HIP as a VPLS solution

draft-henderson-hip-vpls-00

IETF 77 HIPRG Meeting (Monday March 22, 2010)

Tom Henderson (thomas.r.henderson@boeing.com),

Acknowledgments and History

- **This presentation and work is the next step of a lengthy process to use HIP as a component in the Open Group's Secure Mobile Architecture (SMA)**
  - **http://www.opengroup.org/pubs/catalog/e041.htm**
  - **Aspects of this architecture were previously briefed at IETF 73 HIPRG: http://www.ietf.org/proceedings/73/HIPRG.html**
- **Other related, interested standards bodies**
  - **Trusted Computing Group (TCG)**
  - **International Society of Automation (ISA)**
- **Technical contributors:**
  - **Steven Venema and David Mattes (draft co-authors)**
  - **Jeff Ahrenholz, Orlie Brewer, Eric Byres, Craig Dupler, Jin Fang, Darren Lissimore, Jeff Meegan, Richard Paine**

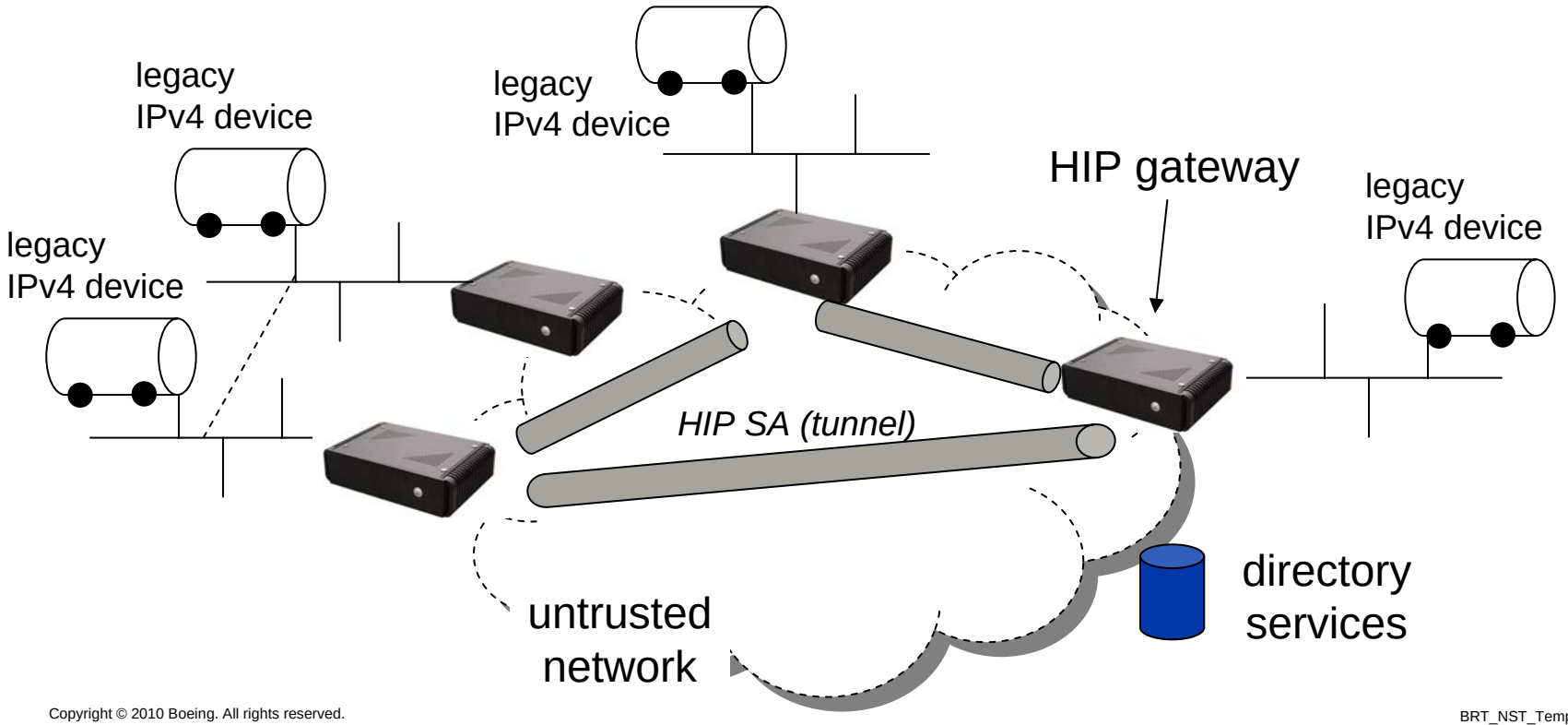
Use case

- **Provide a secure overlay for industrial control systems to operate over a less trusted, shared infrastructure IP network**

- 777 assembly line, Everett WA
- Supported by HIP overlays

Problem statement

- Provide layer-2 connectivity between SCADA (IPv4) devices



Why HIP?

