Managed Emergency Call Handling
VIPER Service Guide

Contents

1.0 INTRODUCTION

This Service Guide describes CenturyLink's VIPER Managed Emergency Call Handling Solution (VIPER – MECH).

2.0 SOLUTION OVERVIEW

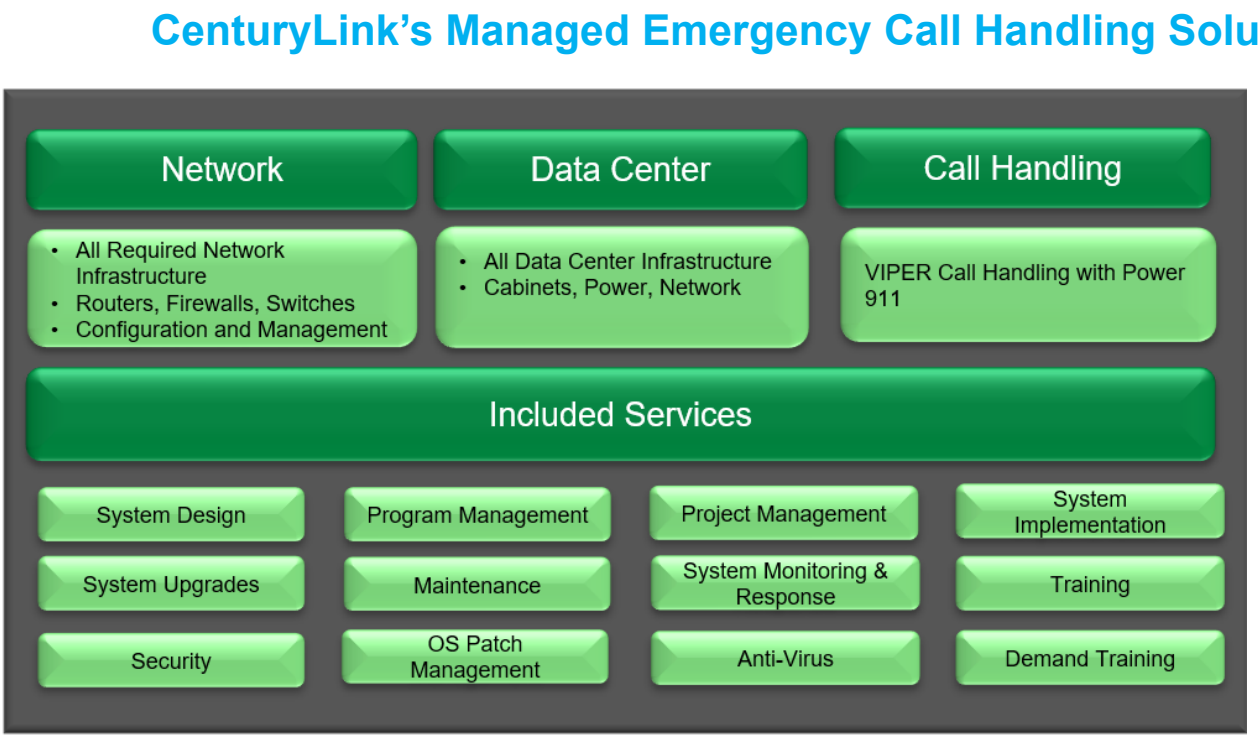
VIPER Managed Emergency Call Handling services offering is a configuration of specialized NG9-1-1 Customer Premises Equipment (CPE) and NG9-1-1 Call Management applications deployed in a Hosted Geo Diverse multitenant architecture and provisioned to serve multiple customer Public Safety Answering Points ("PSAPs"). The PSAPs can be distinct agencies, onboarding to the shared platform at distinct points in time

VIPER Core Call Processing, ALI Controllers, and Management servers resides in CenturyLink Data Centers; VIPER Call Taker CPE sits in the PSAP. Management of the Call Taking equipment is provided through the host over a dedicated Virtual Private Network (VPN).

The Services will support up to 150 call handling endpoints (Power 911 positions, optional IP phones) on a given multi node VIPER instance. CenturyLink will deploy additional multimode VIPER core instances for the next bank of 150 positions.

The Services will use current mainstream releases (VIPER v5.1 or later, Power 911 v6.4 or later).

3.0 VIPER MECH BUNDLE – INCLUDED SERVICES



3.1 Included: VIPER Call Handling Feature Set

Services use the following mainstream releases:

- VIPER v5.1 or later paired with Power 911 v6.4 or later

- Power StationTM Gen3 call handling stations at the PSAP positions

Functionality is as published by Intrado for these releases (Product Bulletins and User Guides)

3.2 Included: Satellite VIPER Node ("SVN")

SVN (at PSAP location)

- SVN with dual softswitches for enhanced survivability of local call flows in the event of loss of connectivity with Core Equipment facilities.

3.3 Included: Sentry Monitoring & Response

- Included in per seat pricing
- Use the following mainstream release: Sentry v2.2 SP2 or later
- Core equipment equipped with Sentry Server Console (Sentry-based monitoring)

3.4 Included: Patch Management and Anti-Virus

- Included in per seat pricing
- This service leverages Intrado's Customer Care Access

3.5 Included: CenturyLink Services

CenturyLink has a fully dedicated team to support all VIPER MECH customers. This team includes staff to perform following functional roles and responsibilities

- Program Management – Manager Technology Management
- Project Management – Lead Project Managers
- NOC Surveillance – Operations Technicians
- Technical Support, engineer design, lifecycle – Sr Lead and Lead Engineers
- Service Manager, Carrier Manager – Sr Network Analyst
- Reporting, SLA, Record, Inventory, Training – Analyst II

Included with VIPER MECH, CenturyLink provides the following design, implementation, training, security, management, and maintenance services:

- System Design
- System Configuration
- System Application Change Management (Example: Adding or removing users)
- System Implementation
- System Upgrades
    - CenturyLink will upgrade VIPER major release software at a minimum once per year.
    - All VIPER software is tested in CenturyLink labs before it is approved for field use. VIPER software will not be updated in the production environment until CenturyLink Support Engineers approve for field use (AFU)
    - If Core Equipment or PSAP Equipment needs to be upgraded or replaced to support release software
- System Maintenance (Includes preventative maintenance)
- System Training – New
- All new systems include the following training
    - Administrative Training on VIPER and Power 911
    - User Training on VIPER Power 911 or Train the Trainer so PSAP can provide their user training
- System Training – Refresher & Demand (Webex)
- System Monitoring and Response

- 7 x 24 x 365 Staffed Network Operations Center
- Security – CenturyLink Managed Adaptive Network Based Security
- VPN Access, Firewall, Malware scanning

3.6 Included: CenturyLink's Public Safety CPE ESInet for VIPER 9-1-1

Provides network connectivity between PSAPs and Host VIPER over a secure private network

- CenturyLink's carrier grade IQ Private Port MPLS network provides all layer 3 connectivity between VIPER Core Multi node hosts and remote PSAP VIPER Positions
- Local access to PSAP from the CenturyLink Private MPLS backbone can be delivered over a variety of transports types. This can include:
  - NxDS1 – supports 1.5mb to 10.5mb
  - Ethernet Local Access (ELA) – Supports up to 1G
  - Wave Local Access (WLA)
  - Optical Wave Services (OWS) – Supports up to 10G
  - Optional Geo-Max – were available
  - Layer 2 and Layer 3 Connectivity between Data Centers – Ethernet or OWS
- CenturyLink will system tag and physically tag all NG911 circuits

CenturyLink provides all routers, firewall, core and VIPER switches at the core data centers and PSAP locations.

