MPLS Security Considerations

Monique J. Morrow, Cisco Systems

mmorrow@cisco.com

November 1 2004

Acknowledgments

- **Michael Behringer, Cisco Systems**

Why is MPLS Security Important?

- **Customer buys “Internet Service”:**

  Packets from SP are not trusted

  → Perception: Need for firewalls, etc.

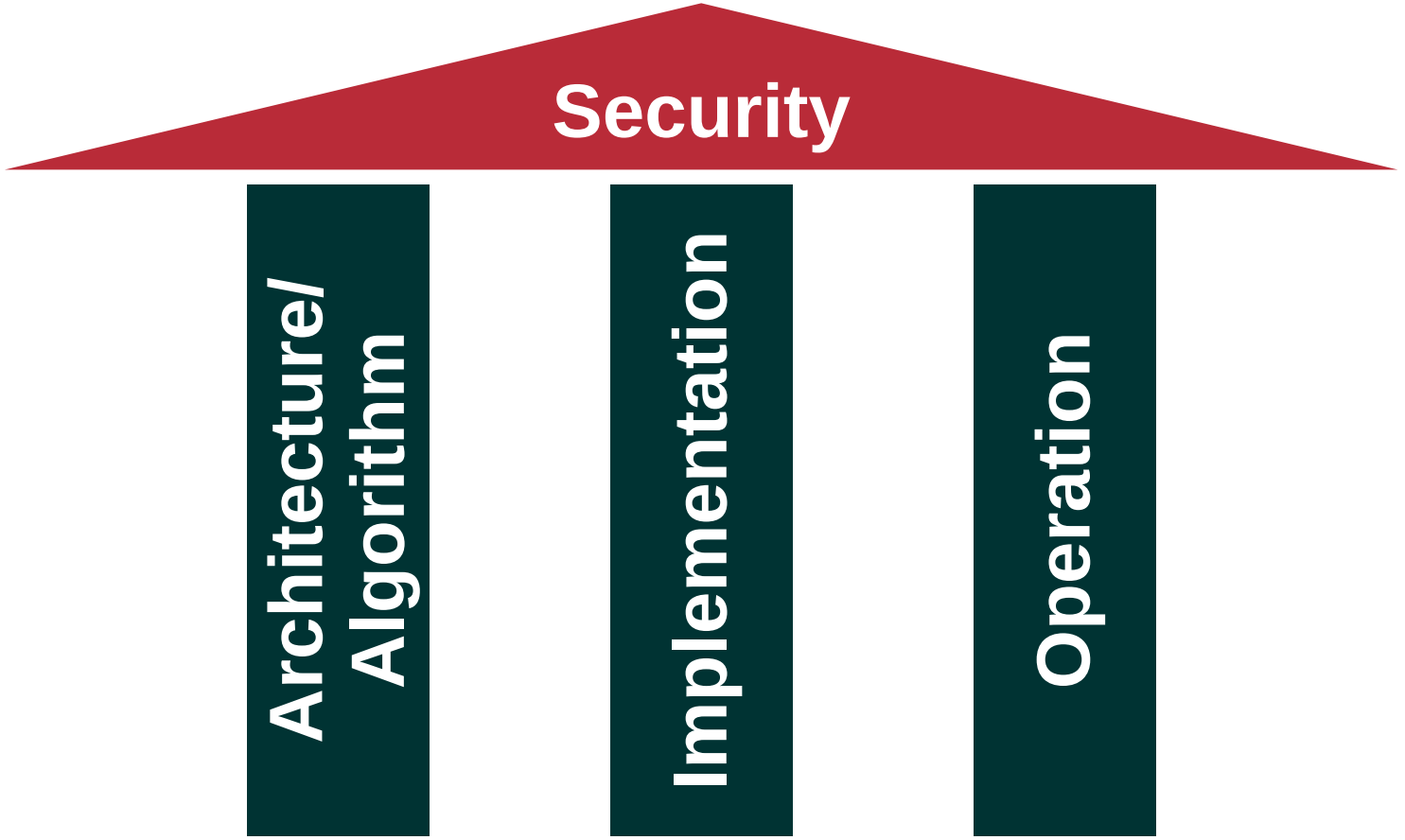
- **Customer buys a “VPN Service”:**

  Packets from SP are trusted

  → Perception: No further security required

SP Must Ensure Secure MPLS Operations

Security Relies on Three Pillars



Break One, and All Security Is Gone!

Basic 2547 Security: Today's Arguments

- Can be misconfigured (operation)
- Routers can have bugs (implementation)

True, but Same on ATM/FR

- PEs can be accessed from Internet, thus intrinsicly insecure

PEs Can Be Secured, as Internet Routers

- Floods over Internet can impact VPN traffic

Engineering/QoS

Correct Security Analysis

- **Security has to be analyzed on three levels:**
  - **Architecture/algorithm**
  - **Implementation**
  - **Operation**
- **Applied to MPLS/VPN:**

1. **The MPLS Architecture is secure (can be operated securely)**
2. **Implementation/operation issues may exist, like in any other technology**

Protecting an MPLS/VPN Core—Overview

1. **Don't let packets into (!) the core**

   No way to attack core, except through routing, thus:

2. **Secure the routing protocol**

   Neighbor authentication, maximum routes, dampening, …

3. **Design for transit traffic**

   QoS to give VPN priority over Internet

   Choose correct router for bandwidth

   Separate PEs where necessary

4. **Operate Securely**

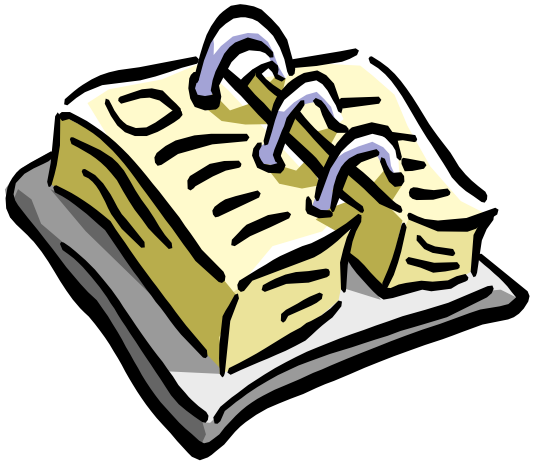
Still "Open": Routing Protocol

Only Attack Vector: Transit Traffic

Now Only Insider Attacks Possible

Avoid Insider Attacks

Agenda



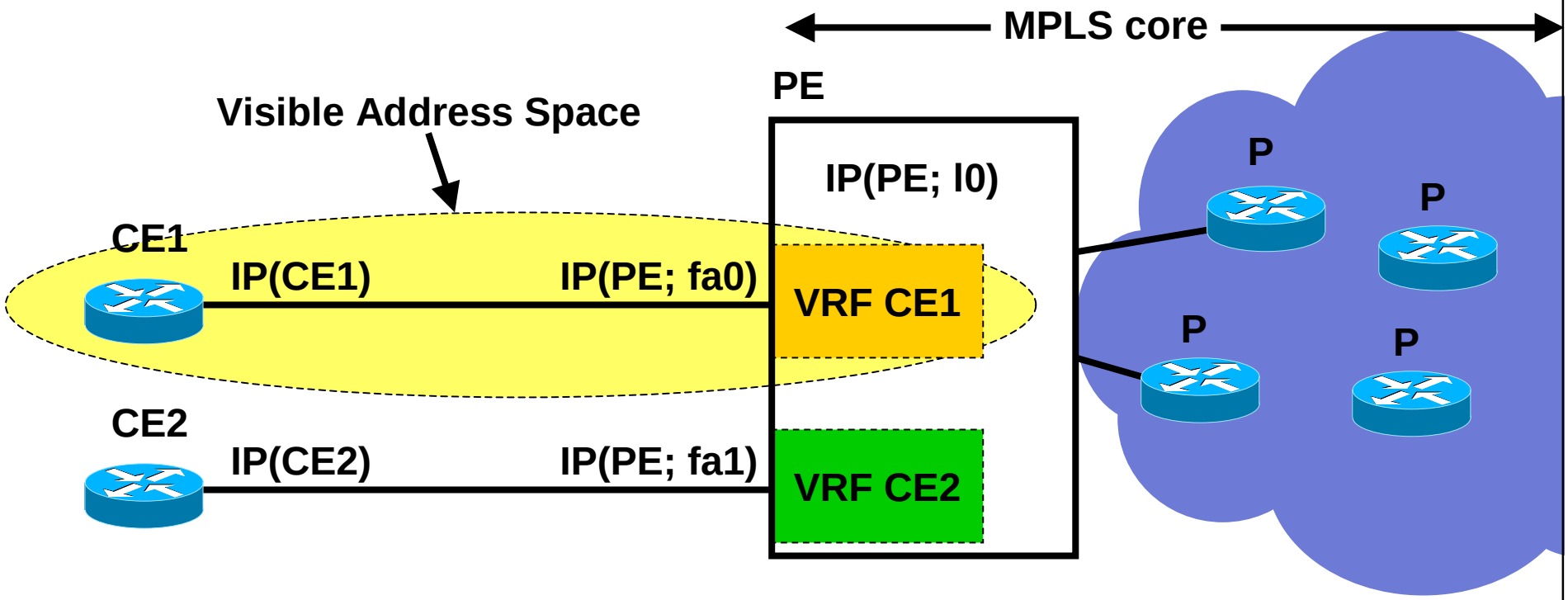
- **Analysis of MPLS/VPN Security**
- **Security Recommendations**
- **Secure MPLS VPN Design**
  - **Internet Access**
- **Secure Operations**
- **Attacking an MPLS Network**
- **IPsec and MPLS**
- **Summary**

General VPN Security Requirements

- **Address Space and Routing Separation**
- **Hiding of the MPLS Core Structure**
- **Resistance to Attacks**
- **Impossibility of VPN Spoofing**

Working assumption: The core (PE+P) is secure

Hiding of the MPLS Core Structure



- VRF contains MPLS IPv4 addresses
- Only peering Interface (on PE) exposed (-> CE)!
  -> ACL or unnumbered

