Routing Issues in deploying MPLS VPNs

Mukhtiar Shaikh (mshaikh@cisco.com)

Moiz Moizuddin (mmoizudd@cisco.com)

Agenda

- Introduction
- Physical Migration to MPLS VPN Backbone
- Routing considerations using

  BGP as PE-CE protocol

  OSPF as PE-CE protocol

  EIGRP as PE-CE protocol
- Default route handling in MPLS VPN
- Preventing routing Loops with SOO
- Limiting vrf routes and potential black holing
- Multi-homing Scenarios
- Summary

Introduction

- Many enterprises are migrating to VPN services based on Layer 3 infrastructure (aka RFC 2547 based VPNs)
- In the traditional Layer 2 VPN Frame or ATM-based networks, Service provider network does not participate in the enterprise routing.
- Change in routing policies may result in network either sub-optimally utilized or even could lead to routing loops
- Enterprise network operators need to fully understand various factors that determine the overall complexity during and after migration such as

  Internal Site routing protocols

  Choice of PE-CE protocols

  Multi-homing, Redundancy and load balancing options

  Existence of backdoor links

  Network size (large number of sites)

  Number of Hub sites etc.
- Various network scenarios are discussed to highlight the issues and possible solutions.

Agenda

- Introduction
- Physical Migration to MPLS VPN Backbone
- Routing considerations using

    BGP as PE-CE protocol

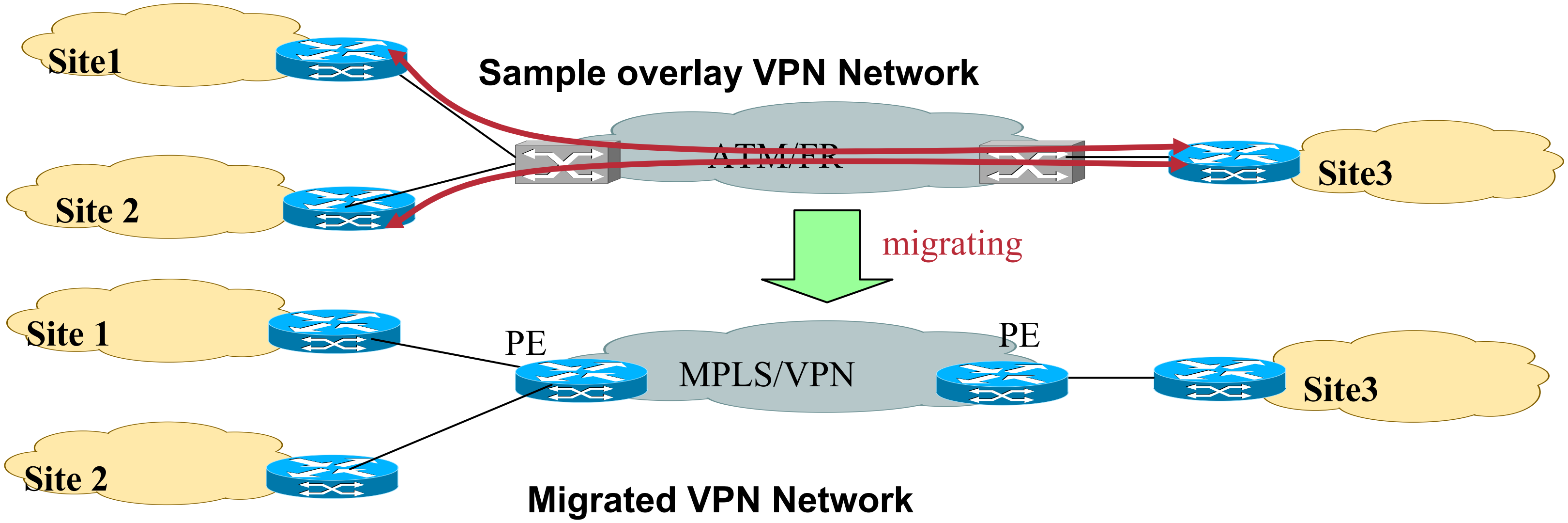
    OSPF as PE-CE protocol

    EIGRP as PE-CE protocol
- Default route handling in MPLS VPN
- Preventing routing Loops with SOO
- Limiting vrf routes and potential black holing
- Multi-homing Scenarios
- Summary

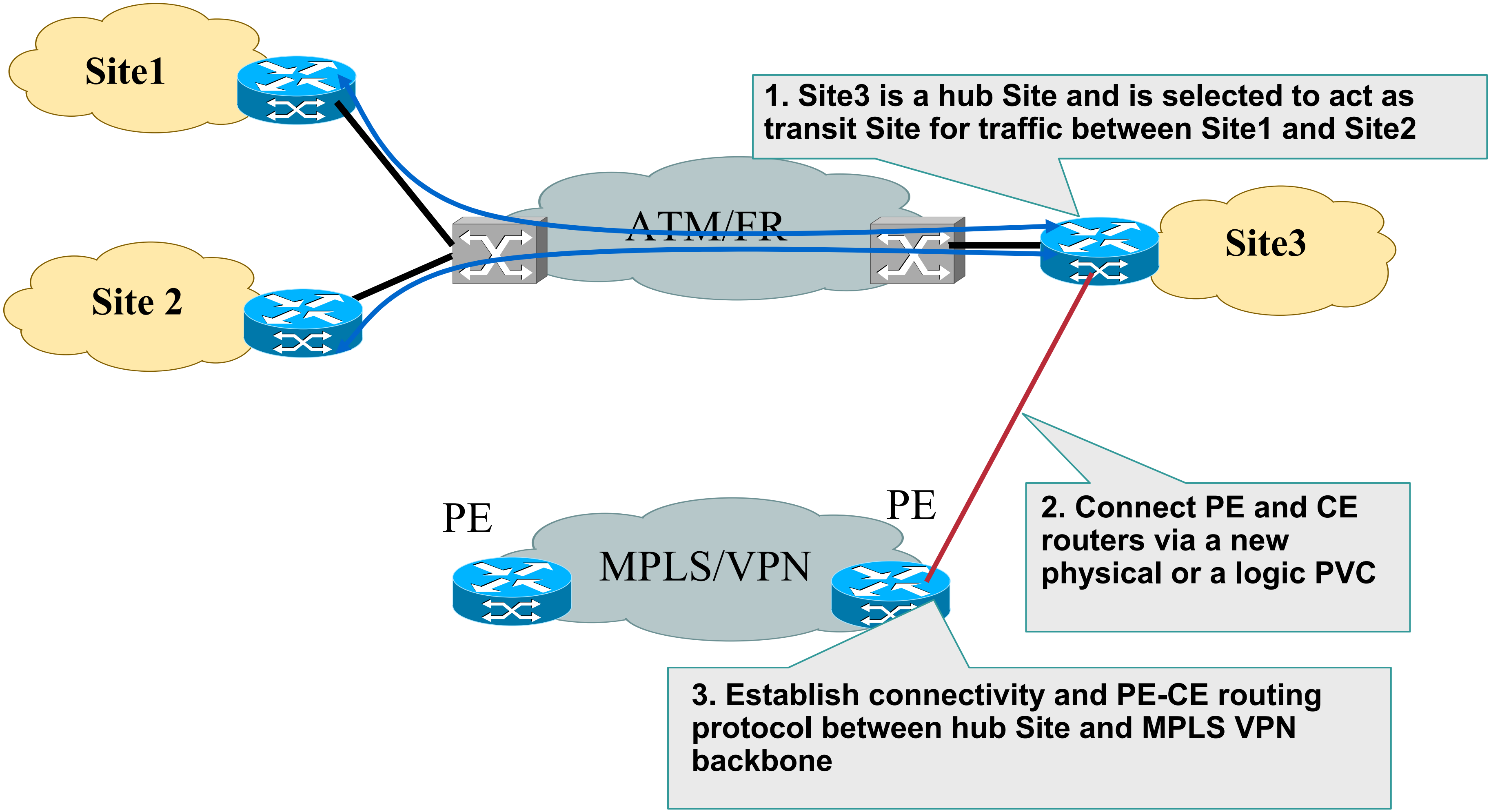
Migration Considerations

- Minimize impact on customer connectivity and traffic forwarding as well as avoid potential Site isolation during migration.
- Routing interaction of PE-CE routing protocols with the Site local IGP

  Customers may not use their existing internal routing protocol to exchange routing information with the provider.
- Need to make sure internal as well internet routing works as desired
- Migration of a large enterprise to MPLS VPN needs phased approach



Migration steps: Hub Site Migration

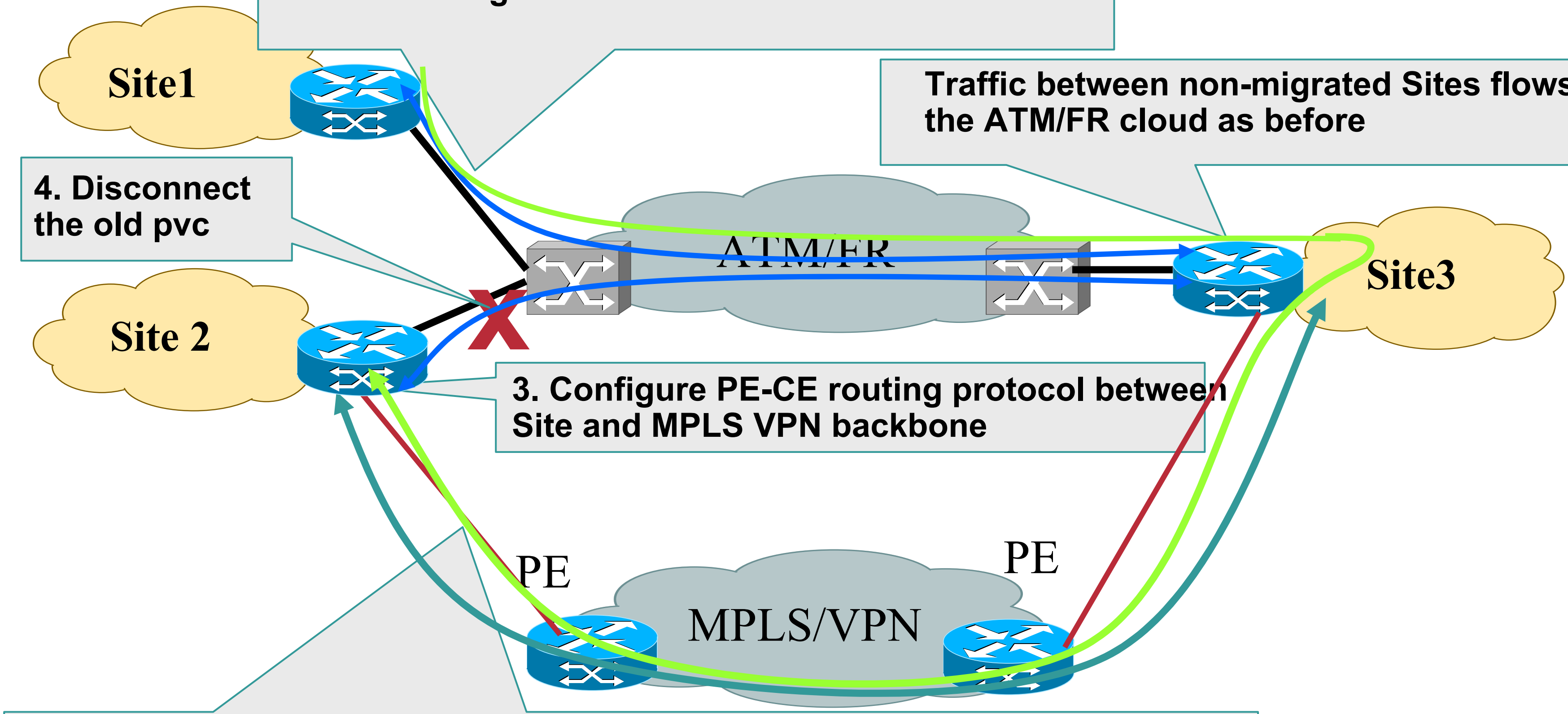


1. Site3 is a hub Site and is selected to act as transit Site for traffic between Site1 and Site2

2. Connect PE and CE routers via a new physical or a logic PVC

3. Establish connectivity and PE-CE routing protocol between hub Site and MPLS VPN backbone

Migration steps: Individual Sites Migration



Traffic between non-migrated and Migrated Sites transits through hub Site

Traffic between non-migrated Sites flows over the ATM/FR cloud as before

4. Disconnect the old pvc

3. Configure PE-CE routing protocol between Site and MPLS VPN backbone

1. Establish a new physical or FR/ATM PVC between Site under migration and MPLS VPN backbone
2. Keep the existing connection

Depending on the routing protocol and the corresponding Admin distance and metrics, traffic will start flowing over MPLS VPN backbone

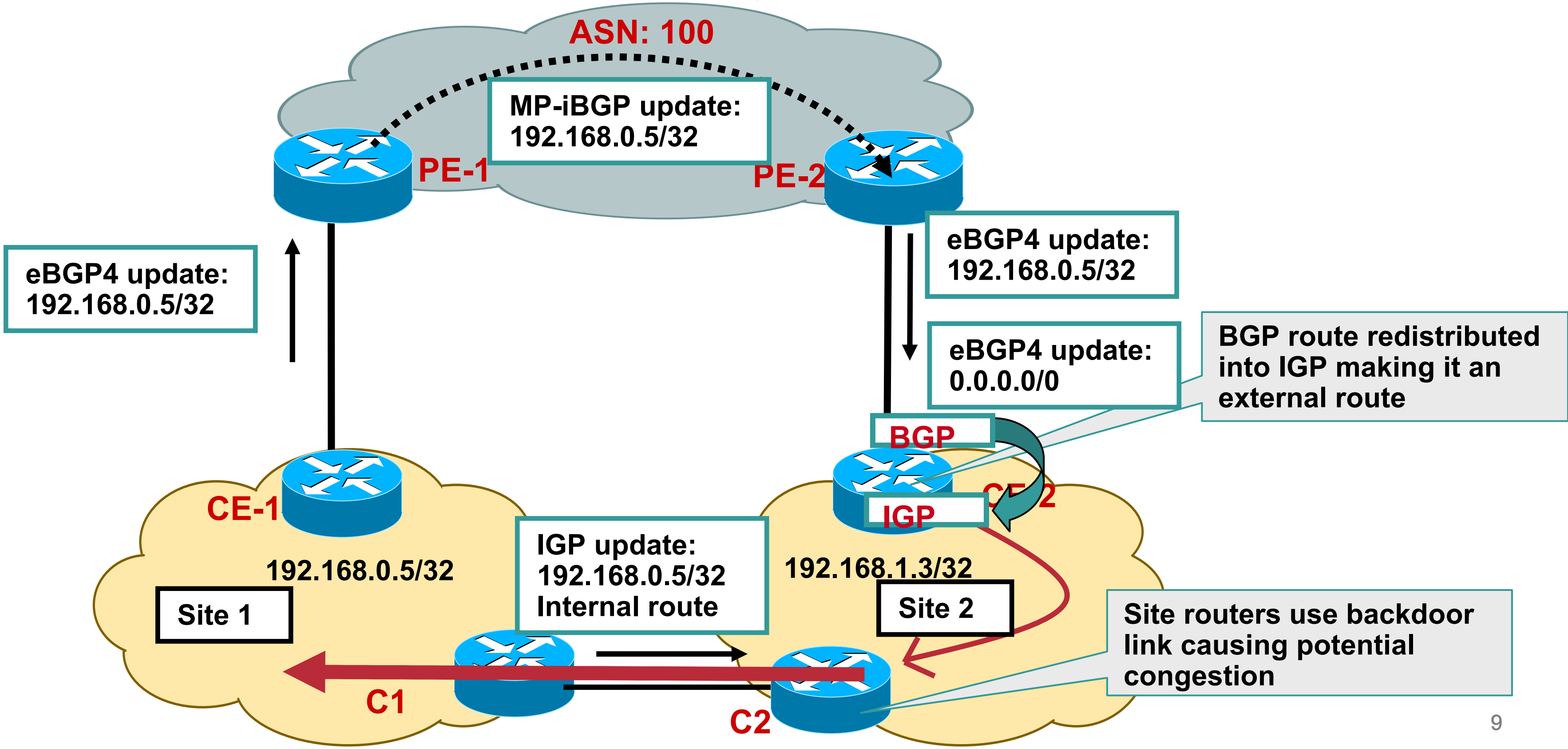
Agenda

- Introduction
- Physical Migration to MPLS VPN Backbone
- Routing considerations using
  - BGP as PE-CE protocol
    - BGP interaction with local Site IGPs
    - AS Considerations and VPN Topologies
  - OSPF as PE-CE protocol
  - EIGRP as PE-CE protocol
- Default route handling in MPLS VPN
- Preventing routing Loops with SOO
- Limiting vrf routes and potential black holing
- Multi-homing Scenarios
- Summary

