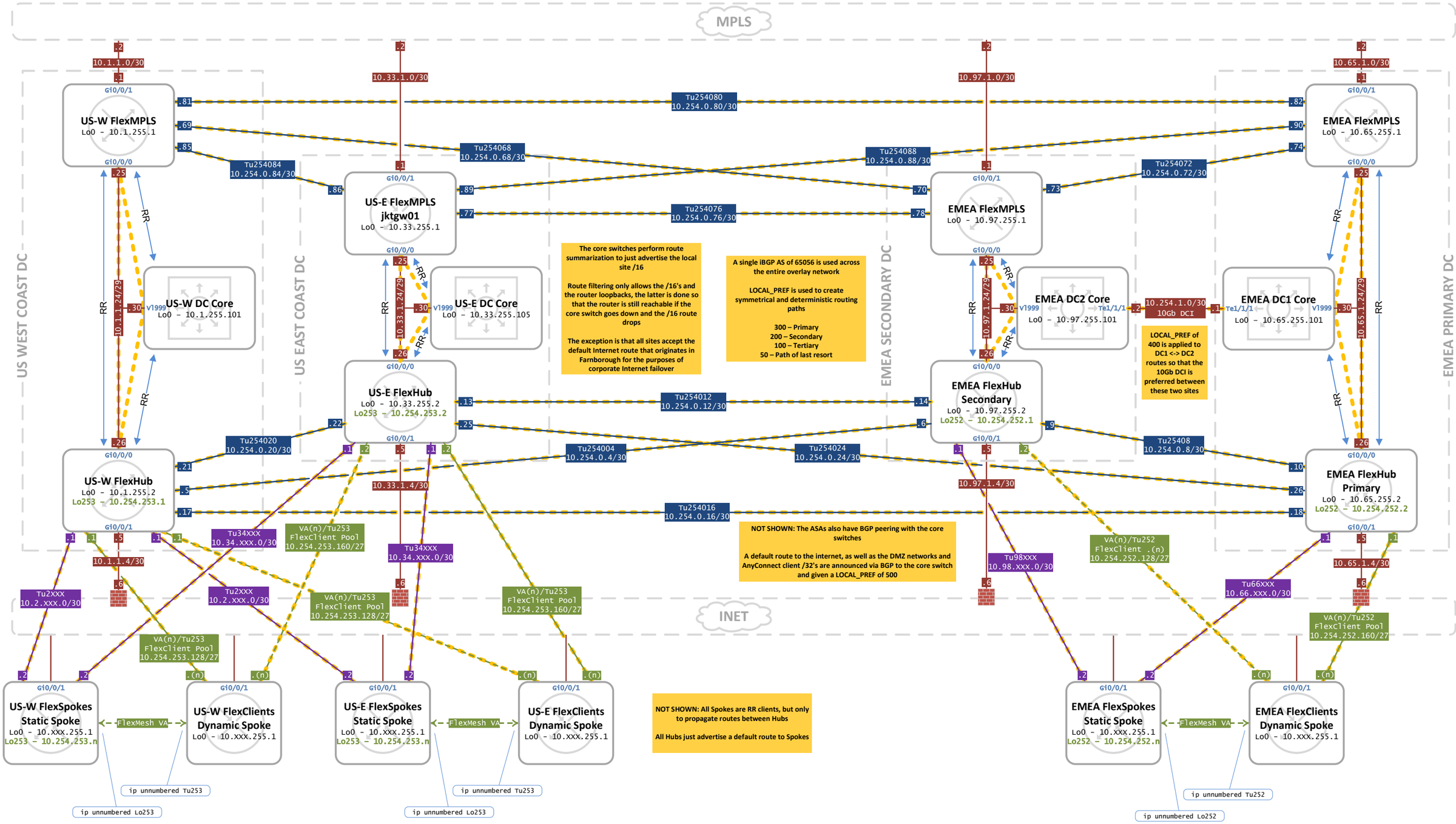
FlexVPN Detailed Design – All Layers

- Physical/underlay network
- Inter-region/country backhaul tunnels
- Static hub-to-spoke tunnels
- Dynamic spoke-to-spoke tunnels
- Dynamic hub-to-spoke primary tunnel
- Dynamic hub-to-spoke secondary tunnel
- iBGP peering
- RR — Route reflector (mutual reflection)
- Public Internet IVRF
- Public Internet GRE tunnel

THIS DIAGRAM USES LAYERS

- Intra-site Transit – Shows the layer 3 network local to each hub site
- Underlay – The underlying MPLS and Internet transport network
- FlexSpoke – The FlexVPN overlay network - static spoke to hub tunnels
- FlexClient – The FlexVPN overlay network - dynamic spoke to hub tunnels
- FlexMesh – The FlexVPN overlay network - dynamic spoke to spoke tunnels
- MPLS Backhaul Tunnels – The FlexVPN overlay network over MPLS transport
- INET Backhaul Tunnels – The FlexVPN overlay network over Internet transport
- BGP – Show BGP peering sessions and route-reflector relationships (excluding spokes, see note)

