BYTESCREEN

CONNECT • DETECT • PROTECT

An Overview
FUSIONMAESTRO

(A Management & Network Service Controller)

CONTENTS

Copyright

Disclaimer

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products cannot be considered binding but shall be defined in the agreement made between BYTESCREEN and the customer. However, BYTESCREEN has made all reasonable efforts to ensure that the instructions contained in the document are adequate and free of material errors and omissions.
BYTESCREEN will, if necessary, explain issues, which may not be covered by the document.

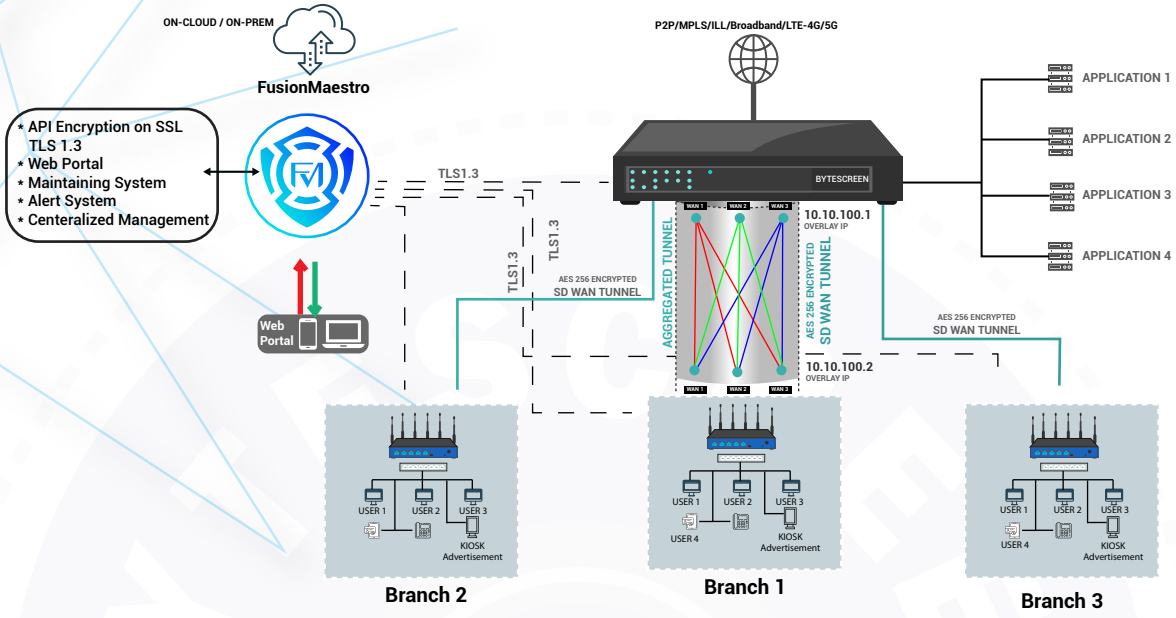
Feedback

BYTESCREEN welcomes customer comments as a part of the process of continuous development and improvement of the documentation.

Trademarks & Registered Trademarks

Products and product names mentioned in this document may be trademarks or registered trademarks of their individual proprietors.

BYTESCREEN –
Typical deployment &Terminology



FusionMaestro SDWAN Terminologies

#	Element	Description	Role/Function
A	Orchestrator (Controller)	Hosted on Public domain (Cloud based). Can be implemented on physical hardware as well as on virtual instances.	A portal which is used to monitor and configure the Concentrator and CPE's mapped. The communication with all devices is happening using encrypted API's with SSL TLS1.3
B	SDWAN Concentrator	Installed on Physical or on Virtual Environment at Central location at on-premises or at customer DC	All CPE's are communicating and establishing the tunnel (Overlay). Also it allows the connection to local applications need to be accessed over overlay towards CPE end points (Users)
C	SDWAN CPE	Deployed at each remote location (Physical appliance)	A hardware form at every remote location /branch which is running with SDWAN firmware. It forms a overlay tunnel with the help of any combination of internet connectivities like (PPPoE, ILL, MPLS, 4G LTE, DHCP)
D	Underlay	Internet connections (Input)	Internet connectivity provided Concentrator End: ILL, MPLS Remote (CPE) End: (PPPoE, ILL, MPLS, 4G LTE, DHCP)
E	Overlay - Tunnel	SDWAN Tunnel	Single aggregated AES 256 bit encrypted Tunnel with compression by using underlays at Concentrator end and Remote end
F	Encrypted API	End to End secured communication between Concentrator and CPE to Orchestrator	Based on SSL TLS1.3 encrypted API to ensure secured data exchange between Concentrator and each CPE to track the status helps to monitor

What is ORCHESTRATION:

It is a platform which smartly communicates to SD-WAN Concentrator and CPE's in that ecosystem and automate the configuration, coordination, and administration of your computing environment's systems, middleware, and services. You can also control automated processes to enable more extensive workflows.

Whether on-premises or in the cloud, orchestrating the scheduling and integration of automated activities between systems and services accelerates and simplifies linked workloads, repeating processes, and operations.

Manual administration simply cannot grow to meet the demands of today. The IT staff is responsible for maintaining hundreds to thousands of servers, customers, and applications.

Delivering highly available, dynamically scaled, performant apps and cloud systems using orchestration is crucial for alleviating a tremendous amount of work from your team.

This is not referred to automation, while automation refers to a single task, orchestration arranges tasks to optimize a workflow and process.

Fundamental roles:

1. Monitoring (H/W, undelay, overlay)
2. Remote config, per box and bulk upload
3. Maintenance and Support
4. Reports and analytics
5. Proactive alerts

Features:

Multitenant

Multi-tenancy is a software architecture that allows a single instance of a software programme to serve many clients.
Each customer is referred to as a renter.

A tenant is a collection of users who have a common access to the programme instance with particular capabilities.
Each tenant is physically integrated yet intellectually distinct in this architecture.

Multi-tenant architectures may be used in both public and private cloud environments, separating the data of each tenant.

In a multi-tenant public cloud, for example, the same servers will be utilised to host several users in a hosted environment.

Within such servers, each user is given a distinct and preferably safe place to store data.

3-Level Authentication [includes 2 factors]

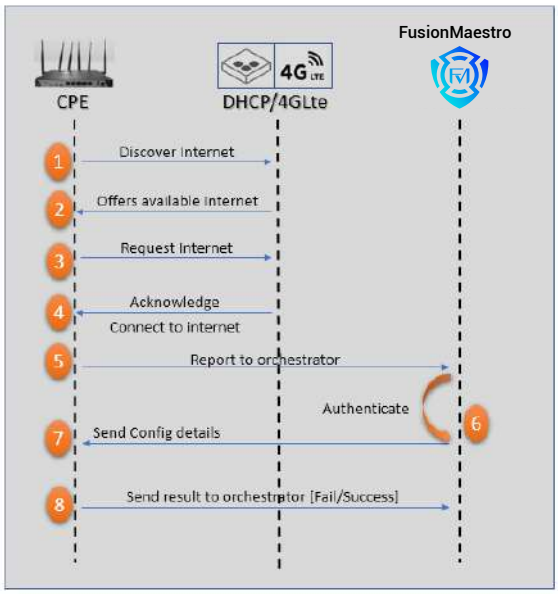
- ***Knowledge Factor*** (something you know) includes things a user must know, e.g., User ID, password, PIN, security question ***[Level - 1]***

- ***Possession Factor*** (something you have) includes things a user has to have in their possession, e.g., Mobile Number – OTP will send to register mobile number [Level - 2], emailID – OTP will send to registered email ID ***[Level - 3]***

Zero config, CPE monitoring

FusionMaestro devices actually function on a zero configuration to implement on the remote side. When powered up and connected to the internet, the client side will contact the server at a predetermined URL, using HTTP or HTTPS as the protocol using REST API. After authentication, the CPE is able to execute the following basic actions:

- Update CPE Configuration.
- Update CPE firmware.
- Reboot CPE
- Run CPE ping diagnostics.
- Reset CPE to factory default.
- Get periodic Status



1. CPE discover available Internet.
2. DHCP/4GLte offers the available Internet.
3. CPE request to connect Internet.
4. DHCP/4GLte replies with options.
5. CPE reports current status to unigr8ways orchestration.
6. Unigr8ways orchestration Authenticates the request.
7. Orchestration sends available Config, Firmware any other information available for CPE.
8. CPE Pulls details & send the result to orchestration after process.

