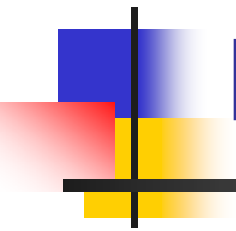


Metro Ethernet

Feedback from the field

Thomas Kernen, Technologist, SIG thomas(at)ip-man.net

Agenda

- Project background
- Design considerations
- Security
- Lessons learnt
- MetroE Business Services

Project background

- Unique in Switzerland (Fibre To The Home). Allowing the average residential consumer to discover the richness of web content, without the constraints of the ‘last mile’ copper ‘bottleneck’
- A pilot, to gain operational experience and to test acceptance and behaviours of end users.

From a technical standpoint

- The network design is service agnostic, no focus on a specific service but on a concept of IP packets with QoS and *security*
- 1 pair of single-mode fibre from the POP to the customer, per customer (last/first mile).
- 1 CPE per customer with 3x 10/100 switched Ethernet ports, 2x POTS
- No basement devices to reduce security issues
- 100 Mbps uplink per customer, 100BASE-LX10 (802.3ah draft 1.3)
- 1 PVLAN per service for isolation and per service QoS and security
- Authentication and authorisation for services using DHCP linked to the CRM solution
- Walled garden for unauthorised/unregistered or “quarantined” users (virus infected PCs, spammers, ...)
- Initial services: 10 Mbps per user for Internet access, streaming video from portal
- Future services: 90 Mbps spare for Live TV, HDTV, telephony, storage, e-learning, the next killer app, etc...

Design Considerations

- “Open” network model
- Deployment time-frame
- Cost of trenching within the urban area of Geneva
- Capex vs Opex

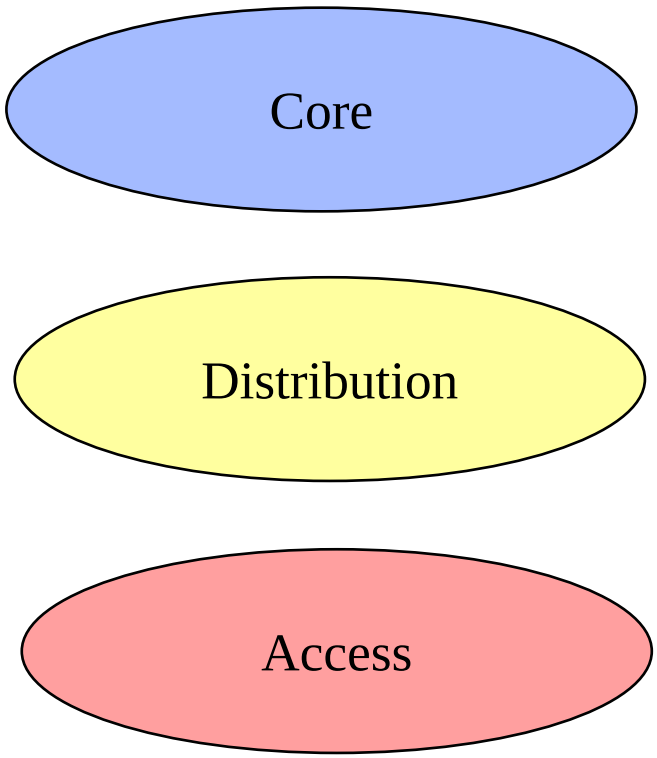
The typical ETTx environment

This is a true Multiservice network

- **Broadcast TV, distributed via Multicast: 4-7 Mbps or more per channel (up to 30 Mbps for HDTV channels)**
- **Telephony using VOIP (G.711)**
- **Video On Demand / Personal Video Recorder using IP unicast**
- **Normal Internet traffic**