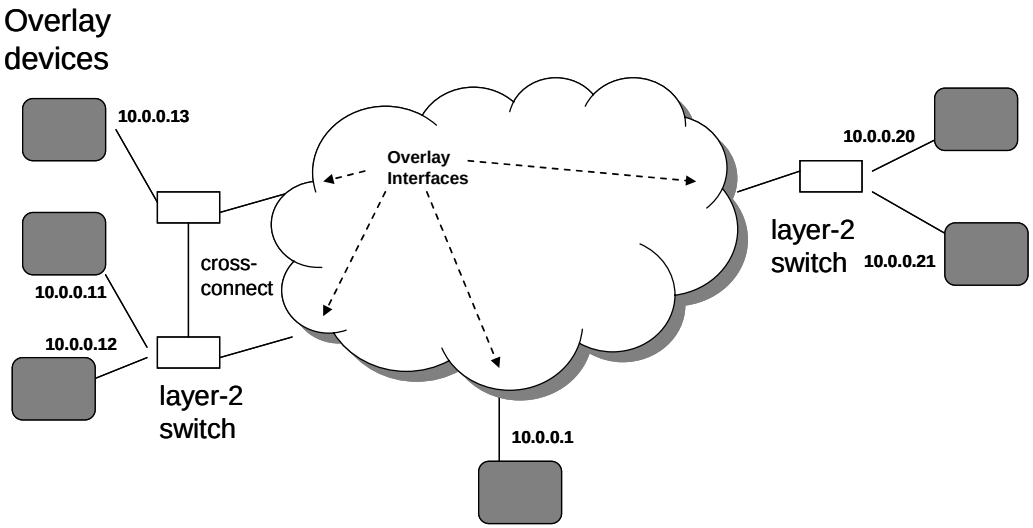
- **Existing VPN implementations and standards are tailored more towards the remote access environment**
  - **We envision the future need for *address family agility* and *mobility***
  - **We want to support *mesh-like* connectivity**

- **Particularly interested in the opportunity to deploy and provision in a *managed identity* environment**
  - **Identity and policy management in backend services such as LDAP and IF-MAP***

* http://www.infoblox.com/solutions/if-map.cfm

User view (existing prototype)

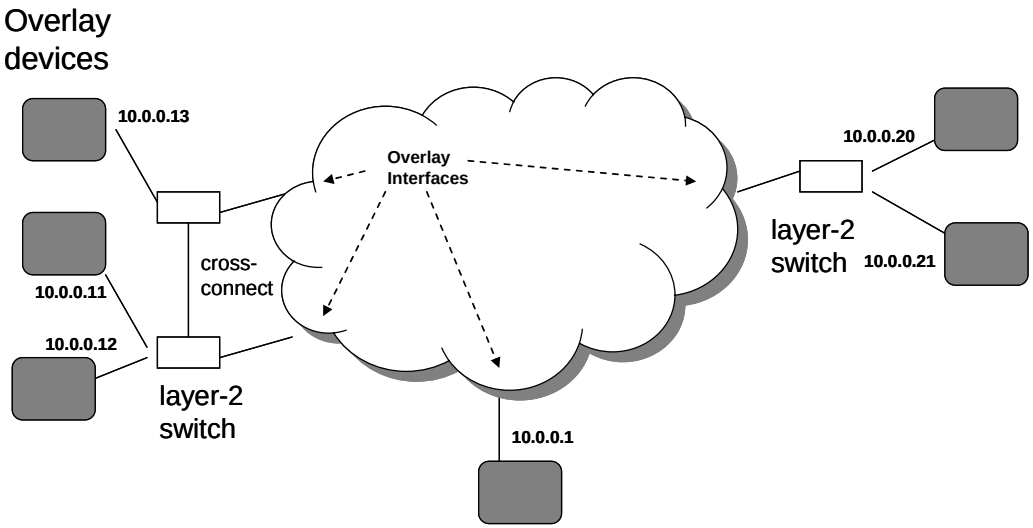
- **Overlay provides a "layer-2 VPN"-like service to legacy IPv4 devices**
  - **Illusion of a single L2 flooding domain (unicast, multicast)**
  - **IP traffic only**
  - **A given device may be reachable from more than one overlay interface**
  - **Ethernet MTU (1500 bytes) is supported**



User view (proposed specification)

