VPN
Virtual Private Network

Mario Baldi

Synchrodyne Networks, Inc.

mbaldi[at]synchrodyne.com

Nota di Copyright

Definizione

Virtual Private Network (rete privata virtuale)
Connettività per gli utenti su di una infrastruttura pubblica imponendo le politiche come se si usasse una rete privata

- Infrastruttura condivisa
  - Rete privata o pubblica
    - Per esempio quella di un Internet Service Provider
    - IP
    - Frame Relay
    - ATM
  - Internet
- Politiche
  - Indirizzamento, sicurezza, qualità del servizio, affidabilità, ecc.

Perchè VPN?

Le reti private sono basate su

- **Linee private affittate (CDN)**
- **Soluzioni dial-up interurbane**

Le VPN permettono di abbattere i costi di queste soluzioni costose

Classificazione

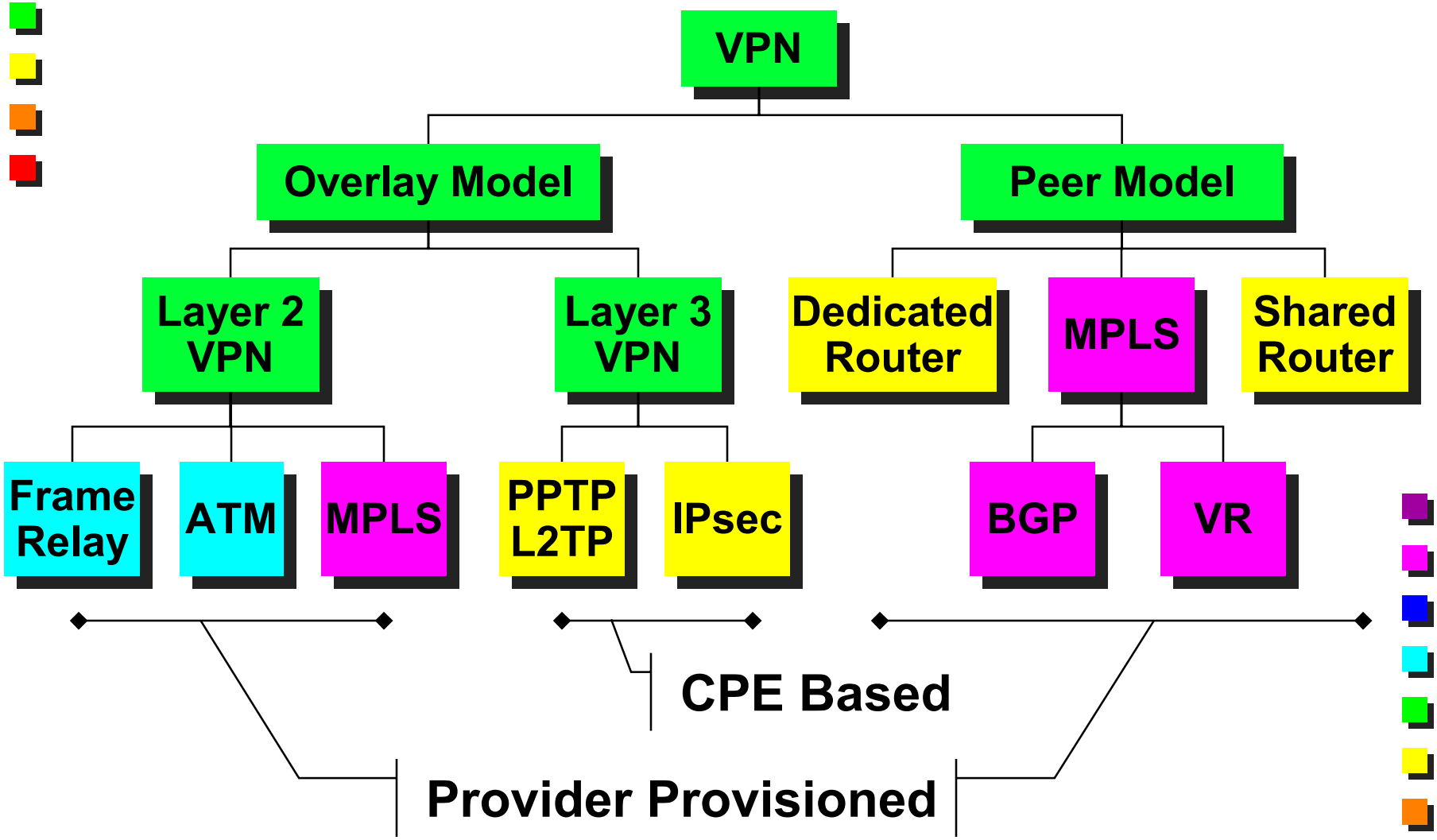
- VPN di accesso
  - Accesso remoto su una infrastruttura condivisa
  - ISDN, PSTN, cable modem, DSL
- Intranet VPN
  - Collega sede aziendale principale, uffici remoti, filiali
- Extranet VPN
  - Collega ad una rete aziendale clienti, fornitori, partner, o comunità di interesse

Fornitura di servizi VPN

- Overlay Model
  - Serivizi (gestiti) basati su IPSec
  - Svariati tunnel altamente magliati
    - Ogni VPN gateway deve “conoscere” gli altri
- Peer Model
  - Rete MPLS
  - Ogni VPN gateway “conosce” solamente il router di accesso del service povider
    - Scambio di informazioni di routing
    - La rete pubblica diffonde informazioni di routing
  - La rete pubblica inoltra il traffico tra i gateway della stessa VPN

