Progress in Standardisation of IP VPN Services

ITU-T IP Workshop - Geneva , 26.04.01

Marco Carugi

France Telecom R& D - IP networks and services

marco.carugi@francetelecom.fr

Outline

- IP VPN services
  - Scenarios, requirements, model
  - VPN types
  - Some reasons for a standardisation effort, some issues
- The current standardisation effort inside ITU-T
  - SG13/Q20 and new Q11
- The current standardisation effort inside IETF
  - PPVPN WG
- VPN standardisation versus VPN market offer

«One definition» (among many) of Virtual Private Network

- **VPN**
  - Telecommunications network built on top of public infrastructures
  - Carrying information flows between customer sites (mobile or not)
    - in a secure way
    - transparently from the point of view of other parties (clients) using these public infrastructures
- **IP VPN**
  - VPN carrying IP flows
  - VPN using an IP network (private IP networks or the public Internet) as a public infrastructure

Virtual Private Networks

- **EMULATION OF A PRIVATE NETWORK OVER A SHARED SP NETWORK**
  - Interconnection of multiple private, geographically dispersed enterprise networks over a Service Provider network
  - Service Provider resources sharing
- **VIRTUAL**
  - There is no correspondent physical network
  - Emulated infrastructure over public networks
- **PRIVATE**
  - Only a defined set of entities may access

VPN requirements

Customer requirements

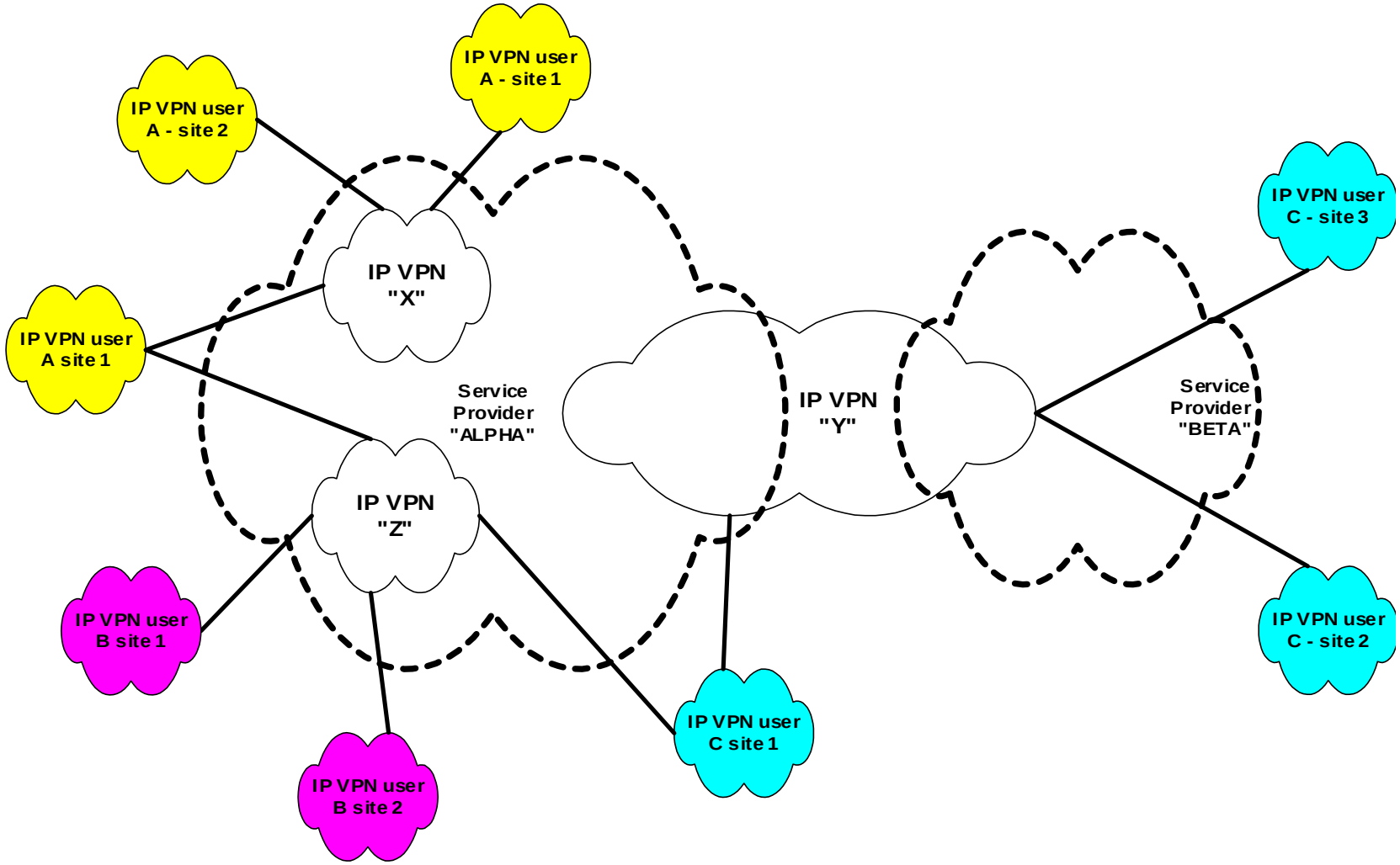
- Security
- Transparency
- Reliability
- Performance
- Flexibility

