



**RCN System Engineering Analysis Report**



**Regional Community Network (RCN)  
System Engineering Analysis  
for  
Phase I – Deployment Area**

Prepared by:



**Kimley-Horn  
and Associates, Inc.**



**MARICOPA  
ASSOCIATION of  
GOVERNMENTS**

REVISED Dec. 04, 2006  
091025018.4.400



# RCN System Engineering Analysis Report

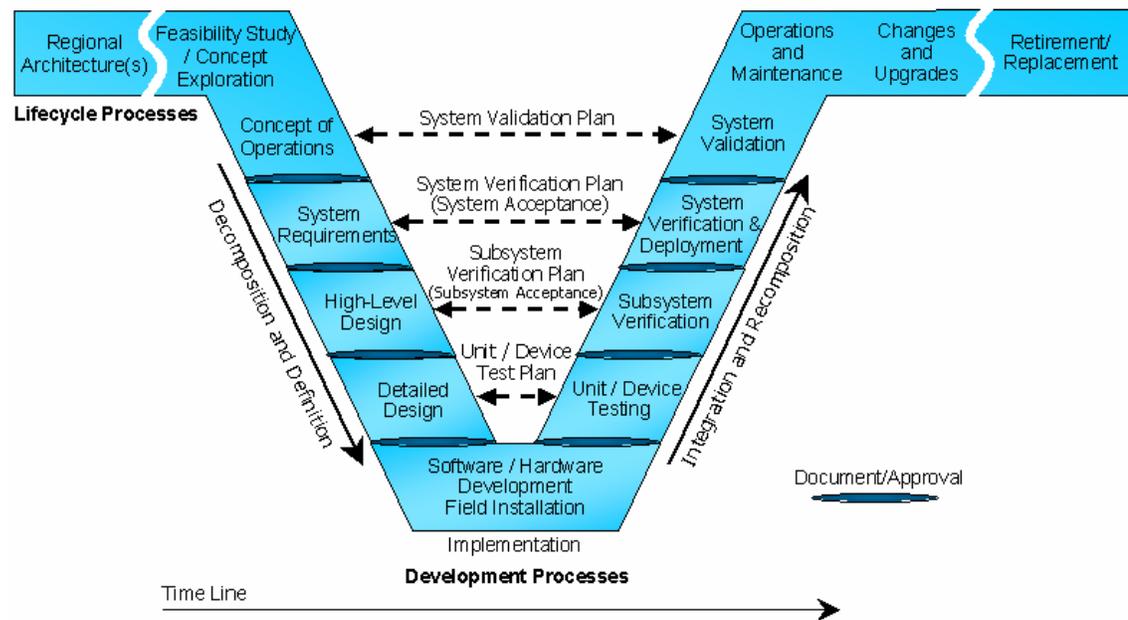
## TABLE OF CONTENTS

<b>EXECUTIVE SUMMARY .....</b>	<b>1</b>
Introduction.....	1
RCN Project Background .....	1
<b>1. INTERFACING WITH THE REGIONAL ITS ARCHITECTURE.....</b>	<b>3</b>
1.1 ITS Applications Supported .....	4
1.2 Project Goals and Objectives.....	5
<b>2. CONCEPT EXPLORATION / FEASIBILITY STUDY .....</b>	<b>6</b>
2.1 Technical Feasibility .....	6
2.2 Financial Feasibility.....	8
2.3 Institutional Feasibility.....	9
<b>3. CONCEPT OF OPERATIONS .....</b>	<b>10</b>
3.1 MAG RCN Study: .....	10
3.2 AZTech™ Telecommunications Overview Report .....	12
3.3 Proof of Concept Test .....	12
3.4 RCN Initial Deployment Concept of Operations .....	14
<b>4. SYSTEM REQUIREMENTS DEFINITION.....</b>	<b>15</b>
4.1 RCN High-Level Requirements.....	15
4.2 Regional Hub Facility Selection Considerations .....	16
4.3 Network Bandwidth Requirements .....	19
4.4 Flexible Interconnection Requirement .....	19
4.5 Network Security Requirements .....	21
4.6 Network Reliability Requirements.....	24
4.7 Other RCN Requirements .....	25
<b>5. SYSTEM DESIGN.....</b>	<b>26</b>
5.1 High-Level Design.....	26
5.2 Metropolitan Hub Connectivity High-Level Design for Initial Deployment: .....	29
5.3 Detailed Design .....	30
<b>6. SYSTEM IMPLEMENTATION.....</b>	<b>30</b>
6.1 Conduit and Fiber Optic Cable System Deployment.....	30
6.2 Active Electronic System Equipment Deployment.....	30
<b>7. SYSTEM TEST AND VERIFICATION .....</b>	<b>30</b>
7.1 Integration and Testing .....	31
7.2 Subsystem Verification .....	31
7.3 System Validation.....	31
<b>8. SYSTEM OPERATIONS &amp; MAINTENANCE.....</b>	<b>31</b>
<b>9. SYSTEM UPDATE, RETIREMENT AND REPLACEMENT .....</b>	<b>32</b>

## EXECUTIVE SUMMARY

### Introduction

A systems engineering analysis is required for all federally-funded Intelligent Transportation Systems (ITS) projects using Federal funds according to the Final Rule on ITS Architecture and Standards Conformity (CFR940) issued on January 8, 2001. This report describes how the Regional Community Network (RCN) Phase 1A project meets this Federal requirement by following the *Interim Guidelines for Systems Engineering Analysis* developed by MAG and the Federal Highway Administration (FHWA) in August 2006. **Figure 1** below shows the process followed in the Systems Engineering Analysis. The analysis utilized relevant products from a number of past ITS and telecommunications planning projects in the Phoenix metropolitan region.



**Figure 1: System Engineering Analysis “V” Diagram**

### RCN Project Background

The links required for effective ITS communications between ten local agencies were identified and temporarily funded in 1998 as part of the AZTech™ Model Deployment Initiative (MDI), a project that was funded in part by an FHWA grant. This was a national demonstration project that involved ten local agencies, Arizona DOT and several private sector partners under the AZTech™ banner. In the 2001 MAG ITS Strategic Plan, AZTech™ was redefined to include all MAG member agencies.



## RCN System Engineering Analysis Report

The *MAG ITS Strategic Plan Update (2001)* included *Technical Memorandum No.5* on the *MAG Regional ITS Architecture*. Section 5.3 (Recommended Future MAG ITS Physical Architecture) of the MAG Regional ITS Architecture states:

“Technical Memorandum No.7 – ITS Telecommunications Plan, will describe in greater detail the types of communications infrastructure that must be deployed in order to achieve the MAG regional architecture vision.”

The *MAG ITS Strategic Plan Update (2001)* also outlined a path of migration from leased lines to a regional fiber optic network. *Technical Memorandum No.7 – ITS Telecommunications Plan* was developed to explore the concept of how the various agencies were going to interconnect their communications infrastructures into a common communications infrastructure to achieve network connectivity between partnering agencies. In Section 3 – ITS Telecommunications Needs of *Technical Memorandum No.7 – ITS Telecommunications Plan* it states:

“The ultimate goal of the communications infrastructure is to have all agencies interconnected via the regional fiber optic network with both data and multiple video communications channels.”

In 2001, the MAG Telecommunications Advisory Group (MAGTAG) and MAG Intelligent Transportation System (ITS) committees began the RCN study which ultimately identified the Concept of Operations for the RCN that would be used by the various public sector agencies to:

- Increase the bandwidth capacity of public sector telecommunications links;
- Increase the reliability of public sector telecommunications links;
- Increase information sharing capabilities across jurisdictional boundaries; and
- Enhance the level of service that public sector agencies provide to the communities they serve.

In 2002, the Arizona Department of Public Safety (DPS), the Arizona Department of Transportation (ADOT), and the City of Phoenix (COP) conducted a proof of concept test to demonstrate possibilities of combining various public agencies resources to solve their network capacity and path diversity problems. This *Joint User Interoperability Communication Enterprise (JUICE) Proof of Concept* test demonstrated that the recommendation in the MAG RCN Study to build a regional network was a viable solution to solving some of the region’s telecommunication problems. By working together and integrating existing and future network infrastructure investments, the various agencies within the region can more efficiently increase their overall bandwidth capacity, network reliability, and the level of service.

In 2003, Maricopa County developed an *AZTech™ Telecommunications Overview* report documenting the immediate need for the region to start establishing center-to-center fiber optic communications links between the various traffic operations centers and between public safety agencies to sustain and enhance the region’s ability to mitigate the impacts of traffic congestion.

In 2004, AZTech™ partners adopted the RCN concept recommended by MAGTAG and MAG ITS committees, and secured federal funding through the AZTech™/Maricopa County Department of Transportation (MCDOT) Public Safety – Transportation Interoperability Grant to develop a Design Concept Report (DCR) for the Phase 1A (initial deployment phase) of the RCN.

In 2005, AZTech™ partners developed a DCR for Phase II (East Valley Deployment) of the RCN. Also in 2005, \$1.6M in federal funds previously programmed for a MAG project to implement the original MAG RCN concept was made available for implementation of the RCN to support ITS communications. MAG and ADOT agreed to utilize these funds to implement RCN Phase 1A (when federal funds become available) as a MAG project implemented by ADOT.

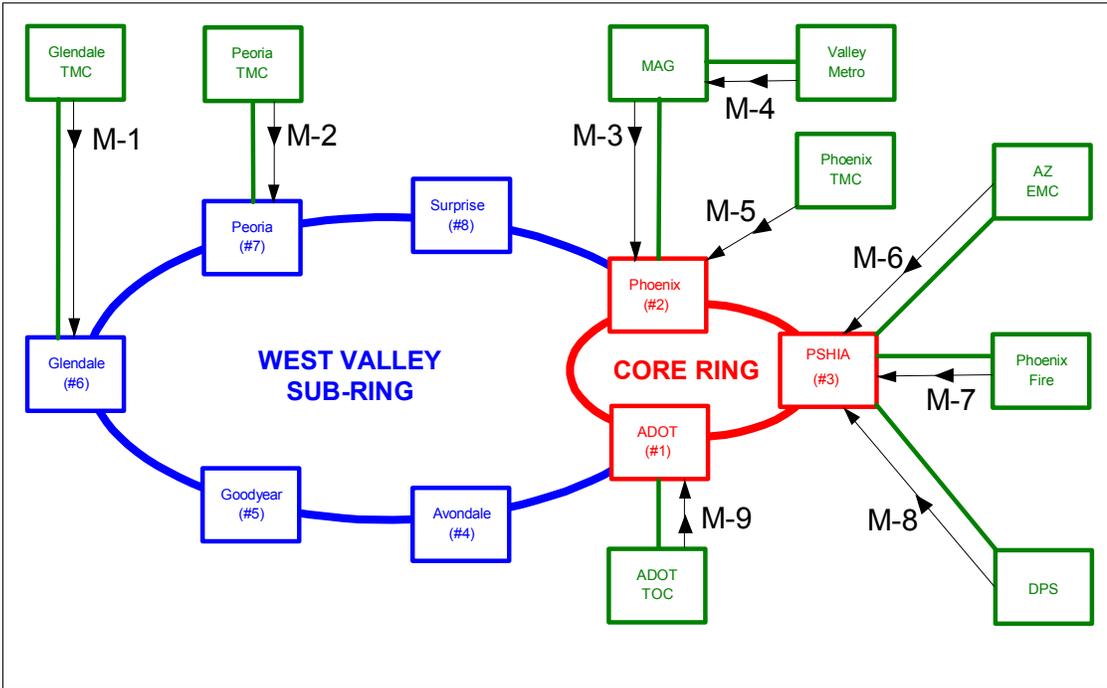
In 2006, ADOT developed the Plans, Specifications, and Estimates (PS&E) for the construction documents for Phase 1A of the RCN.

