



# Implementing Internet Access and MPLS Layer 3 VPNs

Complex MPLS Layer 3 VPNs



# Objectives

- Describe common customer Internet connectivity scenarios and identify design models for combining Internet access with MPLS Layer 3 VPN services
- Describe implementation of the Internet access service totally separate from MPLS Layer 3 VPN services
- Describe implementation of the Internet access solutions in which Internet access is provided as a separate VPN

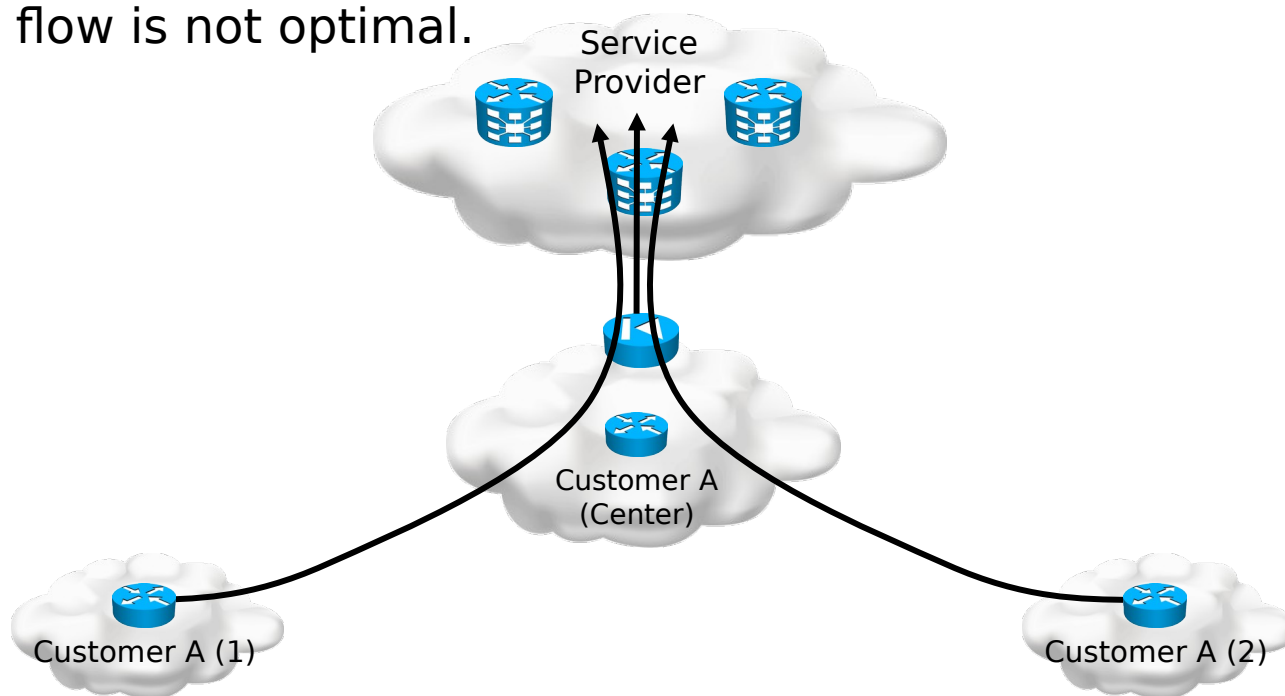
# Internet Access Models with MPLS VPNs

# Customer Internet Connectivity Scenarios

- Internet routing is usually performed via the BGP table of the MPLS VPN network of the service provider.
- By default, the VRF sites:
  - Can communicate only with devices in other VRF sites of the same VPN
  - Cannot communicate with devices in the global routing space
- There is potential security risk in providing Internet connectivity:
  - Firewalls are used to ensure the highest possible level of security.

