Remote Site Connectivity

GRE / IPsec

Remote Connectivity

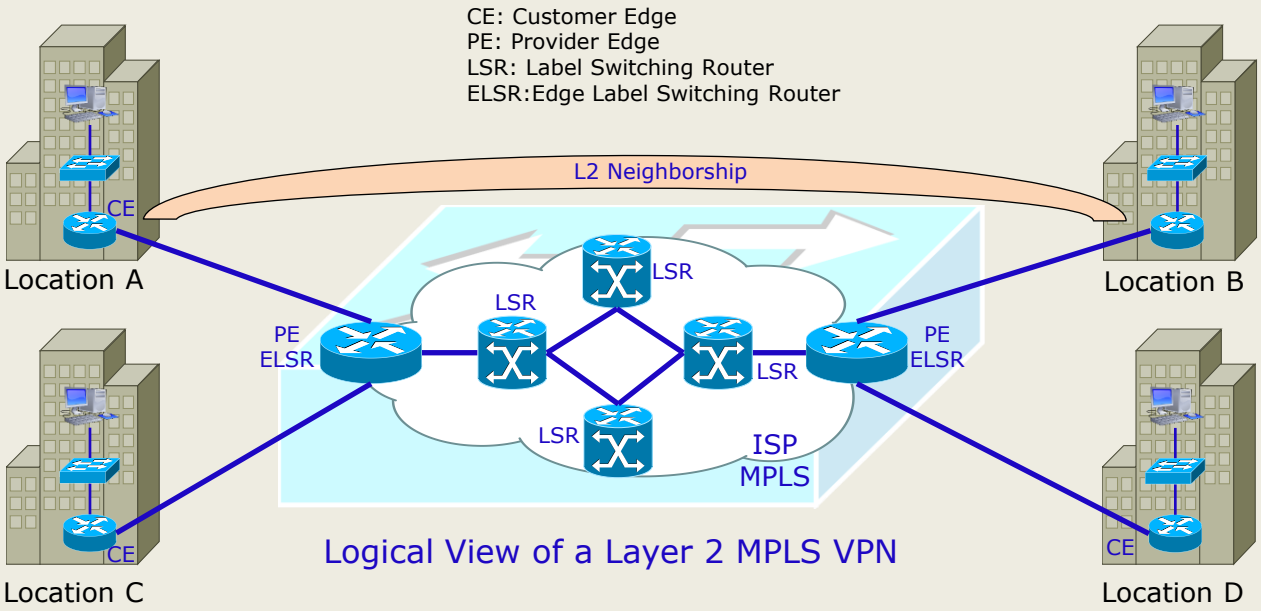
- The voice, video, and data commonly sent between remote offices and central sites often demand low latency and easy provisioning, all while maintaining a low cost.
- Traditional WAN solutions (i.e., Leased lines, Frame Relay, and ATM) typically fail to simultaneously meet all these requirements.
- With the current state of the Internet, high-speed connections are widely accessible.
- A remote site office might purchase a DSL or cable modem connection to the Internet, at a relatively low cost as compared to traditional leased lines or frame/cell switching technologies.
- Over that Internet connection, a virtual private network (VPN) could create a logical path between the site office and the HQ location.

MPLS-Based Virtual Private Networks

- Multiprotocol Label Switching (MPLS) is a technology commonly used by service providers, although many large enterprises also use MPLS for their backbone network.
- MPLS makes forwarding decisions based on labels rather than IP addresses.
- Specifically, a 32-bit label is inserted between a frame's Layer 2 and Layer 3 headers.
- As a result, an MPLS header is often called a shim header, because it is stuck in between two existing headers.
- MPLS-based VPNs can be grouped into one of two primary categories:
  - Layer 2 MPLS VPNs
  - Layer 3 MPLS VPNs