3.7 Included: CenturyLink Tier 3 Data Centers

CenturyLink provides Tier 3 Data Centers for hosting VIPER Multi Node Core CPE

4.0 VIPER MECH – OPTIONAL ADD ON APPLICATIONS and COMPONENTS

CenturyLink provides the following VIPER applications and components at an additional MRC. Some of these applications / components may also include an NRC at startup

4.1 VIPER Applications

4.1.1 Optional Add On: MapFlex 911 – with West Data Update Service

MapFlex 911 uses the following mainstream release:

- MapFlex 911v5.4 or later

Functionality is as published by Intrado for these releases (Product Bulletins and User Guides

This option does not require MapSAG (MapSAG provides the customer additional capability for GIS Data Editing, Discrepancy Management, and MapFlex Data Updates). In lieu of MapSAG, GIS-SER-UPDT is included with this MapFlex 911 Option, whereby Intrado GIS Ops and the Help Desk perform data updates for the customer. 4 updates are included, and customer can purchase additional or do it themselves. For an alternative option that leverages MapSAG instead, see option below.

4.1.2 Optional Add On: MapFlex 911 – with MapSAG

MapFlex 911 uses the following mainstream release:

- MapFlex 911 v5.4 or later
- MapSAG v6.3 or later

Functionality is as published by Intrado for these releases (Product Bulletins and User Guides
This option includes MapSAG (MapSAG provides the customer additional capability for GIS Data Editing, Discrepancy Management, and MapFlex Data Updates). GIS-SER-UPDT is not included with this MapFlex 911 Option or required.

4.1.3 Optional Add On: PowerOps

PowerOps uses the following mainstream release:

- PowerOps v1.1 or later

PSAPs who desire to configure VIPER ACD must also opt for at least one PowerOps display per PSAP.
Not Included: Large Display. Customer may provide their own large display or CenturyLink can provide pricing and provide upon customer request.
Functionality is as published by Intrado for these releases (Product Bulletins and User Guides

4.1.4 Optional Add On: Power Metrics Advanced

Power Metrics Advanced uses the following mainstream release:

- Power Metrics

Functionality is as published by Intrado for these releases (Product Bulletins and User Guides

4.1.5 Optional Add On: TXT29-1-1

TXT29-1-1 uses the following mainstream release:

- TXT29-1-1

Functionality is as published by Intrado for these releases (Product Bulletins and User Guides

4.1.6 Optional Add On: Power Locate

Power Locate uses the following mainstream release:

- Power Locate

Functionality is as published by Intrado for these releases (Product Bulletins and User Guides

4.2 Optional VIPER Add On Components

- VIPER Gateway Shelf
- Admin Interface Module (AIM)
- CAMA Interface Module (CIM)
- 48V Power Supply Module
- Mediant 1000B Prebuilt Building Block
- Mediant 1000 Spare Part Digital Voice Module Single Span
- Mediant 1000 Access License (per chassis)

- SNOM Admin Phones
- 3rd Party Recording Kit (License to connect Non-Intrado Recording)
- 3rd Party SIP Interface
- ECCP Workstation License
- 24 Button External Keypad
- 48 Button External Keypad
- KVM – 2 Port
- KVM – 4 Port
- Touch Screen Monitor

4.3 Other Optional Add On Equipment and Services

If customer has special need for equipment and / or services not listed above, CenturyLink can provide this equipment and / or service at a monthly recurring charge upon customer request. CenturyLink will retain ownership and provide all repair and replacement of defective equipment for the term of the contract. These requests would be configured to meet the specific need of the PSAP. Therefore, all pricing for these requests would be done as an ICB (individual case bases)
Example of equipment would include:

- PSAP front or backroom UPS
- Non-standard sized monitors
- Additional Time Sync devices

Example of services would include:

- Back and front room network cabling
- Electrical
- Removal of decommissioned equipment