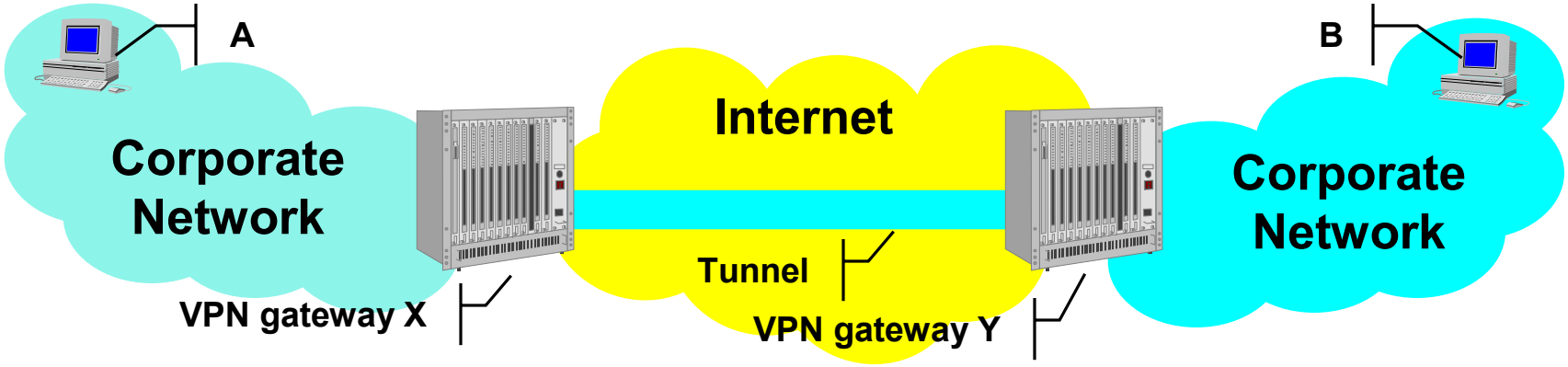
Model	Overlay	Peer
Access	L2TP, PPTP	--
Intranet	IPSec	MPLS
Extranet	IPSec	MPLS