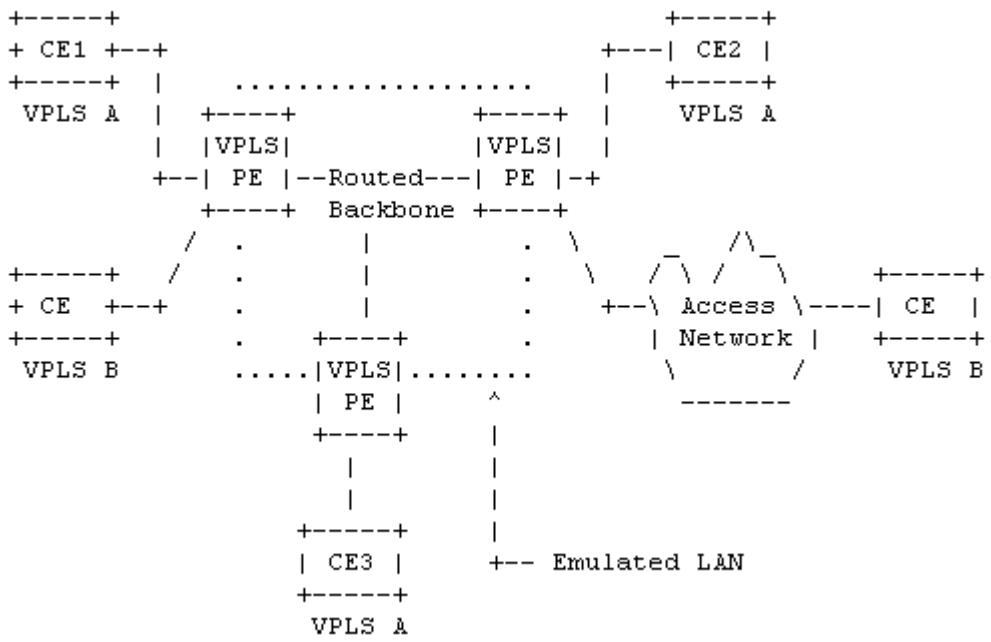
Relax the constraint that this support only IP traffic

- **Overlay provides a "layer-2 VPN"-like service to legacy ~~IPv4~~ devices**
  - **Illusion of a single L2 flooding domain (unicast, multicast)**
  - **~~IP traffic only~~** **All L2 traffic now desired**
  - **A given device may be reachable from more than one overlay interface**
  - **Ethernet MTU (1500 bytes) is supported**



Standards view

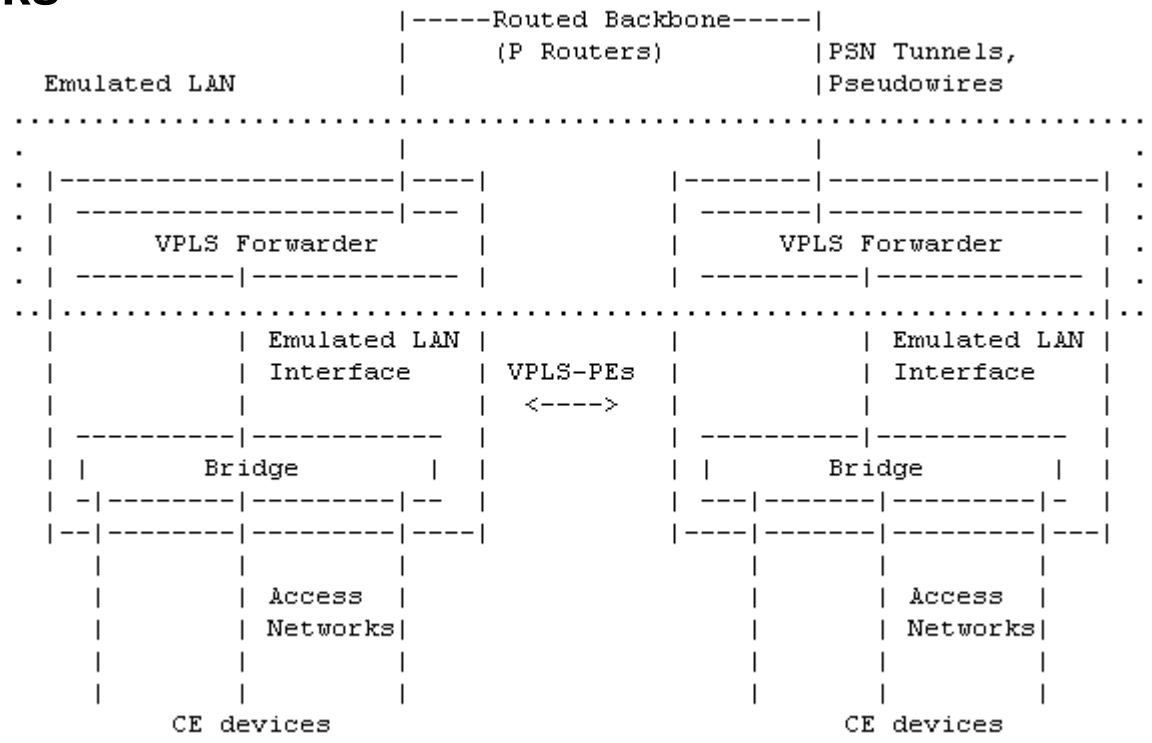
- **Virtual Private LAN Service (VPLS) defined in Section 2 of RFC 4664 “Frameworks for L2VPN”**



VPLS Reference Model (Figure 2 of RFC 4664)

Standards view (continued)

