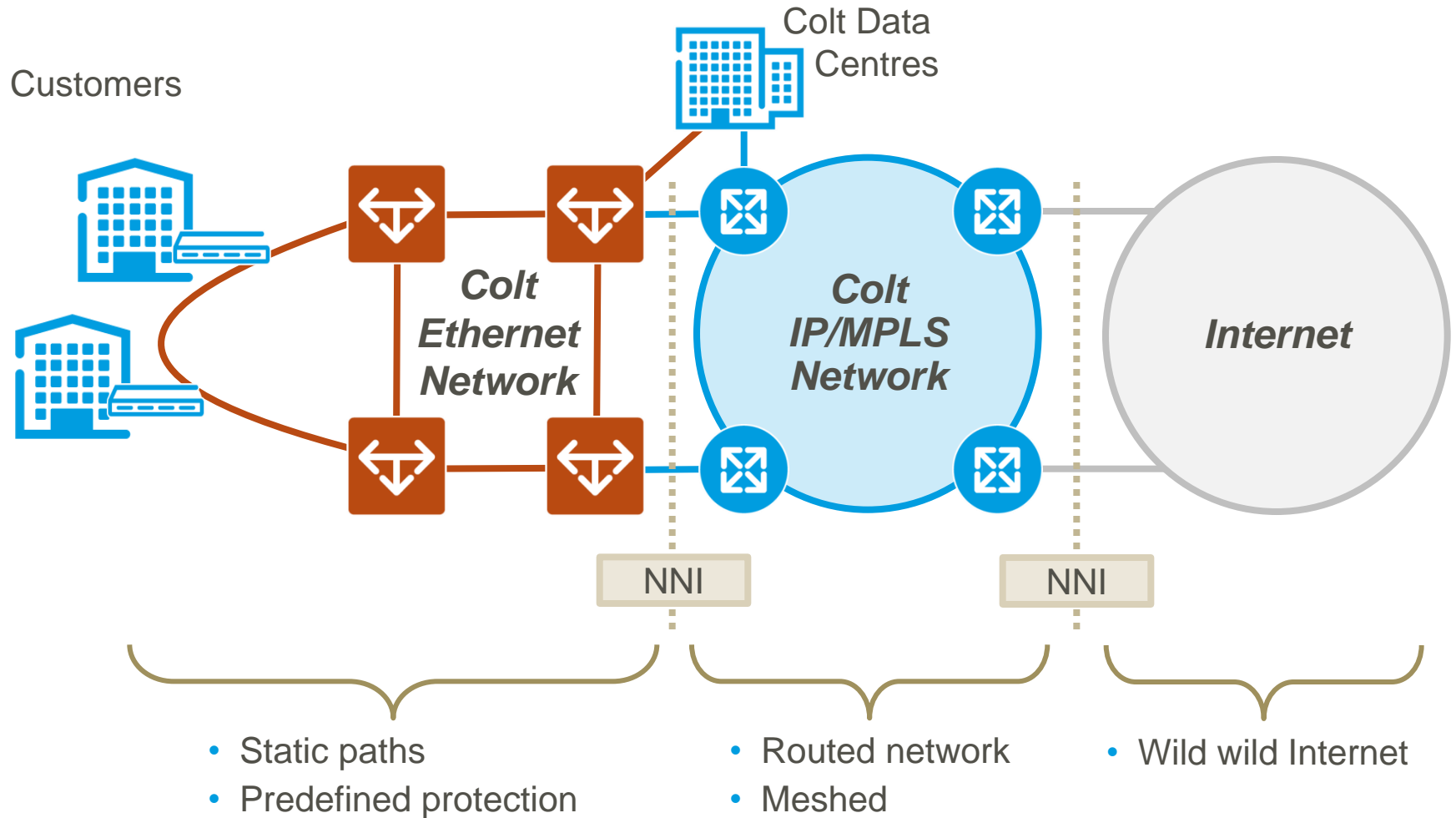
## Ethernet Services

- ✓ Reserved bandwidth
  - ✓ Static path
  - ✓ Dedicated protection path
  - ✓ Low latency & jitter
  - ✓ Transparency for any protocol / application
  - ✓ Security – no switching / address learning for E-Line
- No IP routing in core
  - Connection orientated services
  - Committed bandwidth end-to-end – no traffic shaping

## IP VPN Services

- ✓ Highly scalable
  - ✓ Global reach
  - ✓ Managed IP routing
  - ✓ Meshed architecture – shortest path any-to-any
  - ✓ Distributed protection
  - ✓ Integration with remote access
- IP routed network (Internet)
  - Latency varies
  - CoS used to ensure best latency for priority traffic