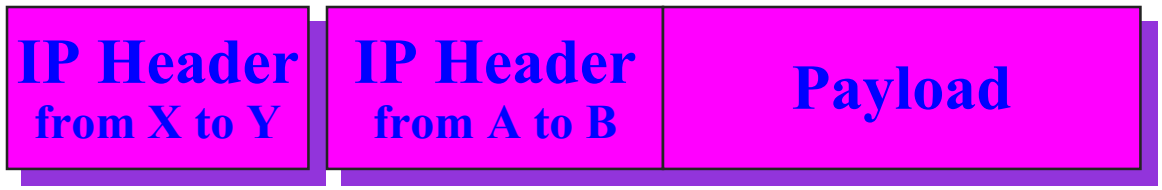
Tassonomia di tecnologie per VPN



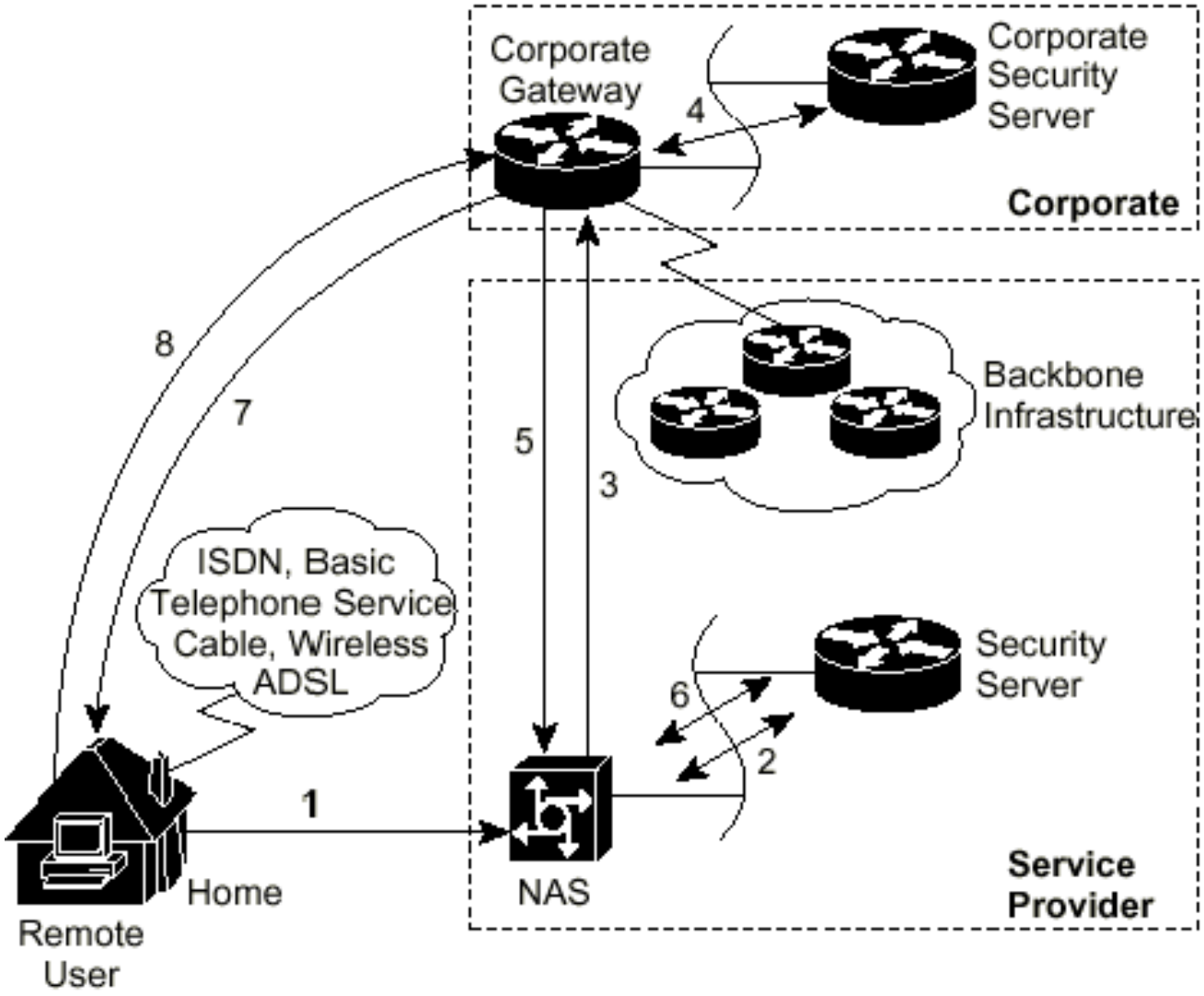
Tunneling

- A e B sono indirizzi aziendali
  - Non devono essere pubblici
- Il tunneling rende possibile il funzionamento
- Il tunneling di per se non garantisce sicurezza





VPN di accesso: due modalità operative



VPN di accesso

1. Remote user initiates PPP connection with NAS that accepts the call
2. NAS identifies remote user
3. NAS initiates L2TP or PPTP tunnel to desired corporate gateway (access server)
4. Corporare gateway authenticates remote user according to corporate security policy
5. Corporate gateway confirms acceptance of tunnel
6. NAS logs acceptance and/or traffic (optional)
7. Corporate gateway performs PPP negotiations with remote users (e.g., IPaddress assignment)
8. End-to-end data tunneled between user and corporate gateway

Protocolli per VPN di accesso

- L2TP (Layer 2 Tunneling Protocol)
  - Non è largamente implementato
  - Indipendente dal protocollo di livello 2
  - Sicurezza basata su IPsec
    - Robusta
- PPTP (Point-to-Point Tunneling Protocol)
  - Microsoft, Apple, …
    - Integrato nel dial-up networking
  - Multiprotocollo
  - Autenticazione e cifratura deboli
  - Gestione delle chiavi proprietaria

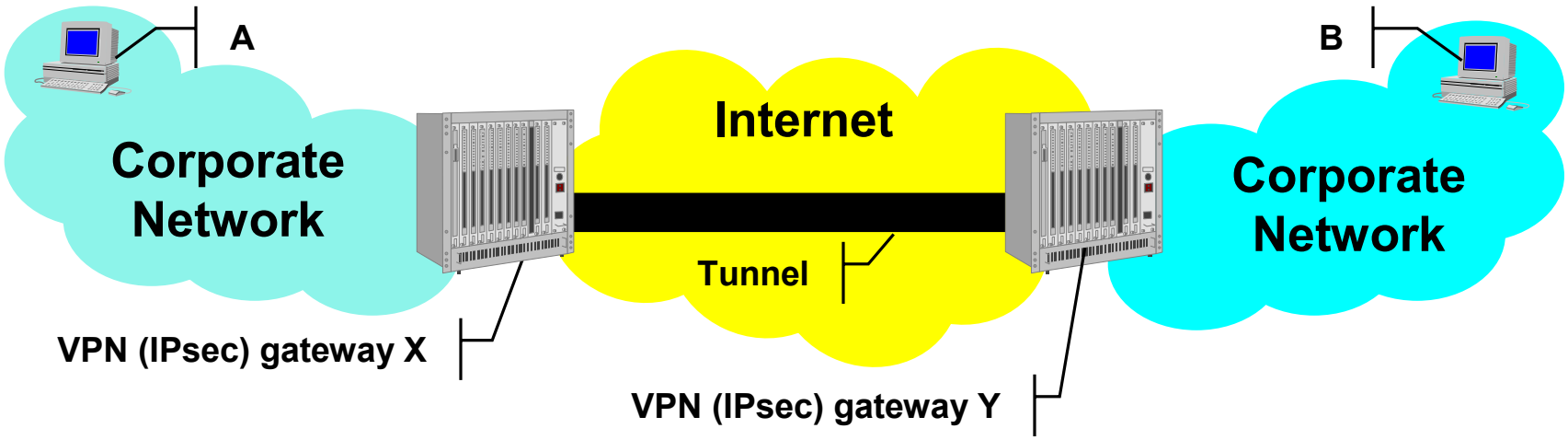
Vantaggi del Virtual Dial-Up

- Autenticazione e sicurezza
  - Fatte dal VPN Gateway
  - Politiche e informazioni della rete aziendale
  - Cifratura basata su IPsec
- Autorizzazione
  - Fatta dal VPN Gateway
  - Politiche e informazioni della rete aziendale
- Allocazione degli indirizzi
  - Indirizzi aziendali sono allocati dinamicamente
  - Stesso tipo di accesso di quando si è collegati direttamente

