PROTECTING AN MPLS/VPN CORE

Rehan Nedaria

CCIE:10971 (SP/R&S)

July 15 2009

Why Is MPLS VPN 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

Agenda

Analysis of MPLS/VPN Security

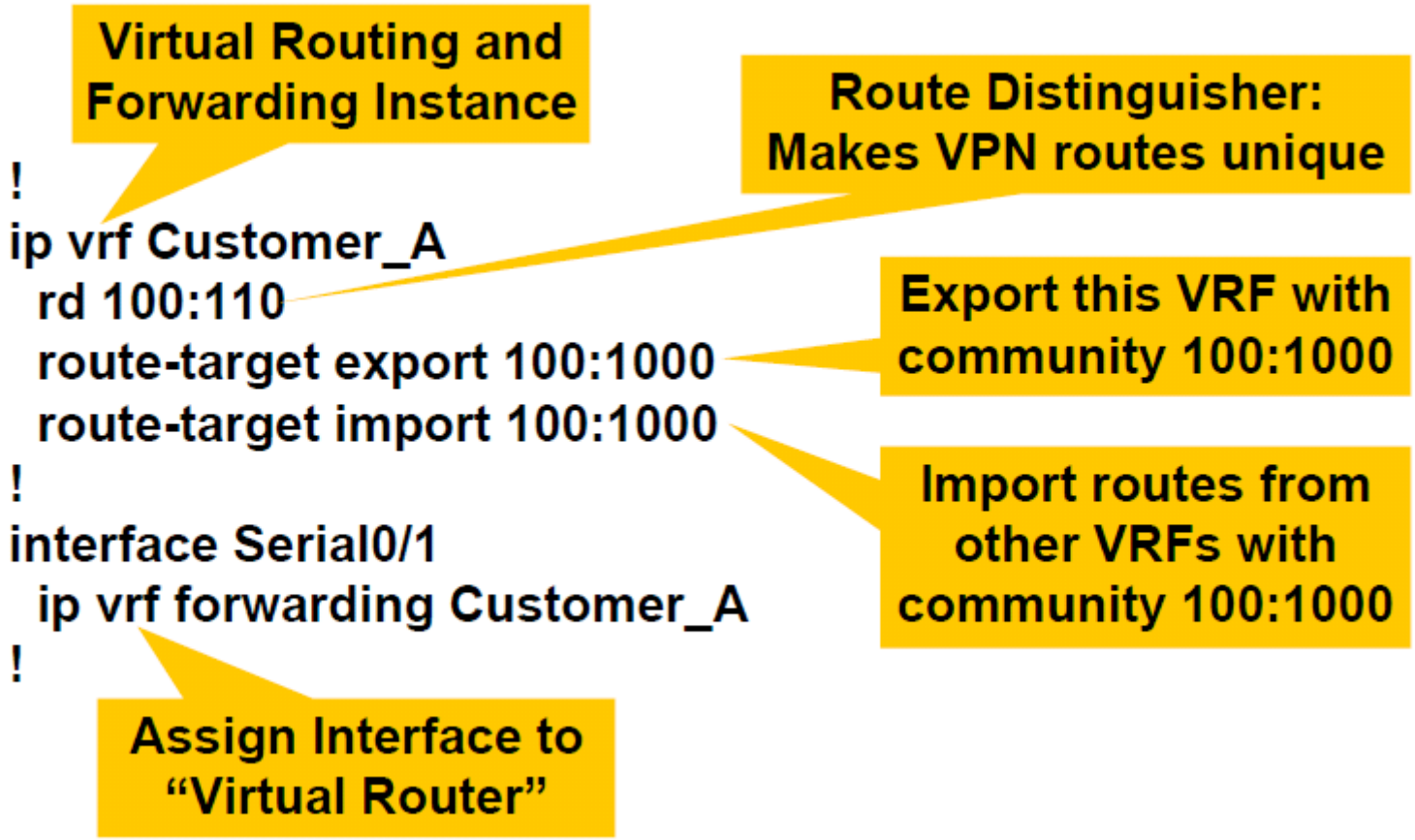
Security Recommendations

MPLS Security Architectures (Internet Access)

IPsec and MPLS

Summary

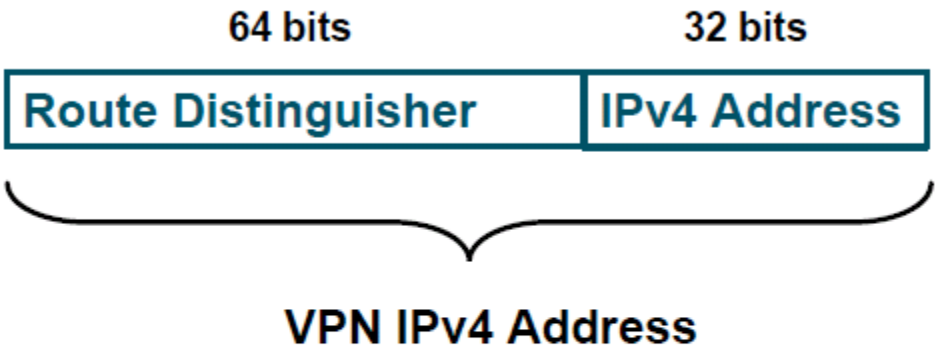
The Principle: A "Virtual Router"



