UMT L3 INGRESS / EGRESS ISSUES AND ARCHITECTURE

A SAMPLE END TO END USE CASE

Author: Mark Laubach

UMT GOALS AND REALIZATIONS

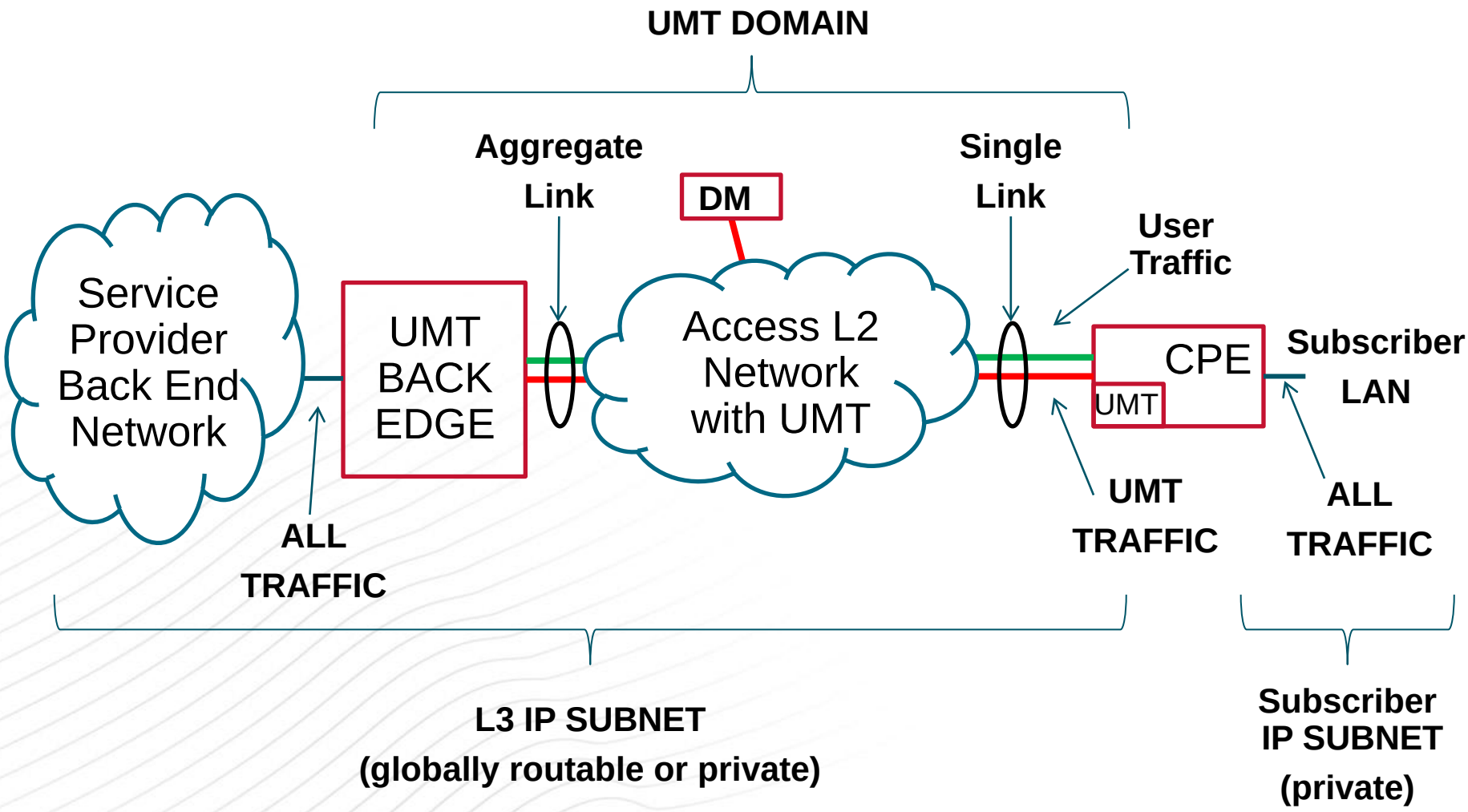
- **One main goal expressed for UMT**
  - Move “management” traffic in the access network out of the “user channel” – avoid impact to user traffic statistics
    - In both directions
    - Management traffic is both L2 Ethernet (e.g., OAM) and L3 IP based