Service Provider requirements

- Scalability
- Interoperability
- Manageability

- More cost-effective solutions than classical Layer 2 VPNs
- Allow the introduction of new features and services
- Smooth integration within existing network infrastructure

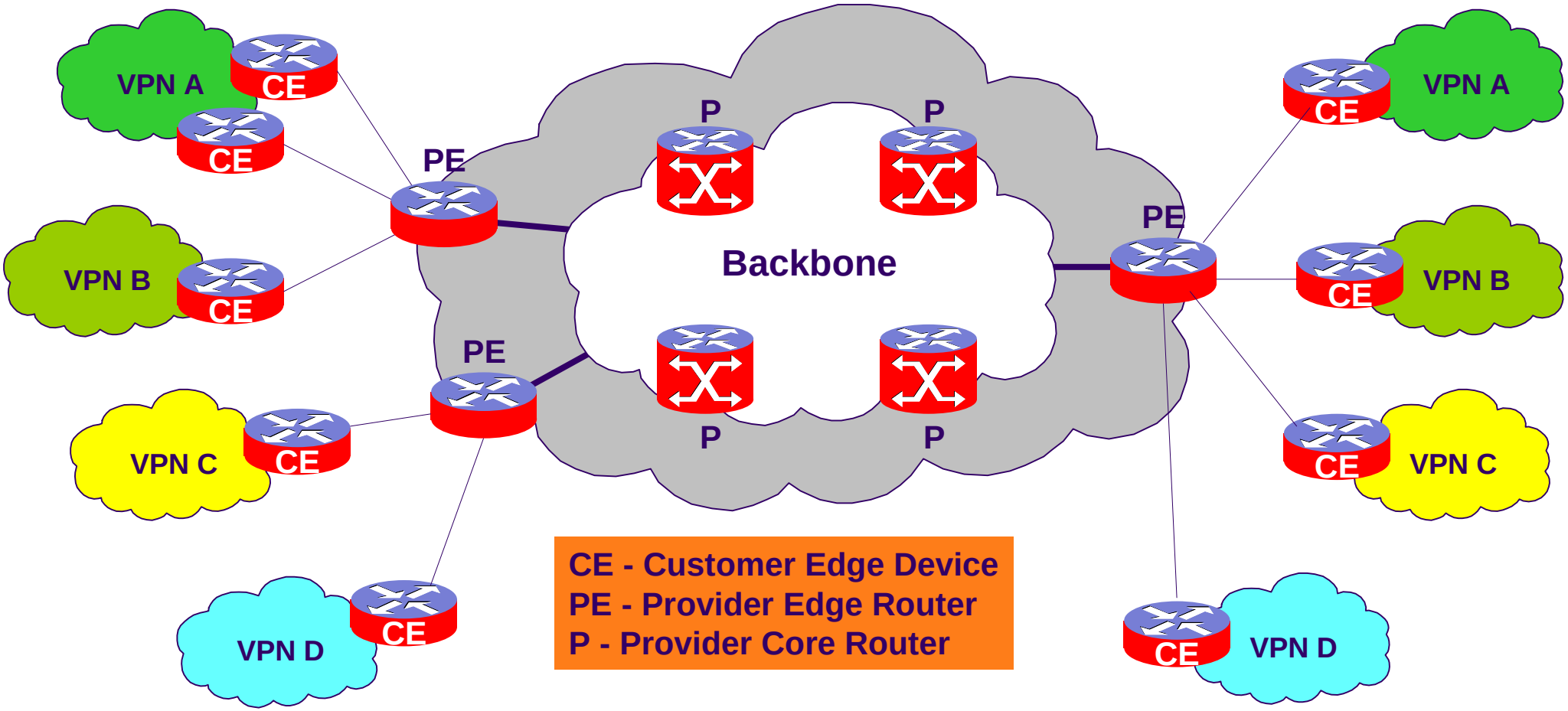
IP VPN Service View



Source: ITU-T Y.1311

France Télécom R&D

IP VPN Network Reference Model



A draft list of service requirements

- **Multi-vendor interoperability (at different levels)**
- **Service management capabilities (Provider/User perspective)**
  - Areas: network connectivity, service monitoring (fault, performance, accounting), security management (access control, authentication, data privacy), SLA and QoS management
  - Some capabilities as examples: single VPN configuration not impacting other sites/VPNs, interoperability with standard management platforms, automated operations, per-VPN and per-device MIBs, dynamic on-demand bandwidth provisioning
- **Security functions**
  - VPN isolation, user identification and authentication, security of the flow, peer identification and authentication, site protection
- **Quality of Service support (SLS)**
  - using DiffServ or IntServ mechanisms, per-VPN (measurable) SLAs, strict QoS (guaranteed bandwidth VPN), QoS support in more complex scenarios (inter-AS VPN, …)
- **Routing capabilities**
  - various routing protocols at edge and core of the SP backbone, scalable routing