Redistributing BGP into local Site IGP

Problem - Backdoor being preferred

- BGP route redistributed in local Site IGP (such as OSPF, EIGRP) becomes external
- Backdoor link is part of the same IGP
- Site 2 for example also learns the same prefix via backdoor link as internal route
- At Site 2, internal route is preferred over external. Traffic is sent over backdoor link instead of VPN provider backbone making VPN service useless



ASN: 100
MP-iBGP update: 192.168.0.5/32
PE-1
PE-2
eBGP4 update: 192.168.0.5/32
eBGP4 update: 192.168.0.5/32
eBGP4 update: 0.0.0.0/0
BGP
IGP
CE-1
CE-2
192.168.0.5/32
192.168.1.3/32
Site 1
Site 2
IGP update: 192.168.0.5/32 Internal route
C1
C2

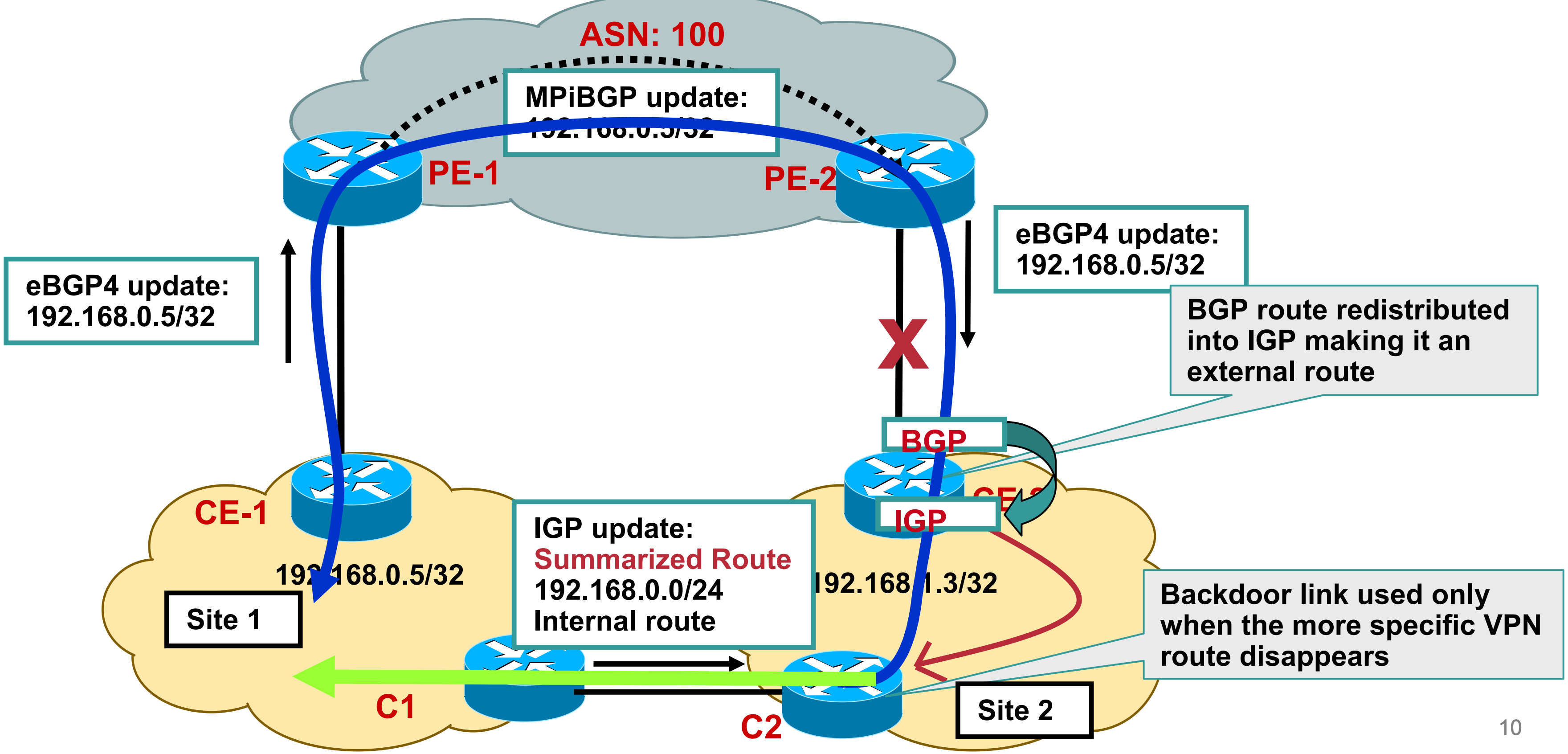
BGP route redistributed into IGP making it an external route

Site routers use backdoor link causing potential congestion

Redistributing BGP into local Site IGP

Solution – Advertise a Summary route

- Simplest solution is to remove the backdoor link
- Other possible solution is to send a summarized route from Site 1 to Site 2 and vice versa over the backdoor link
- In normal conditions, at each Site more specific route learnt from the SP would be preferred over the summary route.
- This solution won't work for default route.



MPiBGP update:
192.168.0.5/32

eBGP4 update:
192.168.0.5/32

eBGP4 update:
192.168.0.5/32

BGP route redistributed into IGP making it an external route

IGP update:
Summarized Route
192.168.0.0/24
Internal route

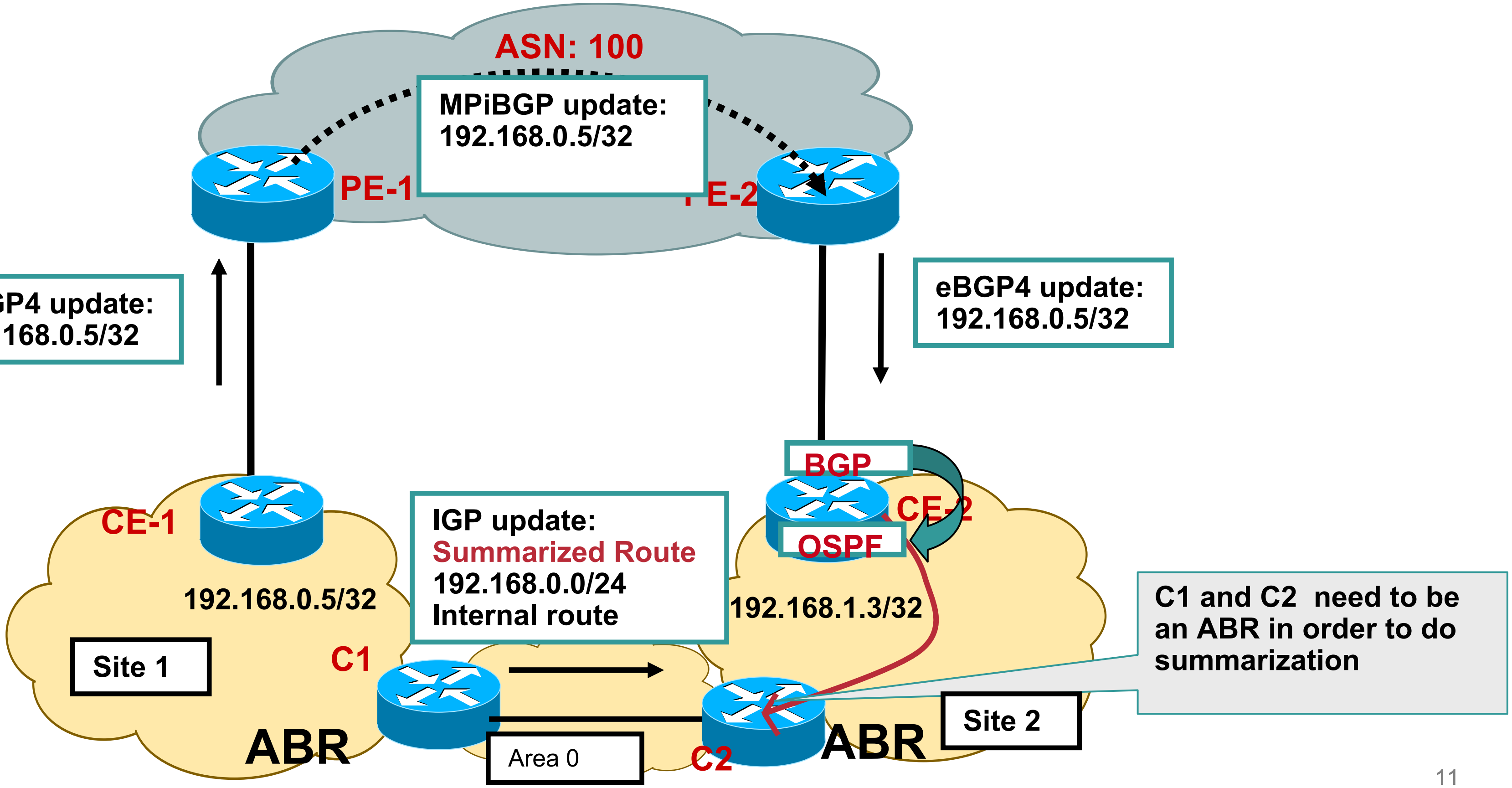
Backdoor link used only when the more specific VPN route disappears

Site 1

Site 2

Redistributing BGP into OSPF local Site IGP
Make backdoor part of area 0

- The summary route solution will not work if OSPF is the local IGP
- Summary generated only if C1 and C2 routers are OSPF ABRs or (ASBRs if routes are external)

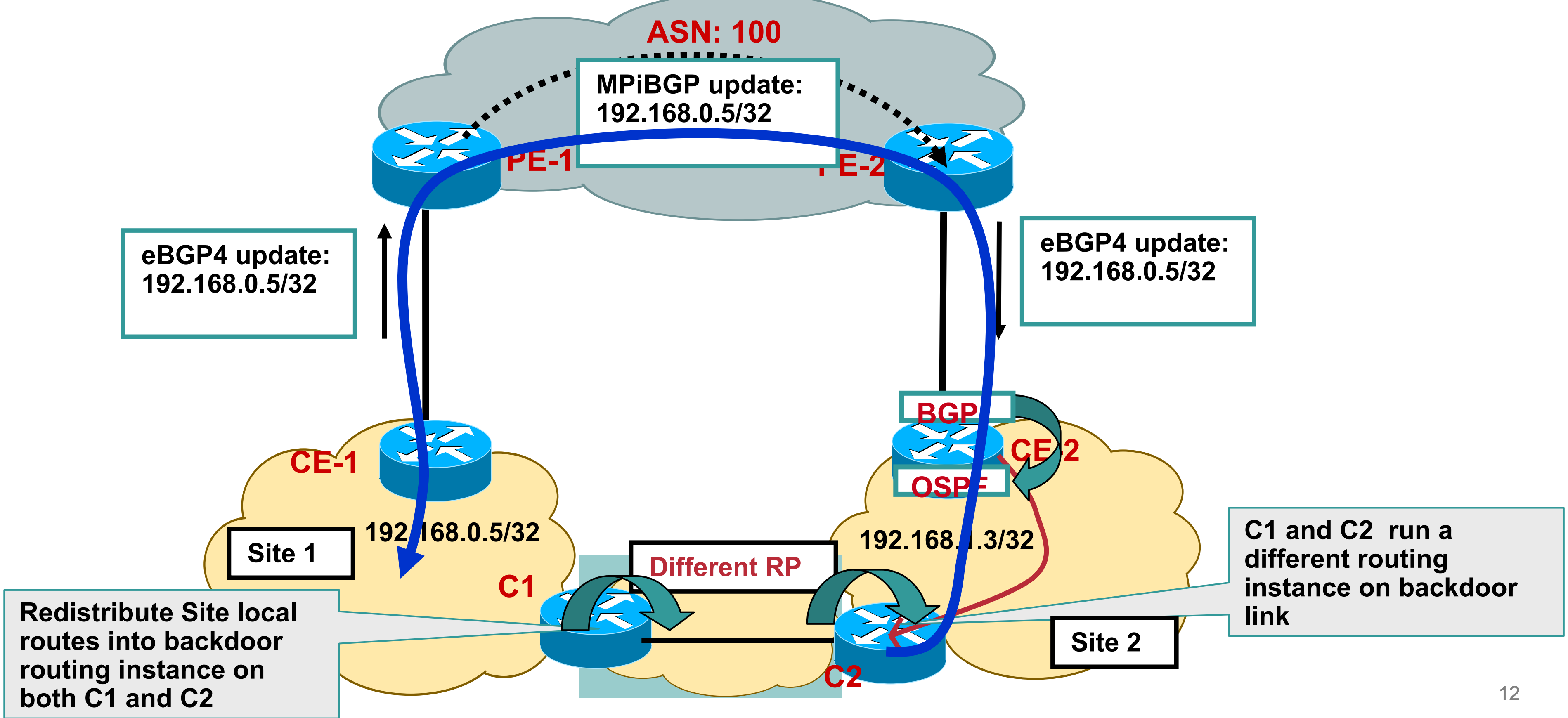


C1 and C2 need to be an ABR in order to do summarization

Redistributing BGP into OSPF local Site IGP

Make backdoor part of a different Routing Protocol

- Run a different routing protocol or different IGP instance on the backdoor link
- Redistribute Site local IGP routes into the backdoor routing protocol instance
- Now routes from SP cloud learnt via BGP and the route learnt over back door are both external
- Change the external route type or tweak the metric to prefer the SP cloud.