## 1. INTERFACING WITH THE REGIONAL ITS ARCHITECTURE

In 20001, the Maricopa Association of Governments developed the *MAG ITS Strategic Plan Update* report which included the Technical Memorandum No.5 on the MAG Regional ITS Architecture. In Section 5.3 (Recommended Future MAG ITS Physical Architecture) of the MAG Regional ITS Architecture states:

“Technical Memorandum No.7 – ITS Telecommunications Plan, will describe in greater detail the types of communications infrastructure that must be deployed in order to achieve the MAG regional architecture vision.”

All Regional ITS Architectures are dependent on establishing a communications infrastructure to achieve center-to-center and center-to-field communications between agencies systems and to the ITS field devices. The RCN Phase 1 network establishes the connections depicted in the following diagram:



**Figure 2: RCN Phase 1 Connectivity**



RCN Phase 1A establishes the following links in the above diagram:

- The Core Ring (3 Regional Hubs)
- Partial West Ring with the Glendale Regional Hub
- Six Metropolitan Hubs: ADOT Traffic Operations Center (TOC), Glendale Traffic Management Center (TMC), Phoenix Public Transit (Valley Metro and Metro Rail), Phoenix TMC, Peoria TMC, and MAG

All of the Metropolitan Hub locations identified in the diagram above (with the exception of the MAG facility) are key agency locations for regional transportation applications, as identified on Figure 6-1 of the *MAG ITS Strategic Plan Update Final Report*. RCN Phase 1A will provide connectivity to Agency Locations ID# 1, 8, 20, 19, and 16 (as identified in the MAG ITS Strategic Plan Update Final Report).

### 1.1 ITS Applications Supported

As the regional ITS communications network, RCN will be built to support regional ITS applications. The following tables provide a summary the specific agency needs of participating agencies (that are documented in the *MAG ITS Strategic Plan Update*) that are supported through the RCN Phase 1A project:

Applications	User Services (Strat. Plan pg 13)	User needs (Strat. Plan pg 14)	Market Packages (Strat Plan pg 18)
CCTV	1.1 Pre-trip Travel Information 1.6 Traffic Control 1.7 Incident Management 2.4 Public Travel Security	2,5,6,8,16,23	ATIS1 ATMS1,ATMS3,ATMS4,ATMS7 ATMS3,ATMS4 APTS5
TI Signals	1.6 Traffic Control 7.1 Archived Data Function	1,2,4,16,17	ATMS3,ATMS7 AD2
DMS	1.7 Incident Management	6,7,8,16	ATMS3,ATMS4
Rental Car Center Display	1.1 Pre-trip Travel Information 1.5 Traveler Services Information	6,49	ATIS1, ATIS2 ATMS5
Regional Video Conf.		10	

Subsystems (Strat Plan pg 24)	
Centers	ADOT TMC, Glendale TMC, Peoria TMC, Phoenix TMC, Phx Transit, Phoenix Sky Harbor, MAG, ADOT Vision Field Office
Roadside	none
Traveler	Sky Harbor
Vehicle	none

The AZTech™ Center-to-Center (C2C) project is addressing the deployment of ITS application needs. The primary regional need that is being addressed by the RCN is the need for a high



## RCN System Engineering Analysis Report

bandwidth communications networks between the TMCs and other locations where Advanced Traveler Information Systems (ATIS) will be deployed to collect and disseminate the traveler information (i.e., the Phoenix Sky Harbor Airport Rental Car Center [RCC]).

The stakeholders involved in the *Joint User Interoperability Communication Enterprise (JUICE) Proof of Concept* identified the following applications that can benefit from this technology and interagency collaboration:

- Alternate paths in the event of common carrier failure. The participating JUICE stakeholders can use a regional telecommunications network as an alternate to leased services or as a back-up telecommunications path during a failure in the private sector infrastructure.
- Enable criminal justice integration of data through law enforcement agency interconnection. Increased coordination through secured links with increased bandwidth to improve and promote data sharing.
- Enable continuity and disaster recovery processes between agencies. Investment in local resources for disaster recovery is preferable to contracts with third-party vendors that require annual funding of renewal fees and testing at remote sites.
- Enhance video and data transmission of freeway traffic status to state and local law enforcement agencies as well as expanding the capacity and reliability of regional ITS communications between the various traffic management centers within the Phoenix metropolitan area.
- Reduce cost and/or improve the reliability of common carrier services. The analog voice lines, data lines, and Internet connection services currently being leased at each agency could be combined into larger circuits through a regional telecommunications network. This will give public sector agencies the ability to leverage their collective buying power and obtain significantly better leased service rates for connection to the Internet. In addition, public sector agencies could obtain these leased services from different parts of the region simultaneously using one or more service providers and/or central office to enhance the reliability of their telecommunications systems.
- Support regional videoconferencing connectivity to help reduce traffic congestion on the roadways and make more efficient use of public sector employees' time.
- Enhance day-to-day data communications between metropolitan agencies and improve e-government and e-commerce services to the community.

### 1.2 Project Goals and Objectives

The goals and objectives for this project have been divided into two basic categories. The first category of goals identified below (Section 1.2.1) is focused on what needs to be accomplished within the overall RCN program over the next 20 years for all public sector agencies in the Phoenix metropolitan area. The second category of objectives defined in section 1.2.2 is more specific to what needs to be accomplished during this initial deployment phase 1A of the RCN network.

#### 1.2.1 RCN Program Goals

The following goals have been established in the *Design Concept Report, Phase 1 – Initial Deployment Area*:



## RCN System Engineering Analysis Report

- Enhance the region's traffic congestion mitigation efforts by expanding the real-time video and data sharing capabilities among public sector agencies in the region;
- Enhance the region's homeland security efforts by providing the telecommunications infrastructure needed to interconnect the various public safety agencies and transportation agencies within the region;
- Provide a more reliable and secure telecommunications infrastructure that builds upon the existing public agency infrastructure investments within the region for all public sector agencies to use;
- Provide an open telecommunications architecture that can be efficiently expanded in geographic coverage area and in information carrying capacity;
- Enhance intra-agency telecommunications to help improve the level of service that the public sector agencies provide to the communities they serve; and

### 1.2.2 RCN Initial Deployment Objectives

In addition to the overall RCN program goals identified above, ADOT has identified the following specific objectives for this initial Phase 1A deployment of the RCN (*ADOT Regional Communications Network Design Concept Report, Phase 1 – Initial Deployment Area, November 2004*):

- Establish the center core ring of the overall RCN three ring topology;
- Provide the primary fiber optic infrastructure needed for West Valley ring;
- Provide West Valley cities the opportunity to get fiber connectivity to the ADOT TOC for AZTech™;
- Support future ADOT Freeway Management System (FMS) phases along Loop 101 on the west side; and
- Eliminate ADOT's biggest fiber bottleneck at the I-10 and I-17 interchange.

## 2. CONCEPT EXPLORATION / FEASIBILITY STUDY

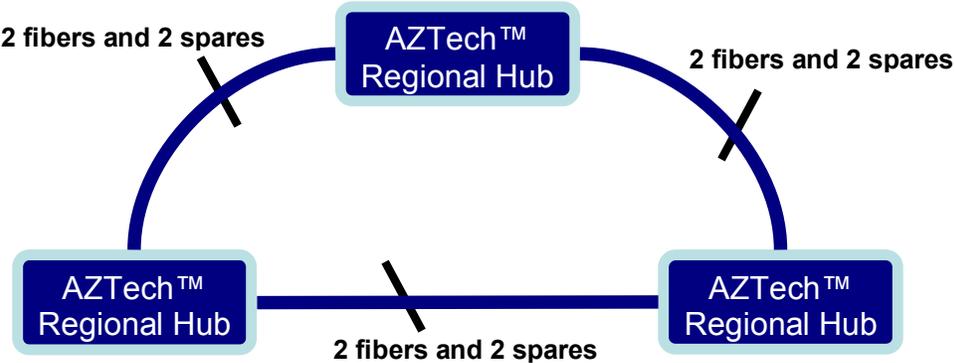
### 2.1 Technical Feasibility

The *JUICE Proof of Concept* project provided proof of Technical Feasibility for the RCN. The following technical objectives were successfully demonstrated, as part of the *JUICE Proof of Concept*:

- Bridge the existing infrastructures of the four participating agencies without the need for any additional conduit and fiber optic cable infrastructure, with the exception of a few new fiber patch cords within each facility;
- Expand the capacity and reliability of an existing fiber optic link without affecting the operation and performance of the link's existing applications;
- Tunnel through an existing IP network in a secure manner; and
- Ultimately achieve path diversity and increased capacity to complement an existing leased communication link that currently has limited capacity and is a single point of failure in one of the agencies networks.

Since the available funds for RCN Phase 1A project are to be focused on providing communications network links to improve transportation information collection and dissemination, the active electronics being purchased with RCN Phase 1A project funds are focused on the expansion of the AZTech™ Transportation Network by establishing a multi-gigabit Ethernet backbone for transportation related communications. Therefore the expense of deploying the Dense Wave Division Multiplexing (DWDM) and Synchronous Optical Network (SONET) active electronic equipment to support other types of public sector closed networks (i.e., police, courts, and education type networks) will be deferred to a later phase of the overall RCN project.