VPN basate su IPsec

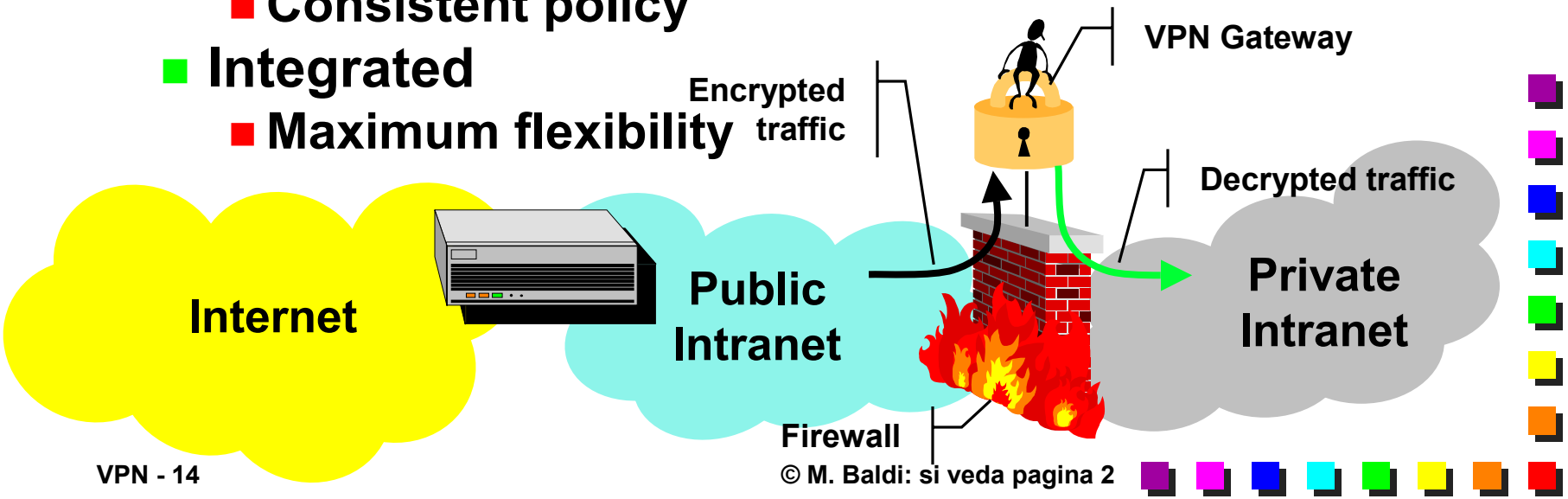
Tunnel IPsec tra VPN gateway

- Cifratura
- Autenticazione
- Imbustamento



VPN Gateway and Firewall

- Inside
  - No inspection of VPN traffic
  - VPN gateway protected by firewall
- Parallel
  - Potential uncontrolled access
- Outside
  - VPN gateway protected by access router
  - Consistent policy
- Integrated
  - Maximum flexibility

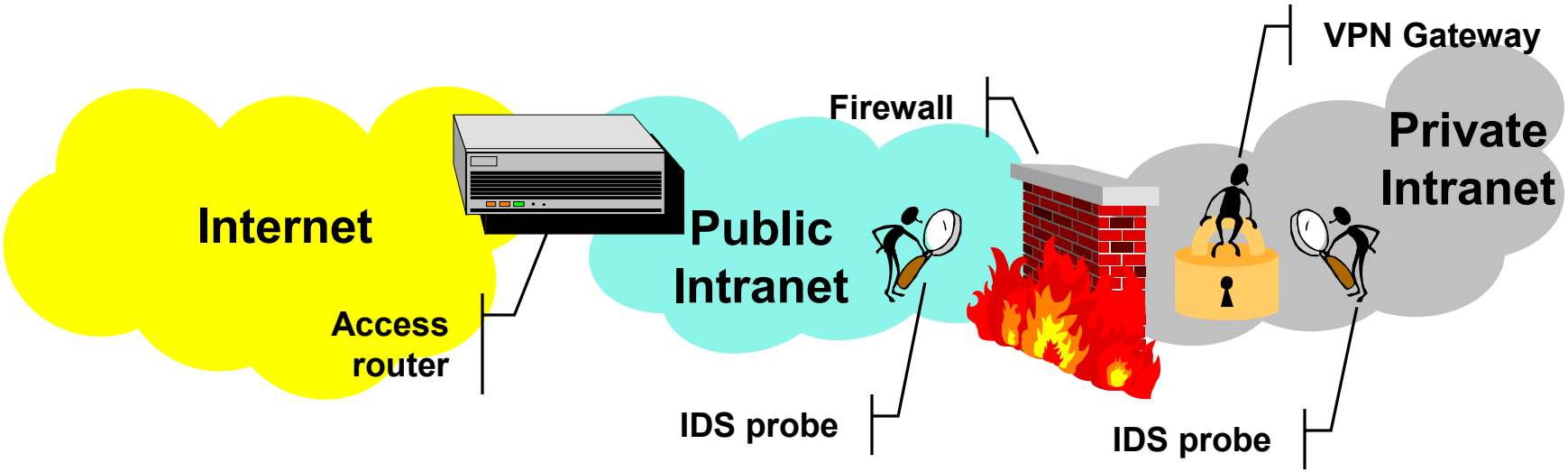


VPN Gateway and NAT

- Authentication Header (AH)
  - IP addresses are part of AH checksum calculation → packets discarded
- Transport mode
  - IP address of IPSec tunnel peer is not what expected → packets discarded
- No PAT (Protocol Address Translation)
- Tunnel mode
  - IP address within secure packet can be changed before entering the gateway
    - E.g., same addresses in two different VPN sites
  - Most often NAT is not needed on external packet

VPN Gateway and IDS

- IDS is usually outside the firewall
- No control on VPN traffic
- Multiple IDS probes
  - Outside firewall
  - Inside VPN gateway



VPN peer basate su IP

- Dedicated router
  - Il service provider realizza una rete di router dedicati ad un cliente
  - Utilizzabile solo per grossi clienti
- Shared/virtual router
  - Il provider crea istanze di router dedicati ad un cliente all'interno dei router fisici
  - Router di fascia alta permettono di avere centinaia di router virtuali
    - Tabella di routing e protocolli di routing per istanza
    - Supporto nel sistema operativo e tramite ASIC
  - Comunicazione tramite tunnel IPsec o GRE