5.0 ARCHITECTURE

5.1 High Level Design

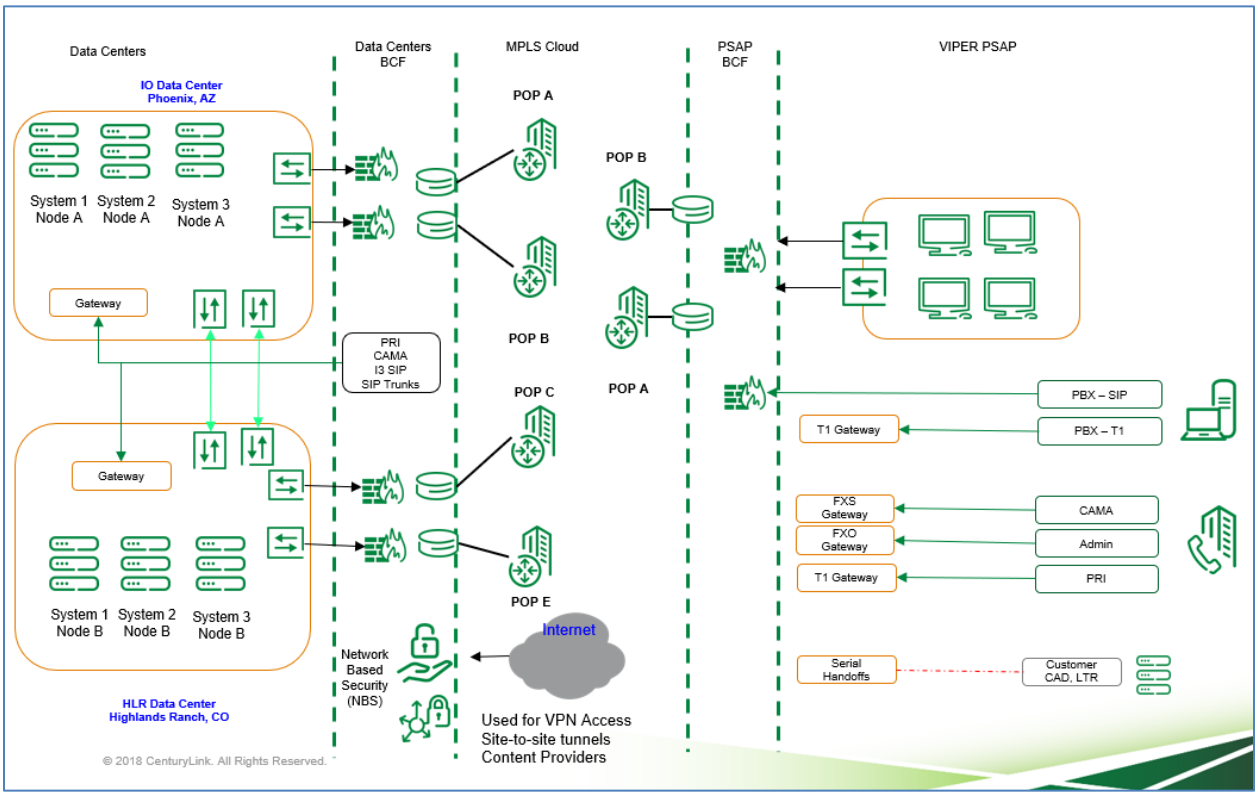


Figure 5.1 – High Level Solution Design

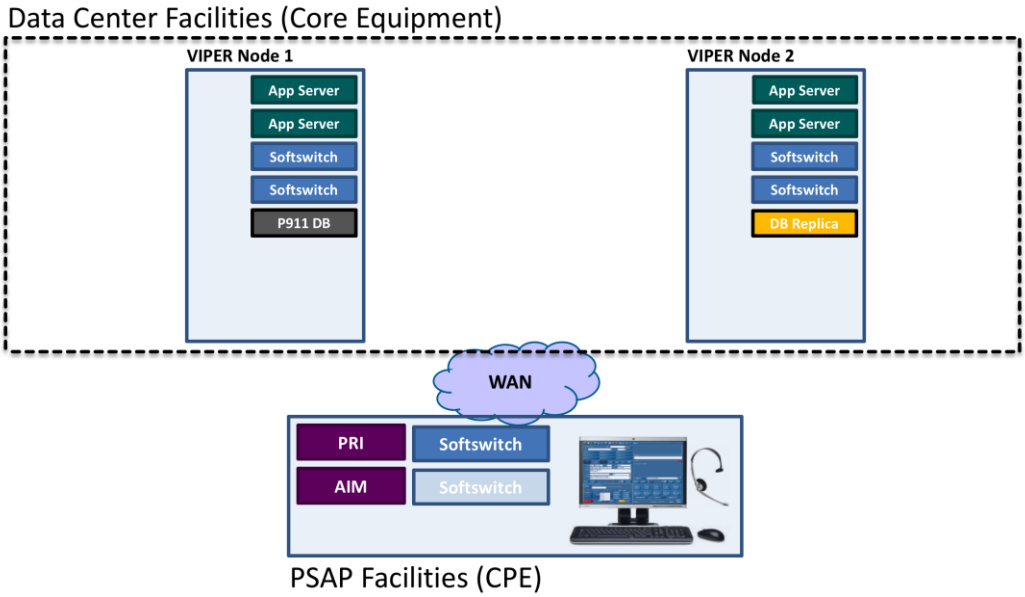
5.2 VIPER Core Equipment

VIPER is deployed in a Geo Diverse Multi-node configuration. Node A resides at one physical data center and Node B resides at a second geo-diverse data center. VIPER nodes are deployed to run in active-active mode. Each VIPER node has a local set of redundant servers for added resiliency.
CenturyLink is responsible for all preventative maintenance activities on all VIPER Core Equipment including software management. CenturyLink will refresh Core Equipment every seven years or sooner if required.
VIPER Host equipment is deployed as a Geo-Diverse multitenant system. The CenturyLink **Managed Emergency Call Handling Solution** includes the following as required for each host data center:

- Co-Location Space for host system components
- All racks and power requirements
- VIPER and Power 911 Application Servers
- Network Management Server
- Master Time Clock – Each host system
- Peripherals – KVM and monitors
- Backup Devices
- LAN switches
- Routers
- Patch Panels
- All cabling

5.3 PSAP VIPER CPE

- PSAP may order services for up to 150 PSAP front-room positions serviced from each multi-node VIPER system instance
- CenturyLink / Intrado will own all PSAP CPE
- If PSAP CPE must be repaired, CenturyLink will repair or replace the PSAP CPE during the service contract term
- CenturyLink is responsible for all preventative maintenance activities on-site, including software management



5.4 CenturyLink's Public Safety CPE ESInet for VIPER 9-1-1

Provides network connectivity between PSAPs and Host VIPER over a secure private network

- CenturyLink's carrier grade MPLS network provides all layer 3 connectivity between VIPER CPE hosts and PSAP remote VIPER CPE
- Supports all Intrado network requirements
- Local access to PSAP from the CenturyLink MPLS backbone can be delivered over a variety of transports types. This can include:
  - NxDS1 – supports 1.5mb to 10.5mb
  - Ethernet Local Access (ELA) – Supports up to 1G
  - Wave Local Access (WLA)
  - Optical Wave Services (OWS) – Supports up to 10G
  - Optional Geo-Max – were available
  - Layer 2 and Layer 3 Connectivity between Data Centers – Ethernet or OWS
- CenturyLink will system tag and physically tag all NG911 circuits

5.5 Core Network (VIPER Core ESInet)

CenturyLink deploys a secure, private, and fully diverse network within the VIPER core infrastructure utilizing our IQ Private Port MPLS (Multiprotocol Label Switching) and OWS (Optical Wave Service). All Core MPLS and OWS circuits are deployed on CenturyLink fiber

Diverse IQ Private Port MPLS circuits are installed at each data center and provides the connectivity from the VIPER Host to the VIPER MPLS cloud for remote PSAP connectivity. Network design for VIPER host data centers exceeds five-9s of reliability.

5.6 DataData Centers

All NG9-1-1 Managed Hosted PSAP CPE equipment will be installed in physical secure cages provided by CenturyLink. Access to these data centers is strictly controlled. Only CenturyLink authorized 9-1-1 support teams will have access to cages where hosted CPE equipment is located.

5.6.1 Data Center Infrastructure Included:

- All required network extensions from Data Center carrier “meet me rooms” to CenturyLink CPE cages
- All equipment cages and racks
- Power and UPS
- Backup Power and UPS
- Network Timing Solution
- Premium Level Data Center Support
- All installation and maintenance

5.6.2 Data Security

5.6.2.1 Physical Security

All solution data is stored and backed up in CenturyLink data centers. Primary storage and backup devices are placed in CenturyLink secure cages. Access to these secure cages are limited to only authorized CenturyLink 911 support teams. All vendors must be escorted by CenturyLink 911 technicians.

5.6.2.2 Data Backups

CenturyLink backs up all system and customer data as required by manufacture best practices. Backup devices are installed and located at each data center to ensure data preservation. Only authorized CenturyLink 911 support teams and manufacture can physically access these devices and the data contained on devices

5.6.2.3 Data Access

All customer (PSAP) data is stored in separate security domains, or sites, and each PSAP can only access their data. However, with proper authorization from each PSAP, permissions may be configured granting other agencies or entities access to PSAP data. This may be useful when a State or regional entity requires access to all PSAP MIS data. Federal Government compliance will require CenturyLink to obtain permission from each PSAP. Only after permission has been received by CenturyLink from the PSAP, will CenturyLink configure the permissions for other entities to access this data.

5.6.3 Data Center Network

CenturyLink has provided two fully diverse 1G MPLS over WLA (Wave Local Access) for all routed layer 3 ingress / egress traffic at each data center for VIPER 9-1-1
CenturyLink has provided four 1G OWS circuits for layer 2 connectivity between data centers. These are configured in two separate link aggregation pairs and each pair are fully diverse
VIPER ESInet – All VIPER host to remote traffic is routed over a pair of diverse 1G MPLS circuits at each data center.
Data Center to Data Center Connectivity – CenturyLink deploys a pair of diverse link aggregated layer 2 OWS circuits for Data Center to Data Center Connectivity

5.6.4 In Production Data Center Locations

CenturyLink has two data centers deployed and in production

- **Data Center 1:** IO Data Center – Phoenix AZ
- **Data Center 2:** Highlands Ranch Data Center – Highlands Ranch CO

911 traffic is delivered to these two data centers over the CenturyLink i3 NGCS ESInet. The i3 NGCS ESInet terminates at each data center where it passes calls into the CenturyLink Managed Emergency Call Handling solution.
The CenturyLink i3 NGCS ESInet is not part of the Managed Emergency Call Handling Solution. CenturyLink can provide a bundle offering at customer' request.

5.6.5 Optional Data Center Deployments

Optional regional data center deployments will be considered. Building new data center infrastructure will be done at additional cost to customer. Depending on deployment model and committed seats, CenturyLink may cover part or all of the data center infrastructure build.

5.7 PSAP Network (VIPER Remote PSAP ESInet)

Each VIPER remote site will be served by a pair of redundant IQ Private Port MPLS circuits. Remote PSAP network design will meet five 9s reliability. Pricing for local, last mile diversity can be provided upon customer request.

With the CenturyLink Managed Emergency Call Handling solution, CenturyLink will provide all connectivity from the PSAP to the CenturyLink CPE NG9-1-1 ESInet. Providing a resilient diverse or redundant connection from CenturyLink MPLS POPs to the PSAP is very dependent on existing local service providers network. CenturyLink will make every attempt to ensure a minimum redundant set of circuits from a pair of PRIV routers at CenturyLink POPs through LEC network to the PSAP.