Source: ITU-T Y.1311.1

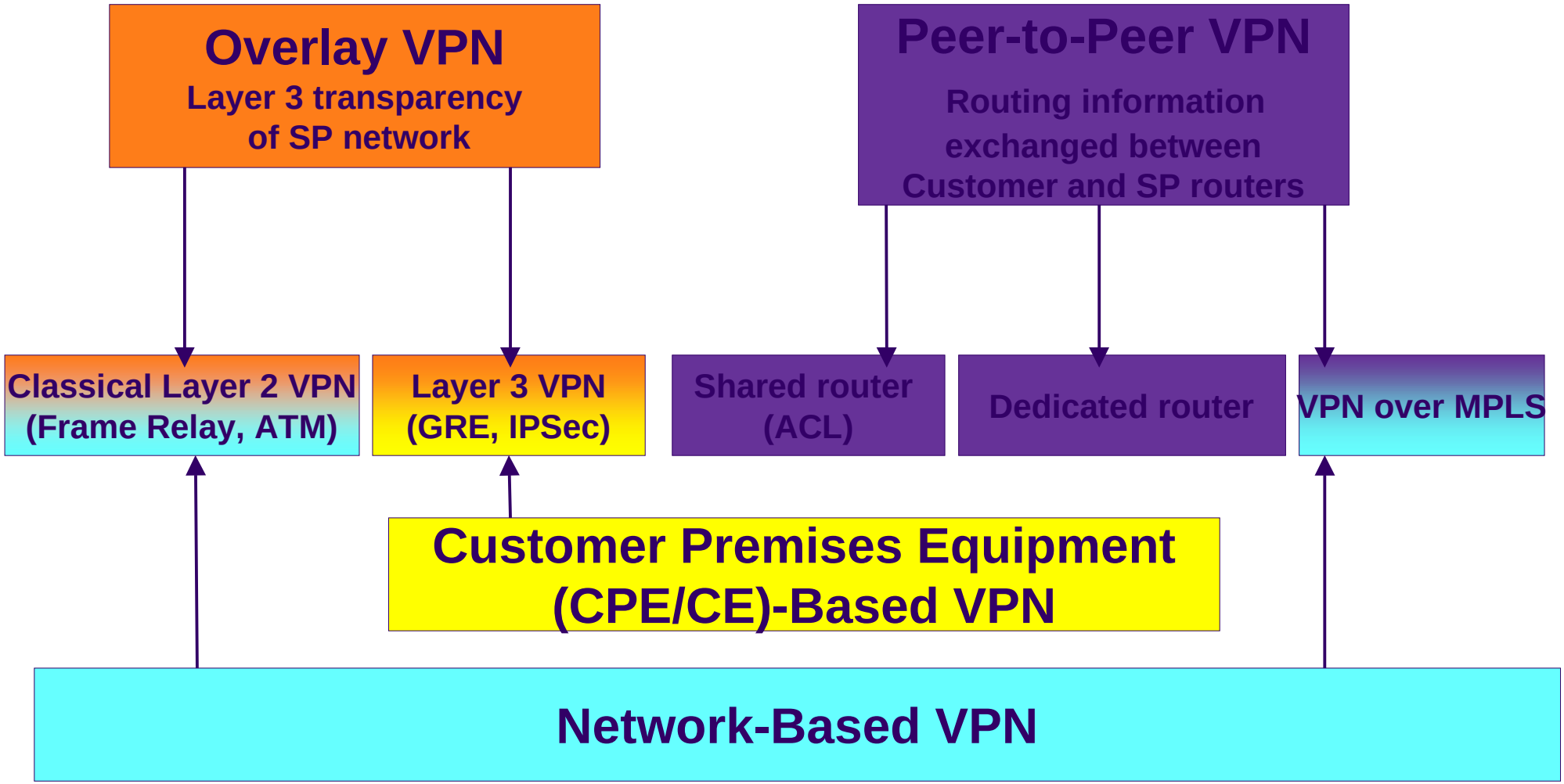
Service requirements - cont.

