CTL-1 **At page 6 of Comtech's Root Cause Analysis (see Exhibit BR-9C, attached to the Direct Testimony of Brian Rosen), Comtech identified as a Corrective and Remedial Action, "[redacted]."**

a. Identify and describe all steps taken by Comtech, prior to and following the December 2018 outage, to use "[redacted]"

RESPONSE:

TSYS objects to this data request as it is overly broad, unduly burdensome, calls for information that is irrelevant and disproportionate to the needs of this case, and is not reasonably calculated to lead to the discovery of admissible evidence. TSYS further objects to this request as it seeks information that may be protected by the attorney work-product doctrine. Without waiving these objections, TSYS provides the following response.

[redacted]

[redacted] For example, copies of TSYS's **confidential** emails requesting such quotes are attached hereto as **Attachment 1**.

[redacted]

b. Produce all documents that support your response to subpart a.

RESPONSE: TSYS objects to this data request as it is overly broad, unduly burdensome, calls for information that is irrelevant and disproportionate to the needs of this case, and is not reasonably calculated to lead to the discovery of admissible evidence. TSYS also objects to this request as it may also seek information that is protected by the attorney work-product doctrine. Without waiving these objections, TSYS provides the **confidential** documents attached hereto as **Attachment 1**.

CTL-2 At page 29 of his Direct Testimony, Mr. Rosen states Comtech "had identified the issue [of supplier diversity] and was in the process of bringing on another supplier that eventually would provide two of the links, leaving CenturyLink to supply the remaining two."

a. Please state whether Mr. Rosen is accurate when he makes this statement.

RESPONSE: Mr. Rosen's statement is accurate. TSYS emphasizes, however, that supplier diversity is not a legal requirement; indeed, many facilities-based legacy 911 providers do not have supplier diversity. That said, if possible, TSYS seeks supplier diversity as a matter of practice.

b. Did Comtech uncover facts that caused Comtech to make a decision to bring on another supplier that eventually would provide two of the links, leaving CenturyLink to supply the remaining two"? If so, describe all such facts.

RESPONSE: No, this was always TSYS's intention.

c. Were there circumstances other than a change in facts that caused Comtech to make a decision to bring "on another supplier that eventually would provide two of the links, leaving CenturyLink to supply the remaining two"? If so, describe all such circumstances.

RESPONSE: No.

d. What caused Comtech to make a decision to bring "on another supplier that eventually would provide two of the links, leaving CenturyLink to supply the remaining two"? links. Please identify all facts and produce all documents supporting your response.

RESPONSE: *See* TSYS Response to CTL-1(a), above.

e. At the time of the December 2018 outage, was Comtech aware that CenturyLink was providing all of the signaling links Comtech was using to support its Washington 911 service?

RESPONSE: Yes, this is why [redacted].

REDACTED

CONFIDENTIAL PER PROTECTIVE ORDER IN DOCKET NO. UT-181051

CTL-3 CSRIC 12-10-0594 recommends that 911 service providers "should follow industry guidelines for validating SS7 link diversity, which should be performed at a minimum of twice a year, and at least one of those validations should include a physical validation of equipment compared to the recorded documentation of diversity."

a. Please state whether Comtech agrees that this is a standard that all 911 service providers should follow.

RESPONSE: The above-quoted CSRIC recommendation is a telecommunications provider-oriented recommendation, which is listed in several CSRIC documents for legacy networks and E9-1-1 networks. NG9-1-1 networks use IP circuits. The complete CSRIC 12-10-0594 recommendation is:

> Network Operators and Service Providers should follow industry guidelines for validating SS7 link diversity, which should be performed at a minimum of twice a year, and at least one of those validations should include a physical validation of equipment compared to the recorded documentation of diversity.[1]

CSRIC "Best Practices" are recommendations that were not designed to be "one size fits all" solutions, but instead are "voluntary in nature and may not apply in every situation due to the need for flexibility, innovation, and control in the management of different carriers' unique business models, cost, feasibility, resource limitations, or other factors."[2]

b. Did Comtech follow this standard in the state of Washington during 2017 and 2018?

RESPONSE: TSYS did not provide NG911 services in Washington in 2017. In 2018, TSYS had four distinct circuits at all times and [redacted].[3]

[1] *See* CSRIC Best Practices Widget, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited Feb. 8, 2022).

[2] Communications Security, Reliability and Interoperability Council IV Working Group 7 Final Report at 6 (2014) ("*CSRIC IV WG 7 Report*"), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC%20IV%20WG7%20Legacy%20Best%20Practices%20Final.pdf.

[3] *See, e.g.*, TeleCommunication System, Inc.'s Response to PC Data Request Nos. 1-9(REVISED) at 3 (filed Sept. 16, 2021).

c. Produce copies of all documents that predate December 28, 2018, where Comtech validated signaling diversity on circuits used to support 911 calls in the state of Washington.

RESPONSE: TSYS is unable to test signal diversity on its own as it is not the facilities-based carrier for such circuits.

181051 Exh. JDW-67RX
181051 Exh. BR-88RX

CTL-4 Citing Comtech's response to Public Counsel data request PC-2, at page 40 of his Direct Testimony, Mr. Webber states that "TSYS . . . explained that its 'intended redundancy was to have [redacted], which is most certain using a single vendor since different vendors will not share information with one another about the physical paths they use.'"

a. Is this an accurate statement?

RESPONSE: Yes, Mr. Webber accurately quoted TSYS's response to PC-2, which related to the circumstances of the CenturyLink Outage. As TSYS further explained in response to PC-2, [redacted]

b. Identify all literature, standards, statutes, regulations or decisional law of which you are aware that make such a recommendation.

RESPONSE: TSYS objects to this data request as it is overly broad, unduly burdensome, calls for information that is irrelevant and disproportionate to the needs of this case, and is not reasonably calculated to lead to the discovery of admissible evidence.

c. Before the December 2018 outage, did you disclose the fact that Comtech relied exclusively upon CenturyLink to provide SS7 functionality for its 911 services in Washington to the following. If your answer is other than no, please fully describe the disclosure and produce all documents supporting your response.

RESPONSE: TSYS objects to this data request as it is overly broad, unduly burdensome, calls for information that is irrelevant and disproportionate to the needs of this case, and is not reasonably calculated to lead to the discovery of admissible evidence. TSYS also objects to this request as it may also seek information that is protected by the attorney work-product doctrine. Without waiving these objections, TSYS provides the following responses:

i. Commission Staff

RESPONSE: TSYS does not have any information to indicate one way or another that such information was or was not provided to UTC staff before the CenturyLink.

ii. WMD

RESPONSE: TSYS does not have any information to indicate one way or another that such information was or was not provided to WMD before the CenturyLink Outage.

iii. CenturyLink

RESPONSE: TSYS does not have any information to indicate one way or another that such information was or was not provided to CenturyLink before the CenturyLink Outage.

iv. Any consultants (if so, identify them by name and address)

RESPONSE: TSYS does not have any information to indicate one way or another that such information was or was not provided to any consultants before the CenturyLink Outage.

v. TNS

RESPONSE: [redacted] however, TSYS has no record to indicate one way or another that TSYS discussed its temporary, exclusive reliance on CenturyLink to provide SS7 functionality for its 911 services in Washington with TNS before the CenturyLink Outage.

vi. anyone else (if so, identify them by name and address)

RESPONSE: TSYS does not have any information to indicate one way or another that such information was or was not provided to anyone else before the CenturyLink Outage.

From: Hobelmann, Gary
To: Loree Parker; Agastya Kohli; Aaron Demorow
Cc: Honghai Liu; Gimbert, Richard; Stegman, Cynthia; Boucek, Jeanne
Subject: RE: Connectivity IPX and SS7
Date: Friday, October 5, 2018 5:02:09 PM
Attachments: image001.png

Hello everyone, just revisiting this one to see if we could clear up next steps and timeline. Let me know how Comtech wants to proceed and when would be a good time to do so.

Thank you,

Gary

From: Hobelmann, Gary
Sent: Thursday, September 13, 2018 6:59 PM
To: Loree Parker <Loree.Parker@comtechtel.com>; Agastya Kohli <Agastya.Kohli@comtechtel.com>; Aaron Demorow <Aaron.Demorow@comtechtel.com>
Cc: Honghai Liu <Honghai.Liu@comtechtel.com>; Gimbert, Richard <RGimbert@tnsi.com>; Stegman, Cynthia <cliggett@tnsi.com>; Boucek, Jeanne <jboucek@tnsi.com>
Subject: RE: Connectivity IPX and SS7

Hi Loree,

Thanks for the clarification. I think my intent was correct, but the names were off. So yes, My thinking is that you would cancel the AT&T orders on the highlighted T1s below. Then we could migrate the existing CenturyLink circuits to SIGTRAN. Do you guys need to do anything special to get the circuits to SIGTRAN? The reason I ask is for scheduling and timing. And then I wondered if you had a preference for how to migrate.

I have it as two projects

1. Migrate one batch of circuits to SIGTRAN over the IPX – then disconnect
2. Migrate the other batch to SIGTRAN and retain.

So let us know what timing you are thinking is realistic.

Thanks,

Gary

From: Loree Parker <Loree.Parker@comtechtel.com>
Sent: Thursday, September 13, 2018 6:29 PM
To: Agastya Kohli <Agastya.Kohli@comtechtel.com>; Hobelmann, Gary <ghobelmann@tnsi.com>; Aaron Demorow <Aaron.Demorow@comtechtel.com>
Cc: Honghai Liu <Honghai.Liu@comtechtel.com>; Gimbert, Richard <RGimbert@tnsi.com>; Stegman, Cynthia <cliggett@tnsi.com>; Boucek, Jeanne <jboucek@tnsi.com>
Subject: RE: Connectivity IPX and SS7

Gary,

The details of your last email aren't entirely accurate, as a few weeks ago Sprint disconnected the remaining TDM circuits terminating to Comtech facilities. Currently, all four existing circuits are from CenturyLink, at least on Comtech's side of the network. This is obviously not an ideal situation, and was intended to be extremely temporary, but AT&T has yet to successfully complete my open T1 orders even after all this time. This has prevented the rest of the TDM conversion.

Here is the current state of each link:

[redacted]

If we have an approximate timeline for the Sigtran conversion of the latter two links, I can cancel my orders with AT&T and we can finally put this project to bed.

Thanks,

Loree Parker | Senior Telecom Engineer | Safety & Security Technologies (SST) | Comtech Telecommunications Corp. | O: 206-792-2450 - M: 206-437-0664 | loree.parker@comtechtel.com

From: Agastya Kohli
Sent: Wednesday, September 12, 2018 12:00 PM
To: Hobelmann, Gary <ghobelmann@tnsi.com>; Loree Parker <Loree.Parker@comtechtel.com>; Aaron Demorow <Aaron.Demorow@comtechtel.com>
Cc: Honghai Liu <Honghai.Liu@comtechtel.com>; Gimbert, Richard <RGimbert@tnsi.com>; Stegman, Cynthia <cliggett@tnsi.com>; Boucek, Jeanne <jboucek@tnsi.com>
Subject: RE: Connectivity IPX and SS7

+Aaron D.

Gary – Loree is currently OOO, our response might be a bit delayed. Thanks.

From: Hobelmann, Gary [mailto:ghobelmann@tnsi.com]
Sent: Wednesday, September 12, 2018 8:29 AM
To: Loree Parker <Loree.Parker@comtechtel.com>; Agastya Kohli <Agastya.Kohli@comtechtel.com>
Cc: Honghai Liu <Honghai.Liu@comtechtel.com>; Gimbert, Richard <RGimbert@tnsi.com>; Stegman, Cynthia <cliggett@tnsi.com>; Boucek, Jeanne <jboucek@tnsi.com>
Subject: RE: Connectivity IPX and SS7

Loree, Agastya,

Here is a summary of where I think we are. Please take a look and let me know if you agree. Then let's get on the phone to discuss and put a plan together with timing, etc.

- Plan is to change from current connectivity of 4 IPX circuits and 4 SS7/TDM circuits to end state connectivity of 4 IPX and 2 SS7.
- We will disconnect two of the existing SS7/TDM circuits and route that traffic using SIGTRAN over the existing IPX circuits
- The two Sprint SS7/TDM circuits will remain until 2021
- Plan would be to convert existing Sprint SS7/TDM circuits to SIGTRAN
- We should have a call to discuss scheduling of a maintenance windows for each of the steps
    - I have it as at least two projects
        - Moving the current links to SIGTRAN (do we do that for just the Sprint circuits or for all four)
        - Then the migration of the traffic on the non-Sprint circuits to the IPX connectivity.
- We will also need to have paperwork prepared that clearly documents the go-forward connectivity for technical and billing reasons.

Let me know what you think about the notes above. We can get together potentially on Friday of this week to discuss if that works for your team.

Thank you,

Gary

From: Hobelmann, Gary
Sent: Friday, August 31, 2018 12:44 PM
To: Loree Parker <Loree.Parker@comtechtel.com>; Agastya Kohli <Agastya.Kohli@comtechtel.com>
Cc: Honghai Liu <Honghai.Liu@comtechtel.com>
Subject: RE: Connectivity IPX and SS7

Hi Loree,

That is a bit surprising that they would hold you to that long of a term. So it sounds like we need to review then and go with the combined approach of the six circuits. Let me grab my team next week and perhaps we can get a call going.

Have a great holiday weekend everyone.

Thank you,

Gary

From: Loree Parker <Loree.Parker@comtechtel.com>
Sent: Friday, August 31, 2018 12:28 PM
To: Hobelmann, Gary <ghobelmann@tnsi.com>; Agastya Kohli <Agastya.Kohli@comtechtel.com>
Cc: Honghai Liu <Honghai.Liu@comtechtel.com>
Subject: RE: Connectivity IPX and SS7

Update from our vendor's account team, we will need to keep the new circuits in place until 3/22/21 in order to avoid early termination charges.

From: Loree Parker
Sent: Friday, August 31, 2018 9:22 AM
To: 'Hobelmann, Gary' <ghobelmann@tnsi.com>; Agastya Kohli <Agastya.Kohli@comtechtel.com>
Cc: Honghai Liu <Honghai.Liu@comtechtel.com>
Subject: RE: Connectivity IPX and SS7

Yes. These are the Comtech-owned T1 transport links that should stay as-is for now:

Comtech Seattle 002-015-001 to TNS Los Angeles 238-091-000
Comtech Phoenix 002-015-002 to TNS Las Vegas 238-090-000

And these are the TNS-owned DS0 transport links we propose to move to IPX in the near future:

Comtech Seattle 002-015-001 to TNS Las Vegas 238-090-000
Comtech Phoenix 002-015-002 to TNS Olympia (Los Angeles) 238-091-000

From: Hobelmann, Gary <ghobelmann@tnsi.com>
Sent: Friday, August 31, 2018 7:48 AM
To: Agastya Kohli <Agastya.Kohli@comtechtel.com>
Cc: Loree Parker <Loree.Parker@comtechtel.com>; Honghai Liu <Honghai.Liu@comtechtel.com>
Subject: RE: Connectivity IPX and SS7

Good morning,

To make sure I am clear, the proposed design would disconnect two of the TDM circuits, ride that traffic over the IPX circuits for a period of time and then migrate to all IP within the next year roughly. Does that sound correct?

Thank you,

Gary

From: Agastya Kohli <Agastya.Kohli@comtechtel.com>
Sent: Thursday, August 30, 2018 11:58 AM
To: Hobelmann, Gary <ghobelmann@tnsi.com>
Cc: Loree Parker <Loree.Parker@comtechtel.com>; Honghai Liu <Honghai.Liu@comtechtel.com>
Subject: RE: Connectivity IPX and SS7

Gary,

181051 Exh. JDW-67RX
CONFIDENTIAL PER PROTECTIVE ORDER IN DOCKET NO. UT-181051
REDACTED
181051 Exh. BR-88RX
Attachment

Just chatted with Loree – our circuit expert. She said:
"I wouldn't be opposed to canceling the pending AT&T circuits and converting the remaining two DS0s to IP now(ish). We'd need to keep the two we've already migrated to T1 for at least another 8 months. And having half IP and half TDM has some redundancy advantages."

Thoughts?

Agastya

From: Hobelmann, Gary [mailto:ghobelmann@tnsi.com]
Sent: Thursday, August 30, 2018 9:52 AM
To: Agastya Kohli <Agastya.Kohli@comtechtel.com>
Subject: RE: Connectivity IPX and SS7

Hi Agastya, Just checking in on this one. Let me know what you think.

Thank you,

Gary

From: Hobelmann, Gary
Sent: Tuesday, August 28, 2018 10:55 AM
To: Agastya Kohli <Agastya.Kohli@comtechtel.com>
Subject: Connectivity IPX and SS7

Agastya,

Some time ago we talked about combining the old SS7 connectivity with the new IPX Connectivity we were putting in. Now that all of the connectivity pieces for IPX are in, is there still a desire to put everything together or should we just leave them as separate connections for a period of time? and if we want to keep them separate, what is a good timeframe for revisiting the combination?

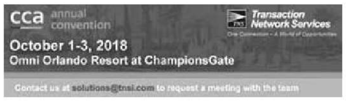
Let me know what you are thinking.

Thank you,

Gary

Gary W. Hobelmann | Sales Account Executive
Transaction Network Services
7311 West 132nd Street | Suite 300 | Overland Park | KS | 66213 | USA
O: +1 913 814 6241 | M: +1 913 515 1238
E: ghobelmann@tnsi.com | http://www.tnsi.com/products-services/telecom

One Connection – A World of Opportunities


cca annual convention
Transaction Network Services
One Connection – A World of Opportunities
October 1-3, 2018
Omni Orlando Resort at ChampionsGate
Contact us at solutions@tnsi.com to request a meeting with the team

TNS Call Guardian
Transaction Network Services
Looking for the most accurate robocall blocking solution?
Looking for spoofed call detection?
Ask me about TNS Call Guardian.
One Connection- A World of Opportunities
www.tnsi.com

This e-mail message is for the sole use of the intended recipient(s)and may
contain confidential and privileged information of Transaction Network Services.
Any unauthorized review, use, disclosure or distribution is prohibited. If you
are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

NOTICE TO RECIPIENT: This email, including attachments, may contain information which is confidential, proprietary, attorney-client privileged and / or controlled under U.S. export laws and regulations and may be restricted from disclosure by applicable State and Federal law. Nothing in this email shall create any legal binding agreement between the parties unless expressly stated herein and provided by an authorized representative of Comtech Telecommunications Corp. or its subsidiaries. If you are not the intended recipient of this message, be advised that any dissemination, distribution, or use of the contents of this message is strictly prohibited. If you received this message in error, please notify us immediately by return email and permanently delete all copies of the original email and any attached documentation from any computer or other media.

This e-mail message is for the sole use of the intended recipient(s)and may
contain confidential and privileged information of Transaction Network Services.
Any unauthorized review, use, disclosure or distribution is prohibited. If you
are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

This e-mail message is for the sole use of the intended recipient(s)and may
contain confidential and privileged information of Transaction Network Services.
Any unauthorized review, use, disclosure or distribution is prohibited. If you
are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

This e-mail message is for the sole use of the intended recipient(s)and may
contain confidential and privileged information of Transaction Network Services.
Any unauthorized review, use, disclosure or distribution is prohibited. If you

are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

CONFIDENTIAL PER PROTECTIVE ORDER IN DOCKET NO. UT-181051

181051 Exh. JDW-67RX

REDACTED

Supplemental Attachment

181051 Exh. BR-88RX

[redacted]

[redacted]

CONFIDENTIAL PER PROTECTIVE ORDER IN DOCKET NO. UT-181051

Supplemental Attachment

181051 Exh. JDW-67RX

181051 Exh. BR-88RX

REDACTED

[redacted]

REDACTED

[redacted]

181051 Exh. JDW-67RX

CONFIDENTIAL PER PROTECTIVE ORDER IN DOCKET NO. UT-181051

REDACTED

Supplemental Attachment

181051 Exh. BR-88RX

[redacted]

181051 Exh. JDW-67RX

181051 Exh. BR-88RX

REDACTED

[redacted]

181051 Exh. JDW-67RX

181051 Exh. BR-88RX

REDACTED

Supplemental Attachment

[redacted]

181051 Exh. JDW-67RX

181051 Exh. BR-88RX

REDACTED

[redacted]

181051 Exh. JDW-67RX

181051 Exh. BR-88RX

REDACTED

[redacted]

181051 Exh. JDW-67RX

181051 Exh. BR-88RX

REDACTED

[redacted]

181051 Exh. JDW-67RX

181051 Exh. BR-88RX

REDACTED

[redacted]

CTL-5 Does Comtech utilize SS7 links anywhere within its 911 network in Washington? If your answer is anything other than yes, fully explain why do not use SS7 in your network today.