Where diversity or redundancy is not present, CenturyLink will advise customer of design limitations and optional solutions. All costs for deploying an optional solution would be the customer's responsibility.
Drawing 5.7a – CenturyLink preferred design
Drawing 5.7b – Only 1 Meet Point is available
Drawing 5.7c – Only 1 Meet Point and CenturyLink POP is available

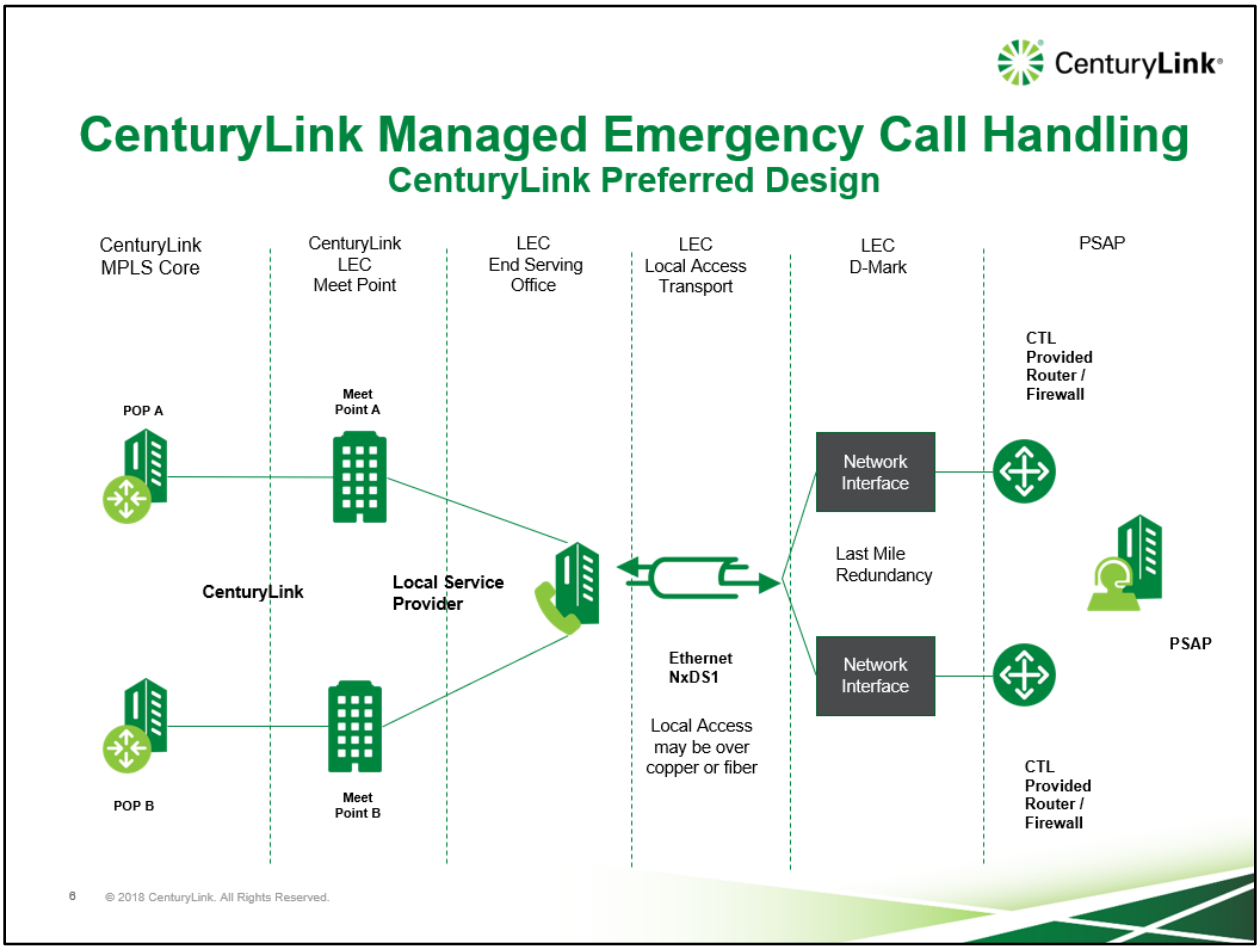

CenturyLink
CenturyLink Managed Emergency Call Handling
CenturyLink Preferred Design
CenturyLink MPLS Core
CenturyLink LEC Meet Point
LEC End Serving Office
LEC Local Access Transport
LEC D-Mark
PSAP
CTL Provided Router / Firewall
POP A
Meet Point A
Network Interface
Last Mile Redundancy
CenturyLink
Local Service Provider
PSAP
Ethernet NxDS1
Local Access may be over copper or fiber
Network Interface
CTL Provided Router / Firewall
POP B
Meet Point B
6
© 2018 CenturyLink. All Rights Reserved.

Figure 5.7a

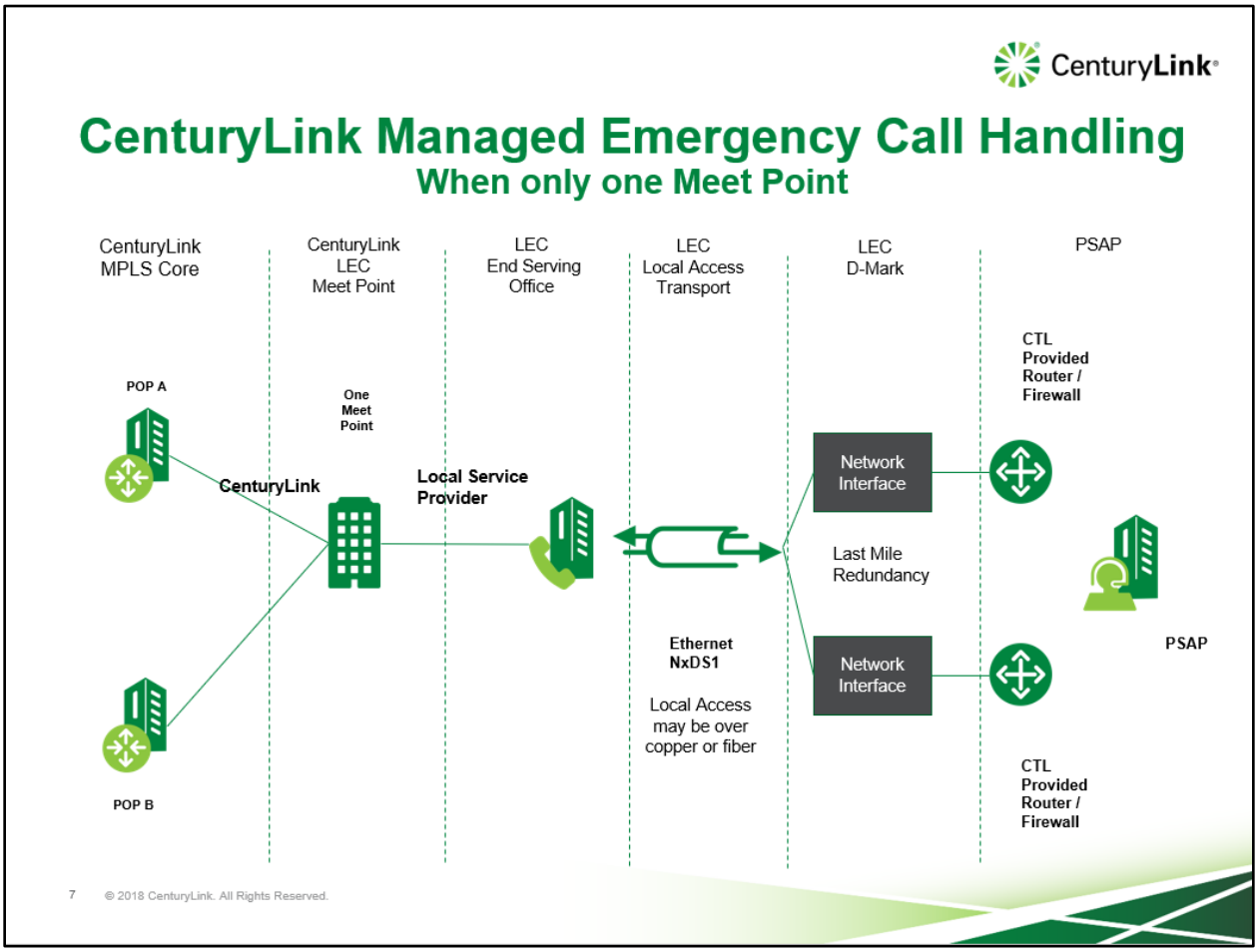

CenturyLink
CenturyLink Managed Emergency Call Handling
When only one Meet Point
CenturyLink MPLS Core
CenturyLink LEC Meet Point
LEC End Serving Office
LEC Local Access Transport
LEC D-Mark
PSAP
CTL Provided Router / Firewall
POP A
One Meet Point
CenturyLink
Local Service Provider
Network Interface
Last Mile Redundancy
Ethernet NxDS1
Local Access may be over copper or fiber
Network Interface
PSAP
POP B
CTL Provided Router / Firewall
7
© 2018 CenturyLink. All Rights Reserved.