In keeping with the future expandability concept of allowing other public sector networks to share the same fiber optic communications paths that will be installed in RCN Phase 1A, the RCN Phase 1A design incorporates a fiber path route and diversity strategy that will allow future DWDM and SONET equipment technologies to be added to the network configuration without disrupting the design intent and service availability of the initial RCN Phase 1A AZTech™ network links. This design strategy is described below:



**Figure 3: RCN Phase 1A Connectivity Logic**

The RCN Phase 1A project will provide the fiber optic cable paths needed to traverse across jurisdictional boundaries between each of the regional hub locations. At these regional hub locations the blue “AZTech™ Regional Hub” Ethernet network switches shown above will be installed to establish multi-gig Ethernet paths between agencies for the expansion of the regional AZTech™ Transportation Network.

At some point in the future, when other agency departments (i.e., IT, courts, education, etc.) want to expand their closed networks using the RCN fibers, they will need to install the remaining RCN Regional Hub active electronic components (see the orange components in **Figure 4**) to realize the full potential of the RCN vision, as established in the *MAG RCN Feasibility Study*.

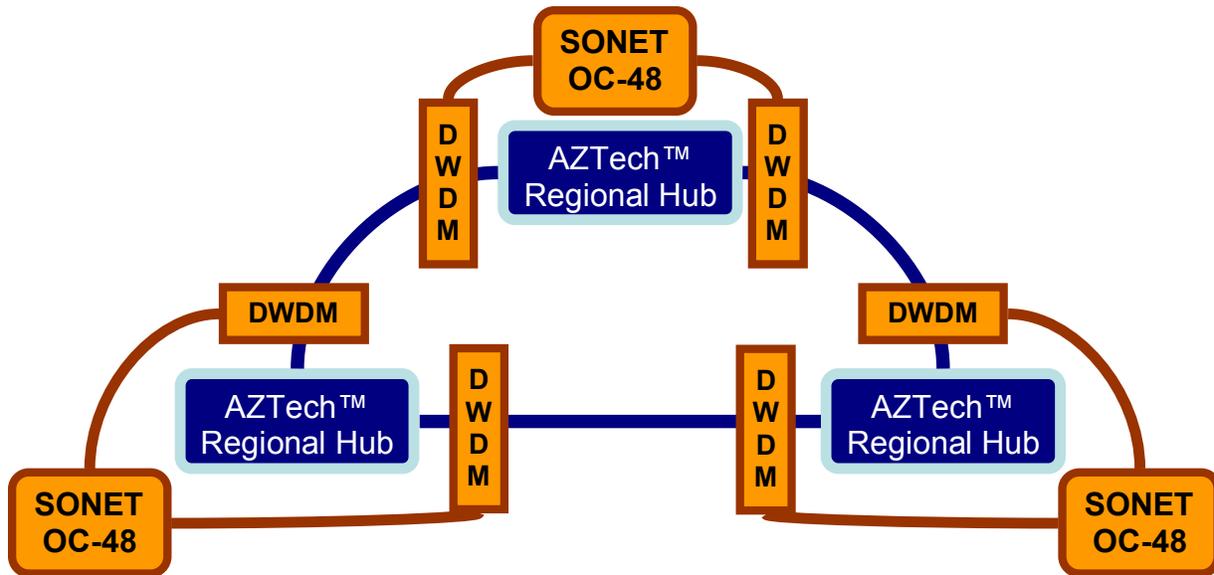


Figure 4: Future RCN Connectivity Logic

## 2.2 Financial Feasibility

Two related Design Concept Reports (DCR) have been completed (one for the west valley and one for the east valley). The cost estimate for RCN Phase 1 (the west valley) is \$10.6M. The cost estimate for RCN Phase 1A (a portion of the West Valley) is \$1.6M. The cost estimate for the East Valley RCN is \$5.3M.

The available funds for RCN Phase 1A equate to \$1.6M of MAG funds that will be transferred over to ADOT to implement the Phase 1A project, and \$100k of ADOT funds to get the ADOT VISION office connected. There are no funds programmed at this time to implement the rest of the RCN segments.

If the complete RCN is not built within the next ten years, there is still significant value that will be realized in Phase 1A by making the following connections:

- The Core Ring (3 Regional Hubs);
- Partial West Ring with the Glendale Regional Hub; and
- Six Metropolitan Hubs: ADOT TOC, Glendale TMC, Phoenix Public Transit, Phoenix TMC, Peoria TMC, and MAG.

The value received from making these connections is not dependent on other phase of the RCN. However, as additional agencies are connected in future phases, the value of the initial deployment phase will grow.

Through discussions with the AZTech™ Operations Committee and Executive Committee, it was agreed that the RCN project would not dictate what leased lines an agency would disconnect when the RCN infrastructure is in place. This decision of removing existing leased lines is a decision that each agency will have to make on their own. Some agencies may want to



## RCN System Engineering Analysis Report

keep the leased lines as another level of back-up communications and other agencies may decide to rely solely on the RCN for some of their communications links. All RCN segments are considered new segments in terms of increasing bandwidth capacity and adding communications redundancy.

### 2.3 Institutional Feasibility

The *Joint User Interoperability Communication Enterprise (JUICE) Proof of Concept* report states that the following institutional feasibility objectives were successfully demonstrated:

- a) The various public sector stakeholders demonstrated their willingness and ability to work together in identifying key links within each agency's infrastructure that can be shared for the common good.
- b) The various public sector stakeholders demonstrated how current network technology can be used to expand the bandwidth capacity within key communication links without jeopardizing the owner's original intent for the existing communication link.
- c) The various public sector stakeholders demonstrated how multiple agencies can share the same fiber paths and still maintain physically separate networks.
- d) The various public sector stakeholders demonstrated how multiple agencies can co-exist and share the pools of bandwidth available within each agency's IP networks without compromising their network security standards.
- e) The various public sector stakeholders demonstrated how they can improve network reliability by combining the network resources of multiple agencies to increase path diversity.
- f) The various public sector stakeholders demonstrated how the amount of available bandwidth for each agency can be increased by combining the network resources of multiple agencies.
- g) The various public sector stakeholders demonstrated their willingness to share equipment mounting space and power resources within each of their facilities to support network equipment installed for another agency.
- h) The various public sector stakeholders demonstrated their willingness to work together to address the O&M and security procedures that are needed in sharing network resources.

The AZTech™ Operations and AZTech™ Executive Committee meetings were the main forum for reaching consensus and agreements among the regional partners during the RCN Phase 1 Design Concept Report (DCR) and Design phase of the project. The ADOT project team has also provided a few project update presentations to the MAG ITS and MAGTAG committees. The agencies that had new RCN Outside Plant (OSP) infrastructure called for within their jurisdiction and/or the RCN was using existing OSP infrastructure were given the RCN plans and spec submittals for review at the various stages of design completion. The ADOT project team has also met with each of the jurisdictions that will be getting new Inside Plant (ISP) infrastructure through the RCN project. In summary, the ADOT project team has conducted a large amount of regional meetings and one-on-one meetings with each of these jurisdictions during the planning and design phases of the RCN Phase 1 project.



## RCN System Engineering Analysis Report

The member agencies that will be receiving RCN infrastructure as part of the RCN initial deployment phase have agreed that they will become the owners of the infrastructure that resides within their jurisdiction. It will be the responsibility of each participating agency to operate and maintain the infrastructure within their jurisdictional boundaries, as defined within JPA #0356 (between ADOT and the City of Phoenix), #0616 (between ADOT and the City of Glendale), and #0617 (between ADOT and the City of Peoria).

As the RCN grows in geographical area and in the number of partnering agencies connected, the MAG ITS and MAGTAG committees will take the lead in developing a more comprehensive RCN expansion and operations and maintenance (O&M) plan at some point in the future. In the near future, the MAG ITS Committee will discuss the formation of an RCN Working Group comprised of member representatives from the MAG ITS and MAGTAG committees. The RCN Working Group will be charged with providing guidance and policies on future RCN planning, design, deployment, and operations/maintenance phases of the RCN program.

### 3. CONCEPT OF OPERATIONS

#### 3.1 MAG RCN Study:

The *MAG RCN Study* established the Concept of Operations for a Phoenix metropolitan area regional telecommunications network that would be used for interconnecting governmental facilities and improving telecommunications service availability in the public sector agency communities.

The *MAG RCN Study* recognized that some government agencies in the region have made significant strides forward in planning for and building telecommunications infrastructure. These agencies that have built their own telecommunications infrastructure have annual operating and maintenance costs that are lower than leasing costs would be for the same infrastructure. Even so, the higher capital cost of installing telecommunications infrastructure has forced agencies to use leased telecommunications links for most of the public sector locations needing connectivity. This reliance on private companies, although less expensive in the short term, can become more costly in the long term. The *MAG RCN Study* recommended that its agencies use a balanced funding approach so that a portion of the available resources would be used to install infrastructure, and the remainder of available funds could be applied to leased lines to help fill gaps in the agencies' infrastructure while being sensitive to budget constraints.

