Chapter 3: Network and Middleware

The campus’s ITS unit provides the campus with much of its underlying IT resources, including the network, and telephony services. With advances in the area of middleware, the common software layer between the network and applications, the campus needs to expand its central provision of IT resources to include Enterprise Directory Services and an “IT services provisioning infrastructure” (which in turn provides the framework to allow standardized and reliable account, access, authentication and authorization, and identity management). These services provide the infrastructure necessary, for example, for a single sign-on from anywhere to specific campus applications and resources.

All network and middleware services must be designed and delivered to ensure reliability, stability, and scalability. Furthermore, in the case of middleware services, they must integrate with UMS and campus applications and data seamlessly. In the implementation and expansion of network and middleware services, the campus must strike a delicate balance between:

- Central authority, coordination, policy, and guidelines;
- Cross-campus collaboration;
- Flexibility to meet needs of campus units and users; and
- Anticipating changes in technology.

Specific recommendations in this chapter include:

- Continue the development of the Enterprise Directory and establish it as the authoritative source for information about faculty, staff, and student identity and roles;
- Develop the infrastructure necessary for central coordination of identity management, authentication and authorization, and single sign-on;
- Expand network bandwidth;
- Expand wireless access to meet demands for mobile access to campus and Internet resources; and
- Prepare for the next generation telephony solution, Voice over IP (voice services over the data network).
3.1 Networking – General (Section I of II)

Recommendation: 1) Increase the bandwidth available to the campus; 2) strengthen the availability and reliability of the network; 3) expand remote access to campus, networked resources.

Discussion of the Recommendation

Current Situation
The previous IT Strategic Plan and the Network Task Force called for a major upgrade to the campus network. Within the last two years, and with substantial one time Total Learning Environment funding from the Chancellor, the campus network was upgraded from an aging and completely shared 10 Mbps Ethernet to a modern, supportable, switched 10 Mbps and 100 Mbps network. The campus core network currently supports 1 Gbps links throughout the backbone connections, all the way out to the switches that connect customer systems. These switches support 10 Mbps and 100 Mbps switched Ethernet connections to customer systems, but fewer than 10% of the connections on campus can run faster than 10 Mbps because existing, old wiring in building structures prevents higher speeds. In approximately half of the buildings on campus, new wiring can be installed on a case-by-case basis to allow individual connections to run at 100 Mbps. In some situations, and certainly within the timeframe of this plan, fiber connections could be made to support 1 Gbps to specific customer systems, but the implications of such increased load for the core network must be carefully considered.

Bandwidth to Internet2 is currently 155 Mbps via a 155 Mbps link that is also shared with the four-campus video network along with access to the global Internet. Near term plans call for upgrading the shared line to 622 Mbps, but there is already pressure from the NSF to provide 1 Gbps access to Internet2 by the year 2004.

The Boulder campus currently subscribes to 60 Mbps of commodity Internet access via the Front Range GigaPOP (FRGP), though a more realistic number would probably be 70 Mbps. A large part of the growing use of the Internet is related to file sharing of music and other entertainment applications. Currently, ITS limits much of the entertainment uses of the Internet so that academic uses are not overwhelmed.

The campus network core currently has sufficient redundancy to be able to function in the event of many single point failures in the core campus backbone. However, the campus is entirely dependent upon the FRGP for its access to Internet2 and the global, commodity Internet.

Using student technology fee funds, ITS currently supports dial-in modem service on 869 v.92 modems. Although we have seen as many as 844 simultaneous modem users, the users of those modems do not get busy signals, even in peak usage times. Also, ITS supports nearly 900 students, faculty, and staff who connect from their homes using Qwest's Digital Subscriber Line (DSL) service.

Rationale
Popular discussion suggests that the demand for global Internet access doubles every 18 to 24 months for the Boulder campus. Thus, in five years, the expected commodity Internet bandwidth demands will be about 500 Mbps and the Internet2 requirements will be about 1 Gbps.

More and more functions of the university in general, and the Boulder campus in particular, depend upon the reliable operation of the network, not just across campus, but also to the global Internet.
Essential network services (such as the Domain Naming System (DNS), the Dynamic Host Configuration Protocol (DHCP), and authentication and authorization services such as RADIUS and Kerberos/IdentiKey) all need to be available at all times.

Growth in modem usage is approximately 50 concurrent connections per year. Growth in DSL customers is less than half of that, presumably because neither Qwest nor ITS have promoted the service.