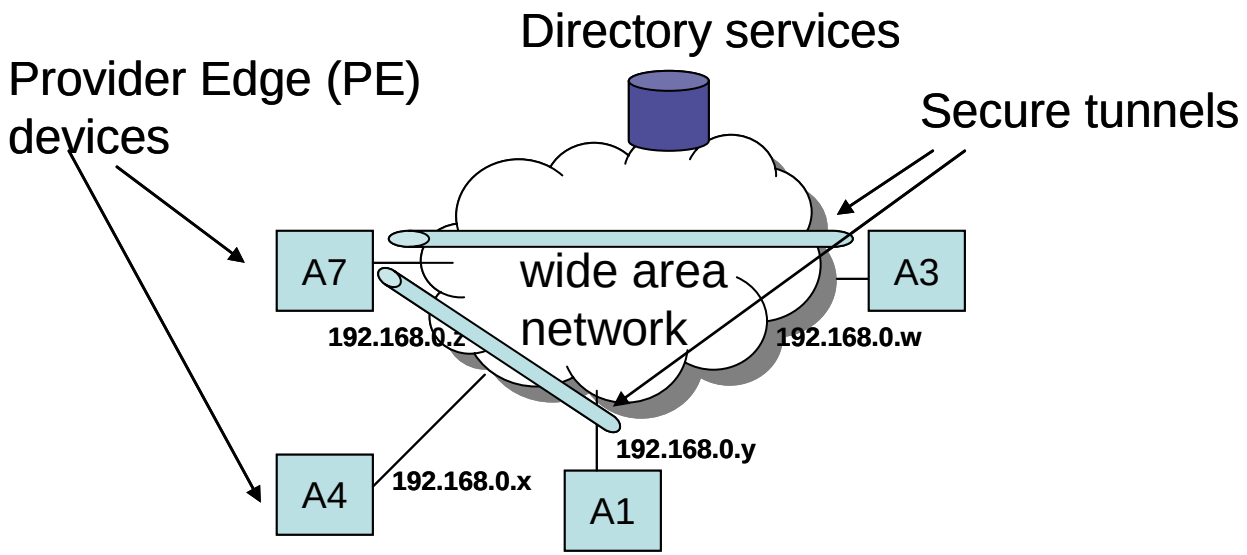
- **Service is described in Section 5 of RFC 4665 “Service Requirements for Layer 2 Provider-Provisioned Virtual Private Networks”**



VPLS-PE Reference Model (Figure 3 of RFC 4664)

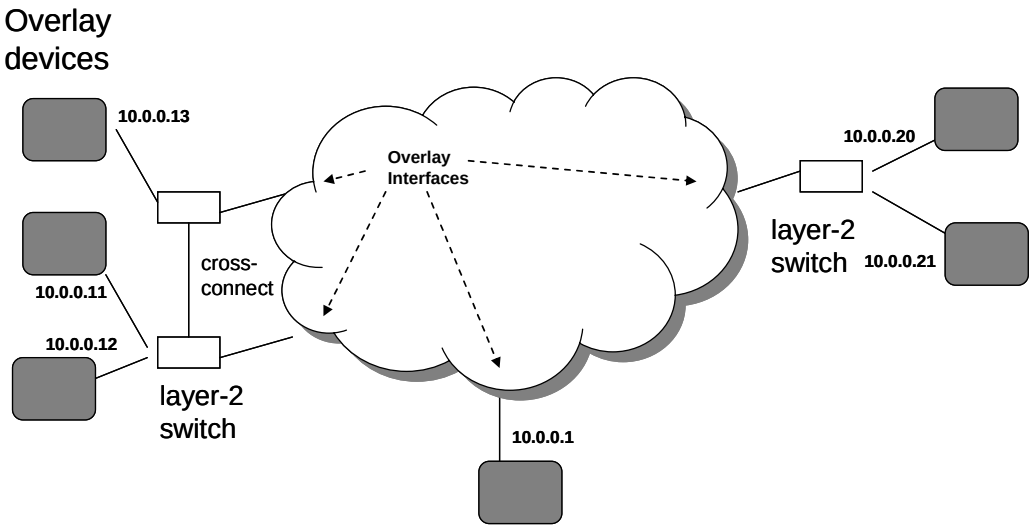
Implementation view

- **Secure tunneling between end points**
  - **HIP gateway-- a VPLS-PE device implementing HIP for the VPLS Forwarder functionality**
  - **May require directory services for tunnel endpoint discovery (overlay definition) and DNS (rendezvous) functions**



Naming view (deployment goals)

- **Multiple overlays supported**
  - **Each overlay has a unique name**
- **Each PE device has a name (an asset tag)**
  - **Also, a DNS name of form <asset-tag>.domain.com**
- **IP address ranges are allowed to overlap in the two domains**



Differences from existing HIP

- **HIP is deployed as a “bump-in-the-wire” (BITW) instead of “bump-in-the-stack” (BITS)**
- **Entire Ethernet frames are encapsulated (not ESP transport mode)**
- **Host identities in the system are bound via certificates to other names (asset tags)**
  - **Requires development of HIP CERT specification**
  - **Could be integrated to enterprise PKI**

