Utah Education and Telehealth Network (UETN) WAN, WiFi, Security and Content Filtering Engineering Study & Road Map

Observations, Opinions and Recommendations based on SB 222

Utah Education and Telehealth Network

Sanity Solutions Inc. *partnering with* Gazos Creek

TABLE OF CONTENTS

TABLE OF FIGURES

DISCLOSURE OF THIS REPORT This report highlights opinions of Sanity Solutions, Inc. and Gazos Creek as it relates to Senate Bill 222 and its impact on UETN's technology resources. Sanity Solutions and Gazos Creek will retain a copy of this report, all other copies released solely to UETN.

Contributors

Sondra Basham	Gazos Creek
Barry Bryson	UETN
Cort Buffington	Kansas Research and Education Network (KANREN)
Kevin Chapman	Millard School District
Jeremy Cox	Washington County School District
Jordon Crane	Wayne School District
Jon Crawford	Emery County School District
Jeff Custard	Front Range Giga PoP (FRGP, Colorado)
Kevin Dutt	UETN
Rich Finlinson	UETN
Wes Furgason	UETN
Rick Gaisford	USOE
Alan Gibbons	Cache School District
Jennifer Griffin	The Quilt
Joleen Hale	UETN
David Hatch	H-Wire
Ryan Hayes	Sanity Solutions
Adriel Jacobson	Utah School for the Deaf and the Blind
Paul James	Piute School District
Dave Jent	Indiana University (I-light and I2 GlobalNOC)
Troy Jessup	UETN
Mark Johnson	MCNC (North Carolina)
Garen Kidd	DaVinci Academy
Steve Kiss	Gazos Creek
Rebecca Knight	Gazos Creek
Linda Lane	UETN
Jen Leasure	The Quilt
David Long	Logan City School District
Scot McCombs	Canyons School District
Kelly McDonald	KCMCDONALD LLC
Bill Mott	Davis School District
Cindy Nagasawa-Cruz	Jordan School District
Cindy Najarro	UETN
Kevin Quire	UETN
Sean Rawlinson	North Sanpete School District
Dave Reese	CENIC (California)
Dennis Sampson	UETN
Alan Shakespear	Box Elder School District
Brian Singleton	Davis School District
Jesse Singleton	H-Wire
Pamela Smith	Gazos Creek
Rik Stallings	Logan City School District
Jim Stewart	UETN
Ray Timothy	UETN
Jens CK Trautvein	Intech Collegiate High School
Jim Woolley	Sanity Solutions
Josh Yaus	Gazos Creek
UEN Advisory Council	
UETN Board	

INTRODUCTION

On March 31, 2015, the Utah State Governor signed Senate Bill 222, the Digital Teaching and Learning Program Proposal. It requires that the Utah State Board of Education and Utah Education and Telehealth Network (UETN) develop a digital teaching and learning program proposal, including technical support, for Local Education Agencies (LEAs). LEAs include public school districts, charter schools, and Utah Schools for the Deaf and Blind.

Through its master plan, Utah's vision is to prepare its future workforce to succeed in today's global economy and to help them thrive in an ever-changing world by providing all students the opportunities and tools needed. The emphasis of Utah's future teaching and learning program focuses on student learning and outcomes; however, to get there, UETN's infrastructure must be able to accommodate all systems that support and improve instruction, student learning and assessment of learning, and teacher effectiveness. This includes all education stakeholders including students, teachers, parents, administration, and state agencies.

UETN's vision translates into overall increased volume of UETN WAN traffic and LEA resources that must be scaled and designed accordingly for the expected forthcoming demands.

BACKGROUND

UETN (formerly UEN and UTN) has a long history of progressive initiatives and pioneering efforts in technology. The Utah Education Network is a nationally recognized innovator in broadband and broadcast delivery of educational services for educators and students. It links more than 800,000 students and educators statewide.[1]

UEN (Utah Education Network) and UTN (Utah Telehealth Network) combined to form UETN (Utah Education and Telehealth Network) on May 13, 2014 based on Utah House Bill 92, signed by the Utah State Governor March 27, 2014.[2] A result of the merger between the two organizations was state-improved efficiencies and the ability to leverage new resources. This created a more dynamic and agile infrastructure to meet the ever-increasing demands of the districts and charter schools.

Today, UETN manages network, application, and support services to provide scalable and affordable solutions to the education organizations within the state of Utah.

As the designated primary provider of Internet access and Wide Area Network (WAN) for public education within Utah, UETN is the single largest applicant for E-rate funds in the state. UETN serves as the E-rate consortium lead in applying for and implementing the E-rate funds received for the services provided to schools. It also provides coordination of the E-rate program at the state level for all eligible E-rate program participants.

[1] About UETN – http://uetn.org/

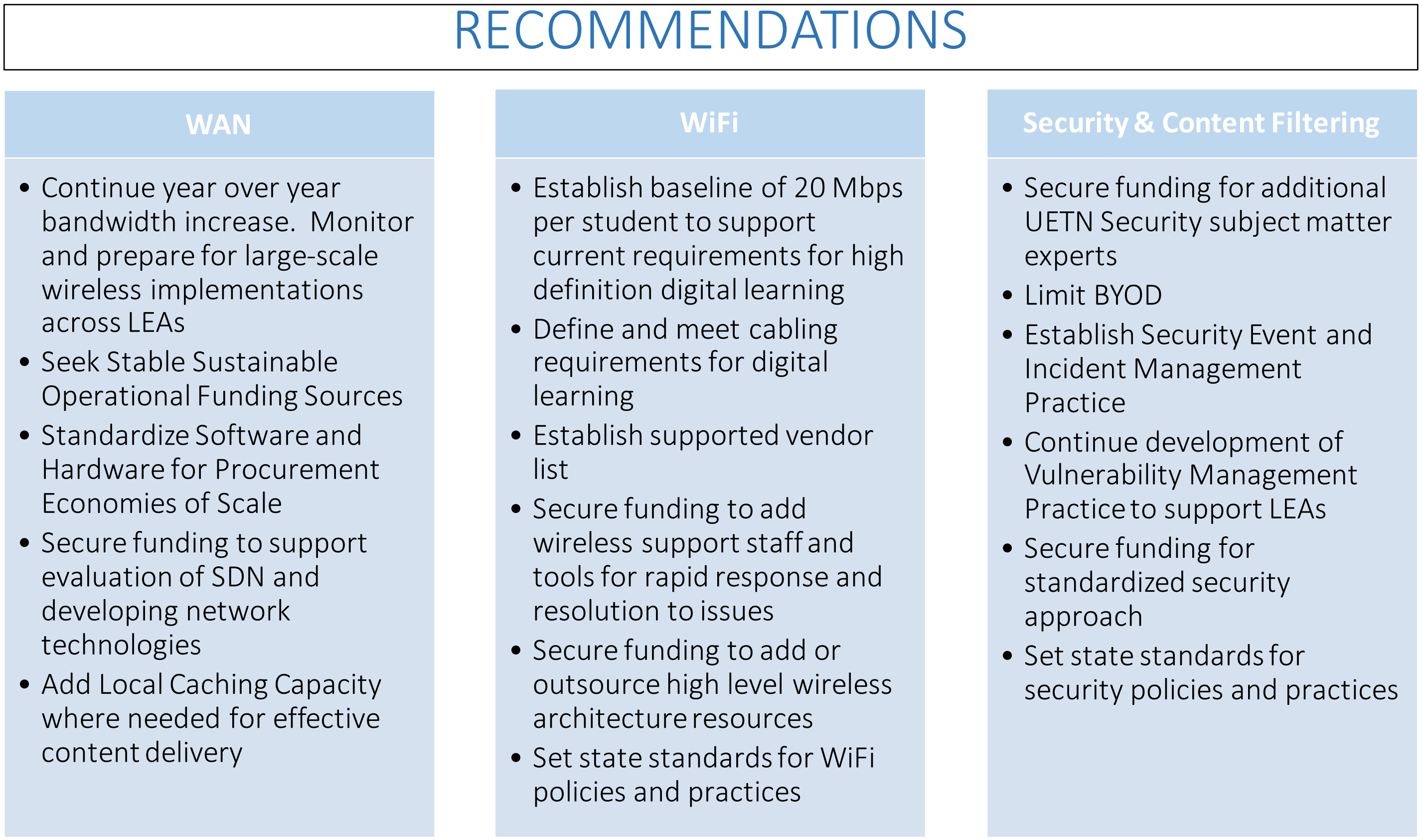
[2] UETN Overview - www.uen.org/board/downloads/uetn-overview.pdf

EXECUTIVE SUMMARY

Sanity Solutions and Gazos Creek performed an engineering study of UETN's technology infrastructure needs for public education K-12 to implement Utah's master plan, "Essential Elements for Technology Powered Learning".[3] This study is the second phase of an on-going program approved via earlier measures.

As a key deliverable of the engineering study, recommendations for UETN's WAN, Internet Security, Content Filtering and LEA WiFi have been developed. Best practices are noted and a 3 year "road map" has been created for UETN and Utah's districts and charter schools' technical readiness as a step toward helping Utah realize its vision of the future Digital Teaching and Learning Program.

Based on information obtained through written surveys sent to LEAs, and focus groups, peer reviews and interviews with key stakeholders in both the LEAs and UETN, recommendations were compiled for UETN as shown in Figure 1. In each of the respective following sections for WAN, WiFi, Internet Security and Content Filtering, the recommendations are further expanded on in summarized format.



RECOMMENDATIONS

WAN

- Continue year over year bandwidth increase. Monitor and prepare for large-scale wireless implementations across LEAs
- Seek Stable Sustainable Operational Funding Sources
- Standardize Software and Hardware for Procurement Economies of Scale
- Secure funding to support evaluation of SDN and developing network technologies
- Add Local Caching Capacity where needed for effective content delivery

WiFi

- Establish baseline of 20 Mbps per student to support current requirements for high definition digital learning
- Define and meet cabling requirements for digital learning
- Establish supported vendor list
- Secure funding to add wireless support staff and tools for rapid response and resolution to issues
- Secure funding to add or outsource high level wireless architecture resources
- Set state standards for WiFi policies and practices

Security & Content Filtering

- Secure funding for additional UETN Security subject matter experts
- Limit BYOD
- Establish Security Event and Incident Management Practice
- Continue development of Vulnerability Management Practice to support LEAs
- Secure funding for standardized security approach
- Set state standards for security policies and practices

Figure 1 – WAN, WiFi, and Internet Security and Content Filtering Recommendations for UETN

[3] "Essential Elements for Technology Powered Learning" - http://www.uen.org/digital-learning/downloads/Utah_Essential_Elements_Technology_Powered_Learning.pdf

From these recommendations, individual projects will be created based on a prioritization process defined by UETN and managed as a complete technology program (Figure 2). This ensures alignment of strategic goals and that each is measured for success at the state and LEA level.

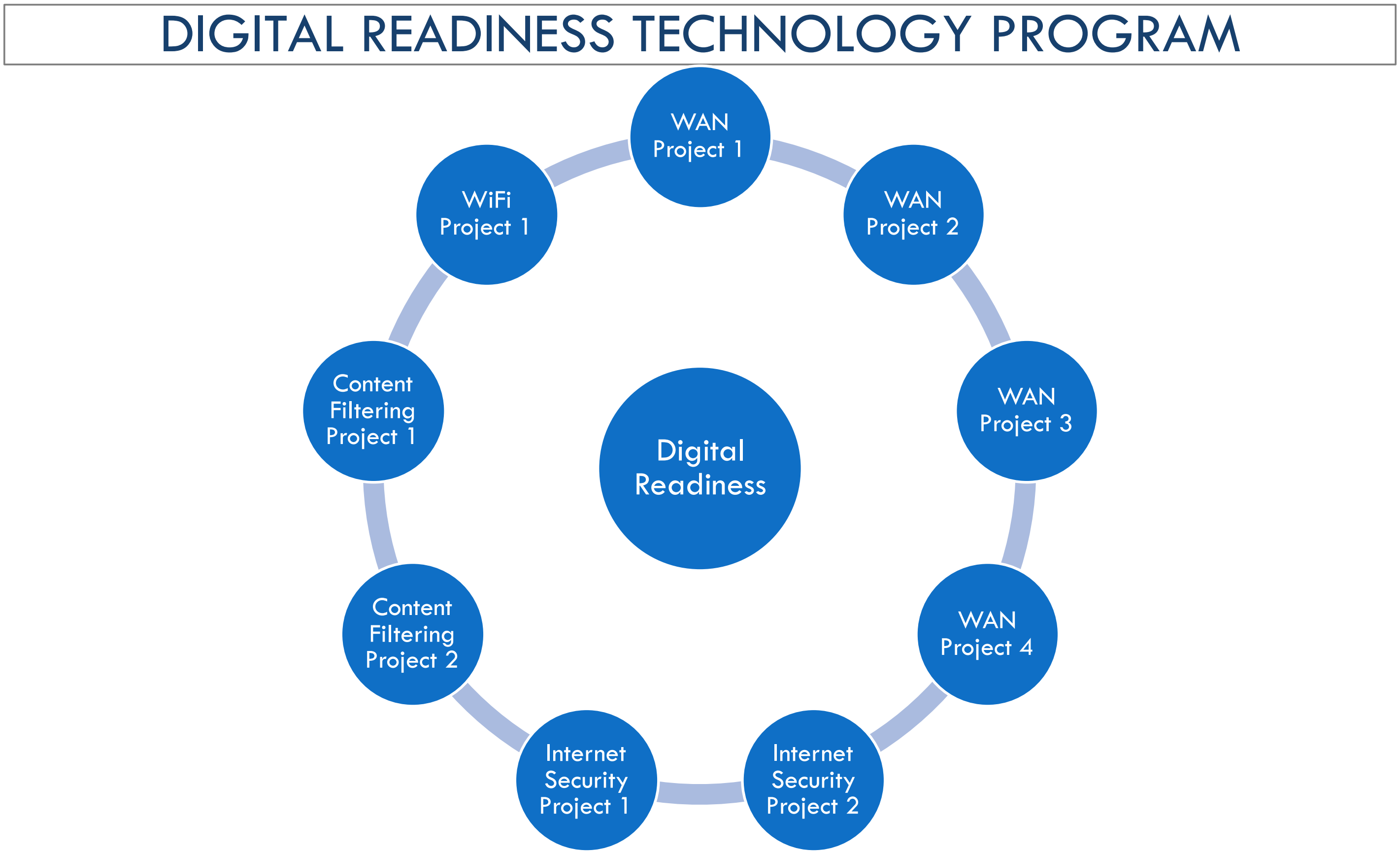

DIGITAL READINESS TECHNOLOGY PROGRAM
Digital Readiness
WAN Project 1
WAN Project 2
WAN Project 3
WAN Project 4
Internet Security Project 2
Internet Security Project 1
Content Filtering Project 2
Content Filtering Project 1
WiFi Project 1

Figure 2 - Digital Readiness Technology Program

Each project team will complete a series of activities and phases defined in its respective section. These phases are listed at a high level in Figure 3. The recommendations expanded upon below use these terms as the vehicles to combine similar activities.

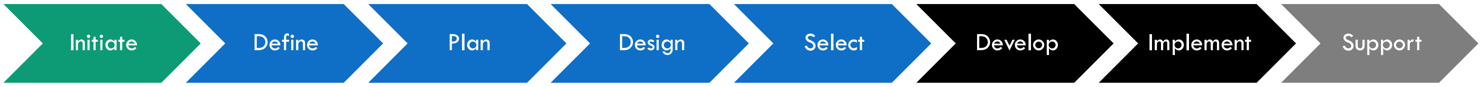


Figure 3 - High Level Activities and Phases

The last phase of each project, Support, transfers ownership of the solution into a steady state of business and institutes the support structure for ongoing health and maintenance. **In this phase it is imperative to seek stable and sustainable operational funding sources. Suggested ways to accomplish this are detailed in the report**. Generally, on-going funding must be provided to not only accommodate the one-time infrastructure costs to implement, but also to maintain and plan for rapidly changing technology, increasing costs, and stakeholder demands.

Annual budgeting, maintenance of long range goals, and strategic planning must become a routine and proactive part of the culture. Planning alone cannot fulfill the visions and strategies developed. Funding is key to success and must not be taken lightly. Without appropriate support from the necessary individuals and organizations, resources cannot be secured to execute against these plans. If funding and resources cannot be fully secured and in a timely manner, digital readiness cannot be achieved. Lack of initial and ongoing funding can single-handedly undermine the vision and prevent success of the technology program.

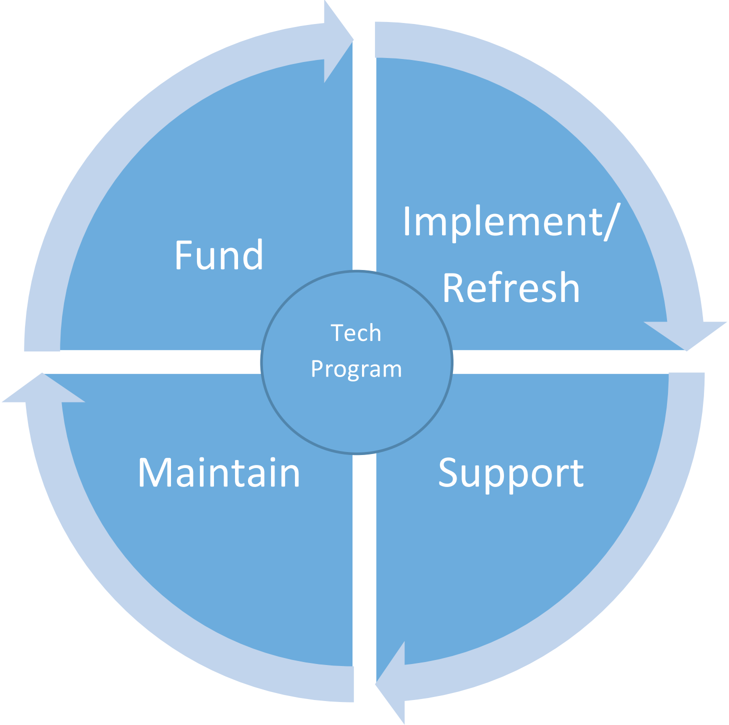


Figure 4 - Executive Summary Technology Program

While some focus in the preceding paragraphs has been on funding, it is only one of many forthcoming obstacles to overcome. Appropriate funding, complexity of dependencies between projects, cultural differences between LEAs including technological capabilities, unknown developing circumstances, rapidly emerging technologies, and complex program management (multiple work streams, disciplines, etc.) all contribute to this being a highly sophisticated, complex program, as the following overviews and recommendations support.

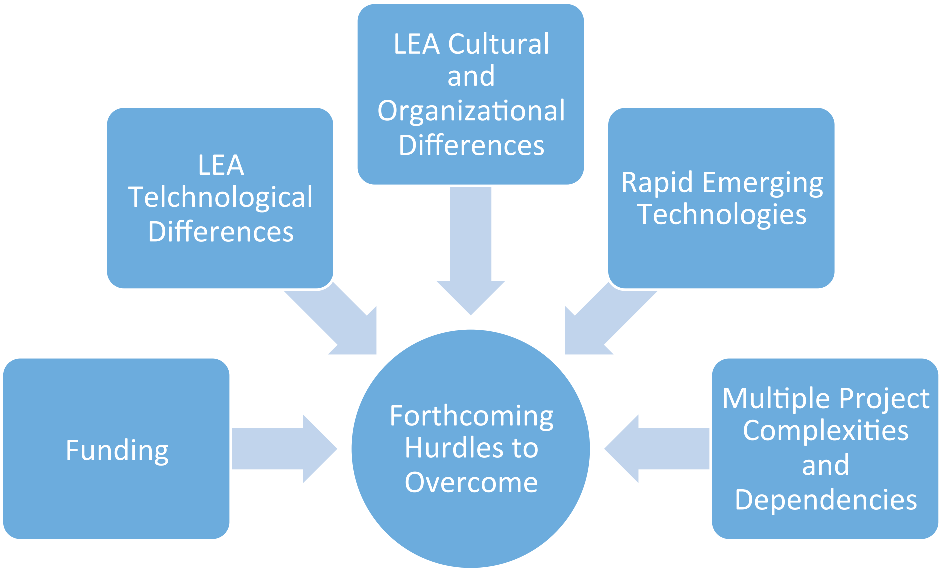

LEA Cultural and Organizational Differences
LEA Telchnological Differences
Rapid Emerging Technologies
Funding
Forthcoming Hurdles to Overcome
Multiple Project Complexities and Dependencies

Figure 5 - Forthcoming Hurdles to Overcome

Note to Reader

The team developed recommendations as individual documents addressing each domain separately (WAN, LEA WiFi, & Internet Security/Content Filtering). After each document was drafted and reviewed by contributors, based on feedback, the team collapsed all three studies into one document. As a result of this action, the reader should expect forthcoming sections to contain redundant language in High Level Activities, Problems to Solve, Recommendations, etc. In the corresponding figures, unique items to each study will be ***BOLDED and noted with an asterisk*** *(*) to aid the reader and direct to the differences.*

WIDE AREA NETWORK (WAN)

UETN WAN Overview

The Utah Education and Telehealth Network (UETN) provides a statewide research and education network connecting all public K-12 schools, higher education institutions, charter schools, libraries, and research locations comprising over 1,400 locations and 800,000 users. The network is funded through annual state appropriation, E-rate reimbursements from the FCC's Universal Service Fund, and from local, state and federal grants[4].

UETN provides networking services to design, develop, build, and maintain the statewide broadband network through partnerships with local telecommunications companies and support services, which provide advanced technology support and troubleshooting.

WAN OBSERVATIONS AND OPINIONS

WAN Current State

The UETN WAN is recognized nationally as a best-in-class network, architected and maintained on limited annual budgets and multiple one-time funding awards. UETN, through partnerships and creative solutions by staff members, manages to maintain a strategic and tactical tool for education that meets the current demands of its tenants.

The WAN services and infrastructure which have been designed, developed, provided, and supported by UETN are appropriate for the current state; however, they need improvements to meet the expected forthcoming demands. Schools are not consistently using fiber for their backbone (customer edge connection). In addition, several schools are not using copper for connectivity; for example, some are on wireless (point-to-point microwave) links as slow as 45mbps. For a customer edge connection, this is very slow and not adequate for the demands of an entire school. Also noted, some of UETN's backbone links (connections between PoPs) have limited capacity.

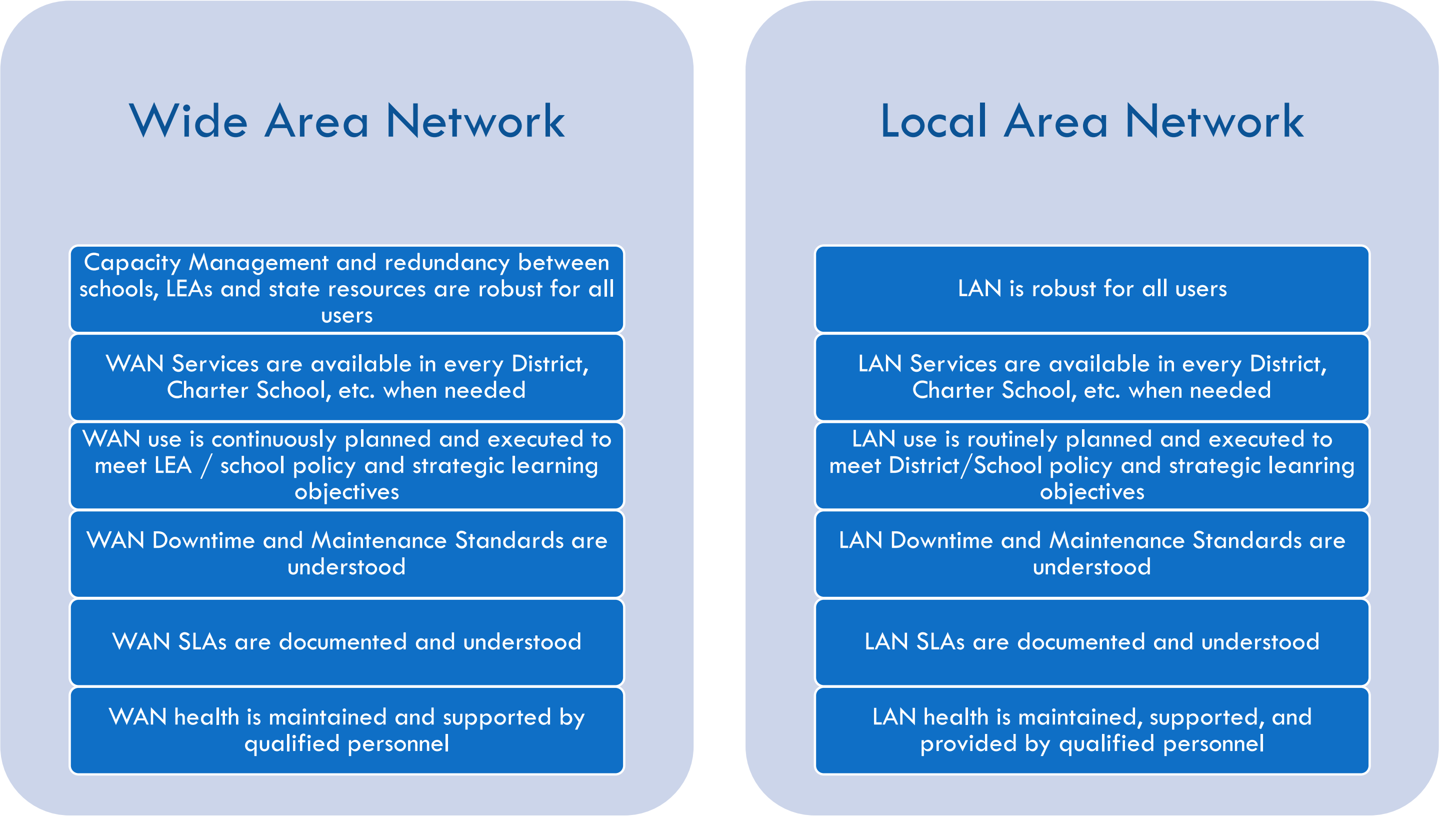
Based on the written surveys and responses garnered through the study, on the average, WAN usage doubles annually. With the increase of devices and users taxing WAN resources, appreciable improvement needs must individually be analyzed based on local requirements from the districts and charter schools.

As UETN technical staff are highly capable and subject matter experts, they are already researching and architecting for the future. Although this report will recommend some work not already in progress by UETN, most of the WAN and LAN recommendations noted below align with in-flight initiatives.

[4] About E-rate - http://www.UETN.org/E-rate/

WAN/LAN Objectives

Noted in Figure 6 are the ideal standards of performance and best practices for the UETN WAN and LEA Local Area Networks (LANs) (where necessary to utilize the WAN effectively). These standards and practices are the basis for developing the recommendations contained in this document.



Wide Area Network

- Capacity Management and redundancy between schools, LEAs and state resources are robust for all users
- WAN Services are available in every District, Charter School, etc. when needed
- WAN use is continuously planned and executed to meet LEA / school policy and strategic learning objectives
- WAN Downtime and Maintenance Standards are understood
- WAN SLAs are documented and understood
- WAN health is maintained and supported by qualified personnel

Local Area Network

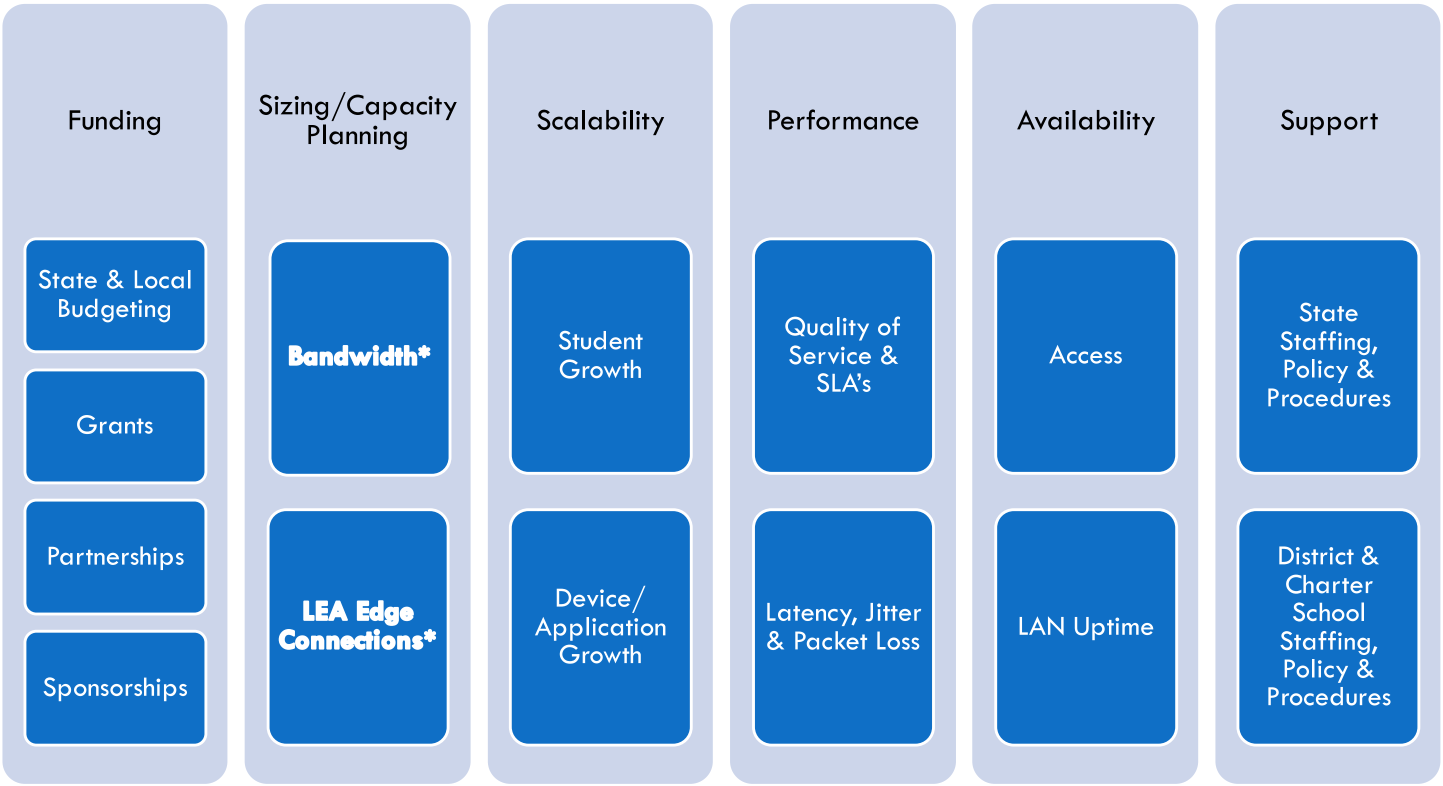
- LAN is robust for all users
- LAN Services are available in every District, Charter School, etc. when needed
- LAN use is routinely planned and executed to meet District/School policy and strategic leanring objectives
- LAN Downtime and Maintenance Standards are understood
- LAN SLAs are documented and understood
- LAN health is maintained, supported, and provided by qualified personnel

Figure 6 - Standards of Performance and Best Practices for the UETN WAN and LEA LANs

WAN Forthcoming or Present Problems to Solve

Based on the findings, listed below are the key and highest probability impacted items to address for the WAN.

PROBLEMS TO SOLVE



Funding
- State & Local Budgeting
- Grants
- Partnerships
- Sponsorships

Sizing/Capacity Planning
- **Bandwidth***
- **LEA Edge Connections***

Scalability
- Student Growth
- Device/ Application Growth

Performance
- Quality of Service & SLA's
- Latency, Jitter & Packet Loss

Availability
- Access
- LAN Uptime

Support
- State Staffing, Policy & Procedures
- District & Charter School Staffing, Policy & Procedures

Figure 7 - WAN Forthcoming or Present Problems to Solve

WAN Recommendations

Funding

UETN must seek stable, sustainable on-going operational funding sources to ensure technical readiness to meet the vision of the Digital Teaching and Learning Program. It is imperative that UETN shift away from using one-time funding sources for its' on-going operational expenses. There are a myriad of ways to accomplish this as stated within this section.