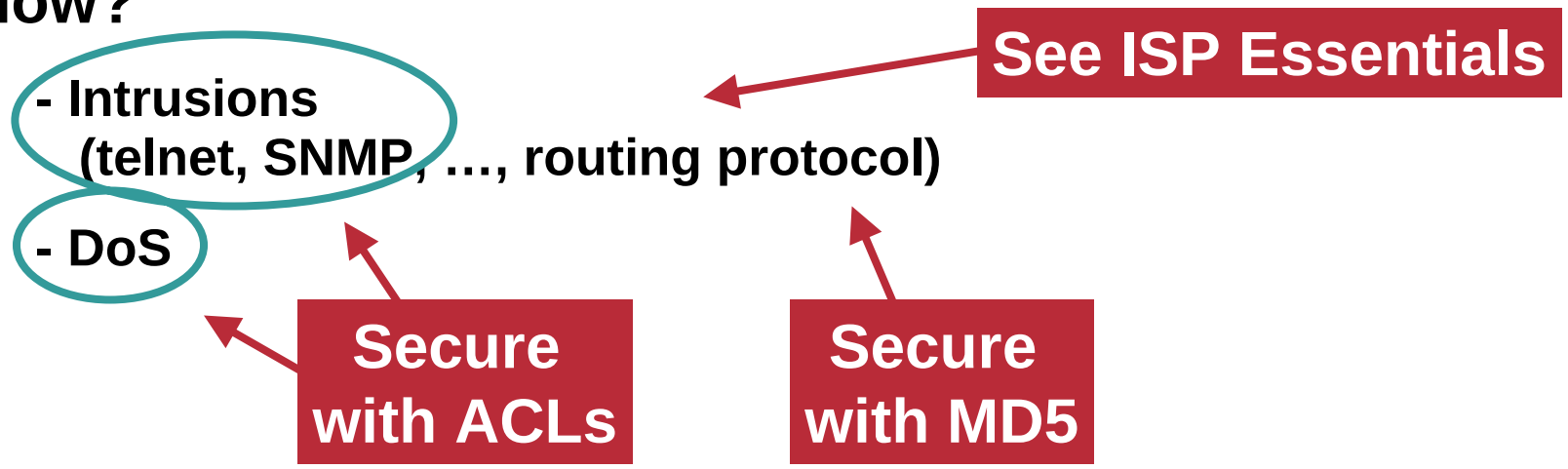
Resistance to Attacks: Where and How?

- **Where can you attack?**

  Address and Routing Separation, thus:

  Only Attack point: peering PE

- **How?**



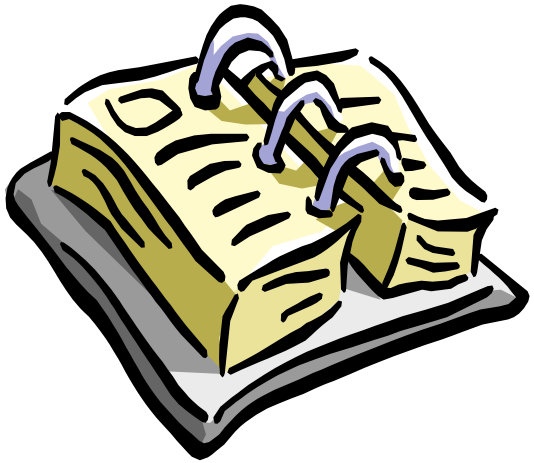
Label Spoofing

- PE router expects IP packet from CE
- Labelled packets will be dropped
- Thus no spoofing possible

Comparison with ATM / FR

	ATM/FR	MPLS
Address space separation	yes	yes
Routing separation	yes	yes
Resistance to attacks	yes	yes
Resistance to Label Spoofing	yes	yes
Direct CE-CE Authentication (layer 3)	yes	with IPsec

Agenda



- Analysis of MPLS/VPN Security
- **Security Recommendations**
- Secure MPLS VPN Design
  - Internet Access
- Secure Operations
- Attacking an MPLS Network
- IPsec and MPLS
- Summary

Security Recommendations for ISPs

- Secure devices (PE, P): They are trusted!
- Core (PE+P): Secure with ACLs on all interfaces

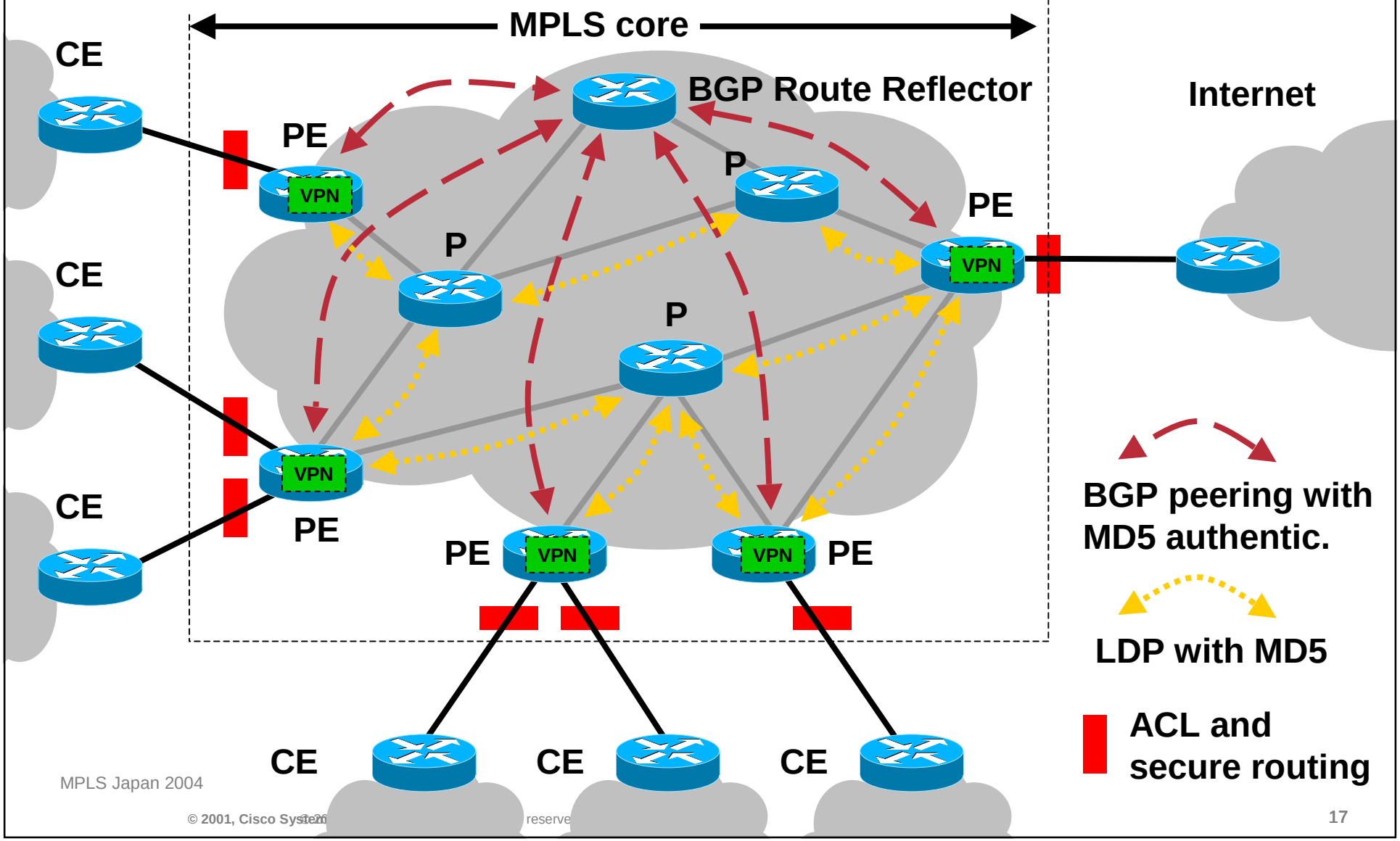
  Ideal: deny ip any <core-networks>
- Static PE-CE routing where possible
- If routing: Use authentication (MD5)
- Separation of CE-PE links where possible (Internet / VPN)
- LDP authentication (MD5)
- VRF: Define maximum number of routes
- Note: Overall security depends on weakest link!

PE-CE Routing Security

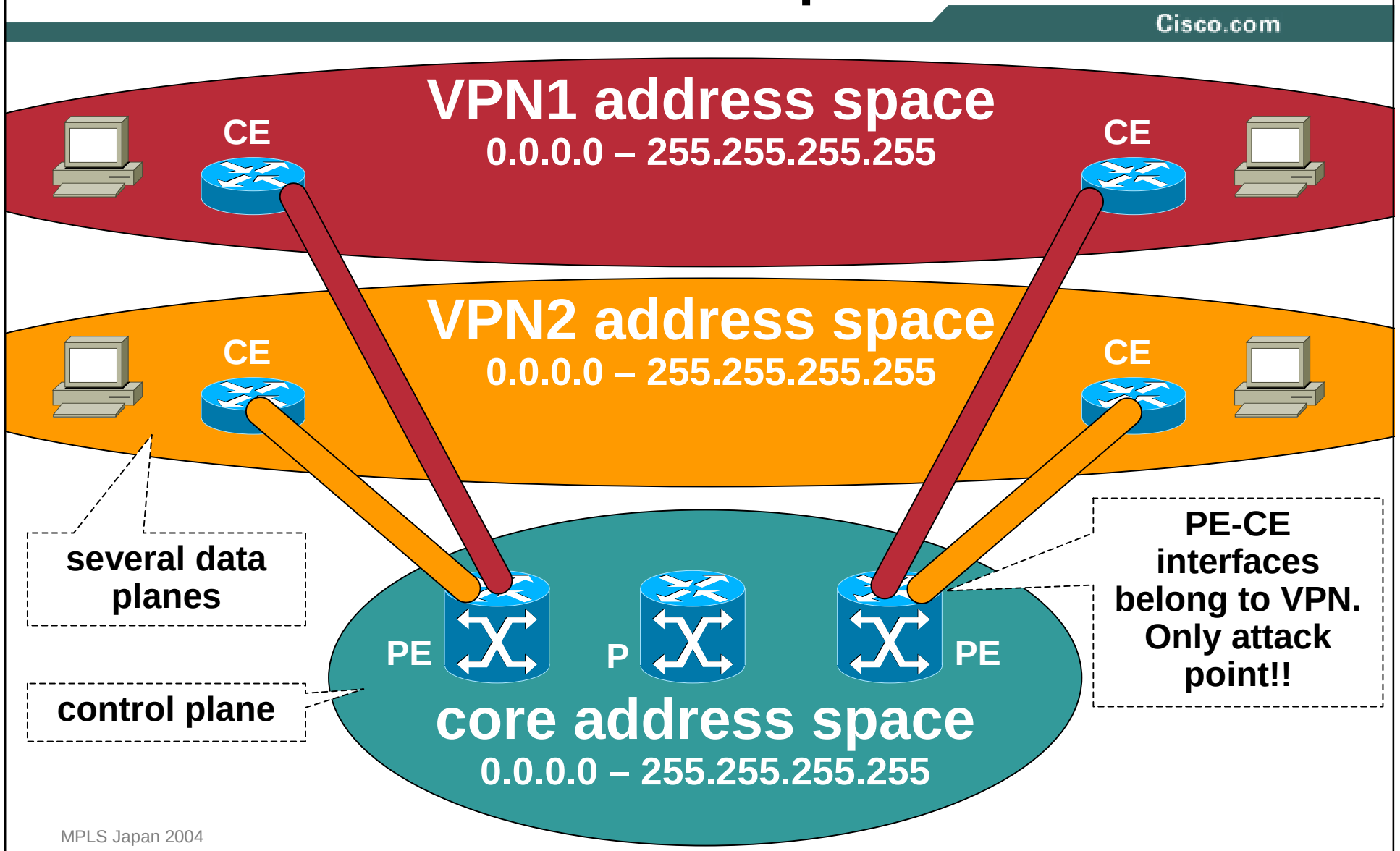
In order of security preference:

1. **Static: If no dynamic routing required (no security implications)**
2. **BGP: For redundancy and dynamic updates (many security features)**
3. **IGPs: If BGP not supported (limited security features)**

Securing the MPLS Core



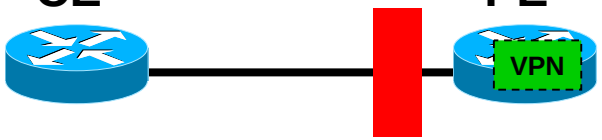
Address Planes: True Separation!



