ACN ASSIGNMENT – 2

State WAN network design

Vijayraj Shanmugaraj

20171026

Dheeraj Reddy Pailla

20161053

Rohan Tiwari

201501150

Objective:

The Aim of this project is to design a highly available, secure and scalable Wide Area Network (WAN) to connect the various IT infrastructure available in various pockets of an typical Indian state government establishments, enabling e-governance – from the state secretariat, District Administration, to the last leg of democracy, the panchayats – using the existing infrastructure – so that it can be implemented within a realistic short time frame, with minimum cost. It also aims at communication and training from the state government to reach the panchayats through Video and Audio streaming. It aims at providing Video conferencing between various levels so that the issues can be resolved instantaneously and information can be obtained on the fly. This will improve the transparency of the administration.

Requirements:

1. The State WAN is a network connectivity – connecting the State Head Quarters (SHQ) to District Headquarters (DHQ), DHQs to Taluk Head Quarters (THQ). It is a hierarchical network between SHQ, DHQ and THQ. The village level is a broadband connectivity through FOC or VSAT network.
    a. Up to THQ level Video Conferencing, VoIP connectivity and Data transfer are the basic requirement. Strict QoS needs to be followed so that good quality VC and VoIP service is achieved.
    b. This connectivity shall be any-to-any – i.e. for example, the Video conferencing can happen between SHQ, DHQ or between one DHQ and another DHQ or may involve a combination of SHQ, DHQs and THQs.
2. At all the three levels – the horizontal connectivity – connecting all the government offices at that level to provide WAN and Internet connectivity.

Assumptions:

- We are considering the main stream states that has invested in IT infrastructure.
- It is assumed that as per BBNL (Bharat Broadband Network Limited) target of March 2018, 250,000 village panchayats of India have Fiber Optic Connectivity.
- If the village panchayats do not have optical cable connectivity, then VSAT connectivity will be considered.
- Up to the District Headquarters level – it is assumed that Metro Ethernet is available and also at least once service provider (BSNL) provides the WAN service infrastructure with latest techniques such as MPLS.
- Considering the latency, Video Conferencing is not considered for remote villages where VSAT communication link is deployed. We assume that any kind of conferencing may happen via VoIP.
- The following assumptions have been made about the headquarter details and their respective connectivity details:
    - Number of SHQs – 1 (24 x 7 connectivity)
    - Number of DHQs – 30 (24 x 7 connectivity)
    - Number of THQs per DHQ – 10 (9 to 5 connectivity – 5 days a week)

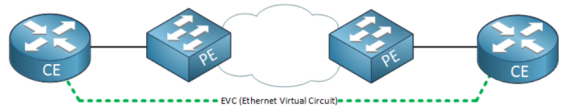
Technologies Considered:

All the technologies that are considered here are supported by most of the service providers in India.

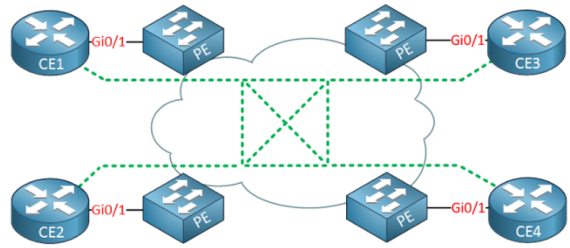
Leased Lines: In India Fiber Optic cables have been laid throughout. BBNL is even planning to lease out the unused fiber (Dark Fiber) to other ISPs also. Hence, leased line is a viable option – though cost is comparatively high. Most of the ISPs, can provide High-Capacity, Convergent (video, voice, data) and resilient mesh architecture and has seamless integration with International Private lines. Three topologies are provided – point-to-point, hub & spoke, any-to-any fully-meshed VPLS.

Metro Ethernet: If the remote sites are in close proximity, then Metro Ethernet is a cheaper option. But as the name implies, the service is limited to specific geographic regions. So, if the remote site falls outside of the Metro-Ethernet boundary, then it may not be a viable solution. But Metro Ethernet is scalable up to hundreds of remote sites. Metro Ethernet also is tremendously easy to manage as the ISP's handoff looks and acts just like a standard Ethernet link on the LAN. It provides three configurations – E-Line, E-Lan, E-Tree. (CE – Customer end, PE – Provider end)

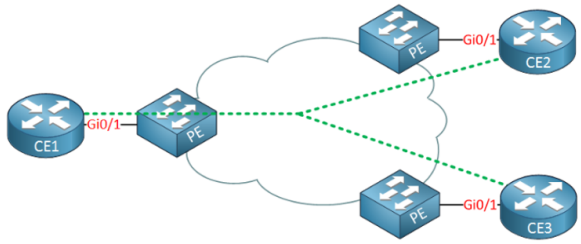
E-Line



E-Lan



E-Tree

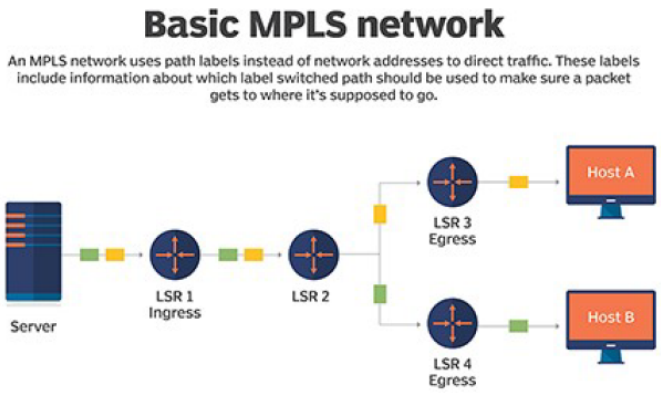


It is a Layer-2 technology. Easily extend Internal LAN QoS policies across Metro Ethernet. From a data transport point of view, all sites look as if they are connected to the same Ethernet switch inside the service provider cloud. Even VLANs can be extended across Metro Ethernet. This is a good choice for interconnecting all the government offices in the State Head Quarters (SHQ) and District Head Quarters (DHQ).