- **Autodiscovery (to convey dynamically VPN information among PEs)**
- **Various types of customer IP traffic and VPN topology**
- **Tunneling mechanism and backbone technology independence**
- **Access requirements**
  - various customer access scenario and technologies, various types of on demand CE access technique (IPSEC, L2TP, …)
- **Addressing requirements**
  - VPN address overlapping, minimized usage of IP addresses, NAT not precluded, various customer IP numbering schemes, support of dynamic allocation and outsourcing
- **Various service deployment scenarios**
  - multiple VPNs per site, VPN plus Internet access, Intranet/Extranet, Inter-AS VPN, Inter-Provider VPN, Carrier's Carrier, alliances of VPNs
- **Reliability and fault tolerance, efficiency (TE)**
- **Outsourcing of IP services (ex. DNS, DHCP), packaging of IP services**

- **See at http://ppvpn.francetelecom.com :**

  «Related ITU-T work»: Y.1311.1/Y.1311 Draft Recommendations
- **«Related Internet drafts/PPVPN WG doc»:draft-ietf-ppvpn-requirements-00.txt**

VPN types based on largely used terminology



A not so simple classification

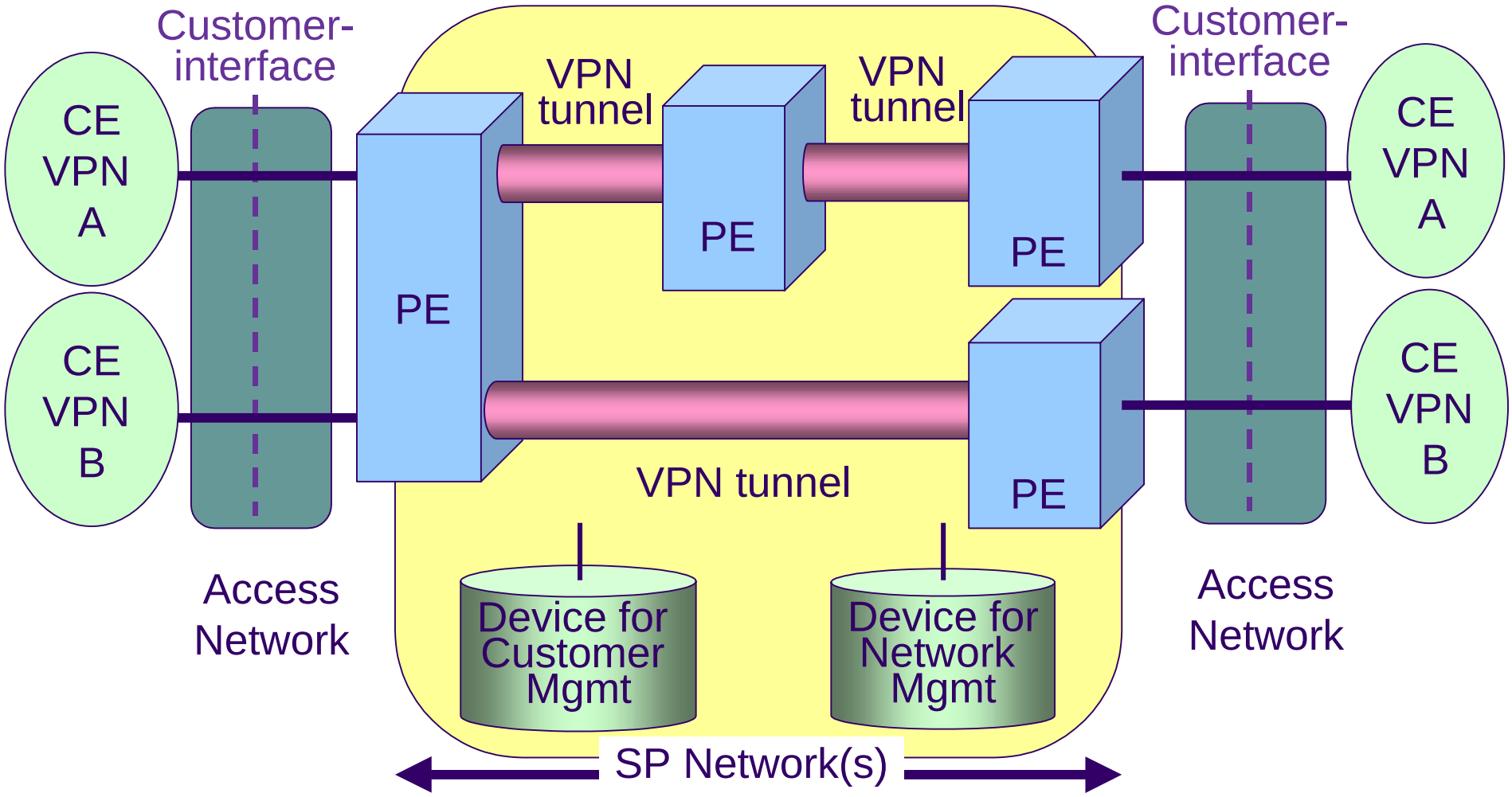
CPE-Based VPNs

- **Various CPE-to-CPE tunneling technologies can be supported**
  - GRE
  - IPSec
  - but also PPTP, L2TP, ...
- **May use independent PE-to-PE tunneling technologies (MPLS)**
- **May be Provider Provisioned or Customer Provisioned**

