Technical Information Document: Hosted 911 CPE Configurations

May 2011

Version	Date	Summary
0.4	05/05/2011	First Proposed Draft
0.41	05/31/2011	Add Satellite CPE

Hosted CPE Configurations

Table of Contents

Hosted CPE Configurations

1.0 Purpose:

To provide a basic technical overview for Hosted 911 Customer Provided Equipment ("Hosted CPE").

This document will:

- List recommended basic requirements for Hosted CPE
- Identify several high-level design options
- Explain features and limitations with various high-level designs

1.1 Background

CPE is considered "Hosted" when "Host" CPE serves PSAP call-taker positions geographically separate from the CPE.

"Host CPE" or "Host" describes CPE that is providing service to Remote or Collocated PSAPs. A Host may be located at offsite facilities such as at a data center or may be collocated with a PSAP. This type of system is called a "Hosted CPE System" or a "Host/Remote System".

"Satellite" describes remote positions that are configured as "survivable" remote CPE. Survivable remote CPE can function with limited capabilities should all connections to the host be lost. The term "Satellite" may not have the same meaning to all vendors.

"Remote" describes the Remote PSAP CPE that is provided services by the Host. The term "Remote" might also describe nonsurvivable remote CPE workstations. Nonsurvivable workstations have no functionality or very limited functionality should all connections to the host be lost.

For the purposes of this document, Remotes will be identified as Survivable or Nonsurvivable.

A "Host/Remote Group" is comprised of a Host or redundant Hosts and its Remotes.

1.2 Capabilities

Hosted CPE leverages modern networking technology to significantly reduce the aggregate cost of 911 CPE. It also reduces the incremental cost of ongoing investments, such as upgrades, by concentrating these investments into a single or small number of Host facilities.

1.3 Constraints

Hosted CPE concentrates network vulnerability towards the location of the Host. If there is any interruption to the function of Host CPE, that same interruption would affect any call-taker position serviced by the Host CPE. Vulnerability is concentrated both at the Host itself and any Time Division Multiplexing (TDM) or IP network utilized by the Host.

1.4 Standards Incorporated by Reference

NG911 standard 9.2.0: *Specifications for Hosted CPE*

2.0 Network Design Considerations

Non-redundant Hosts are generally not recommended as they can introduce a single point of total failure. See Figures 1, 2, and 3. If a non-redundant Host is implemented, it is recommended that EM trunks for the Remote terminate at the Remote PSAP, rather than at the Host. See Figure 3. This allows the PSAP to receive 9-1-1 calls without ALI in the event that it loses its network connection to the Host.

Redundant Hosts are strongly recommended. See Figures 4-7. In the case that one Host fails, an alternate Host can stand-in so that there is no service interruption.

Network diversity is strongly recommended. See Figures 2-7. A cloud network offers the highest level of network diversity, as any one point may connect to any other point. See Figure 7.

2.1 Desired Features

The following features are desired in Host/Remote CPE designs:

- Host redundancy
- Network redundancy/diversity
- EM trunk termination at the PSAP or at redundant/diverse Hosts
- No single point of failure

3.0 High-Level Hosted CPE Design Options:

Hosted CPE designs vary, at a high level, according to the following variables:

- Redundancy of Hosts
- Host collocation at Customer/PSAP site
- Host location at data center/vendor facilities
- Point of EM trunk termination
- Type of network connection (point-to-point, cloud)

This document explores the following configurations:

1. Non-Redundant Host not Collocated at Customer/PSAP Locations
2. Non-Redundant Host Collocated at Customer/PSAP Locations
3. Non-Redundant Host with EM Trunks to Remote
4. Redundant Hosted CPE Collocated at Customer/PSAP Locations
5. Redundant Hosted CPE not Collocated at Customer/PSAP Locations

6. Redundant Hosted CPE not Collocated at Customer/PSAP Locations with “Cloud” Network

3.1 Designs with non-redundant Hosts

These designs feature a single Host CPE system with multiple nonsurvivable Remote PSAPs served by one non-redundant Host. Figure 1 shows two Remote PSAPs with a Host that is not collocated with a PSAP. Figure 2 shows the same system, but in this case the Host is located at a PSAP.

Figures 1 and 2 fully expose multiple PSAPs to any service affecting condition at the Host. Also, they introduce a single point of network failure (Host site).