VPN MPLS di livello 2: PWE3

- Pseudo Wire Emulation End-to-End
- Vari servizi sulla stessa rete:
  - IP, ma anche leased lines, frame relay, ATM, Ethernet
- Customer edge (CE) device offre interfaccia di servizio nativa
- Il traffico è trasportato su un LSP tra i CE
- Due etichette
  - Esterna - usata per il routing nella rete
    - Identifica il punto di accesso alla rete
  - Interna - multiplexing di vari utenti collegati al punto di accesso

VPN MPLS di livello 2: PWE3

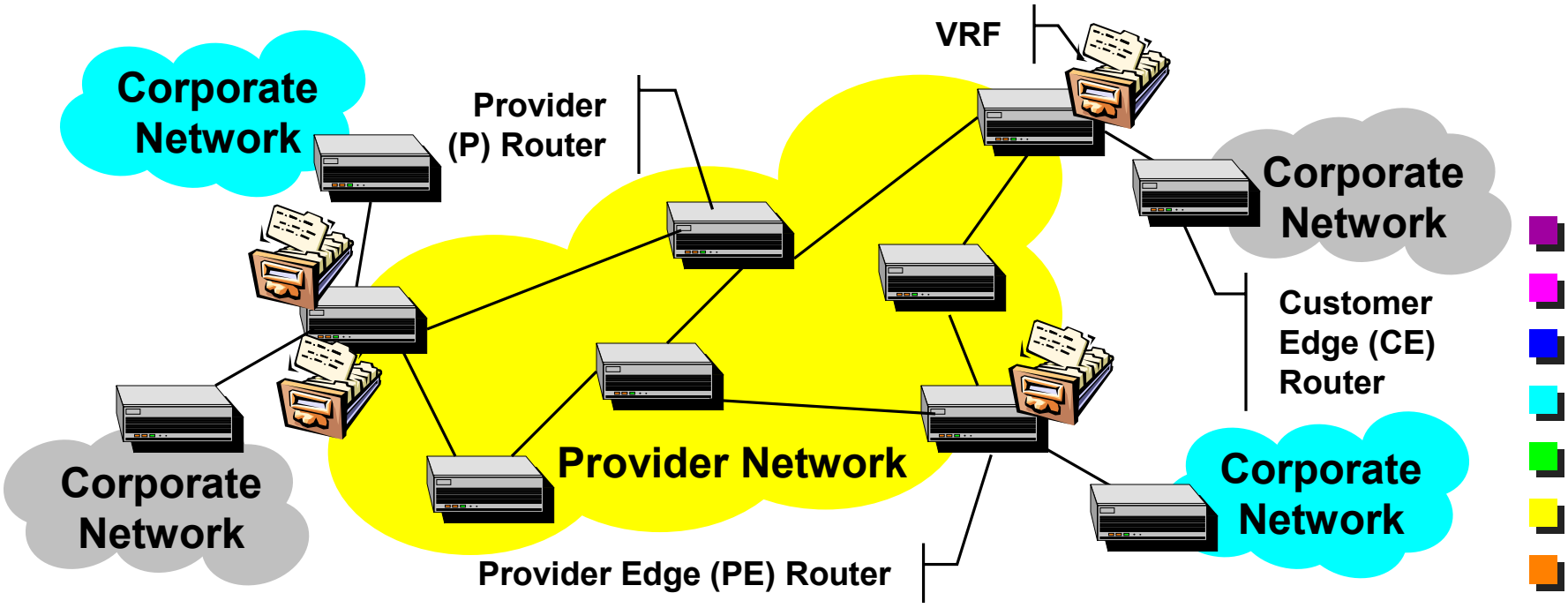
- Ci possono essere apparati interni alla rete
  - Per esempio uno switch ATM all'interno della rete del service provider su cui sono attestati LSP
- Prevalentemente instaurazione manuale di LSP
- Proposte per uso di LDP e BGP

VPN MPLS di livello 3

- Soluzioni provider provisioned
  - Politiche della VPN realizzate dal service provider
  - Non serve esperienza da parte del clienti
- Scalabilità
  - Utilizzo su larga scala
- Due alternative
  - RFC2547bis (BGP)
    - Inizialmente spinto da Cisco
    - Approccio attualmente più utilizzato
  - Virtual router
    - Inizialmente spinto da Nortel e Lucent

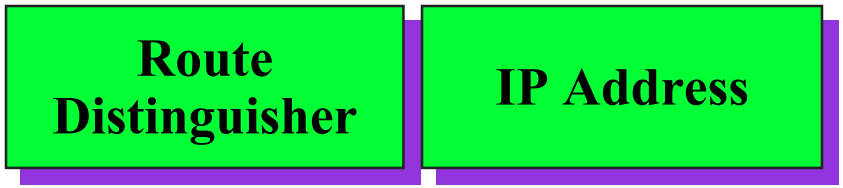
Componenti della soluzione MPLS/BGP

- VRF (VPN Routing and Forwarding) table
  - Associata ad una o più porte
  - Informazioni per l'inoltro dei pacchetti ricevuti da tali porte



Piano di controllo

- Routing exchange at edges
- Route filtering
  - PE routers determine which routes to install in VRF
- Support for overlapping address spaces
  - VPN-IPv4 Address family
    - Route Distinguisher + IPv4 address