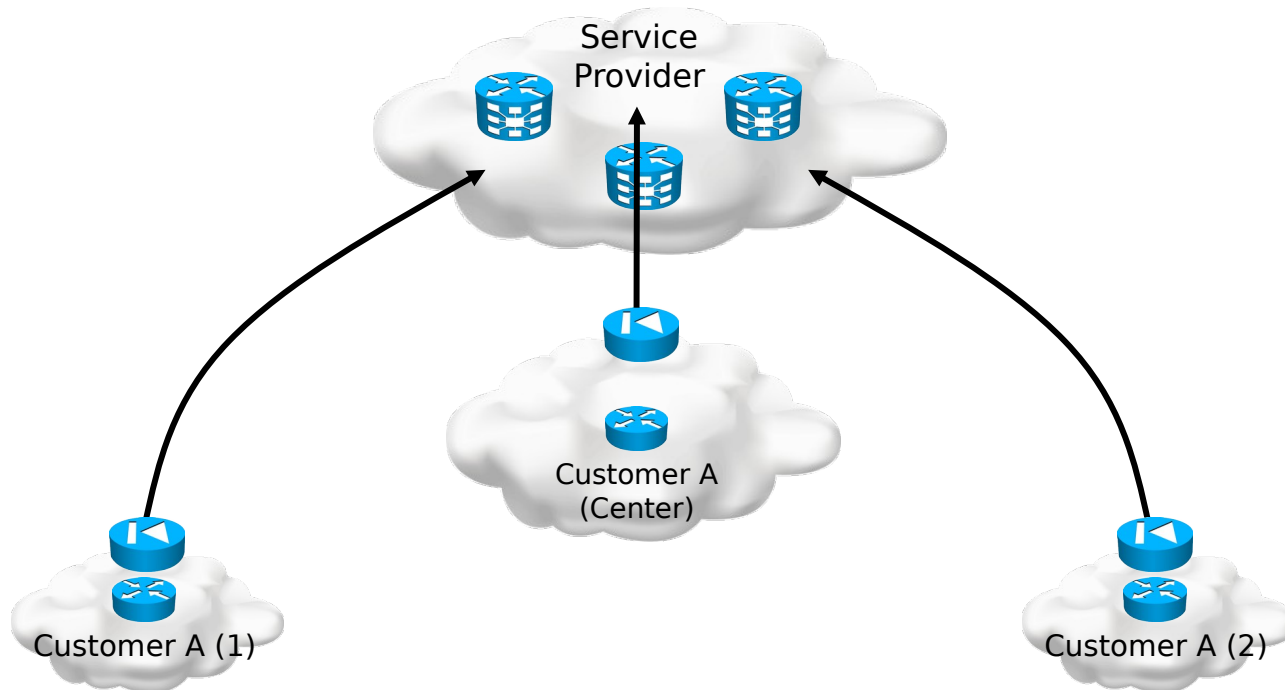
# Classical Internet Access

- Customer connects to the Internet through a central site firewall:
  - Deals with security issues
  - Provides NAT or proxy services as needed
- Internet traffic goes across the central site:
  - Traffic flow is not optimal.



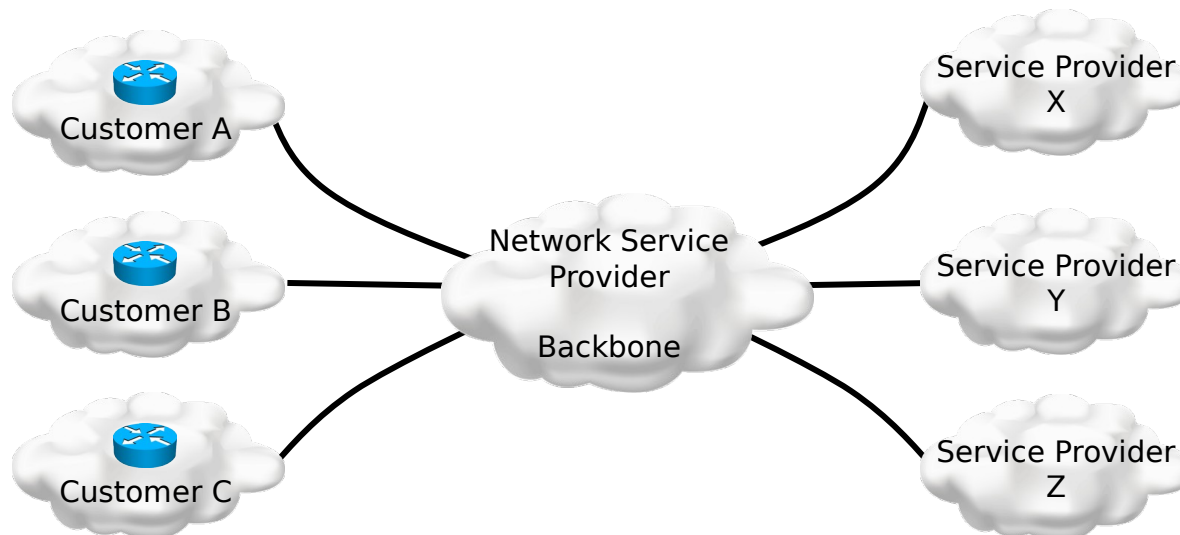
# Multisite Internet Access

- Customers have Internet access directly from every site.
- Optimum traffic flow for Internet traffic
- Each site has to deal with security issues:
  - Managed firewall offered by service provider
  - Customer firewall



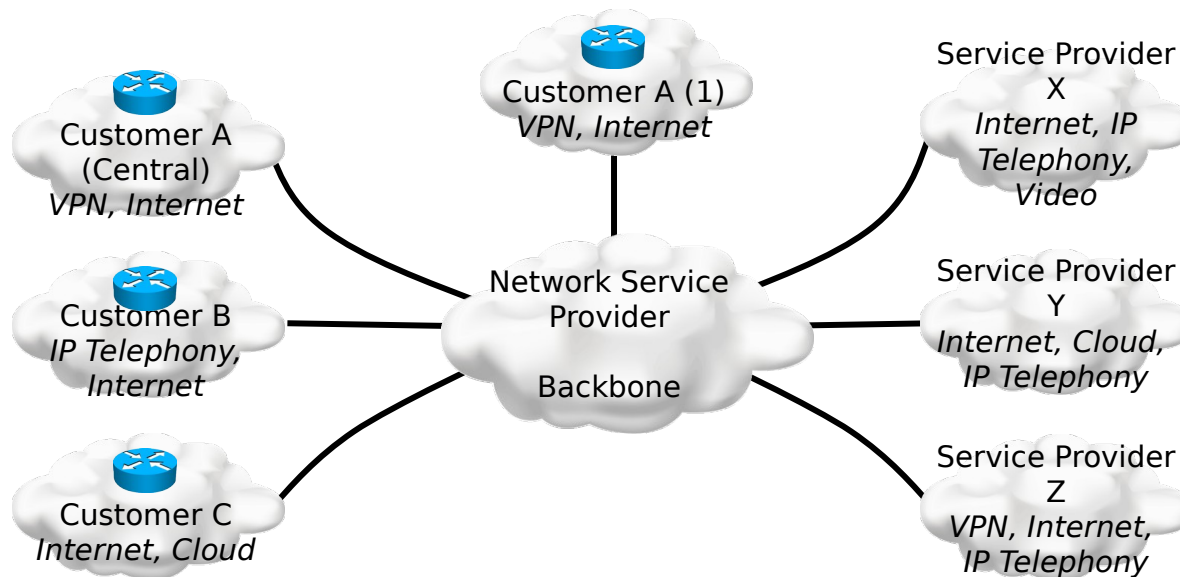
# Wholesale Internet Access

- Customer chooses an ISP and selects services.
- User can access different services offered by different service providers.
- Internet access backbone:
  - Provided by NSP
  - Used to interconnect customer with service provider



# Service Provider Shared Backbone

- Internet used to be the most popular service.
- Clients expect different services from their service providers now:
  - Internet, video, IP telephony, cloud services, and so on
- Cisco IP NGN architecture supports multiple services in a common backbone.