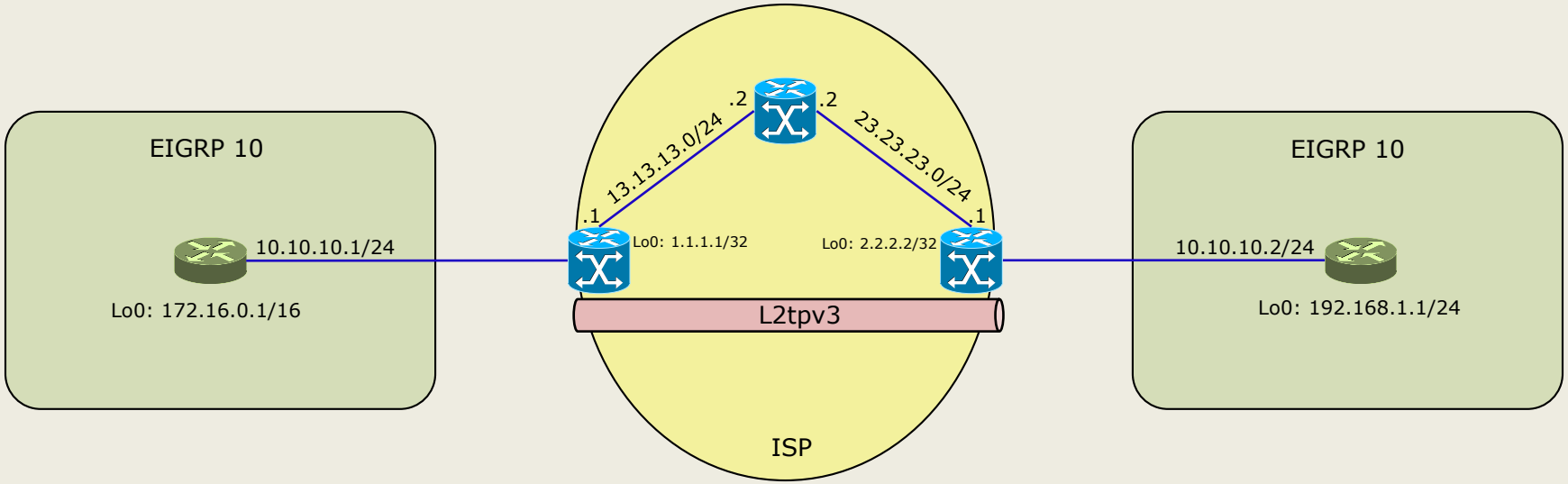
Layer 2 MPLS VPN

- With a Layer 2 MPLS VPN, the MPLS network allows customer edge (CE) routers at different sites to form routing protocol neighborships with one another as if they were Layer 2 adjacent. Therefore, you can think of a Layer 2 MPLS VPN as a logical Layer 2 switch.