- **Realization of this:**
  - Consumer “CPE” requires support for UMT
  - Service provider needs to be in control of what gets carried over UMT
    - Requirements UMT management protocol include:
      - Discovery of UMT support in CPE
      - Control of what management protocols will transit via UMT
      - Specification of UMT method: VLAN and/or UMT Encapsulation
  - Service provider may have multiple L2 hops between consumer CPE and “back edge” of UMT domain
  - Commercial “back edge” support for UMT

GENERAL UMT ARCHITECTURE – A SCENARIO

L3 Scenario Assumption: Subscriber CPE is a Firewall / NAT

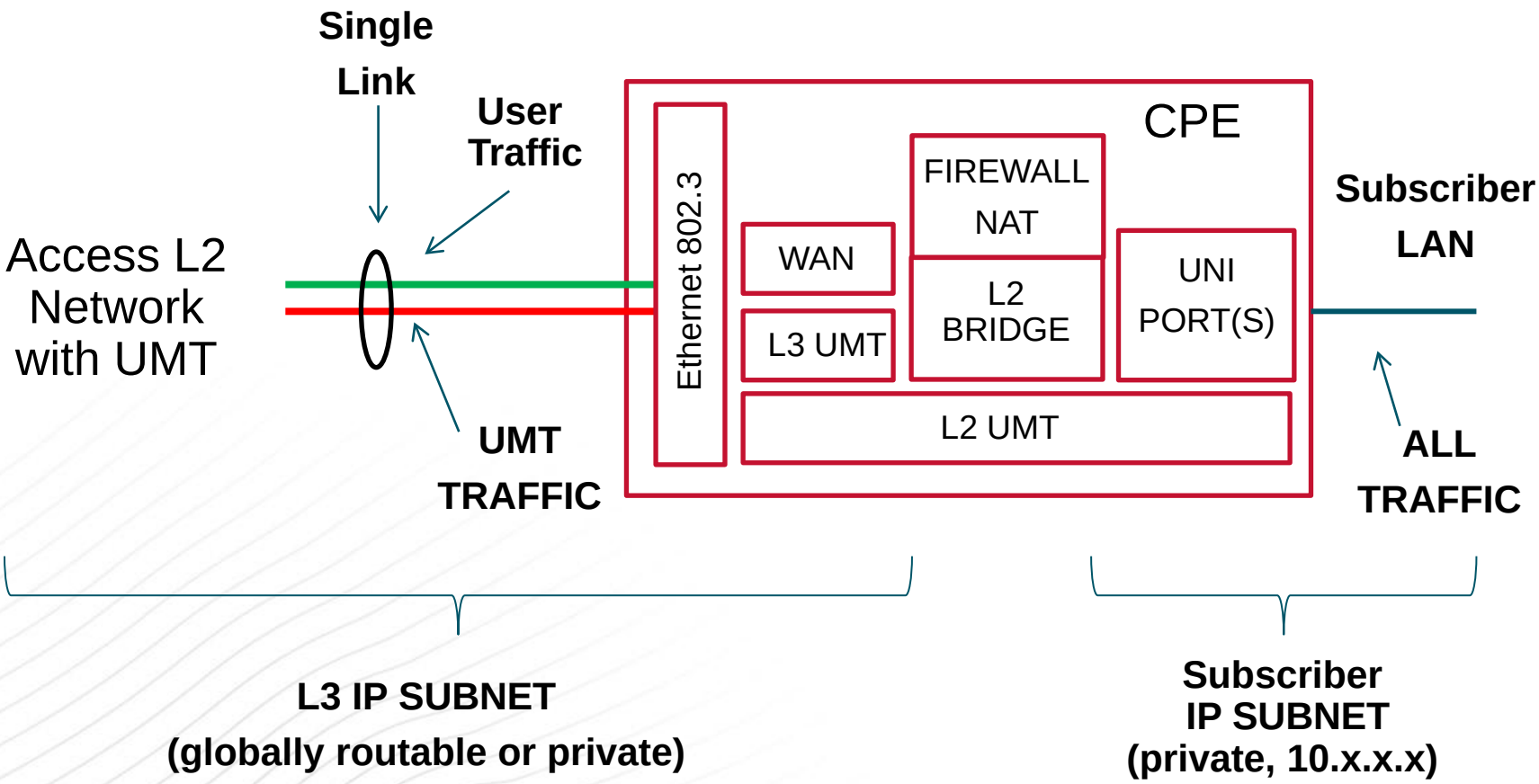
NOTE: UMT "Domain Manager" is DM



SUBSCRIBER CPE VISION

- **UMT functionality would need to be added to existing CPE products**
  - "UMT Certified" label
- **With this functionality, the CPE would participate as a UMT client with the service provider, under direction of the service provider:**
  - UMT discovery
    - Capabilities, MTU size, etc.
  - UMT subtype selection encapsulation
    - Assumption is the UMT encapsulation is always used, regardless of VLAN use
  - L2 processing of Ethernet protocol
    - E.g.. Place / extract OAM to / from UMT type
    - Based on EtherType
  - L3 processing for IP protocol
    - E.g. place / extract IP packets to / from UMT type
    - Requires deeper packet extraction to classify SNMP, TR-069, etc.
      - Firewalls / NATs already know how and must do this
    - Requires that IP routing be maintained
      - E.g. cannot tunnel a private IP subnet into a globally routable IP subnet