All this together requires QoS

The typical ETTx environment

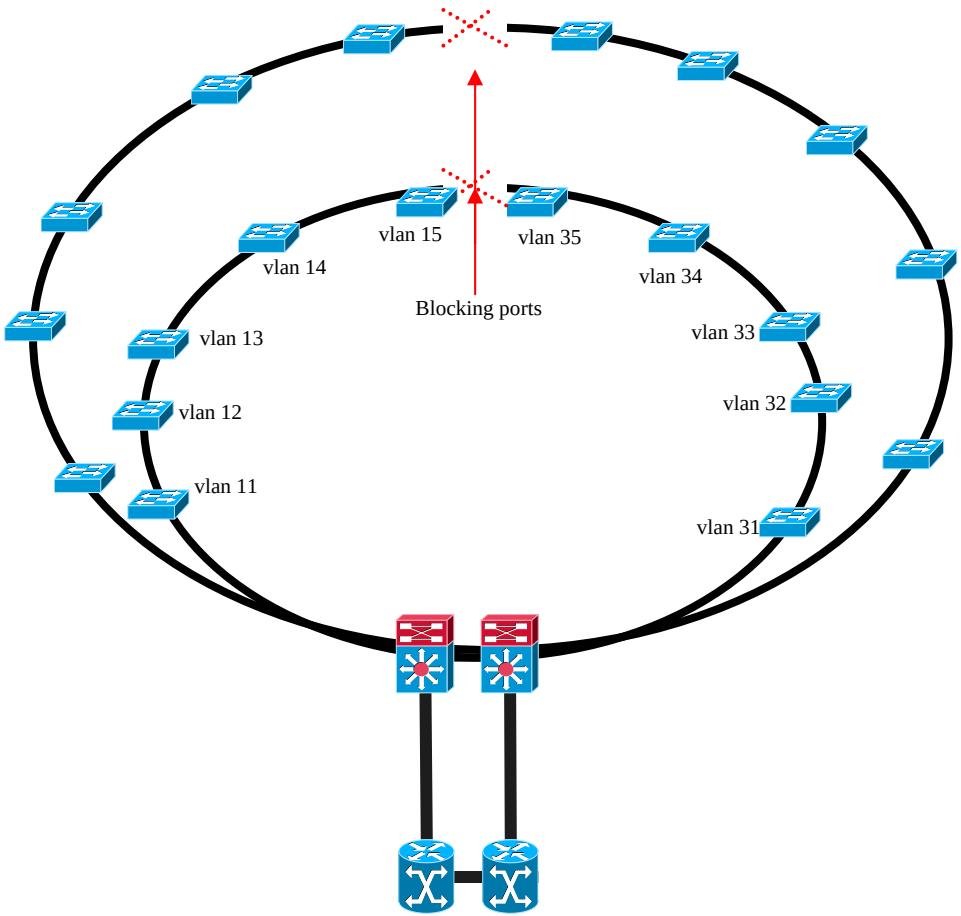


Normal networking model, IP or MPLS core In the Cisco design GSR or 7600

Distribution, L3 routing. In the Cisco design 6500 or 7600

Access, L2 (rapid spanning tree – 802.1sw) or L3. In the Cisco design 2950, 3550 and the 4000.

The typical ETTx environment, L2



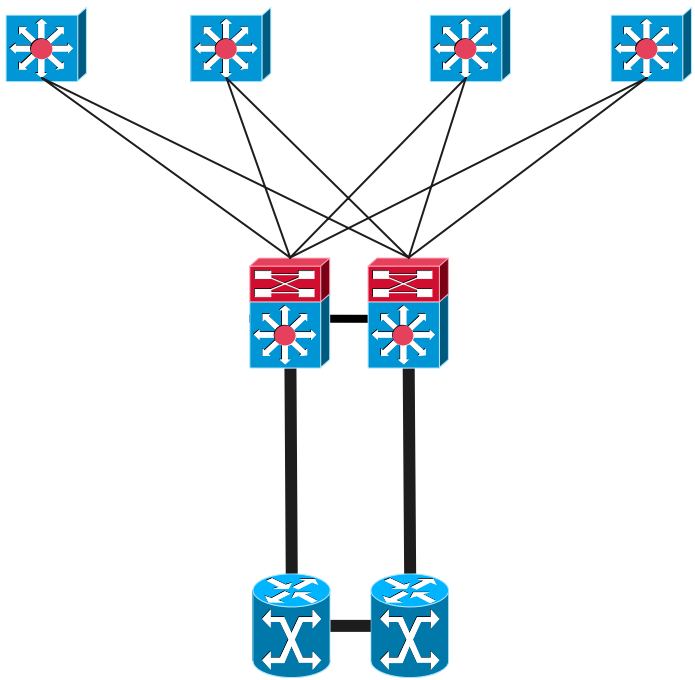
The big issue is cost, to be able to have a good business case

Rapid spanning tree, converges in approx 1,3 sec in this topology

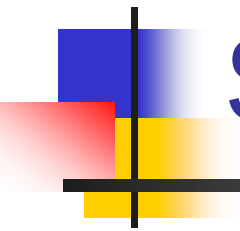
One IP subnet per 2950, all users on one 2950 belongs to the same vlan/subnet

