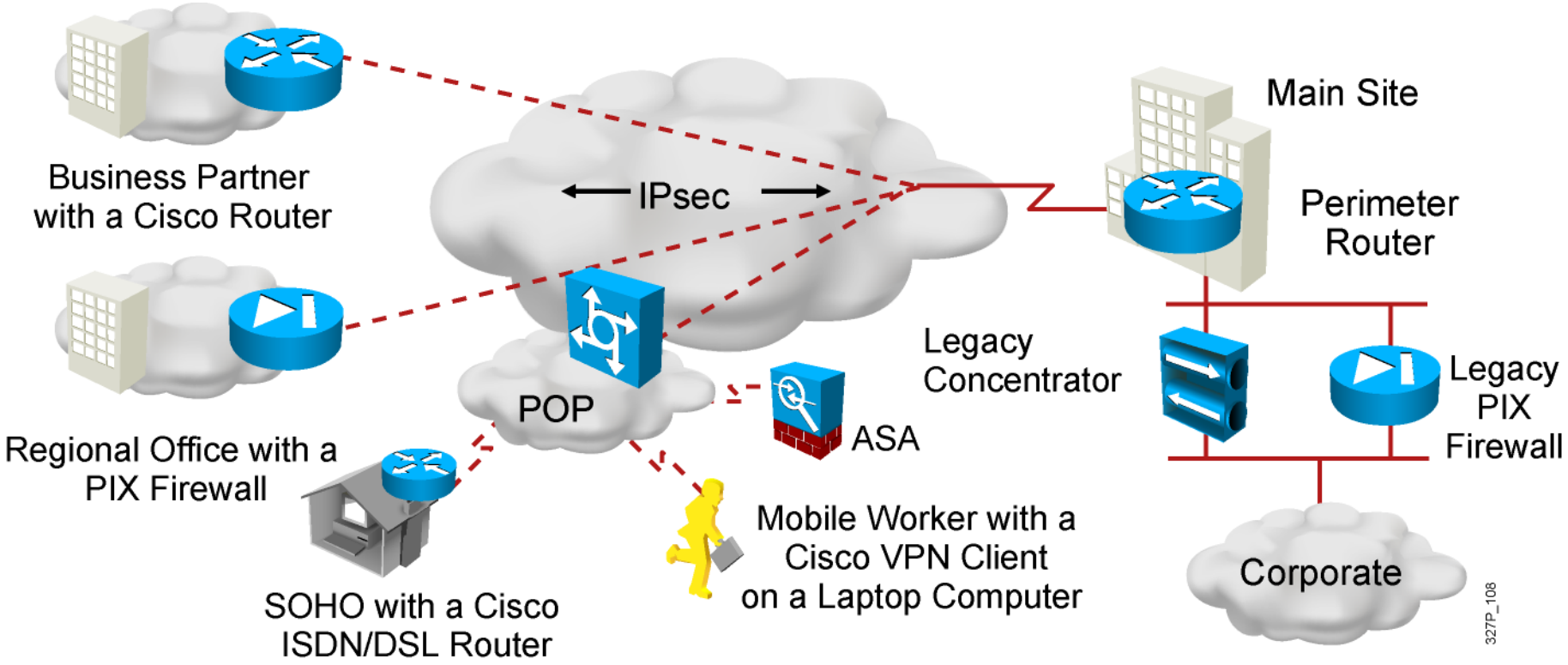
Introducing VPN Solutions

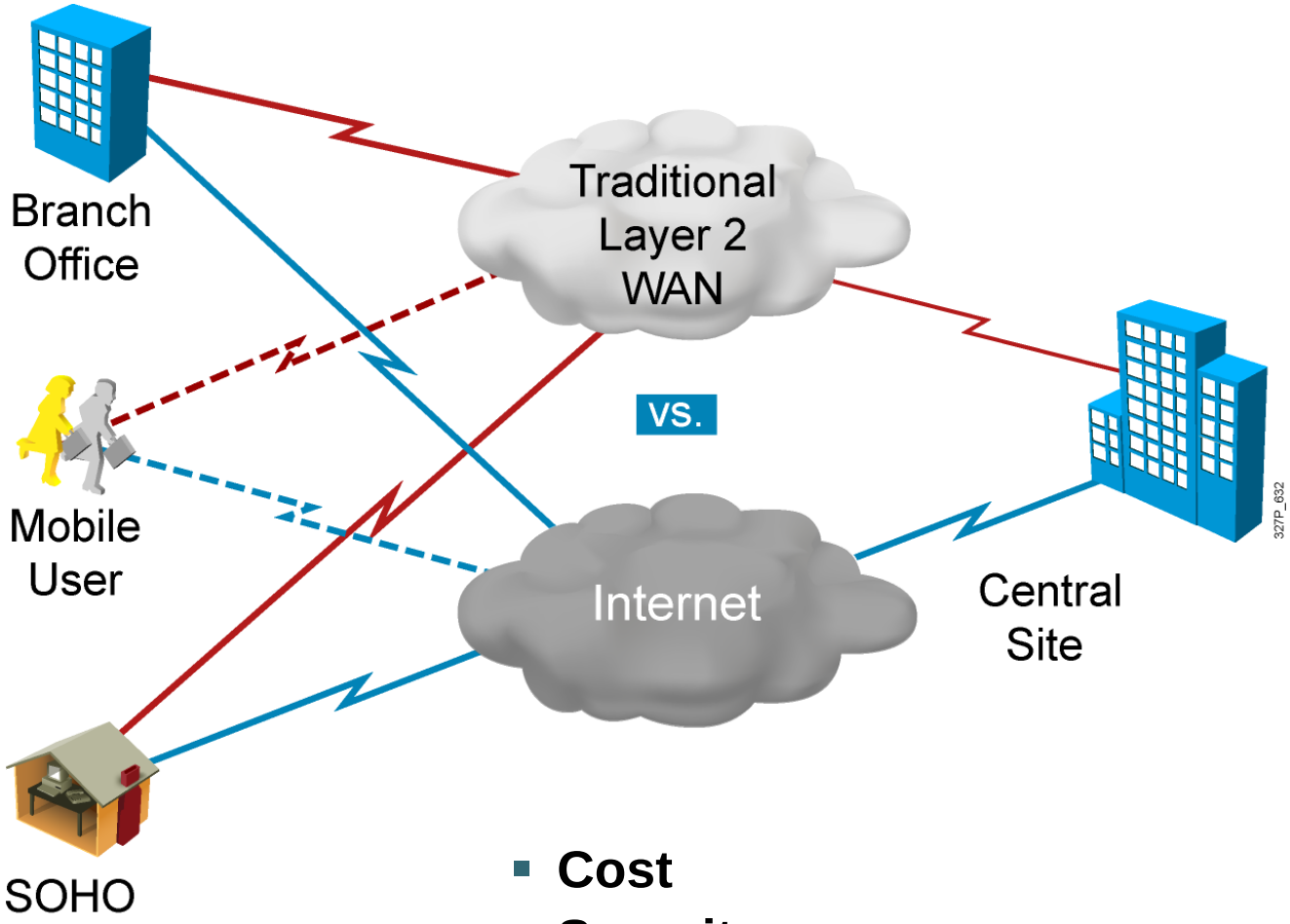
What Is a VPN?