Standardizing process of monitoring

Multiple REST APIs are predefined and transmit distinct sets of data to the orchestration.
Received data is processed and shown in the form of a dashboard and a report.
All processes and dashboards provide various metrics to help understand the CPE and concentration status and behavior.
Orchestration sends alerts to linked and pre-defend users through email and SMS based on different statuses received or not reported.

Time saving for employee / organization

Since entire deployment of CPE and Concentrator are ZTP, helps to reduce time for deployment tremendously. No physical presence required on site for the CPE deployment, will save tremendous time and resources for the organizations.

Remember the goals with speed and accuracy

Any goals related to deployment and configuration based on organization policy and needs, can be scheduled offline too. This will help speedy deployment with accuracy in data and process, as you will get enough time to analyze data that is entered before to push to CPE's.

Simplicity

All CPEs configured using orchestration UI, provide simplicity to do the configuration and monitoring status of through analytical dashboard and simple steps to do the config.
There is no UI or CLI mode available on unigr8ways devices help users to do the config remotely with minimal technical knowledge.

Auditability

All FusionMaestro keep up to 50 rollback changes done by users. This will help any auditor to keep track the changes and rollback if required just in one click.

Scaling in production

CPE and concentrator both can be deployed with any number for clients. There is no restriction on the number of devices to any deployment.
As per structure of orchestration application there is no restriction on connected device [CPEs], or onboarding different clients or in terms of no of employees to connect orchestration.

Data & analytics

Orchestration collects all the data received from FusionMaestro devices and process to so with the simplicity and user readable terms. Also creates the analytical dashboard to get deep drive into devices performance and tracking.

Role Based access

The orchestration is having role-based access with multitenant structure to provide full control on the users, what they can see, download and change with the audit logs.

What is required for Orchestration

Hardware

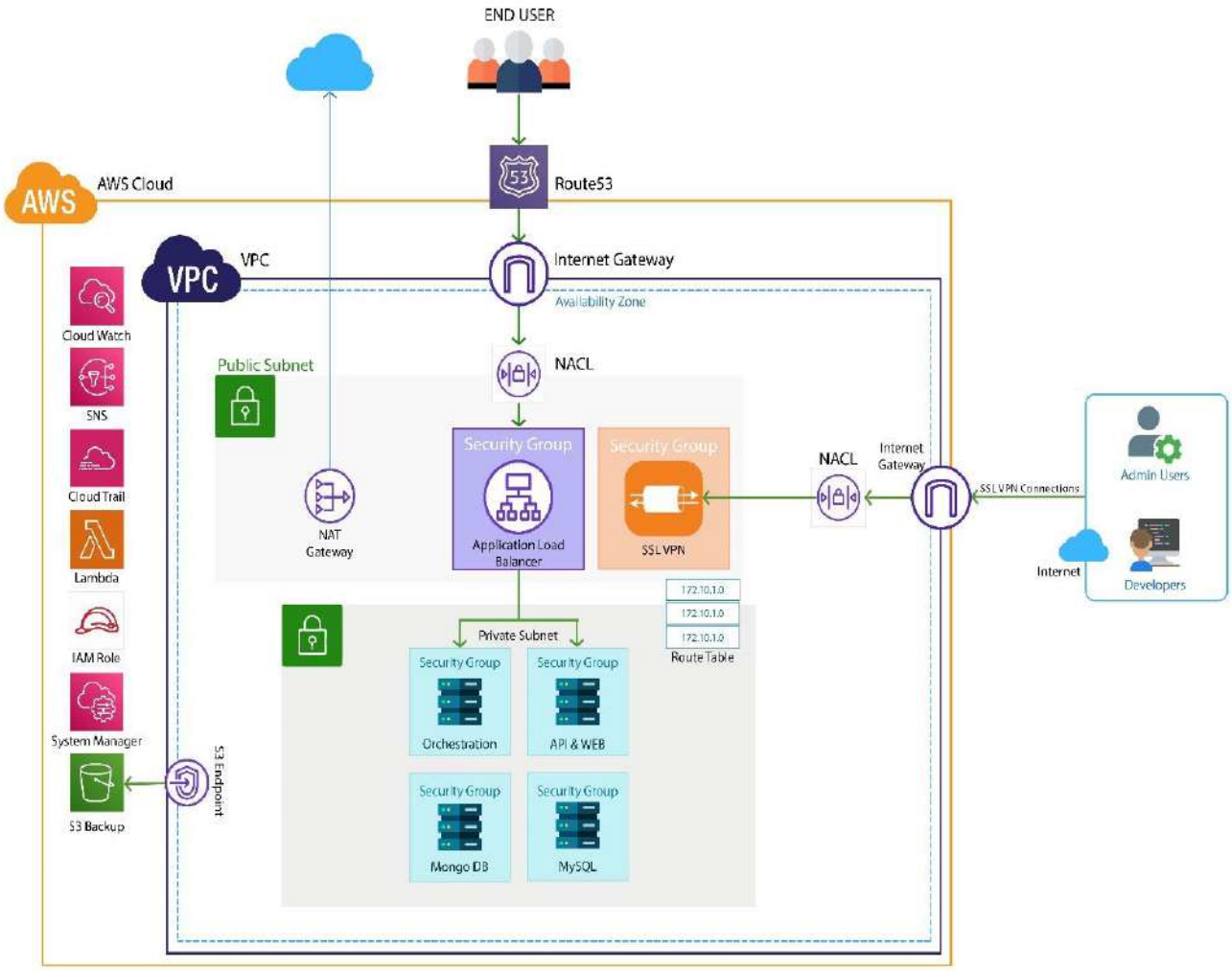
- Physical Server or virtual Instance
- Domain / Sub-Domain for mapping
  - Login, appapi, prdlic, sdwanmon, sermon, ugwconfig, wanpm, webapi, rrdgraph, bbds
- IP to map domain / sub-domain
- EMAIL / SMTP details to send notification

Software

- CentOS-7 Minimal
- WildCard or per domain SSL Certificate
- MySQL
- MongoDB
- Redis

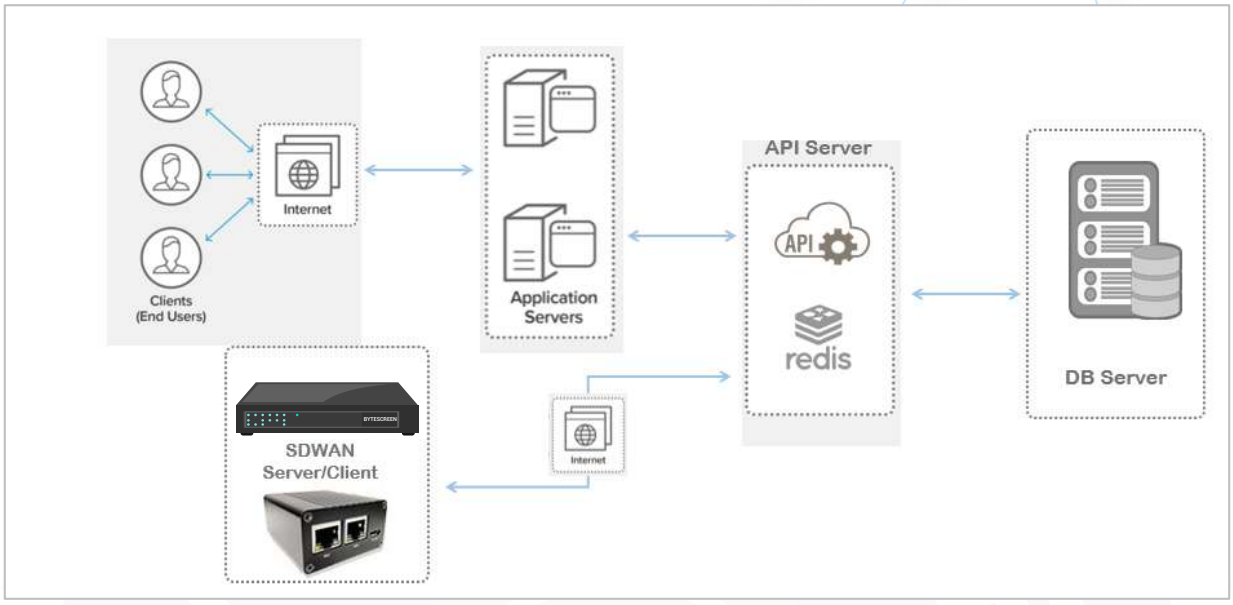
Typical Orchestration Architecture on cloud

Standard AWS setup-based design. Depending on the clientele, it can also be done on a single instance. Additionally, if necessary, this may be scaled both horizontally and vertically.



