

RailMail Telecom

Background Documentation

RMT Information

RailMail Telecom is a US Telecom company that was initially owned by Mr. Morgan 1970, Mr. Morgan sold the company 10 years later when it had 7500 paid subscribers, to National Railway Transportation (NRT) company. NRT company did not have any backbone network at the moment, and it took the another 10 years to build their own backbone network starting from West Coast in Salem, WA and all the way to Atlanta on the East Coast. Initially they had been using SONET technology but eventually they migrated to Ethernet based circuits. Currently their backbone has 100G links all over their backbone.

RMT will keep using their name , not NRT since they have an existing customer base.

RMT is still expanding heavily and their customer growth forecast is 30% year-to-year basis for the next 5-6 years. All the forecasts had been successful for far.

As RMT built their network from scratch, they planned their network very well, so they are using next IP addressing:

For Internal purposes they are using 10.0.0.0/8 block:

- /16 per Data Center
- /16 per State
- /31 for point to point links

For Public routing they are using 151.27.0.0/16 block:

- /22 per State
- /22 per Data Center
- /31 for point to point links

RMT network is QoS enabled but they did not have any need implementing it as all the backbone links are overprovisioned the way that if there's a link failure it will there's always enough available bandwidth and utilization does not go above 90%. There's still some place to grow, but if they are going to have more clients, it might not be the case anymore.

Their IGP is flat ISIS L1 network. They are running BGP as external protocol and they are also using BGP as CE-PE protocol due to the corporate network security policy.

Services provides to clients:

- Internet Access
- L3VPN
- L2VPN VPLS
- L2VPN VPWS
-

RMT using SAP, a TCP based application, as their CRM. It is very slow and very sensitive to any kind of delay and drops. There's also a billing system that primarily using IPFIX to communicate with networking HW and their Corporate File Exchange protocol is NFS.

RMT is internally using Voice over IP and the video conferencing and they are utilizing FTP heavily for their HR applications specifically. They are using an entertaining application but they don't want these applications to consume more bandwidth.

SMT Information

SnailMail telecom lived primarily by acquisitions. They have started in San Francisco 15 years ago and prior to this moment they acquired 3 small Service providers in the different parts of US. There was some IP addressing overlap between the POPs in Raleigh and Austin but they have been able to fix it.

All SPs are connected by full mesh GRE tunnels over the internet.

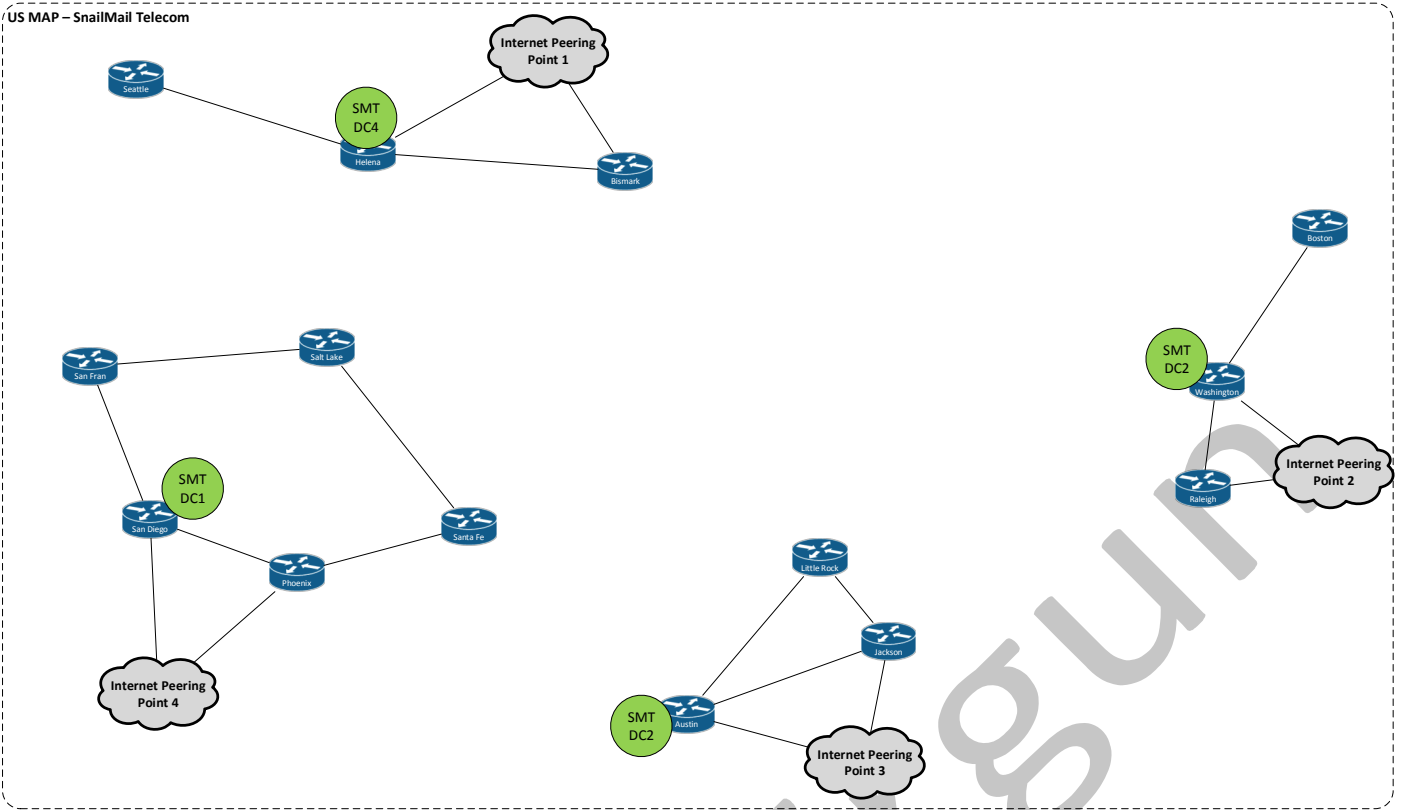
SMT uplink bandwidth to Internet Peering Points is 10G and they are using BGP as their EGP.