Virtual: Information within a private network is transported over a public network.

Private: The traffic is encrypted to keep the data confidential.

Benefits of VPN



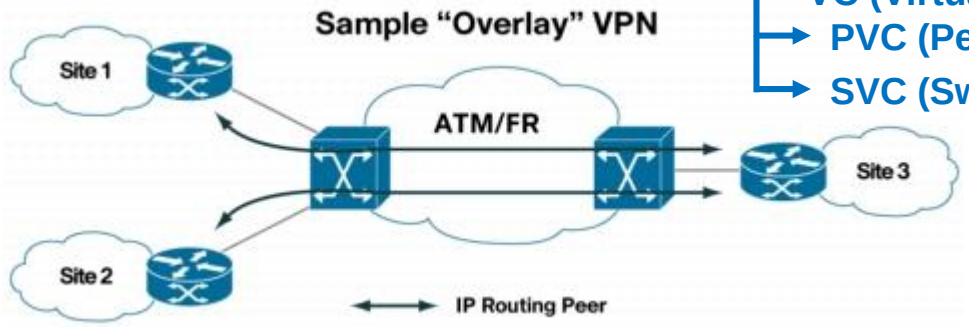
- **Cost**
- **Security**
- **Scalability**

VPN Models

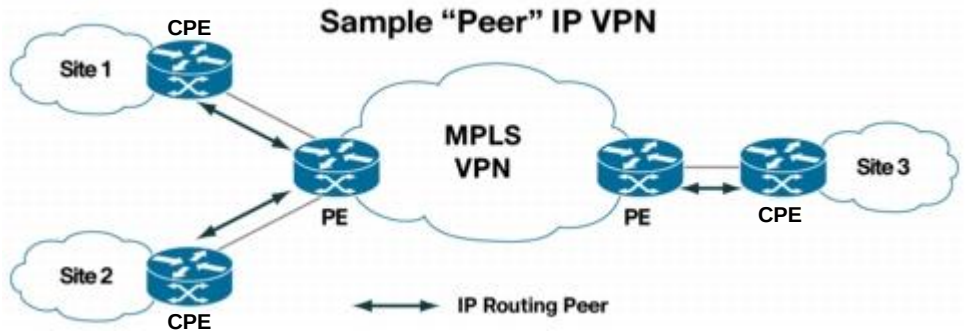
VPN services can be offered based on two major models:

- **Overlay VPNs, in which the service provider provides virtual point-to-point links between customer sites**