Typical Orchestration (FusionMaestro) Architecture on-premise

On premise setup explained as given, in this setup the entire components can be deploy in one system also. This can small to medium scale organization setup.



Terminology

SD-WAN

A software-defined wide area network (SD-WAN) is an automated, virtualized service that manages enterprise network connectivity and extends enterprise networks across globe. WANs use links such as multiprotocol label switching (MPLS), wireless, broadband, virtual private networks (VPNs) and the internet to give users in remote offices access to corporate applications, services and resources, allowing them to work regardless of location. SD-WAN monitors the performance of WAN connections and manages traffic in an effort to maintain high speeds and optimize connectivity thus delivering high-quality user experience, which helps boosts business productivity, agility and reducing overall IT costs.

ZTP – Zero Touch Provisioning

Zero-touch provisioning (ZTP) is a way of configuring devices/CPE that automatically configures the device when it is turned on and connected to the internet.
ZTP aids in the rapid deployment of CPE in a large-scale setting by reducing the majority of the human effort needed in connecting them to a network.

Concentrator (FusionConnect)

FusionMaestro deployed at a data center can function as a headend Gateway Concentrator.
The Concentrators aggregate traffic from all branch offices.
Branch Gateways establish secure tunnels L2/L3 to one or more headend gateways over the Internet or other networks.

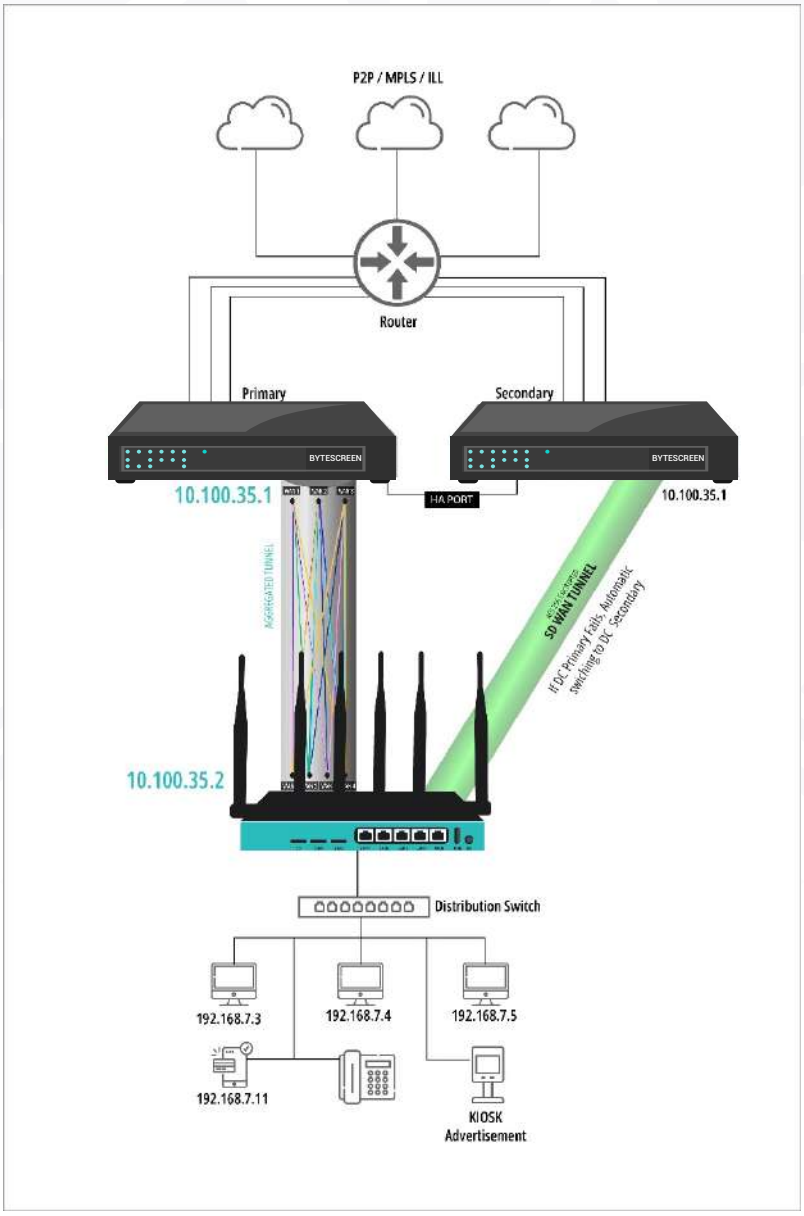
Tunnel / Tunneling

Tunneling, is the transmission of data intended for use solely within a private, generally corporate, network across a public network in such a way that the public network routing nodes are ignorant that the transmission is part of a private network.
FusionMaestro Software Defined Wide Area Network (SDWAN) tunnel create over IP Security Protocol (IPSEC), and Multiprotocol Label Switching (MPLS)

HA

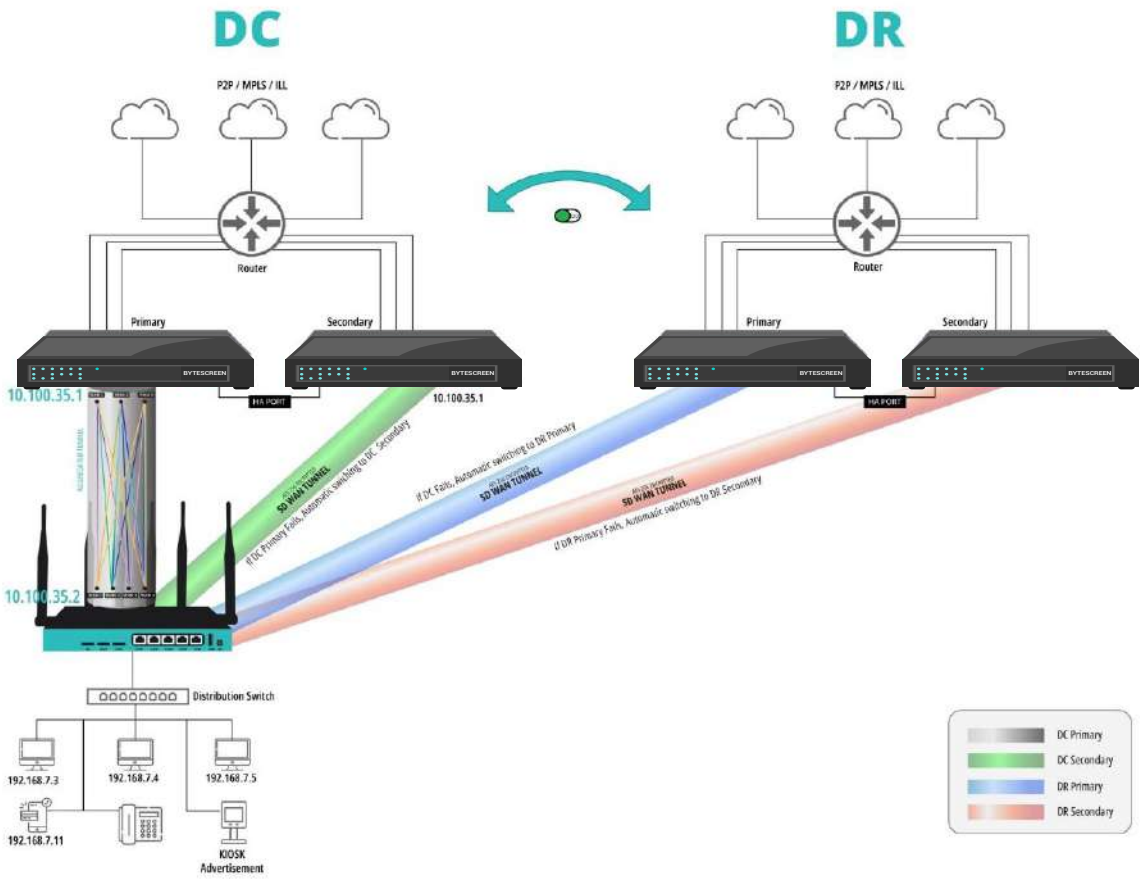
Concentrator (FusionConnect) can be deployed as failover cluster, so if primary concentrator down with any reason, then secondary will take place automatically based on defined HA or failover port. This will ensure almost always available all the services connected using concentrator and accessed by many connected users via CPE's.