# Major Design Models of Service Provider Networks

- Two major design models:
  - Internet access through global routing
  - Internet access as a separate VPN service
- Internet access through route leaking is not an appropriate model for service providers:
  - Scalability problems

# Internet Access Through Global Routing

- Separate interface for VPN and Internet:
  - In global routing table
  - Static default routing on a PE
  - BGP between CE and PE
- Benefits:
  - Well-known setup (equivalent to classical Internet service)
  - Easy to implement
  - Offers a wide range of design options
- Drawback:
  - Requires separate physical links or WAN encapsulation that supports subinterfaces

# Internet Access Through a Separate VPN Service

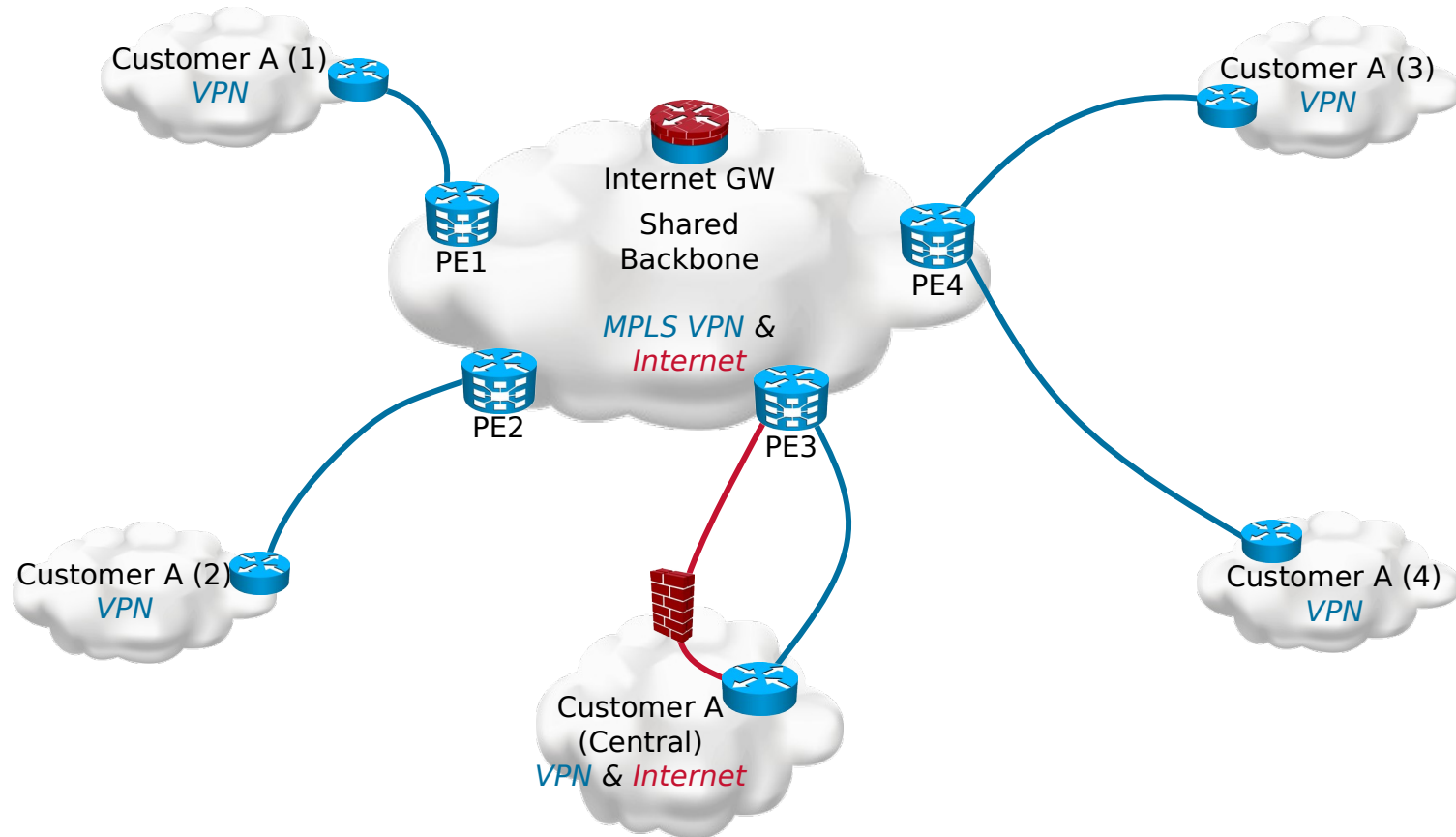
- Implementation through a separate VPN
- Benefits:
  - Provider backbone is isolated from the Internet.
  - Increased security
- Drawbacks:
  - All Internet routes are carried as VPN routes.
  - Scalability problems—full Internet routing table in VPN

