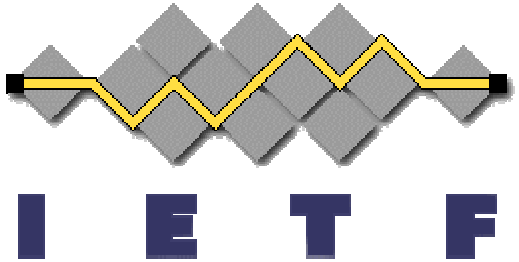


March 2002
Minneapolis

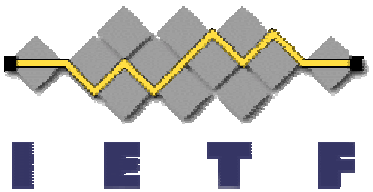
A Method to Signal and Provide Dynamic Routing in IPsec VPNs

draft-knight-ppvpn-ipsec-dynroute-00.txt

Paul Knight **paknight@nortelnetworks.com**
Bryan Gleeson **bryan@tahoenetworks.com**

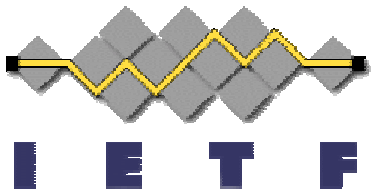
I-D Overview

- **Describes an implementation of IIPtran, as described in draft-touch-ipsec-vpn-03.txt**
- **IPsec "routing problem" and basic solution**
- **Description of method of carrying routing updates**
  - comparison to some other methods (GRE)
  - corrects misconceptions on carrying routing protocols using broadcast or multicast in IPsec
- **Positioning in PPVPN:**
  - CE-CE IPsec VPN – FRAMEWORK: draft-ietf-ppvpn-ce-based-01.txt
  - Provider-Provisioned



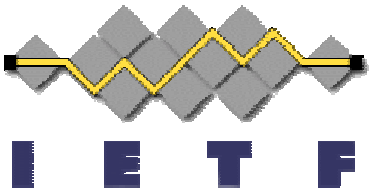
The IPsec “routing problem”

- **Usual conversation:**
  - What’s the problem? You can already carry routing protocols over IPsec.
  - Yes, but you can’t actually use them to ROUTE.
  - Huh?
  - The IPsec Security Associations have selectors that determine the traffic they allow. They are like static routes.
  - Oh… Yeah… I see the problem.