The typical architecture as given



DC / DR

A disaster recovery (DR) site is a facility that a company may employ to recover and restore its technological infrastructure and operations if its primary data center fails.
FusionConnect concentrator can be configure and deploy with DC / DR setup. Here is the typical architecture diagram for the same.



Hardware Requirements - FusionMaestro

This is to explains the minimal software and hardware requirements for orchestration deployment.
Prior to scaling out, it is important to observe the performance of pilot projects to determine the requirements.

Typical hardware requirement for 500 CPE

1. Orchestration Server
   - 8 [Physical] / 12 [VM] - cores
   - 16 GB RAM
   - 500 GB HDD Disk Space
   - Operating System: Centos 7.X

2. API Server
   - 8 [Physical] / 12 [VM] - cores
   - 24 GB RAM
   - 500 GB HDD Disk Space
   - Operating System: Centos 7.X

3. Database Server (VM Instance)
   - 16 [Physical] / 24 [VM] - cores
   - 64 GB RAM
   - 1000 GB HDD Disk Space
   - Operating System: Centos 7.X
   - Database: MySQL and MongoDB

Hardware Requirements - FusionConnect

This is to explains the minimal software and hardware requirements for concentrator deployment. This is support up to **100 CPE**.
Prior to scaling out, it is important to observe the performance of pilot projects to determine the requirements.

- 4 [Physical] / 8 [VM] - cores
- 16 GB RAM
- 120 GB HDD Disk Space
- Minimum 2 ethernet ports
- OS – Customize from BYTESCREEN

Hardware Requirements – CPE

x86 Based

CPU	INTEL Celeron/ i3 /i5 Processor
RAM	DDR3 (8 GB)
Graphics Card	Intel HD, Support 1080P
Onboard SATA	2*SATA Slots 1*MINI SATA (120 GB mSATA SSD HDD) 1*Mini PCI-E
Expansion Slot	1*SIM Card Slot
Network Card	6*Intel 82583V Gigabit Card
Rear Panel I/O	1*Power Button 1*DC Port Power & SATA Lights 2*USB 2.0
Chassis	1U Rack Mountable /Industry grade

MIPS

Protocol	IEEE802.11n/g/b/a/ac IEEE802.3/802.3u/802.3ab
Wireless speed	Dual frequency up to 1200Mbps
Work frequency	2.4GHz&5.8GHz
Interface	1 USB 2.0 interface, 1 TF card interface Power,2.4G,5.8G, PCIE
LED	4G signal 1, 4G signal 2,
Antennas	4pcs 7dbi high-gain 4G antennas 2pcs 10/100/1000M WAN port Auto MDI/MDIX 3pcs 10/100/1000M LAN ports Auto MDI/MDIX 1 DC slot 2pcs SIM card slot 2pcs Built-in PCIE slot
Button	1*Reset button
Power supply	DC 12V/2A
Max power consumption	≤20W
Size(L*W*H)	165MM * 235MM * 23MM (case size)

SD-WAN Tunnel differentiator

Why Dynamic Routing protocol required to run SD-WAN efficiently for all providers.
On concentrator WAN side for tunnel formation required dedicated IP. Redundant and dedicated IPs generally required BGP.

Generally, the LAN side also required Dynamic Routing Protocols. Because all SD-WAN Providers create a tunnel basis of the load balancer. Using multiple underlay links, they create multiple overlay tunnels. Every overlay tunnel has different overlay IPs. Managing traffic flow between multiple overlay links and multiple overlay IPs it's required a Dynamic Routing protocol (BG-

BYTESCREEN SD-WAN is a very unique proposition
On concentrator can connect multiple WAN sources (ILL/P2P/MPLS) and can use in aggregation mode. So automatically WAN redundancy will be achieved.

Over SD-WAN overlay tunnel is also aggregated packet-wise multi-session. Multiple sessions will be in one single overlay tunnel with one static overlay IP. All load balancing with multiple links happed in one overlay tunnel. So, we don't require additional Dynamic Routing Protocol to achieve redundancy and optimal performance of SD-WAN.

Advantages and Benefits

- Low Hardware resources (Dynamic Routing Protocol required high hardware resources)
- Easy to deploy and manage
- Don't require high technical resources

BYTESCREEN Feature Listing

SDWAN Tunnel

Application-aware routing

Application-aware routing only routes traffic on designated WAN links.
Traffic is routed automatically to WAN lines with the necessary network specifications & path conditions to enable these real-time applications.

Advantages and Benefits

- Some latency-sensitive applications can benefit from a low-latency circuit (P2P/MPLS).
- Application-aware routing improves application performance.
- Traffic may be balanced across the available WAN circuits more effectively.

Application priority

When several users utilise multiple apps in the aggregated tunnel, traffic will flow on a first-come, first-served basis. This might have an effect on the performance of some mission-critical applications.
Priority may mark DSCP on the packet as a priority using the Application. Priority application packets might thus be sent first, followed by ordinary application packets.

Can specify numerous priorities based on the criticality of multiple applications.

Advantages and Benefits

- Multiple application traffic can be managed efficiently with a limited number of tunnels.
- Best performance for mission-critical applications

Virtualization

Virtualization is similar to container virtualization. Logical separation of LAN and WAN ports on a concentrator or CPE device to prevent intruders from accessing the LAN side of the host.

Overlay refers to the network connection of application servers or endpoints via an overlay tunnel.

A network that connects numerous sites and allows for data access via different applications, one of which is infiltrated by an attacker. In such a circumstance, the intruder may be able to abuse one service and progress to other services, or perhaps compromise the entire system.

To reduce this danger, virtualization isolation can create a safe environment.

Key Security Features

- Stateful FW on WAN - Allows or denies specific network traffic based on policies configured
- Brute force protection - Blocking specific IP's or traffic based on pattern (no. of attempts etc.) of password access/change
- DDOS prevention
- SPAM control
- URL filter
- Local DNS
- RoadMap
  - IPS/IDS
  - End-point security
  - Geofencing

Concentrator Connectivity

WAN: Static and DHCP (Maximum 3 wan can connect)
Can connect ILL/MPLS /P2P (Any multiple combination)
LAN: DHCP/Static

CPE Connectivity

WAN: Static and DHCP (2 wired WAN and two 4G LTE Sims)
Can connect ILL/DHCP/PPPoE/MPLS/P2P/4G LTE
LAN: DHCP/Static

Overlay Tunnel

Packet-Based Multisession Aggregated Tunnel, whenever a request for application access is initiated from the CPE side, the request will split into multiple packets. These packets will get routed from multiple links of multiple sessions.
All multiple sessions are aggregated in one single tunnel with one single static overlay IP. These packets are re-ordered once they reach the concentrator end and the request gets delivered.

Advantages and Benefits

True aggregation between all available links between Concentrator and CPE, Not load balancer like other providers

2. Big advantage for In-Premises implementation

    a. Assured uptime because of multiple links
    b. Not Required:
        i) Dynamic Routing Protocol (BGP/OSPF/RiP etc)
        ii) AS Nos and Static Public IP's
        iii) ISP or Telco Dependency

3. Biggest advantage is assured tunnel uptime

    a. Connected with multiple links, therefore failure of any one WAN link of a con centrator or CPE, will not affect Tunnel connectivity. So tunnel will be always up and running.
    b. Once WAN links back and is active it will automatically get added in Active Tunnel without disconnection of Tunnel.

4. Available all multisession traffic in one single overlay tunnel with one single overlay static IP

    a. Efficient utilization of all available links
    b. Simple static route
    c. Complex and hardware-hungry Dynamic Routing Protocol is not required at all.

Encryption (AES 128-bit and AES 256-bit encryption)

Per session optional AES 128-bit and AES 256-bit encryption with encryption key lifetime
Inside aggregated packet-based multisession tunnel can apply optional AES 128-bit or AES 256-bit encryption and can define per session encryption key lifetime for dynamic key rotation.