It might be tempting to re-use the vlans on the next ring…

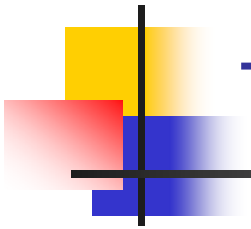
The typical ETTx environment



Access, L2 (rapid spanning tree) or L3 (OSPF) based on the Catalyst 4500 platform



Security

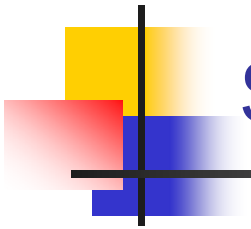


Threats

- All the same old stuff but on different hardware initially intended for enterprise environment:
  - User authentication
  - IP address misuse
  - MAC address misuse
  - VLAN hi-jacking
  - Packet sniffing
  - Packet crafting
  - Service hi-jacking
  - Hardware/infrastructure break-in
  - And so on ...

User authentication

- Any equipment at the end user will be abused, it's only a question of time. History shows this for satellite and cable services.
- Use 802.1x if available to improve the authentication of the CPE.
- Combine with the customer physical port at the POP for authentication if possible. The user would have to swap his fiber with another user or break into the POP in order to gain access.
- Link the DHCP servers with a AAA to enable/disable services based on the option 82 (POP chassis, blade, port)

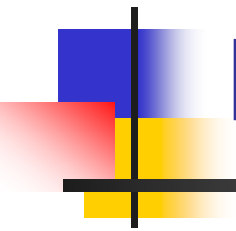


Security (solutions)

- DHCP Snooping (option 82)
- IP Source-Guard (dynamic ACL with IP/MAC src address)
- Private VLANs (PVLAN)
- Virtual ACLS (VACL)
- Port based storm control
- STP (BPDU Guard / BPDU filter)
- Multicast (VACLs, IGMP v3/SSM, IGMP filtering)

Lessons learnt

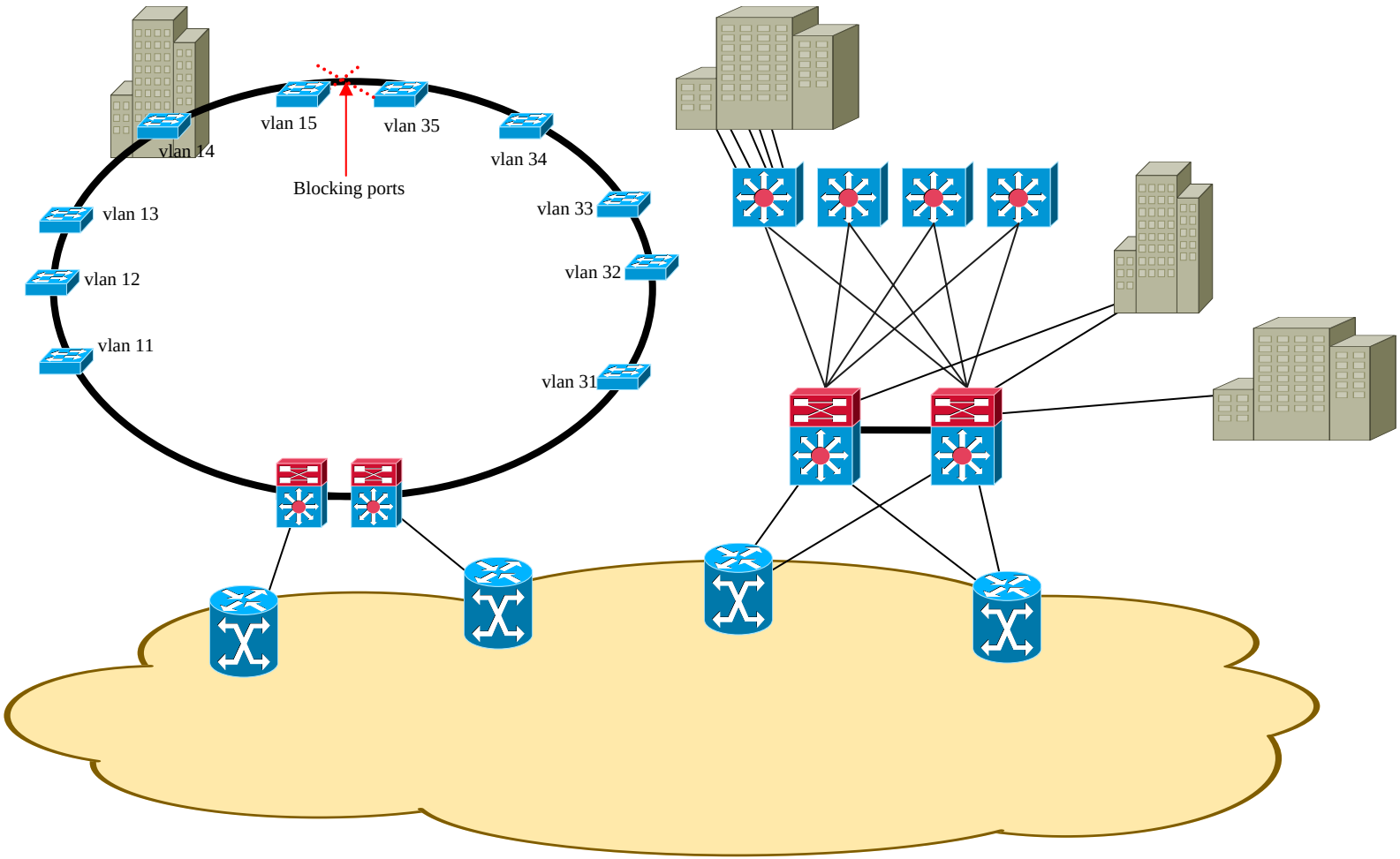
- Keep it simple
- Planning, processes, staging
- Build a lab and (ab)use it
- Don’t trust it until you brake it