Securing the Core: Infrastructure ACLs

Easy with MPLS!

Cisco.com



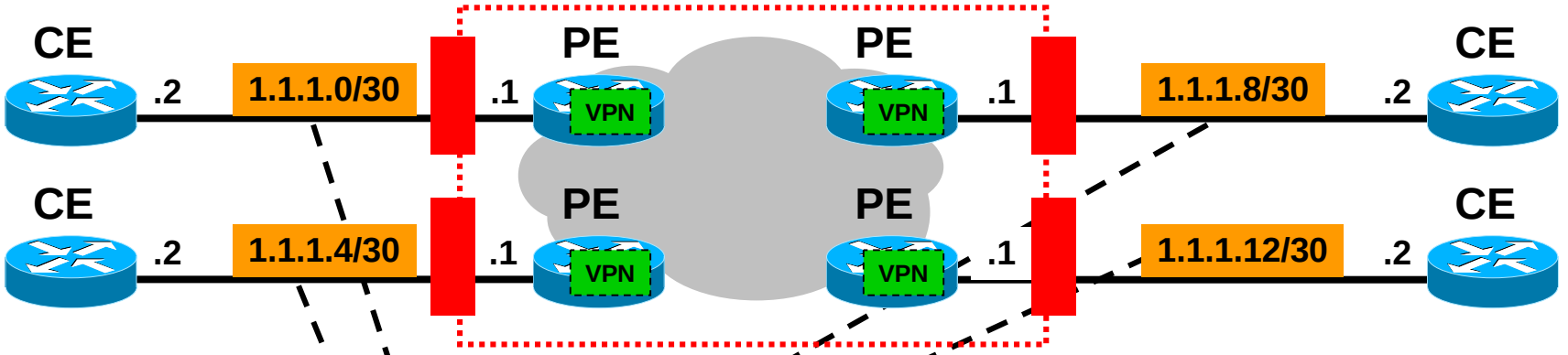
In MPLS: VRF belongs to customer VPN!

- **On PE: “deny ip any <PE VRF address space>”**

  Exception: Routing protocol from host to host

- **Idea: No traffic to PE/P → you can’t attack**
- **Prevents intrusions 100%**
- **DoS: Very hard, but traffic over router theoretically enables DoS.**

Securing the Core: Infrastructure ACLs



- **Example:**

  deny ip any 1.1.1.0 0.0.0.255

  permit ip any any

This is VPN address space, not core!

- **Caution: This also blocks packets to the CE's!**

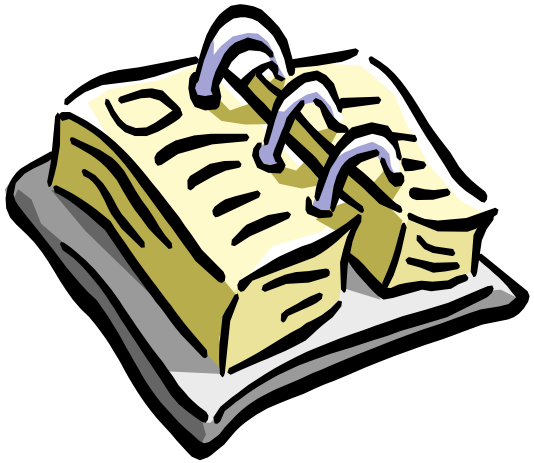
  Alternatives: List all PE i/f in ACL, or use secondary i/f on CE

Best Practice Security Overview

- Secure devices (PE, P): They are trusted
- PEs: Secure with ACLs on all interfaces
- Static PE-CE routing where possible
- If routing: Use authentication (MD5)
- Maximum number of routes per peer (only BGP)
- Separation of CE-PE links where possible (Internet/VPN)
- LDP authentication (MD5)
- VRF: Define maximum number of routes

Note: Overall security depends on weakest link

Agenda



- Analysis of MPLS/VPN Security
- Security Recommendations
- Secure MPLS VPN Design
  - Internet Access
- Secure Operations
- Attacking an MPLS Network
- IPsec and MPLS
- Summary

MPLS Internet Architectures: Principles

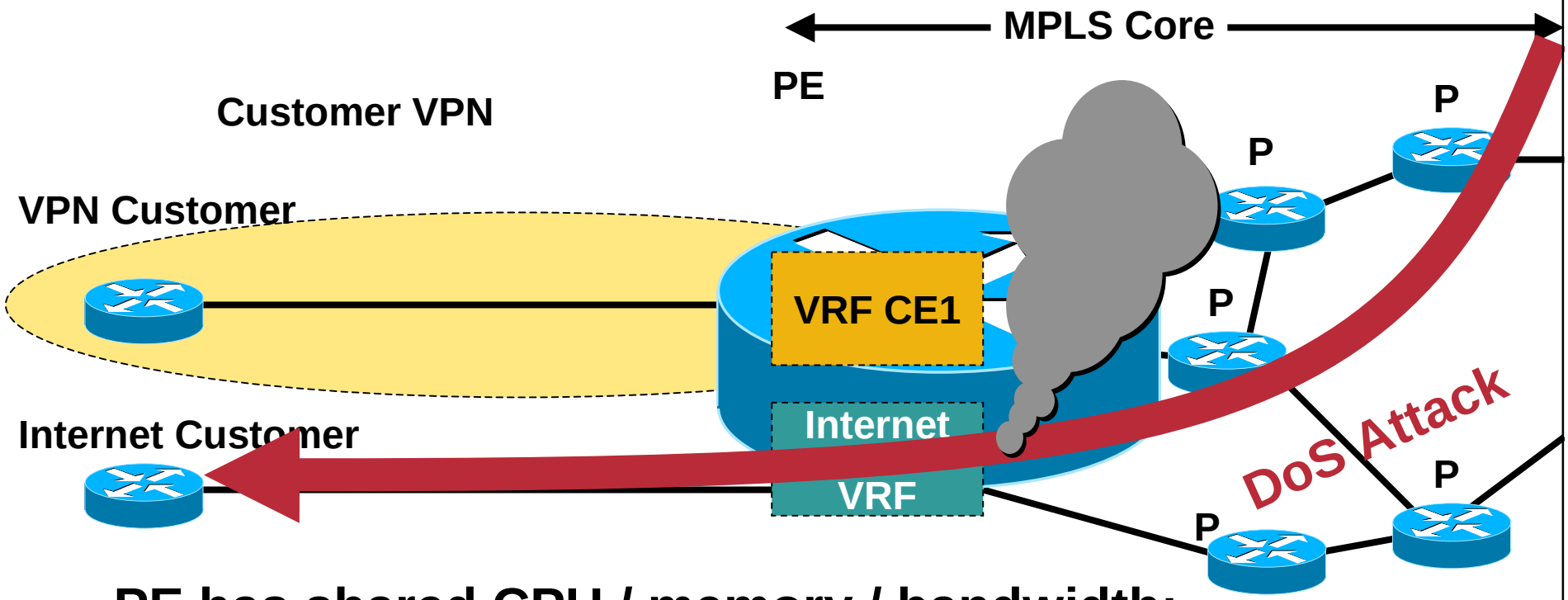
- **Core supports VPNs *and* Internet**
- **VPNs remain separated**
- **Internet as an option for a VPN**
- **Essential: Firewalling**

MPLS VPNs Are Quite Secure

- **Perfect separation of VPNs**
  - **No intrusions possible**
- **Perfect separation of the core from VPNs**
  - **Again, no intrusions possible**

BUT THERE IS ONE REMAINING ISSUE…

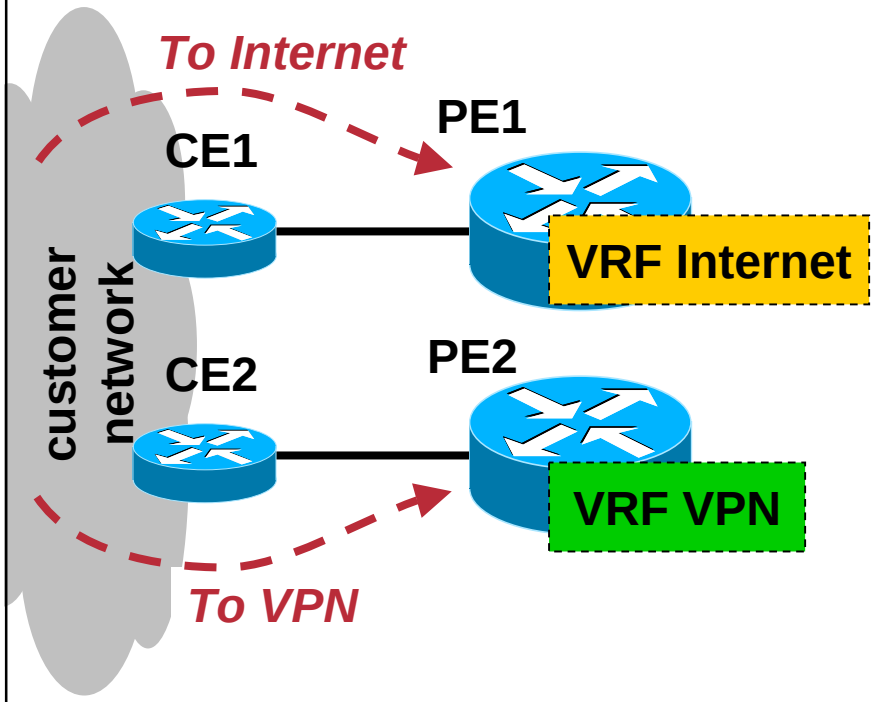
The Key Issue: DoS through a Shared PE Might Affect VPN Customer



