Baseline Network Standard: Architecture
ITRP Development Initiative

The content of this and other documents describing ITRP are the result of the work of a number of development teams established under the Network Technology Alliance committee within the California State University.

Team members who directly contributed to the content of this document are listed below.

<table>
<thead>
<tr>
<th>Name</th>
<th>Development Team</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Johanna Madjedi</td>
<td>Development Team 1 Chair</td>
<td>Cal Poly SLO</td>
</tr>
<tr>
<td>Karen Anderson</td>
<td></td>
<td>San Diego State University</td>
</tr>
<tr>
<td>Chris Bramble</td>
<td></td>
<td>Sonoma State University</td>
</tr>
<tr>
<td>Michel Davidoff</td>
<td></td>
<td>CSU Chancellors Office</td>
</tr>
<tr>
<td>Mike Marcinkevicz</td>
<td></td>
<td>CSU Fullerton</td>
</tr>
<tr>
<td>Will Moran</td>
<td></td>
<td>CSU Northridge</td>
</tr>
<tr>
<td>Jim Noonan</td>
<td></td>
<td>Sonoma State University</td>
</tr>
<tr>
<td>Casey Smith</td>
<td></td>
<td>PlanNet Consulting</td>
</tr>
<tr>
<td>Mark Smith</td>
<td></td>
<td>Callisma Inc.</td>
</tr>
<tr>
<td>Nigel Willson</td>
<td></td>
<td>Callisma Inc.</td>
</tr>
</tbody>
</table>

Valuable administrative support was provided by Adrienne Rappaport
# ITRP Baseline Network Standard: Architecture

## 1. Table of Contents

1. **Document Scope** ........................................................................................................... 7
2. **Introduction** .................................................................................................................. 8
3. **Architectural Principles** ............................................................................................. 10
   3.1. Baseline Compliance .................................................................................................. 10
   3.2. Advantages in Working Together ............................................................................ 10
   3.3. Campus Commitment to Implementation and Deployment ................................... 10
   3.4. The Network is a Critical Technology Infrastructure Utility .................................. 10
   3.5. Standards-based Solutions will be used within the Baseline where Possible .......... 10
   3.6. Evolution not Revolution ......................................................................................... 11
   3.7. Support Innovation from within ............................................................................. 11
   3.8. Best Service with Resources Available ................................................................... 11
4. **Campus Network Models** .......................................................................................... 12
   4.1. Understanding the Model Descriptions .................................................................... 12
   4.2. Interpreting the Icons ............................................................................................... 12
   4.2.1. Primary Core Switching (PCS) ........................................................................... 12
   4.2.2. Secondary Core Switching .................................................................................. 12
   4.2.3. Distribution Switching ....................................................................................... 12
   4.2.4. Server Farm Distribution Switching .................................................................... 13
   4.2.5. Access Switching .............................................................................................. 13
   4.2.6. End-User Platform ............................................................................................. 13
   4.2.7. Server Farm ........................................................................................................ 13
   4.2.8. Routing Component ............................................................................................ 13
   4.2.9. Gateway Component .......................................................................................... 13
   4.2.10. Network Management Component ................................................................. 14
   4.2.11. Network Authentication Components .............................................................. 14
   4.2.12. Layer 2/4 Traffic Filtering Component ............................................................... 14
   4.2.13. Layer 4/7 Inspection and Filtering Component .................................................. 14
   4.2.14. Network Transport Encryption Component ..................................................... 14
   4.2.15. Network Traffic Surveillance Component ......................................................... 15
   4.3. Availability ................................................................................................................. 15
   4.3.1. Measurement ....................................................................................................... 15
   4.3.2. Out-of-band Notification ...................................................................................... 15
   4.3.3. Availability Target ............................................................................................... 15
5. **Physical Layer Design** ............................................................................................... 17
   5.1. Physical Design Concerns ....................................................................................... 17
   5.1.1. Electrical Power .................................................................................................. 17
   5.1.2. Heating Ventilation and Air Conditioning (HVAC) .............................................. 17
   5.1.3. Fiber Plant .......................................................................................................... 17
   5.1.4. Telecommunication Room Layout (Space Plan) ................................................ 18
   5.1.5. Patch Cables ....................................................................................................... 18
   5.2. Considerations beyond “Common Services” ........................................................... 18
   5.2.1. Wireless ............................................................................................................. 18
   5.2.2. Voice over IP ..................................................................................................... 18
ITRP Baseline Network Standard: Architecture

5.2.3. Video over IP ................................................................. 18
5.2.4. Physical Security .......................................................... 18
5.2.5. Uninterruptible Power ................................................. 19

6. Supported Protocols .............................................................. 20
   6.1. TCP/IP ......................................................................... 20
       6.1.1. IPv4 ...................................................................... 20
       6.1.2. IP Storage Protocols ........................................... 20
       6.1.3. Multicast ............................................................. 20
   6.2. Legacy Protocols ............................................................ 20
       6.2.1. Legacy Protocol Retirement Schedule .................... 20
   6.3. Routing Protocols ............................................................ 20
       6.3.1. OSPF ................................................................. 20
       6.3.2. BGP ................................................................. 20

7. Network Performance Architecture ........................................... 21
   7.1. Service Level Targets / Performance Targets .................. 21
   7.2. Devices Requiring Baseline Performance ....................... 21
   7.3. Devices Requiring Enhanced or High Performance .......... 21
   7.4. Performance Attributes .................................................. 21
       7.4.1. Transit Delay ..................................................... 21
       7.4.2. Jitter ................................................................. 22
       7.4.3. Packet Loss ....................................................... 22
       7.4.4. MTU (Maximum Transmission Unit) Support for New Applications 22
       7.4.5. Traffic Profile defines acceptable performance ...... 23
   7.5. Performance Design ....................................................... 23
       7.5.1. Bandwidth Controls ............................................. 24
       7.5.2. Traffic Management/Quality of Service (QoS) ......... 24
       7.5.3. Intra-networking ............................................... 24
       7.5.3.1. Core Infrastructure Performance Requirements .... 24
       7.5.4. Oversubscription and Blocking ......................... 24
   7.6. Site to Site Networking Performance Levels .................... 24

8. Network Security Architecture ............................................... 25
   8.1. Network Security Domain ............................................. 25
   8.2. Design Objectives ......................................................... 26
       8.2.1. Defense-in-Depth .............................................. 26
   8.3. Physical Network Security .............................................. 26
       8.3.1. Physical Infrastructure Components ..................... 26
   8.4. Logical Network Security ............................................... 27
   8.5. Network Component Security ........................................... 27
       8.5.1. Access Layer .................................................... 27
       8.5.2. Distribution Layer .............................................. 28
       8.5.3. Core Layer ....................................................... 28
       8.5.4. Network Enabling Services .................................. 28
       8.5.5. Network Management Services ......................... 28
   8.6. Perimeters ................................................................. 29
       8.6.1. Boundary Perimeter ........................................... 29
       8.6.2. Static Security Zones ........................................... 29
IITRP Baseline Network Standard: Architecture

8.6.3. Management Zone ................................................................. 29
8.6.4. Dynamic Security Zones ....................................................... 29
8.7. Network Security Levels .......................................................... 30
8.7.1. Baseline .............................................................................. 30
8.7.2. Above Baseline .................................................................... 30
8.8. Network Security Components ............................................... 30
9. Network Management Architecture .......................................... 33
9.1. Fault ..................................................................................... 33
9.2. Configuration ......................................................................... 33
  9.2.1. Configuration Control ......................................................... 33
  9.2.2. Change Management .......................................................... 33
9.3. Accounting 'Capable' ............................................................. 34
  9.3.1. Usage by user/department .................................................. 34
9.4. Performance ........................................................................... 34
  9.4.1. Performance Monitoring .................................................... 34
  9.4.2. Alarm Generation .............................................................. 34
  9.4.3. Performance Reporting ...................................................... 34
  9.4.4. Bandwidth Shaping ............................................................ 34
  9.4.5. Network Flows ................................................................. 34
9.5. Security .................................................................................. 34
  9.5.1. Protection Framework ......................................................... 35
  9.5.2. Detection Framework ........................................................ 35
  9.5.3. Response Framework ........................................................ 35
  9.5.4. Management Framework .................................................. 35
9.6. Asset Management .................................................................. 36
10. Network Enabling Services ...................................................... 37
  10.1. DNS .................................................................................... 37
  10.2. DHCP .................................................................................. 37
  10.3. Authentication ..................................................................... 37
  10.4. NMS Servers .................................................................... 37
  10.5. Syslog ................................................................................. 37
  10.6. NTP .................................................................................... 37
  10.7. Other Enabling Services ..................................................... 38
    10.7.1. POE ............................................................................ 38
11. Profiling Campus Network Traffic ............................................ 39
  11.1. Profiles ............................................................................... 39
    11.1.1. User Types .................................................................... 39
    11.1.2. Application Types .......................................................... 41
    11.1.3. Traffic Types ................................................................. 42
12. Modeling Steps ................................................................. 44
  12.1. Determine Network Infrastructure Roles ................................ 44
    12.1.1. End-User Network Infrastructure ..................................... 44
    12.1.2. Server Farm Network Infrastructure .................................. 44
    12.1.3. Gateway Services Network Infrastructure ....................... 44
    12.1.4. Enabling Services Network Infrastructure ....................... 44
  12.2. Determine Traffic Profiles .................................................. 44
ITRP Baseline Network Standard: Architecture

12.3. Determine Area-Specific Availability, Security, and Performance .............................. 44
12.3.1. Determine Area-Specific Availability Requirements .................................................. 45
12.3.1.1. Baseline Availability .......................................................................................... 45
12.3.1.2. Enhanced Availability ....................................................................................... 45
12.3.1.3. High Availability ............................................................................................. 45
12.3.2. Determine Area-Specific Security Requirements ...................................................... 45
12.3.3. Determine Area-Specific Performance Requirements .............................................. 45
12.4. Select and combine each appropriate area model ......................................................... 46
12.5. Determine Network Management Requirements ........................................................ 46
12.6. Determine Routing Architecture .................................................................................. 46
12.7. Availability Model Selection ......................................................................................... 46
12.7.1. End-User N/I: Baseline Availability ......................................................................... 47
12.7.1.1. Connectivity ....................................................................................................... 47
12.7.2. End-User N/I: Enhanced Availability ...................................................................... 48
12.7.2.1. Connectivity ....................................................................................................... 48
12.7.3. End-User N/I: High Availability ............................................................................. 49
12.7.3.1. Connectivity ....................................................................................................... 49
12.7.4. Server Farm N/I ..................................................................................................... 50
12.7.4.1. Connectivity ....................................................................................................... 50
12.7.5. Enabling Services N/I ............................................................................................ 51
12.7.5.1. Connectivity ....................................................................................................... 51
12.7.6. Gateway Services N/I ........................................................................................... 52
12.7.6.1. Connectivity ....................................................................................................... 52
12.7.3. Target Service Level .............................................................................................. 53
12.7.4. Target Service Level .............................................................................................. 53
12.7.5. Target Service Level .............................................................................................. 53
12.7.6. Target Service Level .............................................................................................. 53
13. An Example of Modeling a Campus Network ................................................................. 53
13.1. Napa State University (NSU) Campus Network ............................................................ 53
13.1.1. Determine Network Infrastructure Roles ............................................................... 55
13.1.2. Determine Traffic Profiles .................................................................................... 57
13.1.3. Determine Area-Specific Availability, Performance, and Security .................... 60
13.1.4. Determine Network Management Requirements .................................................... 64
13.1.5. Determine Routing Architecture .......................................................................... 64
13.2. NSU ITRP 2 Network .................................................................................................. 64
14. Document Control .......................................................................................................... 66
2. Document Scope

This document forms part of a group of documents that collectively define version 2 of the Infrastructure Terminal Resources Program (ITRP 2).