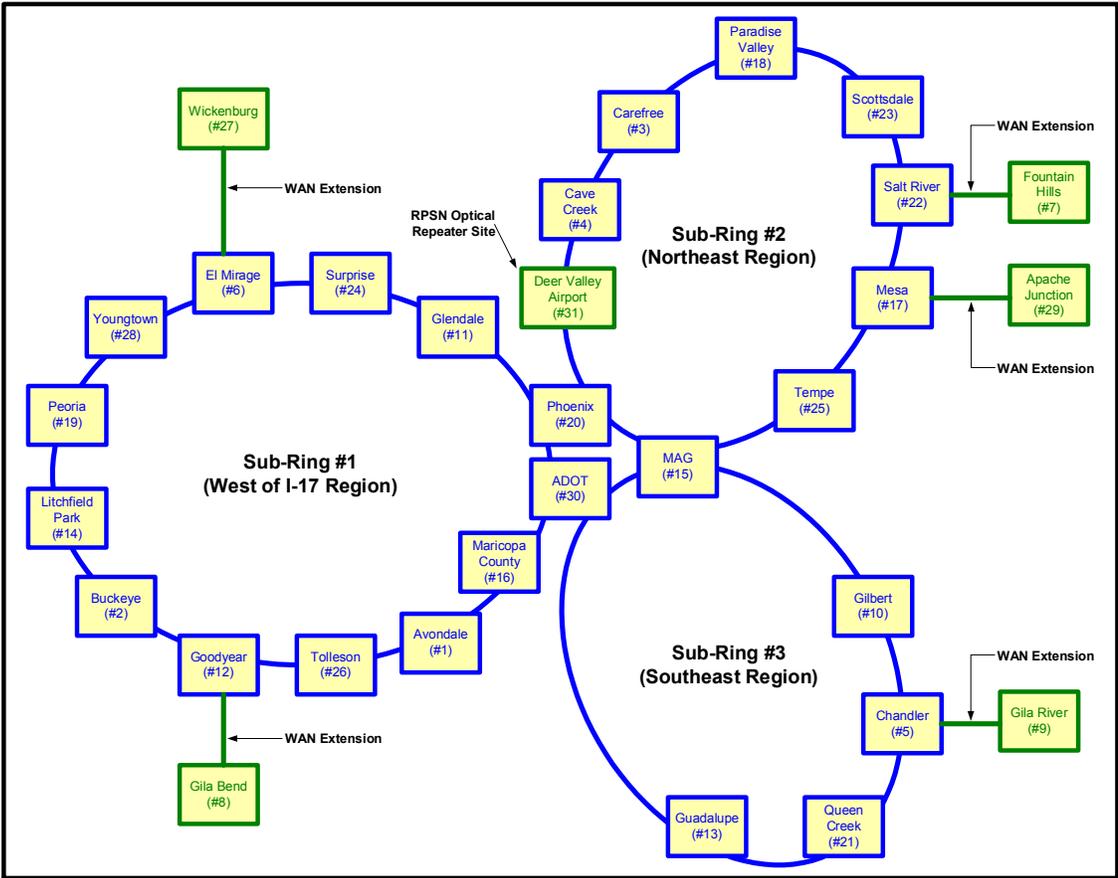
The *MAG RCN Study* also recognized that some of the infrastructure needed by the public sector agencies may span across two or more jurisdictional boundaries. In such a case, it was recommended that the public sector agencies coordinate with each other to identify existing and planned infrastructure within each of the jurisdictions and work together to identify solutions for sharing these infrastructure resources and the associated deployment costs.

The *MAG RCN Study* evaluated various architectures and recommended a three-tier network architecture comprised of three tiers of hub locations: regional hubs, metropolitan hubs, and local hubs. The regional hubs are intended to provide the interagency connectivity needed to cross jurisdictional boundaries; the metropolitan hubs are intended to provide the intra-agency

connectivity needed within each jurisdiction; and the local hubs are intended to provide the intra-agency connectivity needed within each agency department.

The MAG RCN Study recommended the regional telecommunications network be divided into three sub-rings, as shown in **Figure 5**, which will provide regional hub connectivity to the following three sub-regions:

- West of I-17;
- East of I-17 and North of I-10/Loop 202; and
- East of I-17 and South of I-10/Loop 202.



**Figure 5: Recommended Regional Hub Connections**

The *MAG RCN Study* indicated that the first and second tiers (local area network [LAN] and metropolitan area network [MAN], respectively) can use any media (i.e., copper, fiber, airwaves, etc.); however, the *MAG RCN Study* recommended that the third tier (regional hubs) be primarily comprised of fiber optic rings with DWDM equipment that supports SONET and Gigabit Ethernet channels.



## RCN System Engineering Analysis Report

### 3.2 AZTech™ Telecommunications Overview Report

AZTech™ is a voluntary association of local agencies within the Phoenix metropolitan area in Maricopa County, Arizona. The objectives of the AZTech™ program are to:

- Integrate the existing ITS infrastructure into a regional system;
- Establish a regional integrated travel information system; and
- Expand the transportation management system for the Phoenix metropolitan area.

The actions of the program have been categorized under the following five strategies:

- Establish education and outreach programs;
- Expand and strengthen partnerships;
- Optimize regional operations and management;
- Plan, develop, and deploy integrated regional systems; and
- Research and test new technological opportunities.

Telecommunications between agencies is a fundamental component of these objectives and strategies. For example, without complete telecommunications links between traffic management centers, there cannot be a regional integrated travel information system. Likewise, the optimization of regional operations depends on the efficient transmission of video and data from one agency to another.

The *AZTech™ Telecommunications Overview* report updated the documentation of the existing network performed in the *MAG ITS Strategic Plan Update* and identified specific gaps in the migration from leased lines. The *AZTech™ Telecommunications Overview* report also includes recommendations for:

- Maintaining the current level of communication between AZTech™ partners; and
- Fulfilling the goals expressed in the *MAG ITS Strategic Plan Update* regarding regional ITS operations and interconnectivity.

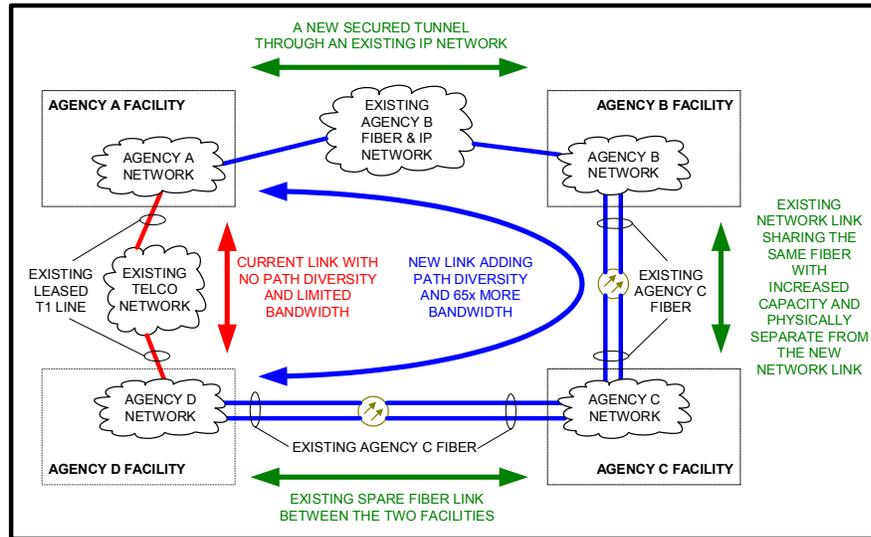
### 3.3 Proof of Concept Test

Representatives from DPS, ADOT, and the City of Phoenix explored the possibility of combining resources to solve their network capacity and path diversity problems. With the help of Nortel Networks (a network solutions provider) and Kimley-Horn and Associates, Inc. (a telecommunications consulting firm) the group identified several opportunities to increase bandwidth and path diversity while reducing or maintaining current operating expenditures. To demonstrate that these opportunities were viable solutions that did not compromise the security and network capacities these existing networks currently support, the stakeholder agencies decided to perform a proof of concept test called the Joint User Interoperability Communication Enterprise (JUICE).

The network configuration used in the JUICE Proof of Concept was a combination of various types of telecommunication media that were pulled together to form a single cohesive network which multiple agencies could share. As depicted in **Figure 6**, the network started with an existing leased T1 line that currently provides network connectivity between two public sector agencies (agencies A and D). This existing leased network link only provides 1.5 Mbps of bandwidth and is critical to the operations of these agencies; therefore, the JUICE Proof of

## RCN System Engineering Analysis Report

Concept test focused on adding a second telecommunications path that provided the added reliability of path diversity needed for the existing link and increased the bandwidth between agencies A and D by more than 65 times.



**Figure 6: JUICE Proof of Concept Network Configuration**

The second telecommunications path (shown in blue) was added using three different segments (shown in green) of existing public sector infrastructure owned by two other agencies. The first segment (starting at the top and working clockwise) was an existing Internet Protocol (IP) based wide area network owned and operated by agency B. To make use of this existing connectivity between agencies A and B, it was critical that a secured path be established that did not compromise the integrity of the information being transferred and stored in each agencies' networks; therefore, network equipment was added that offered firewall protection and Virtual Private Network (VPN) tunnel capabilities with data encryption.

The second public sector owned infrastructure segment that was used for the connection between agencies B and C was an existing single-mode fiber path. This existing path between agency B and C only had four fibers, and two of these fibers were currently being used for regional transportation functions. Although the JUICE Proof of Concept could have just used the other two fibers for the connection, all four fibers were desired to demonstrate the added reliability that a folded ring topology would offer between agencies B and C. It was decided that WDM network equipment would be added to maintain the operational performance of the regional transportation network link, achieve the security of physical separation between the JUICE test path and regional transportation network link, and occupy all four fibers for the folded ring topology. By adding the WDM equipment in the segment, the proof of concept for the JUICE test was enhanced to demonstrate that multiple public sector agencies could share the same fibers without affecting existing network equipment investments; achieve the security benefits of physical separation by using separate optical wavelengths; and significantly increase the bandwidth, reliability, and availability of an existing fiber path that was previously dedicated to serving only a single function.



## RCN System Engineering Analysis Report

The third public sector owned infrastructure segment that was used for the connection between agencies C and D was an existing single-mode fiber path with available fibers that were currently not being used. By making use of these dark fibers, the JUICE stakeholders were able to achieve the final connection needed for a complete network path between agencies A and D without any significant investments in new conduit and fiber infrastructure.

### 3.4 RCN Initial Deployment Concept of Operations

#### 3.4.1 RCN Working Group

The operational aspects of the RCN Phase 1A will be as defined in the JPAs and as defined within the Center-to-Center Systems Operational Guidelines. As the RCN grows in geographical area and partnering agencies connected, regional forums such as the MAG ITS and MAGTAG committees will take the lead in developing new operational policies and procedures, as they pertain to the changing dynamics of the RCN and the types of intra-departmental networks that begin to use the RCN infrastructure in the years to come. In the near future, discussions will begin at MAG for the formation of an RCN Working Group comprised of member representatives from the MAG ITS and MAGTAG committees. The RCN Working Group will be charged with providing guidance and policies for future RCN planning, design, deployment, and operations/maintenance phases of the RCN program.

#### 3.4.2 Center-to-Center Systems Operational Guidelines

As part of the on going efforts to expand the functionality and geographic coverage area of the various types of regional transportation systems, the region has adopted the following guidelines:

- Regional Center-To-Center Video Feed & Camera Control Guidelines
- Regional Center-To-Center Dynamic Message Sign Guidelines
- Regional Center-To-Center Traffic Management Systems Guidelines

Since the initial deployment phase of the RCN communications infrastructure is intended to support these systems, the RCN Working Group will also need to follow the guidelines, as appropriate, while developing the RCN program policies and procedures for future deployment phases of the RCN.