# Internet Access Through Route Leaking

- Not a recommended design:
  - Formerly used in corporate environments
  - Internet access across corporate VPN:
    - Leaking routes between VRF and global routing table
- Benefits:
  - Does not use a separate connection for Internet traffic
- Drawbacks:
  - Insecure—Internet traffic mixed with VPN traffic
  - Hard to apply security policies
  - Scalability problems—hard to implement full Internet routing

# Separate Internet Access and VPN Services

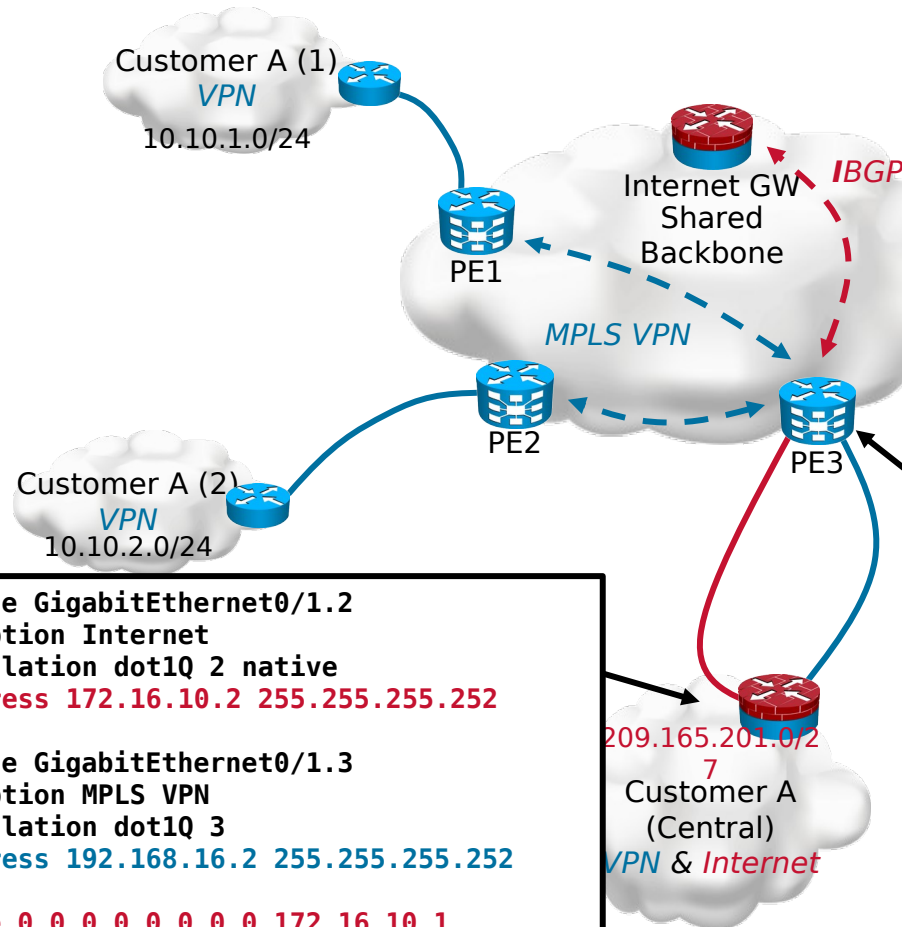
# Classic Internet Access for a VPN Customer



# Using Separate Subinterfaces

- Separating physical links for VPN and Internet is sometimes unacceptable because of high cost.
- Subinterfaces can be used:
  - Over WAN links
    - Frame Relay
    - ATM
  - Over LAN links (802.1Q)
- A tunnel interface could be used over a VRF-aware tunnel, so that VPN traffic does not run over a global tunnel.

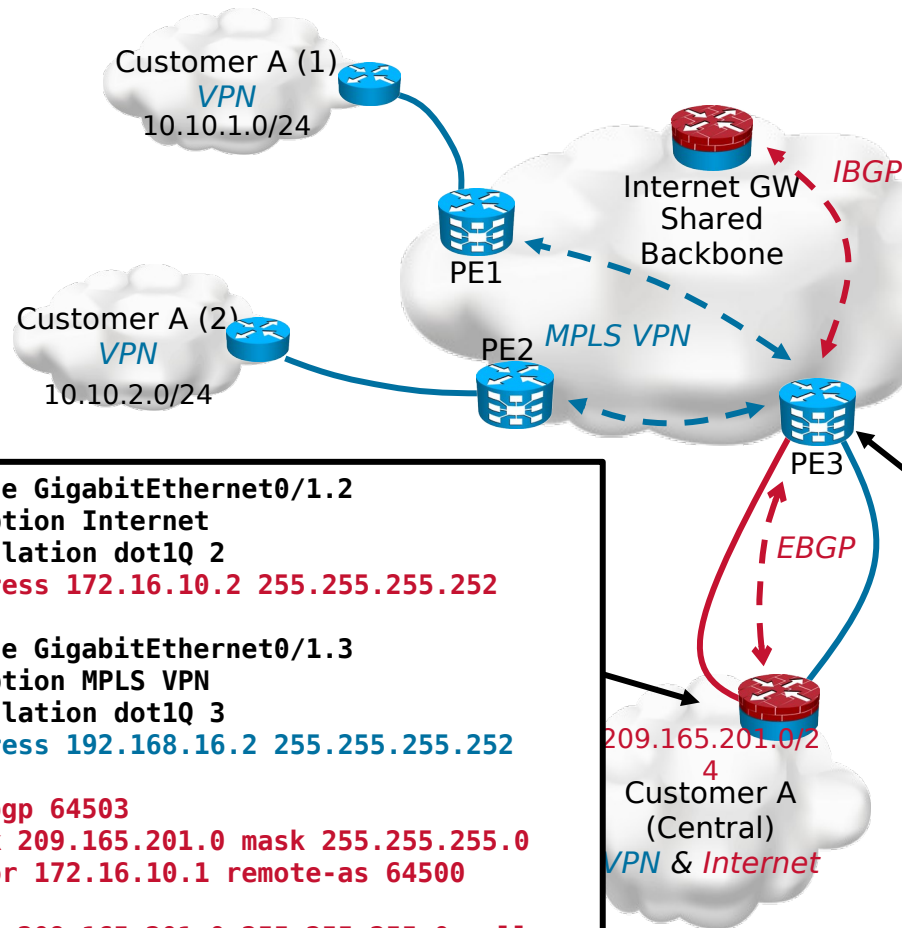
# Internet Access Using Static Routes



```
interface GigabitEthernet0/1.2
description Internet
encapsulation dot1Q 2 native
ip address 172.16.10.2 255.255.255.252
!
interface GigabitEthernet0/1.3
description MPLS VPN
encapsulation dot1Q 3
ip address 192.168.16.2 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 172.16.10.1
ip route 10.10.0.0 255.255.0.0 192.168.16.1
```

```
vrf CustomerA
address-family ipv4 unicast
import route-target
1:210
export route-target
1:210
!
interface GigabitEthernet0/1
no ip address
!
interface GigabitEthernet0/1.2
description Internet
encapsulation dot1Q 2 native
ip address 172.16.10.1 255.255.255.252
!
interface GigabitEthernet0/1.3
description MPL VPN
ip vrf forwarding CustomerA
encapsulation dot1Q 3 native
ip address 192.168.16.1 255.255.255.252
!
router static
address-family ipv4 unicast
209.165.201.0/27 172.16.10.2
!
router bgp 64500
address-family ipv4 unicast
redistribute static
!
```