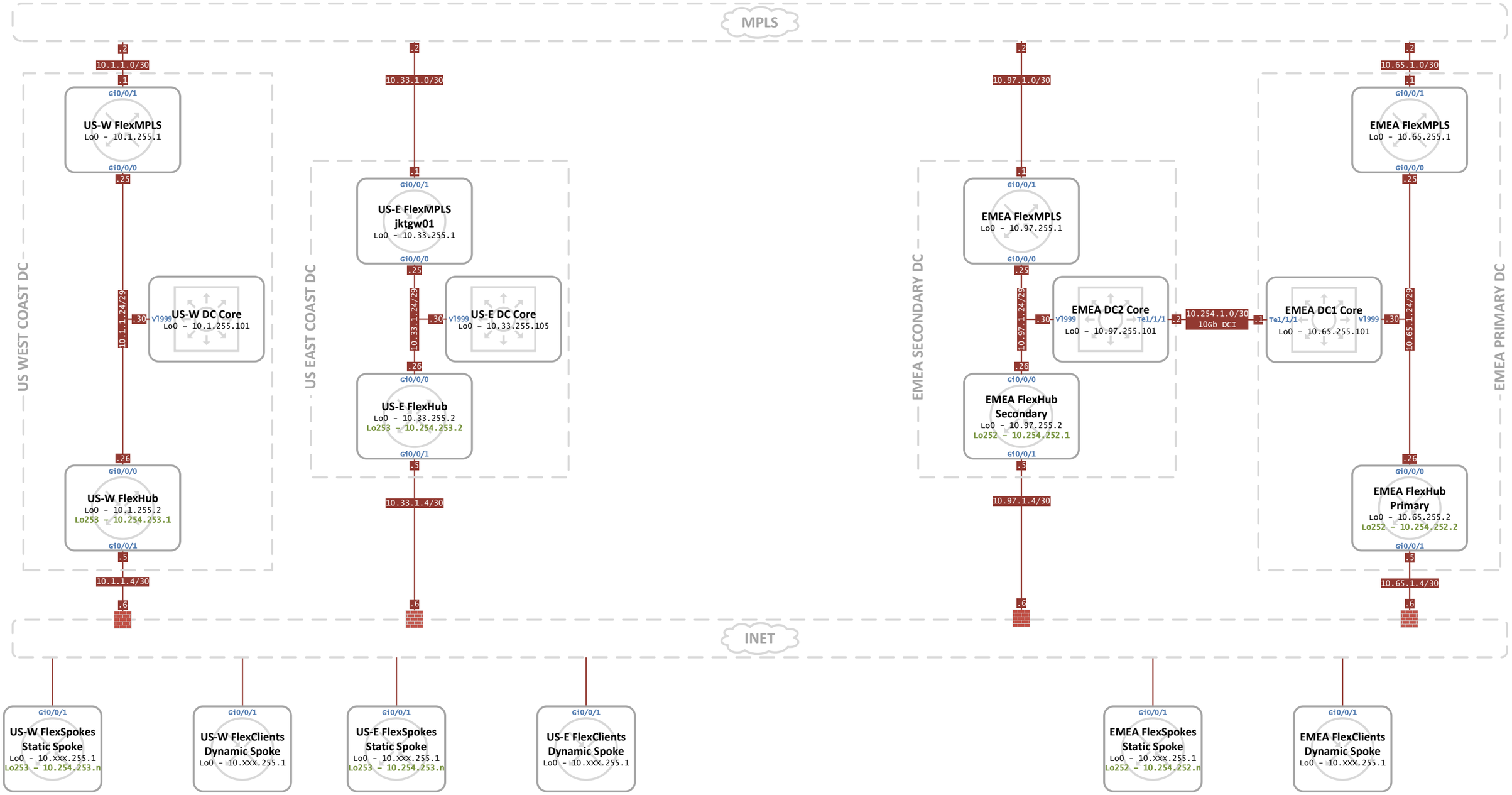


FlexVPN Detailed Design – Underlay

- Physical/underlay network
- Inter-region/country backhaul tunnels
- Static hub-to-spoke tunnels
- Dynamic spoke-to-spoke tunnels
- Dynamic hub-to-spoke primary tunnel
- Dynamic hub-to-spoke secondary tunnel
- iBGP peering
- RR — Route reflector (mutual reflection)
- Public Internet IVRF
- Public Internet GRE tunnel

