BGP L3VPN origin validation (draft-ymbk-l3vpn-origination-02)

November 2012

Problem Statement

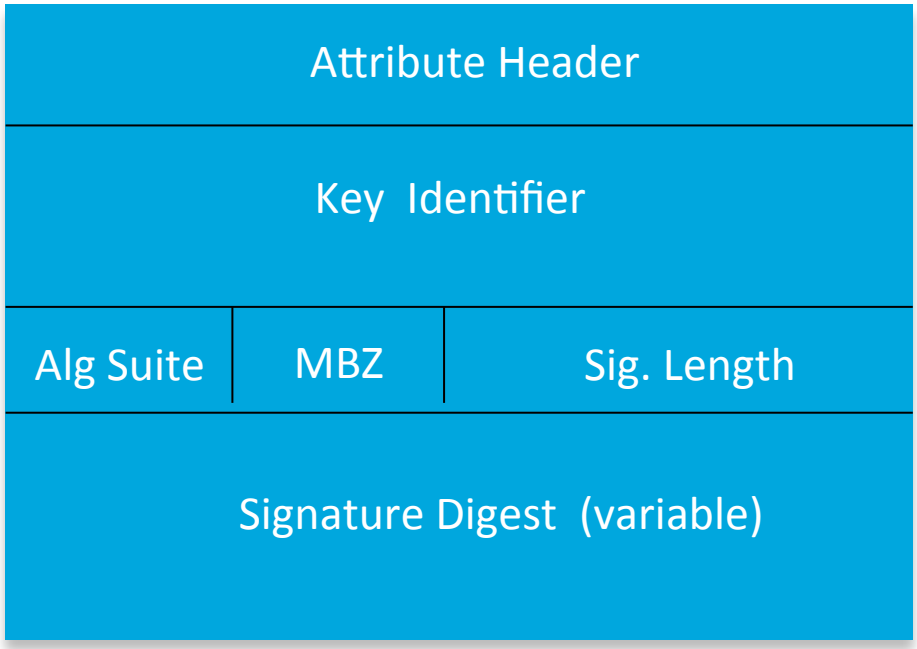
- It is currently possible for BGP based L3VPN routes to accidentally be sourced in a unintended manner in transit.
  - This is usually due to unintentional mis-configuration in a transit service provider (SP) resulting in VPN prefixes originating from the transit SP
  - Malicious attacks are also possible.
- No mechanism in place to authenticate VPN prefixes in terms of origin validation.
- The draft (draft-ymbk-l3vpn-origination-02) attempts to define one such scheme.

BGP L3VPN origin validation– Scheme Description

- Originator of the VPN route signs BGP update using a secret key
- The scheme does not mandate a PKI, though one may be used, and symmetric or asymmetric keys may be used
- The originator and validator have a trust agreement where they agree upon a secret key and associated Key Identifier.
- Key Identifier is a opaque value used to identify the context of the key in the BGP update. Often the VPN-ID can be used as the Key Identifier.
- The signature digest generated from the associated key is carried in a new BGP attribute and is validated at the receiver end by retrieving the key from the key Identifier context and computing the equivalent signature digest.