This document describes the Network Baseline Architecture for the ITRP 2 Program.

The architecture elements are used to describe the functional requirements and performance specifications that lead to the selection of a specific CSU campus implementation, selection and deployment of specific equipment and software. As illustrated on the title page, the Baseline Architecture defines the “what” of the network that must be deployed as each CSU campus. The overall architecture for ITRP is defined by the Technical Architectural Reference Model, which is described in detail in ‘ITRP2: Technical Architectural Reference Model’. For reference, the model is reproduced below:

CSU ITRP SOE 2.0 Technical Architectural Reference Model
3. Introduction

The Network Baseline Architecture is built from many pieces and so represented in several sections as follows:

Section 3: Architectural Principles
These principles are not specific to a certain function or performance criteria, but are necessary to ensure the overall solution meets the vision of the CSU for the ITRP Program 2.

Section 4: Campus Network Models
Each CSU campus is expected to have different user/application profiles as well as unique physical plant designs that drive performance and functional needs and thus a final implementation and deployment plan. These network models describe choices available based on those specific campus requirements. Four different network models, representing various levels of expected service availability, have been established that may be implemented on each campus. It is expected that each campus’ implementation will be comprised of some combination of these models.

Section 5: Physical Layer Design
While the Telecommunications Infrastructure Planning Standards (TIP Standards) reflect the requirements for spaces, pathways and cabling for new and remodeled spaces, some additional physical plant requirements must be in place in order to support the overall Baseline Architecture. This section describes those requirements that are outside TIP or directly specify which TIP standards must be in place to support an implementation.

Section 6: Supported Protocols
The protocols needed to support in the functional and performance specifications as part of the overall Baseline architecture.

Section 7: Network Performance Architecture
Network infrastructure performance criteria have been established to support combined user and application requirements such as low jitter, low delay, and/or loss packet loss. These criteria are layered onto the network models.

Section 8: Network Security Architecture
Network security must be in place to ensure the Baseline solution can meet the functional and performance specifications identified. Network security architecture specifications have been included to reflect those needs not covered by functional or performance specifications.

Section 9: Network Management Architecture
Network management tools must be in place to ensure that campuses can manage the Baseline solution. Network management architecture specification have been included to reflect those needs.

Section 10: Enabling Services
Some overlay services have been identified as essential in order to utilize the network. This section describes the functional and performance specifications for those services.
Section 11: Profiling Campus Network Traffic
Understanding user and application profiles helps define the availability and performance requirements for a campus network. This section describes common user and application types and then proposes how those types can define traffic profiles that drive the campus availability and performance requirements.

Section 12: Modeling Steps
This section describes the steps used to model the campus network. An example of this process is provided in Section 13.

Section 13: An Example of Modeling a Campus Network
This section describes a factious campus and how the network modeling steps described in section 6 can be applied to an ITRP 1.0 environment to establish an ITRP 2 design.
4. Architectural Principles

These principles reflect overarching concepts that will be considered in the Baseline solution.

4.1. Baseline Compliance

The network baseline standard implementation for a campus is expected to provide a baseline service level as identified in this architectural document. At a minimum, campuses are expected to implement the baseline standard. As such, variance from the network baseline standard implementation is prohibited without the written approval of the Assistant Vice Chancellor of Information Technology Services or his/her designee. Requests for variance shall identify the specific standard(s) in question, the reason(s) for the requested variance(s) and a description of the proposed alternative(s).

4.2. Advantages in Working Together

As the overall goal of this program is to provide network services to all state facilities in the CSU, through maximum network reliability on campus and optimal network interoperability between campuses with available resources, campuses will work together to reach that end.

4.3. Campus Commitment to Implementation and Deployment

In order to determine the best implementation and deployment plan, leadership from the campus’ central IT organization is required. Activities will include but are not limited to identification of key applications, users, performance requirements as well as any specific security requirements which must be addressed in the implementation plan.

4.4. The Network is a Critical Technology Infrastructure Utility

Standard wiring and up-to-date standards-based network equipment allow campuses to deliver a set of defined “baseline services,” thus meeting the CSU’s Integrated Technology Strategic goal of providing consistent, reliable access to all CSU campuses. These standards for the baseline deployment establish a specific quality of service, reliability and line speed to faculty, staff and students, thereby assuring that the network does not inhibit, but instead promotes the technology used to enhance learning as well as running the business side of a university.

The network baseline standard architecture, design and implementation must be specified to ensure the ability to actively protect, detect, monitor, and respond in a systematic, disciplined and coherent way to threats that affect the performance and security of the network and consequently the information or services that rely on the network’s performance. For instance, network equipment that has remote management capabilities is required to enable performance and security monitoring.

4.5. Standards-based Solutions will be used within the Baseline where Possible

The baseline architecture will emphasize criteria that is standards based and non-vendor specific. However, a vendor specific solution may be implemented by NTA working groups if it is the best option to meet the architectural criteria.
4.6. Evolution not Revolution
The recognition that performance and security requirements change over time requires the Baseline Architecture to be reviewed and updated on a periodic basis. However, it is expected that the previous Baseline Architecture will be included in that review process with appropriate aspects retained.

4.7. Support Innovation from within
A campus may choose to act as an early adopter of new network technology services, augmenting the network baseline standard. Campuses are encouraged to share their experiences as it is anticipated that many services will follow an evolutionary path from campus specific network service into baseline. This supports a process whereby technology innovation that occurs at individual campuses can be leveraged over time by the whole CSU system.

4.8. Best Service with Resources Available
The method for determining the deployment of baseline network equipment and software is a balance of need and funding resources available. Therefore, it is important that campuses establish reasonable requirements and service expectations for availability, performance and security for their campus deployments.
5. Campus Network Models

This section presents the range of network models that are supported by the ITRP 2 Network Technical Architecture Reference Model (NTARM). All campuses will implement a combination of these models within their network, based on their specific needs. The models support environments with varying criticality, security, performance, and management needs. It is anticipated that every campus environment can be mapped to these models.

5.1. Understanding the Model Descriptions

NOTE: The models represent how areas in a physical network WILL be logically architectured. They do not necessarily correspond to specific physical devices. An icon in the model depicts a component that fulfills a logical function. The physical manifestation of a component may be none, one, or more physical devices. Some functions, for example network management, may be implemented as a hardware element or software element in a physical device. Once the architecture of a campus network has been modeled using the categories below, a logical design and physical implementation of the architecture can follow. These will make clear how the architectural components have been physically implemented.

5.2. Interpreting the Icons

The iconography used in the network models are explained below:

5.2.1. Primary Core Switching (PCS)

Primary Core Switching (PCS) is implemented using a high-performance, high-availability engine that switches and routes data, voice and video (DVV). Depending on physical campus layout, performance needs, and other design-level criteria multiple PCS engines may be present and redundantly linked. The PCS engine is optimized to provide high-speed, low-latency DVV switching and routing. High-availability for the PCS will be achieved via redundant engines. Network layer sub-netting may be implemented at the interface to the distribution layer. In a distributed core environment, PCS engines will be interconnected via a common subnet.

5.2.2. Secondary Core Switching

Secondary core switching (SCS) is implemented using a high-performance switching and routing engine with no redundant elements.

5.2.3. Distribution Switching

Distribution switching is implemented using a high-performance switching engine, which provides control over access and use of the core, both from a security and quality of service perspective. For more complex or larger implementations, network layer sub-netting may be implemented at the interface to the access layer. In this case, distribution switching will use a high-performance routing engine. Note that the distribution switching engine is non-redundant.
5.2.4. **Server Farm Distribution Switching**

Server Farm Distribution Switching (SFDS) is implemented using a high-performance, high-availability engine. High-availability for the SFDS will be achieved via a redundant engine. Where servers are attached to two SFDS engines, the second engine is non-redundant.

5.2.5. **Access Switching**

Access switching provides end-user systems and non-critical servers connectivity to the network. A range of media connectivity options, including UTP and wireless are offered here. Some degree of security and access control may be implemented as well as quality of service tagging.

5.2.6. **End-User Platform**

End-user platforms (EUP) include any network-capable device which is authorized by the campus for connection to the network. Specific levels of service provided to EUPs will depend on the network capability of individual EUPs, including protocol support, connectors, etc. ITRP 2 architecture is capable of addressing impact on large groupings of EUPs.

5.2.7. **Server Farm**

The server farm provides for higher levels of performance, security, and availability. In this architecture, server platforms are defined as critical campus computer resources located in a data center. Server platforms are characterized by the high number of active connections they support, with potentially high data transmission and/or reception rates, or deemed critical by the campus. Critical in this context refers to the strategic value to the campus. The application and user profiles prepared by the campus should indicate which servers support which profiles. Servers supporting a critical profile should therefore be placed in the server farm. The project will provide resources for a single server farm per campus.

5.2.8. **Routing Component**

A routing component indicates where a routing engine function has been deployed. Routing is always implemented in the core layer of the network. However, it may be enabled in other areas of the network when availability, performance, or security considerations require it. For example, routing may be enabled in the distribution layer that services certain area models.

5.2.9. **Gateway Component**

A gateway component is a switching and routing engine that may need to include additional functionality to interface with non-campus environments. For example, a Gateway Component connecting to CalREN would include BGP routing capability.
5.2.10. Network Management Component

Network Management System (NMS) components provide distributed management functions to the campus Network Management System. They may support any of the NMS functions. The models only explicitly show NMCs that are likely to be separate and distinct from the management functions that are typically embedded in present-day network devices. For example, a requirement for a standalone RMON probe function would be indicated by the use of this icon, whereas RMON capability embedded in a network switch function, such as the ASC, DSC, or CSC, is not explicitly shown.

5.2.11. Network Authentication Components

Network Authentication Components intelligently controls access to network resources, enforcing policies, and auditing usage. Authentication provides a way of identifying an endpoint or user, typically by having the user enter a valid user name and valid password before access is granted. The authorization process determines whether the user has the authority to access certain information or some network sub-domains. Accounting measures the resources a user consumes while using the network, which includes the amount of system time or the amount of data a user has sent and/or received during a session, which could be used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities. A dedicated AAA server or a program that performs these functions often provides authentication, authorization, and accounting services.

5.2.12. Layer 2/4 Traffic Filtering Component

Layer 2/4 Traffic Filtering (L2F) components control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the layer 2/4 header information for the source and destination. They provide both alerting and logging capabilities that should be sent to and processed by the network management system.

