Securing a Core Network - Discussion

RIPE, Routing WG, Manchester, 21 Sep 2004

Michael Behringer <mbehring@cisco.com>

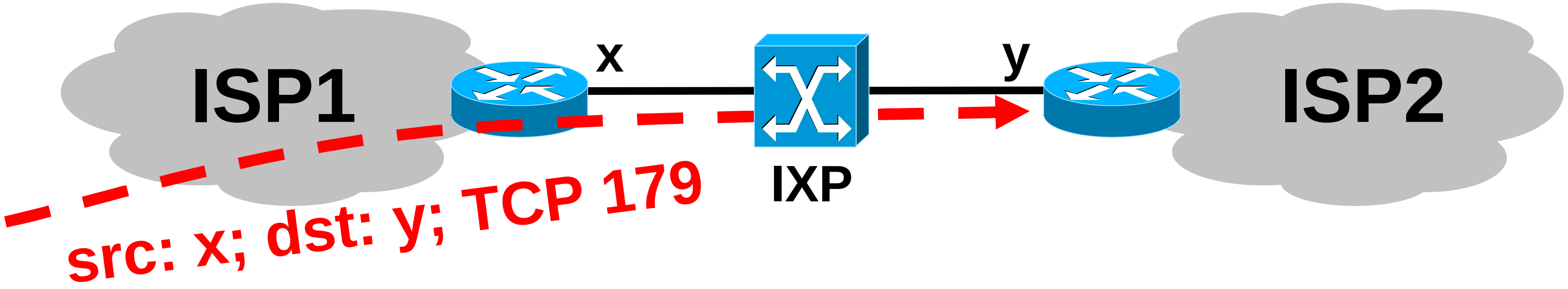
Christian Panigl <panigl@noc.ACO.net>

Goal of this Presentation

- Some core security techniques have an impact on the global Internet
- Currently there is no commonly agreed “best current practice”
- Open discussion of pros and cons

Attacking IXP Peerings

- IXP address spaces are known (IRR)
- → Easy to spoof BGP packets
- Can I get there?



- Not if: ISP 1 does anti-spoofing
- Not if: IXP address space not routed (and nobody defaults to either ISP, or ISPs don’t default to IXP)

Transit ACLs

- Normally: ISP Networks "permit ip any any" for transit
- "Transparency"
- Under extreme stress (worms, DoS):

  ISP apply temporary ACLs to filter attack/worm traffic
- Note: TEMPORARY
- Routers must support this

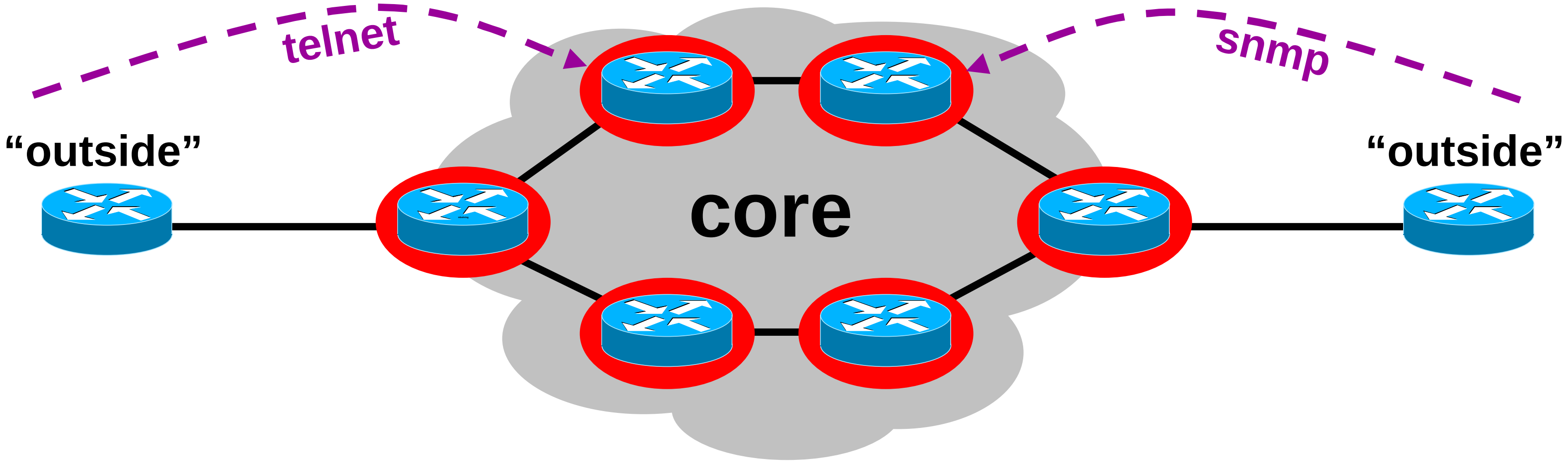
Discussion!