- **PE has shared CPU / memory / bandwidth:**

  →Traffic could affect VPN customer
  (However, risk probably acceptable)

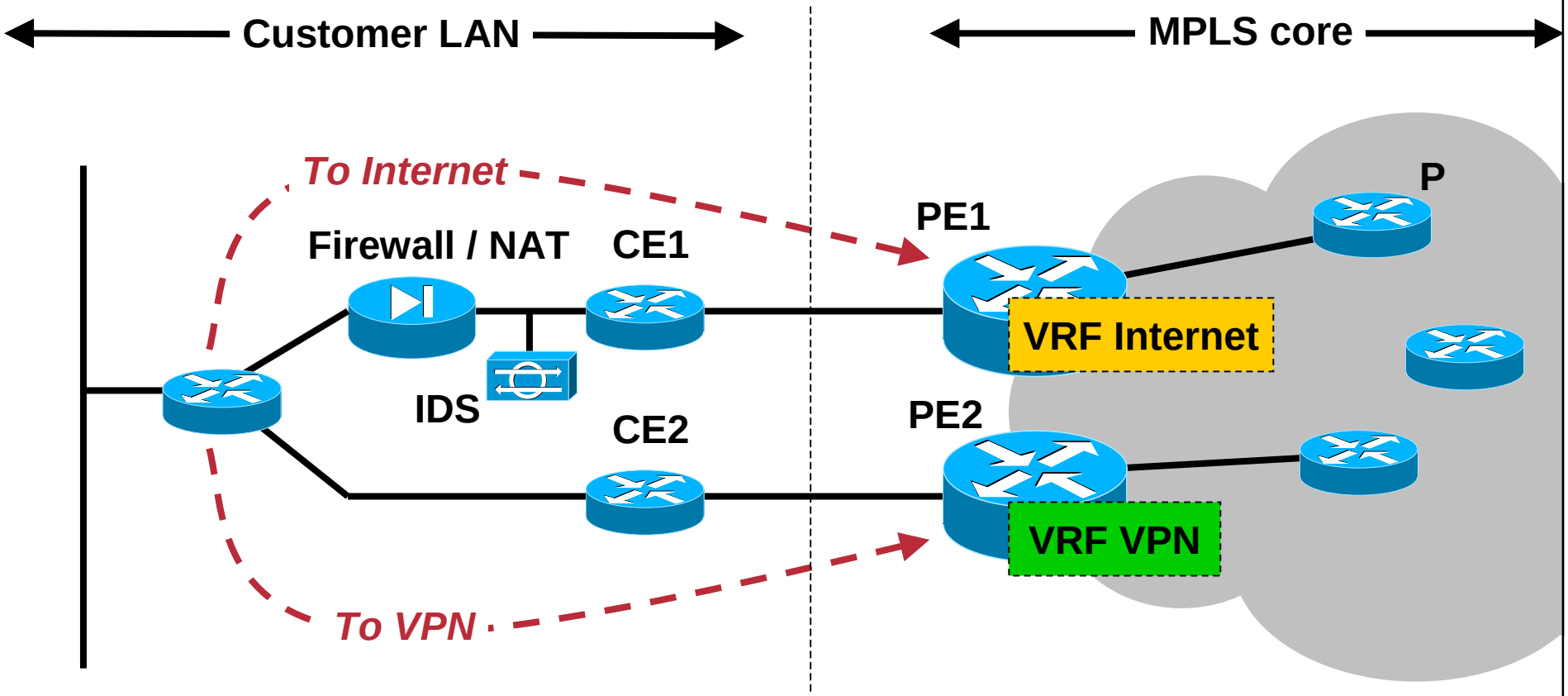
Today's Best Practice:
MPLS VPN Security Recommendation:



- **PE routers should contain only VRFs of the same security level. Example:**
  - **Level 0: Internet**
  - **Level 1: VPN customers**
  - **(Level 2: Mission critical infrastructure)**

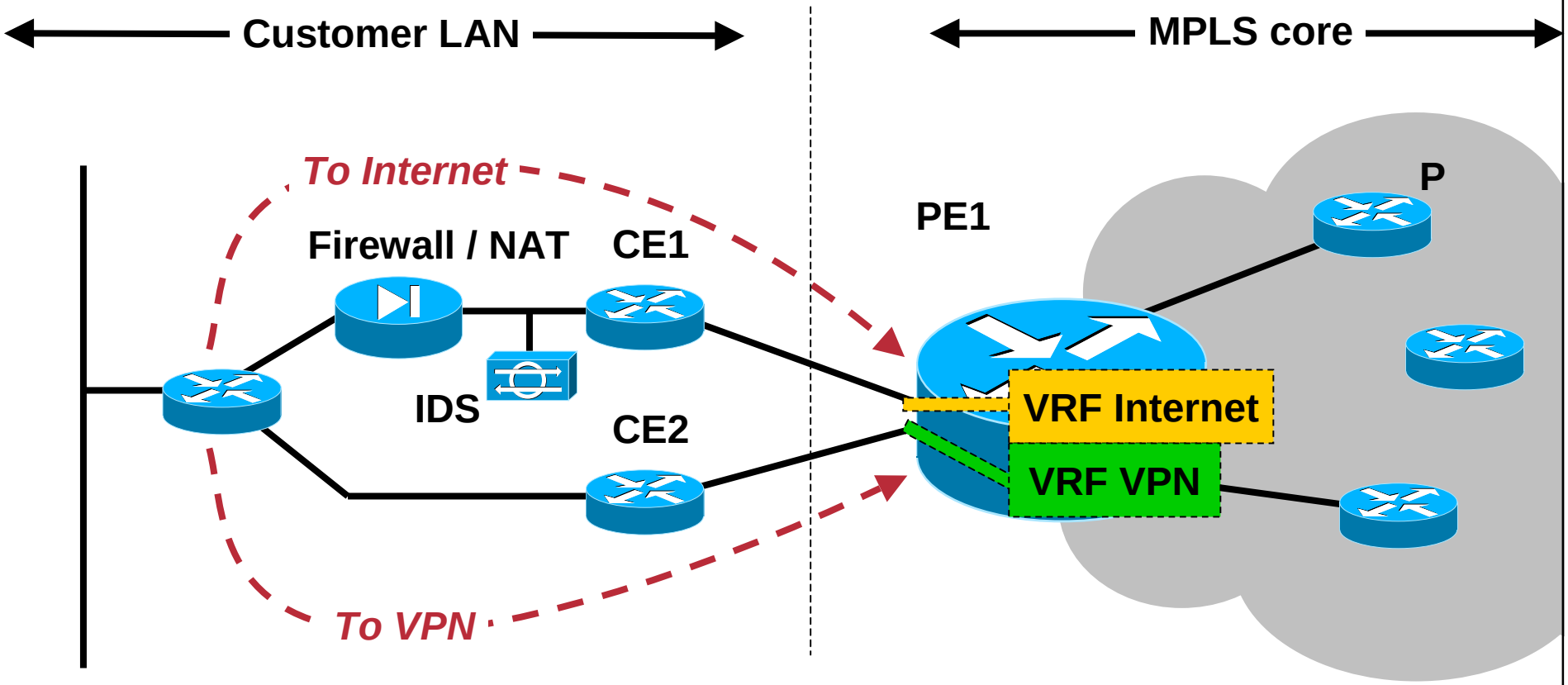
Note: This is negotiable: Shared Internet/VPN PE may be acceptable if price and conditions are right.

Separate VPN and Internet Access



- **Separation:** +++
- **DoS resistance:** +++
- **Cost:** $$$ **(Two lines and two PEs: Expensive!)**

Separate Access Lines + CEs, one PE



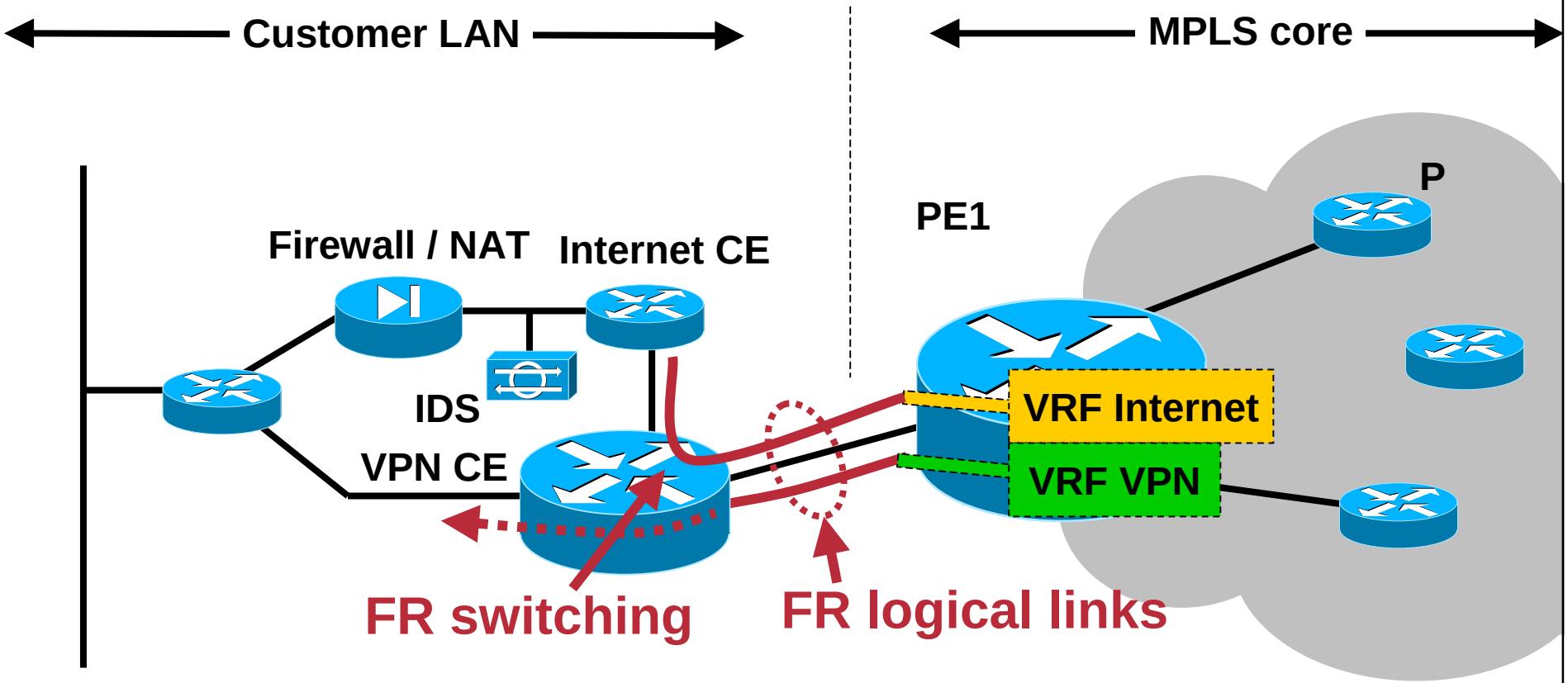
- **Separation: +++**
- **DoS resistance: ++** (DoS might impact VPN on PE)
- **Cost: $$** (Two lines, but only one PE)