So far SMT was providing only Internet services to their customers.

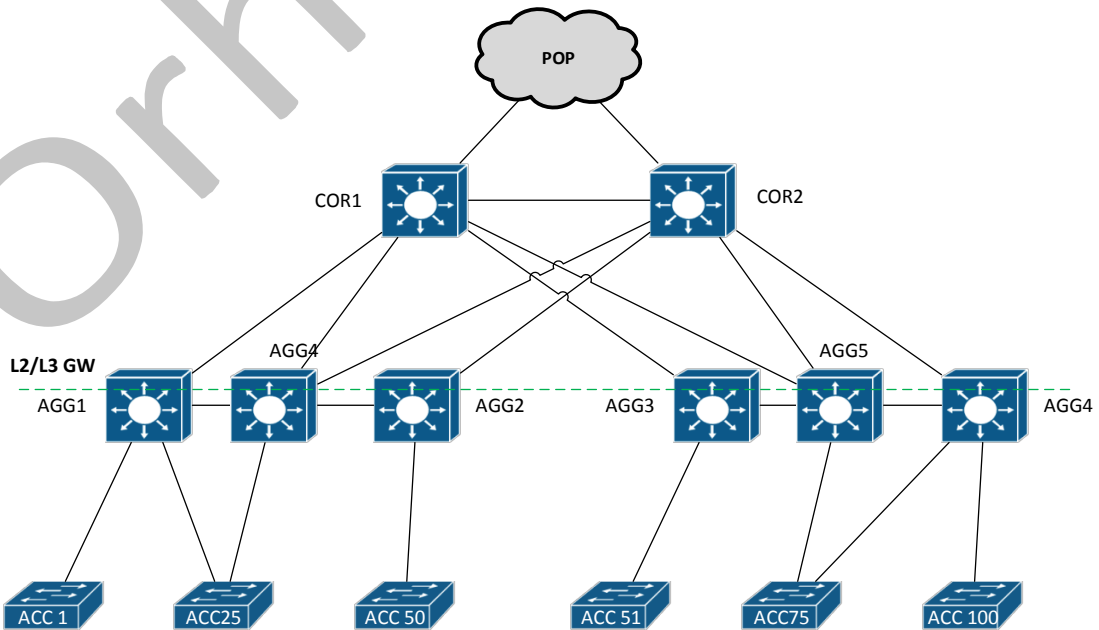
Design Documents

SnailMail Telecom diagrams

US MAP - SnailMail Telecom

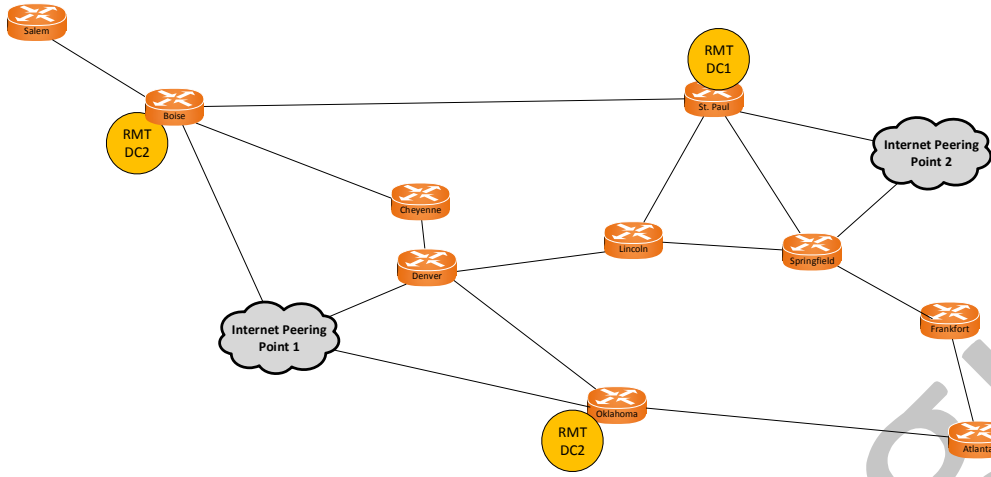


SMT DCs Design



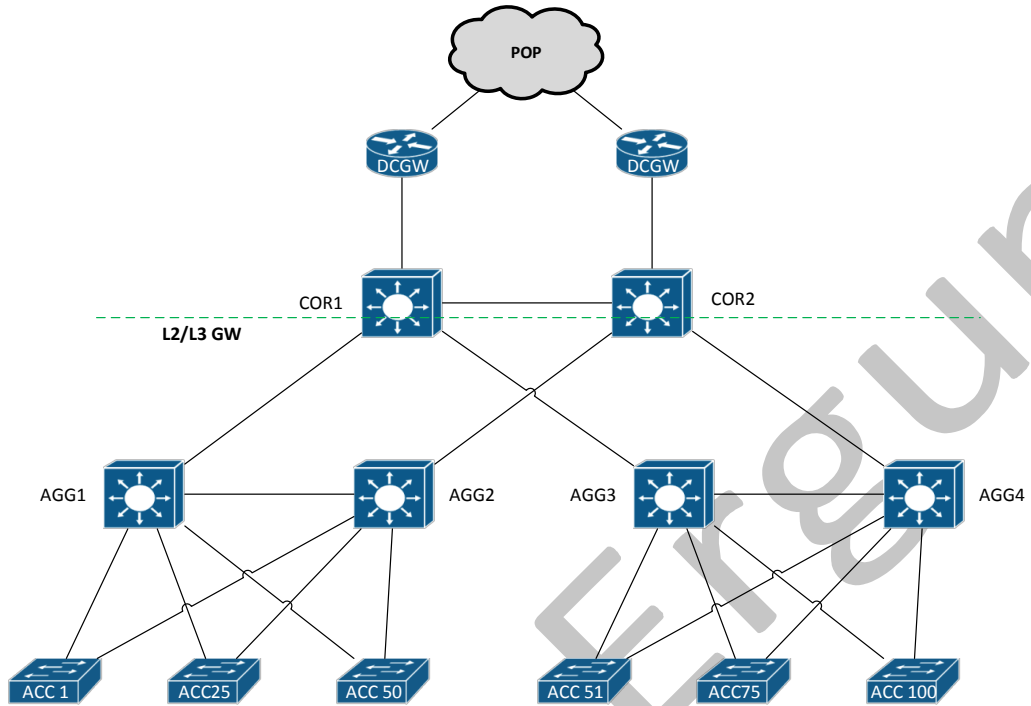
RailMail Telecom diagrams

US MAP - RailMail Telecom



Orhan Ergun

RMT DCs Design



Email 1 is Available

As we have mentioned previously, SMT made 3 more acquisitions few years ago. Unfortunately, they could not keep their promises to main investors so they have just sold company to RMT. Now we have to deal with it. First thing to do is identify which kind of information we are still missing before we proceed with merging both RMT and SMT.

Our main concern and top priority is that merged network should be able to provide all of our current MPLS VPN services.

1. What information you need from RMT to start merging design?

- A- IP addressing
- B- IGP routing
- C- BGP architecture
- D- POP Architecture
- E- Backbone speed
- F- QoS information
- G- MPLS VPN support

Answer 1 : IP address information is already provided so you shouldn't ask it again. In the CCDE exam if information is provided already, you can't ask it again. This is an analyzing the design type question.

IGP routing is given as IS-IS Flat Level 1 design, so you don't need to ask it again as well.

You don't know whether RMT is using single AS or multiple AS such as confederation, we need more information on this, that's why BGP architecture should be learned.

POP architecture should be provided as well , so if we need to remove some POP and so on we can do it.

Backbone speed of RMT is already provided. QoS information is provided as well and also you wouldn't need it in order to start merging design.