Related Work

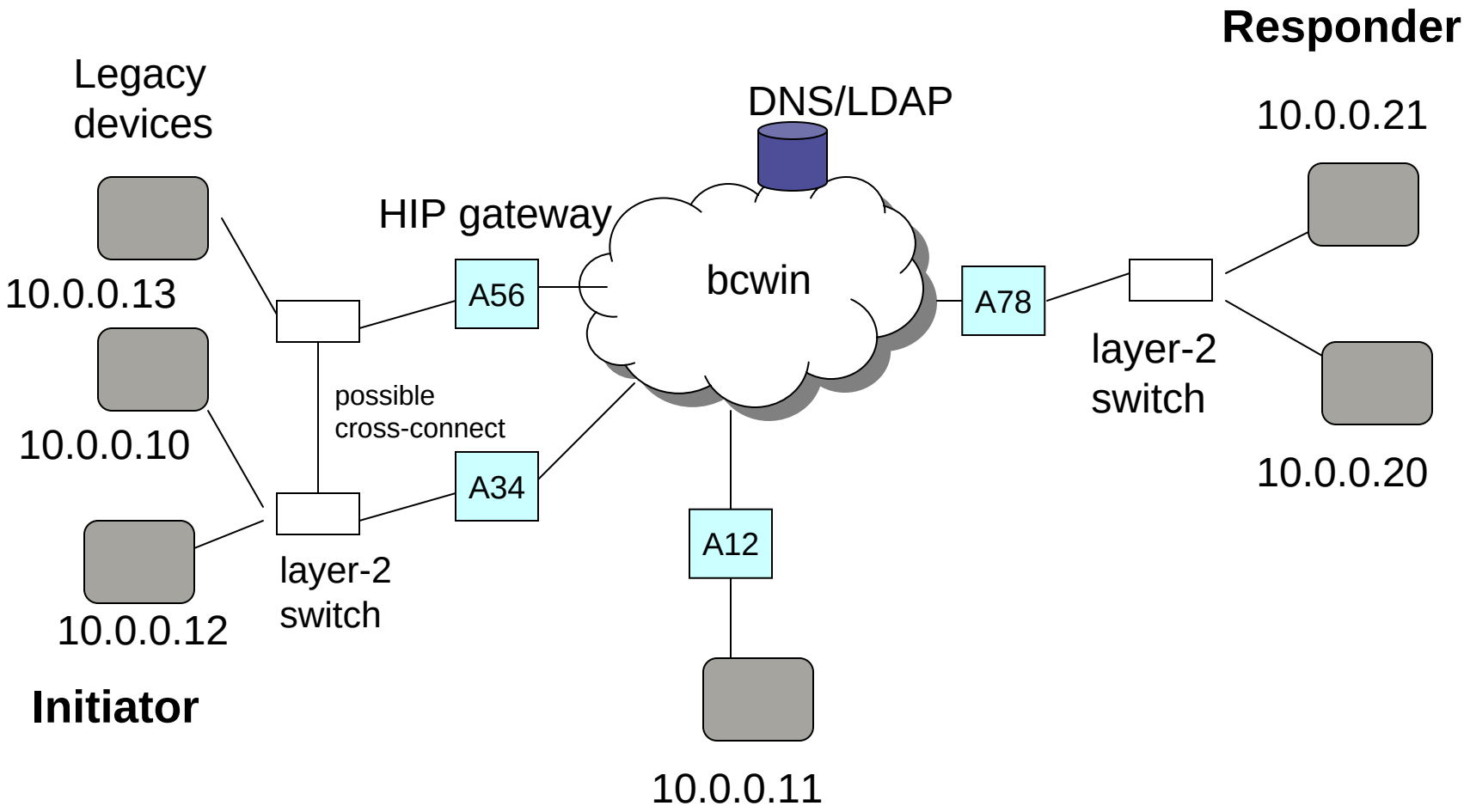
L2VPN solutions

- **Secure Pseudowire with IPsec/L2TPv3**
- **Microsoft Server and Domain Isolation**
- **OpenVPN project, supports ethernet bridging:**
  - **http://openvpn.net/index.php/documentation/miscellaneous/ethernet-bridging.html**