Re-Colouring at Edge

- Precedence 6&7: Reserved for routing
- No transit traffic should use prec 6 or 7
    - Problem with QoS on the core
    - Problem with routing protocols (same priority)
    - Routers look first at prec 6&7 traffic!!
    - → This can be a security risk
- Re-colour at edge!! (CAR)
- Depends on ingress line card / router

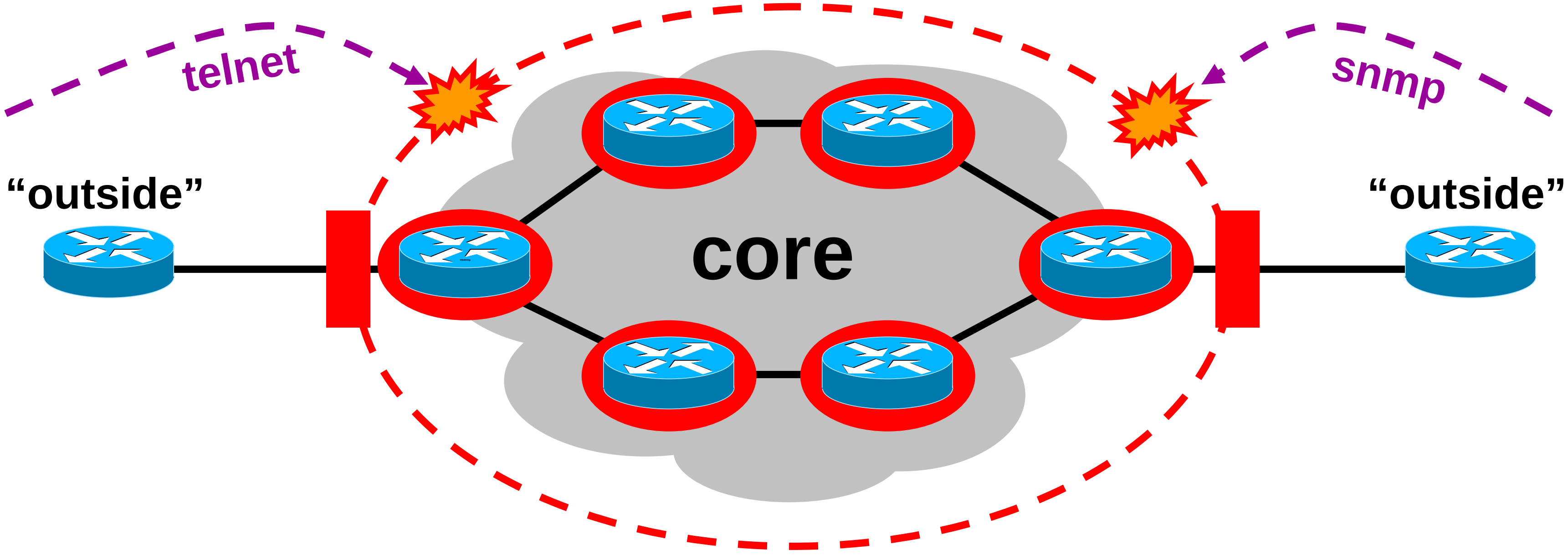
Discussion!

The Old World



- Core routers individually secured
- Every router accessible from outside

The New World



- Core routers individually secured PLUS
- Infrastructure protection
- Routers generally NOT accessible from outside

Core Hiding Techniques

- Private Address Space
- Non-IP Control Plane
  - ISIS
- MPLS

Private Address Space (RFC1918)