It is already given that RMT is providing MPLS VPN to their customers.

That's why you should learn BGP Architecture and POP architecture , answer is C and D.

2. What info you need from SMT to start merging design?

- A- IP addressing
- B- IGP routing
- C- BGP architecture
- D- POP Architecture
- E- QoS information
- F- Backbone speed

G- MPLS VPN support

Answer 2 : IP Addressing is not provided, in order to understand whether there is conflict for the merged network, we need to learn IP addressing of SMT.

IGP routing should be learned as well. Which routing protocol they use, is there any special IGP configuration ?

BGP architecture should be learned as well. We don't know how their Internal and External BGP is setup.

POP architecture should be learned as well. How their POP location is connected to the DCs and the core network.

QoS information can be asked if needed later on, it is not needed to start merging design.

Backbone speed should be known, they haven't provided this information in the initial background information.

Since RMT provide VPN services and merged network should provide VPN as well, we need to know whether SMT support MPLS VPN services.

Orhan Ergun

Email 2 is Available

This is some of the information we have been able to get for you:

RMT BGP is using single AS in their network. Each Pop has a BGP RR for both BGP and VPN services.

RMT POP with Data Center architecture is given below

SMT IGP is Single area OSPF

SMT backbone network bandwidth is 2x10G links

SMT is using 10.10.0.0/16, 10.0.0.0/16, 172.16.0.0/18 and 172.22.0.0/16 IP addressing blocks

SMT does not use any MPLS VPN services at the moment but their equipment has all the support.

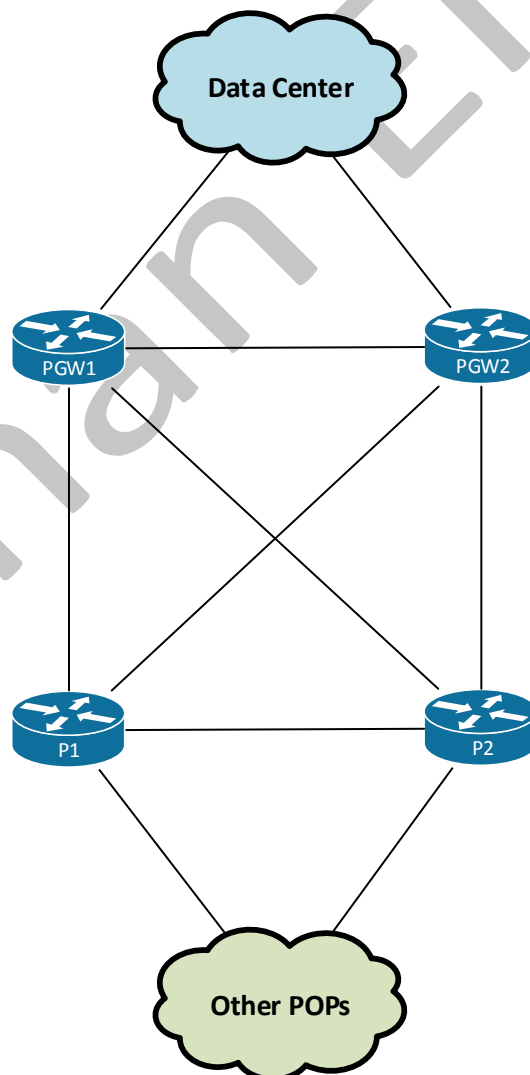
Also SMT has currently full mesh IBGP peering at the moment.