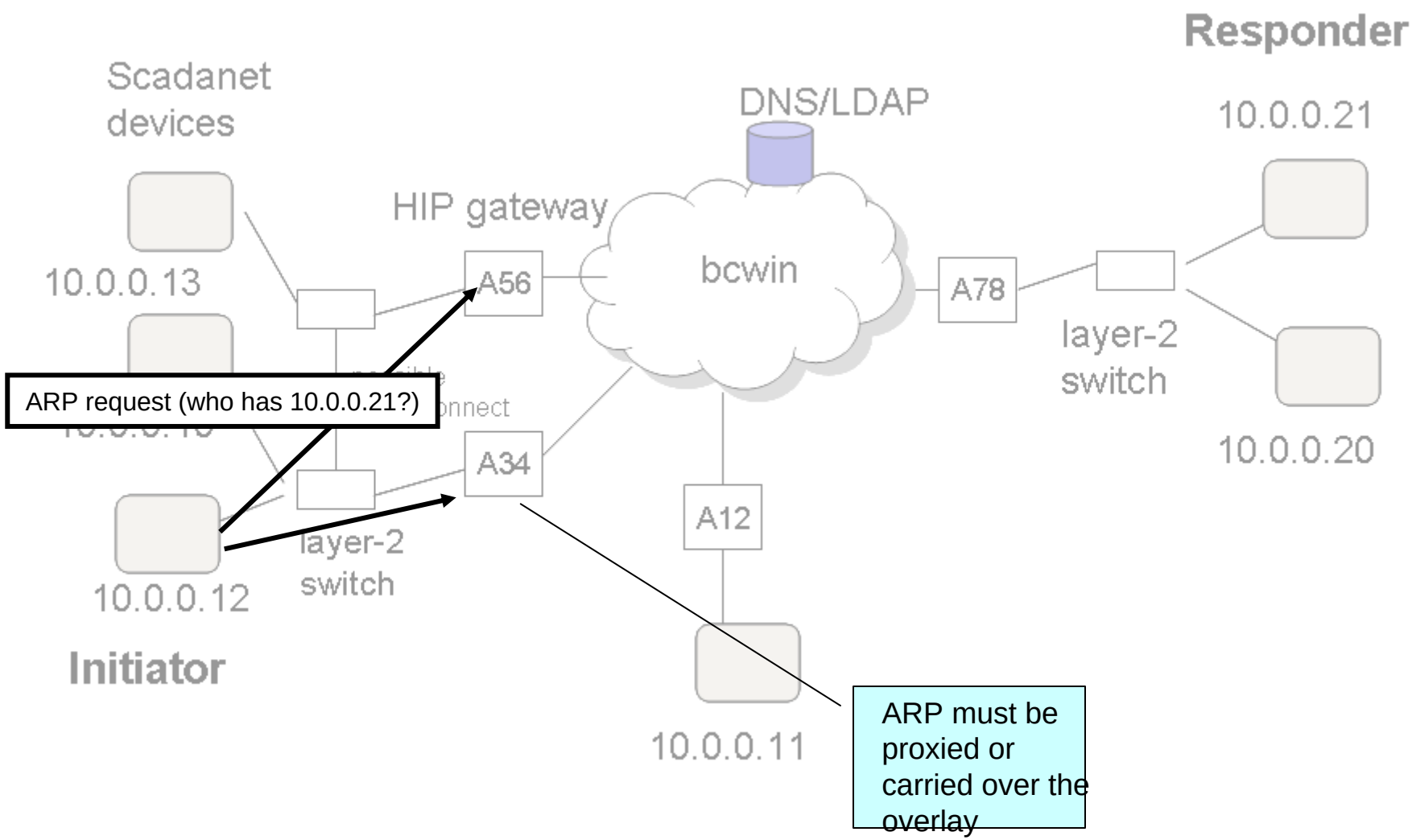
IP-oriented solutions

- **ISI X-Bone**
- **Virtual Enterprise Traversal (VET) with Subnetwork Encapsulation and Adaptation Layer (SEAL)**
  - **RFCs 5558 and 5320, and RFC 5720 (RANGER)**
- **HIP BONE**

