Virtual Private Networks

An introduction and an MPLS case

Lecture slides for S-38.192

28.2.2002

Mika Ilvesmäki

”The idea is to create a private network via tunneling and/or encryption over the public Internet. Sure, it’s a lot cheaper than using your own frame-relay connections, but it works about as well as sticking cotton in your ears in Times Square and pretending nobody else is around.”

- Wired Magzine on VPNs in February 1998 -

Contents

- VPN terminology
- VPNs on IP layer
  - addressing, routing, security
- Engineering VPNs with
  - Controlled route leaking
  - Tunnels
  - MPLS

HELSINKI UNIVERSITY OF TECHNOLOGY Mika Ilvesmäki, Lic.Sc. (Tech.)

What is a VPN?

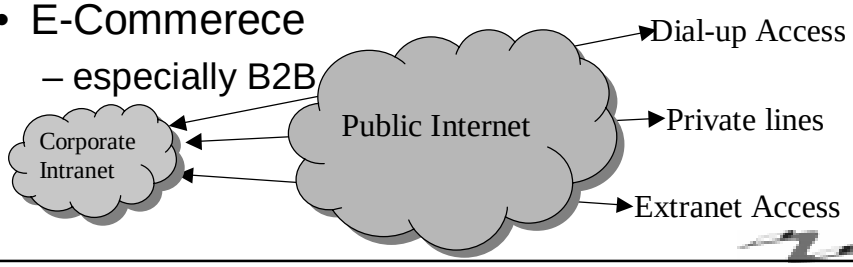
- Virtual
  - network resources used are part of a common shared resource
- Private
  - privacy of addressing and routing – topological isolation
  - security (authentication, encryption, integrity) of the data
  - (seemingly) dedicated use of network resources – temporal isolation
- Network
  - devices that communicate through some arbitrary method

Virtual Private Networks

- A VPN is a private network constructed within a public network infrastructure, such as the global internet
  - Equipment and facilities used to build the VPN are also in other's use->virtual
  - Routing and addressing is separate from all other networks and data is secured -> private
  - Connect geographically dispersed sites -> network
- VPNs require that the flow of routing data is constrained to constrain the flow of user data

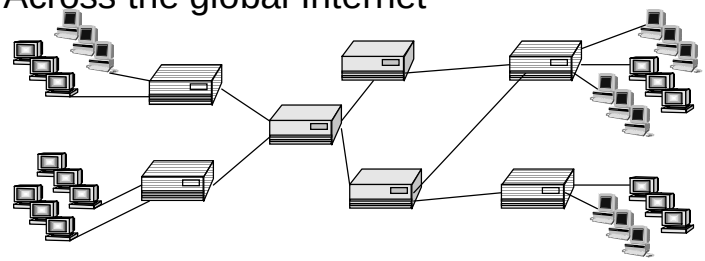
Why VPNs?

- Ominpresent coverage
- Cost reduction
  - no separate private networks
- Security
- E-Commerece
  - especially B2B



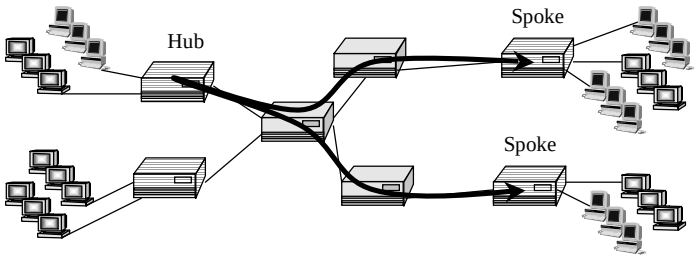
VPN

- Private network where privacy is introduced with some method of virtualization
- Between
  - two organizations, end-systems within single organization or multiple organizations or applications
- Across the global Internet



Intersite connectivity types

- Ranging from
  - full-mesh (n(n-1)/2 connections)
  - to hub and spoke type of connectivity
    - reliability problems!

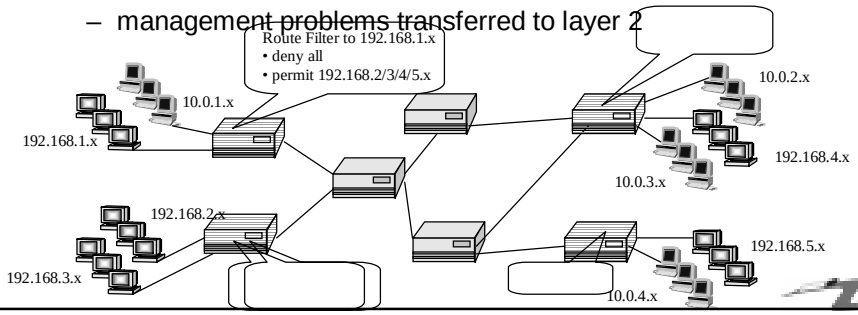


VPN technologies

- Data Integrity and Confidentiality
- Controlled route leaking
  - manually or with BGP communities (RFC 2858)
- Tunneling
  - GRE, IPinIP or MinIP
  - VPDNs
    - Tunneling PPP-traffic with L2TP or PPTP thru dial-up connections
- Layer 2 VPNs with dedicated ATM or FR connections
- VPNs with MPLS (and BGP in RFC 2547)

VPNs and routing

- Virtual private networks require special actions from standard IP routing
  - Controlled route leaking (route filtering), NAT
  - manual management, scalability problems, address space mgmnt
- VPNs can also be constructed on layer 2
  - restricted use of ATM or FR virtual connections
  - management problems transferred to layer 2



Addressing

- Private address space defined in RFC 1918 (BCP)
  - Addresses may be used freely within enterprise networks
    - 10.0.0.0-10.255.255.255 (10/8 prefix)
    - 172.16.0.0-172.31.255.255 (172.16/12 prefix)
    - 192.168.0.0-192.168.255.255 (192.168/16 prefix)
  - ISPs will reject packets with above addresses
    - Need for NAT or application layer gateways for Internet communications