Figure 5.7b

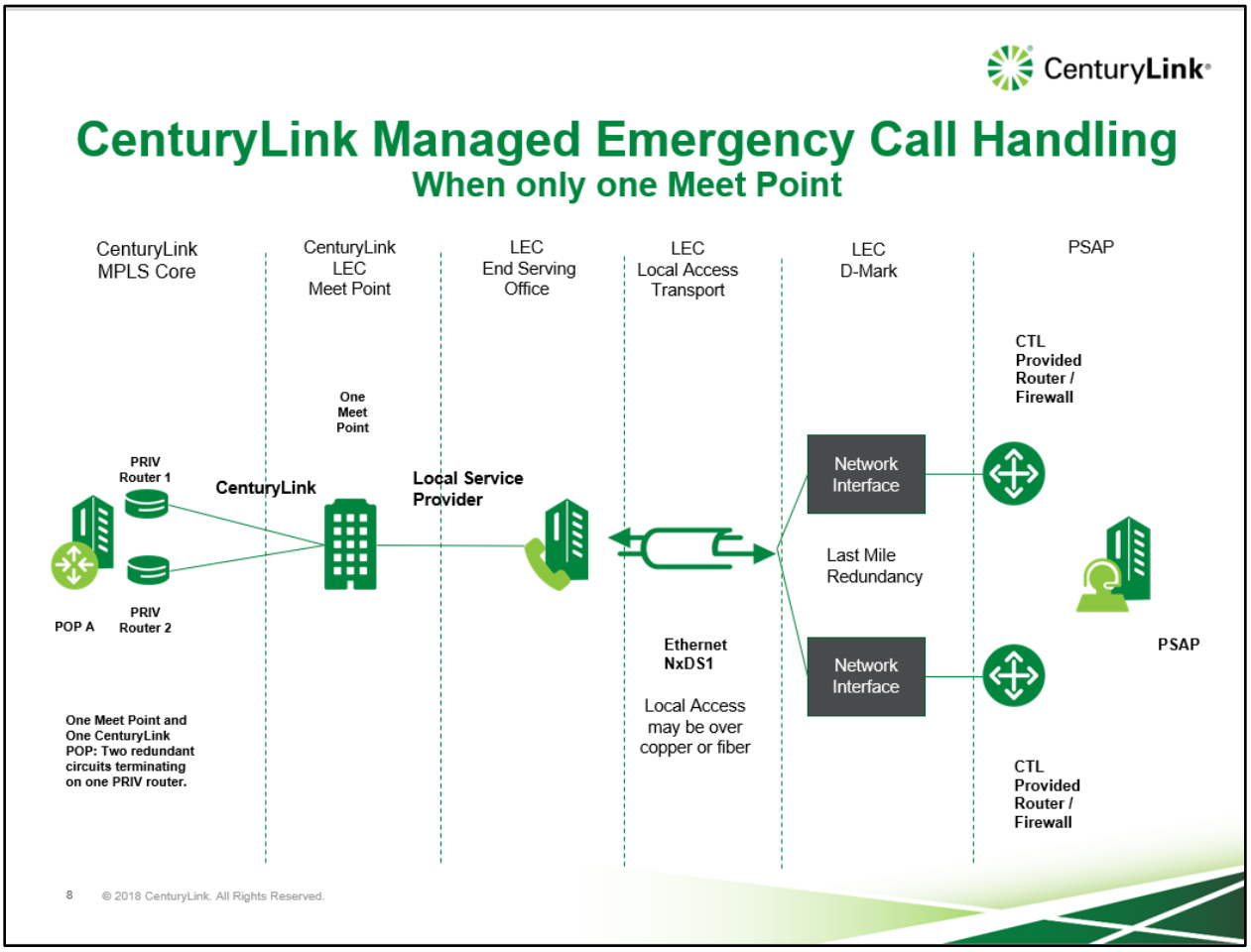


Figure 5.7c

5.8 PSAP Bandwidth

PSAP bandwidth is dependent on several variables that will be taken into consideration during PSAP design. The variables that need to be consider include, but may not be limited to:

- Position Count
- Conferencing
- On-Net Transfers
- Roaming or Hot Seating
- Admin Lines – including termination points
- Content Services (Rich Media, Video, Sensor Data, etc.)

All these services can impact the number of Concurrent SIP Sessions (CCS) and bandwidth requirements. PSAP bandwidth needs to be sized to handle number of CCS and overhead for system applications, control, and management.

5.9 Legacy E9-1-1 and NG9-1-1 Core Services

CenturyLink's Managed Emergency Call Handling Solution does not include legacy E9-1-1 service or NG9-1-1 i3 Core Services. CenturyLink does provide all CPE hardware and CPE configuration services where customer's E9-1-1 services or/and NG9-1-1 services will terminate.

5.9.1 Legacy E911 Services

E9-1-1 CAMA trunks may be installed to one or both VIPER Equipment Cores or directly to the PSAP, terminating on VIPER CAMA Interface Modules (CIM). Legacy ALI circuits must be installed to the VIPER Core Equipment. Customer is responsible for all costs to extend their Legacy E911 Services to VIPER data centers and Core Equipment Cabinets within the data centers.

5.9.2 PSAP NG911 Core Services

Any customer NGCS ESInet may be connected to the VIPER Managed PSAP solution if the ESInet provider has been certified to work with VIPER NG9-1-1 systems. Customer is responsible for all costs to extend their NGCS ESInet to VIPER data centers and Core Equipment Cabinets within the data centers

CenturyLink offers NG911 Core Services with existing connectivity into the VIPER Core datacenters. CenturyLink can provide optional pricing for these services upon customer request.

6.0 SYSTEM CONFIGURATION, INSTALLATION, MAINTENCE

System installation is included with per seat pricing

Responsibility Matrix

Project Management	CenturyLink with PSAP Support
Project Plan	CenturyLink
System Architecture	CenturyLink / Intrado
Network Architecture – WAN/Transport	CenturyLink
Network Architecture – VPER CPE LAN at PSAP	CenturyLink / Intrado
Core Equipment facilities (Data Centers)	CenturyLink
PSAP Facilities	PSAP
PSAP Facility Site Preparation (floor space, power, etc.)	PSAP
PSAP Facility Project Survey for PSAP CPE	CenturyLink / PSAP
Project Survey Analysis and Report	CenturyLink
Project Survey Guideline and Documentation	CenturyLink
Site Readiness as addressed in Project Survey Analysis and Report	PSAP
PSAP Data Collection, Configurations/Lists-Star Codes, Transfer, Contact List, etc.	CenturyLink / PSAP
Receiving and unloading equipment shipped to CenturyLink Core Data Centers	CenturyLink
Receiving and unloading equipment shipped to CenturyLink Core Data Centers	CenturyLink
Core Equipment install and maintain at host	CenturyLink

Provide, monitor, and maintain facilities for Core Equipment	CenturyLink
PSAP CPE – Install and maintain at PSAP facility	CenturyLink
Core Equipment – Stage, configure and ship	CenturyLink / Intrado
PSAP Equipment – Stage, configure and ship	CenturyLink / Intrado
Training	CenturyLink
Pre-production and end-to-end testing	CenturyLink / PSAP
Develop migration plan and execute migration testing	CenturyLink / PSAP
Service production turn-up	CenturyLink / PSAP
Monitoring, maintenance and operational technical support for all elements of Core Equipment and PSAP CPE	CenturyLink
Network monitoring and maintenance	CenturyLink
Upgrades	CenturyLink
Log storage and backups	CenturyLink
Problem reporting	CenturyLink
Tier 1 problem triage and resolution	CenturyLink
Tier 2 problem triage and resolution	CenturyLink / Intrado
Network capacity management	CenturyLink
MPLS network capacity management	CenturyLink

6.1 Intrado VIPER Network Requirements – CenturyLink Network Compliance

CenturyLink's MPLS and OWS networks meets and exceeds all Intrado published network requirements. The network will meet the following requirements:

- ❑ Layer 3 routing will be provided between all locations;
- ❑ Certified CAT5e/CAT6 between all network switches;
- ❑ Guaranteed Bandwidth for all VIPER applications-Bandwidth requirements for each PSAP deployment;
- ❑ Low Latency (< 40ms desirable);
- ❑ Low Jitter (< 5ms desirable);
- ❑ Support for Quality of Service ("QoS") as needed;
- ❑ Security against intrusion and virus attack;
- ❑ Reliable links (fault tolerant)-no single point of failure may cause a Layer 3 disruption for more than four seconds

CenturyLink will provide all network communications equipment, including redundant IP routers, switches, firewalls, etc. to terminate the dual MPLS circuits at the PSAP location
CenturyLink will provide all network communications equipment, including redundant IP routers, switches, firewalls, etc. to terminate the dual MPLS circuits at the location of the Core Equipment.