RESPONSE: [redacted] At the time of the CenturyLink Outage, TSYS also indirectly connected to CenturyLink utilizing SS7 links because CenturyLink refused to connect to TSYS via SIP or directly via SS7.

CTL-6 **Does Comtech utilize SS7 links anywhere within its 911 network in any state other than Washington? If your answer is other than yes, please describe (i) when it made the decision to transition away from SS7, (ii) when Comtech completed the transition away from SS7, and (ii) why it made the decision to transition away from SS7.**

RESPONSE: TSYS objects to this data request in its entirety as it is overly broad, calls for information that is irrelevant and disproportionate to the needs of this case, and is not reasonably calculated to lead to the discovery of admissible evidence. Without waiving these objections, TSYS provides the following response.

[redacted]

CONFIDENTIAL PER PROTECTIVE ORDER IN DOCKET NO. UT-181051

181051 Exh. JDW-67RX

REDACTED

181051 Exh. PR-88RX

[redacted]

CONFIDENTIAL PER PROTECTIVE ORDER IN DOCKET NO. UT-181051

181051 Exh. JDW-67RX

181051 Exh. BR-38RX

REDACTED

[redacted]

DATA REQUESTS

CTL-7. In response to CTL-2(a) you stated that "TSYS seeks supplier diversity as a matter of practice." With regard to this statement:

a. Describe all of the reasons why you believe it is a good practice to obtain supplier diversity.

b. Produce all documents discussing the reasons why it is a good practice to obtain supplier diversity.

RESPONSE:

a. TSYS objects to this data request as it purports to seek more than is required by the applicable rules of the Utilities and Transportation Commission ("UTC" or "Commission"), including the creation of records that are not currently in existence. TSYS further objects as this data request as it is overly broad, unduly burdensome, calls for information that is irrelevant and disproportionate to the needs of this case, and is not reasonably calculated to lead to the discovery of admissible evidence. This data request is also well outside the scope of this proceeding, which "is limited to 'whether CenturyLink violated any statutes or Commission rules resulting in the December 2018 network outage,' per paragraph 15 of the Commission's Order 03 granting the petition to intervene (August 9, 2021)."[1] Without waiving these objections, TSYS provides the following response:

TSYS believes supplier diversity is a generally good practice, if available, based on the significant expertise of its employees and general industry guidance, such as the National Emergency Number Association ("NENA") i3 materials. For example, NENA has acknowledged that "multiple circuits from multiple providers is assumed to create greater diversity and redundancy."[2] NENA qualified this assumption, however, explaining "there are also risks associated with such supplier diversity as several vendors may interconnect upstream and essentially use the same backbone at many points of presence."[3]

b. TSYS objects to this data request as overly broad, unduly burdensome, calls for information that is irrelevant and disproportionate to the needs of this case, and is not reasonably calculated to lead to the discovery of admissible evidence. Without waiving these objections, TSYS provides the NENA Emergency Services IP Network Design Information Document in **Attachment 1** as an example.

[1] Public Counsel Response to CenturyLink DR 2 at 1-2 (January 27, 2022).

[2] NENA Emergency Services IP Network Design Information Document, NENA-INF-016.2-2018 (originally 08-506) (2018), https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-INF-016.2-2018_ESIND_20.pdf, attached here as **Attachment 1**.

[3] *Id.* at 2.

REDACTED

CTL-8. **In response to CTL-3(a), you referenced CSRIC 12-10-0594. With regard to CSRIC 12-10-0594:**

a. Describe all steps that you, TNS or any agent and/or consultant took on your behalf to comply with and/or adhere to this standard in connection with your design, construction, and maintenance of your Phase 1 SS7 network in Washington.

b. Produce all documents showing the steps that you, TNS or any agent and/or consultant took on your behalf to comply and/or adhere to this standard in connection with your design, construction, and maintenance of your Phase 1 SS7 network in Washington.

RESPONSE:

a. TSYS objects to this data request as it purports to seek more than is required by the applicable rules of the UTC, including the creation of records that are not currently in existence. TSYS also objects to this data request as it is overly broad, unduly burdensome, calls for information that is irrelevant and disproportionate to the needs of this case, is significantly outside the scope of this proceeding, and is not reasonably calculated to lead to the discovery of admissible evidence. Without waiving these objections, TSYS provides the following response: TSYS had four distinct circuits at all times in 2018 and [redacted].

b. See above.

REDACTED

CTL-9. At any time prior to the December 2018 network outage, did TNS publish and/or provide written guidance to Comtech regarding the role and importance of diversity in connection with SS7 networks supporting 911 networks? If your answer is other than no, please identify and produce all such writings.

RESPONSE:

TSYS objects to this data request as it purports to seek more than is required by the applicable rules of the UTC, including the creation of records that are not currently in existence. TSYS also objects to this data request as it is overly broad, unduly burdensome, calls for information that is irrelevant and disproportionate to the needs of this case, is significantly outside the scope of this proceeding, and is not reasonably calculated to lead to the discovery of admissible evidence. Without waiving these objections, TSYS provides the following response:

TSYS conducted another diligent review of its records and the archived emails of TSYS personnel subject to the parameters of this data request and found reference to a discussion of vendor diversity. Such communications are subject to the confidentiality provisions of our agreement with TNS and, for this reason, are not attached hereto.

Please note that this additional information regarding communications with TNS also supplements TSYS's response to CTL-4(v).

REDACTED

CTL-10. At any time prior to the December 2018 network outage, did TNS provide verbal guidance to Comtech regarding the role and importance of diversity in connection with SS7 networks supporting 911 networks? If your answer is other than no, please identify and fully describe all such verbal communications.

RESPONSE:

TSYS objects to this data request as it purports to seek more than is required by the applicable rules of the UTC. TSYS also objects to this data request as it is overly broad, unduly burdensome, calls for information that is irrelevant and significantly outside the scope of this proceeding, disproportionate to the needs of this case, and is not reasonably calculated to lead to the discovery of admissible evidence. Without waiving these objections, TSYS provides the following response:

TSYS has no record to indicate one way or another that TNS, prior to the CenturyLink Outage, provided TSYS with verbal or oral guidance regarding the role and importance of diversity in connection with SS7 networks supporting 911 networks.

REDACTED

ATTACHMENT 1

Emergency Services IP Network Design (ESIND) Information Document

NENA Emergency Services IP Network Design Information Document

NENA-INF-016.2-2018 (originally 08-506)
DSC Approval: 01/30/2018
PRC Approval: 03/15/2018
NENA Executive Board Approval: 04/05/2018
Next Scheduled Review Date: 04/05/2021

Prepared by:
National Emergency Number Association (NENA), Interconnection & Security Committee,
NG9-1-1 Architecture Subcommittee, Emergency Services IP Network Design Working Group

Published by NENA
Printed in USA

NENA
INFORMATION DOCUMENT
NOTICE

This Information Document (INF) is published by the National Emergency Number Association (NENA) as an information source for 9-1-1 System Service Providers, network interface vendors, system vendors, telecommunication service providers, and 9-1-1 Authorities. It is not intended to provide complete design or operation specifications or parameters or to assure the quality of performance for systems that process such equipment or services.

NENA reserves the right to revise this Information Document for any reason including, but not limited to:

- Conformity with criteria or standards promulgated by various agencies,
- Utilization of advances in the state of the technical arts,
- Reflecting changes in the design of equipment, network interfaces, or services described herein.

This document is an information source for the voluntary use of communication centers. It is not intended to be a complete operational directive.

It is possible that certain advances in technology or changes in governmental regulations will precede these revisions. All NENA documents are subject to change as technology or other influencing factors change. Therefore, this NENA document should not be the only source of information used. NENA recommends that readers contact their 9-1-1 System Service Provider (9-1-1 SSP) representative to ensure compatibility with the 9-1-1 network, and their legal counsel to ensure compliance with current regulations.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license expressed or implied is hereby granted. This document shall not be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA or any affiliate thereof to purchase any product whether or not it provides the described characteristics.

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA's Committees have developed this document. Recommendations for change to this document may be submitted to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

Intellectual Property Rights (IPR) Policy

NOTE – The user's attention is called to the possibility that compliance with this document may require use of an invention covered by patent rights. By publication of this document, NENA takes no position with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from NENA by contacting the Committee Resource Manager identified on NENA's website at www.nena.org/ipr.

Consistent with the NENA IPR Policy, available at www.nena.org/ipr, NENA invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this document.

Please address the information to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

Reason for Issue/Reissue

NENA reserves the right to modify this document. Upon revision, the reason(s) will be provided in the table below.

Document Number	Approval Date	Reason For Issue/Reissue
NENA 08-506	12/14/2011	Initial Document
NENA-INF-016.2-2018	04/05/2018	Updates to document, addition of new technical sections, and overall refinement based on current information.

Table of Contents

1 EXECUTIVE OVERVIEW 6
2 EMERGENCY SERVICES IP NETWORK DESIGN 7
2.1 WHAT IS AN ESINET? 7
2.1.1 ESInet scope 8
2.1.2 ESInet design considerations..10
3.1.3.1 Redundancy..11
3.1.3.2 Considerations for Redundancy..11
3.1.4 Survivability..11
2.2 LOCAL AREA NETWORK (LAN) ARCHITECTURE 12
2.3 WAN ARCHITECTURE 13
2.4 HARDWARE / EQUIPMENT ELEMENTS 13
2.5 NETWORK / SOFTWARE ELEMENTS 14
2.6 THE OPEN SYSTEMS INTERCONNECTION (OSI) MODEL 14
2.7 OSI LAYER 1 / LINK LAYER..15
2.7.1 Copper facilities 16
2.7.2 Coaxial (Coax) facilities..16
2.7.3 Fiber facilities 18
2.7.4 Cellular Wireless Communication Networks..18
2.7.5 Microwave 19
2.7.6 Satellite..20
2.7.7 Wi-Fi® 21
2.7.8 FirstNet..22
2.8 OSI LAYER 2 24
2.8.1 High-Level Data Link Control (HDLC) 24
2.8.2 Frame Relay 24
2.8.3 Asynchronous Transfer Mode (ATM) 25
2.8.4 Metro Ethernet..26
2.8.5 Multi-Protocol Label Switching (MPLS) 27
2.9 OSI LAYER 3 28
2.9.1 IP Addressing 28
2.9.2 Dynamic Routing Protocols..30
3.9.2.1 Interior Gateway Protocol (IGP)..31
3.9.2.2 Open Shortest Path First (OSPF) 31
3.9.2.3 Enhanced Interior Gateway Routing Protocol (EIGRP) 31
3.9.2.4 Intermediate System to Intermediate System (IS-IS)..31
3.9.2.5 Border Gateway Protocol (BGP)..31
2.10 AVAILABILITY AND RELIABILITY..32
2.10.1 Definitions and Equations of Availability and Reliability 33
2.10.2 Achieving five nines availability in 9-1-1 networks 35
2.10.3 Practical methods for legacy 9-1-1 networks 36
2.10.4 Defining failure metrics for an ESInets 36
2.10.5 Series and Parallel Reliability and Availability in ESInets 37
2.11 NETWORK SECURITY 39
2.11.1 Session Border Controllers (SBC) and Firewalls..39
2.11.2 Distributed Denial of Service (DDoS) mitigation..40
2.11.3 Multiple Service Providers 41
2.11.4 Internet Access within a PSAP..41
2.12 NETWORK MANAGEMENT AND MONITORING 41
2.12.1 Network Performance Monitoring..43
2.12.2 Quality of Service within a PSAP 44

2.12.3 Service Level Agreement 47
2.12.4 Dimensioning ESInet Data Circuits 49
2.12.5 Traffic Engineering 50
2.12.6 Quality of Service (QoS) 50
2.12.7 Interconnection and Peering 51
2.13 DOMAIN NAME SYSTEM (DNS) 51
2.13.1 DNS Architecture 51
2.13.2 DNS Management 52
2.13.3 DNS Naming Schema 52
2.13.4 Multi-homed PSAP DNS operation 52
2.14 NETWORK ARCHITECTURE 53
3 CONCLUSION 56
4 IMPACTS, CONSIDERATIONS, ABBREVIATIONS, TERMS, AND DEFINITIONS 57
4.1 OPERATIONS IMPACTS SUMMARY 57
4.2 TECHNICAL IMPACTS SUMMARY 57
4.3 SECURITY IMPACTS SUMMARY 58
4.4 RECOMMENDATION FOR ADDITIONAL DEVELOPMENT WORK 58
4.5 ANTICIPATED TIMELINE 58
4.6 COST FACTORS 58
4.7 COST RECOVERY CONSIDERATIONS 58
4.8 ADDITIONAL IMPACTS (NON-COST RELATED) 58
4.9 ABBREVIATIONS, TERMS, AND DEFINITIONS 59
5 RECOMMENDED READING AND REFERENCES 59
ACKNOWLEDGEMENTS 61

1 Executive Overview

21st century Public Safety agencies will be required to connect to, and/or build a private Emergency Services IP network (ESInet) as defined by NENA-STA-010 to continue to provide services to their constituents. PSAPs and other public safety agencies will utilize the ESInet to provide interconnection[1] to other ESInets, originating service providers, third-party data providers (e.g., Additional Data about location and caller), Telematics providers, groups of agencies and 9-1-1 service providers[2] within a city, county state or larger regional system via Internet Protocol (IP) networks. The effort and expense required to build this type of shared IP network is a significant undertaking. This document discusses several steps typically taken to ensure each ESInet is built to scale, and is interoperable with other ESInets. Topics such as design considerations, known caveats, lessons learned, technological limitations, as well as the advantages/disadvantages of the various networking technologies are addressed. This document investigates what network architects can do to assure maximum availability during unique systems failures, such as localized IP network failures, call delivery system failures, as well as full ESInet failures.

This document covers the design of ESInets at Open Systems Interconnection (OSI) layers 1, 2, and 3. Network architecture options and methodologies for achieving recommended reliability and availability service levels are discussed. Performance requirements and other aspects of service level agreements for operators of ESInets are covered, as well as several aspects of network security. ESInets must deliver high priority traffic in the face of severe congestion. Traffic engineering strategies for achieving that goal are discussed. Network management and monitoring of ESInets is also covered. The intended audience for this document includes network architects that are tasked with designing ESInets and 9-1-1 entities or state authorities that are working with consultants and service providers to procure an ESInet. One of the objectives of this document is to provide 9-1-1 entities and state authorities with the background information necessary to identify their requirements. Another objective is to define the concepts and vocabulary that will enable 9-1-1 entities and state authorities to guide their service providers and consultants to design solutions that meet their requirements. A number of the topics covered in this document are fields of study to which people devote their entire careers. The information contained in this document by itself does not provide all of the necessary details to properly design ESInets. It is a best practice to engage qualified IP network design engineers when designing ESInets.

This document is intended to provide information that will assist in the development of requirements necessary to design ESInets that meet industry standards and best practices related to the NG9-1-1 systems that will depend on them for services. Readers are encouraged to review and refer to this document during preparations for procuring, building and implementing an ESInet and to use it as an informative resource.

[1] This document does not necessarily use the term "interconnection" to mean, imply, and/or exclude any federal and/or state regulation regarding any such interconnection, and those regulatory issues are beyond the scope of this document

[2] A 9-1-1 Service Provider is considered the provider of 9-1-1 to a PSAP, Region or State.

2 Emergency Services IP Network Design

ESInets are like other IP networks in that they are a collection of routers, switches, core service functional elements, and data security devices, and management tools. ESInets, however, must be designed to meet more stringent requirements for security, resiliency and reliability service levels than most other IP networks.

Per NENA-STA-010 [1] and for the purposes of this document ESInet is defined as follows:

> An ESInet is a managed IP network that is used for emergency services communications, and which can be shared by all public safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core functional processes can be deployed, including, but not restricted to, those necessary for providing NG9-1-1 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national and international levels to form an IP-based inter-network (network of networks).

A summary of the core requirements for an ESInet, as summarized in the NENA-STA-010 Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3 [1], are as follows:

- The network between the PSAP and an ESInet will be a private or virtual private network based upon TCP/IP
- It will have scalable bandwidth to support new enhanced services
- The Emergency Services IP Network shall be a conventional routed IP network
- MPLS or other sub-IP mechanisms are permitted as appropriate
- The PSAP should use redundant local area networks for reliability
- PSAP LAN to an ESInet must be resilient, secure, physically diverse, and logically separate
- ESInets shall be engineered to sustain real time traffic, including data, audio, and video
- Connections between the PSAP and an ESInet WAN shall be secured TCP/IP connections
- ESInets should be capable of operating on IPv4 and IPv6 network infrastructures
- ESInets should consider how the Domain Name System (DNS) is designed and managed
- ESInet implementations should consider coordination efforts to understand Autonomous System (AS) number implications for statewide deployments
- ESInet configurations may impact Voice Quality and shall be designed to support the minimal acceptable levels defined by NENA-STA-010.

2.1 What is an ESInet?

An ESInet is a specialized IP network designed and implemented with the measures described in this document to allow connectivity between public safety agencies. ESInets lay the groundwork for NG9-1-1 configurations by providing the common routed infrastructure to deliver critical information. ESInets provide transport, interoperability, security, and related services.

When properly designed and implemented, an ESInet can improve access to emergency services for all callers and increase the effectiveness and efficiency of emergency communications response. The evolution into an all broadband IP infrastructure via an ESInet can enable centralized applications, support interoperability, create diversity and increase the ability to internetwork with PSAPs outside of current geographic restrictions.

NG9-1-1 is an Internet Protocol (IP) based system comprised of managed ESInets, This is not substantive – just moving from a different section – does not require pub review elements, and databases that replaces traditional E9-1-1 features and functions and provides additional capabilities.

NG9-1-1 provides the logical access to resources from all connected sources, and provides multimedia data capabilities for PSAPs and other emergency service organizations.

It is important to understand that an ESInet and NG9-1-1 are not the same. An ESInet can be implemented without being considered NG9-1-1, but NG9-1-1 cannot operate without an ESInet.

The diagram below illustrates the typical hierarchy of networks utilized to reach a fully functional NG9-1-1 system. The PSAP LAN refers to the connectivity of the workstations and devices necessary for 9-1-1 applications and services and is not intended to mean a LAN for administrative purposes.

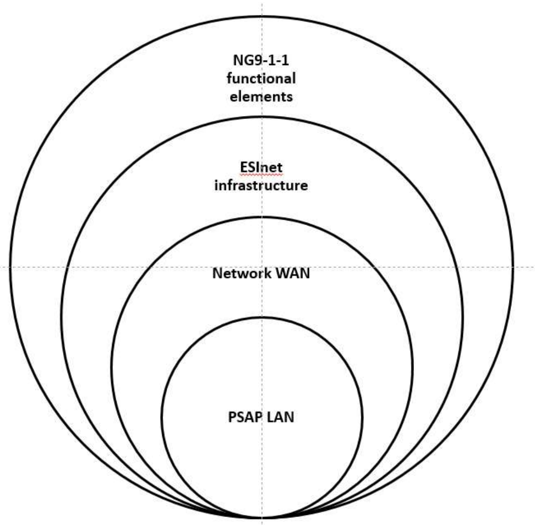


Figure 1

ESInets can be custom built to serve several geographic areas.

2.1.1 ESInet scope

Depending upon the geographic area covered, ESInets can vary in size. Regardless of ESInet size, the information presented in this document is recommended to ensure that ESInets are configured in a similar manner to allow interconnection with other ESInets. Interconnection between ESInets can encourage sharing of resources, systems, and applications, and may increase financial efficiency.