Network-Based VPNs

- **Classical Layer 2 VPNs (FR, ATM), … Eth VLANs (Metro LANs, ...)**
- **VPN over MPLS**
  - **Layer 3 MPLS VPNs (BGP/MPLS VPN, VR VPN)**
  - **Layer 2 MPLS VPNs**
- **VPN over other (than MPLS) PE-to-PE tunneling technologies (IPSEC)**
- **Provider Provisioned**

Reference Model for Network-Based VPNs



Source: draft-ietf-ppvpn-framework-00.txt

France Télécom R&D

Some reasons for a standardisation effort

- **A number of proposals in the market**
  - addressing a lot of common requirements
  - providing different ways to address requirements
  - partial coverage of emerging SP needs
  - not interoperable
  - would like to define applicability scenarios for the various solutions
- **Competition and cost-effectiveness drivers**
  - towards multi-vendor environments
  - (flexible) integration of SP added-value requirements
- **Formal forums provide value**
  - Commonality of interests inside the community is an obvious reason for that

A number of proposals in the market : a non-exhaustive example for NB L3 VPNs

VPN function	BGP- VR	Mcast-VR	2547bis	BGP/IPsec
Discovery	BGP	Multicast	BGP	BGP
Reachability	per VPN	per VPN	backbone	backbone
Tunneling	MPLS/IPsec/ IPinIP/GRE	MPLS	MPLS	IPsec

Source : IETF NBVPN BOF

France Télécom R&D

The scope of the standardisation

IP VPN working context

- **Network-Based** as primary scheme for SP offers
  - **ITU effort (Q11/SG13)**
- **all scenarios where Providers may have an active Provisioning role**
  - **IETF (PPVPN WG)**
    - Provider-managed CPE-based VPN scenarios are included

Diversified IP network infrastructure

- Core : MPLS frequently, but not necessarily (ex. multi-domain VPNs, etc.)
- Access : wide spectrum of access technologies
  - ATM, FR, LL, L2TP, IPSEC, XDSL, cable, ...

A number of service deployment scenarios to be investigated

- Intra-AS, Inter-AS, Inter-SP, VPNs of VPNs, ...