THIS DIAGRAM USES LAYERS

- Intra-site Transit – Shows the layer 3 network local to each hub site
- Underlay – The underlying MPLS and Internet transport network
- FlexSpoke – The FlexVPN overlay network - static spoke to hub tunnels
- FlexClient – The FlexVPN overlay network - dynamic spoke to hub tunnels
- FlexMesh – The FlexVPN overlay network - dynamic spoke to spoke tunnels
- MPLS Backhaul Tunnels – The FlexVPN overlay network over MPLS transport
- INET Backhaul Tunnels – The FlexVPN overlay network over Internet transport
- BGP – Show BGP peering sessions and route-reflector relationships (excluding spokes, see note)

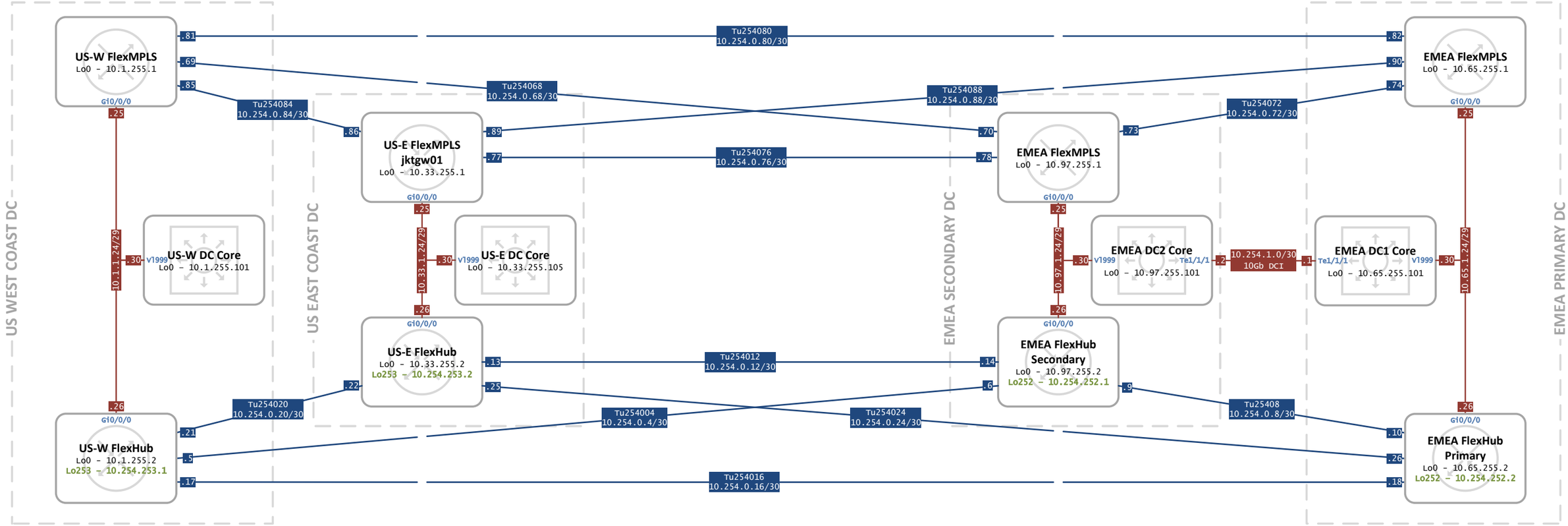


FlexVPN Detailed Design – Backhaul

- Physical/underlay network
- Inter-region/country backhaul tunnels
- Static hub-to-spoke tunnels
- Dynamic spoke-to-spoke tunnels
- Dynamic hub-to-spoke primary tunnel
- Dynamic hub-to-spoke secondary tunnel
- iBGP peering
- Route reflector (mutual reflection) (RR)
- Public Internet IVRF
- Public Internet GRE tunnel

THIS DIAGRAM USES LAYERS

- Intra-site Transit – Shows the layer 3 network local to each hub site
- Underlay – The underlying MPLS and Internet transport network
- FlexSpoke – The FlexVPN overlay network - static spoke to hub tunnels
- FlexClient – The FlexVPN overlay network - dynamic spoke to hub tunnels
- FlexMesh – The FlexVPN overlay network - dynamic spoke to spoke tunnels
- MPLS Backhaul Tunnels – The FlexVPN overlay network over MPLS transport
- INET Backhaul Tunnels – The FlexVPN overlay network over Internet transport
- BGP – Show BGP peering sessions and route-reflector relationships (excluding spokes, see note)