During the strategic planning phase of an ESInet deployment, there are many configuration and design decisions to consider. While many considerations are presented in this document, there are many that are dependent upon the local governance, network and management policy that may also serve to clarify or guide ESInet design.

A key component for any ESInet consideration includes the assessment of alternate networks provided by other governmental agencies or existing networks. For example, using transport from a higher education network or other available existing network may positively impact the costs of the overall design. Connections to networks such as these may allow for an offset of major cost implications in areas where broadband connectivity is expensive, or redundancy is limited. During the initial planning stages, all available broadband network resources should be evaluated for possible utilization in design and deployment of the ESInet.

Logical connections between the NG9-1-1 and other emergency services or external networks must be strictly managed through appropriate security boundaries. ESInet WANs can and probably will utilize leased and private IP transport that leverages appropriate network separation, traffic engineering and security.

Inter-working or inter-agency agreements may be required to ensure that the sharing of services can be expected to function as envisioned, and to the mutual benefit of all participating agencies.

The 9-1-1 Authority may have jurisdiction over how ESInets are planned, deployed and managed.

ESInets may be Local, Regional, State, National, or International. These connections may be grown out of interconnection between adjacent ESInets. A county network can be connected to another county. Multiple counties can be connected together to become a region, although it is not an immediate requirement that these smaller systems be contiguous. Regions can be interconnected to create a statewide network. Multiple statewide networks can be connected to have a nationwide network. International networks may be developed by connecting other nationwide networks. In addition, calls can be routed across the Internet that may allow emergency calls to be delivered globally. These general categories are further defined below:

- **Local ESInets** –a single PSAP, county, or small call center area.
- **Regional ESInets** – an ESInet that may contain multiple PSAPs, counties, or potentially multiple local ESInets.
- **Statewide ESInets** – an ESInet that covers an entire State, Statewide configurations typically may contain several regional and local ESInets.
- **National ESInet** – an ESInet will eventually be deployed across an entire nation, and interconnect all Statewide ESInets, Regions or Local ESInets.
- **International ESInet** – an ESInet could cover the entire world once interconnections are made across all participating ESInets.

Designing an ESInet using this document as a guide may increase the probability for successfully internetworking ESInets to create a Regional, Statewide, National, and eventually, an International ESInet.

2.1.2 ESInet design considerations

ESInet design requirements are necessary to deliver a level of performance suitable for mission critical systems[3] and facilities. The mission critical infrastructure and systems that support NG9-1-1 must be established with the very highest degree of security, reliability, resiliency, redundancy, survivability and diversity, to meet the expectation of the 9-1-1 industry and first responder communities. Further, these systems and networks will remain fully operational during regular daily operations as well as during and immediately following a major natural or manmade disaster on a local, regional, and even nationwide basis.

It is important to point out that even when redundant physical circuits are ordered, for the most part legacy PSAPs do not have dual entrance facilities. This means that the last mile (i.e., from a manhole or pole to the PSAP premise) may be located in the same conduit/trench/pole or be in the same fiber/copper sheath as another path.

When feasible, alternate network access paths are highly desirable to consider during the ESInet design process. It is important to ask questions of the vendor and determine the trade-offs associated with a shared (non-redundant) path[4].

The same level of care should be taken when purchasing circuits from vendors. In many instances multiple circuits from multiple providers is assumed to create greater diversity and redundancy. However, several vendors may interconnect upstream and essentially use the same backbone at many points of presence. It is important to understand where the vendors may interconnect and how they interconnect, and design an ESInet to minimize or avoid situations that lack redundancy throughout the entire network. Costs may prohibit just how much diversity and redundancy can be justified, but the areas that lack redundancy must be clearly identified in the event of an incident or problem that can affect 9-1-1 services.

Those involved in planning and design of an ESInet are urged to look beyond the cost of operations as a restriction to implementing as much diversity as possible in comparison to the costs of liability in the potential event of a service or system failure. A best practice when designing connections into an ESInet is to utilize a mix of diverse transport mediums, technologies and service providers as is operationally and economically feasible.

The emphasis on “no single point of failure” in 9-1-1 applies to all ESInets. Some considerations that should be addressed include:

- Physical entrance facilities (dual entrance, where feasible and cost effective)
- Backhaul facility diversity
- Circuit diversity
- Network diversity

[3] Used in this document, “mission critical systems” are those that, “when their capabilities are degraded, the organization realizes a resulting loss of a core capability or life or property are threatened.” Department of the Interior, http://www.gao.gov/assets/110/107380.pdf.

[4] FCC title 47 of Code of Federal Regulation (CFR), section 202 requires that transport of 9-1-1 services to/from the public networks to the Local Serving Office (LSO) NOT be collapsed. This does not mean ‘core’ redundancy, but does establish requirements that the Local Exchange Carriers (LEC’s) must follow. The FCC does not require circuit redundancy between the LSO to the PSAP or (if provided) dual path or dual entrance.

An important aspect to consider when planning for and designing an ESInet is the interconnections between all providers. In a legacy 9-1-1 network these interconnections are typically managed by a single entity or a single service provider. Since an ESInet is typically designed to allow as many interconnection points as necessary and include many potential network resources, it is important to understand where they are located in the ESInet.

In many cases an ESInet may be comprised of multiple services being provided by different entities. The interconnection points and the operation, administration and management functions are areas where responsibility could change within an ESInet. Understanding where these occur, or may have the potential to occur, is necessary to aid in identifying the responsibility of each provider.

This is especially true when troubleshooting a problem or when a fault within the network occurs. When there are many interconnection points the monitoring of faults can be challenging. There may be service affecting faults that trigger events on an ESInet that are not monitored and controlled by an ESInet itself. Therefore it is very important to understand the matrix of ESInet interconnections, management, monitoring and control. Keeping an up-to-date inventory of all interconnection points and their providers is recommended.

3.1.3.1 Redundancy

The ability to meet redundancy requirements is often included as part of requirements for reliability and resiliency. Typical systems and components that should have redundant (parallel) capabilities include:

- Power systems
- Telecommunications services[5]
- Network electronics
- Cooling
- Fuel

All mission critical systems shall provide at least two geographically-redundant systems that are each capable of processing 100 percent of the potential system load.

3.1.3.2 Considerations for Redundancy

- Redundant data centers, infrastructure, power and cooling of all ESInet mission critical equipment and operations.
- Redundant power supplies and processors.
- Automatic failover for uninterrupted operation, even with failed components.
- Critical loads at a level of 2N, 2N+1, or higher.
- Passive or Active redundancies as the need demands.

3.1.4 Survivability

Survivability is defined as the ability to plan for and then recover in times of a disaster or some other catastrophic failure. The following should be considered:

[5] DHS requires the use of Telecommunications Service Priority for all "vital voice and data circuits".

- A Continuity of Operations Plan (COOP) for all sites.
- Hot standby for ESInet mission critical applications at all sites.
- Disaster Recovery (DR) and Business Continuity Plan (BCP) in place for all sites.
    - Alternate facility or facilities that can be utilized for fail over.
    - Multiple geo-diverse sites.
    - Diverse communications links.
- Periodic testing to ensure that all COOP and DR plans can be successfully executed.
- Validate that normal operations can be restored.

2.2 Local Area Network (LAN) Architecture

If 9-1-1 traffic is using a LAN, that LAN is considered a component of an ESInet. The PSAP LAN is considered to be part of an ESInet even though parts or all of the LAN may be provided by a third party or other local agency. In a hosted model, the best case scenario for a LAN providing access to the Next Generation Core Services (NGCS) would be private to the NGCS application environment. Distribution of NG9-1-1 services from the NGCS may use the ESInet to the PSAP. Best practices would have the connection from the PSAP ESInet demarcation be secure. Only use the PSAP (administrative) LAN if the PSAP LAN is fully within the ESInet security boundary or if a PSAP security boundary is established. In many cases vendors of the IP enabled or NG9-1-1 call taking system will provide and configure the LAN switches and can influence strategic ESInet decisions.

Analysis and assessment of the components for an ESInet can impact the design. It is important to evaluate the functional components residing on the LAN to aid in ESInet planning. This is due in part to the large number of requirements that the IP enabled 9-1-1 call taking systems place on the LAN. It is a best practice to deploy at least two LAN switches at each site.

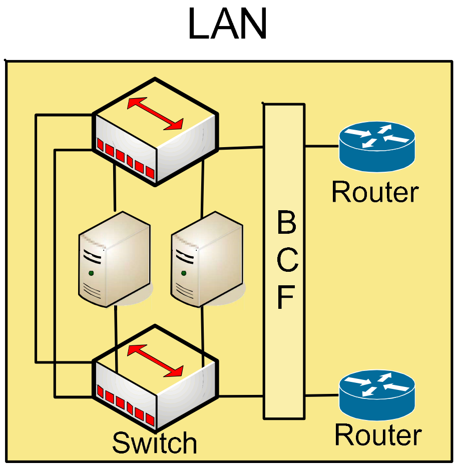


Figure 2

The workstations and/or servers shown above are typically equipped with dual Network Interface Cards (NICs). Each NIC is connected to a LAN switch. The switches are connected to each other and to the BCF (i.e., Session Border Controller(s) and/or firewall(s)) that is attached to an ESInet's router(s). It is a best practice to utilize managed switches in ESInets. Separate networks for different vendors are not recommended. In most cases the use of multiple VLANs (IEEE 802.1Q) can achieve sufficient isolation of network components in a shared infrastructure.

2.3 WAN Architecture

The textbook definition of a Wide Area Network (WAN) is a computer network spanning regions, countries, or even the world. However, in terms of ESInet, it is best to view an ESInet as a WAN since the network can often be used to transmit 9-1-1 data over relatively long distances, and between multiple LANs.

Typically, WANs are built utilizing leased or state/municipality-owned telecommunication services to share information across geographical locations. The public Internet may be considered a WAN as well, but it is not considered an ESInet because it is not restricted to public safety access.

WANs are commonly built using a series of network devices such as routers and Ethernet switches that are connected together by transmission circuits and devices more suitable for longer distances. Technologies such as T1/DS3, SONET, Metro-Ethernet, etc. (further details are provided throughout this section below) are commonly used to build WANs.

WANs are usually connected to LANs by a smaller router, switch, or firewall on the premises that acts as a demarcation point (covered in section 2.12) between the service provider and the PSAP.

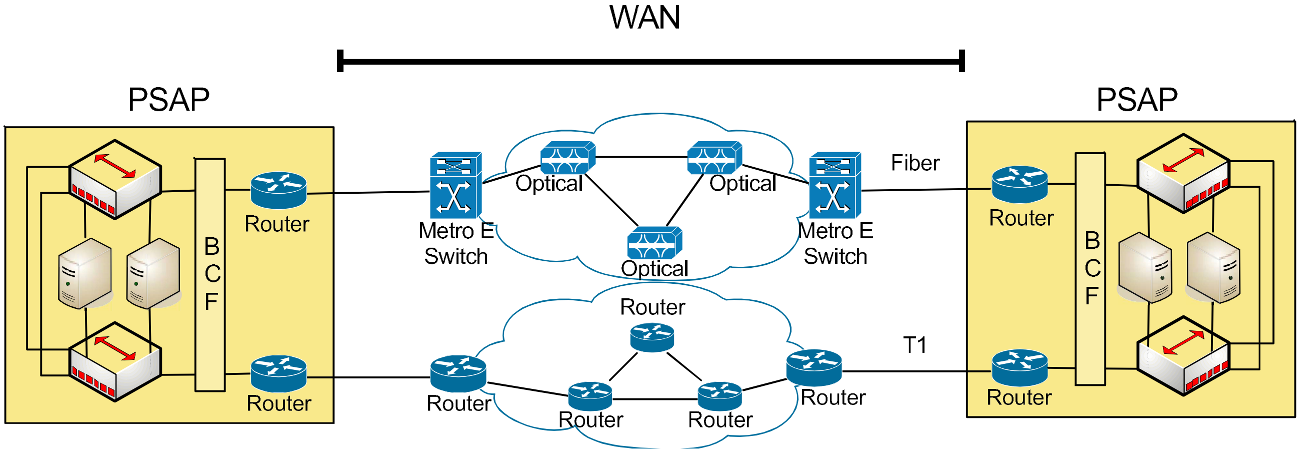


Figure 3

Note: This diagram represents a dual core high reliability model. However a single core is often deployed.

2.4 Hardware / Equipment Elements

Some of the equipment required to build an ESInet (i.e. routers, firewalls, Session Border Controller(s), etc.) can be leased. Many other components will have to be purchased. It is a best practice to purchase and/or lease equipment that meets the following criteria:

- High availability and reliability

- Proven track record
- Acceptable warranty
- Qualified/trained support personnel
- Supported 24/7/365
- Acceptable Mean Time To Repair (MTTR)
- Acceptable Mean Time Between Failures (MTBF)
- Scalability
- Fault tolerant
- Management tools
- Security (which should be evaluated in conjunction with the NENA NG-SEC Security Standard)

2.5 Network / Software Elements

Some of the networks and services that comprise an ESInet may be vendor-specific. Others may be purchased as part of a managed service that can provide ESInet capability for a monthly service fee. It is a best practice to purchase and/or lease equipment that meets the following criteria:

- Conforms to FCC reporting requirements[6]
- Maintains access and password control
- Provides technical escalation for troubleshooting
- Qualified/trained support personnel
- Vendor supported 24/7/365 support
- Offers sufficient redundancy
- Offers a level of scalability
- Procedures for recognition and recovery from faults
- Offers managed service
- Security that meets the NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) [3]

2.6 The Open Systems Interconnection (OSI) Model

The OSI model is a conceptual model that standardizes how computer systems communicate with each other across LANs and WANs. While it is a defined standard (ISO 7498-1 [10]), it is more commonly used as a reference architecture.

[6] Part 4 of the FCC's rules (47 C.F.R. Part 4). Communications providers must also report information regarding communications disruptions affecting Enhanced 9-1-1 facilities and airports that meet the thresholds set forth in Part 4 of the FCC's rules.

A central tenant of the model is that communications take place between systems and devices at discreet layers. Each layer is responsible only for communicating with the layers above and below it as well as the same layer on a different system. In this way, systems may communicate with each other even if they are running completely different applications or operating systems. Although TCP/IP is not technically based on the OSI model, it does fit well within the construct.

The following sections will group various functions, protocols, and applications by their respective layers.

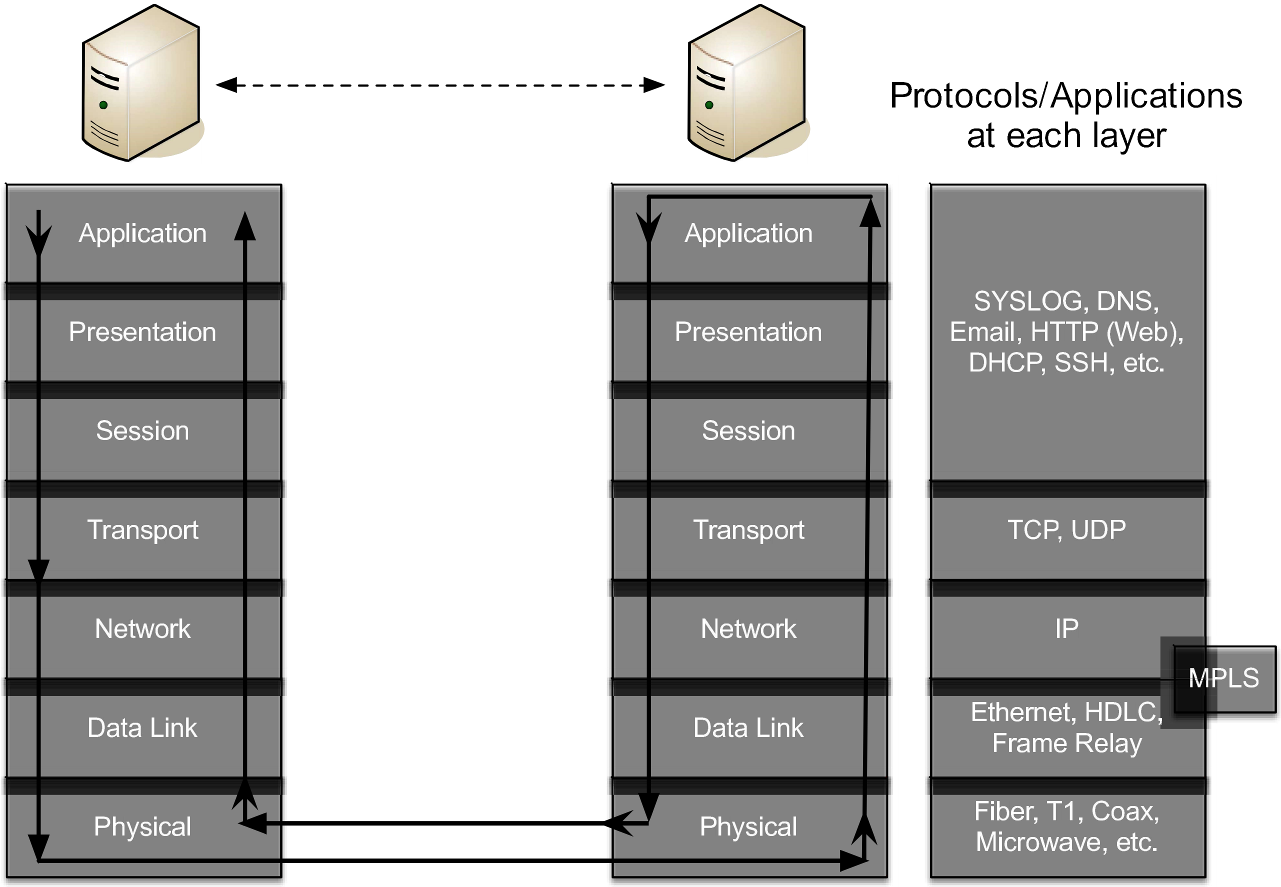

Protocols/Applications at each layer
Application
Presentation
Session
Transport
Network
Data Link
Physical
Application
Presentation
Session
Transport
Network
Data Link
Physical
SYSLOG, DNS, Email, HTTP (Web), DHCP, SSH, etc.
TCP, UDP
IP
MPLS
Ethernet, HDLC, Frame Relay
Fiber, T1, Coax, Microwave, etc.

Figure 4

This document focuses on Physical, Data link, Network and Transport layers.

2.7 OSI Layer 1 / Link Layer

In this section we will discuss different types of physical wired and wireless connections that are typically used to deliver services to a site that is connected to an ESInet, and some of the caveats and best practices utilized when designing the physical layer of an ESInet.

For the most part, circuits are delivered to sites connected to an ESInet over one of the following transport mediums:

- Copper facilities

- Coaxial facilities
- Fiber facilities
- Wireless communication networks
- Satellite communication networks

2.7.1 Copper facilities

Copper continues to be widely utilized for digital infrastructure in the United States. However, many Local Exchange Carriers (LEC) and local Telephone companies are planning for, or have largely eliminated copper within the core network, and are aggressively working to replace copper with fiber in the 'Access' network (distribution from Local Serving Office (LSO) to customer).

During ESInet planning, PSAPs must consider the eventuality that copper based facilities and the services delivered on copper may be discontinued by their service provider. Copper services, including T1/DS1 are typically regulated and subject to FCC unbundled loop regulation, requiring the ILEC to lease these facilities to Competitive Local Exchange Carriers (CLEC). The elimination of copper T1/DS1 may subject the PSAP to unregulated (un-tariffed) pricing for services.

Services delivered over copper are frequently multiplexed onto fiber facilities at the Central Office, but in many cases the last mile of a 3 Mbps or slower data circuit will be delivered over copper. Last mile distribution is common using T1/DS1 for 1.544Mbps DATA circuits. Multiple T1/DS1s can be bonded for higher capacity data pipes offering 3Mbps, 4.5Mbps, and higher capacities. Other copper services (besides T1/DS1) are also available, but not common (ATM, Frame, etc.). When multiplexing is used, it is important to consider where potential areas lack diversity. Circuits may be contained in the same point of presence (POP), same rack, or same equipment shelf. Where this occurs, it can present a potential single point of failure in an ESInet. During the planning phase, it is important to identify potential single points of failure from all service providers being considered for an award.