Broadband and SD-WAN: Broadband is a cost-effective option – Use broadband Internet connectivity and then create a secure overlay using some form of VPN technology. Broadband can be wired such as DSL or cable, or it could be wireless such as 3G/4G or satellite internet services. Primary disadvantage is that – we do not have control over latency or QoS. Hence, if you need to transmit/receive latency-sensitive data across WAN, then this is not a viable option. Else, we need to leverage SD-WAN technology combined with multiple broadband connectivity options to intelligently choose the fastest path from Point A to Point B. So, the design is intricate.

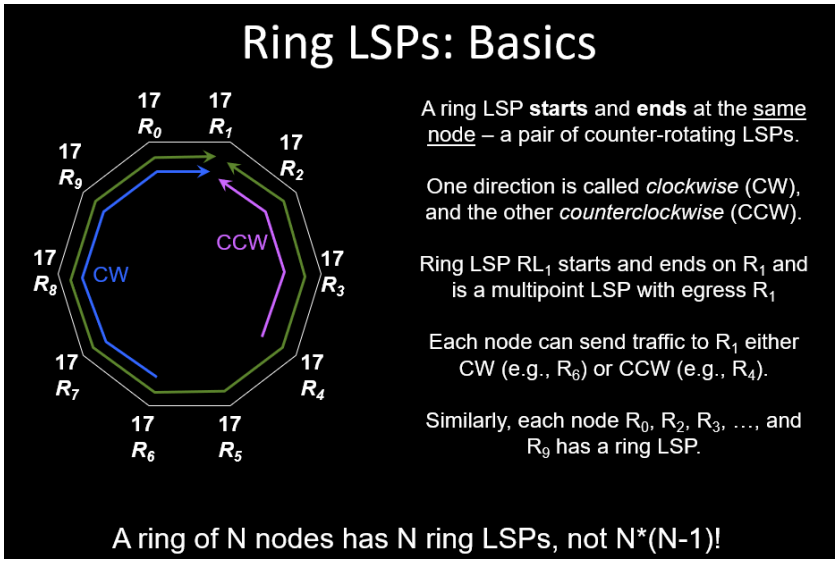
Legacy T1/T3: Point-to Point connection at symmetric 1.5 Mbps up/down speed. If the bandwidth is not enough then multiple lines can be bonded together. But these lines are expensive compared to broadband and in many cases comparable Metro Ethernet options. So, this is the last resort option, if no other WAN connectivity options are available.

MPLS (Multi-Protocol Label Switching): is a widely used WAN solution that intelligently routes packets through a service provider network using a four-byte MPLS header that uniquely identifies each customer. MPLS allows customers to forgo complex WAN routing and Quality of Service (QoS) policies and instead places that burden on the service provider. From the customer's perspective, you simply need to route the appropriate internal network across the link.



Carriers typically offer several throughput options, often ranging from 1 Mbps for very small sites all the way up to thousands of Mbps. MPLS provides dedicated and symmetrical bandwidth, which include strict service-level agreements (SLA) to ensure, you are getting what you pay for. MPLS supports point-to-point, point-to-multipoint and ring topologies.

MPLS-Ring Topology – Each ring is identified by a Ring-ID. The IGP (Interior Gateway Protocol) is used to discover ring neighbors and ring links. Links between a pair of ring nodes may belong to multiple rings. Links between a pair of ring nodes are automatically bundled into a single logical link. Hence, Ring links are discovered and "auto-bundled". All nodes agree on Clockwise and counter-clockwise. Each node knows its CW and CCW neighbor. This increases the resilience of the network. The loops can be avoided by TTL. Hence, MPLS on rings – easy from configuration point of view (auto detection), efficient from protection point of view and flexible from a bandwidth utilization point of view. Hence, this is a good choice for the high bandwidth core network.



MPLS-TE (Transport Engineering): MPLS-TE provides efficient way of forwarding traffic throughout the network, avoiding over-utilized and under-utilized links. It adapts to changing bandwidth. It takes into account configured bandwidth of the links. MPLS-TE also calculates and keeps a backup path when the main path is in use. When there is a failure in main path, then MPLS-TE switches to the backup path. The switching time is typically 50 mSec. This can be used in creating redundant MPLS-Ring configuration.

VSAT Connectivity: Various service providers are able to provide VSAT connectivity to remote locations. For example, JIO has come out with a micro terminal with all the integrated electronics – which is just 15 Kgs of weight and carried by a single person in a suitcase. Also, this can be set up within 15 minutes to provide the connectivity. Even otherwise, Ku band VSAT terminals are much cheaper in cost.

On the downside, the VSAT communication has a large latency, as communication happens through the double hop which introduces a delay of 500 mSec. The communication is also affected by climate and ISPs enforce strict data Cap and the price for a comparative bandwidth is higher for VSAT.

