CAPSNET Roadmap

JUNE 2013

California Public Safety Microwave Network (CAPSNET)

Edmund G. Brown Jr.
Governor

California Technology Agency
Public Safety Communications Office

Karen Wong
Director

Version 1.26

(Page intentionally left blank)

Table of Contents

(Page intentionally left blank)

CALIFORNIA TECHNOLOGY AGENCY
PUBLIC SAFETY COMMUNICATIONS OFFICE

Karen Wong
Director

Dear Fellow Californians:

Every year, natural and man-made disasters in the United States and around the world serve as a reminder of the need for California to plan and prepare for unexpected emergencies. Up-to-date radio and data communications are essential for first responders to provide emergency services to Californians at a moment's notice. With new and emerging technologies, the State has an opportunity to plan and implement sensible improvements to its telecommunications system so that it can provide the best emergency response system for the people of California.

For more than 50 years, the State has relied on the state-owned and operated California Public Safety Microwave Network (CAPSNET) for its emergency and routine operation communication needs. This system lacks the capabilities of a modern network and needs to be upgraded. Through a shared commitment to improve these systems, the CAPSNET roadmap was developed and details the necessary steps to improve the network.

The successful completion of the CAPSNET Roadmap goals and objectives will ensure that up-to-date technologies are used to deliver vital services and a new level of emergency response. The CAPSNET Roadmap outlines how the State can convert from the legacy analog and time division multiplex system to a state-of-the-art Internet Protocol (IP)/Multi-Protocol Label Switching (MPLS) (IP/MPLS) system. The roadmap defines, plans and addresses all aspects of the conversion process including: Administration and Operations, System Design and Implementation, Network Operations and Facility Preparation.

The California Public Safety Microwave Network (CAPSNET) roadmap is a huge endeavor that will positively impact the people of California. This vision of a more efficient and effective microwave network reflects the collaboration and extraordinary efforts of our stakeholders, client agencies and public safety Communications staff. I would like to thank all of our client agencies and stakeholders for their contributions to the development of this plan.

Sincerely,

/S/
Karen Wong, Director
Public Safety Communications Office

(Page intentionally left blank)

SECTION 1 - EXECUTIVE SUMMARY

The California Technology Agency, Public Safety Communications Office (PSCO) owns and operates a statewide microwave network known as the California Public Safety Microwave Network (CAPSNET), which has met the State's needs for nearly half a century; however, many of the network components are well past their projected useful life. To support current public safety voice and future IP-based applications like the California Public Safety Communications (CAPSCOM) System of Systems, and Next Generation 9-1-1 (NG9-1-1) system for its stakeholders, the CAPSNET requires upgrading.

The objective of this project is to develop a roadmap for the conversion of the CAPSNET from a legacy analog and time division multiplex system to a state-of-the-art Internet Protocol (IP)/Multi-Protocol Label Switching (MPLS) (IP/MPLS) system that will carry existing radio control circuits, along with new voice, video and data applications; however, the primary focus of the CAPSNET will continue to be the transport system for public safety dispatch voice circuits. PSCO has begun work on the IP/MPLS system design, with the goal of completing it by the end of 2013. This Roadmap presents a staged implementation plan that focuses first on core areas like Sacramento, San Francisco Bay Area, Los Angeles and San Diego, and key connecting routes. Funding and staffing allocations applied to the CAPSNET upgrade will determine how long the project will take to complete.

In addition to system design and implementation, there are other aspects, such as governance, network operations centers, service level agreements and marketing that must be addressed by PSCO to ensure the long-term success of the CAPSNET. This Roadmap addresses all of these aspects, and provides direction for the completion of each one. The successful completion of the project will result in a system that:

- Allows for the integration of new sites and data services on the public safety microwave system.
- Utilizes path redundancy and automatic route switching to improve reliability and survivability.
- Reduces the cost to provide secure public safety communications and flexibility to the client agencies for the CAPSNET by offering new IP data services that could not be carried on the existing analog and time division multiplex system.
- Uses IP/MPLS technology to support applications like the CAPSCOM System of Systems and NG9-1-1.
- Ensures the security of client agency traffic being transported by the CAPSNET.

SECTION 2 – THE ROADMAP

The California Technology Agency, Public Safety Communications Office (PSCO) owns and operates a statewide microwave radio system known as the California Public Safety Microwave Network (CAPSNET). The objective of this project is to develop a roadmap for the conversion of the CAPSNET from an analog and time division multiplex system to an Internet Protocol (IP)/Multi-Protocol Labeling System (MPLS) network that will support public-safety radio applications. The primary focus for the CAPSNET will continue to be the transport of radio dispatch communications circuits; however, other client agency IP-based public safety applications will also be carried on the system on a secondary basis. The use of the MPLS and IP technologies will allow the system to carry voice, video and data applications on the same network, and to establish priority levels for the different applications. MPLS will also improve transit times across the network by reducing the processing time of the network routers.

The Roadmap identifies the necessary steps to upgrade the CAPSNET from an analog and time division multiplex system to an IP/MPLS network. In preparing the Roadmap, interviews were conducted with PSCO and client agency staff to ascertain the As-Is state of the CAPSNET and to define the desired To-Be State. This roadmap provides the information needed by PSCO to get from the As-Is to the To-Be state, and is aligned with the goals of the CAPSNET Strategic Plan. The new IP/MPLS network will allow for the realization of the California Public Safety Communications (CAPSCOM) and Next Generation 9-1-1 (NG9-1-1) Strategic Plans, which are based on the use of IP technology to provide enhanced services.

The Roadmap is an actionable and sustainable plan and provides a logical approach to implementing the objectives of the CAPSNET Strategic Plan based on current conditions, constraints and industry best practices. It should be used as a benchmark document that is reviewed annually to address new and changing conditions for design, deployment, resources and funding. The resulting system will increase technical capability, improve interoperability and allow for the advancement of next generation public safety communications.

The Roadmap is based on information provided by the PSCO and the client agencies that use the CAPSNET. Each of the project activities described below should be performed concurrently to expedite the schedule. The equipment replacement work and the IP/MPLS system design have already been started.

SECTION 3 - CAPSNET BACKGROUND[1]

CAPSNET History

The CAPSNET has been in service for more than fifty years ago and it has evolved into a statewide network of approximately 329 sites that was deployed using analog radio technology to provide:

- **Radio Communications** connectivity between radio transceivers and the dispatch and emergency communications centers.
- **Remote Management of Radio Communications Equipment and Site Assets,** such as land mobile radio equipment, door alarms and power systems**.**
- **Emergency Telephone Service** serving State public-safety subscribers to ensure that personnel located in dispatch or emergency command centers have telephone service during a disaster when the commercial telephone service might not be available.