# Internet Access Using Dynamic Routing Protocol

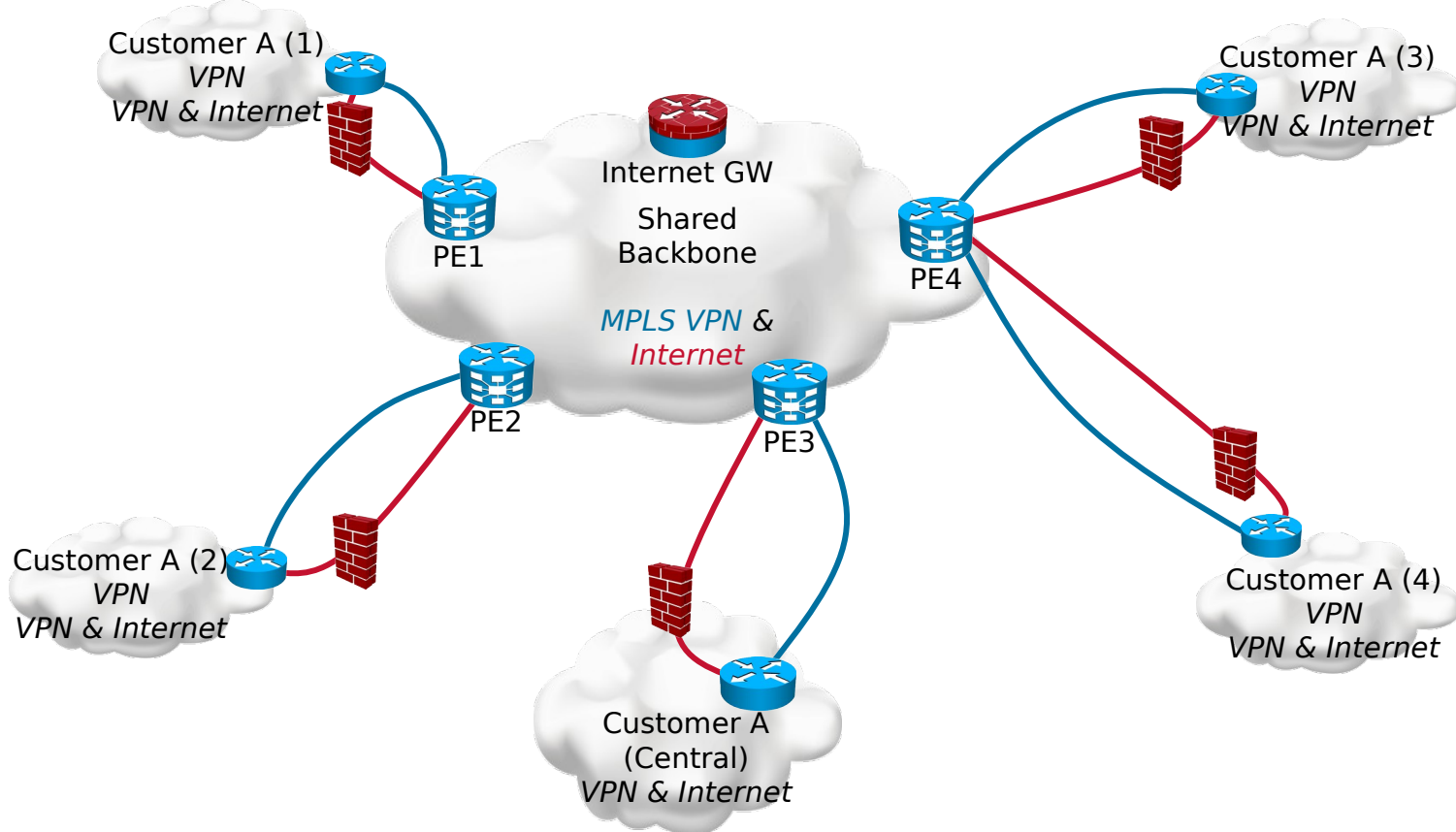


```
interface GigabitEthernet0/1.2
description Internet
encapsulation dot1q 2
ip address 172.16.10.2 255.255.255.252
!
interface GigabitEthernet0/1.3
description MPLS VPN
encapsulation dot1q 3
ip address 192.168.16.2 255.255.255.252
!
router bgp 64503
network 209.165.201.0 mask 255.255.255.0
neighbor 172.16.10.1 remote-as 64500
!
ip route 209.165.201.0 255.255.255.0 null
!
```

```
vrf CustomerA
address-family ipv4 unicast
import route-target
1:210
export route-target
1:210
!
interface GigabitEthernet0/1.2
description Internet
encapsulation dot1q 2
ip address 172.16.10.1 255.255.255.252
!
interface GigabitEthernet0/1.3
encapsulation dot1q 3
vrf Customer-A
ip address 192.168.16.1 255.255.255.252
!
router bgp 64500
address-family ipv4 unicast
neighbor 172.16.10.2
remote-as 64503
update-source GigabitEthernet0/0/0/0.2
address-family ipv4 unicast
route-policy pass in
route-policy Only_Default out
default-originate
next-hop-self
!
route-policy Only_Default
if destination in (0.0.0.0/0) then
pass
endif
end-policy
```