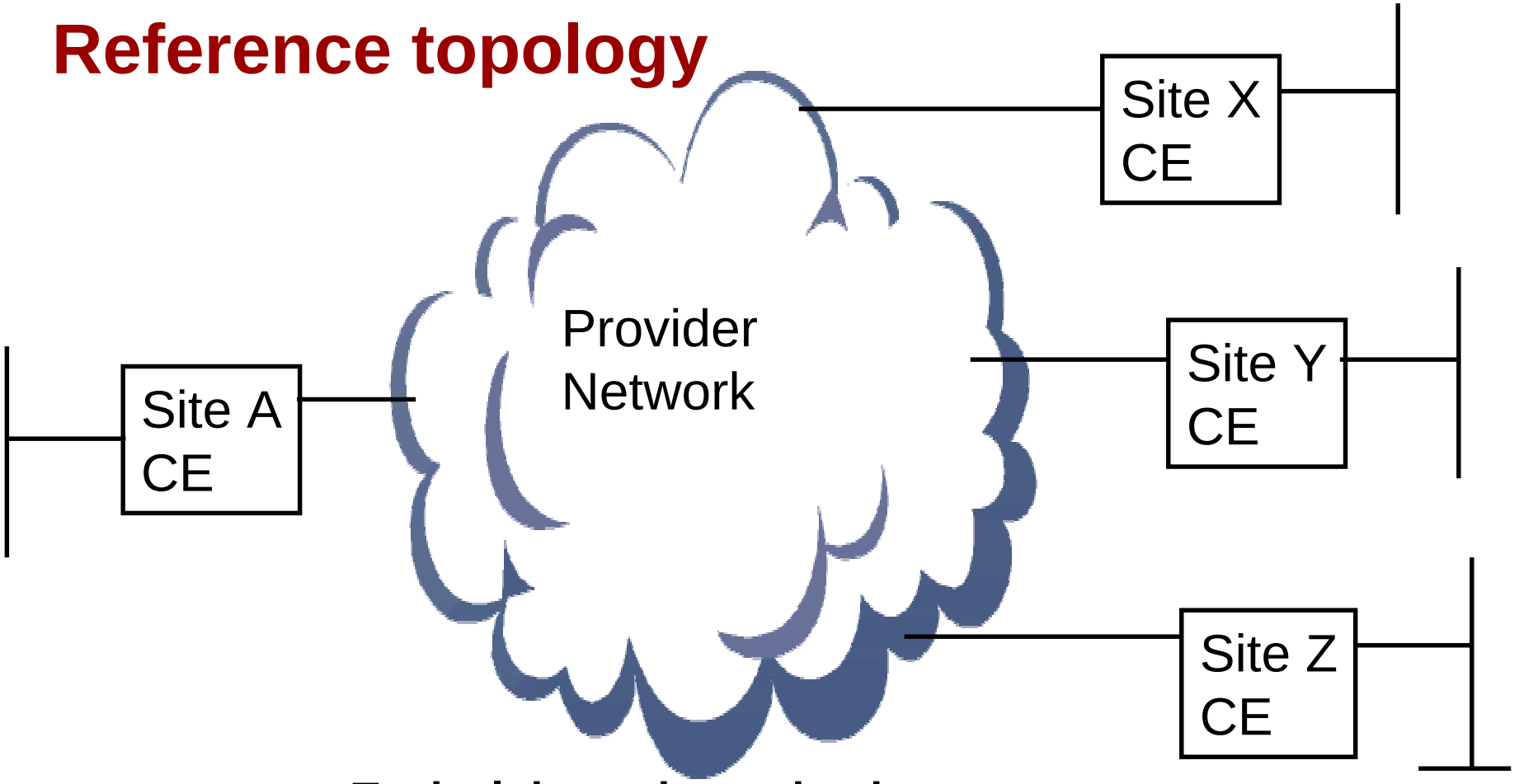


The IPsec “routing problem”

- **Dynamic routing in VPNs is a requirement**
- **Tunnel mode is incompatible with dynamic routing**
  - draft-touch-ipsec-vpn-03.txt
  - draft-wang-cevpn-routing-00.txt
- **WHY? Security Associations are created with selectors → Tunnels have built-in “static routes”**
- **SA Database lookup does the “routing”**
- **SA setup is orders of magnitude slower than routing change →Dynamically changing SA due to routing updates doesn’t scale**