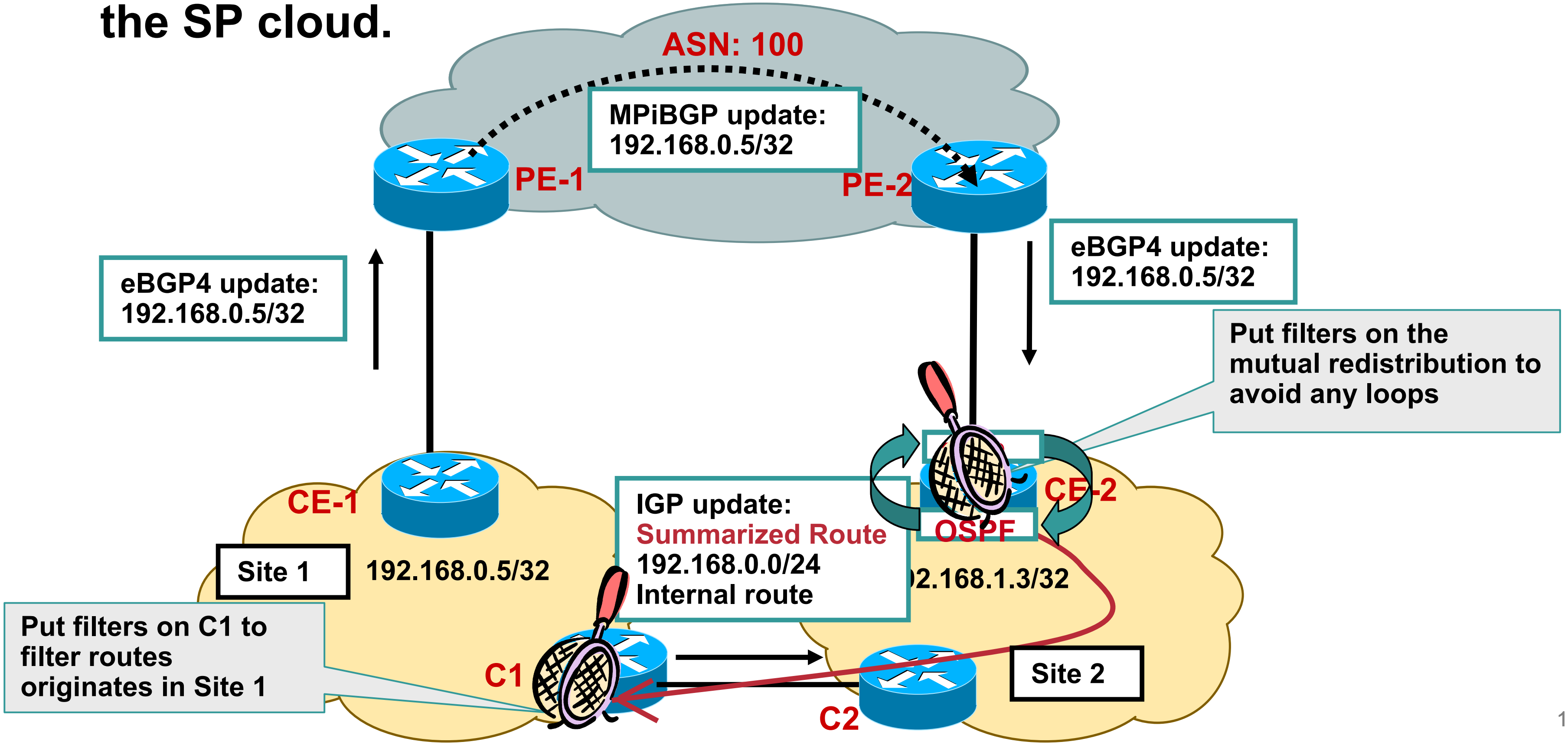


Redistribute Site local routes into backdoor routing instance on both C1 and C2

C1 and C2 run a different routing instance on backdoor link

Redistributing BGP into local Site IGP
Filtering considerations

- Because of mutual redistribution on CE routers at each Site, routing loops are possible
- Need to apply filters to advertise only locally sourced routes from each Site and block Site local routes being received from the SP cloud.



Put filters on the mutual redistribution to avoid any loops

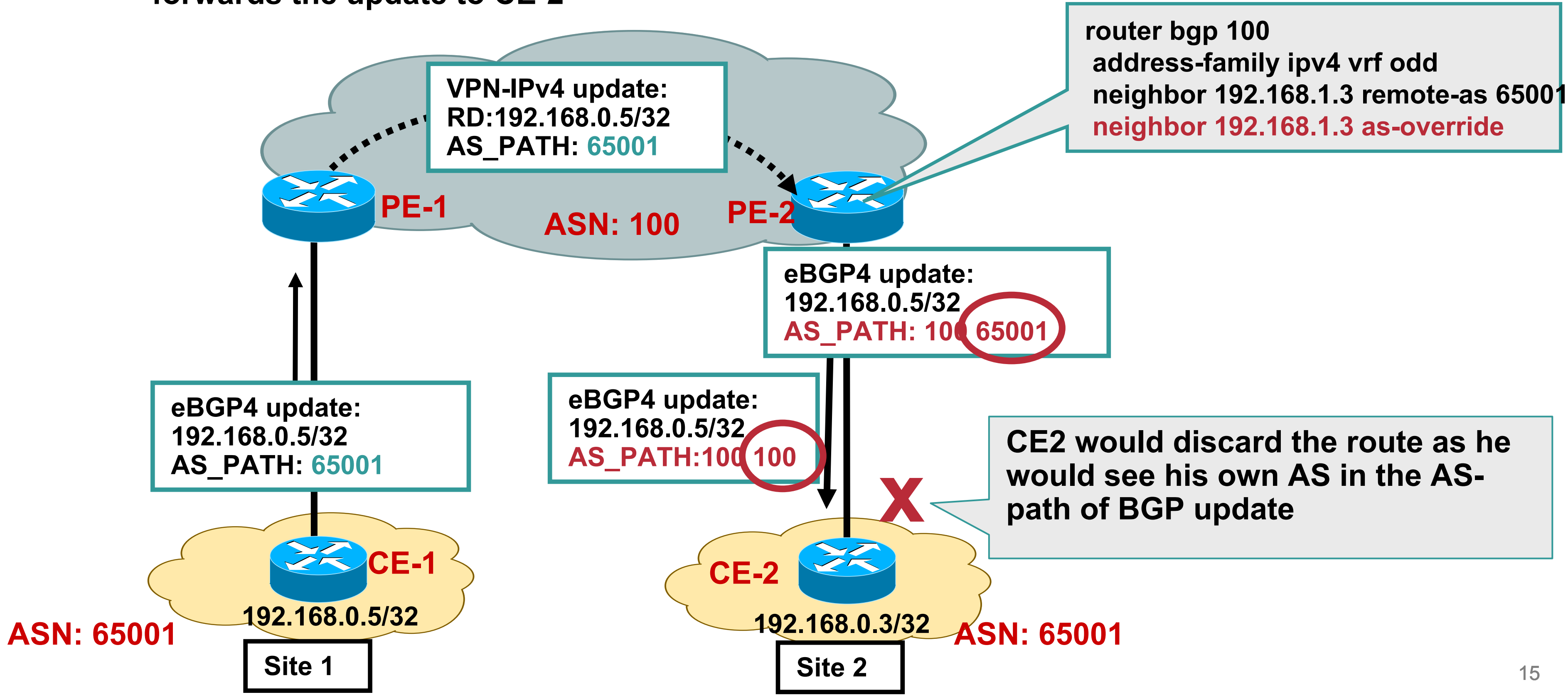
Put filters on C1 to filter routes originates in Site 1

Agenda

- Introduction
- Physical Migration to MPLS VPN Backbone
- Routing considerations using
    - BGP as PE-CE protocol
        - BGP interaction with local Site IGPs
        - AS Considerations and VPN Topologies
    - OSPF as PE-CE protocol
    - EIGRP as PE-CE protocol
- Default route handling in MPLS VPN
- Preventing routing Loops with SOO
- Limiting vrf routes and potential black holing
- Multi-homing Scenarios
- Summary

BGP AS Considerations
VPN Sites belong to same ASN

- Customer may have same AS number in all its Sites
- Default BGP behaviour would force the CE to drop the routing update because of the AS-path loop detection
- "Allow-as in" can be used on the CE to accept the update even if it contains its own AS.
- Service provider can re-write the customer AS using "AS- override" feature
- PE-2 replaces all occurrences of customer ASN in the AS-Path with its own ASN and forwards the update to CE-2



```
router bgp 100
 address-family ipv4 vrf odd
 neighbor 192.168.1.3 remote-as 65001
 neighbor 192.168.1.3 as-override
```

VPN-IPv4 update:
RD:192.168.0.5/32
AS_PATH: 65001

eBGP4 update:
192.168.0.5/32
AS_PATH: 100 65001

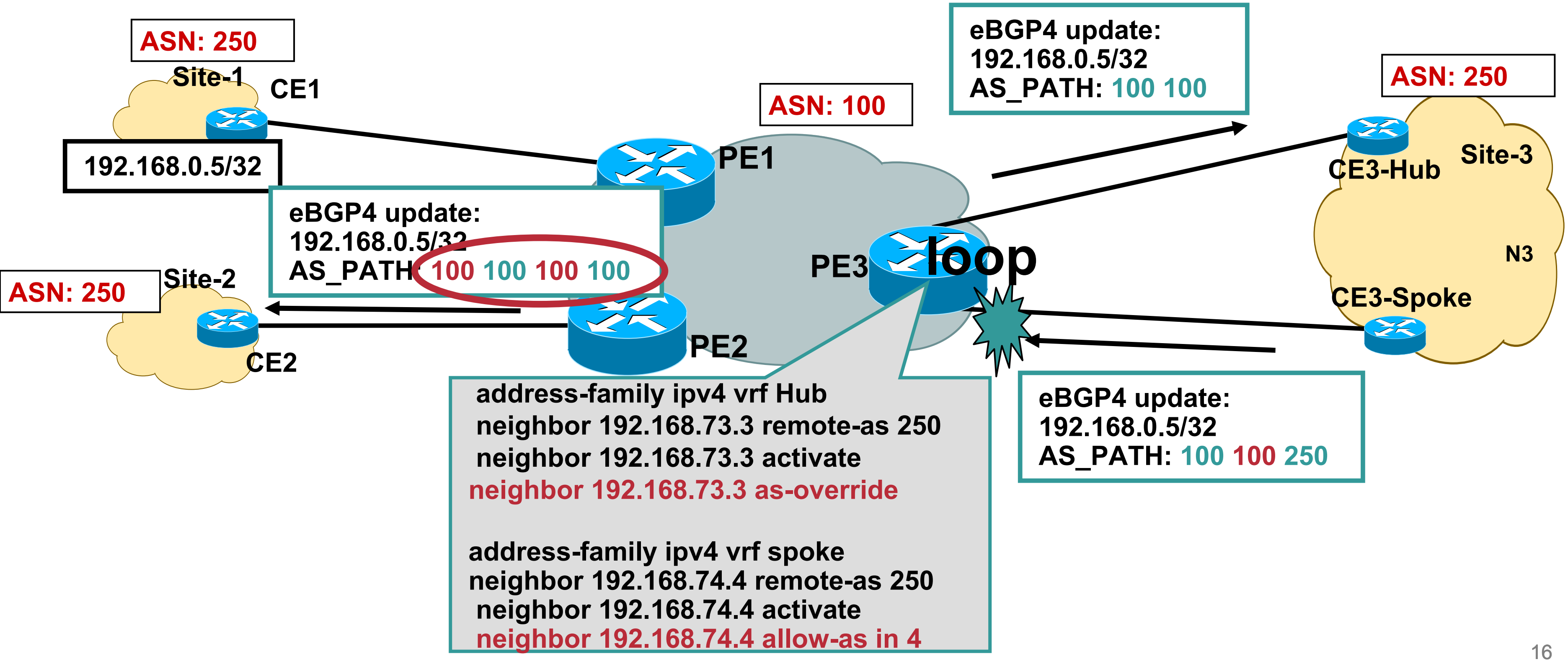
eBGP4 update:
192.168.0.5/32
AS_PATH: 65001

eBGP4 update:
192.168.0.5/32
AS_PATH:100 100

CE2 would discard the route as he would see his own AS in the AS-path of BGP update

VPN Topology considerations
Hub and Spoke Model

- PE3 sees its own AS in the AS-Path and rejects the update
- "Allow-as in" if configured at spoke Site, will allow the update at PE3 if it contains SP's ASN



eBGP4 update:
192.168.0.5/32
AS_PATH: 100 100

eBGP4 update:
192.168.0.5/32
AS_PATH: 100 100 100 100

eBGP4 update:
192.168.0.5/32
AS_PATH: 100 100 250

```
 address-family ipv4 vrf Hub
 neighbor 192.168.73.3 remote-as 250
 neighbor 192.168.73.3 activate
neighbor 192.168.73.3 as-override

address-family ipv4 vrf spoke
neighbor 192.168.74.4 remote-as 250
 neighbor 192.168.74.4 activate
 neighbor 192.168.74.4 allow-as in 4
```

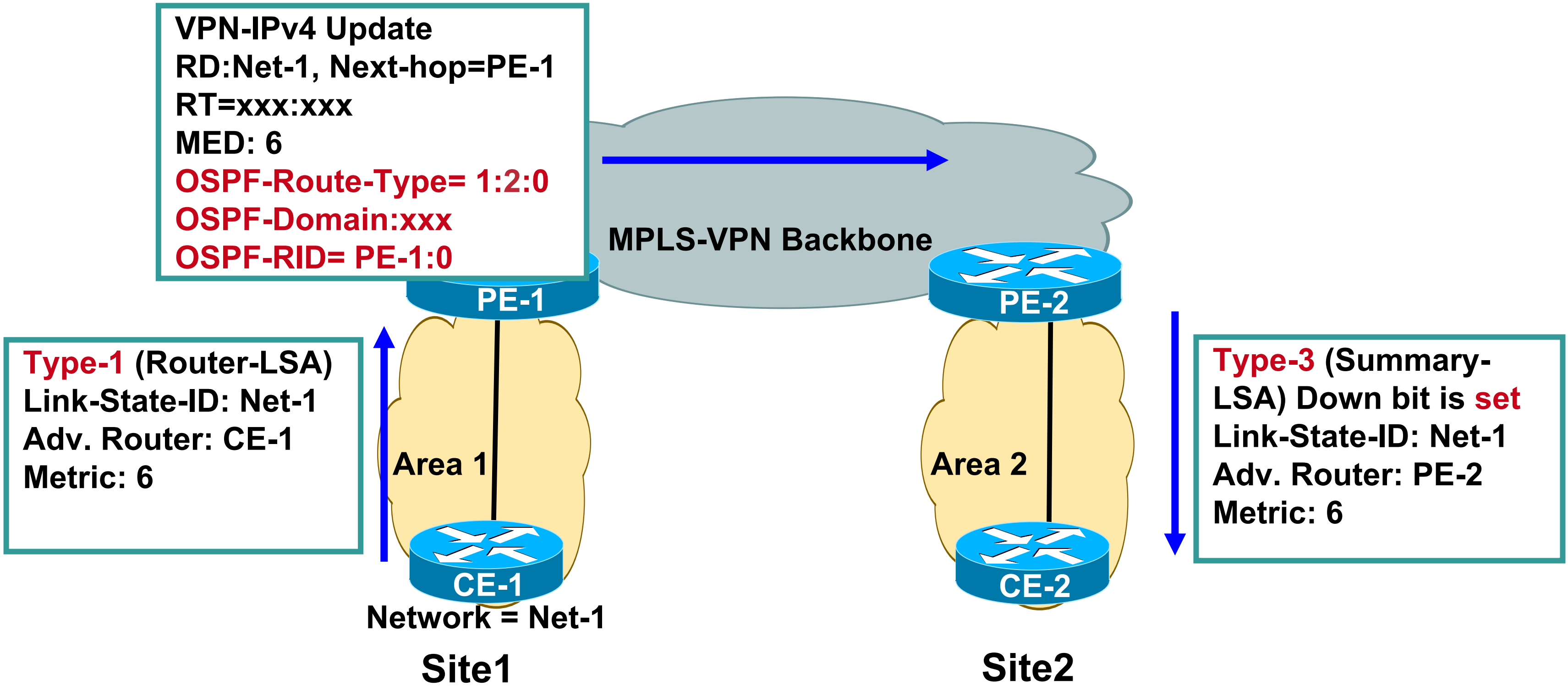
Agenda

- Introduction
- Physical Migration to MPLS VPN Backbone
- Routing considerations using
  - BGP as PE-CE protocol
  - **OSPF as PE-CE protocol**
  - EIGRP as PE-CE protocol
- Default route handling in MPLS VPN
- Preventing routing Loops with SOO
- Limiting vrf routes and potential black holing
- Multi-homing Scenarios
- Summary

Common Design Consideration- OSPF Area placement

OSPF Sites belong to different areas

- Area 0 is not mandatory when migrating to MPLS VPN service
- VPN sites may have different Sites configured for different areas
- If Area 0 exists, it must touch MPLS VPN PE routers.