## RCN System Engineering Analysis Report

### 4. SYSTEM REQUIREMENTS DEFINITION

#### 4.1 RCN High-Level Requirements

The high-level requirements identified for the RCN are shown in the following table:

Requirement	Description
<b>Network Bandwidth</b>	RCN architectures will be evaluated for the capability to support intra-agency, interagency, and community service needs with at least 50% initial bandwidth growth capacity.
<b>Flexible Interconnection</b>	RCN architectures will be evaluated for the ability to support users with diverse needs. This will be based upon the availability of multiple types of interfaces of varying bandwidths.
<b>Video, Voice and Data Telecommunications Standards/Interfaces Support</b>	RCN architectures will be evaluated based upon the ability to support voice, video, and data/Ethernet telecommunications natively (or what level of complexity is required to add support).
<b>Tier 1 Architecture (LAN)</b>	RCN architectures will be evaluated based upon the capability to interconnect an agency's buildings that are within ½ mile of each other.
<b>Tier 2 Architecture (MAN)</b>	RCN architectures will be evaluated based upon the capability to interconnect an agency's buildings that are within five miles of each other or within an area that covers the entire city.
<b>Tier 3 Architecture (WAN)</b>	RCN architectures will be evaluated based upon the capability to interconnect public sector buildings within the entire region using RCN telecommunications hubs to bridge the agency's MANs onto the RCN for interagency connectivity.
<b>Network Security</b>	RCN architectures will be evaluated for the ability to provide physical network separation and logical network separation.
<b>Network Reliability</b>	RCN architectures will be evaluated for the ability to provide path diversity and protection from single points of failure.
<b>Scalability/Expandability</b>	RCN architectures will be evaluated for the ability to scale from Tier 1 to Tier 2 and from Tier 2 to Tier 3. Additionally, architectures will be evaluated for the ability to expand system capacity with minimal infrastructure replacement.



## RCN System Engineering Analysis Report

Requirement	Description
<b>Maintainability</b>	RCN architectures will be evaluated based upon the ability to obtain replacement parts; level of staff sophistication necessary to support the technology; and the ease of replacing equipment with newer equipment.
<b>Cutting Edge</b>	RCN architectures will be evaluated based upon the availability of vendors supporting technologies/features, which indicates the strength of support for current and pending industry standards/technologies.
<b>Interoperability</b>	RCN architectures will be evaluated based upon the availability of independent interoperability tests or standards that provide proof of vendor interoperability claims.
<b>Availability</b>	RCN architectures will be evaluated based upon the ease of which network architectures/leased-services can be acquired and deployed.
<b>Cost</b>	RCN architectures will be compared against one another over a 10-year and 20-year life cycle cost.

### 4.2 Regional Hub Facility Selection Considerations

An analysis was performed to identify the key factors that needed to be considered when selecting a facility that would function as a regional hub. The key regional hub selection considerations are as follows:

**4.2.1 Ability to efficiently achieve interconnectivity to existing video, voice, and data networks**

Because the main function of a regional hub facility is to achieve interconnectivity across jurisdictional boundaries for the various metropolitan and local area networks operating in the region, it is highly recommended that each agency identify a regional hub facility location that is in close proximity to its networks that require the largest bandwidth. In doing so, each agency will ultimately reduce the overall expenses associated with leasing services and/or providing high capacity infrastructure equipment to interconnect metropolitan and local hubs that are located in other facilities within the agency’s jurisdiction.

**4.2.2 Ability to provide 24/7 accessibility for third-party maintenance personnel**

All regional hubs will ultimately require access (escorted or non-escorted) by maintenance personnel who are employees of other agencies or third-party companies hired to maintain one or more of the various network links to which the regional hub will be connected. For



## RCN System Engineering Analysis Report

example, it is highly probable that third-party maintenance personnel will be responsible for operating, maintaining, and/or warranting some of the regional hub DWDM electronics and/or fiber optic infrastructure. These companies will need to have immediate access to the equipment for any trouble-shooting and repair activities that may be required on a moment's notice. In addition to the accessibility needs for maintaining the regional backbone infrastructure, other neighboring agencies with facilities that are within five or more miles of a different agency's regional facility will require access to the regional hub facility for design, construction, and/or maintenance activities in support of their RCN connectivity needs.

### *4.2.3 Ability to provide secured access*

There will ultimately be a variety of networks with various levels of security requirements that will require connectivity into the RCN at each regional hub location and/or passing through one or more regional hubs to obtain connectivity to a different regional hub location on the RCN backbone. All facilities that house regional hub equipment are required to ensure that access to the equipment housed within the regional hub area is in conformance with the most restrictive accessibility requirements of all networks riding the RCN backbone. Because these accessibility requirements will change over time as additional network links are added to the RCN and/or the accessibility requirements of a particular network link changes in the future, each agency hosting a regional hub is expected to accommodate (not necessarily fund) future changes to accessibility requirements of the regional hub equipment. To accommodate the security needs of the agencies that are expected to ride the RCN backbone in the early phases of deployment, each regional hub facility will require, at a minimum, conformance with the Arizona Criminal Justice Information System (ACJIS) security policy prior to the installation of the DWDM regional node equipment.

### *4.2.4 Ability to provide physical space to house new equipment*

To accommodate the DWDM regional node equipment and support the various uplink electronics required for RCN connectivity to the many metropolitan and local hubs within the geographical coverage area of each regional hub facility, an agency hosting regional hub space should initially provide floor space to accommodate a minimum of two new equipment racks (if equipment is going to be placed in an existing secured computer room) or provide a separate, secured room (12'x15' ideally) for regional hub equipment. If physical demands for the regional hub and uplink equipment space grow beyond what was originally planned for in the initial deployment phases, each agency hosting a regional hub facility is expected to accommodate (not necessarily fund) future changes to increase the amount of physical space available to support the additional RCN equipment space needs.

### *4.2.5 Ability to provide the environmental control requirements of the RCN equipment*

To support future (beyond initial deployment) installations of the DWDM RCN regional hub equipment, each agency hosting a regional hub facility will be required to accommodate (not necessarily fund) the following environmental control requirements of



## RCN System Engineering Analysis Report

the RCN equipment (Note that these requirements are based on the recommendations in the 2003 *BiCSi® TDM Manual, 10<sup>th</sup> edition*):

- Maintain continuous and dedicated environmental control (24 hours per day, 365 days per year) of the room housing the RCN regional hub and uplink equipment. If emergency power is available, consider connecting it to the HVAC system that serves the room housing the RCN regional hub and uplink equipment;
- Maintain positive pressure with a minimum of one air change per hour for the room housing the RCN regional hub and uplink equipment; and
- Maintain a temperature range of 64°F to 75°F and a humidity range of 30% to 55% relative humidity. When sizing Heating Ventilation and Air Conditioning (HVAC) equipment for the room, calculations should account for dissipating the heat generated by active devices and provide a minimum of 300 ft<sup>3</sup> of 54°F conditioned air per 20 ampere (A) dedicated electrical outlet.

#### 4.2.6 Ability to provide a FM-200 or “dry pipe” fire protection system loop

Each agency hosting a regional hub facility will be required to accommodate (not necessarily fund) fire protection for the room housing the RCN regional hub and uplink equipment in accordance with the local codes using a FM-200 or “dry pipe” fire protection system, prior to the deployment of RCN regional hub DWDM equipment. This requirement of the equipment room is necessary to protect the regional stakeholder investments in RCN active electronic equipment from any leakage that could occur from wet pipe systems.

#### 4.2.7 Ability to support a minimum floor loading of 50 lbf/ft<sup>2</sup>

Provide a minimum floor loading of 50 lbf/ft<sup>2</sup> for the room housing the RCN regional hub and uplink equipment. (Note that this requirement is based on the ANSI/TIA/EIA-569-B, Commercial Building Standard for Telecommunications Pathways and Spaces.)

#### 4.2.8 Ability to support additional primary power and back-up power loads

To support future (beyond initial deployment) installations of the DWDM RCN regional hub equipment, each agency hosting a regional hub facility will be required to accommodate (not necessarily fund) the following power requirements of the RCN equipment (Note that these requirements are based on the recommendations in the 2003 *BiCSi® TDM Manual, 10<sup>th</sup> edition*):

- Additional branch circuits for equipment power, protected and cabled for 20A capacity;
- A minimum of two dedicated non-switched 3-conductor 120 volt (V) alternating current (ac) duplex electrical outlets for equipment power, each on separate non-switched branch circuits from dedicated power panels (if practical) serving only the active telecommunications/computer equipment in the room and no lighting fixtures, to avoid inadvertent loss of RCN equipment power;
- Separate duplex 120 Vac convenience electrical outlets (for maintenance activities) located at least six inches (in) above finished floor (AFF), and placed at six-foot intervals around perimeter walls;



## RCN System Engineering Analysis Report

- Emergency power (uninterrupted power supply [UPS], generator, and/or separate grids from SRP/APS) with automatic switchover capability; and
- Coordinated light switch locations for easy access upon room entry.

### 4.2.9 Ability to support at least two separate conduit entrances into the facility

All regional hub facilities will need to accommodate at least two separate conduit entrances (separated by a minimum 12 feet) into the facility. If a prospective initial phase regional hub facility location currently cannot support this requirement, the agency hosting the regional hub facility will need to coordinate with the initial deployment phase RCN designers to facilitate additional conduit entrances as part of the initial deployment phase construction activities.

## 4.3 Network Bandwidth Requirements

Before the public sector agencies can make significant strides in promoting and implementing the identified telecommunications application needs, a telecommunications infrastructure has to be in place that will support the bandwidth requirements of such widespread deployment of these applications. Currently, the majority of the telecommunications links at each jurisdiction cannot support these added bandwidth demands. Furthermore, the number of links needed between each of the agencies is very small when compared to the number of links and/or amount of bandwidth needed. The additional bandwidth capacity and connectivity that would be provided to the agencies through the RCN would be required to support the widespread deployment of ITS and traffic signal systems applications needs.

The intra-agency and inter-agency telecommunications components needed to support ITS and traffic signal systems will have a large impact on the bandwidth requirements of the RCN. This is a result of the time-sensitivity and network separation level requirements for data telecommunications to roadside field devices, as well as the high bandwidth required to carry the video images from the closed-circuit television (CCTV) cameras to and between the agencies' traffic management centers. Most of the agencies' ITS and traffic signal networks are considered separate networks from the agencies' IT networks. Separation is necessary to ensure network integrity for time-critical applications and security in order to prevent outside users from compromising the performance of the transportation field devices. The bandwidth requirements of the CCTV video application is approximately five times that of the average videoconferencing video signal of 384 kbps; the speed and number of moving pixels in the digital image make it more difficult to compress while maintaining a real-time quality image.