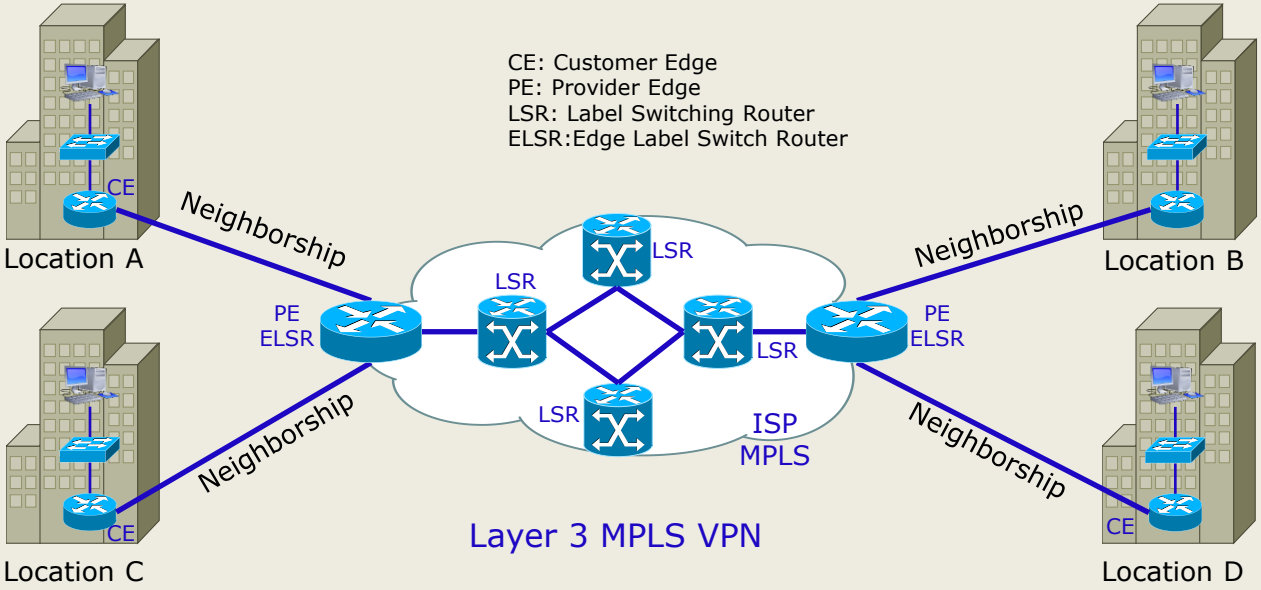
Logical View of a Layer 2 MPLS VPN

L2TP



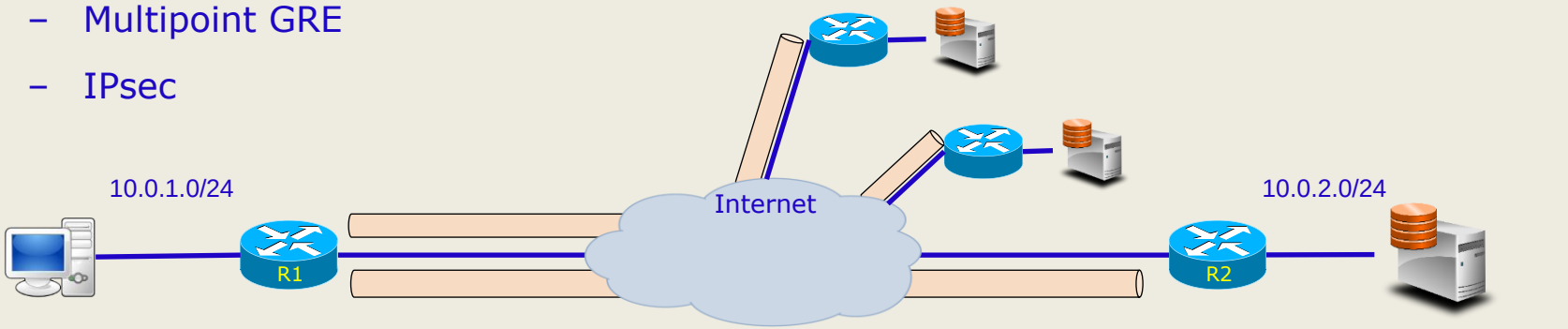
Layer 3 MPLS VPN

- With a Layer 3 MPLS VPN, a service provider's provider edge (PE) router establishes a peering relationship with a CE router. Routes learned from the CE router are then sent to the remote PE router in the MPLS cloud where they are sent out to the remote CE router.



Tunnel-Based Virtual Private Networks

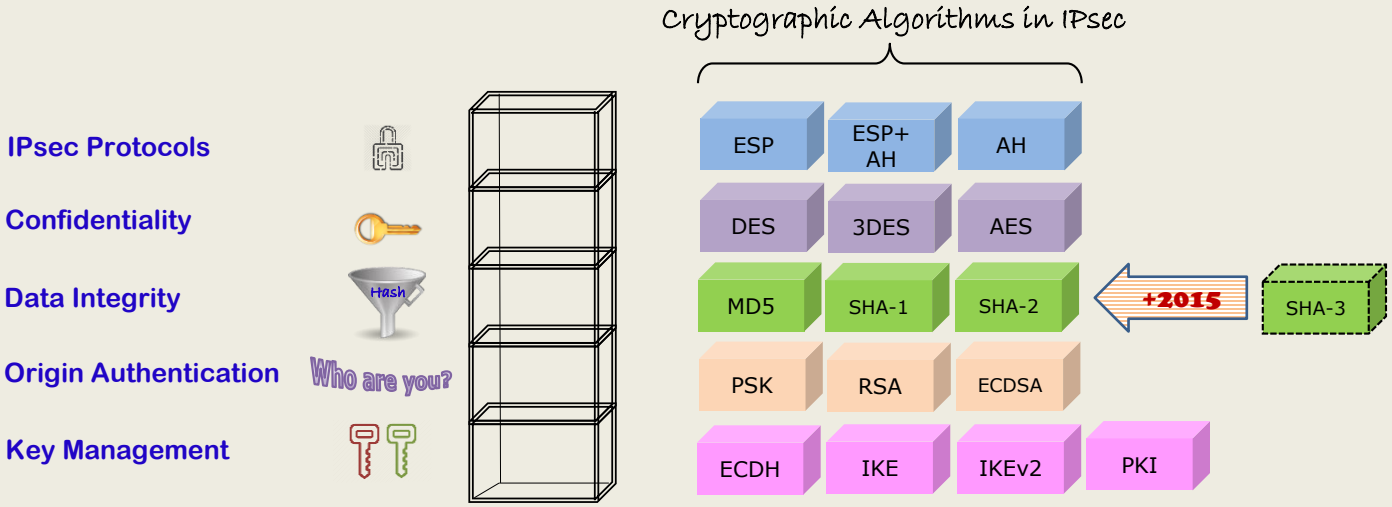
- A tunnel is a virtual connection that can physically span multiple router hops.
- However, from the perspective of the traffic flowing through the tunnel, the transit from one end of a tunnel to the other appears to be a single router hop.
- Multiple VPN technologies make use of virtual tunnels.
  - Generic Routing Encapsulation (GRE)
  - Dynamic Multipoint VPN (DMVPN)
  - Multipoint GRE
  - IPsec



IPsec

IPsec Framework

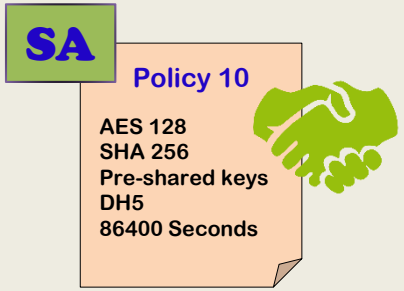
- IPsec is a framework of open standards that spells out the rules for secure communications. IPsec relies on existing algorithms to implement encryption, authentication, and key exchange.