Fixed Wireless Connectivity: Most of the villages in India are connected through wireless mobile networks. 3G connectivity is ubiquitous and 4G connectivity is getting deployed faster. The advantages are low latency, not affected by climate and easy to setup.

Final Technology Selected:

The WAN connectivity between SHQ and DHQs (Tier-1 & 2) is the core of the State WAN. Hence, this needs to be future proof and scalable. Scalable in the sense that we must be able to connect all the government related departments and offices and also connect the state WAN to the national WAN and other knowledge networks. Considering these points and the scale of connection – we have considered the MPLS-TE technology in the **Redundant ring configuration**. To have the horizontal connectivity – connecting all the government departments and offices across the SHQ and DHQs we have considered **Metro Ethernet** in **E-LAN topology**. At THQ level, the broadband connectivity is considered for horizontal connectivity – considering the limited geographical distribution.

The connectivity between DHQ and THQs (Tier-3) follows the **HUB and Spoke topology**, using the **leased lines**. Though some of the THQs may have MPLS connectivity, for uniformity this topology has been followed. In future if MPLS is available across all the THQs then MPLS ring topology can be followed between DHQ and THQs (A second ring).

For the Village Panchayat level, we have chosen a fixed wireless 3G/4G connection. The THQ router is an ISR router and the card slot can have a 3G/4G connecting interface card. But this card is not required, as the ISP can route the data from the villages received through 3G/4G network to THQ router through VPN. Due to the downsides of VSAT (but its ease of setup in remote areas), VSAT connectivity will be used only when there are no other wireless options (In extremely remote villages which do not have mobile wireless connectivity and hence have to be reached through VSAT). (Tier-4)

In a nut shell:

- Connectivity between SHQ and DHQs and between DHQs is through **redundant MPLS ring topology**. (Tier-1 & 2)
- The horizontal connectivity between SHQ and govt. offices in state headquarters is through **Metro Ethernet** in **E-LAN topology**. Then this is connected to the WAN at SHQ. (Tier-1)
- Internet connectivity is provided through **two ISPs** at the SHQ and will be distributed to all offices
- The horizontal connectivity between DHQ and govt. offices in the district head-quarters is through **Metro Ethernet** in **E-LAN topology**. Then this is connected to the WAN at DHQ. (Tier-2)
- Connectivity between DHQ and THQ is through **leased line in Hub and Spoke topology**. (Tier-3)
- Connectivity to the Gram Panchayats will be through fixed wireless connectivity provided by the ISP. VSAT connectivity will be used in extremely remote remote villages which do not have mobile wireless connectivity. (Tier-4)

Bandwidth Selection

Video Conferencing Bandwidth Requirement:

Bandwidth	Resolution	Frame Rate
384 Kbps	CIF	30 fps
512 Kbps	4CIF	15 fps +
768 Kbps	4CIF	30 fps
1 Mbps	HD720	15 fps +
2 Mbps	HD720	30 fps
4 Mbps	HD720	60 fps
6 Mbps	HD1080	30 fps
7 Mbps	HD1080	60 fps

CIF – Common intermediate format; HD – High Definition; fps – frames per second.

The above table is a guidelines value to assess network bandwidth. If the ISP use a **particular Codec** then the requirement may be different – depend on the Codec.

Also, the video conferencing bandwidth requirements in this table are for the amount of traffic supported inside the Real-Time Transport Protocol (RTP) packet payload. The actual bandwidth on the IP network – after adding RTP, UDP, IP and Ethernet headers - will be around 20 % higher. So, 1Mbps video conference calls actually use about 1.2 Mbps of network bandwidth. For clarity we can call them as ***transport bandwidth*** (1 Mbps) and ***network bandwidth*** (1.2 Mbps).

Assumption for number of concurrent video conference calls:

- 30 concurrent Video conference calls (@ 2.4 Mbps) is considered between SHQ and DHQs or between DHQs
- 10 concurrent Video conference calls (@ 1.2 Mbps) is considered between DHQ and THQs

VoIP Bandwidth Requirements:

The following table is taken from "Voice Over IP – Per Call Bandwidth Consumption" by CISCO.

Codec Information				Bandwidth Calculation			
Codec & Bit Rate (Kbps)	Codec Sample Size (Bytes)	Codec Sample Interval (ms)	Mean Opinion Score (MOS)	Voice Payload Size (Bytes)	Voice Payload Size (ms)	Packets Per Second (PPS)	Bandwidth MP or FRF-12 (Kbps)
G.711 (64 Kbps)	80 bytes	10 ms	4.1	160 Bytes	20 ms	50	82.8 Kbps
G.729 (8 Kbps)	10 bytes	10 ms	3.9	20 bytes	20 ms	50	26.8 Kbps
G.723.1 (6.3 Kbps)	24 bytes	30 ms	3.9	24 bytes	30 ms	33.3	18.9 Kbps
G. 723.1 (5.3 Kbps)	20 bytes	30 ms	3.8	20 bytes	30 ms	33.3	17.9 Kbps
G.726 (32 Kbps)	20 bytes	5 ms	3.85	80 bytes	20 ms	50	50.8 Kbps
G.726 (24 Kbps)	15 bytes	5 ms			20 ms	50	42.8 Kbps
G.728 (16 Kbps)	10 bytes	5 ms	3.61	60 bytes	30 ms	33.3	28.5 Kbps
G722_64K (64 Kbps)	80 bytes	10 ms	4.13	160 bytes	20 ms	50	82.8 Kbps
ilbc_mode_20 (15.2 Kbps)	38 bytes	20 ms	NA	38 bytes	20 ms	50	34.0 Kbps
ilbc_mode_30 (13.33 Kbps)	50 bytes	30 ms	NA	50 bytes	30 ms	33.3	26.867 Kbps