MetroE Business Services

Christian Martin, CCIE 5937, Cisco Systems christma@cisco.com

Switched MetroE Architecture



MetroE for Business, what's the Vision

Metro Ethernet

=

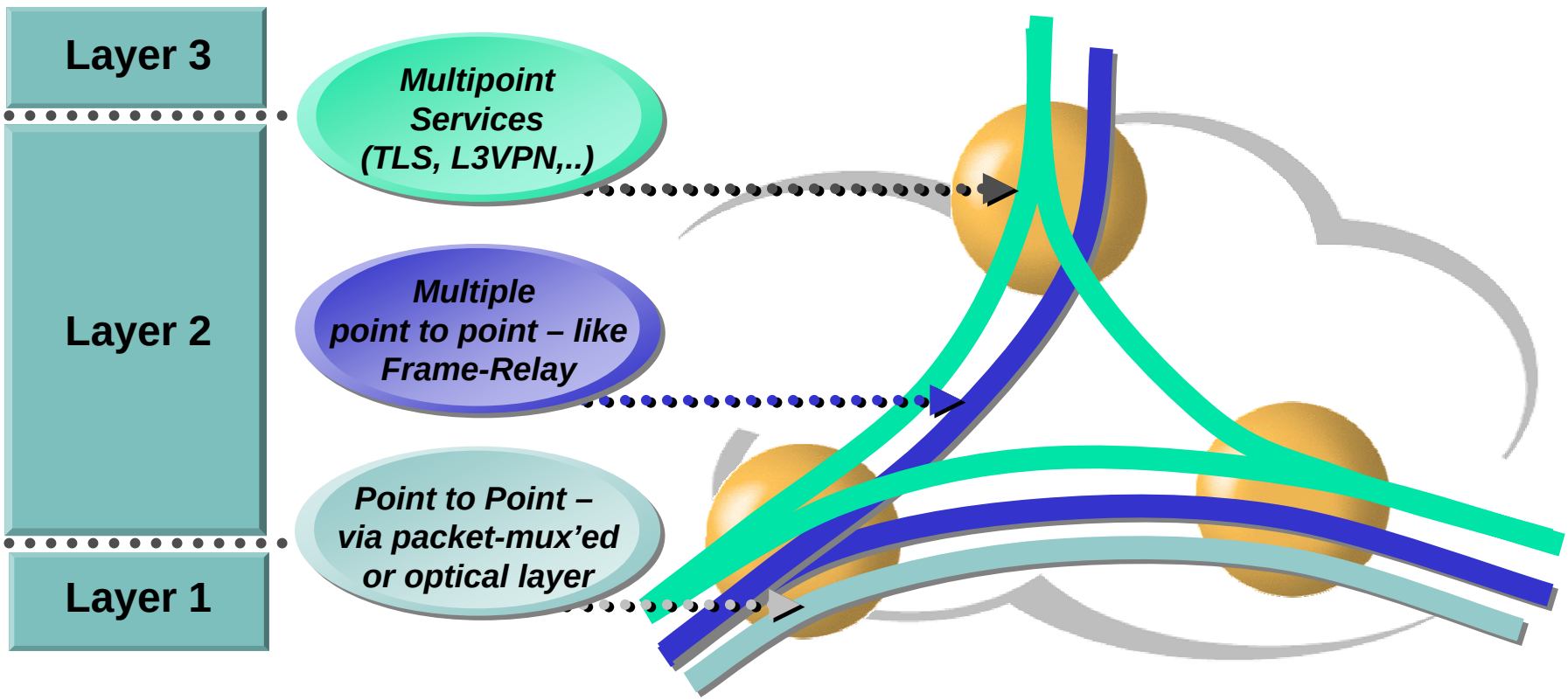
the new leased line / LAN

What Does Ethernet as a LAN/MAN/WAN Transport Offer?

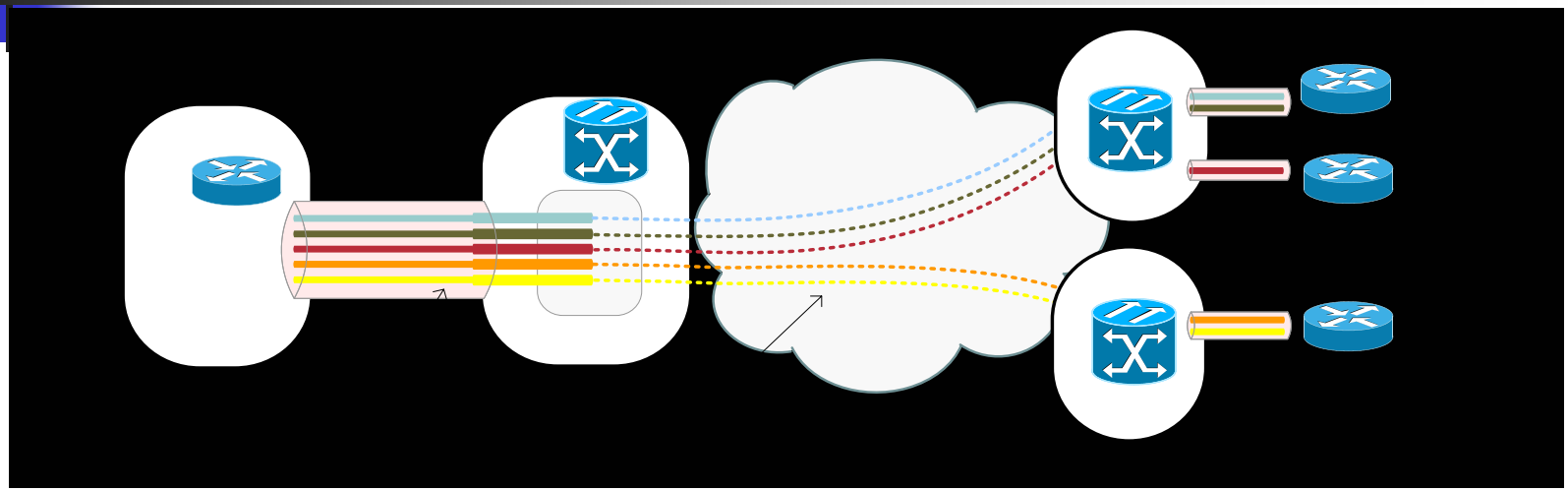
- Ethernet will become the ubiquitous network interface:
  - single technology for LAN, MAN and WAN
- Efficient packet-based infrastructure:
  - IP friendly
- Cost effective interface with flexible bandwidth offerings:
  - 10/100/1000/10000 Mbps
- Geographical independence:
  - Ethernet over Optical, IP or MPLS