# Today: Two networks...

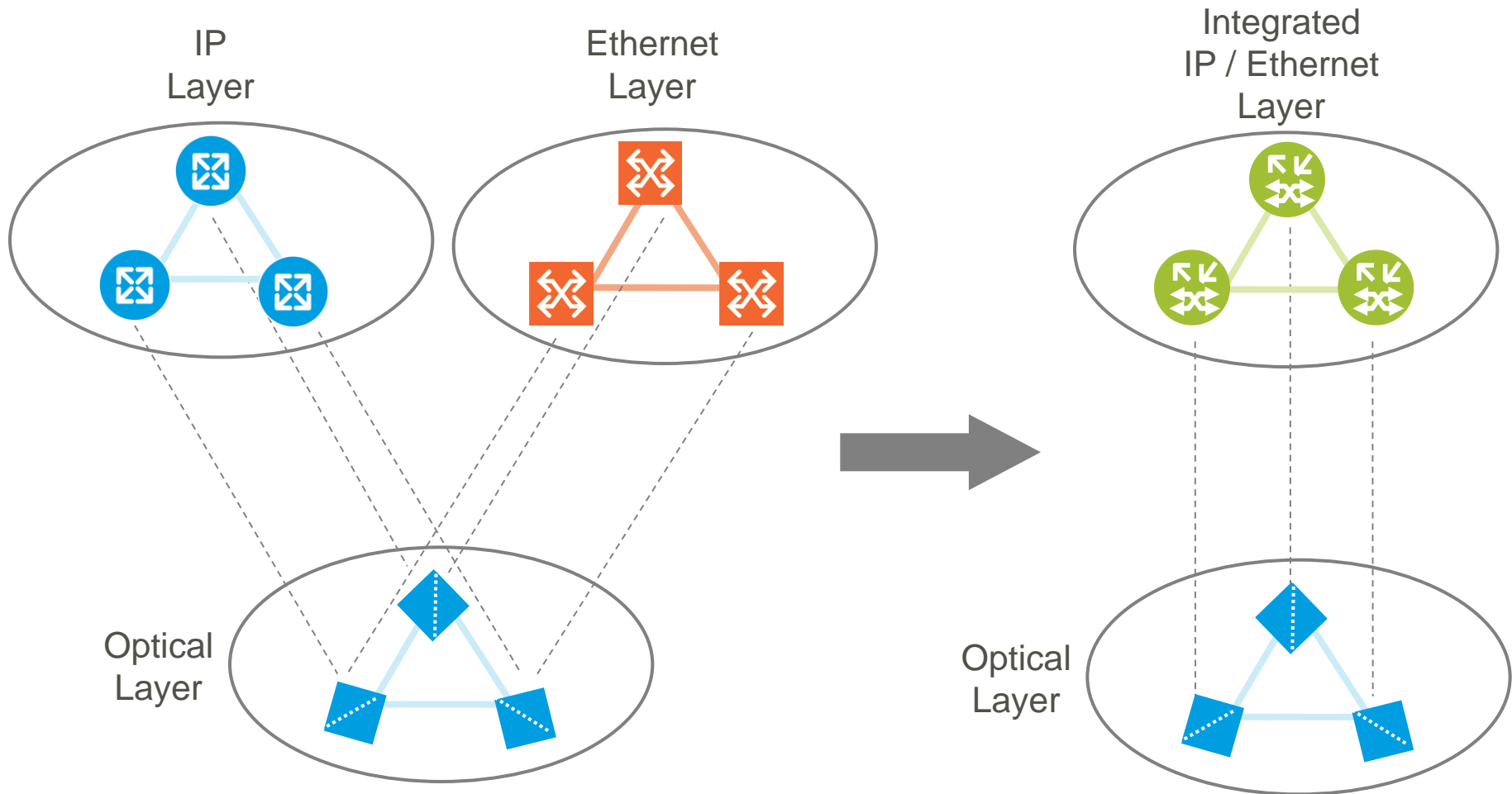


# Why such a separation ?

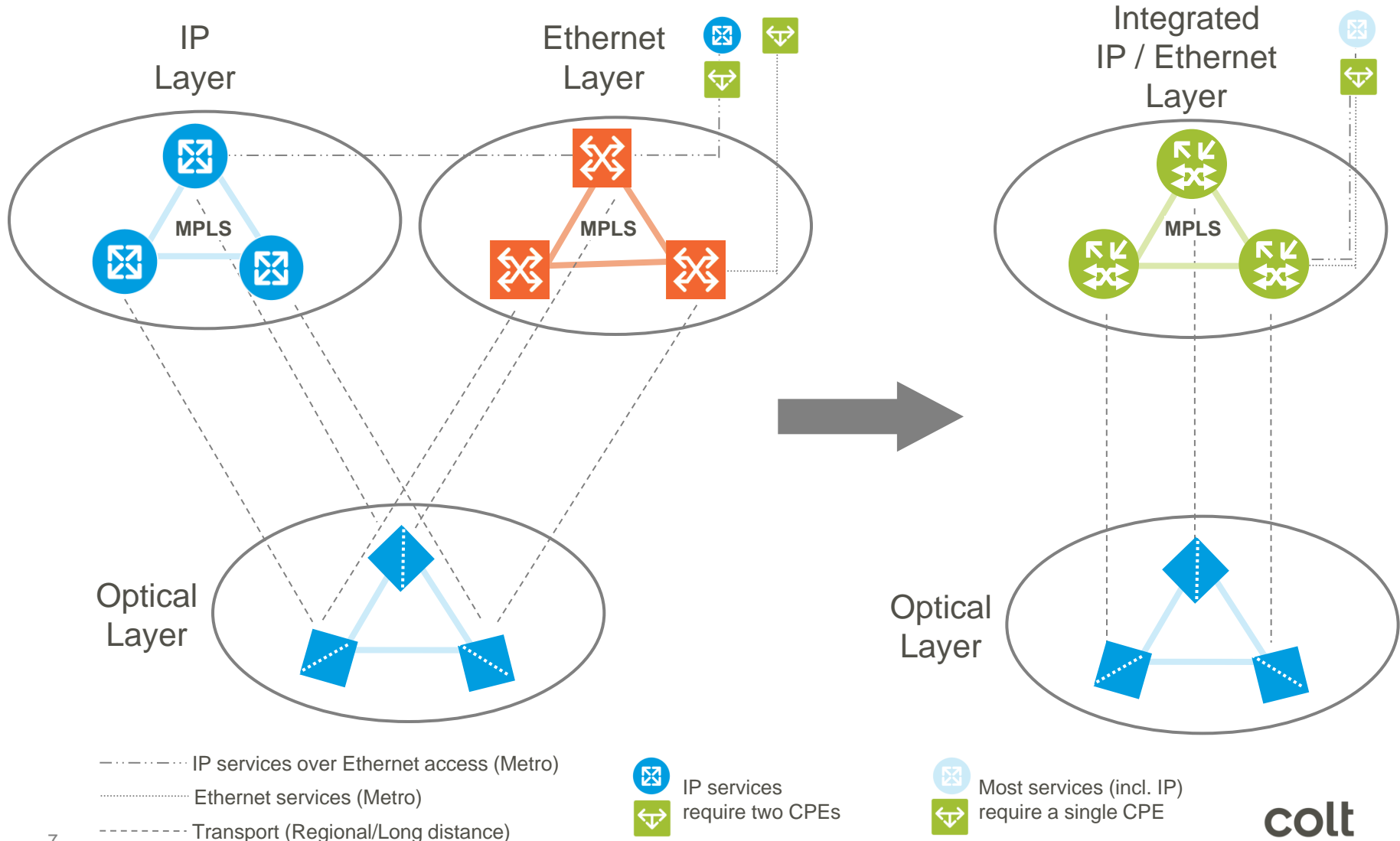
Characteristics	L2 requirements	Gaps (in 2007)
Protection	Sub50ms	BFD, FRR, ... not supported in the L3 core
QoS	Hard QoS & dual colour rates	None deployed in the L3 core
Provisioning	End-to-end point & click	Automated but more complex
Bandwidth scaling	Hard QoS for CIR in the core (per service instance)	L3 core « too small » to serve the L2 traffic forecasts
Security	« Private » network	Internet-originated risks

- What are today's challenges for hybrid networking ?
  - Mostly psychological ?
  - Simplify here, augment complexity there ?
  - Weaken "strong" L2 services because of alignment to L3 (IP) capabilities and shared L2/L3 infrastructure ?
  - How to transport "Internet" traffic and manage/guarantee availability and security