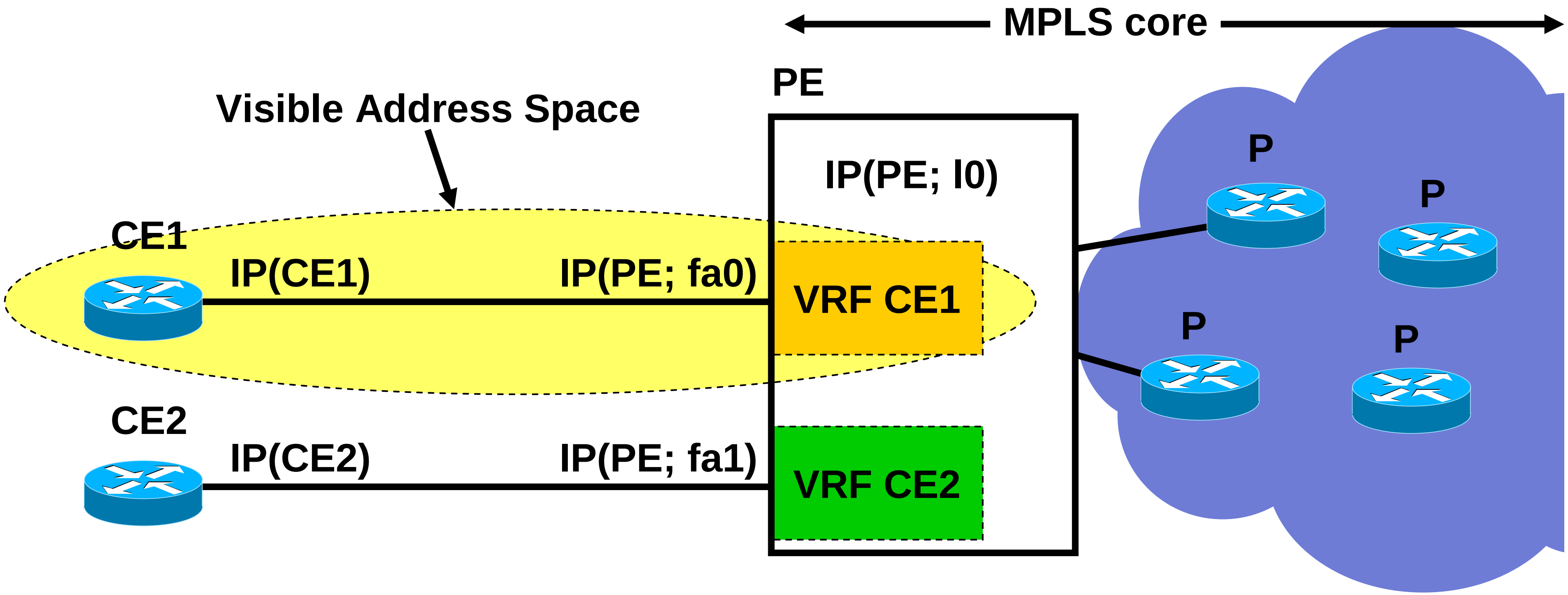
- All core interfaces get RFC1918 addresses
- All traffic from/to RFC1918 addresses blocked at ingress (implicit protection of core) => core interface addresses unreachable from outside core
- Blocking of traffic to edge interfaces (peering/upstream/customers) with non-private IP addresses still needs explicit ACL
- Troubleshooting (ping/traceroute) harder or even impossible from/to core devices
- Traceroute through core work but doesn’t resolve IP addresses externally

Non-IP Control Plane (CLNS/ISIS)

- Use of nonIP addresses & routing protocol for whole core
- Only loopback interface gets (possibly private) IP address
- Doesn’t even need any filtering to block traffic to core interfaces
- Blocking of traffic to edge interfaces (peering/upstream/customers) with IP addresses still needs explicit ACLs
- Troubleshooting (ping/traceroute) harder or even impossible directly from/to core devices