General VPN Security Requirements

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

Address Space Separation



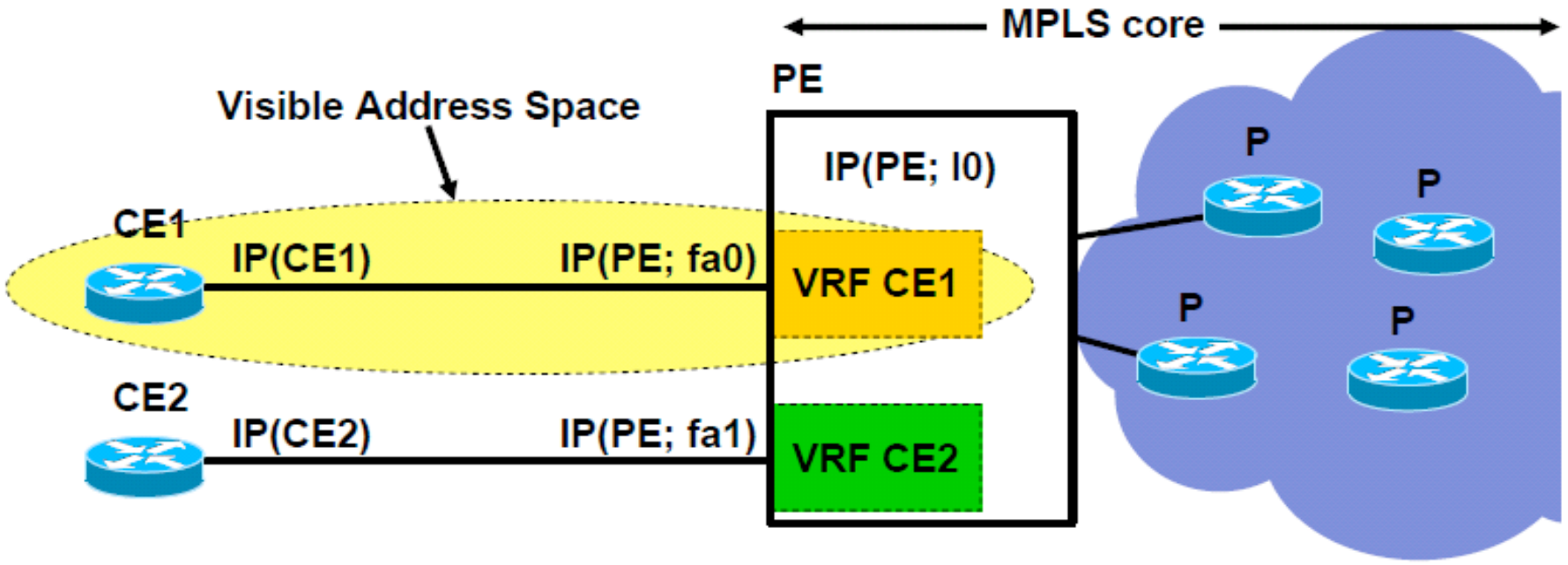
Within the MPLS core all addresses are unique due to the Route Distinguisher

Routing Separation

- Each (sub-) interface is assigned to a VRF
- Each VRF has a RD (route distinguisher)
- Routing instance: within one RD
  -> within one VRF

  -> Routing Separation

Hiding of the MPLS Core Structure



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

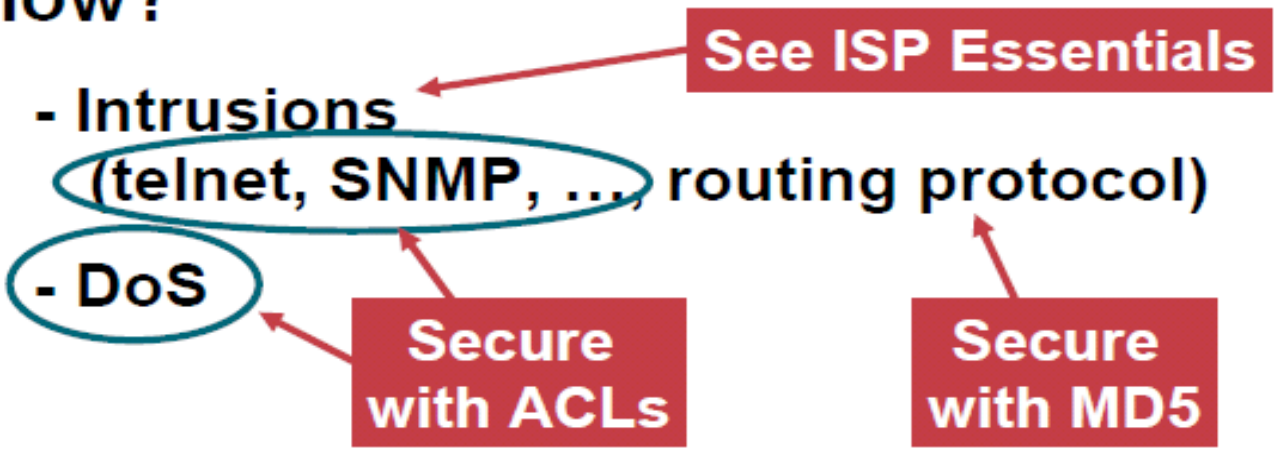
Resistance to Attacks: Where and How?

- Where can you attack?

  Address and Routing Separation, thus:

  Only Attack point: peering PE

- How?



