# Master Course
# Computer Networks
# IN2097

**Prof. Dr.-Ing. Georg Carle**
**Christian Grothoff, Ph.D.**

**Chair for Network Architectures and Services**
**Institut für Informatik**
**Technische Universität München**
**http://www.net.in.tum.de**

# Outline

- Project

- Network virtualisation:
  Link virtualization: ATM, MPLS

Chair for Network Architectures and Services – Prof. Carle
Department for Computer Science
TU München

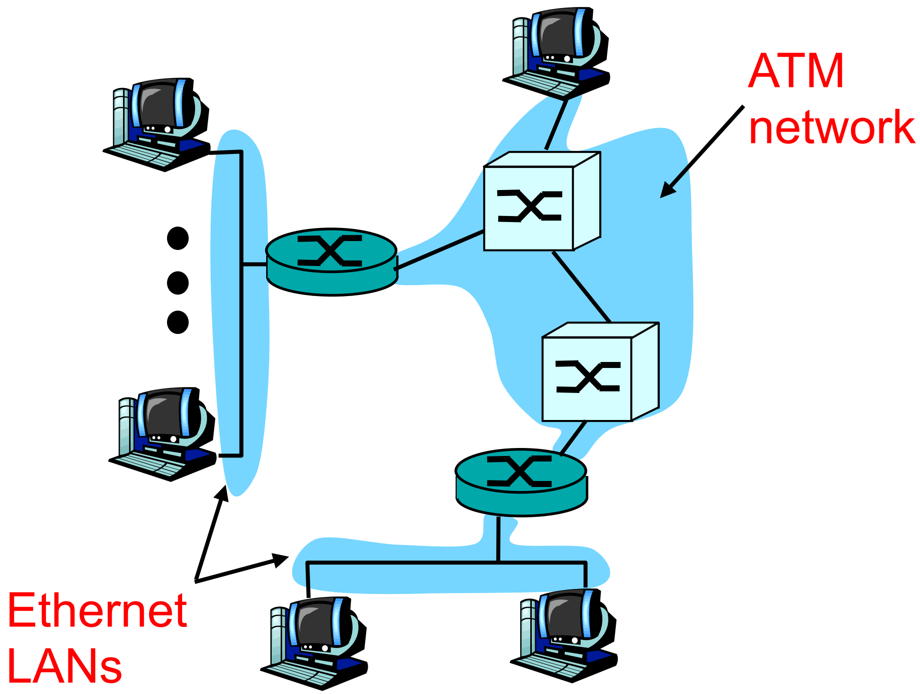
# Network Architectures

## Link virtualization: ATM, MPLS

# IP-Over-ATM

Issues:

- IP datagrams into ATM AAL5 PDUs
- from IP addresses to ATM addresses
  - just like IP addresses to 802.3 MAC addresses
  - ARP server



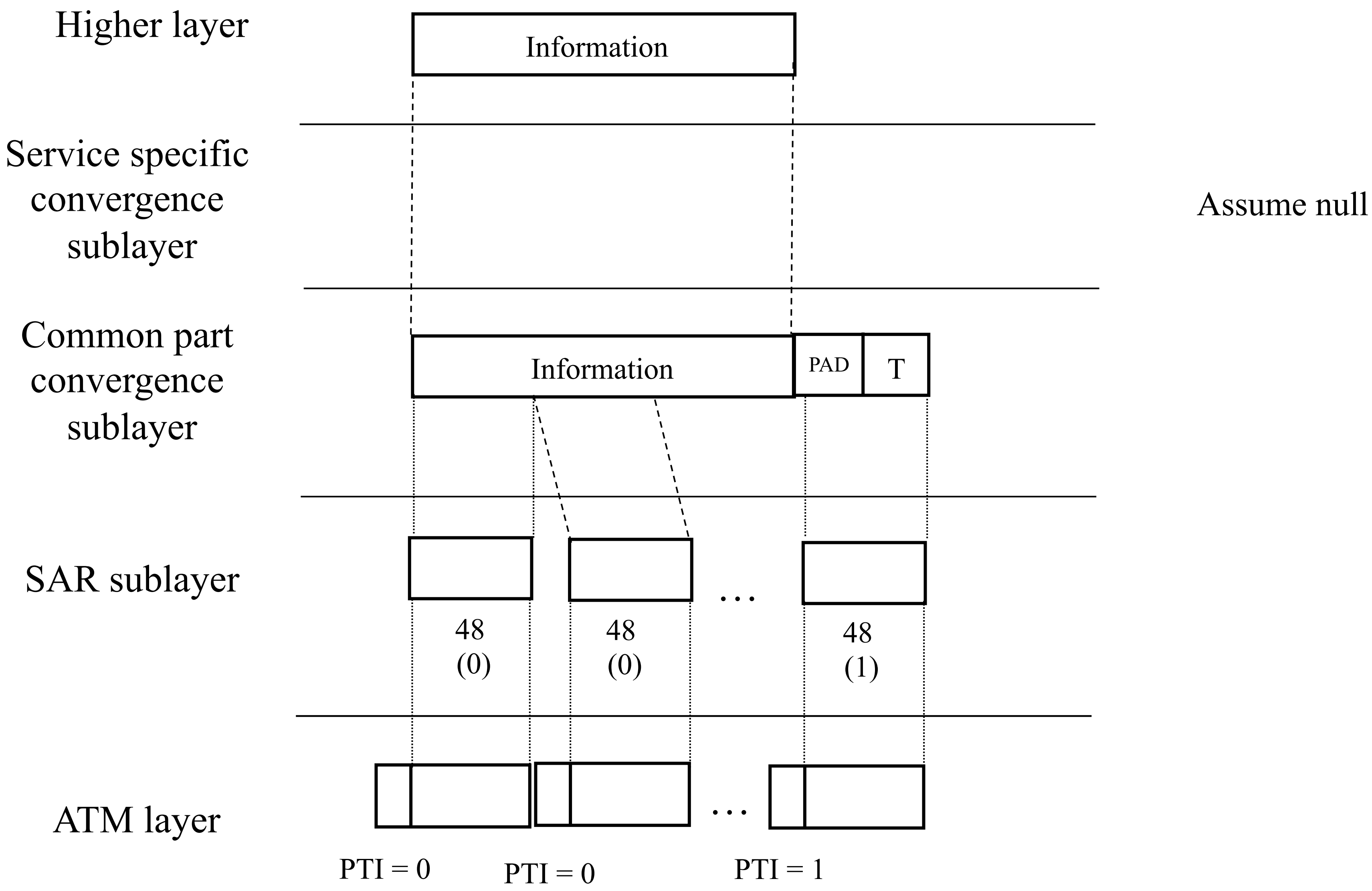
# AAL 5 Protocol

- AAL5 is a simple and efficient AAL (SEAL) to perform a subset of the functions of AAL3/4
- The CPCS-PDU payload length can be up to 65,535 octets and must use PAD (0 to 47 octets) to align CPCS-PDU length to a multiple of 48 octets

| | |
|---|---|
| PAD | Padding |
| CPCS-UU | CPCS User-to-User Indicator |
| CPI | Common Part Indicator |
| Length | CPCS-PDU Payload Length |
| CRC-32 | Cyclic Redundancy Chuck |