In addition to the bandwidth impacts that these telecommunications application needs will have on the RCN, network security, reliability, and future growth variables also need to be considered when determining the needed bandwidth of each intra-agency, inter-agency, and community network link. Although the bandwidth for these additional variables is sometimes difficult to predict at the planning stage, they typically account for at least 50% of the total required bandwidth capacity.

## 4.4 Flexible Interconnection Requirement

The most opportune way to promote shared infrastructure investments and ensure acceptance and usage of the RCN is to provide convenient and flexible options for agencies to join the



## RCN System Engineering Analysis Report

effort. The first key provision for satisfying this requirement is to use standard industry interfaces that are readily available. The second key provision for this requirement is establishing a three-tier architecture (LAN/MAN/WAN) and allow agencies to choose the appropriate level of interconnection to meet their needs.

The three tiers that are needed to support flexible interconnection are Tier 1 – LAN, Tier 2 – MAN, and Tier 3 – WAN. At the LAN level, agencies would be able to interconnect field devices and nearby branch offices without expensive multiplexing equipment. Tier 1 users of this nature would likely not need to share voice, data or video with other agencies. At the Tier 2 MAN level, agencies will generally have multiple office locations over a wider area that also encompasses more bandwidth. Tier 2 users would utilize slightly more sophisticated equipment to interconnect locations using shared media and/or regional backbone equipment. Finally, at the Tier 3 level, inter-agency telecommunications is established by interconnecting MANs from participating agencies that have video, voice, and data to share. Tier 3 equipment will likely be the most costly and is not necessarily required at each office location within each agency. Tier 3 equipment should at least be in two locations for each agency in order to minimize single-points of failure.

The following points require consideration when evaluating the flexibility level of RCN infrastructure components:

- Support video, voice and data telecommunications standards/interfaces such as Motion Picture Entertainment Group (MPEG), Ethernet, time-division multiplexed T-1/T-3, and analog Plain Old Telephone Service (POTS). If the network requires complex conversion equipment to support these interfaces, it will be less likely to be used by the participating agencies.
- Provide telecommunications media/technology options that enable a tiered architecture. Some agency locations might only want to extend their LANs to other branch offices, while others desire to videoconference and share data with one or more agencies. The RCN telecommunications media and technologies need to allow for flexible options. For example, using spare dark fiber for extending a LAN in lieu of expensive Wave Division Multiplexing (WDM)/Switching equipment. Likewise, wireless and leased-line options should allow for disparities between larger and smaller network users.
- Offer tiered architecture options:
  - Tier 1 – LAN: Interconnection of neighboring agency buildings within ½ mile of each other using dark fibers or wireless infrastructure.
  - Tier 2 – MAN: Interconnection of an agency's buildings within several city blocks of each other or within an area that covers the entire city using dark fibers or wireless infrastructure.
  - Tier 3 – WAN: Interconnection of public sector buildings within the entire region using RCN telecommunications hubs to bridge MANs onto the WAN for inter-agency connectivity.



## RCN System Engineering Analysis Report

### 4.5 Network Security Requirements

Various levels of network security are required in the RCN to support the diverse needs of the agencies. This section describes the basic levels of network separation that are required for the RCN. Physical separation of network traffic is described first and represents the highest level of security that can be achieved through the network. Logical separation of network traffic is presented next and it is the least secure approach to sharing network links. Finally, implementation of security policies and firewall end devices to provide security on shared links with no separation of traffic is presented. All three basic security approaches are recommended for the RCN; however, only physical and logical separations of network links will have a direct impact on the RCN infrastructure. It is the responsibility of each individual department within the agencies to decide which level of separation best fits their situation. If encryption and firewall end devices are necessary, then the agencies will need to connect these devices per their security policies prior to connecting to the RCN.

#### 4.5.1 Physical Separation of Networks

Physical separation of network traffic within the RCN will provide the highest level of security by making it physically impossible for someone on a different agency's network to "hack" into another agency's network. For example, two networks would be physically separate if they were on separate fibers in separate conduits using separate end equipment (and the end equipment is not interconnected). This would be the extreme case and is not recommended from a cost perspective.

With today's technology, physical separation can be achieved over the same fiber using technologies such as Time Division Multiplexing (TDM) and WDM. With these technologies, it is physically impossible for network traffic on one "time slice" or wavelength to "hack" into a different "time slice" or wavelength. The RCN can achieve this level of separation with existing fiber or wireless infrastructure owned by the agencies, and through some leased services offered by the telecommunications service providers.

The key to understanding whether or not the network has physical separation is knowing which specific technology is being used or offered. For example, North American Digital Signal standards like Digital Signal (DS) level DS-1 and DS-3 (commonly referred to as T-1 and T-3) and SONET standard links like Optical Carrier (OC) level OC-1, OC-12, OC-48 provide physical separation.

The network equipment technology needed to provide physical separation is typically more expensive, but has a reputation for being reliable. Leasing these types of services also is more expensive and can become cost prohibitive to many agencies or departments that have several remote users and require high security measures. By providing physical separation through the RCN for agencies with highly classified information, many of these agencies will be able to offer more expedient and protected data transmission to remote users than could be provided within existing budgetary limitations.

#### 4.5.2 Logical Separation of Networks

Logical separation is the most economical type of network separation that can be offered through the RCN, but a determined "hacker" on a shared network that is logically separate



## RCN System Engineering Analysis Report

can break into the network traffic path of other logically separate networks. The standards used to create logically separate networks, like Virtual Local Area Networks (VLAN) and Asynchronous Transfer Mode (ATM), were developed to better manage the traffic on a shared network link, to improve data flows, contain the traffic of broadcast messages, and keep the common user from accessing files that do not pertain to his/her working group. Although these standards that provide logical separation within a shared network are recommended for use within the RCN to help manage traffic and make more efficient use of the available bandwidth, they are not recommended as the only source of providing network security for users that require high security levels.

It is also important to keep in mind that Frame Relay service offered by telecommunications service providers fits into this logical separation of networks category. The industry commonly refers to “fractional T-1” when offering Frame Relay technology, and this type of service does not provide the high level of security that a standard T-1 (or DS-1) provides.

### 4.5.3 Security Policies and Firewalls

It is recommended that all agencies implement security policies and firewalls when connecting their networks to the RCN. The only exception to this rule is for those RCN links that provide physical separation of network traffic. It is recommended that the security policies to be followed when connecting to the RCN be decided and adopted by the individual agencies.

The security policies need to specify measures that will minimize intrusions from Internet links and from all data links that only provide logical separation of networks. Internet Protocol (IP) data activity is comprised of both routing and gateway functions, and can include access control list restrictions for additional security. This provides the first line of defense by establishing a policy for permitting only hypertext transfer protocol (HTTP) packets (web page information), file transfer protocol (FTP) packets (file transfer outgoing), and e-mail to pass through. A policy to restrict telnet, which allows remote users to login to a system, would be a good policy to enforce via a firewall. By excluding almost all content and then only including permissible applications, each agency can create a network architecture that is much easier to operate, manage, and troubleshoot. It also reduces the likelihood of attacks generated from other systems or users from remote locations that do not possess the same level of security for their internal network

Another policy to be enforced is the use of the VPN which uses encryption, authentication, and confidentiality measures that restrict outside users from reading information that is being sent across a shared network link. All Federal agencies, contractors of Federal agencies, and other organizations that process information using a computer or telecommunications system on behalf of the Federal government to accomplish a Federal function must use the Data Encryption Standard (DES) and the Triple Data Encryption Algorithm (TDEA, a.k.a. "Triple DES") to protect sensitive data. Within the DES, as published in October 1999, the Triple DES, as specified in ANSI X9.52, was recognized as a Federal Information Processing Standard Publication (FIPS PUB) approved algorithm and is the FIBS approved symmetric encryption algorithm of choice. Single DES is permitted for legacy systems only and all new encryption devices procured for Federal function need to use Triple DES products running in the single DES configuration when



## RCN System Engineering Analysis Report

interfacing with the legacy systems. Public sector agencies may want to consider these standards when creating their own encryption policies.

The SysAdmin, Audit, Networking and Security (SANS) Institute, in conjunction with the Federal Bureau of Investigation (FBI), also provide valuable resources regarding addressing security vulnerabilities. The SANS Institute has recently released a Top 20 list (<http://www.sans.org/top20.htm>) of Internet Security vulnerabilities. The security threats on this list worth particular consideration include:

- Default installations of applications and operating systems containing sample scripts and open access ports;
- Accounts with no passwords or weak passwords;
- Non-existent or incomplete backups;
- Large numbers of open access ports;
- Not filtering packets for correct incoming and outgoing addresses (Example filter: “Any packet coming into your network must not have a source address of your internal network.”);
- Non-existent or incomplete logging. Many security experts recommend sending logs to a central log server that writes the data to a write-once media (CD-R) so that a would-be attacker cannot alter the logs to avoid detection; and
- Vulnerable Common Gateway Interface (CGI) programs (sample CGI programs are pre-loaded on many web servers including Microsoft’s Internet Information Server [IIS]).

As public sector agencies connect to a RCN link that does not provide physical separation, it is recommended that they perform a thorough probe of the potential vulnerabilities that exist prior to connection and periodically conduct updates. The SANS Institute has a link to an automated network vulnerability scanner, which is available for download at <http://oval.mitre.org/>. This scanner is provided by Open Vulnerability Assessment Language (OVAL). The OVAL Board includes representatives from major operating systems vendors, commercial information security tool vendors, academia, government agencies, and research institutions.

Another important area of policy concern is maintaining updated virus scanning software and tools. Viruses such as Trojan and Nimbda can pass through a firewall unnoticed with other e-mail. If left un-checked, viruses can at a minimum be a nuisance, but often destroy or corrupt data before being mitigated. It is of equal importance to check outbound e-mail to prevent viruses from propagating through the network.

In addition to the above security measures, a firewall limits access to internal networks by determining which inside services (HTTP, FTP, email, etc.) are permitted access from the outside, and vice versa. A network firewall is a logical barrier, and is generally used in conjunction with routers, between separate internal networks, as well as between internal and external networks. Accessibility guidelines, coupled with firewall features, allow network administrators to control all inbound network activities down to the application, IP address, and/or the internal or external host server. IP Security (IPsec) protocol is a commonly used standard for providing encryption, authentication (public key and private key), and confidentiality.



## RCN System Engineering Analysis Report

An important feature provided by a firewall is network address translation (NAT). This feature translates the IP address of an internal network element to another IP address for communicating to the external network. An IP address can be seen as the network version of a telephone number. NAT prevents individuals outside the network from discerning the corresponding internal addresses, and in turn generating a full-scale attack on the internal network elements.