Advantages and Benefits

1. Based on requirements can define AES 128-bits or AES 256-bits encryption
2. Per session provides the highest security of data traffic (Multiple sessions and multiple encryption keys)
3. It is not one single Encryption key for the entire tunnel.
4. Highest multilevel packet level Encryption protection
5. Per session encryption key can be rotated based on the time interval for more strong encryption security

Tunnel Rate limit

Can define the size of the Tunnel as per the requirement

Advantages and Benefits

1. Biggest advantage is to balance actual available underlay bandwidth with overlay tunnel for efficient tunnel performance

Domain Based Tunnel

The tunnel can be established based on a domain name instead of an IP

Any SD-WAN concentrator would need a static public IP for CPE device to reach and create tunnel. This at times becomes a challenge to manage in case of change in public IP at server end and would call for a need to change/update the IP on all CPE devices to re-create tunnel with new IP.

To simplify this, our solution offers domain-based tunnel wherein the public IP can be mapped to a domain name and tunnel shall be created using domain name instead of IP address.

This will avoid huge overhead efforts of updating all CPE devices with new IP address every time there is a change in public IP address at concentrator side.

Advantages and Benefits

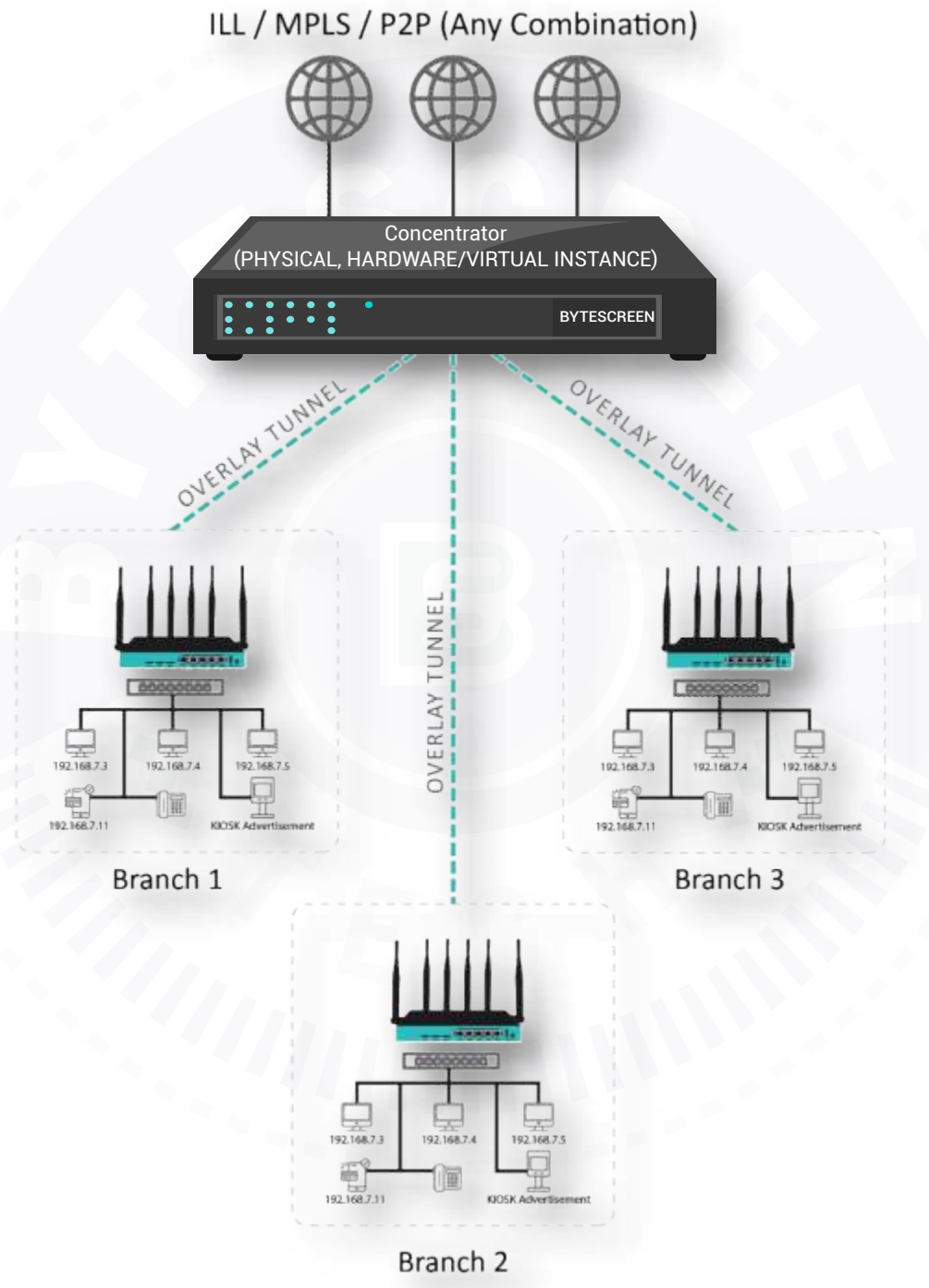
1. No IP dependency means no Telco /ISP dependency
2. IP can be changed as per requirement
3. No need to remember IP at Client side

Network Topology

SD-WAN solution supports all types of network topology

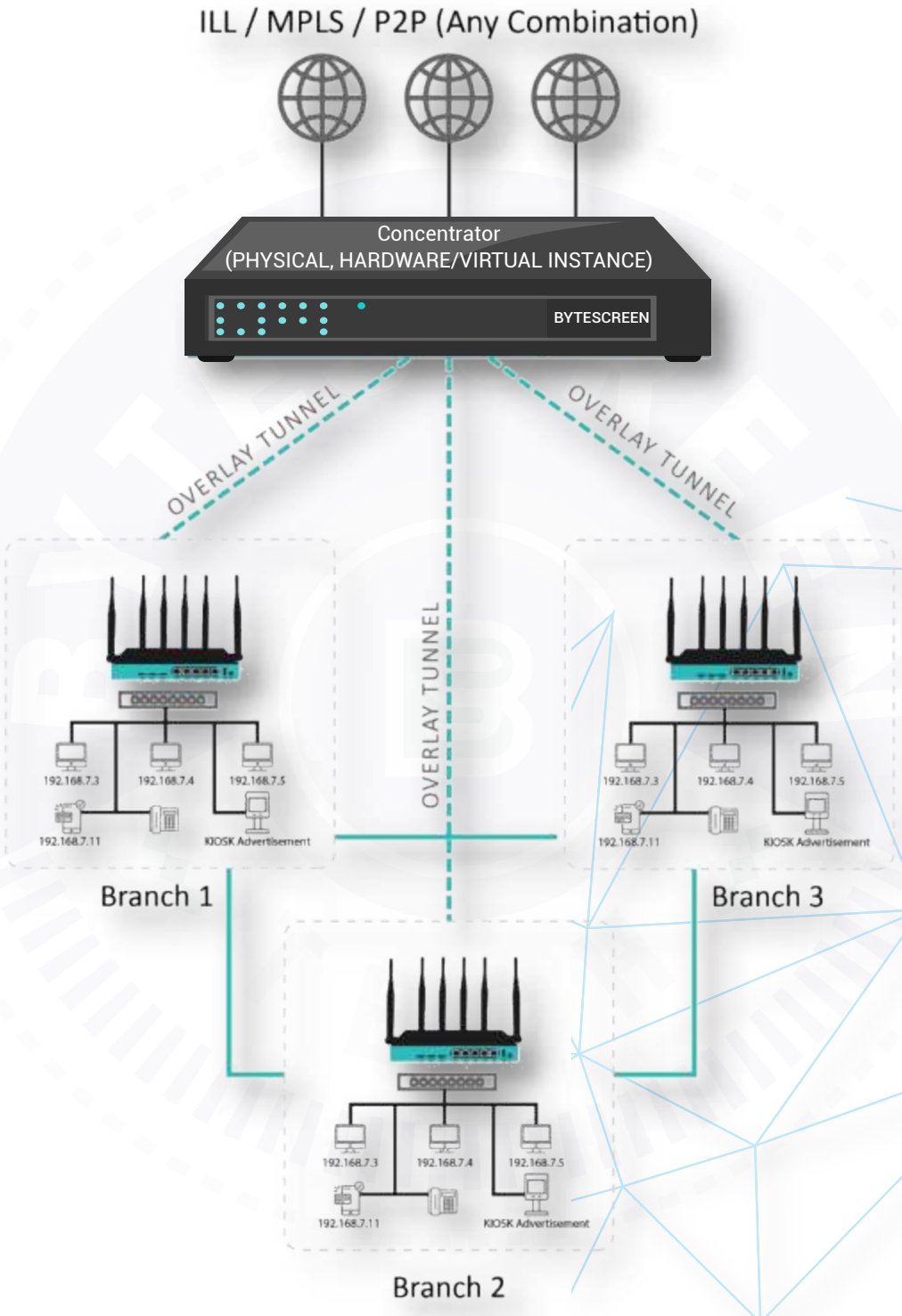
Hub and Spoke

Communication between HUB locations to spoke location for application access. All spoke will communicate from HUB only.



