A Software-defined Wide Area Network (SD-WAN) is a virtual WAN architecture that allows enterprises or any organizations to leverage any combination of transport services – including MPLS, LTE / 4G / 3G and broadband internet services – **to securely connect users to applications.**

They encrypt data AES 256 and products are FIPS complaint The Federal Information Processing Standard (**FIPS**), which are standards for encryption of data

An SD-WAN uses a centralized control function to securely and intelligently direct traffic across the WAN. This increases application performance, resulting in enhanced user experience, increased business productivity and reduced costs for IT.

Traditional WANs based on conventional routers are not cloud-friendly. They typically require backhauling all traffic – including that destined to the cloud – from branch offices to a hub or headquarters data center where advanced security inspection services can be applied.

In Indian Railways where it is complete private network and using a router centric model has its limitations of expansion due to the reasons that they depend on leased line or their own network availability for providing connectivity or have to use cumbersome process like VSAT , as the need to expand network services is ever increasing due to the digitization of services it would be ideal to harness the software defined network to suit Indian railways in a manner suitable for it

Team Engineer, SDN wan devices ensures that without entering into the network of application for example PRS, they are capable of carrying the date securely over Internet to the remote location, the internet can be physical connectivity or GSM

In the case of PRS / UTS etc., we are presently carrying the terminal server port to the remote end and not entering the network of PRS / UTS

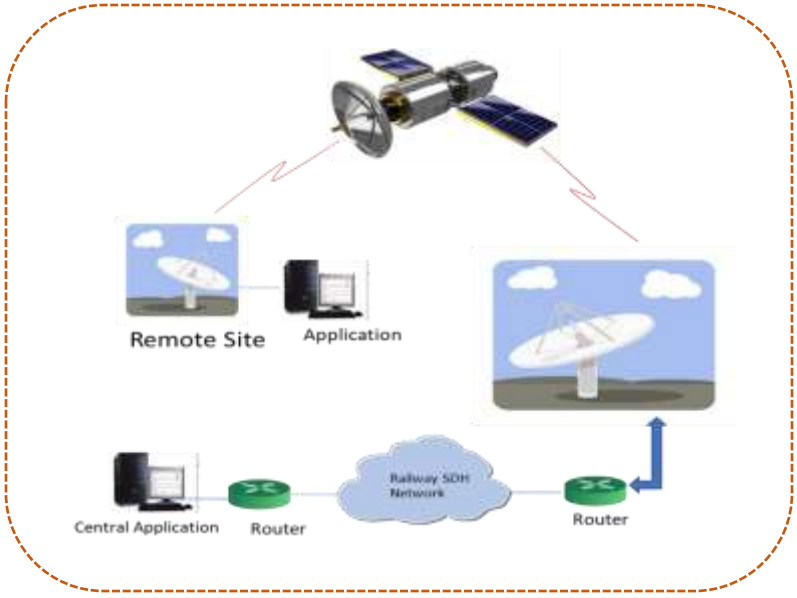
Apart from it we will be able to carry any data of the various applications needs to the destined location using Internet and Internet connection is agnostic and does not

depend on any particular service providers, we can also connect to the existing network and interwork with routers available on traditions V.35 or E1 interface and in case the leased line fails we can go on the internet (GSM) this will be useful where the service providers leased line are not stable say BSNL leased line presently for various reasons

The function of SD- WAN is we have central controller with a public IP which communicates to the remote units and an SD-WAN handles traffic based on priority, quality of service and security requirements in accordance with user needs. The conventional router-centric model distributes the control function across all devices in the network - routers simply route traffic based on TCP/IP addresses and ACLs.

- **Centralized Orchestration.** By centralizing the configuration of an SD-WAN as well as application performance and security policies, user can significantly reduce WAN operational expenses
- **Zero-Touch Provisioning (ZTP).** With ZTP, configurations and policies are programmed once and pushed to all locations without having to manually program each device individually using a CLI. It eliminates the need to send specialized IT resources out to the locations whenever a new application is added or a policy is changed. ZTP also reduces human errors, resulting in more consistent policies across the various networks

Typical VSAT Connectivity:



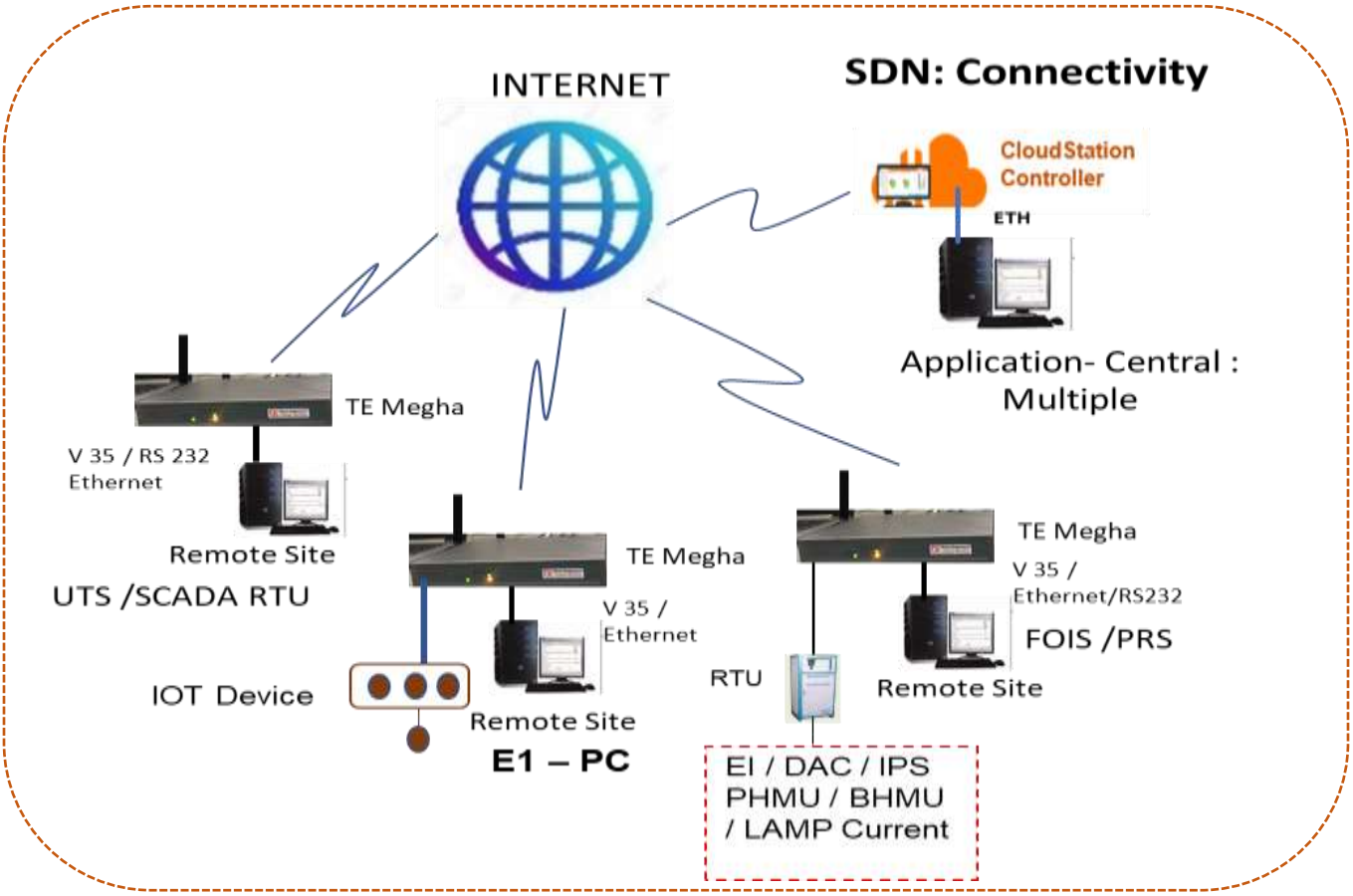
Lot of Hops

Cumbersome process of installation

Bandwidth constraint

Costly and high recurring cost

Typical SDN connectivity:



We can connect multiple applications (be it your upcoming predicative analysis to network multiple data loggers scattered across) or the existing numerous applications and take them to the central side to their respective applications servers or also hand over the data to the routers which in turn can push it to the central servers available at different geographical locations in India or any where

We can help Indian Railways to use a combination of SDN and traditional WAN network so that their end point deployment is eased and in turn have their secure private network and existing server

Security Features available in the proposed network:

- End to End Security of Control plane (SSL) & Data plane (IPSEC)
- Multiple Level identification & Authentication
    - ✓ Device Identity & Authentication based upon multiple identifiers like Serial Number / UUID / MAC address etc.,
- Multiple levels of encryption
    - ✓ Control plane data is encrypted and sent over secured SSL channel
    - ✓ The control plane intelligence is encrypted using 256-bit SSL encryption and guarded against man in the middle attack
- Appliance communication is restricted to only – preprogrammed central control station which is under the user jurisdiction