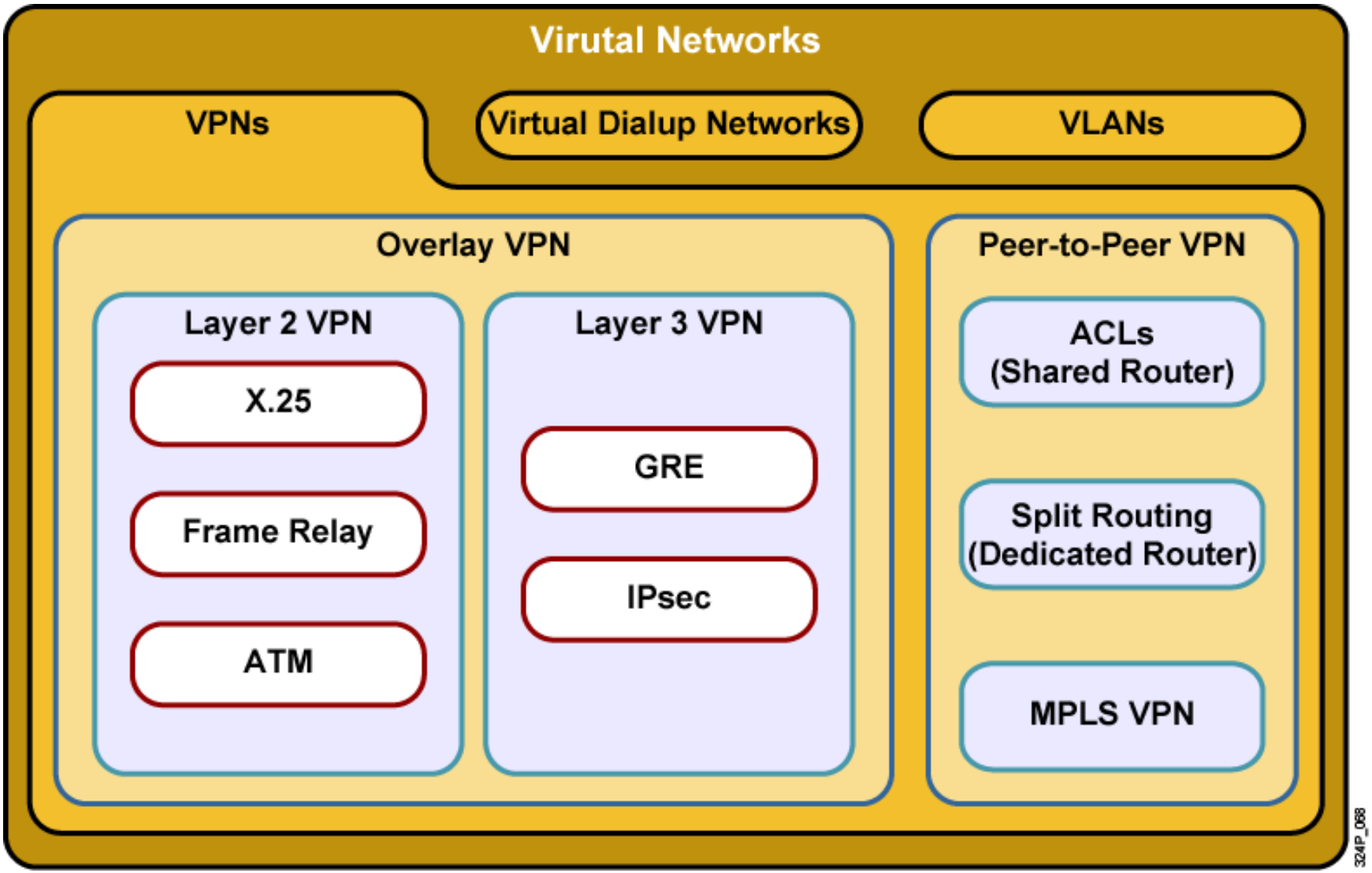
VC (Virtual Circuit)
- PVC (Permanent Virtual Circuit)
- SVC (Switched Virtual Circuit)



- **Peer-to-peer VPNs, in which the service provider participates in the customer routing**



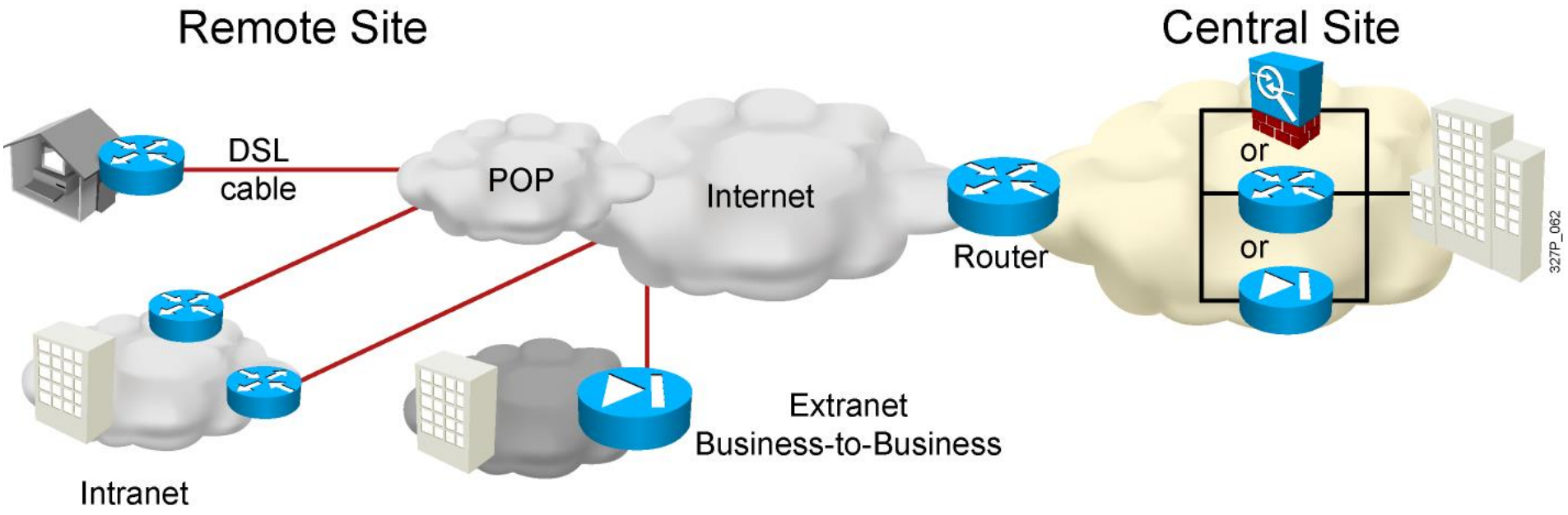
VPN Taxonomy



IPsec VPN Deployment

- **Internet Protocol Security (IPsec) is a network protocol suite that authenticates and encrypts the packets of data sent over a network.**
- **Site-to-site VPNs**
  - Fully meshed (static)
  - Hub (static) and spoke (dynamic)
  - Fully meshed on demand (dynamic)
  - DMVPN
- **Remote-access VPNs**
  - Cisco Easy VPN
  - WebVPN (Cisco IOS SSL VPN)