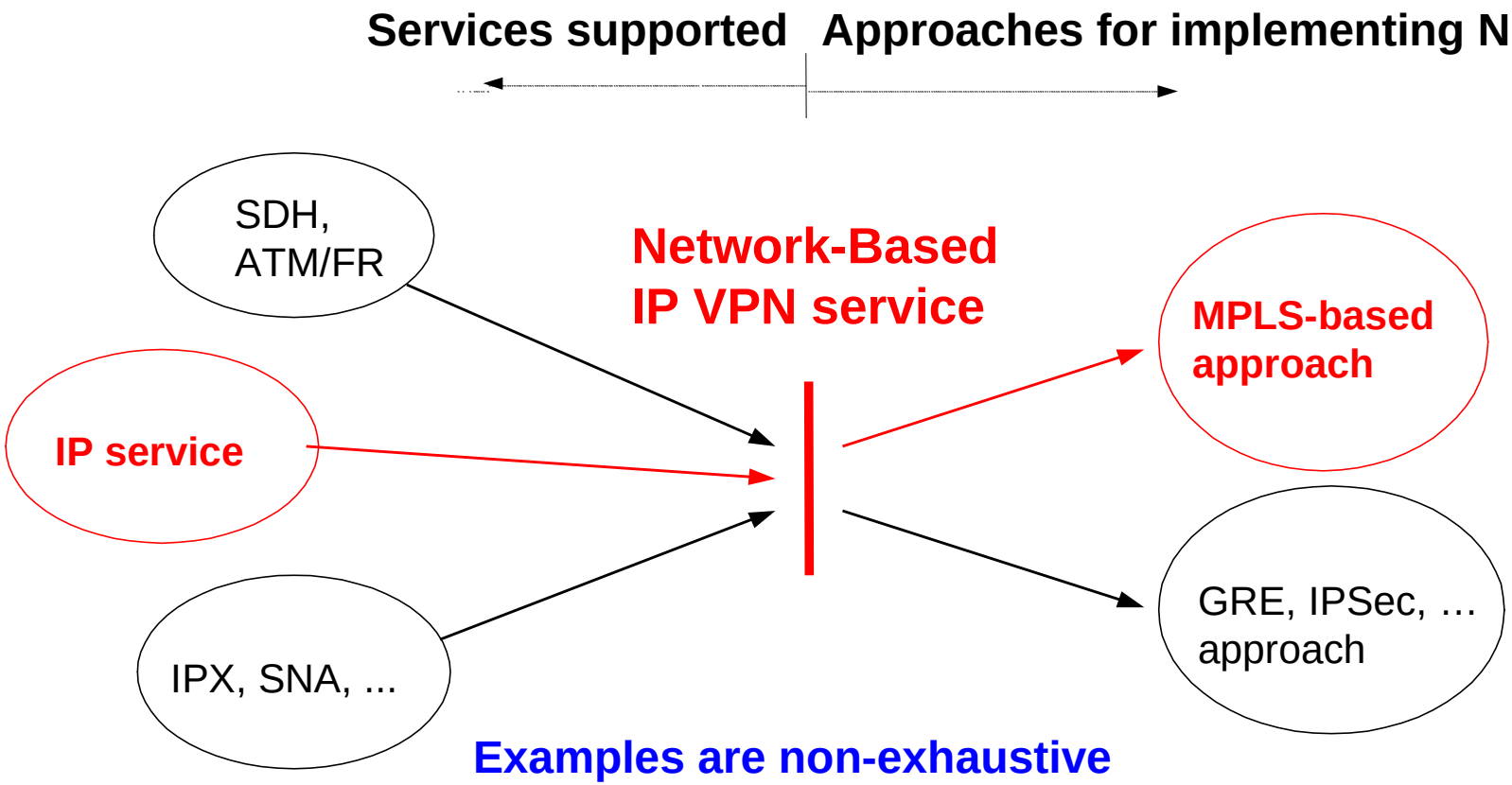
Some issues

- **Ensure scalability over the next several years**
  - Make good numerical projections
- **Flexibility to accomodate future requirements**
  - ex. non-IP services over the same VPN support service architecture
    - ATM/FR/SDH/Ethernet over MPLS (L2 VPN), Layer 1 VPNs (optical VPN) ?
- **Interoperability scope**
  - Interoperability scope: certainly among implementations of the same solution, desirable between different solutions
- **How many solution stacks (approaches) as starting point ?**
  - grouping of various existing solutions into few approaches is not so straightforward
- **Segmentation of the service offer (Carrier/SP VPNs vs Enterprise VPNs)**
  - different requirements, different technical solutions ?

Work on IP VPNs in ITU-T Study Group 13

- **Study Group 13**
  - **« Multi-protocol and IP-based networks and their internetworking »**
- **Question 11 of SG13 - 2000/ 2003 study period**
  - **« Mechanisms to allow IP-based services using MPLS to operate in public networks »**
  - Successor of Question 20 which initialized the work on IP VPNs in previous study period
  - Two Draft versions of Recommendations on IP VPNs have been produced up to now (http://ppvpn.francetelecom.com/ituRelated.html)
    - **Y.1311 “Network based IP VPN Service - Generic framework and service requirements”**
    - **Y.1311.1 “Network based IP VPN over MPLS Architecture”**
      - more advanced status than the previous one
      - up to now it also includes requirements (plan to move them into the more generic Y.1311 in a later version)

Multiple Services over VPN support service



Source : ITU-T Y.1311

Recent steps on IP VPNs inside ITU

- **Q11 Rapporteur 's meeting in Boston (20-23.2.01)**
  - enhancements (QoS support, interworking, inter-AS VPNs), refinements and final edition of Y.1311.1
  - enhancements to Y.1311 (definitions, etc.)
- **Submission of Y.1311.1 as White contribution (for consent call in next SG13 meeting (May 01)**
- **Requirements from ITU provided as input for the first IETF PPVPN Requirements Internet Draft (23.2)**
  - **draft-ietf-ppvpn-requirements-00.txt**
- **SG2/WP3 has launched work on per-VPN Traffic Engineering**

ITU-T Draft Recommendation Y.1311.1 "Network based IP VPN over MPLS Architecture"

- **It does not cover all spectrum included in the IETF PPVPN WG**
  - **IP VPNs just over MPLS**
  - **no CPE-based approaches**
  - **no NB Layer 2 approaches**

- Scope
- Abbreviations and references
- Service definitions and reference model
- Service requirements
- Framework architecture
  - **learning customer-site reachability information**
  - **distributing reachability information**
  - **constrained distribution of routing info**
  - **LSP tunnel establishment and usage**

- Technical approaches for NBVPN (solutions)
  - **2 identified** (based on deployment):
    - **BGP/MPLS (2547)**
    - **Virtual Router**
- QoS approaches
  - Point-to-Cloud SLS, Point-to-Point SLS, Cos Transparency
- Inter-AS (SP) VPN (to be developed)
- Interworking between different solutions (to be developed)
- Service Interworking with other VPN architectures (to be developed)