Label Spoofing

- Label spoofing is the ability of the upstream router to replace or insert a label into a packet that was not originally allocated by the downstream router
- PE router expects IP packet from CE
- Labelled packets will be dropped Thus no spoofing possible
- Cisco router does not accept labelled packets on an interface that is NOT enabled for label switching
- CE router can spoof source or destination address before packet arrives at the PE, but this would only affect the customer's own VPN (address separation attribute)
- Customer would be spoofing self

Agenda

Analysis of MPLS/VPN Security

Security Recommendations

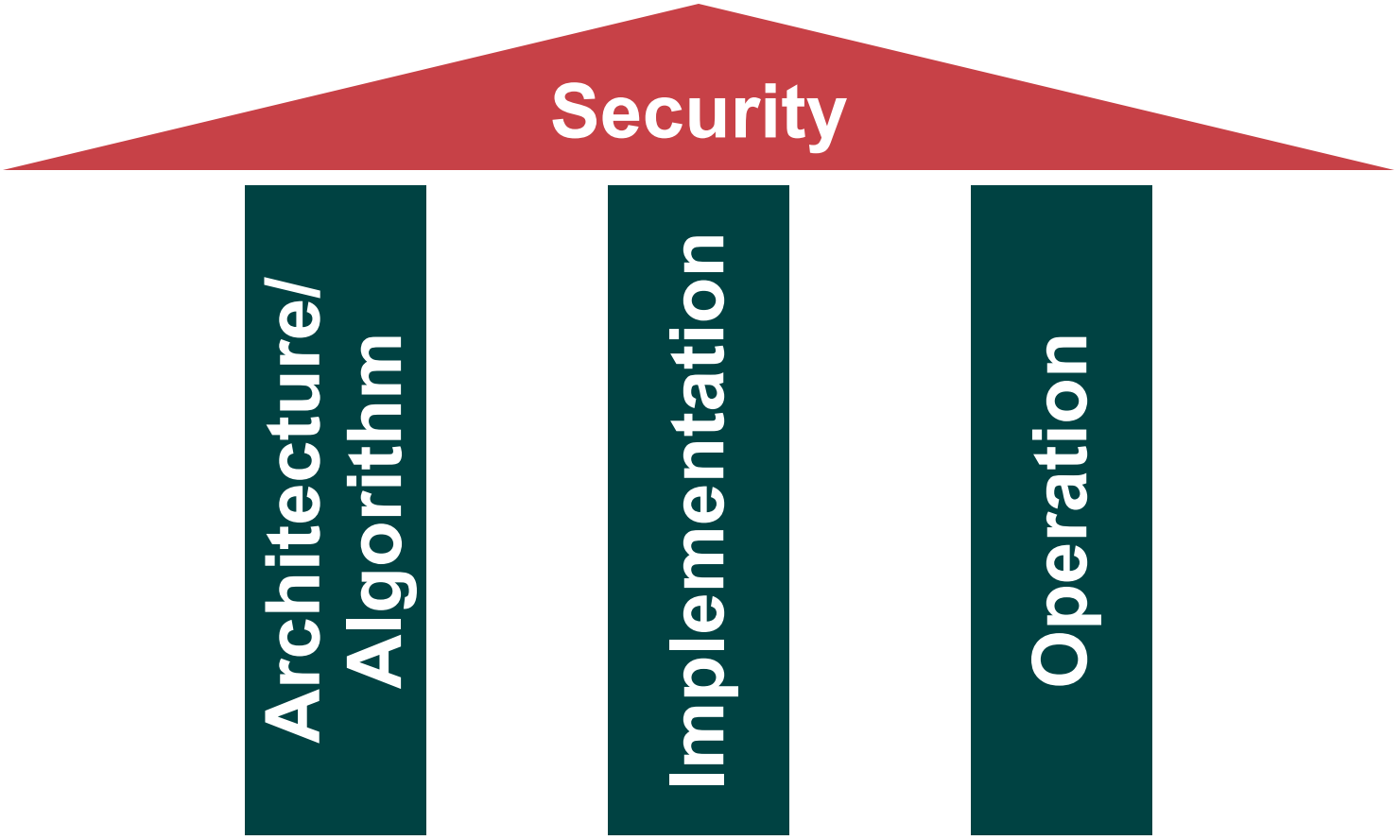
MPLS Security Architectures (Internet Access)

Attacking an MPLS Network

IPsec and MPLS

Summary

Security Relies on Three Pillars



Break One, and All Security Is Gone!

Security Recommendations for ISPs

- Secure devices (PE, P): They are trusted!
- CE-PE interface: Secure with ACLs
- 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

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)**

Neighbor Authentication

- **Router "knows" his neighbors**
  - **Verification through shared MD5 secret**
- **Verifies updates it receives from neighbor**
- **Supported: BGP, ISIS, OSPF, EIGRP, RIPv2**
- **Key chains supported for ISIS, EIGRP, RIP**
  - **Use them where available**
  - **Easier key roll-over**
- **Config easy**

Neighbor Authentication

router bgp 13

address-family ipv4 vrf Peabody1

neighbor 1.1.1.1 remote-as 14

neighbor 1.1.1.1 update-source loopback 0

neighbor 1.1.1.1 password 5 1Sherman2 (establishes use of MD5 password “1Sherman2” for this neighbor)