Using a Single Access Line

Requirements to share a line:

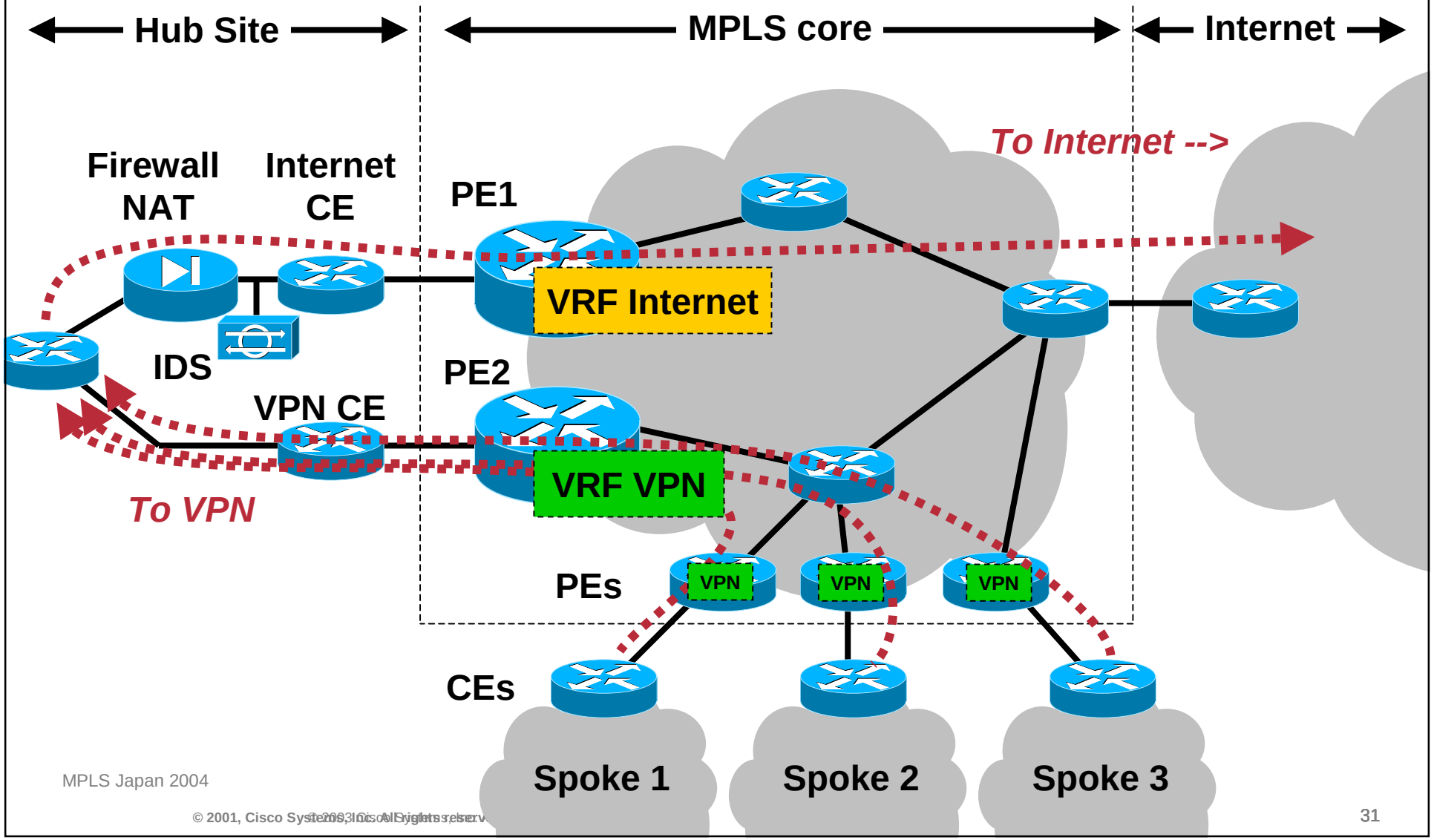
- **PE requires separate sub-interfaces**
- **CE requires separate sub-interfaces**
- **CE side requires separate routing**

Shared Access Line, Frame Relay



- **Separation: +++**
- **DoS resistance: +** **(DoS might affect VPN on PE, line, CE)**
- **Cost: $**

Hub-and-Spoke VPN with Internet Access

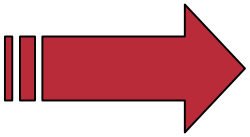


Alternative Topologies

- **Full VPN mesh, one Internet Access**
- **Internet access at several sites**
  - **-> Several firewalls needed**
  - **-> More complex**
- **Internet Access from all sites**
  - **-> Complex, one firewall per site**

From RFC2547bis: Data Plane Protection

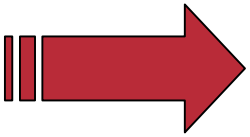
1. a backbone router does not accept labeled packets over a particular data link, unless it is known that that data link attaches only to trusted systems, or unless it is known that such packets will leave the backbone before the IP header or any labels lower in the stack will be inspected, and …



- **Inter-AS should *only* be provisioned over secure, private peerings**
- **Specifically NOT: Internet Exchange Points (anyone could send labelled packets!! No filtering possible!!)**

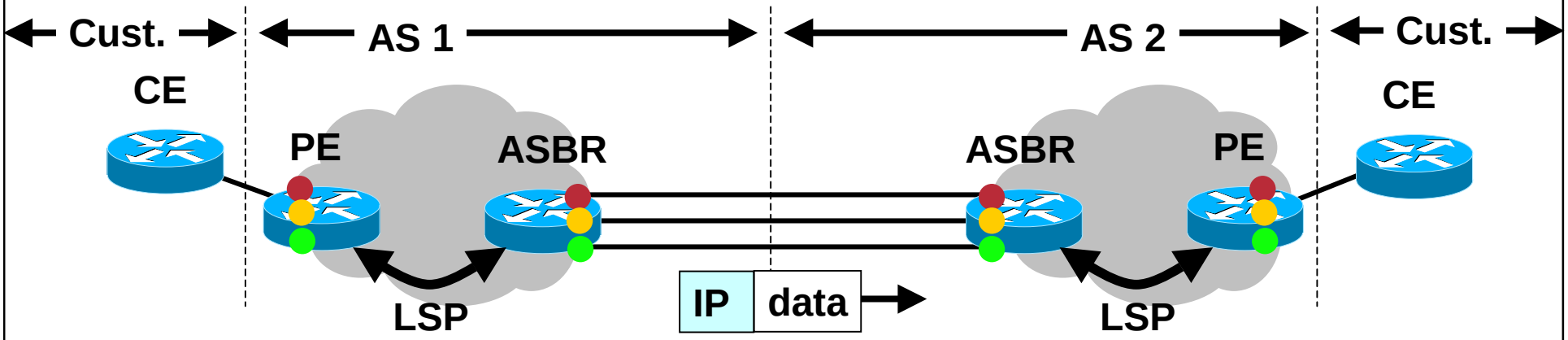
From RFC2547bis: Control Plane Protection

2. labeled VPN-IPv4 routes are not accepted from untrusted or unreliable routing peers,



- **Accept routes with labels only from trusted peers**
- **Plus usual BGP filtering (see ISP Essentials*)**

Inter-AS: Case 10.a)
VRF-VRF back-to-back



- Control plane: No signalling, no labels
- Data plane: IPv4 only, no labels accepted
- Security: as in 2547
- Customer must trust both SPs

Security of Inter-AS 10.a)

- **Static mapping**

  SP1 does not “see” SP2’s network

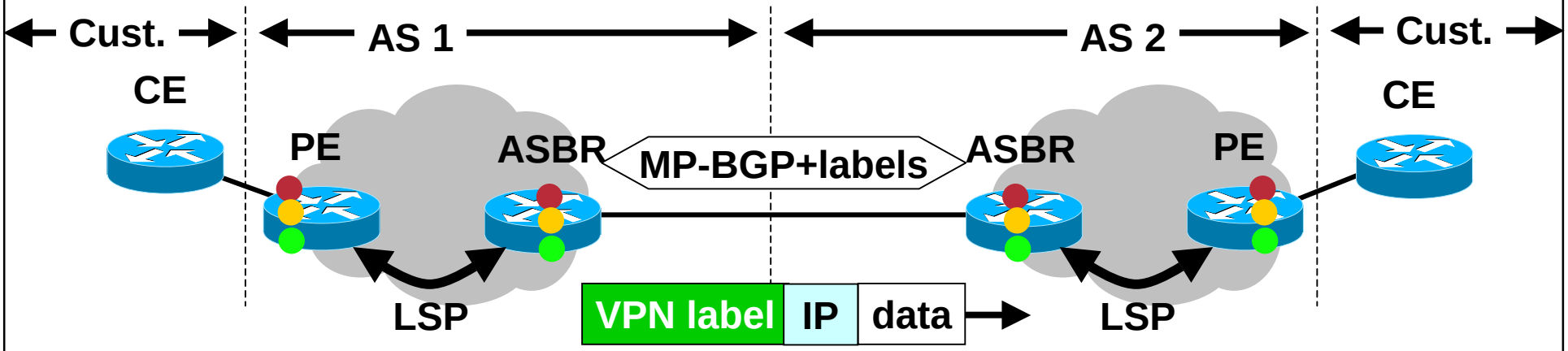
  And does not run routing with SP2, except within the VPNs.

  → Quite secure

- **Potential issues:**

  SP 1 can connect VPN connection wrongly (like in ATM/FR)

Inter-AS: Case 10.b)
ASBR exchange labelled VPNv4 routes



- Control plane: MP-BGP, labels
- Data plane: Packets with one label
- AS1 can insert traffic into any shared VPN of AS2
- Customer must trust both SPs

Security of Inter-AS 10.b)

- **ASBR1 does signalling with ASBR2**

  MP-BGP: has to be secured, dampening etc

  Otherwise no visibility of the other AS
  (ASBR1 – ASBR2 is the only interface between the SPs.)