# Multisite Internet Access

- Every CE router needs two links (or subinterfaces).
- Complex network setup
- Expensive solution



# Benefits and Limitations

- Benefits of separate Internet access:
  - Well-known model
  - Supports all customer requirements
  - Allows all Internet service implementations
- Drawbacks of separate Internet access:
  - Requires separate physical link
  - PE routers must be able to perform Internet routing
    - Potentially carry full Internet routing table
    - Wholesale Internet access cannot be implemented in this model.

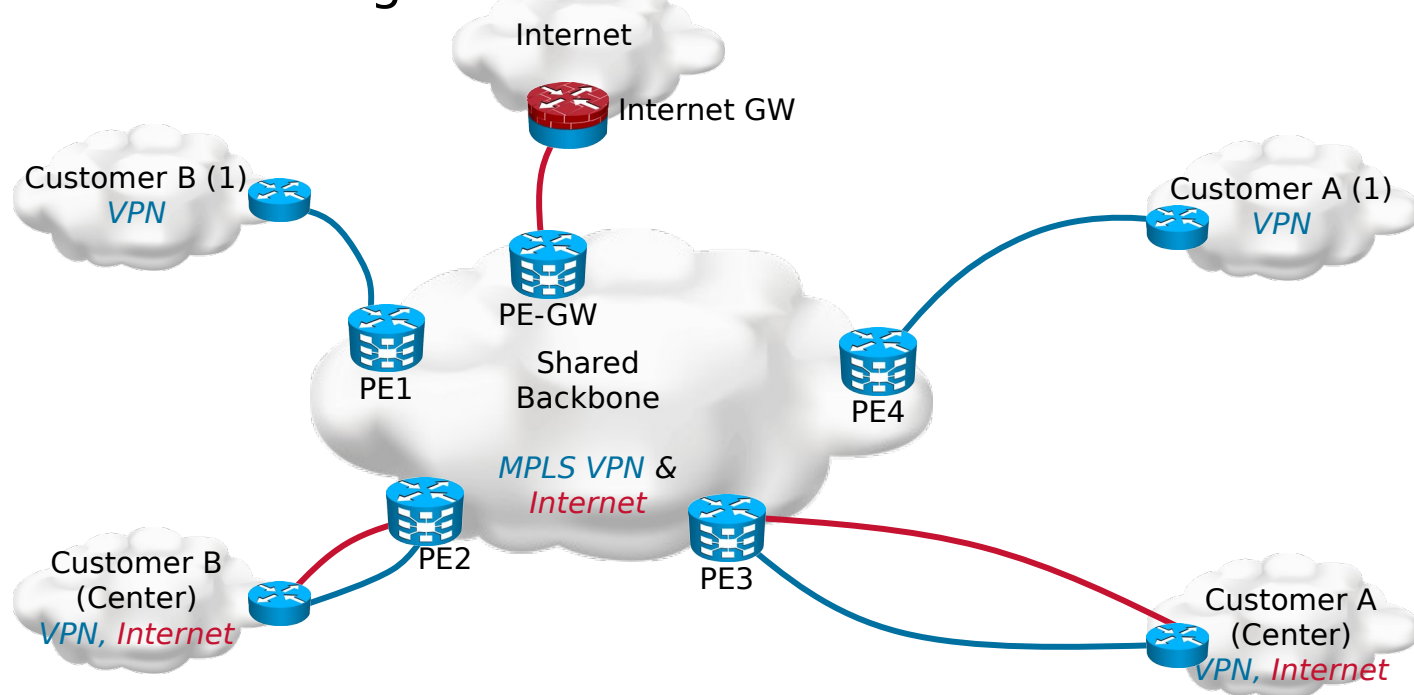
# Internet Access as a Separate VPN

# Internet Access as a Separate VPN

- Service provider gateway is connected as a CE router to the MPLS VPN backbone.
- Global Internet routing table is very big:
  - Only default route and some specific regional routes are distributed to the MPLS VPN network.
- Many service providers on same network backbone:
  - Customer can chose service provider.
  - Customer site is assigned to VRF of service provider.