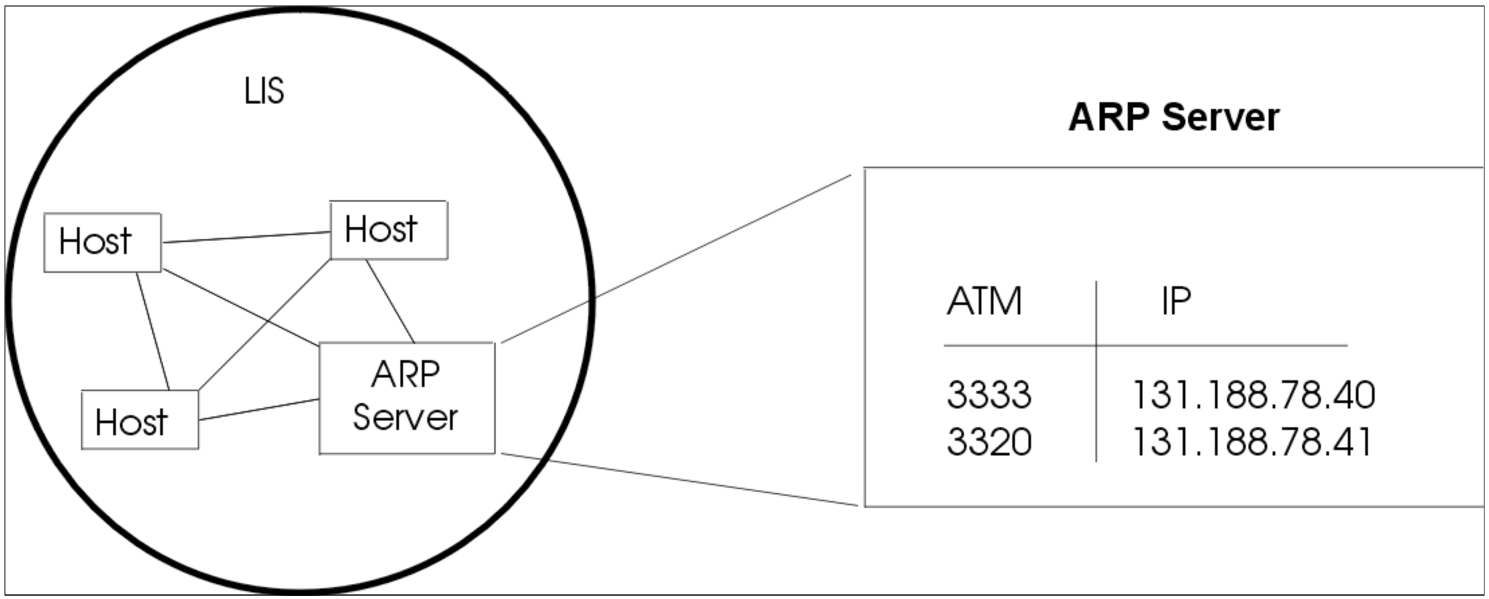
| | 0 - 47 | 1 | 1 | 2 | 4 |
|---|---|---|---|---|---|
| CPCS-PDU Payload | PAD | CPCS UU | CPI | Length | CRC-32 |

# AAL 5 Layering



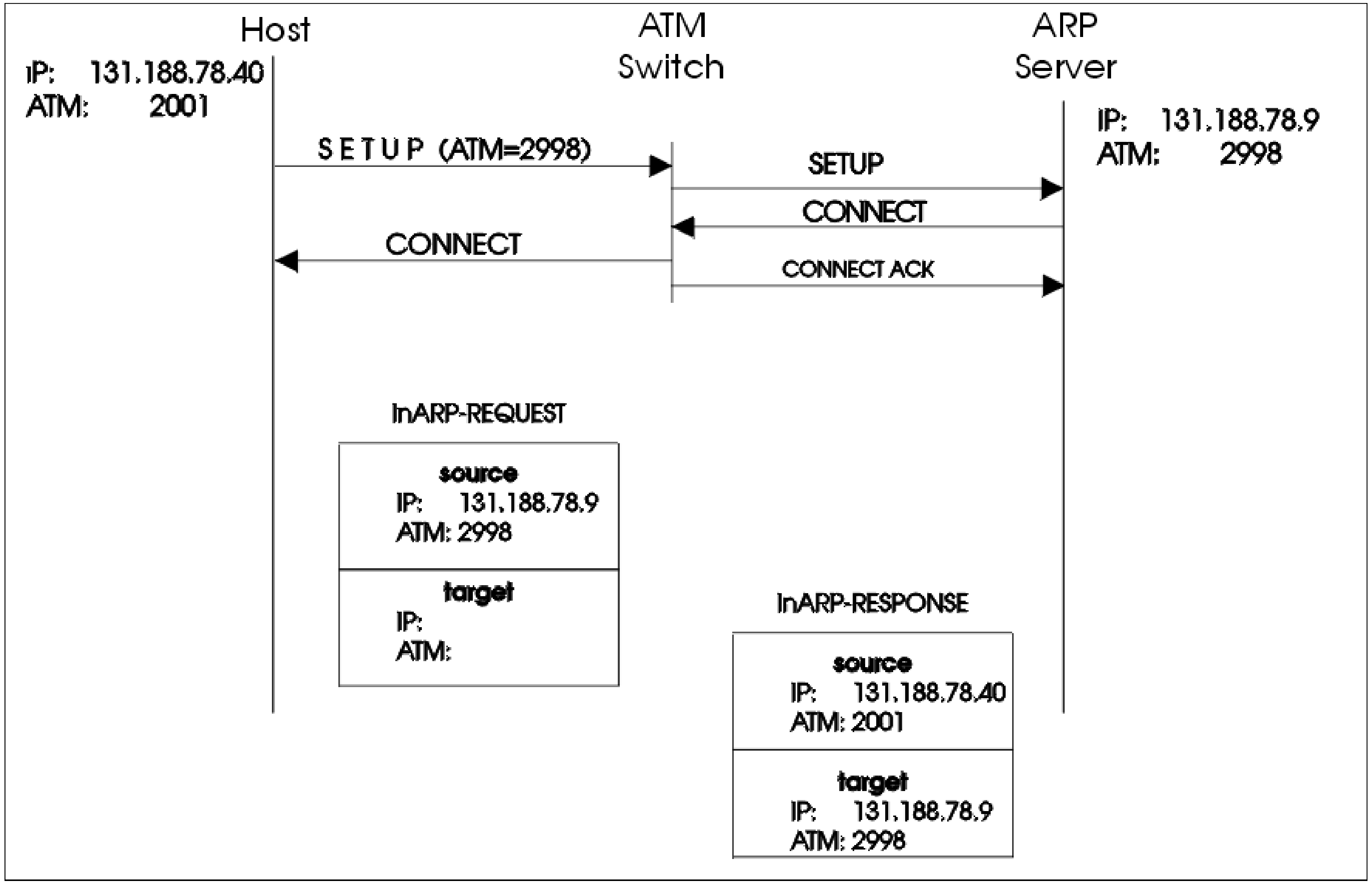
# Classical IP and ARP over ATM (CLIP)