CAPSNET Today

CAPSNET is a hybrid network consisting of older analog and legacy digital time division multiplex radios. As part of the CAPSNET upgrade project, PSCO has begun the process of replacing the existing radios with dual-mode time division multiplex/Ethernet radios which will allow for the transition to IP/MPLS technology. There are a total of 329 microwave sites. Following is a breakdown of the upgrade status for these sites:

- 166 sites on the system that are digital, which includes:
  - 26 sites with the new IP/MPLS-capable radios
  - 140 sites with legacy time division multiplex radios that need to be replaced with the new IP/MPLS-capable radios.
- 72 sites that have analog radios that need to be replaced with the new IP/MPLS-capable radios.
- 91 analog and legacy time division multiplex sites that are currently in the engineering design process for the installation of new IP/MPLS-capable radios.

The CAPSNET has four core attributes that make it uniquely valuable to the public-safety community:

- **Survivability** — it is designed to operate during natural disasters.
- **Reliability** — it is designed for high reliability, with built-in path and equipment redundancy.
- **Connectivity** — it will continue to provide connectivity to remote radio sites where other communications media are not available.
- **Public-Safety Communications –** the focus for CAPSNET is to support public-safety radio, such as the remote control of remote base station and repeater radios from a dispatch center, to allow for communications with field staff over extended distances.

[1] Portions of this section were obtained from the CAPSNET Strategic Plan, published on March 3, 2011.

Need to Upgrade

While the CAPSNET has been in place and has met the State's needs for nearly half a century, many network components are well past their useful life. The analog technology is outdated and difficult to support and the legacy time division multiplex technology will not allow for the migration to IP applications. The continued use of this legacy equipment requires the State to maintain expertise and capabilities in technologies which have been abandoned by much of the private sector. Many of the radio components have been discontinued by the manufacturer, making replacement parts difficult to find. In addition, the current system cannot support the next generation of radio and data transmission technologies which the State will be deploying as part of the 10-year CAPSCOM NG9-1-1 strategies.

Table 1 provides a summary of As-Is and To-Be states of CAPSNET, obtained through interviews with PSCO and client agency staff.

Table 1. CAPSNET Today vs. CAPSNET Future

CAPSNET - Today	CAPSNET - Future
Older analog and time division multiplex technology supporting connection oriented voice services.	IP/MPLS technology supporting packet based voice, video and data traffic with legacy time division multiplex support.
Will not support the migration of CAPSCOM to an IP-based platform.	Backbone that will support the System of Systems and Next Generation Public Safety Applications.
Manual traffic restoration.	Automatic and Remote Traffic Restoration.
Sites in varying states of repair and security levels.	Sites providing a secure and stable environment for the equipment.
High cost due to minimal usage by State Agencies.	Lower per circuit costs by increasing the number of agencies and through greater system utilization.
Manual traffic monitoring.	Real-time traffic monitoring and control.

SECTION 4 - ADMINISTRATION & OPERATIONS

Governance

The PSCO is in the process of creating a governance structure, as described and recommended in the California Public Safety Radio Communications (CAPSCOM) Strategic Plan[2] that will cover the two-way radio systems designed, installed, maintained and repaired by PSCO for its client agencies, and the CAPSNET, whose primary role is and will continue to be, to provide connectivity for public-safety radio systems.

The governance team will enable collaboration with the client agencies. This will provide the client agencies a forum for discussing the progress of the CAPSNET upgrade, the type of services and applications that should be allowed, success stories regarding the use of the new IP/MPLS network and any other issues of interest to the client agencies. The success of the CAPSNET upgrade project will depend on strong leadership and cooperative inter-agency support.

Service Level Agreements

PSCO has not initiated formal Service Level Agreements (SLA's) to its client agencies for the services transported by the CAPSNET, but will with the new IP/MPLS network. SLA's will provide a formal process to describe the CAPSNET service level targets, identify objective metrics, and provide a process to define, collect and report ongoing fulfillment of stated goals. They will also identify the responsibilities of the PSCO and its client agencies. SLA's for the CAPSNET should model Figure 1 below:

Figure 1. Basic Service Level Agreement Structure

Services	SLA Name
List of all applicable tools, reports, and applications.	Definition: A description removing ambiguity and providing universal understanding between agency customer and provider.
	Measurement Process: Instructions on how to measure service provider administration performance in order to determine compliance.
	Objectives: Defines the performance goal/parameters for each SLA. In addition to specific network performance metrics, objectives might include stated minimum or maximum cycle times or delivery date frequency for reports. Objectives might include such things as response times and escalation procedures. Objectives focused on invoicing timeliness and accuracy can also be defined.
	Immediate Rights and Remedies: Allows immediate action by the service provider and the agency customer by defining the escalation process and/or rebates which are usually applied to the monthly invoices on a per occurrence basis.
	Monthly Rights and Remedies: This is applicable to SLA's which require the accumulation of statistics over a period of time. This can be a monthly average, monthly maximum, it can be defined by time period within a month, and just about any other measurement method as it justly applies to the SLA. In some cases, annual rights and remedies are also appropriate. The time period in which remedies are applied also is defined here.

[2] California Public Safety Radio Communications Strategic Plan produced by the Gartner Group in September 2010.