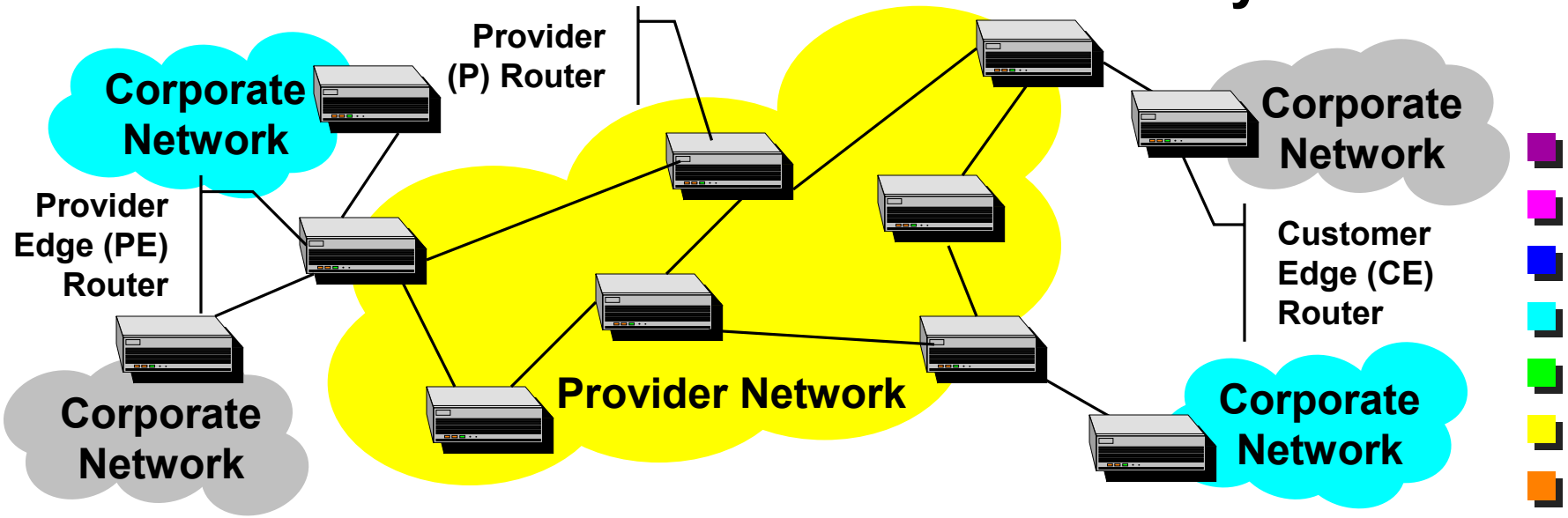
MPLS VPN Components

CE router creates adjacency with PE router

- It advertises its destinations
- It receives advertisements of other VPN destinations
- Static routing, or
- IGP (Interior Gateway Protocol)
  - (e.g., OSPF, RIP)
- E-BGP (Exterior-Border Gateway Protocol)
- PE router does not keep routes for all VPNs

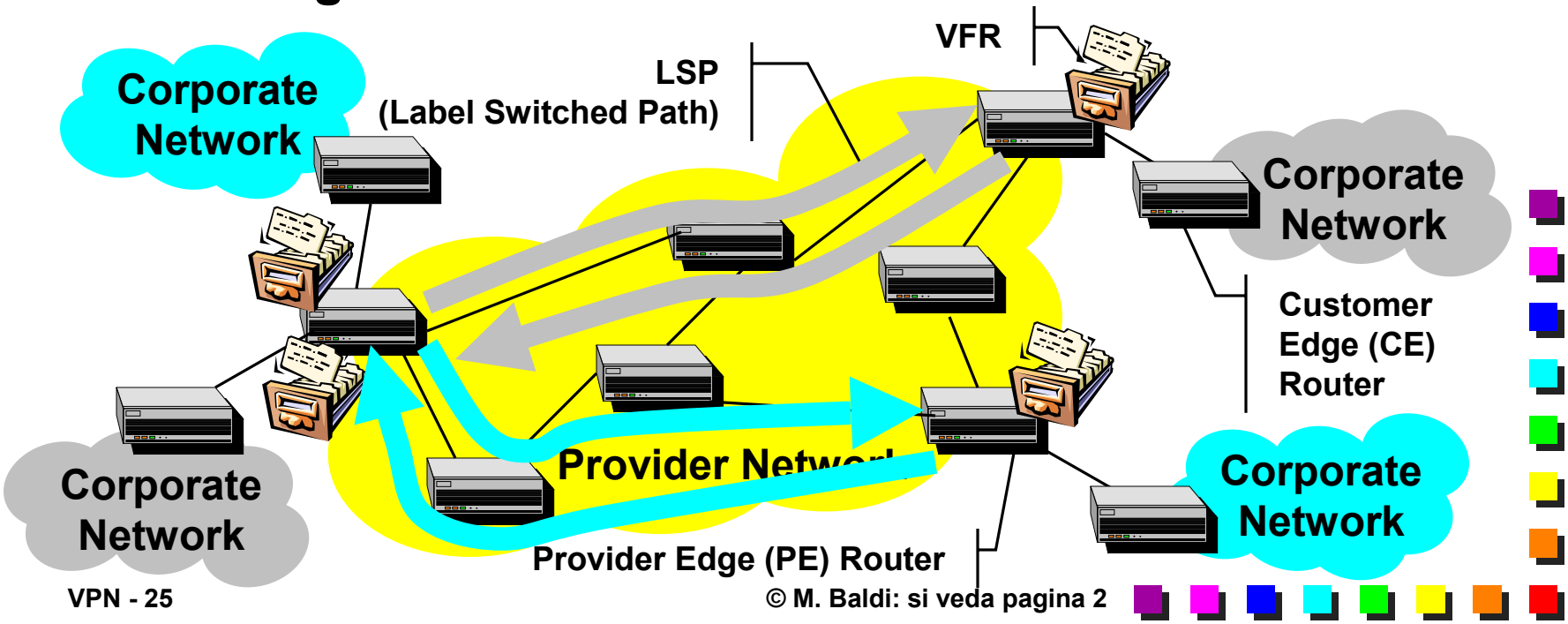
MPLS VPN Components

- PE routers
  - Exchange routing information
    - I-BGP (Interior-Border Gateway Protocol)
  - Are ingress and egress LSR (Label Switch Router) for the backbone
- P routers have routes to PE routers only