VPN-IPv4 Update
RD:Net-1, Next-hop=PE-1
RT=xxx:xxx
MED: 6
OSPF-Route-Type= 1:2:0
OSPF-Domain:xxx
OSPF-RID= PE-1:0

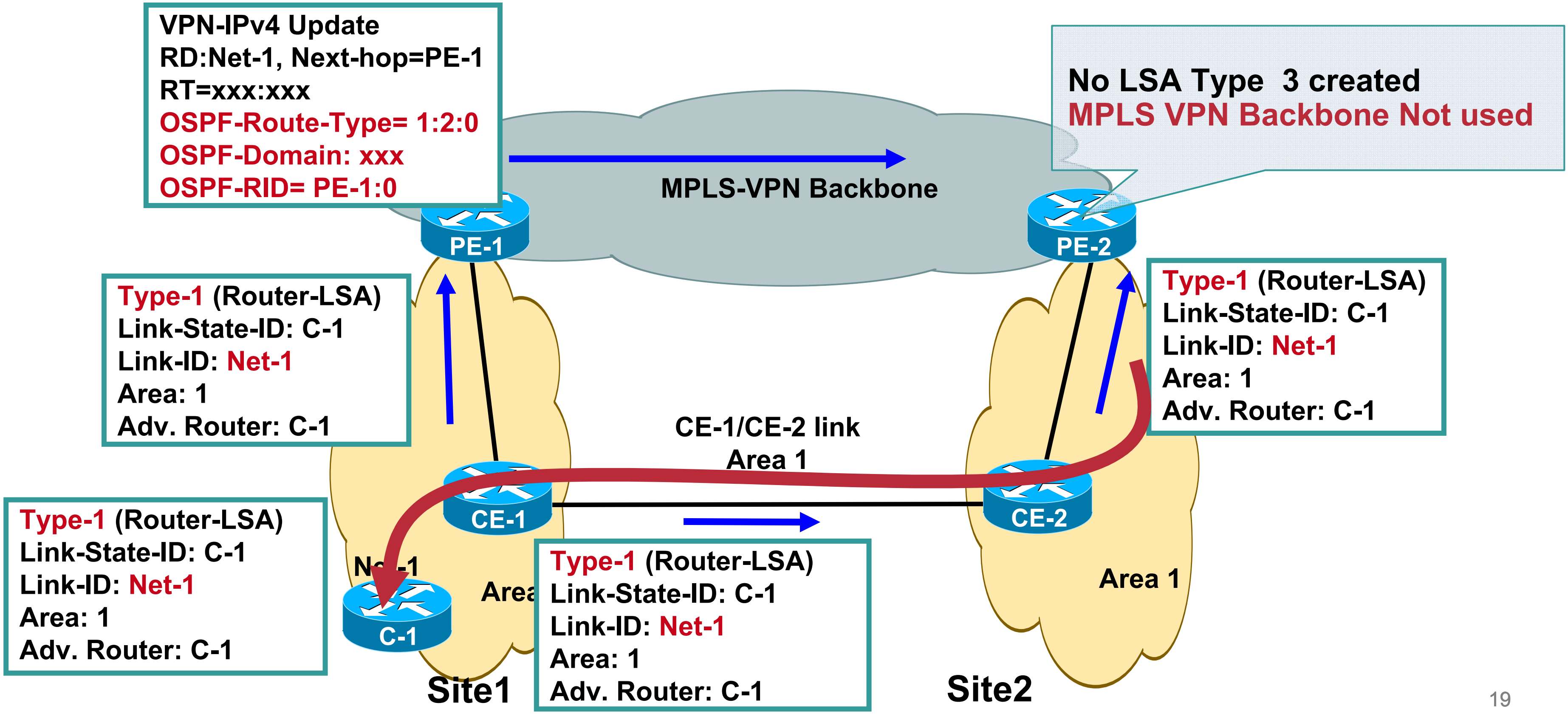
Type-1 (Router-LSA)
Link-State-ID: Net-1
Adv. Router: CE-1
Metric: 6

Type-3 (Summary-LSA) Down bit is set
Link-State-ID: Net-1
Adv. Router: PE-2
Metric: 6

Common Design Consideration- OSPF Area placement

Sites are in the same Area- Backdoor exists

- Customers Sites are in the same area and there is a backdoor link
- Route is advertised to MPLS VPN backbone
- Same prefix is learnt as intra-area route via backdoor link
- PE2 does not generate Type3 LSA once type-1 LSA is received from the site
- Traffic is sent over backdoor link instead of MPLS VPN cloud.



VPN-IPv4 Update
RD:Net-1, Next-hop=PE-1
RT=xxx:xxx
OSPF-Route-Type= 1:2:0
OSPF-Domain: xxx
OSPF-RID= PE-1:0

No LSA Type 3 created
MPLS VPN Backbone Not used

Type-1 (Router-LSA)
Link-State-ID: C-1
Link-ID: Net-1
Area: 1
Adv. Router: C-1

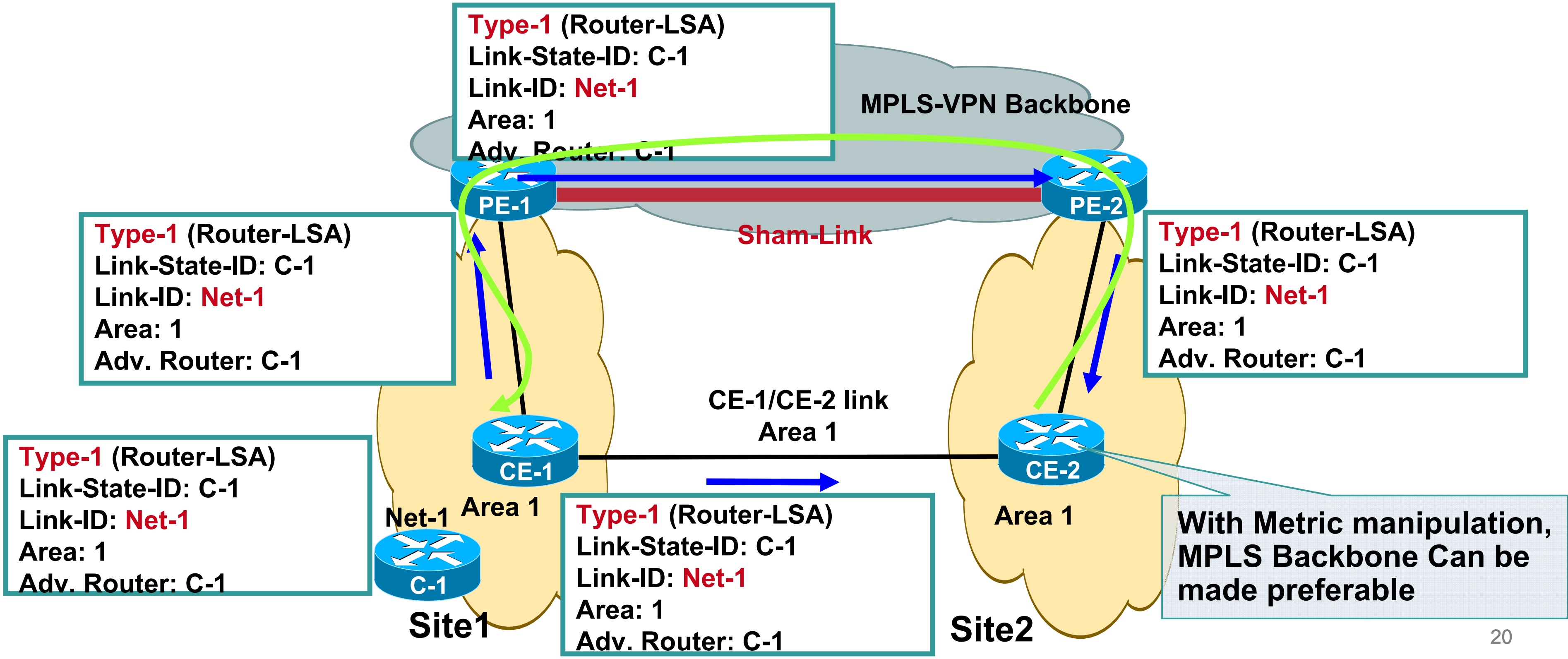
Type-1 (Router-LSA)
Link-State-ID: C-1
Link-ID: Net-1
Area: 1
Adv. Router: C-1

Type-1 (Router-LSA)
Link-State-ID: C-1
Link-ID: Net-1
Area: 1
Adv. Router: C-1

Type-1 (Router-LSA)
Link-State-ID: C-1
Link-ID: Net-1
Area: 1
Adv. Router: C-1

Common Design Consideration- OSPF Area placement
Sites are in the same Area- Backdoor with Sham link

- The sham link is treated as a virtual-link : unnumbered, ptp, DC link
- The sham link is reported in the router LSA's type 1 originated by the two routers connecting to the sham link
- The MPLS VPN backbone or the backdoor link can be made preferred path by tweaking the metrics



Type-1 (Router-LSA)
Link-State-ID: C-1
Link-ID: Net-1
Area: 1
Adv. Router: C-1

Type-1 (Router-LSA)
Link-State-ID: C-1
Link-ID: Net-1
Area: 1
Adv. Router: C-1

Type-1 (Router-LSA)
Link-State-ID: C-1
Link-ID: Net-1
Area: 1
Adv. Router: C-1

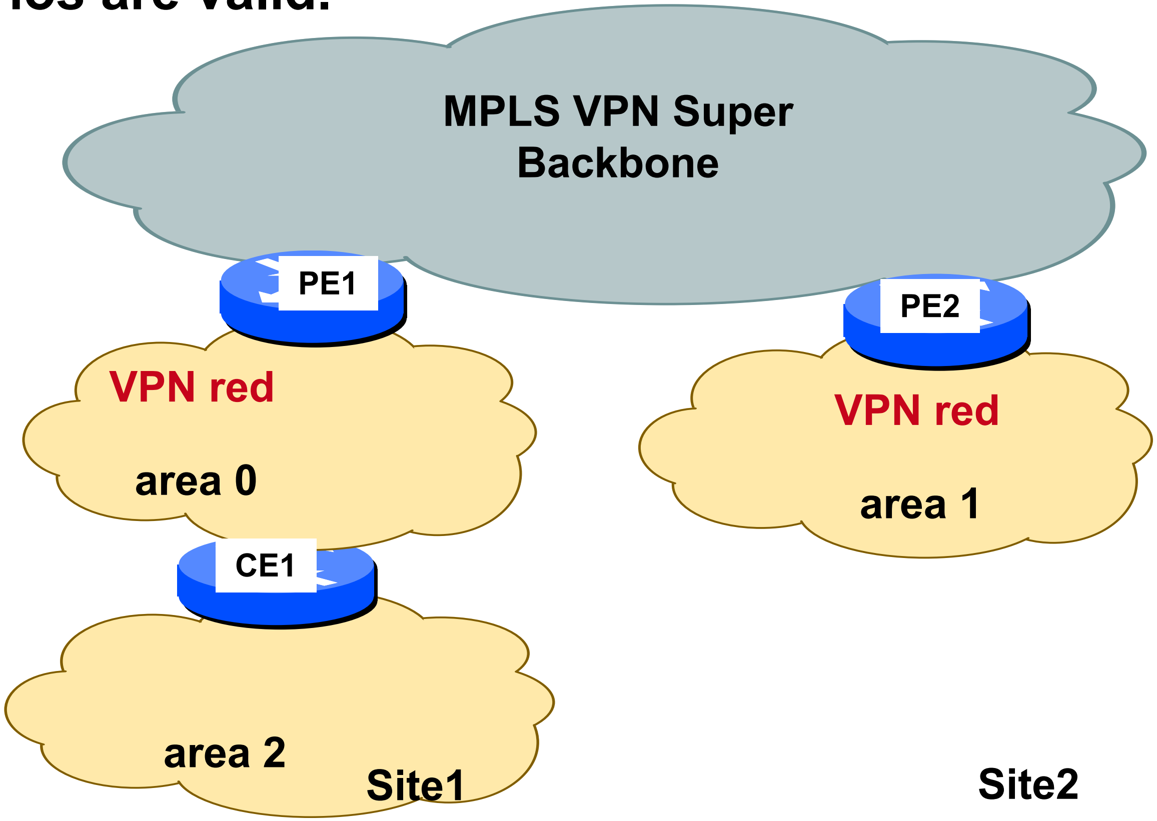
Type-1 (Router-LSA)
Link-State-ID: C-1
Link-ID: Net-1
Area: 1
Adv. Router: C-1