US-W FlexSpokes
Static Spoke
Lo0 – 10.xxx.255.1
Lo253 – 10.254.253.n

US-W FlexClients
Dynamic Spoke
Lo0 – 10.xxx.255.1

US-E FlexSpokes
Static Spoke
Lo0 – 10.xxx.255.1
Lo253 – 10.254.253.n

US-E FlexClients
Dynamic Spoke
Lo0 – 10.xxx.255.1

EMEA FlexSpokes
Static Spoke
Lo0 – 10.xxx.255.1
Lo252 – 10.254.252.n

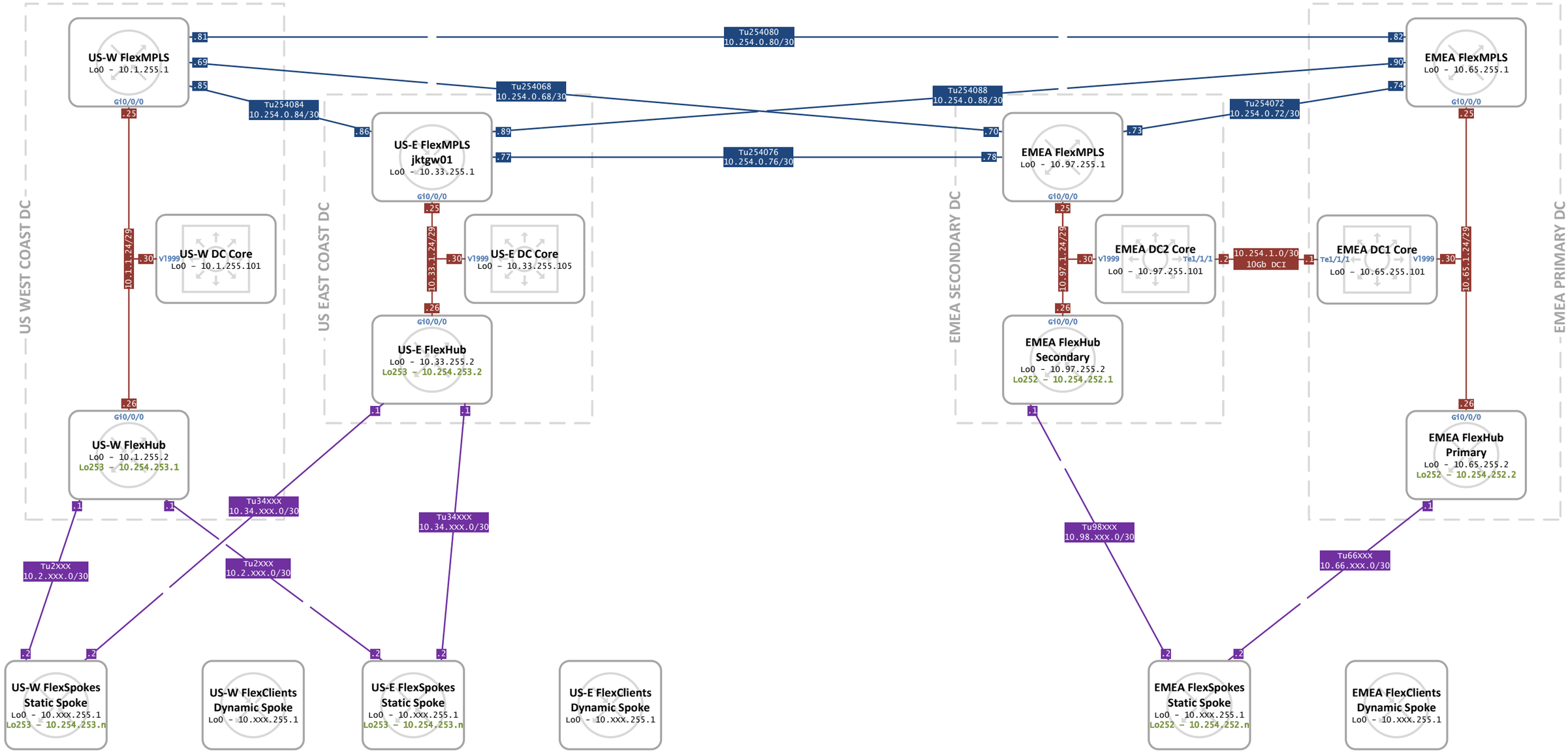
EMEA FlexClients
Dynamic Spoke
Lo0 – 10.xxx.255.1

FlexVPN Detailed Design – FlexSpoke

- Physical/underlay network
- Inter-region/country backhaul tunnels
- Static hub-to-spoke tunnels
- Dynamic spoke-to-spoke tunnels
- Dynamic hub-to-spoke primary tunnel
- Dynamic hub-to-spoke secondary tunnel
- iBGP peering
- Route reflector (mutual reflection) (RR)
- Public Internet IVRF
- Public Internet GRE tunnel

THIS DIAGRAM USES LAYERS

- Intra-site Transit – Shows the layer 3 network local to each hub site
- Underlay – The underlying MPLS and Internet transport network
- FlexSpoke – The FlexVPN overlay network - static spoke to hub tunnels
- FlexClient – The FlexVPN overlay network - dynamic spoke to hub tunnels
- FlexMesh – The FlexVPN overlay network - dynamic spoke to spoke tunnels
- MPLS Backhaul Tunnels – The FlexVPN overlay network over MPLS transport
- INET Backhaul Tunnels – The FlexVPN overlay network over Internet transport
- BGP – Show BGP peering sessions and route-reflector relationships (excluding spokes, see note)