Piano di controllo

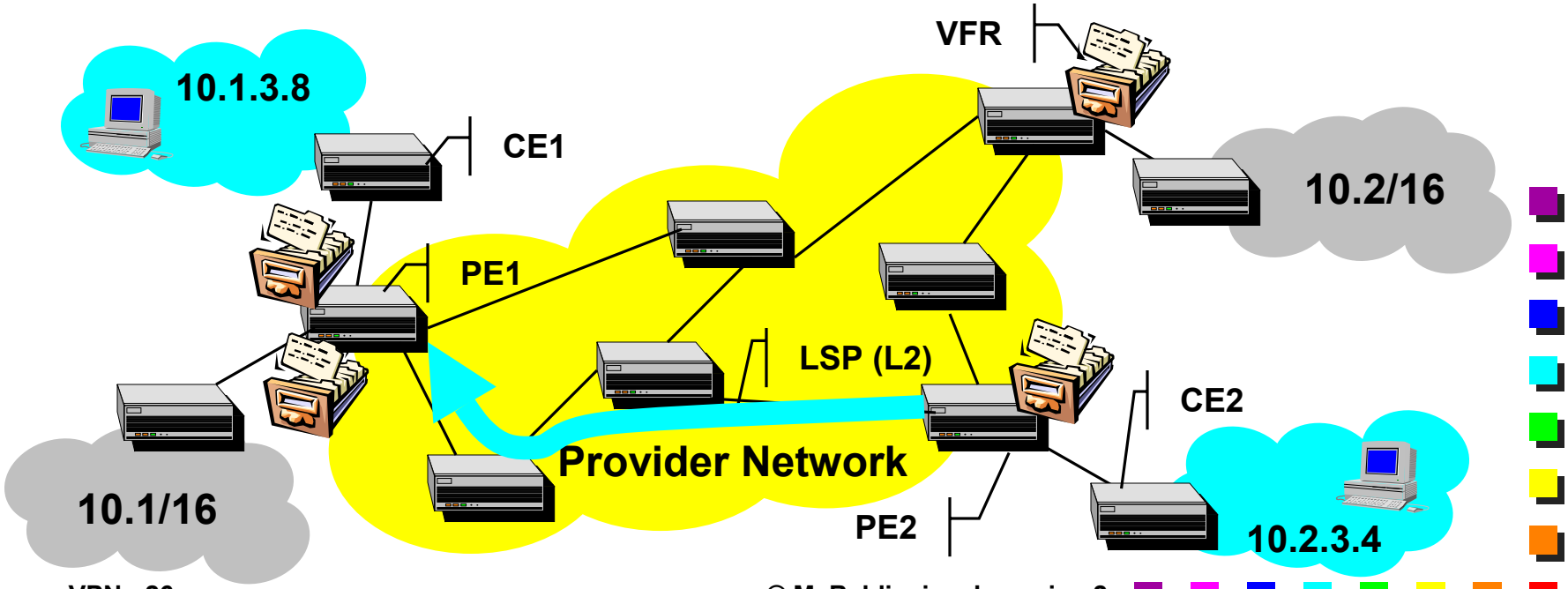
- Creazione di LSP attraverso la dorsale
  - I-BGP porta informazioni sulle etichette
  - LDP (Label Distribution Protocol) e/o
  - RSVP (Resource reSerVation Protocol)
  - Maglia di LSP tra i router PE della stessa VPN