Codec	**Voice Payload Size (ms)**	**Voice Payload Size (Bytes)**	**Comment**
G.711	20 ms (Default)	160 Bytes	Notice that Codec bit rate is always maintained. For example, G.711 Codec = [240 bytes * 8 bits/byte] /30 ms = 64 Kbps
	30 ms	240 Bytes	
G.729	20 ms (Default)	20 Bytes	
	30 ms	30 Bytes	
G.723	30 ms (Default)		

Assumption for number of concurrent VoIP calls:

- 500 concurrent VoIP calls at SHQ/DHQ levels (@ 64 Kbps)
- 50 concurrent VoIP calls at DHQ/THQ levels (@ 64 Kbps)

Data Bandwidth Requirements:

It is very difficult to calculate a bandwidth requirement for data. The users can be divided into three types (given with speed provided to those respective user):

- Light User: 5 Kbps
- Medium User: 8 Kbps
- Heavy User: 12 Kbps

The total bandwidth requirement can be calculated as follows:

For example, if we have 5 heavy users, 5 medium users and 10 light users, our total bandwidth requirement would be (5 *12 + 5 * 8 + 10 * 5) Kbps = 150 Kbps

Bandwidth requirement of MPLS Ring at SHQ/DHQ (Tier-1 & 2):

Considerations for bandwidth consumption:

- 30 Concurrent video conference calls @ 1.2 Mbps
- 200 Concurrent VoIP calls @ 64 Kbps
- Data for 10000 users (2000 heavy users + 2000 Medium Users + 6000 Light Users)

Note: The 25000 users are the ones who are directly on the LANs connected to the SHQ and DHQs directly.

Estimated bandwidth:

30*1.2 Mbps + 200*(64/1000)Mbps + (1/1000)*(2000*12 + 2000*8 + 6000*5) Mbps = 118.8 Mbps

Considering the above and other protocol related data load, it is estimated that 250 Mbps + 250 Mbps redundant MPLS ring bandwidth is a safe one.

Bandwidth of Leased Line between DHQ and THQ (Tier-3):

The link is a dedicated link between DHQ and THQ. Considerations for bandwidth consumption:

- 1 concurrent video conferencing call between DHQ and THQ @ 1.2 Mbps
- 5 Nos concurrent VoIP calls between DHQ and THQ @ 64 Kbps
- Data for 500 users (100 heavy users + 100 Medium Users + 300 Light Users) (These users are the ones connected to the THQ directly)

Estimated bandwidth:

1*1.2 Mbps + 5*(64/1000)Mbps + (1/1000)*(100*12 + 100*8 + 300*5) Mbps = 5 Mbps

Considering the above and other protocol related data load, it is estimated that 10 Mbps bandwidth is considered safe.

VSAT bandwidth Requirement:

For the VSAT utilization, the following are considered:

- Two PC nodes for internet browsing to provide the basic e-Services
- One Audio/Video node for training video streaming
- One VoIP call at 64

Considering the above a Ku band VSAT terminal a bandwidth of 512 Kbps downlink/ 128 Kbps uplink is considered.

Bandwidth for 3G/4G connection:

The following activities are considered:

- 1 Low-resolution video conferencing call @ 384 Kbps
- 1 VoIP call @ 64 Kbps
- 1 Network User

Considering the above, a safe bandwidth to allocate is 1 Mbps.

QoS Design:

The network must ensure that the applications perform across the WAN during times of network congestion. Traffic must be classified and queued and the WAN connection must be shaped to operate within the capabilities of the connection. When the WAN design uses a service provider offering with QoS the WAN edge QoS classification and treatment must align to the service provider offering to ensure consistent and end-to-end QoS treatment of traffic.

In WAN links the congestion can occur when there are speed mismatches. This may occur because there is significant difference between LAN speeds and WAN speeds. To prevent that from occurring, the following two major tools can be used:

- Low-Latency Queueing (LLQ), which is used for higher-priority traffic (voice/video)
- Class-based Weighted-Fair Queueing (CBWFQ), which can be used for guaranteeing bandwidth to data-applications.

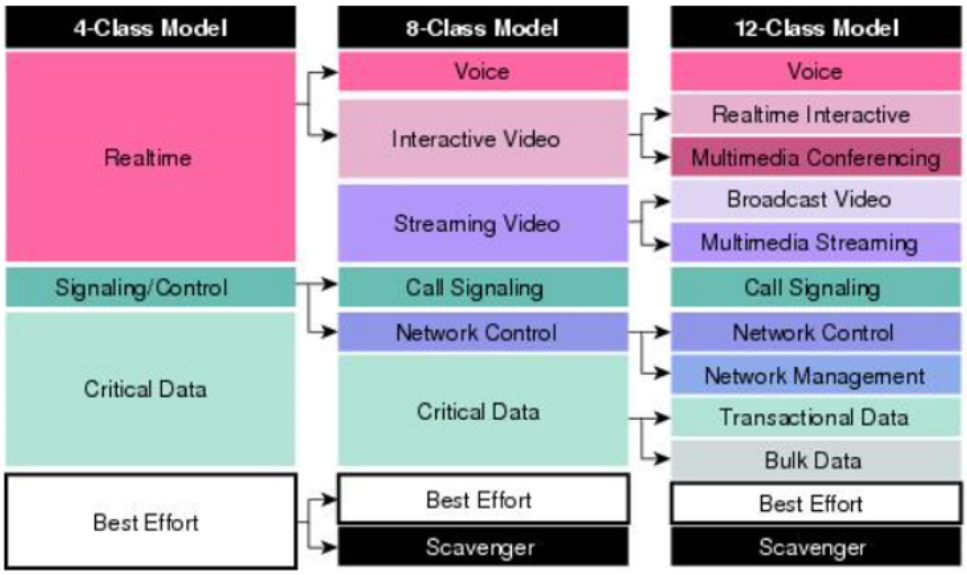
The general guidelines for deploying WAN edge device considerations are as follows:

- For WAN speeds between 1 Mbps to 100 Mbps, use hierarchical policies for sub-line-rate Ethernet connections to provide shaping and CBWFQ/LLQ – This can be configured for connection between DHQ and THQ in the 10 Mbps Leased line.
- For WAN speeds between 100 Mbps to 10 Gbps use routers with QFP or hardware queueing. This will be used in SHQ and DHQ routers connected to MPLS ring

If the ISP provides 7 classes of QoS then a typical policy can be created as shown in the following table:

Class of Service	**Traffic Type**	**DSCP Values**	**Bandwidth %**	**Congestion avoidance**
VOICE	Voice Traffic	Ef	10	--
INTERACTIVE-VIDEO	Interactive video (Video Conferencing)	cs4, af41	23	--
CRITICAL-DATA	Highly interactive (such as Telnet, Citrix, Oracle thin client etc.,)	af31, cs3	15	DSCP-based
DATA	Data	af21	19	DSCP-based
SCAVENGER	Scavenger	af11,cs1	5	--
NETWORK CRITICAL	Routing protocols: operations, administration and maintenance (OAM) traffic	cs6, cs2	3	--
Default	Best effort	Other	25	random

If the ISP provides only 4 Classes of QoS then the following picture shows how the 12 class QoS of LAN can be mapped to 8 Class QoS and in-turn can be matched to 4 class QoS. The table next to that provides a typical QoS policy for 4 Classes of service:



Class of Traffic	**4-Class SP Model**	**Bandwidth Allocated**
Voice, Broadcast Video, Real Time interactive	SP-Real-Time	30%
Network Control, Signaling, Transactional Data	SP-Critical 1	20%
Multi-Media Conferencing, Multimedia Streaming	SP-Critical 2	20%
Bulk Data, Scavengers, Best Effort	SP-Best Effort	30%

The steps to be followed in QoS deployment are:

1. Create the QoS Maps to Classify Traffic
2. Create the policy map that marks BGP traffic
3. Define a policy map that defines the queuing policy
4. Configure shaping and queuing policy
5. Apply the shaping and queuing policy to a physical interface.

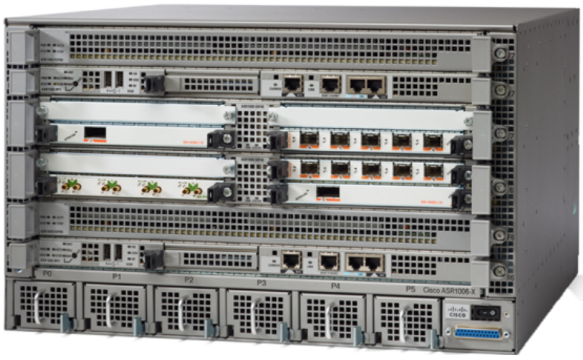
Edge Router Selection:

MPLS-CE-Router and Aggregator:

The router in the SHQ (State Headquarters) does the following functions:

1. Provides the MPLS-CE Edge for WAN (250 Mbps MPLS Ring)
2. Provides dual homed Internet Edge (1GBps Internet – Two ISPs)
3. Connects to the Metro Ethernet for horizontal integration

Considering the above requirements, the ASR 1006 – X has been selected. This router provides hardware redundancy. This router supports the Optical cable connectivity. This is a modular router. The network capacity and services can be increased without a hardware upgrade. The MPLS connectivity can be provided by enabling the CISCO Express forwarding. This router is specifically designed for WAN aggregation, with the flexibility to support a wide range of 3 to 16 mpps (million of packets per second) packet-forwarding capabilities 2.5 to 40 Gbps system bandwidth performance and scaling.



The router in the DHQ (District Head Quarters) performs the following:

1. Provides the MPLS-CE Edge for WAN (250 Mbps MPLS Ring)
2. Connects to the Metro Ethernet for horizontal integration
3. Maximum of 10 Nos of Leased line connectivity with THQs

For DHQ the edge routers can be ASR 1006 – X. By providing the same hardware around the MPLS ring, the configuration and it will enable efficient spare management.

The router in the THQ has the following functionalities:

1. Connect to the leased line from DHQ
2. THQ LAN integration.

CISCO 3945 routers have been selected.

It is an Integrated Services Routers (ISRs) is a routing platform that provides connectivity and security services in a single secure device. Provide IPSec. It has a bandwidth of 150 Mbps, provides 3 on board ports, and has 2 Nos. service module slots and redundant power supplies.

L3 Switches in SHQs, DHQs and THQs

The main function of L3 switches is to provide LAN integration. CISCO Catalyst 4500 series is selected for this functionality.