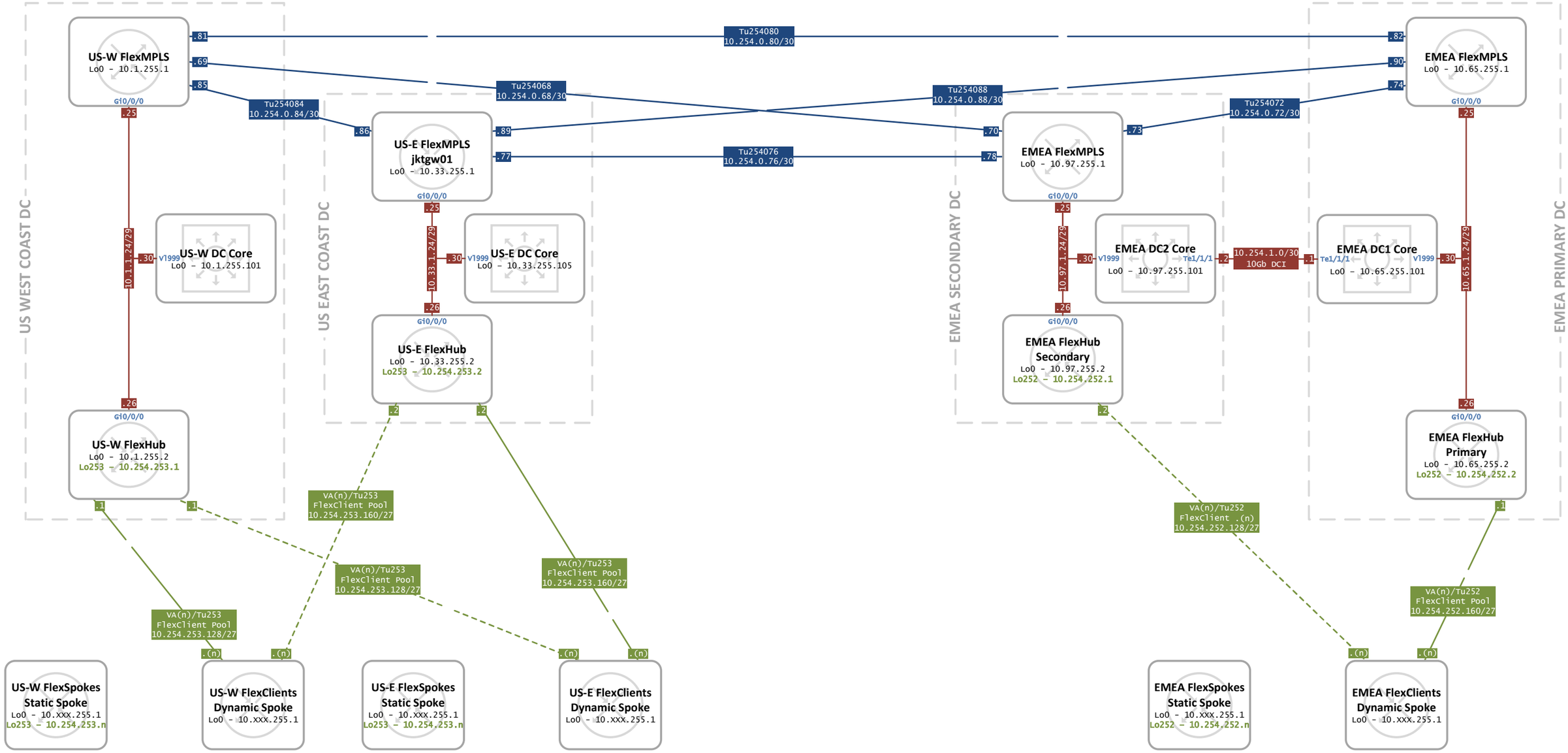


FlexVPN Detailed Design – FlexClient

- Physical/underlay network
- Inter-region/country backhaul tunnels
- Static hub-to-spoke tunnels
- Dynamic spoke-to-spoke tunnels
- Dynamic hub-to-spoke primary tunnel
- Dynamic hub-to-spoke secondary tunnel
- iBGP peering
- RR — Route reflector (mutual reflection)
- Public Internet IVRF
- Public Internet GRE tunnel

THIS DIAGRAM USES LAYERS

- Intra-site Transit – Shows the layer 3 network local to each hub site
- Underlay – The underlying MPLS and Internet transport network
- FlexSpoke – The FlexVPN overlay network - static spoke to hub tunnels
- FlexClient – The FlexVPN overlay network - dynamic spoke to hub tunnels
- FlexMesh – The FlexVPN overlay network - dynamic spoke to spoke tunnels
- MPLS Backhaul Tunnels – The FlexVPN overlay network over MPLS transport
- INET Backhaul Tunnels – The FlexVPN overlay network over Internet transport
- BGP – Show BGP peering sessions and route-reflector relationships (excluding spokes, see note)