Notes on route filtering

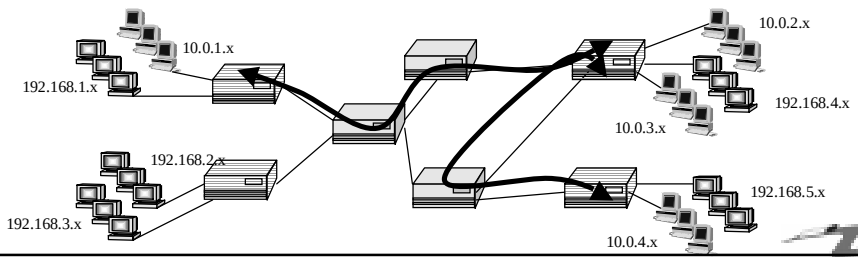
- Privacy through obscurity
  - Security means ISPs managing customer edges
    - or inserting address filters
- Requires common routing core
  - VPN addresses may not overlap within the routing core
- Route filtering is the most basic way of constructing VPNs
  - not recommendable

BGP issues

- RFC 2858 Multiprotocol extensions for BGP-4
  - Network Layer Reachability Identifier
- RFC 1997 BGP communities attribute
  - Mark the NLRI with a community attribute
  - routes within VPN can be marked with a single community instead of keeping up with individual routes

Tunneling

- Configure tunnels across the network
  - Customer edge routers will act as tunnel exit points
  - Allows for multiple use of VPN/IP addresses in different VPNs
- Manual configuration without use of routing protocols
  - Requires connectivity to all customer premises (VPN members)
    - n(n-1)/2 connections -> no management scalability



Notes on tunneling

- Allows for overlapping in VPN addresses
- Multiprotocol capable
- Manual configuration of tunnels
  - Low tolerance on network topology changes
- Concerns on QoS issues
- CE routers (tunnel exit points) have to managed by the ISP

VPN management issues

- Management of traditional VPNs is manual
  - Tunnels are setup manually
  - Routing information is manually configured
- Complexity of VPN management results from the integration of IP route lookup and forwarding decisions

MPLS for VPNs with BGP

- Meeting the objective for flexibility in new service introduction
  - MPLS separates the route lookup and forwarding somewhere in between layers 2 and 3.
    - MPLS basics covered in S-38.180
- Virtual Private Network
  - Tunnel via core network virtual backbones
  - Separate VPN address spaces
  - Advertising of VPN networks either by a routing protocol (RFC 2547 BGP/MPLS VPNs) or label distribution protocol

Requirements for MPLS/VPNs

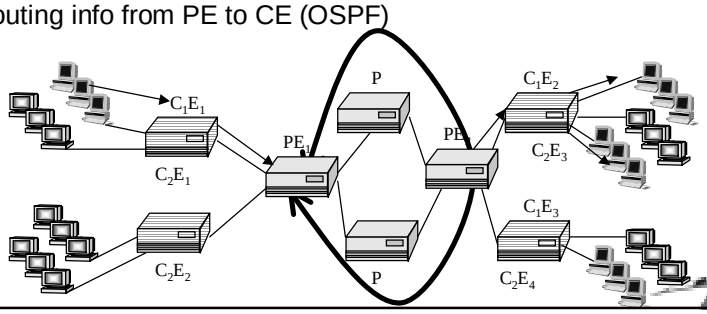
- Use of VPN/IP addresses
- Constrained distribution of routing information
  - BGP, LDP
- Multiple forwarding tables
  - Naturally for traffic inside the VPN
    - outside the VPN
  - At ISP edge VPN addresses may conflict
    - for traffic between VPNs
  - This is where MPLS kicks in!

Note on BGP mechanisms

- Globally non-unique addresses
  - dealt with VPN-IP addresses and Route Distinguisher
  - no constraint on connectivity
- Constrain the distribution of routing info
  - dealt with BGP (extended) community - field

Constrained distribution of routing information

1. Routing info from customer site (CE) to provider edge (OSPF)
2. Export routing info to provider BGP (CE->PE)
   - Attach BGP (extended) community attribute – constrained distribution of BGP info
3. Distribute with other VPN/PEs using BGP
4. Extract routing info on other PEs (opposite to 2.)
   - Route filtering based on BGP community attribute
5. Routing info from PE to CE (OSPF)

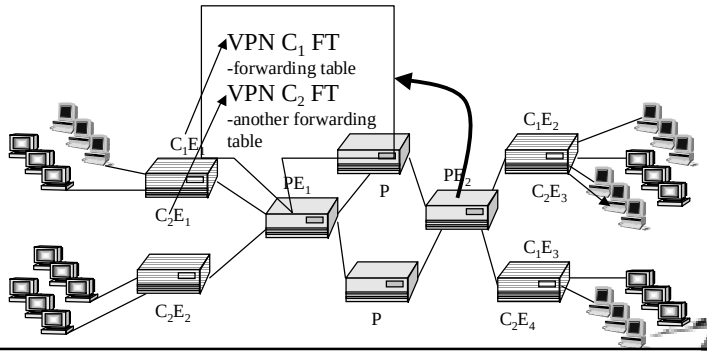


Constrained distribution of routing information - notes

- Distribution of BGP info is handled by the ISP
  - no involvement from the customer
- CE maintains routing peering with only the nearest PE
- To add a new site to an existing VPN only the connecting PE needs to be configured
- PE only maintains routes for the directly connected VPNs

Multiple Forwarding Tables

- To allow per-VPN segregation
  - otherwise packets could be traveling from one VPN to another OR alternatively careful management of address would be needed