Type-1 (Router-LSA)
Link-State-ID: C-1
Link-ID: Net-1
Area: 1
Adv. Router: C-1

With Metric manipulation, MPLS Backbone Can be made preferable

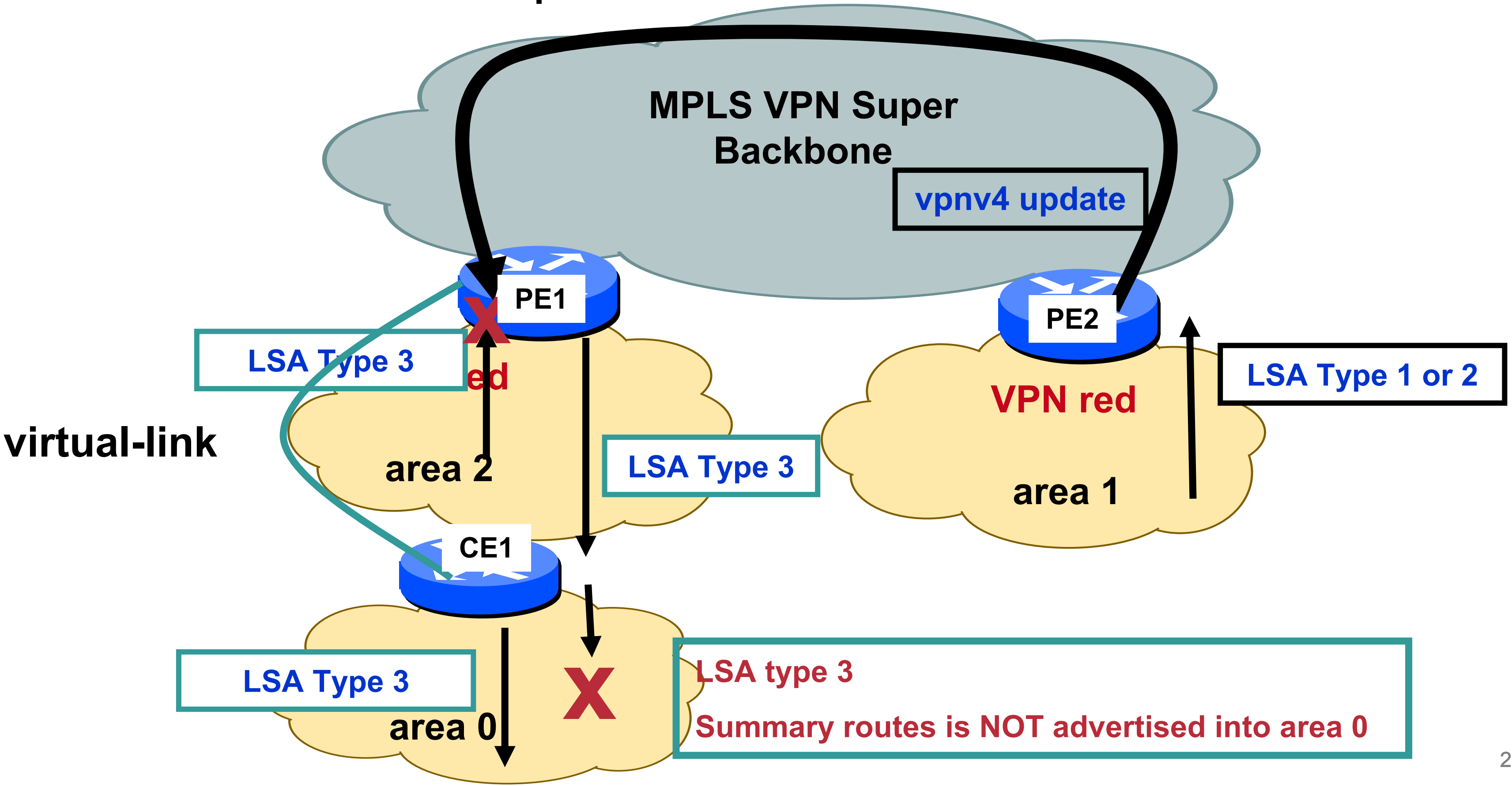
Common Design Consideration- OSPF Area placement
Other scenarios

- Some OSPF sites entirely belong to area 0 and some other sites can belong to non area 0
- Some sites may consist of hierarchical OSPF topology consisting of area 0 as well as non-zero areas.
- Both scenarios are valid.



Common Design Consideration- OSPF Area placement
Area 0 Placement

- As before some sites may consist of hierarchical OSPF topology consisting of area 0 as well as non-zero areas.
- If site contains area 0, it must touch provider PE router.
- OSPF RULE: Summary LSAs from non-zero area's are not injected into backbone area 0
- Inter-area routes will not show up unless a Virtual link is created.



LSA type 3

Summary routes is NOT advertised into area 0

Agenda

- Introduction
- Physical Migration to MPLS VPN Backbone
- Routing considerations using

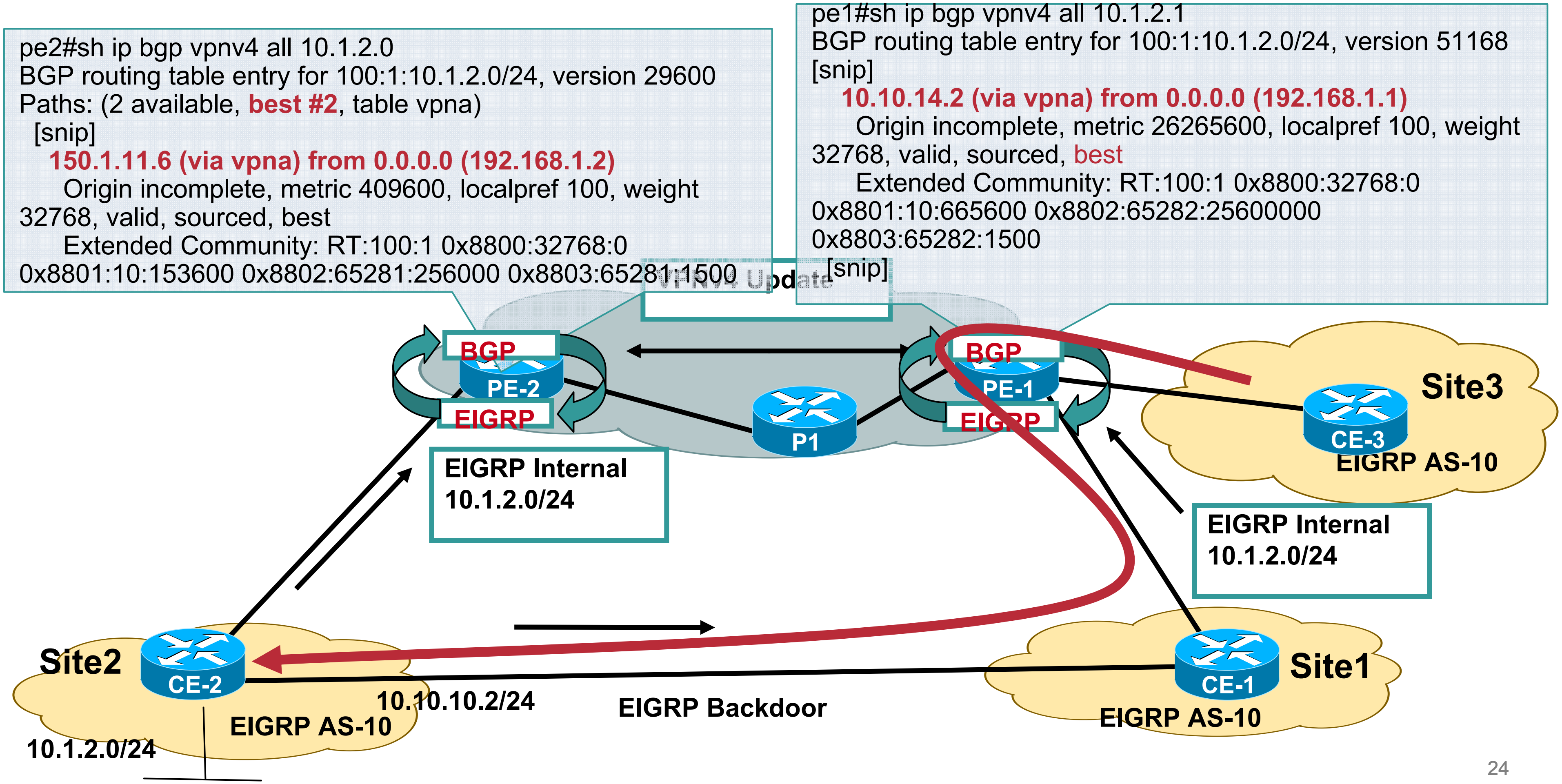
  BGP as PE-CE protocol

  OSPF as PE-CE protocol

  EIGRP as PE-CE protocol
- Default route handling in MPLS VPN
- Preventing routing Loops with SOO
- Limiting vrf routes and potential black holing
- Multi-homing Scenarios
- Summary

EIGRP Without backdoor Support

- Site 1 and Site3 are connected to PE1. In addition a backdoor link exists between site1 and site2.
- PE1 learns the route via EIGRP and also received the same route via iBGP from PE2.
- EIGRP route redistributed in BGP becomes locally sourced and is preferred over iBGP learnt route
- Site3 traffic destined for Site 2 arrives on PE1 but afterwards traverses site1 instead of MPLS BB.



```
pe2#sh ip bgp vpnv4 all 10.1.2.0
BGP routing table entry for 100:1:10.1.2.0/24, version 29600
Paths: (2 available, best #2, table vpna)
  [snip]
    150.1.11.6 (via vpna) from 0.0.0.0 (192.168.1.2)
      Origin incomplete, metric 409600, localpref 100, weight
32768, valid, sourced, best
      Extended Community: RT:100:1 0x8800:32768:0
0x8801:10:153600 0x8802:65281:256000 0x8803:65281:1500
```

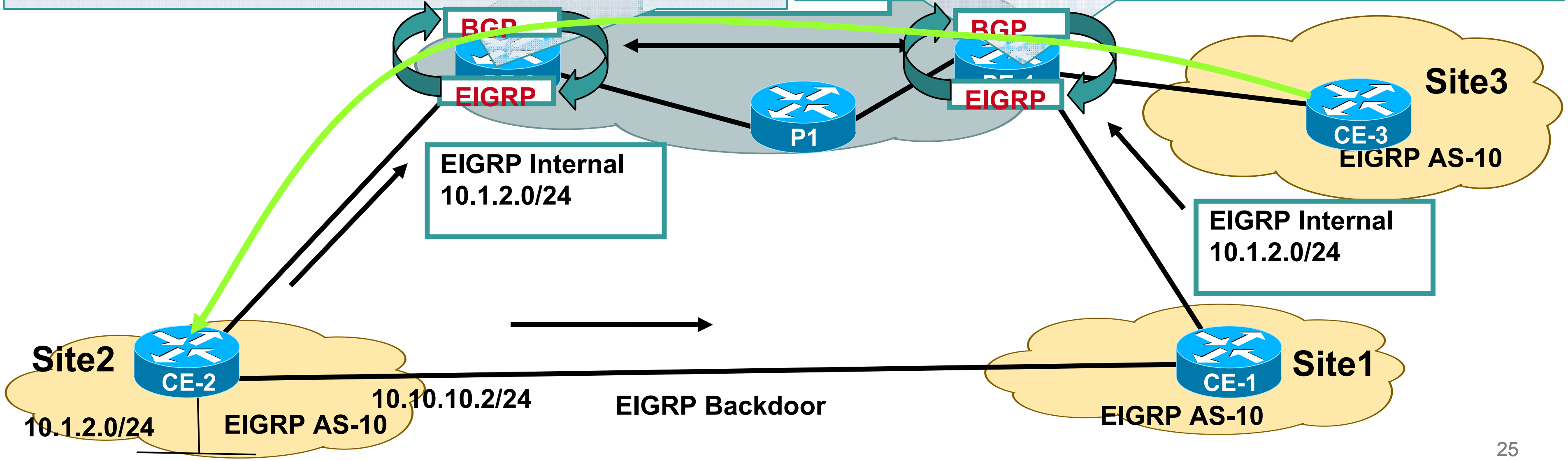
```
pe1#sh ip bgp vpnv4 all 10.1.2.1
BGP routing table entry for 100:1:10.1.2.0/24, version 51168
[snip]
    10.10.14.2 (via vpna) from 0.0.0.0 (192.168.1.1)
      Origin incomplete, metric 26265600, localpref 100, weight
32768, valid, sourced, best
      Extended Community: RT:100:1 0x8800:32768:0
0x8801:10:665600 0x8802:65282:25600000
0x8803:65282:1500
  [snip]
```

EIGRP With backdoor Support

- **With backdoor support, BGP route selection algorithm in the SP network has been modified. EIGRP metric of locally sourced and remote route is compared.**
- **Metric of locally received route is higher and includes the backdoor link metric (MPLS BB does not add additional metric)**

```
pe2#show ip bgp vpnv4 all 10.1.2.0
BGP routing table entry for 100:1:10.1.2.0/24, version 16
[snip]
150.1.11.6 (via vpna) from 0.0.0.0 (192.168.1.2)
     Origin incomplete, metric 409600, localpref 100, weight
32768, valid, sourced, best
     Extended Community: RT:100:1 Cost:pre-bestpath:128:409600
       0x8800:32768:0 0x8801:10:153600 0x8802:65281:256000
0x8803:65281:1500,
     mpls labels in/out 24/nolabel
```

```
pe1#show ip bgp vpnv4 all 10.1.2.0
BGP routing table entry for 100:1:10.1.2.0/24, version [snip]
   192.168.1.2 (metric 11) from 192.168.1.2 (192.168.1.2)
     Origin incomplete, metric 409600, localpref 100, valid,
internal, best
     Extended Community: RT:100:1 Cost:pre-bestpath:128:409600
       0x8800:32768:0 0x8801:10:153600 0x8802:65281:256000
0x8803:65281:1500,
     mpls labels in/out nolabel/24
```

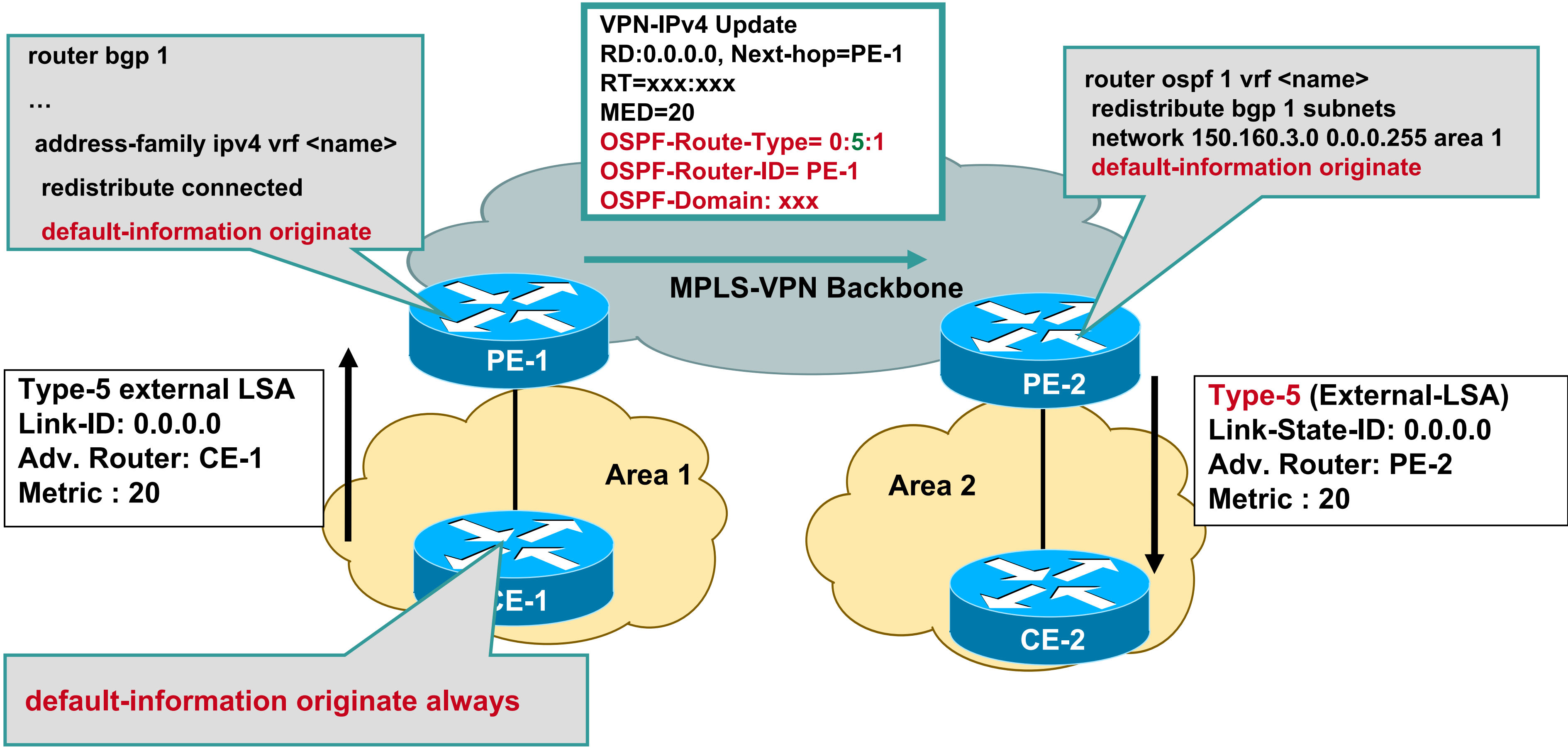


Agenda

- Introduction
- Physical Migration to MPLS VPN Backbone
- Routing considerations using
  - BGP as PE-CE protocol
  - OSPF as PE-CE protocol
  - EIGRP as PE-CE protocol
- **Default route handling in MPLS VPN**
- Preventing routing Loops with SOO
- Limiting vrf routes and potential black holing
- Multi-homing Scenarios
- Summary