Full Mesh

Communication between HUB and Spoke location as well all clients will communicate with each other directly.



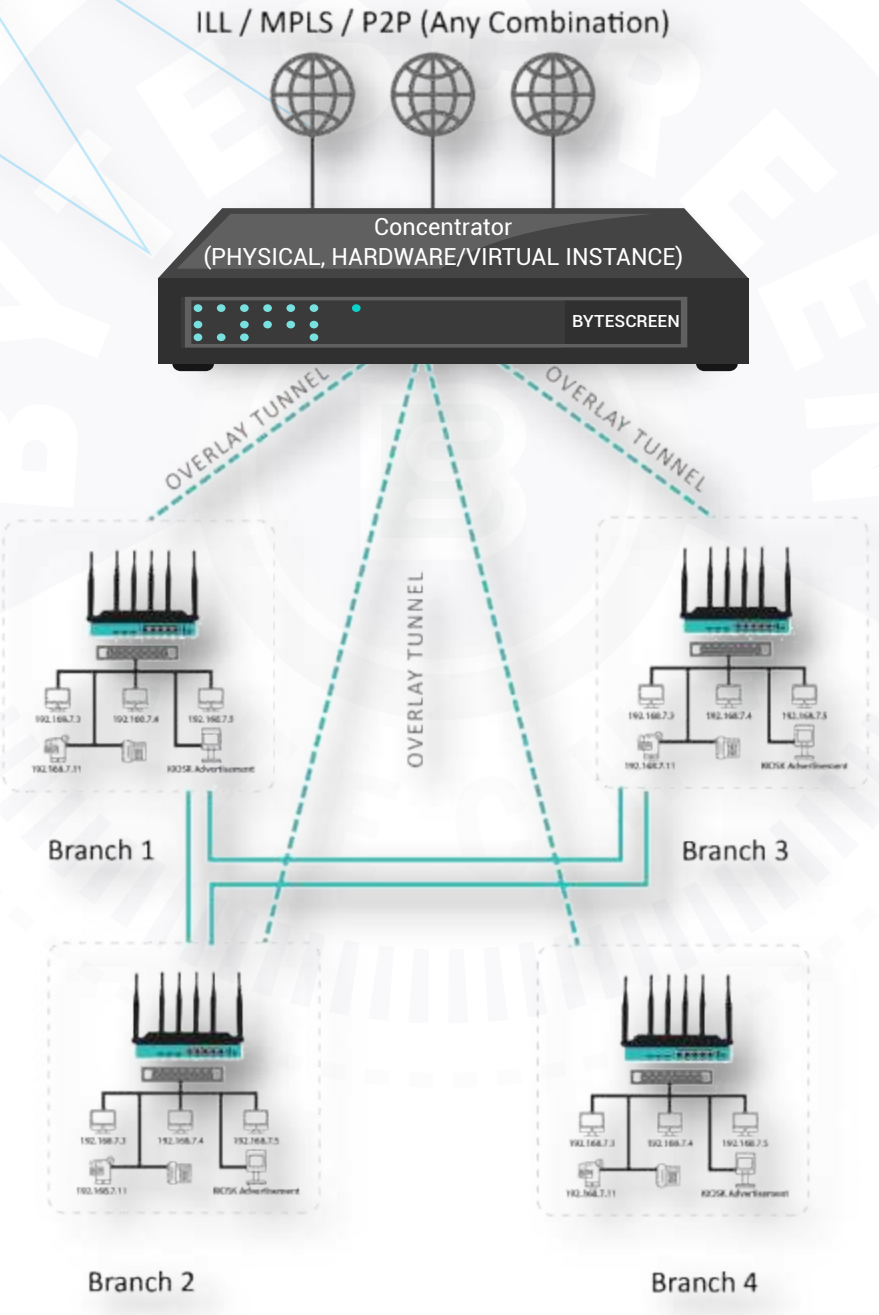
Partial Mesh

Communication between HUB and Spoke location as well all clients will communicate with each other directly.

- Communication between HUB and spoke location as well few defined client locations can communicate with each other in defined groups.
- Multiple groups of clients will only communicate with HUB as well among their defined groups only.
- Two groups of clients will communicate with each other in a HUB and Spoke mode.

Advantages and Benefits

With single solution can configure different scenarios as per require



Packet Redundancy and Packet de-Duplication

Whenever a request for application access is initiated from the CPE side, the request will split into multiple packets. These packets will get routed from multiple links of multiple sessions.

The packet duplication mechanism does packet duplication and keeps duplicate packets on multiple links as redundancy. Suppose while getting a response of packet from any WAN link goes down, the solution senses that and initiates a duplicate packet from another link and gets a response from that packet.

The entire tunnel is packet-based and multi-session. Other packets get responses correctly and Duplicate packets will get responses late. In this scenario, the solution will mark duplicate packets as Dup and do packet reordering and delivery without losing any data.

Advantages and Benefits

a. Zero Data loss

Zero-touch provisioning (ZTP)

Wan optimization

-Multi Hybrid Internet
(ILL, PPPoE, DHCP, 4G LTE)

- Algorithm based Internet
  - o Aggregation and load balancing
  - o Fastest Response
  - o Round Robin
  - o Least Used
  - o Overflow, Enforce

- Group Wise Aggregation
  - o Failover
  - o Fallback

- Intelligent WAN
  - o Auto ISP / TELCO detection
  - o Latency, Available bandwidth on port
  - o RTD based link health checkup & selection
  - o Traffic monitoring
  - o SIM signal strength with SIM details

- User Bandwidth Management
  - o IP Wise rate limit
  - o Application wise QoS
  - o Application based priority
  - o Priority over other IP

- Security
  - o Domain Filter
  - o IP Whitelisting

- WiFi Management
  - o Dual Band WiFi
  - o User connectivity visibility on both bands
  - o WiFi Scanner for minimizing interference
  - o DHCP reservations
  - o WiFi Stealth Mode

CPE/Controller Connectivity to Orchestration

Any CPE can connect with relevant orchestration using http protocol over rest API using the specified points. SSL is recommended to secure connection between CPE and appropriate orchestration.

- Preinstalled CPE/Controller firmware
- CPE/Controller MAC address
- Product code generated from orchestration
- Company Code generated from orchestration
- Basic configuration

CPE/Controller Update

Once the CPE/Controller begins communicating with the orchestration, the orchestration informs the CPE/Controller to fetch the available firmware depending on the CPE/Controller hardware and current firmware version.

Once the firmware has been downloaded to the CPE/Controller, the CPE/Controller will be updated with the new firmware.