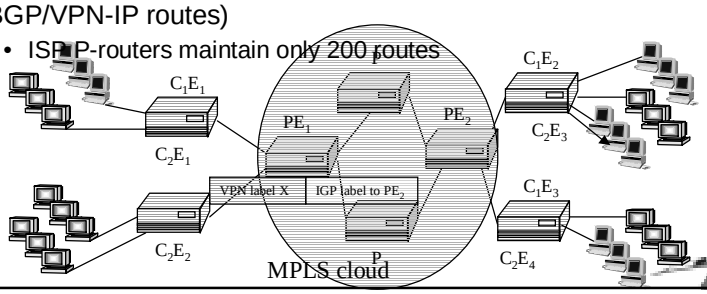


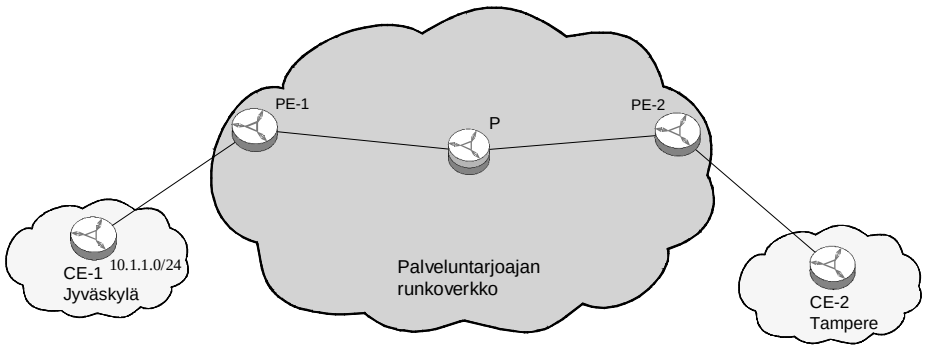
VPN-IP addresses

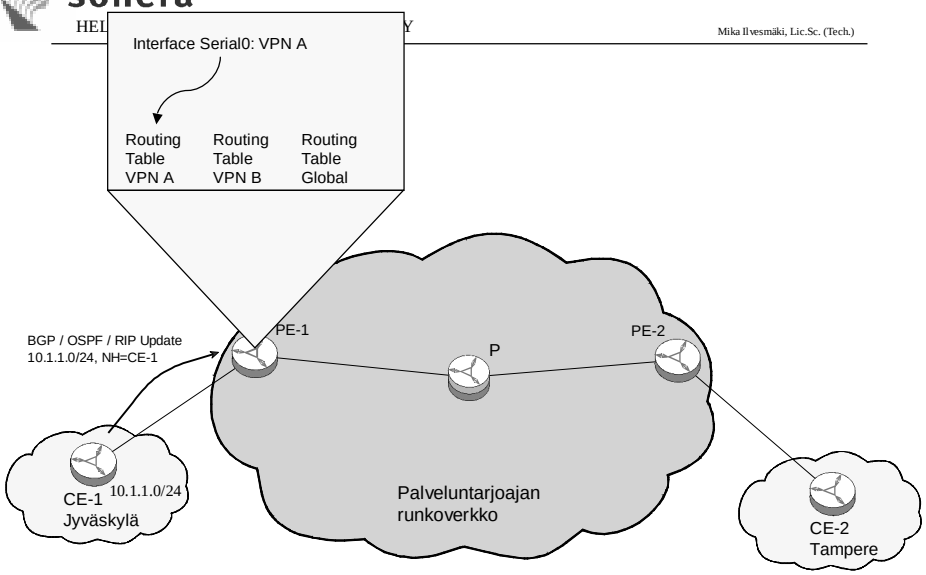
- BGP assumes that IP addresses are unique
  - not valid when using private address space (RFC 1918)
- IP address + Route Distinguisher
  - RD=Type+AS number+Assigned number
    - AS number = ISP AS number
    - Assigned number = VPN identifier given by ISP
- VPN-IP addresses are unique
- Use of VPN-IP addresses is done only in ISP network
  - no customer involvement, conversion done at PE
- VPN-IP addresses are carried only in routing protocol messages, not in IP headers
  - not used for packet forwarding