RMT also has 2x10G links from each POP connected to Internet Peering Points, not sure if you need this information though.

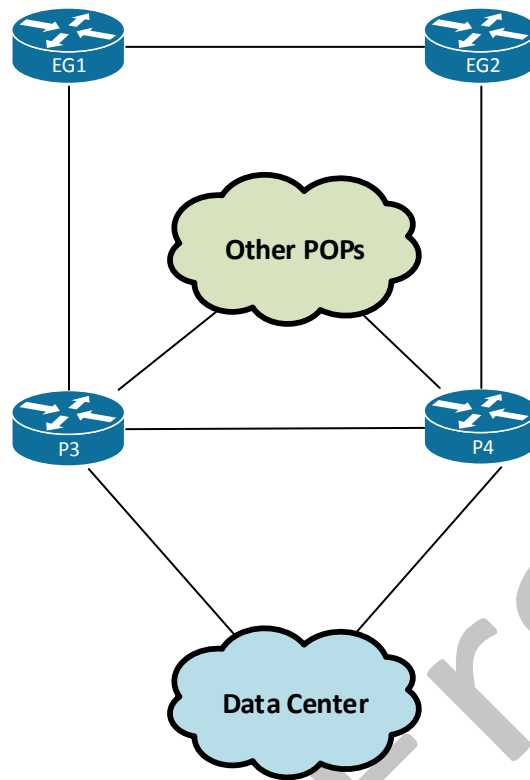
There are few other diagrams that might help you.

Diagrams

RMT POP with Data Center



SMT POP with Data Center



Orhan Ergun

Email 3 is Available

One of our new network architects was concerned about current IS-IS in RMT. He thinks that we might be facing some issues while merging RMT and SMT networks together.

3- Is there any problem with the current ISIS design?

- A- YES
- B- NO

Answer 3: There is no known problem with the current IS-IS design. Detailed answer will be provided in the subsequent answers.

4- What might be the concern of the RMT for their IS-IS ?

- A- Migration from IS-IS L1 to Multiple flooding domains is hard
- B- IS-IS L1 does not support traffic engineering
- C- Redistribution is not possible to ISIS L1
- D- ISIS L1 is not a scalable solution

Answer 4 : Flat IS-IS L1 is not the different from the scalability point of view from the IS-IS L2, that's why Option D is not correct.

Redistribution is possible into IS-IS L1 domains, this is not correct either.

IS-IS L1 provides Traffic Engineering and so far there is no requirement for MPLS Traffic Engineering. It is not the future which every network should have also. Thus Option B is not correct answer either.

Option A is definitely correct, in general it is hard to migrate from flat IS-IS L1 design to multiple flooding domains such as L1 in the POP , L2 in the Core. Answer of this question is Option A.

But this is not a realistic concern in the current situation since we don't know whether merged network will have problem with the scalability. If scalability and manageability is okay for the customer, IGP can be migrated to either different one or to the multiple level one.

5- Should they migrate the IGP protocols to run a common IGP for the merged network ?

- A- Yes
- B- No

Answer 5 : There is no need currently. RMT's main concern and top priority is to extend their MPLS VPN services as it is given in the initial background information. Providing an Inter-AS MPLS VPN services don't

require to use common IGP, although using common IGP would provide additional benefits; especially in the MPLS network. But this can be decided after the first phase of merge, right now there is no need.

6- What would be the problem if SMT wants to deploy BGP Route Reflector based on their current BGP design ? (Choose all that apply)

- A- They would lose path visibility
- B- There is no problem, it is same as running full mesh
- C- BGP RR always bring benefits to BGP design
- D- BGP RR puts additional load into the control plane
- E- BGP RR can cause suboptimal routing

Answer 6 : Classical problem of BGP Route Reflector is path visibility. If you have more than one exit point from the domain for the same prefix, BGP RR selects the best path from its point of view and sends all the BGP RR clients. That's why Option A is one of the correct answers. Less number of total path means might cause sub optimal routing from some BGP RR clients. Thus Option E is the other correct answer.

7- Which below methods can be used eliminate the possible path visibility problem of BGP Route Reflector?

- A- Using BGP Add-Path
- B- BGP Shadow Sessions
- C- Not using BGP Route Reflector
- D- Using full-mesh and BGP Route Reflector in the same network
- E- BGP Shadow Route Reflectors
- F- BGP Best External
- G- BGP PIC-Prefix Independent Convergence

Answer 7 : In general except BGP PIC, all the option is used to send more than one BGP path to the BGP speaker. In order BGP PIC to function properly, one of the above option is used. Additional information : In the MPLS VPN network, using unique RD per PE provides same functionality. That's why to send more than one path for a given customer prefix, unique RD per PE is the best option in MPLS VPN network.

New Question :What would be the migration step for SMT from full-mesh IBGP to BGP route Reflector design ?

Email 4 is Available

One of our customers asked us about the best way to provide connectivity between their HQs and the remote sites. Could you help us out?