5.2.13. Layer 4/7 Inspection and Filtering Component

Layer 4/7 Inspection and Filtering (L4I) components provide stateful inspection that tracks each connection traversing all interfaces of the filter and makes sure that they are valid. A Layer 4/7 filter does not just examine the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination. A stateful inspection filter also monitors the state of the connection and compiles the information in a state table. Because of this, filtering decisions are based not only on administrator-defined rules but also on context that has been established by prior packets that have passed through the filter. They provide both alerting and logging capabilities that should be sent to and processed by the network management system.

5.2.14. Network Transport Encryption Component

Network Transport Encryption (NTE) components allow private communications, such as remote access to a campus network or high security zone using a public infrastructure. NTEs provide endpoint authentication and communications privacy over the network transport using cryptography. In typical use, only the server is authenticated (i.e. its identity is ensured) while the client remains unauthenticated; mutual authentication requires token deployment to clients. The protocols allow client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery.
5.2.15. Network Traffic Surveillance Component

Network Traffic Surveillance (NTS) components inspect all inbound and outbound network activity and identify suspicious patterns that may indicate a network or system attack. In anomaly detection, the network administrator defines the baseline, or normal, state of the network’s traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and looks for anomalies.

5.3. Availability

When designing for higher availability the goal is to reduce the impact, scale or size of a failure. Higher availability may be obtained via redundant components or cables. Cable redundancy can be achieved via multiple cables going through a single or multiple conduits. Ideally, when using multiple conduits they will take different (diverse) paths across the campus.

5.3.1. Measurement

The network infrastructure will provide statistics to measure performance and availability.

5.3.2. Out-of-band Notification

Out-of-band notification is addressed in section 10.

5.3.3. Availability Target

Availability is defined as the presence of functional pathways within the network infrastructure. A high percentage of availability indicates the network is highly available. Various parts of the network infrastructure will have different availability targets based on user profiles and application profiles.

<table>
<thead>
<tr>
<th>Target Designation</th>
<th>Attributes</th>
<th>Applicable Performance Target (if any)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline</td>
<td>Unscheduled Outages are unpopular but well tolerated</td>
<td>Baseline</td>
</tr>
<tr>
<td>99.7% availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(26 hours downtime per year)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enhanced</td>
<td>Unscheduled Outages affect financial and messaging systems and thus slow the movement of the university operations.</td>
<td>Enhanced</td>
</tr>
<tr>
<td>99.9% availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(8.76 hours downtime per year)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target Designation</td>
<td>Attributes</td>
<td>Applicable Performance Target (if any)</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------</td>
<td>----------------------------------------</td>
</tr>
</tbody>
</table>
| **High**  
99.99 availability  
(52 minutes downtime per year) | Unscheduled Outages are poorly tolerated. Unscheduled Outages affect financial and messaging systems and thus slow the movement of the university operations. The majority of university business (instruction, registration, fee payment, procurement, decision making via electronic exchanges) cannot occur. | Enhanced or High depending on application profile |
6. Physical Layer Design

This section presents the physical and environmental considerations when designing the ITRP 2 network. This is not a replacement for the “Telecommunications Infrastructure Planning Standards” (TIP standards), rather, this is a supplement that helps bridge requirements between ITRP 2 and TIPS. For historical purposes, this replaces the architectural elements of the Stage 1 / Stage 2 Integration document that is used for ITRP 1.0. These sections will be elaborated upon with technical specifics in the implementation and deployment documents that will come later.

NOTE: The section references the TIP Standards which can be found at the following web page: “TIP Standards”. Therefore, the reader is encouraged to review them.

6.1. Physical Design Concerns

The following requirements must be addressed when designing the ITRP 2 Network. Local facilities and IT professionals should make every effort to coordinate their efforts to assure that such requirements are identified and accommodated.

6.1.1. Electrical Power

This section discusses the electrical power requirements for ITRP network switches. All switches identified as redundant switches, require two dedicated circuits; some must be capable of supporting significant ampere load.

The campus may need to forecast the TR locations where core or large switches are likely to be located. A good rule of thumb would be those high-density locations where more than 240 cables are served.

In consideration of the above, campus planners must also address the power requirements for the following:

- Network management servers, security devices, VoIP and Video equipment
- Future power requirements will be driven by network convergence (VoIP and Video) therefore the electrical wire gauge selected must be reusable for higher amperage circuits.
- Convenience power must be located close to equipment so that support staff can power diagnostic equipment or laptops.

6.1.2. Heating Ventilation and Air Conditioning (HVAC)

HVAC designs must accommodate the additional heat loads associated with:

- UPS units and redundant power supplies, particularly in consideration of the large chassis-based core switches.
- Redundant switches

6.1.3. Fiber Plant

ITRP 2 will introduce some new equipment and focus on high availability and increased performance for key areas; this will require more utilization of the fiber plant. Sufficient fiber must be available for the following:

- Redundant switches require additional fiber counts when dual-homed (i.e. 4 strands per TR vs. 2).
- Redundant core switches will require additional fiber counts to tie distribution switches together.
Fiber specifications must be validated for any new equipment, as we anticipate that ITRP and not TIP standards, to drive the new requirements.

6.1.4. **Telecommunication Room Layout (Space Plan)**
Sufficient quantities of rack space must be designed into each TR. Sufficient provisions for physical cable management and conveyance must be included in physical designs.

6.1.5. **Patch Cables**
Campus patch cables must meet industry standards to ensure performance requirements.

6.2. **Considerations beyond “Common Services”**
Below are some special considerations for elements that go beyond ITRP 2 common services.

6.2.1. **Wireless**
To be determined, pending wireless working group recommendations.

6.2.2. **Voice over IP**
Several CSU campuses have or soon will migrate toward converged networks.

- Inter-building cabling must meet the needs for the new traffic.
- Copper plant must support migration to the planned converged network, for example additional cable drops for Phones.

Additional details to be determined, pending VoIP development group recommendations.

6.2.3. **Video over IP**
All campuses are using Video over IP for conferencing. Some are using it for distance learning and even as a replacement for RF transmission of Broadcast Television. The following are some new requirements:

- Sufficient fiber and copper to video distribution and terminal locations to provide Ethernet/IP connectivity.

Additional details to be determined, pending Video over IP development group recommendations.

6.2.4. **Physical Security**
The network equipment within the various TR’s provide a vital service and may even one day carry VoIP traffic and therefore the possibility for 911 and other emergency calls. Therefore, we must do what we can to improve the security of these devices. One area that has not had enough scrutiny is the physical security of the rooms this equipment resides in. This section provides only a brief overview with more on Physical Security in sub-section 9.3.
However some general requirements are:

- Only people who require access will have access to the TR.
- TRs must only have equipment required to implement the cable plan, with the only exception being diagnostic equipment or devices intent on improving security.
- TRs are NOT closets or storage facilities. Do not allow them to be used as such.
ITRP Baseline Network Standard: Architecture

- TRs are not Computer Rooms or Data Centers, other IT equipment (e.g. servers, printers, etc.) belong in their own specialized rooms.
- Physical Security must be maintained: In other words TR’s must be audited periodically and keys must be retired and or changed periodically.

6.2.5. Uninterruptible Power

- Uninterruptible Power Supplies (UPS) and generators should be deployed where needed to support the specific availability targets. Note: The ITRP1 baseline supported the deployment of UPS’s for Core Switches if campuses did not already have a UPS.
7. Supported Protocols

This section presents the range of supported protocols that are included in ITRP 2.

7.1. TCP/IP
TCP/IP is the standard protocol supported. It is the only protocol that is routed natively in the baseline. All higher layer application using these protocols are supported (e.g. HTTP, SFTP, Telnet Etc)

7.1.1. IPv4
The baseline implementation will use IPv4 as the primary addressing protocol.

7.1.2. IP Storage Protocols
All IP based storage protocols are supported (e.g. iSCSI)

7.1.3. Multicast
Multicast capabilities are supported. (e.g. video, ghosting, etc.).

7.2. Legacy Protocols
Many campuses use protocols such as IPX, AppleTalk, DecNet, SNA, and other mini- and mainframe-based protocols.

7.2.1. Legacy Protocol Retirement Schedule
Only IP will be routed across the campus backbone. Prior to the start of the ITRP 2 deployment on a campus, the campus must reconfigure equipment to support an IP-based environment if connectivity across the campus backbone is required. While not inclusive, protocols to consider are IPX, AppleTalk, and DecNet.

7.3. Routing Protocols
OSPF and BGP dynamic routing protocols must be implemented. Static routes may be used where dynamic routing is inappropriate.

7.3.1. OSPF
OSPF is the standard dynamic routing protocol for the campus LAN.

7.3.2. BGP
BGP is the standard for gateway services with dual connectivity to the wide area network.
8. Network Performance Architecture

The performance criteria outlined here are those necessary for trouble-free operation of specific critical application and user profiles across the network infrastructure. The baseline infrastructure will support these performance criteria by supporting “performance profiles” across the network.

8.1. Service Level Targets / Performance Targets

Service Level Agreements (SLAs) are common in the telecommunications industry. In short, the agreements call out the expectations for a delivered service, that is, formal expectations or “targets” are set forth.

In lieu of SLAs, Service Level “Targets” are established in this document to define our expectations for end-to-end delivery of traffic by the network for various application and user profiles.

Service level targets for application performance across the network are defined here; that is, how the network positively affects, improves or maintains the transit of application traffic so that the minimum level of performance by the network is adequate for the application.

Applications define minimum acceptable transit delay, jitter, and packet loss, which in all, affect end-to-end performance of applications.

8.2. Devices Requiring Baseline Performance

Baseline performance is provided to Network and network edge elements not called out as “Critical Elements” and which do not place identified or particular demands on the network infrastructure. For example, general-purpose workstations and general-purpose network printers with no application profiles or user profiles would place no identified demands on the network.

8.3. Devices Requiring Enhanced or High Performance

The server farm is an aggregation of servers in a single physical location on the campus.

The network infrastructure for the server farm location must support a high volume of network traffic and support traffic bursts without degradation of end-to-end performance. As such, the network infrastructure for the server farm will provide Gigabit connectivity for each of the active server network interfaces in the server farm.

Processor speed and buffer memory of the network infrastructure in this location will be adequate to handle frequent bursts of network traffic and control packet loss. Uplinks from the server farm will be adequate for the volume of traffic and performance levels served by the server farm’s servers.

8.4. Performance Attributes

8.4.1. Transit Delay

Transit delay is often defined as the time and average network packet takes to move across the network infrastructure.
8.4.2. Jitter
Jitter is defined as the variation in delay. Typically, applications that are commonly affected by variable delay are time-sensitive applications such as “live” audio, video, multi-dimensional imagines, or real-time telemetry. The network infrastructure can most notably introduce jitter by excessive buffering. The infrastructure must address controls for jitter to avoid the aforementioned affects on applications. See example in Endnotes.