As the campus expands its firewall capabilities at the campus border, the demand for more complete and authenticated access from the global Internet will grow. Such a demand is usually met with a Virtual Private Network (VPN) service. ITS is currently testing a VPN service that it expects to rollout to the campus within the next few months. That service will grow as more people use their own ISP for access to the Internet and to campus networked resources.

Specific Recommendations Include

• Continue to provide incremental increases in commodity Internet and Internet2 bandwidth to accommodate demand.
• Given that sufficient bandwidth may not be affordable for all uses, continue to limit the effects of entertainment uses of the Internet and explore options for providing Quality of Service guarantees to certain uses of the Internet such as video conferencing.
• Continue to offer services in support of advanced networking applications such as those offered across Internet2 including multicast and IPv6.
• When the funds become available from the State to rewire the campus, examine the options for installing more optical fiber between buildings as more uses for that fiber develop.
• Once the campus is able to support 100 Mbps to any desktop, the campus backbone, currently using 1 Gbps links, will need to be upgraded to 10 Gbps.
• The campus must place more emphasis and support on the reliability of its network access and services.
• The campus should have at least two separate connections to the commodity Internet, with service coming into the campus at two different locations.
• The campus should invest in more reliable power (i.e., electrical generators) for key locations on campus where essential networking services are provided.
• Continue to provide modem and DSL services to the campus customers. Expand these services as the demand grows.
• Build the Virtual Private Network (VPN) service as demand requires.
• Provide support for mobile computing environments, particularly with respect to wireless and mobility issues, by providing network related training for Tiers 2 and 3 and by providing more networking documentation for Tiers 1, 2, and 3.
• Network security is an important issue and it is addressed in the Security section, 4.2.

Steps

Implementation

• Continue to monitor the bandwidth demands made by the campus and make incremental upgrades to the campus core and to add bandwidth to support increased use of Internet2 and the commodity Internet.
• Task ITS with ensuring that entertainment uses of the Internet do not negatively impact the academic and administrative uses.
• Task ITS with providing at least two separate connections to the commodity Internet, with service coming into the campus at two different locations.
• As part of its disaster recovery and business continuity planning, the campus should determine where additional electrical generators should be provided to insure reliable network services in the face of extended electrical outages.
• Several departments already implement VPN services to provide their clients with authenticated, secure access to networked resources on campus. ITS is about to offer such a service for the campus in general.

Communication
• Access to the campus network via DSL is cost effective, and the campus should encourage its constituents to use that service when appropriate.
• The campus should develop a set of best practices with respect to uses of the campus network.

Policy & Standards
Recommend a policy that clarifies that entertainment uses of the Internet must not interfere with the academic uses of the network and charge ITS to enforce that policy.

Required Involvement

Governance & Authority
Network services for the campus fall under the authority of the Office of the Associate Vice-Chancellor for Campus and Academic Technology (AVCACT) with the advice of the IT Council. Pockets of semi-independent subnetworks on campus are managed by individual departments to meet their own programmatic needs. These subnetworks are termed “Alliance Networks” to reflect that they still rely upon many of the essential network services provided by ITS.

Required Departmental Involvement & Responsibilities
ITS networking will need to continue to manage and maintain the campus network and its connections to Internet2 and the global Internet. Campus departments maintaining alliance networks will coordinate with ITS.

Expected Costs

Annual IT Infrastructure Investment
A second ISP connection of 60 Mbps will cost approximately $15,000 per month or $180,000 annually. Electrical generators at the Engineering Center and at the Computing Center would cost approximately $300,000 one-time plus $10,000 per year maintenance.

Operating and Maintenance
No new operating or maintenance costs are proposed other than for a second ISP.

Personnel
No new personnel are suggested in this section of the plan.

Funding
The funding for these activities will come from existing general fund support for networking and from recharges for network services including the “Alliance Network” fees and the normal charges for 10 and 100 Mbps network connections. That funding still leaves a substantial funding gap that manifests itself in an overly long equipment replacement cycle, insufficient staffing, less Internet bandwidth than is required to meet the growing demands, a lack of redundancy in access to the global Internet, and less reliability in the face of long power outages.
Timing
Continuing funding for a second ISP should be sought as soon as possible.
3.1 Networking – Wireless (Section II of II)

Recommendation: Expand and coordinate wireless LAN access across campus in order to meet increasing demands for more mobile access to campus and Internet resources.