As the WAN is both a strategic and tactical tool, the shift and growth of its services should be anticipated in the normal course of routine operations. Historically, stakeholders do not perceive the WAN in this manner unless a critical incident occurs to heighten awareness, such as an outage or other interruption of service. This creates a cycle of reactive funding rather than proactive approval of recurring budget and grant requests. High prioritization should be placed on this domain.

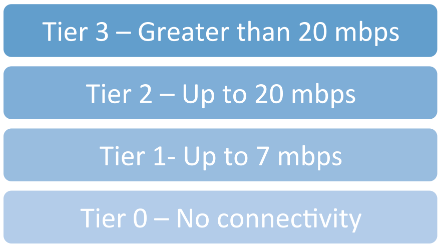
Strategic Partner/Sponsorships – UETN should explore creative approaches for funding and resources through corporate partnerships, grants and sponsorships. Strategic sourcing plays a vital role in the success of cost containment through the development of initiatives such as entering into case study agreements and research programs with corporate and private sponsors.

Standards for Procurement Economies of Scale – Harnessing the value of strategic relationships is not the only avenue for cost containment. Establishing "tiered" networking standards of hardware, software and services across the districts and charter schools allows procurement to negotiate contracts that benefit from the economies of scale for bulk purchasing with preferred providers.

WAN Sizing/Capacity Planning, Scalability, Performance, Availability

High Speed Customer Edge Connections – If not already existing, bandwidth-per-student thresholds should be established with tiers based on each school's needs. For example, schools with more students in a classroom would be in a higher tier and require more bandwidth than a lower tier with fewer students in the classroom, based on application demands. Figure 8 presents Megabits per second (Mbps) per student in the classroom

(example only for reference and suggested as an assumed standard)



Tier 3 – Greater than 20 mbps

Tier 2 – Up to 20 mbps

Tier 1- Up to 7 mbps

Tier 0 – No connectivity

Figure 8 - Megabits per second (Mbps) per student

Move Source Material to Schools – Where not already in place, install caching servers at the school to decrease bandwidth demands by storing content locally. Although not generally considered WAN optimization because it is application dependent, local caching can reduce demands for WAN bandwidth in certain cases. Whether pre-planned (i.e., manually stored locally/ application specific) or dynamic (frequently visited), local caching can solve some existing, and forthcoming, bandwidth constraints in rural areas.[5]

Software Defined Networking (SDN) in WAN Core – Utilizing SDN with virtualized servers in data centers (not between routers and switches) is where SDN shines by letting the virtual server administrator perform some network engineering tasks so that secondary assistance isn't required from network engineers. As application roll-outs accelerate, SDN streamlines data center deployment by putting application developers in charge of their own network resources, eliminating the high-touch cost and risk of human-directed network reconfiguration.[6]

[5] See the KA Lite User Manual for an example of software that allows for caching of educational progress, updating once internet connectivity is achieved - https://learningequality.org/ka-lite/user-guides/embed/user-manual-011#h.funuj6eybc7o

[6] Information Week Network Computing - http://www.networkcomputing.com/networking/applying-sdn-to-education-/d/d-id/1320235

WAN Support

Additional Staff – Charter schools and districts depend on UETN's staff for support and assistance with WAN services. As the demand and utilization increase, so will service requests and assistance from UETN's subject matter experts to assist LEA's.

Continued Training and Mentoring Programs – Whether delivered by or facilitated by UETN, training is a fundamental building block of a healthy network. UETN maintains multiple training and mentoring programs which not only benefit the district and charter school's technology staff, but also benefits UETN statewide WAN staff by engaging to understand specific problems the districts and charter schools encounter. This translates into sharing knowledge of design activities for solutions and policies of the enterprise.

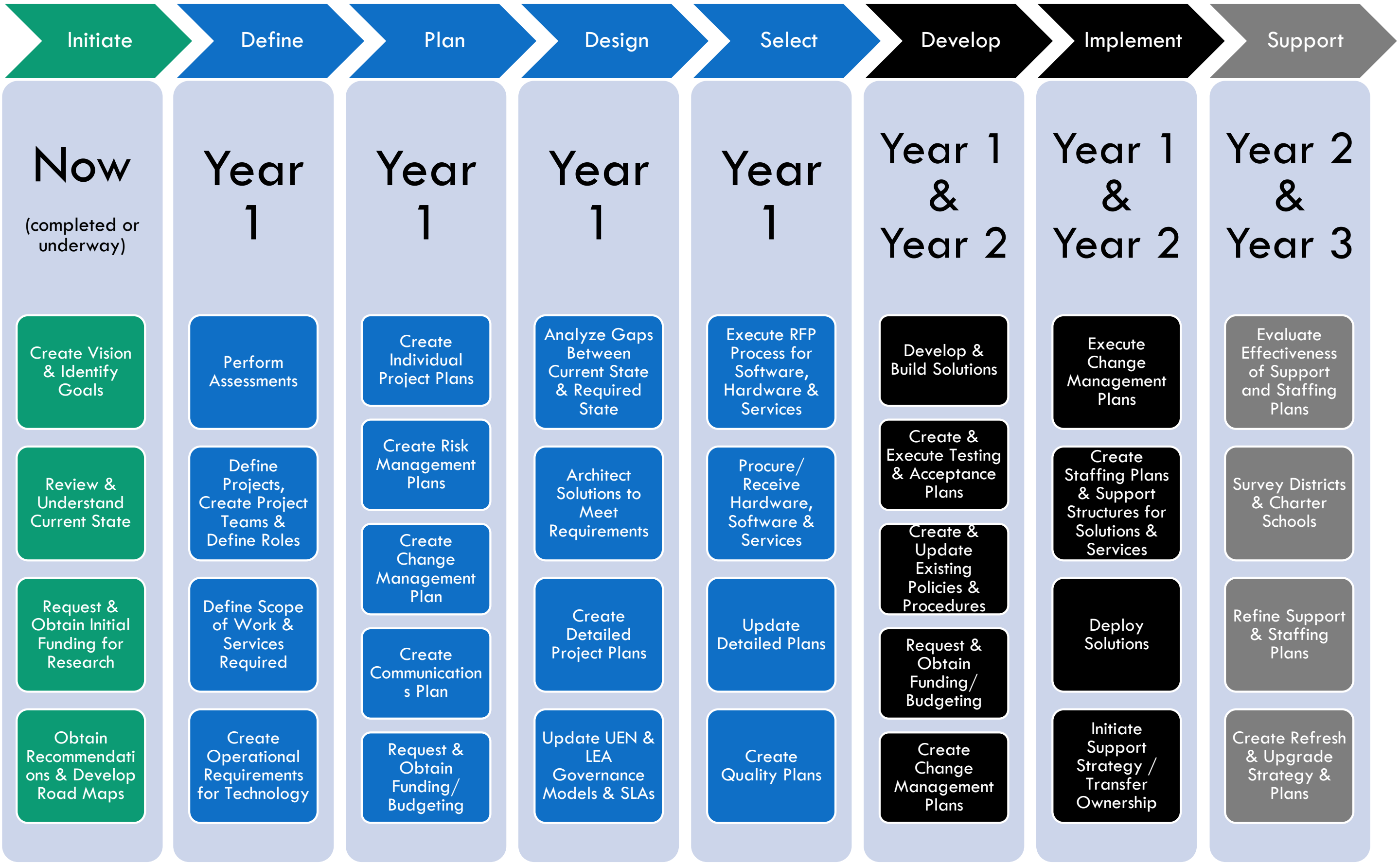
Standardization of Policies and Practices – Standardization of policies and practices facilitates consistent operations in technology with improved cost-saving efficiencies and improved efficiencies with support.

WAN Road Map

Below is a proposed Road Map for UETN's anticipated WAN growth due to SB 222 (Figure 9). The Initiate column with the timeframe labeled "Now" reflects activities fully underway by UETN.

It is not expected that each individual project will progress through each phase of work at the same pace. Instead, they will execute individual applicable tasks based on its own specific constraints, dependencies, funding and prioritization.

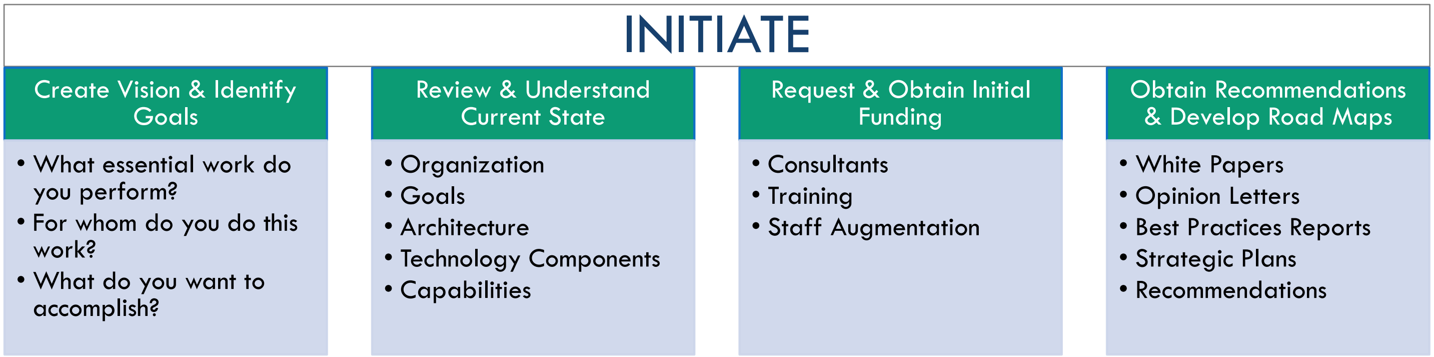
WAN Road Map



Initiate	Define	Plan	Design	Select	Develop	Implement	Support
Now (completed or underway)	Year 1	Year 1	Year 1	Year 1	Year 1 & Year 2	Year 1 & Year 2	Year 2 & Year 3
Create Vision & Identify Goals	Perform Assessments	Create Individual Project Plans	Analyze Gaps Between Current State & Required State	Execute RFP Process for Software, Hardware & Services	Develop & Build Solutions	Execute Change Management Plans	Evaluate Effectiveness of Support and Staffing Plans
Review & Understand Current State	Define Projects, Create Project Teams & Define Roles	Create Risk Management Plans	Architect Solutions to Meet Requirements	Procure/ Receive Hardware, Software & Services	Create & Execute Testing & Acceptance Plans	Create Staffing Plans & Support Structures for Solutions & Services	Survey Districts & Charter Schools
Request & Obtain Initial Funding for Research	Define Scope of Work & Services Required	Create Change Management Plan	Create Detailed Project Plans	Update Detailed Plans	Create & Update Existing Policies & Procedures	Deploy Solutions	Refine Support & Staffing Plans
Obtain Recommendations & Develop Road Maps	Create Operational Requirements for Technology	Create Communications Plan	Update UEN & LEA Governance Models & SLAs	Create Quality Plans	Request & Obtain Funding/ Budgeting	Initiate Support Strategy / Transfer Ownership	Create Refresh & Upgrade Strategy & Plans
		Request & Obtain Funding/ Budgeting			Create Change Management Plans		

Figure 9 - WAN Road Map

WAN High Level Activities



INITIATE

Create Vision & Identify Goals

- What essential work do you perform?
- For whom do you do this work?
- What do you want to accomplish?

Review & Understand Current State

- Organization
- Goals
- Architecture
- Technology Components
- Capabilities

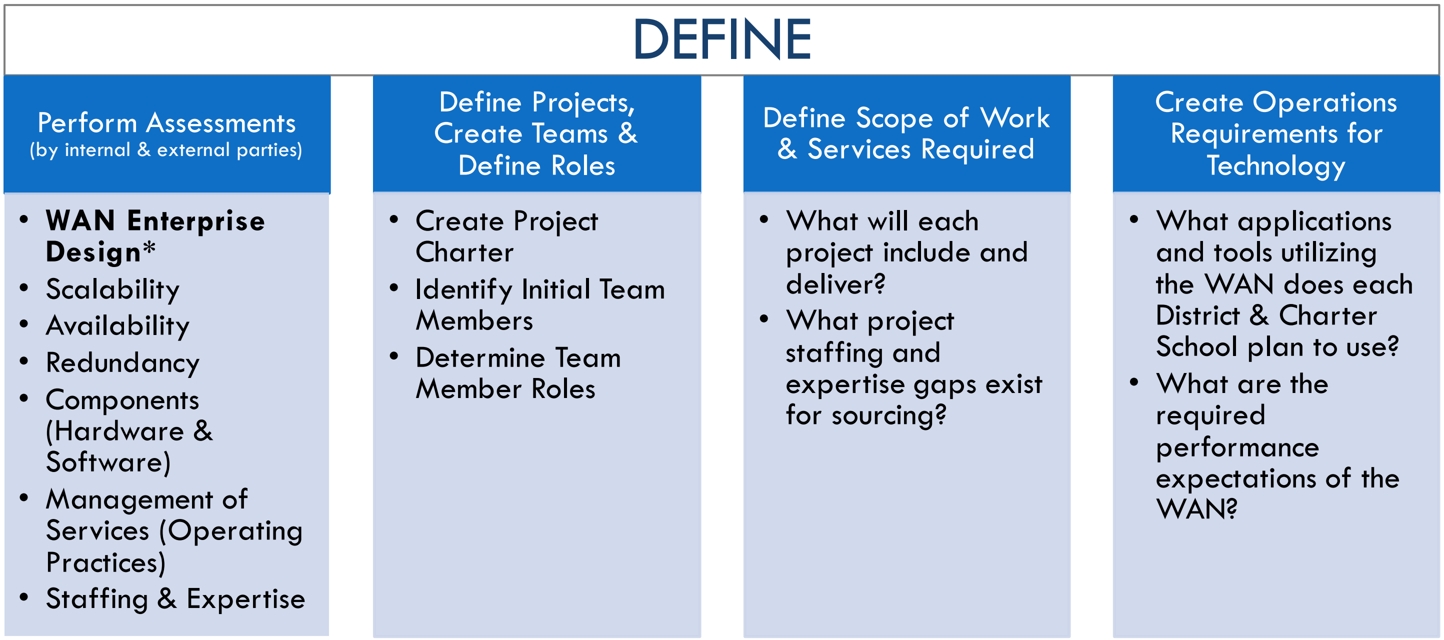
Request & Obtain Initial Funding

- Consultants
- Training
- Staff Augmentation

Obtain Recommendations & Develop Road Maps

- White Papers
- Opinion Letters
- Best Practices Reports
- Strategic Plans
- Recommendations

Figure 10- WAN Initiation Activities



DEFINE

Perform Assessments (by internal & external parties)

- **WAN Enterprise Design***
- Scalability
- Availability
- Redundancy
- Components (Hardware & Software)
- Management of Services (Operating Practices)
- Staffing & Expertise

Define Projects, Create Teams & Define Roles

- Create Project Charter
- Identify Initial Team Members
- Determine Team Member Roles

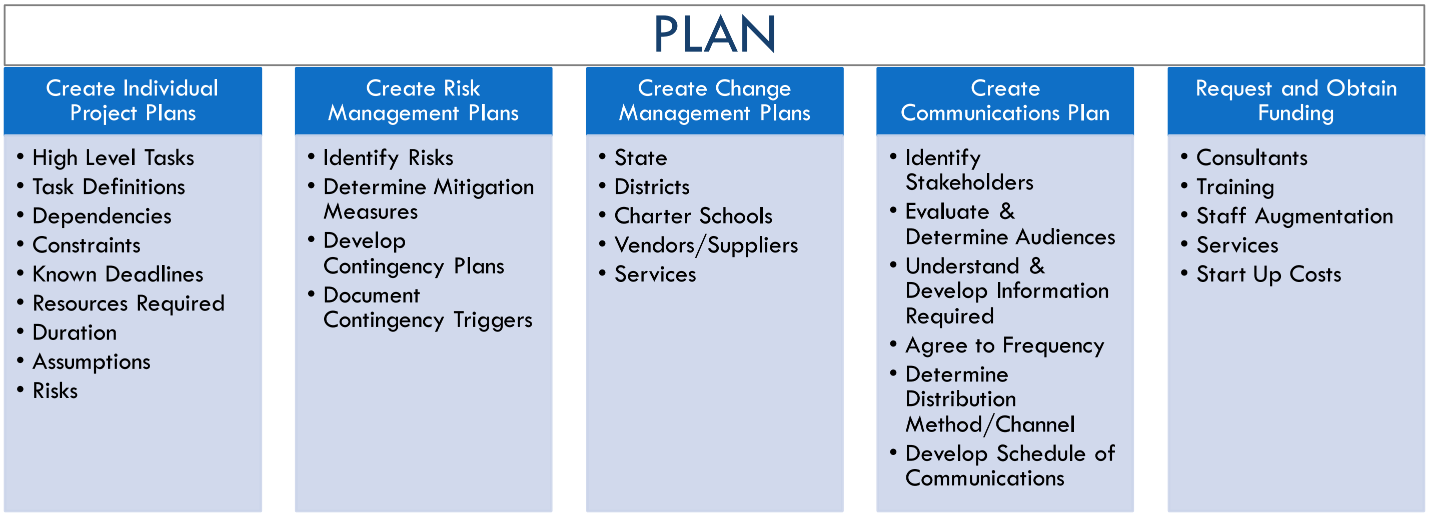
Define Scope of Work & Services Required

- What will each project include and deliver?
- What project staffing and expertise gaps exist for sourcing?

Create Operations Requirements for Technology

- What applications and tools utilizing the WAN does each District & Charter School plan to use?
- What are the required performance expectations of the WAN?

Figure 11 - WAN Definition Activities



PLAN

Create Individual Project Plans

- High Level Tasks
- Task Definitions
- Dependencies
- Constraints
- Known Deadlines
- Resources Required
- Duration
- Assumptions
- Risks

Create Risk Management Plans

- Identify Risks
- Determine Mitigation Measures
- Develop Contingency Plans
- Document Contingency Triggers

Create Change Management Plans

- State
- Districts
- Charter Schools
- Vendors/Suppliers
- Services

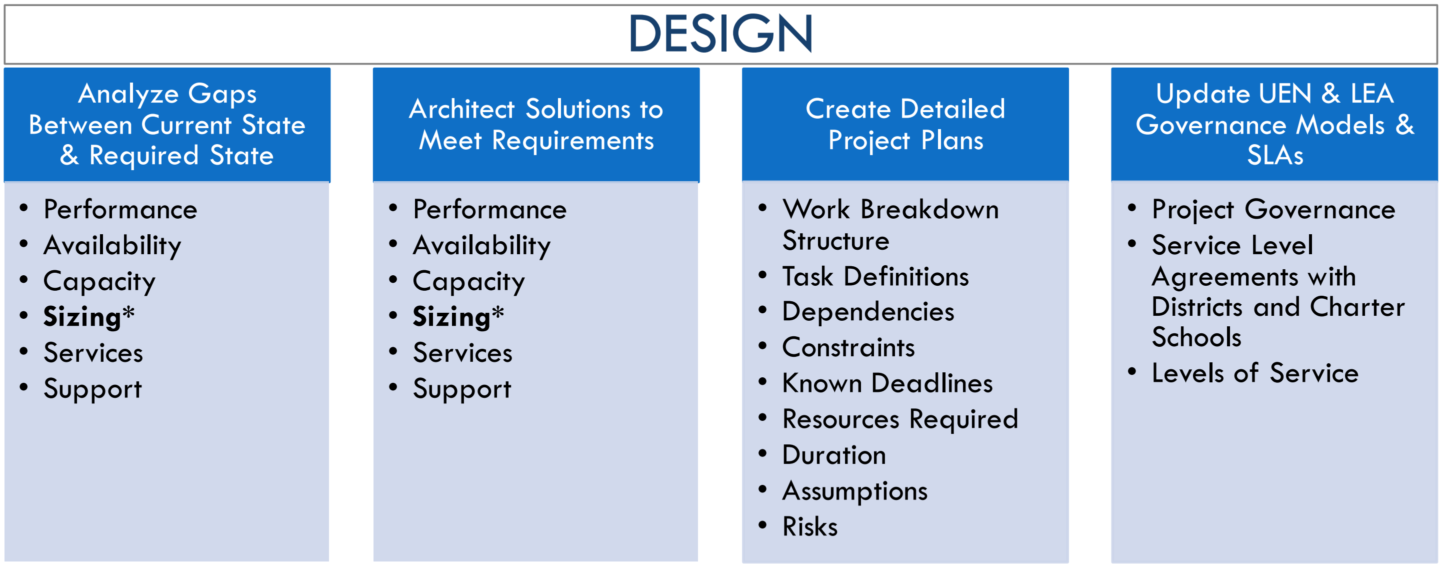
Create Communications Plan

- Identify Stakeholders
- Evaluate & Determine Audiences
- Understand & Develop Information Required
- Agree to Frequency
- Determine Distribution Method/Channel
- Develop Schedule of Communications

Request and Obtain Funding

- Consultants
- Training
- Staff Augmentation
- Services
- Start Up Costs

Figure 12 - WAN Planning Activities



DESIGN

Analyze Gaps Between Current State & Required State

- Performance
- Availability
- Capacity
- **Sizing***
- Services
- Support

Architect Solutions to Meet Requirements

- Performance
- Availability
- Capacity
- **Sizing***
- Services
- Support

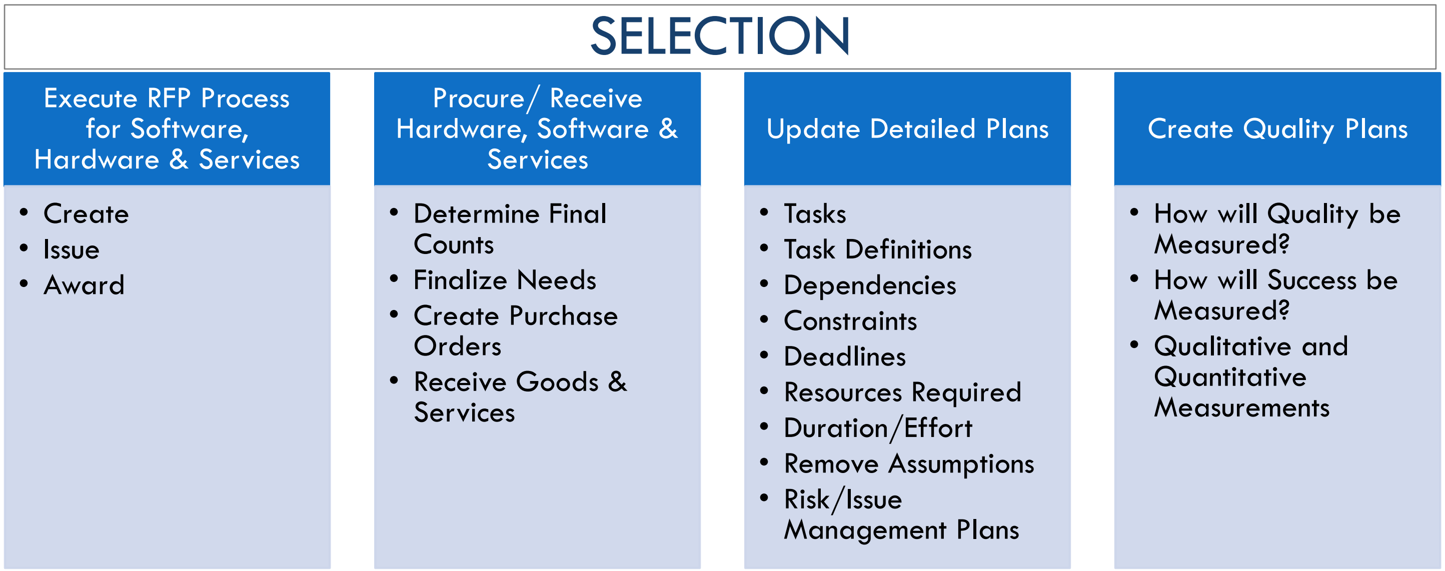
Create Detailed Project Plans

- Work Breakdown Structure
- Task Definitions
- Dependencies
- Constraints
- Known Deadlines
- Resources Required
- Duration
- Assumptions
- Risks

Update UEN & LEA Governance Models & SLAs

- Project Governance
- Service Level Agreements with Districts and Charter Schools
- Levels of Service

Figure 13 - WAN Design Activities



SELECTION

Execute RFP Process for Software, Hardware & Services

- Create
- Issue
- Award

Procure/ Receive Hardware, Software & Services

- Determine Final Counts
- Finalize Needs
- Create Purchase Orders
- Receive Goods & Services

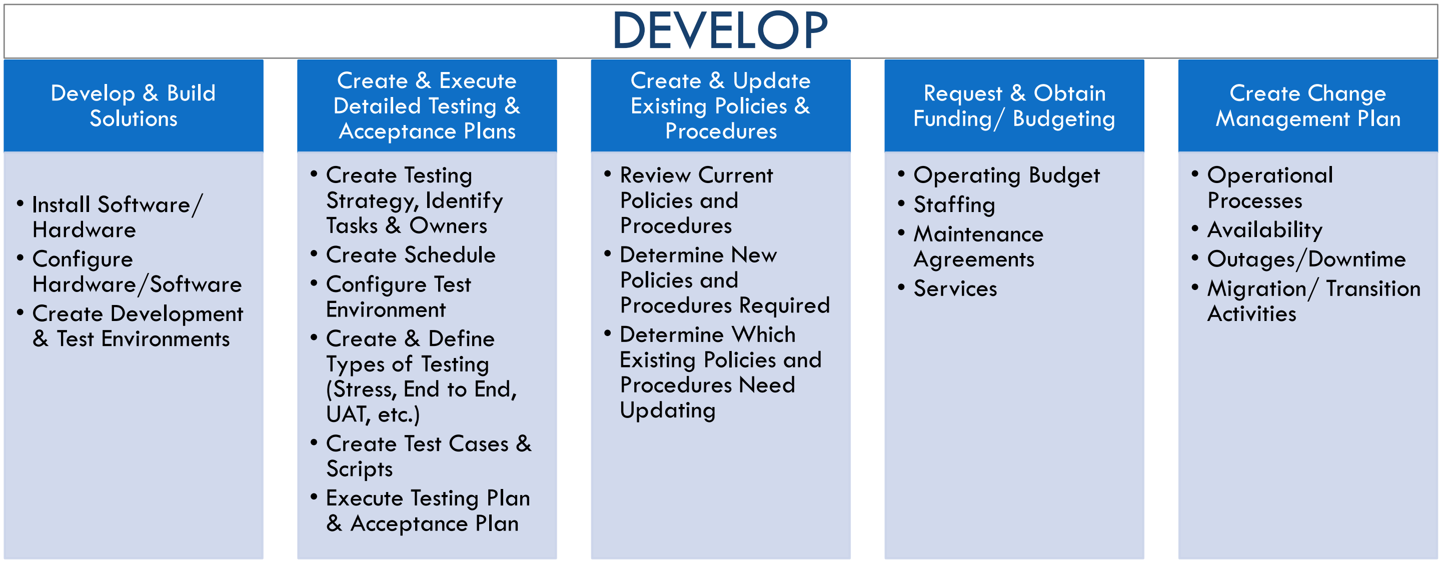
Update Detailed Plans

- Tasks
- Task Definitions
- Dependencies
- Constraints
- Deadlines
- Resources Required
- Duration/Effort
- Remove Assumptions
- Risk/Issue Management Plans

Create Quality Plans

- How will Quality be Measured?
- How will Success be Measured?
- Qualitative and Quantitative Measurements

Figure 14 - WAN Selection Activities



DEVELOP

Develop & Build Solutions

- Install Software/ Hardware
- Configure Hardware/Software
- Create Development & Test Environments

Create & Execute Detailed Testing & Acceptance Plans

- Create Testing Strategy, Identify Tasks & Owners
- Create Schedule
- Configure Test Environment
- Create & Define Types of Testing (Stress, End to End, UAT, etc.)
- Create Test Cases & Scripts
- Execute Testing Plan & Acceptance Plan

Create & Update Existing Policies & Procedures

- Review Current Policies and Procedures
- Determine New Policies and Procedures Required
- Determine Which Existing Policies and Procedures Need Updating

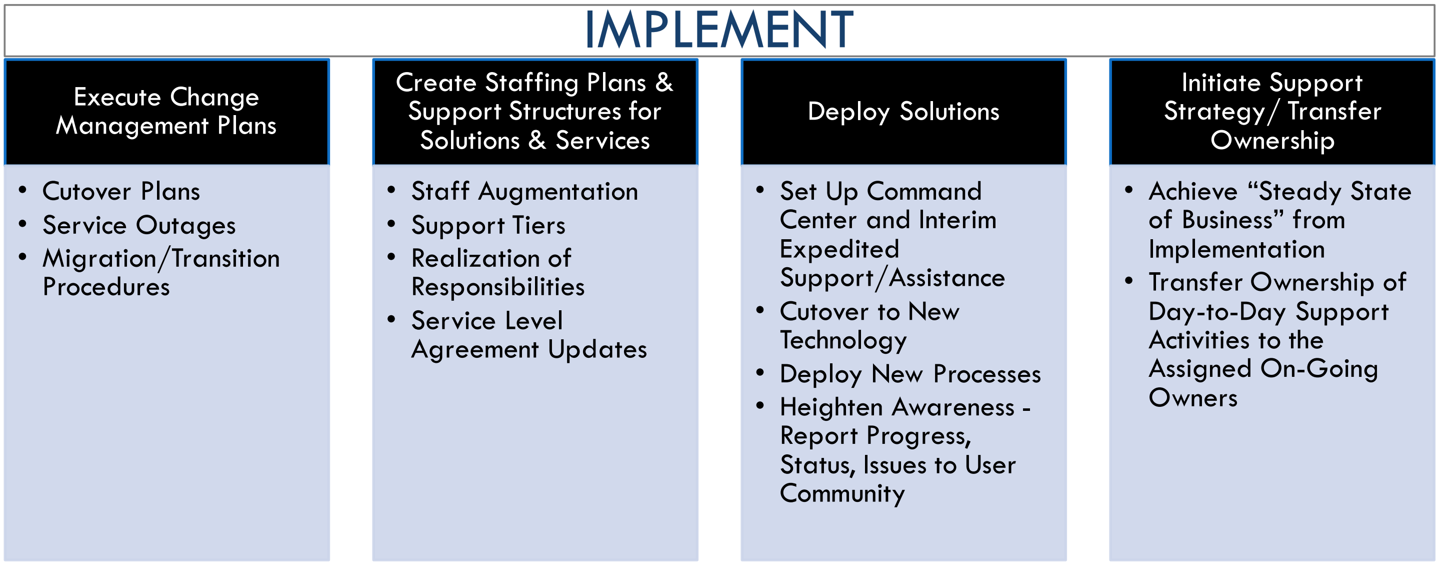
Request & Obtain Funding/ Budgeting

- Operating Budget
- Staffing
- Maintenance Agreements
- Services

Create Change Management Plan

- Operational Processes
- Availability
- Outages/Downtime
- Migration/ Transition Activities

Figure 15 - WAN Development Activities



IMPLEMENT

Execute Change Management Plans

- Cutover Plans
- Service Outages
- Migration/Transition Procedures

Create Staffing Plans & Support Structures for Solutions & Services

- Staff Augmentation
- Support Tiers
- Realization of Responsibilities
- Service Level Agreement Updates

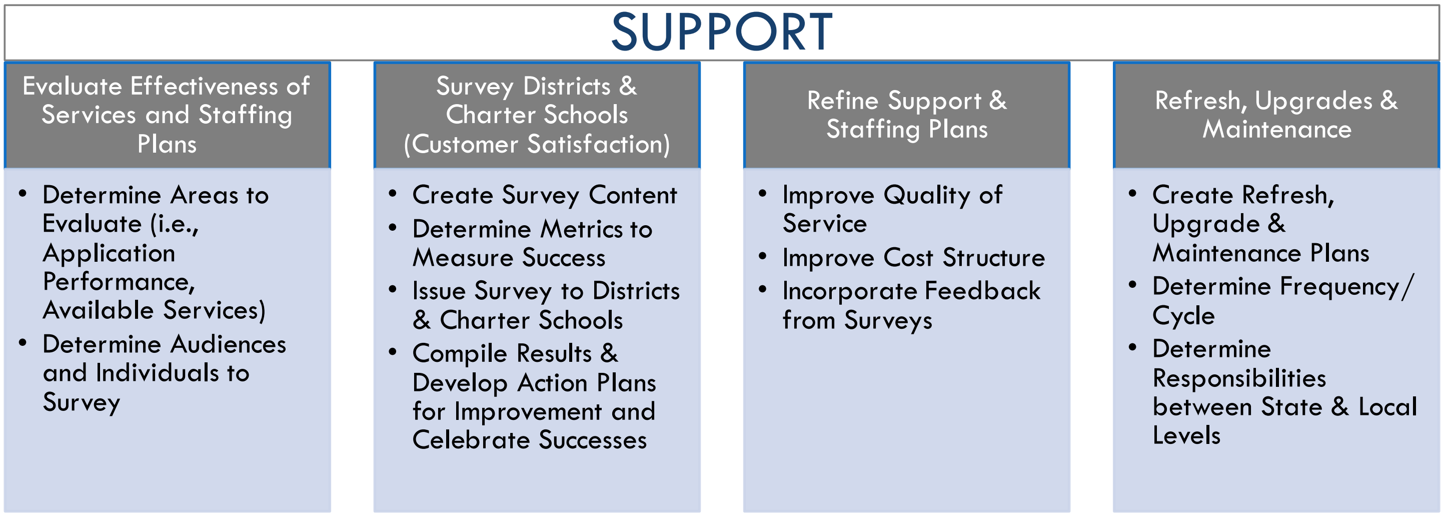
Deploy Solutions

- Set Up Command Center and Interim Expedited Support/Assistance
- Cutover to New Technology
- Deploy New Processes
- Heighten Awareness - Report Progress, Status, Issues to User Community

Initiate Support Strategy/ Transfer Ownership

- Achieve "Steady State of Business" from Implementation
- Transfer Ownership of Day-to-Day Support Activities to the Assigned On-Going Owners

Figure 16 - WAN Implementation Activities



SUPPORT

Evaluate Effectiveness of Services and Staffing Plans

- Determine Areas to Evaluate (i.e., Application Performance, Available Services)
- Determine Audiences and Individuals to Survey

Survey Districts & Charter Schools (Customer Satisfaction)

- Create Survey Content
- Determine Metrics to Measure Success
- Issue Survey to Districts & Charter Schools
- Compile Results & Develop Action Plans for Improvement and Celebrate Successes

Refine Support & Staffing Plans

- Improve Quality of Service
- Improve Cost Structure
- Incorporate Feedback from Surveys

Refresh, Upgrades & Maintenance

- Create Refresh, Upgrade & Maintenance Plans
- Determine Frequency/ Cycle
- Determine Responsibilities between State & Local Levels

Figure 17 - WAN Support Activities

WIRELESS NETWORK (WiFi)

LEA WiFi Overview

UETN does not currently provide WiFi services in the design, development, and maintenance of WiFi networks at the district and charter school levels. All WiFi networks are maintained locally by LEAs.