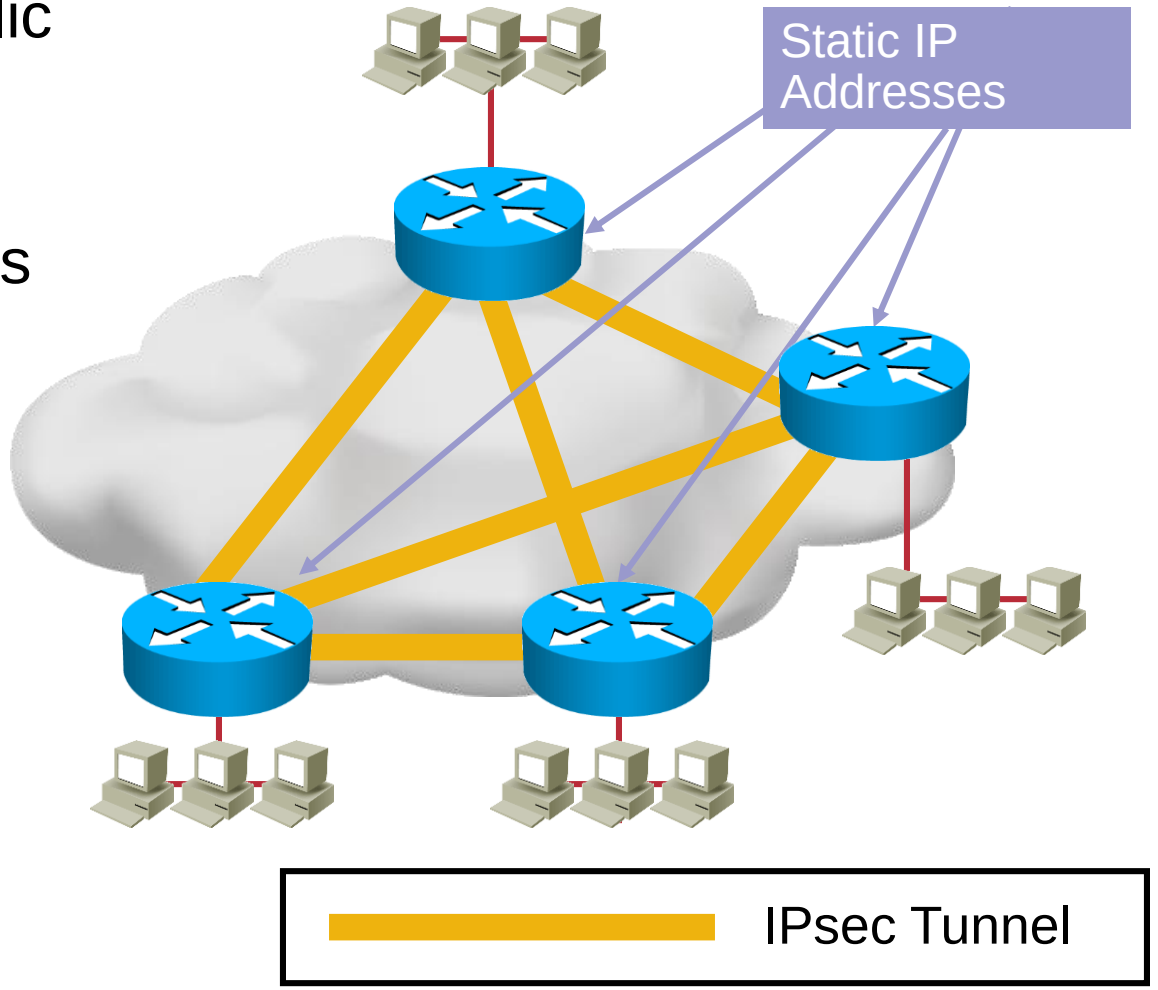
Site-to-Site VPNs



Site-to-site VPN: extension of classic WAN

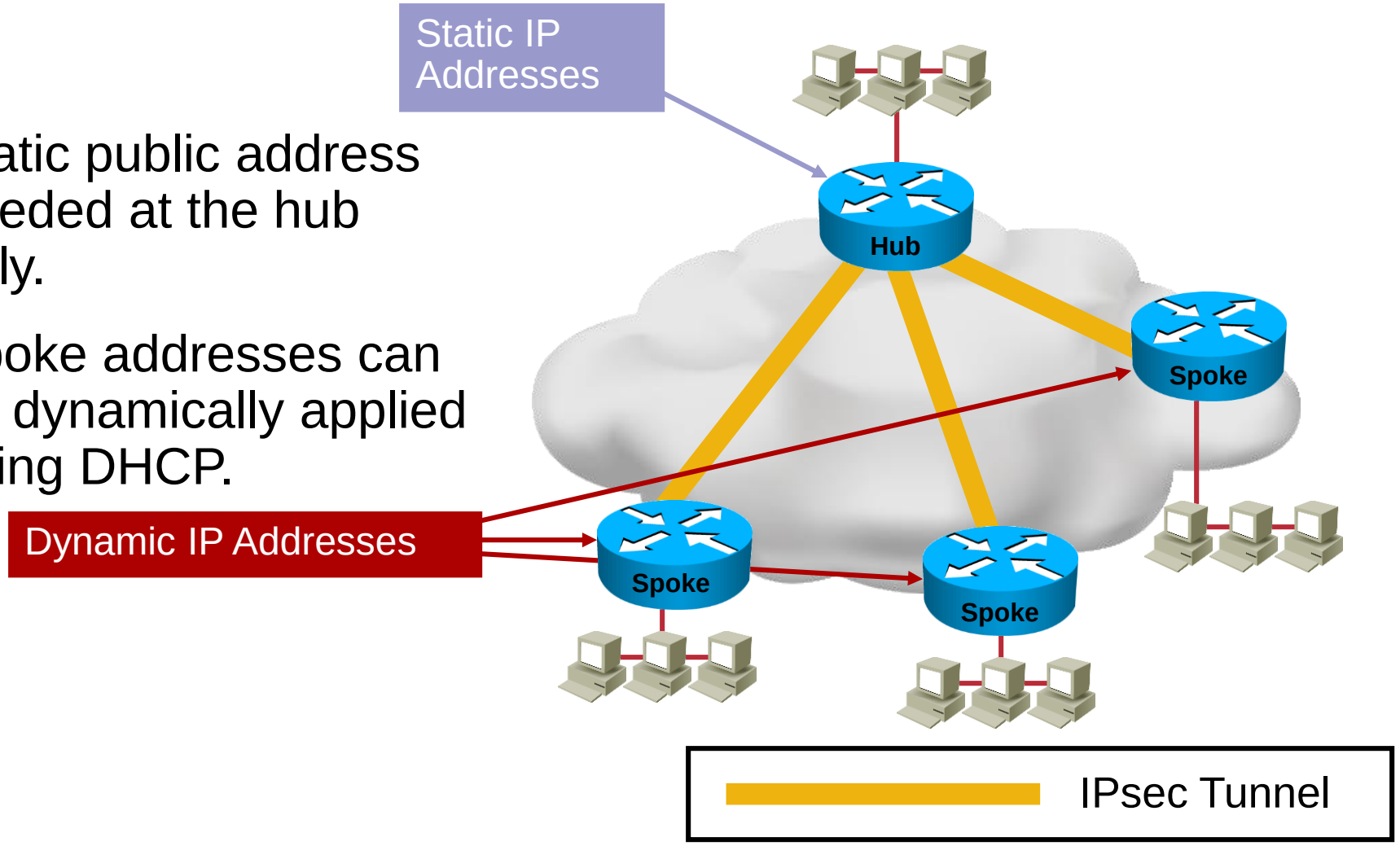
Fully Meshed VPNs

- There are static public addresses between peers.