# Internet Gateway Configuration

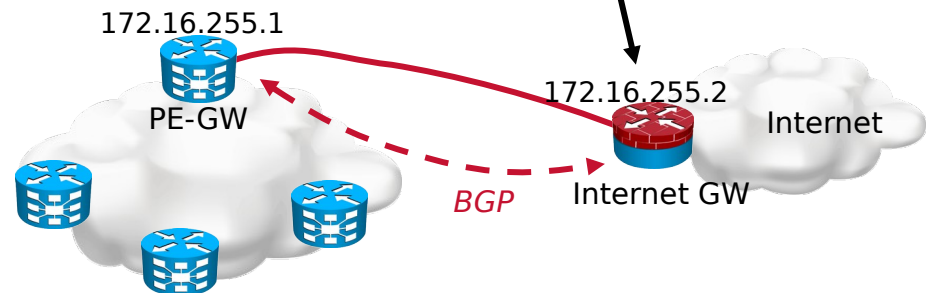
- Internet gateway has full Internet routing table:
  - Only subset of all routes sent to customers
- Internet gateway acts as a CE router.
- Internet VPN is used for Internet access.
- Customers are assigned to Internet VPN.



# Internet Gateway Configuration Example

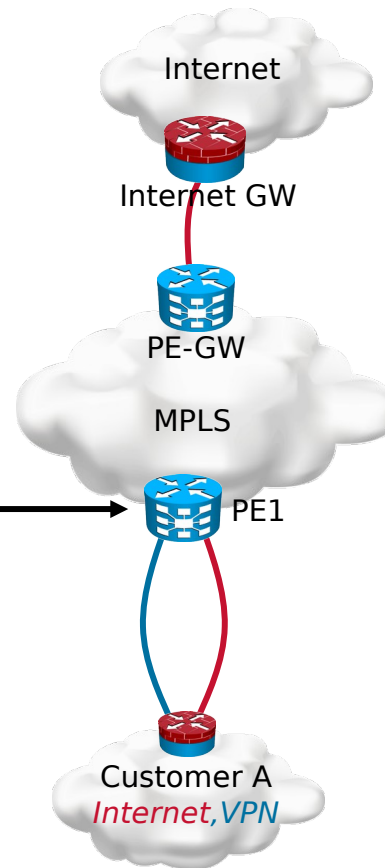
```
PE-GW:
vrf Internet
description Internet
address-family ipv4 unicast
import route-target
  1:2000
!
export route-target
  1:2000
!
interface GigabitEthernet0/1
vrf Internet
ip address 172.16.255.1 255.255.255.252
!
router bgp 64500
vrf Internet
rd 1:2000
address-family ipv4 unicast
!
neighbor 172.16.255.2
remote-as 64510
update-source GigabitEthernet0/1
address-family ipv4 unicast
route-policy pass in
route-policy pass out
next-hop-self
!
```

```
Internet GW:
interface GigabitEthernet0/1
ip address 172.16.255.2 255.255.255.252
!
router bgp 64510
address-family ipv4 unicast
!
neighbor 172.16.255.1
remote-as 64500
update-source GigabitEthernet0/1
address-family ipv4 unicast
route-policy pass in
route-policy Only_Default out
default originate
!
route-policy Only_Default
if destination in (0.0.0.0/0) then
pass
endif
end-policy
```



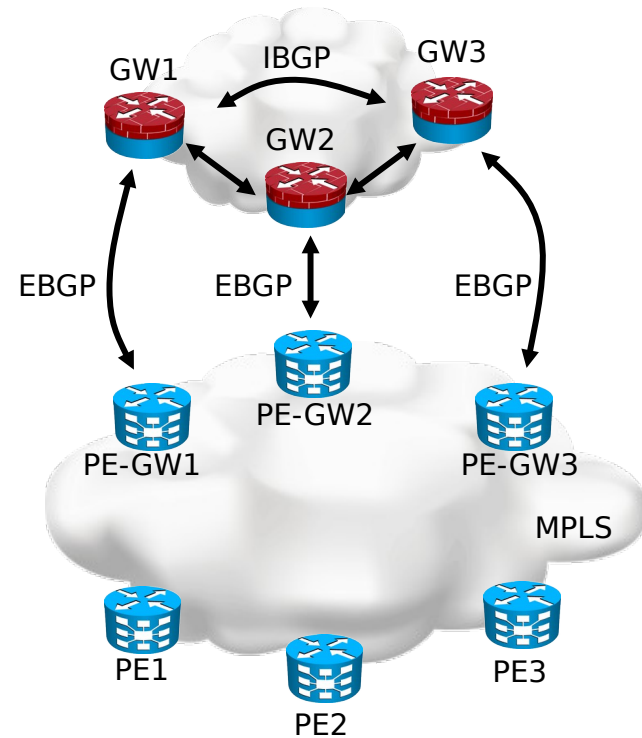
# Customer Internet Access from Central Site

```
PE1:
vrf CustomerA
 address-family ipv4 unicast
  import route-target
    1:210
  export route-target
    1:210
!
interface GigabitEthernet0/1.2
 description Internet
 encapsulation dot1q 2
 ip address 172.16.10.1 255.255.255.252
!
router bgp 64500
 address-family ipv4 unicast
!
 address-family vpnv4 unicast
!
!
vrf Internet
 rd 1:2000
 neighbor 172.16.10.2
 remote-as 64503
 address-family ipv4 unicast
  network 0.0.0.0/0
!
```