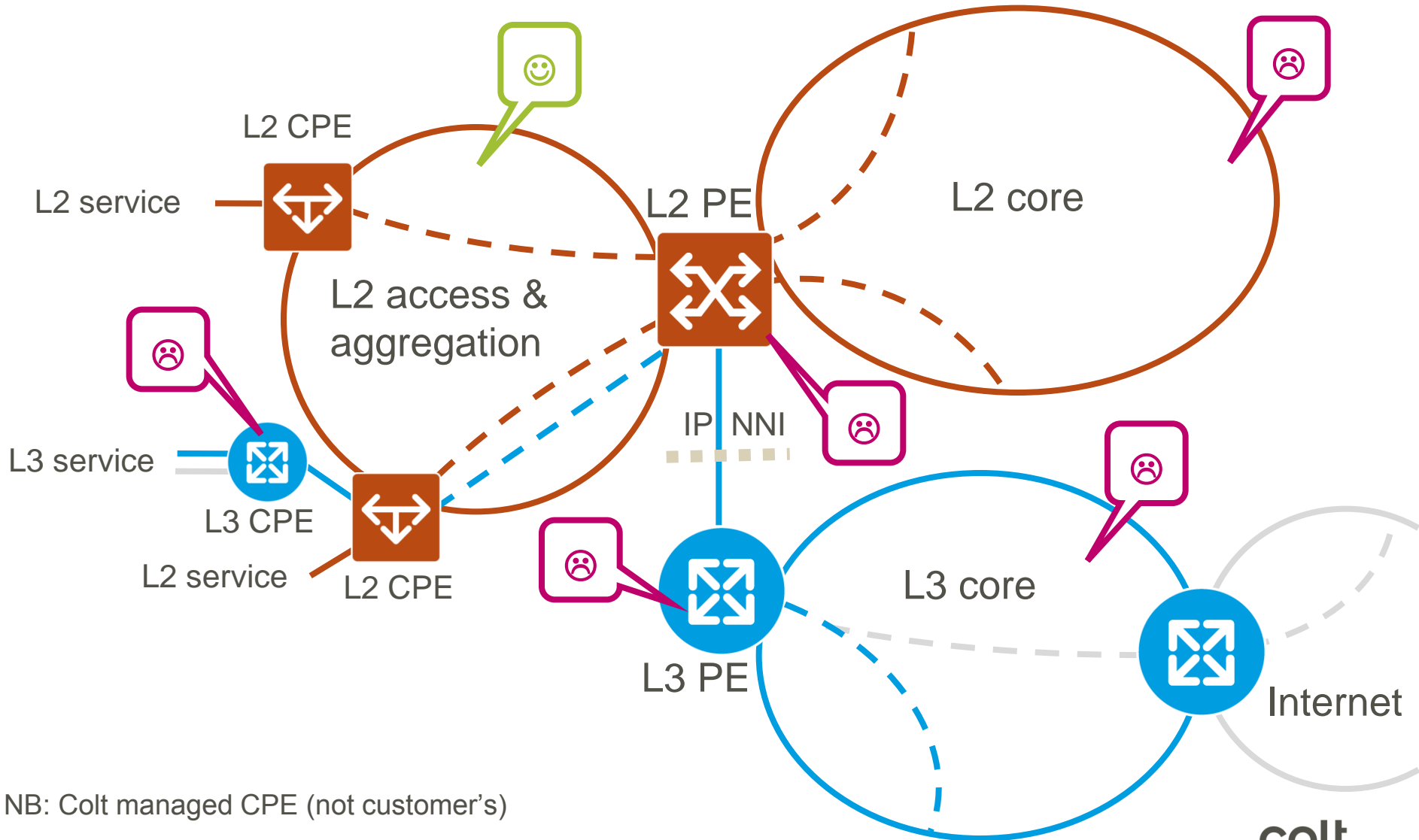
# IP and Ethernet Network Integration



# IP and Ethernet Network Integration (Service View)