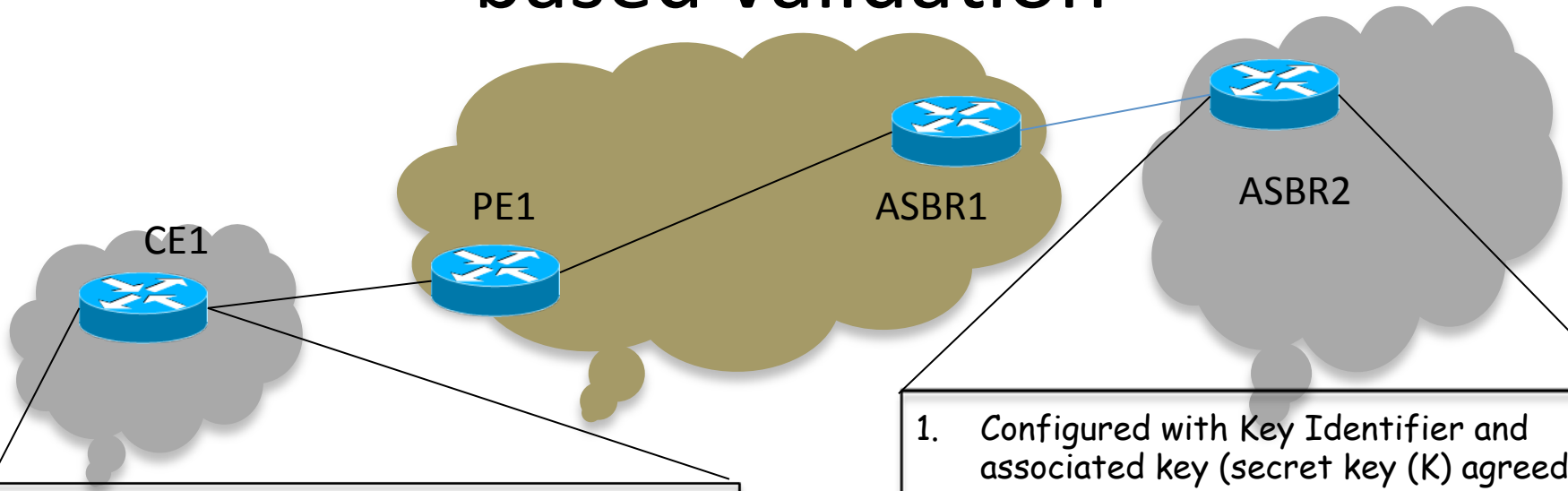
BGP L3VPN origin validation – BGP extensions

- A new optional transitive attribute defined in BGP to carry the signature digest.



- Signature digest is generated as
  - Signature = sign (hash (Prefix/Len || Key Identifier))
- Single BGP Prefix per update to maintain integrity of signature.

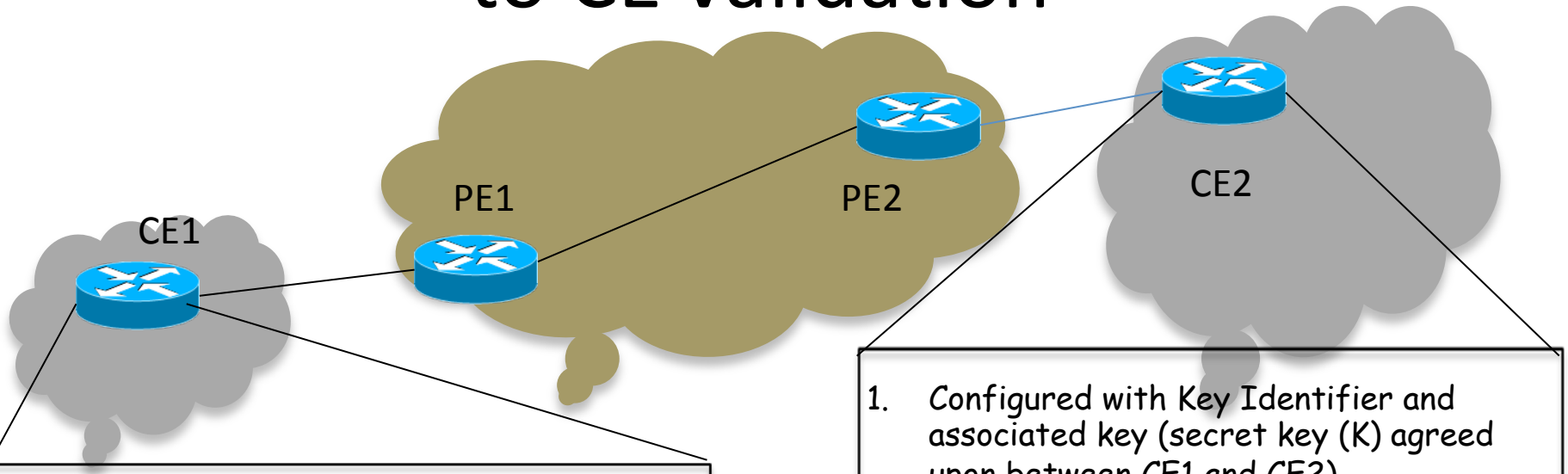
BGP L3VPN origin validation – Provider based validation