8.4.3. Packet Loss
Packet loss typically occurs when congestion is present in the network infrastructure. Packet loss can also occur when a network processor element is overwhelmed. Satisfactory processing power in the appropriate places within the infrastructure can avoid packet loss.

While most applications can tolerate nominal packet loss that is extremely infrequent, the network infrastructure must provide for a very nominal packet loss rate by effectively engineering for packet handling that does not increase jitter by excessive buffering.

8.4.4. MTU (Maximum Transmission Unit) Support for New Applications
The network infrastructure needs to be capable of supporting layer 2 transmissions of jumbo Ethernet Frames (i.e. 9000 bytes vs. 1518 payload).

As such, IP MTU Discovery is required by the Layer 3 network infrastructure.

---

1 Unaddressed jitter problems are often manifest as disruptions in on-way or multicast streaming audio, video, broadcast quality video, voice (point to point or multipoint), teleconferencing, video teleconferencing (unicast and multipoint), and telemetry applications, especially for multi-dimensional imaging telemetry.

Application protocols are often built to address some nominal jitter, however, beyond those limits; the effect of excessive jitter in these applications may include audio and video and image clipping, audio cracking and popping, echo, still frames where motion is expected, unintended silence, etc.
8.4.5. **Traffic Profile defines acceptable performance**

Traffic profiles define the Performance Service Level Target that is used. The specifications on jitter, transit delay and packet loss are specified here based on application categories are:

<table>
<thead>
<tr>
<th>Performance Service Level Target</th>
<th>Parameters required by application</th>
<th>Typical application with such requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Baseline Performance</strong></td>
<td>Nominal yet unpredictable loss, i.e., Unpredictable nominal jitter Infrequent high transit delay Packet Loss - TBD Jitter - TBD Transit Delay – TBD</td>
<td>All TCP, packet loss tolerant apps</td>
</tr>
<tr>
<td><strong>Enhanced Performance</strong></td>
<td>Sustained Low packet loss Sustained Low jitter Packet Loss - TBD Jitter - TBD Transit Delay – TBD</td>
<td>Packet loss sensitive apps and VOIP</td>
</tr>
<tr>
<td><strong>High Performance</strong></td>
<td>Sustained Very Low jitter, Sustained Low transit delay, Sustained Low packet loss Packet Loss - TBD Jitter - TBD Transit Delay – TBD</td>
<td>Intolerant packet loss sensitive and delay sensitive including VIDIP</td>
</tr>
</tbody>
</table>

The VIDIP and VOIP NTA development working groups will define specific values, i.e., “jitter not greater than…”

8.5. **Performance Design**

This section discusses the differences in the hardware capabilities to provide the Performance Level Service Targets outlined in 6.1.4 above.
8.5.1. Bandwidth Controls
Bandwidth controls are present in the network infrastructure to effectively manage the use of the network bandwidth. Waste of bandwidth can be curbed by bandwidth controls. In addition, prioritization of critical application traffic flows over others is possible with bandwidth control mechanisms.

8.5.2. Traffic Management/Quality of Service (QoS)
Quality of Service measures are implemented in the network infrastructure using Class of Service, special buffer queuing, and traffic shaping mechanisms.

See Layered QoS Enabling Service for implementation specifics.

8.5.3. Intra-networking
Inter-network performance design is addressed by the layering of performance models onto the network availability models.

8.5.3.1. Core Infrastructure Performance Requirements
The core will be implemented with high performance. Distribution and access layer performance will be determined by application need.

8.5.4. Oversubscription and Blocking
The ratio between the aggregate bandwidth of downstream ports and the aggregate bandwidth of upstream backplane or uplink speeds is typically referred to as Oversubscription or blocking ratio. Performance as measured at an individual end port is dependent upon the oversubscription ratio. This ratio should be engineered to meet the overall performance requirements of the access layer ports.

8.6. Site to Site Networking Performance Levels
In terms of performance and availability levels, the network infrastructure needs to provide for a means to monitor end-to-end flows across the CalREN inter-campus network - this will assist the campuses in measurement and site-to-site troubleshooting. For example, this would provide a means for troubleshooting between the CMS data center and a campus or between a campus and an off-site center.

In order to support the requirements of critical applications such as CMS, performance levels will be mapped to equivalent performance levels on the CalREN inter-campus network.
9. Network Security Architecture

This section presents the network security architecture as supported by the ITRP 2 Technical Architecture Reference Model (TARM). It is anticipated that every campus environment can be mapped to these network security concepts and components.

9.1. Network Security Domain

A security domain is defined as end-to-end security from the end-user platform across the network transport to the server and defense-in-depth requires actions and controls to be placed on all components and their communications. The scope of the ITRP 2 architecture only includes the network transport, per the diagram below.

Note: End user platform and host layer security is out of scope for this document. For more information about best practices for protecting end user platforms and hosts contact your campus Information Security Office (ISO) or local system administrator.
9.2. Design Objectives
The following design objectives are supported:

- Network security and attack mitigation based on policy
- Network security throughout the network infrastructure (not just on specialized security devices)
- Network security management alerts, events and reporting
- Support the ability to authenticate and authorize devices, users, and administrators to critical network resources, by
  - User identity authentication
  - MAC-based endpoint authentication
  - Port-based network access control
- Network intrusion detection and prevention for critical resources and subnets
- Support for emerging networked applications

9.2.1. Defense-in-Depth
From a threat perspective, the campus network is like most networks connected to the Internet. There are internal users who need access out, and external users who need access in. Several common threats can generate the initial compromise that a hacker needs to penetrate the network with secondary exploits.

ITRP 2 architecture implements a layered network security to provide for gradations of protection against risk. The theory is one of defense in depth. Defense in depth is the proposition that multiple layers of security are better than a single protection mechanism. Use of the Baseline and above baseline security levels and zone segmentation provide a defense-in-depth mechanism and strategy for the network.

9.3. Physical Network Security
If an attacker or intruder were to gain physical access to the physical infrastructure supporting the network, security options are limited. Therefore, the physical infrastructure supporting the campus network must provide controls for authorized access, the ability to monitor access to those spaces and protection against unauthorized physical access.

9.3.1. Physical Infrastructure Components
Physical infrastructure components can be, but are not limited to any of the following:

- Service Entrance Room (SER)
ITRP Baseline Network Standard: Architecture

- Equipment Room (ER)
- Telecommunications Room (TR)
- Station Outlet (SO)
- Network Operations Center (NOC)

All these components are typical physical spaces on a campus where your structured cabling infrastructure is terminated and connected to active network equipment. Access to these spaces must be limited to authorized personnel only and the doors must be locked at all times. Controls for monitoring access, such as logging, must be in place.

Network access control and protection is especially important for Station Outlets that provide network services to business units that deal with financial, personal confidential, health, and student data. Therefore, the ability to limit end-users to connect their computer into any active technology outlets or active networking equipment must be in place.

Active network devices must reside in locked enclosures to limit and restrict physical access if they cannot be installed in one of the physical infrastructure components listed above.

For more detailed information on Telecommunications Infrastructure physical requirements and specifications refer to the Telecommunications Infrastructure Planning Standards (TIPS) located at http://www.calstate.edu/cpdc/AE/TIP_Guidelines/TIP-Whole.pdf.

9.4. Logical Network Security

Logical security comprises of the following:

- Network Component Security
- Network Security Perimeters
- Static Security Zones
- Dynamic Security Zones
- Network Security Components

9.5. Network Component Security

The network provides the campus a ‘utility’ service and the various network components must be secured, as follows:

9.5.1. Access Layer

The access layer is where end-users can directly connect to the campus infrastructure to gain access to network services. At this layer network access and control functions must be implemented to allow only authorized users access. Access layer controls include endpoint management such as port-based network access control.

Baseline component security protections include but are not limited to, the following:

- The transport for access to network devices and management must be secured and/or encrypted
- Access to network devices will be limited to the Network Management Layer
- Turn off unneeded services on network devices
- Log at appropriate levels
9.5.2. **Distribution Layer**
This distribution layer is used as an aggregation point for access layer network traffic before the traffic is forwarded on to the core and typically has the ability to perform routing functions.

The routing interfaces at the distribution layer can provide the campus Layer 3 access control capability. Therefore, it is critical for the campus to decide whether their IP address design will become a significant component in providing network security.

Baseline component security protections include but are not limited to, the following:

- The transport for access to network devices and management must be secured and/or encrypted
- Lock down Simple Network Management Protocol (SNMP) access
- Turn off unneeded services
- Log at appropriate levels
- Authentication of routing updates

9.5.3. **Core Layer**
This layer is the center of the campus network; it is the aggregation point for all your network distribution layer network traffic. In some network implementations the access layer and/or server farm module network devices may connect directly to the core layer.

Baseline component security protections include but are not limited to, the following:

- The transport for access to network devices and management must be secured and/or encrypted
- Lock down Simple Network Management Protocol (SNMP) access
- Turn off unneeded services
- Log at appropriate levels
- Authentication of routing updates

9.5.4. **Network Enabling Services**
Core network enabling services such as DNS, DHCP, and Authentication (AAA) can be distributed throughout the network.

Baseline component security protections include but are not limited to, the following:

- Access to network enabling services must be secured and/or encrypted
- Lock down Simple Network Management Protocol (SNMP) access
- Turn off unneeded services
- Log at appropriate levels

9.5.5. **Network Management Services**
Network Management services as well as TFTP configuration and logging servers are placed in the network management zone.

Baseline component security protections include but are not limited to, the following:

- Access to network enabling services must be secured and/or encrypted
- Lock down Simple Network Management Protocol (SNMP) access
9.6. Perimeters
ITRP 2 architecture introduces multiple security perimeters in support of the new layered architecture. A perimeter is defined as the logical separation of security zones by the use of various network security component(s).

The perimeter of each security zone is governed by the campus’ security standards, practices, procedures and guidelines. Perimeter access controls must cover both inbound and outbound connections. Other components may be deployed to detect violations of the perimeter controls which are logged and reported in the management zone.

9.6.1. Boundary Perimeter
This perimeter is the demarcation point between the networks under campus administrative control and networks not under campus administrative control (un-trusted external network). Multiple boundary layers may exist. The boundary needs to be secured with a network security perimeter that includes network device hardening, layer 4-7 traffic filtering, logging, alerting, traffic surveillance and, where appropriate transport encryption.

9.6.2. Static Security Zones
ITRP 2 architecture introduces static security zones. Campus networks are composed of network resources that vary in terms of communications that are allowed with other network resources. Security requirements also vary across systems with regard to availability, confidentiality, and integrity. The differences among resources and the risks associated with them necessitate the separation of systems into different security zones, as follows:

- Baseline
- Above Baseline

A static security zone is defined as an end-to-end aggregation of networked resources with similar requirements for perimeter protection and security. For example, for a Point of Sale (POS) server to be placed in a high security zone all connectivity requirements and traffic flows to/from the POS server need to be appropriately considered.

9.6.3. Management Zone
This security zone is used for the management of the campus network together with all perimeters and zones. It contains the network management servers, TFTP configuration, and logging servers. The zone additionally contains network security tools. As such, this network zone and its components need to be secured at the network perimeter with administrator access controls and auditing.