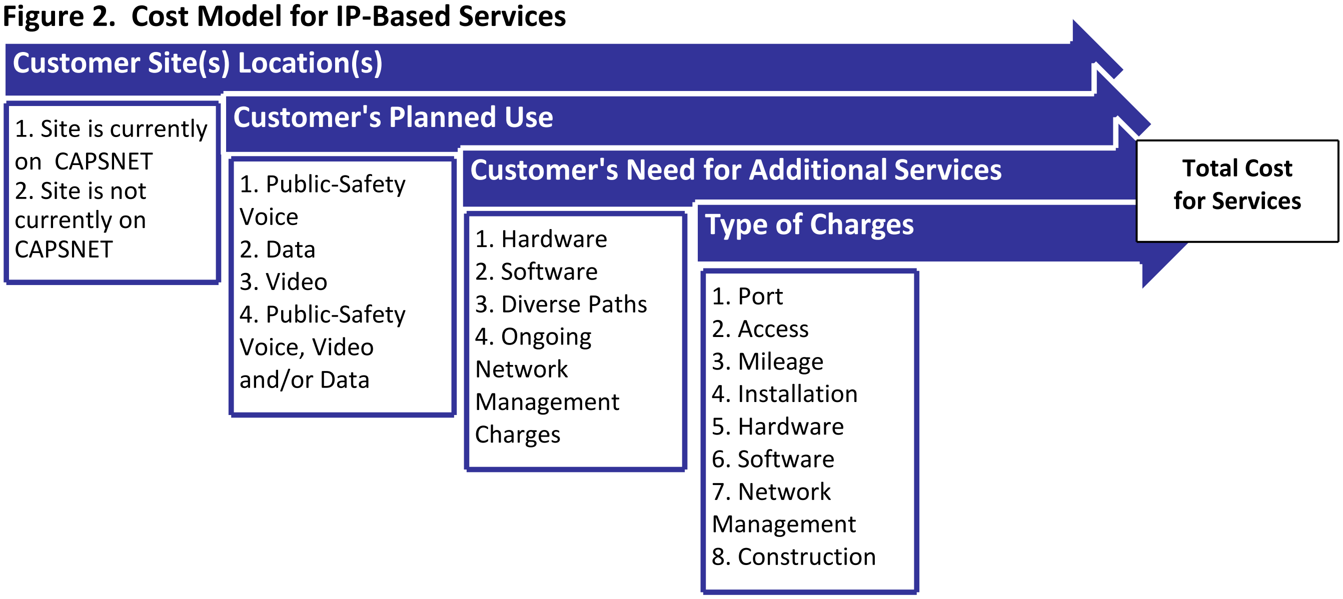
Cost Model

A new cost model should be developed by PSCO for the CAPSNET that will better fit the new IP-based services that will be transported. New IP-based public-safety services planned for CAPSNET should be based on individual client needs, most of which have not been identified yet. PSCO should continue working with each of its client agencies to discuss the capabilities of the new IP/MPLS network and to assist them in identifying applications that could/should utilize the new system. Listed below are some of the services that can be transported over an IP/MPLS backbone, to address public-safety voice traffic currently being transported by the CAPSNET and new applications that may utilize the CAPSNET:

- Radio over Internet Protocol
- Ethernet Virtual Private Line – data service providing point-to-point Ethernet connections.
- Ethernet Virtual Private Local Area Network - a multi-point-to-multi-point Ethernet virtual connection.
- Voice Over IP – commonly refers to the technologies and transmission techniques involved in the delivery of voice communications over IP networks.
- MPLS Virtual Private Network (VPN) – transmitting voice, video or data services over an MPLS network using a VPN.

PSCO should utilize an approach similar to that shown in Figure 2 to determine the cost to transport new IP-based services on the CAPSNET.

Figure 2. Cost Model for IP-Based Services



Customer Site(s) Location(s)

1. Site is currently on CAPSNET
2. Site is not currently on CAPSNET

Customer's Planned Use

1. Public-Safety Voice
2. Data
3. Video
4. Public-Safety Voice, Video and/or Data

Customer's Need for Additional Services

1. Hardware
2. Software
3. Diverse Paths
4. Ongoing Network Management Charges

Type of Charges

1. Port
2. Access
3. Mileage
4. Installation
5. Hardware
6. Software
7. Network Management
8. Construction

Total Cost for Services

The first three categories in Figure 2 (Customer Site Location(s), Customer's Planned Use and Customer's Need for Additional Services) list the items that impact the cost for IP-based services and the fourth category, Type of Charges, is how cost for services is determined. Following is a brief description of each of the items in Figure 2.

Customer Site Location(s)

The initial and primary cost factor is whether or not the customer site is currently on the CAPSNET or not. If not, there will be a one-time cost to provide microwave connectivity to the site. If it is, the cost will be for the additional service provided.

Customer's Planned Use

The next cost factor is the type of service that will be provided: public-safety voice, data, video or all three. In addition, cost is impacted by the performance, reliability, security requirements, and the amount of bandwidth utilized.

Customer's Need for Additional Services

The third cost factor is for additional equipment or services needed by the client, including network hardware, software, path diversity, and/or network management services.

Type of Charges

There is no single cost model for IP-based services. Cost models continually change based on new technology, and the need to develop custom pricing and circuit programs that optimally meet customer needs. Future IP-services have not been fully defined by the client agencies and the cost model for new IP services should also be aligned with service level agreements. In preparing the cost model for new IP-based public-safety services, PSCO should base the cost on factors such as: port, access circuit, mileage, installation, hardware, software, network management and construction.

Project Staffing

Project management staff must coordinate and guide the efforts of the project team to ensure that project goals are met. Engineering and Installation teams will require a ramp-up period to achieve required staffing levels, and equipment and training necessary for each phase. PSCO has flexibility in assigning and rotating staff between engineering, installation and maintenance areas and can utilize this flexibility to meet times of peak demand for field installation. Additional staff may be required to achieve the goals and project timelines for the CAPSNET upgrade project. Specialized training for staff will be required for the network operations center and security personnel.

The useful life of new technology is limited and, as a result, rapid deployment will maximize the cost benefit to the client agencies. Emphasis is needed in the following areas:

- Align policies, procedures, documentation and staff assignments early in the project with the core Project Team given the direction and authority to achieve the project goals.
- Assign internal resources to the project with redefined roles and responsibilities to improve efficiency and to address changes in the system life-cycle.
- Establish new positions the address the shift from analog and time division multiplex to an IP/MPLS-based system.
- Use trained resources to supervise and provide direction for temporary and contract resources.

Training

To accomplish the goal of providing an IP/MPLS transport service to its client agencies, PSCO will need to acquire, assimilate and sustain the IP/MPLS technology. An IP/MPLS system has many rules and processes that change frequently. PSCO is currently training Engineering and Operations staff on IP/MPLS technology; as the system implementation moves forward, the staff will gain the necessary experience and confidence with the technology. IP/MPLS training must be ongoing to meet the ever evolving technology.

Network Operations Center

Training for Network Operation Center staff will center on rigorous radio system engineering and the use of diagnostic tools and techniques for monitoring events, predicting problems, trending performance and the remote trouble shooting of IP/MPLS networks. It cannot be over emphasized that the Network Operations Center is the engine that drives all IP-based networks, and the success of the project depends on a Network Operations Center staff that is well trained in the IP and MPLS technologies.

Security

CAPSNET supports the transport of new services which require secure data delivery. PSCO must ensure that security policies affecting physical and cyber security are aligned with current information security policies and practices and staff are trained prior to engineering and installation.

Engineering and Operations

Training for Engineering and Operations is essential for proper design, maintenance and restoration of the system should there be a failure. The level of training required for Engineering and Operations staff can be mitigated by utilizing highly trained Network Operations Center personnel to support commissioning, trouble resolution and repair activities. The number of products, technologies and the physical integration between analog, digital and IP/MPLS during the design and deployment interval will increase the complexity of field troubleshooting efforts and may introduce system issues that require knowledge not only of the equipment, but also of the sites and transitional integration methods.

Marketing

The client agencies must be aware of the new capabilities of an IP/MPLS network, what type of services can be carried and how it will benefit them. This will lead to increased usage, new users and lower cost for services. PSCO currently does not have a formal plan for marketing the CAPSNET to its client agencies or to other local or county public-safety agencies; however, with the upgrade of the CAPSNET to an IP/MPLS network, an effective marketing plan will be crucial to educate the client agencies and other potential customers as to what the new network has to offer and to promote successful case studies to other client agencies. With an effective marketing program PSCO will realize increased system utilization and lower costs for service.