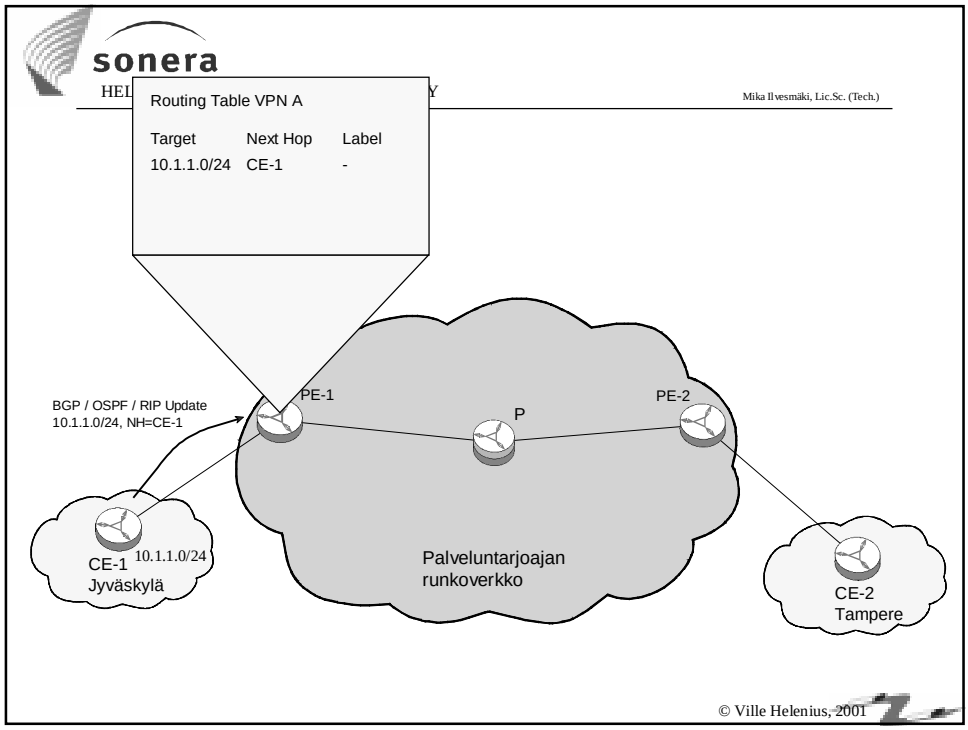
MPLS as a forwarding mechanism

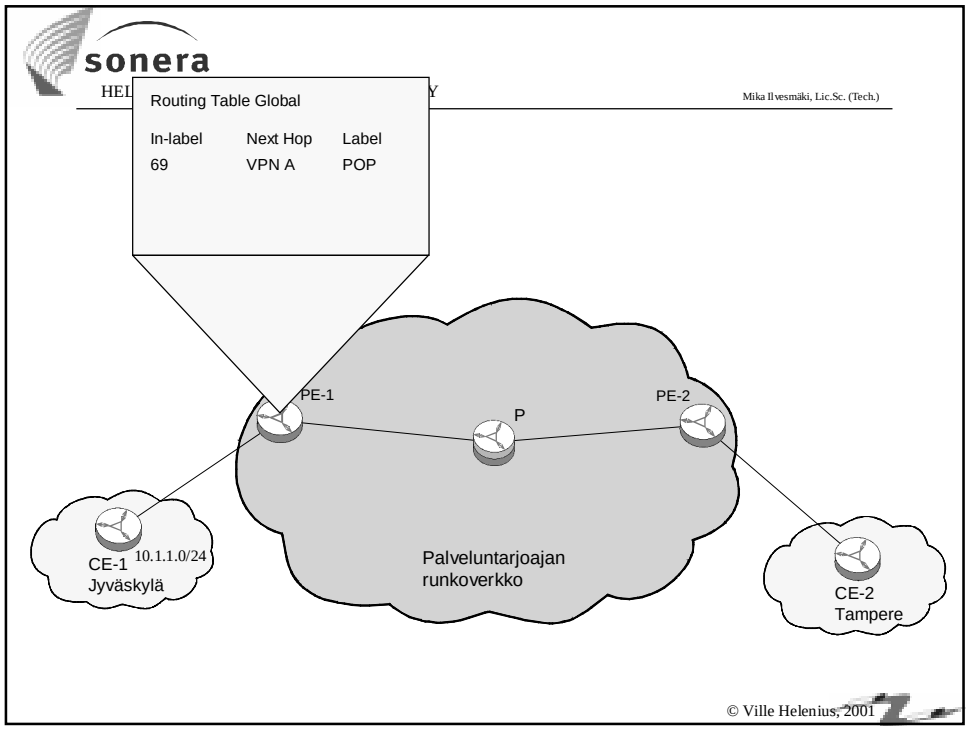
- Bind MPLS labels to VPN-IP addresses at PE
  - ISP with 200 routers (PE and P) with 10000 VPNs with 100 routes per VPN = 10000*100 routes in each P router
- Use two levels of labels (label stacks)
  - 1st level label is from PE to PE (labels distributed with LDP etc.)
  - 2nd level label is from egress PE forward (distributed with BGP/VPN-IP routes)
    - ISP P-routers maintain only 200 routes