- Local LAN addresses can be private or public.



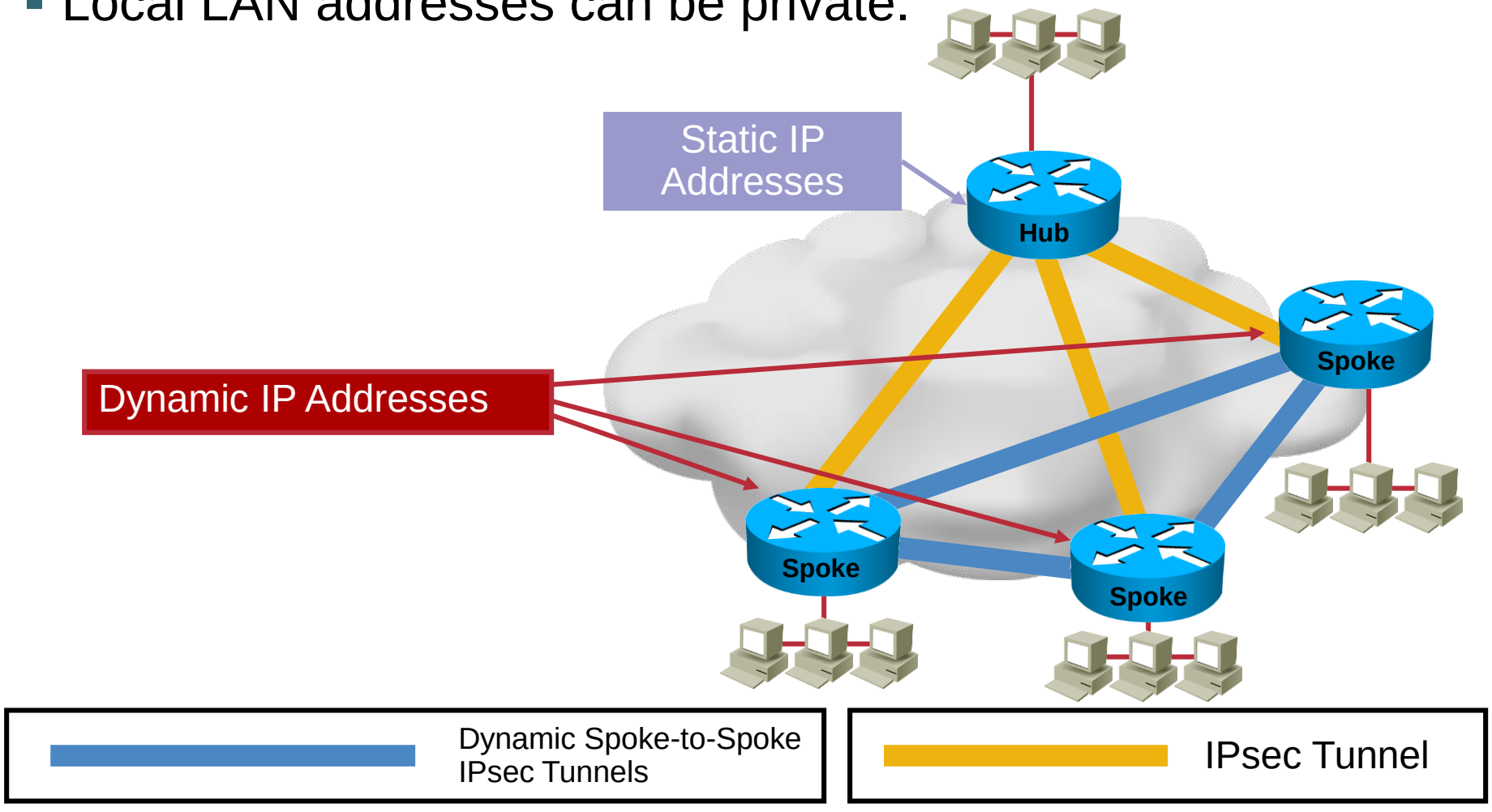
Hub-and-Spoke VPNs

- Static public address needed at the hub only.
- Spoke addresses can be dynamically applied using DHCP.