Another important feature of the firewall is logging activities, especially by time of day and by IP address. These features can detect when a pattern of usage develops, possibly indicating a break-in attempt. All communications with the host involved can be automatically or manually cut off. Some systems are even configured to send e-mail or dial a designated pager when these pre-defined conditions occur. The log might be able to be used as evidence in the prosecution of a suspected hacker.

Firewalls cannot protect against traffic that does not go through the firewall. If internal users are given unrestricted dial-up access to the Internet via the RCN, it would defeat the whole intent of the firewall. Therefore, it is extremely important that all traffic be routed through a firewall.

### 4.5.4 *Impacts of Network Security on Bandwidth*

If the RCN were not required to support physical and logical separation of networks for security reasons, and if all users of the network could share the available bandwidth (similar to the way the Internet is being used), then there would be no additional bandwidth impacts to the network. This is not the case for the RCN, and some level of separation between several of the network links will be required. The use of both logical and physical levels of network separation will ultimately result in network bandwidth that is reserved for specific links and cannot be shared by all users. This additional bandwidth impact that the required levels of separation will have on the RCN cannot be quantified to any degree of accuracy during the early planning stages of the network. The impact is largely dependent on specific links that may be requested by different regional public sector network users.

## 4.6 Network Reliability Requirements

Path diversity and equipment redundancy within the RCN are required to meet the reliability needs of the agencies. Security policies and network equipment built to meet reliability standards can have a significant impact on improving network reliability. However, path diversity and equipment redundancy to protect from single points of failure will provide the greatest improvement in system down time. Network equipment is expected to be down from time to time due to system problems or planned outages for network upgrade activities. The only way to make these inevitable occurrences invisible to the agencies is to have an alternate path for the network traffic to use while the outage is occurring.

### 4.6.1 *Path Diversity*

Path diversity is achieved when an additional telecommunications link is added to the network to provide an alternate path for network traffic to flow in the event of a telecommunications link failure. In order for the RCN to achieve the network reliability



## RCN System Engineering Analysis Report

needs of the public sector agencies, an alternate telecommunications path is required for all RCN telecommunications links.

### 4.6.2 *Telecommunications Hub Equipment Redundancy*

Telecommunications hub equipment redundancy is another type of network reliability requirement that the regional network will have to support to minimize the potential for system down time. With redundant telecommunications hub equipment, the RCN can sustain planned or unplanned down time of the hub equipment without the public sector agencies losing connectivity. It is recommended that all agencies implement future plans for separating this redundant regional hub equipment into two different public sector facilities. It is preferable that these two different facilities reside on separate power grids for enhanced reliability in the event of a disaster or some other condition that causes prolonged power loss.

### 4.6.3 *Impacts of Network Reliability on Bandwidth*

The reliability level that is planned for a network also can have an impact on the amount of bandwidth that is perceived to be available. For example, a telecommunications link between two agencies could have two diverse paths for network traffic to transverse, but the amount of available bandwidth is dependent on the link that offers the least amount of bandwidth. It is easy to confuse this issue and say that the amount of available bandwidth is the combined total bandwidth of the two links, which is the case when there is not a link failure. However, if there is a link failure, then the amount of available bandwidth is limited to the bandwidth of the other link providing the alternate path. If this limited bandwidth perception is kept in mind, then over-allocating of the available bandwidth will not become a factor and the deployment of the RCN will maintain the required reliability level.

## 4.7 Other RCN Requirements

In addition to the bandwidth, flexibility, security, and reliability requirements for the RCN, there are a number of other types of equipment/infrastructure necessary in order to meet the RCN needs. These other requirements identified below correspond directly to many of the needs identified in Section 4.1:

### 4.7.1 *Availability*

The RCN infrastructure equipment and services are required to be evaluated considering ease of which parts and support can be obtained and, in the case of leased service offerings, the coverage area that can be supported.

### 4.7.2 *Cost*

Regional public sector infrastructure investment and service options are required to be evaluated against one another over a 10 year and 20 year life cycle.



## RCN System Engineering Analysis Report

### 4.7.3 *Cutting Edge*

The RCN infrastructure is required to be evaluated considering the availability of vendors supporting technologies and features and the strength of the vendor's support for current and pending industry standards/technologies. The best way to avoid unproven cutting edge technologies is to specify equipment types with successful deployment histories and require adherence to adopted industry standards. The best way to avoid a technology that is on the verge of obsolescence is to require equipment that not only meets the immediate needs of the system, but also is scalable and expandable to meet specified expansion criteria.

### 4.7.4 *Interoperability*

The RCN equipment is required to be evaluated based upon independent interoperability tests or standards that provide proof of vendor interoperability claims. Interoperability criteria will ultimately dictate the importance of using adopted industry standards for the technologies selected. For example, Resilient Packet Rings (RPR) is the newest technology available on the market, but it is not fully standardized. Thus, the vendor that is selected at one end of a telecommunications link also has to be used at the other end of the telecommunications link. These technologies are commonly referred to as "proprietary technologies" because only one vendor can offer future expansion equipment without needing to replace equipment purchased in the initial investment, which is unacceptable for the RCN to succeed.

### 4.7.5 *Maintainability*

The RCN infrastructure equipment and services are required to be evaluated based upon the ability to obtain replacement parts; the level of staff sophistication required to support the technology; and the ease of replacing equipment with newer equipment.

### 4.7.6 *Scalability/Expandability*

The RCN infrastructure equipment and services are required to be evaluated for their ability to scale from Tier 1 to Tier 2, and from Tier 2 to Tier 3. In addition, infrastructure equipment will be evaluated for its ability to expand system capacity with minimal infrastructure replacement.

## 5. SYSTEM DESIGN

### 5.1 High-Level Design

#### 5.1.1 *Regional Hub Connectivity High-Level Design for Initial Deployment:*

The regional hub connectivity approach for the initial deployment area builds upon the same concepts that were identified within the MAG RCN Study. As such, this initial deployment project will establish the core ring and a large portion of the West Valley sub-ring depicted below:

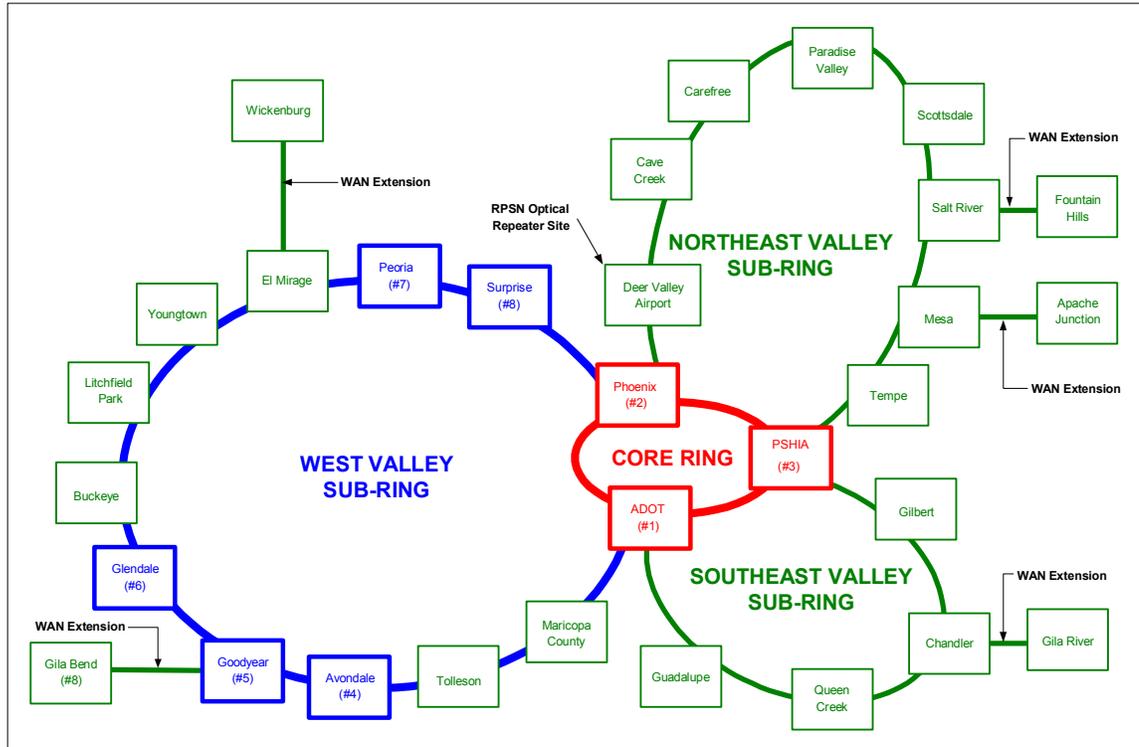


Figure 7: Overall Regional Hub Connections

The core ring consists of the regional backbone fiber links that interconnect regional hubs #1, #2, and #3, as shown in **Figure 7** above in red. This core ring of the RCN functions as the core backbone for interconnecting the three regional sub-rings. For example, if a regional hub on the West Valley sub-ring needs connectivity to a regional hub on the Northeast Valley sub-ring, this interconnectivity between sub-rings is achieved via the core ring.

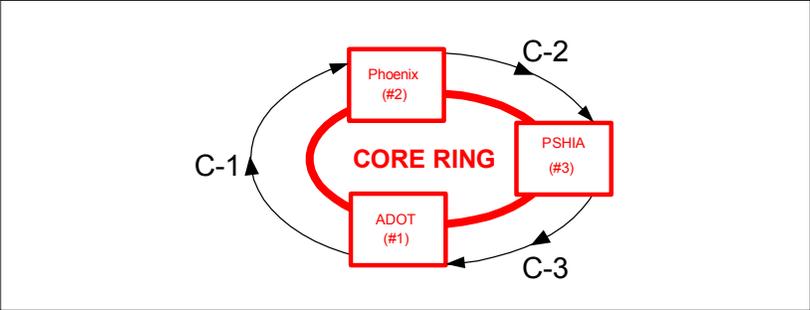
The West Valley sub-ring provides the primary intra-jurisdictional connectivity path for all regional hub locations on the west side of the region. Although the link between regional hub #1 and regional hub #2 is considered part of the core ring, this link is also a critical part of the West Valley sub-ring. The core ring link between regional hub #1 and regional hub #2 completes the redundant path for video, voice, and/or data traffic from one West Valley regional hub to another West Valley regional hub.

### 5.1.2 Core Ring Connectivity

The core ring is comprised of the three regional backbone fiber links that will be used to interconnect the following three regional hub locations:

- ADOT TOC;
- City of Phoenix Calvin Goode building; and
- Phoenix Sky Harbor International Airport Rental Car Center.