Discussion of the Recommendation

Current Situation
The currently supported standard for wireless network access is the IEEE 802.11b standard. This supports 10 Mbps wireless Ethernet service over distances generally limited to 150 feet indoors and up to 1000 feet clear line of sight outside. Devices that support this standard have dropped dramatically in price over the past year and are readily available from most computer/network outlets. This has made these devices increasingly popular. The campus has instituted a policy that requires that departments coordinate their wireless access point installations with ITS.

There are approximately 25 wireless networks on campus using an estimated 60 access points in 20 buildings. There is complete, or nearly complete, coverage in three buildings: Business, Regent Hall, and the Computing Center. In the Engineering Center, for example, there is complete wireless coverage in the classroom wing, the main lobby, and the Real McCoy grill, but there is no official coverage in the departmental laboratory wings. In a classroom in Education, one professor finds that it is much easier and more flexible to use wireless laptops than to try to use wired desktop computers.

Rationale
Wireless network access is particularly attractive in facilitating mobility for the campus community. It is often ideal for common areas such as classrooms, conference rooms, teams rooms, and libraries. Wireless is not generally an acceptable alternative to wired connectivity in an office, due to the slower speed, shared media, and less secure service than wired.

Over the timeframe of this plan, we expect that Personal Digital Assistants (PDA) will begin to replace laptops as the more prevalent choice for mobile computing and that many of them will use wireless network access to stay connected to the Internet.

Customers often need more than the usual technical support when installing wireless access cards and access points. Wireless network access technology is evolving, and easily within the timeframe of this plan, the campus will see substantial changes in the technology as it moves to higher speeds and more restricted coverage. In addition, the campus must work toward offering suitable security that is easy to use.

Specific Recommendations Include

- Continue to implement wireless network access capability across campus, both in public, common places and in dedicated departmental spaces in a coordinated fashion in order to insure that the service is secure and reliable.
- Enforce the wireless policy to ensure that departments that wish to implement network access capability should do so only after consulting with ITS.
Steps

Implementation
• The campus, with technical support from ITS, is already deploying wireless network access in common areas across campus on a limited basis as funds become available.
• ITS already is working with departments to coordinate and even manage their private wireless network access installations.

Communication
• The campus wireless policies must be communicated broadly to the campus through town meetings, website updates, and campus bulletins.
• Implementation plans and schedule must be communicated to the campus through regular website updates, campus bulletins on major milestones, and Tier 2 support community updates for communication to departments.

Policy & Standards
IT Council has established policy that requires any 802.11 wireless network installation be coordinated by ITS to ensure non-interfering use of the available frequency spectrum and to be sure that departmental wireless activities do not compromise broader campus uses of wireless. This policy can be found at: http://www.colorado.edu/its/policies.html

Required Involvement

Governance & Authority
Wireless access implementations on campus fall under the authority of the Office of the Associate Vice-Chancellor for Campus and Academic Technology (AVCACT) with the approval of the IT Council. This responsibility and authority has been delegated to ITS for implementing the policy.

Required Departmental Involvement & Responsibilities
• The AVCACT and IT Council will continue to provide guidance and direction.
• Campus departments must coordinate wireless installations with ITS.
• ITS must develop frameworks for Memorandums of Understanding for departmental partnerships.
• Partner departments will provide funding and input on the developing demands for wireless network access.

Expected Costs

Annual IT Infrastructure Investment
Broad campus coverage would require at least $300,000 initial outlay for installation of 150 access points. Less than one third of that amount is equipment costs with most of the balance devoted to construction. The Information Technology Infrastructure Improvement Plan (ITIIP) includes a budget of $200,000 for wireless network access.

The campus should expect to replace or add 45 access points at $1000 each for each year over the next five years. This requires budgeting $45,000 per year for equipment.

Operating and Maintenance
The above annual costs include maintenance.
Personnel
It is expected that continuing support for 150 wireless access points distributed across campus would cost about $80,000 including salary, benefits, training, and operating expenses.

Funding
Funding for an initial, broad wireless deployment is included in the IT Infrastructure Improvement Plan (ITIIP), but funding for that plan is currently delayed by State fiscal problems. Some additional, earlier, and even continuing funding may be available through the use of student technology fees.

Timing
The timing of this deployment is largely tied to the ITIIP, although ITS is attempting to make some small, initial improvements prior to the availability of that funding.