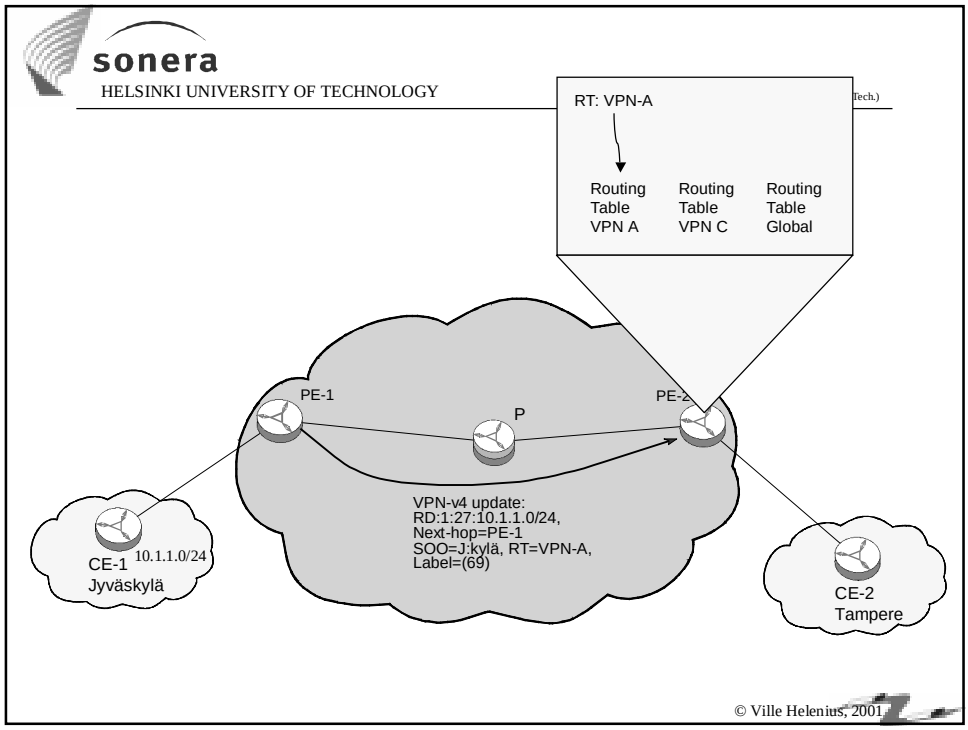


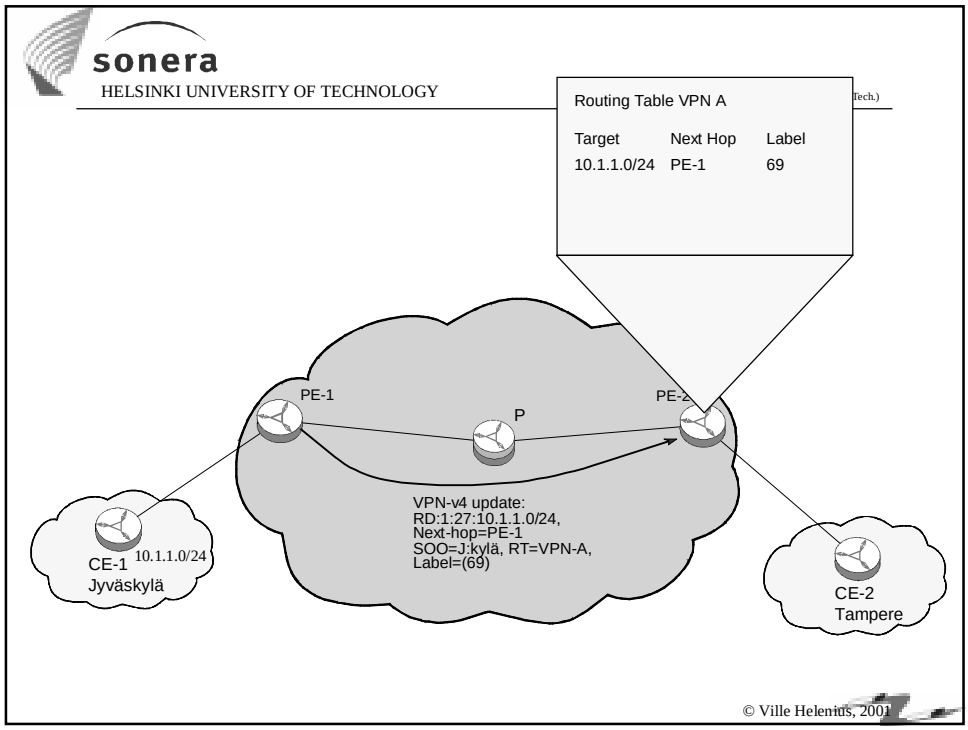


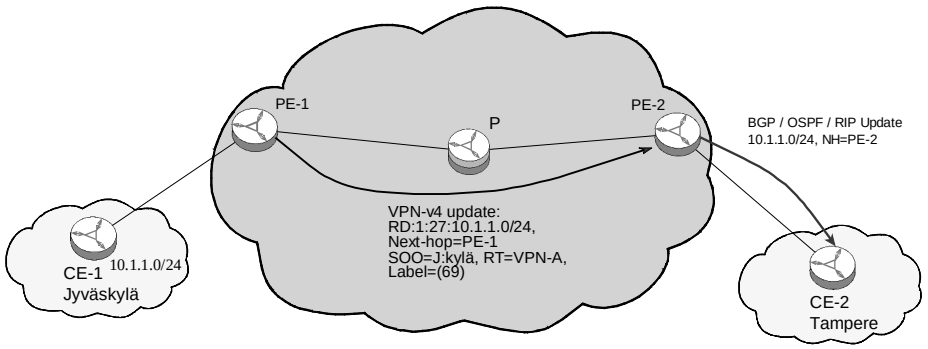


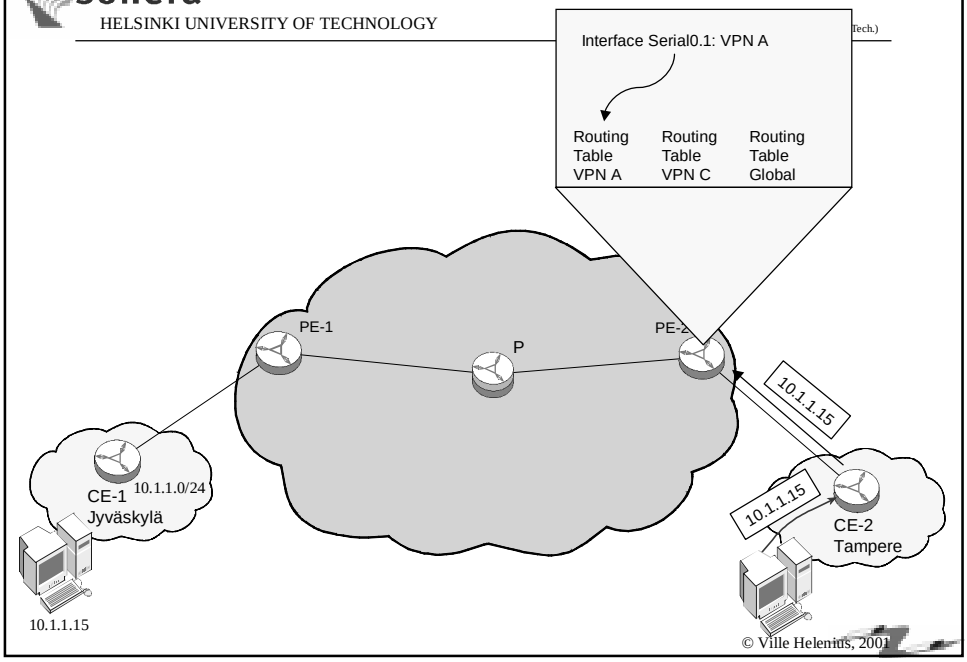

sonera
Mika Ilvesmäki, Lic.Sc. (Tech.)
Routing Table VPN A
Target Next Hop Label
10.1.1.0/24 CE-1 -
BGP / OSPF / RIP Update
10.1.1.0/24, NH=CE-1
PE-1
P
PE-2
CE-1
10.1.1.0/24
Jyväskylä
Palveluntarjoajan
runkoverkko
CE-2
Tampere
© Ville Helenius, 2001

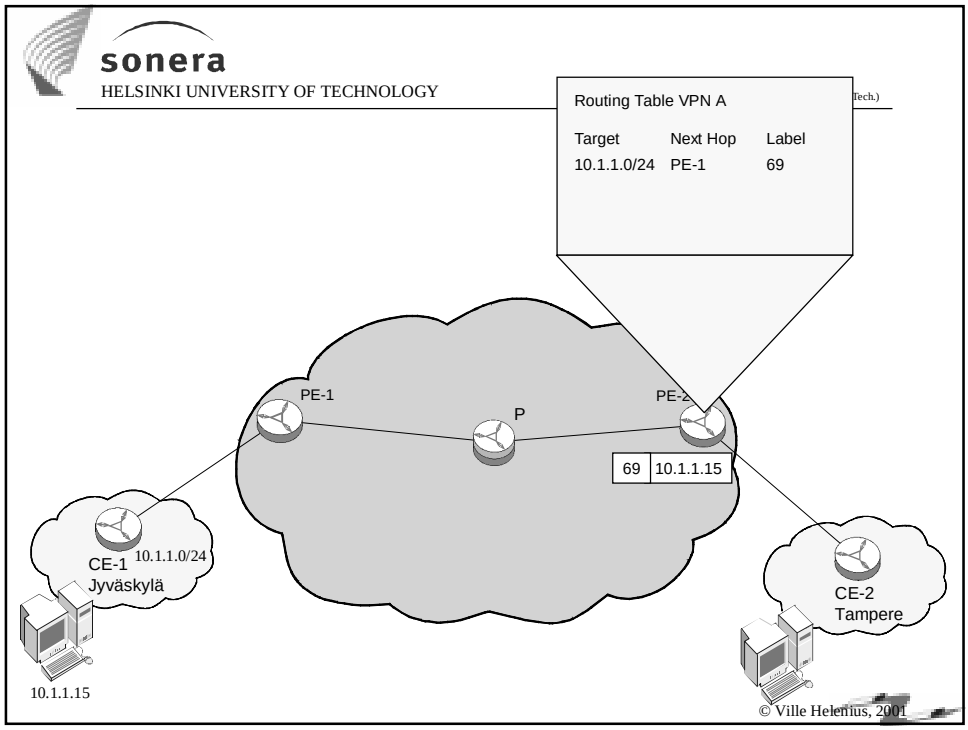

sonera
Mika Ilvesmäki, Lic.Sc. (Tech.)
Routing Table Global
In-label Next Hop Label
69 VPN A POP
PE-1
P
PE-2
CE-1
10.1.1.0/24
Jyväskylä
Palveluntarjoajan
runkoverkko
CE-2
Tampere
© Ville Helenius, 2001