      - Best done on WAN side of Firewall, straight forward extension

GENERAL UMT ARCHITECTURE – A SCENARIO



WHY DOES L3 UMT RESIDE ON WAN SIDE?

- **First: private IP subnet number have no meaning in the access network**
  - Private address space is not globally routable by definition
    - Some cable operators may use private in the access, but separate subnet
      - same problem.
  - Same IP private space generally assigned to *every* subscriber
    - E.g. 10.1.10.0/24, 192.168.0.0/24
- **Second: Firewall/NAT functions already maintain necessary state tables to map IP/protocol/port numbers to proper destination based on CPE WAN IP address**
  - Firewall/NAT already can do UMT IP inspection and classifications function
  - Just need to augment to place / extract to / from UMT tunnel type
    - Based on UMT directive, handles Ethernet encapsulation different on transmit and extractions

UMT CLIENT MANAGEMENT

- **Only over WAN port**
  - Frames received only on UMT EtherType are processed by UMT function
- **No User / Customer Configuration**

SAMPLE SKELETON CONVERSATION

UMT DOMAIN MANAGER		UMT CLIENT
		P.O.S.T.
	<	UMT Client “Hello”
UMT Master Response	>	
	<	UMT Client caps / version
UMT Set <subtype> flush	>	
	<	UMT set ack
UMT Add <subtype> <ipvers> <ipdest/mask>> <proto> <startport> <endport> e.g. Add <TR069> <4> <1.2.3.4/32> <TCP> <80> <80>	>	
	<	UMT add ack
UMT Add <subtype> <ipv> <ipdest/mask>> <proto> <startport> <endport> e.g. Add <TR069> <4> <1.2.3.4/32> <TCP> <443> <443>	>	
	<	UMT add ack
UMT Close	>	
	<	UMT close ack