Copper based facilities considerations:

Advantages

- Repairs are relatively simple and fast
- Easier to troubleshoot and maintain
- Many technicians are already familiar with this technology

Caveats

- Subject to electromagnetic interference (EMI)/Environmental issues
- Grounding issues

2.7.2 Coaxial (Coax) facilities

Coax is a copper core medium that can carry higher bandwidth in the access network as a result of physical transmission characteristics, often used for delivery of T3/DS3 rate facilities.

T3/DS3 circuits which have a capacity of 44.736 Mbps are delivered over coax cables. T3/DS3 signals are used for interconnections and as an intermediate step before being multiplexed onto a larger carriage type of circuit such as Synchronous Optical Networking (SONET).

DS3 stands for Digital Signal level 3; DS is a channelized schema intended for 64kbs voice circuits, but is often used in data networks. The precise T3/DS3 specifications are found in the T-carrier standards developed by Bell Labs for the telephone industry. A DS0 is the smallest unit with a bandwidth of 64 Kbps and can deliver one digitized telephone call using PCM (Pulse Code Modulation), the original digital phone standard. 24 DS0s are combined into a single circuit called a DS1. A DS1 can be delivered on a T1 line to the end location. A DS3 is the equivalent of 28 DS1s or 672 DS0s.

1DS0 = 1 Call
1DS1 = 24 DS0s
1DS3 = 28 DS1s (672 DS0s)

The bandwidth of the combined 672 voice channels is 44.736 Mbps, commonly referred to as 45 Mbps. A DS3 is often ordered and installed as a high capacity trunk for multiple services at a location.

When an order is placed for a DS3 service, it is delivered on a pair of 75 ohm coaxial cables using Bayonet Neill–Concelman (BNC) connectors. The coaxial cable used to connect a DS3 router can be no more than 450 feet in length (only 225 feet if using small diameter coax).

Provisioning of DS3 services can be via fixed wireless transmission or SONET fiber optic service.

Coax based facilities considerations:

Advantages

- Repairs are relatively simple and fast
- Easier to troubleshoot and maintain
- Can provide higher bandwidth than copper
- Can be integrated into a SONET ring architecture or other redundant, resilient transport method
- Can provide MPLS interfaces and/or Metro Ethernet

Caveats

- Limited to TDM bandwidth
- Subject to EMI/Environmental issues
- Grounding issues

2.7.3 Fiber facilities

Largely due to the advantages listed below, most of our nation's digital infrastructure is built on fiber optic circuits. Fiber is also being deployed as a last-mile medium in communities across the country. When fiber can be delivered to the premise it is the preferred option for the physical connection of an ESInet due to several factors. It should be noted that many last mile fiber networks are often referred to as Fiber-to-the-Premise (FTTP). However, most FTTP deployments are often bundled offerings for commercial enterprises, which may not be an effective service offering for an ESInet. A direct dedicated fiber connection to the building (which can be referred to as "dark fiber" or "lit fiber" depending upon the configuration) may be a more effective alternative and could provide a critical aspect of a diversified infrastructure.

Advantages

- Fast Transmission Rates
- High Bandwidth
- Long Distance
- High Resistance to Interference/electromagnetic noise
- Low Maintenance
- Not subject to EMI

Caveats

- Repairs can be relatively difficult and slow
- Commercial or Enterprise grade services are recommended
- Cost

2.7.4 Cellular Wireless Communication Networks

Current network deployment of 3G (e.g., HSPA) and 4G (i.e., LTE) technologies[7] is maturing for more densely populated areas and therefore most PSAPs would have above average coverage to utilize for data link capability. The highest capacity wireless networks currently are 4G (LTE).

Even before 4G (LTE) network coverage is fully deployed, current deployment levels offer advantages to the PSAP for low-cost network connectivity for both primary and backup applications.

Public safety LTE implementations (e.g., FirstNet) will provide multimedia and streaming capabilities to First Responders. ESInets built with 4G (LTE) Public Safety networks should consider using the data path of these networks as a core component of an ESInet and/or as a method of increasing the reliability/redundancy of an ESInet. See section 2.7.8 for more information on the FirstNet initiative.

[7] At the time of publication, 5G standards are being finalized and deployments have been announced for 2018. 5G promises speeds up to 10Gbps.

Advantages

- Adequate data bandwidth for 3G to support data (nominally ~10 Mbps up/down)
- Devices that offer 3G and 4G capabilities provide some amount of built in path redundancy between the respective built in technologies (e.g., EVDO/LTE, HSPA/LTE)
- Additional bandwidth provided by 4G (LTE) provides very good data throughput support. 4G (LTE) increases that to ~75Mbps up/down. Exact bandwidth of 4G (LTE) networks will vary by implementation with the potential to reach 1Gbps.
- The portable nature of 3G mobile hotspot technology provides easy (though limited) scalability to support several call termination endpoints. 4G (LTE) significantly increases the portable hotspot capacity.
- Low cost
- Can scale to take advantage of multiple mobile hotspot devices
- Uses encrypted access path
- Less likely to be interrupted by cable cut that would impact other services to the PSAP

Caveats

- Bandwidth is not guaranteed, but best effort, based on adjacent network capacity
- Shared public access network services unless using Public Safety-specific networks
- Pricing and data transmission caps must be clearly understood and factored into ESInet costing
- Can be limited by the backhaul capacity

2.7.5 Microwave

Microwaves are electromagnetic wavelengths with frequencies between 300 MHz and 300 GHz. In 2002 the FCC designated the 4.9 GHz band for use in support of public safety. The FCC has also approved building wireless broadband networks for first responders in the 700 MHz band. These microwave spectrums and others are being utilized to provide redundant WAN links to PSAPs. A best practice is to have radio links for ESInets engineered by professionals as it tends to significantly increase the reliability of the links.

Advantages

- Physical diversity – over-the-air so not in same conduit/trench as copper/fiber
- No cable(s) required between sites
- Microwave has multiple channels available for use
- Low power requirements for repeaters
- Easy implementation/installation into some areas

- Can be installed on existing support structures/masts

Caveats

- Range is limited to approximately 25 miles
- Line of Sight is required
- Typically point-to-point connections
- Towers are expensive to construct/build
- Attenuation due to atmospheric conditions possible
- Tower maintenance can be problematic

2.7.6 Satellite

Satellite communications provide for connectivity to remote sites where traditional fixed line (copper or fiber) telephony/data lines cannot reach. It may provide an alternate redundant transport facility as part of a PSAP's survivability strategy for both telephone network and data infrastructure. Current satellite communications systems exist that are viable within a disaster contingency plan for continuity of operations.

Satellite communications is achieved using ground stations, which send and receive radio signals to/from orbiting satellites. The satellites orbital path dictates its distances from the earth, which determines the time it takes information to travel to/from the satellite. This round trip delay for transmission alone adds (inherently) about ½ second. This delay mostly affects real time two-way communications such as voice, resulting in echo as perceived by users. However, the impact on voice communication can be minimized by using echo cancelation on the satellite link used for voice. Today there are many Satellite VoIP-based and packet services in operation. New satellite communications systems have been deployed utilizing "medium and low level Earth orbit" satellites that can minimize the negative impact on latency.

Advantages:

- Access to remote locations
- Can be used in emergency situations providing communications to PSAPs, alternate PSAPs, and mobile response centers
- Segregated from the wireline infrastructure
- Can be used for both VoIP, video, and data

Caveats:

- Design efforts that may be needed to overcome satellite behavior characteristics include:
  - Latency (Delay) introduced by the distance the IP packets must transverse require the use of echo cancellation. Echo cancellers used with terrestrial transmission system are

designed to handle tens of milliseconds while satellite echo cancellation function must handle one half second delays.

- Jitter over Satellite requires dynamic jitter buffering on the listening direction to reduce degradation of the voice conversation.
- Large Data Packet Fragmentation is required to insure higher priority voice IP packets are not delayed by the time required to transmit large data packets.

- Cost
- Security - encryption may be required to insure secure transmission over a shared satellite facility
- Highly limited bandwidth

In the event that Satellite communications systems are used, there are several technical and operational considerations that can impact the performance of network.

1) Satellite is not an optimal solution nor is it recommended as a primary system for an ESInet.
2) There may be cases where satellite is available and its use may be a necessary component of ESInets.
3) The use of SIP on a satellite network may require additional configuration changes that are not included in the scope of this document.
4) Protocol operation and timing may require adjustments to ensure that the applications on the ESInet are functional.

There are areas that satellite is an acceptable broadband connection. Where this is the norm, all of the functional components must be reconfigured including the aspects of call delivery.

2.7.7 Wi-Fi®

Connection to an ESInet may require wireless connection via a private or public Wi-Fi® network. Wi-Fi® is a local area wireless technology that allows an electronic device to exchange data or connect to a network using Ultra High Frequency (UHF) or Super High Frequency (SFH) radio waves. The name is trademarked, and is a play on the audiophile term Hi-Fi. The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards".

Many devices use Wi-Fi®, e.g., personal computers, video-game consoles, smartphones, digital cameras, tablet computers, and digital audio players, and can connect to a network resource such as the Internet via a wireless network access point. Access points are part of an in-building wireless network and the network is typically a series of hubs, repeaters, and multiple band antennae placed within the building.

Access points (or hotspots) have a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can comprise an area as small as a single room with walls that block radio waves, or as large as many square kilometers achieved by using multiple overlapping access points. Wi-Fi® can be less secure than wired connections (such as Ethernet), because an intruder does not need a physical connection, however, the Wi-Fi network can and must be secured via the highest security protocol that is available on the equipment being utilized in accordance with an approved wireless security policy or the NENA NG-SEC standard [3].

PSAPs commonly have Wi-Fi® hotspots to facilitate communications for laptops, smartphones, tablets, and other mobile devices, and the hotspots are enabled by indoor antenna systems.

Advantages:

- Allows users to access network resources from nearly any convenient location within their primary networking environment
- Mobility
- Users connected to a wireless network can maintain a nearly constant affiliation with their desired network as they move from place to place
- Expandability
- Relatively low cost

Caveats:

- Security must be planned for and managed
- Range and reach may be limited
- Reliability can be an issue when connecting multiple devices that utilize different protocols
- Speed

It must be pointed out that in some instances compatibility issues among Wi-Fi devices and components may arise. When Wi-Fi is used as a transport medium in an ESInet it is important to understand the entire Wi-Fi solution to avoid errors. Furthermore, the security of Wi-Fi as a transport medium can be limited. ESInet designs using Wi-Fi may require additional security measures to reach the level described in NG-SEC [3].

2.7.8 FirstNet[8]

The First Responder Network Authority (FirstNet) was established by federal law in 2012 to implement an interoperable wireless Nationwide Public Safety Broadband Network (NPSBN), under the National Institute of Standards and Technology (NIST), dedicated to emergency responders for public safety. When the FirstNet network is initially deployed, it will provide mission-critical, high-speed data services to supplement the voice capabilities of today's land mobile radio (LMR) networks. FirstNet users will be able to send and receive data, video, images, text, as well as use voice applications. They will communicate over the network and benefit from the ability to share applications. In time, FirstNet plans to offer Voice over LTE (VoLTE). VoLTE can be used for daily public safety telephone communication. The intent is to configure the network utilizing LTE (4G)

[8] For current information on FirstNet please refer to https://www.firstnet.gov/network

type wireless service under the 700 MHz D block spectrum. 4G is the most advanced wireless technology available and is a globally-available service. There is ongoing research and development on an international set of standards that will allow FirstNet to offer mission-critical voice (MCV) when these capabilities become available. The intent is that the same MCV technologies will then work across all standards-based equipment and networks worldwide.

Funding for FirstNet is provided through FCC-conducted spectrum auctions and the actual build-out of the FirstNet capability is a consultative process, currently underway, where the FirstNet Board is meeting with Federal, State, tribal, and local public safety entities to ensure that the FirstNet network is designed to meet public safety needs. FirstNet is currently involved in defining the standards and is presently working closely with public safety organizations to support the development of standards and technical features and functions that meet the needs of the public safety users.

From a contextual perspective, an ESInet is a more *terrestrial*-based IP network fabric designed to receive and process requests (voice, video, pictures) for emergency service from the public and into the PSAP's associated call processing and dispatch systems. FirstNet is a *wireless* broadband network designed to provide dedicated public safety capacity for first responders to receive data and eventually mission critical voice for use in responding to emergency situations. An ESInet is designed to accept more types of data into the PSAP (voice, video, and pictures) and without an implementation of FirstNet-type capabilities, the PSAP will be less able to push that data out to first responders as the current public safety wireless infrastructure for first responders cannot accept the significant quantity of data that an ESInet will be able to provide.

FirstNet broadly defines its LTE network in distinct layers: Core Network, Transport Backhaul, Radio Access Network (RAN), and Public Safety Devices. Backhaul carries the voice, data, and video traffic on the network and provides the connections between cell sites and the core wireless broadband network. Since backhaul will also connect FirstNet to the Internet and other networks, FirstNet may provide some unique opportunities for ESInet coverage. As the deployment of FirstNet continues, it is important for those involved with ESInet design to remain open to utilizing FirstNet services where appropriate. However, FirstNet (as presently defined) is an external network to the ESInet and all connections to FirstNet must transit through appropriate security boundaries and may be limited by bandwidth restrictions.

FirstNet facilities considerations:

Potential advantages:

- May offer transport options for an ESInet
- Wide geographic coverage

Potential caveats:

- Limited bandwidth coverage (presently)
- Service Management of the network (presently)

2.8 OSI Layer 2

Some of the most popular layer 2 protocols and technologies utilized to build ESInets are High-Level Data Link Control (HDLC) (i.e., T1/T3), Asynchronous Transfer Mode (ATM), Metro Ethernet, and Multiprotocol Label Switching (MPLS)[9]. This section covers some of the advantages, disadvantages, caveats, and best practices utilized when designing the data link layer of an ESInet.

2.8.1 High-Level Data Link Control (HDLC)

HDLC links (i.e., T1/T3) have been utilized as the backbone for data networks for decades. These networks are highly reliable and have very low latency. Typically they are symmetric channels; with data rates in multiples of 1.544 Mbps. Multiple HDLC connections can be delivered to the same site to increase the aggregate capacity. HDLC links can be utilized for dedicated point-to-point connections where they are typically private (i.e., not shared).

HDLC links are provided over copper based facilities and share the advantages and caveats of typical copper plant:

Advantages:

- Repairs are relatively simple and fast
- Easier to troubleshoot and maintain

Caveats:

- Limited capacity in terms of bandwidth
- Subject to EMI/Environmental issues
- Grounding issues
- HDLC is still available in many areas and continues to be a popular choice. However, as with most copper based services, HDLC is expected to be discontinued by the LECs in the near future.

2.8.2 Frame Relay

Frame Relay was deployed in the early 1990s – approximately 10 years before VoIP was introduced to the commercial market. It was initially designed to transport data. After the advent of ATM, upgrades were made to Frame Relay which enabled it to transport real-time data (i.e., voice and video). However, Frame Relay is being phased out. So while it may be possible to design an ESInet based on Frame Relay, it is not recommended.

Frame Relay is provided over copper-based facilities and shares the advantages and caveats of typical copper plant:

Advantages:

- Repairs are relatively simple and fast

[9] MPLS and ATM are not strictly speaking layer 2 technologies; however they are included here because they are alternatives to true layer 2 technologies described in this section.

- Easier to troubleshoot and maintain

Caveats:

- Limited bandwidth
- Subject to EMI/Environmental issues
- Grounding issues

As indicated above, Frame Relay service is also expected to be discontinued for new customers by the LECs and other carriers in the near future.

2.8.3 Asynchronous Transfer Mode (ATM)

Although not commonly available for new applications nowadays, some ATM can still be found in service. If available, Asynchronous Transfer Mode (ATM) may be used in areas that can support an ESInet. ATM is a cell-based[10] switching technology that can guarantee deterministic Quality of Service (QoS). It was designed to transport real-time voice, data, and video. ATM utilizes three main classes of service: Constant Bit Rate (CBR), Variable Bit Rate (VBR), and Unspecified Bit Rate (UBR).

The Constant Bit Rate (CBR) class of service was designed for applications that require a constant guaranteed bit rate between devices located across a Wide Area Network (WAN). CBR emulates Time Division Multiplexing (TDM) and requires more resources than the other classes of service. CBR is not as efficient or economical as other classes of service, but CBR provides an assurance for QoS for real-time services CBR is typically not recommended as a foundational infrastructure for an ESInet.

The Variable Bit Rate (VBR) class of service is utilized by many companies throughout the world to transport a mix of real-time traffic such as voice and video, and traffic without real-time requirements (e.g., data). While it is technically possible to accommodate individual voice and video calls as individual circuits, practically, ESInets would be engineered to have all traffic on a single virtual circuit. Should ATM be available and included in the network design, it is a best practice to utilize VBR connections for ESInets.

Unspecified Bit Rate (UBR) is a best-effort transport and is typically used for IP services with no guaranteed bit rate. UBR is a common class of service for networks such as ESInets. However, the circuits must be over-provisioned/over-engineered in an attempt to prevent the best effort traffic from being dropped or delayed in the service provider's core network(s).

ESInets built on ATM networks typically utilize Permanent Virtual Circuits (PVCs) to build connections between WAN sites. The PVCs are identified by using a Virtual Path Identifier (VPI) / Virtual Circuit Identifier (VCI). A primary benefit of the ATM technology is the ability to reroute PVCs around layer 1 and/or layer 2 network outages.

ATM circuits are typically purchased in bit delivery rates (bandwidth) anywhere from 1.5-Mbps to 155-Mbps. ATM is a proven technology that is well suited for ESInets, but may not be available in

[10] An ATM cell is fixed at 53 octets (5 octets for the header and 48 octets for the payload).

every region of the country or by some service providers in a particular region. Additionally, it is likely to be replaced by newer technologies such as MPLS.

Advantages:

- High Bandwidth
- Dedicated PVCs
- Private
- Low Latency
- Scalable
- Deterministic Quality of Service

Caveats:

- Regional Availability
- Efficiency
- End of Life
- ATM is still available in some areas but is being migrated to Metro Ethernet and MPLS (described below).

2.8.4 Metro Ethernet

There are ESInets in operation today which have been built on Metro Ethernet services. Metro Ethernet provides a scalable, high performance broadband platform that supports next-generation voice, data, and video.

Metro Ethernet is a technology that uses several classes of layer 2 technologies to provide a service that behaves much like an Ethernet (CSMA/CD[11]) over a wide area. Unlike Frame Relay and ATM, where the standards largely define the service offering and the terms used in describing the technology, Metro Ethernet services vary widely depending on the objectives of the service provider.

Metro Ethernet services are sometimes marketed under names such as Business Class Ethernet or Business Ethernet. Metro Ethernet services are typically provisioned over private, managed networks and sometimes monitored by service providers. Symmetrical rates are available anywhere from 1 Mbps to 10 Gbps. Different classes of service may be supported, or it could be best effort.

It is a best practice to utilize a delay-sensitive class of service for emergency 9-1-1 calls. Priority classes of service may be used for various data within ESInets.

Advantages:

- High Bandwidth (typically up to 10Gbps)

[11] Carrier-Sense Multiple Access with Collision Detection

- Low Cost
- Dedicated
- Private
- Low Latency
- Scalable
- Regional Availability

Caveats:

- Wide variation in services and SLAs/SLOs (Service Level Agreement/Service Level Objective[12])
- Complex Traffic Engineering
- Reliability (varies with service provider)

2.8.5 Multi-Protocol Label Switching (MPLS)

The MPLS technology takes advantage of advancements in technology (high speed switching), industry trends such as the pervasive use of SONET, and builds upon the strengths of earlier layer 2 technologies to provide reliable transport of next generation voice, data, and video.

In an MPLS network, packets are labeled as they enter the network. Packets are forwarded through the network based on the information contained in the label, and label(s) are stripped off the packets as they leave the MPLS network.