8- Please fill in the table below

	Multicast support over Internet	Multicast replication at Hub/WAN	Topology P2P/P2MP /MP2MP	Overlay/Underlay Routing	Redundancy	Runs over Internet/WAN/ANY
DMVPN						
GETVPN						
mGRE						
P2P IPSec						
GRE						

	Multicast support over Internet	Multicast replication at Hub/WAN	Topology P2P/P2MP /MP2MP	Overlay/Underlay Routing	Redundancy	Runs over Internet/WAN/ANY
DMVPN	Yes	Yes	MP2MP	Underlay all, Overlay all except is-is	Yes	Any
GETVPN	No	No	MP2MP	Underlay all, overlay is none, since there is no tunnel	Yes	WAN
mGRE	Yes	Yes	MP2MP	Underlay all, Overlay all	Yes	Any
P2P IPSec	Yes	Multicast is not Supported	P2P	Underlay all, overlay only unicast	Yes	Any
GRE	Yes	Yes	P2P	Underlay all, Overlay all	Yes	Any

9-What is the best solution for VPN security with minimal OpEx ?

- A- GETVPN
- B- DMVPN
- C- mGRE
- D- P2P IPSec

Answer 9: GETVPN provides minimum OPEX. More information is available in the online classes.

Email 5 is Available

Top management and company owners have been pushing to come up with new backbone design as soon as possible. They wanted new backbone network to be simple and flexible, efficient and be able to handle any single point of failure at POPs connecting to Data Centers.

After merging both RMT and SMT we have started experiencing bandwidth utilization problems. Between different region the traffic flow always follow the shortest IGP path. Please can you help us to start sending traffic over all the available paths ?

10- Which would be the best short-term solution in this case?

- A- Use MPLS Traffic Engineering- Tactical Approach and distribute the traffic between the regions based on bandwidth constraint
- B- Use static routes and GRE tunnels and optimize traffic flow
- C- Implement DiffServ QoS all over the backbone network
- D- Implement DiffServ QoS at places of traffic congestion
- E- Redesign Backbone network and add few more inter-POP links
- F- Use MPLS Traffic Engineering Strategic Approach

Answer 10 : Using tactical MPLS traffic engineering.

11-What about permanent solution? (Pick all that Apply)

- A- Use MPLS Traffic Engineering Strategic Approach
- B- Use static routes and GRE tunnels and optimize traffic flow
- C- Implement DiffServ QoS all over the backbone network
- D- Implement DiffServ QoS at places of traffic congestion
- E- Redesign Backbone network and add few more inter-POP links
- F- Use MPLS Traffic Engineering- Tactical Approach and distribute the traffic between the regions based on bandwidth constraint

Answer 11: Using Strategic MPLS Traffic engineering.

Email 6 is Available

It seems that MPLS Traffic Engineering Strategic Approach can provide us a better capacity management. Can you help us to setup an MPLS Traffic Engineering on our network. Also we will have series of questions for you regarding MPLS Traffic Engineering.

We have been also told to provide QoS all across the new network within the next couple of months.

12- Which features need to be enabled in order for MPLS TE to function properly? (pick all the apply)

- A- LDP
- B- RSVP
- C- MP-BGP
- D- Unidirectional tunnel headend
- E- Unidirectional tunnel tailend
- F- Bidirectional tunnel headend and tailend
- G- IGP
- H- IGP TE (TED)
- I- VRF
- J- Send-Label

Answer 12 : Option A , E, F, G, H

Email 7 is Available

We created an MPLS tunnels, RSVP and other necessary extensions are in place but unfortunately our traffic doesn't go through the TE tunnels.

Once you help to get the traffic into the MPLS TE tunnels one little thing will left.

We still need to enable DiffServ QoS throughout our new network. One of our engineers told us that it is not possible to run both IntServ and DiffServ QoS.

13- Why do you think RMT cannot send traffic into the MPLS TE tunnels although everything is set ?

- A- Multicast traffic can pass but unicast traffic might have an issue
- B- Routing table should point to the tunnel interface for the TE destination prefixes

- C- TE tunnel links must be advertised into the IGP protocol
- D- RMT probably didn't create reverse unidirectional tunnel

Answer 13: If Multicast is setup in the network and unicast traffic would pass over the TE tunnels, Multicast could follow it. But RMT doesn't say that they have a problem with Multicast, actually they didn't say anything about Multicast yet.

TE tunnels don't need to be advertised as a link into the routing protocol in order to IGP take MPLS TE link in the SPF calculation. This is done through forwarding adjacency and could be one of the solutions for the problem of putting traffic into the MPLS TE tunnel but since the Option C says that 'TE tunnel links must be advertised into the IGP protocol' this statement is wrong. There are many methods for placing traffic into the MPLS TE tunnels, such as ,

RMT even doesn't create reverse uni-directional tunnel, traffic would follow the MPLS TE tunnel in one direction. Return traffic could follow the IGP shortest path. RMT cannot place the traffic into the TE tunnel at all, nothing is said about one direction.

That's why the answer is Option B. Routing table should show that the destination behind the MPLS TE tail-end should be seen from the tunnel interface. This can be done via above mentioned methods. (Static route, PBR, CBTS, Auto Route, Forwarding Adjacency) Thus, Option B is the correct answer.

14-Is it possible and recommend to run IntServ and DiffServ QoS in the same network?

- A- Yes, it's possible but its not a good idea to run both IntServ and DiffServ in the same network
- B- No, there's no specific restrictions and they can both run in the same network

Answer 14 : Answer is Option A.

15-We are considering several QoS models. Which one is the best fit for us?

- A- 1 PQ, 3 BQ
- B- 1 PQ, 4 BQ
- C- 3BQ
- D- 5BQ
- E- 3PQ, 1BQ

Answer 15 : Voice and Video conferencing should go to the PQ, SAP and HR applications go to the same queue, NFS and FTP are the bulk traffic, we can place them into the same queue, company is allowing gaming/entertaining application which should go to the scavenger and the rest of the traffic should go to the best effort.

That's why we need 1 PQ and 4 BQ.