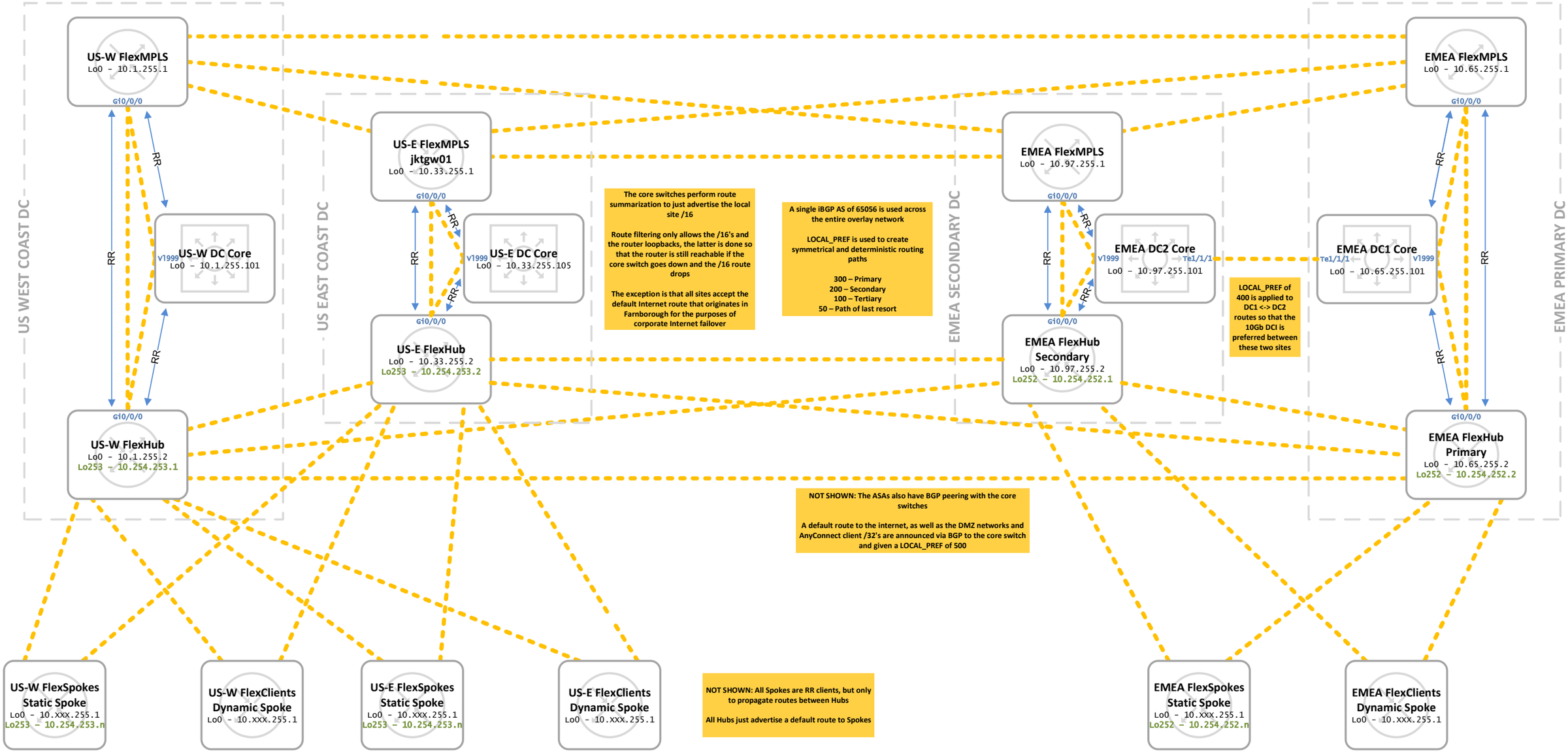


FlexVPN Detailed Design – BGP

- Physical/underlay network
- Inter-region/country backhaul tunnels
- Static hub-to-spoke tunnels
- Dynamic spoke-to-spoke tunnels
- Dynamic hub-to-spoke primary tunnel
- Dynamic hub-to-spoke secondary tunnel
- iBGP peering
- RR — Route reflector (mutual reflection)
- Public Internet IVRF
- Public Internet GRE tunnel