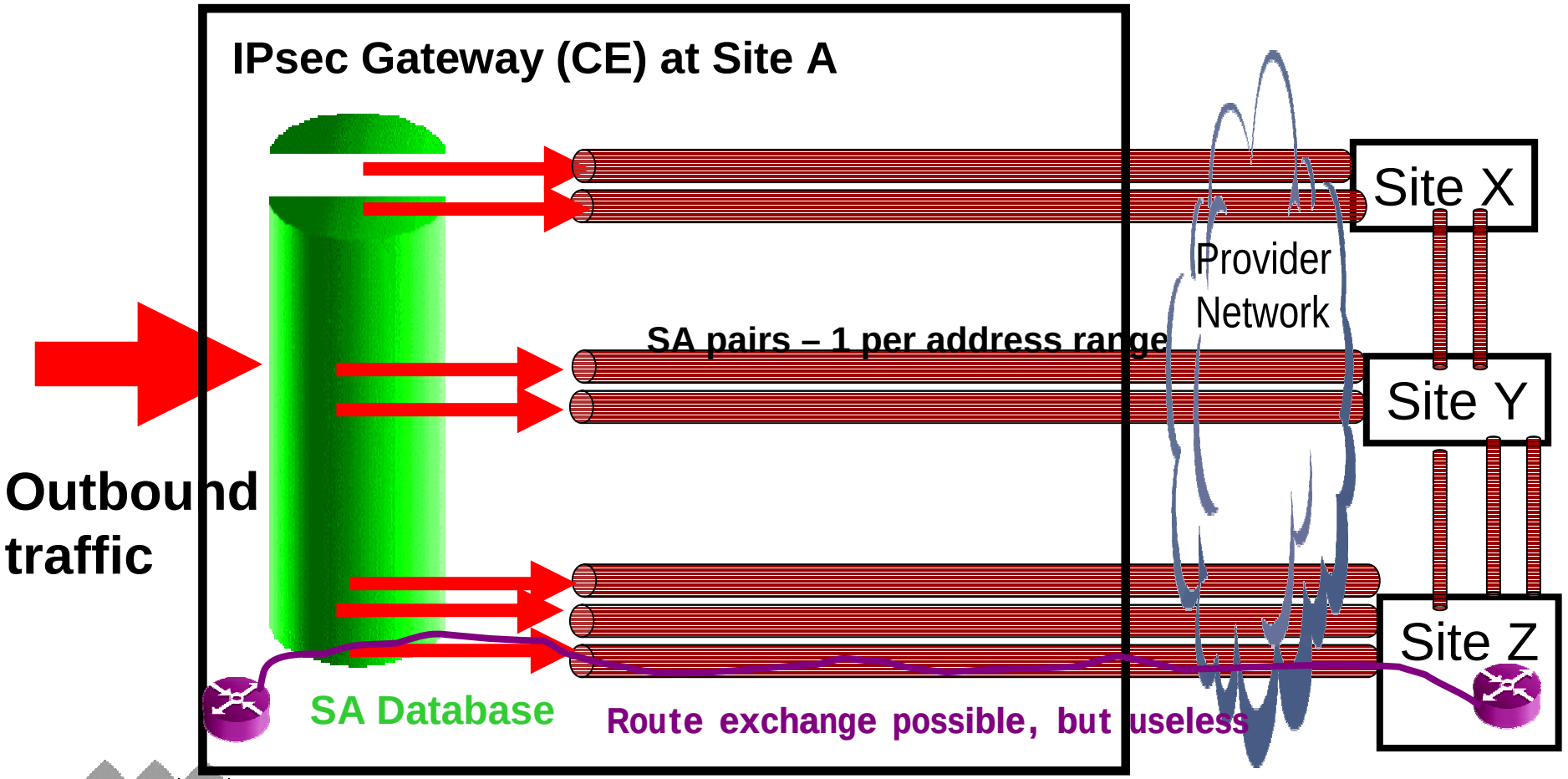


Reference topology



- **Typical dynamic routing issues**
  - "Z" adds a new network
  - New site added (Hub/spoke model)
  - A link (IPsec connection) breaks