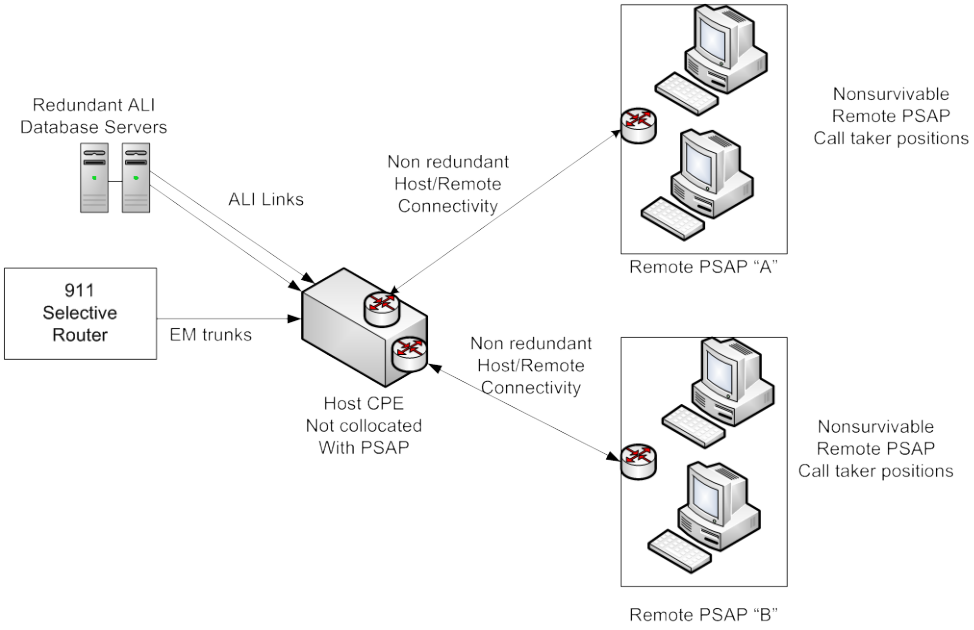

Figure 1: Non-Redundant Host not Collocated at PSAP

Figure 2 introduces redundant network connections to the nonsurvivable Remote and collocates the Host at a PSAP. This design provides a small measure of improved reliability.

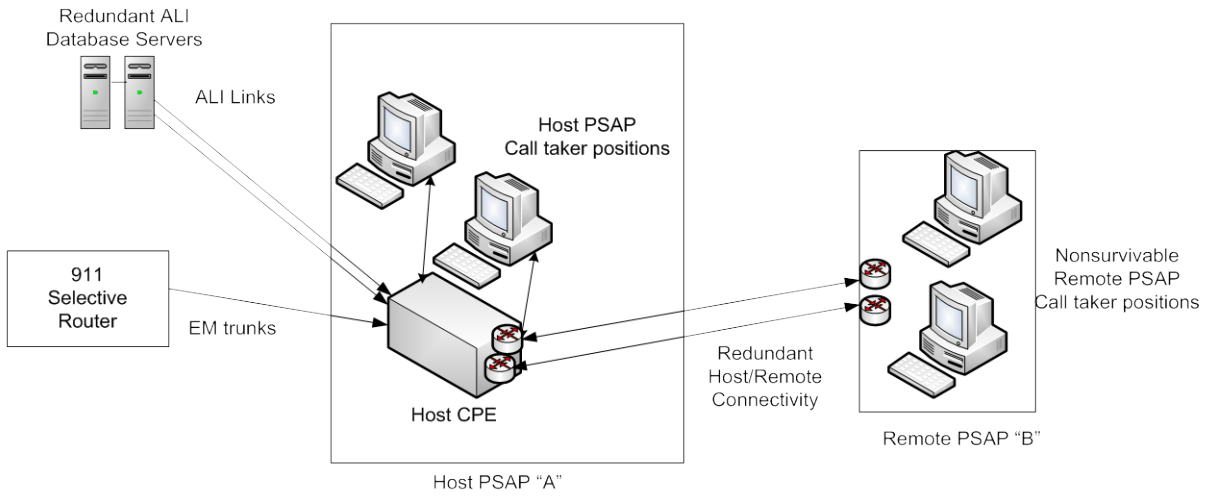

Figure 2: Non-Redundant Host Collocated at PSAP

3.2 Designs with Non-Redundant Hosts with EM Trunk Termination at the PSAP

These designs utilize a non-redundant Host, but EM trunks terminate at the survivable Remote PSAP. This design allows survivable Remote sites to receive 911 calls in the case that the Host or its network connection should fail – if the Remote system supports survivability. These designs do not completely eliminate exposure to a single point of failure, but they do mitigate the impact of Host failure. Figure 3 shows such a design where EM trunks for the survivable Remote terminate at the Remote PSAP, and not at the Host site.