WiFi OBSERVATIONS AND OPINIONS

WiFi Current State

The data below is a representation of Wi-Fi technology and configuration for districts and charter schools throughout the state. This data was collected by surveying the large majority of districts and charter schools. While not all districts and charter schools are included in this data, it does include a thorough representation of the state.

The survey conducting in November 2015, audited current equipment, bandwidth, wireless solutions and specifications at the LEAs. Survey topics included:

- Wi-Fi infrastructure make / model
- Wi-Fi management solutions
- Count of Wireless Access Points
- Wi-Fi density
- Currently supported Wi-Fi standards

As demonstrated in Figures 18 and 19, charter and district schools use a variety of different solutions to meet their wireless needs, making wireless standards inconsistent amongst them, which equates to inconsistent achievable bandwidth.

Charter Schools

Hardware Manufacturer

This data outlines the wireless infrastructure vendors that are being utilized in charter schools throughout the state.

Brand	Schools Using
Aerohive	0
Aruba	15
Avaya	1
Cisco	10
Extricom	5
Fortinet	1
HP	2
Meraki	4
Meru	2
Motorola	1
Ruckus	8
Ubiquiti	16
Xirrus	36

Bandwidth Allocated per Connection (Mbps)

This data outlines the allocated bandwidth per connection in charter schools throughout the state.

Speed (Mbps)	School Stats
1	15
5	4
10	7
15	4
20	15
25	3
30	5
50	1
60	1
70	2
80	17
100	5
150	5
Unlimited	3

Wireless Management Solution

This data outlines the wireless management solutions used in charter schools throughout the state.

Vendor	Schools Using
Aruba	15
Cisco Prime	2
Cisco WCS	11
Extricom	4
Meraki	1
Motorola	1
None	2
Ruckus Zone Director	7
Ubiquti	12
Xirrus	32

Environment Size

This data outlines the various sized environments in charter schools throughout the state.

Size	Schools Using
Large Enterprise	36
SME	18
SMB	30
SOHO	3

Wireless Standards

This data outlines the wireless standards and technologies currently supported in charter schools throughout the state.

Technology	Schools Using
802.11/ac	29
801.11/ad (WiGig)	3
802.11 a/b	45
802.11 n	71
802.11 g	67
2.4 GHz	43
5 GHz	77

Connections Per Access Point

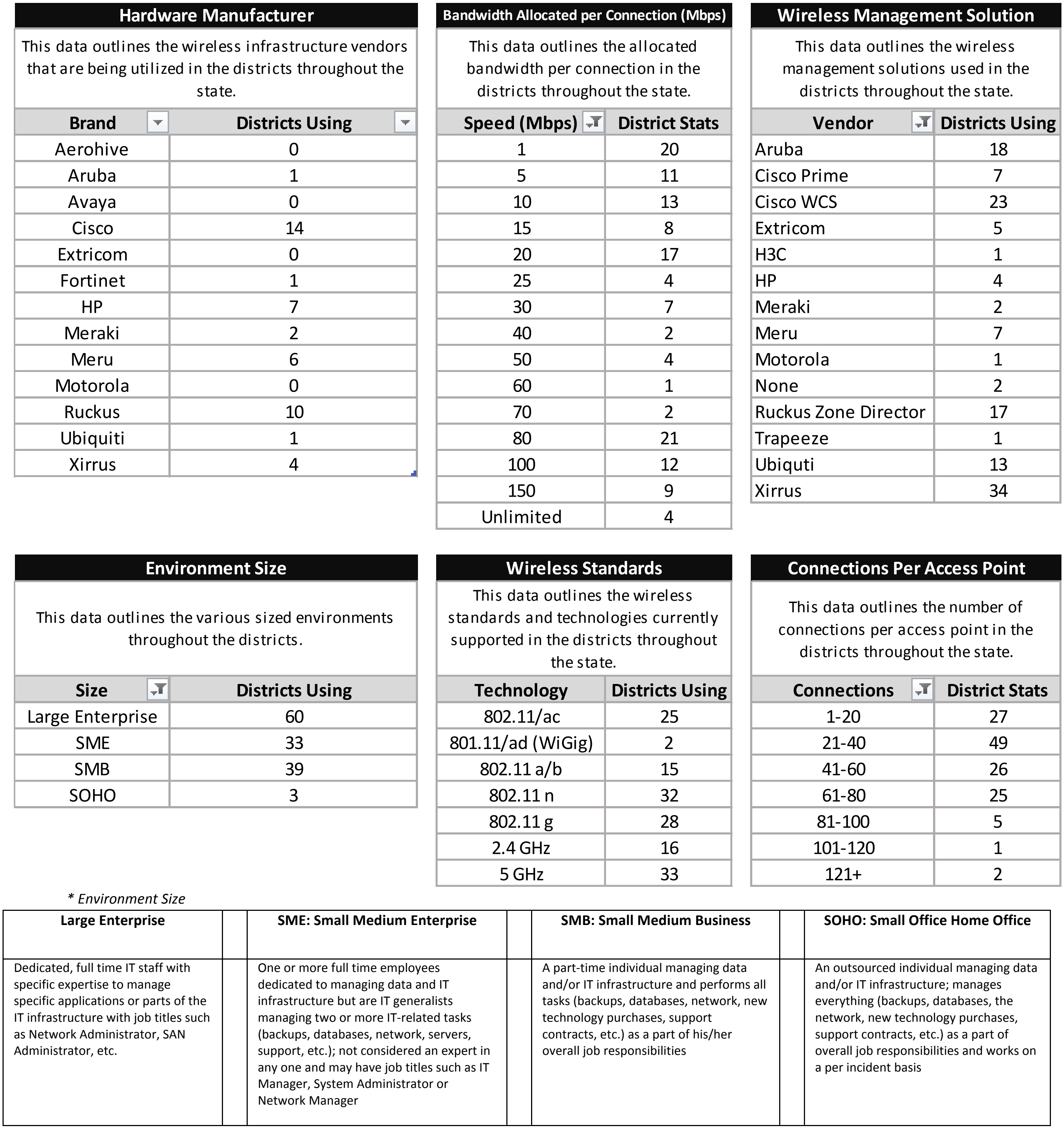
This data outlines the number of connections per access point in charter schools throughout the state.

Connections	School Stats
1-20	27
21-40	49
41-60	26
61-80	25
81-100	5
101-120	1
121+	2

Large Enterprise	**SME: Small Medium Enterprise**	**SMB: Small Medium Business**	**SOHO: Small Office Home Office**
Dedicated, full time IT staff with specific expertise to manage specific applications or parts of the IT infrastructure with job titles such as Network Administrator, SAN Administrator, etc.	One or more full time employees dedicated to managing data and IT infrastructure but are IT generalists managing two or more IT-related tasks (backups, databases, network, servers, support, etc.); not considered an expert in any one and may have job titles such as IT Manager, System Administrator or Network Manager	A part-time individual managing data and/or IT infrastructure and performs all tasks (backups, databases, network, new technology purchases, support contracts, etc.) as a part of his/her overall job responsibilities	An outsourced individual managing data and/or IT infrastructure; manages everything (backups, databases, the network, new technology purchases, support contracts, etc.) as a part of overall job responsibilities and works on a per incident basis

Figure 18 – UTAH LEA Wireless Survey Data - Charter School WiFi

Districts



Hardware Manufacturer	
This data outlines the wireless infrastructure vendors that are being utilized in the districts throughout the state.	
Brand	**Districts Using**
Aerohive	0
Aruba	1
Avaya	0
Cisco	14
Extricom	0
Fortinet	1
HP	7
Meraki	2
Meru	6
Motorola	0
Ruckus	10
Ubiquiti	1
Xirrus	4

Bandwidth Allocated per Connection (Mbps)	
This data outlines the allocated bandwidth per connection in the districts throughout the state.	
Speed (Mbps)	**District Stats**
1	20
5	11
10	13
15	8
20	17
25	4
30	7
40	2
50	4
60	1
70	2
80	21
100	12
150	9
Unlimited	4

Wireless Management Solution	
This data outlines the wireless management solutions used in the districts throughout the state.	
Vendor	**Districts Using**
Aruba	18
Cisco Prime	7
Cisco WCS	23
Extricom	5
H3C	1
HP	4
Meraki	2
Meru	7
Motorola	1
None	2
Ruckus Zone Director	17
Trapeeze	1
Ubiquti	13
Xirrus	34

Environment Size	
This data outlines the various sized environments throughout the districts.	
Size	**Districts Using**
Large Enterprise	60
SME	33
SMB	39
SOHO	3

Wireless Standards	
This data outlines the wireless standards and technologies currently supported in the districts throughout the state.	
Technology	**Districts Using**
802.11/ac	25
801.11/ad (WiGig)	2
802.11 a/b	15
802.11 n	32
802.11 g	28
2.4 GHz	16
5 GHz	33

Connections Per Access Point	
This data outlines the number of connections per access point in the districts throughout the state.	
Connections	**District Stats**
1-20	27
21-40	49
41-60	26
61-80	25
81-100	5
101-120	1
121+	2

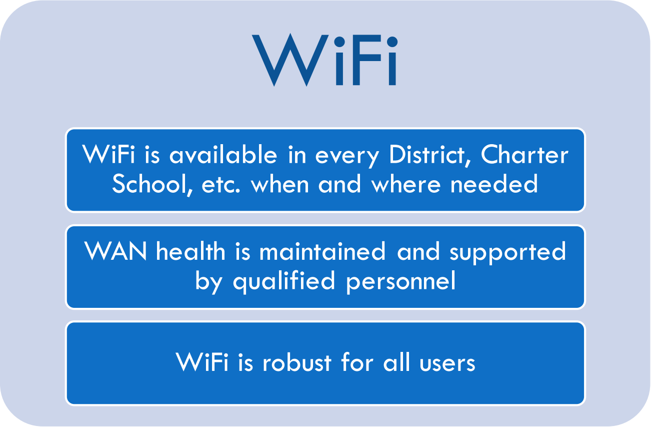
** Environment Size*

Large Enterprise		SME: Small Medium Enterprise		SMB: Small Medium Business		SOHO: Small Office Home Office
Dedicated, full time IT staff with specific expertise to manage specific applications or parts of the IT infrastructure with job titles such as Network Administrator, SAN Administrator, etc.		One or more full time employees dedicated to managing data and IT infrastructure but are IT generalists managing two or more IT-related tasks (backups, databases, network, servers, support, etc.); not considered an expert in any one and may have job titles such as IT Manager, System Administrator or Network Manager		A part-time individual managing data and/or IT infrastructure and performs all tasks (backups, databases, network, new technology purchases, support contracts, etc.) as a part of his/her overall job responsibilities		An outsourced individual managing data and/or IT infrastructure; manages everything (backups, databases, the network, new technology purchases, support contracts, etc.) as a part of overall job responsibilities and works on a per incident basis

Figure 19- UTAH LEA Wireless Survey Data - Districts WiFi

WiFi Objectives

Figure 20 defines the ideal standards of performance and best practices for LEA WiFi. These standards and practices where used to develop the recommendations defined below.



WiFi

WiFi is available in every District, Charter School, etc. when and where needed

WAN health is maintained and supported by qualified personnel

WiFi is robust for all users

Figure 20 -Standards of Performance and Best Practices for LEA WiFi

WiFi Forthcoming Problems to Solve

As new devices and applications are added to the UETN network on each LAN, the demands on WiFi will grow at an increased pace over previous years. UETN is planning a large scale rollout of end user mobile computing devices and software. This will lead to a significant jump in user densities and the capacity health of each location must be examined to determine what is required and what can be achieved in support of this change at each individual location.

LEAs are faced with the challenge of providing increased levels of service, with very little funding. Although in some cases adding more AP's would be useful, this alone is not always helpful. Capacity health, channel overlap, interference, and other factors must also be considered in the new design instead of traditional WiFi designs. The highest impact and probability issues are noted below in Figure 21.

PROBLEMS TO SOLVE

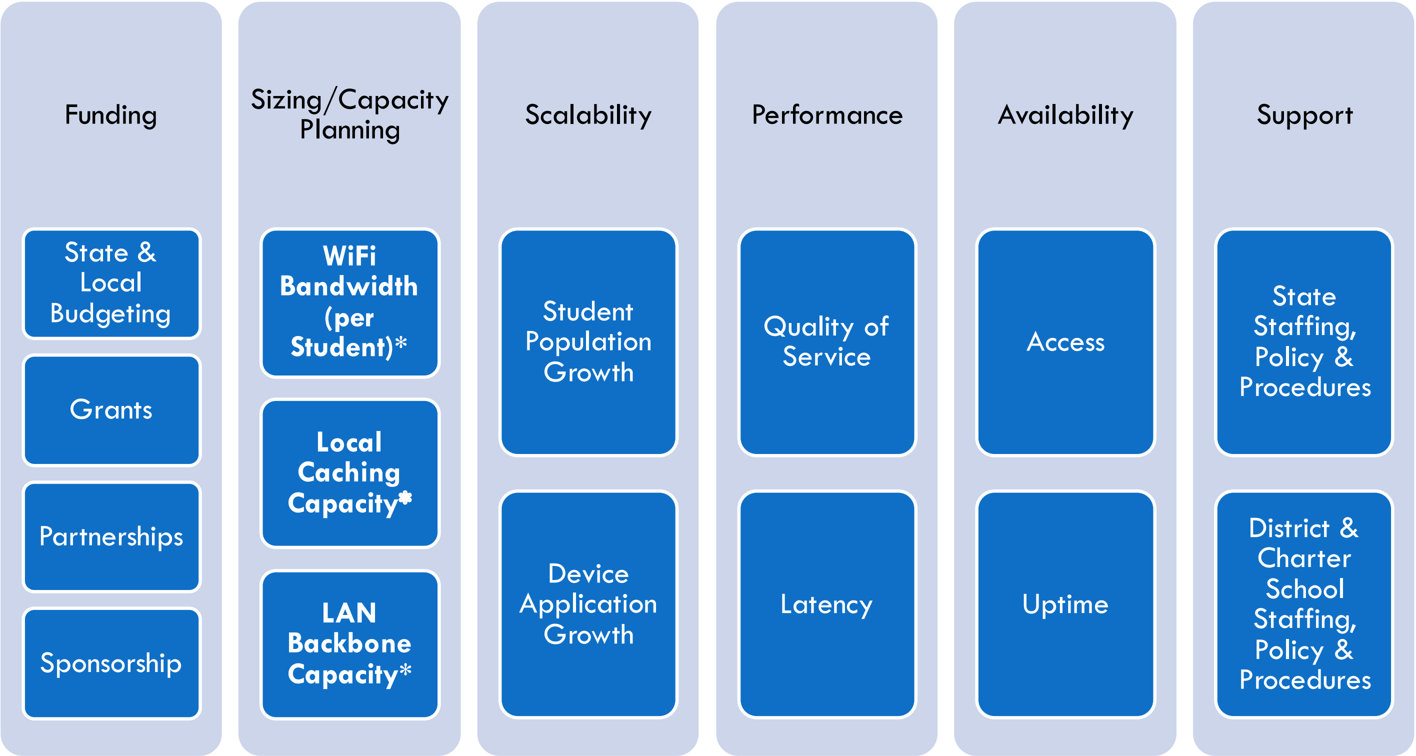


Figure 21 - High Impact and Probability Issues

WiFi Recommendations

Funding

UETN must seek stable, sustainable on-going operational funding sources to ensure technical readiness to meet the vision of the Digital Teaching and Learning Program. It is imperative that UETN shift away from using one-time funding sources for its’ on-going operational expenses. There are a myriad of ways to accomplish this as stated within this section.

Partner/Sponsorships – Now more than ever, it is necessary for UETN to explore creative approaches for funding and resources through partnerships, grants and corporate sponsorships. Strategic sourcing plays a vital role in the success of cost containment through the development of initiatives such as entering into case study agreements and research programs with corporate and private sponsors.

Economies of Scale from Procurement Standards – Harnessing the value of strategic relationships is not the only avenue for cost containment. Establishing “tiered” networking standards of hardware, software and services across the state for districts and charter schools allows procurement to negotiate contracts that benefit from the economies of scale for bulk purchasing from preferred providers.

WiFi Capacity Planning, Scalability, Performance, Availability

Improved School Cabling & Density Wireless Design – Some schools do not have a single CAT 5e cable in classrooms. For High Speed WiFi in the classrooms, 2 or more cable connections with Access Points (APs) will likely be required depending on the size, education content delivered and number of students in the classroom. As a sizing example only for illustration, if we assume High Definition Video Learning requires 20 Mbps per student, times 30 students, then approximately three Wireless Access Points are needed to support performance over a 30' X 30' classroom. This in turn requires three cables, which requires collateral equipment in data closets (switches, routers, etc.). If an as-built cable inventory does not exist for each school, it should be developed for analysis and decision-making purposes during detailed WiFi design for each school.

Support

Additional Local Staff – With added devices and users, the need for real-time correction of issues will be required along with additional staffing based on multi-tiered technical support models to manage and maintain security and filtering solutions. Although all districts and charters have some support structure for their schools, the level of support varies and does not address the increasing growth of technology footprints at local levels.

Continued Training and Mentoring Programs – Whether delivered by UETN or facilitated by UETN, training is a fundamental building block of a healthy network. UETN maintains multiple training and mentoring programs. These not only benefit the district and charter school's technology staff, but also UETN's state-wide WAN staff by engaging to understand specific problems the districts and charter schools encounter. This translates into knowledge imparted upon design activities for solutions and policies of the enterprise.

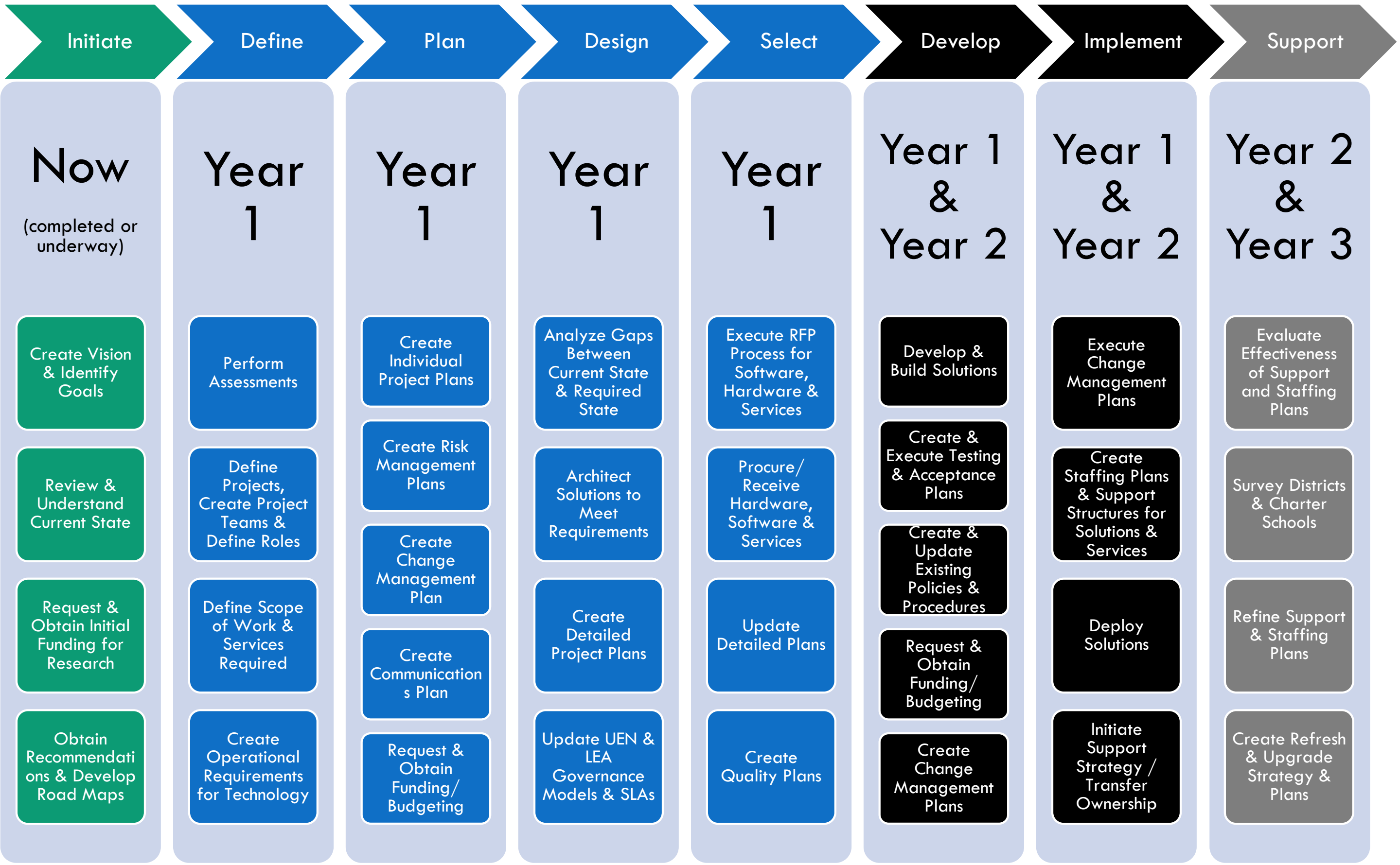
Standardization of Policies and Practices – Standardization of policies and practices facilitates consistent experiences with technology and improved efficiencies with support.

WiFi Road Map

Below is the proposed Road Map for LEA's WiFi growth (Figure 22). The Initiate column with the timeframe labeled "Now" reflects activities that may or should be underway presently.

It is not expected that each LEA will progress through each phase of work at the same pace. Instead, they will execute individual applicable tasks based on its own specific constraints, dependencies, funding and prioritization.

WiFi Road Map



Initiate – Now (completed or underway)
- Create Vision & Identify Goals
- Review & Understand Current State
- Request & Obtain Initial Funding for Research
- Obtain Recommendations & Develop Road Maps

Define – Year 1
- Perform Assessments
- Define Projects, Create Project Teams & Define Roles
- Define Scope of Work & Services Required
- Create Operational Requirements for Technology

Plan – Year 1
- Create Individual Project Plans
- Create Risk Management Plans
- Create Change Management Plan
- Create Communications Plan
- Request & Obtain Funding/Budgeting

Design – Year 1
- Analyze Gaps Between Current State & Required State
- Architect Solutions to Meet Requirements
- Create Detailed Project Plans
- Update UEN & LEA Governance Models & SLAs

Select – Year 1
- Execute RFP Process for Software, Hardware & Services
- Procure/Receive Hardware, Software & Services
- Update Detailed Plans
- Create Quality Plans

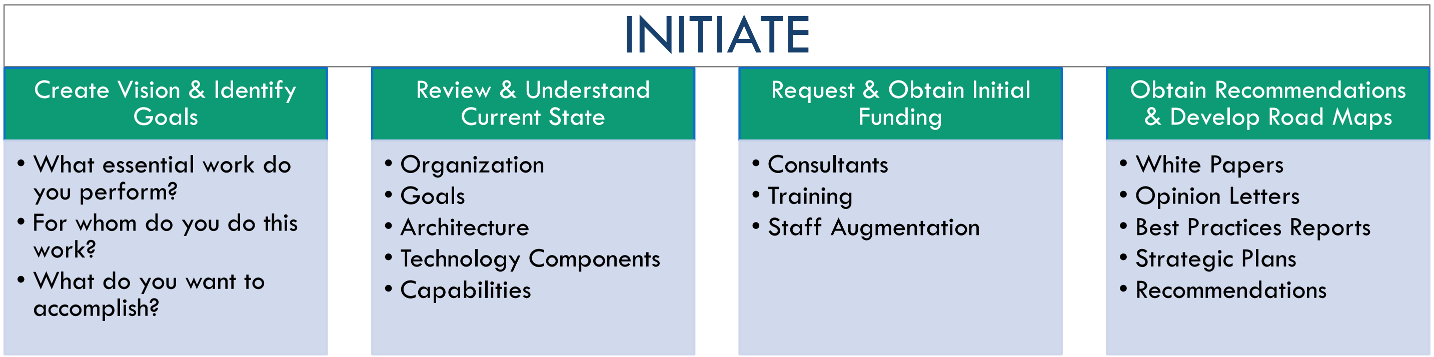
Develop – Year 1 & Year 2
- Develop & Build Solutions
- Create & Execute Testing & Acceptance Plans
- Create & Update Existing Policies & Procedures
- Request & Obtain Funding/Budgeting
- Create Change Management Plans

Implement – Year 1 & Year 2
- Execute Change Management Plans
- Create Staffing Plans & Support Structures for Solutions & Services
- Deploy Solutions
- Initiate Support Strategy / Transfer Ownership

Support – Year 2 & Year 3
- Evaluate Effectiveness of Support and Staffing Plans
- Survey Districts & Charter Schools
- Refine Support & Staffing Plans
- Create Refresh & Upgrade Strategy & Plans

Figure 22 - WiFi Road Map

WiFi High Level Activities



INITIATE

Create Vision & Identify Goals

- What essential work do you perform?
- For whom do you do this work?
- What do you want to accomplish?

Review & Understand Current State

- Organization
- Goals
- Architecture
- Technology Components
- Capabilities

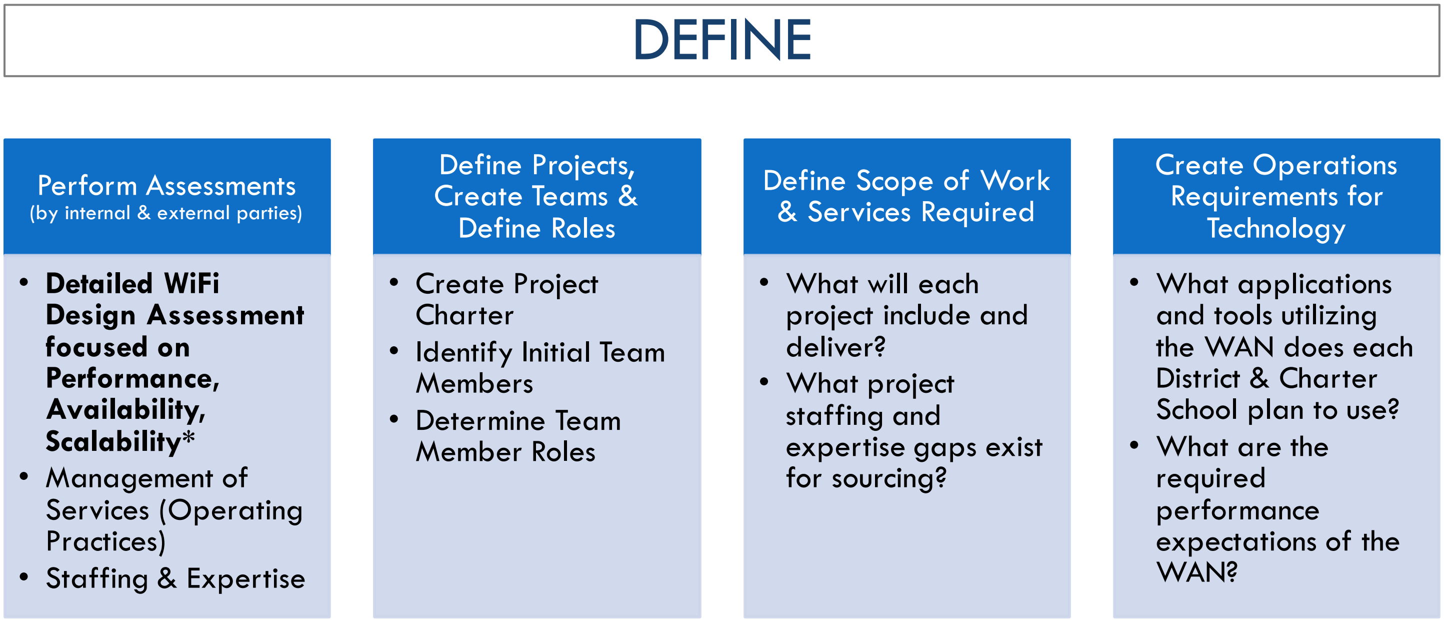
Request & Obtain Initial Funding

- Consultants
- Training
- Staff Augmentation

Obtain Recommendations & Develop Road Maps

- White Papers
- Opinion Letters
- Best Practices Reports
- Strategic Plans
- Recommendations

Figure 23 - WiFi Initiation Activities



DEFINE

Perform Assessments (by internal & external parties)

- **Detailed WiFi Design Assessment focused on Performance, Availability, Scalability***
- Management of Services (Operating Practices)
- Staffing & Expertise

Define Projects, Create Teams & Define Roles

- Create Project Charter
- Identify Initial Team Members
- Determine Team Member Roles

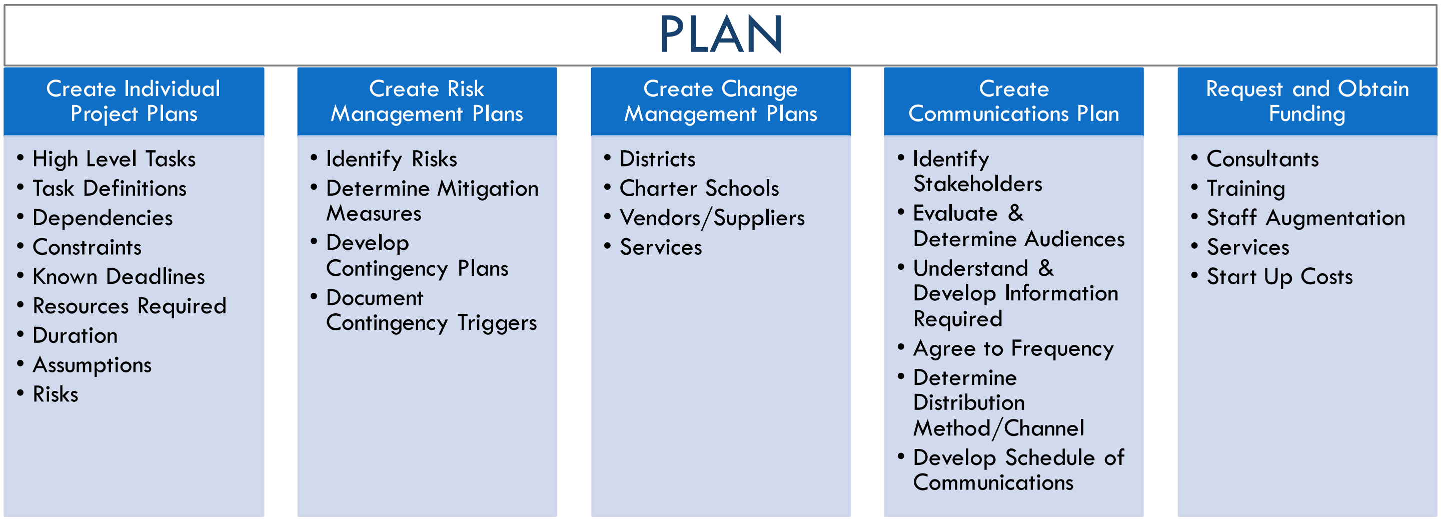
Define Scope of Work & Services Required

- What will each project include and deliver?
- What project staffing and expertise gaps exist for sourcing?