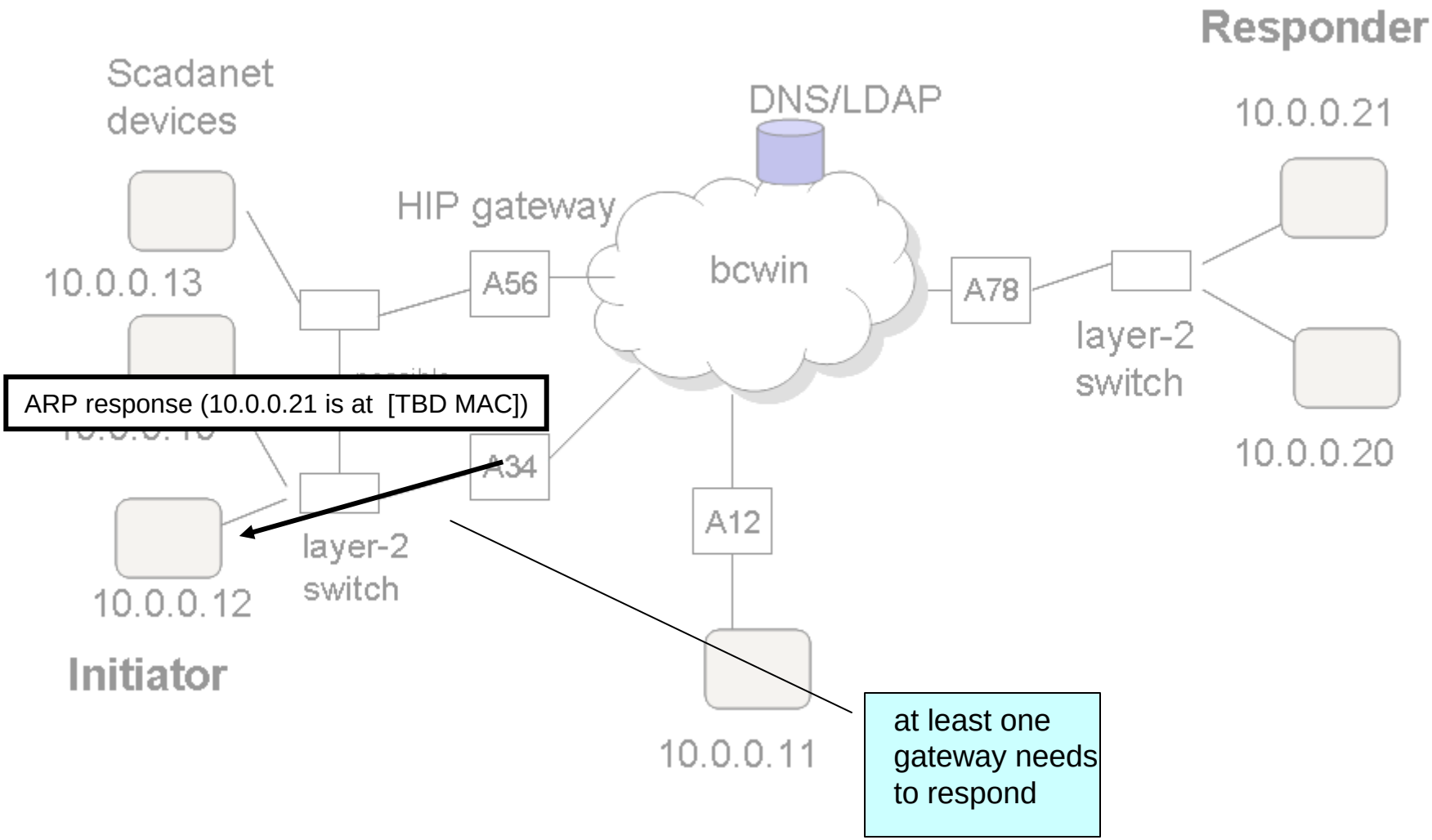
Walk-through



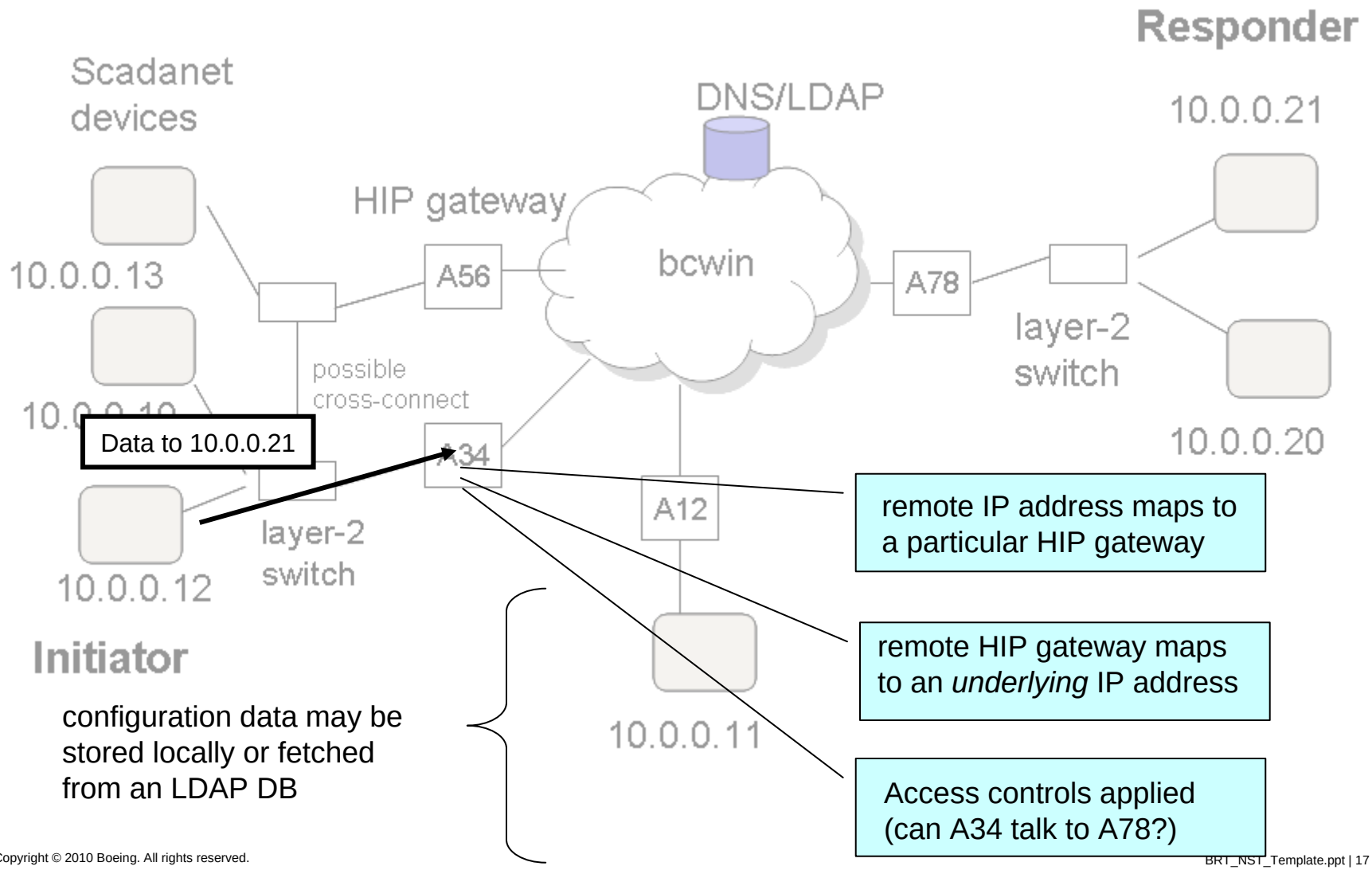
Walk-through