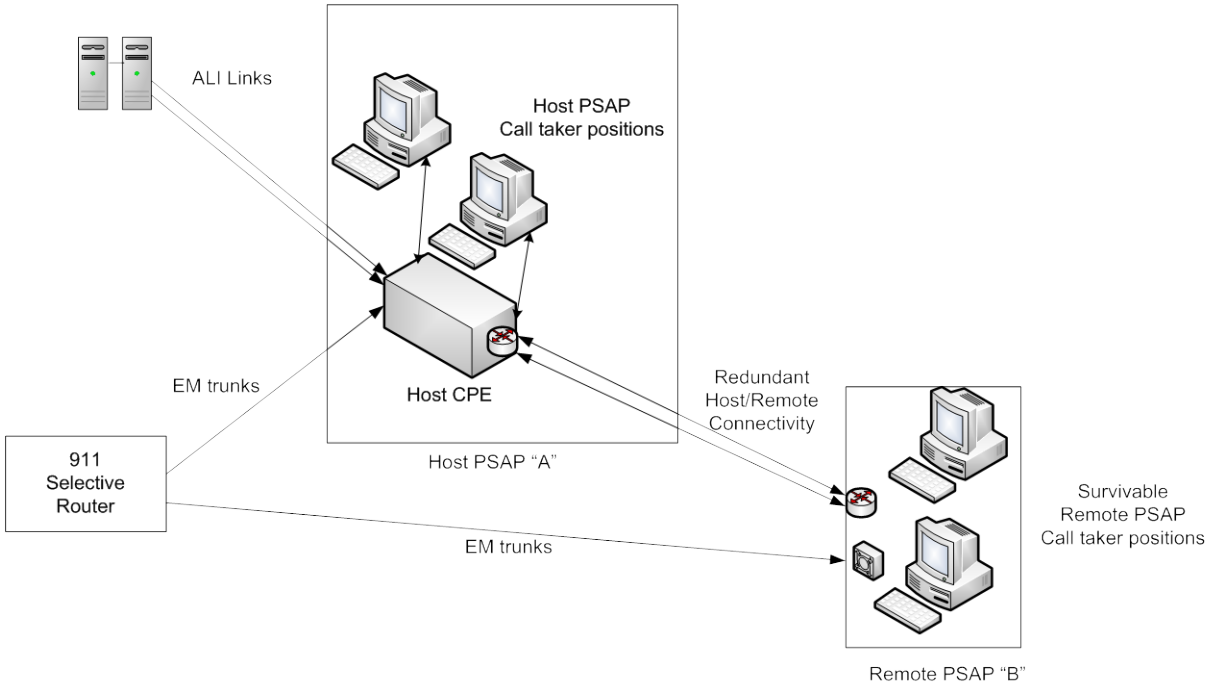

Figure 3: Non-Redundant Host with EM Trunks to Remote

3.3 Designs with Redundancy and Diversity

These designs utilize redundant Hosts. Figure 4 shows many PSAPs connected to many Hosts. It shows point to point connectivity between the Host sites and survivable Remotes along with redundancy and diversity.

As before, Hosts may be either located at PSAPs (see Figure 4), or may be located at an offsite location such as a customer data center or a vendor-provided facility (see Figure 5). With geographic diversity/redundancy and network diversity, as long as one Host is operating normally and there is connectivity between that Host and the Remotes, 911 call processing and ALI data delivery will function normally.