9.6.4. Dynamic Security Zones
ITRP 2 architecture introduces dynamic security zones. A dynamic security zone is defined as the end-to-end communications path initiated by the client that passes across the secure transport to the server. ITRP 2 provides security services such as transport encryption in order to secure the transport path.
9.7. Network Security Levels
The ITRP architecture introduces security levels, as follows:

9.7.1. Baseline
Baseline is a minimum level of network security and monitoring for all campus network equipment, perimeters, and zones.

9.7.2. Above Baseline
Above baseline includes an increased level of network security and monitoring for access to certain critical or sensitive data and applications based on exceptional confidentiality, integrity, privacy, and/or regulatory requirements.

Design of these levels should be based on CSU and campus security policies.

9.8. Network Security Components
The ITRP architecture introduces a basic set of network security components that are used to implement the defense-in-depth strategy providing access control and security management of campus assets. They are identified, as follows:

- Network Authentication
- Layer 2-4 Traffic Filtering
- Layer 4-7 Inspection and Filtering
- Transport Encryption
- Traffic Surveillance and Mitigation

This list of components will be reviewed annually.
<table>
<thead>
<tr>
<th>Network Security Components</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Authentication</td>
<td>Network Security Functions –</td>
</tr>
<tr>
<td></td>
<td>• Identity</td>
</tr>
<tr>
<td></td>
<td>• Authentication</td>
</tr>
<tr>
<td></td>
<td>• Authorization</td>
</tr>
<tr>
<td></td>
<td>• Audit</td>
</tr>
<tr>
<td></td>
<td>• Accounting</td>
</tr>
<tr>
<td>Layer 2-4 Traffic Filtering</td>
<td>Network Security Functions –</td>
</tr>
<tr>
<td></td>
<td>• Policy Enforcement</td>
</tr>
<tr>
<td></td>
<td>• Controlled Access (Access Control Lists)</td>
</tr>
<tr>
<td></td>
<td>• Layer 2-3 Traffic Filtering</td>
</tr>
<tr>
<td></td>
<td>• Address Translation</td>
</tr>
<tr>
<td></td>
<td>• Encryption</td>
</tr>
<tr>
<td></td>
<td>• Alerts/Events</td>
</tr>
<tr>
<td></td>
<td>• Logging and Statistics</td>
</tr>
<tr>
<td>Layer 4-7 Inspection and Filtering</td>
<td>Network Security Functions –</td>
</tr>
<tr>
<td></td>
<td>• Policy Enforcement</td>
</tr>
<tr>
<td></td>
<td>• Controlled Access</td>
</tr>
<tr>
<td></td>
<td>• Layer 4-7 Traffic Filtering</td>
</tr>
<tr>
<td></td>
<td>• Address Translation</td>
</tr>
<tr>
<td></td>
<td>• Encryption</td>
</tr>
<tr>
<td></td>
<td>• Application Proxies</td>
</tr>
<tr>
<td></td>
<td>• Stateful Inspection</td>
</tr>
<tr>
<td></td>
<td>• Deep Packet Inspection</td>
</tr>
<tr>
<td></td>
<td>• Alerts/Events</td>
</tr>
<tr>
<td></td>
<td>• Logging and Statistics</td>
</tr>
<tr>
<td>Transport Encryption</td>
<td>Network Security Functions –</td>
</tr>
<tr>
<td></td>
<td>• Remote Access</td>
</tr>
<tr>
<td></td>
<td>• Authentication</td>
</tr>
<tr>
<td></td>
<td>• Key Exchange</td>
</tr>
<tr>
<td></td>
<td>• Encrypted Tunnels</td>
</tr>
<tr>
<td></td>
<td>• IP Address Translation</td>
</tr>
<tr>
<td></td>
<td>• Alerts/Events</td>
</tr>
<tr>
<td></td>
<td>• Logging</td>
</tr>
</tbody>
</table>
### ITRP Baseline Network Standard: Architecture

<table>
<thead>
<tr>
<th>Network Security Components</th>
<th>Attributes</th>
</tr>
</thead>
</table>
| Traffic Surveillance and Mitigation | Network Security Functions –  
• Monitor and Analyze Network Activities  
• Pattern Matching Detection  
• Statistical Deviation Detection  
• Analysis of Abnormal Activity Patterns  
• Tracking Policy Violations  
• Alerts/Events |
| Network Management System | Network Security Functions –  
• Central Logging  
• Data Normalization  
• Root Cause Analysis  
• Event Correlation  
• Incident Reporting  
(see NMS section 9.5 Security) |
10. **Network Management Architecture**

Network Management has been an integral part of the CSU’s strategy for its networks since the inception of the ITRP project. The Network Management System (NMS) requirements have mostly been adopted from those outlined in the FCAPS model. They are:

- The Network Management System should not appreciably degrade network performance
- The NMS applications need to integrate with each other
- Training should be provided for the system
- Adequate documentation should be available
- Notifications from the NMS need to be customizable by device and/or event type, by user group, by frequency of notification, and by notification means (email, console, pager, etc)
- A mechanism for out-of-band notification of events should be available (support team is notified of events even though the network is down)
- Communication between the NMS and network devices will not involve clear text
- NMS will allow for partitioning according to security levels (e.g., different SNMP strings for different segments of the network or for different user groups)
- Out-of-band management is a requirement for high-availability areas.

10.1. **Fault**

The system needs to report both pervasive faults with the network and transitive ones. The system needs the capability to collect, analyze and archive large amounts of data from SNMP traps, SNMP polling, and Syslog messages. Notification levels need to be customizable to prioritize faults based on root cause and severity. Alarms for the same event from different applications need to be consolidated into a single notification.

Thresholds for performance-based notifications should be customizable per device and/or device group.

10.2. **Configuration**

The system needs to be capable of managing device configurations and system images (including the update of devices from the NMS either en masse or individually) and the archival of past configurations.

10.2.1. **Configuration Control**

Configuration retrieval should offer customized scheduling and current archived configurations will be up to the minute (automatically update as configurations are changed). Access to archived configurations will be flexible based on user/user group and device/device group. Archived configurations will be searchable by device, type of device, string, IOS version, etc.

10.2.2. **Change Management**

The system will provide a means to schedule changes, such as configuration changes and image upgrades, to single or multiple network devices. The system will log date, time, action and user for all changes applied via the NMS or via command line. System will provide a means for changes to be approved prior to implementation. The system will be capable of notification of changes to devices.
10.3. Accounting 'Capable'
The NMS needs to be capable of accounting for network usage. In the future there may be a need for this capability (for instance, if CENIC starts charging for bandwidth).

10.3.1. Usage by user/department
Ideally, accounting could be done by user or department, perhaps through subnet statistics.

10.4. Performance
The system needs to be able to provide network performance monitoring and alarm generation based on abnormal conditions through intelligent use of baselining and network performance trend reporting.

10.4.1. Performance Monitoring
The system should be capable of polling and event-based data collection that at least addresses availability, response time, accuracy, and utilization. Data aggregation and reduction is important due to the large amounts of data involved. Policy-based network management capability should be available for future QoS deployment.

10.4.2. Alarm Generation
If the performance feature of the NMS catches network-impacting events that the fault system cannot detect, alarms should be generated. Thresholds for alarms should be customizable per device and/or device group.

10.4.3. Performance Reporting
Reporting should at least include network and device health, usage trending, fault identification and notification, and capacity planning.

10.4.4. Bandwidth Shaping
The system will provide for a means to control bandwidth usage by application, user, and network segment. Notifications will be customizable for varying thresholds, etc.

10.4.5. Network Flows
Network flows will be gathered, stored, and analyzed. Flow-based data can be leveraged to improve performance analysis, troubleshooting, security, and accounting.

10.5. Security
From a security perspective, a management network is defined as a segmented security zone used to host network and network security management components and tools. Additionally the management network hosts both configuration and logging data where it is maintained, processed and, stored.

Tools to manage the security components and the overall security of the network will be included, and if possible integrated into, the existing Network Management platform.

The network management zone integrates together four key network security overlays, as follows:

- Protection Framework
- Detection Framework
10.5.1. Protection Framework
The protection framework enables policy-based network security controls, such as network security component access control lists (ACLs), rules and proxies. These control functions are placed at network boundaries between, for example, a campus and external networks or between security zones.

10.5.2. Detection Framework
The detection framework enables policy-based network security monitoring, such as security alarms and events from layer 4-7 analysis components, deep packet inspection, network security component logs and so on. The monitoring components are placed at security zone boundaries, perimeters and near critical components.

10.5.3. Response Framework
The response framework leverages the NMS (enhanced with security) and enables the manual and automated processing of security events and the generation of network security prevention controls, such as blocking and shunning, access control lists and rules, SNMP, and so on.

10.5.4. Management Framework
The management framework enables policy-based management of the network to provide visibility and coordinate the protection, detection and response components.

The NMS, its components and tools, will be secured according to industry best practices – i.e. AAA-compatible, restricted/privileged access, applications utilize users/groups with separate passwords. Both the operating system and applications are patched as soon as security-related patches are released.
10.6. Asset Management

The NMS needs to interface with the Asset Management System (AMS), minimally by exporting a device list. The NMS maintains a current, detailed database of dynamic device information. The AMS is expected to draw data from the databases of the NMS. This is to ensure a single source for any particular data item, a concept which is fundamental to the long-term success of the system as a whole.

The NTA Working Group on Infrastructure Asset Management presented a table of data element requirements to the NTA in June 2005. The following table is an extraction from the June, 2005 report (NIAMS Baseline Data Elements_GP 030205rev.4(a).xls). The NTA asset management working group will determine the final list of elements whose values will be provided by the NMS.

<table>
<thead>
<tr>
<th>Routers</th>
<th>Switches</th>
<th>Blades/Cards for chassis-based systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make</td>
<td>Make</td>
<td>Make</td>
</tr>
<tr>
<td>Model</td>
<td>Model</td>
<td>Model</td>
</tr>
<tr>
<td>Serial number</td>
<td>Serial number</td>
<td>Serial number</td>
</tr>
<tr>
<td>Router ID</td>
<td>Switch ID</td>
<td>Unit ID</td>
</tr>
<tr>
<td>Interfaces used</td>
<td>Ports used</td>
<td>Ports used</td>
</tr>
<tr>
<td>Interfaces available</td>
<td>Ports available</td>
<td>Ports available</td>
</tr>
<tr>
<td>Failure data</td>
<td>Failure data</td>
<td>Failure data</td>
</tr>
<tr>
<td>Software version</td>
<td>Software version</td>
<td>Slot number</td>
</tr>
</tbody>
</table>
11. Network Enabling Services

Network enabling services are services and corresponding protocols required to run a network efficiently. Note: For this section, the term “highly available” means the service is fault-tolerant and can withstand the failure of one full instance of that service. This typically translates to there being two or more systems or appliances physically in separate locations on the campus that can assume the others’ duties should one fail. Methods to accomplish this requirement will be discussed in the subsequent implementation document.