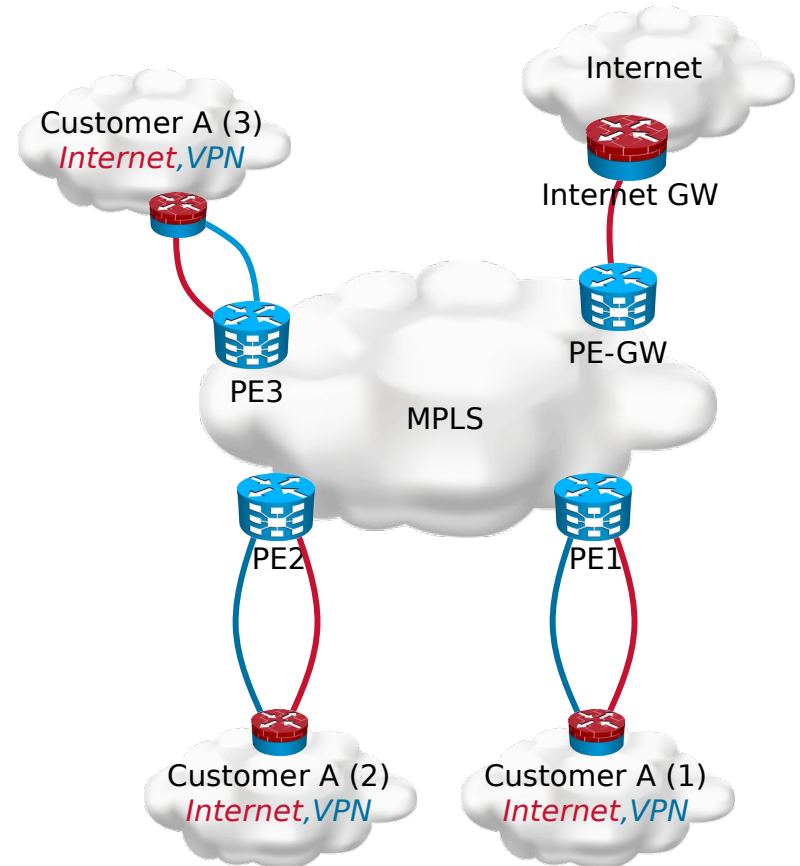
# Redundant Internet Access

- All Internet gateways advertise routes.
- Internet gateways are connected to the same VRF.
- BGP metric is used to select the best route to the Internet.
- MED is used to define the primary Internet gateway.



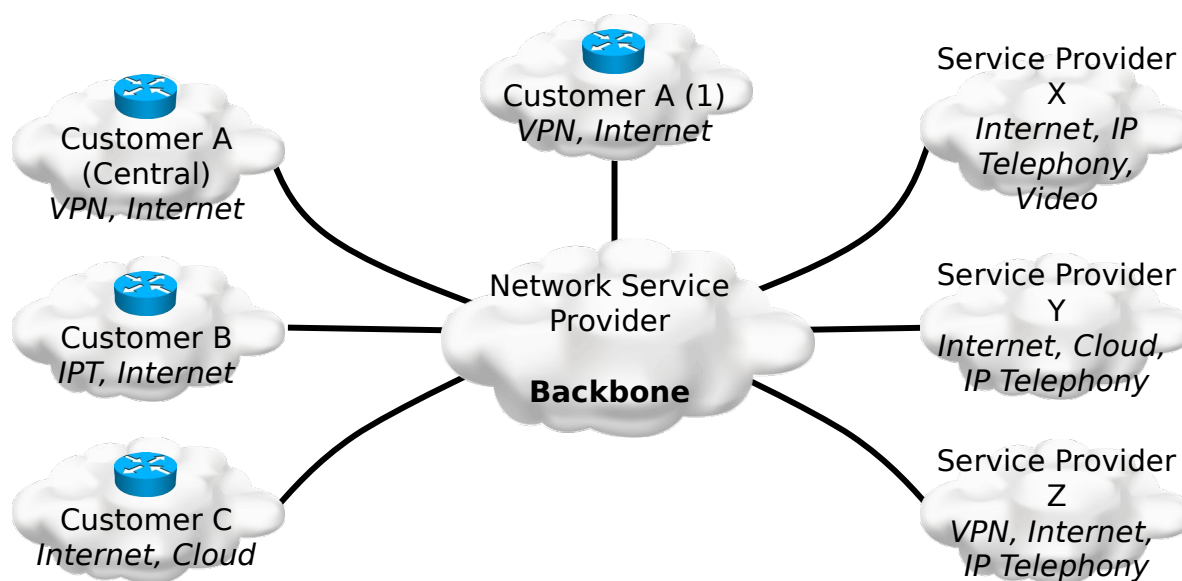
# Multisite Customer Internet Access

- Internet VRF is configured on every location.
- Adds complexity
- Firewall on every site:
  - Managed firewall can be used.



# Wholesale Internet Access

- A separate VPN is created for each upstream ISP.
- Each ISP gateway announces the default route to the VPN.
- Customers are assigned into the right VRF:
  - VRF assignment corresponds to ISP selection.
- ISP change is easy for administrator:
  - Only VRF has to be changed.



# Limitations of Running Internet in a VPN

- Benefits:
  - Supports all Internet access service types
  - Easy to make changes
  - Can support customer requirements
- Drawbacks:
  - Full Internet routing cannot be carried in the VPN:
    - Suboptimal routing
  - Overlapping Internet and VPN backbone design requires special care.

# Summary

- Internet access types include the following:
  - Classical Internet access
  - Multisite Internet access
  - Wholesale Internet access
- Two recommended service provider designs are as follows:
  - Global routing (global routing table is used for Internet routing)
  - Internet service as a separate VPN
- Wholesale Internet access is easy to implement when you use Internet service as a separate VPN.