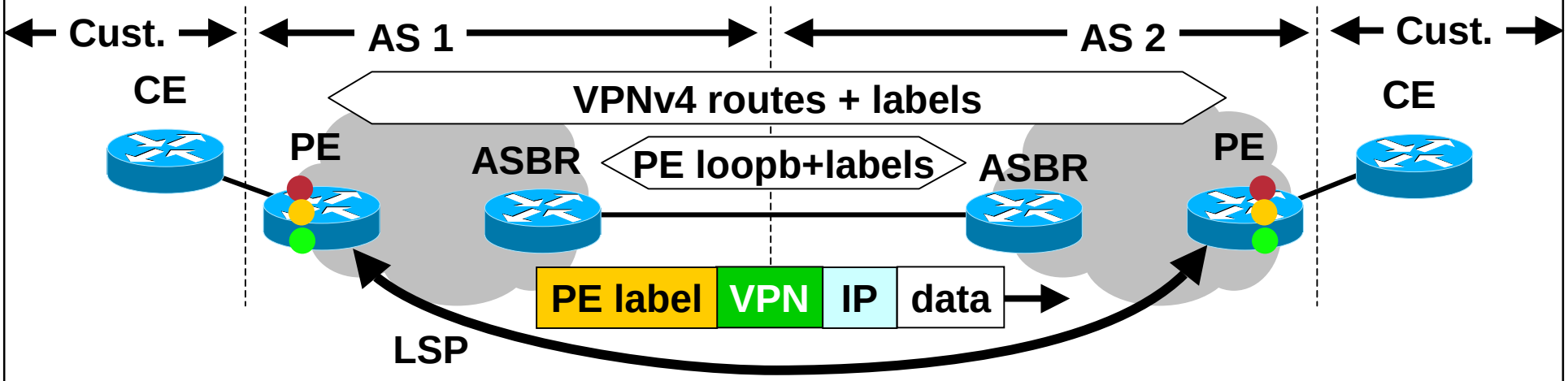
- **Potential Issues:**

  SP1 can bring wrong CEs into any shared VPN

  SP1 can send packets into any shared VPN (not into VPNs that are not shared, since label is checked);

  → SP can make any shared VPN insecure

Inter-AS: Case 10.c)
ASBRs exchange PE loopbacks



- Control plane: ASBR: just PE loopback + labels; PE/RR: VPNv4 routes + labels
- Data plane: PE label + VPN label
- AS1 can insert traffic into VPNs in AS2
- Customer must trust both SPs

Security of Inter-AS 10.c)

- **ASBR-ASBR signalling (BGP)**
  RR-RR signalling (MP-BGP)
  - **Much more “open” than 10.a) and 10.b)**
  - **LSPs between PEs, BGP between RR, ASBR**
- **Potential Issues:**
  - **SP1 can bring a CE into any VPN on “shared” PEs**
  - **SP1 can intrude into any VPN on “shared” PEs**
- **Very open architecture**
  - **probably only applicable for ASes controlled by the same SP.**

Inter-AS Summary and Recommendation

- **Three different models for Inter-AS**
  - **Different security properties**
  - **Most secure: Static VRF connections (10.a), but least scalable**
- **Basically the SPs have to trust each other**
  - **Hard / impossible to secure against other SP in this model**
- **Okay if all ASes in control of one SP**
- **Current Recommendation: Use 10.a)**

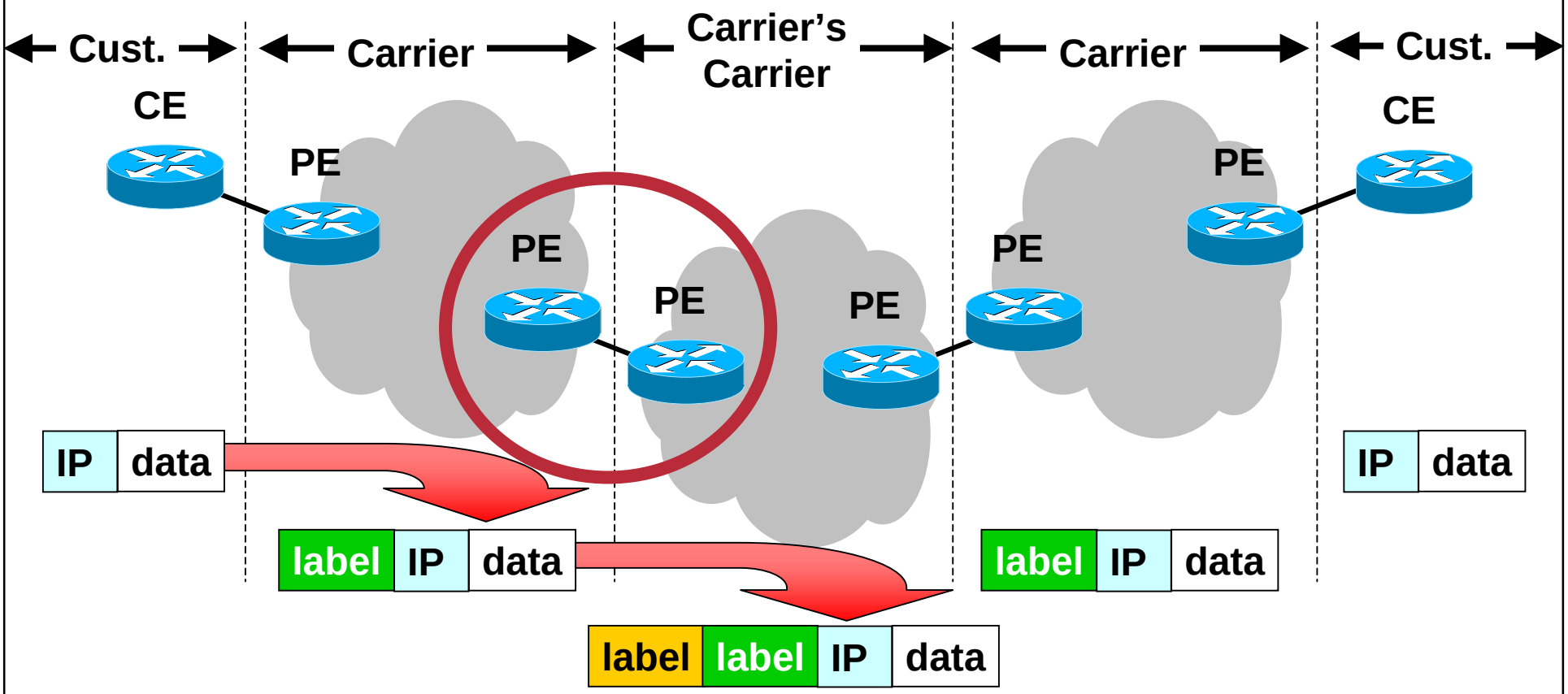
Inter-AS Recommendation

- **Start with 10.a) (static VPN connections)**

  Not many Inter-AS customers yet anyway → Easy start

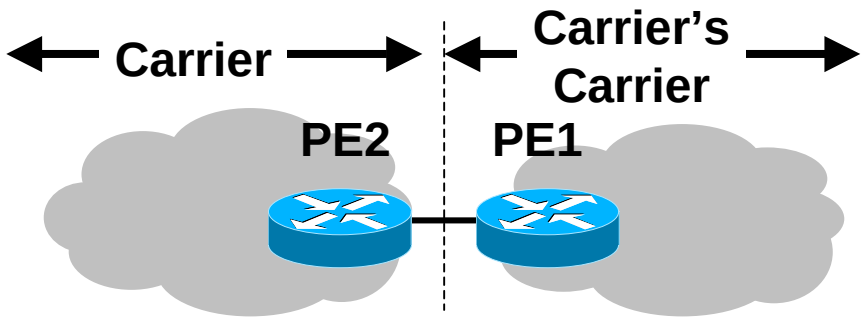
- **Maybe at some point (when many Inter-AS customers), move to 10.b) (ease of provisioning)**
- **10.c) felt by most SPs as too open. Current recommendation: Only when both ASes under one common control**

Carrier's Carrier



- Same principles as in normal MPLS
- Customer trusts carrier who trusts carrier

Carrier's Carrier: The Interface



- **Control Plane:**

  PE1 assigns label to PE2

- **Data Plane:**

  PE1 only accepts packets with this label on this i/f

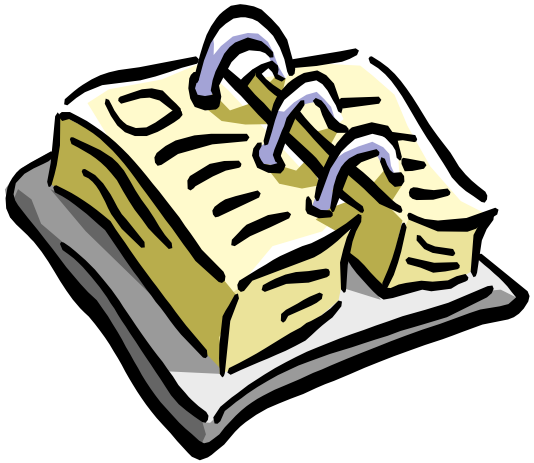
  →PE1 controls data plane

  →No label spoofing possible

Carrier's Carrier: Summary

- **Can be secured well**
  - **Carrier has VPN on Carrier's Carrier MPLS cloud**
  - **Carrier cannot intrude into other VPNs.**
  - **Carrier *can* mess up his own VPN (VPNs he offers to his customers)**
- **End customer must trust both SPs.**

Agenda



- Analysis of MPLS/VPN Security
- Security Recommendations
- Secure MPLS VPN Design
  - Internet Access
- Secure Operations
- Attacking an MPLS Network
- IPsec and MPLS
- Summary

Key: PE Security

- **What happens if a single PE in the core gets compromised?**

  Intruder has access to all VPNs; GRE tunnel to “his” CE in the Internet, bring that CE into *any* VPN.

  That VPN might not even notice…

  Worst Case!