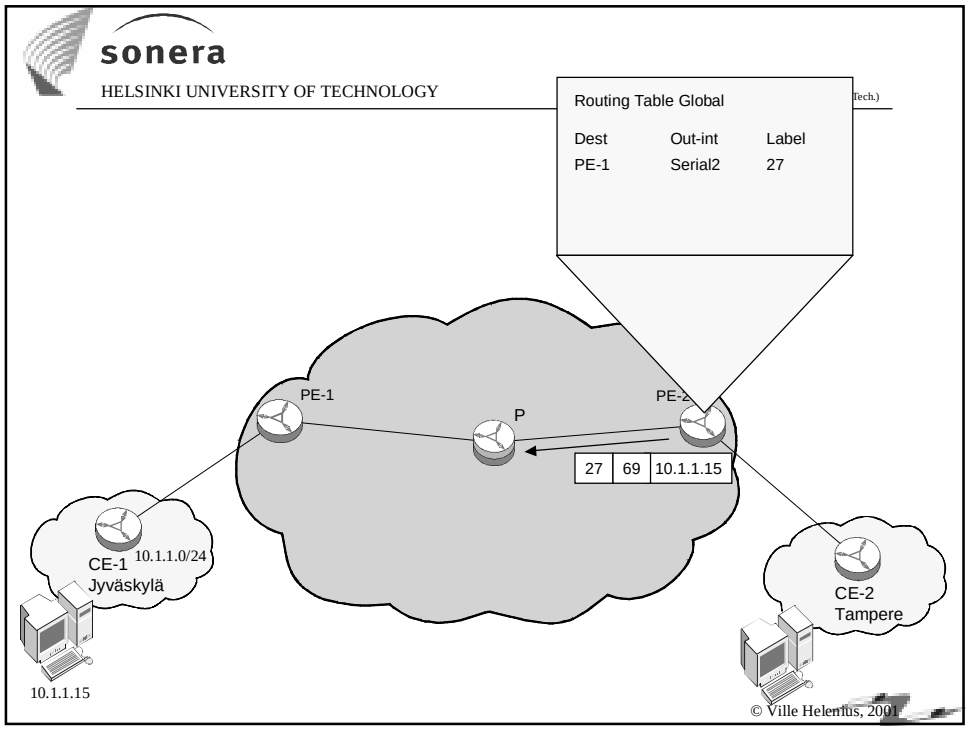

sonera
HELSINKI UNIVERSITY OF TECHNOLOGY
Tech.)
RT: VPN-A
Routing Table VPN A
Routing Table VPN C
Routing Table Global
PE-1
P
PE-2
VPN-v4 update:
RD:1:27:10.1.1.0/24,
Next-hop=PE-1
SOO=J:kylä, RT=VPN-A,
Label=(69)
CE-1
10.1.1.0/24
Jyväskylä
CE-2
Tampere
© Ville Helenius, 2001

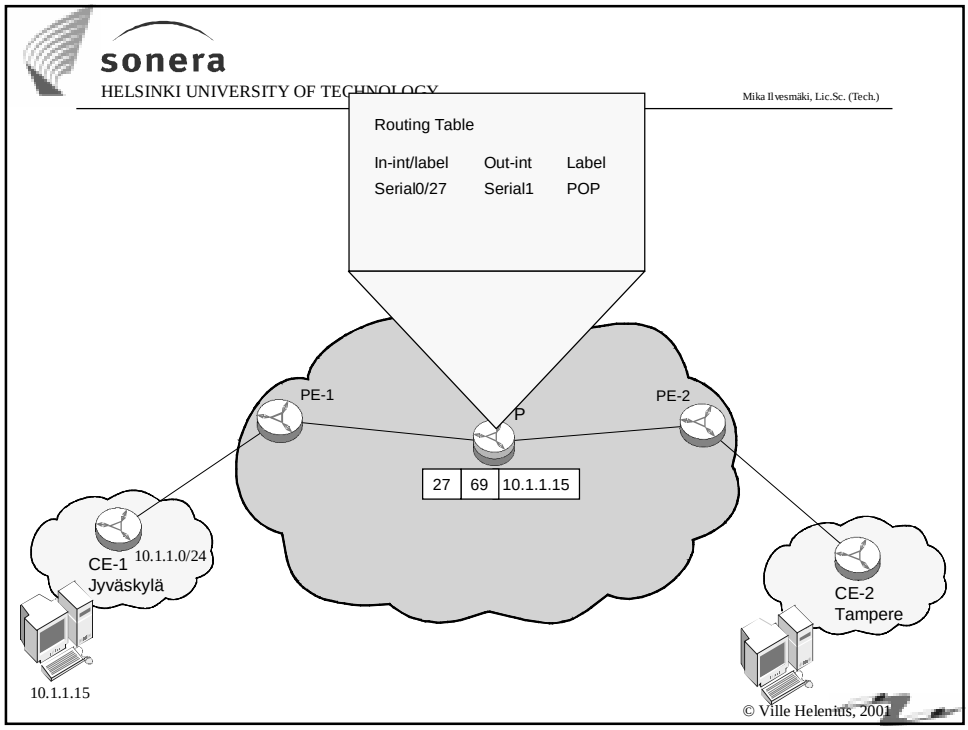

sonera
HELSINKI UNIVERSITY OF TECHNOLOGY
Tech.)
Routing Table VPN A
Target
Next Hop
Label
10.1.1.0/24
PE-1
69
PE-1
P
PE-2
VPN-v4 update:
RD:1:27:10.1.1.0/24,
Next-hop=PE-1
SOO=J:kylä, RT=VPN-A,
Label=(69)
CE-1
10.1.1.0/24
Jyväskylä
CE-2
Tampere
© Ville Helenius, 2001