Create Operations Requirements for Technology

- What applications and tools utilizing the WAN does each District & Charter School plan to use?
- What are the required performance expectations of the WAN?

Figure 24 - WiFi Definition Activities



PLAN

Create Individual Project Plans

- High Level Tasks
- Task Definitions
- Dependencies
- Constraints
- Known Deadlines
- Resources Required
- Duration
- Assumptions
- Risks

Create Risk Management Plans

- Identify Risks
- Determine Mitigation Measures
- Develop Contingency Plans
- Document Contingency Triggers

Create Change Management Plans

- Districts
- Charter Schools
- Vendors/Suppliers
- Services

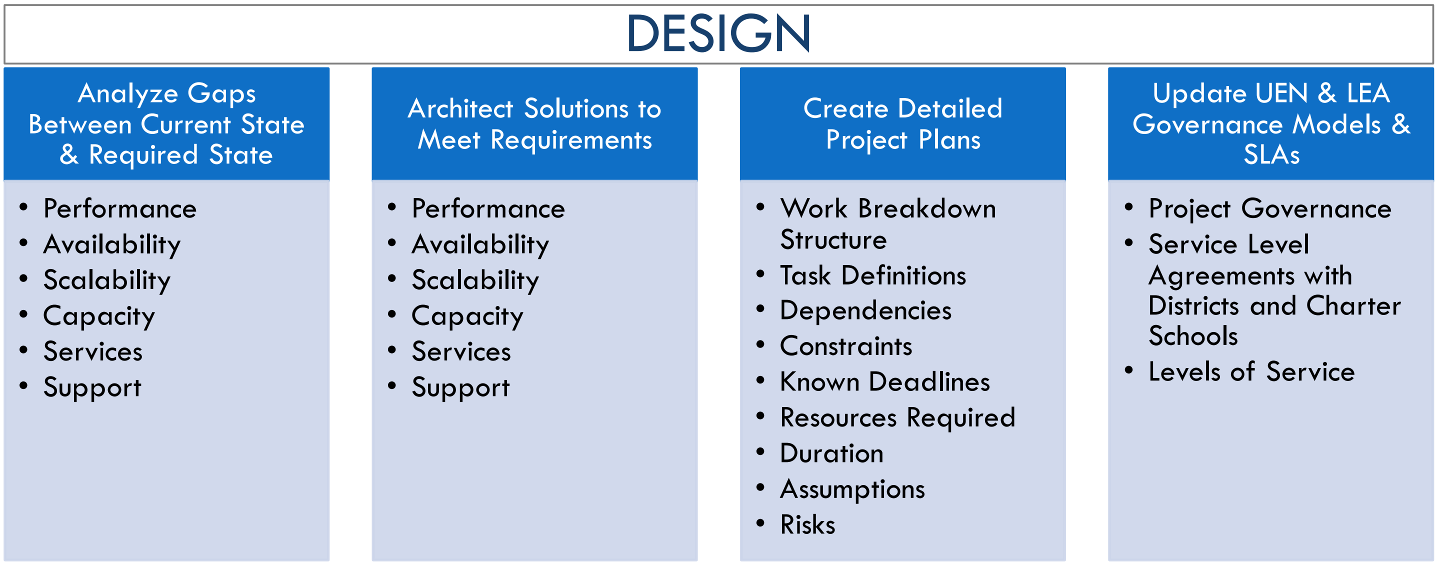
Create Communications Plan

- Identify Stakeholders
- Evaluate & Determine Audiences
- Understand & Develop Information Required
- Agree to Frequency
- Determine Distribution Method/Channel
- Develop Schedule of Communications

Request and Obtain Funding

- Consultants
- Training
- Staff Augmentation
- Services
- Start Up Costs

Figure 25 - WiFi Planning Activities



DESIGN

Analyze Gaps Between Current State & Required State

- Performance
- Availability
- Scalability
- Capacity
- Services
- Support

Architect Solutions to Meet Requirements

- Performance
- Availability
- Scalability
- Capacity
- Services
- Support

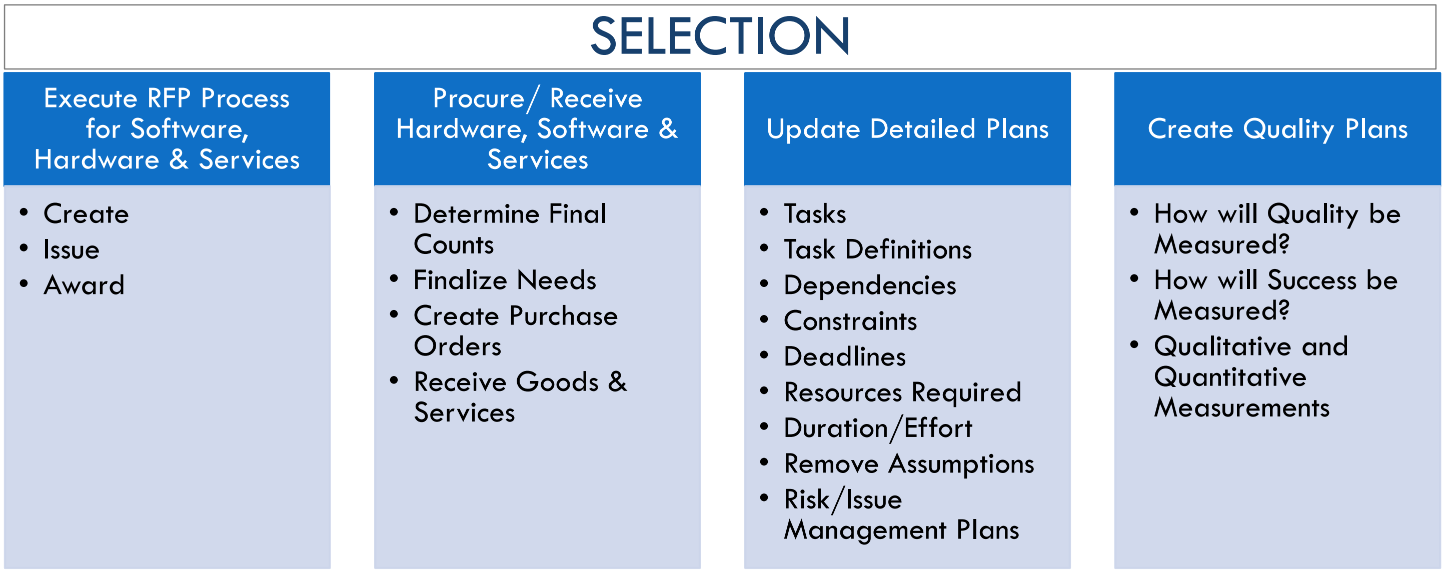
Create Detailed Project Plans

- Work Breakdown Structure
- Task Definitions
- Dependencies
- Constraints
- Known Deadlines
- Resources Required
- Duration
- Assumptions
- Risks

Update UEN & LEA Governance Models & SLAs

- Project Governance
- Service Level Agreements with Districts and Charter Schools
- Levels of Service

Figure 26 - WiFi Design Activities



SELECTION

Execute RFP Process for Software, Hardware & Services

- Create
- Issue
- Award

Procure/ Receive Hardware, Software & Services

- Determine Final Counts
- Finalize Needs
- Create Purchase Orders
- Receive Goods & Services

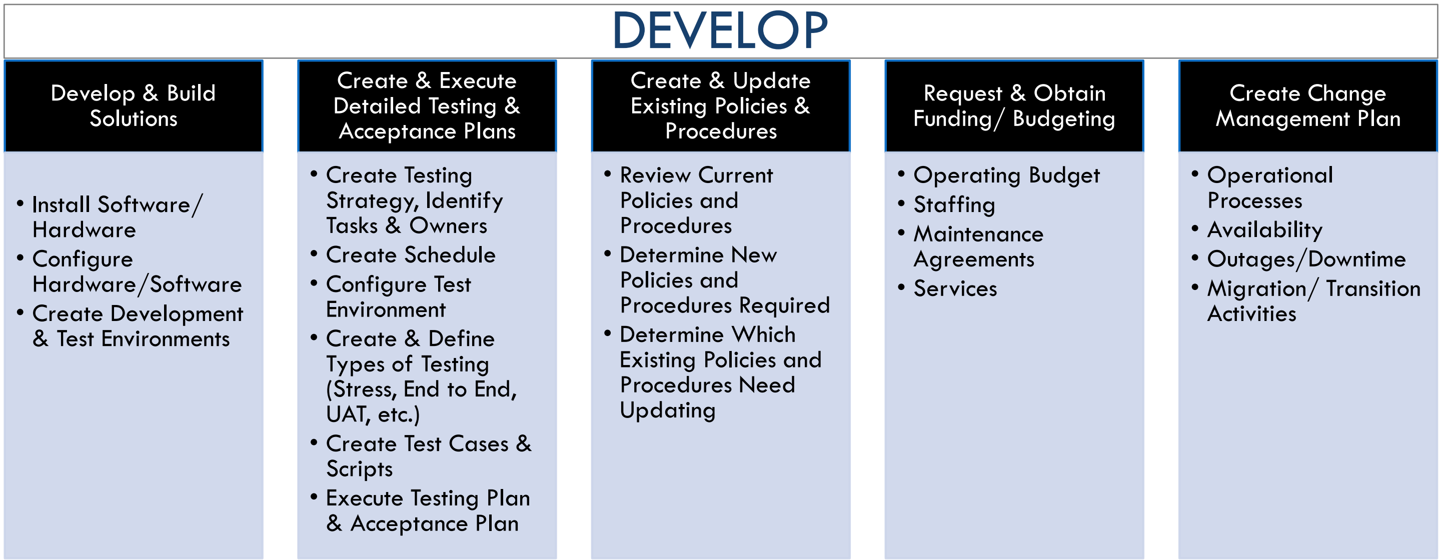
Update Detailed Plans

- Tasks
- Task Definitions
- Dependencies
- Constraints
- Deadlines
- Resources Required
- Duration/Effort
- Remove Assumptions
- Risk/Issue Management Plans

Create Quality Plans

- How will Quality be Measured?
- How will Success be Measured?
- Qualitative and Quantitative Measurements

Figure 27 - WiFi Selection Activities



DEVELOP

Develop & Build Solutions

- Install Software/ Hardware
- Configure Hardware/Software
- Create Development & Test Environments

Create & Execute Detailed Testing & Acceptance Plans

- Create Testing Strategy, Identify Tasks & Owners
- Create Schedule
- Configure Test Environment
- Create & Define Types of Testing (Stress, End to End, UAT, etc.)
- Create Test Cases & Scripts
- Execute Testing Plan & Acceptance Plan

Create & Update Existing Policies & Procedures

- Review Current Policies and Procedures
- Determine New Policies and Procedures Required
- Determine Which Existing Policies and Procedures Need Updating

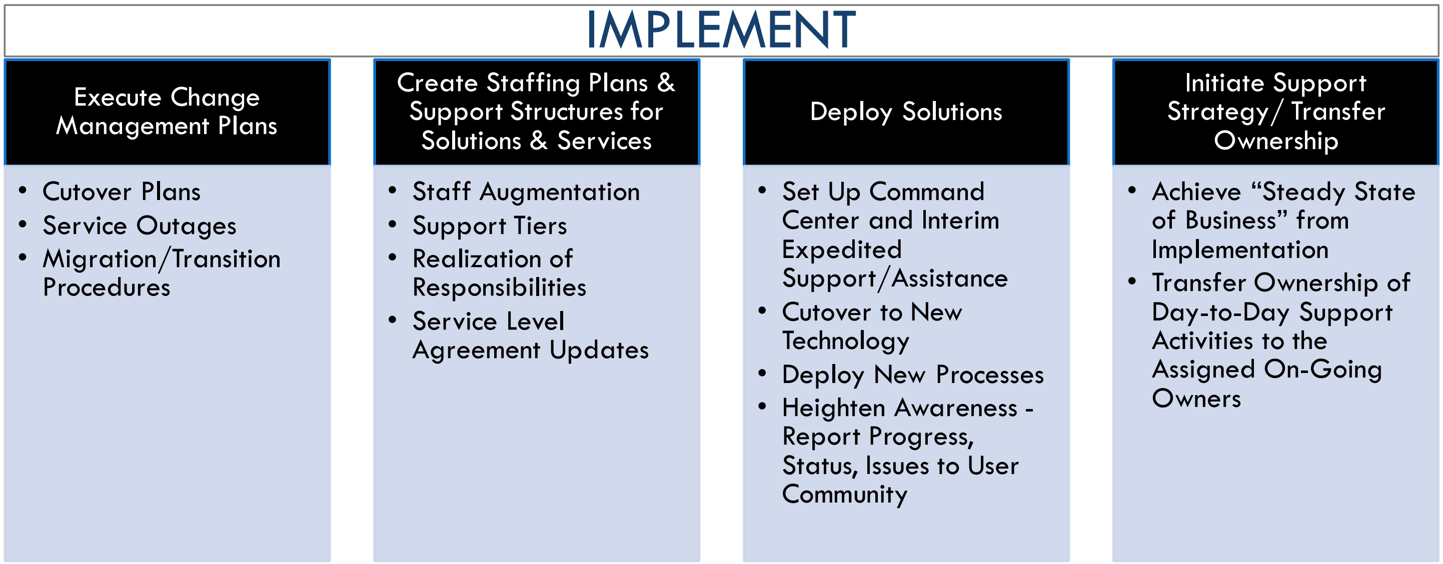
Request & Obtain Funding/ Budgeting

- Operating Budget
- Staffing
- Maintenance Agreements
- Services

Create Change Management Plan

- Operational Processes
- Availability
- Outages/Downtime
- Migration/ Transition Activities

Figure 28 - WiFi Development Activities



IMPLEMENT

Execute Change Management Plans

- Cutover Plans
- Service Outages
- Migration/Transition Procedures

Create Staffing Plans & Support Structures for Solutions & Services

- Staff Augmentation
- Support Tiers
- Realization of Responsibilities
- Service Level Agreement Updates

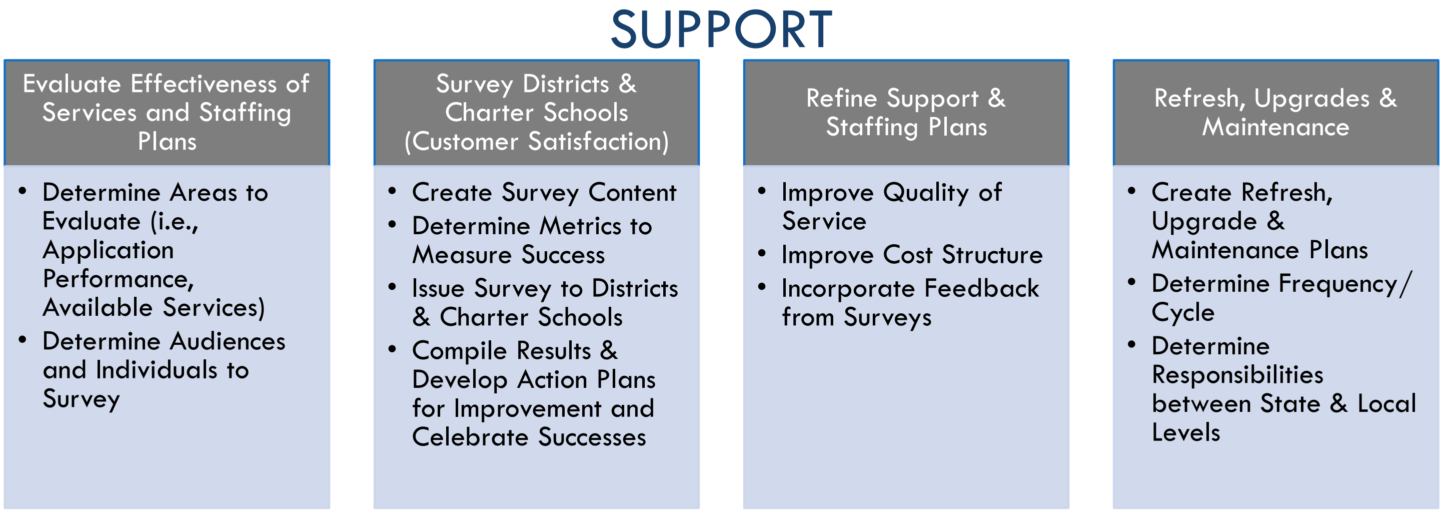
Deploy Solutions

- Set Up Command Center and Interim Expedited Support/Assistance
- Cutover to New Technology
- Deploy New Processes
- Heighten Awareness - Report Progress, Status, Issues to User Community

Initiate Support Strategy/ Transfer Ownership

- Achieve “Steady State of Business” from Implementation
- Transfer Ownership of Day-to-Day Support Activities to the Assigned On-Going Owners

Figure 29 - WiFi Implementation Activities



SUPPORT

Evaluate Effectiveness of Services and Staffing Plans

- Determine Areas to Evaluate (i.e., Application Performance, Available Services)
- Determine Audiences and Individuals to Survey

Survey Districts & Charter Schools (Customer Satisfaction)

- Create Survey Content
- Determine Metrics to Measure Success
- Issue Survey to Districts & Charter Schools
- Compile Results & Develop Action Plans for Improvement and Celebrate Successes

Refine Support & Staffing Plans

- Improve Quality of Service
- Improve Cost Structure
- Incorporate Feedback from Surveys

Refresh, Upgrades & Maintenance

- Create Refresh, Upgrade & Maintenance Plans
- Determine Frequency/ Cycle
- Determine Responsibilities between State & Local Levels

Figure 30 - WiFi Support Activities

SECURITY AND CONTENT FILTERING

Security and Content Filtering Overview

UETN provides networking services to design, develop, build, and maintain the statewide security and internet filtering solutions offered. It also provides support services, such as advanced technology management and troubleshooting.

UETN Security Services currently include:

- **Intrusion Prevention** – a preemptive approach to network security used to identify ***potential*** threats and respond to them swiftly
- **Intrusion Detection** – the process of monitoring network or system traffic for malicious activities or policy violations to produce reports for analysis
- **Distributed Denial of Service (DDoS) Mitigation** - is a set of techniques for resisting distributed denial-of-service (DDoS) attacks on networks attached to the Internet by protecting the target and relay networks
- **Vulnerability Assessment/Penetration Testing** – active test(s) run on systems or devices connected to the network (wired or wireless) to check the current configurations of systems against publicly known vulnerabilities and gauging the level of exposure while determining the overall effectiveness of current controls
- **Firewalls** – a network security system (hardware & software) that monitors and controls the incoming and outgoing network traffic based on predetermined security rules (establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted)

UETN Content Filtering Services include:

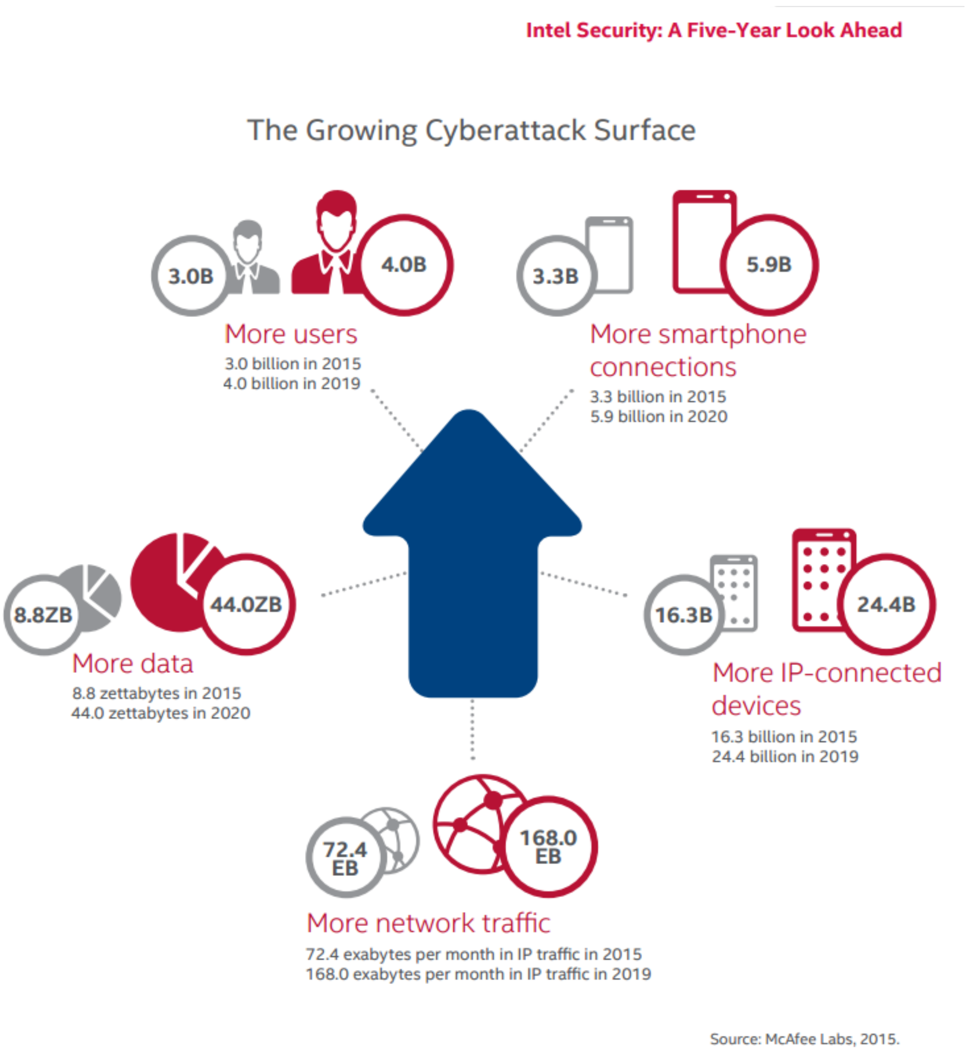
- **Internet Content Filtering** – screening and excluding access or availability to Web pages
    - Adult Content
    - Inappropriate Content (social media, chat, gaming, etc.)
    - Malicious Content (spyware, malware, viruses, etc.)

SECURITY AND CONTENT FILTERING OBSERVATIONS AND OPINIONS

Security and Content Filtering Current State

UETN's security and content filtering services and solutions have been designed, developed, provided, and supported to follow best practices and are flexible to meet current needs.

Additional functionality necessary may not be present or even fully understood based on the demands of SB 222 and the ever-changing technology landscape at the state and local levels. Future demands will be required on short notice in the Security and Content Filtering Domains with expected swift responses to incidents and issues. With the increase of devices and users consuming the service, areas of improvement must be considered and individually analyzed. These will be based on compliance, legal, and regulatory drivers, as well as operational requirements from the districts and charter schools.



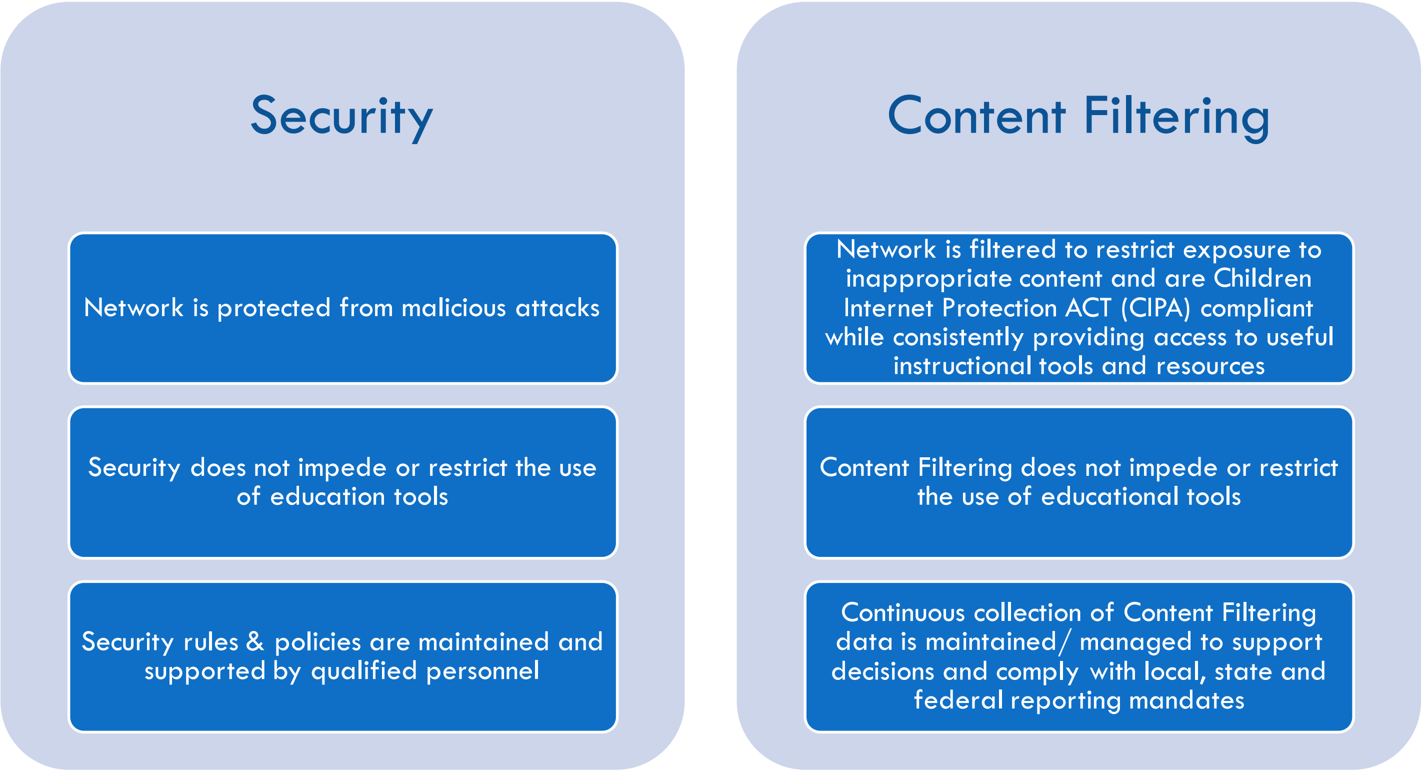
Source: McAfee Labs, 2015.

Figure 31 - The Growing Cyberattack Surface

As UETN technical staff are highly capable and subject matter experts in this field, they are already researching and planning for the future. Although recommendations are made for some work not already underway by UETN, most of the security and content filtering problems and recommendations noted below align with in-flight initiatives by UETN. These initiatives will be explored in future project status reports.

Security & Content Filtering Objectives

The Figure below shows ideal standards of performance and best practices for UETN/LEA Security and Content Filtering. The Security and Content Filtering recommendations were developed based on these standards and practices.



Security

Network is protected from malicious attacks

Security does not impede or restrict the use of education tools

Security rules & policies are maintained and supported by qualified personnel

Content Filtering

Network is filtered to restrict exposure to inappropriate content and are Children Internet Protection ACT (CIPA) compliant while consistently providing access to useful instructional tools and resources

Content Filtering does not impede or restrict the use of educational tools

Continuous collection of Content Filtering data is maintained/ managed to support decisions and comply with local, state and federal reporting mandates

Figure 32 - Standards of Performance and Best Practices for UETN/LEA Security and Content Filtering

Security and Content Filtering Forthcoming Problems to Solve

"Five years ago, we thought that more users, more data, more devices, and more clouds were creating a perfect security storm of threats and vulnerabilities. Many of those predictions came true, but they were only the leading indicators of a much bigger storm, the acceleration of "more.""[7] –McAfee Labs

Mobility is blurring the concept of the "network perimeter" due to work occurring outside the confines of trusted networks, along with the explosion of device types coupled with "free" services.