11.1. DNS
Domain Name Services enable the use of canonical names, (rather then IP addresses) in addressing network resources. To provide a highly available network, DNS servers should be placed in an Enabling Services Network Infrastructure Model (see section 13.7.5). DNS services must also be highly available.

11.2. DHCP
Dynamic Host Configuration Protocol is used to manage the allocation of IP addresses. To provide a highly available network, DHCP servers should be placed in an Enabling Services Network Infrastructure Model (see section 13.7.5). DHCP services must also be highly available.

11.3. Authentication
We need to know who is accessing the network devices. The design must adhere to the CSU system-wide authentication standards when they become available. Until the CSU standards are available, we will need to integrate with standard authentication services in particular those implemented by the campuses. (i.e. LDAP)

11.4. NMS Servers
Network Management Services support fault, configuration and performance management. The three create a suite of applications that enable robust management of the network. They assist with performance analysis, troubleshooting and preventative maintenance.

11.5. Syslog
Syslog is essential to capturing system messages generated from network devices. Devices provide a wide range of messages, including changes to device configurations, device errors, and hardware component failures.

11.6. NTP
Although it might not appear to be intrinsic to network functionality, this service is critical for consistent time stamps across the network. Time stamp accuracy and standardization facilitates troubleshooting and post-intrusion forensics.
11.7. **Other Enabling Services**

These are Out of Scope (OOS) for the Dev-1 group as these are considered meta-services according to the matrix defined at
http://itrp.calstate.edu/csutrack/soe20/CSU%20ITRP%20SOE%202.0%20Architecture.htm. Other groups will define these as part of their scope.

11.7.1. **POE**

Power over Ethernet is considered out of scope but needs to be taken into account as optional for the campuses deploying network devices that need it.
12. Profiling Campus Network Traffic

The ITRP 2 architecture is designed to provide support for the wide range of users and applications that make up a CSU campus. In particular, the availability, performance, and security requirements of particular users and applications will typically vary. It is not financially viable, nor is it technically required, to provide the highest required levels of availability, performance, and security across the whole infrastructure, but it is important that the specific needs of users and the applications they access are met. ITRP 2 addresses these conflicting needs by providing design templates or modules that meet specific availability, performance, and security needs.

Campuses should use the profiling and modeling approach detailed in this document to determine the needs of their specific campus. Campuses should determine what constitutes criticality, high availability, performance, and security within their own environment. There will be additional implementation constraints, including financial, that may modify the design, but these are outside the scope of this architectural document. Please see the implementation documentation for details.

The design for a specific campus will consist of a collection of these modules, each chosen to meet the needs of the local users and applications it serves. In order that the appropriate module is chosen for each part of the network, it is important to understand the need of the traffic that flows within that part of the network. The campus may have to add user and application types unique to the campus. Traffic profiles represent a collection of traffic flows that are present on the campus network, and that require similar levels of availability, performance, and security. Designing the network is then equivalent to the task of selecting appropriate modules for each part of the network, based on the traffic profiles present in that part of the network.

This section provides guidelines on how to determine the specific traffic profiles that are present on a specific campus.

12.1. Profiles

12.1.1. User Types

A user type represents a collection of users that are present on the campus network, and that require similar levels of availability, performance, and security. There are typically several different types of user on a campus network. This table lists several common user types:

<table>
<thead>
<tr>
<th>User Type</th>
<th>Role</th>
<th>Sub-Role</th>
<th>Description/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1</td>
<td>Faculty</td>
<td>Part-Time</td>
<td>Faculty members whose contract is renewed on a semester-by-semester basis. No assumption that they will be affiliated with the University after the end of the semester/academic year.</td>
</tr>
<tr>
<td>F2</td>
<td>Full-Time</td>
<td></td>
<td>Faculty members who have a long term relationship with the University. May have research needs which define the access needed or desired. May serve on committees which make them cross organizational boundaries. May be</td>
</tr>
<tr>
<td>User Type</td>
<td>Role</td>
<td>Sub-Role</td>
<td>Description/Comments</td>
</tr>
<tr>
<td>-----------</td>
<td>------</td>
<td>----------</td>
<td>----------------------</td>
</tr>
<tr>
<td>G1</td>
<td>Guest</td>
<td>Contractors</td>
<td>Short term users who need access to all types of resources acting more like a staff member in their present capacity.</td>
</tr>
<tr>
<td>G2</td>
<td>Vendors</td>
<td></td>
<td>Examples are vendors who need access to campus resources to fulfill their contracted support responsibilities.</td>
</tr>
<tr>
<td>G3</td>
<td>Visitors</td>
<td></td>
<td>Persons not normally associated with the university. Examples are a visiting professor or conference group meeting on campus for a week or two.</td>
</tr>
<tr>
<td>SA1</td>
<td>Staff</td>
<td>IT</td>
<td>Information Technology support staff that may need specialized access to core IT systems in order to fulfill their support functions.</td>
</tr>
<tr>
<td>SA2</td>
<td>All others</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA3</td>
<td>Security</td>
<td></td>
<td>Information Security staff that may need specialized access to core IT systems in order to fulfill their support functions.</td>
</tr>
<tr>
<td>SU1</td>
<td>Students</td>
<td>Off-Site</td>
<td>Students associated with the University that need access to campus systems that support their learning and administrative needs.</td>
</tr>
<tr>
<td>SU2</td>
<td>Labs</td>
<td></td>
<td>Smart classrooms, computer labs, etc.</td>
</tr>
<tr>
<td>SU3</td>
<td>Open Jacks</td>
<td></td>
<td>Network access in open areas not associated with a particular user base.</td>
</tr>
<tr>
<td>A1</td>
<td>Admin</td>
<td>Facilities</td>
<td></td>
</tr>
<tr>
<td>A2</td>
<td>Alarms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A3</td>
<td>Security</td>
<td>web-cams</td>
<td></td>
</tr>
</tbody>
</table>
### 12.1.2. Application Types

An application type represents a collection of applications that are present on the campus network and that require similar levels of availability, performance, and security. There are typically several different types of application on a campus network. This table lists several common application types:

<table>
<thead>
<tr>
<th>Application Type</th>
<th>Scope</th>
<th>Name</th>
<th>Description/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>AG1</td>
<td>CSU Wide</td>
<td>CMS</td>
<td>Could include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(a) Direct sql queries – developers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(b) Two tier</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(c) Three tier</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(d) Campus portal</td>
</tr>
<tr>
<td>AG2</td>
<td>CVS (CalVIP)</td>
<td></td>
<td>Need to consider bandwidth and security needs</td>
</tr>
<tr>
<td>AG3</td>
<td>HTTP</td>
<td></td>
<td>Need to have a good experience but kind of self-correcting. Should not drive performance/security requirements as opposed to https</td>
</tr>
<tr>
<td>AG4</td>
<td>LMS (Blackboard/ WebCT)</td>
<td>Various uses – security probably a bigger issue than bandwidth unless video involved – see CVS.</td>
<td></td>
</tr>
<tr>
<td>AG5</td>
<td>Student card ID</td>
<td></td>
<td>Confidentiality is key. All traffic of this kind should be encrypted by application not network.</td>
</tr>
<tr>
<td>AG6</td>
<td>Building management systems</td>
<td>(a) Real-time response times.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(b) Criticality of information</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(c) Security</td>
</tr>
<tr>
<td>AG7</td>
<td>IP surveillance</td>
<td></td>
<td>Absent legal issues – needs to be secure and may have bandwidth issues.</td>
</tr>
<tr>
<td>AG8</td>
<td>Ghosting</td>
<td></td>
<td>Multicast needs to be considered. Need to consider multicasting across core of network.</td>
</tr>
<tr>
<td>AG9</td>
<td>data warehouse</td>
<td></td>
<td>Bandwidth.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security/access</td>
</tr>
<tr>
<td>AG10</td>
<td>Library services</td>
<td></td>
<td>Licensing – who is allowed to use resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Bandwidth – see CVS</td>
</tr>
<tr>
<td>AG11</td>
<td>Portal</td>
<td></td>
<td>Portal to system with functionality such as: access to grades, financial systems, class information – need to consider:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(a) Reliability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(b) Bandwidth</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(c) Security</td>
</tr>
<tr>
<td>AG12</td>
<td>POS</td>
<td></td>
<td>Credit cards require security to ensure confidentiality and integrity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reliability of the network for appropriate response times</td>
</tr>
<tr>
<td>AG13</td>
<td>CashNet (A/C receivable)</td>
<td>Credit cards require security to ensure confidentiality and integrity</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reliability of the network for appropriate response times</td>
</tr>
</tbody>
</table>
### ITRP Baseline Network Standard: Architecture

<table>
<thead>
<tr>
<th>Application Type</th>
<th>Scope</th>
<th>Name</th>
<th>Description/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>AG14</td>
<td>Virus/Desktop mgmt. services and clients</td>
<td>Access across various parts of the network Security issues Is ghosting related to this.</td>
<td></td>
</tr>
<tr>
<td>AL15</td>
<td>Campus Specific</td>
<td>VidIP</td>
<td>QOS – more important here than in VOIP portion. Different from CALVIP. Streaming webcast Desktop ad-hoc Could have substantial bandwidth and QoS requirements</td>
</tr>
<tr>
<td>AL16</td>
<td></td>
<td>VoIP</td>
<td>Reliability to meet voice availability requirements. Bandwidth – probably not an issue within a campus QoS</td>
</tr>
</tbody>
</table>

#### 12.1.3. Traffic Types

The combination of an application and the user types that access it form a traffic type.

![User Type + Application Type = Traffic Type](image)

A traffic profile represents a collection of traffic types that are present on the campus network and that require similar levels of availability, performance, and security.
ITRP Baseline Network Standard: Architecture

Each traffic profile can then be mapped to the areas of the network that need to support it. In this way, the availability, performance, and security requirements of each area of the network can be determined.

<table>
<thead>
<tr>
<th>Traffic Profiles</th>
<th>Traffic Type</th>
<th>Availability</th>
<th>Performance</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>TP 1</td>
<td>TT 1</td>
<td>H</td>
<td>H</td>
<td>Components as required</td>
</tr>
<tr>
<td></td>
<td>TT 2</td>
<td>H</td>
<td>H</td>
<td>Components as required</td>
</tr>
<tr>
<td>TP 2</td>
<td>TT 3</td>
<td>H</td>
<td>H</td>
<td>Components as required</td>
</tr>
</tbody>
</table>
13. Modeling Steps

The following steps summarize the process of modeling a campus. Note that the resulting model may have several options which are not fully defined by this process. Additional criteria (e.g. least cost design) may apply to resolve any design options. These criteria form part of the process to determine a specific implementation of the architecture described in this document. As such, they are out of the scope this document. See the ITRP 2 Implementation Guide for more details.

13.1. Determine Network Infrastructure Roles
Divide the campus network into non-overlapping areas which can be categorized as providing one of the following network infrastructure roles:

13.1.1. End-User Network Infrastructure
This includes all network devices and links that support the end-user directly, or transport end-user data up to the core of the campus network.

