RANGER, VET, SEAL and IRON

IETF77
Fred L. Templin
fred.l.templin@boeing.com

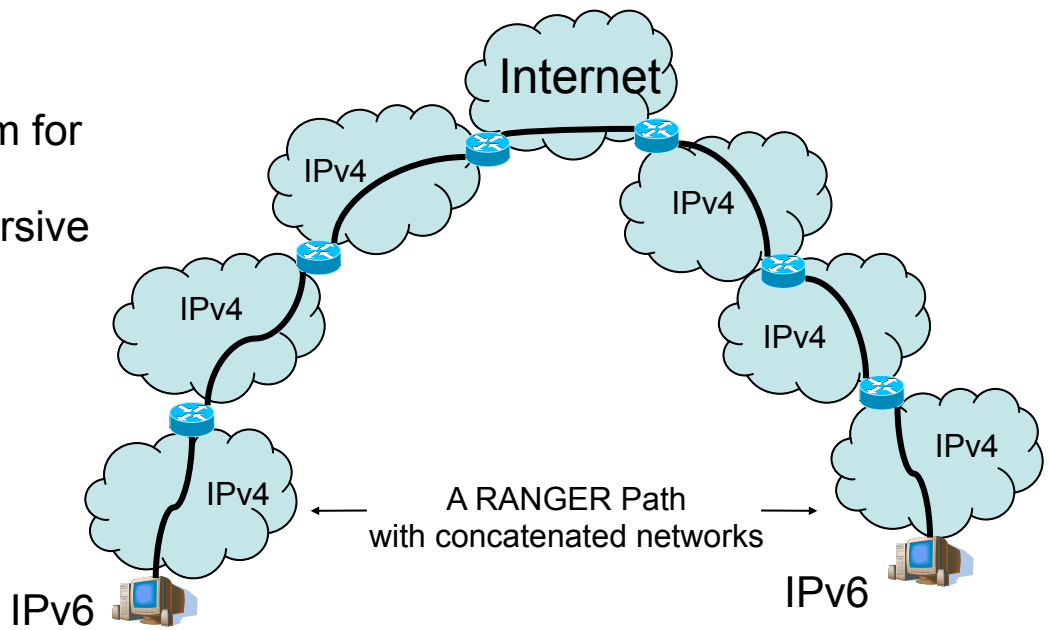
Routing and Addressing in Networks with Global Enterprise Recursion (RANGER) – RFC5720

- Recursively-nested connected local network regions joined by Enterprise Border Routers (EBRs) – a network-of-networks
- each distinct local network region is an “enterprise” unto itself
- PI and PA addressing, multihoming, traffic engineering, etc.
- PI prefixes are *portable* - no need for autoconfiguration
- example use cases:
  - Internet interdomain core
  - large academic campus network
  - corporate enterprise network
  - ISP networks
  - SOHO networks
  - civil aviation networks
  - Mobile Ad-hoc Networks

How RANGER Works

- **RANGER "concatenates" networks with recursive re-encapsulation**
- **Example: IPv4 for local routing and addressing; IPv6 for global routing and addressing (other IPvX/IPvY combinations also supported)**

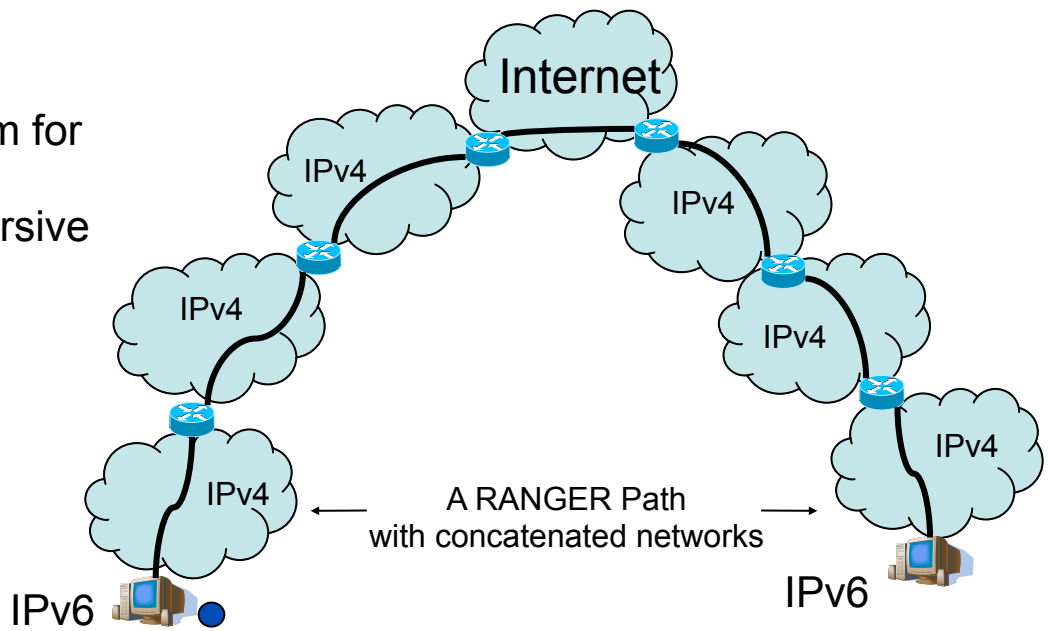
•Routing scaling through local routing regions (RLOCs) with mapping system for global addresses (EIDs)
•Global communications through recursive re-encapsulation across local routing regions (EIDs)
•VET and SEAL



How RANGER Works

- **RANGER "concatenates" networks with recursive re-encapsulation**
- **Example: IPv4 for local routing and addressing; IPv6 for global routing and addressing (other IPvX/IPvY combinations also supported)**

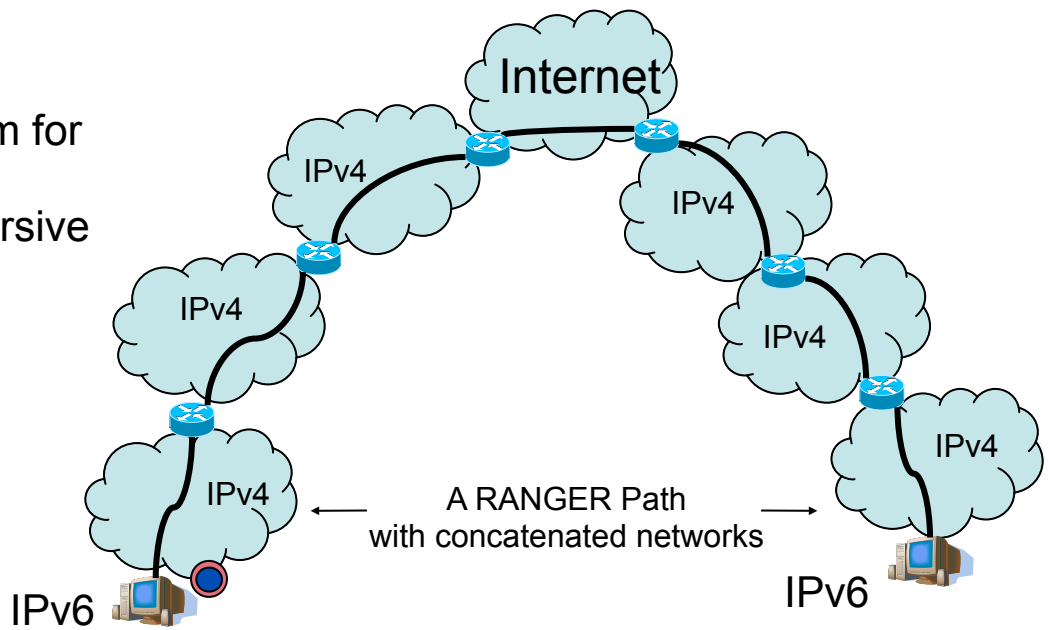
•Routing scaling through local routing regions (RLOCs) with mapping system for global addresses (EIDs)
•Global communications through recursive re-encapsulation across local routing regions (EIDs)
•VET and SEAL



How RANGER Works

- **RANGER "concatenates" networks with recursive re-encapsulation**
- **Example: IPv4 for local routing and addressing; IPv6 for global routing and addressing (other IPvX/IPvY combinations also supported)**

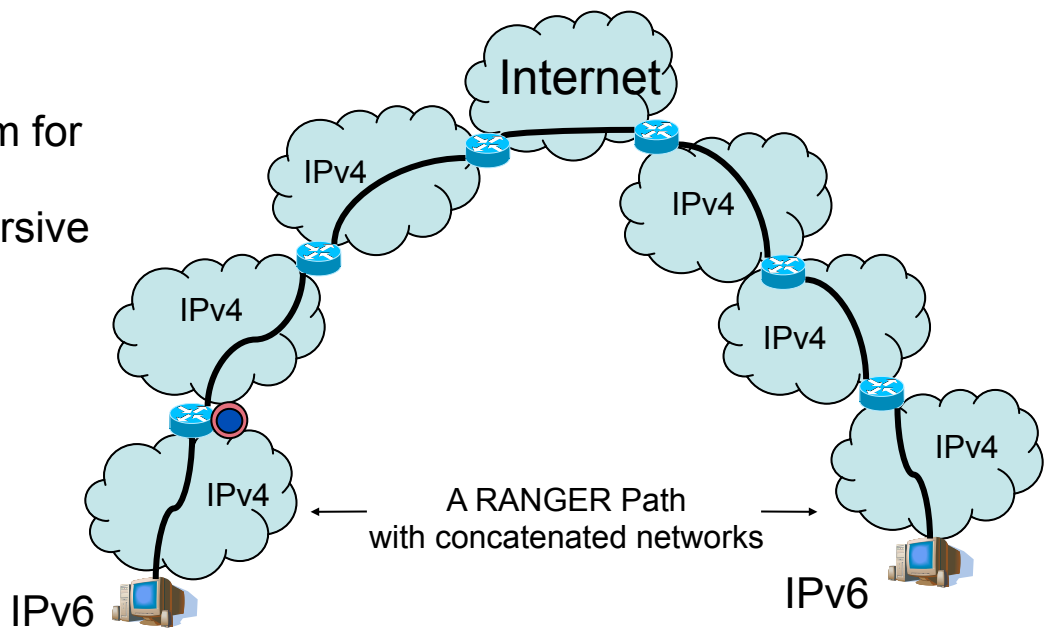
•Routing scaling through local routing regions (RLOCs) with mapping system for global addresses (EIDs)
•Global communications through recursive re-encapsulation across local routing regions (EIDs)
•VET and SEAL



How RANGER Works

- **RANGER "concatenates" networks with recursive re-encapsulation**
- **Example: IPv4 for local routing and addressing; IPv6 for global routing and addressing (other IPvX/IPvY combinations also supported)**

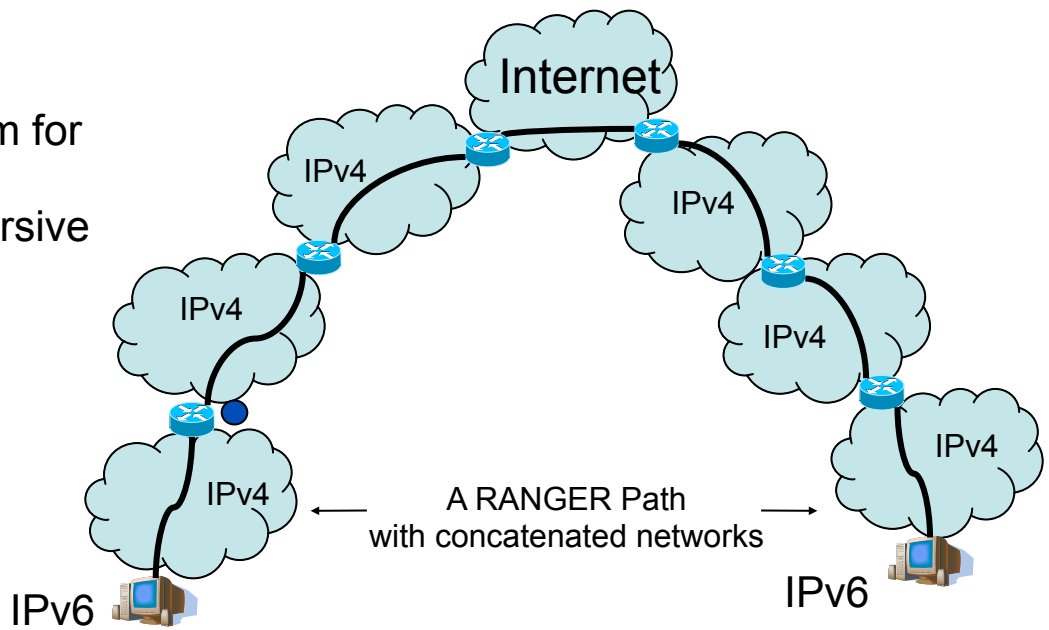
•Routing scaling through local routing regions (RLOCs) with mapping system for global addresses (EIDs)
•Global communications through recursive re-encapsulation across local routing regions (EIDs)
•VET and SEAL



How RANGER Works

- **RANGER "concatenates" networks with recursive re-encapsulation**
- **Example: IPv4 for local routing and addressing; IPv6 for global routing and addressing (other IPvX/IPvY combinations also supported)**

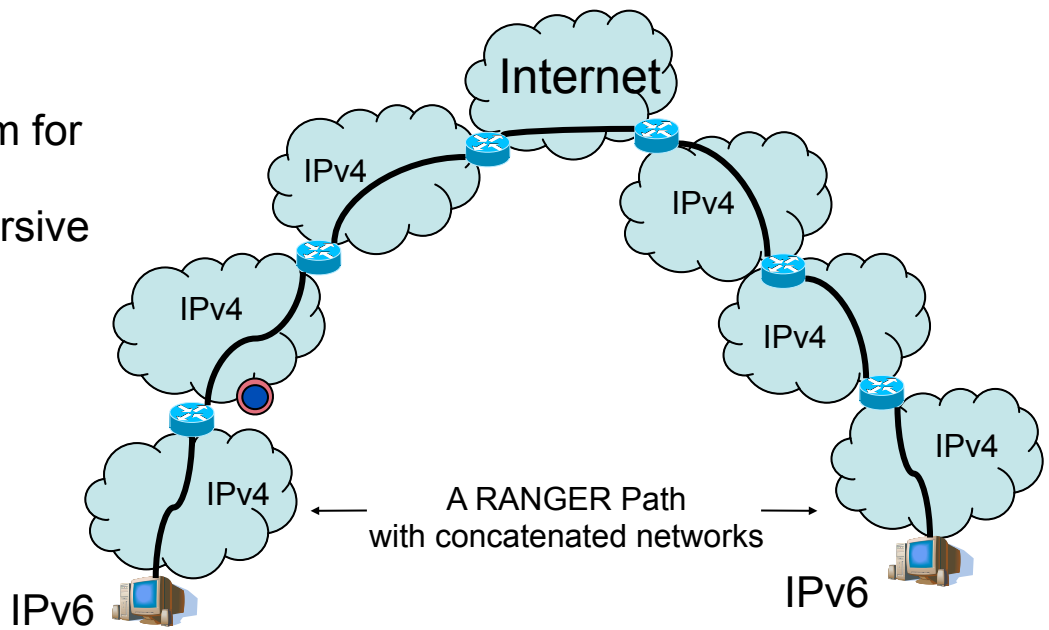
•Routing scaling through local routing regions (RLOCs) with mapping system for global addresses (EIDs)
•Global communications through recursive re-encapsulation across local routing regions (EIDs)
•VET and SEAL



How RANGER Works

- **RANGER "concatenates" networks with recursive re-encapsulation**
- **Example: IPv4 for local routing and addressing; IPv6 for global routing and addressing (other IPvX/IPvY combinations also supported)**

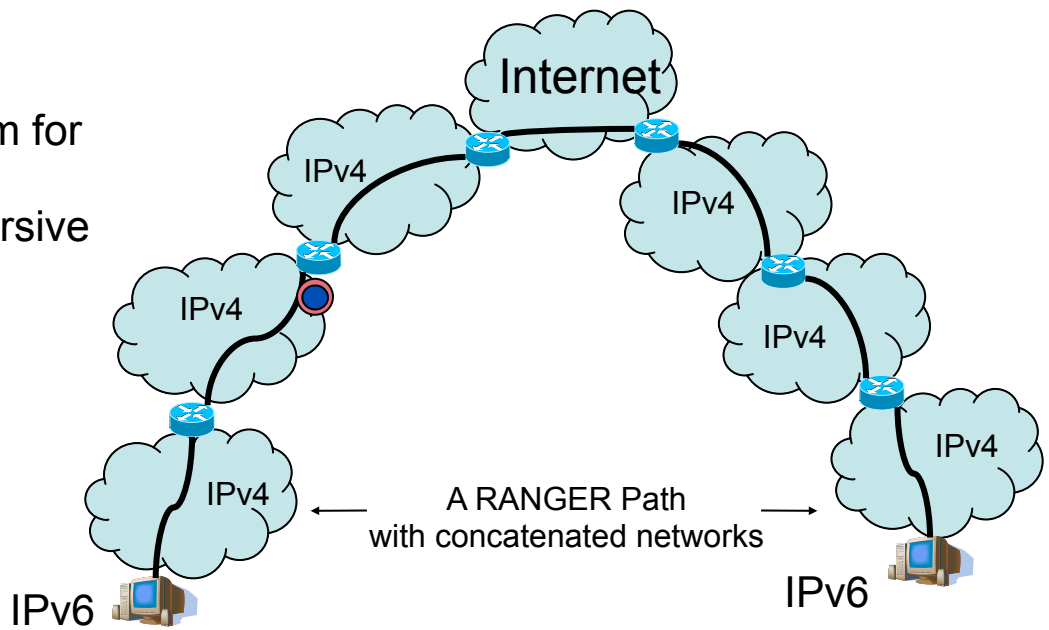
•Routing scaling through local routing regions (RLOCs) with mapping system for global addresses (EIDs)
•Global communications through recursive re-encapsulation across local routing regions (EIDs)
•VET and SEAL



How RANGER Works

- **RANGER "concatenates" networks with recursive re-encapsulation**
- **Example: IPv4 for local routing and addressing; IPv6 for global routing and addressing (other IPvX/IPvY combinations also supported)**

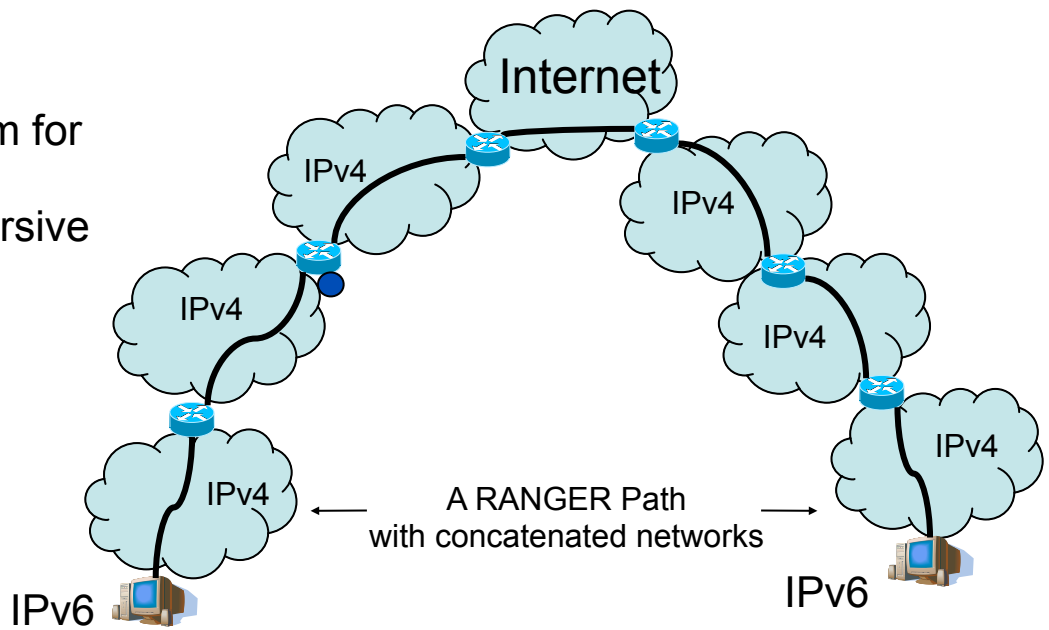
•Routing scaling through local routing regions (RLOCs) with mapping system for global addresses (EIDs)
•Global communications through recursive re-encapsulation across local routing regions (EIDs)
•VET and SEAL



How RANGER Works

- **RANGER "concatenates" networks with recursive re-encapsulation**
- **Example: IPv4 for local routing and addressing; IPv6 for global routing and addressing (other IPvX/IPvY combinations also supported)**