address- family ipv4 vrf Dudley1

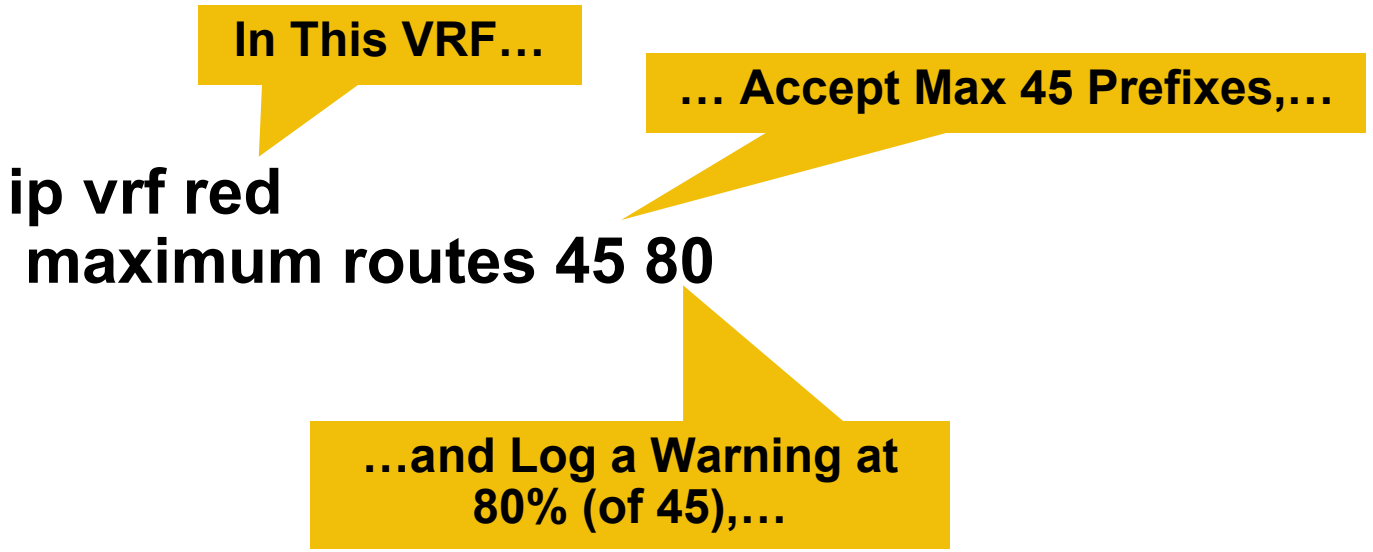
neighbor 2.2.2.2 remote-as 15

neighbor 2.2.2.2 update-source loopback 0

neighbor 2.2.2.2 password 5 77doright2 (# establishes use of MD5 password “77doright2” for this neighbor)

VRF Maximum Prefix Number

- **Injection of too many routes:**
  - **Potential memory overflow**
  - **Potential DoS attack**
- **For a VRF: Specify the maximum number of routes allowed**



P to P/PE Security

- Routing authentication: IGP BGP and MPBGP MD5 Authentication

- Label Distribution Protocol [LDP] MD5 authentication:
  The LDP can also be secured with MD5 authentication across the MPLS cloud. This scenario prevents hackers from introducing bogus routers, which would participate in the LDP.

- Hide the addressing structure of the MPLS core to the outside world

  no mpls ip propagate-ttl forwarded on PE (mitigate traceroute results)

Configuring IP TTL Propagation—Extended Options

router(config)#

no mpls ip propagate-ttl [forwarded | local]

Cisco IOS Release 12.1(5)T

Selectively disables IP TTL propagation for:

- **Forwarded traffic (traceroute does not work for transit traffic labeled by this router)**
- **Local traffic (traceroute does not work from the router but works for transit traffic labeled by this router)**

Agenda

Analysis of MPLS/VPN Security

Security Recommendations

MPLS Security Architectures (Internet Access)