13.1.2. Server Farm Network Infrastructure
This includes all network devices and links that support servers co-located in one physical facility, typically known as a server farm, or transport data to and from those servers up to the core of the campus network. The server farm is typically located in a data center, which provides specialized support for critical servers, included redundant power feeds, environmental control, etc.

13.1.3. Gateway Services Network Infrastructure
This includes all network devices and links that support access to and from networks external to the campus infrastructure itself, or transport data to and from these networks up to the core of the campus network. Examples would include the infrastructure supporting CALREN connectivity, and that supporting remote access.

13.1.4. Enabling Services Network Infrastructure
This includes all network devices and system platforms that support enabling services. This includes but is not necessarily limited to: DHCP server(s), DNS server(s), Network Management System.

13.2. Determine Traffic Profiles
For each identified area, determine the user and application types that use it. Distinct user types and applications should be developed where the availability, performance, or security requirements of the user or application differ. This analysis should be as comprehensive as possible. There may be many user and application types defined in this section. Examples of typical user and application types are given in section 12.

13.3. Determine Area-Specific Availability, Security, and Performance
The application and user types identified in the previous step should now be aggregated together, based upon their common availability, performance, and security requirements. Upon completion of this stage, it should be possible to determine by area the specific availability, security, and performance needs. Each area can then be architected and designed to meet the needs of its specific users and applications.
13.3.1. **Determine Area-Specific Availability Requirements**

Based on the criticality of the users and applications, assign a level of required availability to each area. The models distinguish between three categories of availability: baseline, enhanced, and high. These are described in more detail below. Note that the mechanisms used to provide specific levels of availability are implementation specific, but will typically include the use of dual-power supplies and feeds, redundant components in modular devices and redundant links.

**13.3.1.1. Baseline Availability**

Baseline availability relies on redundant components within the core, the inherent stability of the network devices and the links between them. No redundancy is built into the areas below the core of the network (with the exception of the Server Farm Distribution). This should translate into a service level meeting the baseline service level targets, but one that might infrequently experience intermittent outages if individual devices or links fail. Restoration of service will depend upon physical replacement of the defective devices, physical re-routing of failed links and campus operational practices.

**13.3.1.2. Enhanced Availability**

Enhanced availability expands redundancy to include the connections between the core and distribution layers. This provides a higher-level of availability, as a single core card or a single link failure no longer affects end-users. This also provides greater localization of network outages, as only distribution layer device failures are unprotected.

**13.3.1.3. High Availability**

High Availability expands redundancy to include the connections between the distribution and access layers and redundancy of the distribution layer. This provides a higher-level of availability, as single-points of failure in the distribution and core are eliminated. This also provides greater localization of network outages, as only access layer device failures are unprotected.

Where multiple availability requirements exist in the same area, try to sub-divide the area until only one level of required availability is reached.

**13.3.2. Determine Area-Specific Security Requirements**

For each identified area, determine the security components required for each of the traffic flows that are present based upon criticality, risk and, vulnerabilities. Section 9 provides details of the security components that may be required. Where different traffic flows require different components of security the aggregate should be implemented. Note the mechanisms used to provide specific levels of security are implementation specific, but will typically include the use of traffic filtering, traffic surveillance, and transport encryption devices.

**13.3.3. Determine Area-Specific Performance Requirements**

For each identified area, assign a level of performance to each of the traffic flows that are present. Section 8 provides details of the three performance levels – Baseline, enhanced, and high. Where different traffic flows require different levels of performance the highest required level should be implemented. Note the mechanisms used to provide specific levels of performance are implementation specific, but will typically include the use of specific ratios of user ports to devices, and the software configuration of quality of service and other traffic management features.
13.4. Select and combine each appropriate area model
For each identified area, the appropriate model can be selected, based on the role of the area and the level of availability required. Recombining the network models that apply to each area then forms the proposed campus network architecture. The recombination of area models may reduce the overall switch count. For example, a distribution layer switch in two separate area diagrams may physically be the same switch, if the ratio of downstream ports is acceptable from a performance and availability perspective.

13.5. Determine Network Management Requirements
Reviewing the network model as a whole, determine on an area-by-area basis where network management functionality is required. Using appropriate icons designate the location of each required network management function.

13.6. Determine Routing Architecture
Reviewing the network model as a whole, including the location of security and network management functionality, determine on an area-by-area basis, where the network layer boundary should exist. Layer 3 functionality may extend into the distribution layer, particularly when security requires it.

13.7. Availability Model Selection
The following sections outline the possible network models that can be selected for each distinct area of the network, based on the role and availability needs of that area. The key to this section is the following assumption: Each campus will have different availability requirements (baseline, enhanced, high). The different availability requirements lead to an environment with primary (PCS) and secondary (SCS) switching cores. All distribution layers will be connected to the PCS engine, while the distribution layer that requires enhanced or high availability will also be connected to the SCS engine.
13.7.1. End-User N/I: Baseline Availability
The baseline availability end-user model consists of an end-user platform supported by PCS, a single distribution engine, and a single access engine.

13.7.1.1. Connectivity
The baseline availability end-user model provides a single link between the PCS and the distribution layers, and a single link between the distribution and access layers. End-user devices are singly attached to the access layer. Note that where only a few end-user devices need support, for example a kiosk, additional access layer switches may be serially attached to the access switch connected to the distribution layer when there is insufficient cabling infrastructure to support a direct connection to the distribution layer. All downstream access switches should be directly connected to the access switch connected to the distribution layer.

13.7.1.2. Target Service Level

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Baseline</td>
</tr>
<tr>
<td>Performance</td>
<td>B, E, or H</td>
</tr>
<tr>
<td>Security</td>
<td>Components as required</td>
</tr>
</tbody>
</table>
13.7.2. End-User N/I: Enhanced Availability
The enhanced availability end-user model consists of an end-user platform supported by a PCS and an SCS, a single distribution engine, and a single access engine.

13.7.2.1. Connectivity
The enhanced availability end-user model provides two distinct links from the distribution layer engine to the PCS and the SCS, and a single link between the distribution and access layers. End-user devices are singly attached to the access layer engine.

13.7.2.2. Target Service Level

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Enhanced</td>
</tr>
<tr>
<td>Performance</td>
<td>B, E, or H</td>
</tr>
<tr>
<td>Security</td>
<td>Components as required</td>
</tr>
</tbody>
</table>
13.7.3. **End-User N/I: High Availability**
The high availability end-user model consists of an end-user platform supported by a PCS and a SCS, two distribution engines, and a single access engine.

13.7.3.1. **Connectivity**
The high availability end-user model provides two distinct links from the access layer component to the distribution layer, and single link between each distribution layer engine and the PCS. End-user devices are singly attached to the access layer engine.

13.7.3.2. **Target Service Level**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>High</td>
</tr>
<tr>
<td>Performance</td>
<td>B, E, or H</td>
</tr>
<tr>
<td>Security</td>
<td>Components as required</td>
</tr>
</tbody>
</table>
13.7.4. Server Farm N/I
The server farm model consists of a server component supported by a PCS, an SCS, and Server farm distribution switching (SFDS).

13.7.4.1. Connectivity
The server farm model provides two distinct links from the distribution layer engine to the PCS and the SCS. Servers can be directly attached to a single distribution layer engine, or diversely attached to two distribution layer engines. Where servers are attached to two SFDS engines, the second engine is non-redundant.

13.7.4.2. Target Service Level
The server farm has the following availability, security, and performance requirements:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>High</td>
</tr>
<tr>
<td>Performance</td>
<td>High</td>
</tr>
<tr>
<td>Security</td>
<td>Components as required</td>
</tr>
</tbody>
</table>
13.7.5. Enabling Services N/I

The enabling services model houses the platforms that provide the Network Enabling Services detailed in section 11. These are essentially server components, serving network related data (such as DHCP assignments, DNS names, etc). The enabling services model consists of these server components supported by a redundant core with redundant components, and one or two distribution components.

13.7.5.1. Connectivity

The enabling services model provides two distinct links from the distribution layer engine to the PCS and the SCS. Servers supporting the network enabling services can be directly attached to a single distribution layer engine, or diversely attached to two distribution layer engines. Where these servers are attached to two SFDS engines, the second engine is non-redundant.

13.7.5.2. Target Service Level

The enabling services have the following availability, security, and performance requirements:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>High</td>
</tr>
<tr>
<td>Performance</td>
<td>High</td>
</tr>
<tr>
<td>Security</td>
<td>Components as required</td>
</tr>
</tbody>
</table>
13.7.6. **Gateway Services N/I**
The gateway services model provides an external interface supported by network security components, gateway components, and a redundant core with redundant components. Depending on the level of criticality of the services that the gateway supports, these components may be duplicated to provide enhanced availability, as shown in the shaded region in the diagram. For example, CalREN access would typically be high availability, whereas remote dial-up access may not. Flow management devices may also be present in the gateway services model, in order to meet the performance criteria of applications that interact with systems not resident on the campus (for example CMS).

13.7.6.1. **Connectivity**
The gateway services model provides one or two (depending on criticality) distinct physical links from the access layer component to the distribution layer, and single logical links between each distribution layer component and distinct core layer components.

13.7.6.2. **Target Service Level**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>High</td>
</tr>
<tr>
<td>Performance</td>
<td>High</td>
</tr>
<tr>
<td>Security</td>
<td>Components as required</td>
</tr>
</tbody>
</table>
14. An Example of Modeling a Campus Network

NOTE: This section is for illustrative purposes only. It is intended to show how the architectural models described in this document might map to a specific network implementation at a campus. It does not form part of the modeling standards described above, and should not be taken to define any requirements on the use of the models in this document. If there are inconsistencies between statements in this section and other sections of the document, the other sections take precedence.

14.1. Napa State University (NSU) Campus Network

The diagram below represents a fictional campus, Napa State University, which is intended to include many of the characteristics of a CSU campus. The diagram below represents part of the current layout of NSU which will illustrate an application of the models described above. This is the starting point for the modeling analysis.
The sections below are taken from section 13 in this document.

14.1.1. **Determine Network Infrastructure Roles**

The first step is divide the existing campus network into non-overlapping areas that can be categorized as providing one of the following network infrastructure roles: end-user network infrastructure, server farm network infrastructure, or gateway services network infrastructure. The definition of each of these roles can be found in section 13.7. In this example, the Network Enabling Services have not been analyzed. The diagram below shows these roles for NSU.
14.1.2. Determine Traffic Profiles

Next, application and user types present on the network need to be determined. The following table provides a sample of the distinct locations on NSU and assigns 3-letter acronyms for them.