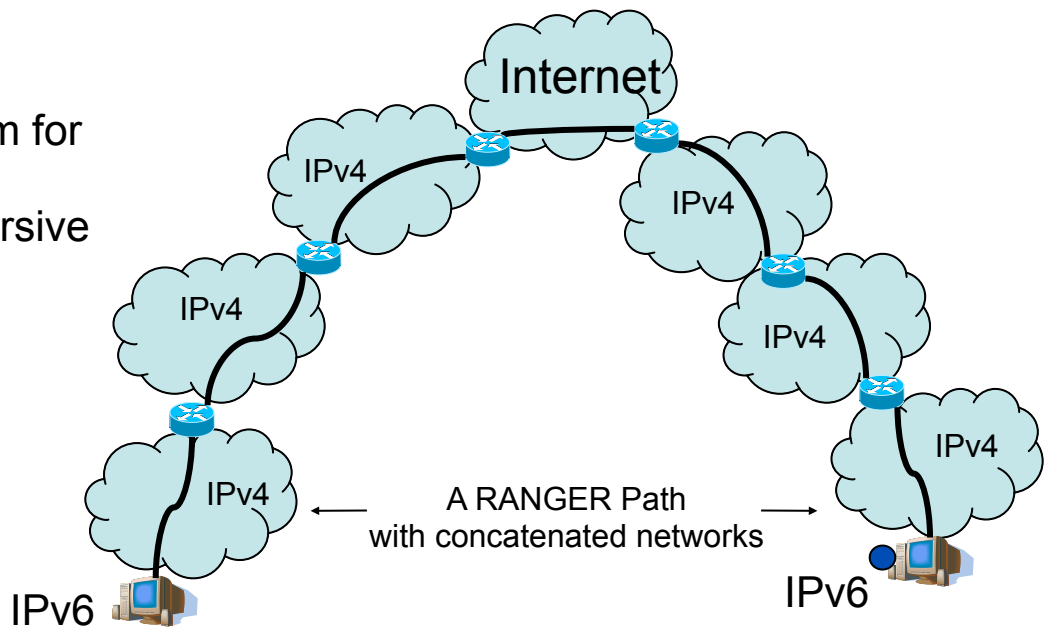
•Routing scaling through local routing regions (RLOCs) with mapping system for global addresses (EIDs)
•Global communications through recursive re-encapsulation across local routing regions (EIDs)
•VET and SEAL



How RANGER Works

- **RANGER "concatenates" networks with recursive re-encapsulation**
- **Example: IPv4 for local routing and addressing; IPv6 for global routing and addressing (other IPvX/IPvY combinations also supported)**

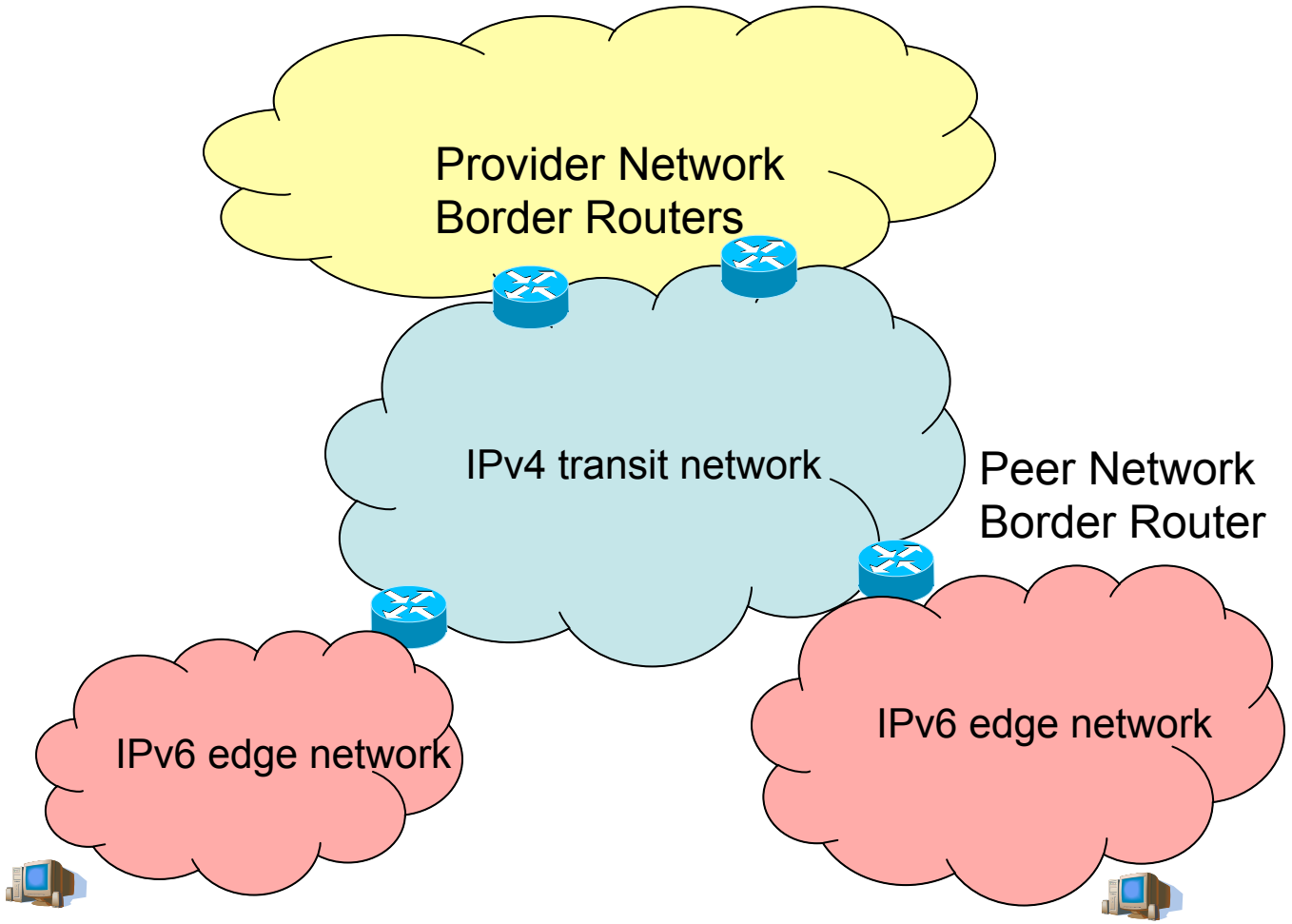
•Routing scaling through local routing regions (RLOCs) with mapping system for global addresses (EIDs)
•Global communications through recursive re-encapsulation across local routing regions (EIDs)
•VET and SEAL



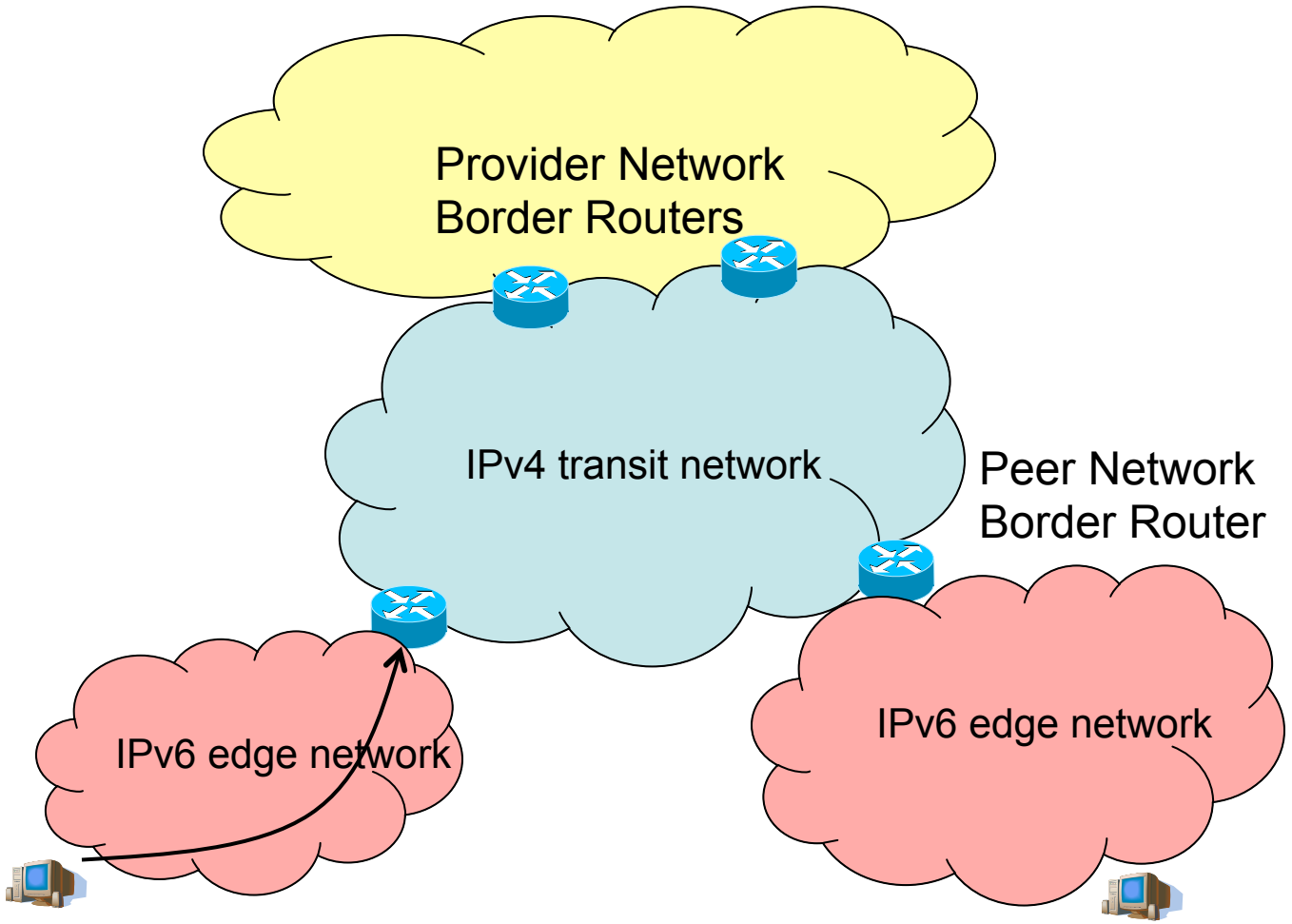
Virtual Enterprise Traversal (VET) – RFC5558

- Traversal of a single network within the recursive nesting
- Automatic point-to-multipoint tunneling (NBMA)
- Discover enterprise network exit routers:
  - default routes through border routers on provider networks
  - more-specific routes through border routers on peer networks
  - Secure Redirection
- Router-to-router tunneling
- Only border routers are modified
- Version 2 of ISATAP