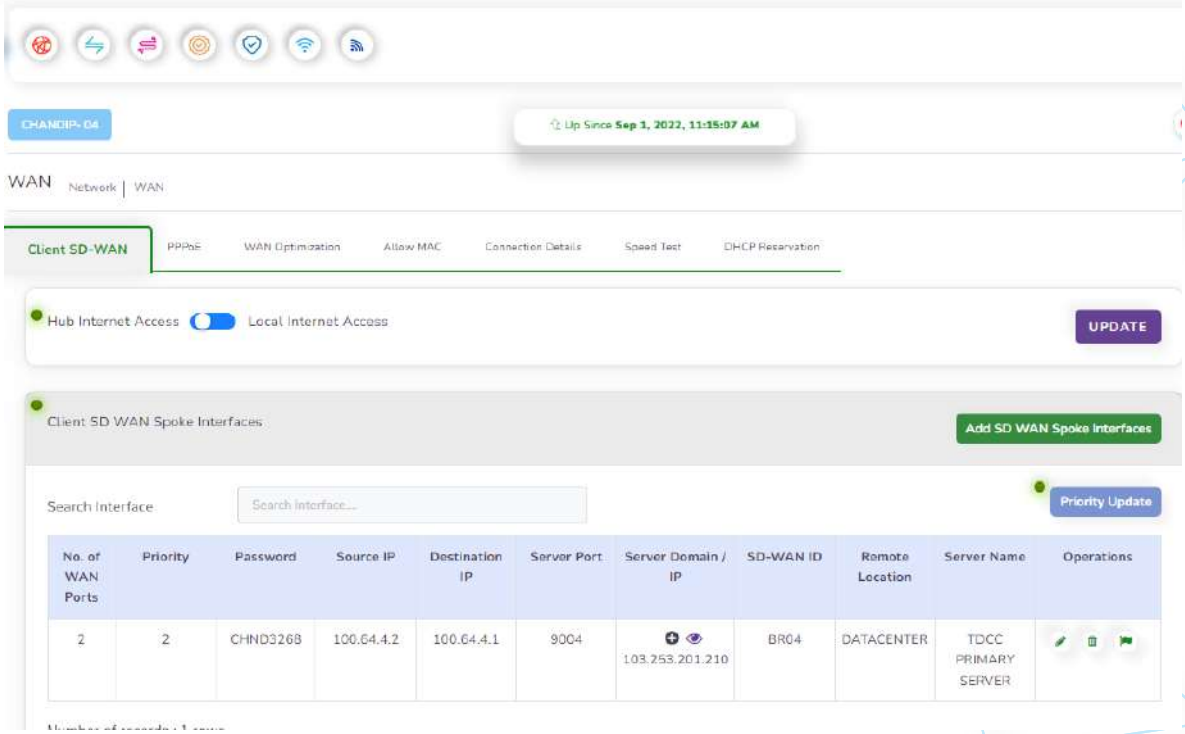
If a network outage occurs during the download, the CPE/Controller will continue to operate using the existing firmware with no impact on the CPE.

CPE/Controller Configuration

CPE/Controller setup can be done individually as well as in bulk [under development]. This may be done both online and offline.

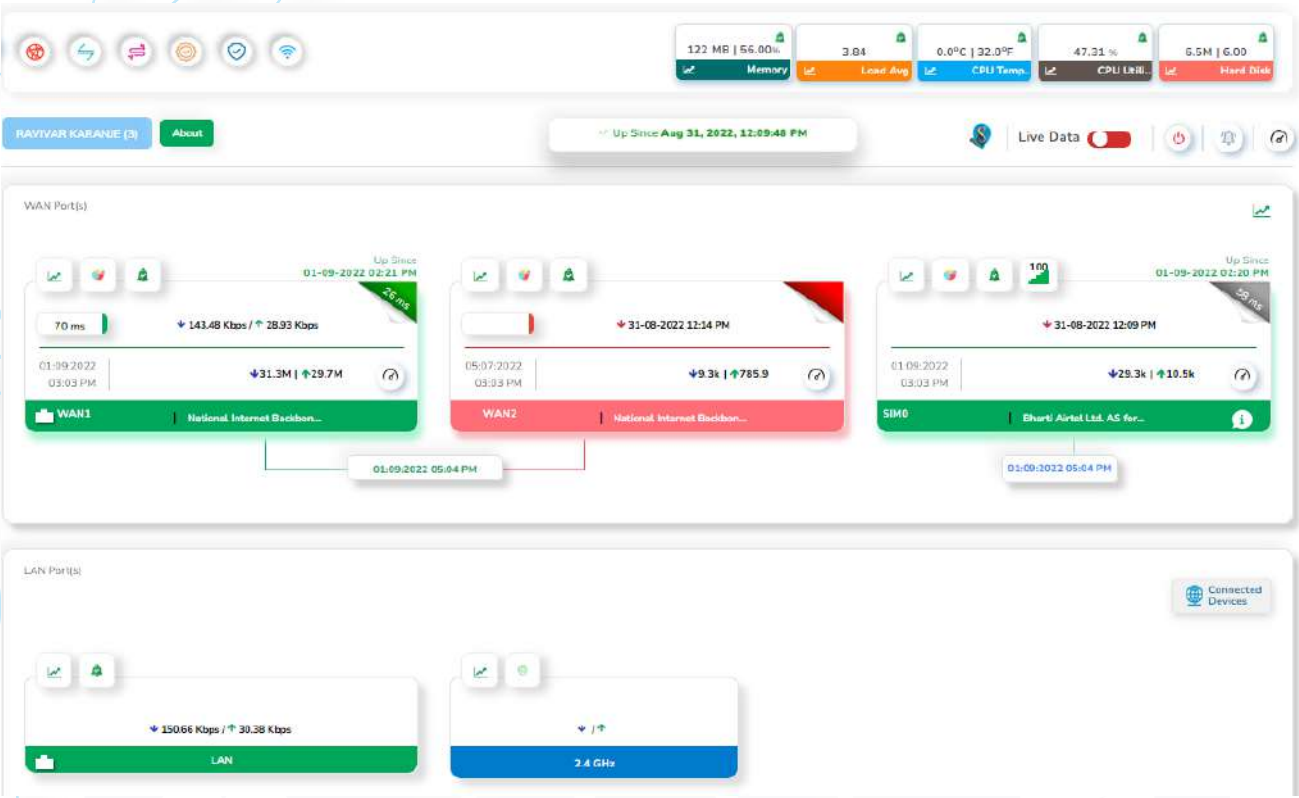
If you configure offline, anytime the CPE/Controller communicates with the orchestration, the orchestration informs the CPE/Controller of the new configuration that is accessible with orchestration.

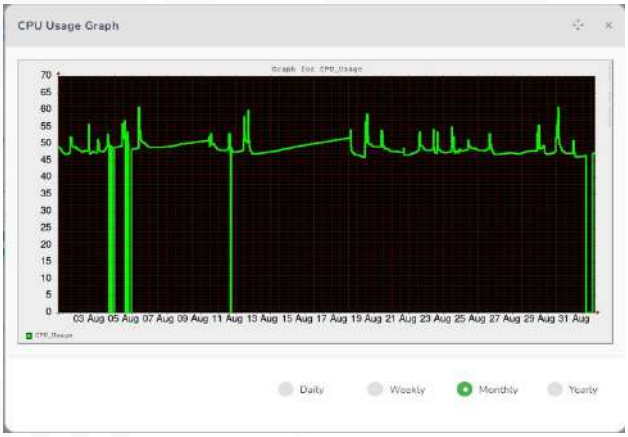
Typical screen for configuration



CPE/Controller Monitoring

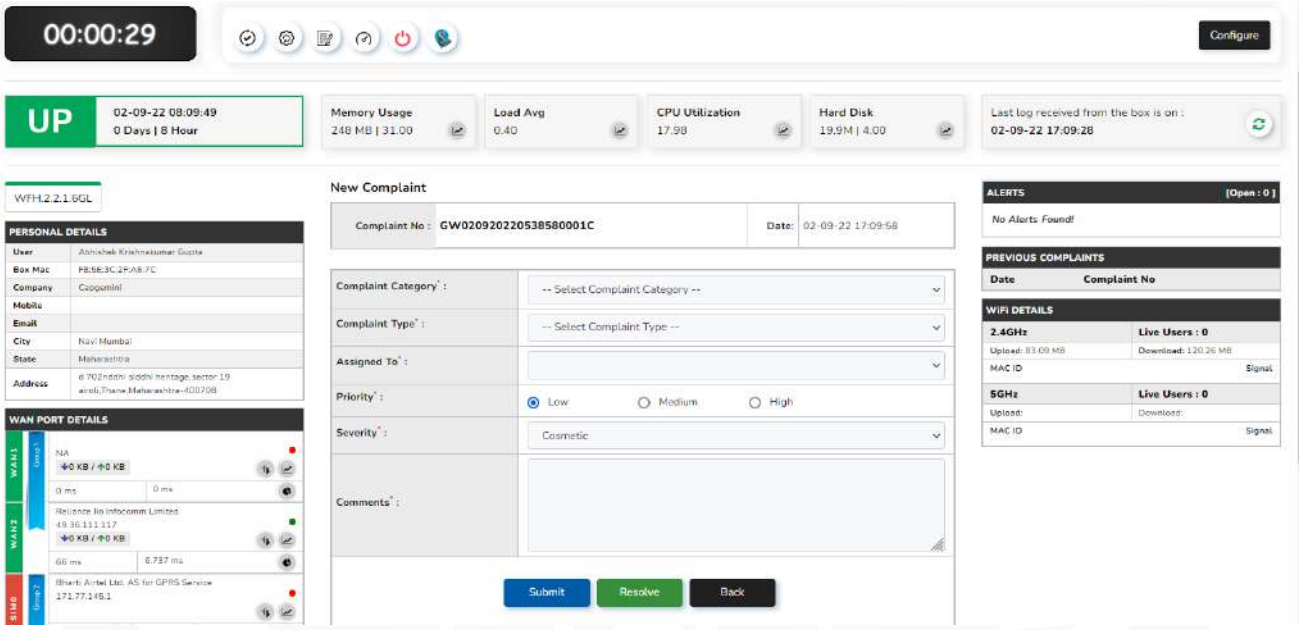
CPE/Controller monitoring is strengthened with a 360-degree dashboard view that includes analytics and status. Monitor remote devices and offer high-level information on device status. Create an alert and send it to the associated shareholder by SMS or email..