The governance structure that is developed for the CAPSCOM should include the identification of solutions offered and service expectations. Since the governance structure will include the Statewide Interoperability Committee (SWIC), this outreach will include local government. In addition, development of an outreach program will be a key to a marketing program success.

SECTION 5 - SYSTEM DESIGN

This section describes the design required to replace the existing analog and legacy time division multiplex system with an IP/MPLS network. A comprehensive system design will:

- Allow for the integration of new sites
- Identify future data services while improving survivability.
- Reduce the cost to provide secure public safety communications to participating agencies.
- Ensure the security of client agency traffic being transported over CAPSNET.

The success of a multi-year microwave project depends on a fully integrated design, which results in a reduction in the time and cost to deploy, the amount of rework required and the effort necessary to produce an operational system. PSCO is preparing the system design with a target of completion by the end of 2013. The following constraints were used in the estimate for system design:

- **Path Design and Optimization** was based on 300 paths and included a budget for frequency coordination.
- **Traffic Plans and Engineering** included overall network design, system specifications and documentation, the migration of existing client agency traffic, compatibility testing for new services and the development of the technical requirements for Service Level Agreements.
- **Network Management System** included the design and documentation of remote site monitoring and the Network Operations Center equipment, development of graphical user interfaces, update of notification and trouble ticket systems, design of the traffic control and testing platform, and the development of maintenance and performance reports.
- **Security Design** included participating in the development of standards, configuration of security policies on network elements, and design of the automated security monitoring system.

The resources needed for the system design activities include the current engineering staff, engineering support staff and the Department General Services (DGS), which is responsible for site construction work. The design activities also require deliverables provided through contracted services for frequency coordination and manufacturer subject matter experts to expedite integration and configuration tasks.

Path Design and Optimization

Microwave radio path design and optimization define the connectivity of the network, and identify system capacity restraints and traffic routing requirements. Path design is also critical in defining additional tower load requirements for temporary and/or permanent antennas required for the system upgrade. Identifying tower loading issues early in the project will provide time for tower modifications to be completed before they impact the project schedule.

The following activities should be completed for the path design and optimization effort:

- Map studies to confirm coordinates and terrain data.
- Analysis of existing and future paths using engineering design software to determine the antenna heights required to meet performance goals, and field investigations to identify path obstruction heights.
- Frequency coordination to reserve spectrum and capacity for each path.
- Optimize antenna placement to improve performance and to reduce tower loading.
- Evaluate alternate or additional microwave paths to improve performance, resiliency and redundancy.

- FCC license preparation when the sites are ready to deploy.
- Develop antenna loading reports to assist the Department of General Services (DGS) in performing the structural analysis and/or the design of new or replacement towers.
- Develop system maps that identify each of the microwave links and capacities.

Issues, dependencies and risks associated with path design and optimization are:

- Identifying the site upgrade requirements depends on completing the Path Design and Optimization effort, which defines the tower loading and facility requirements.
- Due to frequency congestion in the lower 6 GHz radio band, frequencies may not be available to upgrade the existing analog and/or legacy time division multiplex paths to a 150 Mbps IP/MPLS radio for certain paths.
- Upgrading longer microwave paths to IP/MPLS may require intermediate repeaters due to lower system gain of the higher capacity IP/MPLS radios as compared to the existing analog and legacy time division multiplex radios.
- Potential path obstructions should be re-evaluated since conditions may have changed since the paths were originally installed.

Traffic Planning and Engineering

The IP/MPLS system design for the CAPSNET should provide high reliability and path redundancy across the network core. This includes automatic restoration and protection; minimizing the time it takes for the network routers to collect all available topology information; minimize the time it takes for traffic to traverse the network; and ensure adequate traffic throughput and connectivity in the event of equipment, system, path or site failures.

The following activities should be completed for Traffic Planning and Engineering:

- Identification of the type of services that will be offered on the system.
- Develop or refine circuit identification scheme to allow for easy identification of circuit type and routing.
- Identify existing voice circuits and routing per site, by agency.
- Develop traffic plans for each agency that identify capacity, routing, protection and latency.
- Identify capacity needed over each link for all agencies during normal and protected operation.
- Identify special integration needs for agency equipment that interfaces to the backbone and handoffs between analog, digital and IP/MPLS segments during the different stages of deployment and cut-over.
- Develop an IP Plan that includes:
    - IP addressing and protocols for each network element.
    - Identification of network elements that will be integrated into the system, including, but not limited to: routers, switches, firewalls, gateways and servers.
    - Identification of Quality of Service (QoS) requirements to prioritize traffic on the network.
    - Testing requirements for the system design and configuration in lab and field environments.

Issues, dependencies and risks associated with Traffic Planning and Engineering are:

- Traffic Engineering is constrained by available bandwidth of each path and physical system topology.
- The types of service that will be integrated into the system have not been identified by the client agencies. Integration may require additional equipment to meet client needs.
- Compliance testing to determine network interfaces with client equipment, gateways, firewalls and security has not been performed. Agency network elements and interfaces may not integrate seamlessly into the new CAPSNET equipment.
- The clients are not currently prepared to interface existing radios to the new IP/MPLS backbone nor have they identified any additional capacity or service needs for future growth. The link, segment and backbone capacities should be evaluated on a continuous basis to accommodate future growth.

Network Management System

Designing the Network Management System (NMS) design for the new IP/MPLS network should include the following activities:

- Develop Simple Network Management Protocol (SNMP) traps for each network element.
- Identify the alarms, controls and status points to be monitored for equipment, power and facilities.
- Develop the NMS for traffic engineering and restoration.
- Develop User Interfaces and security for the NMS.
- Define and develop alarm, performance and statistical reports for operations, Service Level Agreement's and client needs.
- Develop billing and financial reports using the NMS.
- Define hardware, software and firmware inventory control.
- Monitoring of facility and equipment alarms needs to be expanded and appropriate responses better defined. Facility outages typically take considerable time to repair and many prolonged outages result from poor facility maintenance.

Security

The CAPSNET must adhere to all State security requirements. In addition, network guidance for security can also be obtained from the Catalog of Control Systems Security: Recommendations for Standards Developers[3], which is based on National Institute of Standards and Technology (NIST) SP800-53 Rev 3 to facilitate the security management of control system environments; however, the document is adaptable to provide guidance in developing the CAPSNET Security Plan while providing a framework for the protection of networks supporting critical infrastructure.

[3] Department of Homeland Security, April 2011.

Following are the primary security tasks identified in the Catalog of Control Systems Security: Recommendations for Standards Developers that PSCO should implement for new IP/MPLS network.