Different classes of service are available on some MPLS-based service offerings. Classes of service are not defined in the MPLS standards. The traffic engineers of each service provider utilize traffic trunks, resource allocation, and constraint based routing to implement traffic management within their MPLS network thereby defining the classes of service that will be supported. MPLS classes of service are typically based on some combination of the following: delay/jitter sensitive, high, medium, and/or low priority traffic. It is a best practice to utilize a delay/jitter sensitive class of service for emergency 9-1-1 calls delivered over an MPLS network.

It is not uncommon for service providers to offer an SLA of three nines (99.9%) for services based on MPLS technology. This is due in part to reluctance on the part of the service provider to compensate customers for downtime and may not be a true indication of the availability that is typically achieved on the MPLS networks. Some service providers may offer higher availability, but on an SLO (Service Level Objectives) basis.

[12] Per the Information Technology Infrastructure Library (ITIL) – A Service Level Objective (SLO) refers to a negotiated document that defines the service that will be delivered to a Customer in qualitative terms, although a small number of Key Performance Indicators (KPIs) might also be defined. SLOs are provide a clearer understanding of the true nature of the service being offered, focusing on the contribution of the service to the business value chain. SLO's become quantified by an SLA and the penalties assigned within an SLA.

MPLS was designed to replace existing IP transport technologies such as ATM and Frame Relay, and in many regions of the country the industry is moving in that direction.

Advantages:

- High Bandwidth
- Private
- Scalable
- Regional Availability
- Low Latency
- Efficiency

Caveats:

- Limited Build-out
- Service Level Agreements (SLAs) or Service Level Objectives (SLOs) need to be carefully constructed and managed to ensure adequate service

2.9 OSI Layer 3

This section covers some of the advantages, disadvantages, caveats, and best practices utilized when designing the network layer of an ESInet. Typically, Layer 3 is operated through the use of the Internet Protocol (IP) routing functions. IP routing utilizes the transport components discussed in the previous section and enables routers to interconnect with each other resulting in a logical network.

2.9.1 IP Addressing

Devices that are connected to an ESInet will be configured with an IP address. Today 98% of all devices that are configured with an IP address are utilizing IP version 4 (IPv4). Due to the proliferation of devices that utilize an IP address, the pool of public/registered IPv4 addresses is rapidly approaching exhaustion.

Researchers have been developing methods of extending the life of IPv4 addressing for decades. Two of the most commonly deployed methods are RFC 1918 Private Address Space and RFC 2663 the Network Address Translator (NAT). Among other things, NAT enables devices that are configured with private IP addresses to be able to reach the Internet and/or vice versa (devices on the Internet able to reach devices configured with private IP address). In order to delay the transition to IPv6 some service providers are deploying IPv4 NAT within the core networks which results in multiple NATs between the caller and the PSAP. However, there is a limit to the effectiveness of these methods to extend the life of IPv4. For example, NATs generally don’t know how to fix addresses that are embedded in protocols such as SIP.

Network Address Translations (NATs) are not recommended to be used within an ESInet. However, NATs may be needed in specific deployments, and therefore all network elements must operate in the presence of NATs. When designing an ESInet, NATs and their location within an ESInet are an important consideration, especially regarding traffic flow through an ESInet.

It is recommended that elements connected to an ESInet not be referred to by their IP address but rather through a hostname using DNS. Use of statically-assigned IP addresses should be limited, and should never be used with IPv6 addresses. Dynamic Host Configuration Protocol (DHCP) must be implemented on all network elements to obtain IP address, gateway, and other services.

When networks deploy NAT, there are often issues where some protocols embed IP addresses in signaling messages. NATs often "fix" the problem for protocols like HTTP, but don't for other protocols. Application Level Gateways (ALGs) are used to fix the problem for other protocols. For SIP, the Session Border Controller (part of an ESInet Border Control Function) performs this function. However, many SBCs, especially low-cost SBCs, don't address Message Session Relay Protocol (MSRP), which is used to transport text. Note that Short Message Service (SMS) is interworked to MSRP prior to enter the ESInet and thus MSRP support is required to support SMS. Sending MSRP through a NAT, even with a low-end SBC, may result in the inability to handle text and SMS. Again, a recommended method is to avoid the use of NATs.

Where sufficient IPv4 addresses are available for use on an ESInet, it is recommended that all addressable elements in such ESInets are given a globally-routable IPv4 address.

Private addresses will be necessary for many ESInet elements where insufficient IPv4 address assignments are available. RFC 1918 Private Address Space should be utilized in the smallest possible ESInet configuration.

If there are regional ESInets, private addresses should be limited to those regional networks.

Where there is no regional network and the State ESInet connects to PSAPs directly, private addresses may be required on the State ESInet (Reference NENA-STA-010 [1] call paths).

Internet Protocol version 6 (IPv6) is the version of the Internet Protocol designed to succeed IPv4. IPv6 is not all that much different from IPv4. It has a number of incremental improvements, yet can be summarized as IPv4 with 128 bit addresses. This allows for a practically unlimited number of IP addresses (about $3.4x10^{38}$). One of the challenges with IPv6 is that it is not backwards-compatible with IPv4. In other words, a host with an IPv6 address cannot directly communicate with an IPv4 host.

In accordance with North American Network Operators Group (NANOG) best current operational practices, addressing plans for IPv6 should be allocated as follows:

- /48 for a regional ESInet

- /56 per site (PSAP)
- /64 per network segment
- /126 or /127 for point-to-point links (given vendor compliance with RFC 6164)
- /128 for loopbacks

For further reference and details see NANOG (http://bcop.nanog.org/index.php/IPv6_Subnetting) or ARIN (https://getipv6.info/display/IPv6/IPv6+Addressing+Plans).

The original intent of the developers of the IPv6 technology was to include a period of "transition". During this transition, all end systems, ISPs and services would support both IPv4 and IPv6 simultaneously. When the point was reached where this “dual stack” environment was universally deployed, IPv4 could be dropped and an IPv6 only version of the Internet would result.

The IPv4 registered address pool is nearing exhaustion and IPv6 deployment is between 0.2 and 2% of the Internet. The organizations that assign IP addresses expected the effects of IPv4 address depletion would be felt beginning in 2011. Largely due to cost, complexity, and other more pressing issues, many organizations have put off IPv6 migration. At this time, it seems unlikely that the transition period will be short.

It is a best practice to design and deploy ESInets in a dual stack (IPv4 and IPv6) environment so as to allow for the interoperation of existing IPv4 devices and infrastructure with future emergency services devices and infrastructure that will be constrained to operate only with IPv6 addresses.

Services within an ESInet should be designed to use IPv6.

2.9.2 Dynamic Routing Protocols

Dynamic routing protocols are commonly used within ESInets to determine the best route/path to use to transport IP packets to their destination. Routing protocols dynamically discover and re-route around outages, and they simplify the configuration and maintenance of routing within an ESInet. It is a best practice to utilize a dynamic routing protocol within an ESInet where two or more paths to a destination exist. IPv6 uses the same types of routing protocols as IPv4, but with some slight modifications to account for specific requirements of IPv6. This section evaluates some of the routing protocols which are commonly used for ESInets.

When working with dynamic routing protocols, one of the important concepts that may require additional attention is the autonomous system (AS). An AS is a network or a group of networks that is controlled by a common network administrator (or group of administrators) on behalf of an entity (such as a regional 9-1-1 authority.)

It is a best practice to configure regional ESInets to be their own AS. Thus, routers at individual PSAPs can be configured to run an Interior Gateway Protocol (such as Open Shortest Path First –

OSPF, Intermediate System to Intermediate System – IS-IS, etc.). State and national level ESInets should utilize Border Gateway Protocol (BGP) to route between autonomous systems.

It is recommended that networks also utilize bidirectional forwarding detection (BFD) to quickly detect failures in links between routers. BFD allows routers to become aware of anomalies in the network on a millisecond scale, whereas the default timers on the higher level routing protocols will not suffice and can lead to momentary outages.

3.9.2.1 Interior Gateway Protocol (IGP)

The choice of an Interior Gateway Protocol (IGP) is dependent on local experience or interaction. IGP should be configured carefully and a strategy for the entire network implementation must be considered. For example, static routes to each element should be avoided. Use of the Routing Information Protocol (RIP) should be carefully planned and not used as a primary method of routing within a single routing domain. When RIP is used at any point in the entire network problems could occur ranging from slow convergence to routing loops.

3.9.2.2 Open Shortest Path First (OSPF)

OSPF is a link-state routing protocol that was defined in RFC 2328 in 1998. It is one of the most widely used Interior Gateway Protocols (IGP). OSPF is frequently used in conjunction with BGP for MPLS networks. OSPF is used to route within a single routing domain (i.e., autonomous system - AS) and BGP is used to interconnect autonomous systems. OSPF Version 2 is limited to IPv4. When utilizing OSPF for routing within a regional ESInet, it is a best practice to utilize OSPF Version 3 which includes support for IPv6.

3.9.2.3 Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is a proprietary Interior Gateway Protocol developed by Cisco. EIGRP is very efficient and feature rich routing protocol that supports IPv6 and is appropriate for use within regional ESInets. EIGRP is primarily utilized by Cisco routers and can provide similar IGRP (predecessor of EIGRP) functionality for networks that utilize Cisco hardware.

3.9.2.4 Intermediate System to Intermediate System (IS-IS)

IS-IS is a link-state routing protocol standardized by RFC 1142. IS-IS is an Interior Gateway Protocol that provides fast convergence, scalability, and is very efficient in its use of network bandwidth. It is commonly used in large service provider networks, supports IPv6, and is appropriate for use in regional ESInets.

3.9.2.5 Border Gateway Protocol (BGP)

BGP (version 4) is an Exterior Gateway Protocol that is defined in RFC 4271. Unlike the previously discussed routing protocols which are used to find a specific network within an Autonomous System

(AS), BGP is used to find the AS where the given network can be found. Since BGP requires peer authentication, a router that wants to share route information with a BGP router should first authenticate. BGP is also very flexible in terms of how routing updates are to be handled. BGP routers can be configured to send specific route updates to specific peers and/or not receive updates from specific peers. These are only a few of the characteristics that make BGP the routing protocol of choice when connecting to untrusted networks. In many cases BGP is the only dynamic routing protocol supported by service providers when connecting to an MPLS network. It is a best practice to utilize BGP in state-level and national-level ESInets.

BGPSEC is an option to BGP to consider that allows an Autonomous System (AS) to verify the legitimacy and authenticity of route advertisements. BGPSEC uses Resource Public Key Infrastructure (RPKI) certificates that are issued to AS number and IP address holders that allow specific authorization for AS numbers to originate BGP routes to them and vice versa.

In many networks, there are multiple independent ISPs that supply connectivity to an ESInet. It is often the case that a primary path is announced (via BGP for example), while the secondary path is available, but not announced unless the primary ISP connections fail. Network management must recognize that these secondary paths are vitally important. They must be maintained vigilantly as the primary paths because the secondary may be called upon if the primary fails. This is because clients, such as call origination networks, may be directly connected to the ISP that provides the secondary path. Should this be the case, the ISP may deliver traffic via its network (and thus the secondary path) rather than using the primary network, because it would result in “on-net” traffic.

When an ESInet is using primary and secondary connections it is a good practice to test both connections on a consistent basis. It is also important to factor in the switch-over time between primary and secondary to maintain voice calls.

2.10 Availability and Reliability

Availability and reliability are key concerns for 9-1-1. It is well known that the availability objective for 9-1-1 service is five nines (99.999%). It is not well known that this standard typically has not been met in terms of network connections to the PSAPs in legacy 9-1-1 (i.e., CAMA trunks and ALI circuits). ESInets provide an opportunity for 9-1-1 entities to build to a higher standard, though the resources required to do so must not be assumed, and must be factored in during the design phase.

In this section the definitions of reliability and availability are given[13]. The formulas used by reliability engineers to design and calculate the reliability and availability of systems are described, and examples are given showing the application of each equation.[14] What it takes to achieve five nines availability on network connections is examined. And, a description is given of how five nines availability for 9-1-1 service has been achieved in legacy 9-1-1 while operating on networks that are

[13] Call failures that occur before the call reaches an ESInet (P.01, Wireless Service, VoIP Service Provider networks, etc.) are outside the scope of this document.

[14] Reliability engineering is a science. Most of the sections in the document cover topics that could affect availability and reliability. It is a best practice to engage qualified engineers when designing highly available systems.

less than five nines is given. Failure metrics for ESInets are discussed. And finally, the formulas used to calculate series and parallel availability and reliability are covered and applied to an ESInet.

2.10.1 Definitions and Equations of Availability and Reliability

The difference between reliability and availability is often misunderstood. High availability and high reliability often go hand in hand, but they are not interchangeable terms.

Reliability is the ability of a system or component to perform its required functions under stated conditions for a specified period of time [IEEE 90].[15]

For example, the primary goal of an airline is to complete the flights safely - with no catastrophic failures.

Availability, on the other hand, is the degree to which a system or component is operational and accessible when required for use [IEEE 90].

For example, if a lamp has 99.9% availability, there will be one time out of a thousand that someone needs to use the lamp and finds out that the lamp is not operational, either because the lamp is burned out or the lamp is in the process of being replaced.

An attribute of reliability is,

$$R_a = \frac{Successes}{Attempts}$$

$$where\ attempts = successes + failures$$

For example, if there were 99,999 calls completed to 9-1-1 out of 100,000 attempts, you could claim 99.999% reliability.

Mean Time Between Failure (MTBF) is a basic measure of a system's reliability. The higher the MTBF, the higher the reliability of the system. The equation below illustrates this relationship.

$$R = e^{-\left(\frac{Time}{MTBF}\right)}$$

where e = the mathematical constant e or 2.718281828459045
and Time = time of the mission in hours

[15] IEEE 90 – Institute of Electrical and Electronics Engineers, IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York, NY: 1990

When time is set to 8,760 hours (1 year), the formula above yields the following results:

Reliability	Time (hrs)	Required MTBF (hrs)
0.9	8760	83,143
0.99	8760	871,613
0.999	8760	8,755,619
0.9999	8760	87,595,620
0.99999	8760	875,995,620
0.999999	8760	8,759,995,620

Typical commercial-grade routers often have an MTBF ranging from 240,000 to 340,000 hours. (It should be noted that MTBF is often computed using methods that may not correlate to actual results. Thus depending on the methods used by the manufacturer to calculate the MTBF it may be necessary to reduce the MTBF by as much as half.)

Availability, in its simplest form, can be calculated as,

$$A = \frac{UpTime}{(UpTime + DownTime)}$$

Availability is often thought of in terms of downtime per year according to the following table:

Availability	Downtime
90% (1-nine)	36.5 days/year
99% (2-nines)	3.65 days/year
99.9% (3-nines)	8.76 hours/year
99.99% (4-nines)	52 minutes/year
99.999% (5-nines)	5 minutes/year
99.9999% (6-nines)	31 seconds/year

Mean Time to Repair (MTTR) is the time to recover from a component failure, a failed system upgrade, operator error, etc. The formula below illustrates how both MTBF and MTTR impact the overall availability of the system. As the MTBF goes up, availability goes up. As the MTTR goes up, availability goes down.

Inherent availability looks at availability from a design perspective:

$$Ai = \frac{MTBF}{(MTBF + MTTR)}$$

When an outage occurs, what’s the probability that the redundant system will fail during the MTTR? If the MTTR is low (e.g., one hour), then the probability for redundant system failure during the outage is low. Repair and response times are key factors in achieving high availability for ESInets. It is a best practice to have a spares plan and SLAs/SLOs on response time.

The procedure for software upgrades to the system must also be taken into account. If not properly designed, taking the system offline to upgrade the software may put the SLA/SLO in jeopardy. Another aspect of designing for five nines availability in an ESInet is the requirement that software upgrades can be installed without taking the system down, or require the system to be offline for a very short period of time.

Another consideration is that software upgrades sometimes fail. There must be a procedure to back out the change. So system repair procedures must include policies and procedures for software upgrades.

2.10.2 Achieving five nines availability in 9-1-1 networks

It is fashionable to demand that all aspects of 9-1-1 be maintained as five nines reliable, and then ignore blatantly obvious failures to achieve such a lofty goal. It is possible to achieve five nines in an NG9-1-1 system, and therefore in the design and operation of an ESInet, but it may be expensive and difficult to implement.

If jurisdictions determine that five nines is a requirement, then it is incumbent upon them to ensure that all aspects of the design for the solution, and especially the ESInets themselves are designed, built and operated to verifiable SLAs/SLOs, and provide adequate funding to achieve that goal.

If funding or other impediments prohibit achieving five nines, then SLAs/SLOs should be established that are actually achievable, and affordable. An NG9-1-1 system that is specified and achieves three nines is more valuable than a system that is nominally said to be designed to meet five nines but actually achieves three nines.

In order to achieve five nines availability using two fully independent systems, telcos historically implemented a strict set of technical and operational standards for their employees and central offices which include the following:

- Utilize Network Equipment-Building System (NEBS) Level 3 Compliant Equipment
- DC-powered
- Redundant fans and power supplies
- Highly reliable components, tested at environmental extremes
- Installed in secure, environmentally controlled facilities
- Engineered to deal with a variety of common issues for failover and recovery
- Monitored by a Network Operations Center (NOC) 24 x 7 x 365
- Spare parts available on site or within one (1) hour

- Approval for use testing
- Key network elements should be designed to be fault tolerant where possible

It is essentially impossible to obtain IP equipment that meets these standards. Using commercially- specified equipment, achieving five nines requires redundancy greater than two (2) of everything.

2.10.3 Practical methods for legacy 9-1-1 networks

Five nines availability is a widely accepted standard for emergency 9-1-1. This objective is achieved for call completion within legacy 9-1-1 systems primarily through the use of backup PSAPs and 10-digit numbers. In NG9-1-1 we will achieve five nines on individual call completion for even the smallest PSAP service area by answering calls from out of area.

Five nines availability was rarely achieved at any individual PSAP largely due to limitations at the physical layer (i.e., a single entrance for facilities into each PSAP, CAMA trunks and ALI circuits in the same trench from CO to PSAP, etc.).

For these reasons, it is estimated that most legacy PSAPs achieve an availability on the order of two nines. Availability varies by region, year, and service provider.

There are other mechanisms that can be used to achieve five nines (e.g., more redundancy). Calculating actual reliability is complex.

> *Special Note: When determining the Availability and Reliability for an ESInet, the metrics defined in this guide should serve as a recommendation at the highest level. However, Availability and Reliability may increase costs of an ESInet, and may require additional considerations that are dependent upon the financial conditions of the entity implementing an ESInet.*

2.10.4 Defining failure metrics for an ESInets

An ESInet's availability and reliability is determined by what constitutes a failure. A failure could be defined as one of the following:

1) The termination of the ability of the overall 9-1-1 system to perform its required function within a specific geographic region.
2) The termination of the ability of any individual PSAP to perform its required function but not the termination of the ability of the overall 9-1-1 system to perform within that specific geographic region.

For example, if all the circuits from the PSAP to an ESInet are all located in the same conduit, and there is a fiber cut, typically one of two things will happen:

1) NG9-1-1 call handling system automatically routes calls to backup PSAP.
2) Someone at the PSAP will take action on the management console that will reroute the 9-1-1 calls to a 10-digit number or back-up PSAP.

The failure does not prevent 9-1-1 calls in that region from being completed. However the failure does prevent the calls from being delivered to the primary PSAP. Therefore, according to definition 1, this is not a failure, but according to definition 2, it is a failure.

9-1-1 entities should define what constitutes a failure within their system, and thereby determine how availability and reliability will be calculated.