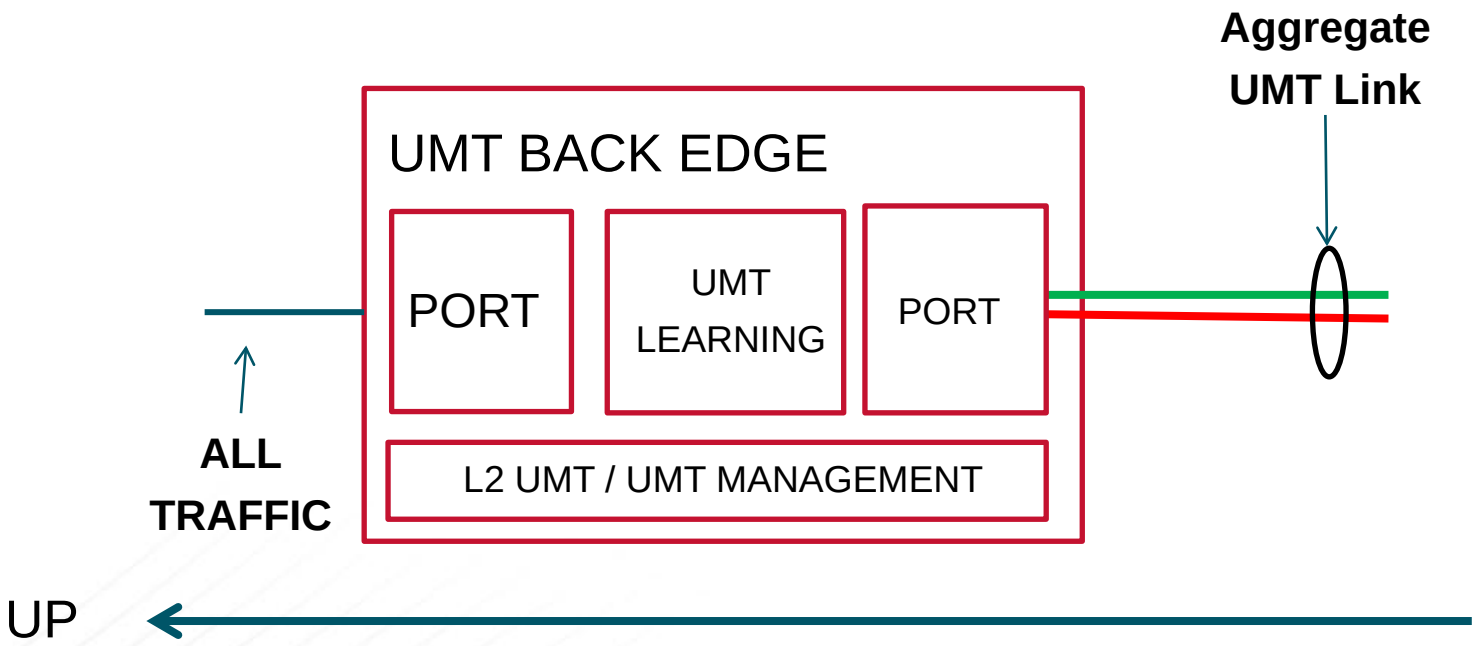
SUMMARY OF ADDING L3 UMT TO CPE FIREWALL/NAT CPE DEVICES

- **Looks straight forward**
  - Need to define UMT protocol support required
  - Need to specify required UMT tunnel types:
    - VLAN and UMT encapsulation
  - Vendors will need to augment Firewall/NAT WAN Ethernet interface to add necessary VLAN and UMT encapsulation support
- **IPv4 is easiest to overview, need to look at IPv6 addressing enhancements versus Firewall / NAT forwarding, etc.**
  - Need IPv6 expertise

UMT “BACK EDGE” L3 NETWORK ELEMENT

- **Basic functions**
  - Remove upstream traffic from UMT tunnel
  - Places downstream traffic into UMT tunnel
  - UMT Domain is anchored from Back Edge device to each subscriber “WAN” edge CPE (Firewall / NAT)
- **Issues**
  - Since each CPE Firewall / NAT will assign different source port numbers, this information must be learned by the UMT Back Edge network element
  - Desired IP packet destined (down) for a subscriber CPE needs to be inspected
    - If UMT match criteria is met, traffic needs to be placed into UMT tunnel type