6.2 PSAP CPE

CenturyLink / Intrado will retain ownership of all PSAP CPE
Customer (PSAP) is responsible for damage to such equipment caused by the PSAP, reasonable wear and tear expected.

CenturyLink will maintain software versions at latest official releases and have been approved for field use by CenturyLink Final Tech Support Engineering

6.3 Call Ingress and Location Methods

A variety of methods can be selected for call delivery and location. Pricing is based on RFAI call delivery environment with legacy ALI and will need to be modified for other environments.

6.3.1 Other Delivery Environment

Services can support operation in a legacy delivery environment:

- Receive a voice emergency call via RFAI (SIP)
- Query an ALI Database for location

6.3.2 i3 Delivery Environment (priced upon request* see note)

Services can also support i3 functions and protocols. As defined within the NENA i3 Reference Architecture, and subject to pre-production interoperability testing, Services will support the ability for the PSAP to:

- Receive a voice emergency call with SIP/PIDF-LO
- Query the ECRF for emergency responder information using the LoST protocol
- Query a CIDB to obtain additional caller information data
- Query a LIS to obtain updated information during a call using the HELD protocol
- Receive/display text emergency call information with PIDF-LO
- Query and display enhanced data information on the PSAP workstation

* Note: Regarding “Pricing upon request”, VIPER software and licenses are included, however delivery design may drive additional costs, generally in relation to network connectivity.

6.3.3 Legacy Delivery Environment (CAMA/ALI) (priced upon request)

Services can support operation in a legacy delivery environment:

- Receive a voice emergency call via CAMA
- Query an ALI Database for location

6.4 System Configuration

This section addresses configuration of the Services

6.4.1 VIPER Configurable Attributes

CenturyLink will use a standard project survey collection form to support the information required to configure Services for each PSAP.
CenturyLink and PSAP will complete list of configurations for each PSAP in accordance with the detailed project plan.

6.4.2 Services Configuration

6.4.2.1 CenturyLink / Intrado Responsibility

CenturyLink and Intrado will support comprehensive system configuration in conjunction with system administrator training and using the CCS (Customer Configuration Service). CCS is a configuration tool designed to understand PSAP operational practices and call flows and joint participation with the PSAP to configure its own Power 911 system. Completed configuration will be uploaded as part of the staging process.

Training on CCS encompasses one day of Administrator training. (Note that ACD design session - if used - is conducted at the same time as the CCS training and encompasses one additional day of Administrator training.)

The CCS is currently a DVD, which includes Power 911 Admin and User Guides, ACD configuration information (used for ACD sites), VMware Player, CCS Virtual Machine, and instructions on how to install the VMware player and CCS Virtual Machine. This DVD may be used by Channel Partner or the PSAP on its own computer to create the configuration for the PSAP's Power 911 workstations that can be later used in staging.

6.4.2.2 CenturyLink Responsibility

PSAP will provide CenturyLink with support as needed to work with the PSAP to gather the call distribution configuration requested for each PSAP, including ring group or ACD preferences, and rollover tiers.
PSAP will support CenturyLink as needed to work with the PSAP to gather a complete list of configurations for each PSAP. These PSAP configurations lists include:

- Power 911 profile configurations, including screen layout, agency access, transfer profiles, etc.
- Current ALI and NRF response formats

Once installed, CenturyLink Intrado-certified technician technician can then input the desired configuration in the virtual environment and then export the saved configuration file in a format that can be imported into the production environment.

As an output of CCS, CenturyLink Intrado-certified technician will configure Services based on each PSAP's preference for distributing voice calls.

A CenturyLink Intrado-certified technician will configure ACD if the PSAP requests to distribute 9-1-1 voice calls based on the longest idle time, fewest completed calls, or round-robin. PSAPs who elect to configure ACD must also opt for at least one PowerOps server per PSAP.
Alternately, a CenturyLink Intrado-certified technician will configure ring groups if the PSAP requests to distribute 9-1-1 voice calls to all available call takers.

Each ring group or an ACD queue can be configured with an alternate destination that is either another ring group or an ACD queue (rollover tier) for various situations. An agent can be a member of one or more ACD queues; a workstation can be a member of one or more ring groups.

6.4.3 PSAP Management Gateway, Profile

PSAPs will not have access to the VIPER PSAP Management Gateway. For each PSAP, the Power 911 configuration will be set up as a "square" system, meaning that all positions will be presented with the same profile, including screen layout, agency access, transfer profiles, etc. CenturyLink will be responsible for configuration changes for the PSAP once deployed.

6.4.4 PSAP CPE

CenturyLink will provide PSAP CPE, including Power Station Gen3 workstations, backroom servers, peripheral, hardware, and local LAN switches at each PSAP Customer Facility. CenturyLink will be responsible for all installation and support of PSAP onsite Services equipment.

CenturyLink will conduct a Project Survey used to collect customer site data in accordance with two principles: 1) collecting data from site elements (both physical and operational) that are in place at the time of the survey and 2) new elements that will be used within the scope of the project. Based upon the Output of the Project Survey and Analysis Report, CenturyLink will work with each PSAP to determine the appropriate location for the Intrado PSAP CPE.

CenturyLink will conduct a project survey at each PSAP Facility. During the project visit, CenturyLink will assess the PSAP Facility compliance against Services facility requirements and will consult with the PSAP on alternatives and any necessary site changes.

CenturyLink will provide, install, and maintain new LAN connectivity within each PSAP facility for interconnectivity between the Power 911 workstations. Interconnectivity between the Customer provided LAN and and/or the Public Internet is not supported.

Customer will provide and install all cabling to interconnect between position equipment and equipment room components. Upon request, CenturyLink can provide a quote and perform these services for the customer or PSAP.

CenturyLink will engineer Services interconnection with auxiliary equipment, such as CAD and CDR ports per applicable NENA Standards. CenturyLink will provide post-deployment support of the interconnections. The CAD interface is the industry standard RS232C serial interface specification and follows NENA Standard NENA 04-001.

PSAP CPE is privately managed and closed to all third-party software applications (any software not provided by CenturyLink) and internetworking.

6.5 General Facility Requirements

6.5.1 PSAP Responsibility

Each PSAP facility will provide at minimum a 1000VA uninterruptible power supply (“UPS”) equipment for networking and server equipment at the PSAP. Each workstation should be protected with a 650VA UPS or equivalent.
CenturyLink will notify each PSAP of the need to provide CenturyLink / Intrado with the following:

- Security access to each PSAP facility for West personnel or authorized agents
- Ability to freely access all appropriate areas within each PSAP facility
- Parking and building access to move tools and equipment in and out of the facilities
- Secured storage for West-supplied equipment shipped to the PSAP facility in preparation for installation
- Trash and/or recycling removal as needed, including disposal of system packing materials.
- Safe, locked, and limited access to equipment room, including adequate security to prevent theft of computer equipment, tools, test sets, and employees’ personal effects
- Working space, access to computers and other technology, telecommunications equipment, and any other services and materials that may be reasonably necessary.
- 24 x 7 access for problem isolation

6.5.2 Equipment Room

6.5.2.1 CenturyLink Responsibility

For most PSAPs, PSAP CPE located in the equipment room will be installed in one standard 19” data cabinet. PSAP CPE may require additional standard 19” data cabinets at some very large PSAPs.