Default Route origination (OSPF/EIGRP)

BGP by default does not redistribute 0.0.0.0/0



```
router bgp 1
…
 address-family ipv4 vrf <name>
  redistribute connected
  default-information originate
```

VPN-IPv4 Update
RD:0.0.0.0, Next-hop=PE-1
RT=xxx:xxx
MED=20
OSPF-Route-Type= 0:5:1
OSPF-Router-ID= PE-1
OSPF-Domain: xxx

```
router ospf 1 vrf <name>
 redistribute bgp 1 subnets
 network 150.160.3.0 0.0.0.255 area 1
 default-information originate
```

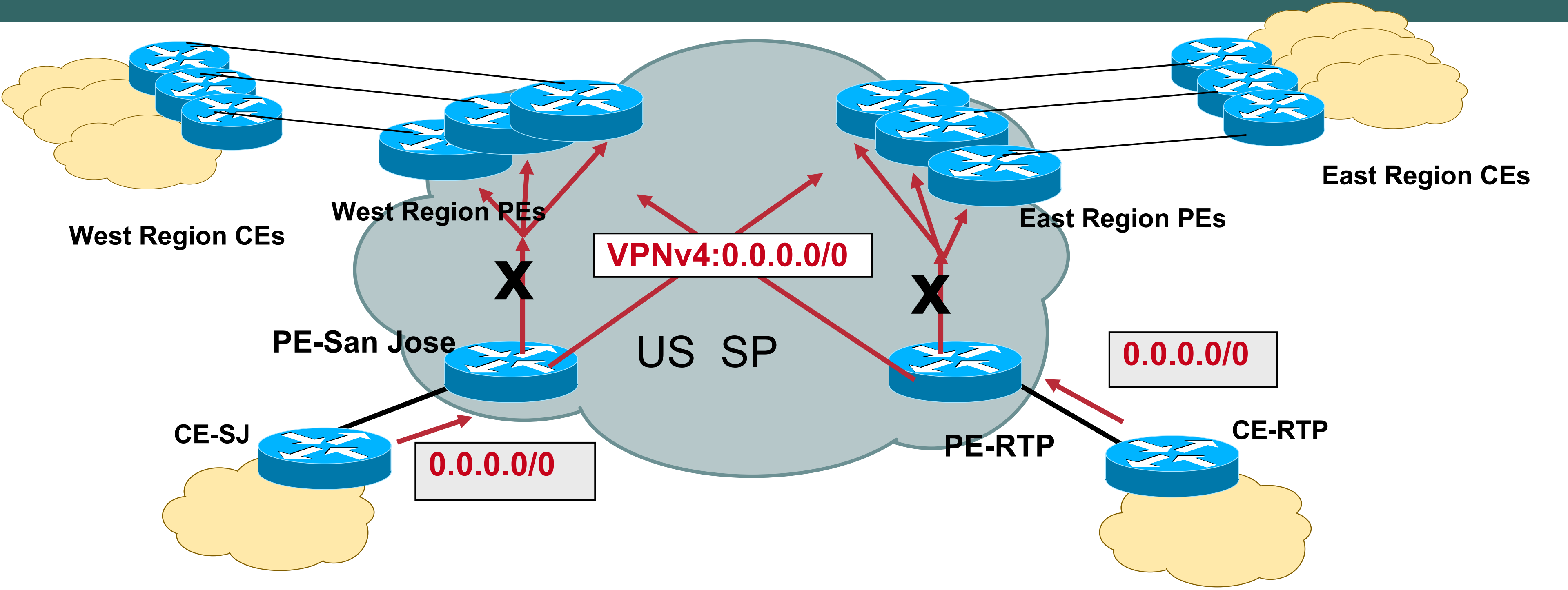
Type-5 external LSA
Link-ID: 0.0.0.0
Adv. Router: CE-1
Metric : 20

Type-5 (External-LSA)
Link-State-ID: 0.0.0.0
Adv. Router: PE-2
Metric : 20

```
default-information originate always
```

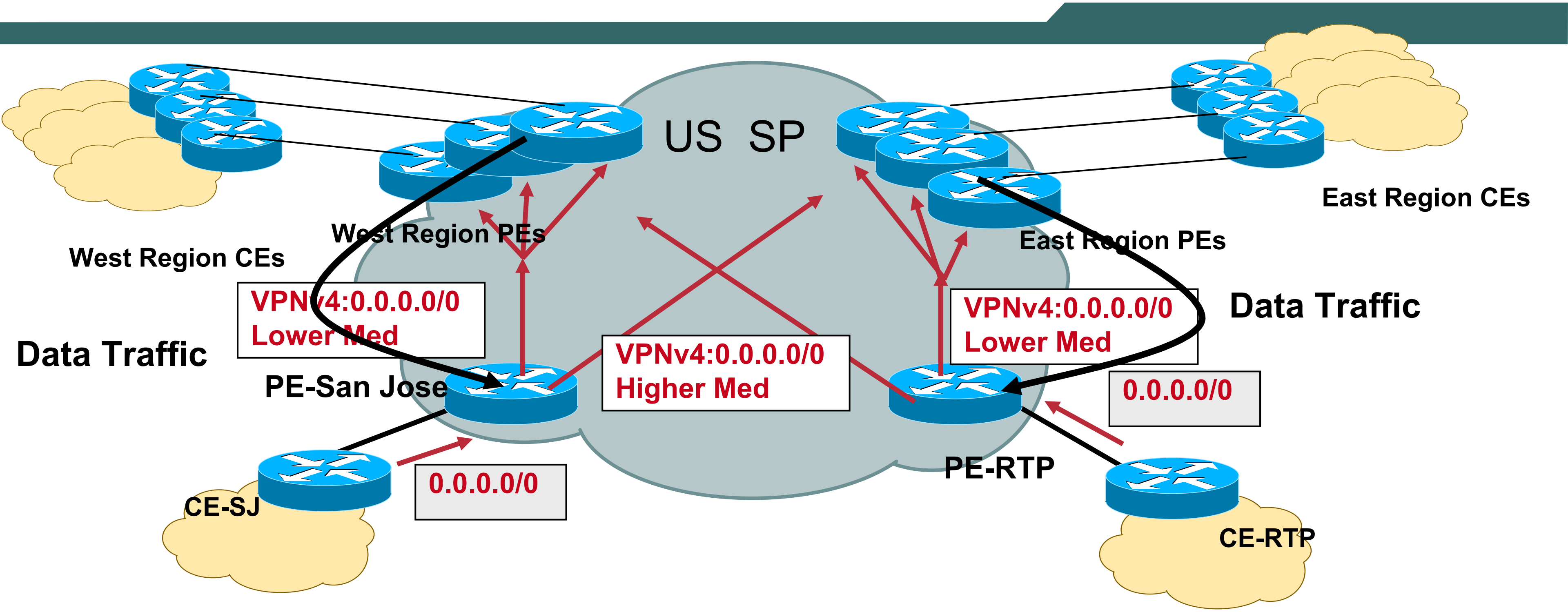
Similar configuration needs to be done for EIGRP

Default Route in Multi-hub Environment Design Objective



- Both San Jose and RTP advertise Default routes to the spoke Sites
- Satellite Sites in West Coast Region should take the default route to SJ and East Coast Sites should use RTP for default route
- In case of failure, spoke Sites should take the non-preferred default route

Default Route in Multi-hub Environment Possible Solution



- •Over here it is proposed that when we advertise default route it would be in such a way that West Region PEs receives a lower med from SJ and higher med from RTP .
- •Similarly East Region PEs receives a default route with a lower med from RTP and higher med from SJ
- •In this way if SJ lost is route West Coast can then revert to the RTP
- •Note: We have used med as an example any other BGP attribute can be used

Agenda

- Introduction
- Physical Migration to MPLS VPN Backbone
- Routing considerations using

  BGP as PE-CE protocol

  OSPF as PE-CE protocol

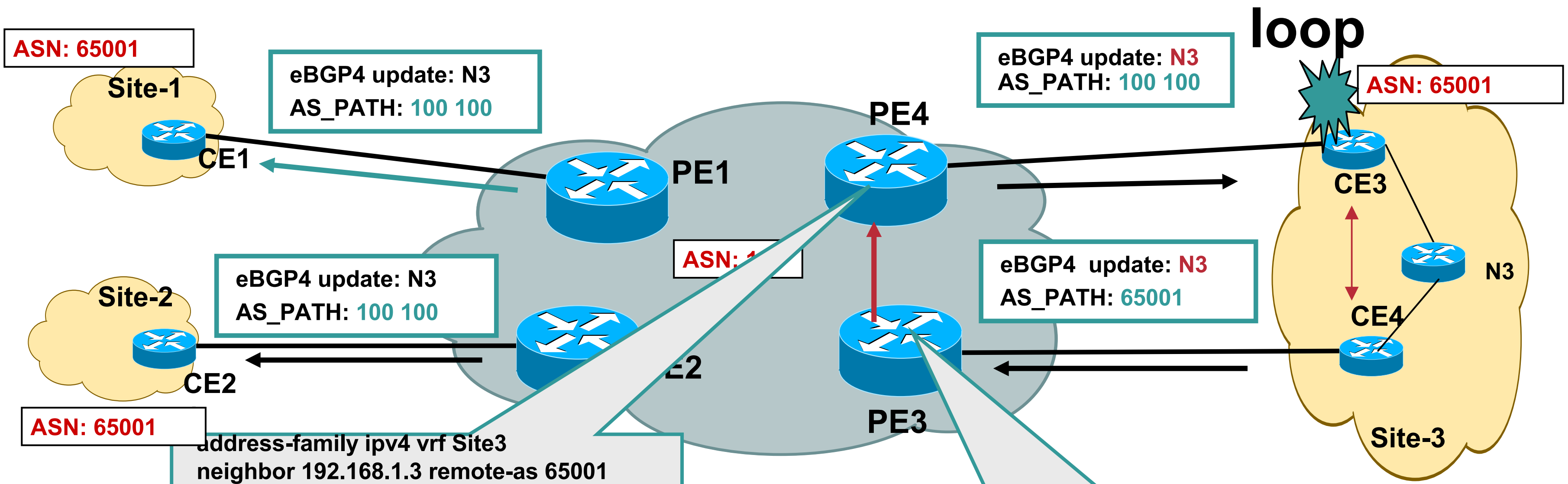
  EIGRP as PE-CE protocol
- Default route handling in MPLS VPN
- Preventing routing Loops with SOO
- Limiting vrf routes and potential black holing
- Multi-homing Scenarios
- Summary

Implementing SOO for Loop Prevention

- The SOO (extended BGP community) can be used to prevent loops in these scenarios.
- The SOO is needed only for multihomed sites.
- When EBGP is run between PE and CE routers, the SOO is configured through a route map command.
- For other routing protocols, the SOO can be applied to routes learned through a particular VRF interface during the redistribution into BGP.

Avoiding loops with SOO

- Not a hub and spoke scenario
- You don’t want the routes sent from site3 CE4 to be sent back to site3 via PE4



ASN: 65001

eBGP4 update: N3
AS_PATH: 100 100

eBGP4 update: N3
AS_PATH: 100 100

ASN: 65001

eBGP4 update: N3
AS_PATH: 100 100

ASN: 65001

ASN: 1

eBGP4 update: N3
AS_PATH: 65001

```
address-family ipv4 vrf Site3
neighbor 192.168.1.3 remote-as 65001
neighbor 192.168.1.3 activate
neighbor 192.168.1.3 as-override
neighbor 192.168.1.3 route-map set_ soo in
no auto-summary
no synchronization
exit-address-family
!
route-map set_soo permit 10
 set extcommunity soo 100:65003
```

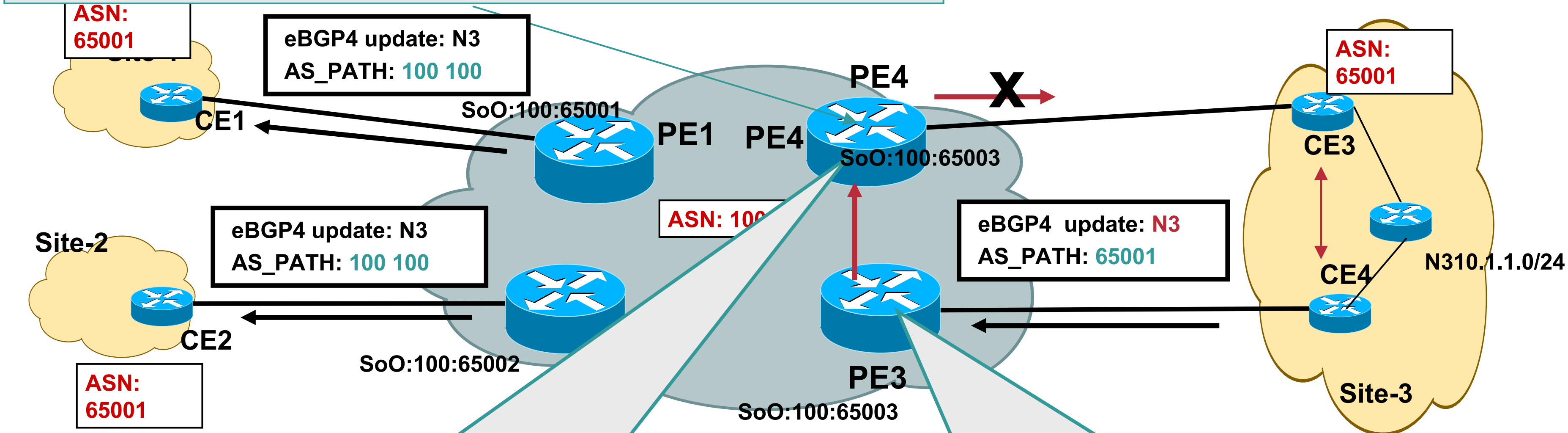
```
!
 address-family ipv4 vrf Site3
 neighbor 192.168.2.3 remote-as 65001
 neighbor 192.168.2.3 activate
 neighbor 192.168.2.3 as-override
 neighbor 192.168.2.3 route-map set_ soo in
 no auto-summary
 no synchronization
 exit-address-family
 !
route-map set_soo permit 10
 set extcommunity soo 100:65003
```

ip vrf sitemap *route-map-name*

Avoiding loops with SOO

- **PE3 and PE4 are configured with the same SoO value**
- **If SoO in the BGP update matches with the configured value, update will not be forwarded to CE3**
- **Note: In fact PE4 will never forward the update to CE3 even if the site-3 is segmented (and say CE3 and CE4 can not communicate with each other using intra-site routing)**

```
BGP(2): 192.168.2.3 soo loop detected for 192.168.0.5/32 - sending unreachable
```



```
PE4#show ip bgp vpnv4 vrf sit3 10.1.1.0/24
!
 192.168.1.1 (metric 20) from 192.168.1.1 (192.168.1.1)
    Origin incomplete, metric 0, localpref 100, valid, internal, best
    Extended Community: SoO:100:65003 RT:1:2
```

```
PE3#sh ip bgp vpnv4 vrf Site3 10.1.1.0/24

[snip]
   192.168.2.3 from 192.168.2.3 (10.1.1.1)
     Origin incomplete, metric 409600, localpref 100, valid, external
     Extended Community: SoO:100:65003 RT:100:1
```