- Specification of a complete IP implementation for ATM
- Suitable for ATM unicast communication
- Encapsulation of IP packets into AAL PDUs
- Support for large MTU sizes
- There must be an ATMARP server in each LIS (Logical IP Subnet)



# Classical IP and ARP over ATM (CLIP)

- The host registers its IP/ATM address information at the ATMARP server using the InARP protocol



# Classical IP and ARP over ATM (CLIP)

- RFC 1577: Classical IP and ARP over ATM
- ATMARP Server Operational Requirements
  - The ATMARP server, upon the completion of an ATM call/ connection of a new VC, will transmit an InATMARP request to determine the IP address of the client.
  - The InATMARP reply from the client contains the information necessary for the ATMARP Server to build its ATMARP table cache.
  - This information is used to generate replies to the ATMARP requests it receives.
- InATMARP is the same protocol as the original InARP protocol presented in RFC 1293 but applied to ATM networks: Discover the protocol address of a station associated with a virtual circuit.
- RFC 1293: Bradely, T., and C. Brown, "Inverse Address Resolution Protocol“, January 1992.

# Classical IP and ARP over ATM (CLIP)

- RFC 1577: Classical IP and ARP over ATM
- ATMARP Client Operational Requirements
  1. Initiate the VC connection to the ATMARP server for transmitting and receiving ATMARP and InATMARP packets.
  2. Respond to ARP_REQUEST and InARP_REQUEST packets received on any VC appropriately.
  3. Generate and transmit ARP_REQUEST packets to the ATMARP server and to process ARP_REPLY appropriately. ARP_REPLY packets should be used to build/refresh its own client ATMARP table entries.
  4. Generate and transmit InARP_REQUEST packets as needed and to process InARP_REPLY packets appropriately. InARP_REPLY packets should be used to build/refresh its own client ATMARP table entries.
  5. Provide an ATMARP table aging function to remove own old client ATMARP tables entries after a period of time.

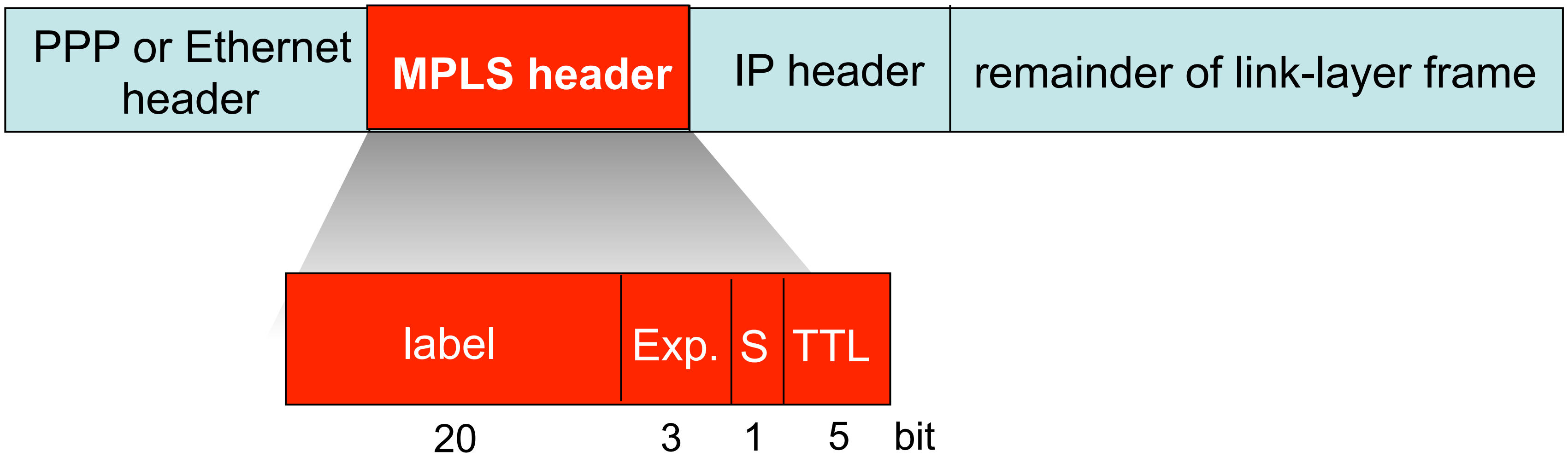
Chair for Network Architectures and Services – Prof. Carle
Department for Computer Science
TU München

# MPLS

Multi-Protocol Label Switching

# Multiprotocol label switching (MPLS)

- Initial goal: speed up IP forwarding by using fixed length label (instead of IP address) to do forwarding
  - borrowing ideas from Virtual Circuit (VC) approach
  - IP datagram still keeps IP address
  - RFC 3032 defines MPLS header
    - Label: has role of Virtual Circuit Identifier
    - Exp: experimental usage, may specify Class of Service (CoS)
    - S: Bottom of Stack - end of series of stacked headers
    - TTL: time to live