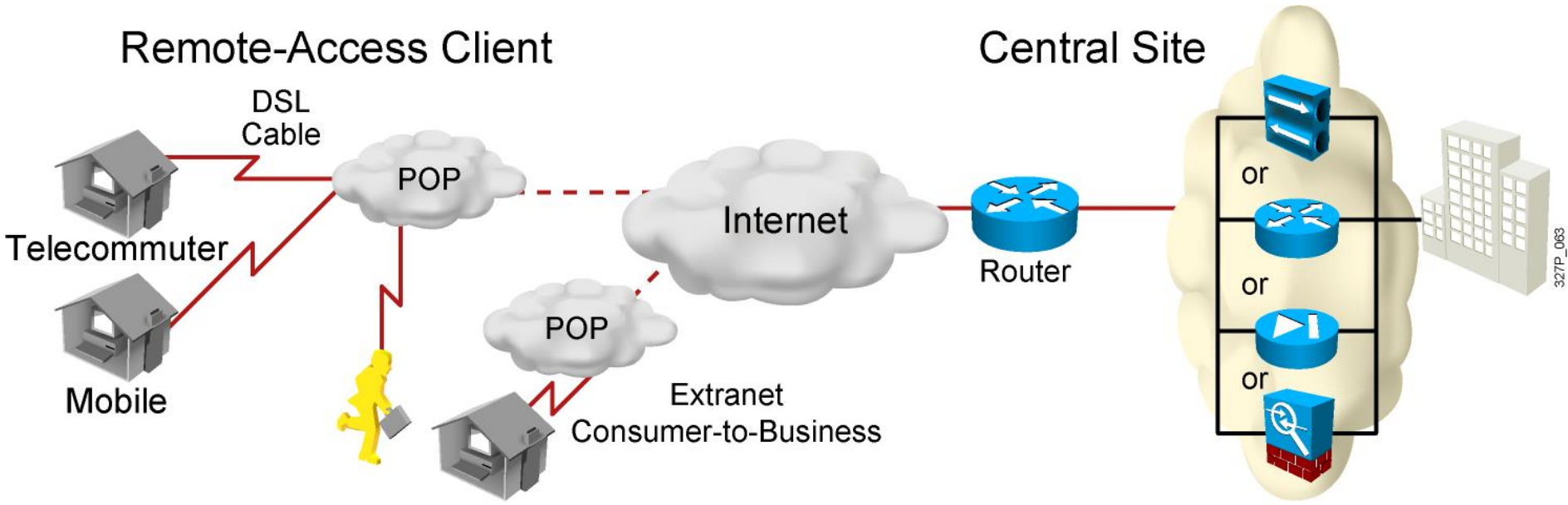


Dynamic Multipoint VPNs (DMVPN)

- Local LAN addresses can be private.