<table>
<thead>
<tr>
<th>Code</th>
<th>Location</th>
<th>Primary Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mal</td>
<td>Malbec</td>
<td>Residence Hall Network</td>
</tr>
<tr>
<td>Rie</td>
<td>Riesling</td>
<td>Academic and Administrative Offices</td>
</tr>
<tr>
<td>Zin</td>
<td>Zinfandel</td>
<td>Administrative Offices</td>
</tr>
<tr>
<td>Pal</td>
<td>Palomino</td>
<td>Teaching Block</td>
</tr>
<tr>
<td>Mus</td>
<td>Muscat</td>
<td>Teaching Block</td>
</tr>
<tr>
<td>Cab</td>
<td>Cabernet</td>
<td>Administrative Offices</td>
</tr>
<tr>
<td>Pin</td>
<td>Pinot</td>
<td>Teaching Block</td>
</tr>
<tr>
<td>Lib</td>
<td>Library</td>
<td>Library Facilities</td>
</tr>
<tr>
<td>Mer</td>
<td>Merlot</td>
<td>Laboratory Facilities</td>
</tr>
<tr>
<td>Siz</td>
<td>Shiraz</td>
<td>Teaching Block</td>
</tr>
<tr>
<td>DC</td>
<td>Data Center</td>
<td>IT Facilities</td>
</tr>
<tr>
<td>MDF</td>
<td>Main Distribution Frame</td>
<td>IT Facilities</td>
</tr>
</tbody>
</table>

The following table provides a sample of the distinct user types present on the network, and the locations that they exist. The user type classifications are based on those given in section 12.1.1. Note that a specific campus may identify additional user types that are not listed in this document. In this example, user type SU4 was identified by NSU.

<table>
<thead>
<tr>
<th>User Type</th>
<th>Role</th>
<th>Sub-Role</th>
<th>Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1</td>
<td>Faculty</td>
<td>Part-Time</td>
<td>Pal, Mus, Pin, Lib, Mer, Siz, DC</td>
</tr>
<tr>
<td>F2</td>
<td>Full-Time</td>
<td></td>
<td>Rie, Pal, Mus, Pin, Lib, Mer, Siz, DC</td>
</tr>
<tr>
<td>G2</td>
<td>Vendors</td>
<td></td>
<td>Lib</td>
</tr>
<tr>
<td>G3</td>
<td>Visitors</td>
<td></td>
<td>Lib</td>
</tr>
</tbody>
</table>
Based on this analysis, the end-user areas identified earlier need to be sub-divided to represent the distinct areas identified above. The diagram below illustrates these separate areas:
The following table provides a sample of the distinct applications present on the network, and the user types that access them. The application types are based on those given in section 12.1.2. Note that a specific campus may identify additional application types that are not listed in this document. In this example, application types IN1, and N1 were identified by NSU.

<table>
<thead>
<tr>
<th>Traffic Types</th>
<th>Name of Application</th>
<th>App Type</th>
<th>Users by User Types</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CMS 7.x (GUI, SQL, remote printing) HR and Finance</td>
<td>AG1</td>
<td>A1, A2, A3</td>
</tr>
<tr>
<td></td>
<td>CMS 7.x (GUI, SQL, remote printing) Student System</td>
<td>AG1</td>
<td>F1, F2, SA1, SA2</td>
</tr>
<tr>
<td></td>
<td>HTTP Internet Browsing</td>
<td>IN1</td>
<td>SU1, SU2, SU3, SU4</td>
</tr>
<tr>
<td></td>
<td>H.323 Instructional and Administrative Video Teleconferencing</td>
<td>AL16</td>
<td>F1, F2, SA1, SA2</td>
</tr>
<tr>
<td></td>
<td>On-Campus Financial System</td>
<td>N1</td>
<td>A1, A2</td>
</tr>
<tr>
<td></td>
<td>Building Management Systems</td>
<td>AG6</td>
<td>A1, A2</td>
</tr>
</tbody>
</table>

14.1.3. Determine Area-Specific Availability, Performance, and Security
For each identified traffic type, determine the availability, security, and performance requirements. The table below shows this analysis for the sample traffic types identified above.

<table>
<thead>
<tr>
<th>Requirements by Traffic Type</th>
<th>Traffic Type</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>App Type</td>
<td>User Type</td>
</tr>
<tr>
<td></td>
<td>AG1</td>
<td>A1, A2, A3</td>
</tr>
<tr>
<td></td>
<td>AG1</td>
<td>F1, F2, SA1, SA2</td>
</tr>
<tr>
<td></td>
<td>N1</td>
<td>A1, A2</td>
</tr>
<tr>
<td></td>
<td>AG6</td>
<td>A1, A2</td>
</tr>
<tr>
<td></td>
<td>IN1</td>
<td>SU4</td>
</tr>
<tr>
<td></td>
<td>AL16</td>
<td>F1, F2</td>
</tr>
</tbody>
</table>
For each identified area, the appropriate model can be selected, based on the role of the area and the level of availability required. Recombining the network models that apply to each area then forms the proposed campus network architecture.

Using the sample table above, the requirements for each location can be determined. For an actual campus, there may be many more traffic types identified. For the purposes of this example, only a small sample of the total number of distinct traffic types is dealt with. The first step is to restructure the traffic type table by location, as shown below:

<table>
<thead>
<tr>
<th>Location</th>
<th>Traffic Type</th>
<th>User Type</th>
<th>Availability</th>
<th>Performance</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Riesling</td>
<td>AG1</td>
<td>A1, A2, A3</td>
<td>H</td>
<td>B</td>
<td>As required.</td>
</tr>
<tr>
<td>Zinfandel</td>
<td>AG1</td>
<td>A1, A2, A3</td>
<td>H</td>
<td>B</td>
<td>As required.</td>
</tr>
<tr>
<td>Library</td>
<td>AG1</td>
<td>F1, F2, SA1, SA2</td>
<td>H</td>
<td>B</td>
<td>As required.</td>
</tr>
<tr>
<td>Library</td>
<td>IN1</td>
<td>SU4</td>
<td>B</td>
<td>B</td>
<td>As required.</td>
</tr>
<tr>
<td>Cabernet</td>
<td>N1</td>
<td>A1, A2</td>
<td>B</td>
<td>B</td>
<td>As required.</td>
</tr>
<tr>
<td>Cabernet</td>
<td>AG6</td>
<td>A1, A2</td>
<td>B</td>
<td>B</td>
<td>As required.</td>
</tr>
<tr>
<td>Malbec</td>
<td>IN1</td>
<td>SU4</td>
<td>B</td>
<td>H</td>
<td>As required.</td>
</tr>
<tr>
<td>Palomino</td>
<td>AL16</td>
<td>F1, F2</td>
<td>B</td>
<td>H</td>
<td>As required.</td>
</tr>
<tr>
<td>Muscat</td>
<td>AL16</td>
<td>F1, F2</td>
<td>B</td>
<td>H</td>
<td>As required.</td>
</tr>
<tr>
<td>Pinot</td>
<td>AL16</td>
<td>F1, F2</td>
<td>B</td>
<td>H</td>
<td>As required.</td>
</tr>
<tr>
<td>Shiraz</td>
<td>AL16</td>
<td>F1, F2</td>
<td>B</td>
<td>H</td>
<td>As required.</td>
</tr>
</tbody>
</table>

From this table, the requirements by location can be determined. Notice that in the example given, the library and Cabernet have conflicting requirements, based on the different traffic flows that relate to them. These conflicts arise from availability and security requirements respectively. In these cases, two options exist. If within the affected area distinct workstations can be allocated for the different traffic flows, then the areas can sub-divided into separate areas to reflect these distinct workstation groups, and the area modeled independently. This approach has been taken for Cabernet. If the same workstations are used to access both traffic types, then the higher requirements must be used, to ensure that all traffic flows are adequately supported. For Library, the latter case applies, so the library entries are combined into one entry, with the higher requirements.
The modified table is shown below:

<table>
<thead>
<tr>
<th>Location</th>
<th>App Type</th>
<th>User Type</th>
<th>Availability</th>
<th>Performance</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Riesling</td>
<td>AG1</td>
<td>A1,A2,A3</td>
<td>H</td>
<td>B</td>
<td>As required.</td>
</tr>
<tr>
<td>Zinfandel</td>
<td>AG1</td>
<td>A1, A2, A3</td>
<td>H</td>
<td>B</td>
<td>As required.</td>
</tr>
<tr>
<td>Library</td>
<td>AG1, IN1</td>
<td>F1, F2, SA1, SA2, SU4</td>
<td>H</td>
<td>B</td>
<td>As required.</td>
</tr>
<tr>
<td>Cabernet</td>
<td>N1</td>
<td>A1, A2</td>
<td>B</td>
<td>B</td>
<td>As required.</td>
</tr>
<tr>
<td>Cabernet</td>
<td>AG6</td>
<td>A1, A2</td>
<td>B</td>
<td>B</td>
<td>As required.</td>
</tr>
<tr>
<td>Malbec</td>
<td>IN1</td>
<td>SU4</td>
<td>B</td>
<td>H</td>
<td>As required.</td>
</tr>
<tr>
<td>Palomino</td>
<td>AL16</td>
<td>F1,F2</td>
<td>B</td>
<td>H</td>
<td>As required.</td>
</tr>
<tr>
<td>Muscat</td>
<td>AL16</td>
<td>F1,F2</td>
<td>B</td>
<td>H</td>
<td>As required.</td>
</tr>
<tr>
<td>Pinot</td>
<td>AL16</td>
<td>F1,F2</td>
<td>B</td>
<td>H</td>
<td>As required.</td>
</tr>
<tr>
<td>Shiraz</td>
<td>AL16</td>
<td>F1,F2</td>
<td>B</td>
<td>H</td>
<td>As required.</td>
</tr>
</tbody>
</table>

The appropriate availability models can now be chosen for each of the locations. Examples below show the selection for the Library and the Shiraz locations:
Shiraz Availability Model

Note that the Shiraz model includes two distribution layer switches. The number of access ports to distribution layer ports determines the number of distribution layer switches supported in the model.
Cabernet Security Model

14.1.4. **Determine Network Management Requirements**
Reviewing the network model as a whole, determine on an area-by-area basis, where network management functionality is required. Using appropriate icons, designate the location of each required network management function.

14.1.5. **Determine Routing Architecture**
As with all campuses, the core layer of the network will be routed. OSPF will be used at the dynamic routing protocol. In addition, because of the enhanced security and high traffic volumes associated with the server farm location, routing will also be implemented in the distribution layer that feeds the server farm. For similar reasons, routing will be implemented in the distribution layer that feeds the network enabling services infrastructure (although this is not shown on the final NSU diagram).

14.2. **NSU ITRP 2 Network**
The diagram below shows a part of the NSU core campus network as it will look after the ITRP 2 refresh.
15. **Document Control**

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/16/05</td>
<td>Dev 1</td>
<td>Team</td>
<td>Initial Combined Draft</td>
</tr>
<tr>
<td>7/19/05</td>
<td>Dev 1</td>
<td>Team</td>
<td>Final Draft</td>
</tr>
<tr>
<td>8/10/05</td>
<td>Dev 1</td>
<td>Team</td>
<td>Version submitted to ITAC for review at 8/18/05 meeting</td>
</tr>
</tbody>
</table>

**CONTACTS**

<table>
<thead>
<tr>
<th>Original Author</th>
<th>Johanna Madjedi (805) 756-7691</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revisions</td>
<td></td>
</tr>
</tbody>
</table>

**DISTRIBUTION**

<table>
<thead>
<tr>
<th>Name/Distribution list</th>
<th>Email address/Maintainer</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CONFIDENTIALITY**