AVISTAS

Business Vision

Real-World Results

The Case for IPv6 in Secure Networks Supporting Next Generation 9-1-1 and Radio Systems Interoperability

Mart D. Nelson, P.E., ENP

In the CSEC report “Final Report for Texas Emergency Service IP Network (ESInet) Functional Requirements and Interconnection”, dated September 29, 2009, the following recommendations and comments are provided:

- **The state-level and regional ESInets must plan for the support of both IPv4 and IPv6 addresses, with a tactical goal of deploying IPv4 addresses to initialize the network and a strategic goal of ultimately deploying IPv6 addressed throughout the entire network.**
- **It mentions DNSSEC, the security extensions for the domain Name Service.**
- **It mentions NTP, the Network Time Protocol.**
- **It mentions SNMP, the Simple Network Management Protocol.**

The current NENA Technical Committee draft, “Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3“, dated January 7, 2010 supports IPv6, secure ESINets and DNS for addressing, but also allows IPv4 as an alternative.

The remainder of this paper recommends specific requirements and provides rationale for a secure network design to support ESINET functions, related Next Generation 9-1-1 functionality and IP interconnection of Emergency Services radio systems for Level 5 or Level 6 interoperability.

Recommended Network Requirements:

A Next Generation 9-1-1 ESINet or related Public Safety IP (Internet Protocol) network should be implemented with the following characteristics:

- Use of IPv6 addressing throughout with IPSec security enabled
- Implementation of Secure Domain Name Services (DNSSEC) within the network(s)
- Redundant, diverse Network Time Servers, with each network device using Network Time Protocol (NTP) directed to at least 2 reference servers.
- Simple Network Management Protocol, Version 3 (SNMPv3) with appropriate security protocols engaged
- Assignment of all entity names via fixed DHCP references (Dynamic Host Configuration Protocol)
- Use of Dynamic DNS, sourced to the DHCP Servers
- Establishment of an internal Public Key Infrastructure (PKI) certificate authority, potentially referenced to a Statewide PKI Registration authority.

Each of the above recommendations contributes to a network infrastructure that:

- Protects the confidentiality of communications
- Provides for resistance to outside tampering
- Provides resistance to inside errors and tampering
- Supports effective network and systems management
- Supports unique, direct addressing of any Emergency Services device or endpoint in the State.

Rationale:

With regard to each recommendation above, specific rationale are provided below. These recommendations will provide for a stable, long term network infrastructure that will allow a wide variety of IP Emergency Communications functions to be implemented in a secure and tamper-resistant network environment. There are more detailed underlying technical justifications in some cases, which are beyond the scope of this document.

IPv6 Addressing with IPSec

- IPv6 provides for unique, Statewide (and Nationwide) addressing for each device in the network, since IPv6 provides for about 400 trillion trillion (sextillion) unique addresses for each square inch of the Earth's surface.
- IPv6 can be implemented with IPSec, encrypting all communications on the network.
- The US Government mandates the use of IPv6 addressing in new government networks.
- Emergency Service networks will be, by their nature, closed, private networks with clearly defined and controlled interfaces to other networks and to outside IPv4 Internet addresses.

Secure Domain Name Services (DNSSEC)

- DNSSEC provides for significant resistance to DNS attacks (internal or external) designed to falsify the identity of devices on the network intended to redirect communications to the address under the control fo the attacker.
- DNSSEC acts as a gateway to outside DNS systems to reduce exposure to DNS attacks in the Internet.
- OMB mandate M-08-23 requires every U.S. federal government IT organization to deploy DNSSEC

Network Time Servers

- Accurate time-of-day across all devices in a network is critical to consistent logging and to investigating and resolving problems across the network.
- Two or more accurate, stable time sources (Network Time Servers) should be in the network, with each network device accessing the correct time from one server via NTP, with a second server as a backup.

Simple Network Management Protocol, Version 3 (SNMPv3), with security

- SNMP provides for access to device operational and performance data and, in some cases, allows modification of the device configuration.
- SNMPv3 can be configured with a level of security that resists external or internal attempts to illegitimately access device information.

Fixed DHCP references (Dynamic Host Configuration Protocol)

- Assignment of all device addresses in a central DHCP server allows easier control of network and systems changes and modifications.
- Unassigned devices appearing on the network should be assigned an address that will restrict the access of the device in the network and allow new devices to be detected and investigated.

Dynamic DNS, sourced to the DHCP Servers

- DNSSEC servers should obtain all device name and address data from the DHCP servers, so as to assure consistency of names and accurate addresses as network changes are made over time.

Public Key Infrastructure (PKI) Certificate Authority

- PKI services are required for IPSec secure communications set-up as connections are created in the network.
- A Certificate Authority in the network allows encryption keys to be managed automatically and with validation of authenticity.
- Ultimately a Statewide Registration Authority could manage and maintain the authenticity of each Certificate Authority and each encryption key issued in the Emergency Services networks.

A commitment to establish secure Public Safety networks using internationally recognized network and security standards will simplify the control, management and security of these networks.

Note:
Requirements for overall NG 9-1-1 Security and Management can be found in:
"*NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)*", Standard Number: 75-001