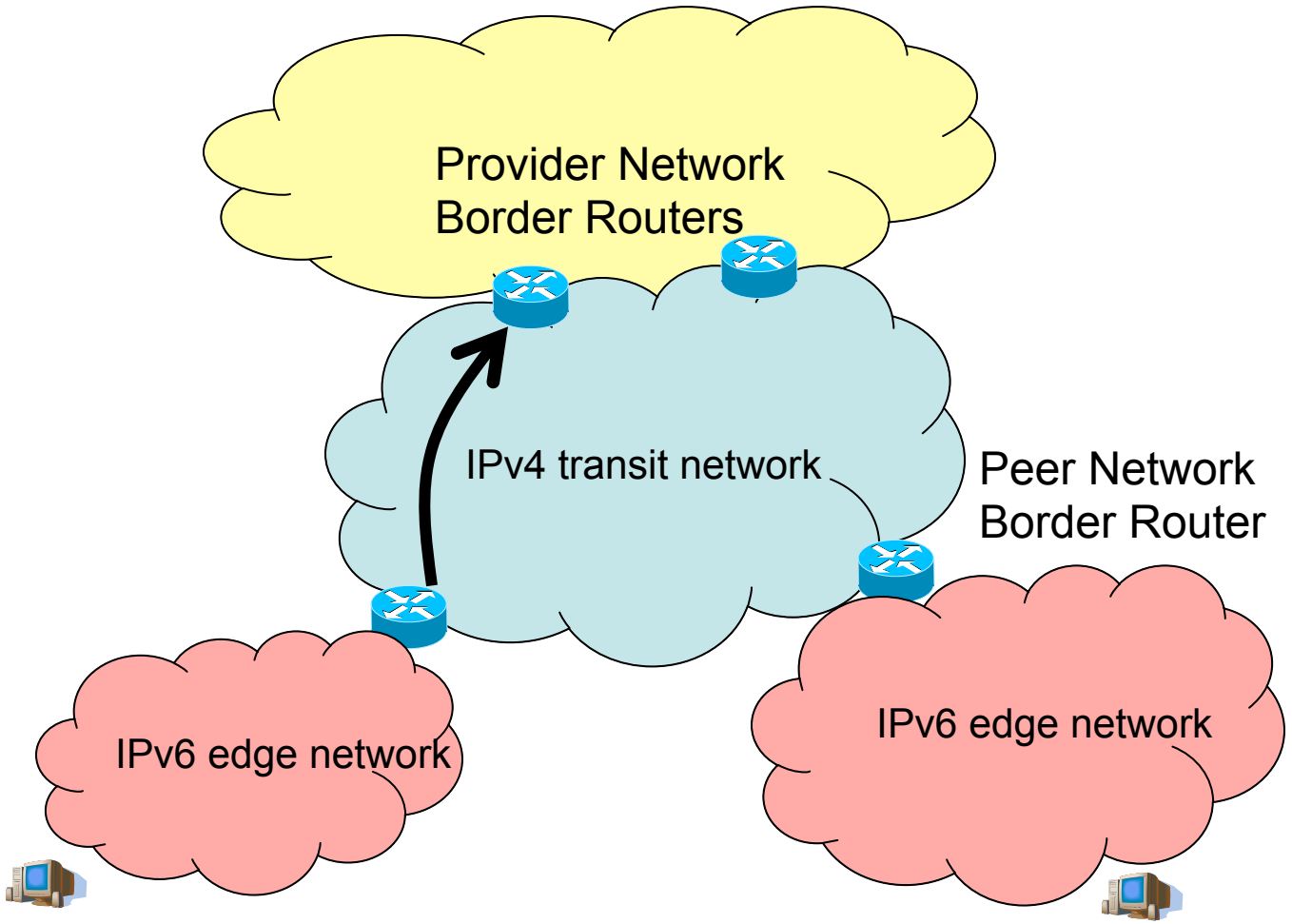
How VET Works



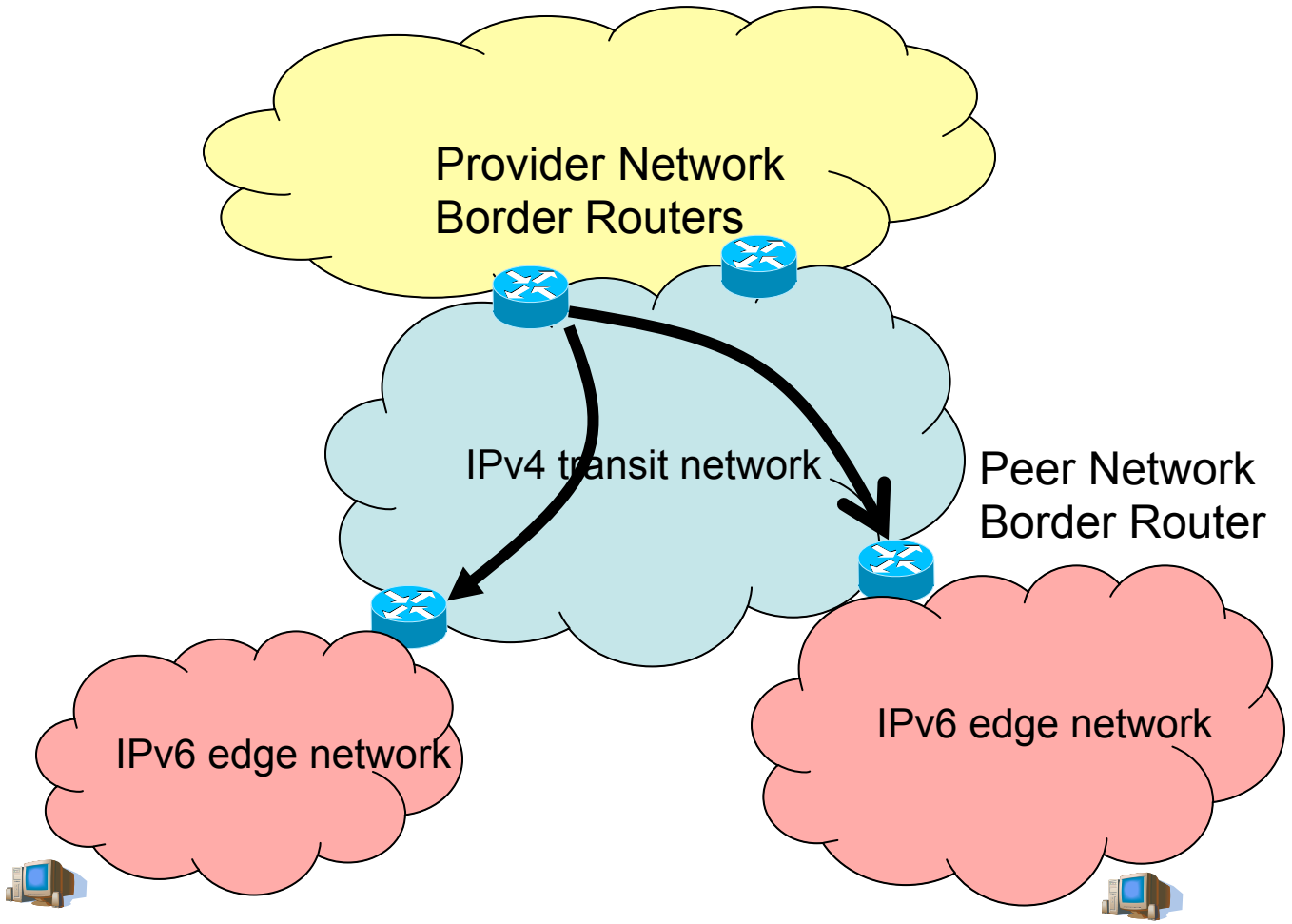
How VET Works



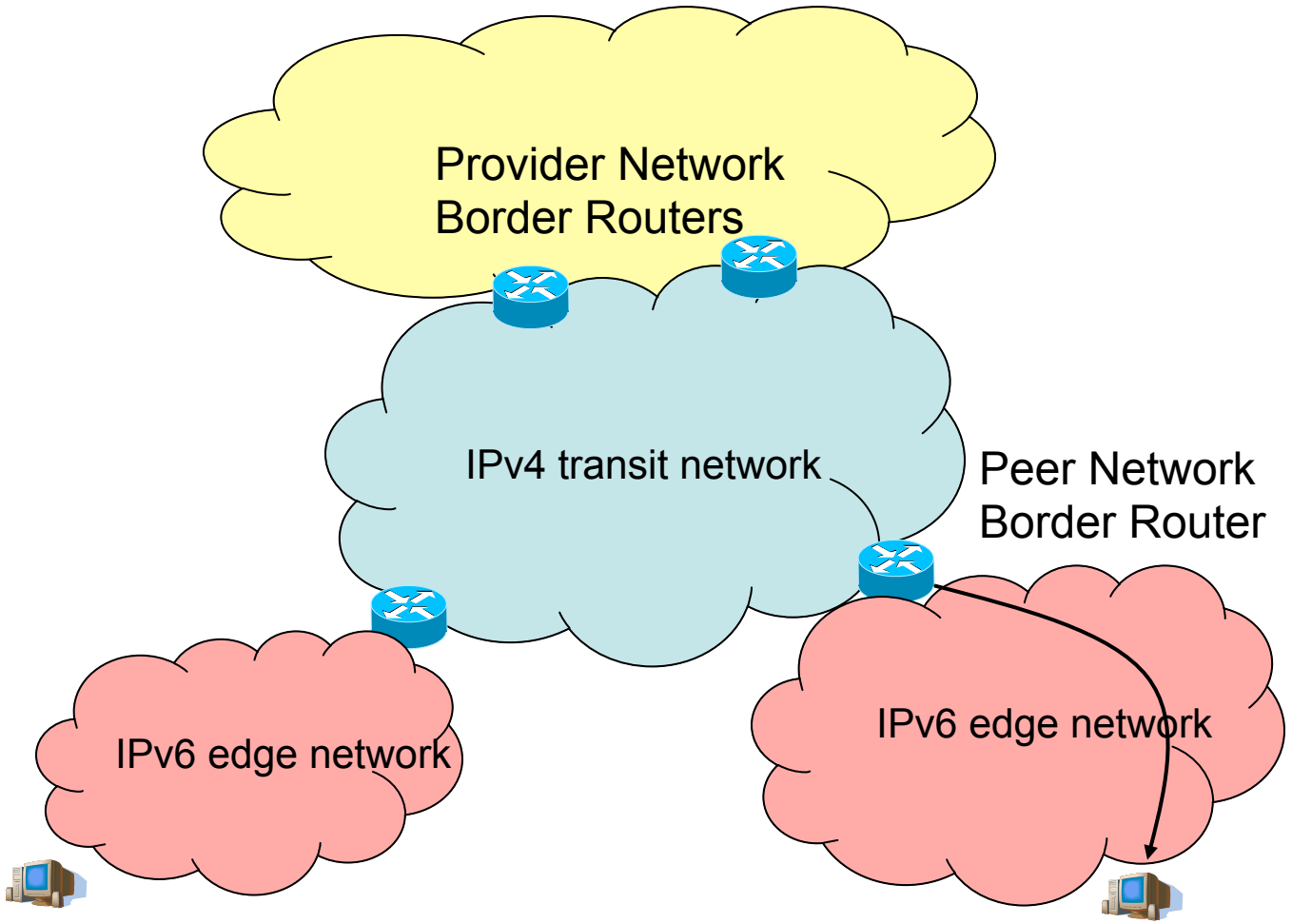
How VET Works



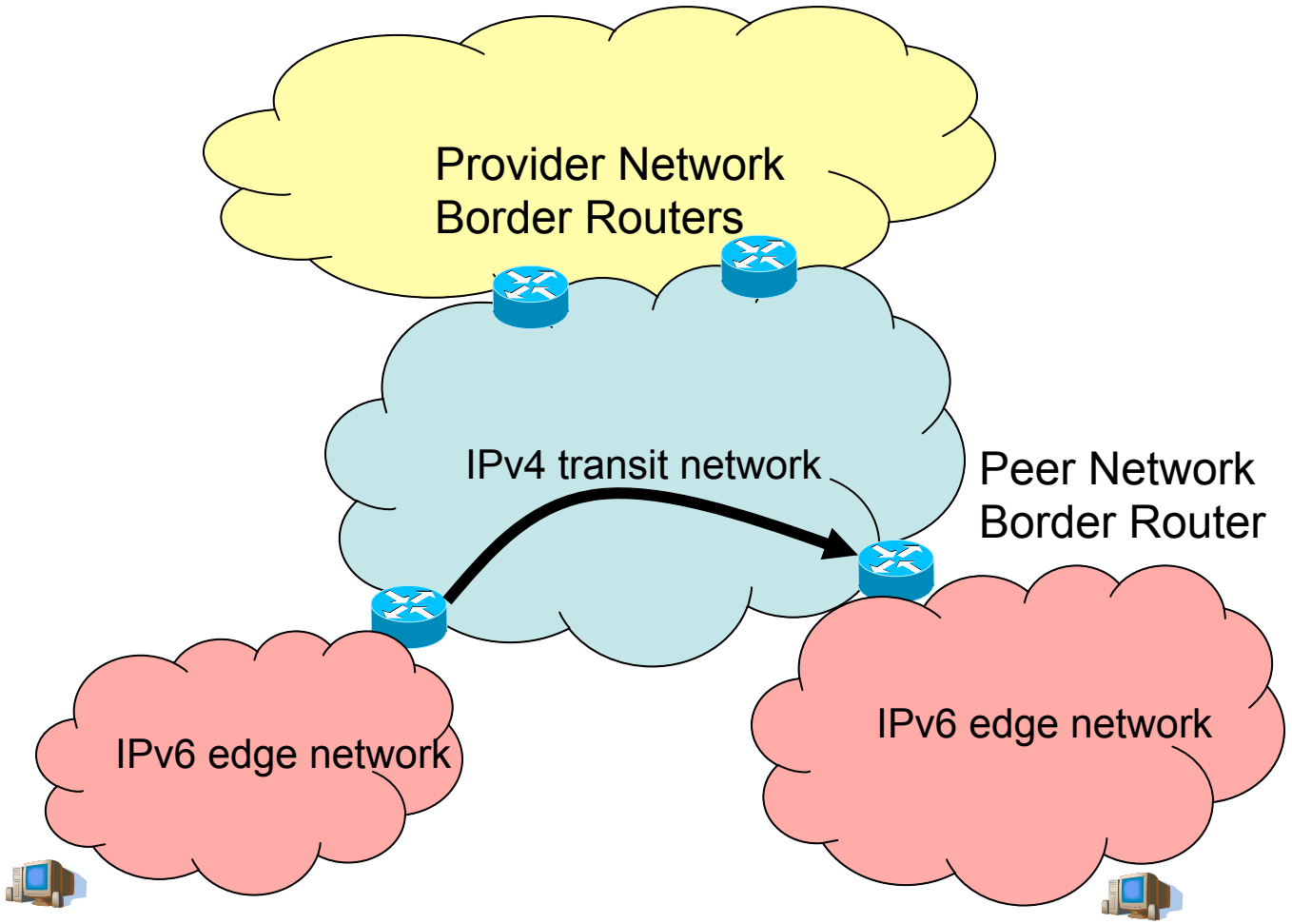
How VET Works



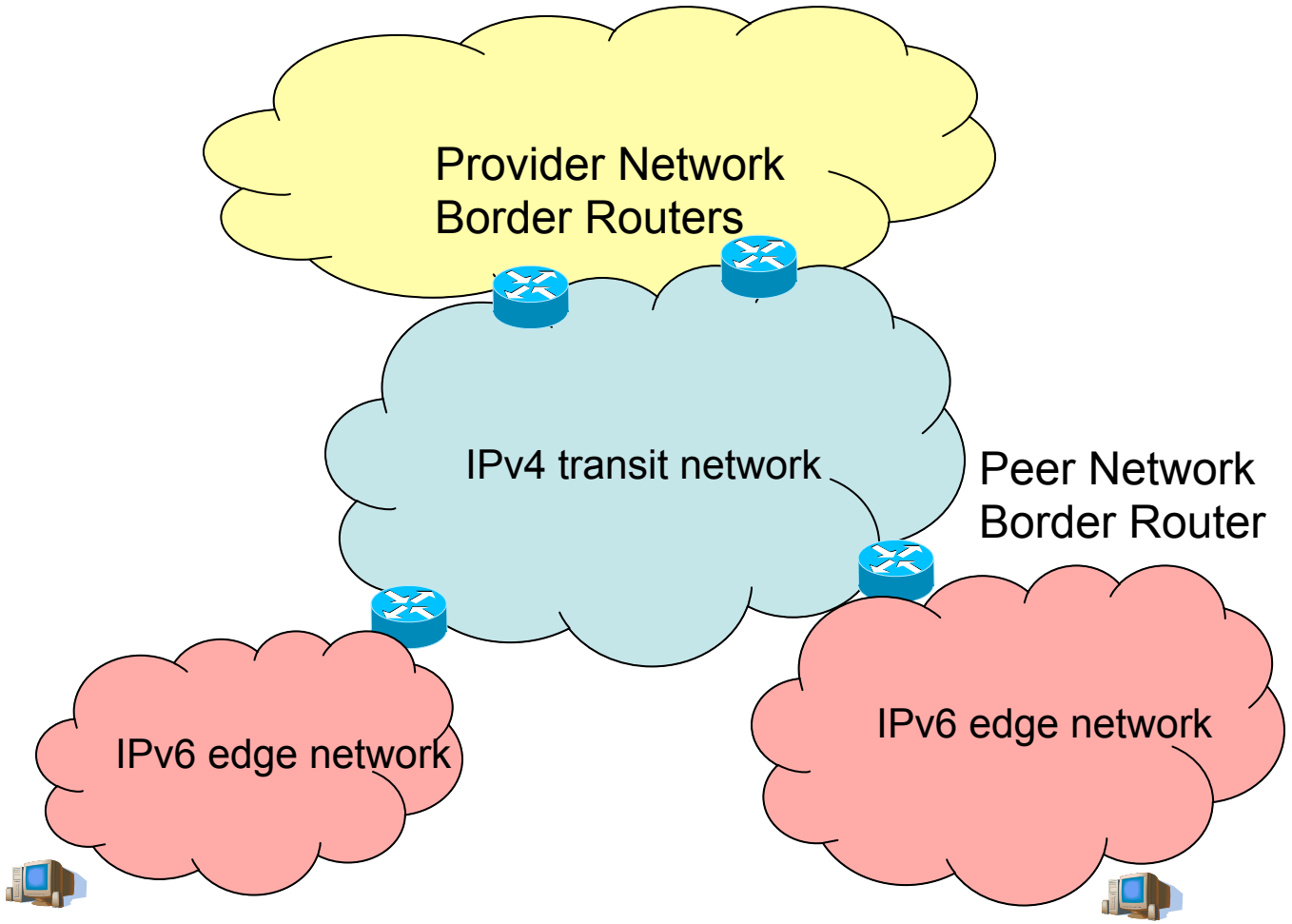
How VET Works



How VET Works



How VET Works

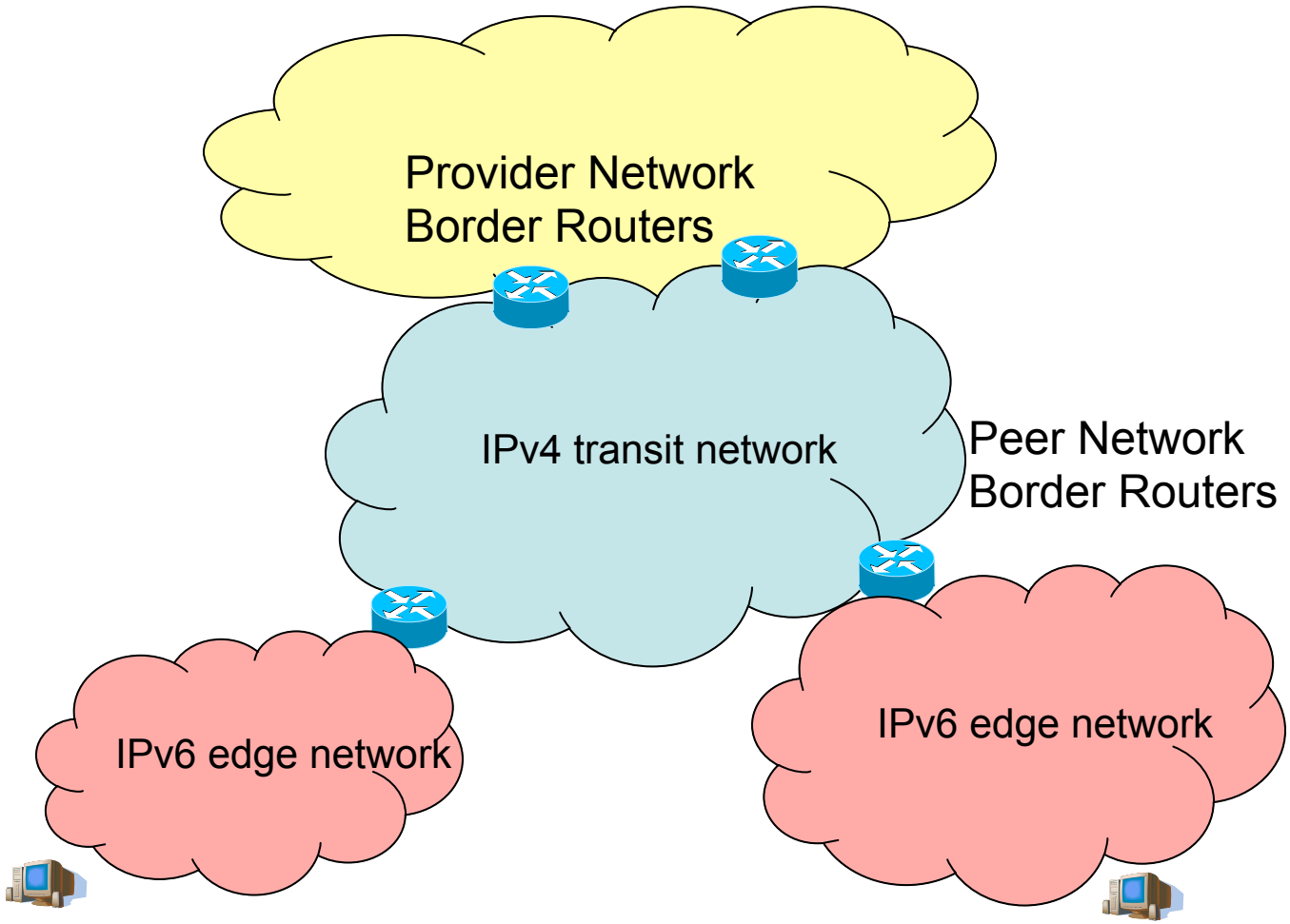


Subnetwork Encapsulation and Adaptation Layer (SEAL) – RFC5320

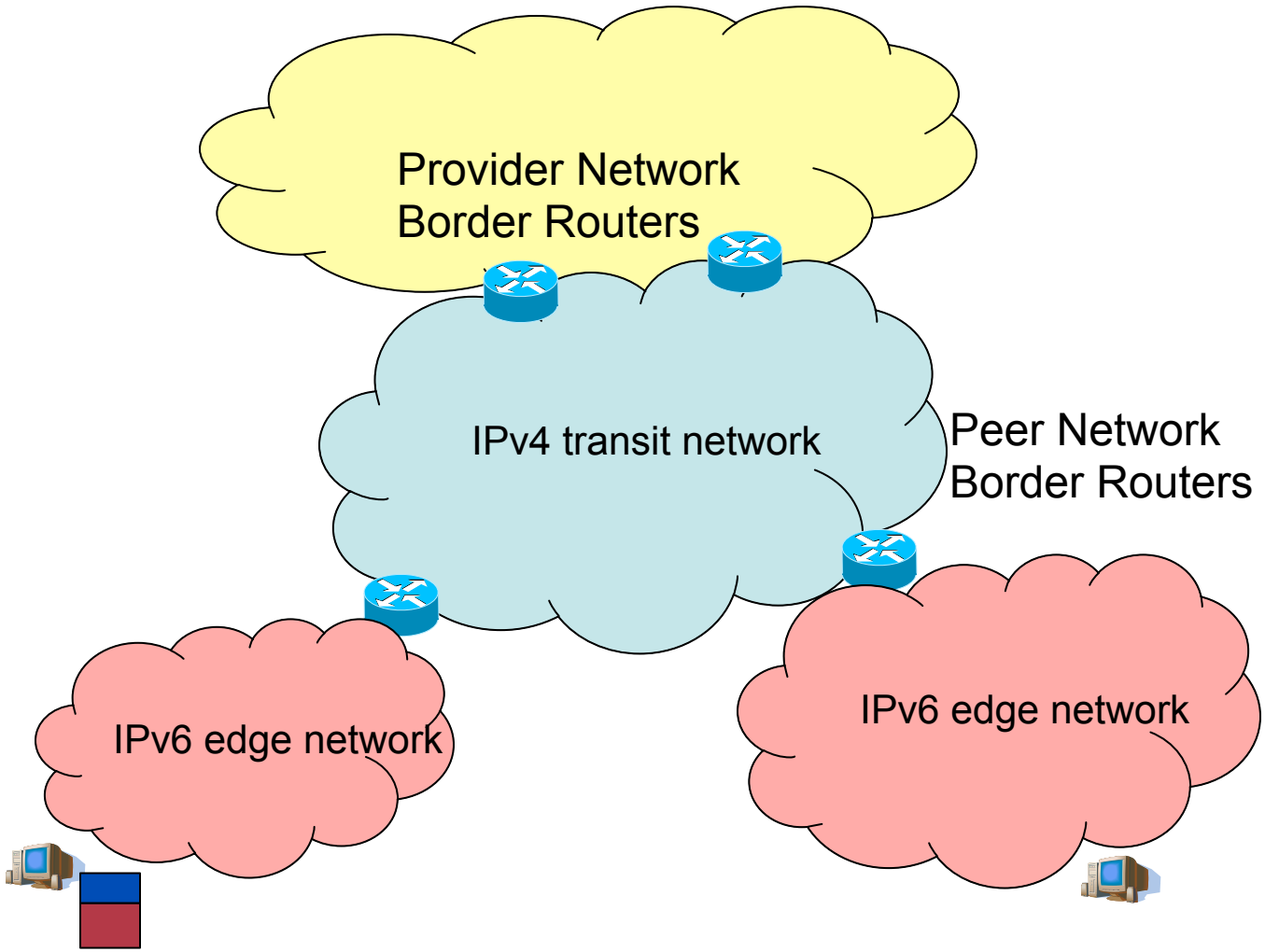
- tunnel encapsulation overhead reduces path MTU
- avoid path MTU discovery if possible due to unnecessary packet loss; black-holing due to ICMP filtering
- have the tunnel do transparent link-layer adaptation
- tunnel ingress discovers MRU of tunnel egress
- end result is 1500 and larger gets through

- SEAL supports synchronization between tunnel endpoints, so off-path DOS attacks are prevented
- SEAL also supports “semi-stateless” mode with no fragmentation/reassembly but robust MTU discovery