6.5.2.2 PSAP Responsibility – Backroom Equipment

PSAP will ensure that each PSAP equipment room where the CenturyLink – provided communications equipment rack is located meets the following requirements:

- 24”x 87” of floor space for a West-provided cabinet measuring 24”x 39”
- Floor space within 20 feet of the main telecommunications demarcation point
- 24” of space in front and behind the rack
- 36” between the end of the racks and the wall
- The floor must be capable of supporting 104 pounds per square foot
- Dry, clean, and well ventilated
- Well lit, easily accessible and free from excess vibrations
- The equipment rack should be in an area that does not receive consistent building traffic

In most cases, the back-room PSAP CPE provided by CenturyLink will be housed in one standard 19” data cabinet.

If the PSAP wants to place PSAP CPE into a pre-existing rack, West requires a minimum of nine contiguous rack units of rack space in a single rack, depending on PSAP configuration. CenturyLink will provide the number of contiguous rack units required to the PSAP after completion of site survey and configuration requirements.

PSAP will provide power, ground, and environmental controls for the PSAP CPE to be installed in the equipment room at each PSAP as follows:

- Two dedicated 110volt /20 AMP power feeds are required with A & B feed (separate power source) with receptacle for plug type NEMA L5 20P twist lock
- Any metallic component that is part of the PSAP infrastructure (such as equipment, racks, ladder racks, enclosures, cable trays, etc.) must be bonded to the grounding system
- The facility will have adequate HVAC controls, monitoring and redundancy in order to maintain:
    - Cooling for maximum heat output under full load is 4,000 BTU/hour
    - Data Center HVAC systems must maintain a constant dry bulb temperature between 68- and 77-degrees Fahrenheit
    - Relative humidity between 40% and 55%
- Surge/Lightning Protection

6.5.2.3 PSAP Responsibility – Front Room Equipment

PSAP will need to provide the following space for each Power Station Gen3 station:

- Appliance dimensions are 3”/7.7 cm (Height) x 8”/20 cm (Width) x 10”/25 cm (Depth) (2U metal enclosure).
- 18” x 10” x 21” on the desktop for each monitor.

PSAP will provide power, ground, and environmental controls for the Power Station Gen3 to be installed at each PSAP facility as follows:

- HVAC: Each call taker and supervisor Power Station Gen3 position with two 21” Monitors will dissipate a maximum of 1950 BTUs per/hour.
- A minimum of two 15-ampere circuits to provide diverse power for the Power Station Gen3 station. Each circuit must be wired to an individual 15-ampere circuit breaker. Each circuit must provide two fourplex outlets with individual hot, neutral, and ground wires. One 15-ampere circuit can support up to three Power 911 positions. Workstations should be distributed evenly across the circuits.
- Additional circuits may be required for other non-emergency equipment.
- Each position should be prepared with two (4 x 120 VAC) outlets as follow:
    - Two power receptacles for monitors.
    - One power connector for the PC (NEMA 5 15P).
    - One power receptacle for speakers (for Power 911 ringing)

6.6 Interconnectivity with Third Party Vendor Systems

When installation of third-party vendor systems requires coordination with CenturyLink technicians, CenturyLink will make all reasonable efforts to work with the PSAP to schedule a mutually agreeable time to complete the work. CenturyLink will not provide, install, maintain, or support cabling to connect any components provided by third party vendors. The CenturyLink Project Manager will include this work in the overall project plan and provide coordination.

During the installation of PSAP CPE, PSAP will make all reasonable efforts to have an authorized third-party vendor technician whose equipment will interconnect with PSAP CPE on site during the installation.

If applicable, the PSAP will ensure that a PBX technician is available to work with CenturyLink to make sure that all the phones work together and configure the PBX to interface with the CenturyLink PSAP CPE.

PSAP will provide, install, maintain, and support all cabling to interconnect between any components provided by third party vendors and the Power 911 systems. This includes connectivity to CAD and the Radio system, if any. Interconnection between the Power 911 system and any third-party component that uses an IP interface is not currently supported.
PSAP will work with the CAD system to implement any programming changes required in the CAD system. Services serial interface follows the NENA 04-001 Section 3.4 standard.

6.7 PSAP Training

6.7.1 CenturyLink Responsibility

CenturyLink will provide on-site training for PSAP Call Takers/Dispatchers and Administrators.

6.7.2 PSAP Responsibility

PSAP will provide facilities for each on-site training session. On-site training will be scheduled after the Power 911 equipment has been installed and configured at the designated training location.

PSAP will be responsible for identifying the PSAP training attendees and ensuring they attend the CenturyLink-provided training. PSAP will provide CenturyLink with a complete list of attendees for each training session and their positions a minimum of five business days prior to the start date for each training session. Each PSAP will be responsible for training additional personnel within its organization, as necessary, unless additional Optional Training services are ordered by PSAP from CenturyLink.

6.7.3 PSAP Call Takers / Dispatchers

CenturyLink will provide either PSAP training or train-the-trainer training including:

- Training the Trainer: one on-site training session on six workstations for up to eight PSAP Power 911 call takers/dispatchers. This training is expected to last for two full days (six training hours per day). Training will be provided in train-the-trainer format.
- PSAP Training: in lieu of Training the Trainer CenturyLink will provide all PSAP Training. Training is provided to a maximum of eight PSAP call takers/dispatchers, per training session, with a maximum of two training sessions per day. One workstation for each two students is required. Additional Optional Training days may be purchased to accommodate all call taker/dispatchers.

6.7.4 PSAP Administrators

CenturyLink will provide one on-site training session for PSAP administrators. This training is expected to last for two full days (six training hours per day). PSAP may determine the number and type of employees

attending the CenturyLink on-site training as long as the PSAP provides an adequate training facility and workstations/computers for number of attendees. One day of administrator training is typically used to support the cutover. This training will focus on:

- Power 911
- Optional Managed Services elements such as PowerOps, Power Metrics, and MapFlex 911

6.8 Long-Term Recording Support

Services provide per-position recording interfaces as per NENA 04-002 for analog recording systems of the PSAP's choice.

6.9 Long-Term Recording – IP Recording Solution

Additionally, to standard interfaces per above section, CenturyLink can propose an IP recording solution as a service. Pricing for this solution is on an individual case basis and can be provided after a site survey and capture of the PSAP's total recording requirements.

6.10 CenturyLink Project Plan

CenturyLink will provide each PSAP customer with a customized project plan detailing all CenturyLink and Customer requirements and deliverables.

7.0 SYSTEM TESTING and PRODUCTION MIGRATION

CenturyLink will work with PSAP to finalize and mutually agree on testing and production migration plans for Services. The testing and production migration plans will define:

- Tests to be conducted prior to and as part of migration to Services
- System testing and the production migration for each PSAP
- (Note that Core Equipment purchase includes a required extra position to be located at each
- node for testing purposes)

If requested by CenturyLink PSAP will provide personnel at each PSAP to assist CenturyLink in the execution of the migration testing to:

- Answer the test voice and text calls
- Join conference bridges
- Provide test call screen prints and/or voice recordings/text transcripts to CenturyLink on request (unless PSAP is prohibited by law to do so)
- Provide test call feedback on voice quality, functionality, and other information
- Text call interactions including predefined standard messages

8.0 MONITORING, MAINTENANCE, and OPERATIONAL TECHNICAL SUPPORT

CenturyLink is responsible for all monitoring, maintenance, and operational technical support for all Core Equipment and PSAP CPE.
Maintenance and support include periodic software upgrades, OS upgrades, and other system maintenance as necessary for the operation of the equipment. CenturyLink will notify PSAP before performing any activity that may impact the Core Equipment, PSAP CPE or the Services (including any installations, changes, or upgrades to software, hardware, or network).