- **Therefore: PE SECURITY IS PARAMOUNT!**
- **Therefore: No PE on customer premises!**

  (Think about console access, password recovery…)

Solution: Operational Security

- **Security depends on SP!**

  Employee can make mistake, or malicious misconfiguration

- **Potential Security hole:**

  If PE compromised, VPNs might be insecure

- **Cannot *prevent* all misconfigs**

  → Need to operationally control this

Operational Security

- **Logging config changes**

  Dual Control: Network operators must have no access to logging facility

  Otherwise they can hack the network, and delete the logs

- **AAA for access**
- **AAA for command authorization**

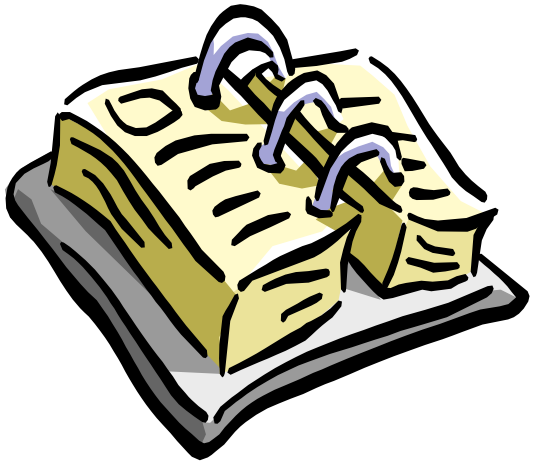
  → Keep logs in a secure place

  (Malicious employee might change logs too)

- **Tight control**
- **No service password-recovery where available**

Secure Operations is Hard!!!

Agenda



- Analysis of MPLS/VPN Security
- Security Recommendations
- Secure MPLS VPN Design
  - Internet Access
- Secure Operations
- **Attacking an MPLS Network**
- IPsec and MPLS
- Summary

Ways to Attack

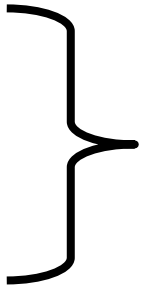
- **“Intrusion”: Get un-authorized access**

  Theory: Not possible (as shown before)

  Practice: Depends on:

  - Vendor implementation

  - Correct config and management



No Trust?

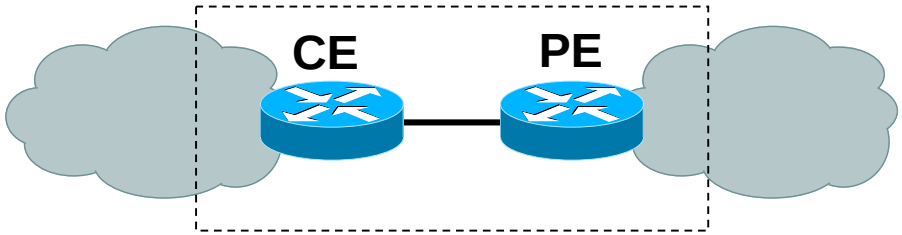
Use IPsec between CEs!

- **“Denial-of-Service”: Deny access of others**

  Much more interesting…

DoS Against MPLS

- **DoS is about Resource Starvation, one of:**
  - **Bandwidth**
  - **CPU**
  - **Memory (buffers, routing tables…)**
- **In MPLS, we have to examine:**



- **Rest is the same as in other networks**

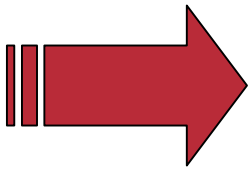
Attacking a CE from MPLS (other VPN)

- **Is the CE reachable from the MPLS side?**

  -> only if this is an Internet CE, otherwise not!
  (CE-PE addressing is part of VPN!)

- **For Internet CEs:**

  Same security rules apply as for any other access router.



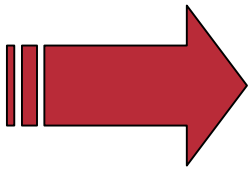
MPLS hides VPN-CEs: Secure!
Internet CEs: Same as in other networks

Attacking a CE-PE Line

- Also depends on reachability of CE or the VPN behind it
- Only an issue for Lines to Internet-CEs

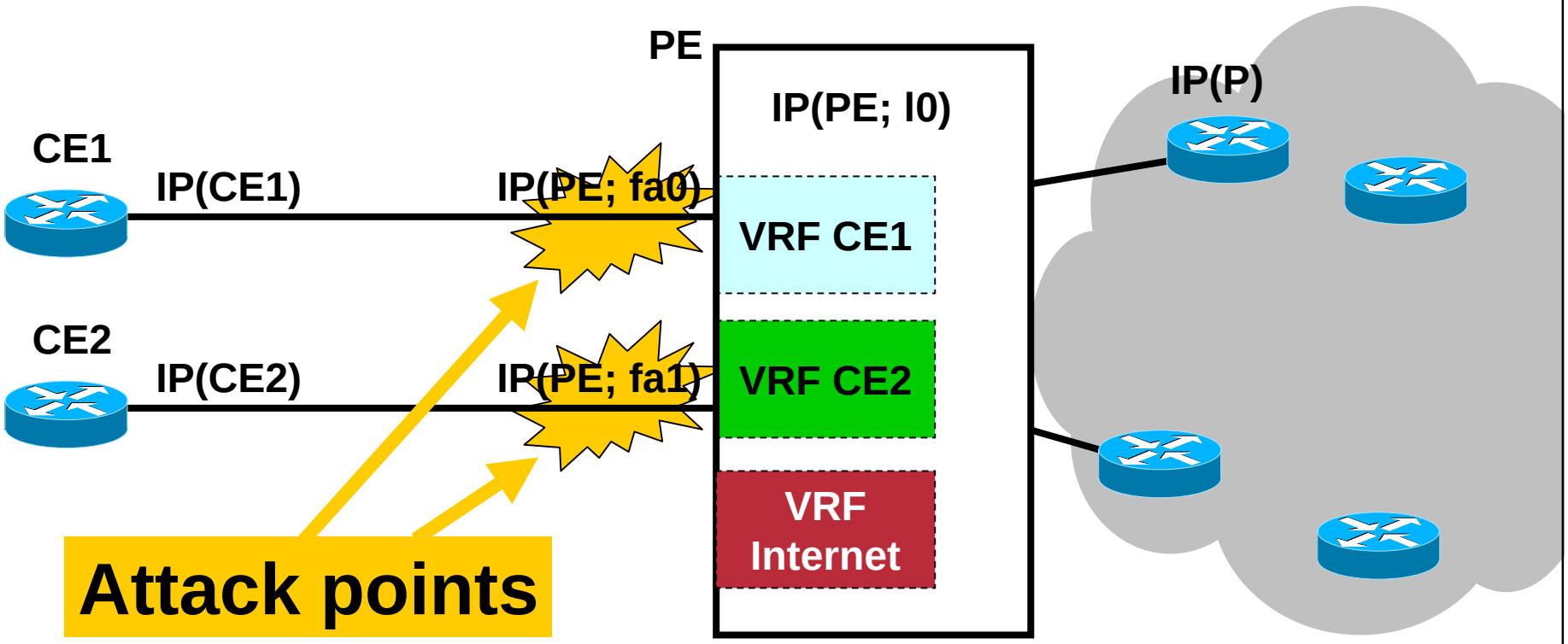
  Same considerations as in normal networks
- If CE-PE line shared (VPN and Internet):

  DoS on Internet may influence VPN! Use CAR!



MPLS hides VPN-CEs: Secure!
Internet CEs: Same as in other networks

Attacking a PE Router



Only visible: “your” interface and interfaces of Internet CEs

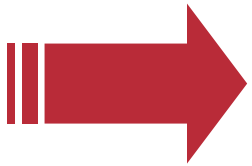
DoS Attacks to PE Can Come from…

- Other VPN, connected to same PE
- Internet, if PE carries Internet VRF

Possible Attacks:

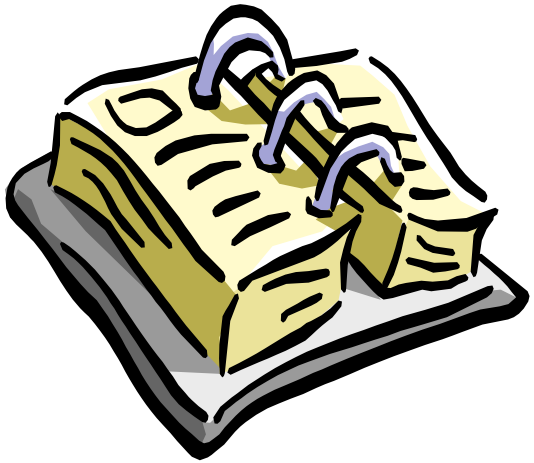
- **Resource starvation on PE**

  Too many routing updates, too many SNMP requests, small servers…



Has to Be Secured and Can Be Secured!

Agenda



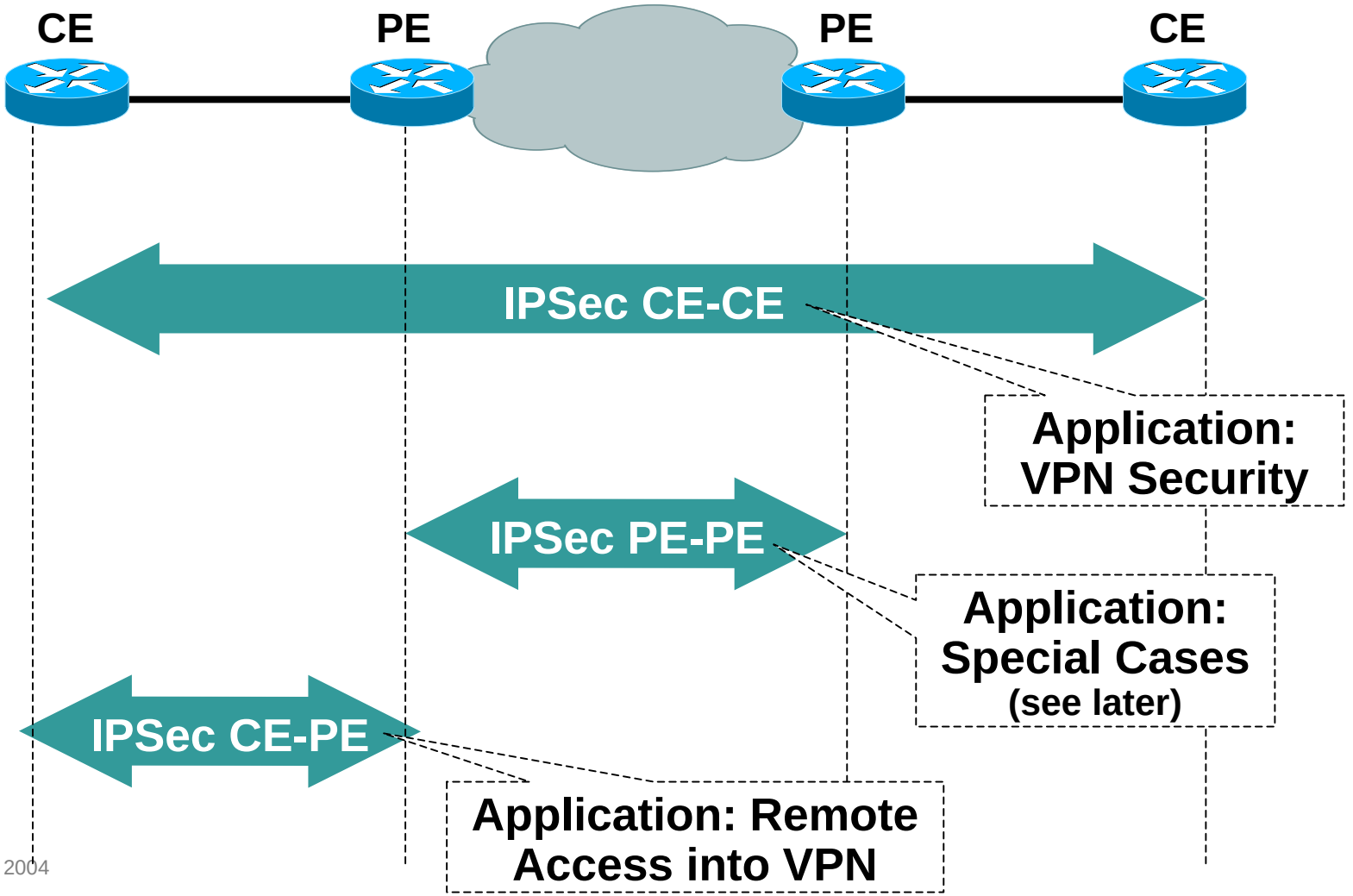
- Analysis of MPLS/VPN Security
- Security Recommendations
- Secure MPLS VPN Design
  - Internet Access
- Secure Operations
- Attacking an MPLS Network
- IPsec and MPLS
- Summary