- **Risk Assessment –** Perform a risk assessment to determine physical and cyber vulnerabilities to sites, equipment, and data sources that contain sensitive information. Identify a methodology to mitigate risks to data integrity and system operation, and establish an ongoing risk management process**.**
- **Network Protection -** Establish a network protection strategy that mitigates risk and requires varying levels of authentication and encryption to secure network resources. Establish backup security systems and a lab to test security functions prior to placing new services and equipment on the system**.**
- **Security Officer -** Assign a Security Officer and develop a security plan for the transport of data on the microwave system that at a minimum follows the Homeland Security recommended standards and enforces Virtual Private Network, authentication and encryption at agency interfaces to ensure end-to-end data integrity over the microwave system.
- **Staff Roles and Responsibilities -** Identify roles and responsibilities for staff and align security policies and access requirements for normal and emergency situations**.**
- **Physical Security** - Implement a policy for protection against the access of equipment and system interfaces. Identify all connections to the microwave system and disconnect/disable unnecessary connections, ports and services. Secure equipment connections from unauthorized access.
- **Access Control** - Establish strong controls over public interfaces that could allow an intruder to bypass all other controls and have direct access to the network. Utilize access lists, proxy servers, flow control, call back schemes and other mechanisms to minimize risks from off network interfaces.
- **Vendor Equipment Security** - Test and implement the security features provided by equipment vendors and do not rely on default settings and proprietary protocols.
- **Configuration Management** - Protect the privacy of the information being carried on the microwave system by implementing policies and procedures to prevent attacks.
- **Location for Security Appliances** - Establish location for security appliances and documentation, and implement firewalls, access control lists and intrusion detection and prevention systems.
- **Intrusion Detection** - Implement automated intrusion detection and prevention systems.
- **Audits** - Perform routine audits of devices and connected networks, and identify security concerns.
- **Training** - Conduct staff training to minimize the inadvertent disclosure of sensitive information.
- **Service Level Agreements** - Incorporate security policies into the Service Level Agreement's with the client agencies.
- **Client Data**[4] - Identify network security standards applicable to the transport of client data and define network security requirements that will ensure end-to-end integrity. Client agencies must ensure Virtual Private Network authentication and encryption requirements are met as well as implement firewalls and virus protection on their network connections.

[4] Refer to NIST Recommended Security Controls or Federal Information Systems and Organizations Sections 2.5, 3.1, 3.2, 3.3 and 3.4 and ITU Security in Telecommunications and Information Technology Sections 1, 2 and 3.

Issues and risks associated with security are:

- Homeland Security and NIST classify microwave radio as a wireless access connection. Although microwave signals are inherently safe, anyone with the appropriate technology can intercept it, violating the fundamental principles of information security.
- The system design must be complete to identify how the network operates before the design of the security system can begin.
- PSCO cannot control the threats and vulnerabilities inherent to the client agency networks. Considerable effort will be required to implement the necessary security for the client agency networks. Refer to the CLETS Policies, Practices and Procedures for guidelines in this area.
- Physical security and direct access to network components is the greatest risk to network security. The biggest challenge will be the physical security of CAPSNET sites that are not owned or managed by PSCO; including, but not limited to: fences, card key access and video surveillance.
- Remote access into the Network Management System opens the potential for cyber attacks on the microwave system. Virtual Private Network connection with log-in authentication should be used to control access to the Network Management System.
- New procedures and countermeasures are needed to address network and physical attacks on the system. Sources for incident response assistance must be identified and established.

SECTION 6 - SYSTEM IMPLEMENTATION

System Implementation includes planning, site engineering and installation, commissioning and cutover to the new IP/MPLS-capable equipment, and overhead functions such as project management, logistics and procurement to support the design and field activities. The final step of system implementation is to decommission and remove the existing equipment.

The CAPSNET upgrade is a multiyear deployment requiring the replacement of existing microwave equipment at 329 sites (about 8% of these sites have already been upgraded with IP/MPLS-capable radios). This section provides a list of major activities and tasks, and defines the timeline and methodology for completing the project in stages, which will allow for progressive migration of existing traffic from the existing infrastructure to the new IP/MPLS platform.

Successful implementation of the CAPSNET upgrade project will require flexibility in the planning, coordination and execution efforts to accommodate evolving conditions and client agency needs. The scale and reach of the CAPSNET project demands a significant commitment of resources and coordination with all client agencies. Funding and resources must be planned and available to meet the timeline for the staged implementation, both for PSCO activities and the facility modifications. The following tasks are core activities needed to provide a cost effective and timely implementation, and to address the evolving needs of the project and the client agencies.

Create a Project Team

A project team should be developed that is structured to address the specific needs of large-scale projects. The roles and responsibilities of the team members must correspond to the needs of the project and do not necessarily reflect the position held by an individual in the organization. The following things should be accomplished for the development of the project team:

- Assign a project manager to manage the project, and to provide direction and coordination.
- Assign support staff to address procurement, logistics, scheduling and material coordination.
- Assign staff to perform quality control of engineering and installation activities to ensure conformity, improve efficiency and minimize mistakes and project delays.
- Assign a facility preparation team lead to coordinate and facilitate the site upgrade activities.

Site Engineering

Site engineering identifies the site specific needs and defines the physical and technical requirements to install and test equipment. This includes antenna mounting, rack installation and cabling, power and circuit installation requirements. The primary tasks are:

- Identify requirements, specify materials and prepare installation instructions for the new antenna systems using the path design data.
- Identify requirements, specify materials and prepare installation instructions for the new radio and network equipment and cables.
- Identify requirements, specify materials and prepare installation instructions for network components, channel termination modules and network monitoring interfaces.

- Identify requirements, specify equipment and prepare installation instructions for new or upgraded DC power systems to support the additional load for new equipment.
- Prepare instructions for the PSCO Microwave Lab to assemble, configure and test the radio and network equipment per the system design and IP plans developed during system design.
- Analyze and prepare instructions to migrate existing circuits to the new equipment.
- Collaborate with installation and quality control teams to refine installation drawings and instructions as needed to improve efficiency of the deployment efforts.

Issues, dependencies and risks related to site engineering are:

- System implementation depends on completion of the system design. An incomplete system design will limit the ability to identify facility issues that need to be expedited.
- Site engineering activities rely heavily on accurate documentation. Inaccurate documentation creates inefficiencies, by contributing to errors in planning the work, incorrect or missing parts being provided, and additional effort by field personnel to install the equipment.
- Need to develop internal standards for routers, switches, servers or other network equipment.
- Quality control and specification compliance for microwave products is performed by technicians in the Microwave Lab. The capability of the Microwave Lab must be expanded to address traffic simulation, stress testing and performance verification for new services and network interfaces.
- Some sites do not have the required infrastructure for the new equipment required for the system upgrade. These sites must be upgraded before the new equipment can be installed. Upgrading these sites frequently requires several years after funding source is identified.