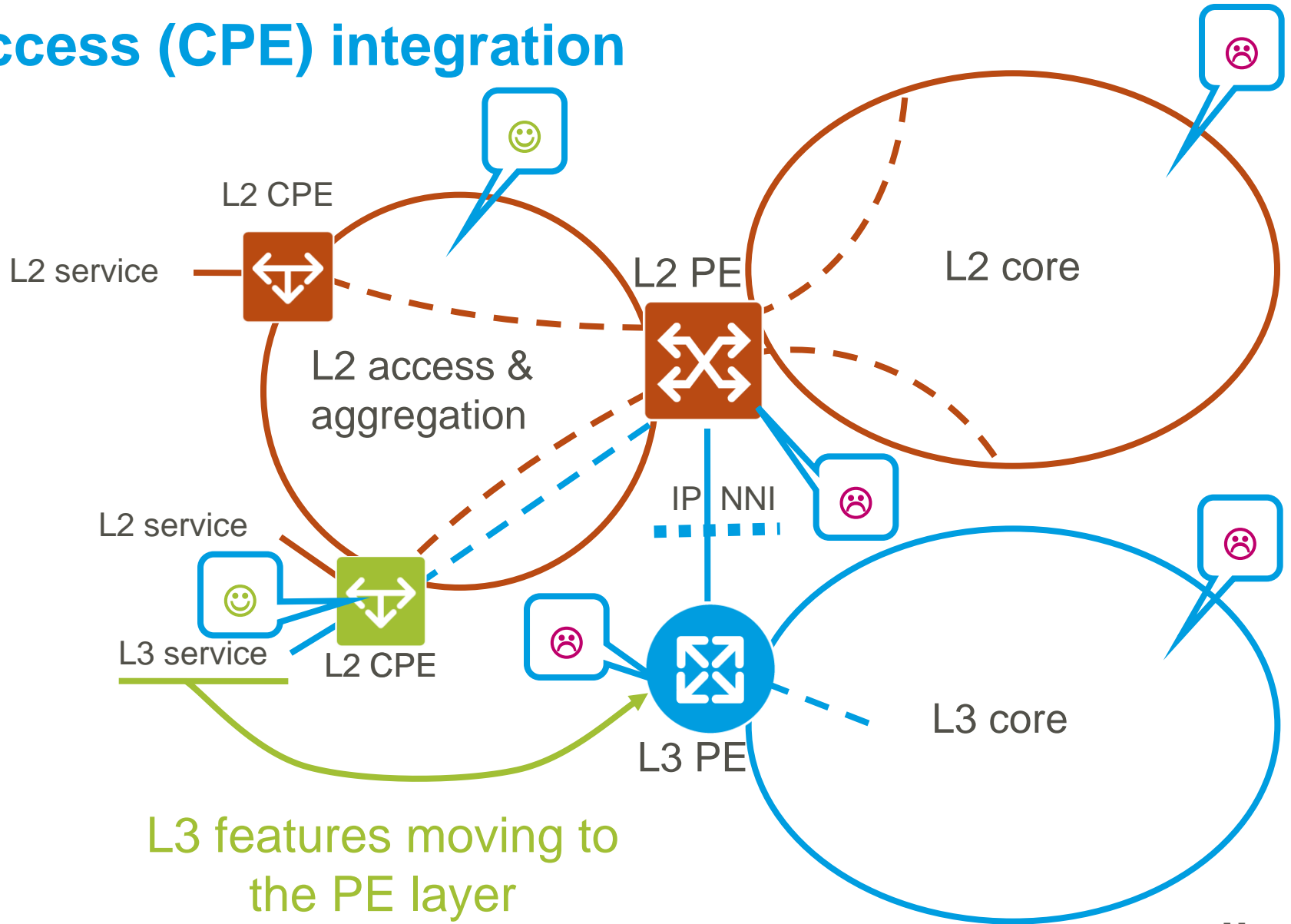


# Three areas to simplify (and secure)

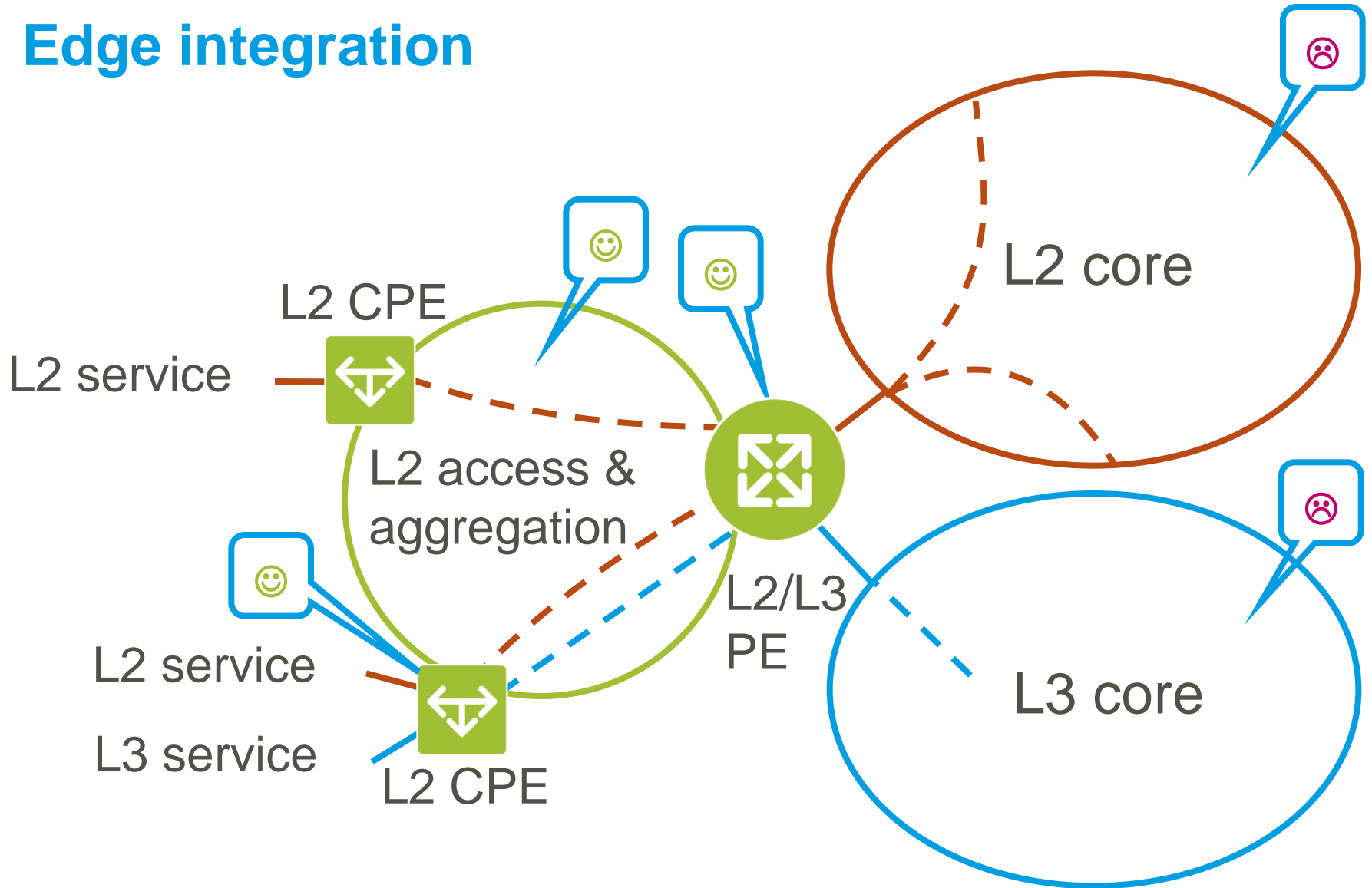


NB: Colt managed CPE (not customer's)