Support

Support team can check the entire details related to any CPE/Controller just on one click and see if any issue on the box. Also support can update / change any configuration and alert setup to push to BOX or inform to orchestration to perform the task if such scenario come again.



FAQ

Work from Anywhere

Five features of this device or why should I use this device over my existing router?

a) ZTP (Zero Touch Provisioning)
b) WAN1+WAN2---> Aggregation
c) SIM1+SIM2---> Aggregation
d) Centralized Monitoring
e) Managed Services
f) WIFI Management

- How to connect WIFI from Desktop?
  You can connect WiFi Adapter with your desktop and configure WFA SSID + Passkey on it for using WIFI on desktop.

- Why reboot WFA after SIM insert?
  The SIM has to latch onto the nearest available network tower; hence a restart is required in a live scenario.

- How to use existing WIFI extender with WFA device?
  WFA SSID and Passkey has to be configured on the WIFI extender console.

- Will WFA work if 5G is introduced?
  Currently this box supports 4G LTE SIM module. Once 5G is introduced and 5G module is available for the chipset, we can replace it.

- Why power backup option is not provided or can it be provided?
  Currently this is not available with WFA, if required, you can purchase WIFI router backup (UPS).

- What is the range of the antennas
  Upto 50meters in open radius

Note: Line of sight should be clear with no obstacles.

- How to/Can I change WIFI SSID and Passkey?
  Two ways: Either talk to company admin or share us your details to change.

- How to/Can I change WIFI SSID and Passkey with WIFI extender?
  WFA SSID and Passkey has to be configured on the WIFI extender console.

- How to use SD Card and USB slot?
  That feature is not available.

- How much temperature can the box sustain?
  Operating temperature: -10° ~60°
  Storage temperature: -40° ~70°
  Operating Humidity:10%~90% non-condensing
  Storage Humidity:10%~90% non-condensing

  Power adaptor range?
  20V or 2A

- Antenna exchange, will it work?
  No antenna exchange does not work
  4 4G labelled antennas to be fixed at the back and 2 Wifi band labelled antennas to be fixed on both sides of the device.

- If I want to see the orchestrator how to do it?
  Talk to company admin

- How to directly connect internet link with WFA device
  This is a ZTP device which means you do not have to disturb your existing internet setup. This device will work along with your router.

  If you want to directly connect WFA with internet link for PPPoE user, then fix the internet cable to any of the WAN ports of the WFA device. Add the username and password on Orchestrator and ask your ISP (Internet Service Provider) to reset the MAC to connect to the internet.

- On which technology does this device work?
  Share email id, send WFA feature list document.

- How will I know if my broadband plan or SIM is expired?
  Connection details (complete plan details like plan name, plan expiry date etc.) for both SIM and broadband can be setup on the orchestrator portal.
  Alerts can be generated and sent to the end customer based on these details

- How can I prioritize and check the software/APP?
  Prioritization of apps can be done from orchestrator portal by admin

- How can I monitor the bandwidth usage?
  Through orchestrator portal which offers MRTG (Multi Router Traffic Grapher) Graph port wise.

- I am having 2 SIM of different providers but whenever I do Speed test it only shows 1st provider but not the 2nd one
  We really do not know what mechanism speed test works on and how it captures the IP

- Either or both (2.4GHz or 5GHz) SSID not showing
  Check whether antenna is properly fixed on both sides of the device, these antennas detect the WIFI range

- How to insert the second sim?
  To insert SIM, slide the SIM card carefully into the card slot (the cut-off corner facing inward) until it clicks in place. Reboot the box immediately to detect SIM.

Note: Do not try to forcefully push the SIM card in the slot as this may result in the card getting stuck in the slot.

- LED status not showing properly
  As soon as box is powered on,
  PWR LED turns green
  After approx. 40 secs, 5.8GHz & 2.4GHz turns green
  Subsequently, 4G1 & 4G2 LEDs will start blinking

- How is signal strength calculated? And what is the signal strength marking for a good inter net speed?
  50% and above

- WIFI Speed on both bands
  2.4GHz-----> up to 50Mbps
  5.8GHz-----> up to 300Mbps

- How much time does it take to communicate between the physical box and orchestrator portal or why does it take time for data to reflect on the orchestrator portal?
  Monitoring: approximately 30secs
  Configuration: up to 3mins
  Reboot and firmware upgrade: Up to 15mins

- How does physical device connect with orchestrator portal?
  Through APIs

SDWAN

SR No	Question	Root Cause	Troubleshooting	Resolution
1	My internet is not working	1) Tunnel Down 2) PPPoE credentials mismatch 3) Internet Down, LED blinking	1) Check tunnel on Orchestrator- SDWAN Interfaces- Tunnel Visibility Either or both TX(bytes) or RX(Bytes) will show zero value 2) Check whether PPPoE credentials are correct	1) On WAN Interface > Update Client SDWAN Spoke Route (Wait for 3mins) 2) If still Tunnel is down escalate to L2
2	How to insert Sim in SIM slot	SIM Insert in CPE		To insert SIM, slide the SIM card carefully into the card slot (the cut-off corner facing inward) until it clicks in place. Reboot the box immediately to detect SIM. Note: Do not try to forcefully push the SIM card in the slot as this may result in the card getting stuck in the slot.
3	My application not working	1) Tunnel Down 2) Application not reachable	1) Check Application reachability (ping application IP)	1) On WAN Interface > Update Hub Internet Access (Wait for 3mins) 2) If still Tunnel is down escalate to L2
4	My device's LED not blinking	Device hang	1) Check on UI whether Latency is red 2) Check tunnel, it will show green	Ask customer to pull the adaptor cable from the device and fix it again, wait for device to show up on orchestrator
5	Fluctuating Internet	ISP link fluctuating	1) Unplug plug WAN link 2) Disconnect ISP link and check whether site working on SIM	Contact ISP for internet fluctuation check
6	Internet not working on SIM	SIM Data Exhausted	On Orchestrator, check whether port is up and latency is red 1) If Airtel SIM, check on CMP fro SIM data 2) If other SIM, check with customer whether there is data and ask them to renew	Recharge SIM Card

BYTESCREEN Tech Pvt. Ltd.

BYTESCREEN Tech Pvt Ltd stands firm in our mission to redefine the landscape of networking solutions through innovation, reliability, and customer-centricity. We are committed to pushing the boundaries of technology to deliver products and services that not only meet but exceed the evolving needs of our clients. As we continue to evolve and grow, our dedication to excellence remains unwavering. We invite you to explore our comprehensive range of networking solutions, tailored to empower businesses of all sizes and industries to thrive in the digital era. Whether you're seeking robust security measures, seamless connectivity, or advanced management tools, BYTESCREEN Tech is here to support your journey towards success.

Contact Details:

For inquiries, collaboration opportunities, or to learn more about how BYTESCREEN Tech can elevate your network infrastructure, please don't hesitate to reach out to us.

www.bytescreentech.com