[7] McAfee Labs, "2016 Threats Predictions" - http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf

PROBLEMS TO SOLVE

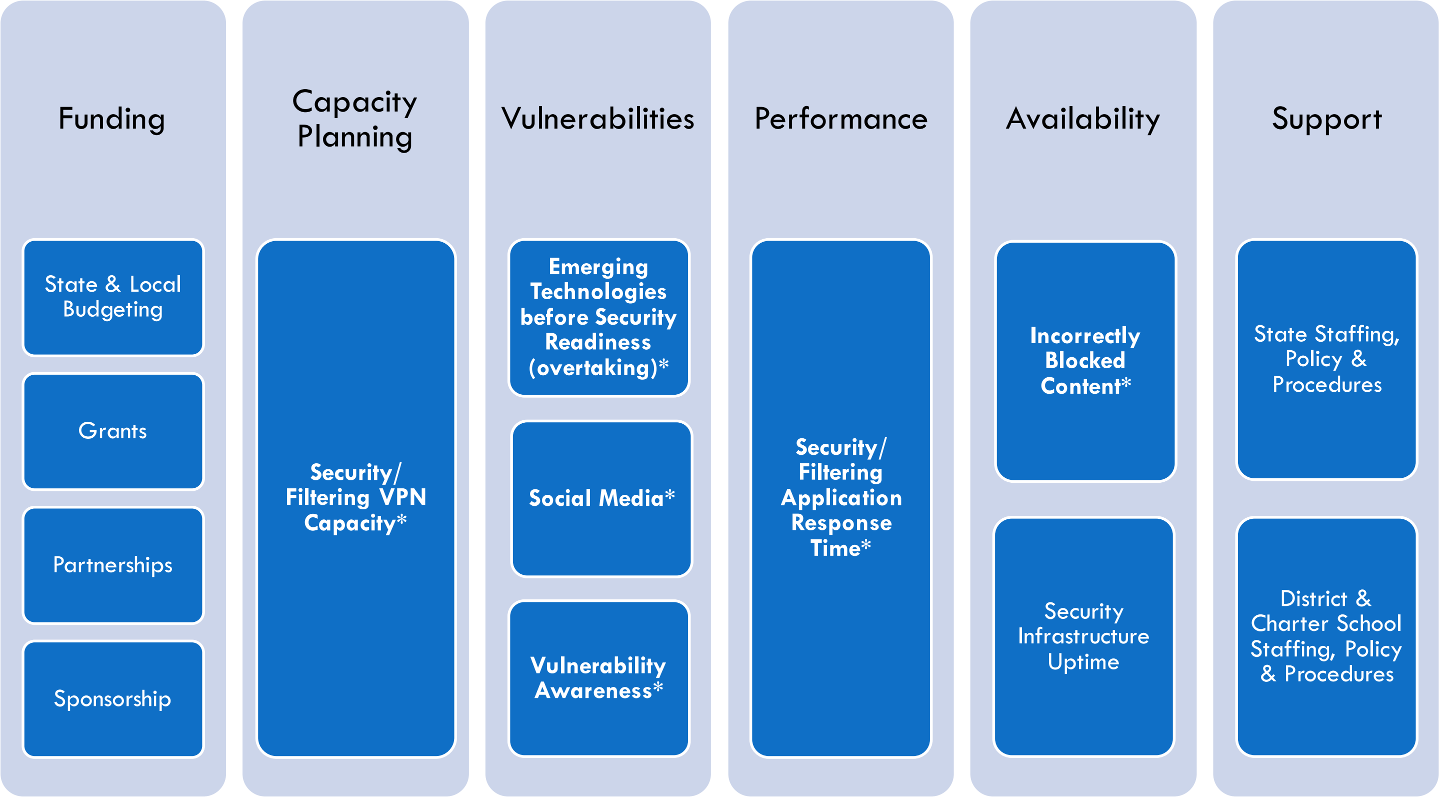

Funding
State & Local Budgeting
Grants
Partnerships
Sponsorship
Capacity Planning
Security/ Filtering VPN Capacity*
Vulnerabilities
Emerging Technologies before Security Readiness (overtaking)*
Social Media*
Vulnerability Awareness*
Performance
Security/ Filtering Application Response Time*
Availability
Incorrectly Blocked Content*
Security Infrastructure Uptime
Support
State Staffing, Policy & Procedures
District & Charter School Staffing, Policy & Procedures

Figure 33 - Security and Content Filtering Forthcoming Problems to Solve

Security & Content Filtering Recommendations

Funding

UETN must seek stable, sustainable on-going operational funding sources to ensure technical readiness to meet the vision of the Digital Teaching and Learning Program. It is imperative that UETN shift away from using one-time funding sources for its' on-going operational expenses. There are a myriad of ways to accomplish this as stated within this section.

Security and Content Filtering Solutions require regular monitoring, management, analysis and change to keep up with the latest vulnerability, attack, threat and filtering requests. Too often a preventable incident occurs that heightens an organization's awareness, such as an outage, interruption of service or, worse, compromised personal data. This can create a cycle of reactive funding rather than proactive approval of recurring budget and grant requests.

Strategic Partner/Sponsorships - Now more than ever, it is necessary for UETN to explore creative approaches for funding and resources through partnerships, grants and corporate sponsorships. Strategic sourcing plays a vital role in the success of cost containment through the development of initiatives such as entering into case study agreements, lab experiments and research programs with corporate and private sponsors.

Standards for Procurement Economies of Scale – Harnessing the value of strategic relationships is not the only avenue for cost containment. Establishing “tiered” networking standards of hardware, software and services across the state for districts and charter schools allows procurement to negotiate contracts that benefit from the economies of scale for bulk purchasing from preferred providers.

Capacity Planning

Expanded Use of Virtual Private Networks - With the volume of new mobile devices to be on boarded in all schools and the constraint of keeping them secure and safe both inside and out of the classroom the task seems close to unachievable without giving up some flexibility for each district and charter. Programs and protocols that may be treated as exceptions include BYOD (bring your own device) and split VPN tunneling until affordable management tools become mainstream.

Vulnerabilities

UETN Controls Standards – As a part of standards for procurement cost containment, standards also help control security. All devices connected to the WAN and LANs, especially security appliances and equipment, should conform to existing standards. If it is not recognized on a UETN standards document (existing or under development), it should follow a formal review and approval process by UETN to certify.

Security Incident and Event Management (SIEM) – As a part of the security toolkit, SIEM should become a core practice. Through constant monitoring, this type of tool establishes a baseline of routine behaviors, learning regular patterns by legitimate users and alerts management when expected routines are not followed. Although this technology is in the early stages, it is anticipated that it will mature very quickly based on market demands to extract meaningful and actionable information.

Vulnerability Assessment (VA) – As a proactive measure for securing your organization, a formal routine practice must be maintained to assess, identify and implement changes to remediate vulnerabilities. Vulnerability assessments are an important mechanism through which organizations can identify potential security exposures and have a process in place to correct any deficiencies. Routine self-assessments provide a good picture of how security is managed and improved over time and help to identify areas most in need of attention.[8]

Performance

Robust Security Appliance CPUs – Security monitoring and enforcement are computationally intensive. As such, security appliances at the local levels should not be overlooked when planning for performance. Utilizing all functionality on these devices - such as complex filtering, Deep Packet Inspection (DPI), and Intrusion Detection Signature (IDS) signature matching - can often double the CPU and memory demands on security appliances, bringing application performance to its knees. Other measures to improve performance would be to decrease computational intensive features not required, when available as an option.

[8] SANS Institute Reading Room, “Vulnerability Assessments: The Pro-active Steps to Secure Your Organization - https://www.sans.org/reading-room/whitepapers/threats/vulnerability-assessments-pro-active-steps-secure-organization-453

Support

Additional Local Staff – With added devices and users, the need for real time correction of issues will require additional staffing based on a multi-tiered technical support model to manage and maintain security and filtering solutions. Although all districts and charters have some support structure for their schools, the level of support varies and does not address the upcoming growth of technology footprints at local levels.

Continued Training and Mentoring Programs – Whether delivered or facilitated by UETN training is a fundamental building block of a healthy network. UETN maintains multiple training and mentoring programs which not only assist the district and charter school's technology staff but also UETN state wide WAN staff by engaging to understand specific problems the districts and charter schools encounter. This translates into knowledge imparted upon design activities for solutions and policies of the enterprise.

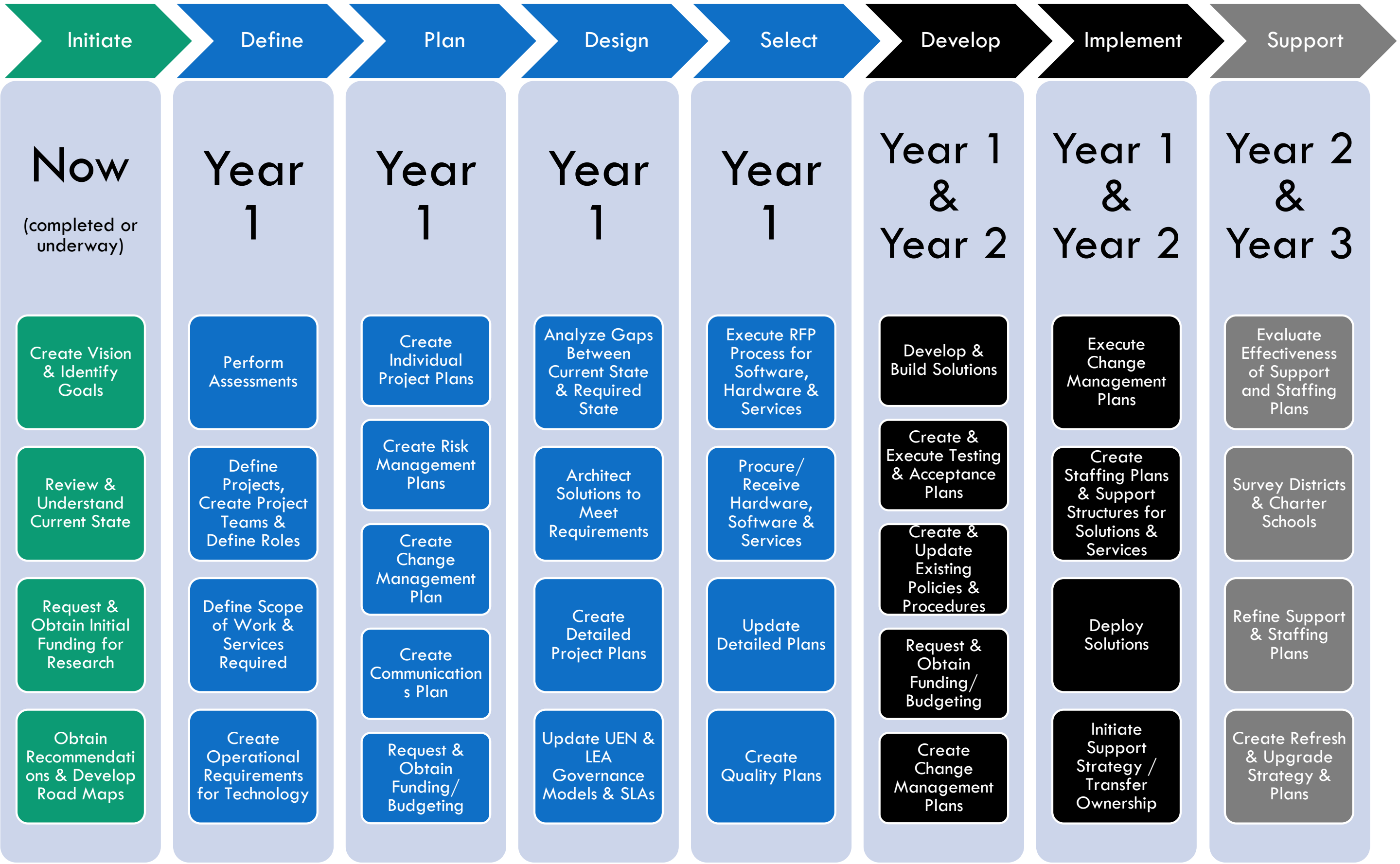
Standardization of Policies and Practices – By continued efforts with district and charter schools, standardization of policies and practices facilitates consistent experiences with technology and improved efficiencies with support.

Security & Content Filtering Road Map

Below is the proposed Road Map for the UETN and LEA Security & Content Filtering Program (Figure 34). The Initiate column with the timeframe labeled “Now” reflects activities that are underway.

It is not expected that each individual project will progress through each phase of work at the same pace. Instead, they will execute individual applicable tasks based on its own specific constraints, dependencies, funding and prioritization.

Security and Content Filtering Road Map



Initiate: Now (completed or underway)
- Create Vision & Identify Goals
- Review & Understand Current State
- Request & Obtain Initial Funding for Research
- Obtain Recommendations & Develop Road Maps

Define: Year 1
- Perform Assessments
- Define Projects, Create Project Teams & Define Roles
- Define Scope of Work & Services Required
- Create Operational Requirements for Technology

Plan: Year 1
- Create Individual Project Plans
- Create Risk Management Plans
- Create Change Management Plan
- Create Communications Plan
- Request & Obtain Funding/ Budgeting

Design: Year 1
- Analyze Gaps Between Current State & Required State
- Architect Solutions to Meet Requirements
- Create Detailed Project Plans
- Update UEN & LEA Governance Models & SLAs

Select: Year 1
- Execute RFP Process for Software, Hardware & Services
- Procure/ Receive Hardware, Software & Services
- Update Detailed Plans
- Create Quality Plans

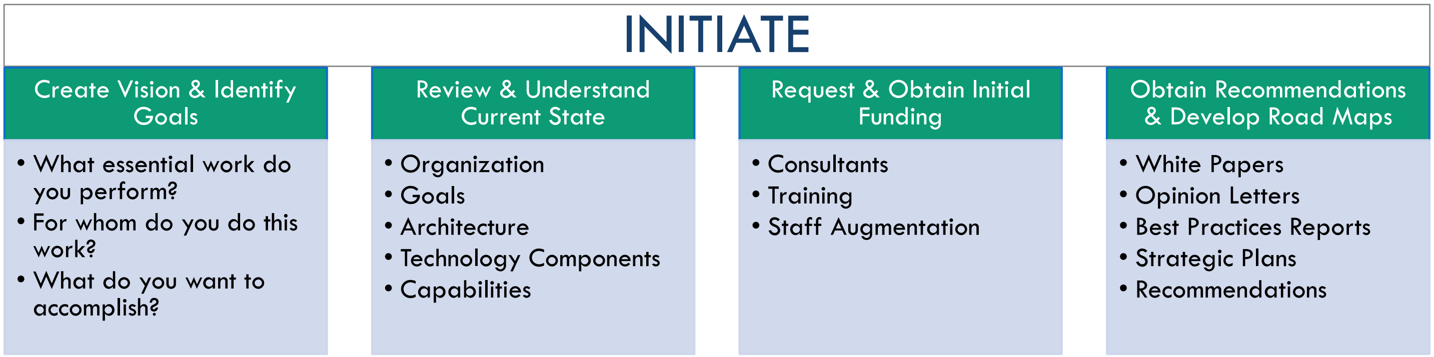
Develop: Year 1 & Year 2
- Develop & Build Solutions
- Create & Execute Testing & Acceptance Plans
- Create & Update Existing Policies & Procedures
- Request & Obtain Funding/ Budgeting
- Create Change Management Plans

Implement: Year 1 & Year 2
- Execute Change Management Plans
- Create Staffing Plans & Support Structures for Solutions & Services
- Deploy Solutions
- Initiate Support Strategy / Transfer Ownership

Support: Year 2 & Year 3
- Evaluate Effectiveness of Support and Staffing Plans
- Survey Districts & Charter Schools
- Refine Support & Staffing Plans
- Create Refresh & Upgrade Strategy & Plans

Figure 34 - UETN and LEA Security & Content Filtering Program Road Map

Security and Content Filtering High Level Activities



INITIATE

Create Vision & Identify Goals

- What essential work do you perform?
- For whom do you do this work?
- What do you want to accomplish?

Review & Understand Current State

- Organization
- Goals
- Architecture
- Technology Components
- Capabilities

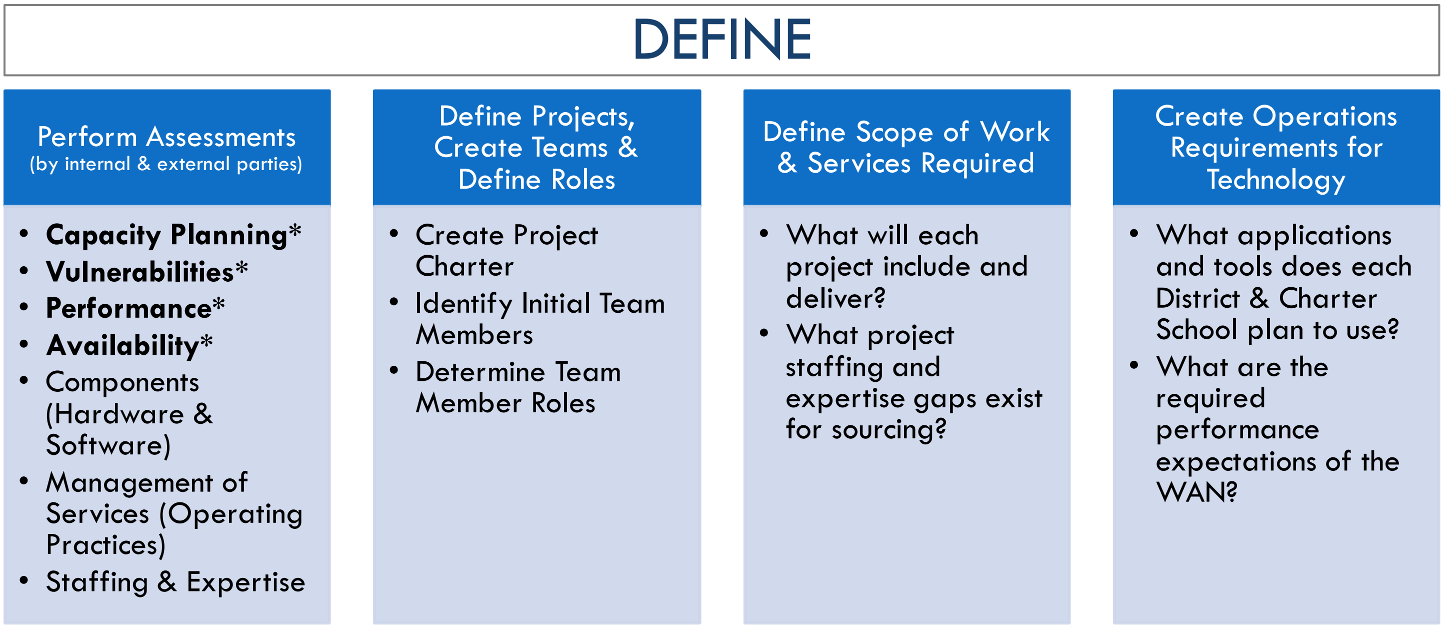
Request & Obtain Initial Funding

- Consultants
- Training
- Staff Augmentation

Obtain Recommendations & Develop Road Maps

- White Papers
- Opinion Letters
- Best Practices Reports
- Strategic Plans
- Recommendations

Figure 35 - Security & Content Filtering Initiation Activities



DEFINE

Perform Assessments (by internal & external parties)

- **Capacity Planning***
- **Vulnerabilities***
- **Performance***
- **Availability***
- Components (Hardware & Software)
- Management of Services (Operating Practices)
- Staffing & Expertise

Define Projects, Create Teams & Define Roles

- Create Project Charter
- Identify Initial Team Members
- Determine Team Member Roles

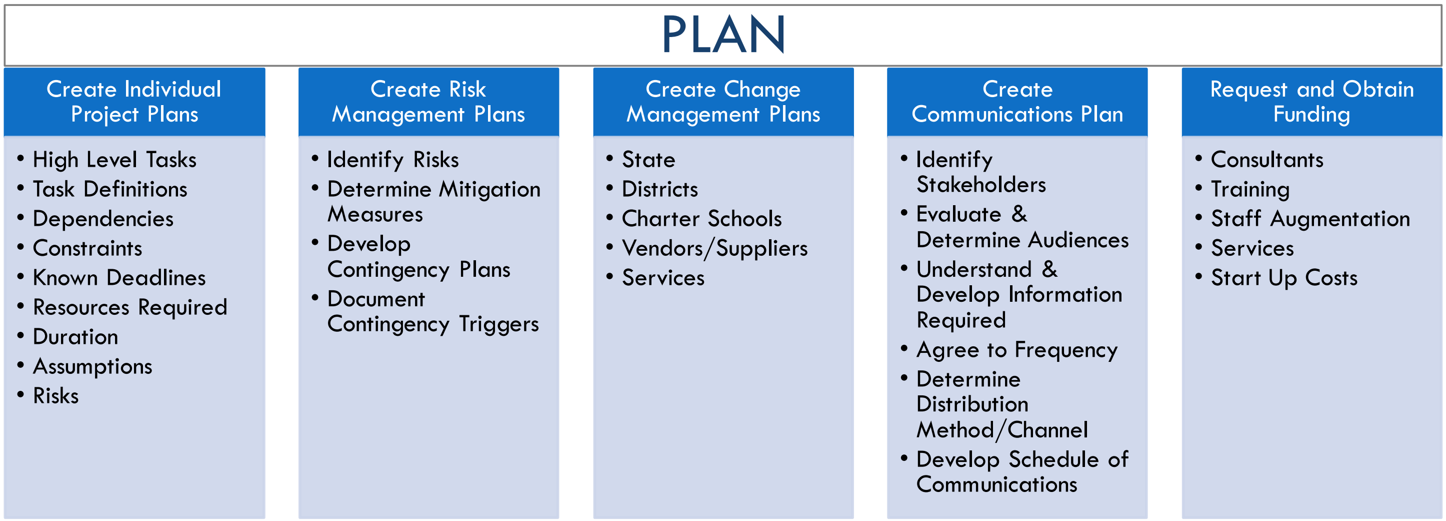
Define Scope of Work & Services Required

- What will each project include and deliver?
- What project staffing and expertise gaps exist for sourcing?

Create Operations Requirements for Technology

- What applications and tools does each District & Charter School plan to use?
- What are the required performance expectations of the WAN?

Figure 36 - Security & Content Filtering Definition Activities



PLAN

Create Individual Project Plans

- High Level Tasks
- Task Definitions
- Dependencies
- Constraints
- Known Deadlines
- Resources Required
- Duration
- Assumptions
- Risks

Create Risk Management Plans

- Identify Risks
- Determine Mitigation Measures
- Develop Contingency Plans
- Document Contingency Triggers

Create Change Management Plans

- State
- Districts
- Charter Schools
- Vendors/Suppliers
- Services

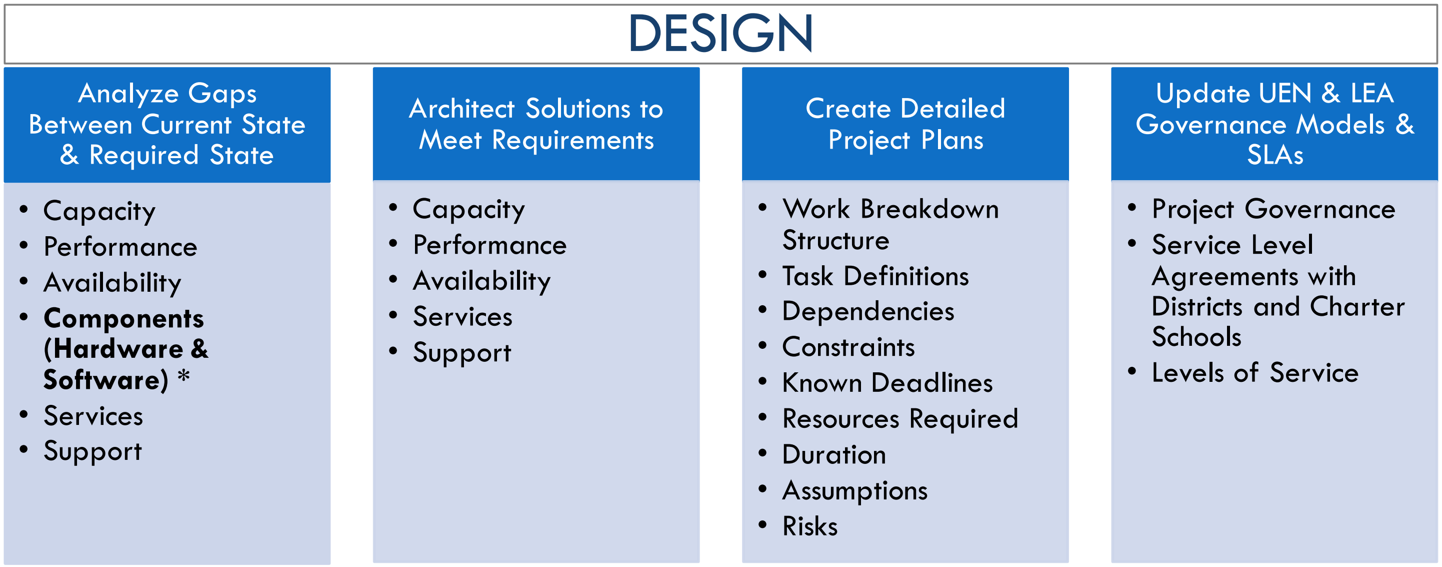
Create Communications Plan

- Identify Stakeholders
- Evaluate & Determine Audiences
- Understand & Develop Information Required
- Agree to Frequency
- Determine Distribution Method/Channel
- Develop Schedule of Communications

Request and Obtain Funding

- Consultants
- Training
- Staff Augmentation
- Services
- Start Up Costs

Figure 37 - Security & Content Filtering Planning Activities



DESIGN

Analyze Gaps Between Current State & Required State

- Capacity
- Performance
- Availability
- **Components (Hardware & Software)** *
- Services
- Support

Architect Solutions to Meet Requirements

- Capacity
- Performance
- Availability
- Services
- Support

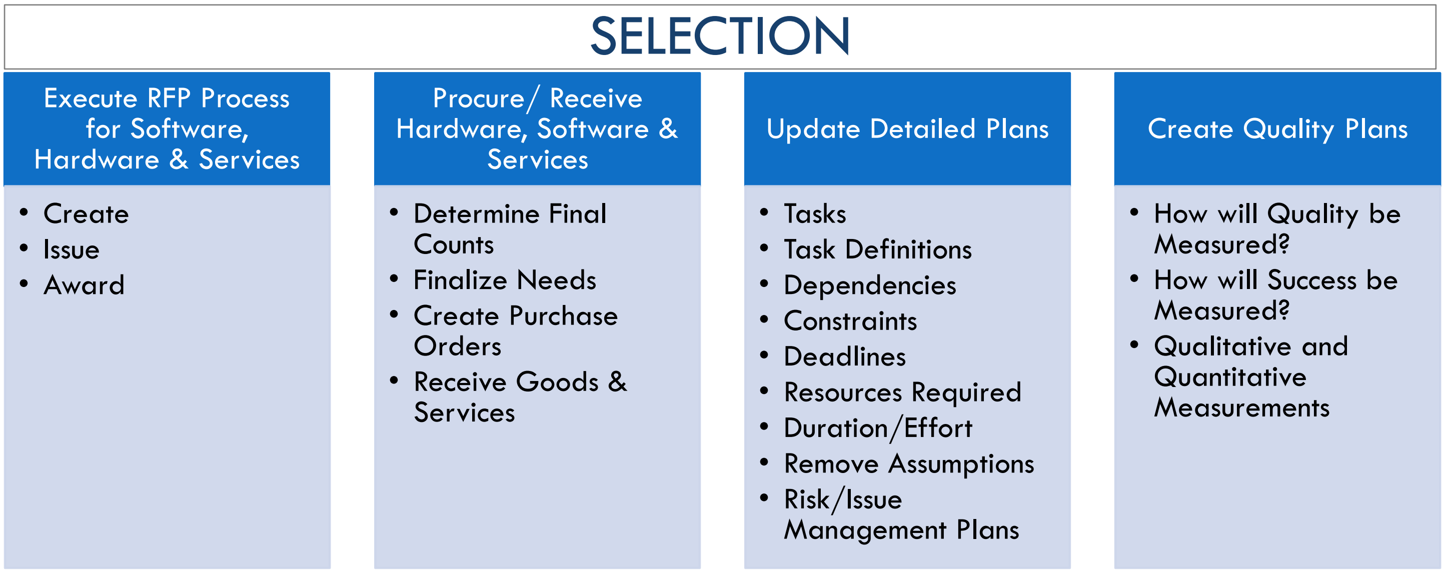
Create Detailed Project Plans

- Work Breakdown Structure
- Task Definitions
- Dependencies
- Constraints
- Known Deadlines
- Resources Required
- Duration
- Assumptions
- Risks

Update UEN & LEA Governance Models & SLAs

- Project Governance
- Service Level Agreements with Districts and Charter Schools
- Levels of Service

Figure 38 - Security & Content Filtering Design Activities



SELECTION

Execute RFP Process for Software, Hardware & Services

- Create
- Issue
- Award

Procure/ Receive Hardware, Software & Services

- Determine Final Counts
- Finalize Needs
- Create Purchase Orders
- Receive Goods & Services

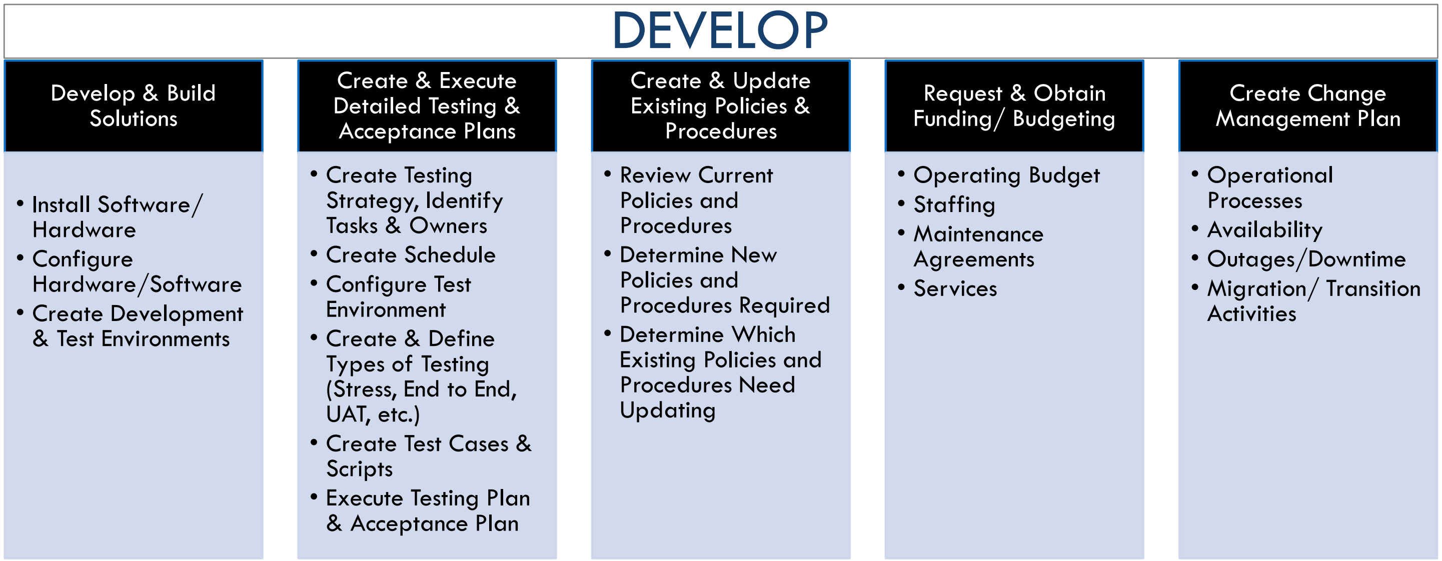
Update Detailed Plans

- Tasks
- Task Definitions
- Dependencies
- Constraints
- Deadlines
- Resources Required
- Duration/Effort
- Remove Assumptions
- Risk/Issue Management Plans

Create Quality Plans

- How will Quality be Measured?
- How will Success be Measured?
- Qualitative and Quantitative Measurements

Figure 39 - Security & Content Filtering Selection Activities



DEVELOP

Develop & Build Solutions

- Install Software/ Hardware
- Configure Hardware/Software
- Create Development & Test Environments

Create & Execute Detailed Testing & Acceptance Plans

- Create Testing Strategy, Identify Tasks & Owners
- Create Schedule
- Configure Test Environment
- Create & Define Types of Testing (Stress, End to End, UAT, etc.)
- Create Test Cases & Scripts
- Execute Testing Plan & Acceptance Plan

Create & Update Existing Policies & Procedures

- Review Current Policies and Procedures
- Determine New Policies and Procedures Required
- Determine Which Existing Policies and Procedures Need Updating