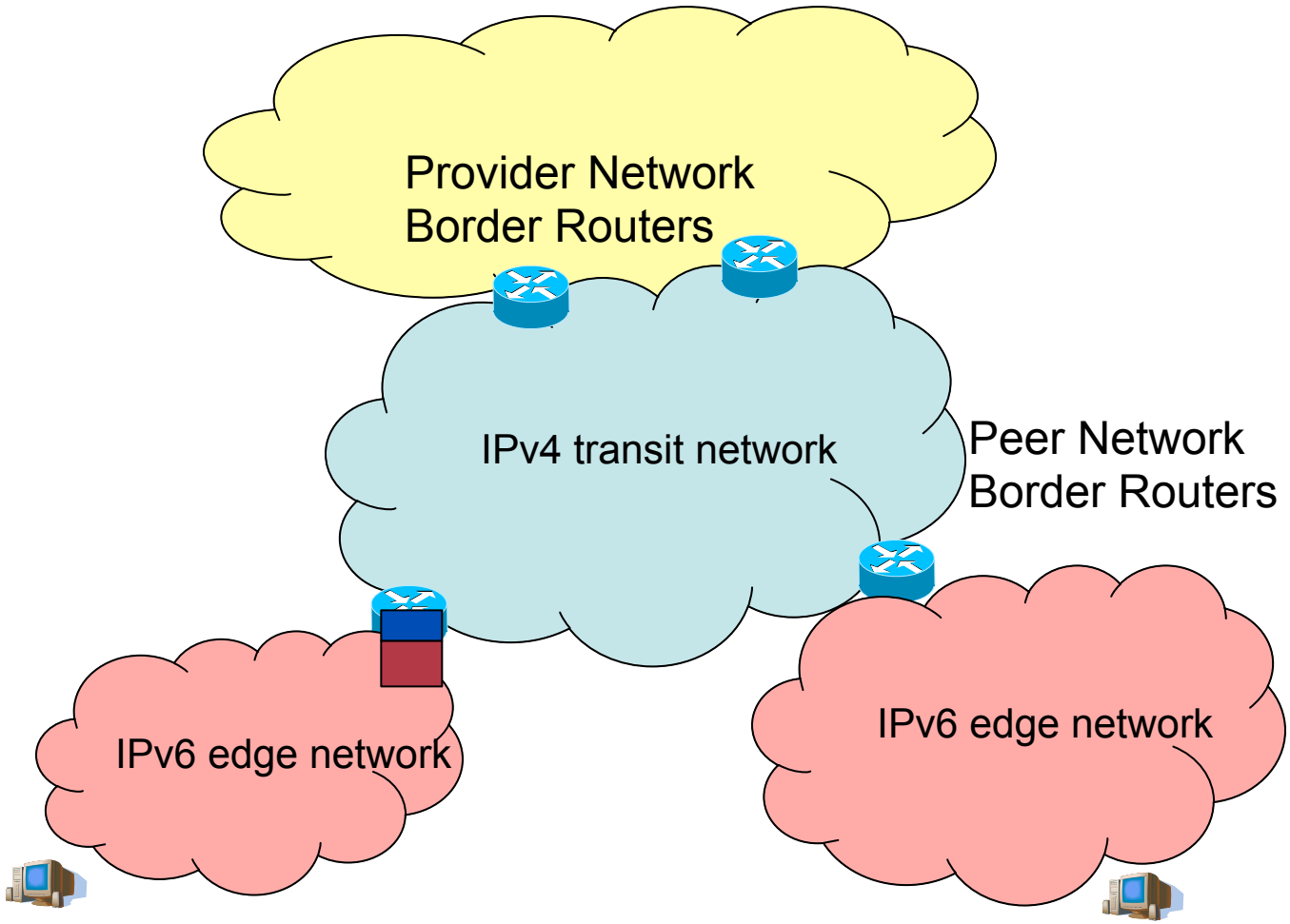
How SEAL Works



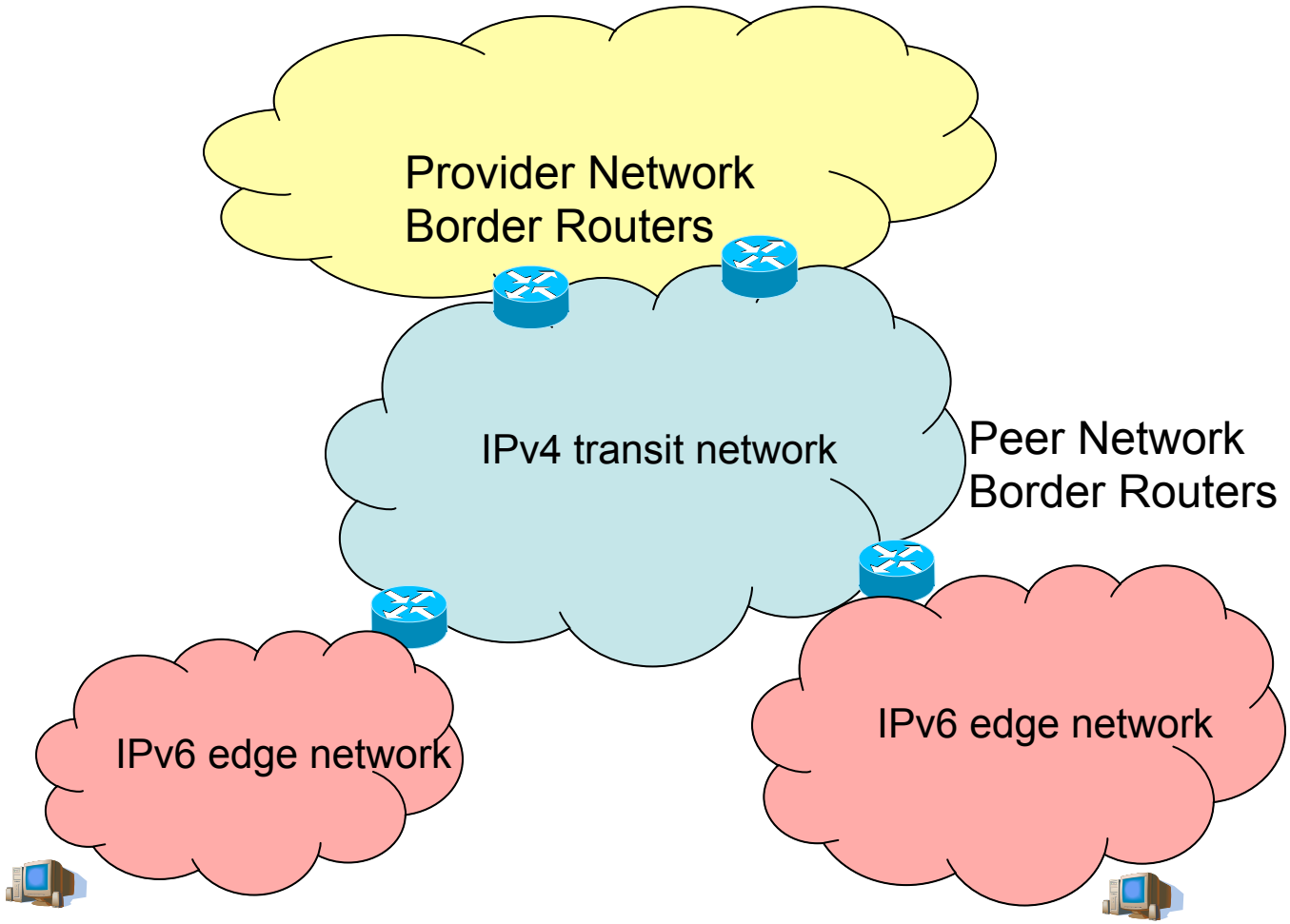
How SEAL Works



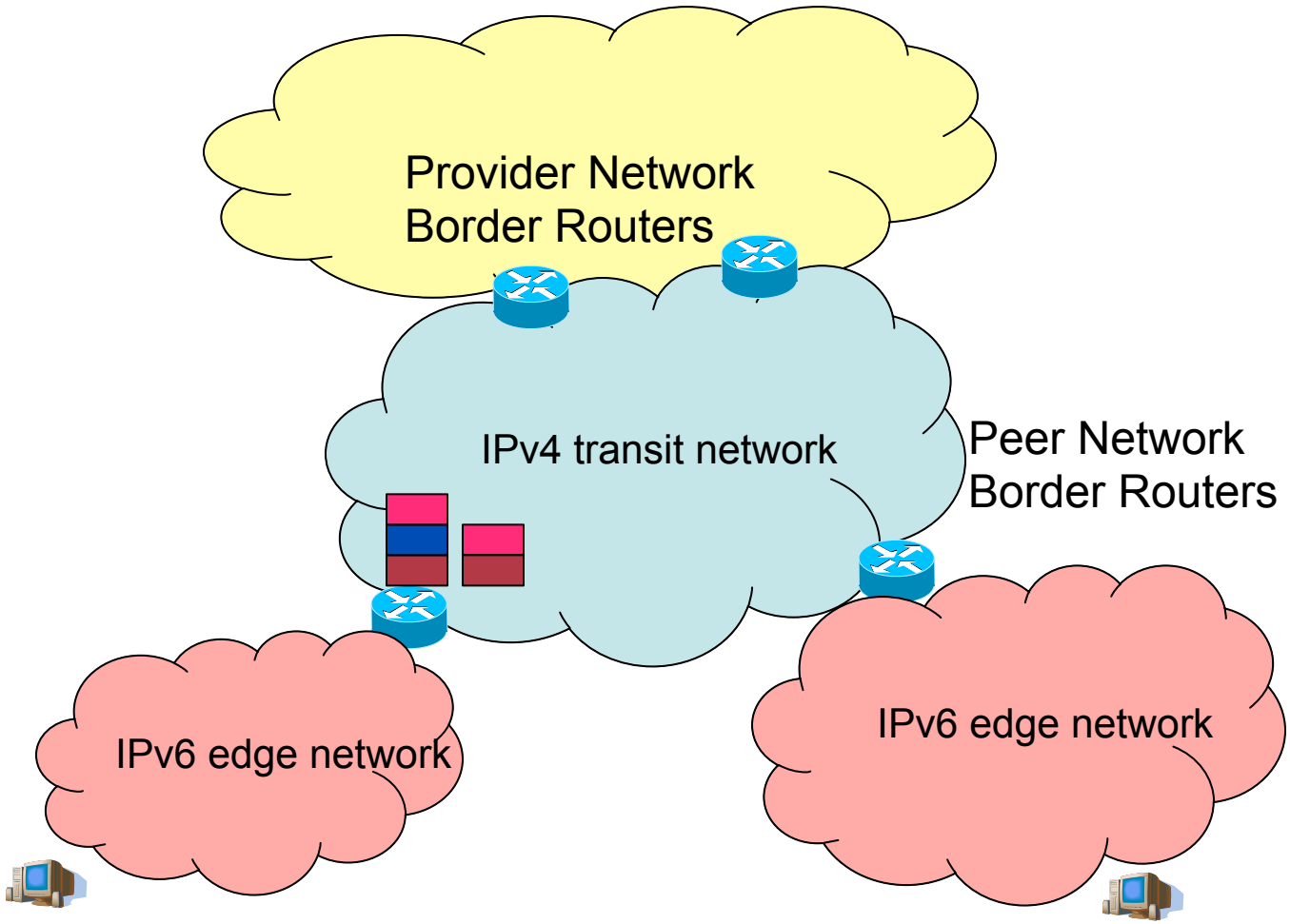
How SEAL Works



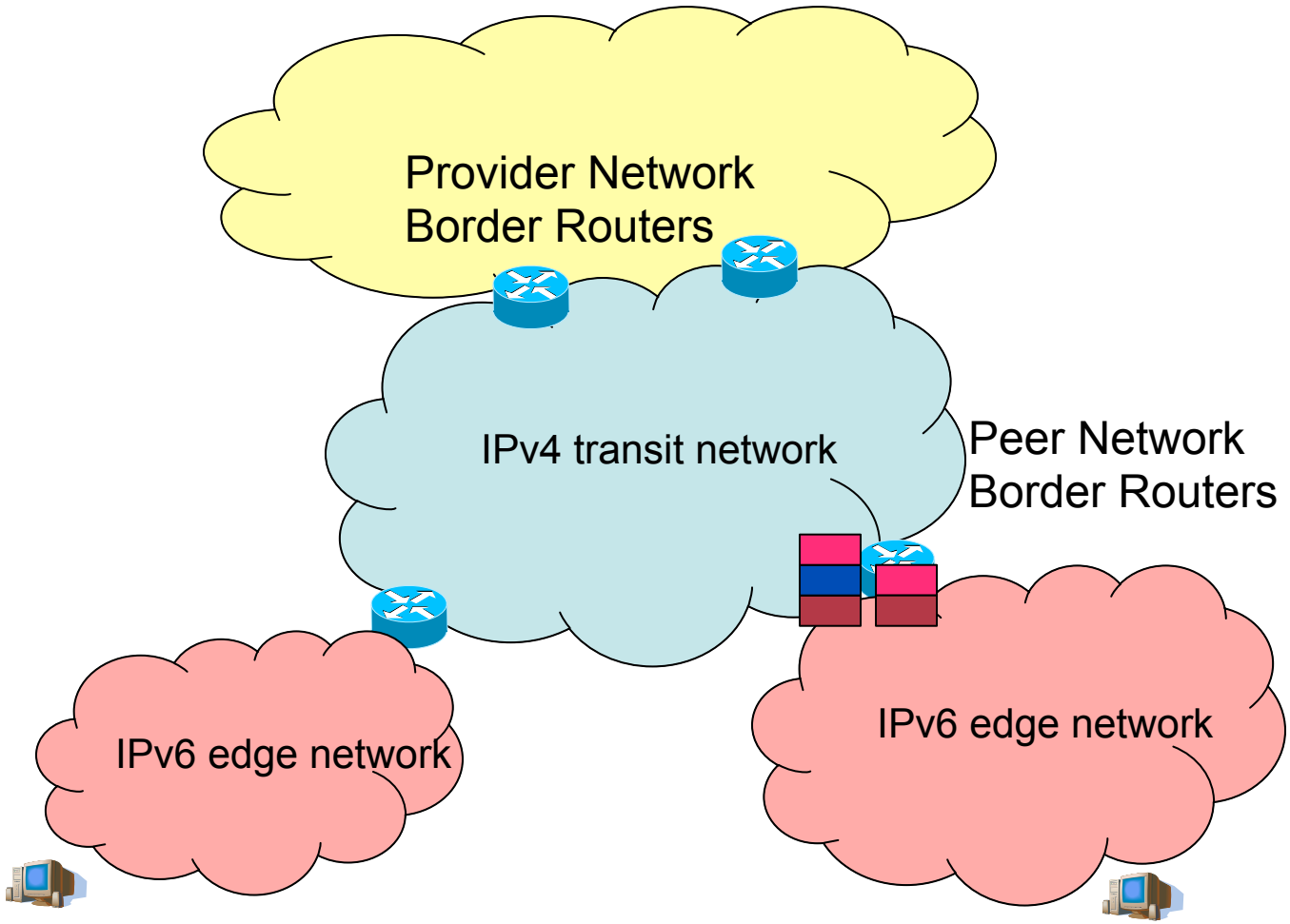
How SEAL Works



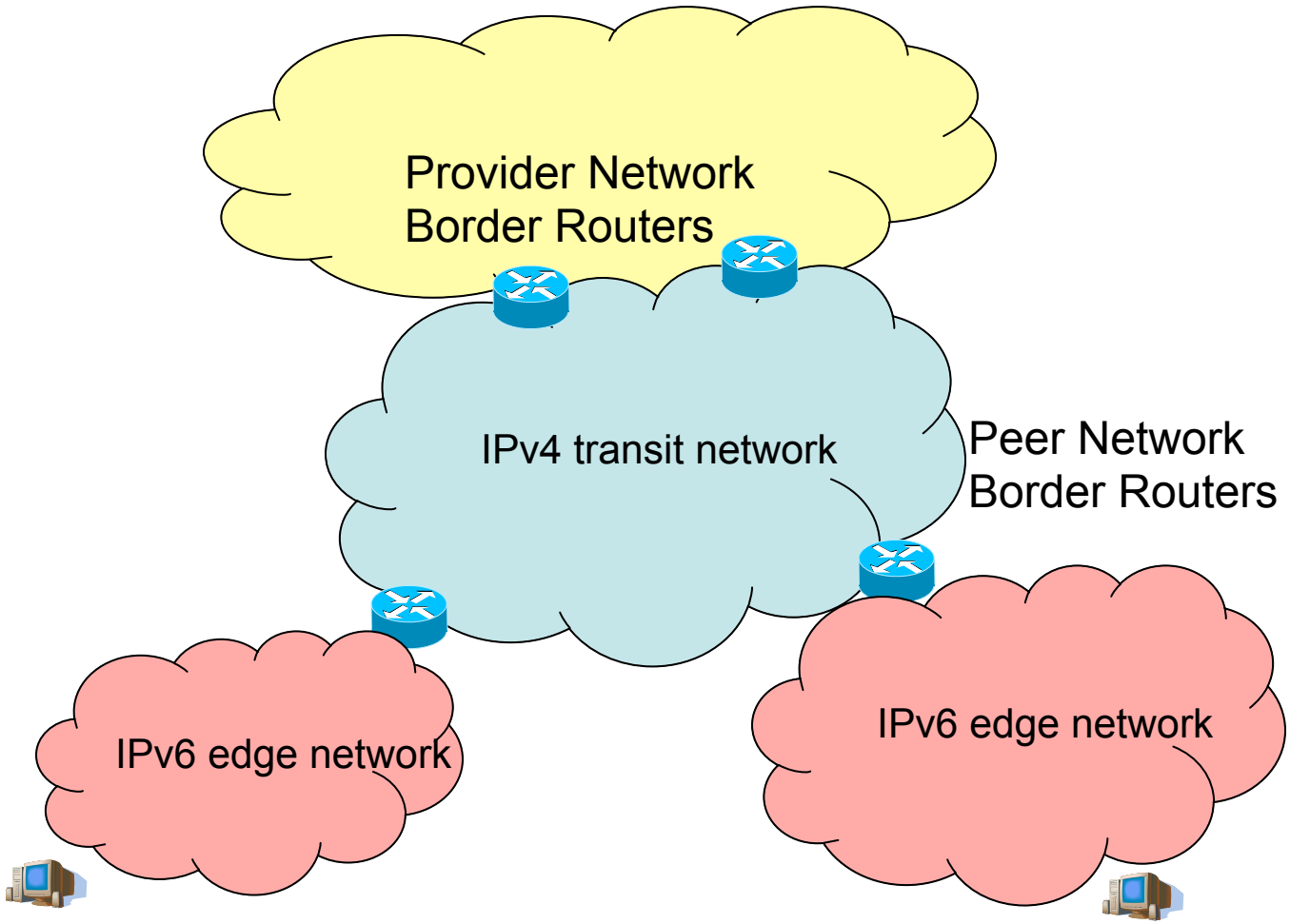
How SEAL Works



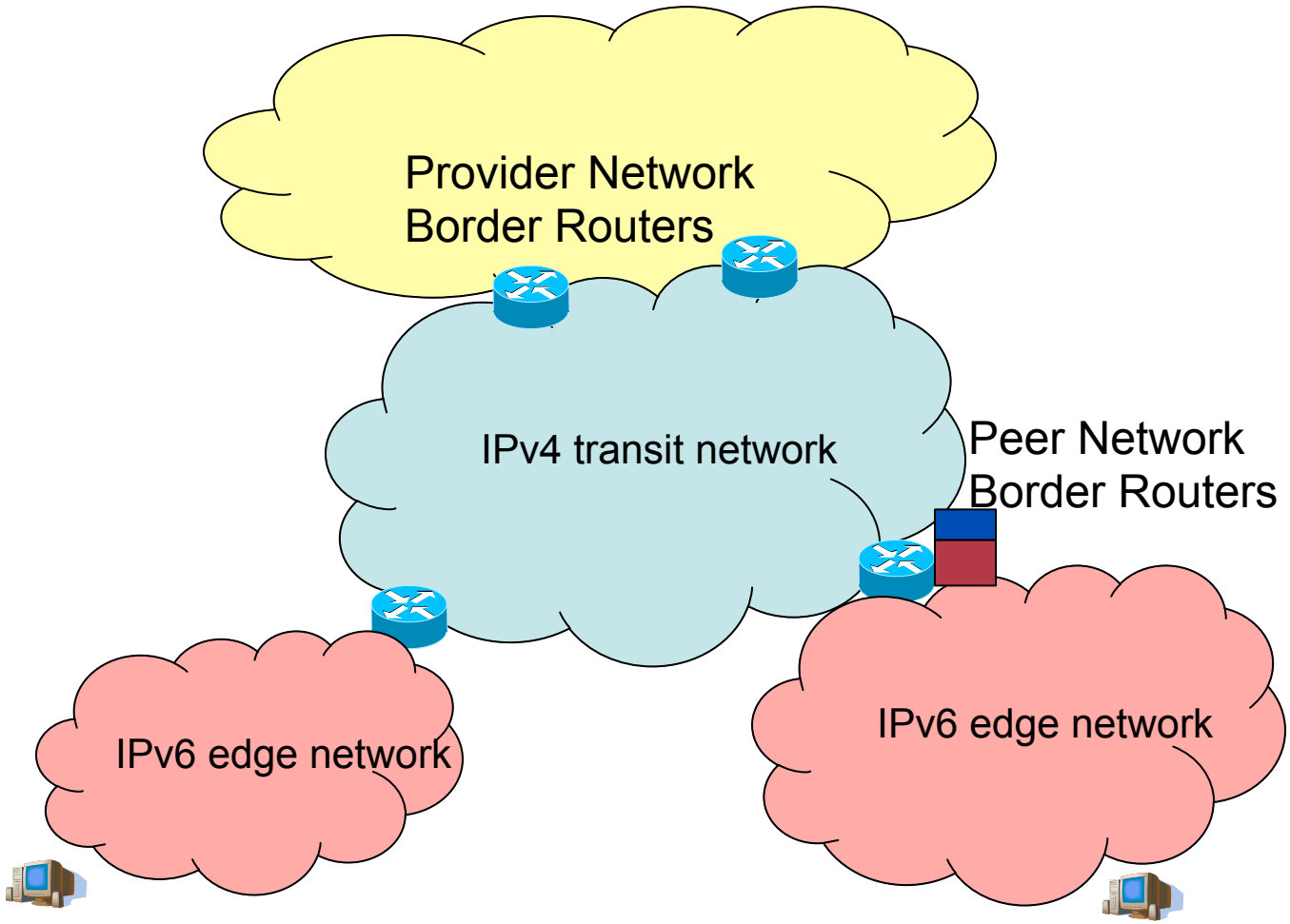
How SEAL Works



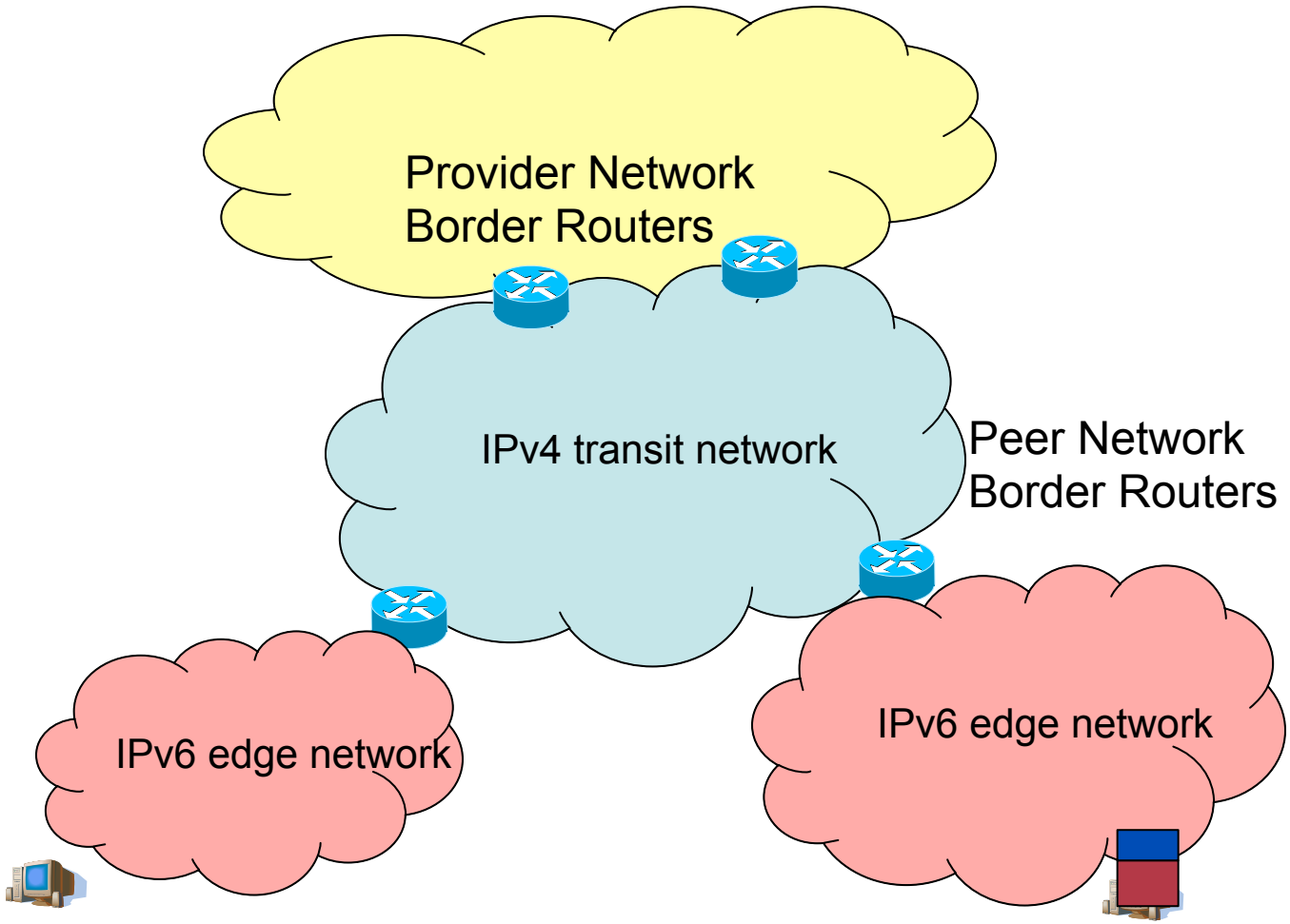
How SEAL Works



How SEAL Works



How SEAL Works



The Internet Routing Overlay Network (IRON)