1. Configured with Key Identifier and associated key (secret key (K) agreed upon between CE1 and ASBR2)
2. Originates Prefix and signs it with secret key to generate sig. digest -
   Signature = sign (K) (hash (Prefix || Key Identifier)) carried in L3POA
3. BGP update sent - single Prefix per update along with PATH attribute

1. Configured with Key Identifier and associated key (secret key (K) agreed upon between CE1 and ASBR2)
2. Validates BGP Updates from ASBR1 by computing verification digest using secret key (K) corresponding to key ID from BGP update as well as associated Prefix
   Verify_Signature = sign (K) (hash (Prefix || Key Identifier in rcvd update))
3. If verify_signature matches signature in PATH attribute the BGP update is classified as valid, else invalid.

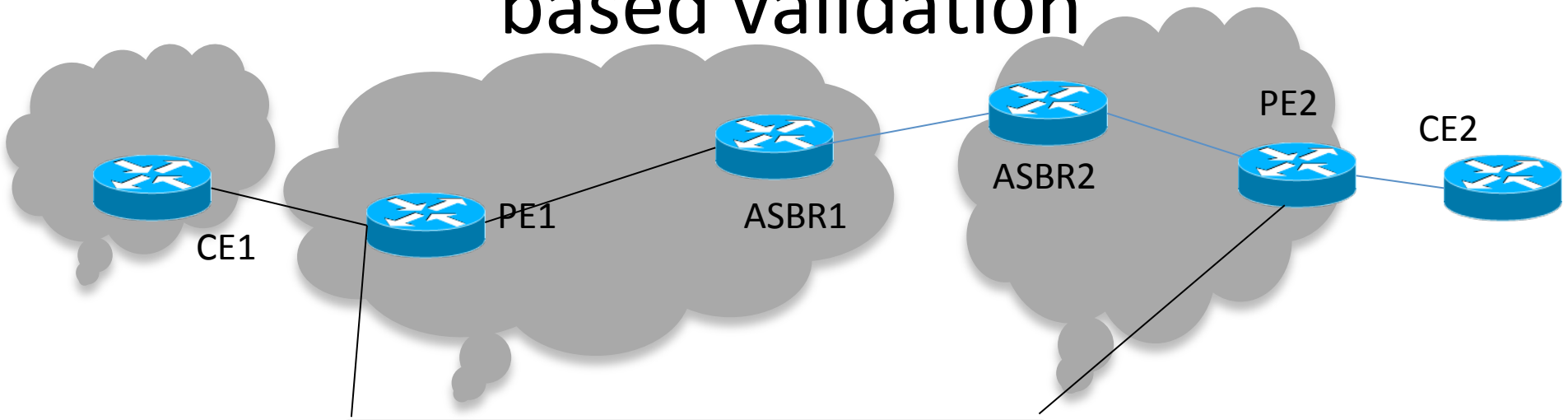
BGP L3VPN origin validation – End CE to CE validation



1. Configured with Key Identifier and associated key (secret key (K) agreed upon between CE1 and CE2)
2. Originates NLRI and signs it with secret key to generate sig. digest -
   Signature = sign (K) (hash (Prefix || Key Identifier))
   carried in L3POA attribute
3. BGP update sent - single Prefix per update along with PATH attribute

1. Configured with Key Identifier and associated key (secret key (K) agreed upon between CE1 and CE2)
2. Validates BGP Updates from PE2 by computing verification digest using secret key (K) corresponding to key ID from BGP update as well as associated Prefix
   Verify_signature = sign (K) (hash (Prefix || Key Identifier))
3. If verify_signature matches signature in PATH attribute the BGP update is classified as valid, else invalid.

BGP L3VPN origin validation– PE - PE based validation



1. Here PEs, possibly across ASes, agree on the keying.
2. The Key Identifier and associated keys would normally be configured on a per VPN basis, with the PE1 signing and PE2 validating similarly
3. Here we are protected against route originating from unauthorized PEs.

BGP L3VPN origin validation - Advantages

- Origin validation for common L3VPN scenarios (inclusive of InterAS) – Provider based and CE based validation
- Does not mandate a PKI and can provide for lightweight authentication.
- Only end routers need to be aware of the new mechanism. Intermediate speakers do not need to be aware/upgraded so incrementally deployable