The three regional backbone fiber links needed to create the core ring are identified as C-1, C-2, and C-3 as depicted below in **Figure 8**:



**Figure 8: Core Ring Regional Hub Connectivity Links**

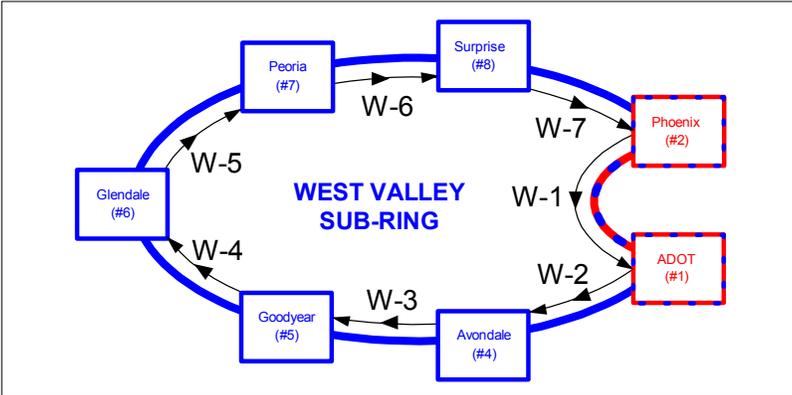
The core infrastructure segments needed to create regional backbone infrastructure links C-1, C-2, and C-3 with their proposed routes as shown in **Figure 8** above. These segments are described in further detail in the DCR.

**5.1.3 West Valley Sub-Ring Connectivity**

Initial RCN deployment for the West Valley sub-ring is comprised of seven regional backbone fiber links that will be used to interconnect the following seven regional hub locations that are part of the initial deployment project focus area:

- City of Phoenix (251 West Washington Street, Phoenix Arizona 85003);
- ADOT TOC (2302 West Durango Street, Phoenix, Arizona 85009-6452);
- City of Avondale (11465 West Civic Center Drive, Avondale, Arizona 85323);
- City of Goodyear (190 North Litchfield Road, Goodyear, Arizona 85338);
- City of Glendale (6835 North 57th Drive Glendale, Arizona 85301);
- City of Peoria (8401 West Monroe Street, Peoria, Arizona, 85345); and
- City of Surprise (14225 West Paradise Lane, Surprise, Arizona).

The seven regional backbone fiber links needed to create the West Valley Sub-Ring are identified as W-1, W-2, W-3, W-4, W-5, W-6, and W-7, as depicted below:



**Figure 9: West Valley Sub-Ring Regional Hub Connectivity Links**

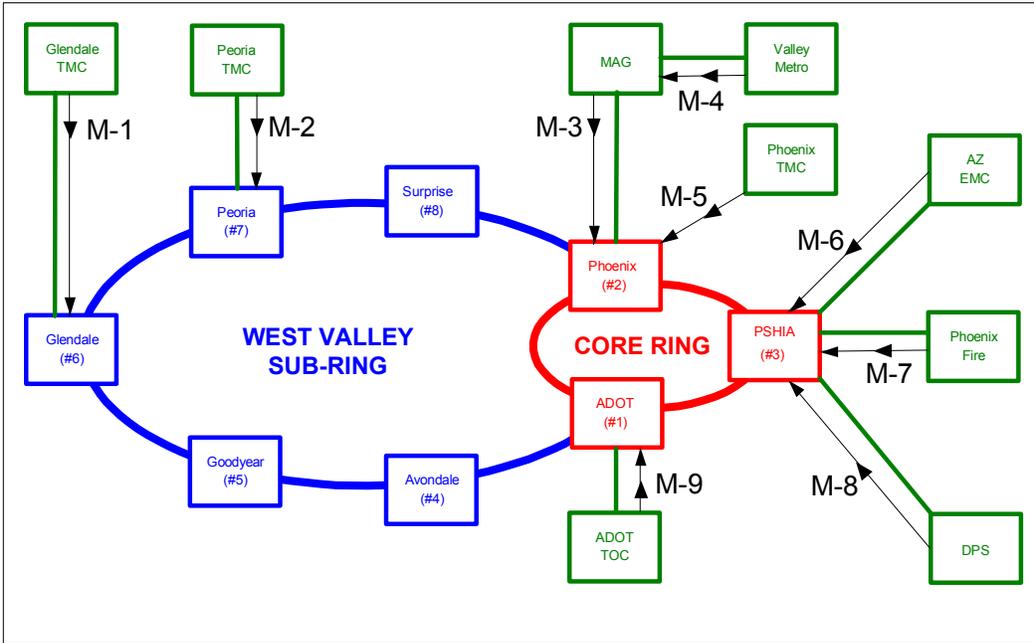
The initial RCN West Valley sub-ring infrastructure segments needed to create regional backbone infrastructure links W-1, W-2, W-3, W-4, W-5, W-6 and W-7 with their proposed routes are summarized above in **Figure 9** and described in further detail in the DCR.

**5.2 Metropolitan Hub Connectivity High-Level Design for Initial Deployment:**

The RCN initial deployment project focus area includes the connection of eight metropolitan/local hub locations into the RCN infrastructure. (Note that the MAG and Valley Metro locations are counted as one hub location.) The following eight metropolitan/local hub locations have been identified for this RCN initial deployment project:

- ADOT TOC (2302 W. Durango Street);
- Arizona Department of Emergency Management (5636 E. McDowell Road);
- City of Glendale TMC (9658 N. 59th Avenue);
- City of Peoria TMC (8501 W. Monroe Street);
- City of Phoenix Fire (150 S. 12th Street);
- City of Phoenix TMC (200 W. Washington Street);
- Department of Public Safety Central Bureau Office (2610 S. 16th Street); and
- MAG / Valley-Metro (302 N. 1st Avenue).

The RCN fiber links needed to connect these metropolitan/local hub locations to their respective regional hub facilities are identified as M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-8 and M-9 as depicted below in **Figure 10**:



**Figure 10: Metropolitan and Local Hub Connectivity Links**



## RCN System Engineering Analysis Report

The initial RCN deployment infrastructure segments needed to create the metropolitan and local hub links M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-8 and M-9 with their proposed routes are described in further detail in the DCR.

### 5.3 Detailed Design

In 2006, ADOT and its AZTech™ partners plan to complete the Plans, Specifications, and Estimate (PS&E) construction documents for Phase 1 of the RCN. These PS&E construction documents are currently at the 95% level of completion. Environmental clearances for the RCN Initial deployment areas have already been obtained, in accordance with FHWA requirements.

## 6. SYSTEM IMPLEMENTATION

ADOT will take the lead managing the construction efforts of RCN Phase 1A. The ADOT project manager will send quarterly reports on construction progress to MAG and FHWA, as mutually agreed upon. Phase 1A of the RCN project will be procured using the following two procurement approaches:

### 6.1 Conduit and Fiber Optic Cable System Deployment

In early 2007, ADOT plans to procure the services of the general contractor that provides the lowest reasonable bid for installation of conduit, inner-duct, pull / junction boxes, cable trays, equipment racks and minor electrical work that is associated with the RCN Phase 1A project. It is anticipated that the ADOT VISION office will administer the construction of this work using ADOT Standard Specifications in conjunction with the project design Plans and Technical Special Provisions.

### 6.2 Active Electronic System Equipment Deployment

Because the cost of active electronic network components rapidly changes as technology advancements are released within the industry, and the skill set of the individuals installing this equipment depends on the vendor systems that are to be deployed (i.e., certified system installers), it was agreed that the deployment of the RCN Phase 1A active electronic systems would be procured through the *Statewide Network Equipment* contract (T06-59-00015). Using this procurement approach, ADOT will solicit proposals from three or more pre-approved network solution providers for the procurement of a turn-key active electronic network solution. It is anticipated that the selection of this solution provider will be based on the type of solution being proposed and the cost of the proposed solution.

## 7. SYSTEM TEST AND VERIFICATION

The connectivity, bandwidth, security, devices, transportation applications, and other components of the RCN will need to be tested, verified and validated. This section describes, at a high level, process that will be used to accomplish this requirement.



## RCN System Engineering Analysis Report

### 7.1 Integration and Testing

The integration and testing requirements of the conduit and fiber infrastructure being installed as part of RCN initial deployment phase have been included in the 95% Project Technical Specifications submittal. System integration and testing of the RCN Phase 1A active electronics will be defined as part of the procurement process in selecting a turn-key solution provider from the *Statewide Network Equipment* contract.

### 7.2 Subsystem Verification

Sub-system verification of the RCN initial deployment phase network nodes will be accomplished through video and FTP file transfers between the connected agencies. This will verify that all proposed functions are included.

### 7.3 System Validation

System validation of the RCN will be accomplished via the MCDOT C2C TMS and DMS project, as well as inter-jurisdiction deployments of the Cameleon ITS advanced transportation management software supporting hybrid IP/analog video in a server-to-server environment.

## 8. SYSTEM OPERATIONS & MAINTENANCE

Operations and maintenance of the RCN initial deployment phase will initially be the responsibility of each participating agency with RCN conduit and fiber infrastructure within their jurisdictional boundaries, as defined in the various JPAs between agencies. As the RCN grows in geographical area and partnering agencies connected, regional forums such as the MAG ITS and MAGTAG committees will take the lead in developing a more comprehensive operations and maintenance plan at some point in the future, as deemed necessary by the RCN Working Group.

The following table identifies the major items of system components that will be installed as part of RCN Phase 1A deployment and the owning jurisdictions that will be responsible for operations and maintenance of this equipment within their jurisdiction:



## RCN System Engineering Analysis Report

Major Item Description	ADOT	Phoenix	Glendale	Peoria	MAG
Conduit and Pull Box System Components	x	x	x	x	x
Fiber Optic Cable System Infrastructure	x	x	x	x	
Equipment Cabinet, Cable Tray, and Power Distribution	x	x	x	x	x
Regional Layer 3 Switch w/ GBICS	x	x	x		
Metro Layer 2 Switch w/ GBICS	x	x	x	x	x
Video Codec	x	x	x	x	x
Video Display [40" LCD Monitor]					x
Uninterruptible Power Supplies	x	x	x	x	x
Operator Console [AZTech Workstation]					x
Upgrade Regional Video Conferencing System					x

### 9. SYSTEM UPDATE, RETIREMENT AND REPLACEMENT

The policies and procedures for RCN system updates, retirement, and replacements will be defined by the RCN Working Group.