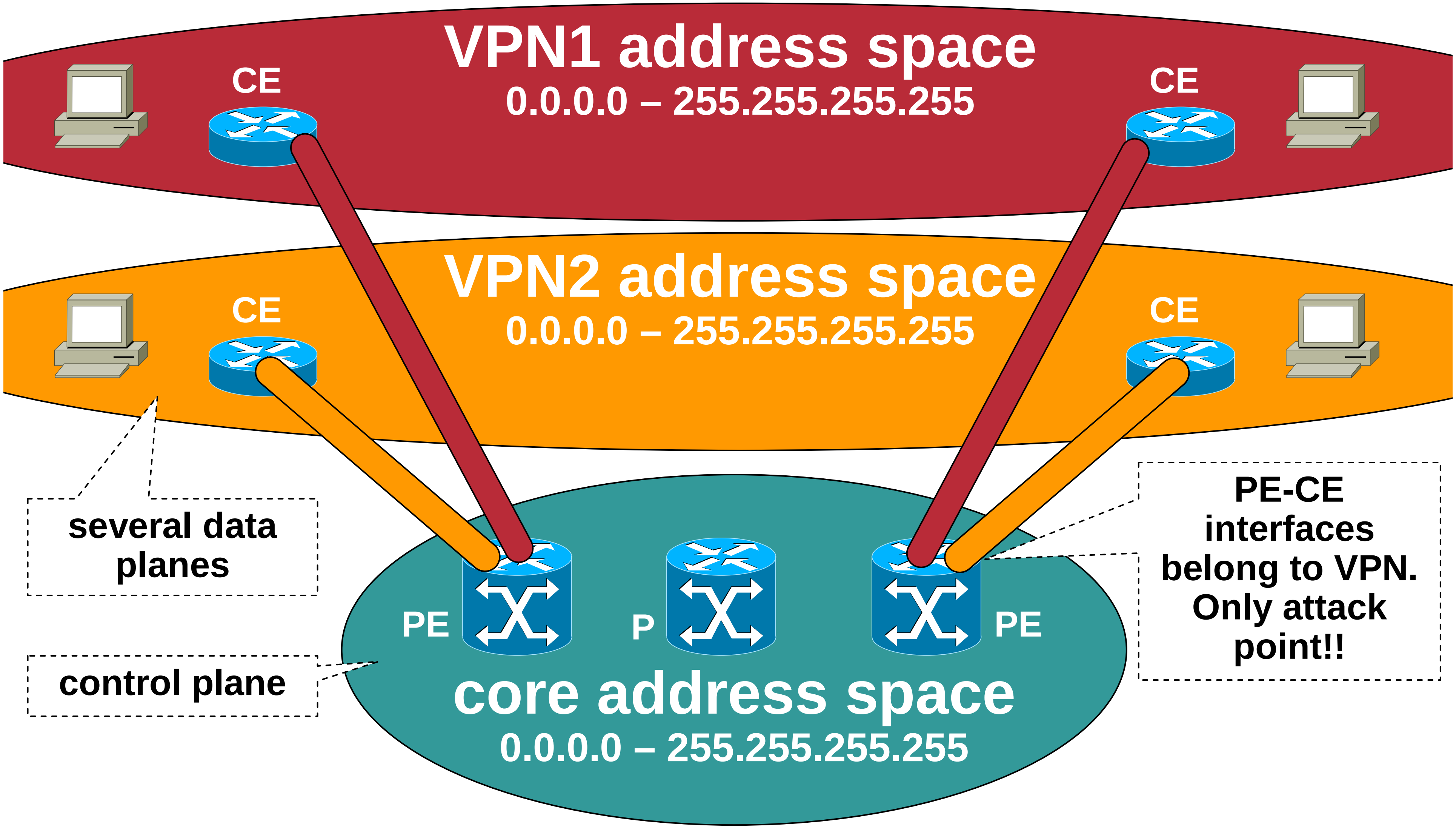
More Work Needed

Hiding of the MPLS Core Structure

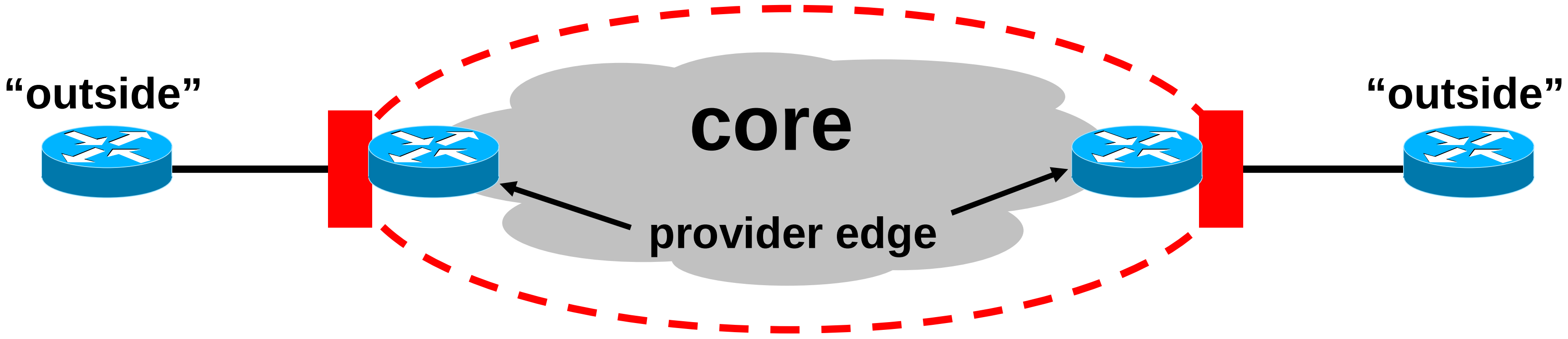


- VRF contains MPLS IPv4 addresses
- Only peering Interface (on PE) exposed (-> CE)!
  -> ACL or unnumbered

MPLS Core Hiding
Address Planes: True Separation!