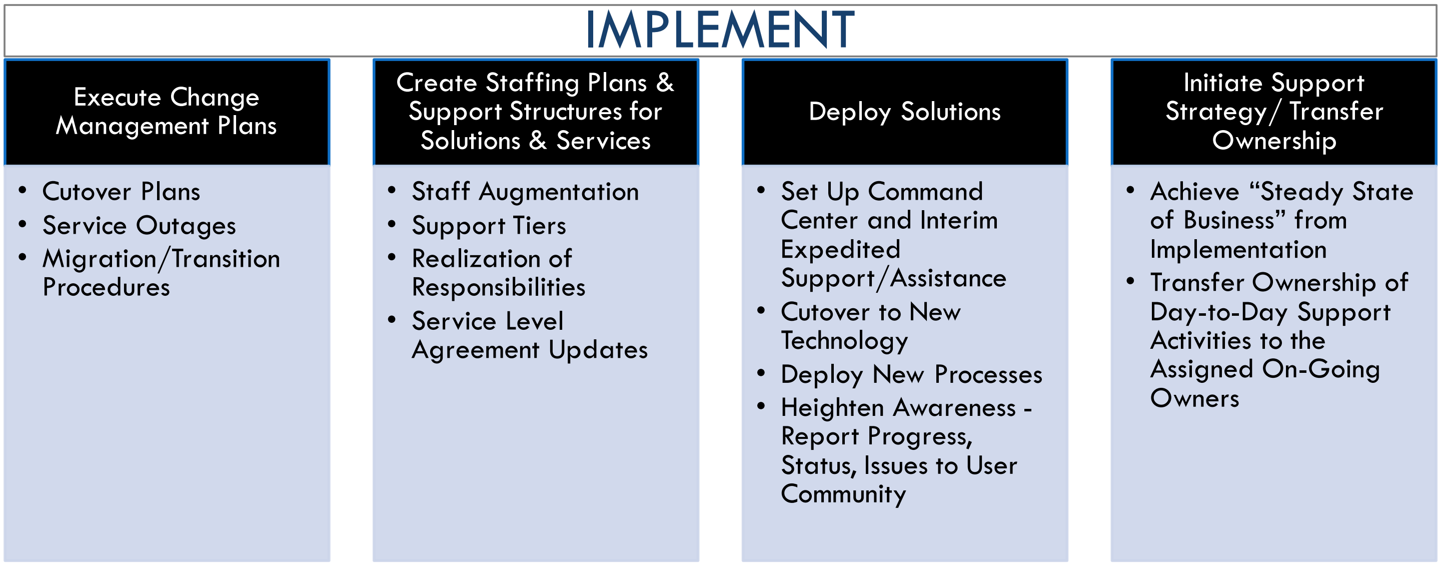
Request & Obtain Funding/ Budgeting

- Operating Budget
- Staffing
- Maintenance Agreements
- Services

Create Change Management Plan

- Operational Processes
- Availability
- Outages/Downtime
- Migration/ Transition Activities

Figure 40 - Security &Content Filtering Development Activities



IMPLEMENT

Execute Change Management Plans

- Cutover Plans
- Service Outages
- Migration/Transition Procedures

Create Staffing Plans & Support Structures for Solutions & Services

- Staff Augmentation
- Support Tiers
- Realization of Responsibilities
- Service Level Agreement Updates

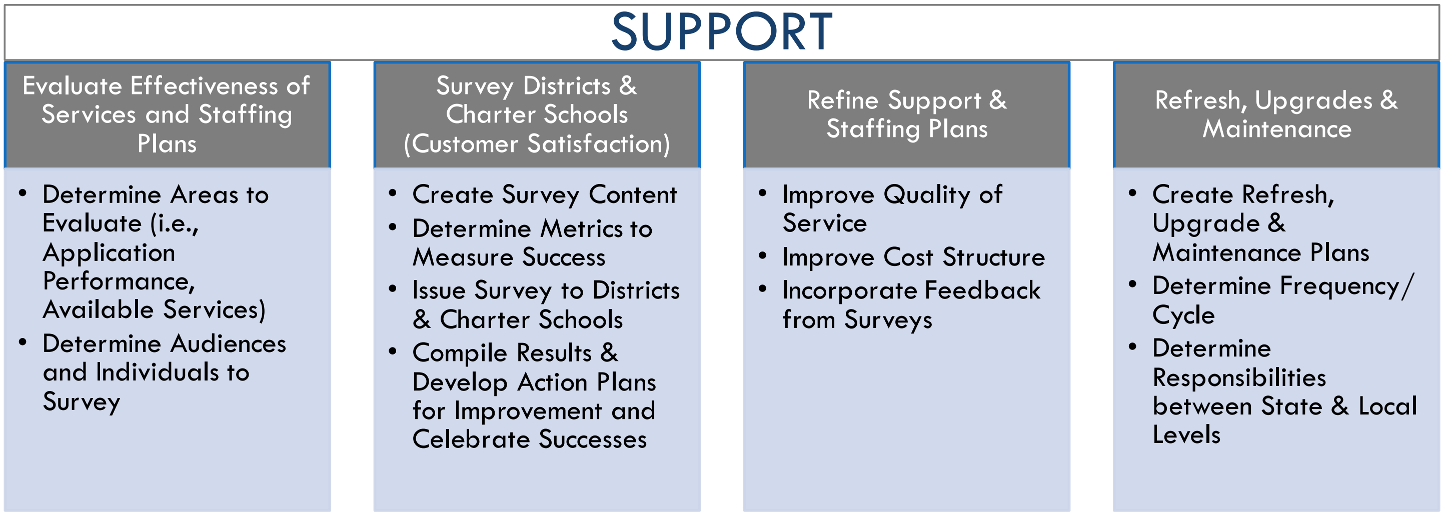
Deploy Solutions

- Set Up Command Center and Interim Expedited Support/Assistance
- Cutover to New Technology
- Deploy New Processes
- Heighten Awareness - Report Progress, Status, Issues to User Community

Initiate Support Strategy/ Transfer Ownership

- Achieve "Steady State of Business" from Implementation
- Transfer Ownership of Day-to-Day Support Activities to the Assigned On-Going Owners

Figure 41 - Security & Content Filtering Implementation Activities



SUPPORT

Evaluate Effectiveness of Services and Staffing Plans

- Determine Areas to Evaluate (i.e., Application Performance, Available Services)
- Determine Audiences and Individuals to Survey

Survey Districts & Charter Schools (Customer Satisfaction)

- Create Survey Content
- Determine Metrics to Measure Success
- Issue Survey to Districts & Charter Schools
- Compile Results & Develop Action Plans for Improvement and Celebrate Successes

Refine Support & Staffing Plans

- Improve Quality of Service
- Improve Cost Structure
- Incorporate Feedback from Surveys

Refresh, Upgrades & Maintenance

- Create Refresh, Upgrade & Maintenance Plans
- Determine Frequency/ Cycle
- Determine Responsibilities between State & Local Levels

Figure 42 - Security & Content Filtering Support Activities

CLOSING

UETN must prepare its WAN, Wi-Fi, and Security/Content Filtering business operations for “technical readiness” in order to accommodate changing and future needs as defined in Utah’s future teaching and learning program.

Sanity Solutions, partnering with Gazos Creek, has recommended a strategic approach including recommendations and 3-year road map for Utah’s teaching and learning program that would require financial investment. These recommendations could also realize cost-savings through creative measures, such as offering standardization of policies and practices, realizing economies of scale for hardware, software, and services purchases through state procurement program, and targeting grants and sponsorship opportunities.

As echoed in each study area above, UETN must seek stable, sustainable on-going operational funding sources to ensure technical readiness to meet the vision of the Digital Teaching and Learning Program. It is imperative that UETN shift away from using one-time funding sources for its’ on-going operational expenses. There are a myriad of ways to accomplish this, which were addressed within each study area.

By building a solid strategy based on Sanity Solution’s and Gazos Creek’s recommendations, Utah will be one step closer to realizing its vision of preparing its students for the 21st-century global economy. It will increase college and career readiness of all students in all Utah schools which will ultimately result in growth and viability in Utah’s economy.

GLOSSARY OF TERMS AND DEFINITIONS

Terms	Definitions
ARP – Address Resolution Protocol	a telecommunication protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks.
ATM – Asynchronous Transfer Mode	a telecommunications protocol used in networking
AToM – Any Transport Over MPLS	See MPLS definition
BGP – Border Gateway Protocol	a standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet.
BTOP – Broadband Technology Opportunity Program	a grant program associated with the American Recovery and Reinvestment Act (ARRA). The grant program was created to promote the development and adoption of broadband throughout the United States, particularly in unserved and underserved areas.
CE (Customer Edge) router	the router at the customer premises that is connected to the Provider Edge (PE) of a service provider IP/MPLS network.
DHCP – Dynamic Host Configuration Protocol	a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.
DNS - Domain Name System	a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network.
DPI – Deep Packet Inspection	is a form of computer network packet filtering that examines the data part (and possibly also the header) of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may pass or if it needs to be routed to a different destination, or, for the purpose of collecting statistical information.
DWDM – Dense Wavelength Division Multiplexing	refers originally to optical signals multiplexed within the 1550 nm band so as to leverage the capabilities (and cost) of erbium doped fiber amplifiers (EDFAs), which are effective for wavelengths between approximately 1525–1565 nm (C band), or 1570–1610 nm (L band).
eBGP – Exterior Border Gateway Protocol	a standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet
HDLC – High-Level Data Link Control	a bit-oriented code-transparent synchronous data link layer protocol developed by the International Organization for Standardization (ISO).
iBGP – Interior Border Gateway Protocol	a standardized interior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet
IGP – Interior Gateway Protocol	a type of protocol used for exchanging routing information between gateways (commonly routers) *within* an autonomous system.
IDS – Intrusion Detection Signature	is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.
IPv6 (Internet Protocol version 6)	the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4.

IRU – Indefeasible Rights of Use	a contractual agreement between the operators of a communications cable, such as a fiber optic network and a client.
LDP – Linked Data Platform	a Linked Data specification defining a set of integration patterns for building RESTful HTTP services that are capable of read-write of RDF data.
LSP – Label Switched Paths	a path through an MPLS network, set up by a signaling protocol.
MPLS – Multi-protocol Label Switching	a mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.
OOB – Out of Band	refers to activity outside of a defined telecommunications frequency band.
OSPF – Open Shortest Path First	a routing protocol for Internet Protocol (IP) networks.
PE (Provider Edge) router	a router between a network service provider's core network and the Customer Edge (CE) router. The network provider is usually an Internet service provider as well.
PoP – Point of Presence	an artificial demarcation point or interface point between communications entities.
PPP – Point-to-Point Protocol	a data link protocol used to establish a direct connection between two nodes.
RFC – Remote Function Call	Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems.
ROMMON	a boot-loader on Cisco routers.
SDN - Software Defined Networking	an approach to computer networking that allows network administrators and application developers to manage network services through abstraction of higher-level functionality. This is done by decoupling the system that makes decisions about where traffic is sent (the control plane) from the underlying systems that forward traffic to the selected destination (the data plane).
SNMP – Simple Network Management Protocol	an Internet-standard protocol for managing devices on IP networks.
SONET – Synchronous Optical Networking	a standardized protocol that transfer multiple digital bit streams synchronously over optical fiber using lasers or highly coherent light from light-emitting diodes (LEDs).
TDM – Time-division multiplexing	a method of transmitting and receiving independent signals over a common signal path
URPF - Unicast Reverse Path Forwarding	an evolution of the concept that traffic from known invalid networks should not be accepted on interfaces from which they should never have originated.
VLAN – Virtual Local Area Network	any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).
VPLS – Virtual Private LAN Service	a way to provide Ethernet-based multipoint to multipoint communication over IP or MPLS networks.

ADDITIONAL READING

Additional Reading

For a full reading of the bill:
http://le.utah.gov/~2015/bills/static/HB0213.html

For more information related to WAN:
https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/intelligent-wan/wan-architecture-and-design.pdf
https://opennetworkingusergroup.com/wp-content/uploads/2015/05/Network-State-Collection-White-Paper_2015_V5.pdf

For more information related to Security:
http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/us-state-of-cybercrime.pdf
https://www.sans.org/reading-room/whitepapers/threats/vulnerability-assessments-pro-active-steps-secure-organization-453

APPENDIX

Exhibit A

UETN's *Current State* Wide Area Network (WAN)

Provided by UETN

1. Overview

The Utah Education and Telehealth Network (UETN) is a statewide research and education network connecting all public K-12 schools, Higher Education Institutions, Charter Schools, Libraries, and research locations comprising over 1,400 locations. The network is funded through state appropriations and E-rate. As the designated primary provider of Internet access and the Wide Area Network for public education within Utah, the Utah Education Network is the single largest applicant for E-rate funds in the state. UETN serves as the E-rate consortium lead in applying for and implementing the E-rate funds received for the services provided to schools under UETN's purview. UETN also provides E-rate Program Coordination at the state level for all eligible E-rate Program participants.

2. Transport Services

2.1. Ethernet

The UETN network utilizes Ethernet services and equipment exclusively for all WAN transport which provides a lower cost alternative to traditional Time-division Multiplexing (TDM) and Synchronous Optical Networking (SONET) based services. All circuits on the network whether they connect individual schools and libraries or between UETN backbone locations are Ethernet. A mixture of 100Mb, Gigabit, 10 Gigabit, and 100 Gigabit are used on the network according to specific requirements for services needed. UETN has contracts for WAN services with (16) providers all of whom provide point-to-point Ethernet services covering rural to urban areas in the state of Utah. These providers are using a mixture of Dense Wavelength Division Multiplexing (DWDM), dark fiber, shared Ethernet, and licensed radio to provide these services.

2.2. Dark Fiber and DWDM

UETN procured a small number of dark fiber Indefeasible Rights of Use (IRU), with Broadband Technology Opportunity Program (BTOP) funding, which connect some Higher Education Institutions with key aggregation and research locations on the network. IRUs were chosen for these segments to provide services that are not available commercially (i.e., 100GB, Fiber Channel, etc.) and to allow for rapid, economic growth of bandwidth between these locations utilizing DWDM.

UETN operates a (10) node DWDM network over these IRUs providing 50+ wavelengths which are used for research, the UETN IP backbone and to connect geographically diverse data centers between Universities. This DWDM network is limited in scope and is not intended to replace leased services that provide the majority of WAN circuits.

2.3. Microwave

UETN owns and operates twelve licensed microwave paths in rural areas of the state. These paths provide services to remote locations where fiber builds are either too expensive or non-existent. Speeds provided are between 45Mb – 300Mb with Ethernet handoffs that integrate easily with the UETN network. The microwave footprint has been shrinking in recent years due to fiber build outs, but it is expected many locations will always require wireless connectivity.

3. Network Equipment

3.1. Vendors

UETN has standardized on routers and switches to provide all Layer 2 and Layer 3 services on the network. The ASR 9000 and 7600 series platforms are used for backbone and school district aggregation routers while the 3560 and 3750 are typically used for end sites such as individual schools. All models of routers in the network have undergone extensive testing prior to deployment and backbone routers were tested during on-site CPOC (Customer Proof of Concept Testing) at Cisco labs.

4. Routing Protocols

4.1. Open Shortest Path First (OSPF) – A routing protocol for Internet Protocol networks.

OSPF is used as the Interior Gateway Protocol that operates between all the backbone (P/PE) routers. OSPF carries next-hop routing information and does not have any customer or Internet routes. Keeping the OSPF routing table small enables fast re-convergence in the event of link or router failure. UETN's OSPF network is all in area 0 and carries less than 200 routes.

4.2. Label Distribution Protocol (LDP) – a protocol in which routers capable of Multiprotocol Label Switching (MPLS) exchange label mapping information.

All router links with established OSPF neighbors are also running LDP neighborships (includes all P/PE). This enables the network to run LSP's (Label Switched Paths) between backbone routers so packets are forwarded by the label database as opposed to the Remote Insight Board.

4.3. Border Gateway Protocol (BGP) – A standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet.

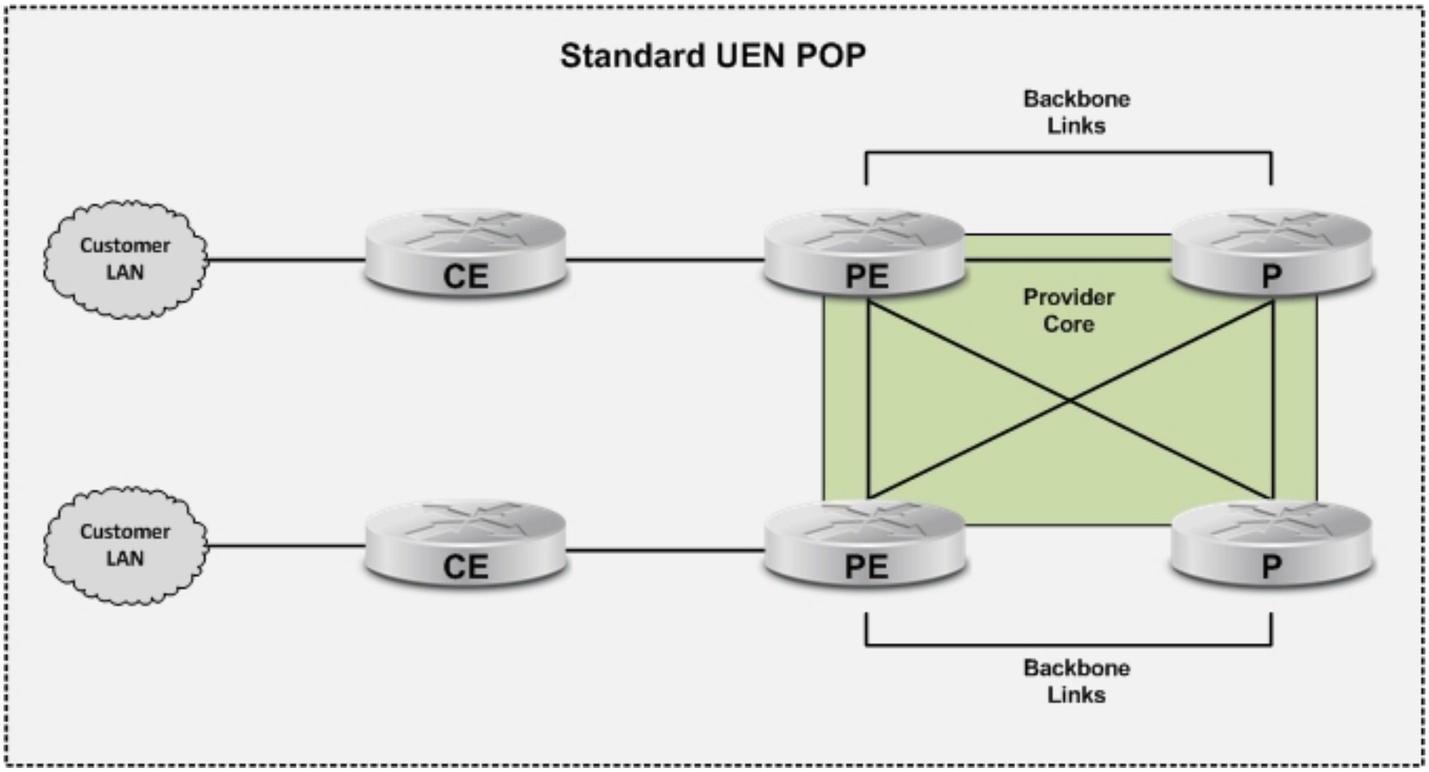
BGP is used to carry all customer and Internet routes. P devices on the network do not run BGP and are only utilizing OSPF/LDP to forward packets. All PE devices are running BGP.

5. Network Architecture

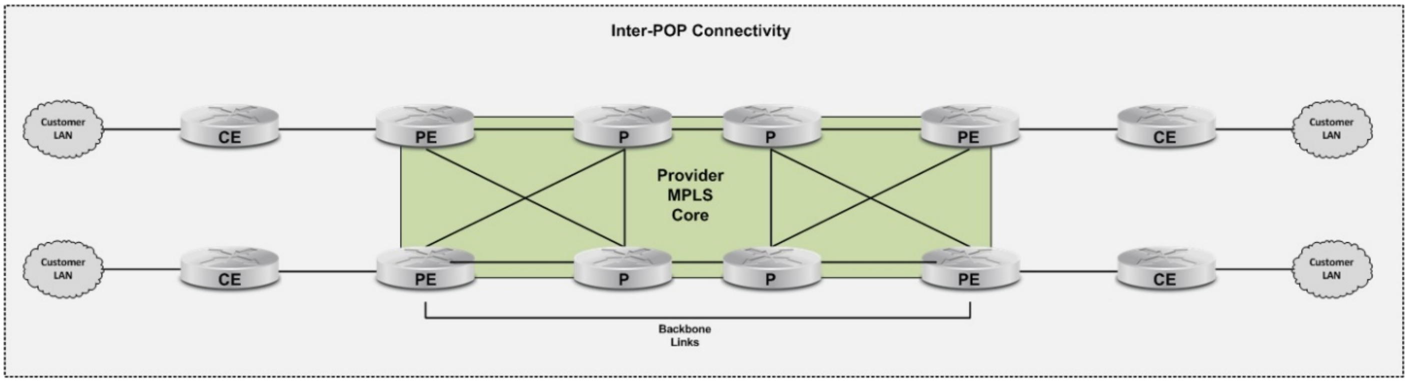
Between 2007 and 2008 the Utah Education Network first rolled out a simple Multiprotocol Label Switching network architecture that was used primarily for MPLS Traffic Engineering Tunnels. Initially, the MPLS features were intended to provide quicker failover for backbone links as well as simple Layer 2 point-to-point services (pseudo-wires) for geographically diverse UETN customers. Since that time UETN has implemented a fully converged IP/MPLS network architecture replacing its traditional IP routed core.

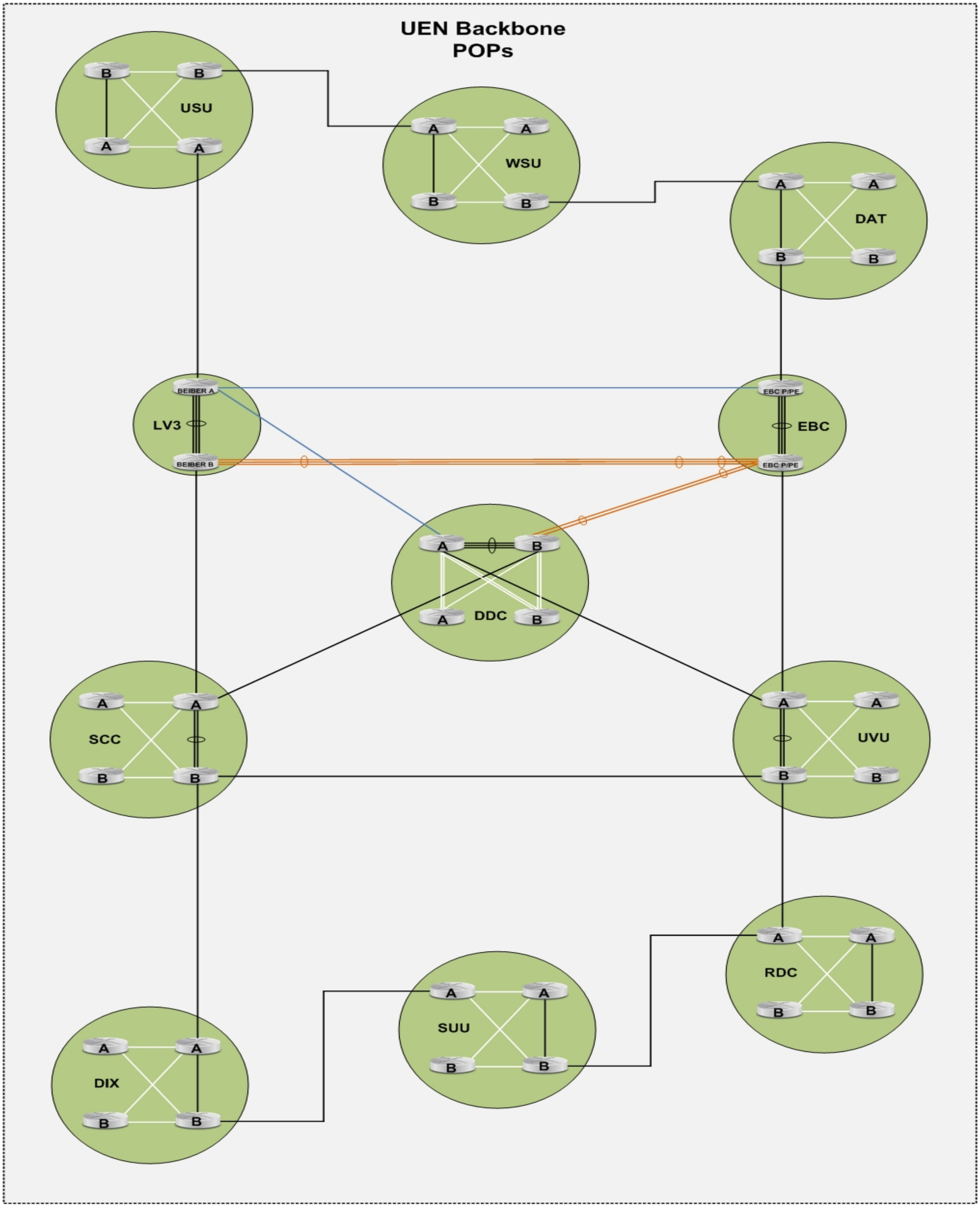
This next-generation design has vastly improved performance, reliability, and redundancy, more importantly, the MPLS core has also afforded UETN the ability to provide Layer 2 and Layer 3 services such as L2/ L3 Virtual Private Networks (point-to-point and any-to-any topologies) to its customers. Additionally, the MPLS architecture has provided a flexible infrastructure to transition from IPv4 to IPv6 for customers based on the individual customer's needs and ability to deploy IPv6. UETN's implementation of its MPLS network architecture insures stability, redundancy, and scalability for the demanding needs of its customers.

The UETN MPLS Backbone consists of a series of Points-of-Presence (POPs) interconnected via the respective Ethernet transport circuits previously mentioned. Furthermore, each POP can be broken down into smaller component parts by the different roles and responsibilities of the routers that collectively constitute the POP; Provider (P), Provider Edge (PE), and Customer Edge (CE) routers. Generally speaking, the standard UETN POP consists of 2 (P) routers and 2 (PE) routers, intra-connected for redundancy and capacity. The (P) routers are also inter-connected to the (P) routers of other POPs to create the UETN Backbone. Where possible, every POP has at least 2 Inter-connects to different POPs for redundancy.



Any connection between (P) routers, (PE) routers, or (P) to (PE) routers are considered "Backbone" circuits and collectively define the UETN Backbone. Each POP serves as an aggregation point for customers for the specific geographic region in which the POP is located. Customer devices (CEs) may or may not physically exist on the premise but physically or logically terminate on one or more of the (PE) devices.



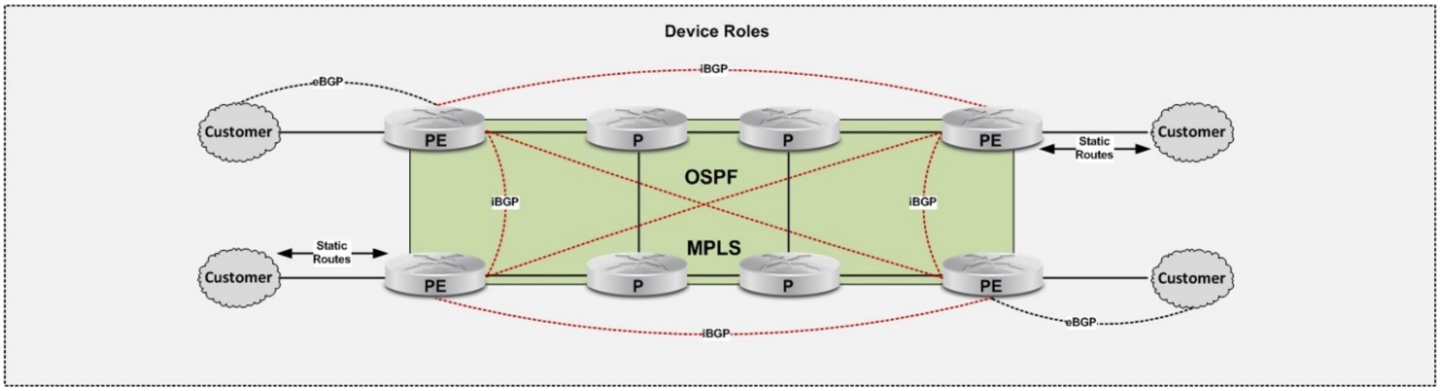

UEN Backbone
POPs
USU
B
B
A
A
WSU
A
A
B
B
DAT
A
A
B
B
LV3
BEIBER A
BEIBER B
EBC
EBC P/PE
EBC P/PE
DDC
A
B
A
B
SCC
A
A
B
B
UVU
A
A
B
B
RDC
A
A
B
B
SUU
A
A
B
B
DIX
A
A
B
B

5.1 P/PE/CE Routers

The main components of a traditional MPLS network are the Provider (P), Provider Edge (PE), and Customer Edge (CE) routers. Not only does each of these routers perform specific functions within an effective MPLS design, they also provide distinct points of demarcation between a provider and it is for simplified network design.

The (P) router, often referred to as the “Core Router”, is just that, the service providers’ core routers. The (P) device does not peer with any customer devices nor does it participate in any customer routing protocols. Typically, a (P) router provides Layer 2 and Layer 3 transit for customers via MPLS label switching. A (P) router participates in the providers IGP, OSPF in the case of UETN, on which the MPLS core is built. (P) devices peer with the (PE) devices via this common IGP and is responsible for providing Next-Hop reachability to the (PE) routers on which the Interior Border Gateway Protocol (iBGP) mesh is built. Since the (P) devices do not participate in BGP or customer routing but MPLS label switch most traffic, the processing and memory loads are greatly reduced while the performance and efficiency is greatly enhanced.

The (PE) router is also known as the Multiservice Edge Router and is responsible for terminating customer connections, routing between customers over the provider core, and participating in the “core” IGP and MPLS on all core-facing interfaces. Additionally, the (PE) router provides the Layer 2 and Layer 3 services that are made possible because of MPLS. Within the UETN network, the (PE) routers participate in a full iBGP mesh with all other (PE) routers via BGP Route-Reflection and in essence provide the “heavy lifting” of moving Internet and Customer routes throughout the UETN network. The (PE) routers peer directly with customers per the UETN routing policy via Exterior Border Gateway Protocol (eBGP) or Static routes (see Routing Policy) while specialized (PE) routers, called Internet Border Routers (IBR) by UETN, peer directly with Internet Service Providers via eBGP. Due to the large routing tables, multiple routing processes, IP routing forwarding decision, and network edge security, the (PE) routers are the work horses of the provider network requiring larger amounts of memory, processing, and forwarding capacity than a traditional (P) router.



(CE) routers define the customer edge and are subject to the routing policy of UETN. The (CE) routers generally are “customer owned” however many (CE) devices are owned and managed by UETN. Either way the “customer edge” defines the peering point with the UETN backbone. Per UETN policy, (CE) devices peer with UETN (PE) devices Layer 3 via eBGP or Static routing, or Layer 2 as Ethernet Access or Trunk VLANs. (CE) routers do not participate in the Provider IGP or MPLS infrastructure.

5.2 MPLS

The UETN network architecture is based on a traditional Multi-Protocol Label Switched core. This means that all backbone links forward traffic using MPLS labels to make forwarding decisions instead of performing hop-by-hop IP route lookups as performed by traditional IP Routed networks. Using MPLS label switched paths greatly reduces router processing and forwarding time while also allowing for additional network services to customers such as L2 /L3 VPNs which are not possible on traditional IP Routed networks.