Procurement of Equipment and Parts

The timely supply and availability of materials as they are needed to perform the work is critical in maintaining project costs, resource allocations and schedules. Major equipment items should be forecasted and procured in advance and miscellaneous materials should be acquired through the standard requisition process, as needed. Following are the primary support tasks:

- Purchase the equipment and materials specified by engineering.
- Forecast and purchase adequate inventory to support project needs. Create installation material kits that are commonly needed for a standard installation, to simplify parts ordering and tracking.
- Expedite purchases identified by installation teams.
- Track the progress of purchases and provide status reports with delivery schedules.

Issues, dependencies and risks related with the procurement of equipment and parts are:

- Purchases must be planned well in advance. Material shortages and the inability to expedite parts will delay deployment efforts.
- The requirement to procure parts on a per site/path basis increases labor and coordination costs as opposed to bulk purchases and deliveries.
- Procurement contracts for tower analysis and modification work are dependent on defining the scope of work and are considered to be long-lead-time items.

Installation

Installation activities include delivery, mounting and cabling of new equipment and antenna systems, and the commissioning of the new equipment. Installation activities are defined by the engineering team and dependent on facility preparation work performed by site owners, including tower, vault and power modifications. The installation work is based on a phased deployment, which focuses on completing geographic segments of the system. The primary tasks for installation include:

- Empower quality control staff to ensure safety on the job site, inspect installation workmanship and to ensure that as-built documentation and test records are accurate.
- Install new antenna systems, including mounts, antennas, waveguide and grounding per the path design documents and installation instructions.
- Test new antenna systems including return loss, path alignment and pressurization. Document any radio frequency (RF) interference and identify any conditions that could affect path performance.
- Install new radios and IP/MPLS equipment.
- Install network connections, alarm/control/monitoring connections, power cables and grounding per the network design documents and the installation instructions.
- Install new DC power plants and interface the alarm and control functions to the local alarm RTU.
- Commission new per the installation instructions.
- Coordinate the software download of final router and switch configurations from the Network Operations Center, verify the configurations and coordinate testing with the Network Operations Center.
- Document IP addresses and configurations for all network components.
- Document audio levels and radio signaling and control interfaces to land mobile radios.
- Test and document alarm reporting, network management and remote control operation of the new equipment and facility.

Issues, dependencies and risks related to field installation are:

- Install crews must be supplemented with staff from the local shops to meet schedule goals.
- Inaccurate documentation and instructions create delays and increase cost.
- Facility modifications necessary to support the new equipment must be completed prior to antenna and equipment installation.
- New processes, procedures and documentation must be developed to commission, troubleshoot and maintain the IP/MPLS Network.
- Quality Control for engineering and installation is crucial when introducing new methodology.
- Documentation and test reports are necessary to benchmark new installations.
- New and additional test equipment is necessary to support commissioning, cut-over and maintenance of the IP/MPLS network components.
- Establishing the new Network Operations Center and operations structure in the initial stage of the project is necessary for commissioning, cut-over and monitoring of the new system.
- The integration and testing of facility alarms and controls may uncover additional maintenance and/or repair requirements for the environmental control and back-up power systems.

Migration, Cutover and Removal

Migration and cutover involves the transition of existing client agency services to the new equipment, and includes coordination/notifications, physical cabling, installation and test services. Also included in the migration and cutover process is the removal of old equipment. This includes antenna systems, DC power systems, microwave radios, multiplex, channel termination equipment and miscellaneous wire, cable and materials associated with the analog and digital-time division multiplex systems that are being replaced by the new IP/MPLS equipment. The primary tasks for migration, cutover and removal include:

- Prepare a cutover plan to transition existing circuits to the new system and provide all required notifications prior to transferring circuits to the new system.
- Execute the migration, cutover and removal tasks to minimize down-time of existing systems and to ensure end-to-end operation during the cut-over process.
- Verify that the new system operates end-to-end, including the performance of system tests and circuit verification.
- Decommission existing radio, multiplex and DC Power equipment. Remove existing antennas, mounts, waveguide and miscellaneous attachment hardware from the tower.

Issues, dependencies and risks associated with the migration, cutover and removal of equipment are:

- Downtime of existing microwave systems may be necessary during installation to make room on towers for new antennas and during cutover while circuit terminations are transferred. This may result in downtime of client agency land mobile radio systems if an alternate path is not available during cutover.
- End-to-end circuit continuity and testing is necessary to confirm proper operation prior to transferring the existing traffic to the new system.
- Coordination and notification of each affected agency is necessary prior to cutover. Emergency requirements may limit or postpone cutover.
- Equipment removal is a major activity and requires significant attention and resources to accomplish efficiently. Equipment removal minimizes structural loading of the tower, vault space and reduces the drain on power and environmental systems.

The Implementation Plan

The goal for the CAPSNET upgrade project is to migrate from the existing analog and legacy time division multiplex system to an IP/MPLS network as quickly as possible. PSCO has begun the system implementation work, with the replacement of existing radios with dual-mode radios capable of operating as time division multiplex or IP/MPLS.

To develop the implementation plan, the microwave system was broken down into geographic segments or stages, as shown in Figure 3 and described below. The stages were prioritized to maximize the benefit to the client agencies by focusing on core areas and key connecting routes first. The staged approach will provide the flexibility needed to accelerate the implementation as additional funding and/or staff are available to work on the project. The time it takes to complete the project will be based on staffing and funding that PSCO can allocate for engineering and installation activities.