Packet Routing

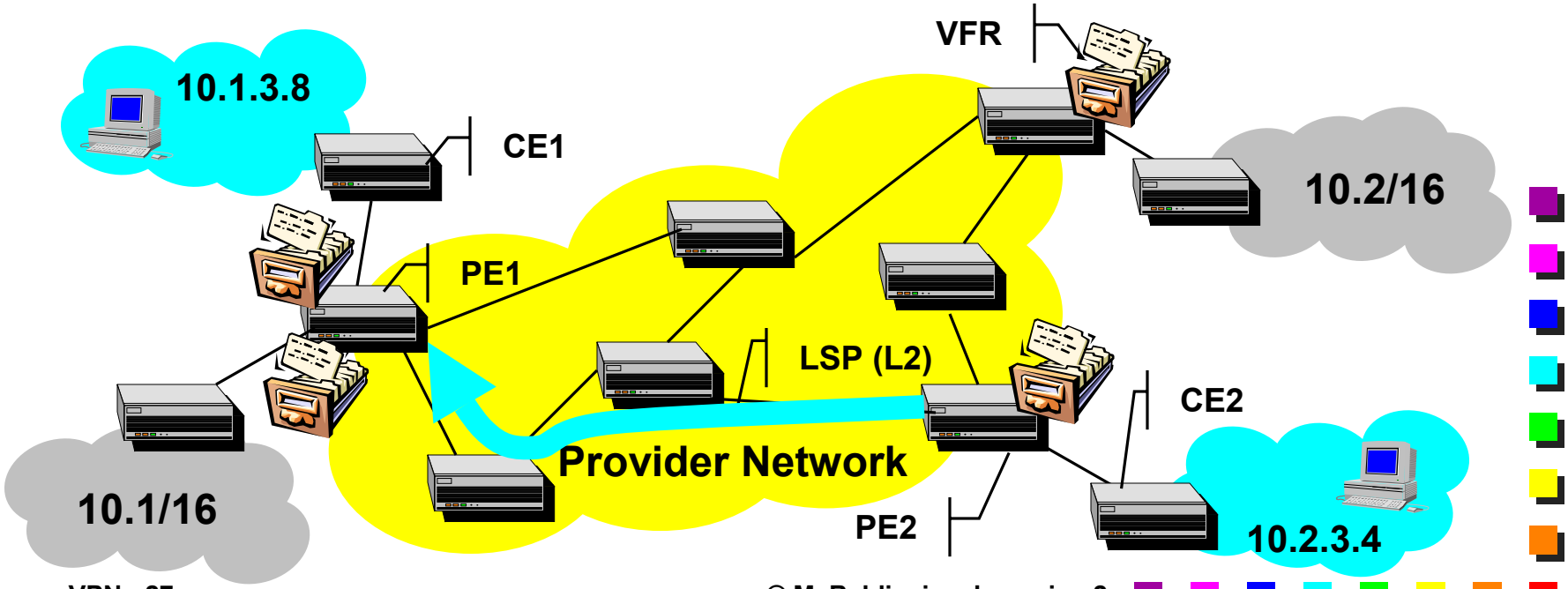
Packet from 10.2.3.4 to 10.1.3.8

- **Default gateway → PE2 router**



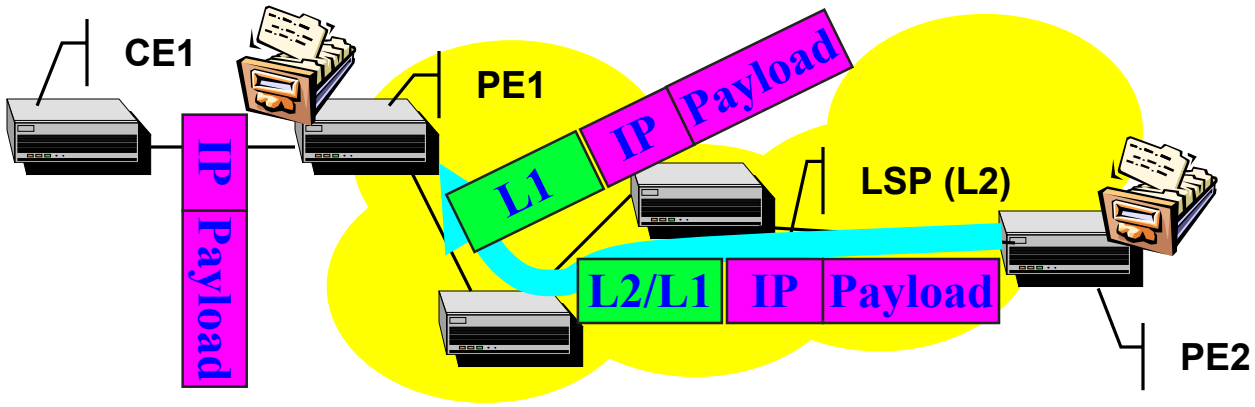
Packet Routing

- PE2 looks-up VRF
  - MPLS label advertised by PE1 for 10.1/16: L1
  - BGP next hop (PE1)
  - Outgoing interface for LSP to PE1
  - Initial label for LSP from PE2 to PE1: L2



Packet Routing

- PE2 pushes L1 and L2 on label stack
- P routers forward packet to PE1 using L2
- Last hop before PE1 pops L2
- PE1 receives packet with L1
  - PE1 pops L1: plain IP packet
  - PE1 uses L1 to route packet to proper output interface



Vantaggi

- Non ci sono vincoli sul piano di indirizzamento
  - Unicità degli indirizzi solo all'interno della VPN
- I router CE non scambiano informazioni di routing tra di loro
- Il cliente non deve gestire la dorsale
- Il gestore non ha una dorsale per ogni cliente
- La VPN può essere definita attraverso le reti di vari provider
- Sicurezza equivalente a quella di Frame relay o ATM
  - Isolamento del traffico
  - No cifratura (confidenzialità)
- Supporto di QoS (qualità di servizio) mediante gli experimental bit di MPLS

Supporto Multi-Protocol

- Access VPN
  - Trasparente
    - L2TP e PPTP
- Overlay (basato IPsec)
  - Generic Routing Encapsulation (GRE)
    - Trasporto di qualsiasi protocollo all'interno di IP
- Peer (basate su MPLS)
  - Insito in MPLS (*Multi-Protocol* Label Switching)

Riferimenti bibliografici

- E. Rosen and Y. Rekhter, “BGP/MPLS VPNs,” RFC 2547, March 1999.
- E. Rosen et al., “BGP/MPLS VPNs,” <draft-rosen-rfc2547bis-02.txt>, July 2000.
- C. Semeria, “RFC 2547bis: BGP/MPLS VPN Fundamentals,” Juniper Networks, White paper 200012-001, March 2001.
- IETF MPLS Working Group, http://www.ietf.org/html.charters/mpls-charter.html

Riferimenti bibliografici

- Hanks, S., Editor, "Generic Routing Encapsulation over IPv4", RFC 1702, October 1994.
- Brian Browne, “Best Practices For VPN Implementation,”Business Communication Review, March 2001.
- http://www.ietf.org/html.charters/l2vpn-charter.html
- http://www.ietf.org/html.charters/l3vpn-charter.html