2.10.5 Series and Parallel Reliability and Availability in ESInets

Series and parallel reliability and availability are key components to the design of highly reliable ESInets. Series reliability is calculated as:

$$R_s = R_1 * R_2 * R_3$$

For example, the series reliability of an ESInet shown below is:

$.9743 * .999 * .9743 = .948$

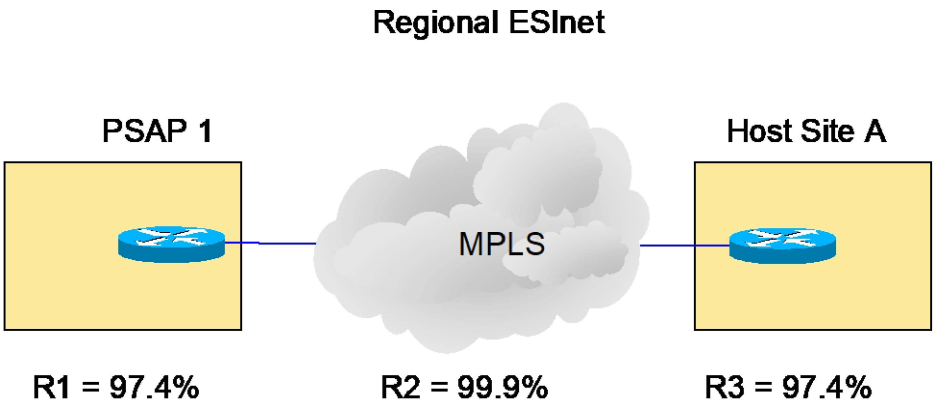


Figure 5

An interesting property of series reliability is that it is always less than the least reliable component in the series. For example, a two nines router connected to a three nines circuit yields an overall reliability of less than two nines.

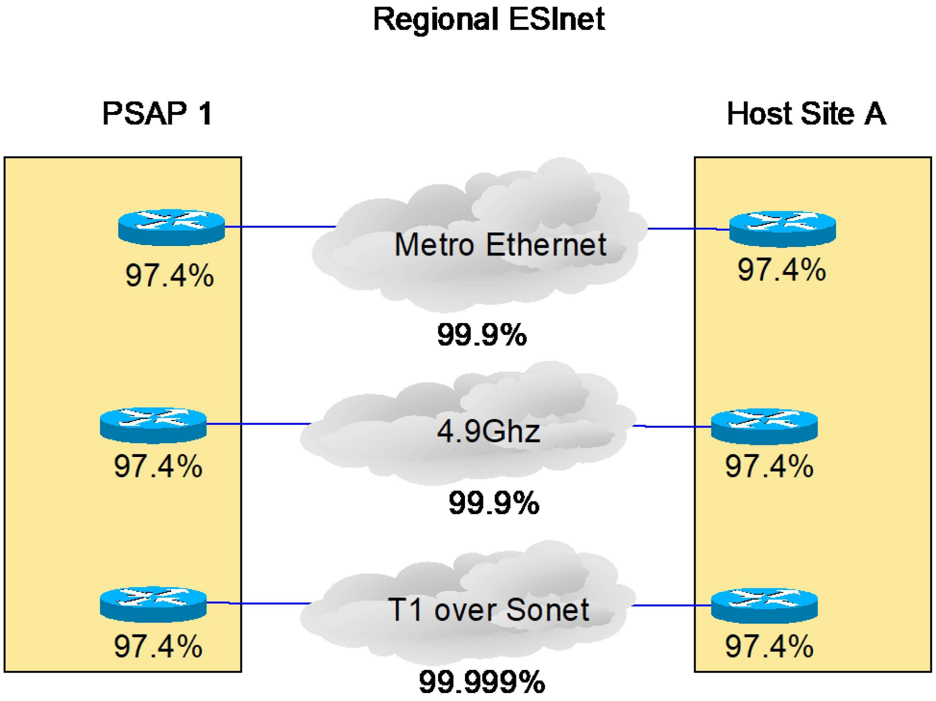


Figure 6

Parallel reliability is calculated as:

$$R_P = 1 - ((1-Rs_1) * (1-Rs_2) * (1-Rs_3))$$

Where Rp = Parallel Reliability
and Rs1..3 = the series reliability of each independent link

So, if the series reliability of each link is 94.8%, then the reliability for the three (3) fully independent and physically diverse links in parallel is almost four nines.

$$R_P = 1-((1-.948) * (1-.948) * (1-.948)) = 1 – (0.052 * 0.052 * 0.052) = 0.99985$$

As shown below, four fully independent and physically diverse links in parallel are required to achieve a reliability of five nines. (Note: In order to be fully independent and physically diverse, the links must not share any components in common (i.e., not in the same trench, not running through the same Digital Cross Connect at the Central Office, routers not from the same vendor, etc.)

$$R_P = 1 - ((1-.948) * (1-.948) * (1-.948) * (1-.948))$$
$$= 1 – (0.052 * 0.052 * 0.052 * 0.052)$$
$$= 0.9999927$$

In most cases, higher overall reliability can be achieved by purchasing several physically diverse low cost links (e.g., Metro Ethernet, T1 over SONET, etc.) as opposed to a single high cost service. Surprisingly, series and parallel availability are calculated using the same formulas shown above for series and parallel reliability.

So, assuming all of the necessary considerations have been taken into account (i.e., environmental considerations, operational and technical procedures are developed and adhered to, equipment is replaced as it reaches end of life, etc.), a PSAP connection to an ESInet that consists of four (4) fully independent and physically diverse links that have a series reliability (taking routers into account) of at least 94.8% can expect to achieve five nines availability (five (5) minutes or less of downtime per year) on that ESInet – every year.

2.11 Network Security

The NENA 75-001 Security for Next Generation 9-1-1 Standard (NG-SEC) [3] contains a number of sections which apply to ESInets including: Security Policies, Information Classification, Safeguarding Information Assets, Physical Security Guidelines, Network and Remote Access Security Guidelines, Change Control Documentation, and Compliance Audits and Reviews. ESInets should be NG-SEC compliant.

The NENA-STA-010 Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3 [1] contains additional requirements for ESInets, including encryption and authentication mechanisms. ESInets should comply with the NENA-STA-010.

It is a best practice to ensure that the following Security elements are considered when securing an ESInet:

- Physical site security and access to the equipment or service
- Personnel access to the equipment
- Appropriate level of access for each authorized user

2.11.1 Session Border Controllers (SBC) and Firewalls

It is a best practice to utilize Session Border Controllers on ESInets to provide firewall-like security for call signaling and call media streams. In most cases, it will be necessary to put a firewall in parallel with the SBC[16] in order to be able to process all the different types of traffic. Logs and alerts from SBCs and firewalls should be continuously monitored to identify performance issues as well as successful and unsuccessful attacks.

SBCs and firewalls should be deployed to protect state-level i3 core services from attacks originating both from the access network and from the state-level ESInet. In order to contain virus outbreaks

[16] The i3 Border Control Function (BCF) includes SBC and firewall functions.

and/or intrusions, it is strongly recommended to deploy SBCs and firewalls at regional host sites. Session Border Controller functions should comply with NENA-STA-010 [1].

An important consideration when planning for SBCs and Firewalls is to determine who has the authority to manage the devices and to document the manner to address potential interactions between the supporting agencies.

2.11.2 Distributed Denial of Service (DDoS) mitigation

ESInet plans and designs should take into consideration DDoS detection, mitigation and remediation service(s). There are three general ways a DDoS attack could interfere with an ESInet; attack on the DNS, attack on protocol specifics, and packet flooding. A BGP route must be configured so that it can be withdrawn to eliminate the infected route, and replace it with a route to the mitigation service. Where DNS is not provided in the same route, separate arrangements may be necessary for DNS service. Depending on how the external ECRF/LVF is configured, the paths to that ECRF may also be exposed to DDoS outside of an ESInet and require additional protection.

The resources that must be publicly addressable from the Internet, both with respect to IP address and global DNS entries, is a complex subject and not all ESInets will work the same way in this regard. NENA-STA-010 [1] defines which resources must be publicly addressable, but it is not explicit in several areas, and the information is dispersed throughout the document.

Here is a summary of the considerations for public addressing:

1. There must be an external ECRF and an external LVF. These could be in an ESInet DMZ, or on a completely separate public network. The external ECRF and LVF must have global DNS entries.

2. NENA-STA-010 states that PSAPs must provide public addressable endpoints for media to avoid the need for NAT traversal gyrations. If the BCF anchors media, it would supply the global media addresses.

3. The entrance ESRP and/or the BCF which is the target of the URL in the external ECRF for PSAPs inside an ESInet must be publicly addressable and its entry (the domain in the URL found in the ECRF) must be in the global DNS.

4. A LIS may provide a “Presence” URL for location provided by reference using SIP SUBSCRIBE/NOTIFY methods. Any entity that wishes to dereference such an URL requires a public address, and typically a global DNS entry. The list of such de-referencers includes all ESRPs, all PSAPs, all responders, etc.

5. A call may include additional data about a call, caller, or location. That information may be sent by reference, requiring access from an entity inside an ESInet to the external Additional Data Repository (ADR) or Identity Searchable Additional Data Repository (IS-ADR).

PSAPs, responders and other agencies may need this information. It is possible for a Policy Routing Rule to use such data, and thus all ESRPs may need to query. In these cases, the query is HTTPS, and could be through a NAT.

6. There are circumstances where 9-1-1 Authorities may provide a provisioning feed to an ECRF or LVF maintained by some outside entity such as a service provider. The feed might be provided by the external ECRF/LVF, but if it is not, the Spatial Interface (SI) for such a feed needs a global address and global DNS entry.
7. There are circumstances where an agency may wish to provide an Emergency Incident Data Document (EIDD) feed to an external entity. If that is permitted, the entity providing the EIDDs must be publicly addressable. It is possible the feed is a subscription, in which case the EIDD source needs a global DNS entry.

2.11.3 Multiple Service Providers

There are many circumstances where ESInets will be configured utilizing multiple providers. When multiple providers are used, an ESInet should be configured to operate seamlessly, but allow for logical separation between the internal network resources. All addressable resources internal to an ESInet should have separate addresses from each ISP so that a single attack or failure of an ISP will not affect the entire network. The logical components will enable the network to route around errors and maintain connectivity.

2.11.4 Internet Access within a PSAP

As ESInets are planned and implemented, a review of the physical and logical security mechanisms is necessary. Presently, the most utilized method of security is to "wall off" or create a zone of protection specifically within the PSAP. If an ESInet is implemented with a walled-off approach, it may limit the full capabilities of an ESInet and minimize some of the effectiveness of full functional NG9-1-1. While legacy networks are in place this method is effective, but can limit the greater advantages that an ESInet can offer. ESInets will increase the PSAP exposure to the public internet and PSAPs must be prepared to alter their policies to accommodate the new capabilities available.

In the strictest sense, Internet access at a PSAP must be controlled. This can be accomplished through the use of Access Control Lists (ACLs) at the edge of the ESInet. Non-ESInet authorized personnel may be granted guest Internet access on a separate service.

2.12 Network Management and Monitoring

Critical circuits for E9-1-1 calls (e.g., PSAP trunks and ALI circuits) are monitored. Outages may be FCC reportable. By the same token, ESInet(s), which provide transport for emergency 9-1-1 calls, should also be monitored. Although there are neither reporting nor certification requirements in current regulation specifically on 9-1-1 entities, the FCC regulations require Covered 9-1-1 Service Providers to take reasonable measures to provide reliable 9-1-1 service with respect to three substantive requirements: (i) 9-1-1 circuit diversity; (ii) central office backup power; and (iii) diverse network monitoring. See, 47 CFR § 12.4(a)(4) (defining Covered 9-1-1 Service Providers as entities that "provide 9-1-1, E9-1-1, or NG9-1-1 capabilities such as call routing, automatic location information (ALI), automatic number identification (ANI), or the functional equivalent of those capabilities, directly to a public safety answering point (PSAP), statewide default answering point, or appropriate local emergency authority," or that "operate one or more central offices that directly serve a PSAP"). Therefore, 9-1-1 entities and/or their vendors should be prepared to report ESInet outages and provide certifications in the event FCC regulations might be modified, even if they are not currently applicable.

All data circuits and network components which comprise an ESInet should be monitored. All network components should provide Simple Network Management Protocol (SNMP) traps to an approved management system. Vendors of all operational network components that form an ESInet should provide an SNMP Management Information Base (MIB) for each component to organizations authorized to operate SNMP management systems. At least one SNMP based network monitoring system should be implemented by an organization with access to the resources necessary to perform effective network maintenance services.

Vendors of all non-network components, such as NG9-1-1 application servers, should also be encouraged to provide SNMP MIBs for their products. This would allow a network management system to monitor all of the network and application components necessary for the reliable operation of NG9-1-1 on an ESInet. Companies that connect to an ESInet for the purpose of monitoring and/or management of devices should be NG-SEC [3] compliant.

Effective network management requires:

- Proper/accurate documentation of the network
- Current network diagrams
- IP address range management/assignments
- Demarcation points
- Contact and escalation lists – vendor, service provider, NOC
- Near-real-time monitoring/alarming
- Benchmarks for Service Level Agreements (SLAs) or Service Level Objectives (SLOs) to be implemented by the service providers
- Capacity management/trending analysis
- Monitoring the state of element configuration (e.g., QoS)
- Configuration Management/Change Control

Some of the methods above can be used to measure SLA/SLO metrics, but may not be reported to the end user.

The significance of the demarcation point is that it can define responsibility. When multiple service providers are involved (e.g., ECRF, ESRP, ESInet), it may be advantageous to have the service providers agree to forward SNMP traps and management alarms to a central network management system. Where appropriate, heartbeats can be used to verify the availability of network facilities.

Each participant within the ESInet should be responsible for ensuring that the appropriate tools and additional resources, including trained staff required to diagnose, test, and monitor traffic within their portion of the network, are available and able to respond 24x7x365. Provisions should be made for capturing network traffic, generating alarms and producing other metrics for monitoring and troubleshooting outages on ESInets.

Monitoring packet data can be done in a variety of ways. This can be done both physically and virtually (through software using existing physical interconnections). The same access provisions may also be required for Intrusion Detection Systems (IDS) and loggers. Provisions should be made for supporting access to the network or assuring the equipment is capable of supporting monitoring without degrading performance.

Active test equipment that can interrupt normal network activity should only be used on a case-by-case basis when needed to troubleshoot. Passive/monitoring test equipment should be treated differently than active (i.e., traffic-generating) equipment. Active testing for Functional Elements (FEs) of NG9-1-1 beyond OSI layers 1-3 may help resolve outages.

ESInets should allow for monitoring of packets across the network. Monitoring solutions should be enabled to provide statistics on the performance of all functional elements in an ESInet. Typically the network elements that require monitoring are:

- Transport network components and devices
- Routing components and devices

Within the ESInet, monitoring should be designed to provide information about each of the devices.

Network Monitoring should also be able to provide the metrics to allow for service-level monitoring to occur at the component level so that any service level may be documented and reviewed on a regular basis to gauge performance.

2.12.1 Network Performance Monitoring

Unlike traditional TDM-based networks, it may be difficult to monitor quality at each point along an IP network. As voice and data may originate from anywhere in the world, operators of an ESInet may be forced to work with multiple parties when troubleshooting a source of poor quality.

Operators of ESInets that cover larger geographical areas or contain many intermediate nodes may wish to utilize some of the same tools service providers use to monitor network quality. The following are some examples of additional tools to monitor network quality:

Tool	**Purpose**
Network Probes	Probes are generally hardware devices that are placed in the direct path traffic or on a mirrored port. Probes are commonly capable of providing quality metrics (such as a MOS score, packet loss, mal-formatted messages, etc.) that are not available from other systems.
Active Monitoring	Active monitors are usually software agents embedded in either routers/switches or in network probe. These software agents may be configured to emulate applications such as VoIP, streaming video, file transfers, etc. These traffic streams may be configured to run frequently and record very accurate statistics about the quality of service similar traffic might receive.
Packet Captures	Packet captures are a recording of live traffic from a network. They may be recorded either by an intermediate system (such as a probe, router, or switch) or by an end system such as a work station configured with packet capture software. Packet captures are very useful for troubleshooting problems such as incompatibilities between protocols and vendors as well as network configuration problems that may be causing unseen errors or degrading quality.
Flow Collection	In TCP/IP a flow is essentially a complete end-to-end communication. Many routers and switches are capable of recording information about these flows such as source and destination address, type of application, throughput, duration, etc. As flow collection only operates on the headers of packets, it does not record any actual data (such as the voice or video streams themselves). However, flow data can be very useful to understand where traffic is sourced from and destined to as well as the types of applications in use on the ESInet.

During implementation and ongoing management of NG9-1-1, low-level packet analysis tools may be required for performance diagnostics and trouble resolution. These tools are equivalent replacement tools for the existing trunk monitoring techniques and tools that are used in legacy 9-1-1.

2.12.2 Quality of Service within a PSAP

There are a number of factors that affect the overall quality of multimedia traffic on an ESInet including packet loss, jitter, and latency. This section outlines some of the important properties of packet loss, jitter, and latency as pertaining to ESInets.

2.12.2.1 Packet Loss

Packets can be dropped by various devices in the network (e.g., routers, ATM and MPLS switches), or the packet may have been corrupted during transport and dropped at the destination. An overall (end-to-end) packet loss budget for maintaining intelligible voice transmission is about 5%. Out of that 5% budget, approximately ½ of the packet loss should be allocated for an ESInets with the remaining allocated for the origination network. It is a best practice to engineer ESInets to keep the packet loss budget under 2.5%. Audio media streams are the most sensitive to packet loss. ESInets should be designed without oversubscription. Packet loss of less than 1% should be achievable on such ESInets.

2.12.2.2 Jitter

A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably. Arrival time of packets is ideally equal to the packetization period (i.e., sample rate times samples per packet). Because of the effects of queuing and because two (2) sequential packets sent from the same source may not arrive via the same paths, variation in the actual arrival time of packets may occur. It is this variability in the delay that causes jitter. Jitter buffers are utilized to smooth out the variation. It is a best practice to design ESInets to maintain less than 20 ms variation in the end-point jitter buffers.

When jitter in excess of 20 ms is present, voice traffic can be adversely affected due to the packet loss that is introduced along the voice path.

2.12.2.3 Latency

Latency is the amount of time it takes for a packet to reach its destination. The one-way transit delay (i.e., end to end, mouth to ear) for real-time media packets should not exceed 150 ms (ITU-T-G.114 [14]).

When latency exceeds 150 ms, turn taking is significantly impaired. Because the access network is outside the scope of an ESInet, and considerable latency may be incurred there, the maximum acceptable delay for packets traversing an ESInet should be less than or equal to 50 ms. It is a best practice to design ESInets to operate with the less than 50 ms of latency. This allows for the original encode and decode, and a conference bridge in the middle of the path and still achieve the maximum 50 ms or less packet delay.

Latency in an ESInet may be induced in many places (including outside an ESInet). The following diagram illustrates just some of the many places latency (as well as jitter and packet loss) may be induced. Any design of an ESInet should take into account latency that has already occurred prior to reaching an ESInet as well as latency that may occur in the access network or at the premise.