Phase One of the ITS deployment plan, which includes public areas in the Norlin Library, the Engineering Center complex, and public areas of the University Memorial Center, will be nearing completion in fall 2002. This initial phase will be completed as funding is developed.

Phase Two of the ITS deployment plan includes large classrooms and auditoriums across the campus. This phase will begin once funding is established. Expected start: spring 2003.

Phase Three of the ITS deployment plan includes departmental installations and administrative offices across campus. Campus departments have been prioritizing themselves in the deployment by providing funding for hardware and network access charges, which will continue to be an option throughout the deployment process. Expected start: winter 2003/spring 2004.
3.2 Enterprise Directory Services

Recommendation: Provide a framework of policy, data, tools and processes for Directory Services for CU-Boulder within the context of the University-wide environment.

The Enterprise Directory must become a trusted and authoritative data source for CU Boulder resources. The Directory Service—scalable, flexible and robust—must be usable by a variety of authorized, independent applications and services, supporting security mechanisms, enabling relationships, and resolving discrepancies in information between communities, systems and services.

Discussion of the Recommendation

Current Situation
The CU-Boulder Enterprise Directory was implemented November 5, 2001. Since that time, the Directory Services continues to mature as its production environment is strengthened, policy is reviewed and established by the Directory Governance Board (DGB) and requests for usage are addressed. Based upon the first few months of the Directory’s life, it is apparent that a continuous stream of requests for enhancements and usage must be prepared for and effectively handled.

Rationale
An Enterprise Directory is a critical component of any institution’s middleware infrastructure. It is the glue that holds together the applications our institution is dependent upon and the networking and hardware upon which these applications are built. A robust Enterprise Directory Service provides the foundation that allows an institution to maximize the effectiveness of all components of its IT environment. To accomplish this, the Directory Service must offer:

- A clear direction toward enterprise-wide, general purpose Directory Services (and away from special purpose, system-specific directories).
- A trusted data source.
- Accessibility by a wide range of applications and services.
- Integration with campus-wide and application-specific security services.
- Identity management, data management and relationship management services set within a unified and consistent management model.
- A robust production environment to ensure availability and responsiveness.
- Location-independent access to directory information.
- A Directory Governance Board that ensures appropriate use of the directory, appropriately prioritizes directory-related requests, and addresses process issues highlighted by the Enterprise Directory.
- Collaboration with major initiatives such as CU-Boulder security, ITS service provisioning, University of Colorado four campus directory deployment, and Internet2 initiatives.

Specific Recommendations Include
Over the next five years, the primary goal of CU-Boulder’s Enterprise Directory Service is to become the centerpiece for middleware services for the campus. This goal plays an integral role with Section 3.3 (IT Service Provisioning Infrastructure) of this strategic plan.
• The Enterprise Directory must be positioned to support the security initiatives of CU-Boulder-ITS, particularly authentication and authorization.

• As it matures, the Enterprise Directory Service should adhere to its strengths and continue to expand upon these (i.e., manage the identity and attributes of objects stored within the directory, ensuring the integrity, accuracy and currency of these objects; supply commonly-needed data from trustworthy sources to trusted inquirers; support those applications which would benefit from directory-enablement; maintain an inquiry vs. transaction orientation.)

• An all-campus effort should be undertaken to establish the Registry 1 as the central authority for university-wide identity management.

• The Directory Governance Board must continue its active involvement with the Enterprise Directory, reviewing pending requests for Enterprise Directory enhancements and usage, prioritizing these requests, and delivering its recommendations to ITS with the goals of maximizing the directory’s utility to the campus, adhering to directory policy and making the most effective use of directory development resources – all within the context of concurrent IT initiatives.

Steps

Implementation

• Directory support of authentication and authorization requires collaboration among the ITS Security Coordinator, IT Architect, Enterprise Directory Project Manager, and Directory Manager as well as coordination of strategic directions of Security and Directory initiatives. The Enterprise Directory must ensure a single identity and properly defined affiliation(s) for each directory entry. Specific attributes required by authorization schemes must be evaluated by the Security Coordinator and Directory Manager to determine appropriateness of inclusion within the Enterprise Directory.