Ethernet-based Services

More than just point to point…

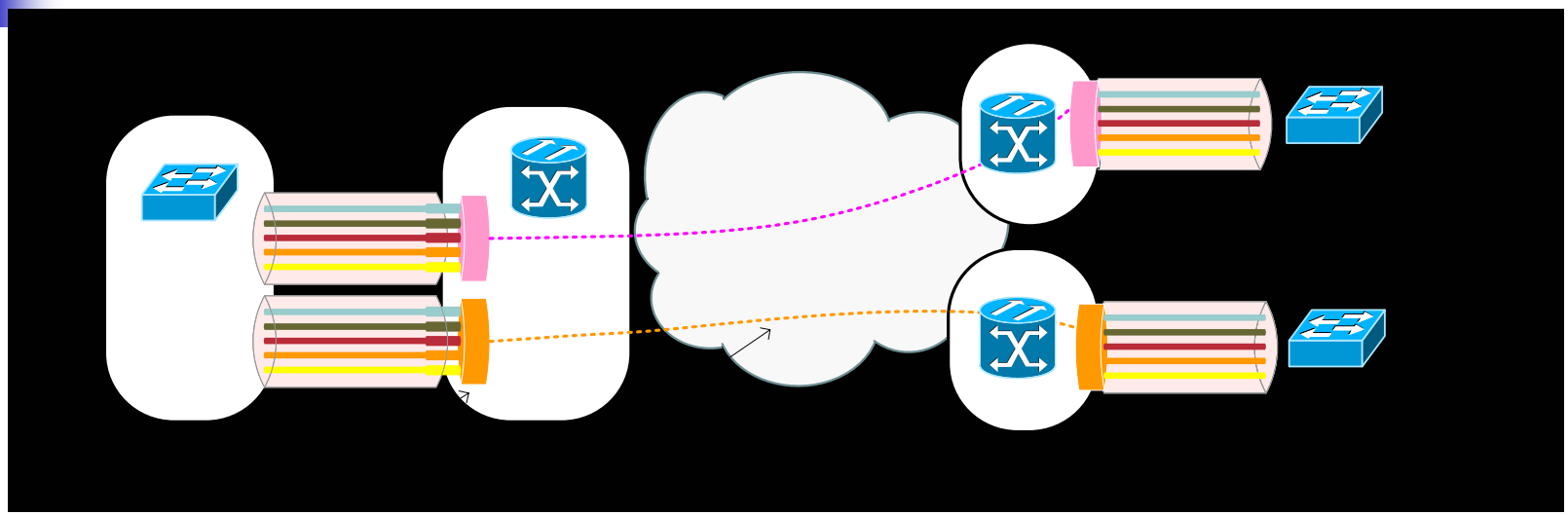


Ethernet Relay Service (ERS)



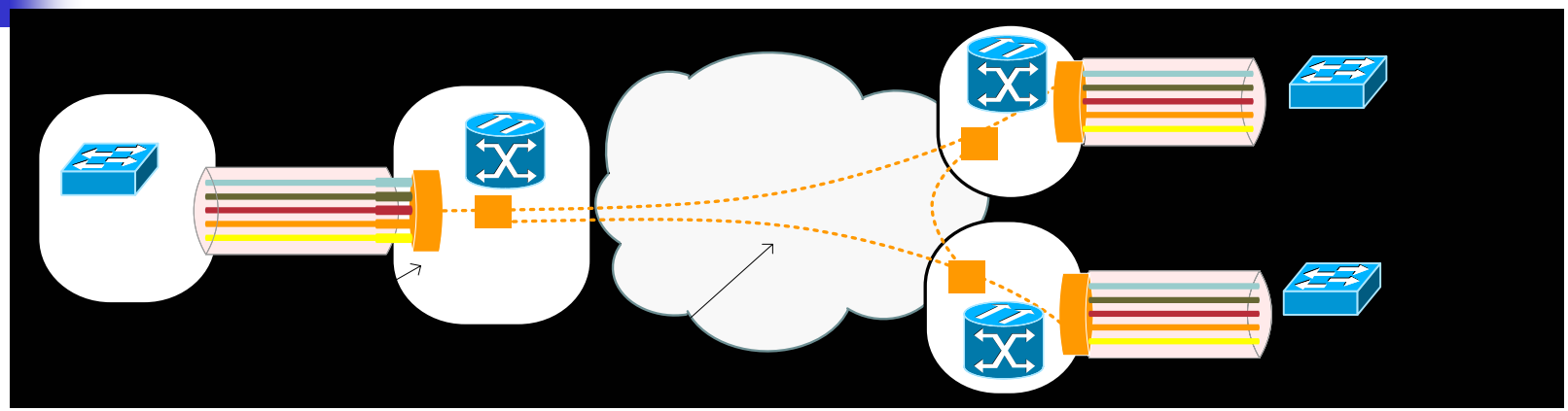
- Defines a point-to-point service
  (analogous to Frame Relay using VLAN tags as VC IDs)
- Service multiplexed UNI (e.g. 802.1Q trunk)
- Opaque to customer PDUs (e.g. BPDUs)
- Recommend a router as CE device
- Future: Interworking with FR/ATM