181051 Exh. JDW-67RX

REDACTED

181051 Exh. BR46RX

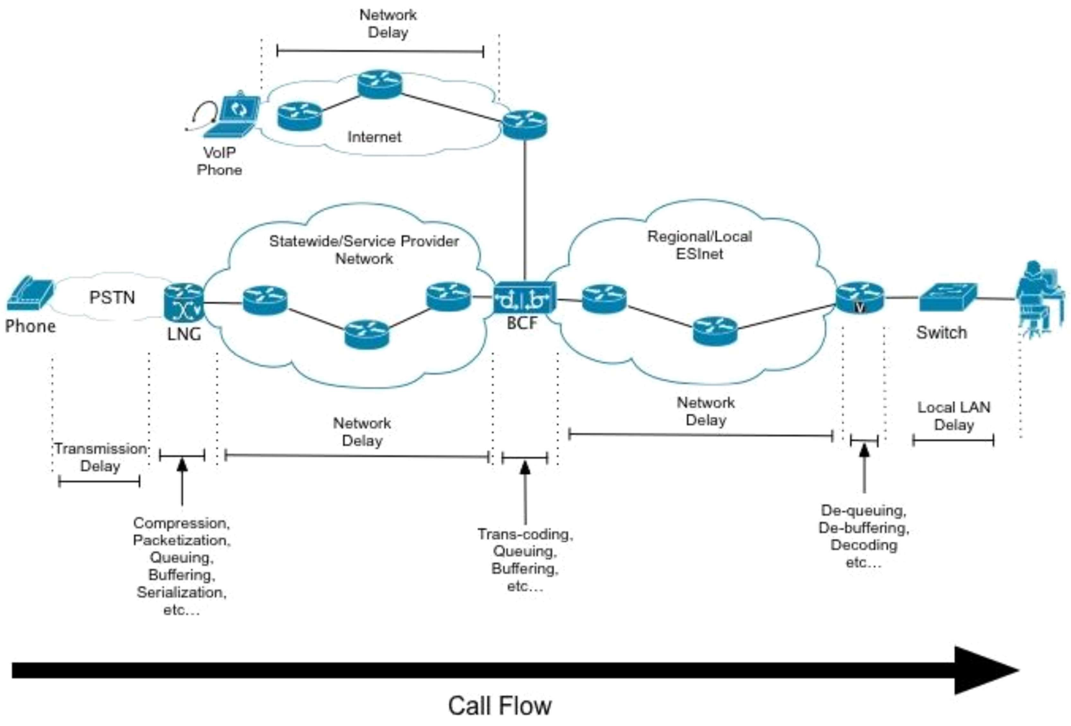


Figure 7

Using the diagram above as a guide – moving left to right – a latency budget may look something like this:

Delay Type	Average	Maximum
Transmission delay	5ms	5ms
Encoding/Compression/Buffering	20ms	30ms
Service Provider Network	25ms	30ms
Transcoding/Queuing/Buffering	2ms	2ms
ESInet	25ms	50ms
Decoding/Debuffering	20ms	30ms
Local LAN	1ms	2ms
Total	**97ms**	**149ms**

- Encoding - The process of turning raw audio (or video) samples into symbols in the chosen codec used (such as G.711). Compression is optionally applied to make the data stream smaller without significantly affecting quality. Symbols are then packed into packets, and no further processing can be completed until a full packet is available.
- Transcoding - For some codecs, the PSAP won't have the matching codec, and a transcoder is needed to convert from the codec used at the origination device to the codec used at the PSAP.

- Decoding - Reverses the process of encoding (and includes debuffering) and turns symbols in the codec to raw audio samples.

2.12.3 Service Level Agreement[17]

A service level agreement is a mutually agreed upon formal document negotiated between the 9-1-1 entity and the vendor that defines the service level commitment the vendor is agreeing to provide. A fundamental commitment in a SLA is contracted availability metrics for the described service or system. This is typically represented in terms of uptime (e.g., 99.9%, 99.99%, 99.999%). Uptime metrics are typically described as three nines, four nines, five nines, etc.

Another aspect of an SLA is the ability to sustain active calls within the system. An event may cause a failure of one half of a redundant system that may terminate all services (and active calls) on that system, but the second half of the system is available immediately for new services (i.e. new calls) to be created. This maintains 99.999% availability, yet all live services had been dropped. Assurance of availability needs to be addressed in appropriate Service Level Agreements, including maintaining calls that are in progress.

The SLA typically describes where and how the measurement is made, and how often they are calculated and reported. For example, an SLA might be measured over a one month period, a one year period, or both. It is a best practice for 9-1-1 entities to ensure that there are provisions within the SLA that require the service provider(s) to notify the 9-1-1 entity in the event of impairments affecting service, and do so immediately upon learning of a disruption. The SLA should also include an escalation procedure with identification of personnel who must be contacted. An important consideration when developing an SLA strategy is to ensure the alignment of the SLAs for components, systems, services, and service providers. SLAs often span these areas and may become cumbersome to manage how each individual SLA integrates into a complete package. It is important to construct SLAs that meet the objectives strategically as well as tactically, and ensure that appropriate responsibilities are defined in advance for all vendors contributing functionality to the ESInet. This is often accomplished by establishing an Operating Level Agreement (OLA) that presents a clear understanding of the relationship of the SLAs that protect each function of the ESInet and responsibilities of each contributing vendor.

Since the ESInet may not be provided by a single vendor, or may be constructed to include subcontracted components or service providers, it is important that the SLA for each portion of the network also addresses individual responsibilities. The OLA needs to maintain agreed upon service levels for all SLAs and resolve issues on an end-to-end basis, not just within the confines of the portion of the network being provided by an individual vendor.

Another important consideration is to determine how the SLAs will be measured. Some may be annually; others may be quarterly or monthly. Alignment between the measurement cycles is necessary to ensure that the blanket SLA coverage meets the desired goal. Furthermore, when the SLA measurement is deemed outside the threshold(s), a corrective action may be required to bring the system back under control. Such monitoring should be kept current with any identified anomalies

[17] SLA includes a clear penalty for missing a measurable objective. An SLO does not include a penalty but defines the service objective.

so that issues are resolved as quickly as possible with cooperation between any vendors providing portions of the network that may be affected.

Service impact levels are typically used to define the severity of the outage denoted by some range of values (e.g., 1 through 5, or a reference to scale of trouble such as minor, major and critical.).

Failure to meet agreed-upon service impact levels may result in pre-negotiated financial penalties to the vendor/service provider.

ESInets are complex and may involve management of SLAs from a number of different vendor/service providers. Best practices include:

- Where multiple service providers are involved, there should be a demarcation point that defines the boundaries of responsibilities as described in an agreement.
- Obtain or establish the MTTR for each piece of equipment used in an ESInet as well as an SLA for the network service. To maintain reliable service and ensure efficient testing, benchmarks should be established, documented, and periodically reviewed for accuracy.
- Contracted levels of service should be established to ensure adequate response times for repair.
- To minimize downtime critical hot spares should be identified, purchased, and maintained on site.
- Maintenance should include regularly scheduled audits of hardware revision levels and code compatibility (including firmware) with hardware revisions.
- Redundant systems should be regularly exercised by deliberate fail-over as part of routine maintenance.
- Escalation paths should be documented and known to the 9-1-1 entity so that responses to failures can be adequately addressed.
- An Operating Level Agreement (OLA) should be established to define the responsibilities of each vendor and relationships that correlate SLAs for all contributing vendors, including how issues need to be addressed.
- SLAs should be reviewed on a regular basis for modifications related to the introduction of new technologies, network modifications, or other changes that may permit agreeing to a higher standard for reliability.

It is recommended that ESInets include SLA thresholds such as:

- Up/downtime
- Troubleshooting
- Escalation
- Reporting
- Break/Fix

- Spares
- Quality of Service
- Maintenance periods/windows
- Consistent SLA measurement and compliance
- Daily/monthly/quarterly/annually reporting and reset thresholds
- Consequences for not meeting the SLA are necessary
- Authority for accessing and changing the network resources

2.12.4 Dimensioning ESInet Data Circuits

Traditionally, bandwidth sizing requirements for wide area networks are based on the bandwidth requirements of the applications being utilized on that network. One of the challenges of designing ESInets today is that some of the applications that are expected to be implemented may be outside 9-1-1 and others are yet to be developed.

NENA-STA-010 [1], within the SIP call section 4.1 and Media 4.1.8; Section 4.1.8.2 Video, requires support for video using the H.264 codec, baseline profile, levels 1-3. The maximum video bit rate for level 3 is 10 Mbps. However, reasonable quality can be supported by less bandwidth given typical environments for emergency calls, which usually do not have rapid scene changes, and often have “talking heads”. Further, while best practice for PSAP design would be to support all media at all positions, it does not necessarily imply that all positions must support the full level 3 bandwidth simultaneously. The bandwidth required is subject to some differences of opinion among practitioners. One possible formula is 2 Mbps per PSAP + 2 Mbps per call-taker position equipped for video, but more (or less) bandwidth may be appropriate for a given ESInet. The actual bandwidth requirements for any individual installation should be properly designed by qualified network design engineers.

There has been an update to the Americans with Disabilities Act (ADA) expected for some time. There is a possibility that at some point in time the Department of Justice may require PSAPs to support video in NG9-1-1. The following link can be used to remain up to date with any new progress (https://www.justice.gov/crt/publications). It is considered a best practice to always design and deploy ESInets that are scalable with regard to bandwidth allocation. This way, when bandwidth intensive applications need to be deployed, ESInets can be quickly scaled to meet these adjusted requirements. One concept that has been discussed and generally agreed to among the authors of this document is that the bandwidth requirements will expand over time, and will use up all available bandwidth capacity. Therefore, it is recommended that a fundamental best practice is to provision as much bandwidth capacity during an ESInet design phase as is reasonable for application use to cover at least a two (2) year planning horizon, and that is economically feasible.

The circuits upon which Internet-based emergency 9-1-1 calls will be delivered have some unique design considerations. Some of the following may impact final ESInet data circuit design:

- Access to online mapping tools
- Potentially social media access

- Additional supplemental data (floor plans, campus maps)
- Streaming media

The primary factor that drives the bandwidth requirement for these circuits is the potential for a Distributed Denial of Service Attack (DDoS). Per NG-SEC 75-001 [3], these circuits must be terminated into a Border Control Function (BCF). BCFs (SBC and firewall parts) are programmed to recognize and thwart attacks, but the resources required to be able to receive an emergency 9-1-1 call via the Internet during a DDoS attack are significant. The ingress to the BCF should be designed to withstand the largest feasible attack. It is a best practice to engage qualified security professionals knowledgeable about current DDoS mitigation techniques to develop and implement strategies to protect ESInets against DDoS attacks. The NG-SEC [3] documentation contains additional information on the way that ESInets can withstand DDoS attacks.

2.12.5 Traffic Engineering

ESInets should be designed to provide non-blocking service for high priority traffic. Bandwidth, Traffic Policing, Traffic Shaping and Quality of Service are some of the main design considerations that must be taken into account. The sub-sections below describe some of the caveats to be avoided and best practices that should be observed with regard to traffic engineering in ESInets

2.12.5.1 Traffic Policing

Some of the layer 2 technologies that can be utilized to provide transport for ESInets require that the traffic that is being sent into the network conforms to a number of requirements including peak and sustainable cell/packet rate. Traffic that exceeds the rate purchased from the service provider may be discarded immediately, marked as non-compliant, delayed, or left as-is, depending on administrative policy and the characteristics of the excess traffic.

It is a best practice to confirm agreements for traffic policing in an ESInet with the service provider.

2.12.5.2 Traffic Shaping

Traffic shaping is commonly applied at the network edges to control traffic entering the network. Traffic shaping is frequently required when the port speeds exceed the amount of bandwidth purchased from the service provider. For example, assume a 10 Mbps Metro Ethernet service is purchased from a service provider. If the 100 Mbps Fast Ethernet port of a router is connected to that circuit, in many cases even though the data being transmitted over a period of one (1) second is less than 10 megabits, the router (transmitting at 100 Mbps) will exceed the rates deemed acceptable by the service provider and packets will be dropped. When port speeds are not equal to the amount of bandwidth being purchased from the service provider, it is a best practice to configure traffic shaping on the routers to ensure that the traffic being transmitted is in compliance with the traffic contract.
It is a best practice in an ESInet design to know what the service providers traffic policing policy is and ensure that the traffic shaping complies with the agreed upon requirements.

2.12.6 Quality of Service (QoS)

Quality of service is the ability to give priority to different data flows.

Per the Detailed Functional and Interface Standards for the NENA i3 Solution (NENA-STA-010) [1], IP traffic within an ESInet must implement Differentiated Services (RFC 2475 [18]):

- Functional Elements must mark packets they create with appropriate code points.
- The BCF must police code points for packets entering an ESInet.
- Code points and Per Hop Behaviors (PHB) must be used on ESInets and must be configured to comply with the defined parameters (see NENA-STA-010, section 3.7 for details).

It is a best practice in an ESInet design to know what the service provider's traffic policing policy is and ensure that proper QoS provisions are included in the network design so the network is implemented correctly.

2.12.7 Interconnection and Peering

By design, individual ESInets can enable peering with other ESInets through BGP. BGP is the preferred method of enabling multiple ESInets within a region, state or nationwide to interconnect seamlessly.

Typically, there are two ways to implement a peering in an ESInet:

1) Entirely separate from a single provider;
2) Constructed as an overlay on an existing network.

There is also the potential of a third configuration that would essentially be a hybrid of the two primary methodologies.

2.13 Domain Name System (DNS)

The careful management and continuous operation of Domain Name System (DNS) in an ESInet should be held in the utmost regard. DNS must be secure and responsive as its functioning is crucial to the delivery of emergency calls. DNS is the underlying protocol that will resolve which hosts to route requests for emergency services. Having multiple ECRFs, ESRPs, circuits and routers will be to no avail if there is a DNS failure. For example, an originating ESRP needs to send a call to sip:police@psap.example.com. Without DNS, the ESRP will not be able to determine what host handles SIP calls at psap.example.com.

Considering the critical nature of DNS and the requirement that external DNS resource records for core functions must be in the global DNS, it may be desirable to have DNS services hosted by a reputable provider that can handle sustained, high bandwidth Distributed Denial of Service (DDoS) attacks.

2.13.1 DNS Architecture

In building a robust and secure DNS architecture for an ESInet refer to NIST-800-81-2[17].
In general a solid DNS architecture should:

- Use dedicated, geographically diverse external name servers
- Place DNS servers behind firewalls
- Remove any unnecessary services and disable dynamic DNS (DDNS).

- Utilize a hidden primary server
- Use authenticated zone transfers (TSIG)
- Use separate recursive name servers which do not host any DNS zones
- Implement DNS Security Extensions (DNSSEC)
- Split-zone DNS may be used as most end hosts on an ESInet do not have a functioning role in the delivery of an emergency call

2.13.2 DNS Management

The management of an ESInet's DNS resource records (RR) should include a well-established change control process. On–the-fly changes to RRs could have grave and disastrous consequences to the availability of emergency services on an ESInet. The logging of additions, changes and deletions to critical RRs should include who, what, and when to allow for auditing on a future date.

2.13.3 DNS Naming Schema

An ESInet should utilize a logical and understandable forward and reverse naming scheme. An incoherent naming scheme can lead to delays in troubleshooting, the accidental misconfiguring of applications, and general difficulty for NOC personnel. Interested parties within a state or regional ESInet should agree to a domain name and naming standard. From a NANOG case study (reference: https://www.nanog.org/meetings/nanog31/presentations/ringel.pdf) the naming standard should consider the following:

- No institutional memory (seasoned IT veteran knows that "alice" is the print server)
- Relying on security by obscuring names does not work
- Avoid using device hardware, make, or model in naming (hardware will be swapped out eventually)
- The name should be representative of both location and role
- Use CNAMEs if a brief reference is desired for a host
- Within the network infrastructure: multi-homed devices (router layer 3 links) should specify type of link [border (b), transit (x), terminus (t) and location] and origin to destination. For example: arlenpolice-x-myprovider-springfieldfire.atlantis.esinet.tld.
- For single-homed devices (such as an access switch), items such as building name, room number, type and instance should be included. For example, elbonia-room07-cabinet2-unit01.midearth.esinet.tld.

2.13.4 Multi-homed PSAP DNS operation

Typically, a PSAP is considered as being connected to "an ESInet", where an ESInet is delivered as a managed IP network obtained from a contractor, or built by a contractor to connect all the NG9-1-1 pieces together. While this is the ideal situation, obtaining a single IP network that is ultra-reliable is often difficult, and therefore expensive. Networks go “down” for a variety of reasons, and it’s challenging to engineer them to never fail.

An example of a realistic problem that arises is when a BGP route announcement error blocks the target addresses from being reached correctly. This can occur when you have a single network, even with multiple connections to that network. While broken route announcements are rare, it’s also rare to find a network where they never happen.

Another example is a software bug in a network switch or router than affects all such boxes from the same manufacturer. Since networks tend to be homogenous on that low level hardware, a serious bug can affect all the routers or all the switches. There are famous examples of this kind of problem that caused sustained network outages.

Enterprises have developed techniques that connect their own systems that need ultra-reliability to more than one network. This is beyond simple peering with multiple peers, but rather through multiple IP addresses from different networks with different links that address a single function. Implementing a design where a function is a key piece of infrastructure, such as the incoming proxy server for emergency calls on two or more networks with two or more IP addresses can minimize and prevent routing failures, link failures and other problems that may plague any one network.

Even if there is a formal ESInet, consider having the critical infrastructure connected to one or more other networks that are completely separate, from different providers, using different technology and different routes. Sometimes the physical boxes require more than one physical network interface. Alternatives using Virtual Private Network techniques can sometimes be used to enhance diversity.

Be aware that multi-homing as described in this section is complex to set up and maintain, and should not be used unless sufficient network expertise is available to create and maintain the systems. Debugging problems when multi-homing is deployed is extremely difficult. Multi-homing in this fashion means that an addressable resource has more than one IP address, and thus the DNS system has a more complex entry for the resource than when it is on a single network.

2.14 Network Architecture

This section covers some of the most commonly utilized ESInet architectures, and some of their caveats, advantages, and disadvantages. Common objectives for ESInet architectures are to maximize availability and reliability within budgetary constraints. The diagram below shows a regional ESInet that is connected to state-level i3 core services via a state-level ESInet[18].

[18] In an effort to simplify the diagrams the physical connections within the sites (i.e., router to switch, switch to server, etc.) are not shown.

Regional ESInet I

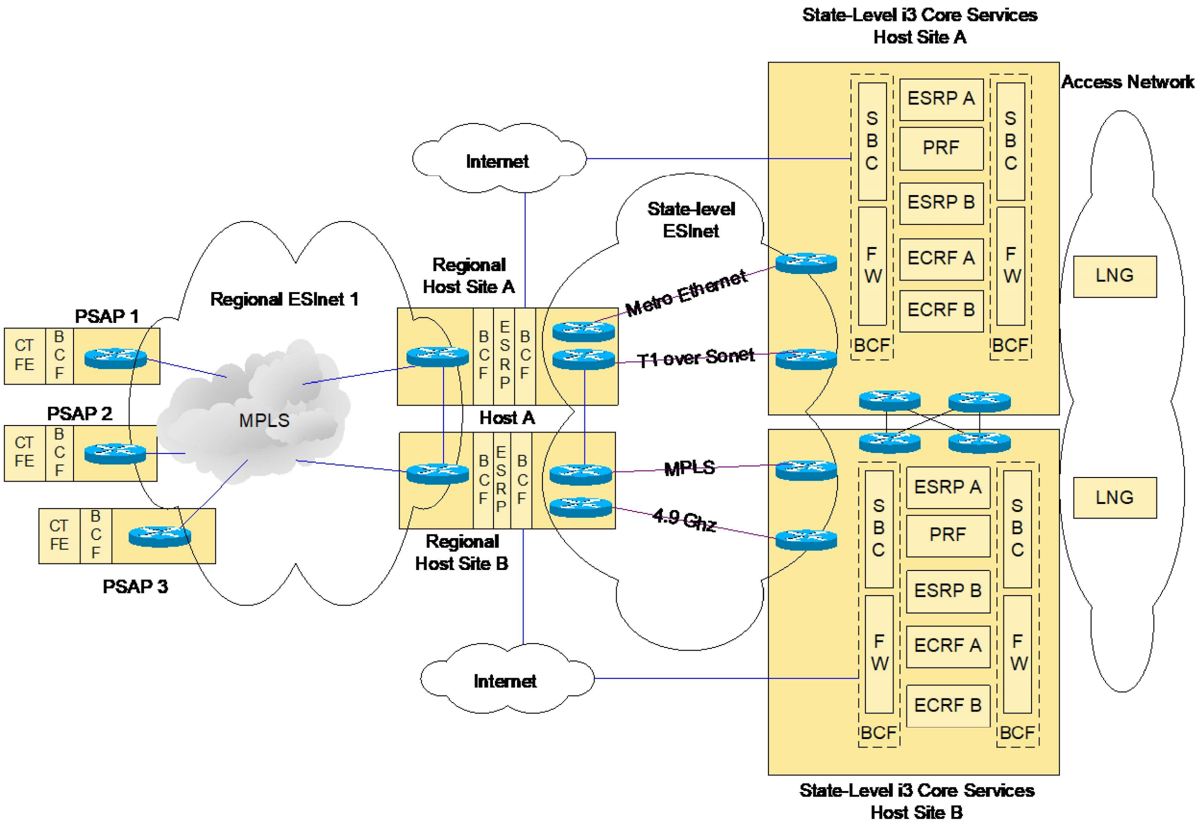


Figure 8

The state-level i3 core services are located at two (2) geographically-diverse sites – Host Site A and Host Site B. In order to assure high availability, redundant firewalls, Session Border Controllers (SBCs), ESRPs, and ECRFs are located at each of the state-level host sites. The i3 NGCS (e.g. ESRP, ECRF, and PRF) and the Legacy Network Gateways (LNGs) are outside the scope of the ESInet, but it was the consensus of the authors of this document that it would be advantageous to show how the i3 core services should be connected into an ESInet. It is a best practice to build state-level host sites and regional host sites in highly available data centers.