Agenda

- Introduction
- Physical Migration to MPLS VPN Backbone
- Routing considerations using

  BGP as PE-CE protocol

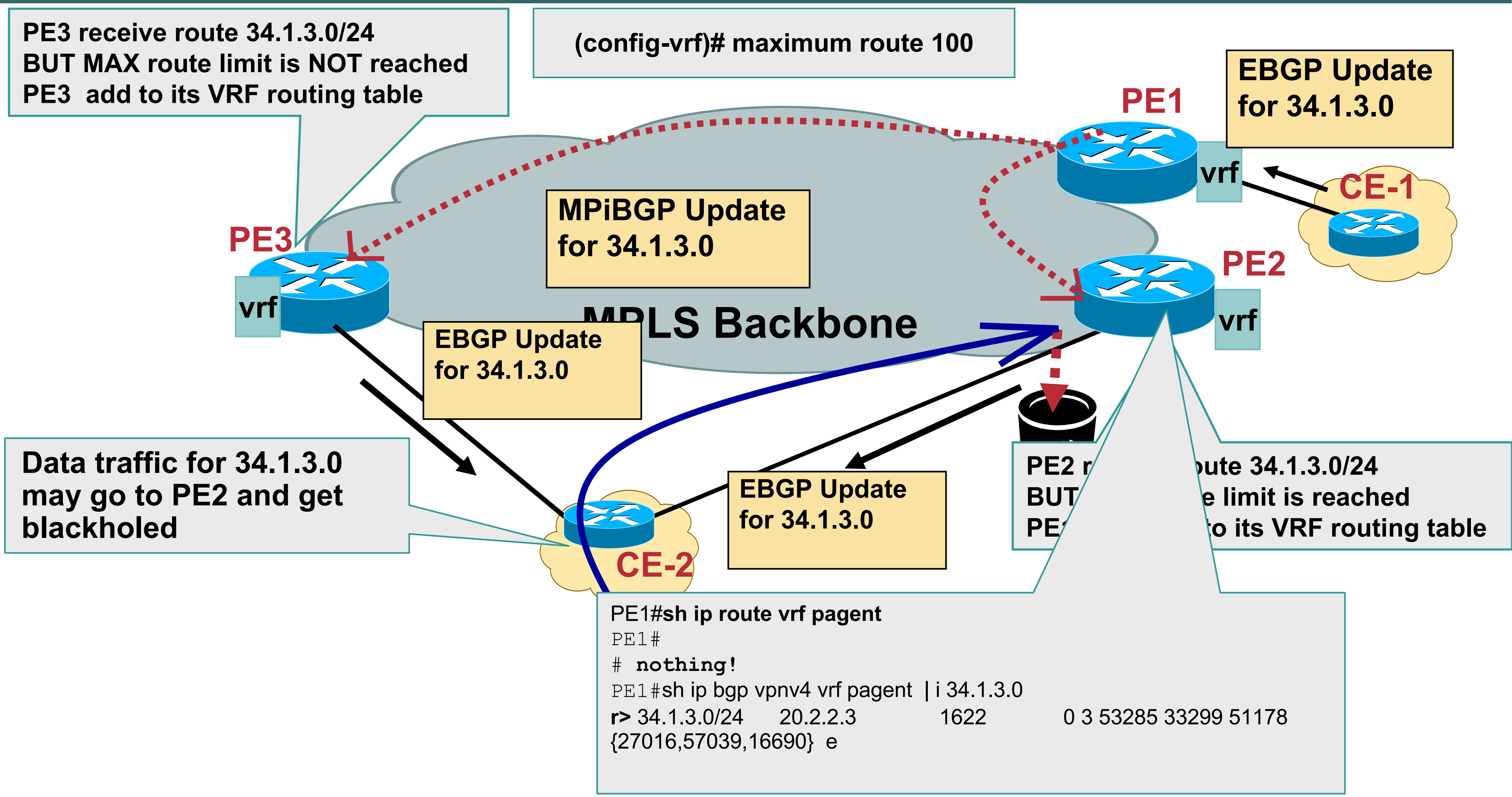
  OSPF as PE-CE protocol

  EIGRP as PE-CE protocol
- Default route handling in MPLS VPN
- Preventing routing Loops with SOO
- **Limiting vrf routes and potential black holing**
- Multi-homing Scenarios
- Summary

VRF route limit

- VRF route limit allows the Service Provider to protect his PE routers from uncontrolled route advertisements from CE routers
- VRF route-limit allows to limit the number of routes that are imported into a VRF
  - Routes coming from CE routers
  - Routes coming from other PEs (imported routes)
- The route limit is configured for each VRF
- If the number of routes exceed the route-limit
  - Syslog message is generated
  - Routes are not inserted into VRF anymore
    - Optional

Max Routes exceeded- Route propagation Potential Blackholing



PE3 receive route 34.1.3.0/24
BUT MAX route limit is NOT reached
PE3 add to its VRF routing table

(config-vrf)# maximum route 100

EBGP Update
for 34.1.3.0

MPiBGP Update
for 34.1.3.0

EBGP Update
for 34.1.3.0

EBGP Update
for 34.1.3.0

Data traffic for 34.1.3.0
may go to PE2 and get
blackholed

PE2 r oute 34.1.3.0/24
BUT e limit is reached
PE o its VRF routing table

```
PE1#sh ip route vrf pagent
PE1#
# nothing!
PE1#sh ip bgp vpnv4 vrf pagent  | i 34.1.3.0
r> 34.1.3.0/24       20.2.2.3             1622            0 3 53285 33299 51178
{27016,57039,16690}  e
```

- Enable suppress-inactive feature on PE2 to disable advertisements of BGP routes that don’t make it to the routing table

Agenda

- Introduction
- Physical Migration to MPLS VPN Backbone
- Routing considerations using

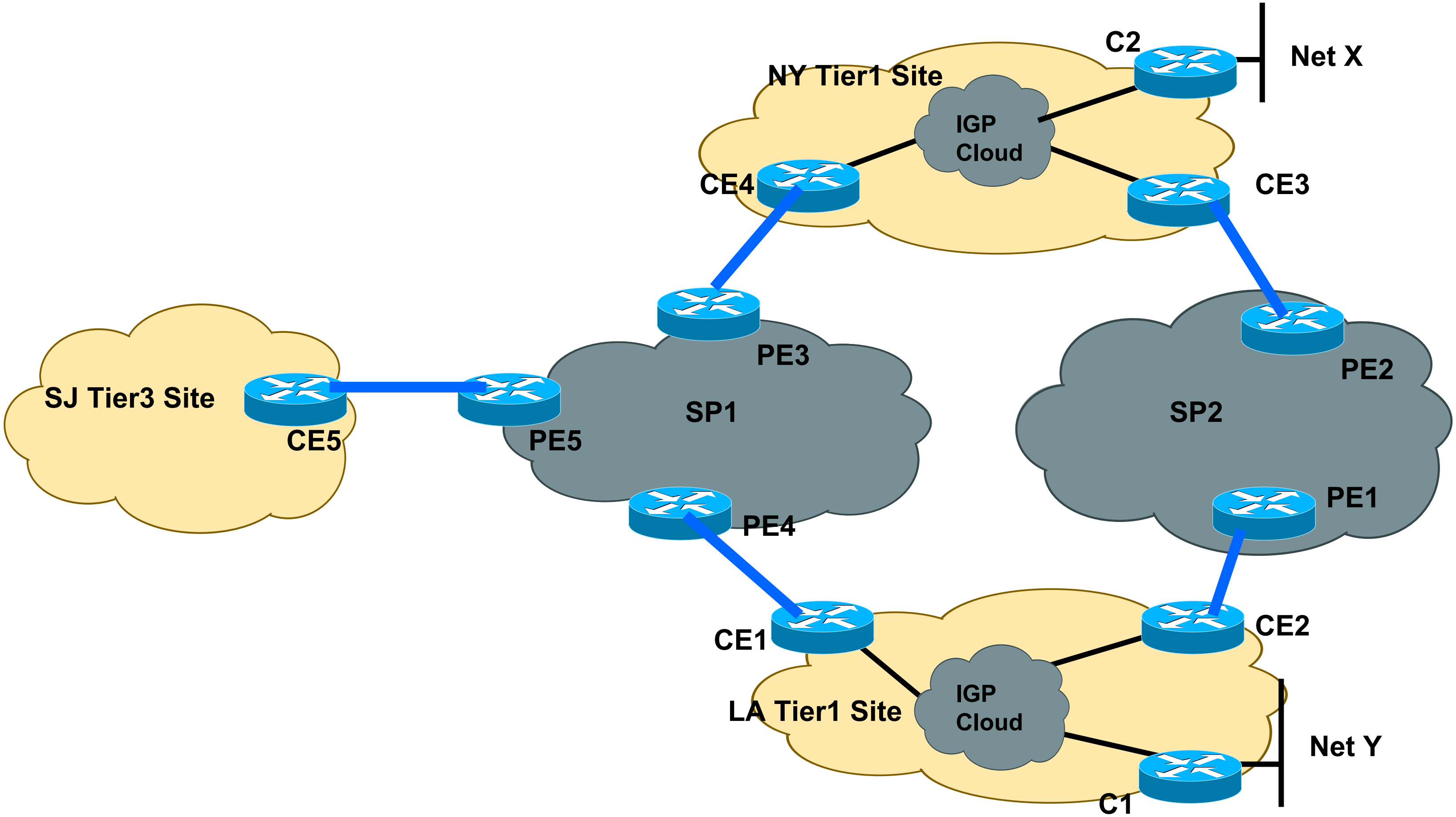
  BGP as PE-CE protocol

  OSPF as PE-CE protocol

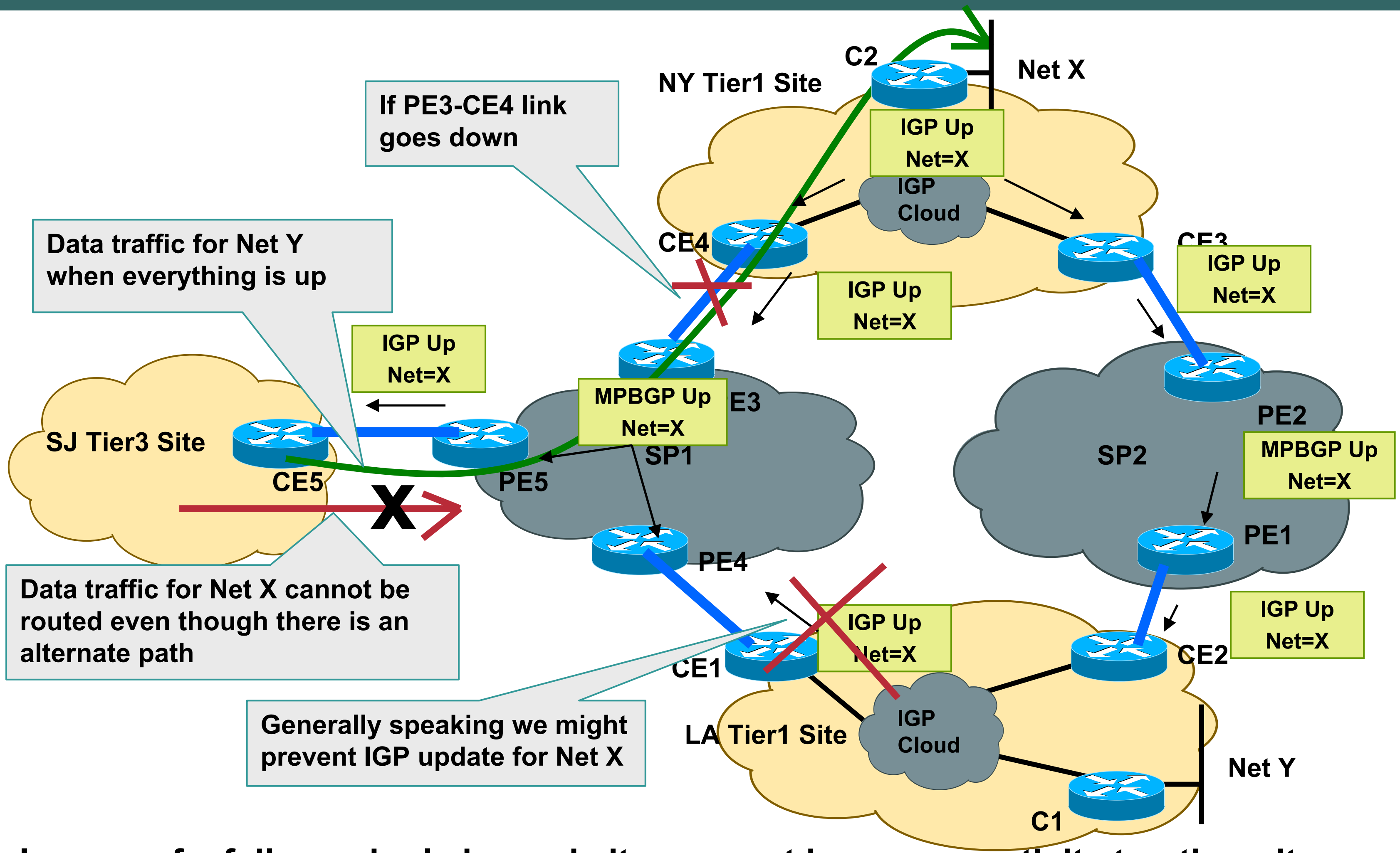
  EIGRP as PE-CE protocol
- Default route handling in MPLS VPN
- Preventing routing Loops with SOO
- Limiting vrf routes and potential black holing
- **Multi-homing Scenarios**
- Summary

Multi-tier Sites in Multi-homed Enterprise

- An enterprise might choose multiple providers for their L3VPN services
- It is possible that some of the enterprise satellite sites might be single homed.
- Unpredictable routing behavior may occur in the steady state or after a failure