Ethernet Wire Service (EWS)



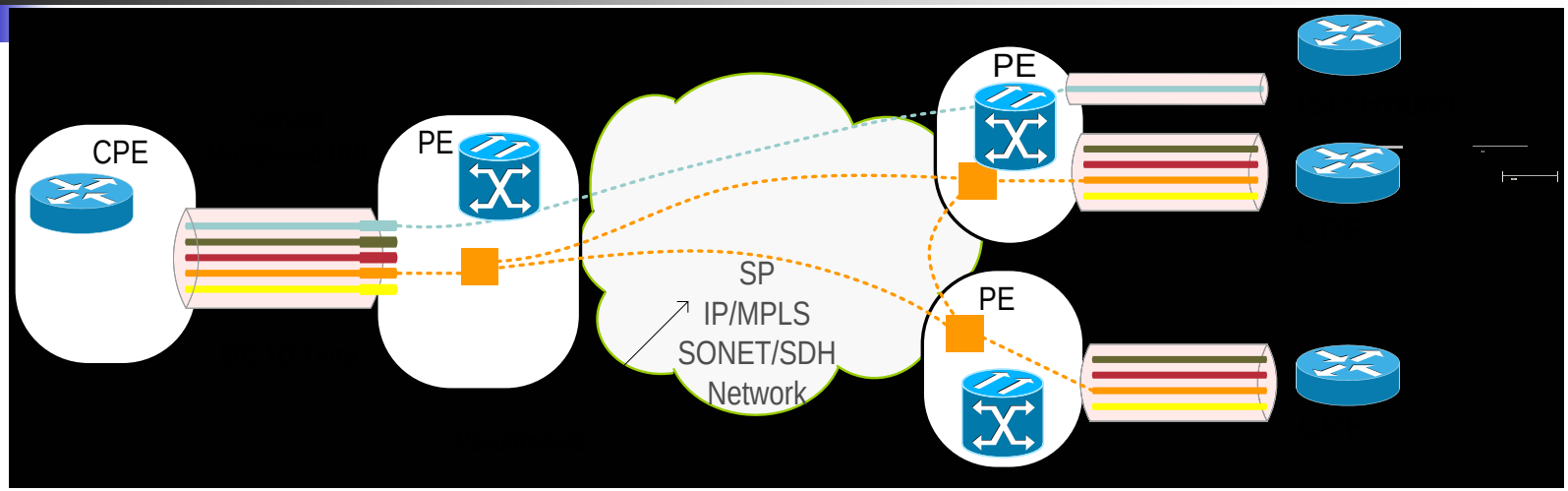
- Defines a Point-to-Point, Port-Based service
- No Service Multiplexing —“All-to-One” bundling
- Transparent to Customer BPDUs
- Allows for Over-Subscription using Stat Muxing
- Routers and/or switches as CE Devices

Ethernet Multipoint Service (EMS)



- Multipoint service where all devices are direct peers
- No Service Multiplexing — all VLANs are presented to all sites (“all-to-one” bundling)
- Transparent to Customer BPDUs
- Also called Transparent LAN Service (TLS), E-LAN, or VPLS
- Routers and/or Switches as CE Devices

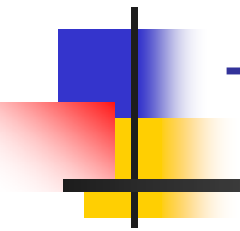
Ethernet Relay Multipoint Service (ERMS)



- Both P2P and MP2MP Services can coexist on the same UNI
- Service multiplexed UNI (e.g. 802.1Q trunk)
- Recommend Routers as CE Devices

MetroE Business Services (Take a ways)

- Ethernet, one technology for LAN, MAN and WAN
- “Low Cost” technology to offer high bandwidth
- IP friendliness
- Flexible Bandwidth @ UNI
- Technology ready to offer transparent and mhaultiplexed L2 Services
- New Services such as: ERS, EWS, EMS



Thank you for your attention