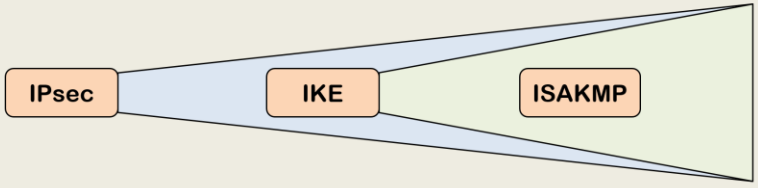
- IPsec is in use today for both remote-access VPNs and site-to-site VPNs.

Internet Key Exchange (IKE)

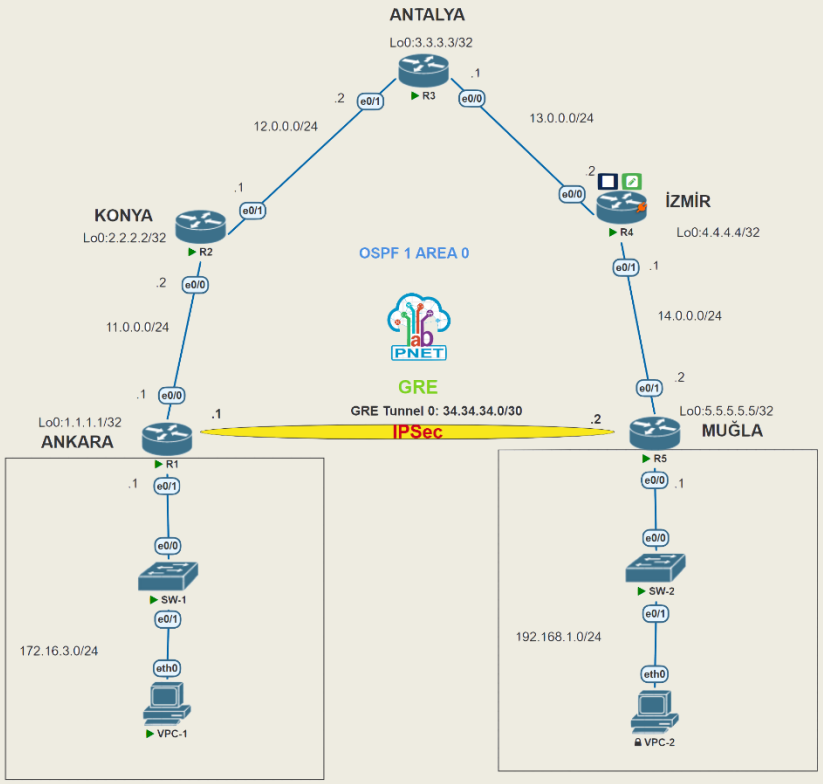
- **IPsec** implements a VPN solution using an encryption process that involves the periodic changing of encryption keys. **IPsec uses the IKE protocol to authenticate a peer computer and to generate encryption keys.**
- **IKE negotiates a SA.** An SA is an agreement between two peers engaging in an IPsec exchange, and the SA consists of all the required parameters that are necessary to establish successful communication.



- IPsec uses the IKE protocol to provide these functions:
  - Negotiation of SA characteristics
  - Automatic key generation
  - Automatic key refresh
  - Manageable manual configuration



IPsec



IPsec

```
ANKARA(config)#crypto isakmp enable

ANKARA(config)#crypto isakmp policy 10
ANKARA(config-isakmp)#authentication pre-share
ANKARA(config-isakmp)#encryption 3des
ANKARA(config-isakmp)#hash sha
ANKARA(config-isakmp)#group 2
ANKARA(config-isakmp)#end


ANKARA# show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
encryption algorithm:Three key triple DES
hash algorithm:Secure Hash Standard
authentication method:Pre-Shared Key
Diffie-Hellman group:#2 (1024 bit)
lifetime:86400 seconds, no volume limit
```

IPsec

```
MUGLA# show crypto ipsec sa

interface: Ethernet0/1
    Crypto map tag: S2S-MAP, local addr 14.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (172.16.3.0/255.255.255.0/0/0)
   current_peer 11.0.0.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 14.0.0.2, remote crypto endpt.: 11.0.0.1
     path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/1
     current outbound spi: 0x9C256F77(2619699063)
```

QUESTIONS?

Prepared by Ayhan KOŞAR
ayhankosar@gmail.com
www.inetworkeskisehir.com
ayhan.k@inetworkeskisehir.com

linkedin.com/in/ayhankosar