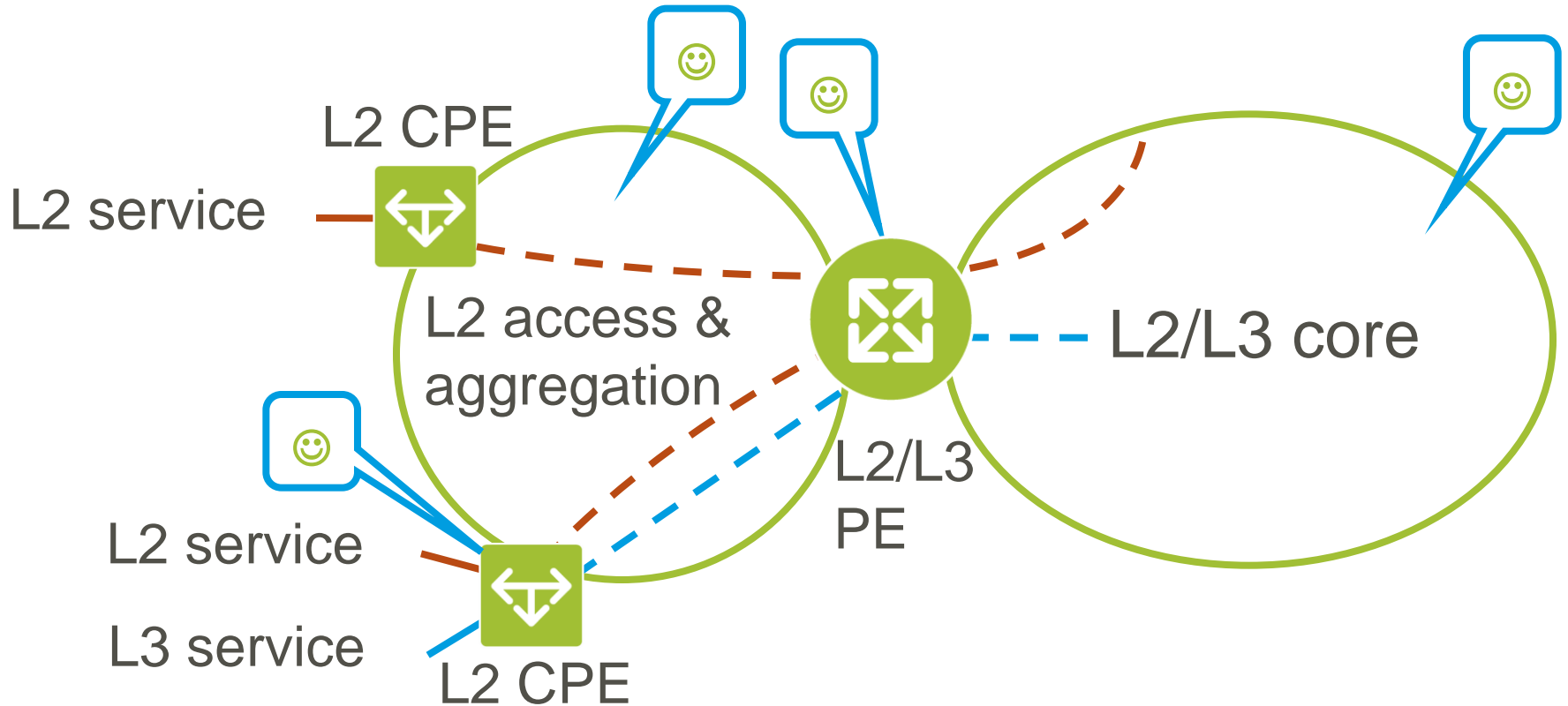
# Access (CPE) integration



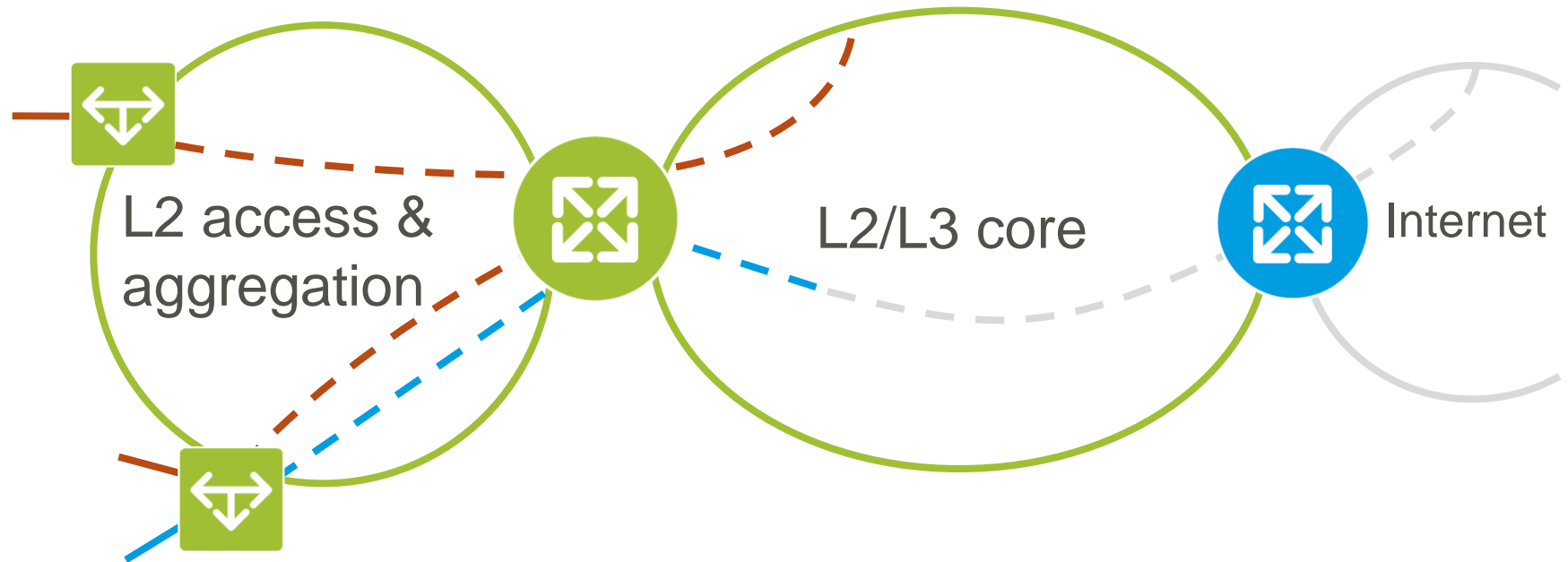
# Edge integration



# Core integration

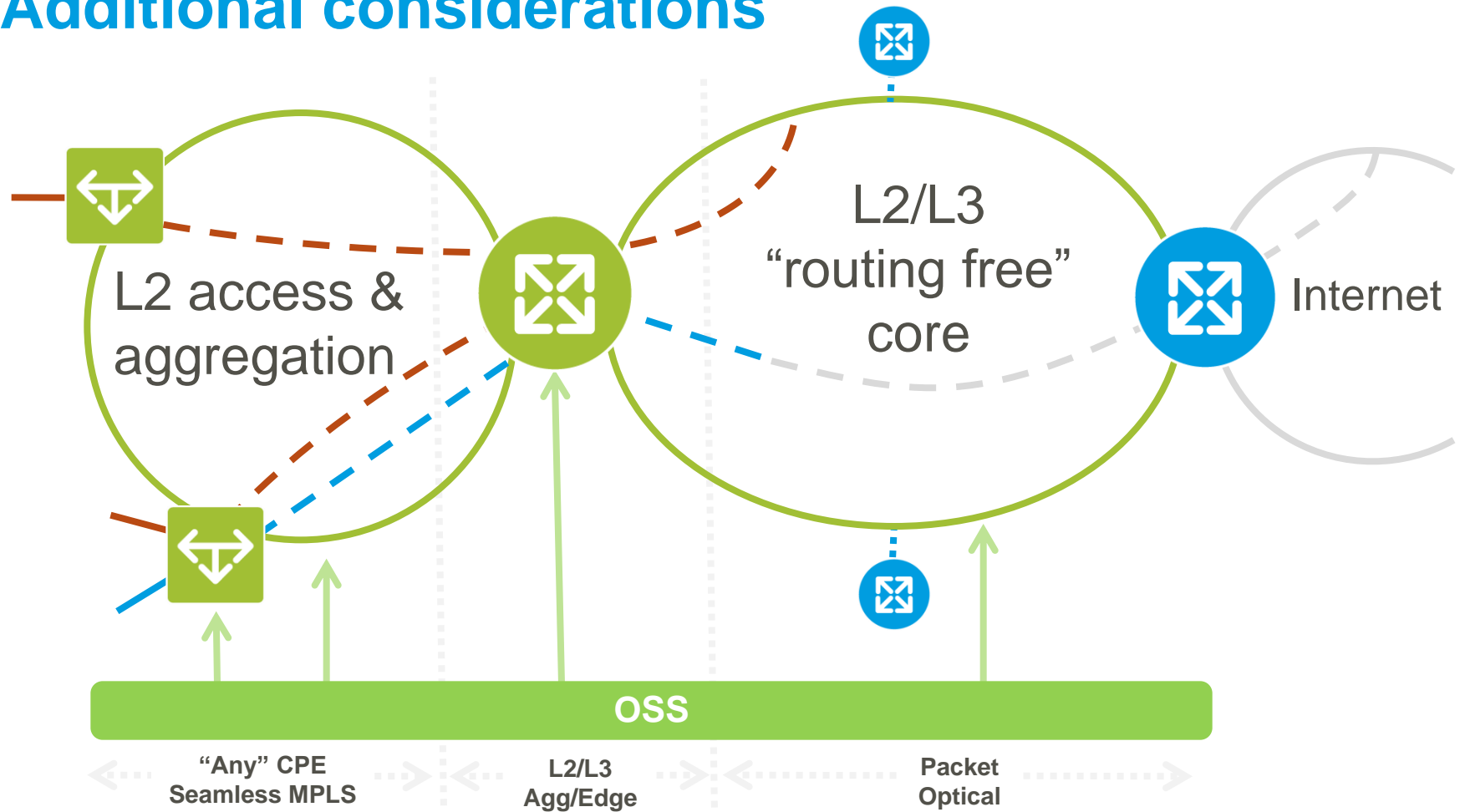


# Simplified e2e view



- Services: **Carrier Ethernet**, **IP VPN** and **IP Access**
- Access/Aggregation: 2 to 4 layers depending on Tier model (incl. PE)
- Core (P): 2 routers per city
- MPLS NNIs and IP Peering/Transit: 1 per IX, multiple IXes

# Additional considerations



- IPv4/v6 and VPNv4/v6 Route Reflectors and Multicast
- OSS and Dual Vendor Approach

# Security requirements / issues

- MPLS only core (“No routing”)
  - Run the Internet in a VRF
- “Out-of-band” management (which requires routing)
- Properly defined planes and plane separation
- Layer 2 broadcast domain and security features
- Per-VRF/RI features
  - General and per (sub)interface
- Fine grained AAA (CLI, XML-type APIs, etc)
- Netflow v9/IPFIX
- All/Most security enforcement features in hardware (incl. IPv6 !)
- Bandwidth / QoS management

# Conclusion / Next Steps

- Carrier Ethernet continuity is an absolute requirement for Colt L2 products
- Ability to blend IP (Access/VPN) and Carrier Ethernet services
- Security (especially availability, segmentation and visibility) is key
- Network automation is a must
- Next steps
  - Dual-vendor solution (incl. umbrella OSS for Service Delivery, Service Activation and Service Assurance)
  - Progress research on L1/L2/L3 integration (incl. MPLS-TP)

# Thank You ! Questions?

Nicolas Fischbach - Director, Network Architecture

[nico@colt.net](mailto:nico@colt.net)

**colt**

smarter / faster / further