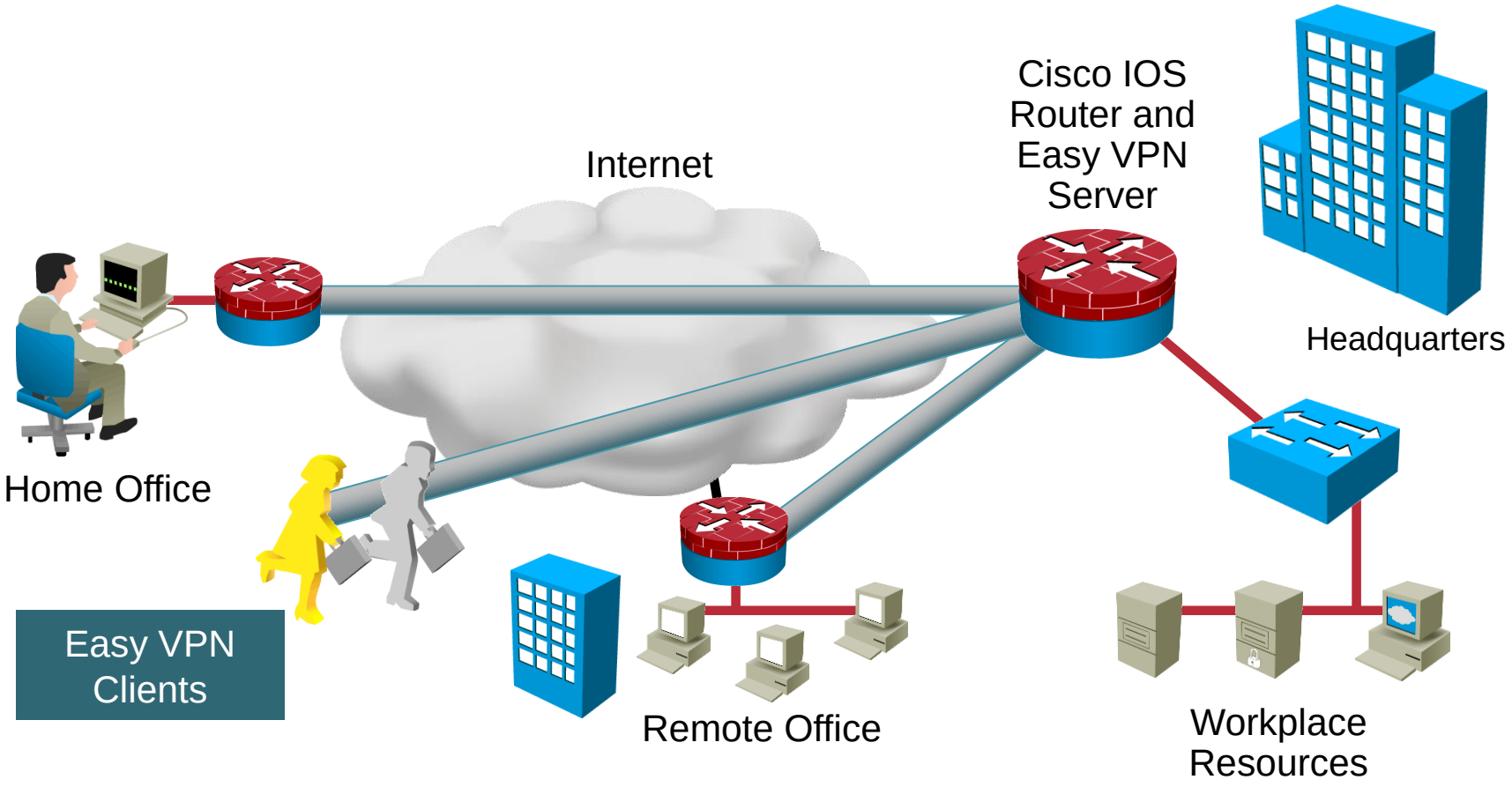
Remote-Access VPNs



Remote-access VPN: evolution of dial-in networks and ISDN

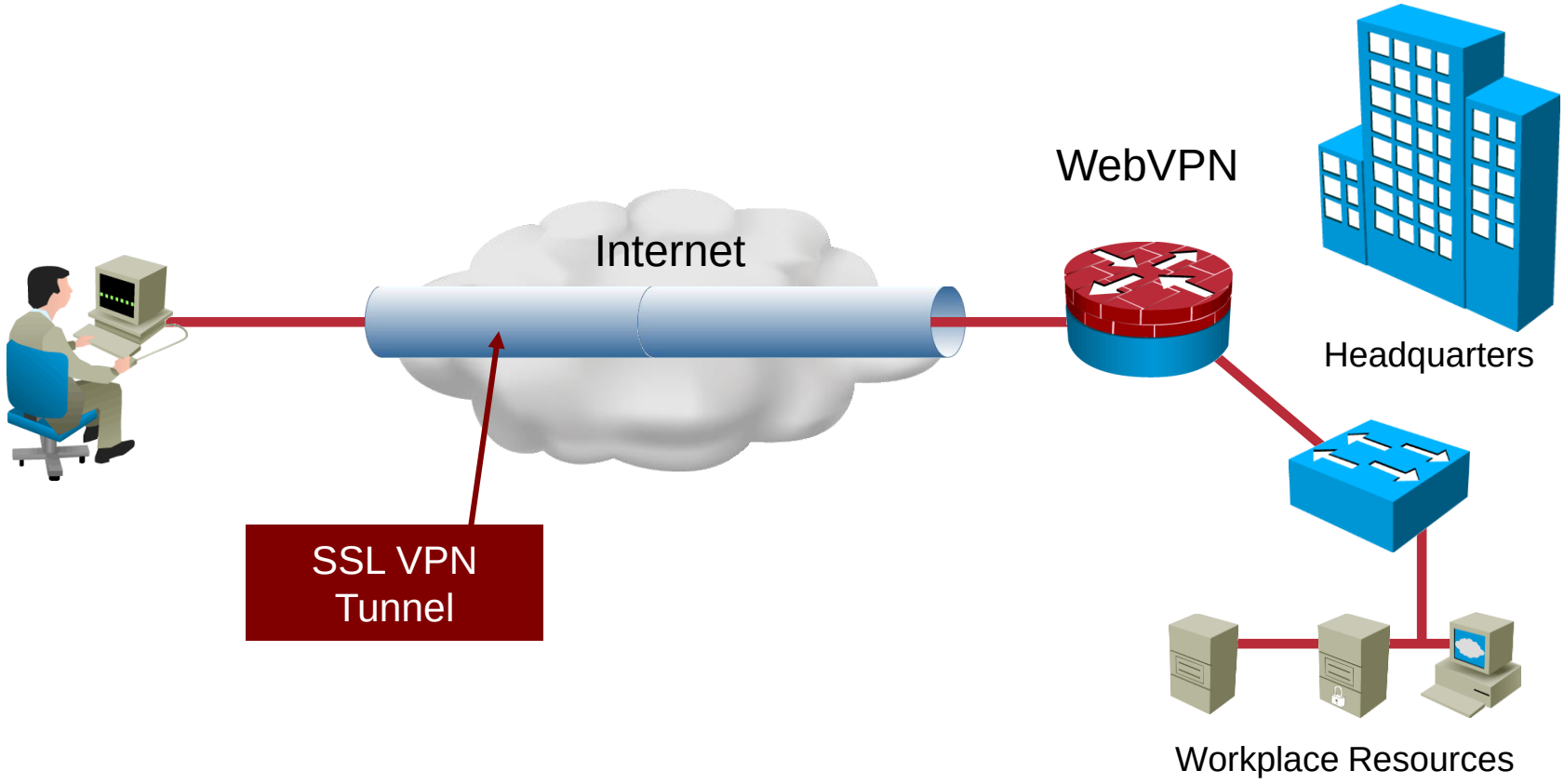
Cisco Easy VPN

- Cisco Unity is the common VPN language between Cisco devices.