• The directory must be positioned to continue to support new initiatives without compromising performance, stability or integrity. To do this:
  o The directory should be flexible enough to accept new sources of data yet adhere to robust identity reconciliation processes within the Registry.
  o The directory should be flexible enough to add new attributes while cognizant of industry best practices regarding design issues such as multiple vs. single use attributes and application-specific attributes.
  o Access to information within the directory should be available to those who demonstrate need through appropriate authentication and access control mechanisms.
  o Secure processes must be built by ITS that allow entries to be created in the directory for individuals or objects that fall outside the realm of the University’s source systems in order to provide Directory-dependent services to all affiliates who are entitled to these services.
  o Secure processes must be built by ITS that allow individuals to add and update information about themselves that is not available from systems of record in order to ensure the completeness of information for entries within the directory.
  o The directory structure must accommodate additional objects such as organizations, services, systems and groups in order to support the middleware services depended upon by these entities.

• Create an all-campus task force to address issues and craft an implementation plan for a university-wide identity management infrastructure.

1 Registry: a university wide database that houses information used by the Enterprise Directory. Logic applied at the database level (prior to populating the database) enforces the identity management and data reconciliation business rules upon which the Directory depends.
• Requests for directory usage and enhancements must be handled through continued communication between the Directory Project Manager, Directory Manager and Directory Governance Board coupled with monthly DGB meetings. Requests should come through the Directory Manager for an initial feasibility review and resource estimate. This review should consider: appropriate directory usage (query vs. transaction), evaluation of requests for new attributes (appropriateness for a general directory vs. an application specific database), and potential sources for new data. The initial analysis of the directory-related requests should be forwarded to the DGB for prioritization considering both directory-specific initiatives and campus-wide initiatives.

Communication

• Communication within the Directory Services development environment focuses on the Directory Services Project Manager and the Directory Manager and their collaboration with concurrent IT initiatives (i.e., Security, Account Management, email, portals, etc.) as well as with the technical staff involved with supporting the Directory. This communication will be accomplished by:
  o Meeting individually with project leads for various initiatives.
  o Building project teams for specific directory enhancement initiatives.
  o Monthly meetings with the Directory Core Team for as long as the directory initiative work warrants these meetings.

• Communication with the campus and University will be focused primarily on:
  o Monthly Directory Governance Board meetings. DGB members are responsible for bringing their constituents’ concerns to the Board and for relaying Directory-related information to their constituents.
  o Periodic updates from the Directory Services Project Manager to the IT Council.
  o Formal presentations to various university governance boards upon request.

Policy & Standards

Directory Policy, which is subject to periodic review and update. See: http://www.colorado.edu/committees/DirectoryServices/

Required Involvement

Governance & Authority

Office of the Associate Vice Chancellor for Academic and Campus Technology

Directory Governance Board, with decision-making representatives from key constituencies of the Enterprise Directory (Registrar, Human Resources, Faculty Affairs, Libraries, Housing, University Management Systems, and ITS)

Required Departmental Involvement & Responsibilities

• ITS to provide directory management, operational support and development work.
• Web Communications to provide directory development work.
• IT Council to provide guidance and programmatic direction.
• Human Resources representatives and Registrar to provide data-related expertise.

Expected Costs

Personnel

• Existing Costs: Directory management, project administration and directory infrastructure development and support costs are approximately $240,000 annually.
• New Costs: Personnel for design, development and implementation of core campus services and applications based on the Enterprise Directory is expected to require 1.5
additional full time employees (FTE), which will cost approximately $135,000 annually (including salaries, benefits, training, travel, etc.).

**Operating and Maintenance**

- **Existing Costs:** Enterprise Directory hardware maintenance and software licensing costs are approximately $10,000 annually.
- **New Costs:** Capital costs to upgrade hardware and ensure adequate performance for expanded use of the Enterprise Directory is expected to cost approximately $40,000 annually.

**Funding**

The general implementation and ongoing production/operation costs of basic directory services are currently funded by ITS. New costs associated with development of core campus applications and costs of capital upgrades to accommodate core services require general fund support. Departmental-specific enhancements and applications that require modifications to use the directory should be funded by the specific department application/system owner.