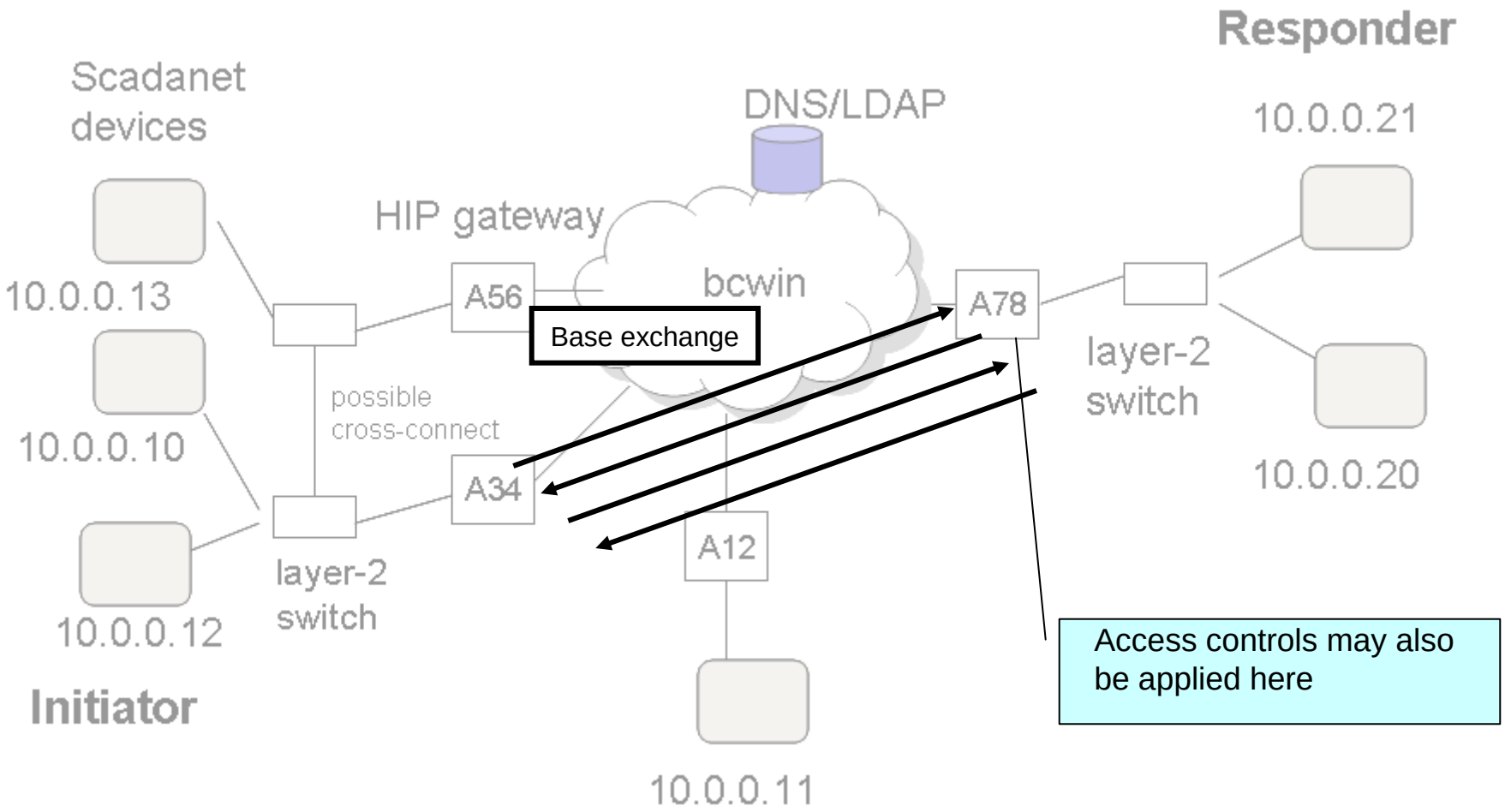
Walk-through



Walk-through



Walk-through



Walk-through