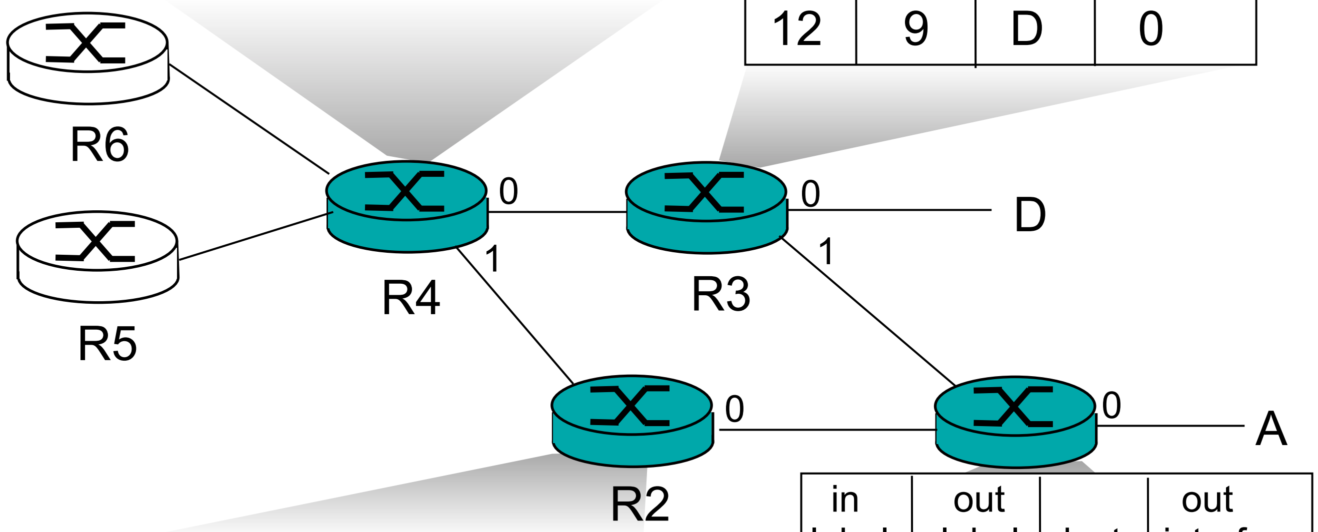
# MPLS capable routers

- a.k.a. label-switched router
- forwards packets to outgoing interface based only on label value (don't inspect IP address)
  - MPLS forwarding table distinct from IP forwarding tables
- signaling protocol needed to set up forwarding
  - Label Distribution Protocol LDP
    (RFC 3036 → obsoleted by RFC 5036)
  - RSVP-TE (RFC 3209
    → updated by RFCs 3936, 4420, 4874, 5151, 5420, 5711)
- forwarding possible along paths that IP alone would not allow (e.g., source-specific routing)
- MPLS supports traffic engineering
- must co-exist with IP-only routers

# MPLS forwarding tables

| in label | out label | dest | out interface |
|---|---|---|---|
| | 10 | A | 0 |
| | 12 | D | 0 |
| | 8 | A | 1 |

| in label | out label | dest | out interface |
|---|---|---|---|
| 10 | 6 | A | 1 |
| 12 | 9 | D | 0 |

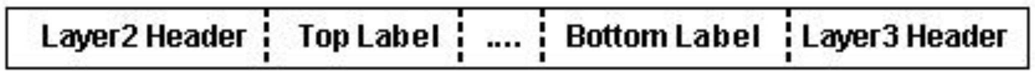



| in label | out label | dest | out interface |
|---|---|---|---|
| 8 | 6 | A | 0 |

| in label | out label | dest | out interface |
|---|---|---|---|
| 6 | - | A | 0 |

# MPLS

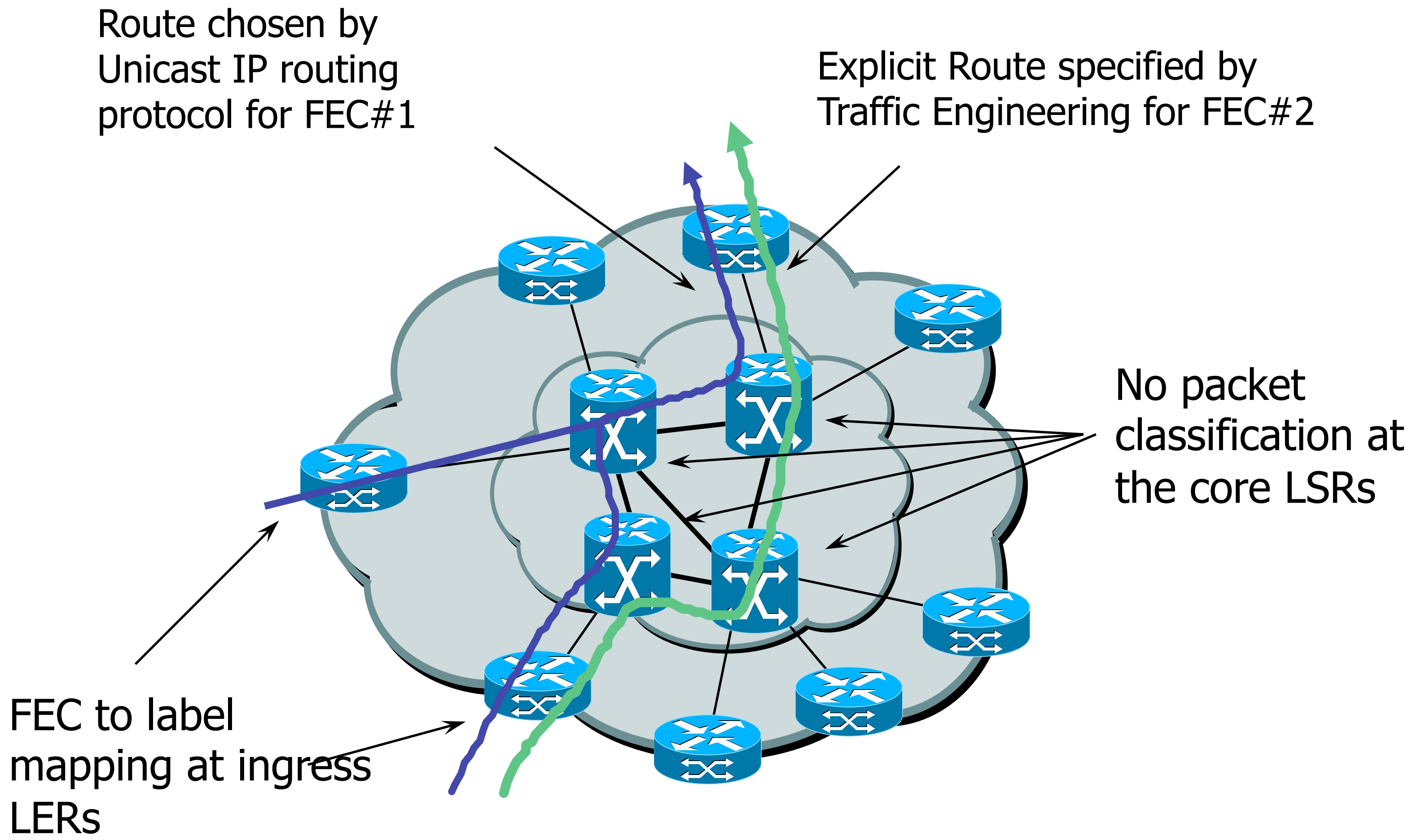
- Label Switched Path (LSP)
  - set up by signalling protocol
  - has sequence of labels
- Forwarding Equivalence Class (FEC)
  - specification of packets treated the same way by a router
  - forwarded over same LSP
  - can be specified by destination prefix, e.g. FEC 10.1.1.0/24
- Label Switching Router
  - MPLS-capable IP router; may bind labels to FEC
- MPLS node
  - does not need IP stack
- stacked labels
  - label push; label pop



# Benefits of MPLS

- High Speed Switching
  - facilitates construction of nodes with wire-line speed
- Simplifying packet forwarding
  - Routing decision can be limited to edge of AS
- Traffic Engineering
  - MPLS may control paths taken by different flows, e.g. to avoid congestion points for certain flows
- Quality of Service (QoS) support
  - resources may be specified for specific flows, isolation among flows
- Network scalability
  - label stacking allows to arrange MPLS domains in a hierarchy
- Supporting VPNs
  - tunneling of packets from an ingress point to an egress point