Securing the Core: Infrastructure ACLs



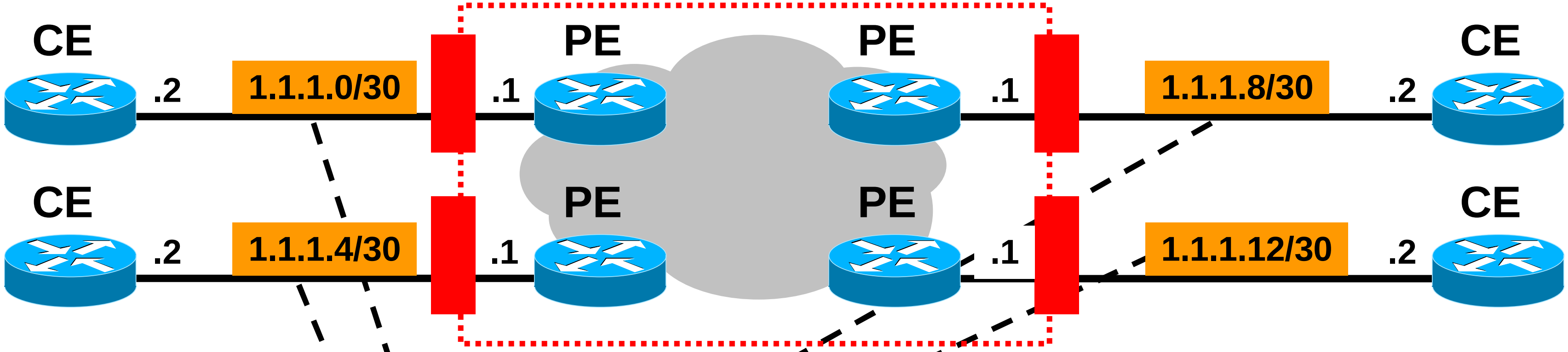
- On “PE”: “deny ip any <core address space>”

  some exceptions, e.g. routing protocol from host to host

- Idea: No traffic to core → you can’t attack
- Prevents intrusions 100%
- DoS: Very hard, only with transit traffic

Note: “PE” and “CE” are meant here as generic terms, not necessarily in the context of MPLS.

Securing the Core: Infrastructure ACLs



- **Example:**

  deny ip any 1.1.1.0 0.0.0.255

  permit ip any any

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

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

Example: Infrastructure ACL

```
! Deny our internal space as a source of external packets
    access-list 101 deny ip our_CIDR_block any
! Deny src addresses of 0.0.0.0 and 127/8
    access-list 101 deny ip host 0.0.0.0 any
    access-list 101 deny ip 127.0.0.0 0.255.255.255 any
! Deny RFC1918 space from entering AS
    access-list 101 deny ip 10.0.0.0 0.255.255.255 any
    access-list 101 deny ip 172.16.0.0 0.0.15.255 any
    access-list 101 deny ip 192.168.0.0 0.0.255.255 any
```

Example: Infrastructure ACL

! The only protocol that require infrastructure access is eBGP. Define both src and dst addresses

```
access-list 101 permit tcp host peerA host peerB eq 179
access-list 101 permit tcp host peerA eq 179 host peerB
```

! Deny all other access to infrastructure

```
access-list 101 deny ip any core_CIDR_block
```

! Permit all data plane traffic

```
access-list 101 permit ip any any
```

Infrastructure ACLs: Pros

Security against:

1. Operational mistakes (mis-configuration)
2. Bugs on the router (vulnerabilities)

- generally speaking, another layer of security around the core

Infrastructure ACLs: Cons

1. Breaks transparency: Access from the outside through pings, traceroute *into* the core does not work. (Note: traceroute across n/w works!)
2. As a consequence, makes troubleshooting harder: from the outside, and from the core (traceroute from core routers to outside)
3. hard to deploy if core address space is not contiguous, or not easily expressed in an ACL
4. hardware does not support line speed ACLs on all platforms
5. hard to maintain (when core address space changes)

Discussion

Infrastructure ACLs: Bug or Feature?

Core Hiding: The right way forward?