CenturyLink provides remote monitoring of all CPE equipment in corporation with West. Alarms are captured and responded to 365 x 7 x 24. Any alarms identified as critical or major, the affected PSAPs will be notified.

Alarms will be resolved remotely and when required, a technician dispatch will be initiated by the CenturyLink 911 NOC.

CenturyLink will provide 365x7x24 monitoring and response of all CenturyLink provided network transport and terminating equipment. All circuits provided by CenturyLink will be both System Tagged and Physically Tagged, identifying them as critical NG9-1-1 infrastructure, ensuring priority response and repair.

8.1 PSAP Obligations

For on-site support services the PSAP will:

- Brief on-site CenturyLink technician on issue(s) and actions taken.
- Allow CenturyLink both on-site and remote access to the System. Remote access is made utilizing a secure VPN to each site.
- Validate issue resolution prior to close of the case.
- Cooperate with CenturyLink and perform all acts that are reasonable or necessary to enable CenturyLink to provide the On-Site Support services. These include maintaining a suitable environment (heat, light, and power) and providing the technician with full, free, and safe access to the System. All sites must be accessible by standard service vehicles.

8.2 Replacement Parts Procedures for Onsite Support

Replacement parts will be provided by CenturyLink.

8.2.1 Critical Core Equipment Spares

Critical Core Equipment spares are stored at CenturyLink Core Data Centers

8.2.2 Critical PSAP Equipment Spares

CenturyLink will provide all manufacture critical spares within reasonable distance from PSAP. CenturyLink will identify where Crash Kits will be located during planning stages of each customer's implementation.

8.2.3 Shipment of Replacement Parts

Intrado will ship all replacement equipment not contained in spares to CenturyLink. When received, CenturyLink will replace defective equipment at PSAP

8.3 CenturyLink Managed NG9-1-1 PSAP ESInet

Customer will be responsible for replacement cost of any equipment damaged not due to normal wear and tear, due to customer misuse "Acts of God", such as lighting, flooding, roof leaks, etc.

8.4 Preventative Maintenance

- CenturyLink will perform onsite PSAP preventative maintenance quarterly or 4 times a year
- CenturyLink will perform onsite Data Center Core preventative maintenance minimum monthly

8.5 Operating System Patch Management

- CenturyLink will install all OS patches as manufacture tests and approves for field use
- OS Patches are normally released and installed monthly
- CenturyLink technicians will deploy all OS patches on all servers
- CenturyLink may push patches out to PSAP call taking positions and may require customer to reboot workstations
- CenturyLink Project Manager will schedule all OS patch dates with PSAP customers.

8.6 Application Patch Management – Security and / or Hotfixes

- CenturyLink will install all critical application patches as instructed by CPE equipment manufactures
- CenturyLink will install all application patches on all servers and critical system components. This may include routers, switches, or gateways
- CenturyLink will install all application patches on site if required.
- CenturyLink will remotely push all application patches to workstations when only a reboot is required
- CenturyLink Project Manager will schedule all application updates with PSAP customer

8.7 Anti-Virus Updates

- CenturyLink will update all anti-virus definition files monthly as released by manufacture
- Updates will be pushed remotely, and no rebooting of workstations or servers will be required
- CenturyLink will notify customer of all scheduled pushes of definition files

8.8 Firmware and IOS updates

- CenturyLink will update gateway device firmware, firewall, router and switch IOS as recommended by manufacture

9.0 System Upgrades

As Intrado makes available software release upgrades applicable to Core Equipment and PSAP CPE, CenturyLink will inform PSAP of software release upgrades

CenturyLink's Managed Emergency Call Handling Solution per-seat pricing includes all system upgrades at no cost to PSAPs. CenturyLink will perform minimum of one upgrade per year that adds features and functionality to the VIPER CPE solutions. This does not include hotfixes or service packs to address software and hardware fixes which are covered under Section 8 of this document

- CenturyLink will provide all software required to for upgrade
- CenturyLink will provide any required hardware upgrades or hardware replacement to support the system upgrade
- CenturyLink will provide all field engineering and technician resources to implement upgrade

10.0 Software and Equipment EOL and EOS notices

10.1 EOL and EOS notices

CenturyLink will advise customer of all EOL (End of Life) and EOS (End of Services) with respective milestone dates.

10.2 EOL and EOS Process

When a manufacture announces a product will be going EOL, CenturyLink will evaluate:

- End of Sale date – Last day product can be purchased
- Last date to renew manufacture support services
- Will manufacture support beyond the EOS date?

- Availability of replacement devices beyond EOS date
- Criticality of device in call delivery

Devices determined unsupportable before or after EOS date will be replaced by CenturyLink

11.0 Billable Move, Add, or Change Orders (MAC)

Any service or equipment not described in this service guide may be billable to customer.
The following are examples of billable work activities:

- Add new call taking positions (Monthly recurring rate would also apply)
- Adding new admin or CAMA trunk gateways (Monthly recurring rate would also apply)
- Terminating new admin lines on existing system
- Interfacing to new admin phone system
- Interfacing to new logging recorder
- Interfacing to new CAD system
- Interfacing to new radio system
- Move or rearrangement of existing 9-1-1 equipment, network, wiring and cabling
- Moving existing equipment at PSAP request
- Rewiring console furniture at PSAP request
- Moving equipment to new PSAP building

While the above are the most common examples of billable activities, the list is not inclusive of all possible billable MAC requests

12.0 OPTIONAL DEPLOYMENT OPTION

VIPER Emergency Call Handling can be deployed with CenturyLink providing all system building blocks or VIPER Emergency Call Handling can be deployed with CenturyLink providing Call Handling and VIPER add-on components and services with customer providing Network and / or Data Center building blocks. Pricing would be based on the final solution design

12.1 Customer provides some solution building blocks and building block elements

CenturyLink's VIPER Managed Emergency Call Handling is offered with CenturyLink providing some of the required solution building blocks and customer providing other required solution building blocks. Customer has the option of providing the following solution building blocks:

- Network Building Blocks
  - See Section 12.2 for MPLS Network Requirements
  - See Section 12.3 for Internet VPN Access
- Data Center Building Blocks
  - Must be deployed in certified Tier 3 Data Centers
  - Must be secure from other datacenter tenants
  - Provide all cabinets, cabling, x-connects, timing sources, power and UPS
- Services – Demand Training
  - All follow up VIPER Administrative and User training

12.2 Customer Provided MPLS Network Requirements

Customer will provide MPLS network with adequate network redundancy from the CenturyLink VIPER core equipment facilities to each PSAP. The MPLS network will meet the following requirements:

- Layer 3 routing will be provided between all locations;
- Certified CAT5e/CAT6 between all network switches;
- Guaranteed Bandwidth for all VIPER applications-Bandwidth requirements to be provided by CenturyLink for each PSAP deployment;
- Low Latency (< 40ms desirable);
- Low Jitter (< 5ms desirable);
- Support for Quality of Service ("QoS") as needed;
- Security against intrusion and virus attack; and
- Reliable links (fault tolerant)-no single point of failure may cause a Layer 3 disruption for more than four seconds
- Customer will provide all network communications equipment, including redundant IP routers, switches, firewalls, etc. to terminate the dual MPLS circuits at the PSAP location.

12.3 Internet VPN Access

Customer will provide and manage all Internet VPN access and security when VIPER core equipment is installed at customer data centers

12.4 Legacy E9-1-1 and NG9-1-1 Core Services

CenturyLink's Managed Emergency Call Handling Solution does not include legacy E9-1-1 service or NG9-1-1 i3 Core Services. CenturyLink does provide all CPE hardware and CPE configuration services where customer's E9-1-1 services or/and NG9-1-1 services will terminate.

13.0 MIGRATION EXISTING MIS DATA (Not Included)

- CenturyLink will not migrate existing CPE MIS data to VIPER – MECH
- CenturyLink will leave existing MIS servers onsite for customer use
- CenturyLink will not be responsible for maintaining old system servers, customer data, or customer backups.

14.0 ADENDUMS