# Forwarding Equivalence Class Routing



# MPLS Flexibility

Label semantics

- ❑ Fine or coarse grained
- ❑ Unicast or multicast
- ❑ Explicit or implicit route
- ❑ VPN identifier

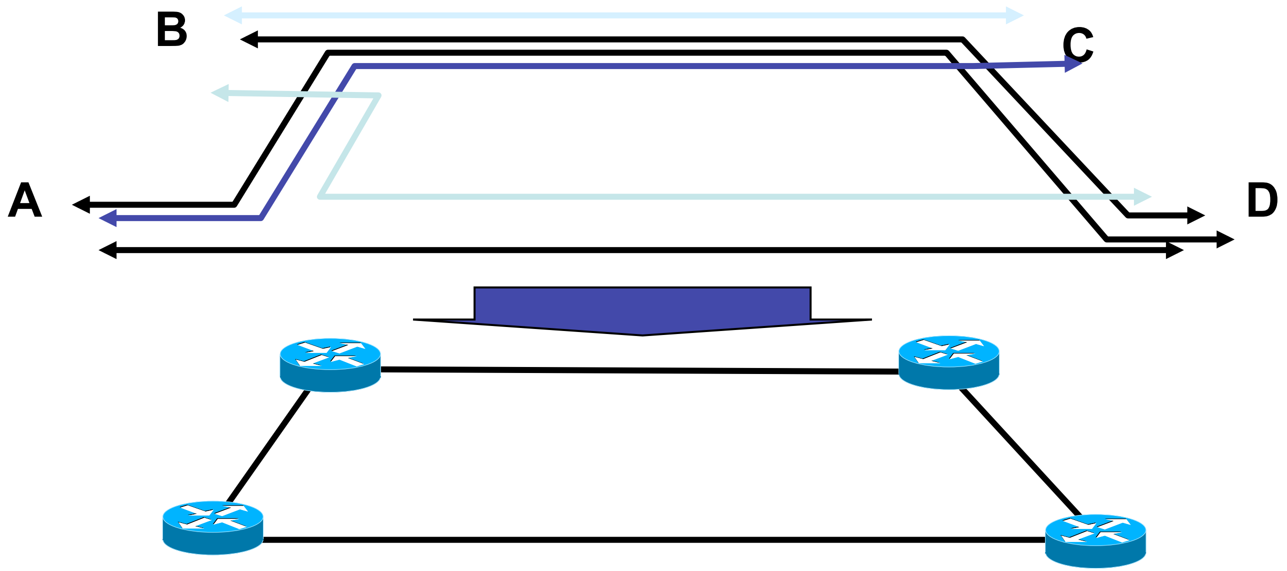
⇨ Loose semantics create flexible control

# Traffic Engineering

- Traffic engineering: process of mapping traffic demand onto a network

*Demand*

*Network Topology*




- Purpose of traffic engineering:
  - Maximize utilization of links and nodes throughout the network
  - Engineer links to achieve required delay, grade-of-service
  - Spread network traffic across network links, reduce impact of failure
  - Ensure available spare link capacity for re-routing traffic on failure
  - Meet policy requirements imposed by the network operator

⇨ Traffic engineering key to optimizing cost/performance

# Virtual Private Networks

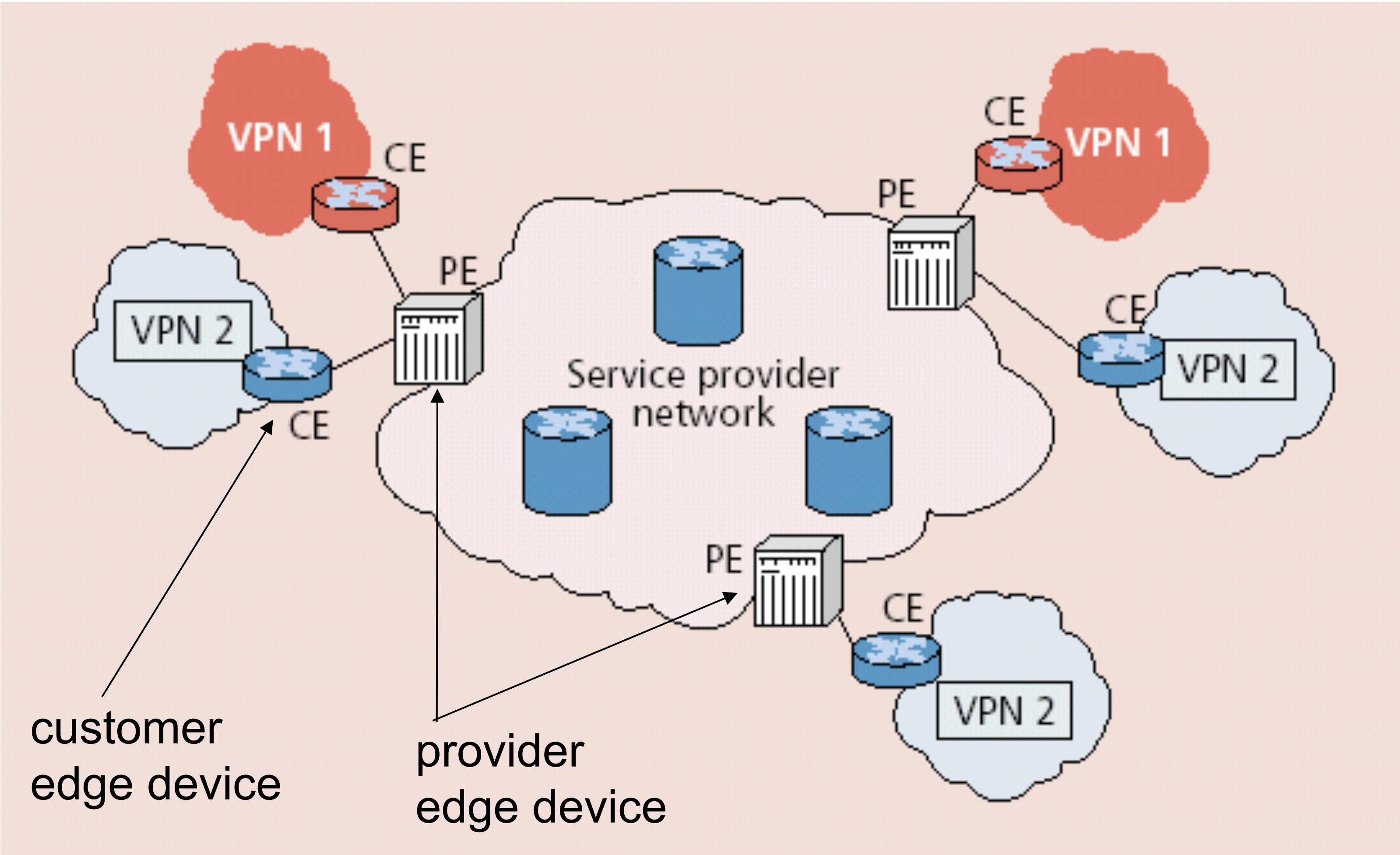
# Virtual Private Networks (VPN)