THIS DIAGRAM USES LAYERS

- Intra-site Transit – Shows the layer 3 network local to each hub site
- Underlay – The underlying MPLS and Internet transport network
- FlexSpoke – The FlexVPN overlay network - static spoke to hub tunnels
- FlexClient – The FlexVPN overlay network - dynamic spoke to hub tunnels
- FlexMesh – The FlexVPN overlay network - dynamic spoke to spoke tunnels
- MPLS Backhaul Tunnels – The FlexVPN overlay network over MPLS transport
- INET Backhaul Tunnels – The FlexVPN overlay network over Internet transport
- BGP – Show BGP peering sessions and route-reflector relationships (excluding spokes, see note)



Public Internet – Static Spoke – Backhauled

Physical/underlay network
Inter-region/country backhaul tunnels
Static hub-to-spoke tunnels
Dynamic spoke-to-spoke tunnels
Dynamic hub-to-spoke primary tunnel
Dynamic hub-to-spoke secondary tunnel
iBGP peering
RR Route reflector (mutual reflection)
Public Internet IVRF vrf#PUBLIC-INET#
Public Internet GRE tunnel

Loopback23 is the source interface for Tu25323 on the hub side and has the same IP address on both hubs. It is essentially an Anycast address, but it is not announced to any BGP peers.

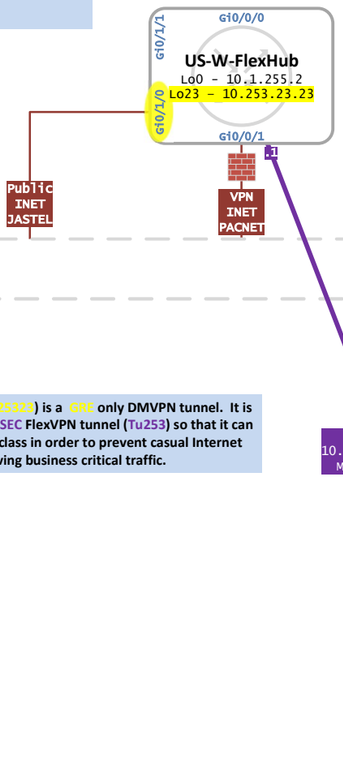
Reachability to Lo23 is achieved via the default routes advertised to the spokes over the FlexVPN tunnels. LOCAL_PREF dictates the preferred default route and thereby which hub the spoke will attempt to establish a tunnel with.

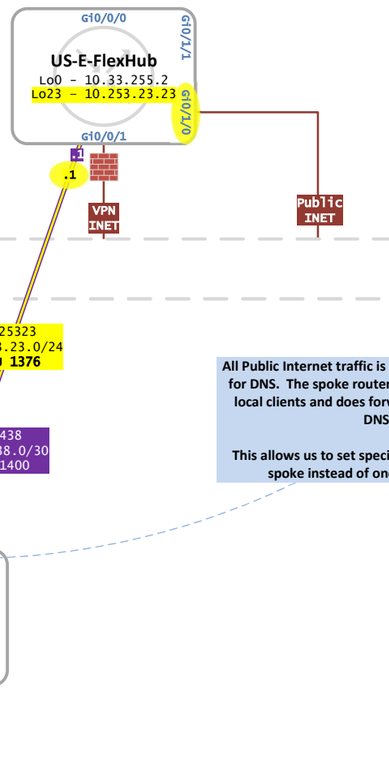
This also results in an inherent failover mechanism becuase if the preferred default route is removed the spoke will simply re-establish the Public Internet tunnel on the secondary hub.

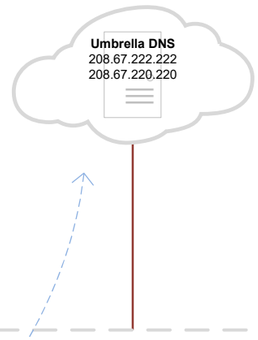
EIGRP running in vrf#PUBLIC-INET# on both the hubs and spokes is used to:
- Send the Public Internet default route from hub to spoke
- Send 10.x.23.0/24 from spoke to hub

ZBFW Is used on the hubs to control access

Tu25353, which is a mGRE tunnel on the hub side, has the same IP address on both hubs







The Public Internet tunnel (Tu25323) is a GRE only DMVPN tunnel. It is transported within the GREoIPSEC FlexVPN tunnel (Tu253) so that it can be put in the scavenger QoS class in order to prevent casual Internet traffic from starving business critical traffic.

All Public Internet traffic is backhauled to the hubs EXCEPT for DNS. The spoke router acts as the DNS server for the local clients and does forward lookups to the Umbrella DNS servers.