Figure 3. Implementation Stages

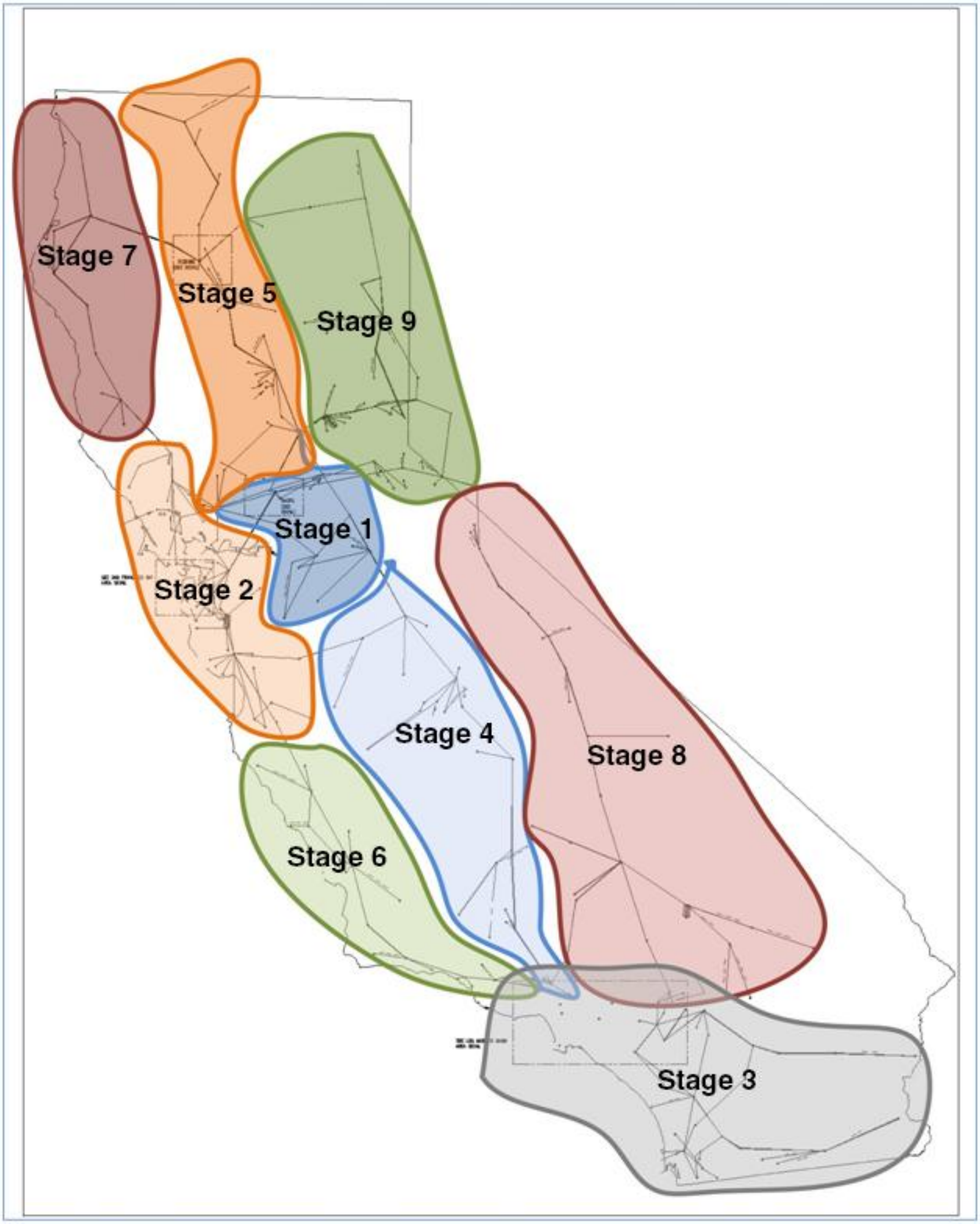
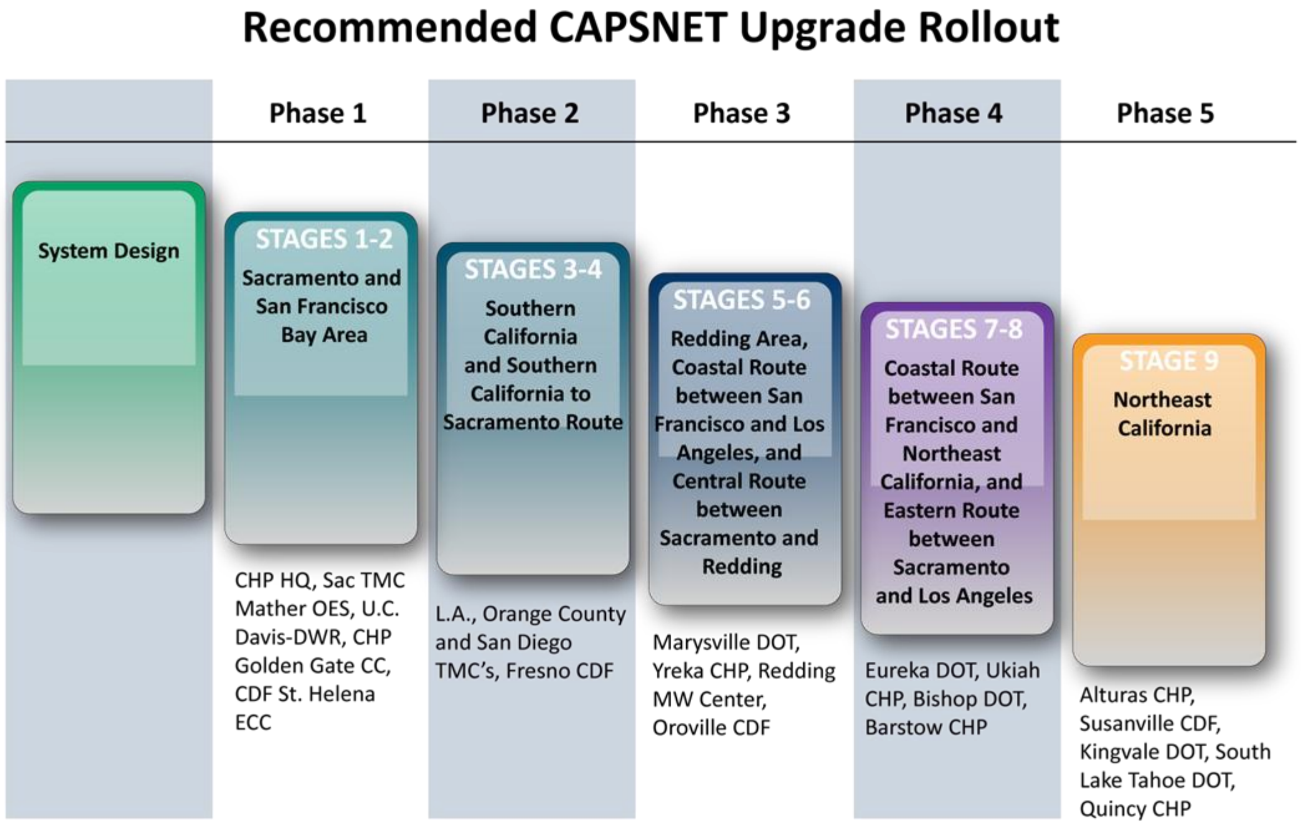


Figure 4. Phased Implementation Plan


Recommended CAPSNET Upgrade Rollout
Phase 1
Phase 2
Phase 3
Phase 4
Phase 5
System Design
STAGES 1-2
Sacramento and San Francisco Bay Area
CHP HQ, Sac TMC Mather OES, U.C. Davis-DWR, CHP Golden Gate CC, CDF St. Helena ECC
STAGES 3-4
Southern California and Southern California to Sacramento Route
L.A., Orange County and San Diego TMC's, Fresno CDF
STAGES 5-6
Redding Area, Coastal Route between San Francisco and Los Angeles, and Central Route between Sacramento and Redding
Marysville DOT, Yreka CHP, Redding MW Center, Oroville CDF
STAGES 7-8
Coastal Route between San Francisco and Northeast California, and Eastern Route between Sacramento and Los Angeles
Eureka DOT, Ukiah CHP, Bishop DOT, Barstow CHP
STAGE 9
Northeast California
Alturas CHP, Susanville CDF, Kingvale DOT, South Lake Tahoe DOT, Quincy CHP

Benefits

Each of the nine stages can be completed in approximately one year at current PSCO staffing and funding levels. The schedule can be accelerated with additional funding and staff, which has some distinct advantages. A shorter implementation schedule will provide quicker access to the client agencies for the rollout of new IP-based applications in core areas and will provide new capabilities for PSCO to monitor and troubleshoot the network through the network management system at the Network Operations Center. A longer implementation schedule will delay access to these benefits, and if it takes too long poses the risk that the system may approach technology obsolescence by the time the project is completed.