**VPNs**

Networks perceived as being private networks by customers using them, but built over shared infrastructure owned by service provider (SP)

- Service provider infrastructure:
  - backbone
  - provider edge devices
- Customer:
  - customer edge devices
    (communicating over shared backbone)

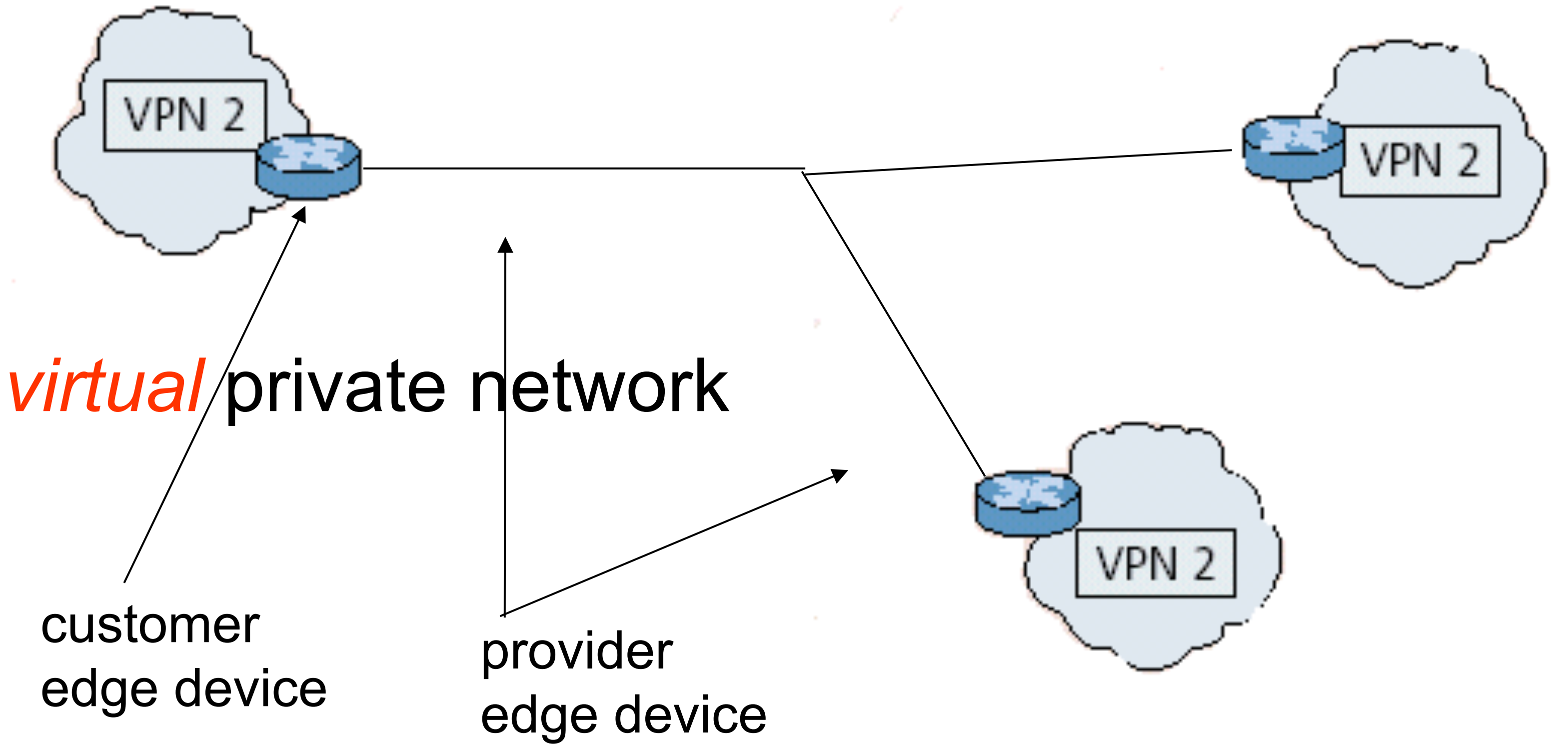
# VPN Reference Architecture



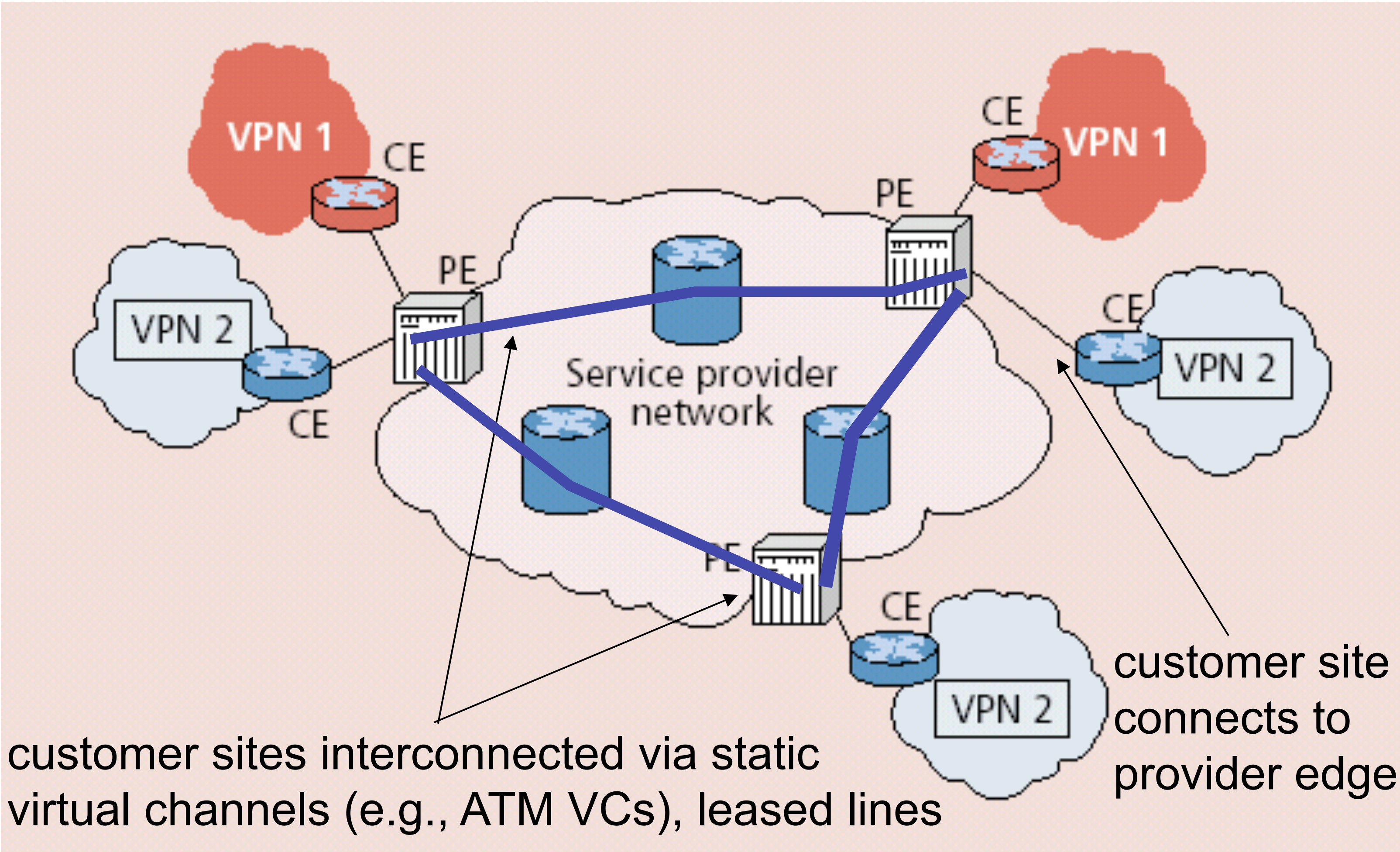
# VPNs: Why?