A key benefit to running an MPLS core is the ability to remove BGP from all core (P) routers. Due to the size of the global Internet table, the overhead and processing of the BGP protocol and the requirement for a full mesh peering topology, for a network of UETNs size, a BGP based IP routing infrastructure is not scalable. In that environment, as the UETN network continued to grow, the performance and reliability began to decrease. BGP instability on one end of the network would propagate throughout the entire network taxing every core router's CPU, memory, and forwarding capacity and ultimately affecting all network services on or through UETN. BGP re-convergence times grew exponentially as BGP routing tables grew or as the size of the BGP router mesh multiplied. Migrating to the MPLS core has removed the need to carry BGP routes across all backbone routers and has greatly enhanced performance, reliability, and scalability.

5.3 Route Reflection

While an MPLS network core has removed the need for BGP on all (P) routers, iBGP is still a crucial component of an MPLS network architecture. Multi-protocol BGP or MBGP is essential for effective and efficient MPLS solutions. Every (PE) router on the UETN network runs iBGP and as is required by the BGP protocol, a fully meshed topology is required for proper iBGP peering and route propagation. To minimize the exponential effects of growing route tables and expanding BGP router meshes, UETN leverages Route-Reflection. UETN has defined 3 Route-Reflectors, in essence 3 routers to which all other iBGP speaking routers peer with which emulate a fully meshed topology. The 3 Route-Reflectors are strategically located geographically, all in hardened data centers, to insure seamless route propagation in case of failures in hardware, software, circuits, etc.

5.4 Redundancy

From redundant hardware within each POP to multiple exit points from each POP, over diverse fiber paths where possible, network redundancy is a key focus of the UETN network architecture. As illustrated in the "Standard POP design", UETN makes every effort to have 2 (P) and 2 (PE) routers in each POP, redundantly intra-connected as well as redundantly inter-connected to other POPs over diverse fiber paths off of diverse routers. UETNs topology, for the most part, is inter-connected in a series of "rings". Certain sites, generally in very remote locations of the state, technology or costs are sometime prohibitive and UETN must deviate from their "standard" however the exceptions are rare and becoming less and less commonplace as technology and availability become more readily accessible.

In addition to the redundant design of the POPs and their interconnects, UETN peers with 5 Tier one service providers for Internet access, as well as connections to multiple research networks, most notably Internet 2. UETN also has multiple peering arrangements with different caching servers, local ISPs, and other public and private entities (please refer to the "Connectivity" section of this report for a detailed description of these different peers). These respective peer points are located again in geographically diverse locations across multiple POPs to insure the greatest amount of redundancy and resiliency for UETN and its customers.

5.5 Customer Routing

As was stated earlier, all UETN customers connect to the UETN at or more POPs, into one or more (PE) devices based on the redundancy needs of the respective customer. Generally speaking, institutions of Higher Education peer to multiple

POPs, larger school districts often times peer to either multiple POPs or a single POP but into (2) different (PE) routers. Smaller entities such as charter schools or libraries will most often have a single connection into one (PE) at whichever POP they aggregate into. While the amount and types of customer connections vary, UETN has a standard routing policy for all customers.

Per the routing policy (explained in greater detail in the "Routing Policy" section) all customers either eBGP peer with UETN or static routes are used. Either way all customer routes are put into BGP, either via the respective eBGP peering with the customer or by way of redistribution of Connected and Static routes on the (PE) routers themselves. All customer routes are then shared with all other (PE) routers via iBGP as was discussed earlier.

Multi-homed customers peer via eBGP to leverage the dynamic failover of the routing protocol as well as to leverage features like path preference, load balancing, etc. Single-homed customers generally use static routes as there is only one way in or out of their respective networks and also for the sake of simplicity. This form of customer routing applies to both IPv4 and IPv6 peering arrangements.

5.6 Routing Policy

UETN has defined routing policy that governs how customers, providers, and partners peer with UETN.

Customer – First and foremost, all UETN customers must provide a security appliance (i.e., Firewall) that sits between the customer LAN and the UETN backbone. Per the security policies, this security is both for the customers looking to connect and also to protect all of the existing customers already connected to the backbone. Generally, customers will have what is termed as an "inside" device and an "outside" device with the firewall or comparable network security device sitting between those devices. The "inside" gives access to the customer LAN while the "outside" device is the customer WAN device (CE) that physically connects to the UETN backbone (PE).

These (CE) devices can share their routing information in one of 2 ways; 1) via static routing or 2) via eBGP peering.

> Static Routing- Single-homed customers, customers with relatively little IP space, or customers with limited hardware or IT staff generally use static routes, usually just a default route out to the UETN (PE) device. Conversely, the terminating (PE) device has static routes for all of the customers routed networks pointing out the directly connected interface. Those static routes are then re-distributed into the BGP process on the (PE) device and propagated across the network infrastructure as previously explained. UETN will provide public IP space for customers who do not owned their own IP addresses.
>
> BGP – Multi-homed customers or customers with large IP networks will participate in an eBGP session with the UETN (PE) device. As with statically routed customers, UETN will provide IP addressing for customers who do not own their own IP addressing. Additionally, UETN will provide private BGP AS numbers for customers who wish to BGP peer but do not have their own assigned AS. traffic engineering, which allows multi-homed customers to "mark" their route advertisements so that they may control which paths they want to prefer for ingress and egress traffic. This ability gives customers the autonomy to preference traffic, suppress advertisements to specific providers, etc.

Providers – UETN peers with all of its Service Providers via eBGP. The (PE) routers used for Service Provider connections are referred to as Internet Border Routers (IBR) to identify their specialized role in the network. All IBRs receive a full Internet table from their respective Provider, as well as, a default route. IBRs modify the Local Preference, tag the ISP routes with Provider specific communities, and pare down the full Internet table to a subset of optimal routes from that specific provider before passing them into the UETN iBGP mesh. By adjusting the routes in this way, UETN is able to keep the size of BGP tables manageable while still optimizing path selection. Additionally, UETN works with the specific providers and adheres to their policies for marking traffic to influence the flow of traffic into the UETN network to load balance ingress and egress traffic as evenly as possible.

Partners – UETN "partners" include research entities such as Internet 2, the Idaho Regional Optical Network (IRON), Transit Rail, educational organizations such as Brigham Young University, the PAC 12 network, the University of Montana and peering exchanges and caching servers like Google and Akami. These 'Partners" in many ways act as both "Customers" and "Providers" and may peer Layer 3 via Static routes or BGP or Layer 2 as "pass throughs" to other partners generally as Ethernet VLANs. Layer 3 peering follows the same standards as traditional "customers" and/ or "Providers".

5.7 Layer 2/ Layer 3 Services

Beyond the increased stability and efficiency of running an MPLS core, one of the greatest advantages over an IP Routed core is the ability to provide Layer 2 (L2) and Layer 3 (L3) services. L2 and L3 services generally refer to Layer 2 VPNs and Layer 3 VPNs. Juniper Networks compares L2VPNs and L3VPNs as follows:

- Layer 3 VPNs—The service provider participates in the customer's Layer 3 routing. Layer 3 VPNs allow customers to leverage the service provider's technical expertise to ensure efficient site-to-site routing. The customer's CE switch uses a routing protocol such as BGP or OSPF to communicate with the provider's PE switch to carry IP prefixes across the network. MPLS-based Layer 3 VPNs use IP over MPLS. Other protocol packets are not supported.

- Layer 2 VPNs – The service provider interconnects customer sites using Layer 2 technology. Layer 2 VPNs give customers complete control over their own routing.

The most common L2 service requested by UETN customers are L2 pseudo-wires which allow customers to connect remote locations/extension sites back to a main campus. These AToM circuits (Any Transport over MPLS) provide a virtual Layer 2 circuit that is "transparent" to the UETN network in that it provides full autonomy to the customer and requires no peering with UETN. What is more, these AToM circuits not only support Ethernet but other common legacy circuit framing such as Asynchronous Transfer Mode (ATM), Frame Relay, High-level Data Link Control (HDLC), and Point-to-Point Protocol (PPP). This technology allows customers to aggregate geographically located sites on common IP subnets/ LANs, enforce security and traffic filtering at a single location, and full autonomy of routing.

These pseudo-wires generally are a point-to-point solution however point-to-multipoint or multipoint-to-multipoint topologies are also supported on the UETN network. Virtual Private LAN Service (VPLS) offers an any-to-any L2 service which provides additional flexibility and autonomy to UETN's customers.

The L3VPNs, much like the L2VPNs, afford customers another method to aggregate multiple sites into a common private network where the customer can control the flow and direction of routing and traffic. The L3VPN solution makes sense for customers with remote sites with multiple subnets that are no longer scalable at a Layer 2 level. UETN leverages this L3 Service for its advanced Video network. The Video VPN affords UETN the ability to collocate its video classrooms with the customer's facilities throughout the state while remaining independent of the customer's network. The L3VPN also allows UETN to enforce a single point of enforcement for security, access, and filtering for the video traffic.

IPv6 is another L3 service UETN provides for its customers. Using a 6PE design which leverages Multiprotocol BGP (MBGP) UETN is able to run IPv6 natively on its PE devices and peer directly with customers while keeping the provider core free of the additional overhead and security risks of running IPv6 on its (P) routers.

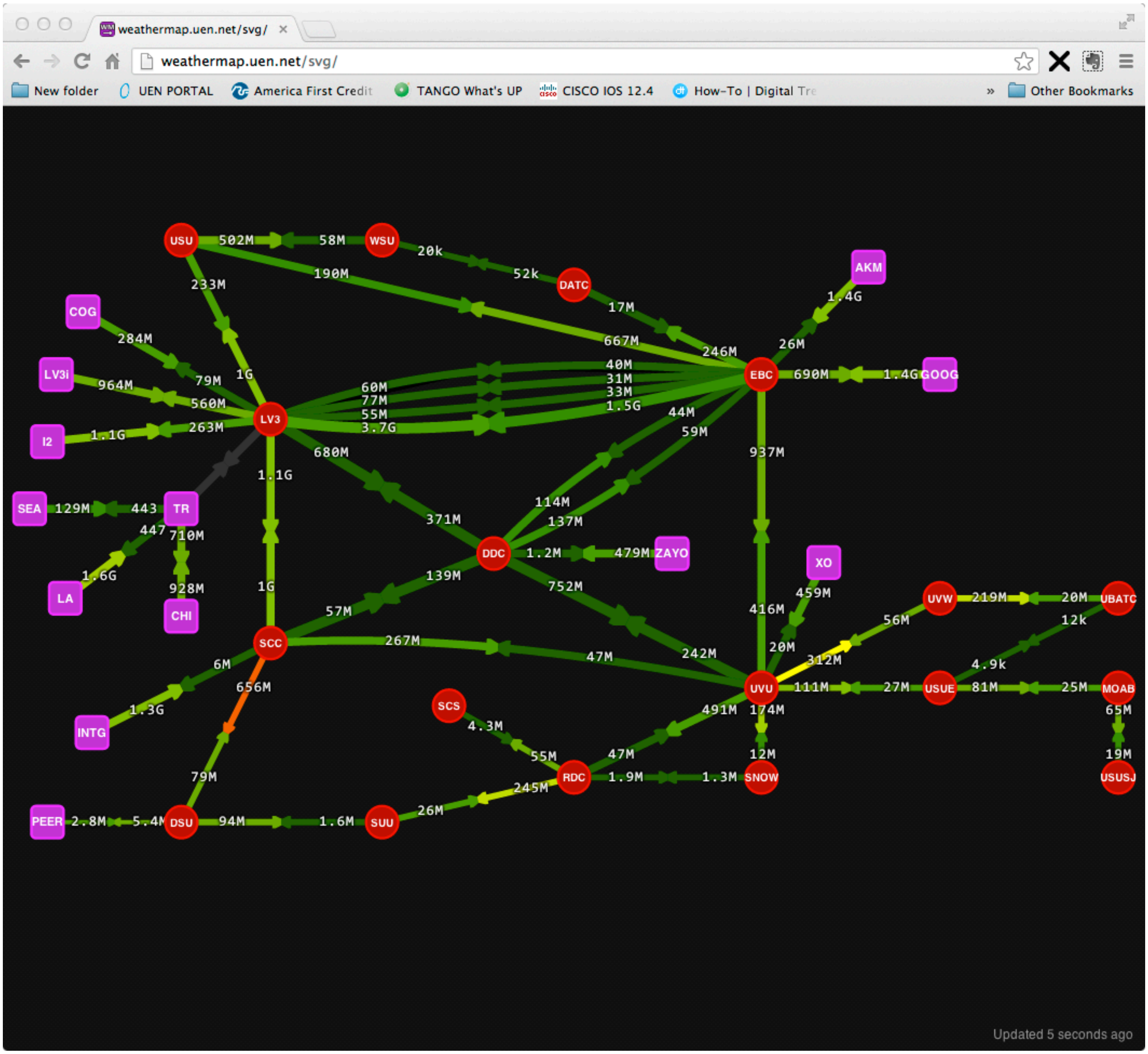
Multicast routing, like IPv6, runs natively on the (PE) routers for support for Multicast enabled customers. UETN provides Multicast services to requesting customers leveraging its peering connection with Internet2 allowing for collaborative Multicast communication at a Wide Area level, not only across the state but the Internet community as a whole.

5.8 Capacity Planning

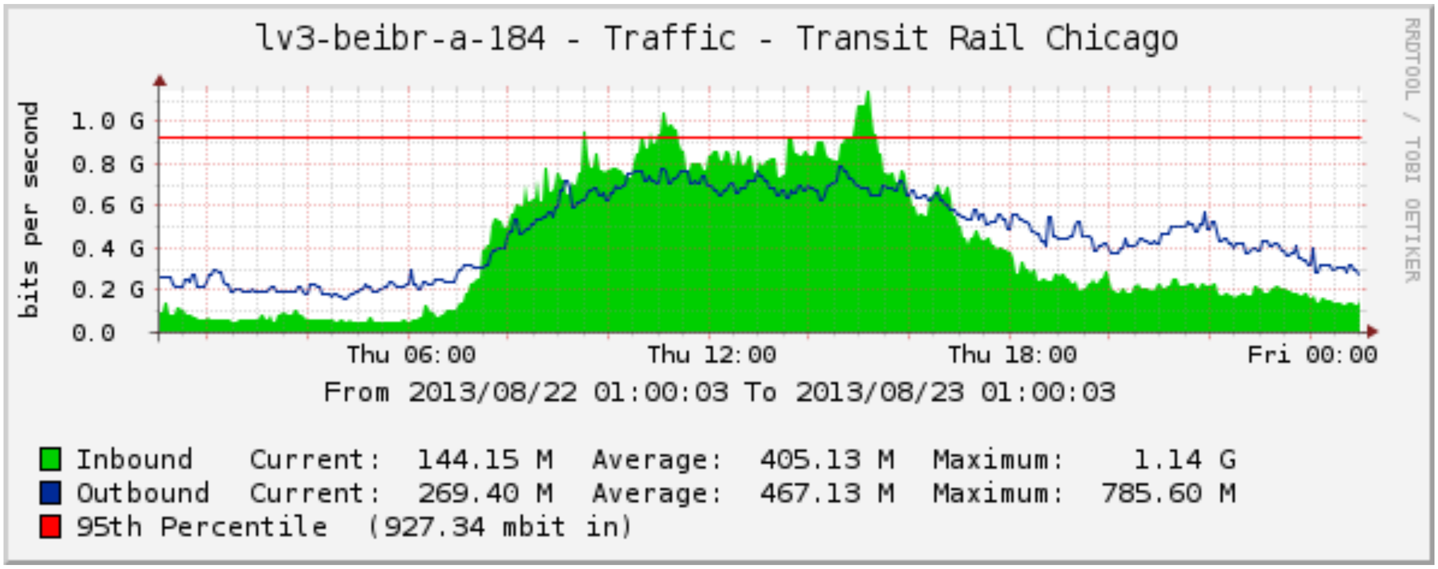
Due to the size and scope of the UETN network, the scope and scale of the UETN video network, and demands of the educational and research communities for network bandwidth, network capacity and capacity planning are crucial to UETNs success. UETN boasts a fully redundant 10 Gigabit core backbone, with the central backbone ring that offers 40 and 100 Gigabit speeds. Even more, the UETN network Internet capacity is in excess of 60 Gigabits with each Provider connected at 10 Gigabit speeds.

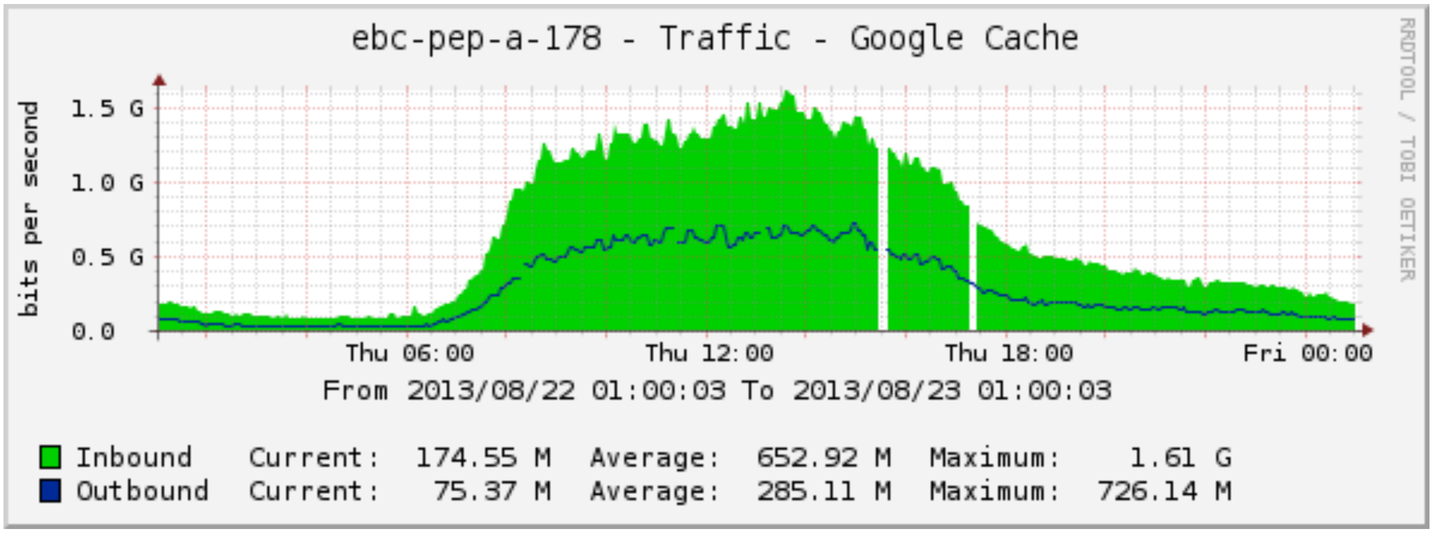
Through the use of state-of-the-art tools UETN is able to monitor traffic utilization, throughput, jitter, latency and other metrics down to the minute. These tools provide real-time data that allows UETN to identify potential network capacity issues among other crucial operational information. The information gathered and traffic patterns allow UETN to design and engineer solutions that will insure a seamless flow of traffic.

Weathermap is a real-time visualization of the UETN backbone and its current traffic loads as well as customer aggregation within the respective POPs. The individual links not only show the current traffic load in bits per second but also change color on a temperature scale where “hotter” colors easily identify circuits approaching their throughput capacity.



The UETN Internet Report gives a daily traffic report for all of UETNs provider and caching peers.





5.9 Out-of-Band Management

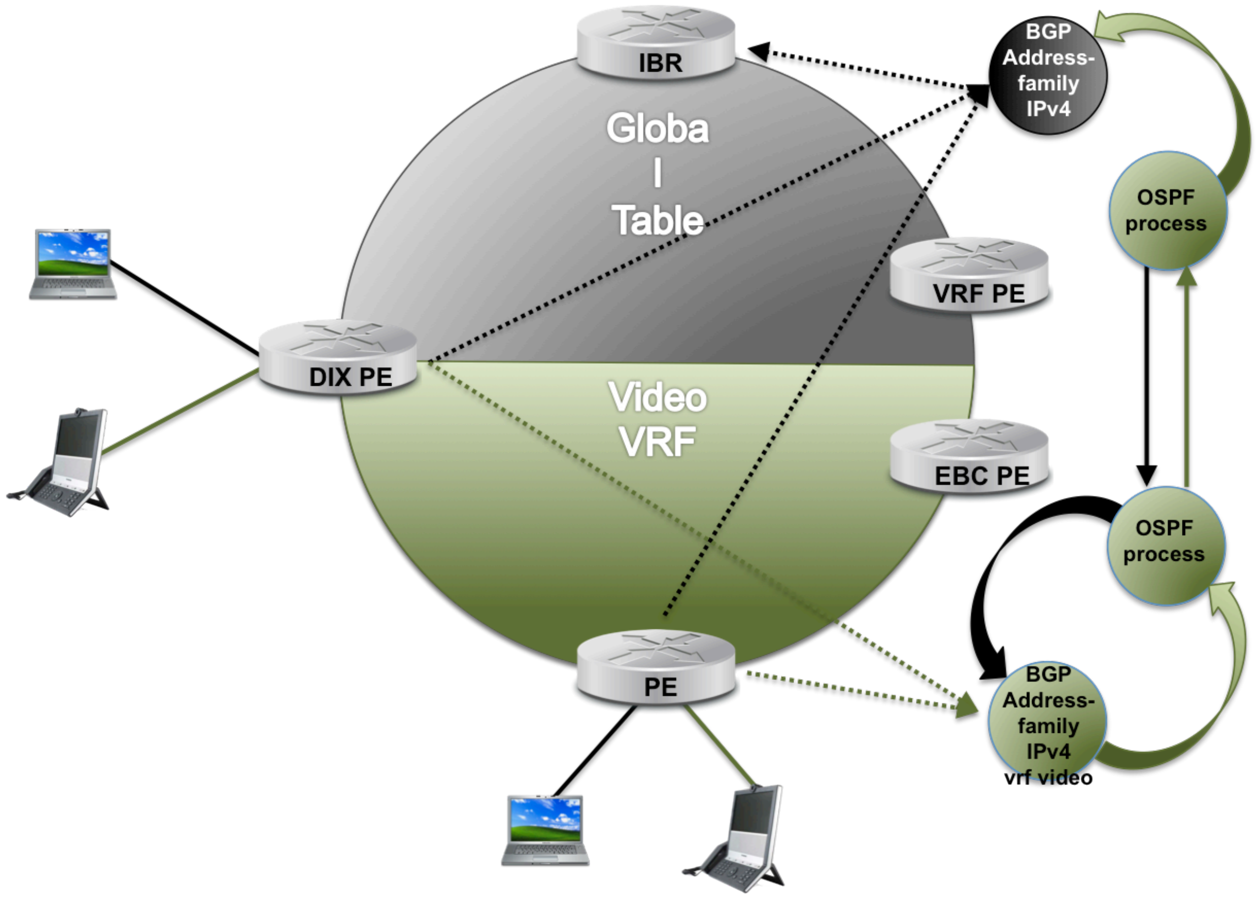
While UETN manages its expansive network via in-band connectivity, leveraging the networks capacity, redundancy, and speed, UETN also runs and manages a completely out-of-band (OOB) network as a back-up management network. Specifically this network is used for console access to critical backbone devices when either network failures such as power outages, circuit cuts, or device failures leave a POP or network device inaccessible via the traditional network. The console access also provides additional advantage when hardware is stuck in a powered but non-operational state, such as ROMMON. Console connectivity allows network engineers the ability to restore devices remotely without needing to travel onsite. The OOB network is also leveraged during maintenance windows where software and hardware upgrades can take a device offline, affording the preforming engineer the opportunity to watch the boot down and boot up process, rollback changes, or restore configurations.

5.10 Video

UETN operates, schedules, and manages a state-of-the-art video network with 100’s of end-points and thousands of classes, conferences, and other video collaborations. With its astounding capacity and efficiency, many of these video classes are run in High-Definition and greatly extend and enhance the educational footprint in Utah. Thousands of students across the state, many of which live in the remote reaches of the state, have access to the finest educational programs that would otherwise be unavailable due to cost and access.

The video services are crucial to the UETN charter and due to their “high visibility” are treated with the top priority. To insure the security, integrity, and manageability of this essential service, UETN has leveraged a Layer 3 VPN solution with strict access control to protect the end device, simplify its management, and guarantee its scalability. The Layer3 VPN solution allows the video network to run in parallel with the data network without compromising its security or performance.

VRF & MPLS Layer 3 VPN



5.11 Security

UETN takes a multi-pronged approach to security focusing on securing its network assets, its customers, and providers as listed below:

Network Assets – UETN defines its network assets all networking hardware such as routers, switches, firewalls, etc., all video devices such as codecs and controllers and other network supporting hardware such as Domain Name System (DNS) servers, Universal Power Supplies (UPS) and other network enabled devices that are owned and/or managed by UETN. Where possible UETN incorporates device templates to secure access and services to and from the networking device. Items such as Virtual Terminal Line (VTY) access will be locked down with access lists, insecure protocols such as Telnet or Simple Network Management Protocol (SNMP) will be disabled/ limited or services like proxy Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP), etc. will be disabled. Additionally, access, where possible, will leverage 2-factor authentication, and VPN only access. Network access best practice are enforced and tracked with granular logging and constantly updated templates.

Customers - UETN faces a unique challenge as both a traditional service provider and specialized Education network provider. Different entities require certain access or restrictions based on the education base they serve. Higher Education institutions for example must have unfiltered connectivity while elementary schools require stricter access policies. Furthermore, with varying levels of IT knowledge and resources, different entities have different levels of skill to implement and enforce good network security practices.

All entities which connect to the UETN backbone are required to have a security appliance (firewall). This requirement serves a 2-fold purpose. 1st, it protects the customer from high level, well known vulnerabilities from any outside entity. 2nd, it protects other UETN customers and Internet sites in general from possible threats originating inside the customer's LAN. UETN also will apply IP Access-Lists when and where necessary in case of vulnerabilities or infections that are not mitigated in a timely manner by the customer.

UETN also helps customers fulfill their Internet filtering requirements as laid out for educational institutions, for example certain types of Web traffic such as pornography or illegal file sharing.

Providers – Unlike customers, there are no security appliances in-line with UETNs ISPs however UETN does block known malicious traffic and follows networking best practices in limiting traffic advertisements. If a customer device or devices is compromised, UETN will "blackhole" traffic attempting to compromise hosts on other customer networks or other Internet hosts. UETN also filters route advertisements such as RFC 1918 addressing, IP addressing identified in RFC 6890.

Leveraging network technologies such as Unicast Reverse Path Forwarding (URPF), destination and source-based blackholing and Bogon route advertisements UETN can protect its assets, customers and providers. UETN heavily invested in security tools to help alert and mitigate network attacks. Tools that take advantage of Netflow, logging, intrusion prevention and other security resources allow UETN to stay proactive in its security role.

Peering, Internet and Caching

Peering

UETN connects with two peering points in the state to ensure local traffic routes local and does not route outside of the state only to come back. One peering point has been established in Salt Lake City and the other in St. George. UETN peers with local service providers and other content networks at these peering locations. As the Internet has continued to grow connection speeds has increased while costs have plummeted local peering points have become less important and they now constitute less than 1% of traffic exchanged on the UETN backbone.

Internet

UETN connects with no fewer than four different Internet carriers to ensure redundancy and uptime for the network. Internet traffic is load balancing using BGP to ensure links do not become over utilized and it gives UETN control over how traffic routes both out and into the network. Internet connections currently use 10GE Ethernet transport and will be upgraded to Nx10GE when required. Internet connections are dispersed throughout the state into multiple PoPs for redundancy while also dispersing load across the backbone.

Caching

UETN is currently using three caching services to augment Internet bandwidth. The three services are Akamai, Netflix, and Google. Akamai provides caching for multiple content providers including Apple. These caching services keep frequently used content local so that it is not passed across the Internet but rather served from local servers. These services are provided free of charge and are exclusively managed by the service providers. Caching helps keep Internet costs down while providing the content with high bandwidth and low latency. Because these services are co-located directly on the UETN network, we have more control of traffic flows throughout the network.