**Timing**

- **Enhancements/Initiatives review:** Directory Governance Board meets monthly and will continue to do so through the life of the Enterprise Directory or until no longer deemed necessary (as the Directory matures and demand decreases).
- **Security initiatives:** coordinate with security, authentication and authorization security plans (target timeframe: spring/summer, 2002 (authentication) through calendar 2002 for various security components).
- **Ongoing Enhancements:** no drop in directory development demand is anticipated over the next five years. Sequencing of individual initiatives will occur as the initiative presents itself. Each request will be reviewed and prioritized by the Directory Governance Board, working with a three-to-six month detailed project plan. All requests will be considered in conjunction with the overall IT Strategic Plan, which includes many directory-dependent initiatives.
3.3 IT Service Provisioning Infrastructure

Recommendation: Create a campus-wide infrastructure that establishes and maintains an identity for each campus affiliate and enables the provisioning\(^2\) of access to campus resources.

The IT Service Provisioning Infrastructure (ITSPI) will address account maintenance processes, naming protocols, persistent identity, enterprise authentication, and enterprise authorization.

Discussion of the Recommendation

Current Situation

Technology has advanced to the point where a rich set of on-line services can be delivered to the campus user. The consequence, however, is that administrative control over various services and resources are distributed among many entities on-campus and off. This has resulted in:

- A heterogeneous technical environment as each entity independently chooses a technology for providing and managing their specific service.
- A diverse and inconsistent set of policies and processes as each entity uniquely addresses the issues of security, privacy and managing access to entity-specific services and resources. Practices within one department may place others on campus at risk.
- A wide variety of identifiers that are potentially overlapping or inconsistent: user-based, role-based, core system-based (SIS, HR), or administrative-function-based (i.e., ID Card), etc., with little or no reconciliation between the identifiers.
- Redundancies and inefficiencies as individual campus entities develop their own processes and solutions for provisioning and managing departmental or system-specific accounts.
- A multitude of identifiers, passwords and processes creating both a fragmented user experience and an insecure environment as individuals build homegrown solutions for managing their logins and passwords.
- Inconsistent and most likely insecure mechanisms for assigning, storing and transmitting passwords.
- Potential for improvements and enhancements restricted by departmental budgets that focus, justifiably, on the department’s primary mission rather than on IT development.
- A level of responsibility that may exceed the department’s ability or desire to manage increasingly complex IT issues.

Rationale

Centralizing the campus IT Service Provisioning Infrastructure and providing appropriate delegated authority enables campus IT service providers to devote their energies and resources toward meeting department-specific business needs while capitalizing upon the features of a centrally-provided, readily available infrastructure. This model offers significant economies of scale by minimizing the inefficiencies inherent in redundant solutions scattered throughout the campus. At the same time, it offers a flexible suite of tools that can be used by IT managers to provide end-to-end services specific to their individual constituencies’ requirements.

Authentication and access management policies, mechanisms, and administrative interfaces will be consistent, robust, and trusted campus-wide, offering multiple benefits:

- Decreased management burden.

---

\(^2\) Provisioning: The act of determining who can access what services and assigning identities, roles, permissions, and criteria at the user and system level that allow for that access.
• Reduced risk throughout campus IT.
• Enhanced data and process flow capabilities and compatibilities between systems, departments and campus-wide entities.
• All campus IT services built upon the centralized infrastructure will be in auditable compliance with regulations such as FERPA and HIPAA.

Much as the campus network infrastructure is taken for granted and, consequently, has become an integral component of IT and campus life today so, too, should an IT Service Provisioning Infrastructure become a given that can be relied on to serve campus IT needs. Future applications, IT-enabled learning objectives, middleware, and other facets of IT-enhanced campus life increasingly expect various aspects of ITSPI to already be in place. If the infrastructure is not built centrally then CU-Boulder will realize significant inefficiencies and increased risks as departments attempt to build these components separately.

Specific Recommendations Include
• Build a single authoritative identity per person – across the university and its systems – with attributes that can be referenced by authentication and authorization mechanisms. Use this authoritative identity to facilitate single/same sign on and to help establish trust relationships between campus systems, between campuses and with UMS.

Adopt the industry direction of middleware services built around a robust Enterprise Directory
• Centralize the storage and management of institutional identity data increasing the ability to manage it consistently, in compliance with regulations, and so it is auditable for compliance.
• Establish Identity and Role management policy that answers the questions of: who gets an identity, under what circumstances can or should an identity or role be established, what roles can be established for each identity, who has access to identity, who can change attributes, and what are the valid sources for identity and role creation.
• Centrally coordinate authentication and authorization policies and mechanisms, and trust relationships among data owners and specific applications. Coordination will take the form of mandates, best practices and standards.
• Design and implementation must carefully consider concurrent technological developments, the momentum of other IT architectural initiatives and Higher Education’s IT directions – balanced with the university’s capabilities for implementing technical solutions within a particular timeframe.