UMT L3 “BACK EDGE” ARCHITECTURE – A SCENARIO



UMT Learning: UMT packets examined and learned:

- UMT Encapsulation type, Source: IP, Protocol, Port, MAC WAN SA

UMT traffic removed from the UMT tunnel

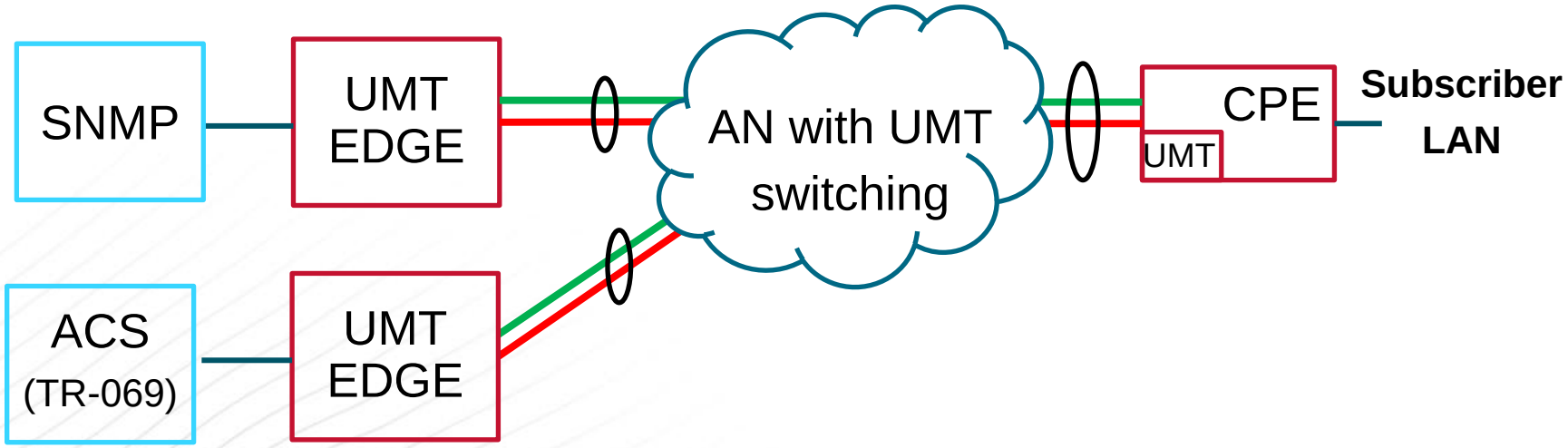
DOWN

All IP packets examined, those matching:

- UMT Encapsulated, Destination MAC, placed in UMT tunnel
- All non-matching packets follows normal user traffic