Exhibit B

UEN Infrastructure Map

Backbone and Internet Connections

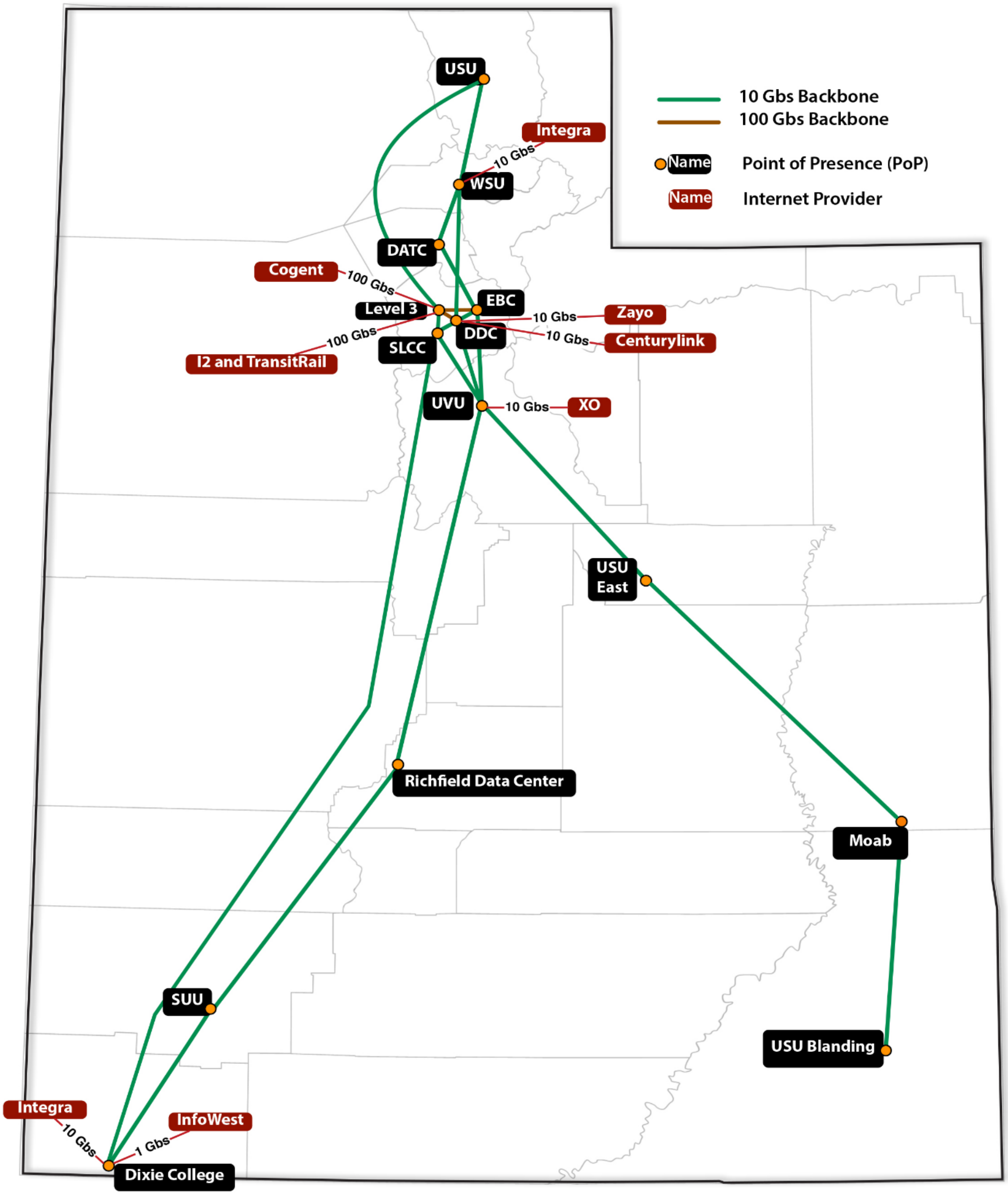


Exhibit C

UEN Infrastructure Map

Backbone and District Office Connections

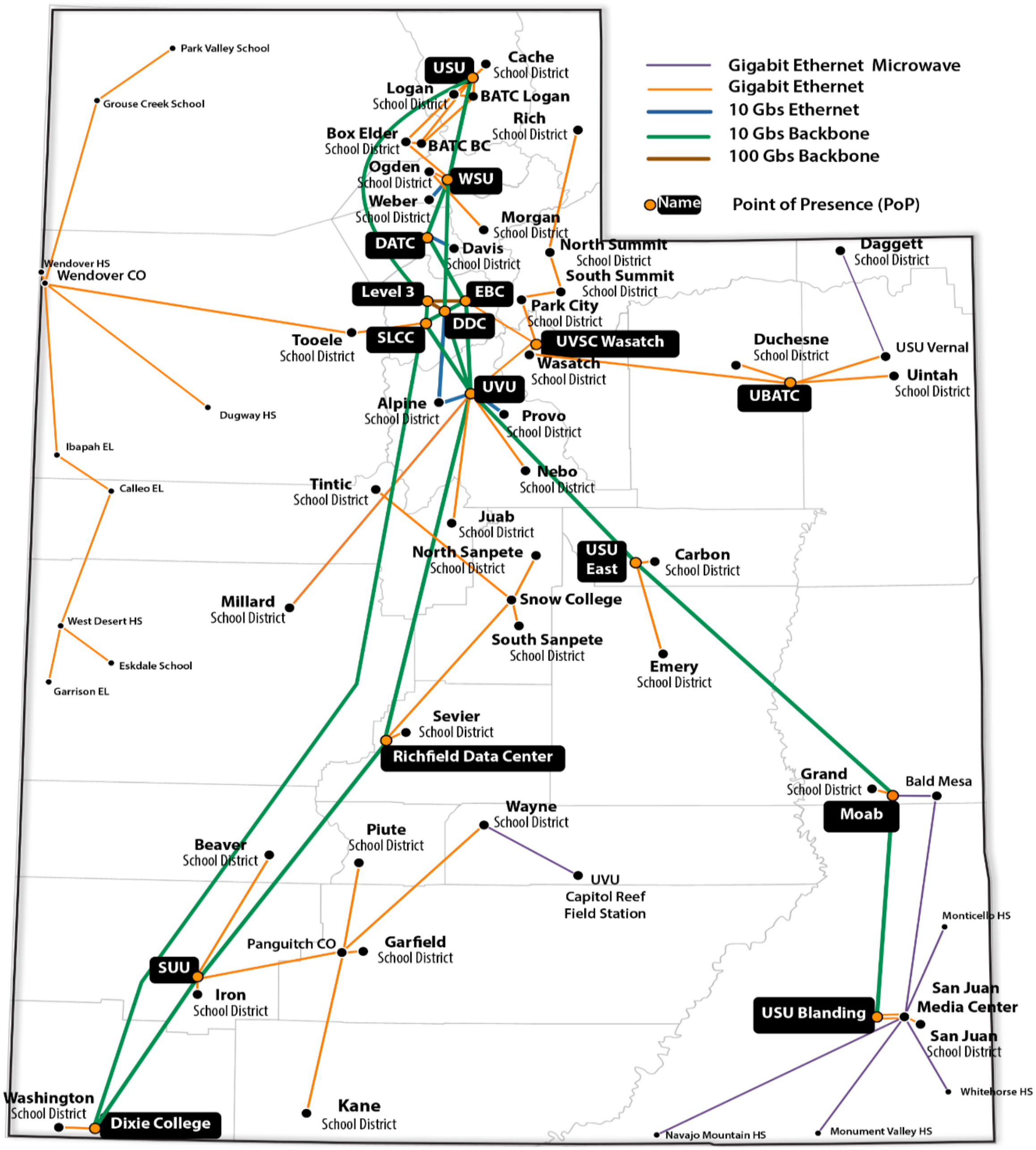


Exhibit D

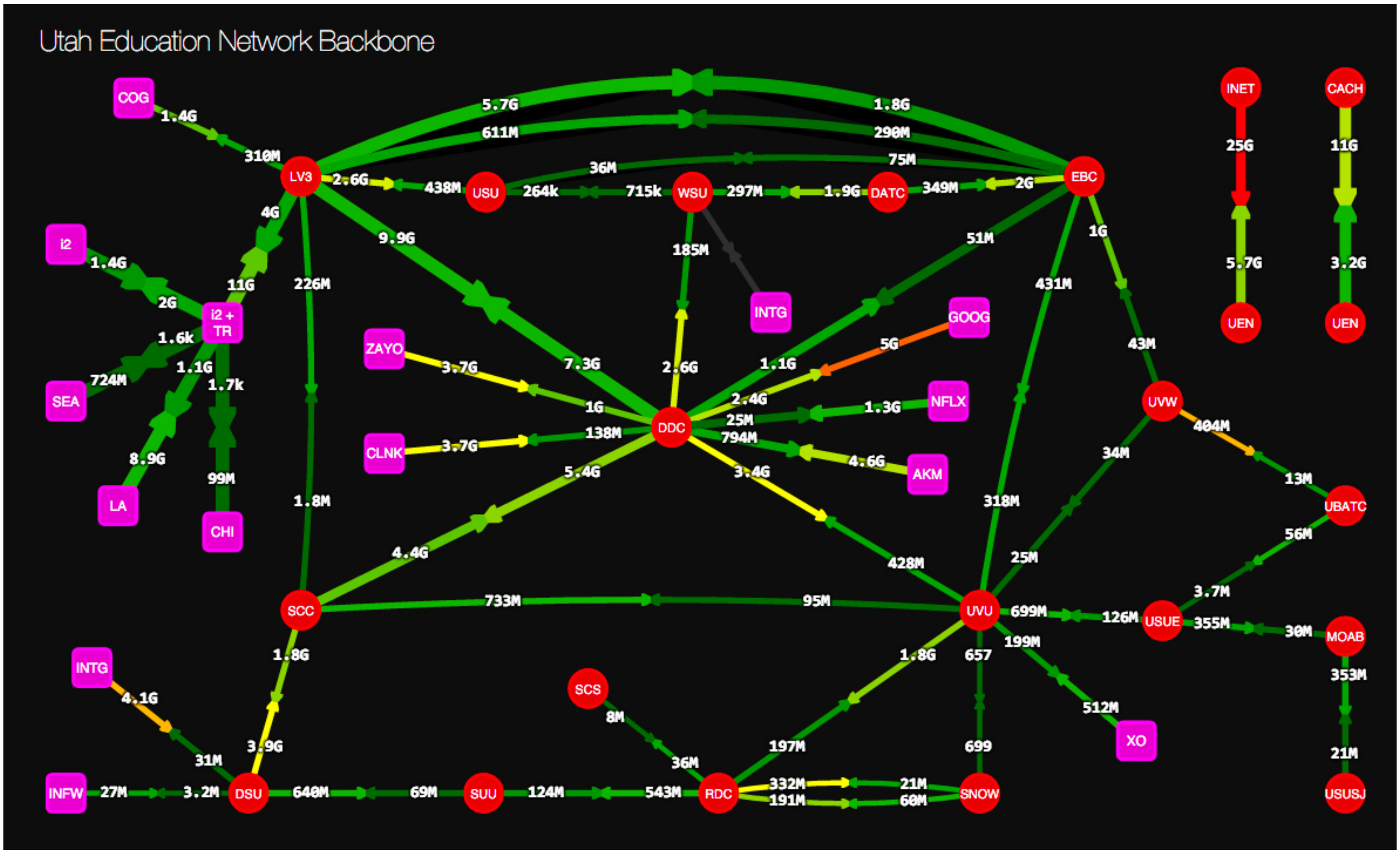

Utah Education Network Backbone
COG
1.4G
310M
LV3
5.7G
611M
1.8G
290M
75M
36M
2.6G
438M
USU
264k
715k
WSU
297M
1.9G
DATC
349M
2G
EBC
INET
25G
5.7G
UEN
CACH
11G
3.2G
UEN
i2
1.4G
2G
4G
11G
226M
9.9G
185M
INTG
51M
431M
1G
i2 + TR
1.6k
1.1G
1.7k
SEA
724M
8.9G
LA
99M
CHI
ZAYO
3.7G
7.3G
2.6G
1.1G
GOOG
5G
43M
1G
2.4G
25M
NFLX
1.3G
UVW
CLNK
3.7G
138M
DDC
794M
4.6G
AKM
404M
34M
13M
5.4G
3.4G
318M
UBATC
1.8M
56M
4.4G
428M
25M
3.7M
SCC
733M
95M
UVU
699M
126M
USUE
355M
30M
MOAB
1.8G
1.8G
657
199M
INTG
4.1G
SCS
8M
512M
XO
353M
3.9G
31M
36M
197M
699
21M
INFW
27M
3.2M
DSU
640M
69M
SUU
124M
543M
RDC
332M
191M
21M
60M
SNOW
USUSJ

Exhibit E

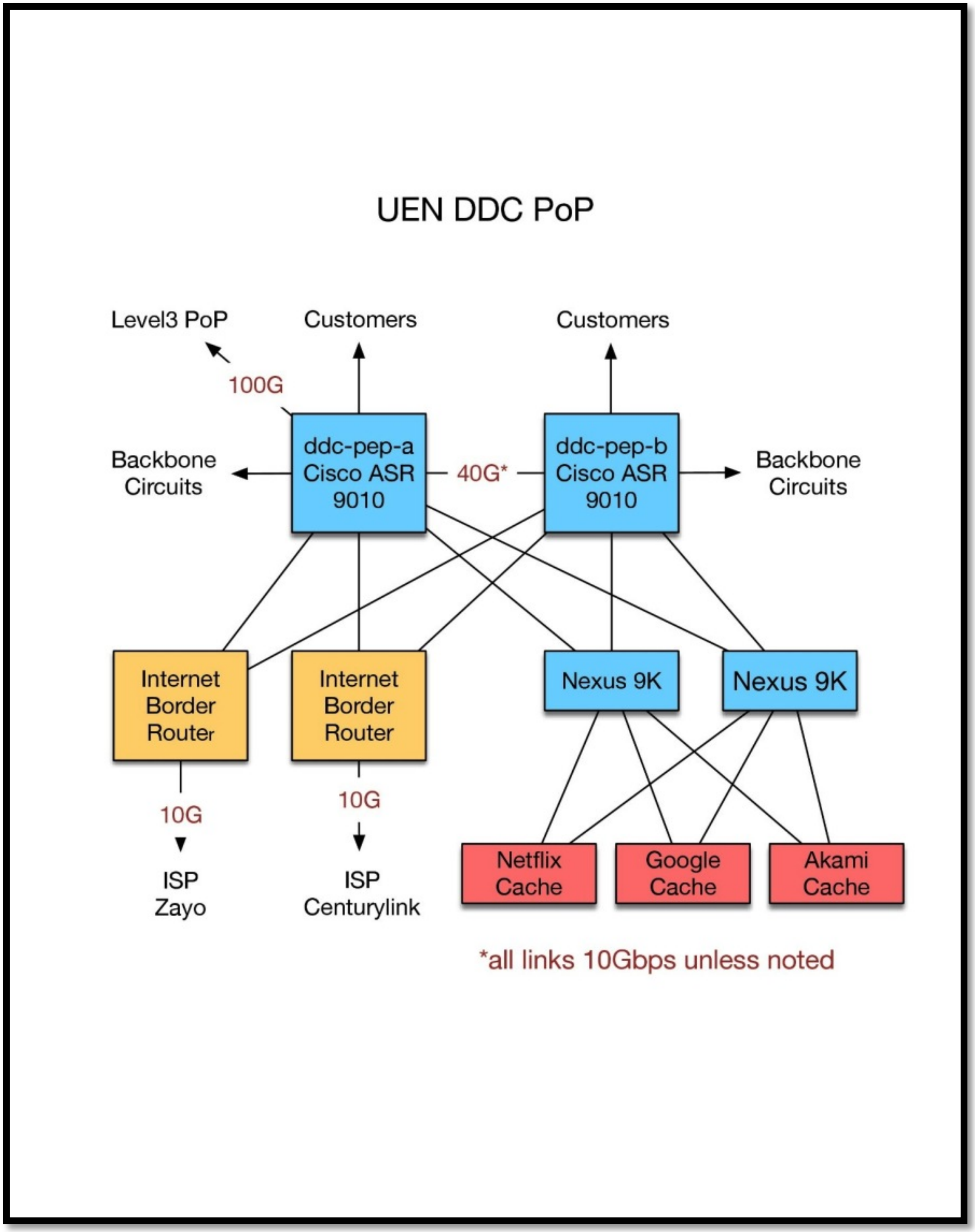

UEN DDC PoP
Level3 PoP
Customers
Customers
100G
Backbone Circuits
ddc-pep-a Cisco ASR 9010
40G*
ddc-pep-b Cisco ASR 9010
Backbone Circuits
Internet Border Router
Internet Border Router
Nexus 9K
Nexus 9K
10G
10G
ISP Zayo
ISP Centurylink
Netflix Cache
Google Cache
Akami Cache
*all links 10Gbps unless noted

Exhibit F

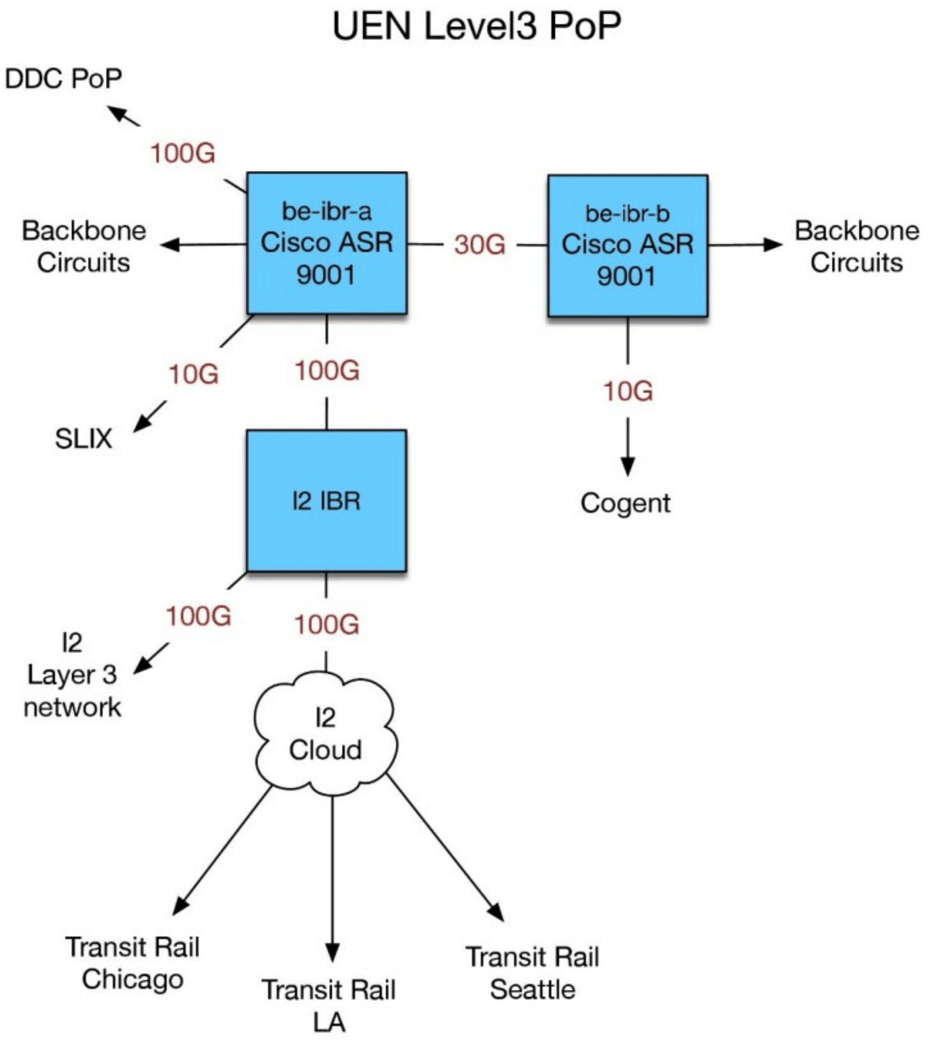

UEN Level3 PoP
DDC PoP
100G
Backbone Circuits
be-ibr-a Cisco ASR 9001
30G
be-ibr-b Cisco ASR 9001
Backbone Circuits
10G
100G
10G
SLIX
I2 IBR
Cogent
100G
100G
I2 Layer 3 network
I2 Cloud
Transit Rail Chicago
Transit Rail LA
Transit Rail Seattle

Exhibit G

UETN's Security *Current State* Overview

Provided by UETN

The UETN Security Operations Center (SOC) is responsible for maintaining the security of the Utah Education Network infrastructure and enterprise. SOC's focus for security remains around the UETN enterprise network. Traditionally, UETN's security controls have NOT extended beyond the network handoff to connected sites and customers. UETN also provides advanced assistance to some customers in Incident Response and Incident Handling, Tools Management and Monitoring, etc.

Tools and Technology

UETN uses NetFlow technology to monitor and store all metadata for network INBOUND and OUTBOUND traffic. This data is currently stored for 7-8 months before being expunged due to disk space considerations. This system is custom-built for use specifically on the UETN network. It's highly adaptive and one of UETN's more powerful analytics tools for security.

UETN uses platforms for firewalling data centers, enterprise applications and services which are configured for "High Availability" and provide a white-listed security posture for all of UETN systems and services. Networks internally are well segmented and intra-network rules are applied providing as much protection from one area to another without impeding operations requirements from the districts.

UETN facilitates high-end security training for not only their customers, but to the entire state of Utah. This is performed through UETN's support of the UtahSAINT Organization and their annual SAINTCON conference.

UETN uses current security control standards for securing access to, and monitoring of its critical infrastructure and architecture. These include 2-factor authentication, log monitoring, intrusion detection, etc.

Security Capabilities (declassified)

UETN has the ability to detect and mitigate DDoS attacks targeting the network. Some mitigation can be limited, depending on the attack type. All attacks can be fully mitigated, but the resulting impact on the destination site may cause them to also be offline.

UETN has the ability to "off-ramp" traffic on the network for analysis. This includes the ability to perform deep packet inspection on designated traffic. This is most often employed for malware analysis and response.

UETN has the ability to detect scans, compromise attempts and actual compromises of machines on the network using data analytics from tools built in-house. These incidents are responded to depending on their impact on the network or network stakeholders.

Incidents and Events
UETN's Network is a continuous "hotbed" of security issues and incidents and is under attack 24/7. There are constant attacks against services and systems hosted on the network.

1. Distributed denial-of-service (DDoS) Attacks – an attack in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

UETN is experiencing exponential growth in the number of and impact from DDoS attacks. UETN encounters an average of 5 impactful DDoS attacks each day. These attacks are most often targeting K-12 education sites. UETN quickly mitigates impactful DDoS attacks with tools and systems developed and managed by their Security Operations Center (SOC).

2. Compromised Machines / Malware – Malware is any software used to disrupt computer operations, gather sensitive information, or gain access to private computer systems.

UETN has a large number of connected sites and devices using the network. These devices and their security are managed independently from UETN, and are often prone to compromise. Once compromised these devices are often used to propagate attacks and collect information from a site/customer.

3. Digital Millennium Copyright Act (DMCA) and Abuse Complaints - A United States copyright law, implemented to comply with the two 1996 World Intellectual Property Organization (WIPO) copyright treaties.

The UETN Network is used by a diverse group of individuals. It is very common for UETN to receive and respond to DCMA or Abuse complaints for IP addresses registered to the UETN organization and allocated to schools, libraries or other connected organizations.

4. Law Enforcement Queries and Information – computer access to law enforcement.
UETN receives numerous requests for information and assistance in locating or tracking information that flows through the network. These requests follow strict processes for information disclosure with the majority ending up being served without a subpoena (basic subscriber information).

Standards
The UETN Security office follows industry supported standards for its security planning and architecture. UETN has been using the SANS Top 20 Security Controls Recommendations for over (4) years and are in the process of converting to the NIST SP800 series standards.[9]

Training and Education
UETN works closely with the UtahSAINT Organization a (501(c)(6) non-profit) to provide quality security training for UETN connected customers.[10] Nearly all institutions connected to UETN participate in the annual SAINTCON conference.

[9] SANS Top 20 SCS – http://csrc.nist.gov/publications/PubsSPs.html#SP 800
[10] "Documents", UtahSAINT Organization, *Article 2, Section 1* - https://www.utahsaint.org/

UETN Customer Capabilities

The UETN Security Operation Center (SOC) provides a significant amount of resources to assist school Districts and other connected customers, but the primary responsibility of security both in detection and enforcement are that of the connected customer. UETN requires that all connected entities provide a firewall or similar border protection system to keep their network secure. The maintenance and development of these firewalls are the responsibility of the individual customers. In rare cases UETN does provide this service for qualified customers.

Generally speaking, all connected sites to UETN have a firewall and those devices provide basic security monitoring and enforcement for each customer. The districts are equally distributed between 2 types of firewalls manufacturers.

Security staffing resources are limited for connected customers with only institutions of higher education maintaining full time personnel committed to this kind of work. Some other customers do retain qualified staff but this is not the norm.

Tools and services used by Districts include the use of free tools provided by UETN. The most prominently used UETN provided tool is Mantella, a net flow monitoring and management tool developed and maintained by UETN. It provides real-time monitoring of network traffic and aides in the detection of malicious traffic and compromised machines.

Exhibit H

Content Filtering *Current State* Overview

Provided by UETN

UETN manages an ongoing process to provide education organizations within the state of Utah with a scalable, affordable Internet content filtering solution that will allow them to comply with state and federal laws. To comply with Law, the solution must block inappropriate content on and off campus for all district owned internet browsing capable devices. It must also monitor and log traffic for reporting purposes. An additional consideration includes that the solution be scalable to the various sizes of organizations supported by UETN. Lastly, the solution should be intuitive enough to be manageable for the administrators of the various organizations.

Tools and Technology

UETN uses industry-leading Secure Web Gateway Solutions (SWG). SWG's to protect Web-surfing devices from infection by enforcing company policies that filter unwanted software/malware from user-initiated Web/Internet traffic including enforcement of legal and regulatory policy compliance.

In the past, UETN tried to locate a central filtering service at Eccles Broadcast Center. As the network grew along with complexity, it became necessary to decentralize content filtering and turn the management of content filtering over to the organizations served by UETN. Today, UETN purchases licensing for SWG that covers all UETN customers statewide. This licensing is currently priced at $115,000.00 per year for the entire state. Education organizations are only required to purchase the appropriate size SWG appliance hardware.

UETN's SWGs are used in all but one of the 41 school districts and are deployed in over 65 charter schools, Applied Technology Colleges, libraries, community providers and private schools. The single outlier is using a different solution which was previously endorsed as a viable. Prior to purchasing the current SWG licensing, 25% of UETN customers chose to use a different product for content filtering. However, since the move to the current solution, all but the one remaining district, who is currently nearing the end of a multiyear contract, have migrated to the current solution as their chosen content filtering tool.

Historically, Child Internet Protection Act and Protecting Children in the 21st Century Act have been the compliance focus for Federal and State Legislation.[11] On March 25, 2015, House Bill 213 was passed by the Utah State Legislature that adds the mandate to filter district owned devices when off campus [12] but no funding was attached to the Bill.

Although the current SWG has options available to account for offsite filtering, this need requires significant hardware upgrades and expense for those institutions actively working toward compliance.

Current SWG – Blocks and monitors content in the following ways:

[11] FCC Children's Internet Protection Act - https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

[12] Utah State Legislature - http://le.utah.gov/~2015/bills/static/HB0213.html

Secure Web Gateway - Content Blocking and Monitoring Protocols

URL	Application Signature	SSL	Decryption	Keyword	Social Media	Browser & OS	Search Engine Controls	Ports	Mime Types	Domain Extensions	File Extensions
HTTP and HTTPS (standard and non-standard ports)	Streaming	Domain Enforcement	Per subnet	Blocking on unencrypted or decrypted traffic with alerts	Facebook	Limit browser applications used and version	Block encrypted search				
Block list (per user group)	Chat	Non-standard ports	Per domain		Pinterest		Image scrubbing				
Category 49	Gaming	Rogue encrypted connections	Per category		Spotify		Limit additional search engine products				
Category priorities (additional granularity)	File Sharing				Linkedin		Restrict Google service domains				
Direct IP access	News Groups				Youtube		Enforce safe search				
Legacy HTTP 1.0 requests	Remote Protocols										
Reverse DNS lookup support	High Risk Activities										

UETN's current SWG is capable of monitoring and alerting inappropriate user actions, clustering multiple appliances, blocking content in an inline layer 2 bridge manor, as well as, TAP Mode out of line, and proxy mode for off-site filtering. It will integrate with multiple Lightweight Directory Access Protocol (LDAP) directories, work with Windows, Mac, Chrome devices and many of the blocking features can be configured based on time frames to provide greater flexibility for the districts, an important consideration.

Support Resources

Currently, UETN has (4) network security analysts assigned to support the current SWG solution and a security analyst on call 24/7 to respond for content filtering issues. UETN purchased a small pool of spare content filtering hardware to provide for a quick, temporary replacement of failed hardware to aid with support.

To ensure that UETN is always providing the best solutions available, UETN adheres to a process of constant evaluation. UETN conducts RFP processes asking for vendors who sell a product in this technology space to respond with technical specifications and features of their product. The initial responses are qualified or eliminated by a core group consisting of UETN Network Operations staff, UETN Security Operations staff and other volunteers selected from the body of UETN stakeholders (usually 4 people). The responses are evaluated based on specified criteria listed in the RFP. Once the core group narrows the candidates to 3, a larger group of volunteers pulled from the body of UETN stakeholders (ideally, one representative from each organization type when possible) is selected to do a more in-depth evaluation in which the hardware is tested in various environments to evaluate its ease of use, feature set, scalability, reliability, support etc. as defined the RFP. This larger group is deemed the "Filtering Committee" containing approximately 15 participants.

Once the top three products are thoroughly evaluated and scored on their technical ability to perform the desired function, the cost analysis is done by procurement and added to the technical scores. Lastly the results are evaluated and a product is selected. Through this process UETN is able to choose the best product available and get the best price while also getting a high level of "buy in" support from UETN stakeholders. This process generally takes 6 to 9 months with contracts generally negotiated for a (3) year license and an option to extend at the same cost for an additional (2) years based on adequate performance of the product over time. If the product does not perform well in the first (3) years, the process is started over again. If the contract is renewed, UETN will still start a new RFP process at the onset of the 5th year.

Issues

The biggest issue encountered in relation to content filtering is funding. Many of UETN's customers do not have the budget to implement all the hardware needed or the budget to employ security professionals to implement it and are just doing the best they can with what they have. UETN's budget for filtering has not changed in over a decade and it becomes increasingly difficult to provide the level of service needed in this area with the funding that we have.

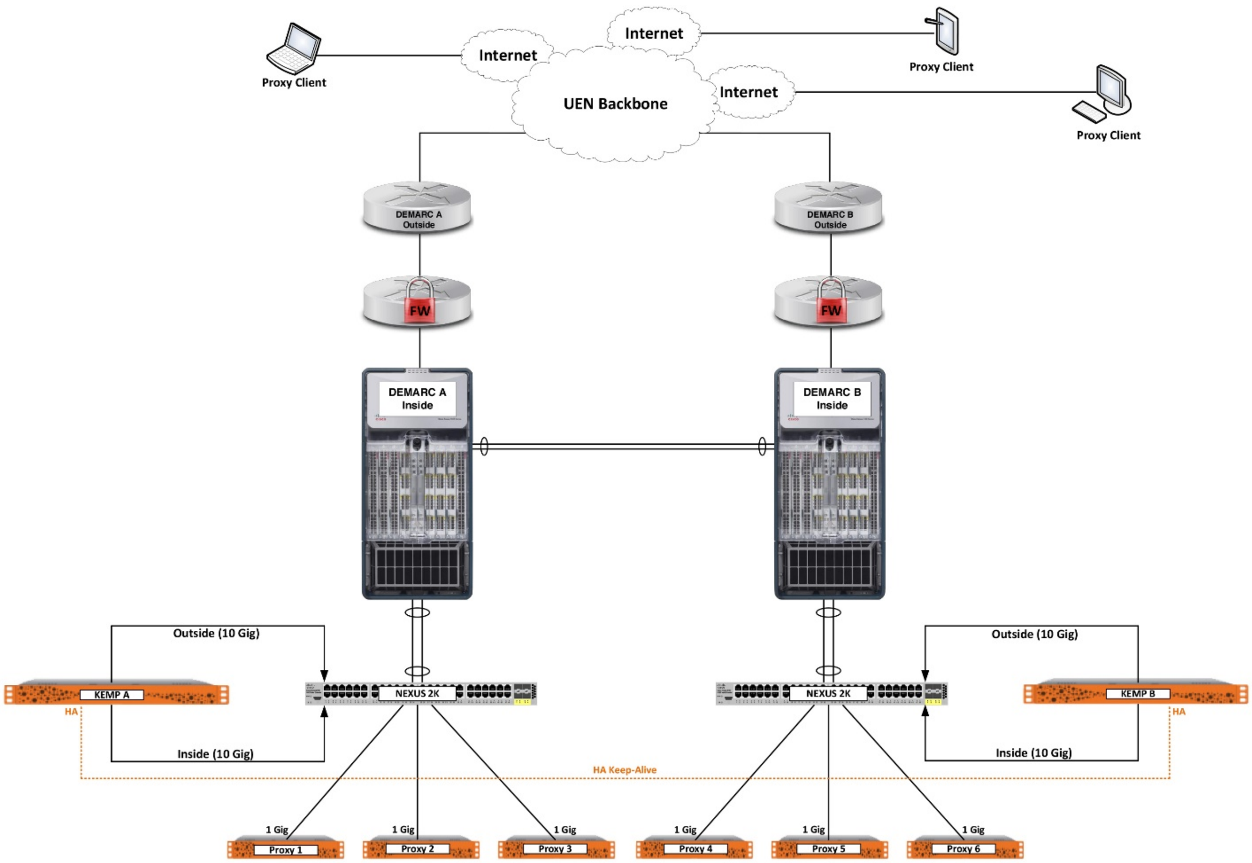
The second issue is the education of UETN's customers on how to deploy, configure, monitor and administrate the SWG appliances such that they are able to take advantage of all features and benefits. Most events are caused when a student is able to gain access to inappropriate content because of misconfigurations within the product.

In today's internet environment, Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption, SSL's replacement, are preventing SWG solutions from identifying traffic content beyond the domain and IP address of its origination. SSL decryption technologies can mitigate some of these issues and allow the SWG solutions to continue performing keyword and individual page filtering. Enabling this feature breaks many applications and services that utilize SSL pinning, it often also requires additional hardware to handle the increased load. As more applications adopt SSL pinning, this option becomes less and less viable. Because of this, few customers are implementing this technology.

UETN Considers a Solution for HB213

UETN is considering assistance for stakeholders to comply with HB213 by installing a "Proxy Filtering Cluster" at the Downtown Data Center (DDC). The proxy cluster, to be effective, would need to be centrally located and redundant in every way to ensure 100% availability.

UETN is considering the build out of a redundant proxy service using load balancers and content filters.



The current proxy service could be balanced (TCP 8009). Session persistence is a requirement as is maintaining the source IP of the client request via transparent or routed load balancing architecture where x-forwarded-for (XFF) headers are not needed. Due to these specific requirements, a specific load balancer would be required to handle the specific requirements for this architecture. The proxy appliances can use the load balancers as their default gateway. DNS based load balancing and or gratuitous Arp would be ideal methods for handling failover. The load balancers and the current proxy appliances would be connected via infrastructure already in place and protected behind UETN's firewall.

The load balancer includes (3) year 24/7 Premium Support. The 14600 appliances are covered under UETN's current SWG support contract and include a (5) year hardware warranty. It's estimated that (1) FTE be added to the UETN Network Security team to support this service.