Tier3 Site transiting Tier 1 Site- Problem



If PE3-CE4 link goes down

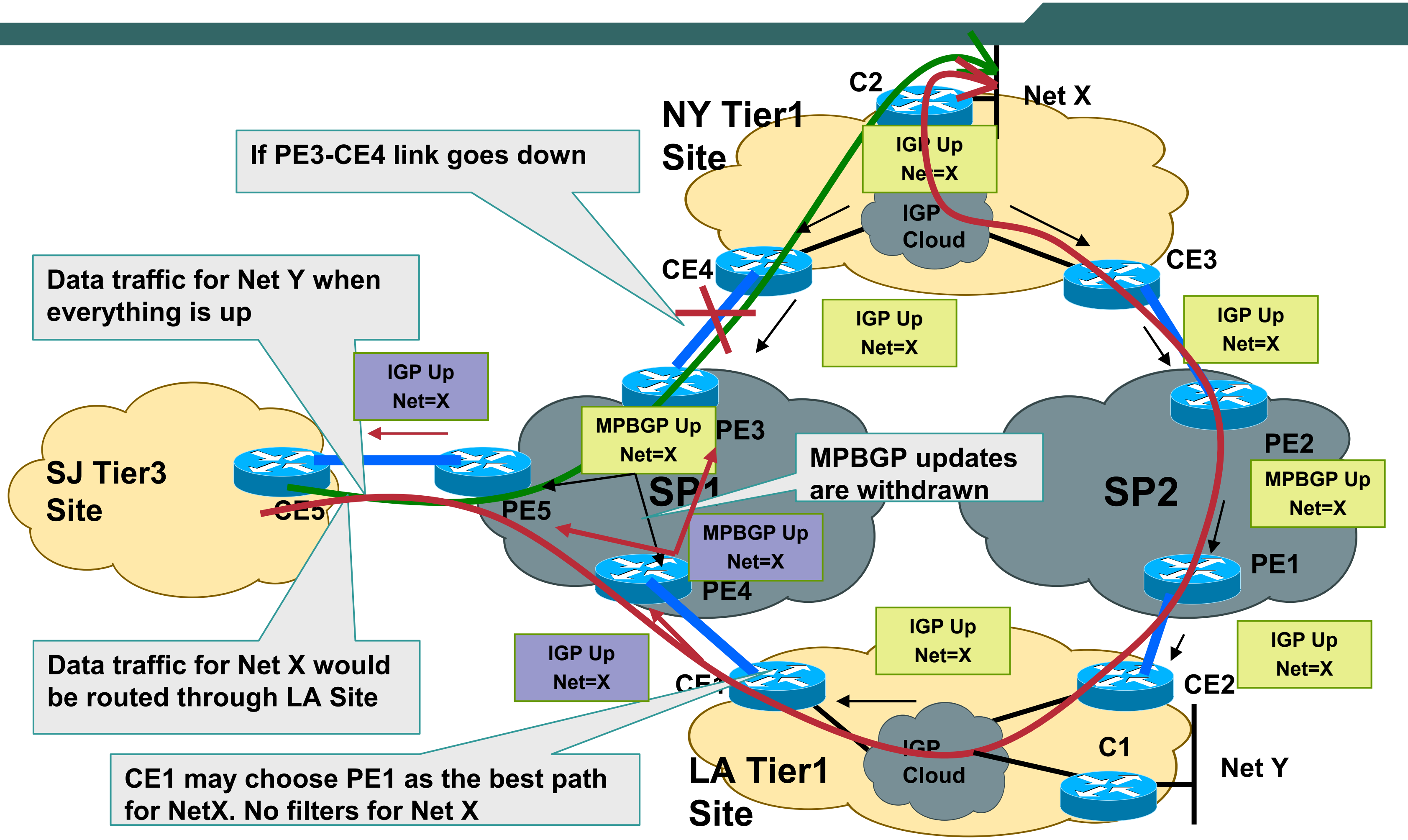
Data traffic for Net Y when everything is up

Data traffic for Net X cannot be routed even though there is an alternate path

Generally speaking we might prevent IGP update for Net X

- In case of a failure, single homed site may not have connectivity to other sites
- Even though an alternate path exists but update was blocked to ensure traffic doesn’t take sub-optimal path by transiting the enterprise site

Tier3 Site transiting Tier 1 Site – Possible Solution



If PE3-CE4 link goes down

Data traffic for Net Y when everything is up

Data traffic for Net X would be routed through LA Site

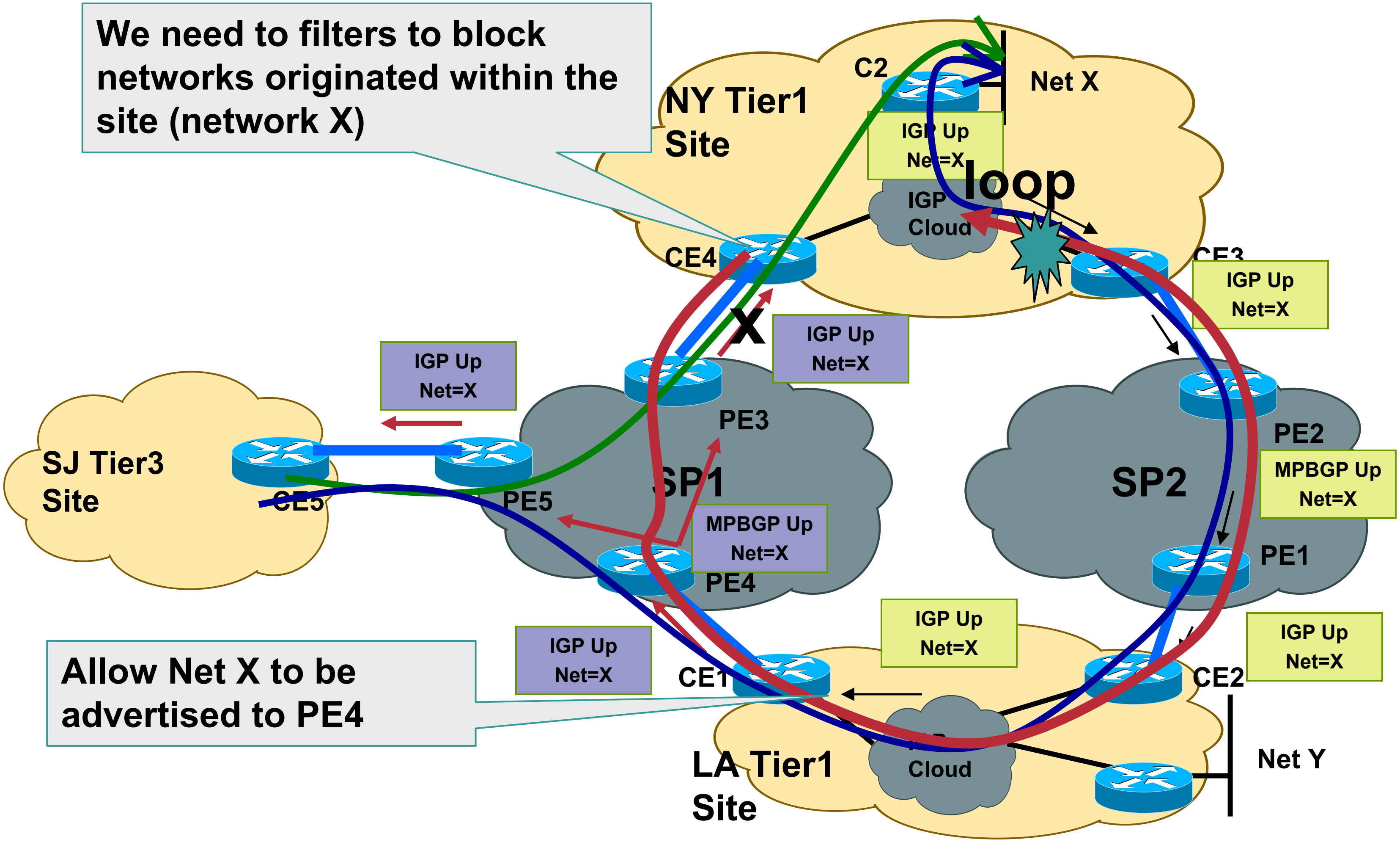
CE1 may choose PE1 as the best path for NetX. No filters for Net X

MPBGP updates are withdrawn

- Don’t filter the routes that do not belong to the site
- SP cloud now sees two routes. With appropriate metric manipulation, PE5 can choose path via PE3 as the primary path.
- In case of failure, an alternate valid path will be available via PE4

Tier3 Site transiting Tier 1 Site
Suboptimal Routing and Routing Loops - Caveat

We need to filters to block networks originated within the site (network X)



Allow Net X to be advertised to PE4

- CE4 can possibly choose PE3 as the best path for Net X which can result in suboptimal routing and possible routing loops

Agenda

- Introduction
- Physical Migration to MPLS VPN Backbone
- Routing considerations using

  BGP as PE-CE protocol

  OSPF as PE-CE protocol

  EIGRP as PE-CE protocol
- Default route handling in MPLS VPN
- Preventing routing Loops with SOO
- Limiting vrf routes and potential black holing
- Multi-homing Scenarios
- Summary

Summary

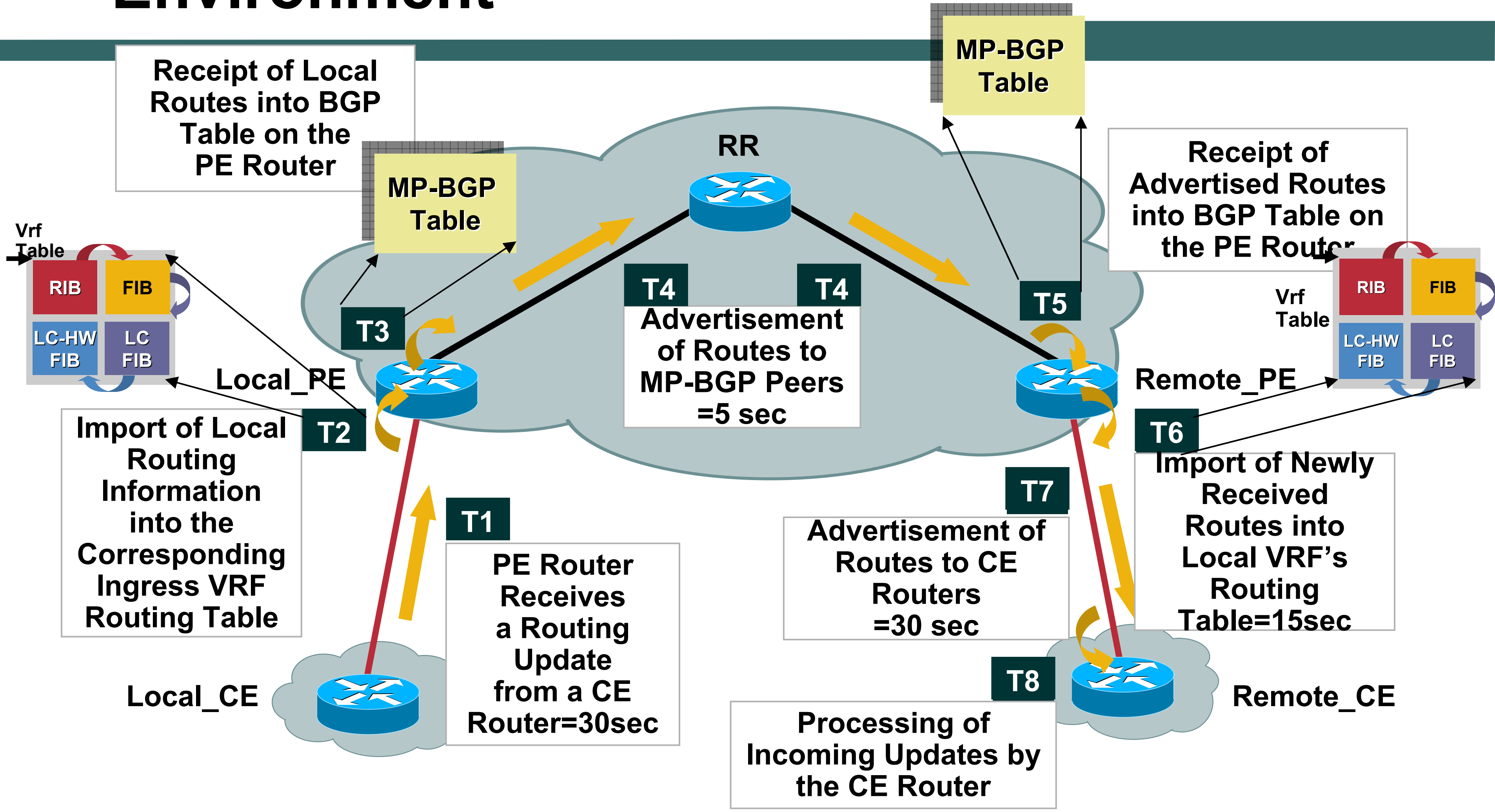
- For large enterprises, migration to L3VPN service requires a phased approach so that disruption to existing services is minimal
- Existing site local routing protocols policies and their interaction with PE-CE routing protocols should be carefully analyzed
- Topological considerations such as backdoor links, multi-homing scenarios, OSPF areas placement and BGP AS number scheme etc should be taken into account to avoid sub-optimal routing or loops.
- Default route and Summarization is important for proper routing to the internet or to the central sites and could be coordinated with the service provider for optimal results.
- Site-to-site VPN routing convergence should be kept in mind while deploying delay sensitive application
- Redundancy and Multi-provider topologies may result in loops if not properly implemented.

Q&A

Backup slides

Site-to-Site VPN Routing Convergence

Site-to-site Convergence in MPLS VPN Environment

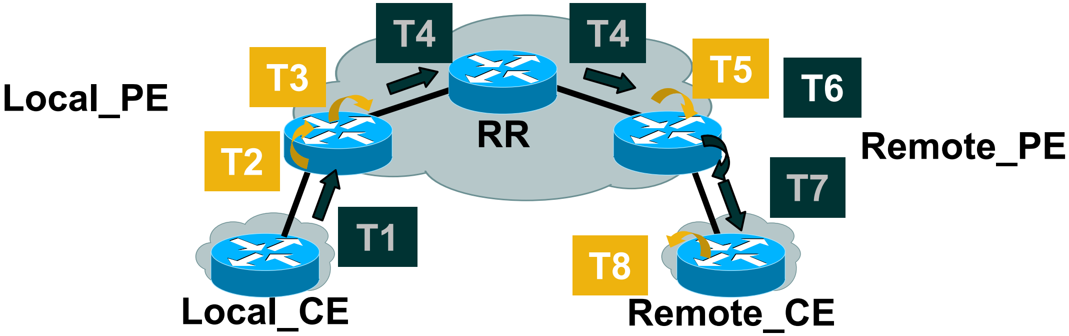


Receipt of Local Routes into BGP Table on the PE Router
MP-BGP Table
MP-BGP Table
RR
Receipt of Advertised Routes into BGP Table on the PE Router
Vrf Table
RIB
FIB
LC-HW FIB
LC FIB
Vrf Table
RIB
FIB
LC-HW FIB
LC FIB
T3
T4
T4
T5
Advertisement of Routes to MP-BGP Peers =5 sec
Local_PE
Remote_PE
T2
T6
Import of Local Routing Information into the Corresponding Ingress VRF Routing Table
Import of Newly Received Routes into Local VRF's Routing Table=15sec
T7
T1
Advertisement of Routes to CE Routers =30 sec
PE Router Receives a Routing Update from a CE Router=30sec
T8
Local_CE
Remote_CE
Processing of Incoming Updates by the CE Router

- Convergence depends on the Service provider network
- Site-to-Site convergence heavily dependant on MP-BGP convergence in the provider network
- End-to-End convergence sum of highlighted Convergence PointsT1 thru T8

Summary (Theoretical Convergence)

- Two sets of timers; first set consists of T1, T4, T6 and T7; second set comprises of T2, T3, T5 and T8
- First set mainly responsible for the slower convergence unless aggressively tweaked down
- Theoretically sums up to ~ 85 seconds [30 (T1)+5*2 (T4)+15(T6)+30 (T7)]
- Once different timers are tuned, convergence mainly depends on T6; min T6=5 secs
- Assuming ~“x” secs for T2, T3, T5 and T8 collectively



PE-CE Protocol	Max Conv. Time (Default Settings)	Max Conv. Time (Timers Tweaked Scan=5, Adv=0)
BGP	~85+x Seconds	~5+x Seconds
OSPF	~25+x Seconds	~5+x Seconds
EIGRP	~25+x Seconds	~5+x Seconds
RIP	~85+x Seconds	~5+x Seconds