Email 8 is Available

We have chosen unified 1 PQ and 4 BQ model. One of our large banking customers requested MPLS VPN with 8 Class QoS model. But as a policy, we provide 3 different QoS models. Among our offerings, they can get Gold QoS Service which can give 5 classes.

Here's brief information about QoS configuration on our gear for the Gold QoS Service :

- EXP0 – Best effort, FIFO, BW remainder (all non SLA traffic by default put into EXP0)
- EXP3 –CBWFQ, BW 30%
- EXP4 – WRED, BW 20%
- EXP5 –PQ, BW 30%
- EXP1- CBWFQ , BW %5

Here's brief information about QoS and applications configuration on our customer:

- CS1 – FTP for file sharing, UDP
- CS3 – Internal gaming platform, UDP,
- AF33 - Internet web browsing, TCP
- AF41 –Network storage replication, TCP
- AF42 – Corporate CRM, TCP
- EF – Videoconference, UDP, traffic loss sensitive
- CS6 - Financial department business application, real-time, delay sensitive
- DF- All remaining applications

16-Provide the right DSCP to EXP mapping for banking customer

	EXP0	EXP1	EXP3	EXP4	EXP5
CS1			X		
CS3		X			
AF33			X		
AF41				X	
AF42				X	
EF					X
CS6					x
DF	x				

Email 9 is Available

All our users have a problem accessing to cloud gaming application we have deployed recently and it looks like the somewhere in our network, but we are not sure where. We need your help to identify the problem!

17-Which part of the network should we focus on?

- A- Place the monitoring probes closer to application
- B- Place the monitoring probes closer to end users
- C- Place the probes closer to both end users and application
- D- Place the probes at all the POPs
- E- Place the probes everywhere in the network

Answer 17: Answer is closer to the application since all the users have a problem at the same time, so the problem should be with the application. All the traffic should come through that nodes which the probe is running. Correct answer is Option A.

18-Why should we put the probes there?

- A- Because RMT can monitor individual flows from every user
- B- Centralized place for monitoring which can ease of the operation
- C- Better data flow visibility

Answer 18: Answer is Option B.:

Email 10 is Available

Since we have done merging, we have lots of requests from the RMT customers to extend their current VPN networks to different locations where SMT have presence at. RMT wants to have separation of their core network task from the Inter domain task, that's why they implemented a new ASBR routers but SMT is okay with the existing routers for new inter domain communication.

19- Which option would you suggest to implement in order to extend your VPNs to SMT backbone?

- A- Inter-AS Option A
- B- Inter-AS Option B
- C- Inter-AS Option C
- D- Inter-AS Option D
- E- Inter-AS Option E

Answer 19 : Since there is overlapping IP addresses between RMT and SMT that's why we cannot leak the internal prefixes, so Option C cannot be chosen. Option A cannot be chosen either since it is stated in the email that lots of request is coming for the Inter-AS service.

Answer is Option B.

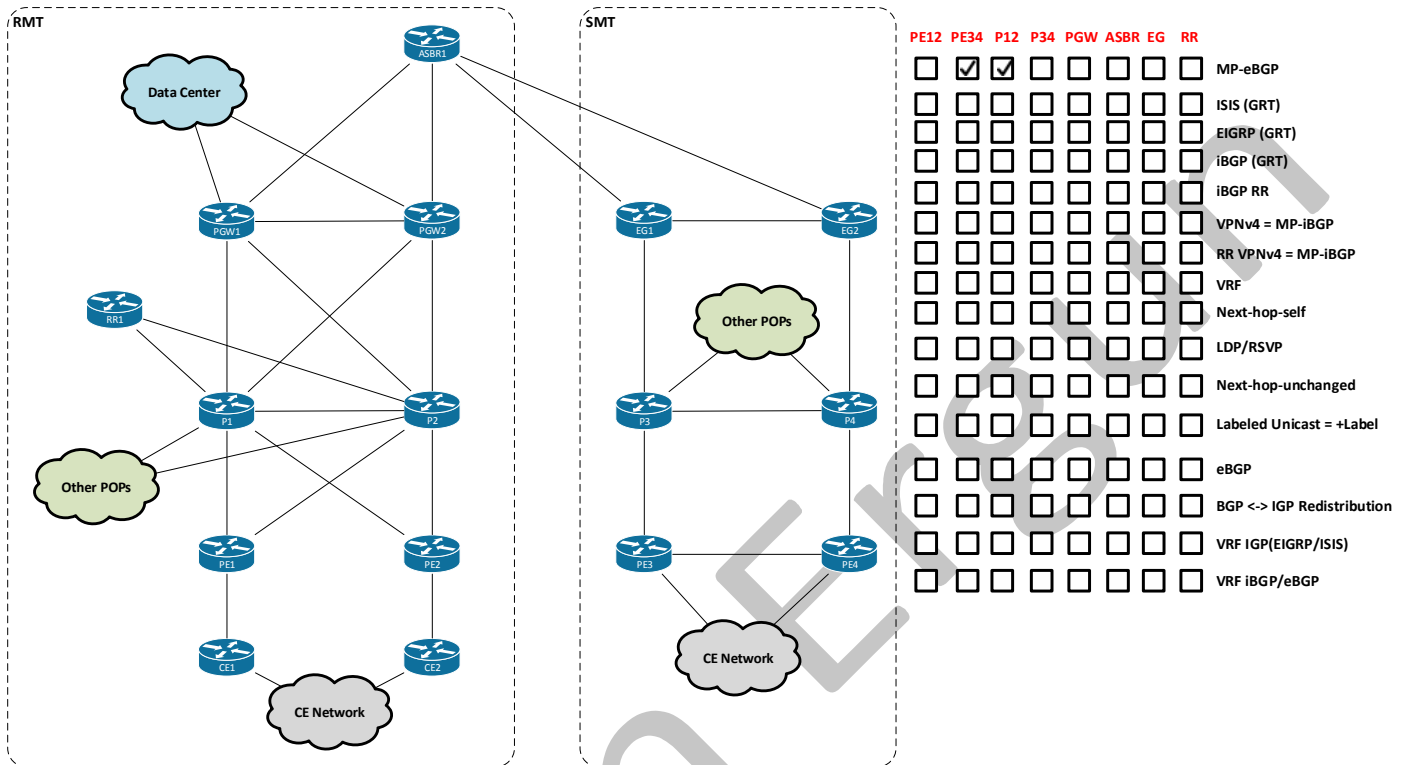
20- What is the main reason to implement it?