Regional ESInet 1 is comprised of an MPLS network. The PSAPs have a single entrance facility through which all circuits are delivered. A single router that provides connectivity into the regional ESInet is located in the backroom of each PSAP. Each PSAP has one or more call taker positions and a Border Control Function (BCF) which consists of a session border controller and a firewall. As discussed in section 3.4, reliability engineering calculations show the reliability and availability of Regional ESInet 1 to be on the order of two nines (99%). PSAPs utilizing this solution must therefore rely on traditional methods (i.e., back-up PSAPs and 10-digit numbers) to achieve five nines (99.999%) availability for the overall 9-1-1 service in their region. The state-level ESInet, which transports call signaling message exchanges, call media streams that carry the call's audio, and data from the state-level i3 NGCS to the regional host sites, is designed to achieve five nines availability. Connections to Internet border controllers from outside an ESInets are shown at both the regional hosts and state-level host sites. Among other things these connections could be utilized to support requirements to receive emergency 9-1-1 calls via the Internet and/or to support remote access requirements for monitoring and maintenance.

Regional ESInet II

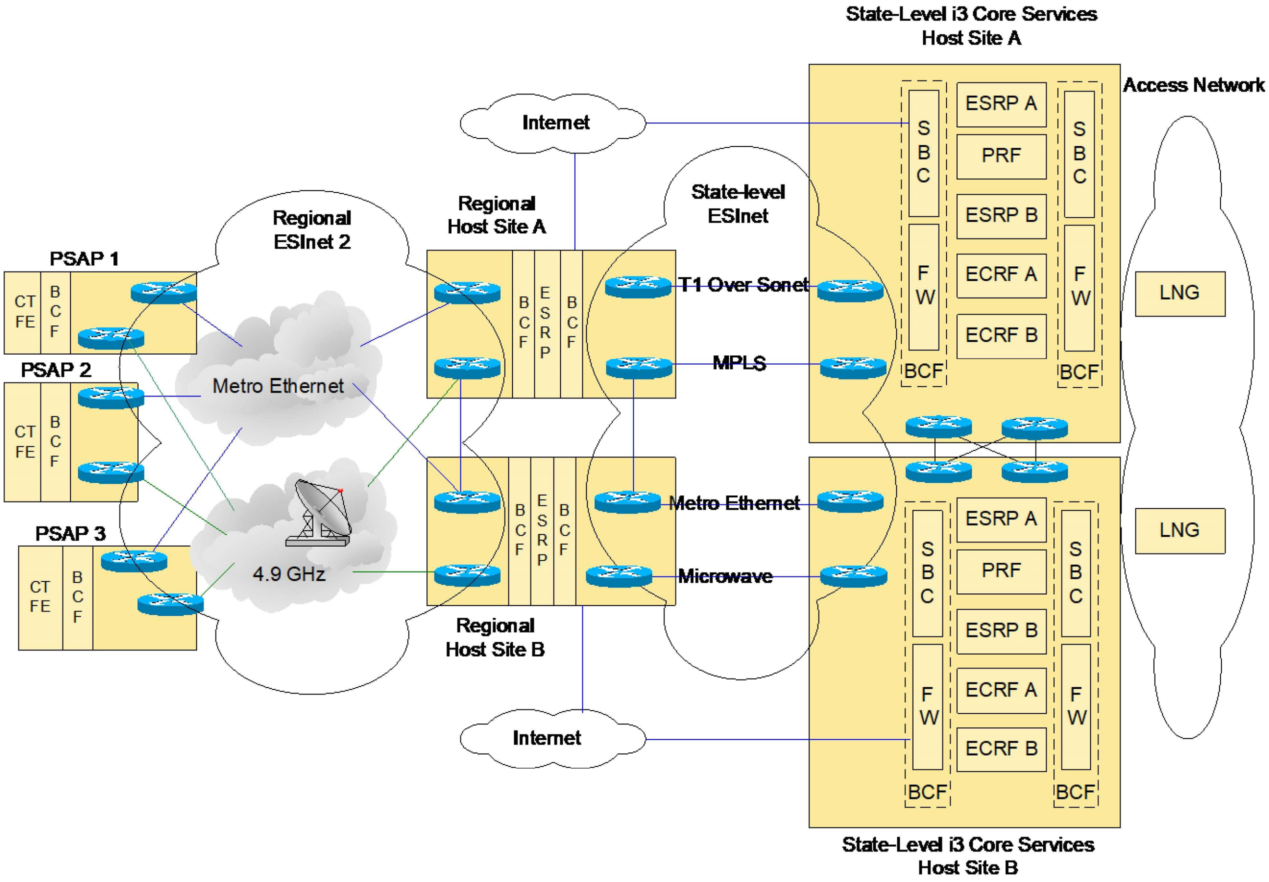


Figure 9

Regional ESInet II (above) is comprised of two physically diverse and independent networks; a Metro Ethernet and a 4.9 GHz microwave network. Separate routers and entrance facilities are utilized for each of the layer 2 technologies. As described throughout this document, there is a long list of other criteria which must be met, but assuming a typical PSAP environment, if properly designed and maintained, reliability engineering calculations show ESInet II to be capable of achieving three nines (99.9%) availability.

It is anticipated that many regional 9-1-1 entities, and possibly individual PSAPs, will connect into the state-level i3 NGCS. The diagram below shows how ESInets might be interconnected[19]. It is a best practice to design connections from regional host sites to state-level i3 core services (i.e., state-level ESInets) to achieve five nines availability.

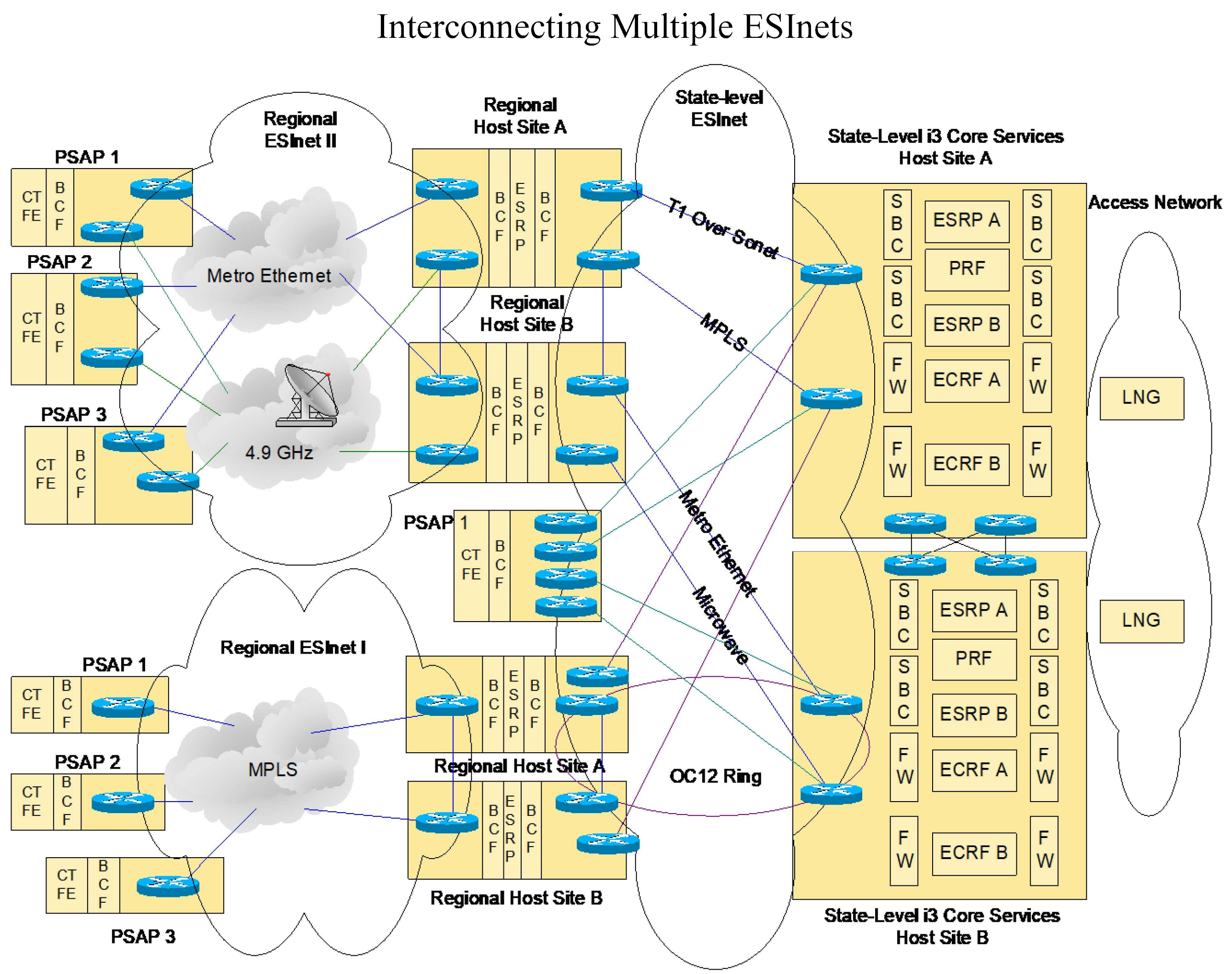


Figure 10

3 Conclusion

In this document many aspects underlying the design and construction of an ESInet supporting NG9-1-1 at OSI layers 1, 2, and 3 are addressed from both a technical and operational perspective. Given that resilient networks can be built using different approaches, a variety of network architecture options and methodologies for achieving recommended reliability and availability service levels are discussed throughout the document. In addition to the specific performance

[19] PSAP connections to the Internet are not shown

requirements that are included, operational requirements such as those that relate to service level agreements for operators of ESInets are discussed, as well as several aspects of network security. Further, since ESInets must deliver high priority traffic in the face of severe congestion, this document provides a variety of traffic engineering strategies for achieving these goals which are discussed alongside ESInet network management and monitoring.

After covering and reviewing the topics above and noting that a number of the topics covered in this document are fields of study to which people devote their entire careers, this working group has concluded that the information contained in this document by itself, although helpful and educational, does not provide all of the necessary details required to thoroughly design an ESInet supporting NG9-1-1. It is rather a best practice document, meant to stimulate discussion and provide background and overall guidance for qualified IP network design engineers tasked with designing ESInets supporting NG9-1-1.

It is not expected that the reader of this document will be prepared to design and implement an effective ESInet without first assembling a competent project team prepared with the knowledge and resources to take both a high level operating perspective, and also insure that the appropriate details have been addressed. An ESInet certainly is a critical aspect of the NG9-1-1 environment, but much more needs to be addressed to create a fully functioning NG9-1-1 operation as envisioned by NENA.

4 Impacts, Considerations, Abbreviations, Terms, and Definitions

4.1 Operations Impacts Summary

Implementation of Next Generation 9-1-1 (NG9-1-1) carries a significant amount of change to the administration, operation and physical infrastructure of the legacy 9-1-1 system. The deployment of NG9-1-1 standards requires that ESInets operate effectively to support the functions for NG9-1-1 call delivery.

At the foundation of an NG9-1-1 network is the ESInet. While IP networks, when properly designed, offer considerable improvements to the existing TDM-based platform with its CAMA format trunks, it is important to align ESInet implementations to common criteria. In addition to technical capability, management and security, the design of ESInets must consider factors such as availability, capacity, interconnection and interoperability. This applies to ESInets that have already been deployed as well as those being implemented or still in the planning stage.

This document provides recommendations based upon best practices and standards for IP networking, information delivery, service management, resiliency, and redundancy. The concepts referenced in this document are intended to be consistent with the NENA-STA-010 [1] standard.

4.2 Technical Impacts Summary

This is an informational document. As such, the recommendations made throughout this document may be considered as a guideline for use when specifying, designing and deploying ESInets. When implemented, some of the recommendations within this document may have significant technical impacts.

4.3 Security Impacts Summary

ESInets are utilized to provide IP transport between a number of different agencies and resources including PSAPs, regional host sites, and state-level Next Generation Core Services (NGCS). Many of the agencies connected to an ESInet will also be connected to untrusted networks including the Internet. Given the operating environment that NG9-1-1 requires, it seems likely that PSAPs, regional 9-1-1 entities, and state authorities will experience deliberate attacks on their systems. Maintaining high degrees of reliability, resiliency and security in this new environment will require a fundamental change in the approach taken to both physical and cyber security. The NENA Security for NG9-1-1 standard (NENA 75-001) is applicable and recommended. Qualified security engineers should be consulted when designing and deploying ESInets.

4.4 Recommendation for Additional Development Work

The Interconnection and Security Committee recommends that some of the material in this document be further developed into a NENA recommended standard. Outage reports for ESInets and NG9-1-1 elements in an ESInet have not been standardized[20]. There are no generally accepted mechanisms for reporting outages of such networks. The ESIND working group recommends NENA undertake an effort to define standardized outage reporting mechanisms consistent with ATIS Network Reliability Steering Committee (NRSC) efforts. This effort needs to address the analysis of outages and distribution of resolution.

4.5 Anticipated Timeline

This document addresses ESInets that are already being planned, designed and deployed and offers suggestions for consideration of future ESInet implementation.

4.6 Cost Factors

ESInets will replace existing legacy telecommunications infrastructures. The design, engineering and deployment of ESInets will drive costs that will vary based on the level of redundancy and reliability, as well as on the technologies used. Design criteria including bandwidth, Quality of Service, Jitter, redundancy, path diversity, and reliability requirements have the potential to impact the cost of the ESInet. Evolving security requirements and policies will increase the cost of the ESInet over time. Also, costs will increase as the scope increases in the use of the ESInet for interconnection to networks like FirstNet (and others), or the use of the ESInet for Internet access to additional data repository providers.

4.7 Cost Recovery Considerations

Normal business practices shall be assumed to be the cost recovery mechanism where available.

4.8 Additional Impacts (non-cost related)

ESInets provide the infrastructure upon which NG9-1-1 will be deployed. Transition to NG9-1-1 will have additional impacts. In many cases the deployment of ESInets will replace existing

[20] The Federal Communications Commission (FCC) requires reporting for any vendor or provider of 9-1-1 products or services within the 9-1-1 service path. The FCC web portal provides a Network Outage Reporting tool.

communications facilities for PSAPs. ESInet may add responsibilities for system monitoring, configuration management, maintenance and service management to ensure the expected level of service for 9-1-1.

4.9 Abbreviations, Terms, and Definitions

See NENA Master Glossary of 9-1-1 Terminology, NENA-ADM-000 [2], for a complete listing of terms used in NENA documents. All abbreviations used in this document are listed below, along with any new or updated terms and definitions.

Term or Abbreviation (Expansion)	Definition / Description
DS3 (Digital Signal 3)	Digital Signal Level 3 (DS3) service consists of a high capacity channel provisioned for transmission speeds of 44.736 Megabits per second (Mbps) isochronous serial data. Digital Signal Level 3 (DS3) facility can be channelized to provide 28 DS1 circuits with the multiplexing ability to enable a platform for voice, video, or data services.
FTTP (Fiber to the Premise)	A description of a fiber optic connection between a location and the service provider.
NANOG (North American Network Operators Group)	A governing body that provides guidance and instructions for the design of an IP network. NANOG is typically involved in the best current operational practices for IPv6 planning

5 Recommended Reading and References

1 Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3, National Emergency Number Association, NENA-STA-010

2 NENA Master Glossary of 9-1-1 Terminology, National Emergency Number Association, NENA-ADM-000.

3 NENA Security for Next-Generation 9-1-1 Standard (NG-SEC), National Emergency Number Association, NENA 75-001

4 Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, P. Ferguson, Internet Engineering Task Force, RFC 2267

5 Address Allocation for Private Internets, Internet Engineering Task Force, RFC 1918

6 IP Network Address Translator (NAT) Terminology and Considerations, Internet Engineering Task Force, RFC 2663

7 NENA 53-503 PSAP Survivability Operations Information Document

8 NENA 53-001 PSAP Disaster and Contingency Plans Model Recommendation

9 IEEE 802.1Q is the networking standard that supports virtual LANs (VLANs) on an Ethernet network.

10 ISO 7498-1 reference model provides a common basis for the coordination of standards development for the purpose of systems.

11 RFC 2328 documents version 2 of the OSPF protocol

12 RFC 1142 documents the OSI IS-IS Intra-domain Routing Protocol

13 RFC 4271 discusses the Border Gateway Protocol (BGP), which is an inter-Autonomous System routing protocol.

14 ITU-T G.114 is an ITU recommendation that addresses acceptable delays for voice applications, is oriented to national telecommunications and is more stringent than what is normally applied in private voice networks.

15 G.711 is an ITU-T standard for audio companding.

16 H.264 or MPEG-4 Part 10, Advanced Video Coding (MPEG-4 AVC) is a block-oriented motion-compensation-based video compression standard.

17 NIST 800-81-2 (Identified as Special Publication 800-81-2, Secure Domain Name System (DNS) Deployment Guide

18 RFC 2475, An Architecture for Differentiated Services

ACKNOWLEDGEMENTS

National Emergency Number Association (NENA), Interconnection & Security Committee, NG9-1-1 Architecture Subcommittee, Emergency Services IP Network Design Working Group

NENA Board of Directors Approval Date: 04/05/2018

NENA recognizes the following industry experts and their employers for their contributions to the development of this document.

Members	Employer
Nate Wilcox, Interconnection & Security Committee Co-Chair	Emergicom
Steve O’Conor, ENP, Interconnection & Security Committee Co-Chair	Synergem Technologies, Inc.
Theresa Reese, Interconnection & Security Committee, NG9-1-1 Architecture Evolution Subcommittee Co-Chair	Ericsson Inc.
Guy Caron, ENP, Interconnection & Security Committee, NG9-1-1 Architecture Evolution Subcommittee Co-Chair	Bell Canada
Jim Lockard, ENP, Working Group Co-Chair	Lockard Strategic Advisors, LLC
Joel McCamley, ENP, Working Group Co-Chair	911 Authority, LLC
Tina Bone	North Carolina 9-1-1 Board
Rob Clark	ATOS Public Safety
Dennis Cleary	Clear Results, LLC
Dave Corn	North Carolina 9-1-1 Board
David Curran	Frontier Communications
Jeremy Duncan	City of Grand Junction, CO
Mike Hayes	Greater Harris County Emergency Network TX
David Hopkins, ENP	Steuben County NY
Maria Jacques, ENP	State of Maine
Keith Martin	AT&T
Steve McMurrer, ENP	Fairfax County VA
Chuck Ploof	Charles R. Ploof & Associates
Pierce Power, ENP	Teleira
Brian Rosen	Neustar Inc.
Milton Schober, Jr.	Mission Critical Partners Inc.
Mark Suson	Stephens County OK
Raymond Vilis	Solacom Technologies
Michael Vislocky	Network Orange Inc.

Special Acknowledgements:

Delaine Arnold, ENP, Committee Resource Manager, has facilitated the production of this document through the prescribed approval process.

The Emergency Services IP Network Design Working Group is part of the NENA Development Group that is led by:

- Pete Eggimann, ENP, and Jim Shepard, ENP, Development Steering Council Co-Chairs
- Roger Hixson, ENP, Technical Issues Director
- Chris Carver, ENP, PSAP Operations Director