- RANGER overlay network over the Internet DFZ
- RLOC addresses in underlying network; EID addresses in overlay
- IRON router RIB has EID Virtual Prefix (VP)-to-RLOC mappings
- RIB includes manageable number of coarse-grained EID VPs (e.g., 100k ::/32's)
- More-specific EID prefixes added to router FIBs on-demand
- More-specific EIDs added only on routers that need them

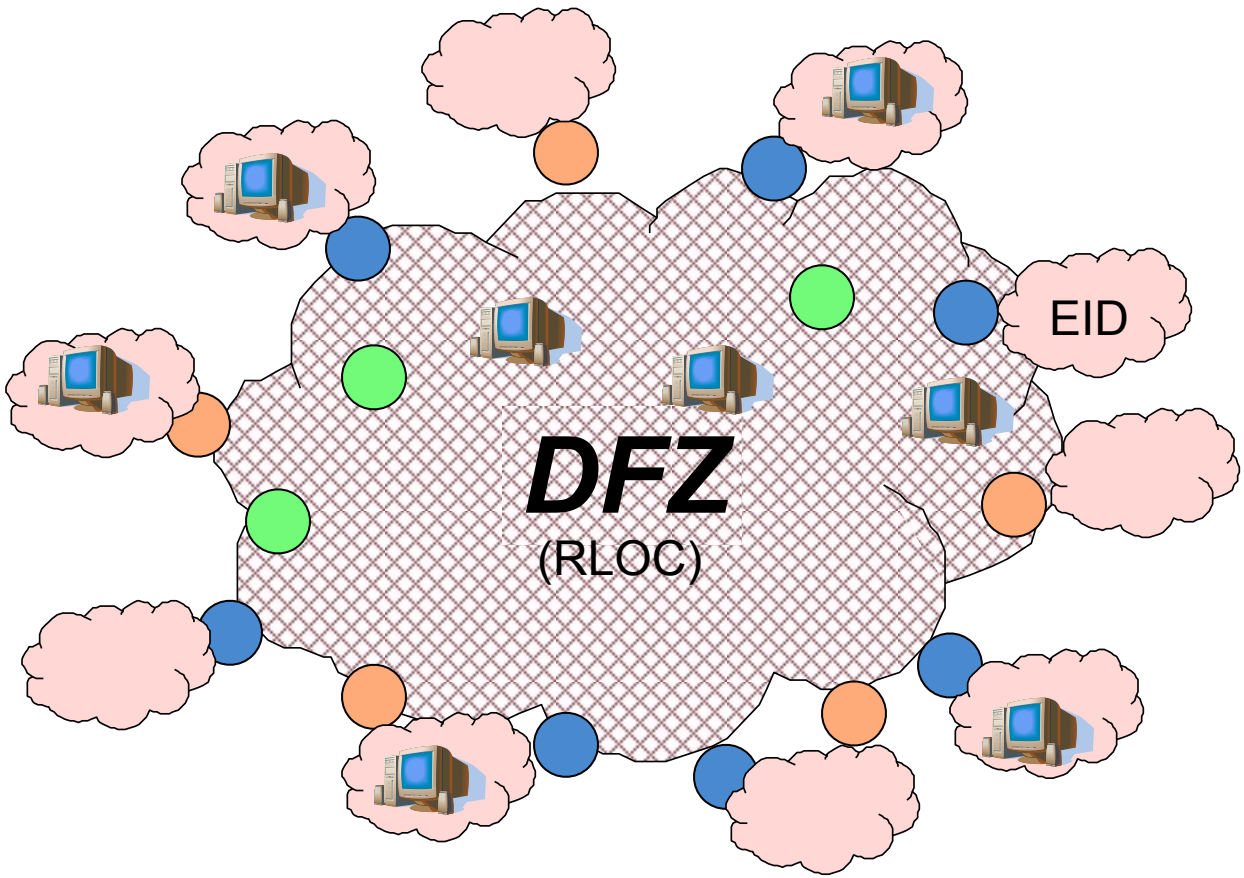
➢ **RIB loaded from centrally-managed file; no dynamic routing protocol needed**

➢ **Excellent scaling properties**

IRON Routers

- IRON Routers (IRs) are tunnel endpoint routers
- IRs form the borders of the IRON; encapsulate inner EID-addressed packets in outer RLOC-addressed headers
- Different IR roles:
  - IR(VP) – an IRON router that holds a Virtual Prefix
  - IR(EID) – an IRON router that connects an EID-based enterprise network to the IRON
  - IR(GW) – an IRON router that relays packets between EID- based endpoints and DFZ-based endpoints
- A single IR can serve multiple roles

The IRON – IRON Routers Connected to the DFZ



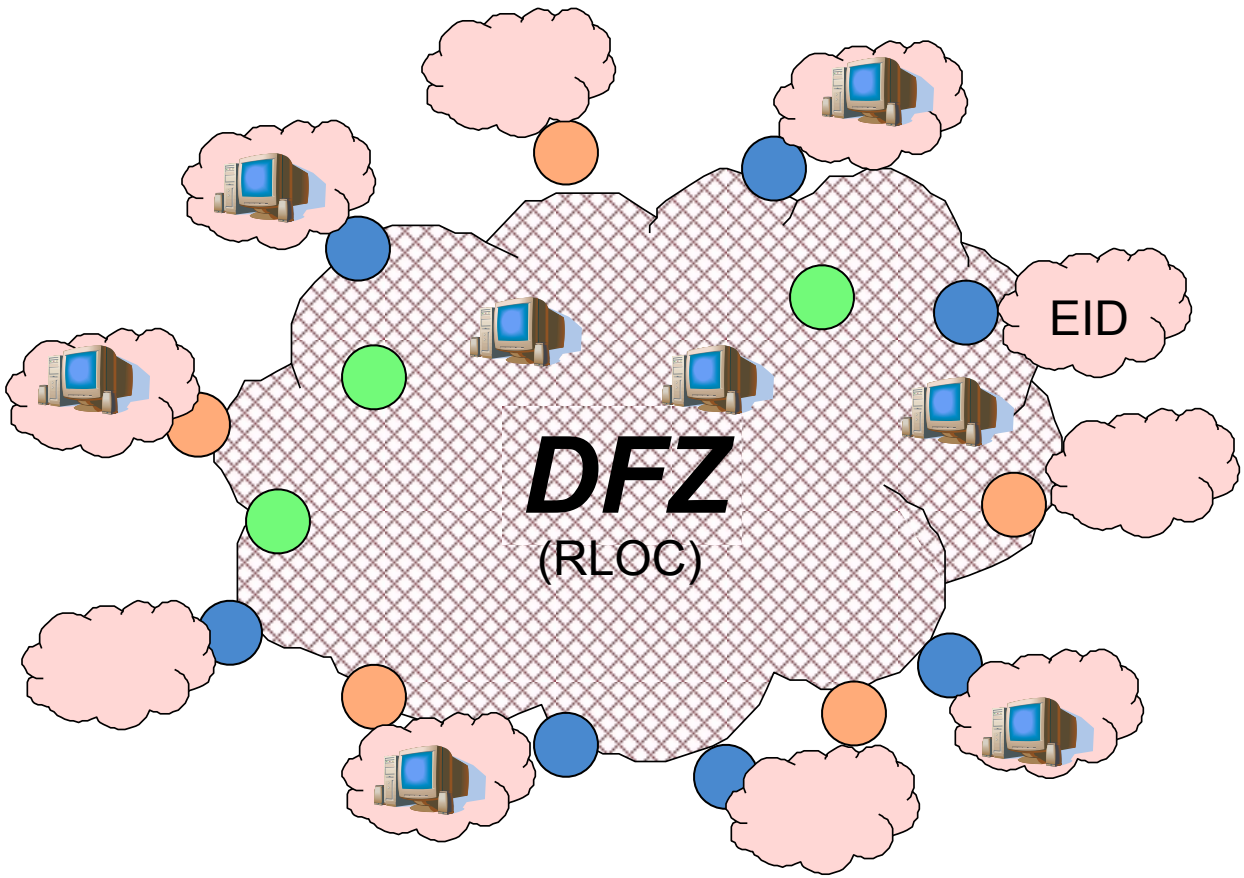
IR(VP):

IR(EID):

IR(DFZ):

Host:

EID End System to EID End System Example



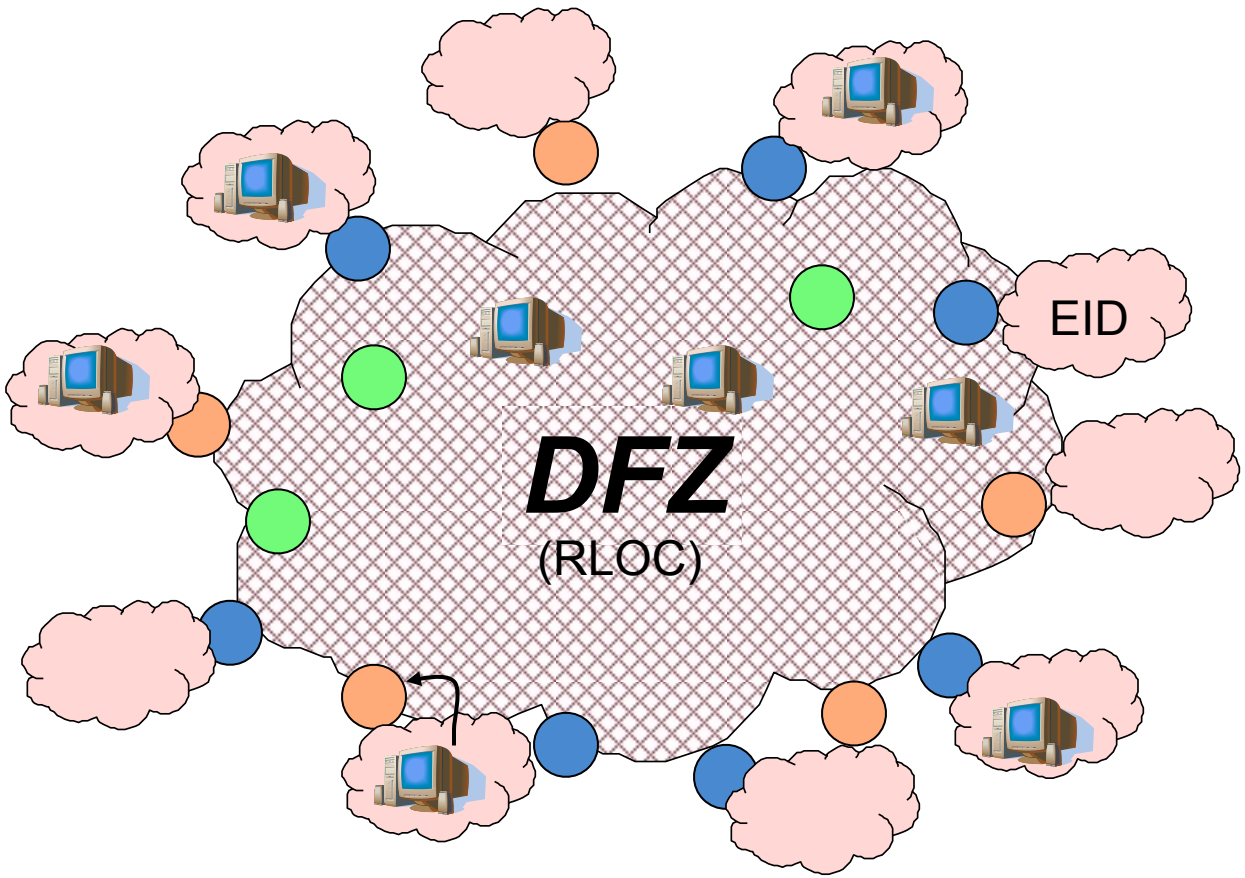
IR(VP):

IR(EID):

IR(DFZ):

Host:

EID End System to EID End System Example



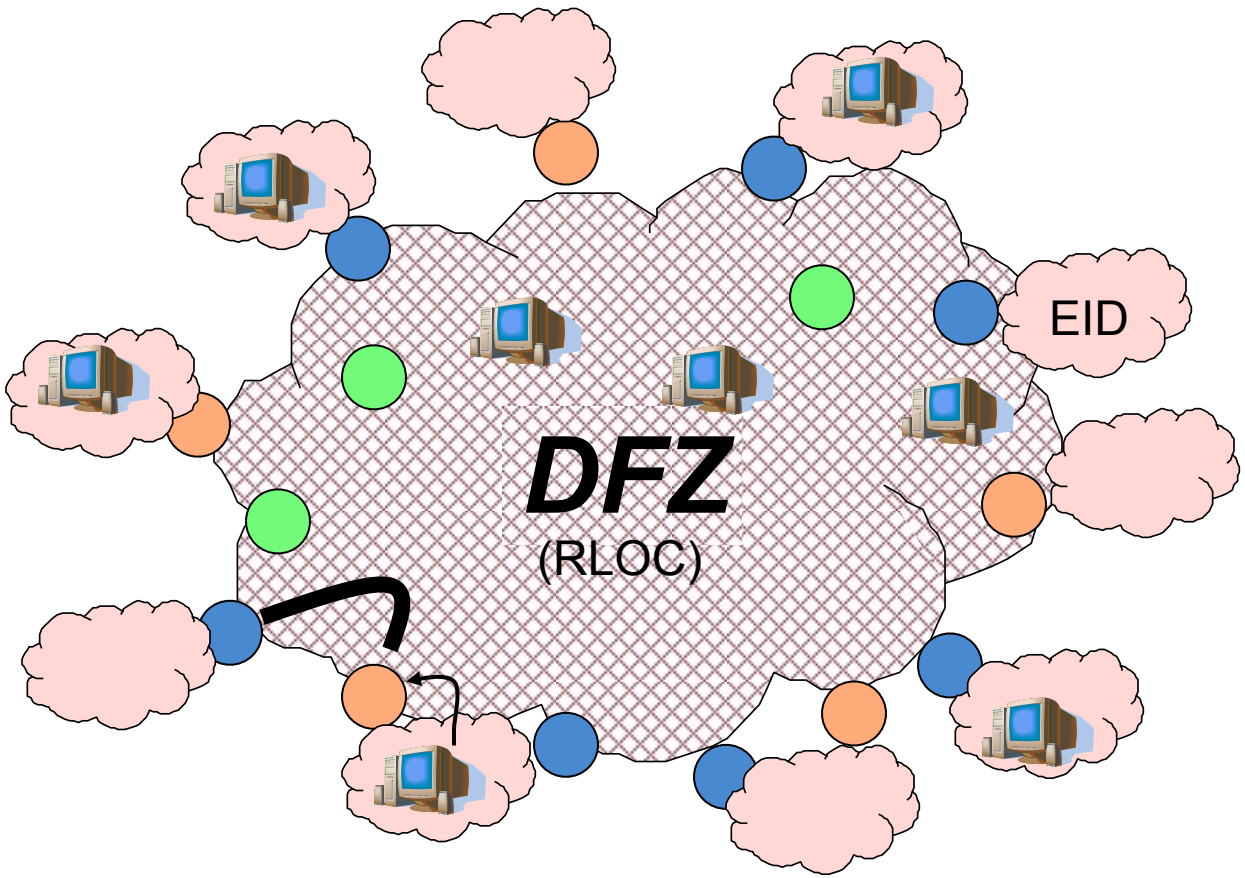
IR(VP):

IR(EID):

IR(DFZ):

Host:

EID End System to EID End System Example



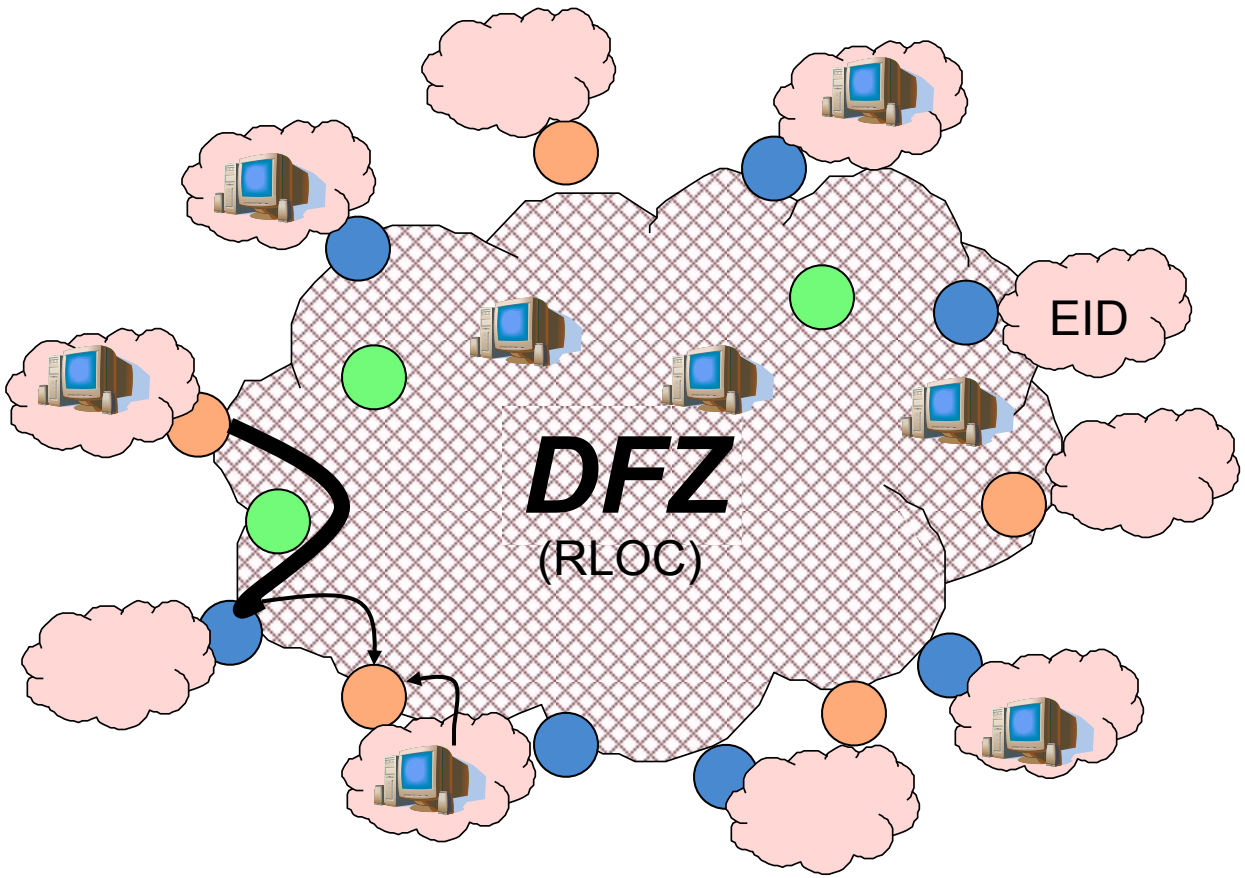
IR(VP):

IR(EID):

IR(DFZ):

Host:

EID End System to EID End System Example



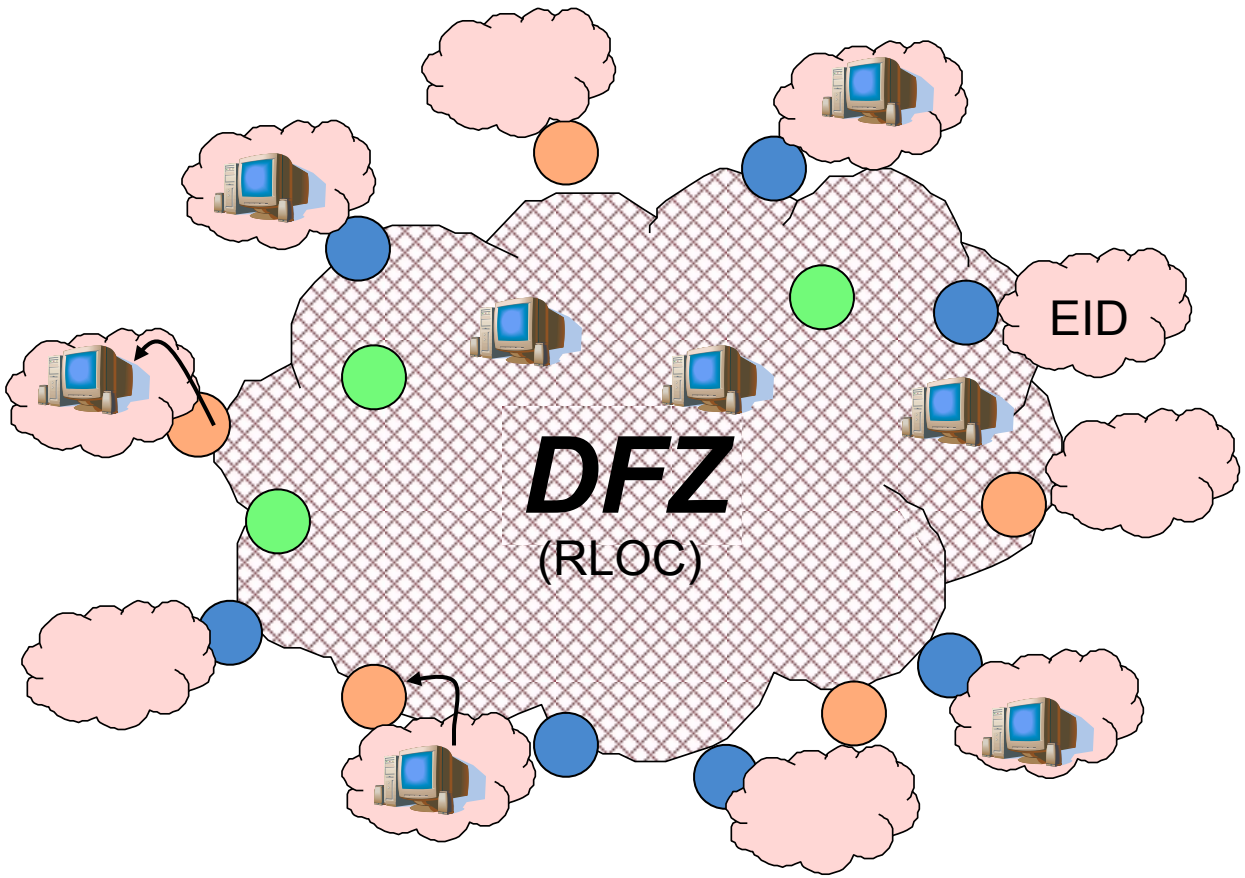
IR(VP):

IR(EID):

IR(DFZ):

Host:

EID End System to EID End System Example



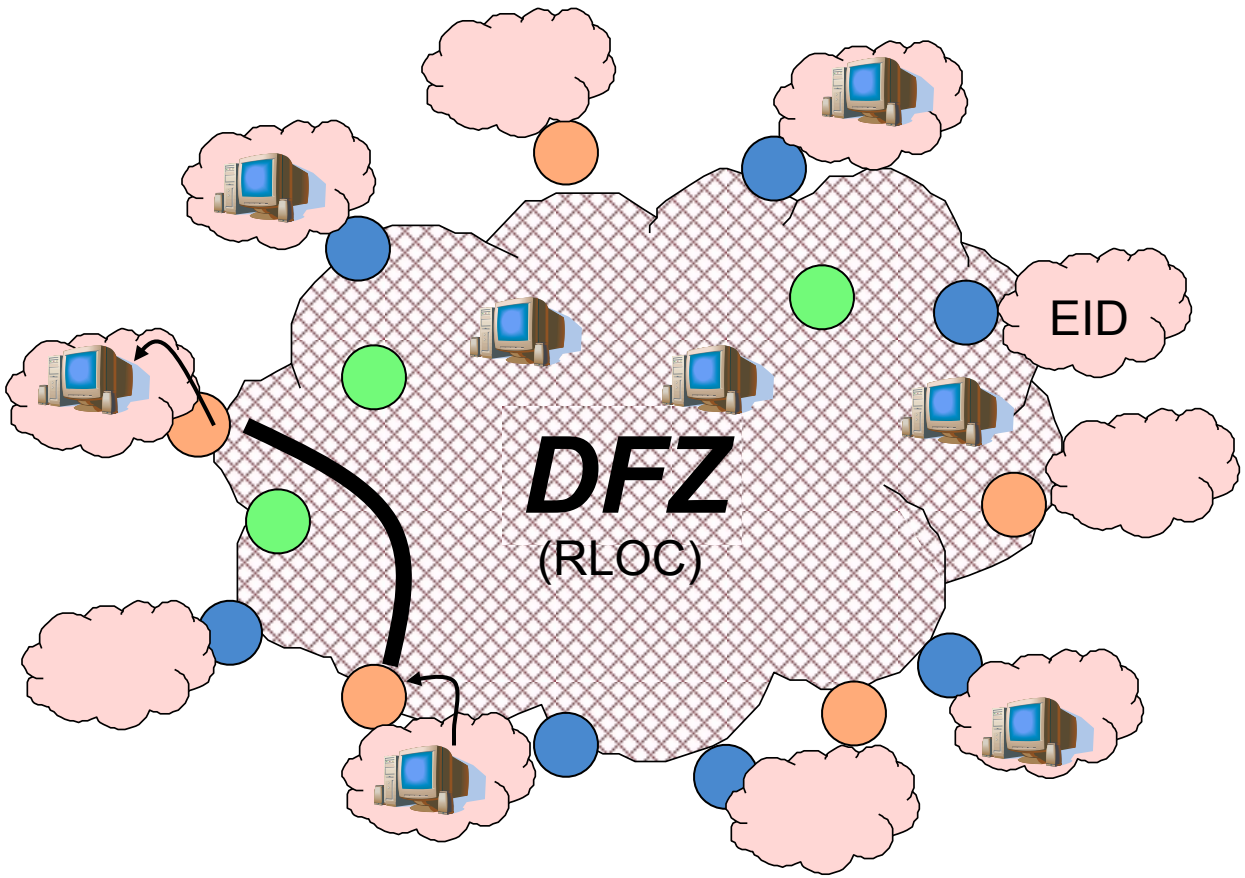
IR(VP):

IR(EID):

IR(DFZ):

Host:

EID End System to EID End System Example



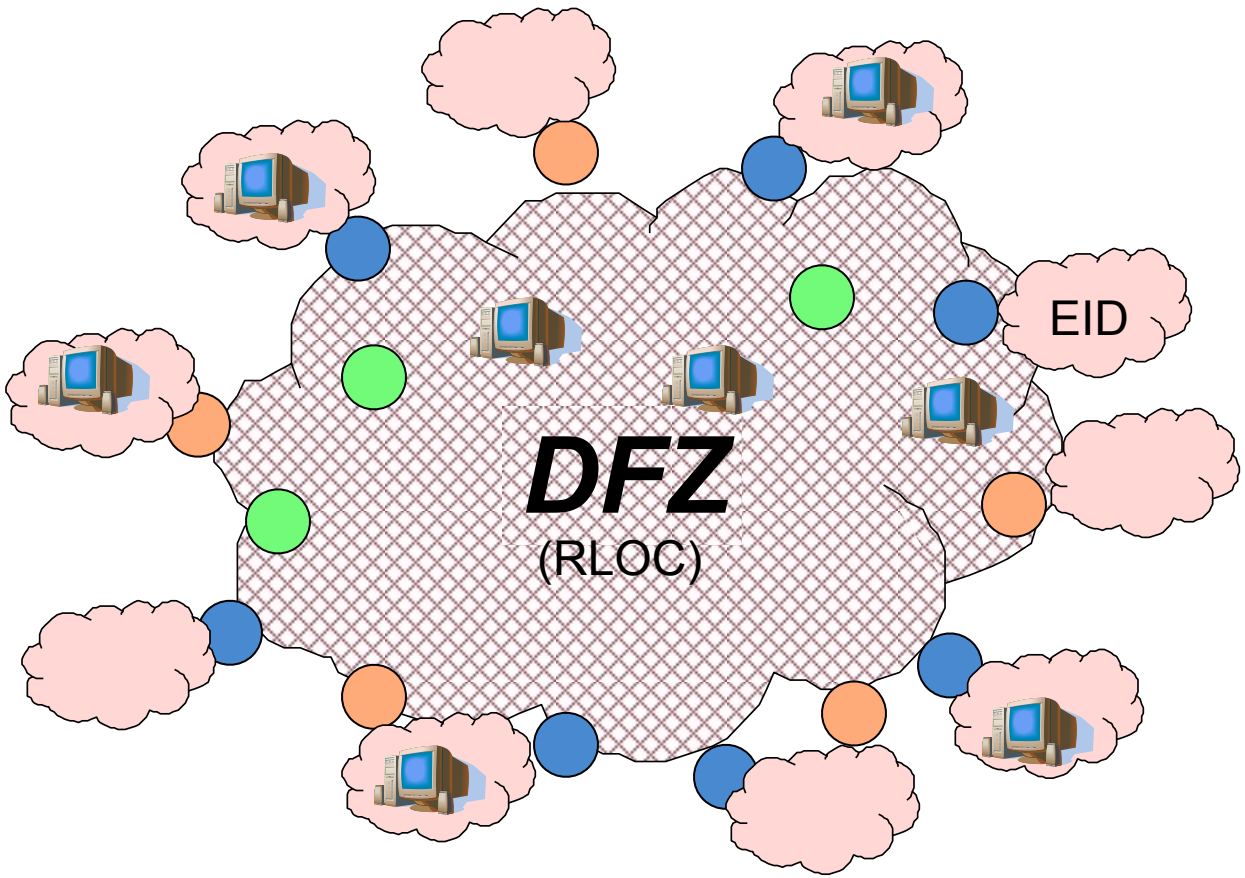
IR(VP):

IR(EID):

IR(DFZ):

Host:

RLOC End System to EID End System Example



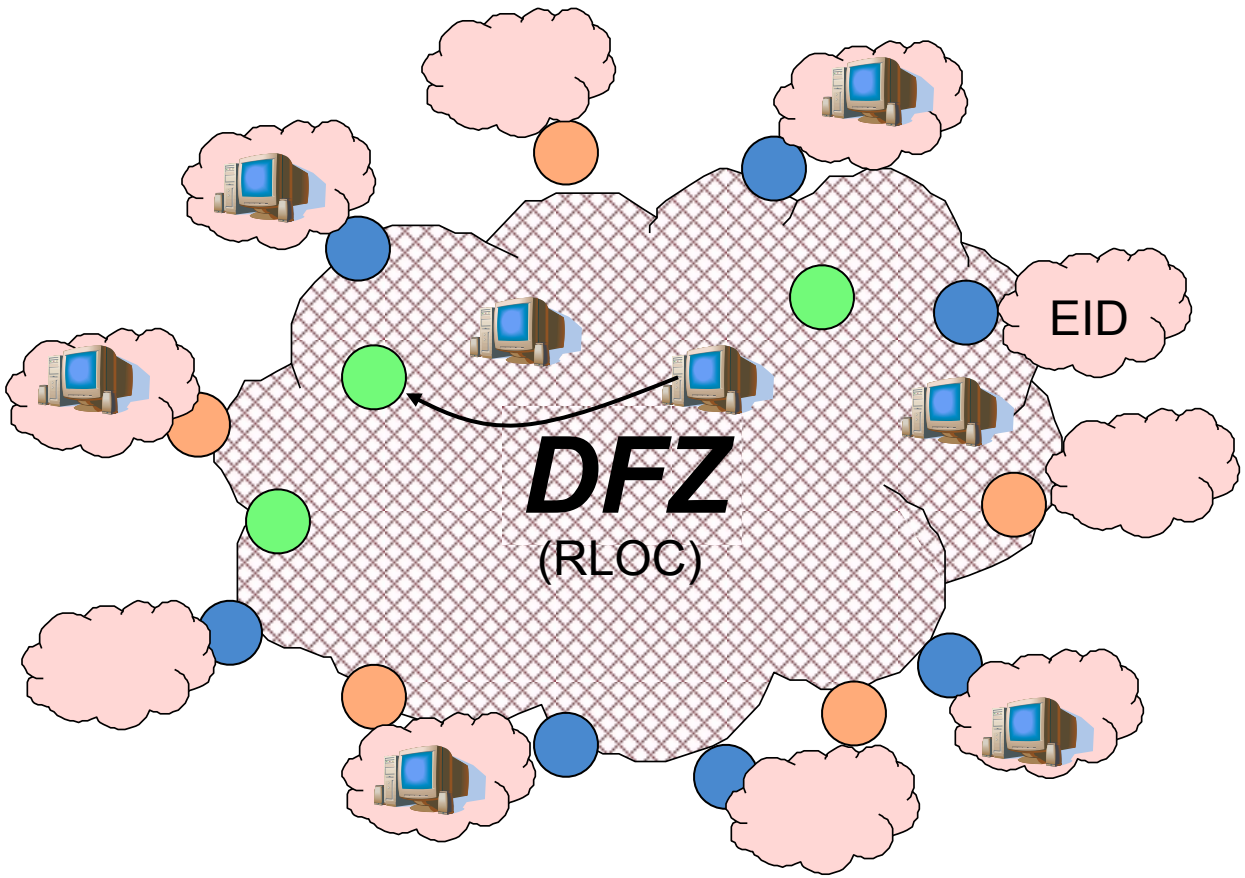
IR(VP):

IR(EID):

IR(DFZ):

Host:

RLOC End System to EID End System Example



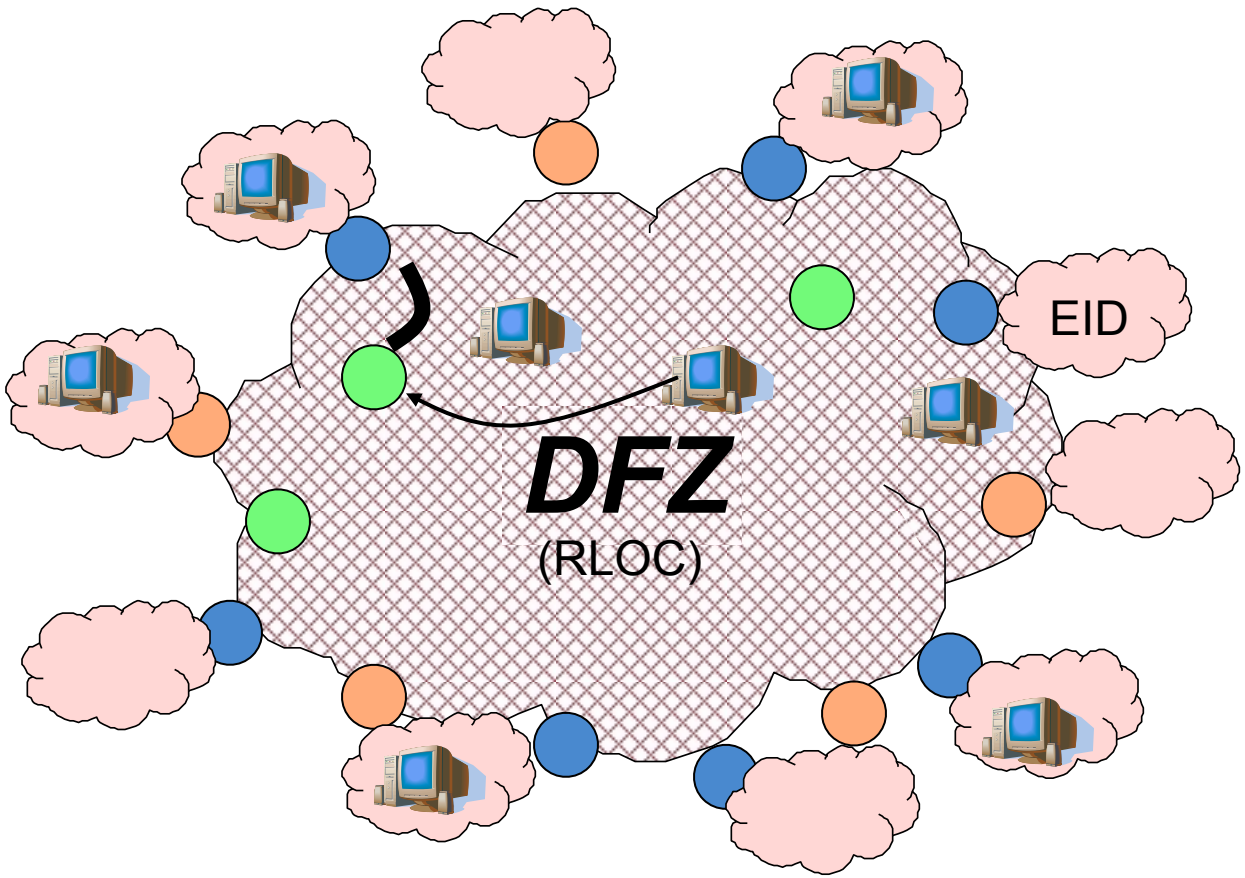
IR(VP):

IR(EID):

IR(DFZ):

Host:

RLOC End System to EID End System Example



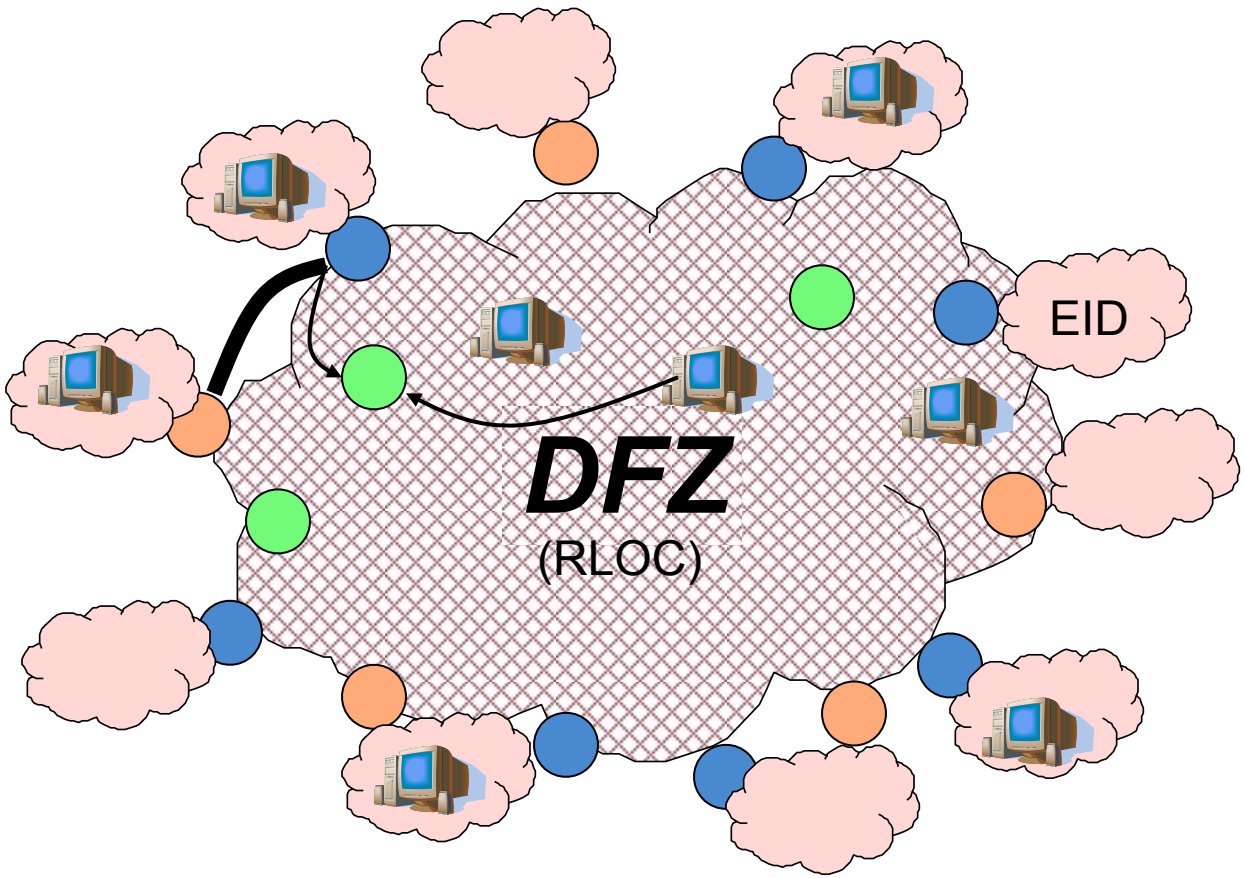
IR(VP):

IR(EID):

IR(DFZ):

Host:

RLOC End System to EID End System Example



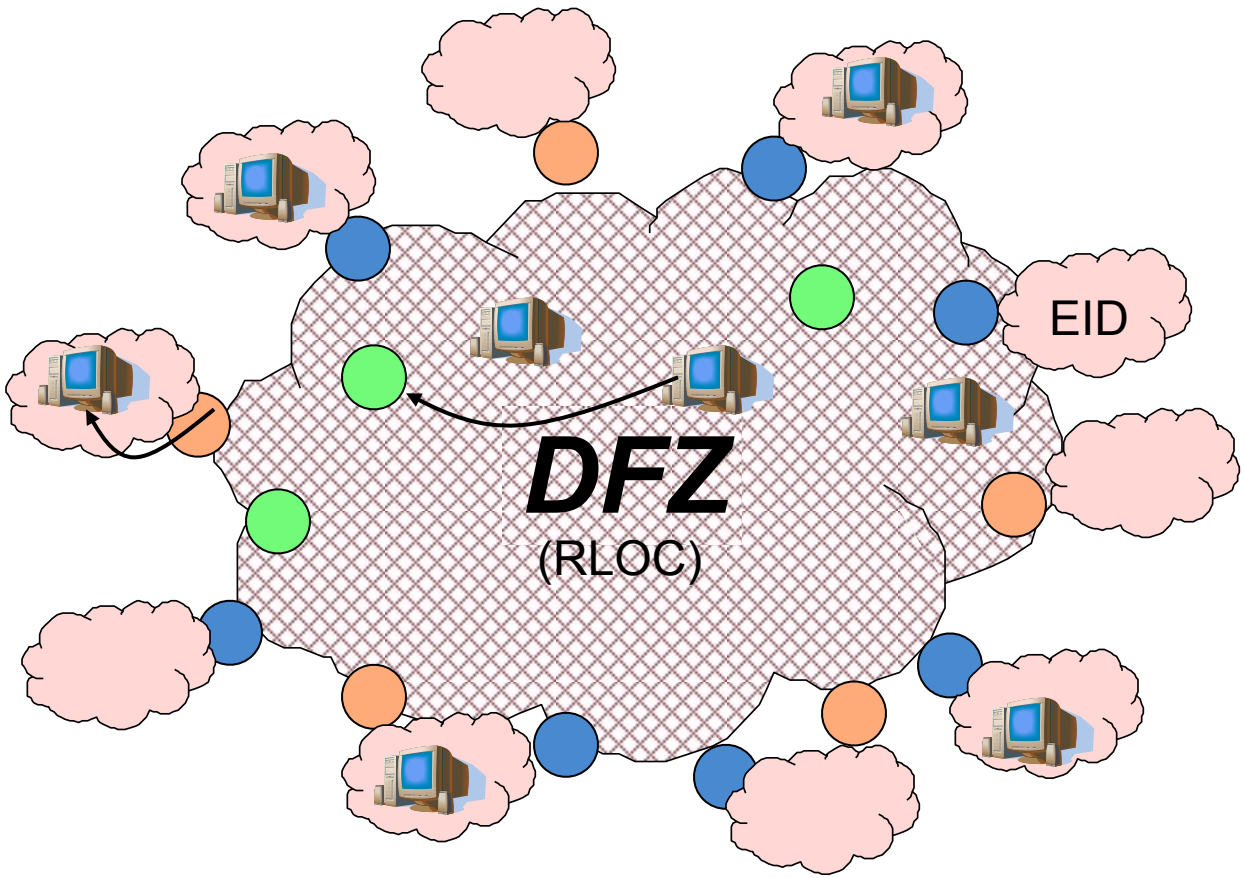
IR(VP):

IR(EID):

IR(DFZ):

Host:

RLOC End System to EID End System Example



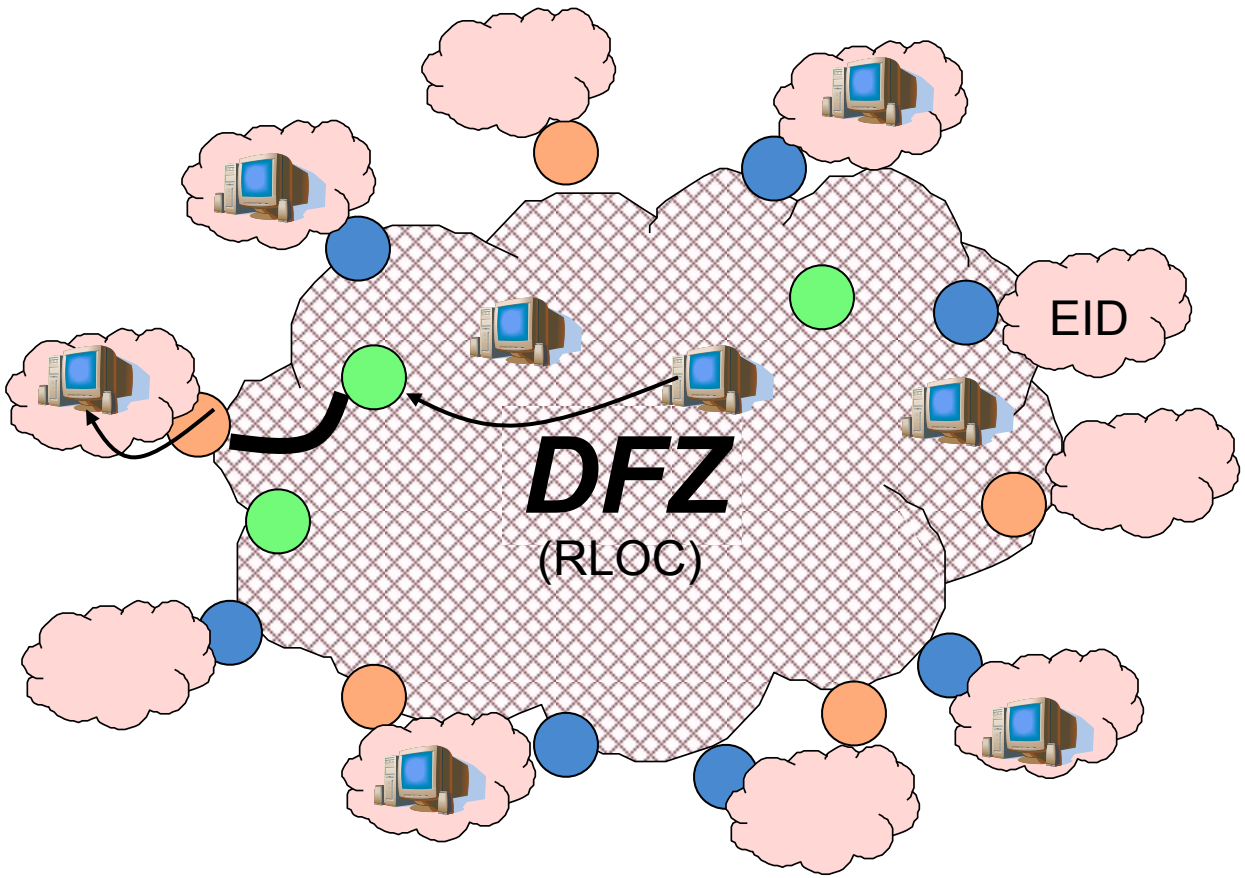
IR(VP):

IR(EID):

IR(DFZ):

Host:

RLOC End System to EID End System Example



IR(VP):

IR(EID):

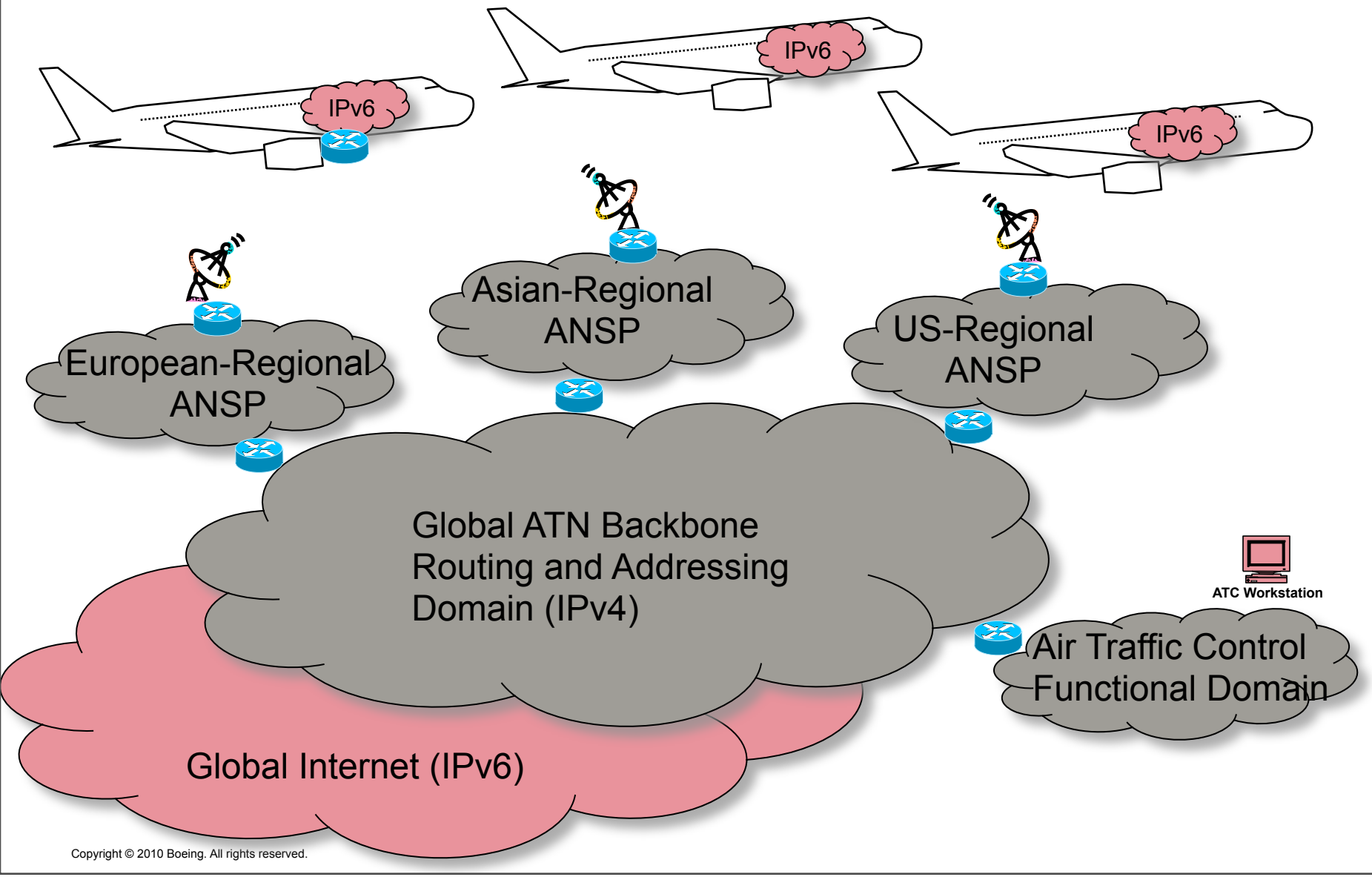
IR(DFZ):

Host:

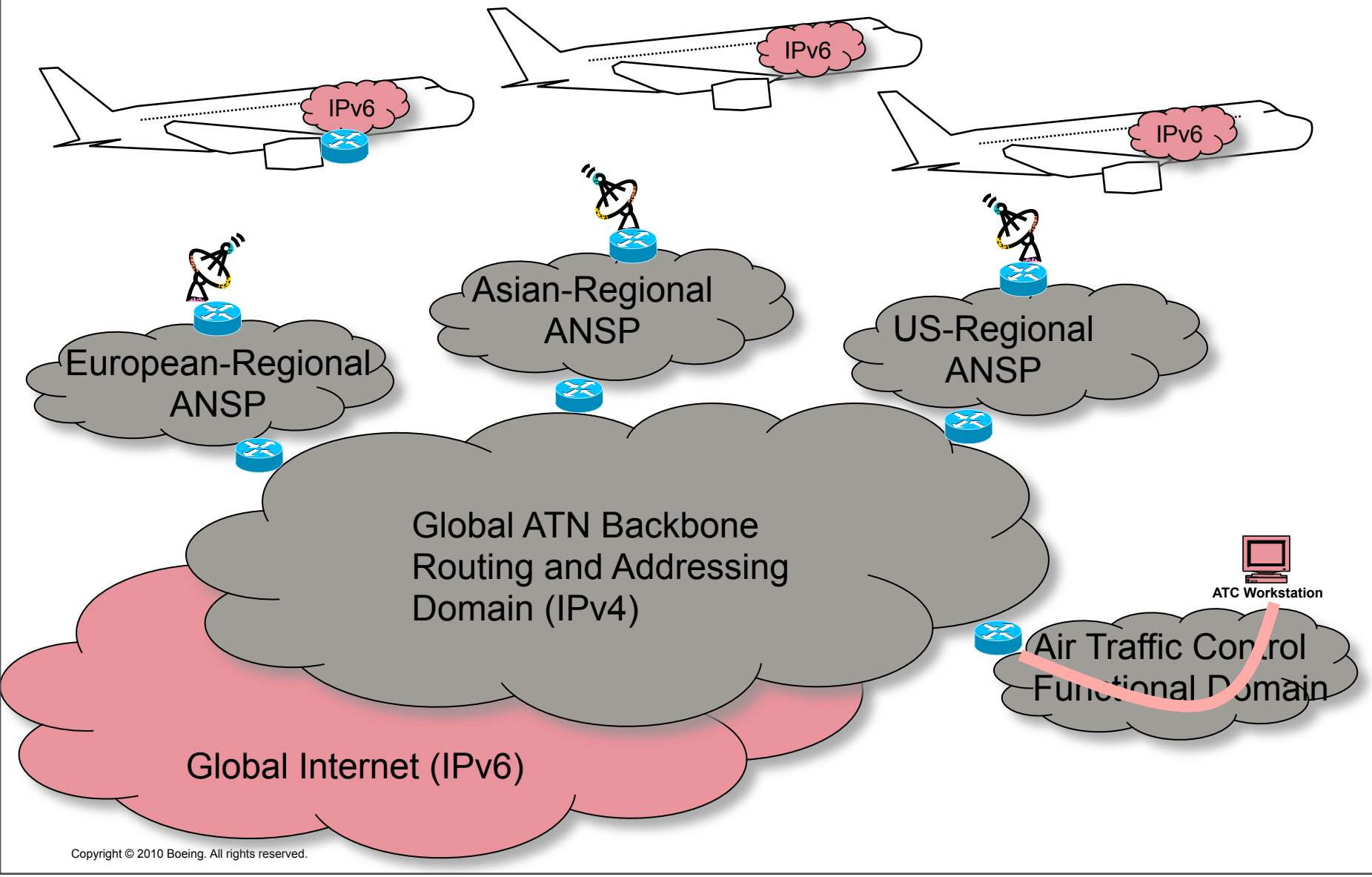
IRON Scaling

- **VPs:**
  - **Assume O(100K) VPs (e.g., ::/32s)**
  - **Assume IRON RIB changes only very rarely**
  - **RIB size is 100K entries – fully populated in each IR**
- **EIDs:**
  - **Assume O(100K) EID prefixes per VP**
  - **Yields 10^{10} EID prefixes in the IRON**
  - **Populated to IR FIBs on-demand**
- **RIB Size: 100K VPs in each IR**
- **FIB Size: 100K EID prefixes + 100K VPs = 200K**