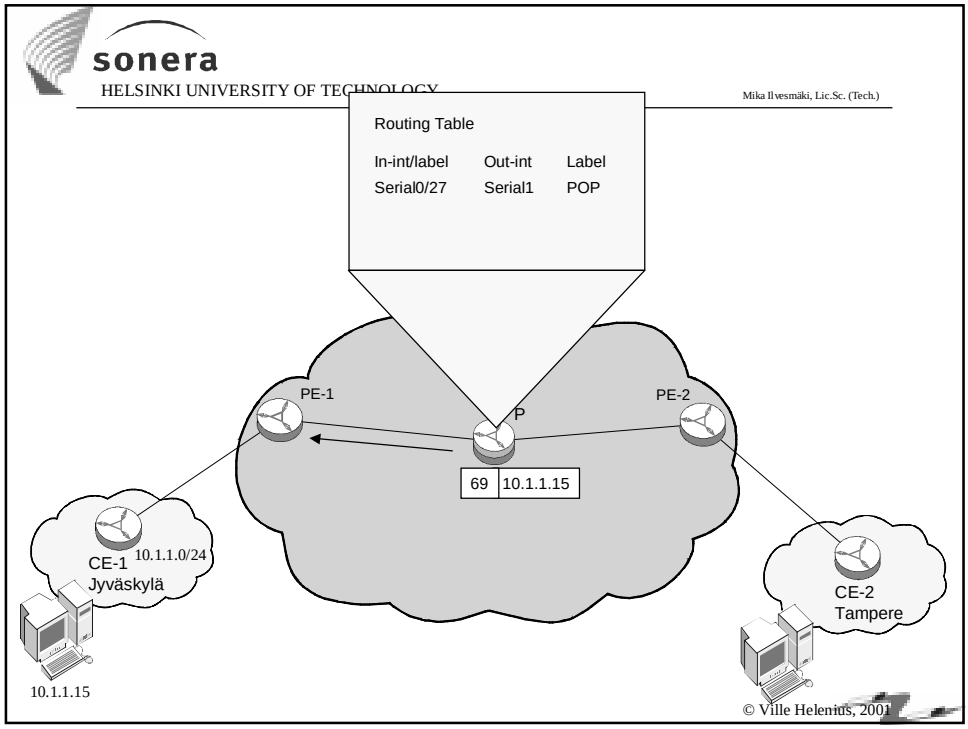


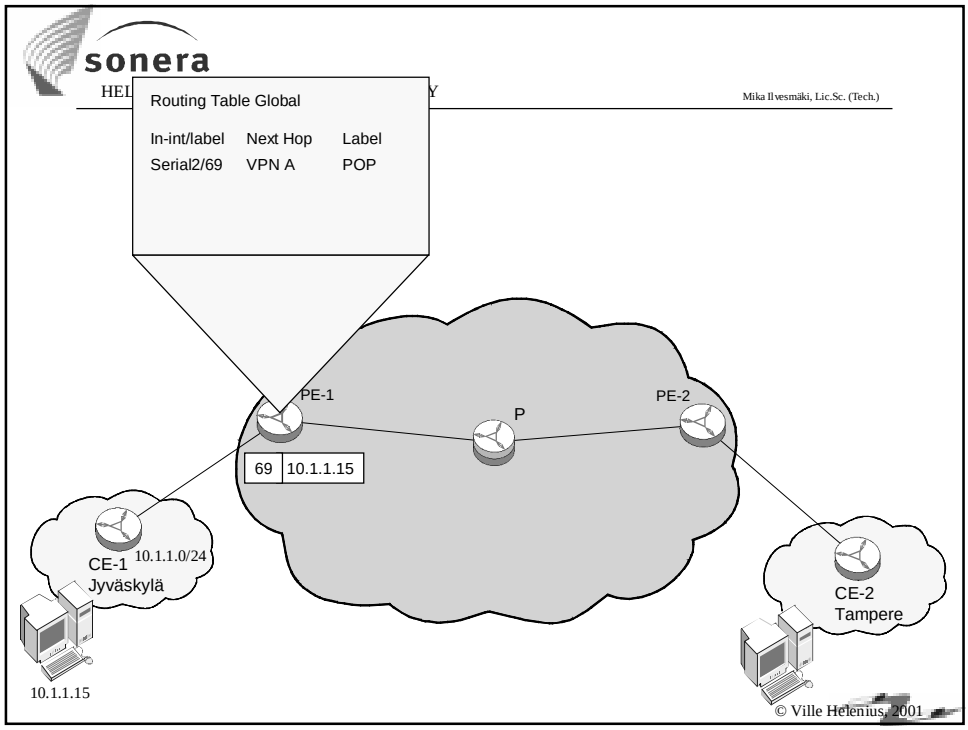


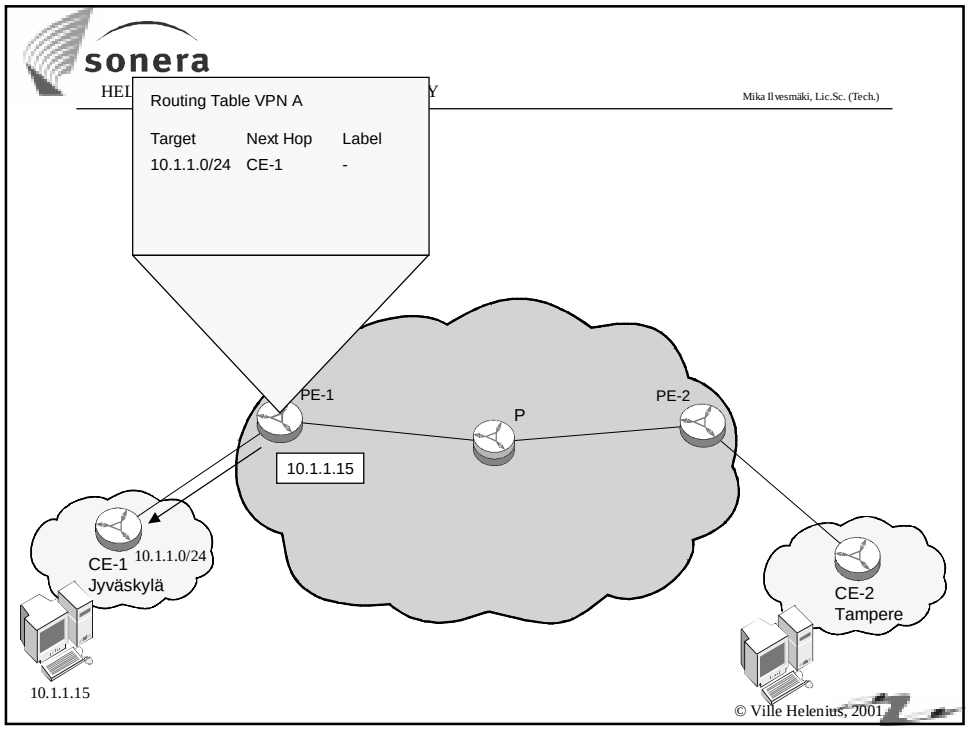

sonera
HELSINKI UNIVERSITY OF TECHNOLOGY
Routing Table VPN A
Target Next Hop Label
10.1.1.0/24 PE-1 69
PE-1
P
69 10.1.1.15
CE-1
Jyväskylä
10.1.1.0/24
10.1.1.15
CE-2
Tampere
© Ville Helenius, 2001

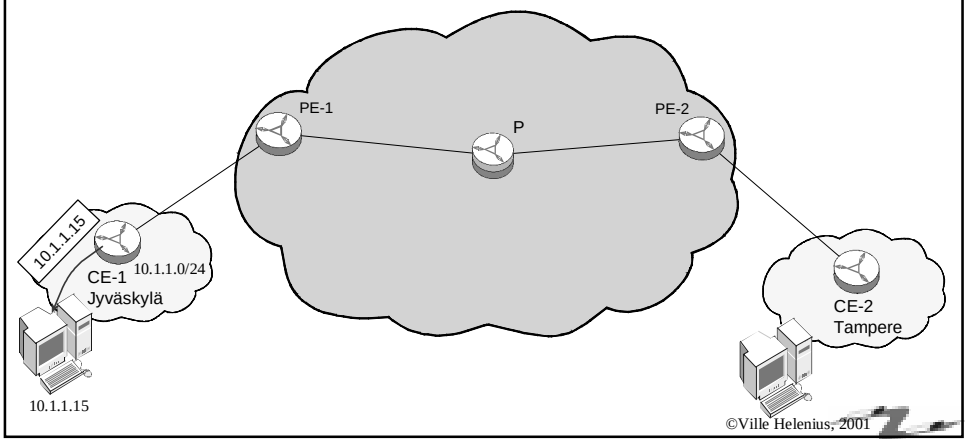

sonera
HELSINKI UNIVERSITY OF TECHNOLOGY
Routing Table Global
Dest Out-int Label
PE-1 Serial2 27
PE-1
P
27 69 10.1.1.15
CE-1
Jyväskylä
10.1.1.0/24
10.1.1.15
CE-2
Tampere
© Ville Helenius, 2001


sonera
HELSINKI UNIVERSITY OF TECHNOLOGY
Mika Ilvesmäki, Lic.Sc. (Tech.)
Routing Table
In-int/label Out-int Label
Serial0/27 Serial1 POP
PE-1
P
PE-2
27 69 10.1.1.15
CE-1
Jyväskylä
10.1.1.0/24
10.1.1.15
CE-2
Tampere
© Ville Heleniüs, 2001


sonera
HELSINKI UNIVERSITY OF TECHNOLOGY
Mika Ilvesmäki, Lic.Sc. (Tech.)
Routing Table
In-int/label Out-int Label
Serial0/27 Serial1 POP
PE-1
P
PE-2
69 10.1.1.15
CE-1
Jyväskylä
10.1.1.0/24
10.1.1.15
CE-2
Tampere
© Ville Heleniüs, 2001


sonera
Mika Ilvesmäki, Lic.Sc. (Tech.)
Routing Table Global
In-int/label Next Hop Label
Serial2/69 VPN A POP
PE-1
P
PE-2
69 10.1.1.15
CE-1
Jyväskylä
10.1.1.0/24
10.1.1.15
CE-2
Tampere
© Ville Helenius, 2001


sonera
Mika Ilvesmäki, Lic.Sc. (Tech.)
Routing Table VPN A
Target Next Hop Label
10.1.1.0/24 CE-1 -
PE-1
P
PE-2
10.1.1.15
CE-1
Jyväskylä
10.1.1.0/24
10.1.1.15
CE-2
Tampere
© Ville Helenius, 2001



IPsec, IP Security Architecture

- IETF IP Security Working Group