- Privacy
- Security
- Works well with mobility (looks like you are always at home)
- Cost
  - many forms of newer VPNs are cheaper than leased line VPNs
  - ability to share at lower layers even though logically separate means lower cost
  - exploit multiple paths, redundancy, fault-recovery in lower layers
  - need isolation mechanisms to ensure resources shared appropriately
- Abstraction and manageability
  - all machines with addresses that are “in” are trusted no matter where they are

# VPN: logical view

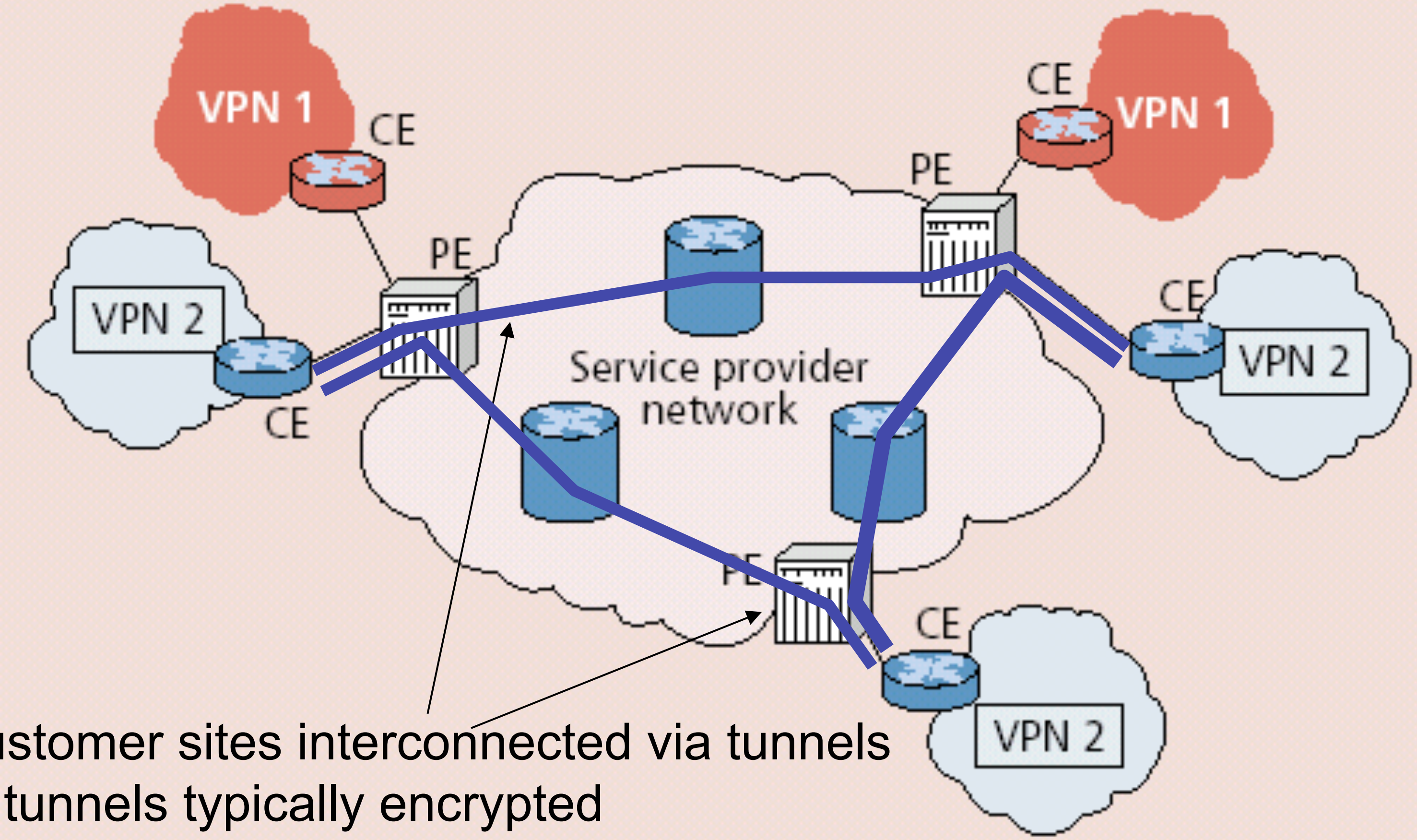


# Leased-Line VPN



# Customer Premise VPN

- all VPN functions implemented by customer



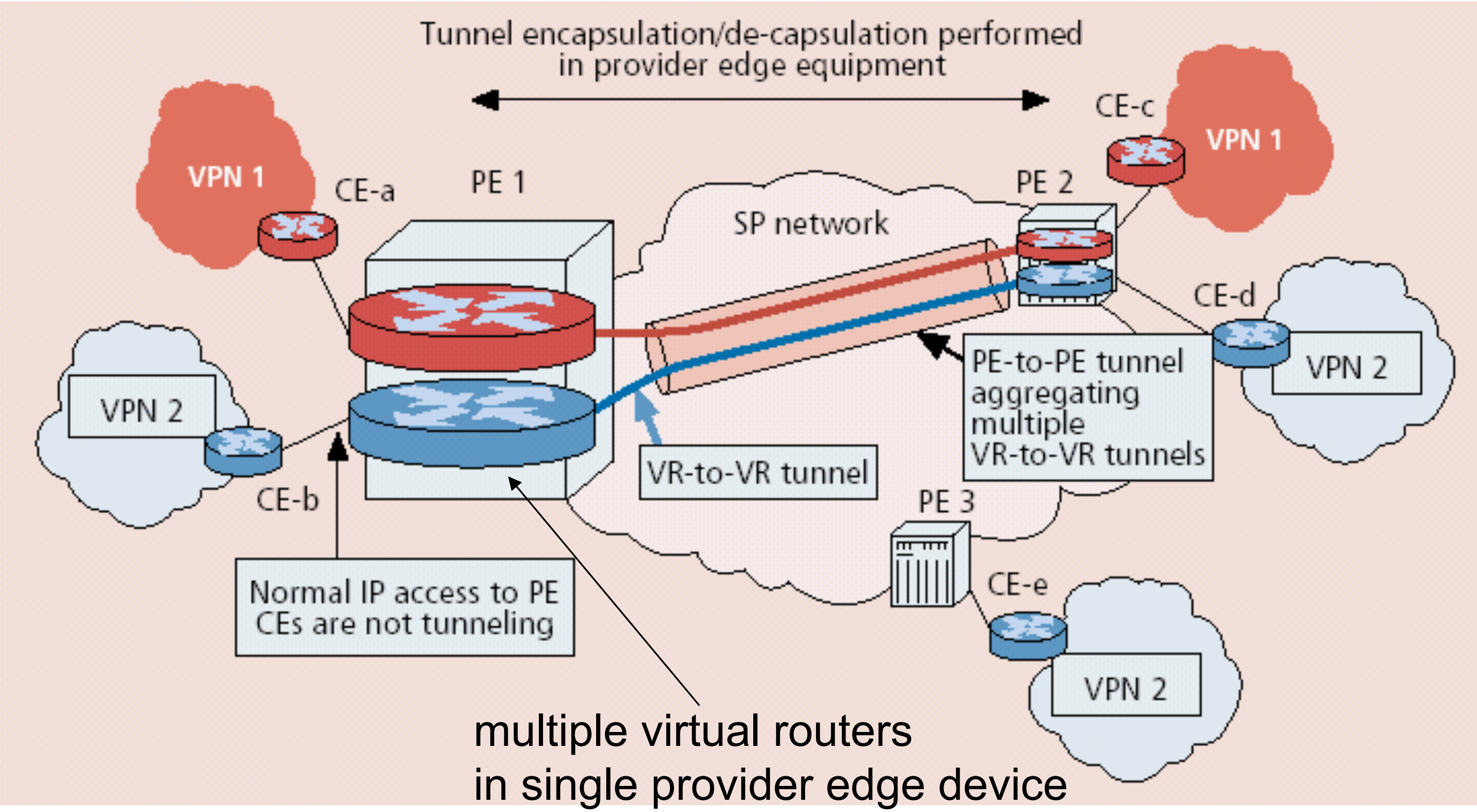

customer sites interconnected via tunnels

- tunnels typically encrypted
- Service provider treats VPN packets like all other packets