- A- It is the most secure option among the others
- B- It fits RMT scalability needs
- C- It is the most easiest option to configure
- D- It provides end-to-end LSP

Answer 20: It fits RMT scalability needs, also check the answer of the previous question.

Answer is B.

21- Please check the right boxes to implement it.



22- What is the right set of steps in order to perform that merging?

- A- Add link between EG1-ASBR
- B- Activate MP-BGP between ASBR1 and EG1
- C- LDP between PGW2-ASBR1
- D- Activate MP-BGP between ASBR1 and EG2
- E- IS-IS between PGW2-ASBR1
- F- Verify the connectivity
- G- LDP between PGW1-ASBR1
- H- Remove the leftovers if any
- I- IS-IS between PGW1-ASBR1
- J- Add link between EG2-ASBR

Answer 22:

Start first physical things. Then we are activating IGP, then LDP, after that MP-BGP and verification

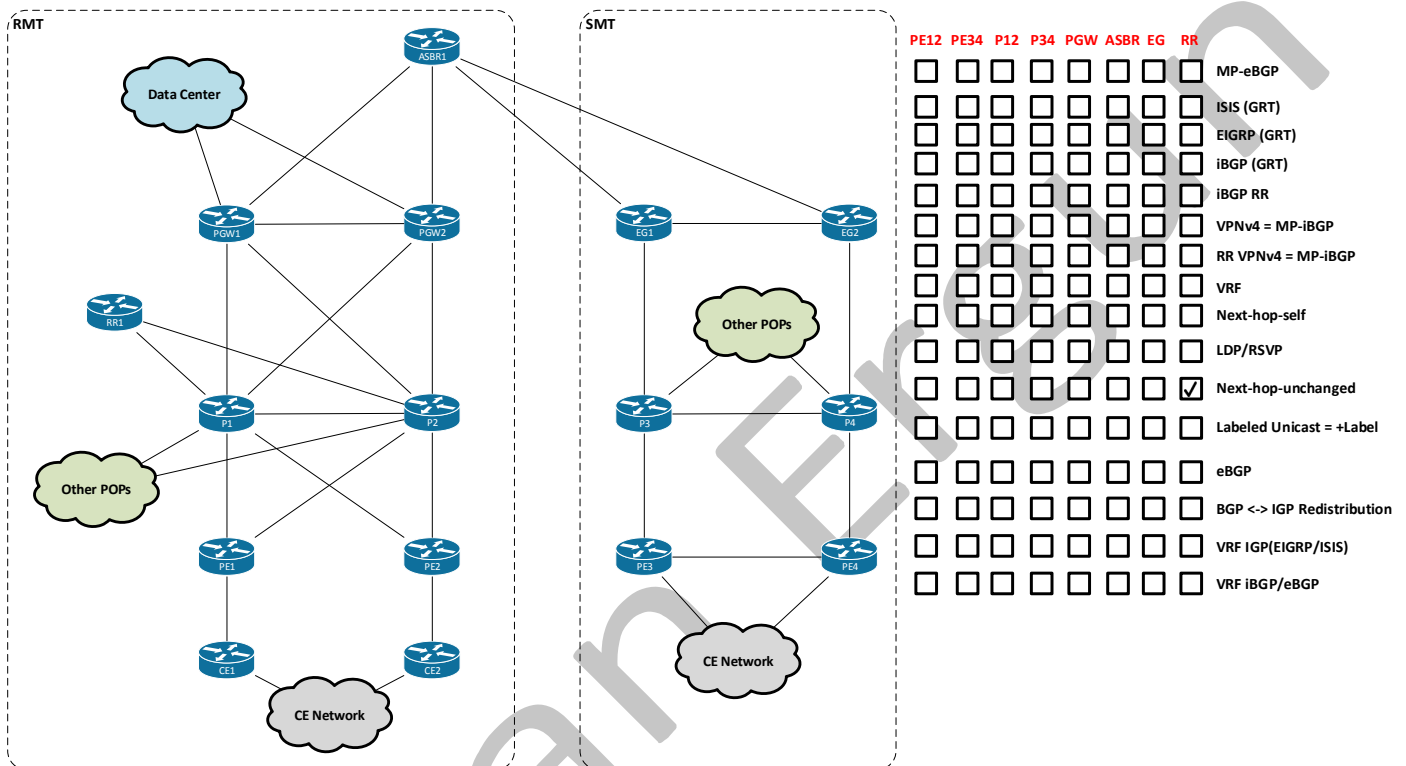
A- J- E – I – C-G- B-D-F-H

Orhan Ergun

Email 11 is Available

One of our lead architect came up with new IP addressing scheme that new network is going to migrate to within the next 6 months. It gives us opportunity to use Inter-AS Option C.

23-Please check the right boxes to implement Inter-AS Option C.