IPsec and MPLS

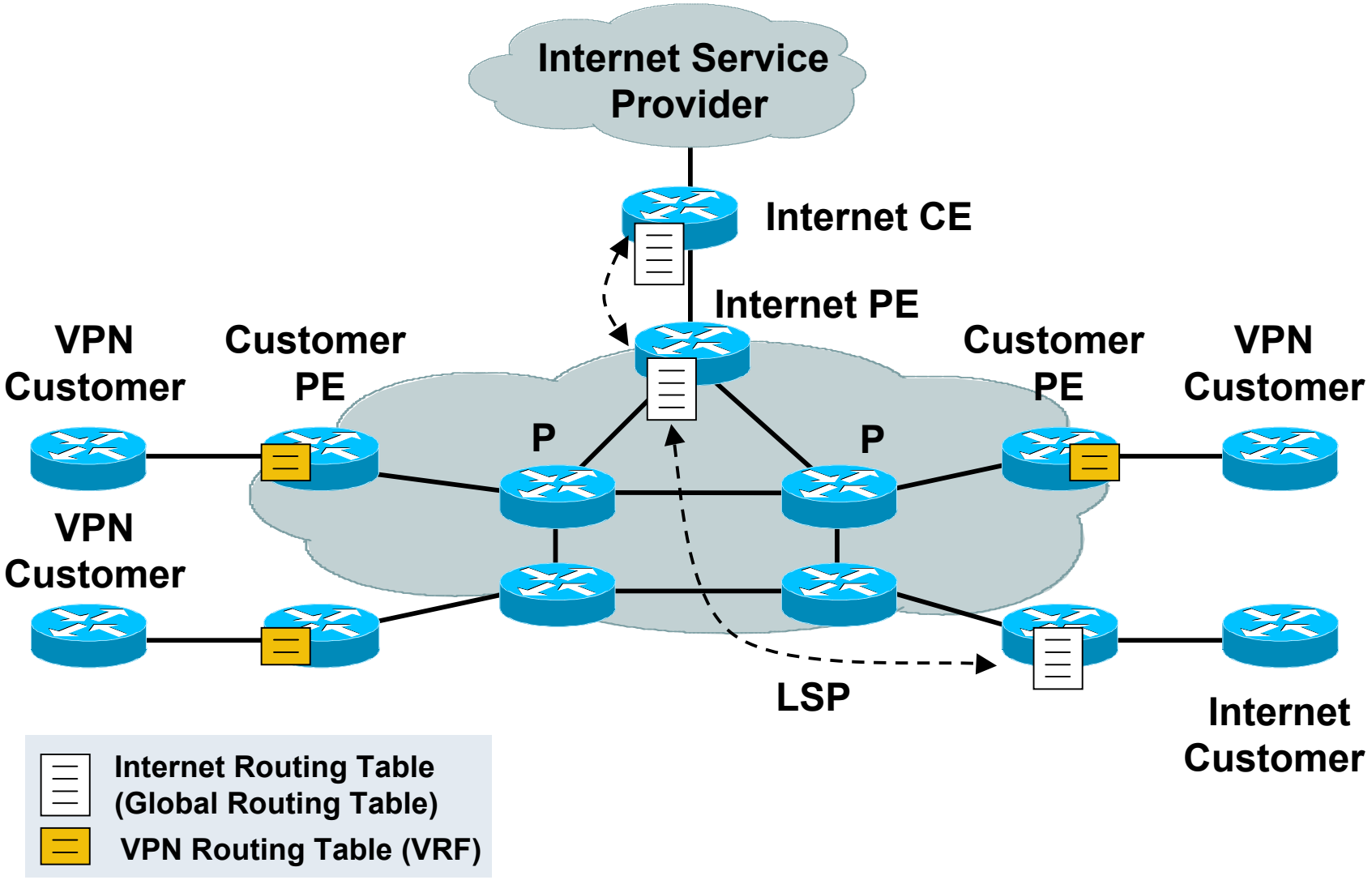
Summary

Internet Provisioning on an MPLS Core

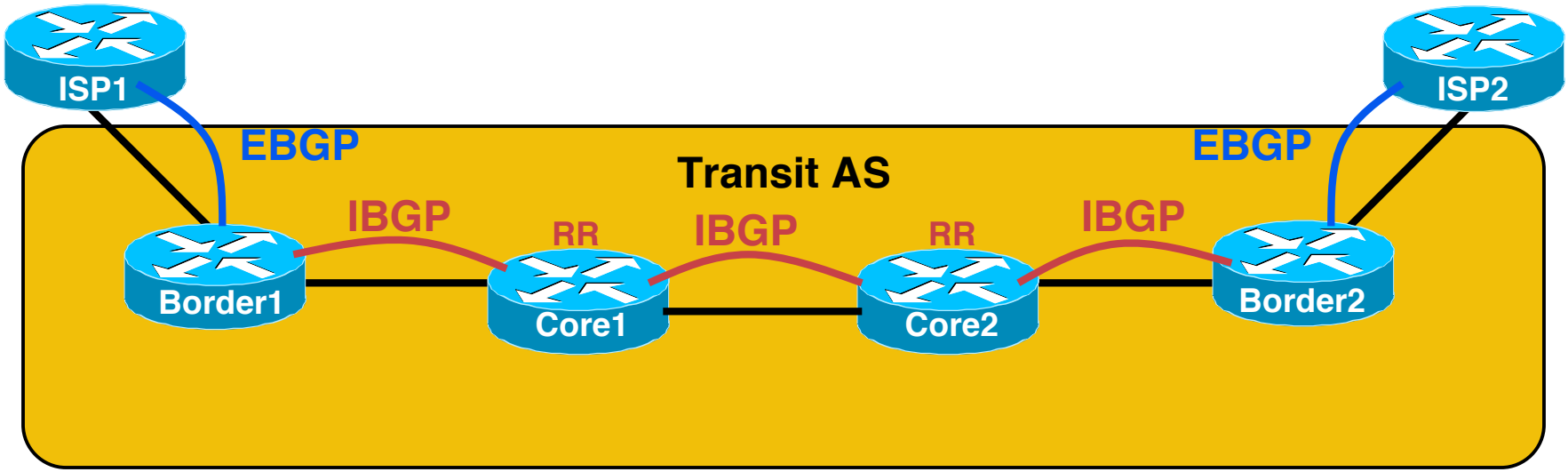
Two basic possibilities:

1. **Internet in global table, either:**
   - 1a) Internet-free core (using LSPs between PEs)
   - 1b) hop-by-hop routing
2. **Internet in VRF**
   - Internet carried as a VPN on the core