Our ability to muster resources will influence our ability to deploy ITSPI. Campus-wide participation requires people with appropriate skill sets and the proper prioritization of duties in order to ensure a successful deployment of the infrastructure.

Steps

Implementation
• Establish the Enterprise Directory as the single authoritative source of Identity and Roles; tie campus applications to this source.
• Build a flexible framework that accommodates application-specific directories as extensions of the Enterprise Directory.
• Increase campus-wide trust in IT direction. To do this, ITS must demonstrate its understanding of departmental issues by partnering with individual concerned departments to arrive at appropriate solutions.
• Evaluate the costs, benefits and capabilities of commercial technologies that may offer desired ITSPI component functionality.
• Implement ITSPI in a modular fashion so that components can accommodate changes in technology, enhancing the infrastructure without disrupting the infrastructure.
Establish campus technology standards based on industry standards that allow all complying systems and applications to take advantage of campus middleware services. Implement authentication services as a key component of ITSPI striving for single/same sign-on.

- Use the Enterprise Directory and emerging web standards for the implementation and policy management of a centralized Provisioning and Access Management infrastructure. See the ITS working document “E-mail Address and Account Provisioning for ITS Systems.”
- Incorporate Active Directory into the IT Service Provisioning Infrastructure as an extension of the Enterprise Directory.

**Policy & Standards**
- Establish campus authentication policies and standards.
- Establish campus entitlement and access management policies and standards.
- Establish Active Directory policy and Service Agreement to set expectations for administrators, AD administration, and policy exceptions.
- Establish standards that the campus can follow to take advantage of middleware services.
- See also Enterprise Directory policies regarding identity and role management.

**Required Involvement**

**Governance & Authority**
- The Office of the Associate Vice Chancellor for Academic and Campus Technology.
- Directory Governance Board as the leadership board for the Enterprise Directory and its role in identity management.

**Required Departmental Involvement & Responsibilities**
- Individual campus departments and IT providers. ITS must know the campus well enough to understand the impact of proposals on current departmental practices, workflows, and IT management personnel as well as the issues involved with integrating existing technologies into the new infrastructure.
- IT Council to provide guidance, programmatic direction, and policy review and approval.
- Campus Tier 2 support representatives to provide insight into their specific business needs.
- ITS initiative leaders for coordination amongst initiatives.
- ITS to provide core leadership in the design, maintenance, operation and management of the ITSPI.
- UMS as a partner in the implementation of ITSPI.
- Campus Card program as a key player in the identity arena.

**Expected Costs**

**Research, development and implementation**

*ITS-campus trust building:*
Combination of new and existing resources

- Initial investment: Dedicated effort to assess and understand campus business needs; six months, two people at 50% each (one existing FTE, one new FTE).
- Existing resources:
  - Ongoing: Continuous effort at something less than half time.
Campus technology standards:
Existing resources:
   Ongoing committee (assume a highly skilled representative from each of ITS’s core services, meeting monthly plus research)

Access Management Solution:
There is a wide range of options in this area. Some packaged vendor solutions provide complete identity and access management with policy engines and application programming interfaces. On the other end of the scale are “freeware” options that provide simpler web single sign-on services, but lack administrative tools or interfaces. Either approach requires a robust hardware and network infrastructure in order to provide highly available campus services. Some example pricing:
Vendor solution (eg. Oblix, Netegrity, iPlanet):
   $140,000 - $500,000 plus 3-6 person months
WebISO / Shibboleth:
   Software is free.
   Servers: $40,000; Proxy or Switch: $20,000;
   Development/install: $15,000 plus 3-6 person months.
The freeware solution is likely to be adequate initially, provided it is coupled with some provisioning mechanism (see below) for controlled services. The capabilities of the free solution, along with enhancements provided by peer institutions, may improve as our needs increase, thus keeping this a viable approach. The cost of a vendor solution is included under the assumption that we will, eventually, outgrow a free software solution. The degree to which we do outgrow it will dictate the cost.

Account Provisioning Utilities
While it is a long term objective to manage access via well established identities and roles, the reality is that many systems will continue to require system-specific accounts or provisioned access. An account provisioning system translates entitlement and access management policies into the creation of accounts on systems, using system aware agents. The DURM/Uniquid/Adduser suite, written in-house, is the current such system in place and is used widely on campus. It will need to be rewritten or replaced as a component of the new Directory driven infrastructure.
Vendor solution (eg. Access360, Waveset, Business Layers):
   Gross est. $500,000 plus 4-8 person months
Rewrite DURM:
   4 people 10 months each
(Assume central components could share existing hardware resources).