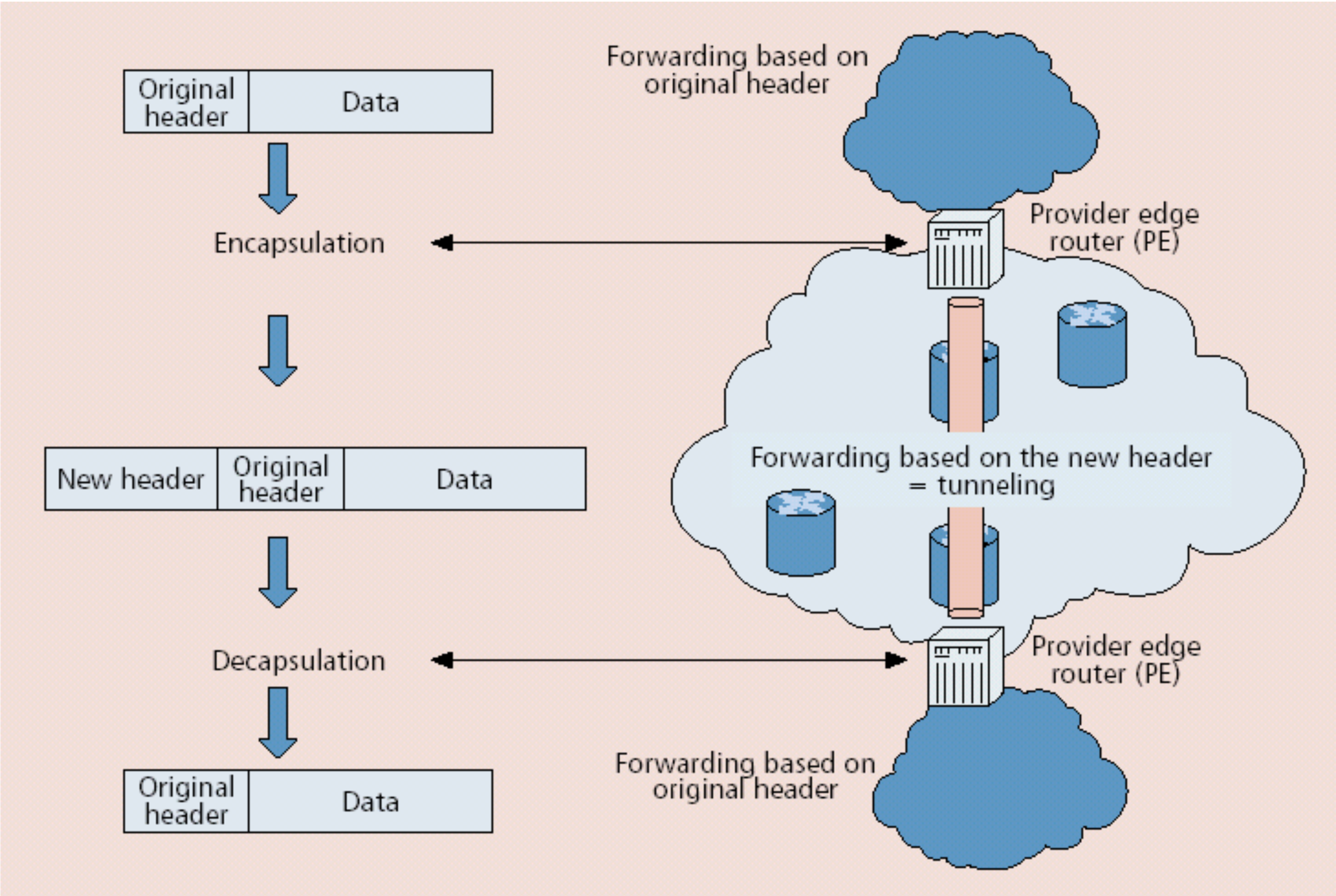
# Variants of VPNs

- Leased-line VPN
  - configuration costs and maintenance by service provider: long time to set up, manpower
- CPE-based VPN
  - expertise by customer to acquire, configure, manage VPN
- Network-based VPN
  - Customer routers connect to service provider routers
  - Service provider routers maintain separate (independent) IP contexts for each VPN
    - sites can use private addressing
    - traffic from one VPN cannot be injected into another

# Network-based Layer 3 VPNs



# Tunneling



Original header
Data
Encapsulation
New header
Original header
Data
Decapsulation
Original header
Data
Forwarding based on original header
Provider edge router (PE)
Forwarding based on the new header = tunneling
Provider edge router (PE)
Forwarding based on original header

# MPLS-based VPN