- Several commercial implementations
  - Authentication header (AH)
    - provides for access control, message integrity, authentication and anti-replay
  - Encapsulated Security Payload (ESP)
    - provides for AH services + confidentiality
  - Key Exchange Protocol
    - ISAKMP + Oakley/SKEME

IPSEC tunneling methods

- Encrypting of the IP Datagram (IPinIP)

IP gateway address	ESP	Original, but encrypted TCP/IP

•preventing traffic analysis

- Encryption of transport layer data

Original IP address	AH	ESP	Original, but encrypted TCP

•securing the contents of a connection

QoS in VPNs

- Manual link provisioning
  - dedicated connection oriented layer 2 links guarantee performance
  - Internet is not connection oriented layer 2
- CE or PE routers set the DSCP-byte
  - traffic classification?
- Alternative routes
- Quality of Service in the Internet dealt in S-38.180

VPNs with or without ISPs

- VPNs realized with ISP
  - Strategic partnership with ISP
    - ISP may manage the CE devices
  - Centralized management, outsourced VPN mgmnt
- VPNs realized on your own
  - Restricted knowledge on network outside the company
  - Need for VPN specialists
  - Flexibility

Final words

- VPNs are an existing solution
  - due to the need of Intranets
- VPNs may connect anything from two end devices to two networks
  - with tunnels, routing, MPLS
    - and naturally with leased lines
- Use of VPNs adds network management load
  - either in the company or within the ISP