- CISCO Catalyst 4507R is selected.
- Provides Supervisor engine redundancy
- Redundant power supplies
- Has five nos. line cards

Router at Tier 4:

CISCO 881G Series 3G Wireless ISR routers can be deployed at the Village Administrative Office (VAO). This router also has four 10/100 Mbps managed ethernet ports for LAN interface. Hence, a separate switch is not required.

Network Architecture:

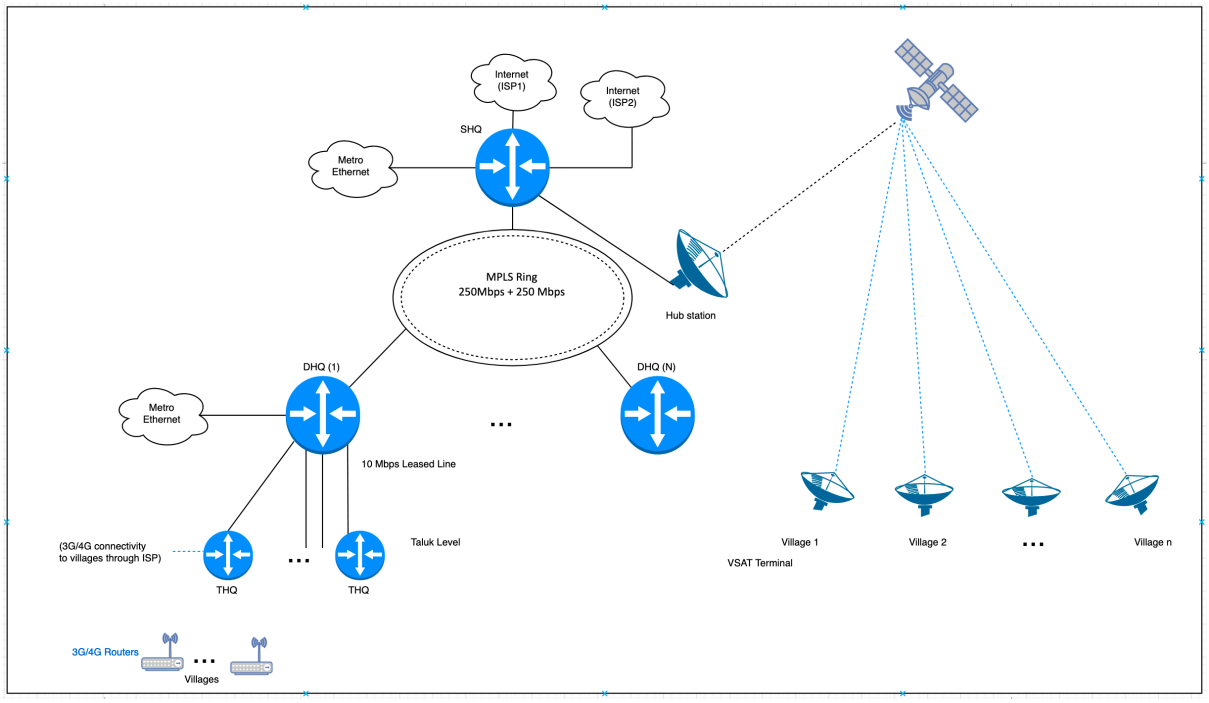


Figure 1: Overall architecture

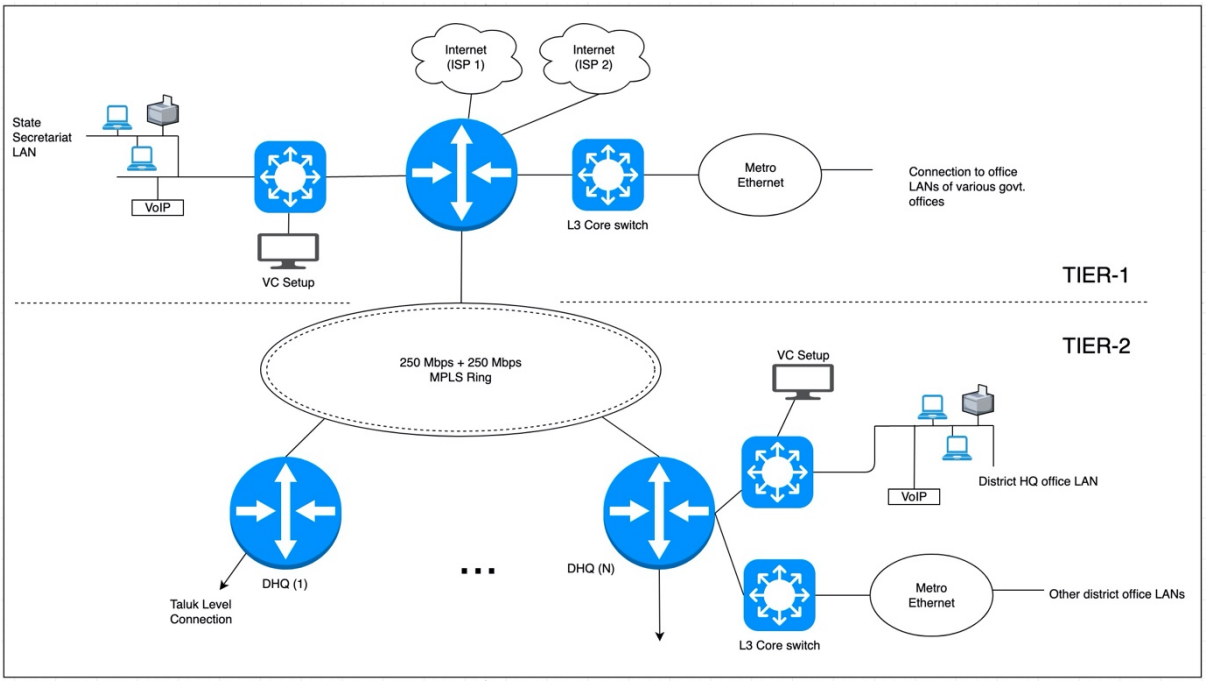


Figure 2: Tier 1 - Tier 2 Architecture

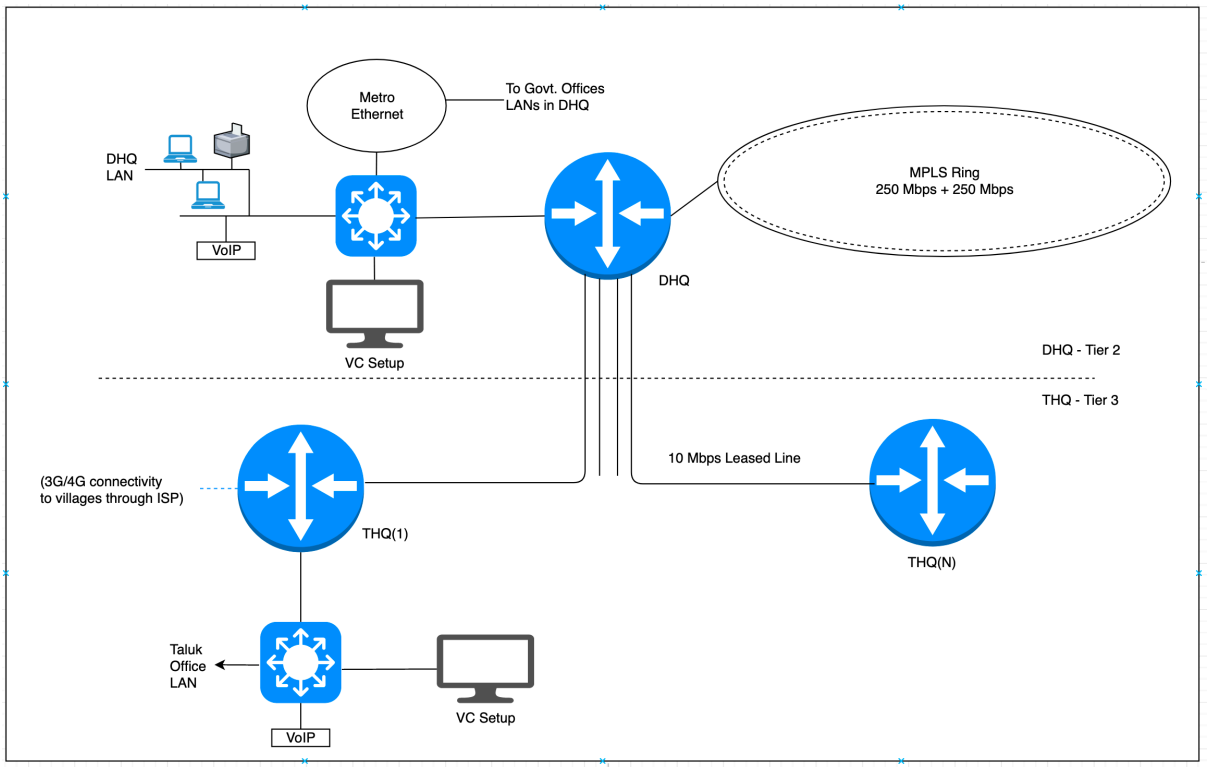
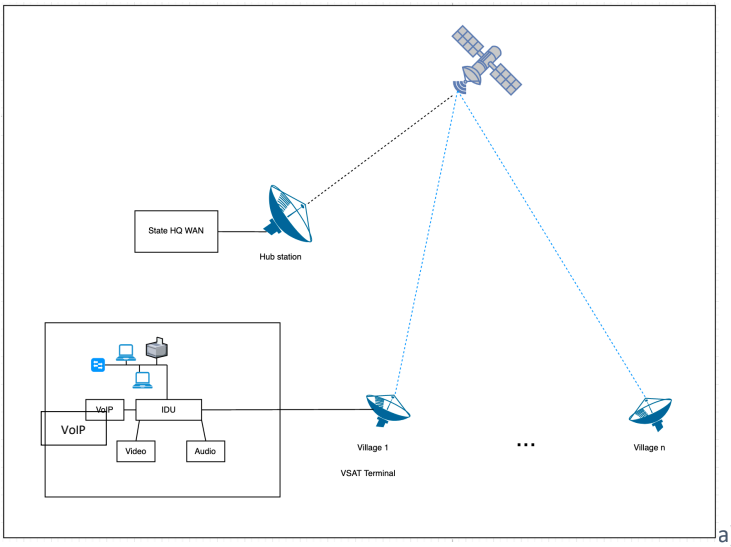
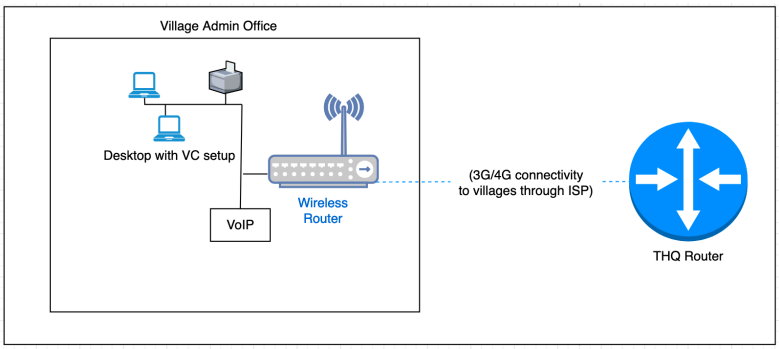