Internet in the Global Routing Table Using LSPs Between PEs

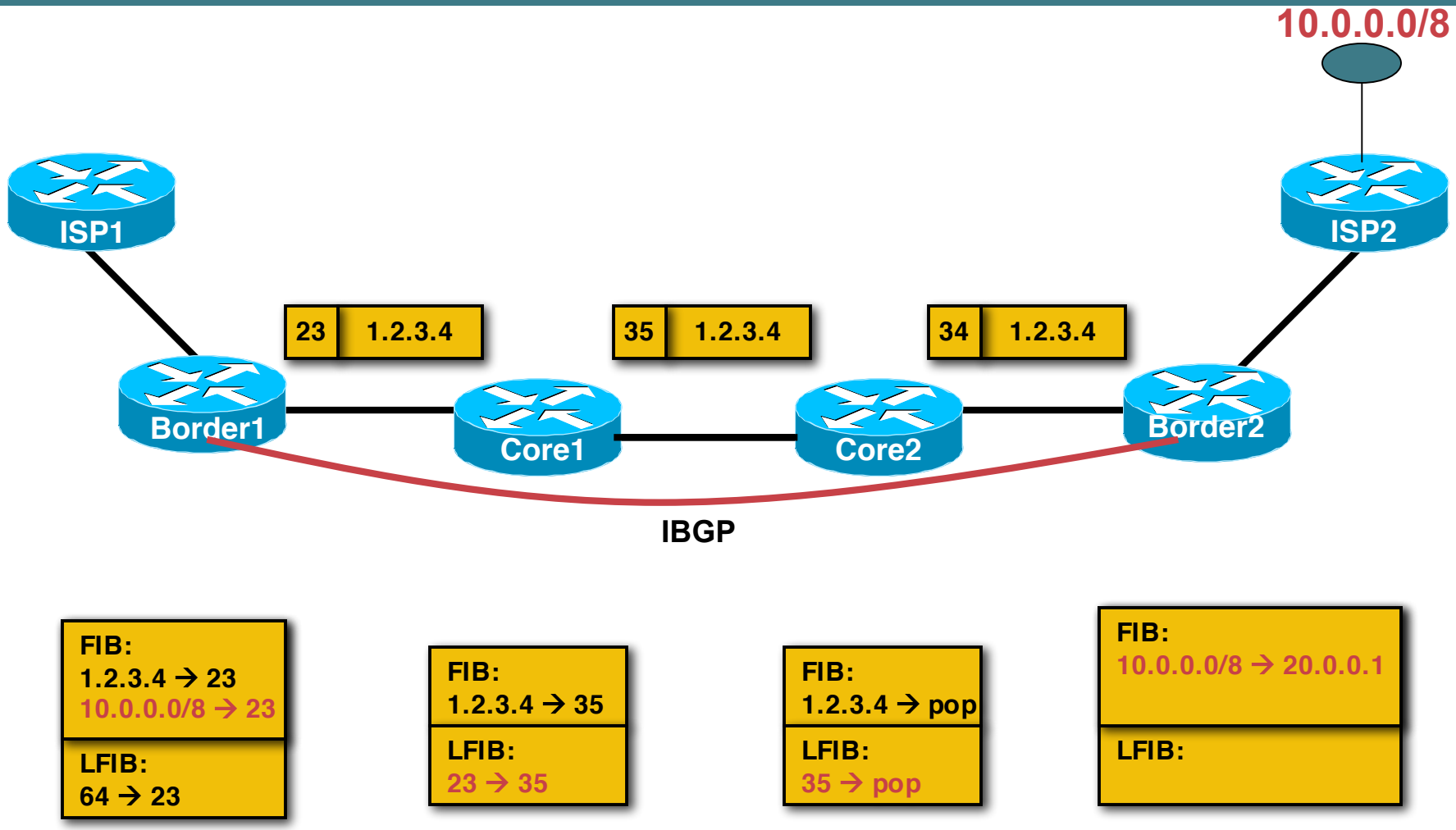


Traditional BGP AS System Design Requirements



- **All core routers are required to run BGP.**
- **All core routers require full Internet routing information (more than 100,000 networks) to be able to forward IP packets between ISP1 and ISP2.**

MPLS-Based Transit AS Packet Propagation



Internet in the Global Routing Table Using LSPs Between PEs

- **Default behavior, if Internet in global table!!**
  - **On ingress PE: BGP next hop: Egress PE loopback**
  - **Next hop to egress usually has label!**
  - **LSP is used to reach egress PE**
  - **P routers do not need to know Internet routes (nor run BGP)**
- **Security consequence:**
  - **PE routers are fully reachable from Internet, by default (bi-directional)**
  - **P routers are also by default reachable from Internet; but only uni-directional, they don't know the way back!**

Internet in the Global Routing Table Using LSPs Between PEs

Recommendations:

- **Fully secure each router!**
- **Do not advertise IGP routes outside**

  (This is a general security recommendation for all cores!)

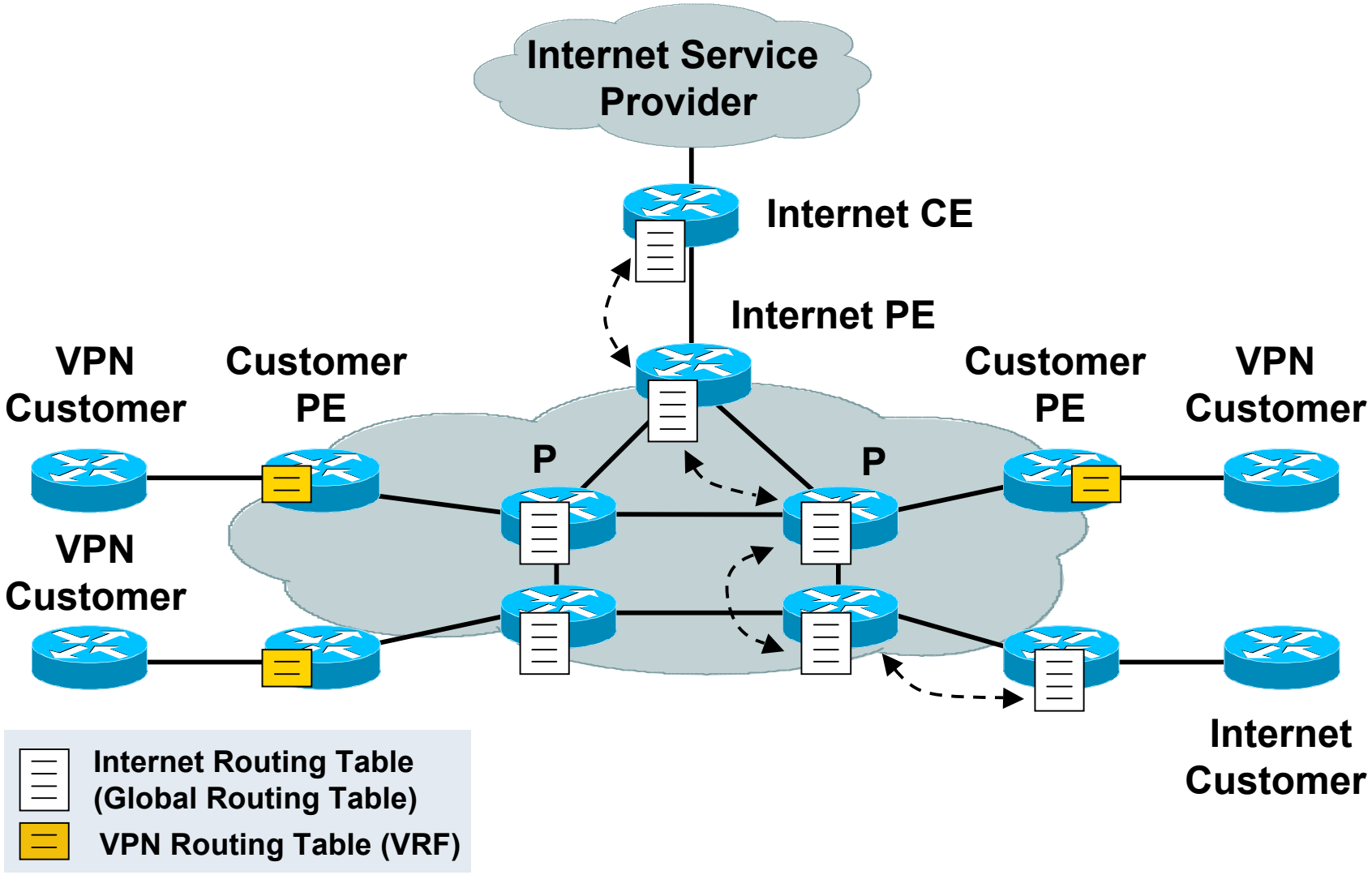
  P routers not reachable (unless someone defaults to you)