Use IPsec if you need:

- Encryption of traffic
- Direct authentication of CEs
- Integrity of traffic
- Replay detection

- Or: If you don’t want to trust your ISP for traffic separation!

Where to Apply IPSec



PE-PE IPSec Internet Draft

- **“Use of PE-PE IPSec in RFC2547 VPNs” (E. Rosen et al) draft-ietf-l3vpn-ipsec-2547-02.txt**
- **IPSec instead of LSP inside 2547bis core**
- **Does not define IPSec specific mechanism**

  Key exchange, SA scalability, …

Applications of PE-PE IPSec

- **If core is not pure MPLS, but IP based**

  Standard 2547bis requires MPLS core, PE-PE IPSec does not

  Alternative: MPLS in IP/GRE/L2TPv3, but with PE-PE IPSec spoofing impossible

- **Protect against misbehaving transit nodes**
- **Protection against sniffing on core lines**

Non-Application: Customer Security

Cisco.com

Hacker wants to …	IPSec CE-CE	IPSec PE-PE
… read VPN traffic	Protects Fully	Protects Partially
… insert traffic into VPN	Protects Fully	Protects Partially
… join a VPN	Protects Fully	Doesn't Protect
… DoS a VPN / the core	Doesn't Protect	Doesn't Protect

Non-Application: Customer Security

"IPSec Security Associations that associate ingress PE routes with egress PE routers do not ensure privacy for VPN data. The data is exposed on the PE-CE access links, and is exposed in the PE routers themselves."

draft-ietf-l3vpn-ipsec-2547-02.txt

PE-PE IPSec: Encapsulation
(draft-ietf-l3vpn-ipsec-2547-02.txt)

1. Pre-pend the VPN label, as in normal MPLS

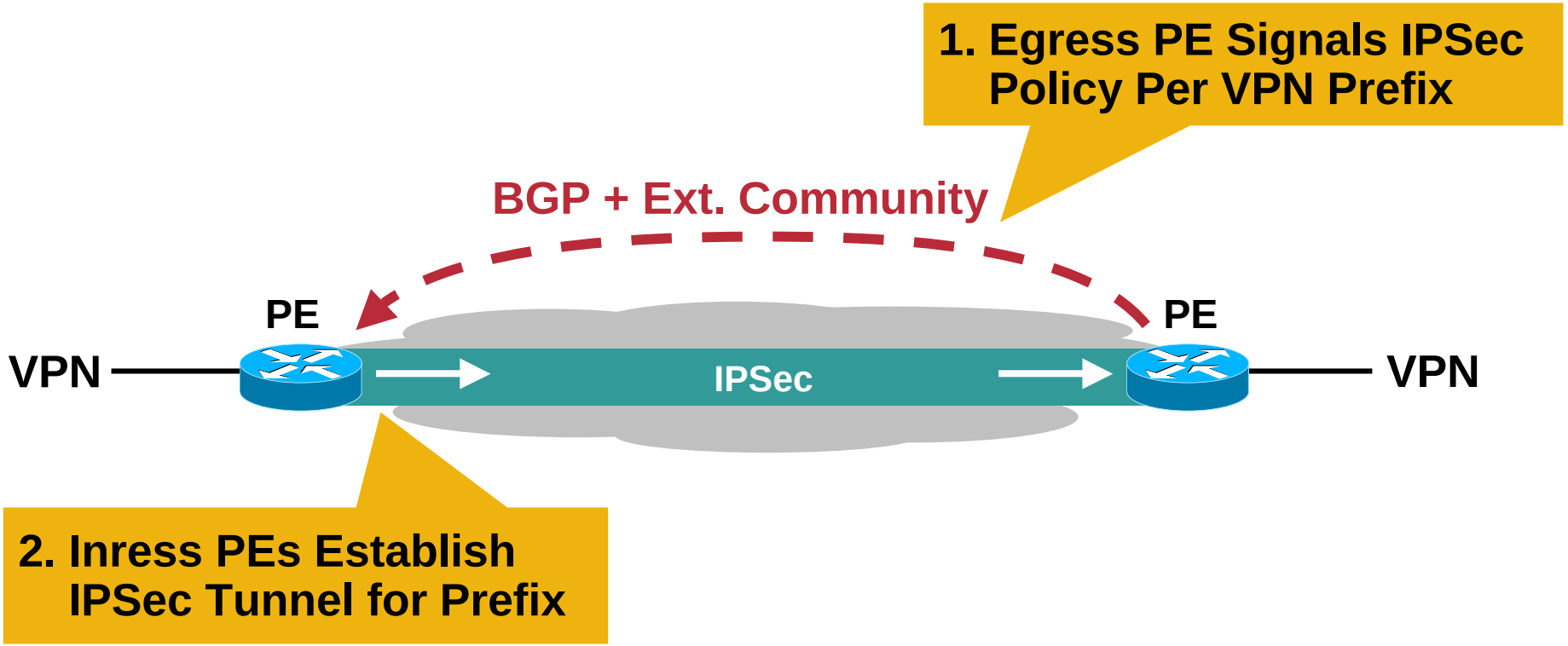
2. Encapsulate: MPLS in GRE or IP (tunnel between PEs)

3. Apply IPsec transport mode

(Normal MPLS:

)

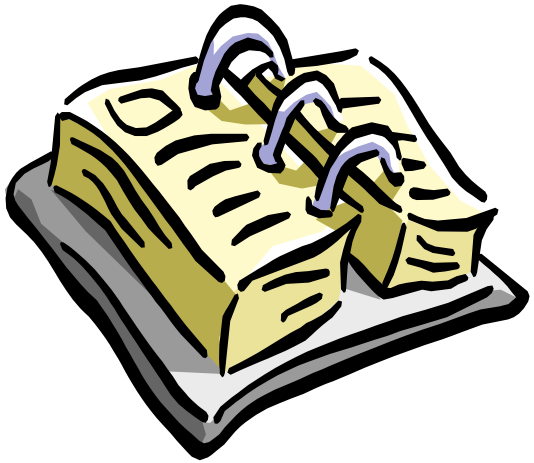
PE-PE IPSec: How It Works



- **Not defined in draft:**

  How to establish IPSec tunnel

Agenda



- Analysis of MPLS/VPN Security
- Security Recommendations
- Secure MPLS VPN Design
  - Internet Access
- Secure Operations
- Attacking an MPLS Network
- IPsec and MPLS
- Summary

MPLS Doesn’t Provide…

- Protection against misconfigurations in the core
- Protection against attacks from within the core
- Confidentiality, authentication, integrity, anti-replay
  - Use IPSec if required
- Customer network security

MPLS Security Overview

1. **Don't let packets into (!) the core**

   No way to attack core, except through routing, thus:

   → **Still "Open": Routing Protocol**

2. **Secure the routing protocol**

   Neighbor authentication, maximum routes, dampening, …

   → **Only Attack Vector: Transit Traffic**

3. **Design for transit traffic**

   QoS to give VPN priority over Internet

   Choose correct router for bandwidth

   Separate PEs where necessary

   → **Now Only Insider Attacks Possible**

4. **Operate Securely**

   → **Avoid Insider Attacks**

Summary

- **MPLS VPNs can be secured as well as ATM/FR VPNs**
- **Security depends on correct operation and implementation**
- **MPLS backbones can be more secure than "normal" IP backbones**
  - **Core not accessible from outside**
  - **Separate control and data plane**
- **Key: PE security**
  - **Advantage: Only PE-CE interfaces accessible from outside**
  - **Makes security easier than in "normal" networks**

References

- RFC2082 – RIP-2 MD5 Authentication
- RFC2154 – OSPF with Digital Signatures
- RFC2385 – Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC3013 – Recommended Internet Service Provider Security Services and Procedures
- RFC2196 – Site Security Handbook
- MPLS and VPN Architectures – ISBN 1-58705-002-1
- Cisco ISP Essentials – ISBN 1-58705-041-2 (http://www.ispbook.com/)
- http://www.cisco.com/public/cons/isp/documents/IOSEssentialsPDF.zip
- General Information on Securing Cisco Routers
- http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080120f48.shtml
- Cisco Secure Virtual Private Networks - ISBN 1-58705-033-1

Q and A

Backup Material

Non-IP networks: Not 100% secure!! Example: Telephone Network

“I had access to most, if not all, of the switches in Las Vegas,” testified Mitnick, at a hearing of Nevada's Public Utilities Commission (PUC). “I had the same privileges as a Northern Telecom technician.”

Source:
http://online.securityfocus.com/news/497

Non-IP networks: Not 100% secure!! Example: ATM Switch

“a single 'land' packet sent to the telnet port (23) of either the inband or out-of-band interface will cause the device to stop responding to ip traffic. Over the course of 6-1/2 minutes, all CPU will be consumed and device reboots.”

Source: Bugtraq, 15 June 2002: “Fore/Marconi ATM Switch 'land' vulnerability”, by seeker_sojourn@hotmail.com;