Figure 3: Tier 2 - Tier 3 Architecture



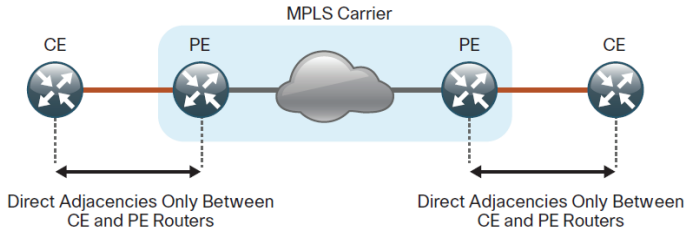
a)



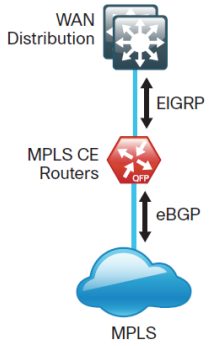
b)

Figure 4: a)VSAT-star network and b)3G/4G connectivity for Gram Panchayat Connectivity

Routing Protocol selection(Tier-1 and Tier-2):



At the WAN-aggregation sites (Both SHQ and DHQ), the MPLS CE router must be connected both to the distribution layer and to its respective MPLS carrier. Multiple routing protocols (EIGRP and BGP) are used to exchange routing information



MPLS Dynamic

As all the hardware selected (both routers and L3 switches) are from CISCO, EIGRP protocol is selected at the IGP. EIGRP is easy to configure, does not require large amount of planning and has flexible summarization and filtering and can scale large networks. By performing IP summarization, you can reduce the amount of bandwidth, processor and memory necessary to carry large routing tables and reduce convergence time associated with a link failure. CISCO uses EIGRP named mode. Named EIGRP includes features such as wide metrics, supporting larger multi-gigabit links. For added security, EIGRP neighbor authentication has been implemented to prevent unauthorized neighbor associations.

EIGRP LAN process is configured at the WAN-aggregation site to connect to the primary site LAN distribution layer.

BGP: We chose BGP as the routing protocol for PE and CE routers to connect to the MPLS VPNs because it is consistently supported across virtually all MPLS carriers. In this role, BGP is straight forward to configure and requires little or no maintenance. BGP scales well and you can use it to advertise IP aggregate addresses for remote sites.

To use BGP, we need Autonomous System Number (ASN). We can use a private ASN number in the range 64512 to 65534.

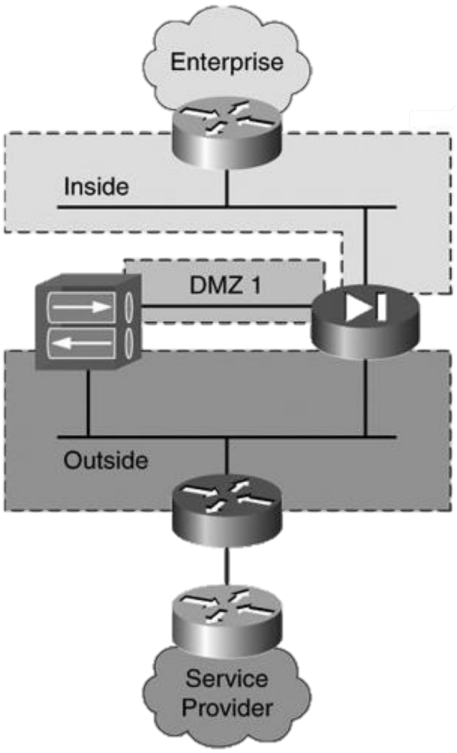
Routing Protocol selection (Tier-2 and Tier-3):

The interconnection between Tier-2 and Tier-3 is through leased line. Hence, EIGRP is configured on the DHQ router and the THQ router.

Security Design:

Security is an integral function of the Integrated Service Routers (ISRs). The selected ISRs are enabled with IPSec security. Hence, all the voice, video and data communication will be configured to flow through secure VPNs. Hence, all the communication is secure on the WAN.

The ISR acts as the router-cum-firewall and has the capability to function as a stateful inspection intrusion protection device, which provides a DMZ port. The ISR routers themselves can work as VPN gateway also. For extra protection, we can have a VPN concentrator such as CISCO VPN3000 in the DMZ. This will reduce the load on the ISR and improve the security levels as the VPN is handled by a separate device.



Future improvement to the State WAN topology:

Tier-1 and Tier-2 are on MPLS – Redundant Ring configuration. So even if the bandwidth requirement increases, without any change in hardware.

The connectivity between Tier-2 (DHQ) and Tier-3(THQ) is provided through leased line. This is because all the THQs do not have MPLS connectivity. In future, if all the THQs have MPLS connectivity, then a second MPLS ring topology can be provided for connecting the THQs related to a DHQ. This also can be a redundant

There is no connectivity between Tier-3 (THQ) and Gram Panchayats. But as per commitment by the Indian Government all the villages will be Internet ready by March 2018. If this becomes true, then the VSAT connectivity to the villages can be replaced with Broadband connectivity through Bharat Fiber.