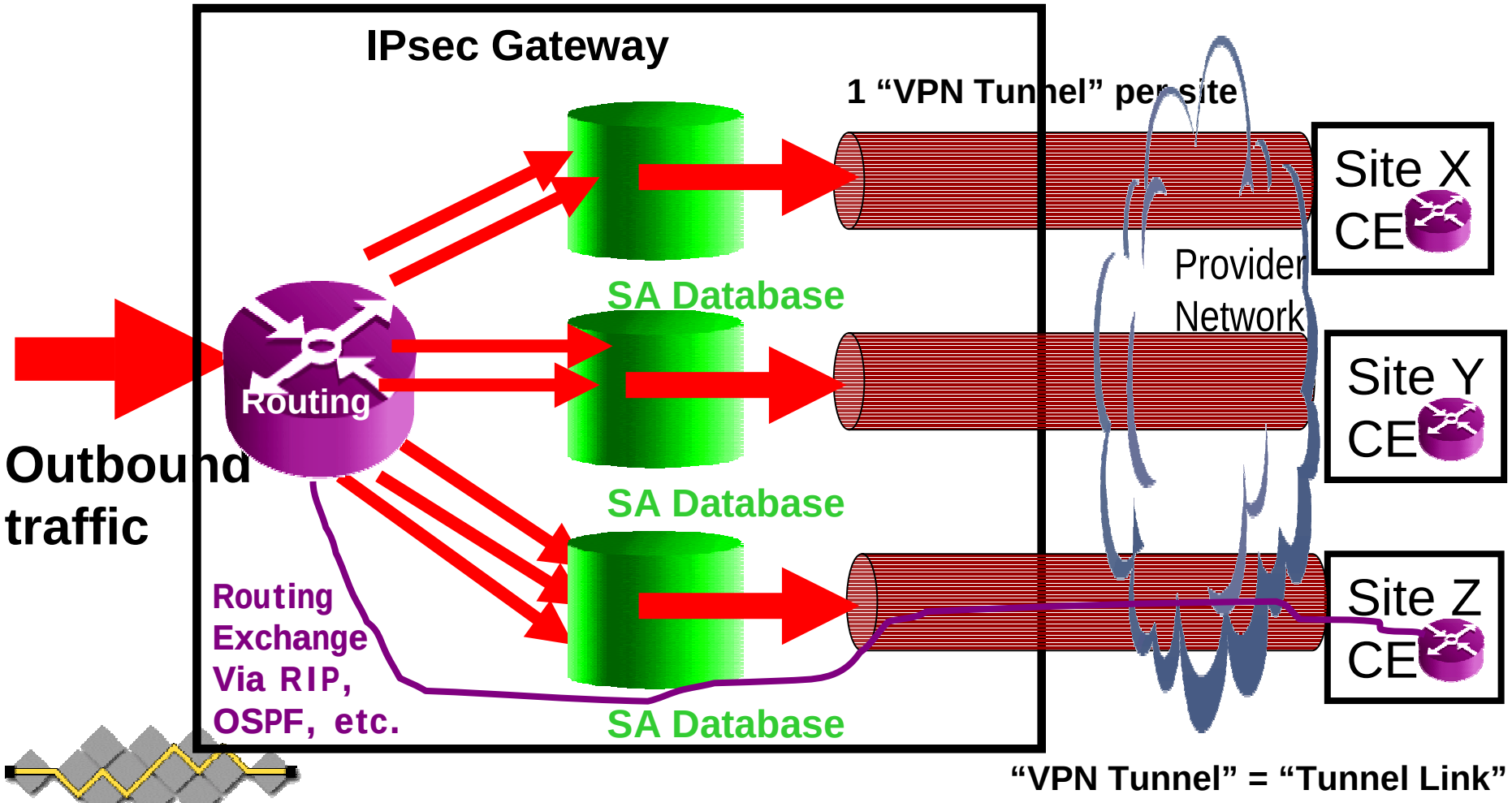
SA Database Determines “routing” into tunnels – Cannot adapt



The basic solution

- **Remove the tunnel's "static route" …. HOW?**
- **(1) Use "wild card" in tunnel SAs (allow all traffic) OR**
- **(2) Use encapsulation to make the traffic fit the "static route", by setting destination address in the encapsulated traffic**
  - Generic Routing Encapsulation (GRE) or L2TP
  - IP-in-IP over Transport (IIPtran)
- **Both approaches are essentially similar in key ways**
- **Either way, you must do "routing" (SA selection or encapsulation addressing) outside IPsec, and push traffic into a "VPN Tunnel" (may be transport)**

Routing outside IPsec



Related IPsec developments as of Wednesday, March 20

- **RFC 2401bis**
  - Being updated by Steve Kent et al.
  - Discusses routing before/after IPsec application
  - How it affects transport/tunnel mode
  - Should clarify the use of encapsulation within transport mode between gateways
- **Draft-touch-ipsec-vpn-04.txt will be submitted as informational RFC**
  - This draft (dynroute) is an implementation demonstrating the methods of IIPtran

Future steps

- **This draft will provide input into forthcoming CE-CE IPsec PPVPN documents**
  - Clarify routing issues discussion
  - Comparing encapsulation methods
- **It will provide implementation proof and applicability demonstration for “Touch” draft, moving toward Informational RFC**
- **Questions ????**
- **Now (time permitting) Professor Touch can discuss his draft**