Cisco IOS WebVPN

- Integrated security and routing
- Clientless and full network SSL VPN access

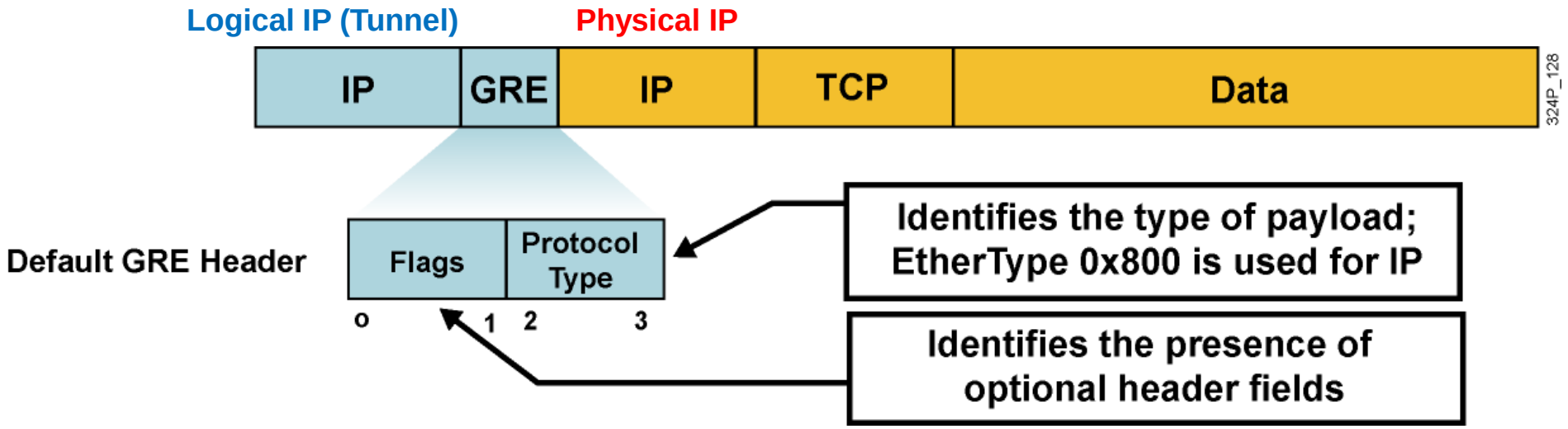


Generic Routing Encapsulation

OSI Layer 3 tunneling protocol:

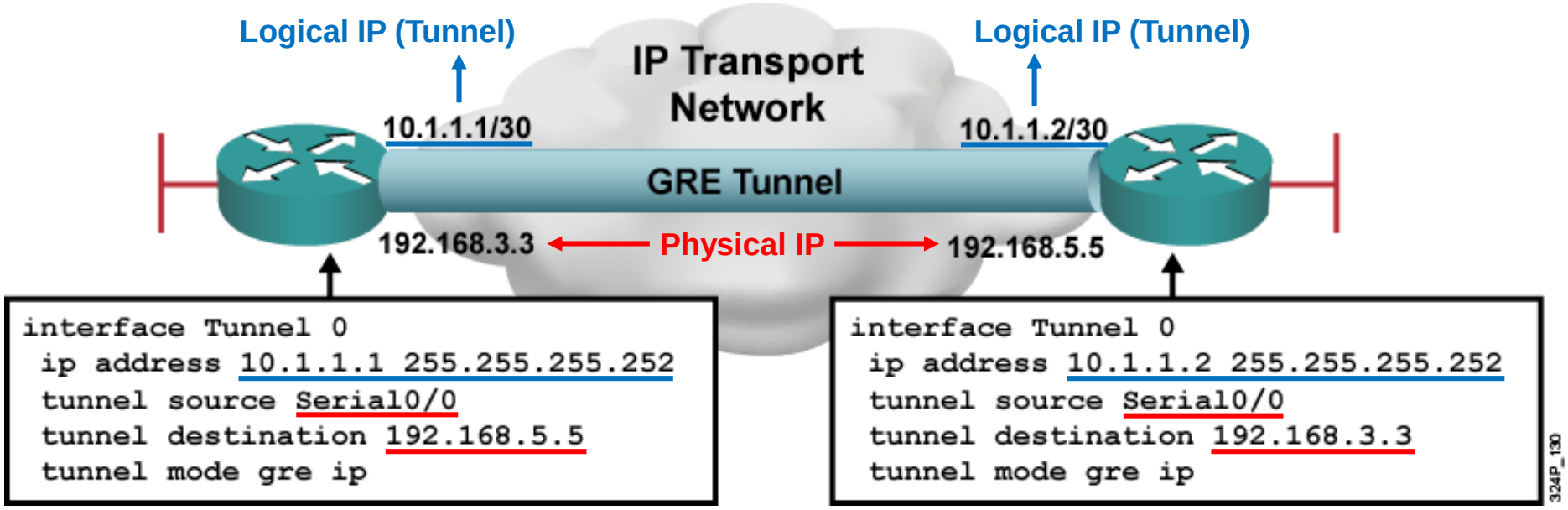
- Uses IP for transport
- Uses an additional header to support any other OSI Layer 3 protocol as payload (e.g., IP, IPX, AppleTalk)

Default GRE Characteristics



- 24-byte overhead by default (20-byte IP header and 4-byte GRE header)
- Tunneling of arbitrary OSI Layer 3 payload is the primary goal of GRE
- Stateless (no flow control mechanisms)
- No security (no confidentiality, data authentication, or integrity assurance)

GRE Configuration Example



- **GRE tunnel is up and protocol up if:**
  - Tunnel source and destination are configured
  - Tunnel destination is in routing table
  - GRE keepalives are received (if used)
- **GRE is the default tunnel mode.**


CISCO