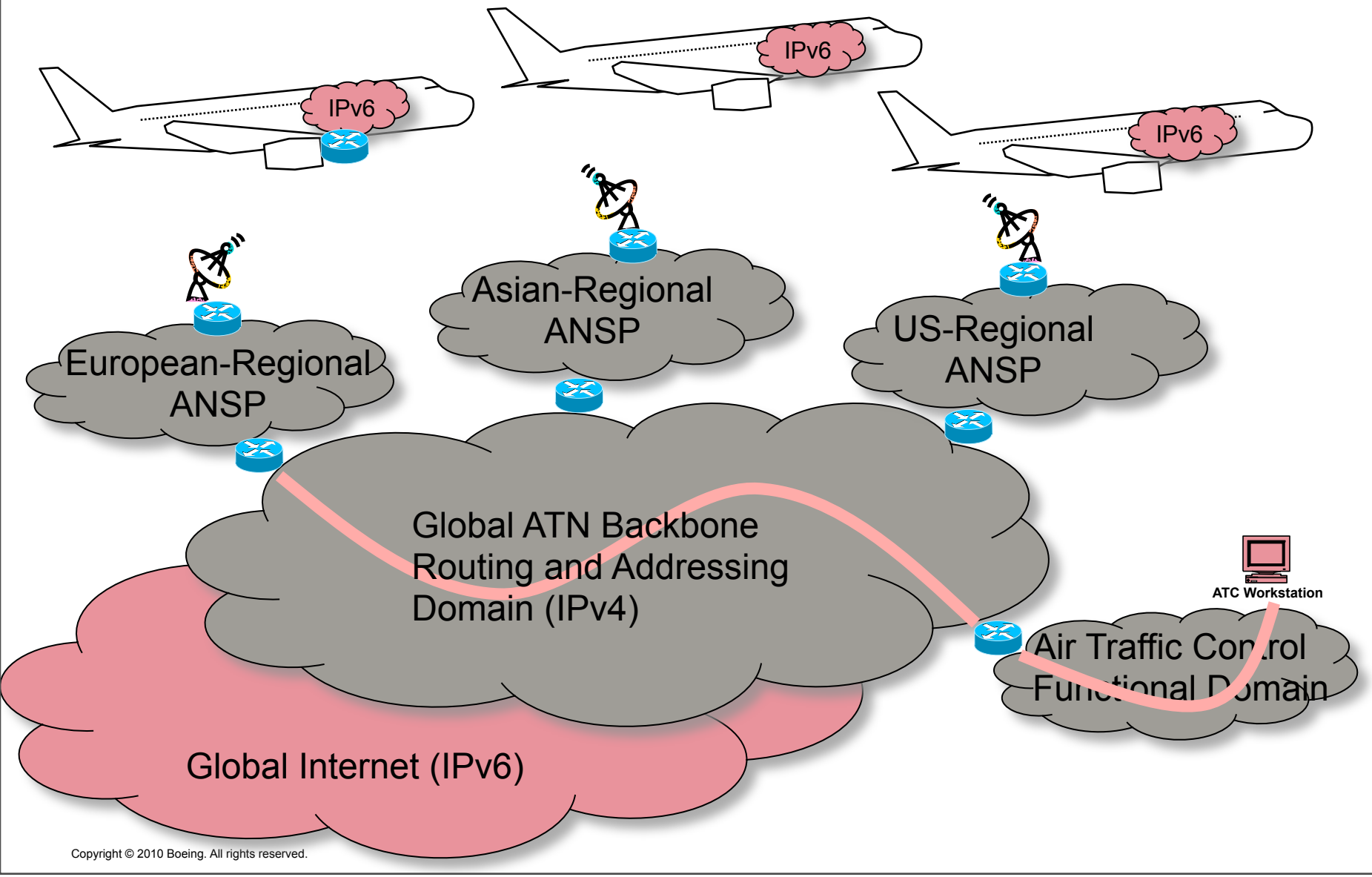
Civil Aviation Example



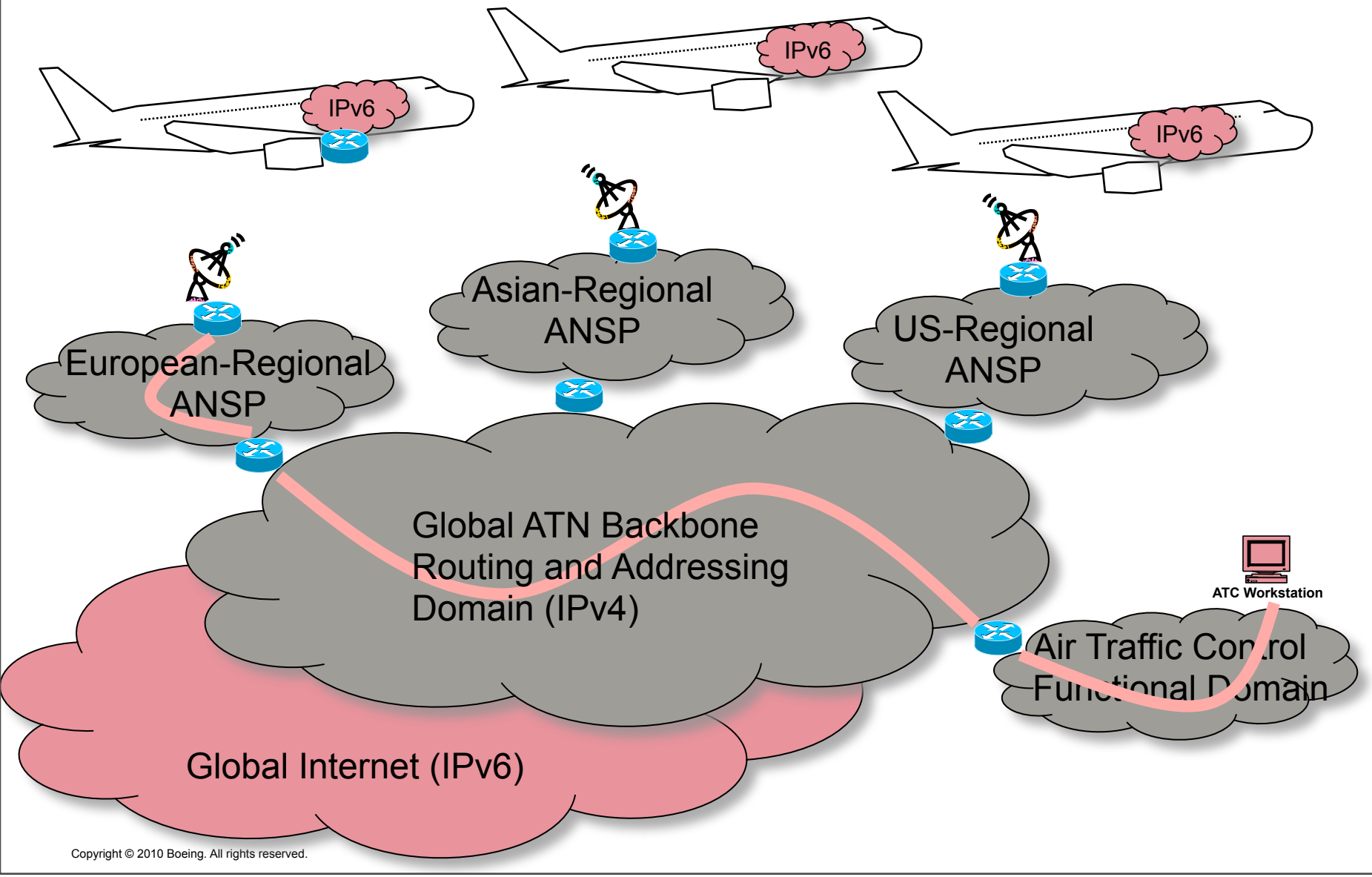
Civil Aviation Example



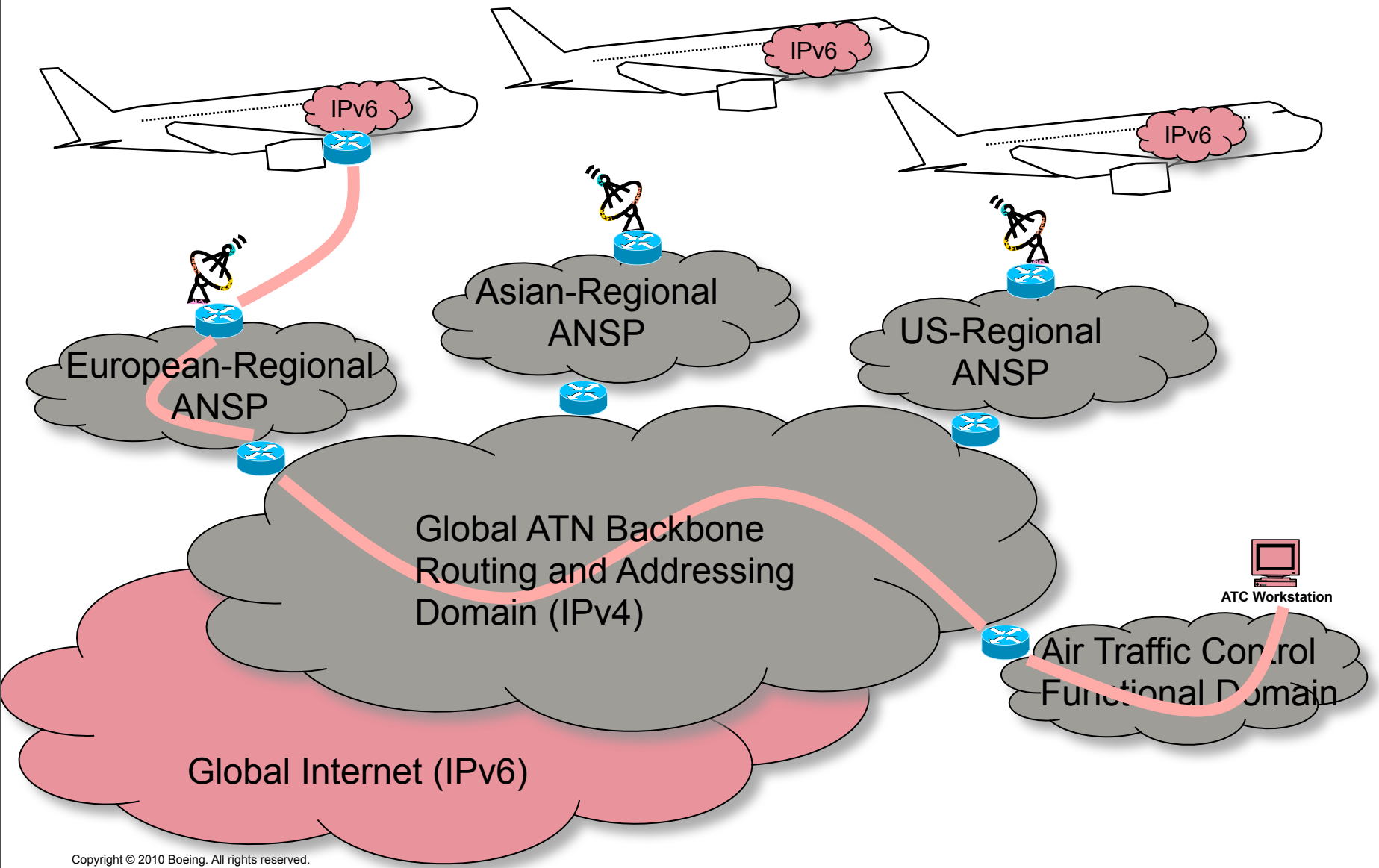
Civil Aviation Example



Civil Aviation Example

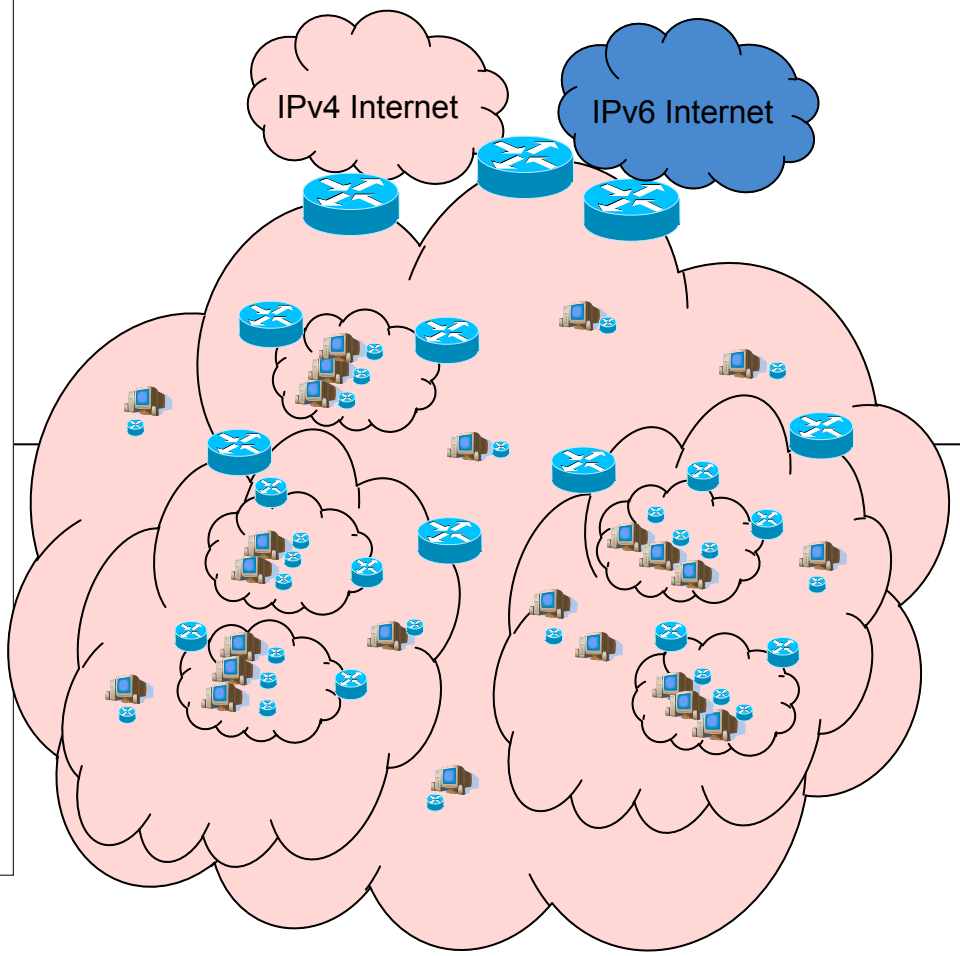


Civil Aviation Example



Enterprise Network Example

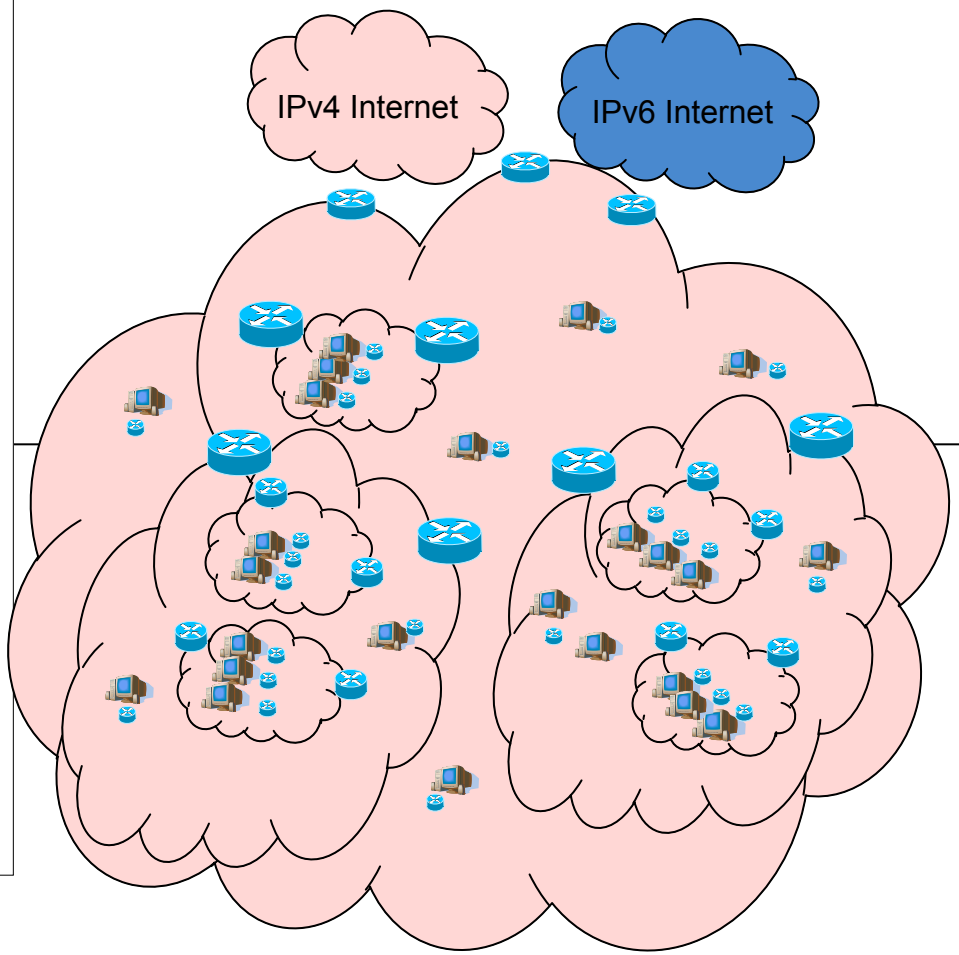
- Routing & Addressing in Next Generation EnteRprises (RANGER)
  - **Network-of-networks architecture**
  - **Minimal touch-points (border routers only)**
  - **No changes to most hosts and routers**
  - **Fully-provisioned IP services; balanced blend of tunneling, translation and native**
- Gradual integration of IPv6
  - **Customer-driven requirements lead policy and strategy**
  - **IPv6 and IPv4 in peaceful co-existence**
  - **It's not an "either-or" decision**
- Tangible Benefits
  - **Secure Mobile Architecture (SMA)**
  - **simplified management**
  - **logical partitioning**
  - **traffic engineering**
  - **end-to-end addressing**
  - **mobility and multihoming**



Enterprise Network
IPv4-Only

Enterprise Network Example

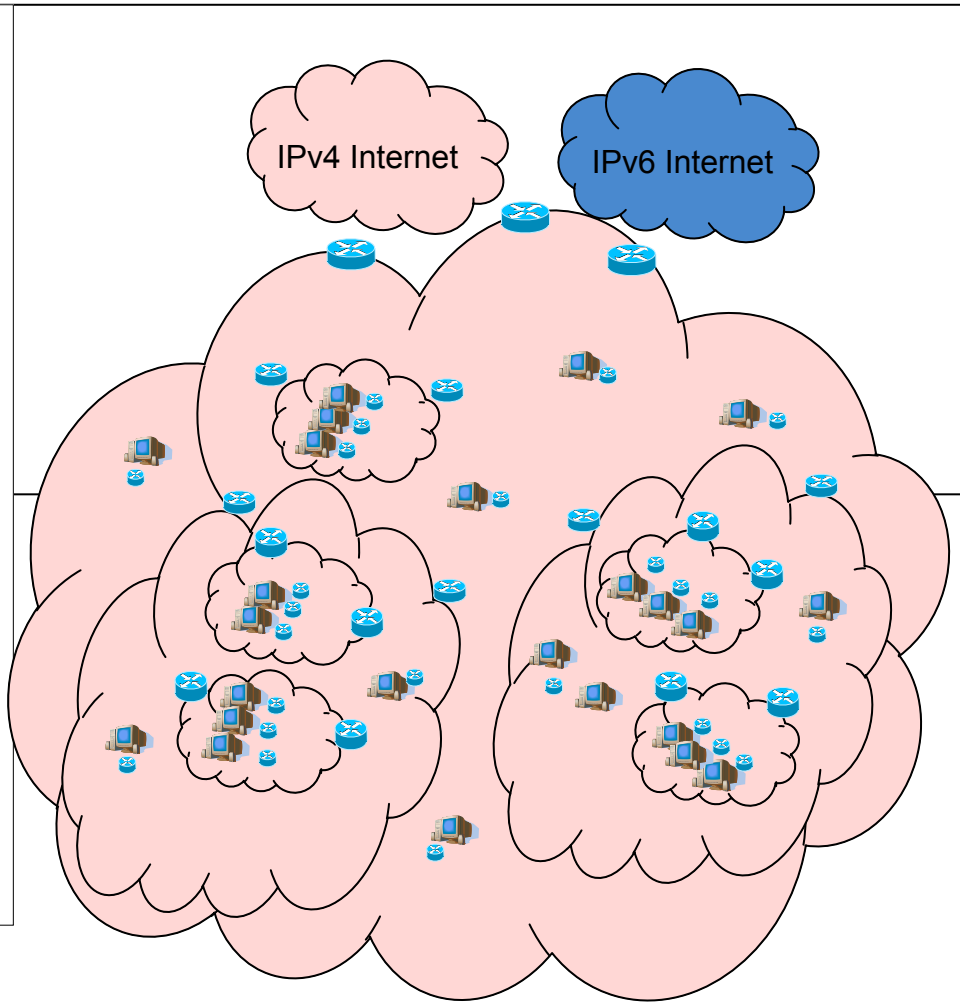
- Routing & Addressing in Next Generation EnteRprises (RANGER)
  - **Network-of-networks architecture**
  - **Minimal touch-points (border routers only)**
  - **No changes to most hosts and routers**
  - **Fully-provisioned IP services; balanced blend of tunneling, translation and native**
- Gradual integration of IPv6
  - **Customer-driven requirements lead policy and strategy**
  - **IPv6 and IPv4 in peaceful co-existence**
  - **It's not an "either-or" decision**
- Tangible Benefits
  - **Secure Mobile Architecture (SMA)**
  - **simplified management**
  - **logical partitioning**
  - **traffic engineering**
  - **end-to-end addressing**
  - **mobility and multihoming**



Enterprise Network
Initial IPv6 Deployment

Enterprise Network Example

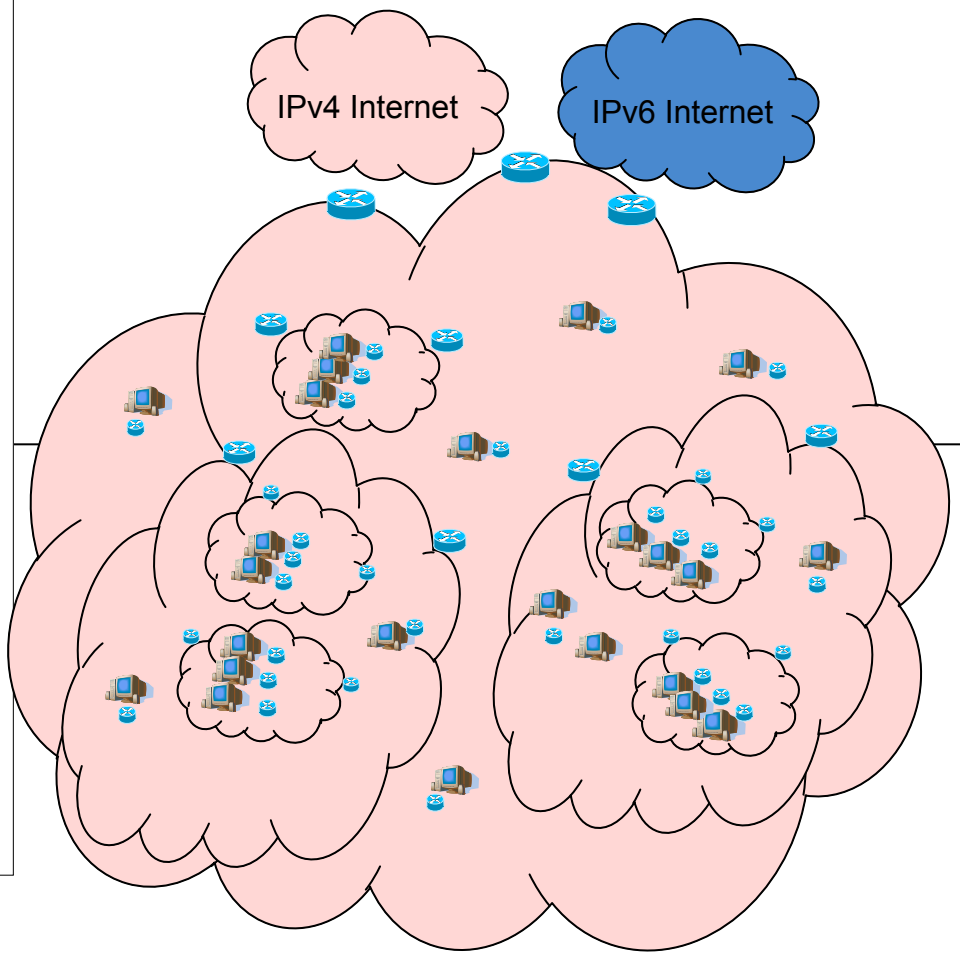
- Routing & Addressing in Next Generation EnteRprises (RANGER)
  - **Network-of-networks architecture**
  - **Minimal touch-points (border routers only)**
  - **No changes to most hosts and routers**
  - **Fully-provisioned IP services; balanced blend of tunneling, translation and native**
- Gradual integration of IPv6
  - **Customer-driven requirements lead policy and strategy**
  - **IPv6 and IPv4 in peaceful co-existence**
  - **It's not an "either-or" decision**
- Tangible Benefits
  - **Secure Mobile Architecture (SMA)**
  - **simplified management**
  - **logical partitioning**
  - **traffic engineering**
  - **end-to-end addressing**
  - **mobility and multihoming**



Enterprise Network
Advanced IPv6 Deployment

Enterprise Network Example

- Routing & Addressing in Next Generation EnteRprises (RANGER)
  - **Network-of-networks architecture**
  - **Minimal touch-points (border routers only)**
  - **No changes to most hosts and routers**
  - **Fully-provisioned IP services; balanced blend of tunneling, translation and native**
- Gradual integration of IPv6
  - **Customer-driven requirements lead policy and strategy**
  - **IPv6 and IPv4 in peaceful co-existence**
  - **It's not an "either-or" decision**
- Tangible Benefits
  - **Secure Mobile Architecture (SMA)**
  - **simplified management**
  - **logical partitioning**
  - **traffic engineering**
  - **end-to-end addressing**
  - **mobility and multihoming**



Enterprise Network
Fully Provisioned IP Services

- **Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)**
  http://www.ietf.org/rfc/rfc5214.txt
- **Routing and Addressing in Networks with Global Enterprise Recursion (RANGER)**
  http://www.ietf.org/rfc/rfc5720.txt
- **RANGER Scenarios**
  http://tools.ietf.org/html/draft-russert-rangers
- **Virtual Enterprise Traversal (VET)**
  http://www.ietf.org/rfc/rfc5558.txt
  http://tools.ietf.org/html/draft-templin-intarea-vet
- **Subnetwork Encapsulation and Adaptation Layer (SEAL)**
  http://www.ietf.org/rfc/rfc5320.txt
  http://tools.ietf.org/html/draft-templin-intarea-seal
- **The Internet Routing Overlay Network (IRON)**
  http://tools.ietf.org/html/draft-templin-iron