GENERAL UMT ARCHITECTURE – A SCENARIO

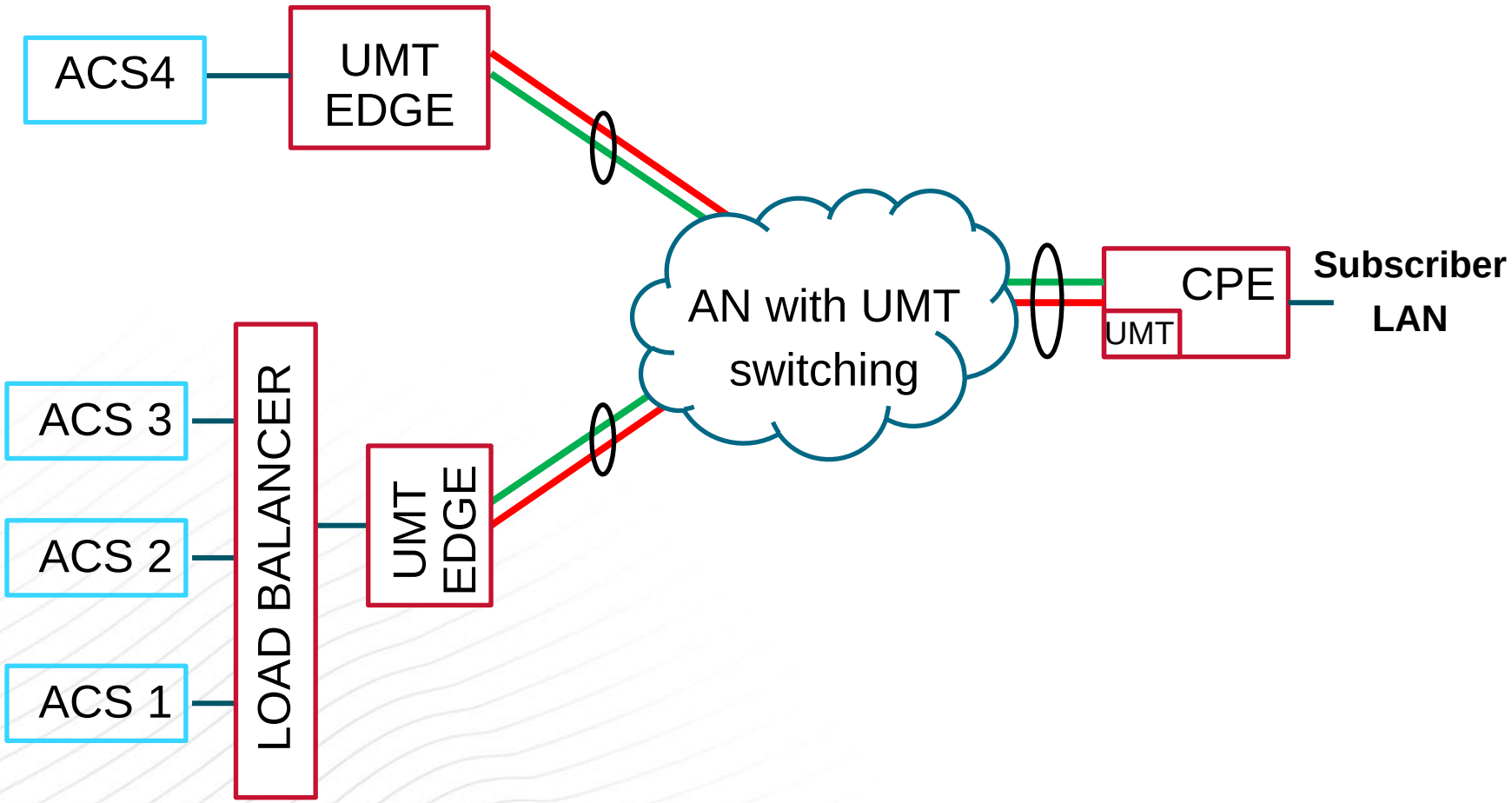
Access Network can be UMT EtherType and UMT Subtype aware for L2 switching to support traffic to/from different servers:



Upstream UMT learning in UMT Back Edge devices support flexible back end architectures

GENERAL UMT ARCHITECTURE – SCENARIO

Example: ACS load balancing with failover ACS



UMT BACK EDGE NETWORK ELEMENT

- **Viable**
- **Upstream UMT learning is essential**
  - One enabled for UMT, process is self learning
- **Permits different switching and aggregation architectures**
  - Enables flexibility for service providers
- **May be embedded function, may be a stand alone device**
  - Needs to support aggregation, load balancers, fail-over and other service provider configurations

UMT SYSTEM ELEMENTS

Suggested Focus for UMT Version 1:

- **UMT Domain Master**
- **UMT Client**
- **UMT “Back Edge” function**
- **UMT Master <> Client protocol**

Thank you