This allows us to set specific Public Internet policies per spoke instead of one blanket policy per hub

FlexHub Egress QoS

VOICE class is a strict priority queue

```
policy-map qos-pm-queue#WAN#OUT#8c#
 class qos-cm-classify#VOICE#DSCP#
  priority level 1
  police-cir percent 7
```

VIDEO class is a DSCP based WRED bandwidth queue

AF41 is Telepresence Video
AF42 is Jabber (CUCILync) Video

```
class-map match-any qos-cm-classify#VIDEO#DSCP#
 match dscp af41
 match dscp af42

policy-map qos-pm-queue#WAN#OUT#8c#
 class qos-cm-classify#VIDEO#DSCP#
  bandwidth remaining percent 39
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
```

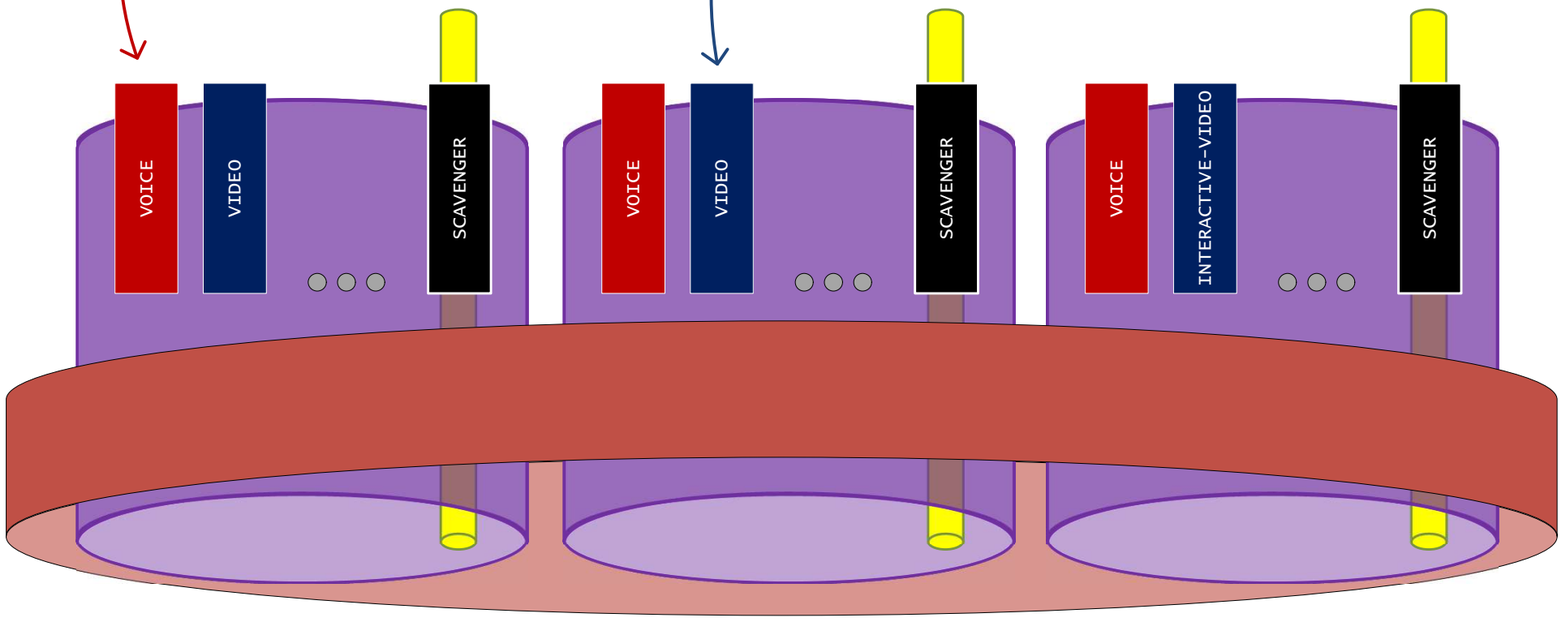
NOTE: The following command is only needed in WRED classes for **ISR 4K** platforms due to an inadvertent change in the default setting when Cisco transitioned ISRs from IOS to IOS XE

CSCve15383 is committed so the default will change automatically in an upcoming release

Public Internet tunnel interface does not have a shaper or policy of any kind

Ingress traffic on the Public Internet interface gets marked CS1

CS1 traffic goes into SCAVENGER class on the tunnel egress




```
class qos-cm-classify#SCAVENGER#DSCP#
 match dscp cs1

policy-map qos-pm-queue#WAN#OUT#8c#
 class qos-cm-classify#SCAVENGER#DSCP#
  bandwidth remaining percent 1
```

Tunnel interfaces shape to contract rate of destination spokes

References a CBFWFQ child service policy

'bandwidth remaining ratio' is used to divide bandwidth inherited from physical interface shaper

```
policy-map qos-pm-shape#WAN#OUT#10m#HUB#TUN#
 class class-default
  shape average 10m
  bandwidth remaining ratio 33
   service-policy qos-pm-queue#WAN#OUT#8c#
```

Physical interface shapes to contract rate of hub

Default class only, doesn't reference a service policy

```
policy-map qos-pm-shape#WAN#OUT#20m#HUB#PHY#
 class class-default
  shape average 20m
```