Functional areas in Y.1311.1 framework architecture

- Learning customer-site reachability information
  - discover VPN IP addresses reachable via directly connected CEs (for PE) and in other VPN sites (for CE)
- Distributing reachability information within the VPN
  - distribute information from PE towards other PEs having customer sites attached for the VPN
- Constrained distribution of routing information
  - per-VPN PE determination of the set of other PEs to which it must distribute the reachability information
- LSP tunnel establishment and usage

Some future work items inside ITU

SG13/Q11 May meeting

- **Consent call for the first version of Y.1311.1 Draft Recommendation**
- **Integrate inputs from IETF ?**
  - **Expanded scope ? (L2 VPNs, CPE-based VPNs, …)**
- **Continue work on Y.1311 and Y.1311.1**
  - **interworking, non-IP based services, QoS support, inter-AS, per-VPN TE (jointly with SG2), ...**

The IETF standardisation effort : the Network-Based VPN BOF in Aug 2000

2 SPs as co-chairs (Broadband Office, France Telecom)

Much interest in the IETF community (300 participants at the BOF)

Requirements/goals in this initial draft charter

- Define and specify one or more sets of mechanisms for NBVPNs
- Framework and service requirement documents, specific protocol definitions focusing on scalability an manageability
- Limited number of (but likely more than one) solutions
- **Enable multivendor interoperable implementations for each solution**
- tunneling schemes to be considered: MPLS, IPSEC, GRE

PPVPN meeting in San Diego IETF (Dec OO)

The Working Group is officialised :

Provider Provisioned Virtual Private Networks (PPVPN)

- **Included in the new IETF Sub-IP Area**
  - new Area also includes TE, CCAMP, MPLS, GSMP, IPO, IPORPR

Updated charter

- **High level objective : functional architecture of the VPN service, profile specifications independent from underlying technology**
- **Provider Provisioned context includes additional service deployment scenarios such as Provider-managed CPE VPNs**
- **Layer 2 VPNs are included**
- **Reaffirmed importance of security aspects (security analysis of each solution, inclusion of various IPSEC-based scenarios)**

Meeting

- High interest (420 attendees)
- First drafts on BGP/MPLS MIBs, multicast in BGP/MPLS VPNs, BGP/MPLS VPNs for IPv6, Autodiscovery using BGP as a way for RFC2547-VR PE-to-PE interworking (discussed initially inside ITU)

First steps of the PPVPN WG

Charter finalisation and work launch at end January 01

- **2 design teams : framework and requirements**
  - **draft-ietf-ppvpn-requirements-00.txt**
    - Generic, Customer, SP requirements
  - **draft-ietf-ppvpn-framework-00.txt**
    - functional blocks, 3 ref. models, taxonomy (L2,L3, CPE-based, Network-based)
- working context related to IPSEC VPNs and L2 VPNs under study
  - work sharing with IETF PWE3 WG on L2 VPNs
  - cooperation with Security Area (first draft on IPSEC usage in VPNs (March 01))

2nd PPVPN meeting in Minneapolis (March 23rd)

(see http://ppvpn.francetelecom.com)

- Presented IDs on framework, requirements, security issues, VPN info model, VPN tunnel systems, Metro LAN services, optical VPNs
- Started discussion on applicability statements , Future WG work items presented by the Chair for (IESG and WG) discussion
- WG input needed concerning possible extensions of working context : Eth VLANs (YES), (Optical) L1 VPNs ? Metro LAN services ?
- Other work (to be discussed when solutions will be analysed) : VR enhancements (hierarchical VPNs, etc.), BGP/MPLS security extensions, MIBs

PPVPN WG charter

Defining and specifying a limited number of sets of solutions for supporting PPVPNs

- **Development of a framework document**
  - The framework will define the common components and pieces that are needed to build and deploy a PPVPN. Deployment scenarios will include provider-managed VPN components located on customer premises
- **Development of a service requirements document**
  - requirements that individual PPVPN approaches must satisfy from a Service Provider (SP) perspective
  - attention on security, privacy, scalability and manageability
  - **not intended to define the requirements that all approaches must satisfy, but to become a "checklist" of requirements, not all of which will be required in all deployment scenarios**
  - **provide a consistent way to evaluate and document how well each individual approach satisfies the individual requirements**

PPVPN WG charter (cont.)