Figure 4 shows redundant Hosts that are collocated with PSAPs with network diversity:

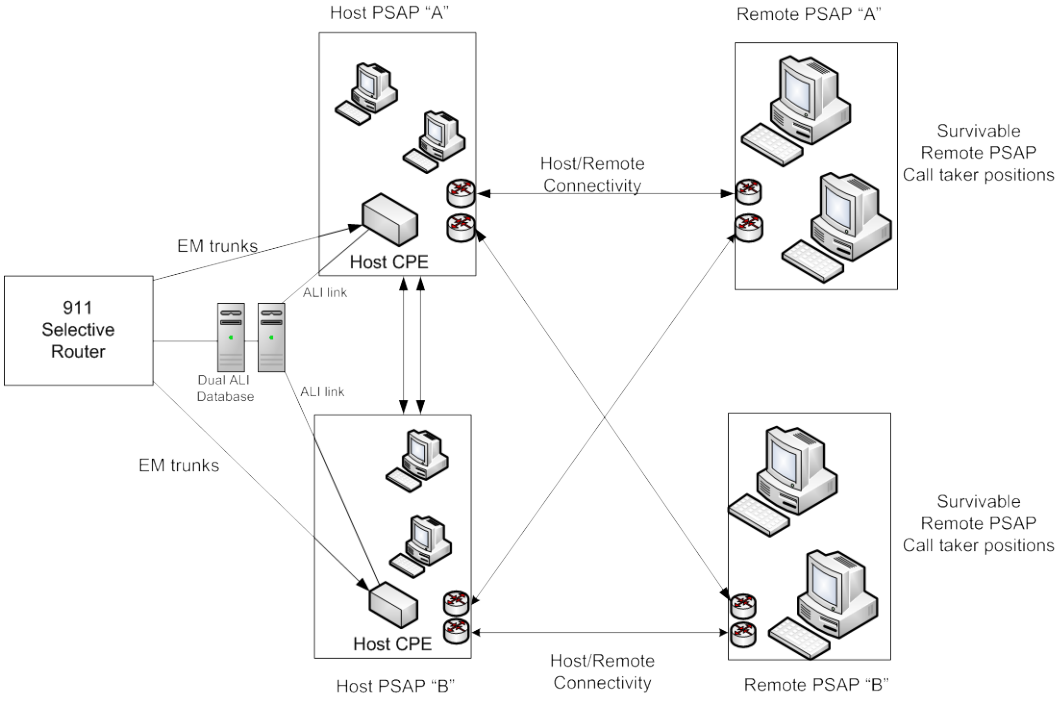

Figure 4: Redundant Hosted CPE Located at Customer/PSAP Locations

Figure 5 shows redundant Hosts that are not collocated with PSAPs with network diversity:

Hosted CPE Configurations

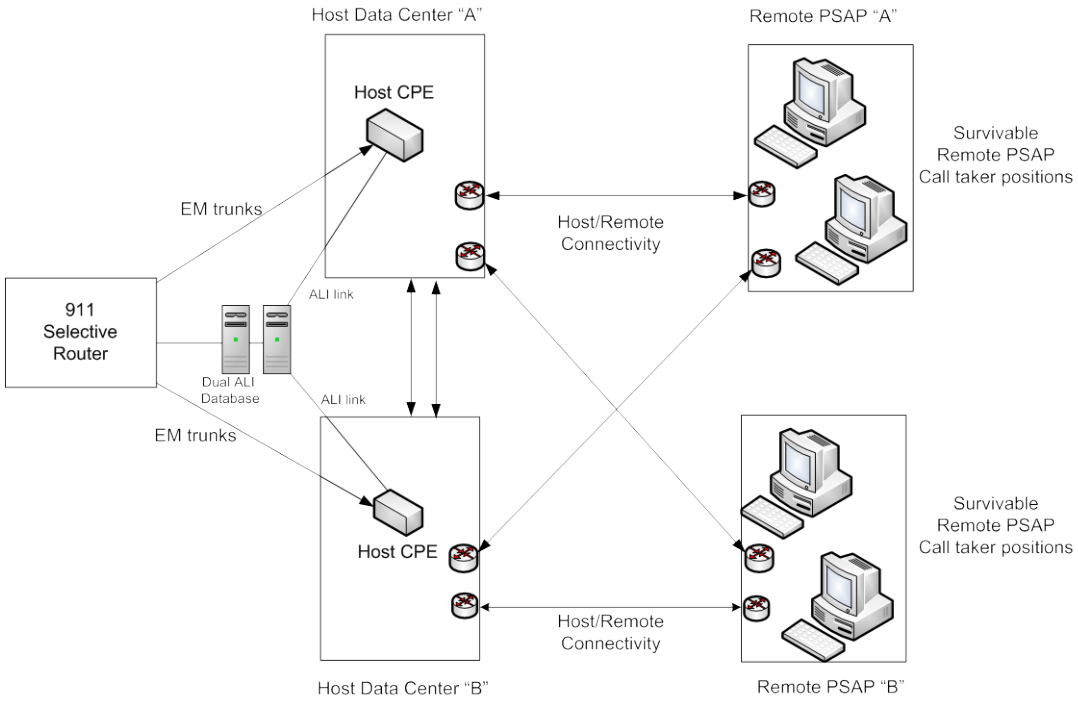

Figure 5: Redundant Hosted CPE not Collocated with PSAP

Figure 6 shows redundant Hosts with a mesh network (or "cloud"), which is inherently diverse:

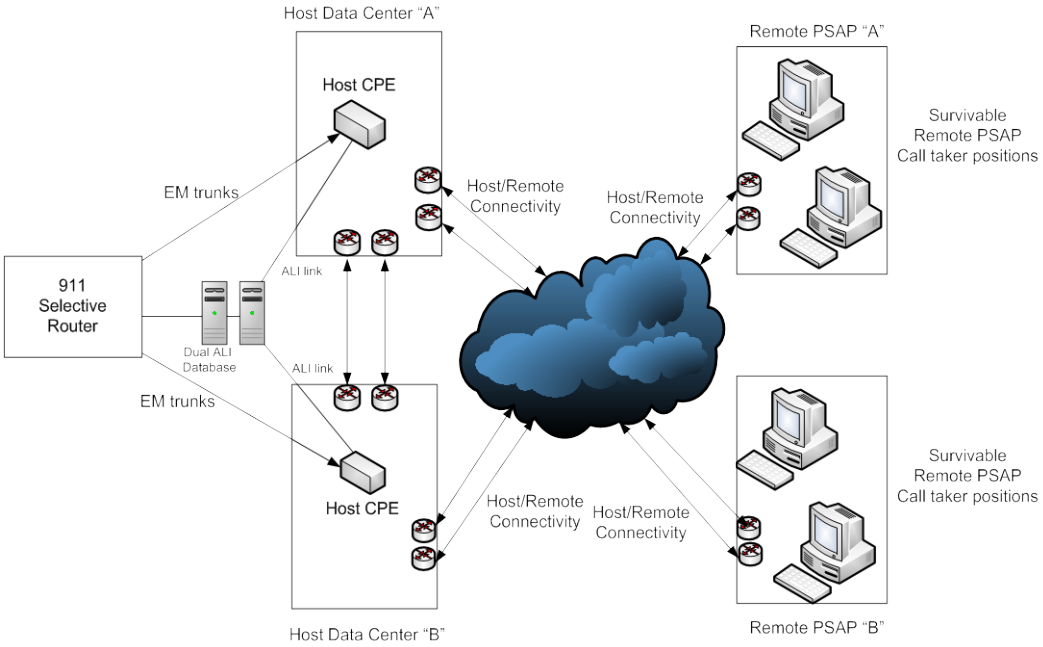

Figure 6: Redundant Hosted CPE not collocated with PSAP utilizing Cloud Connectivity

4.0 Operational Considerations

4.1 Cost-Sharing and Governance

It is recommended that disparate jurisdictions who are utilizing any Host/Remot system establish a governance structure.

A governance structure can mediate costs associated with system upgrades and maintenance. These costs should be shared between invested parties accordingly. Certain cost-bearing factors in a Host/Remote system – such as optional features or system upgrades – may not benefit each party equally.

Governance structures should be neutral and representative of each major stakeholder group.

4.2 Reporting

Report generation for Host/Remote systems can differ from standalone system, as reporting in a Host/Remote system may not be solely under the control of each individual PSAP. PSAPs must approve the process for report generation and report data when considering a Host/Remote configuration.

4.3 Control Over Data

Each individual PSAP should have control over and responsibility their own data. Access to the system must be controlled and tracked. The PSAP should have recourse In the event that data is corrupted, lost, stolen, or otherwise compromised.