24- What are the main benefits of implementing Inter-AS Option-C between RMT and SMT?

- A- The only option with the support of 6vPE
- B- Better scalability compared to Inter-AS Option B
- C- Allows end to end QoS for VPN services
- D- The easiest Inter-AS Option to implement
- E- More secure compare to Inter AS Option B

Answer 24 : Correct answer is B.

Email 12 is Available

Hi Designer,

As you know we have MPLS Layer 3 VPN, Internet, Point to point MPLS VPN and VPLS customers. Especially for the VPLS customers, when we want to add a new site to the current VPLS of the customers, it is operationally very hard for us to touch every PE of the customer. We are afraid that this will be a bigger problem for the merged network since we want to span the VPLS and our other services throughout the merged network. But especially for the VPLS issue, we want to have an immediate solution.

Please note that we have an LDP-based VPLS in our network and the SMT network doesn't have VPLS at all currently.

Can you help us to fix our operational problem.

25- Which below option is defined the RMT's operational problem ?

- A- Their network engineers don't have a capability to manage merged network
- B- Their existing gear don't have a capability to keep the state of merged network
- C- They want to reduce the operational touch point for the existing services, especially VPLS
- D- They don't know whether VPLS service can be extended over the Inter-AS links

Answer 25 : Answer is Option C.

26- What would be your solution for their VPLS service ?

- A- Use H-VPLS
- B- Use A-VPLS
- C- Replace VPLS with EVPN
- D- Replace VPLS with PBB-EVPN
- E- Use BGP AD for their VPLS solution

Answer 26 : Answer is Option E.

27- If RMT would request to have the most granular QoS support for their Inter-AS VPLS service, which below option you would recommend ?

- A- inter-AS Option A
- B- VPLS cannot be extended over Inter-AS
- C- Inter-AS Option B
- D- Inter-AS Option C
- E- Inter-AS Option AB

Answer 27 : Answer is Option A.

28- Would you recommend RMT to deploy BGP-VPLS in the SMT locations ?

- A- Yes
- B- No

Answer 28 : Correct answer is Option A , Yes.

29- Is there any problem for LDP and BGP based VPLS to support end to end VPLS ?

- A- Yes
- B- No

Answer 29 : Correct answer is No. With adding interconnect nodes between the LDP-VPLS and BGP-VPLS domains, end to end VPLS service is created.

Email 13 is Available

One of our customers is asking whether we can provide IPv6 L3 VPN services for them. We have not been thinking about it, but as our assessment all our networking nodes support IPv6

30- Which technology will help RMT to meet the requirements above?

- A- 6PE
- B- DMVPN
- C- 6vPE
- D- NAT64
- E- NAT46

Answer 30 : Correct answer is 6VPE, Option C.

31- Which additional technology/protocol is needed as an underlay transport to support 6VPE service for RMT ?

- A- IPv6 LDP in the core
- B - IPV6 IGP in the core
- C- IPv6 RSVP-TE
- D- Both IPv6 IGP and LDP
- E- Pv4 transport is enough for 6VPE

Answer 31 : Correct answer is Option E.

32- In case if there would be no support for 6vPE, which below methods can be implemented at Customer side in order to overcome the problem? (Choose all that apply)

- A- 6PE
- B- DMVPN
- C- PAT
- D- NAT64
- E- NAT46

Answer 32 : Option B and D is the correct answers

33- If customer would choose to run DMVPN over MPLS VPN for both IPv4 and IPv6 traffic, how many DMVPN tunnels per site they would need ?

- A- One
- B- Two
- C- Three
- D- Four

Answer 33 : Answer is One, Option A.

34- How much of an effort it is to upgrade current network and provide L2 and L3 VPN for IPv6 services? (Choose all that apply)

- A- Little to no changes for L3VPN IPv6 support
- B- Little to no changes for L2VPN to support IPv6
- C- Major changes for L2VPN to support IPv6 support
- D- Major changes for L3VPN IPv6 support

Answer 34 : Option B and D is the correct ones.

Email 14 is Available

In the future, we are planning to expand to EMEA region. Our management has found one of the small local service provider in UK that they are going to acquire within the next several months. We are looking for a cost effective short-term solution for acquisition to extend MPLS VPN services between the two networks.

We also need a good design and migration plan for a long-term solution if this acquisition goes well. We don't have a budget issue for long haul links. As we are planning to provide different value added services for our customers, both short-term and long-term solutions must support end-to-end QoS and Multicast.

35- What is the fastest short-term solution to connect current RMT network and a new one in the UK?

- A- Use L2VPN from another MPLS Service Provider to connect current RMT network and a new one with MPLS and QoS over that L2VPN
- B- Use L3VPN from another MPLS Service Provider to connect current RMT network and a new one with MPLS and QoS over that L3VPN
- C- Build GRE tunnels over Internet and run MPLS and the necessary services on top of it
- D- Order dedicated circuits

Answer 35 : Answer is Option C.

36- What would be the problem with this short term solution ? (Choose all that apply)

- A- It is not reliable and there is no SLA guarantee
- B- It is not secure
- C- QoS configuration is not under control of RMT
- D- For each customers require separate overlays
- E- Multicast routing is not supported with it
- F- All of the above

Answer 36 : Correct answer, Option A, B,C

37- What is the best long-term solution to connect current RMT network and a new one in the UK?

- A- Use L2VPN from another MPLS Service Provider to connect current RMT network and a new one with MPLS and QoS over that L2VPN
- B- Use L3VPN from another MPLS Service Provider to connect current RMT network and a new one with MPLS and QoS over that L3VPN
- C- Build GRE tunnels over Internet and run MPLS
- D- Order dedicated circuits

Answer 37 : Correct answer is Option D.