  PE routers not reachable (possible exception: Peering PE)
- **Infrastructure ACLs to block core space:**

  Additional security mechanism

  Even if someone defaults to you, he cannot reach the core

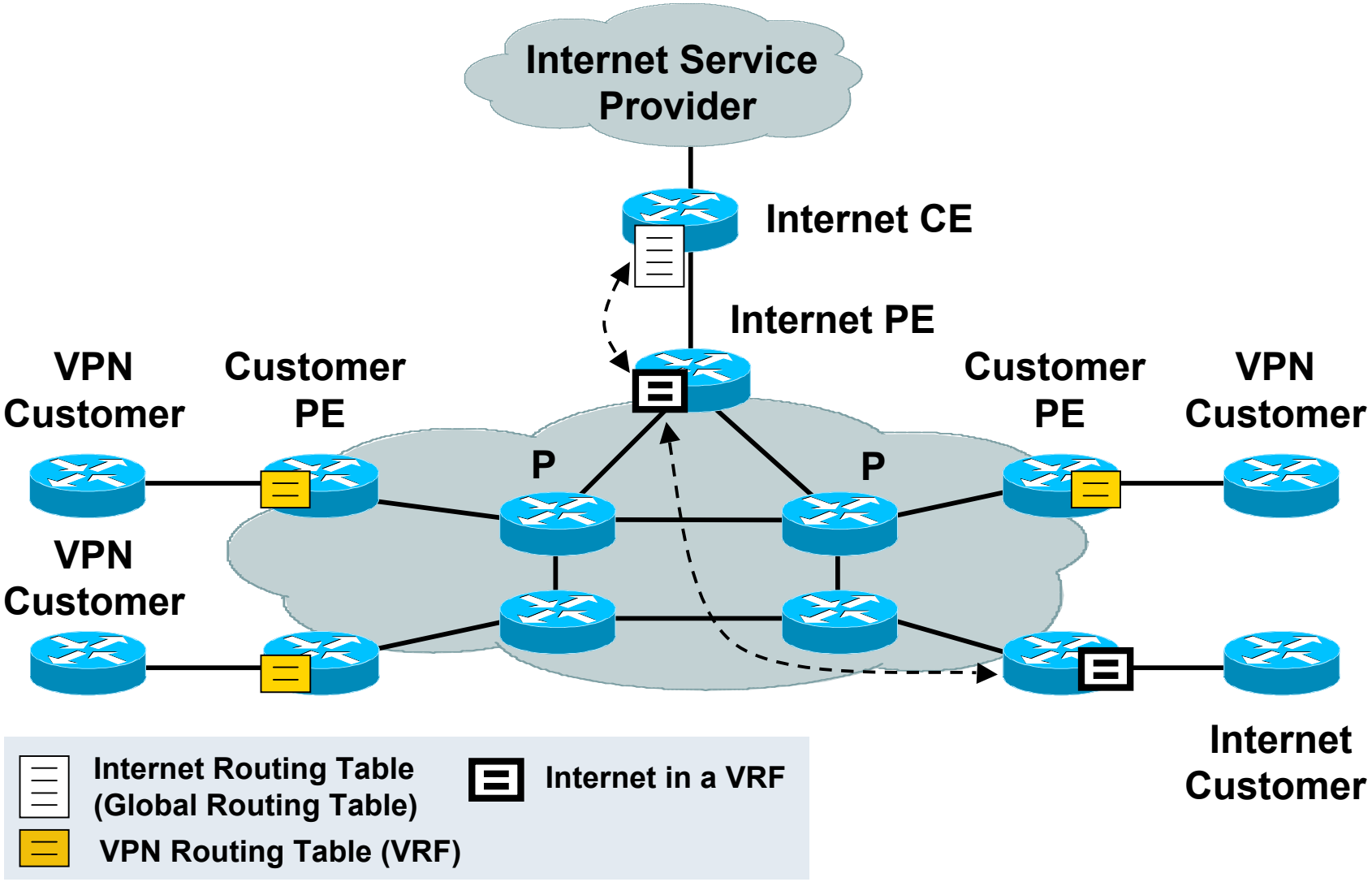
Internet in the Global Routing Table
Hop-by-Hop Routing



Internet in the Global Routing Table Hop-by-Hop Routing

- **Like in standard IP core**
  - **Each router speaks BGP, and carries Internet routes**
  - **Not default, must be configured!**
- **Security consequence:**
  - **P and PE routers by default fully reachable from Internet**
- **Recommendations: (like before)**
  - **Fully secure each router!**
  - **Do not advertise IGP routes outside**
  - **Infrastructure ACLs**

Internet in a VRF



Internet in a VRF

- **Internet is a VPN on the core**
  - **Full separation to other VPNs, and the core, by default!**
  - **“Connection” between Internet and a VPN (for service) must be specifically configured**
- **Security consequence:**
  - **P routers not reachable from anywhere!**
  - **PE routers only reachable on outbound facing interfaces;**
  - **Very limited**
  - **Much easier to secure**
- **But!!!**
  - **Routes in a VRF take more memory!!**
  - **Convergence times increase**