Staging the implementation as described above will allow PSCO to rollout the IP/MPLS technology in the Sacramento area first, which will allow the engineers and technicians to gain some practical experience on a smaller scale to provide lessons learned that can be used for the remaining stages. Client agency applications can also be rolled out on a trial basis to work out potential migration issues prior to full rollout.

Implementation Stages

Following is a brief description of each implementation stage and some of the client agency sites associated with each:

- **Stage 1** includes the Sacramento area and portions of connecting routes from the Central Route to the Coastal and Eastern Routes.
- **Stage 2** includes the San Francisco Bay Area with connections to Sacramento and the Central Route between Sacramento and Los Angeles, which will provide an alternate route between Northern and Southern California.
- **Stage 3** includes the Southern California area and connecting routes to the Los Angeles area and the Central and Eastern routes.
- **Stage 4** includes the segment of the Central Route connecting Sacramento to Los Angeles.
- **Stage 5** includes the Redding area and the segment of the Central Route connecting Sacramento and Redding.
- **Stage 6** includes the Coastal Route between the San Francisco Bay Area and Los Angeles, and connectivity between the Coastal and Central routes.
- **Stage 7** includes the Coastal route between the San Francisco Bay Area and the Northwest Area, and a connecting route between the Coastal Route and the Central Route at Redding.
- **Stage 8** includes the Eastern Route between the Sacramento area and the Los Angeles area. Although this is a lightly loaded route, it will provide a redundant route on the backbone between Northern and Southern California.
- **Stage 9** includes the northeast segment of the Eastern Route with connections to the Central Route at Redding and Sacramento. Although this is a lightly loaded route, it will provide a redundant route on the backbone between Sacramento and Northern California**.**

Recommended Implementation

The recommended implementation utilizes a phased approach, with each phase taking approximately one year to complete at current staffing and funding levels. The first four phases will include two stages each, with the final stage completed in Phase 5. The stages are described above and shown in Figure 3, and Figure 4 shows each phase, the areas that will be upgraded for that phase and some of the key client agency sites in that phase. There are other client agency sites that are currently not connected to the microwave backbone that are not shown in Figure 4, but will be near one of the upgraded areas or routes, and could have access to the new IP/MPLS technology/connectivity with the installation of a new microwave hops from their facilities to the nearest microwave site, such as the California Department of Corrections and Rehabilitation (CDCR) prisons.

SECTION 7 - NETWORK OPERATIONS CENTER

The main function of a Network Operations Center (NOC) is to identify issues that can negatively impact the productivity and health of the network before they occur. The NOC is a critical component in the deployment of the new IP/MPLS equipment and will serve as the central point for controlling facility access, security, equipment elements and client agency traffic. Primary and secondary NOC facilities will provide improved response to outages by extending full diagnostic, control and configuration to 24 x7 manned facilities. This allows for network problems to be identified and/or resolved remotely, with technicians dispatched to the field only as needed to address known issues. For these reasons, it is imperative that the NOC be operational at the beginning of the project.

The following tasks should be completed to implement the NOC for the new IP/MPLS network:

- Define the functions, roles, responsibilities and skill sets of NOC staff.
- Design the NOC configuration and security processes.
- Gather Information and set initial objectives for NOC locations.
- Select primary and backup NOC locations and specify tenant improvements necessary for staff, equipment, documentation and security enforcement.
- Obtain approval and funding for selected site(s).
- Construct NOC facilities and install tools, equipment, security and office facilities.
- Recruit and train staff.

Industry Best Practices

Following are industry best practices associated with Network Operations Centers[5]:

Tools

The essential tools for a NOC are:

- A ticketing system to keep track of open issues.
- Trained staff in IP/MPLS technologies.
- A knowledge base for all knowledge and documentation that is accessible to the entire team.
- Reporting and measurements to show major incidents and root cause for every resolved incident.
- Infrastructure Monitoring.
- Process Automation.

[5] Some of the information in this section was obtained from Ayehu; Network Operations Center Best Practices, by Gabby Nizri; April 2012.

NOC Staff

The NOC should be staffed with both engineers and technicians that are responsible for sustaining the network, maintaining network performance at a high level and network optimization. They will also be vital in deploying new links, replacing equipment, and commissioning and testing, and should be highly trained in radio, IP transport, MPLS and security.

Following are industry accepted roles for the NOC:

- **NOC Manager -** responsible for the supervision and coordination of the activities of all NOC staff to provide sustained services, network surveillance, service and performance restoration, and to ensure quality of experience for all end users.
- **NOC Section Manager -** prioritizes tasks, assigns work and verifies that tickets are opened properly and relevant personnel are notified.
- **NOC Engineers** - manage the network and assists technicians with troubleshooting and interpreting test results.
- **NOC Project Managers** - manage and sustain the existing system, and proactively project system expansion needs.
- **NOC Technicians -** monitor events, report anomalies and are the first line of response to incidents and outages.

Processes

The operational processes that should be implemented are:

- Monitor and report events.
- Create trouble tickets for incident remediation and resolution.
- Escalation of issues in a well-defined manner.
- Establish a process for prioritizing incidents, based on importance and impact.
- Incident handling, including: solution development, escalation to appropriate personnel, and notification of users affected.
- Develop temporary solutions for complex problems that may take longer than usual to resolve.

SECTION 8 - FACILITY PREPARATION

Many CAPSNET radio sites require tower and/or radio vault upgrades to support the new microwave equipment being installed. Facility readiness requires a long lead time for funding, architectural and engineering services, and outside contract services. Early identification and execution of contracts to prepare the facilities is critical to completing the system upgrade on time.

The majority of the radio sites are owned by other State agencies that are responsible for funding and performing the upgrade work. Facility preparation is a multi-year program that is currently in process. For the timelines presented in this Roadmap, it is assumed that facility preparation will be aligned with the CAPSNET schedule objectives.

Facility preparation work is in progress and is being monitored and coordinated by PSCO to fit into the implementation schedule; however, facility preparation presents a serious risk to the project schedule. PSCO should continue to proactively monitor the work and may need to adjust the implementation plan and schedule periodically due to delays in site preparation. Monitoring the work closely will also allow PSCO to identify and address risks as soon as possible to minimize the impact to project budget and schedule.