- **Development of several individual technical approach documents that group technologies to specify specific VPN service offerings**
  - a small number of approaches based on collections of individual technologies that already exist
  - **Goal : to foster interoperability among implementations of a specific approach.** Standardization gauged on (I)SP support.
  - **Not a goal of this WG to develop new protocols or extend existing ones.** The purpose is to document and identify gaps, shortcomings in each approach with regards to requirements.
  - **In the case that specific work items are identified, such work will be done in an appropriate WG.** Taking on specific protocol work items in this WG will require rechartering.
  - at least three specific approaches including BGP-VPNs (e.g. RFC 2547), virtual routers and port-based VPNs (i.e., where the SP provides a Layer 2 interface, such as Frame Relay or ATM, to the VPN customer, while using IP-based mechanisms in the provider infrastructure to improve scalability and configurability over traditional L2 networks).

PPVPN WG charter (cont.)

- **Consideration of inter-AS (SP) VPNs**
- **Each technical approach document will**
  - **evaluate how well it meets the requirements (req. doc)**
  - address scalability and manageability issues, operational aspects
  - analyze the threat and security aspects of PPVPNs, including appropriate mandatory-to-implement technologies and management mechanisms to ensure adequate security, privacy of user data. Analysis will include cryptographic security from customer site to customer site using IPSEC.
- **An applicability statement for each approach**
  - **describing the environments in which the approach is suitable for deployment, including analysis of scaling impact of the approach on SPs and threat analysis**
- **Coordination with IETF PWE3 and ITU-T efforts**

Goals and Milestones

- **DONE :**
  - **Formulate a plan and begin approaching SPs for input on scaling and other requirements**
  - **Begin discussion (based on submitted IDs) on candidate approaches against the service requirements**
  - **Begin discussion of the framework and the service requirement documents (two design teams formed, an interim meeting was held)**
    - **2 IDs (moved to WG documents in agreement with ADs) : framework ID, requirements ID**
- **NOT DONE** :
  - Identify a limited set of candidate approaches, build design teams
  - Mar 01: Begin discussion of applicability statements
  - Aug 01 : Submit framework, req IDs to IESG -> Info RFCs
  - Mar 02 : Submit candidate approaches, applicability statements to IESG for publication
  - Mar 02: Charter update or WG disband

A working plan for the next IETF PPVPN meeting - London , Aug O1 (currently under discussion)

- Consolidated versions of REQ and FRAME IDs (to prepare Info RFC process)
- One WG document for each candidate approach
  - including the Provider Provisioned CPE-based approach
- 3 starting Applicability Statements IDs based on current framework classification (CPE-based VPN, L3 NB-based VPN, L2 NB-based VPN)

- Other expected contributions
  - all work related to the various candidate approaches and based on produced requirements

ITU Q11/13 - IETF PPVPN synergy

- **The synergy is clearly stated in :**
  - **the PPVPN WG charter**
  - **the Y.1311.1 (Y.1311) introductory text**
- **Some steps on this direction :**
  - PPVPN WG context presented by myself in Boston Feb 01 Q11 meeting
  - **most of ITU service requirements** (implication of several SPs) used as **input for draft-ietf-ppvpn-requirements-00.txt**
- **In order to ensure mutual exchange, cooperation and progress**
  - Constant exchange of information between the two groups
    - short term: the last versions of Frame and Req IDs and PPVPN WG meeting minutes will be submitted as TDs for the SG13 May meeting
  - Avoid overlapping and “Grey Zones” (identify areas of responsability of each group where possible)
  - Keep IP experts’ interest high in both groups

VPN standardisation effort vs Provider-oriented market offer

- VPN standardisation effort will start from the most significative Provider-oriented “Solutions”
  - “BGP/MPLS VPNs”, “Virtual Routers VPNs” and, recently, “Scalable Layer 2 VPNs” and “Provider-managed CPE-to-CPE VPNs”
- There are and there will be other approaches on the market
  - standard bodies should constantly have a pragmatic attitude towards the evolving context
  - standardisation should strongly pursue “intra/inter-solution” interoperability (multi-vendor infrastructure is a SPs’ must)
  - to foster interoperability: functional decomposition of the VPN space, maximisation of commonalities among solutions, negociation capabilities inside mechanisms

SPs and Users as market drivers

- Market proposals
  - They will be basically driven by the SP and User requirements
    - Scaling projections
    - End-to-end security requirements
    - Management requirements
    - Requirements for Carrier VPNs and for Enterprise VPNs
    - Which other requirements in the future (Voice, Optical, Metropolitan services, …) ?
    - Different service and network architectures among SPs
  - No single solution will probably fit all requirements
    - strong need of Applicabilty Scenarios for each solution
  - Universal or specialised Provider Edge devices ?
  - Impact of multicast and IPv6 on VPN solutions ?

Main ingredients of a successful standardisation effort

- Start from SP and User « Key Requirements »
- Joint work of Users, SPs and Vendors
- Apply pragmatism in the process
- Feedback from deployment

- The first steps towards « Provider-oriented VPN standards » are promising