Fixed in IOS XR
(fast convergence)

Internet in a VRF

Recommendations:

- **Fully secure each router (you never know…)**
- **Secure external facing PE interfaces!**

  Use Infrastructure ACLs for this (see earlier)

  (Internal PE i/f and P cannot be reached from outside)

Agenda

Analysis of MPLS/VPN Security

Security Recommendations

MPLS Security Architectures (Internet Access)

Attacking an MPLS Network

IPsec and MPLS

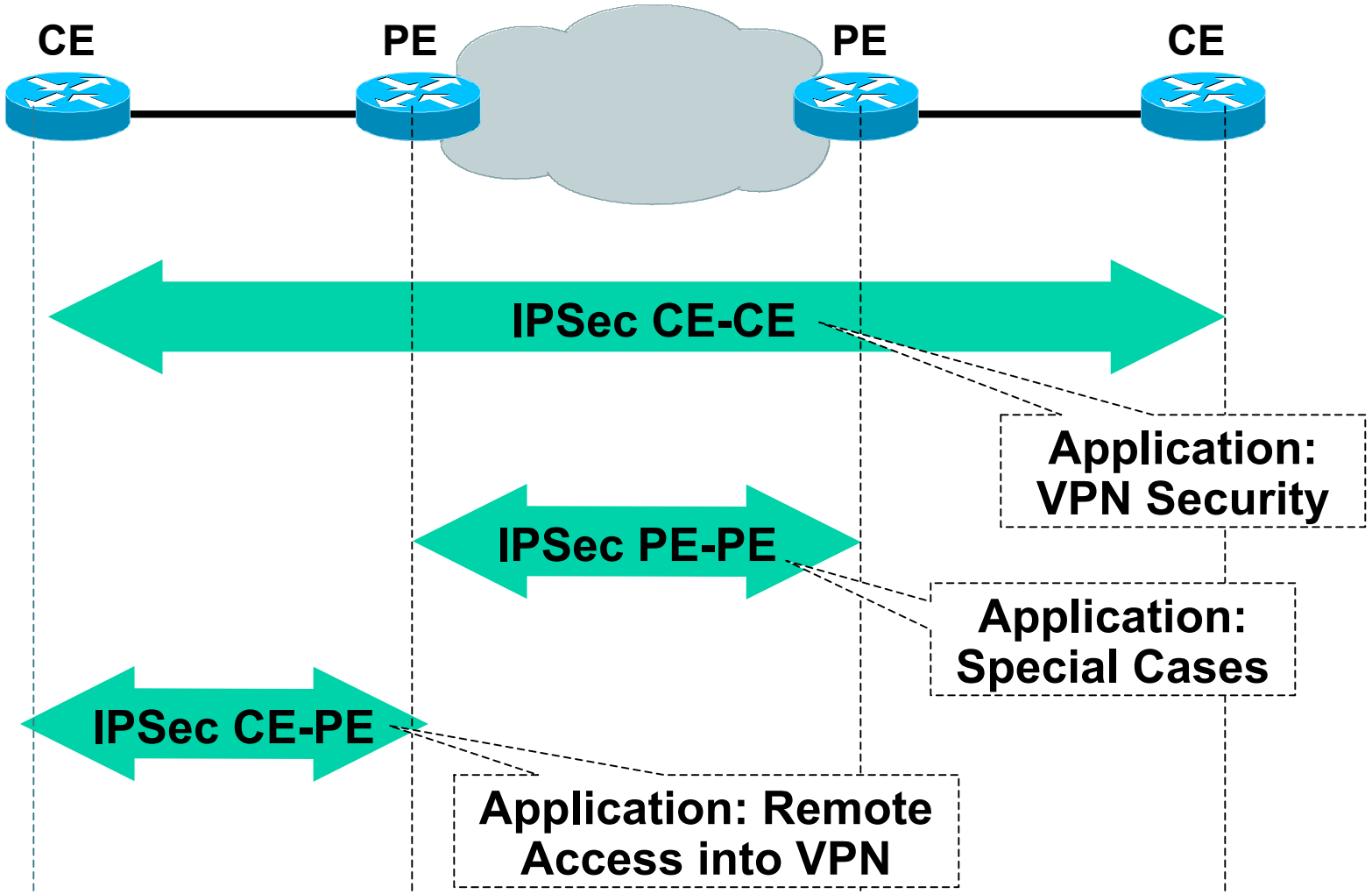
Summary

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



How to Establish IPSec: Options

- **Option 1: Static IPSec**
  - Pre-configure static IPSec tunnels
  - Works, but does not scale well
- **Option 2: Dynamic Cryptomap/ Tunnel Endpoint Discovery**
  - Scaling improvements over 1).
- **Option 3: DMVPN**
  - Dynamic tunnel establishment
  - Easy to configure and maintain
  - Some scaling issues
- **Option 4: GET VPN**
  - Easy to configure and maintain
  - Scales well

Dynamic Multipoint VPN

Group Encrypted Transport

RECOMMENDED

Agenda

Analysis of MPLS/VPN Security

Security Recommendations

MPLS Security Architectures (Internet Access)

Attacking an MPLS Network

IPsec and MPLS

Summary

MPLS doesn't provide:

- **Protection against mis-configurations in the core**
- **Protection against attacks from within the core**
- **Confidentiality, authentication, integrity, anti-replay -> Use IPsec if required**
- **Customer network security**

Summary

- **MPLS VPNs can be secured as well as ATM/FR VPNs**
- **Security depends on correct operation and implementation (everywhere!)**
- **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

THANKS