Application-specific ITSPI requirements:
New Resource requirement: 1.5 FTE
   Note: Estimate will vary greatly by application. Assume two new application requests per month plus a multitude of existing applications that may request directory enablement (Libraries, Recreation Center, Wardenburg, Facilities Management, Housing, Bookstore, iVote, Off Campus Housing, Faculty Information System, Telecom Management system, PLUS, etc.)

Active Directory deployment:
Today: 1000 machines, budget in place for hardware requirements to support FY03 new requests if requests are not actively solicited.
Aggressive marketing estimate: 4000 new machines. Hardware budget already requested. Up to two new FTE would be needed for support.
Highest level of saturation likely would total an estimated 7,000 machines and require a minimum of 2 additional FTE.
Active Directory build from Enterprise Directory:
Existing resources:
  Two person months for development and implementation (analyst/programmer)

Cost of not implementing an IT Service Provisioning Infrastructure
Approximately 20 departments on campus are currently managing significant IT assets with their own staff. All of these departments will rely at least upon an Active Directory infrastructure for mission critical operations. Absent any central middleware services, all 20 of these departments will be required to spend some effort accommodating their future needs in this area.

There are six departments (in addition to ITS) that support vendor-supplied mission critical administrative applications with campus-wide impact. Within the next four years it is highly likely that without a campus infrastructure, all of these departments will need to implement some form of directory/middleware services to support their applications. The departments are: Libraries, Recreation Center, Wardenburg Student Health Services, Housing, Facilities Management, and the Bookstore. If each of these departments requires 1 FTE and $200,000 in one-time capital spending to develop a modest but functional departmental service, the cost to the campus is 6 FTE and $1.2M. The result is six disparate implementations, none as robust as the proposed set of central services. This cost and result would be in addition to the infrastructure that ITS will (must!) build to support campus-wide student and faculty IT-dependent services.

Funding
Funding for the development and deployment of the IT Service Provisioning Infrastructure should be handled at a campus-wide level. Consideration should be given to department-specific funding for migration to the ITSPI of department-specific applications and services.

Timing
The Enterprise Directory, Active Directory, ITS Account Provisioning, and WebISO components of the ITSPI are all in process - each with its own level of resources, project plan and schedule. These initiatives are interrelated and, as such, must be coordinated within the ITSPI. The future momentum of each of these initiatives is dependent upon the strength and continuity of funding streams. Also dependent upon the funding stream and its impact on these ITSPI components are the multitude of initiatives that await the build-up of the IT Service Provisioning infrastructure. Only as the ITSPI components are further developed and implemented, can new initiatives – which must necessarily be aligned with the ITSPI – be developed and implemented, assuming the necessary resources (development staff, operational staff and funding) are in place.
3.4 Telephony – Voice over IP (Section I of II)

Recommendation: Prepare the campus for the next generation of telephony services by evaluating and deploying limited integrated voice and data services over campus data network by VoIP\(^3\).

*Discussion of the Recommendation*

**Current Situation**
Campus telephony today is based upon traditional circuit switched technology that is distinct from the campus data network. However, these two networks ride on much of the same infrastructure, and the campus data network is expected to be the basis for the next generation of voice related services.

**Rationale**
The campus is one year into the planned seven-year lifecycle for the existing phone system. Voice over IP (VoIP) is expected to be the next generation telephony solution. This technology would allow the university to manage voice and data services across a single network and provide campus customers with a wider variety of services. The key to successful transition to the next generation of telephony solutions is to start exploration and small-scale deployment of this technology well in advance of the next expected upgrade.

**Specific Recommendations Include**
- Test VoIP solutions beginning in the summer of 2002.
- Deploy VoIP solutions as a remote service option for all new remote voice solutions beginning in 2003.
- Deploy VoIP in pockets on campus as appropriate.
- Prepare campus network for VoIP deployment.

**Steps**

**Implementation**
- Complete a VoIP test on campus using a variety of sets, customer needs and campus network locations.
- Deploy smaller VoIP solutions in remote areas not connected to campus.
- Prepare campus network to meet the needs of VoIP as the next generation phone system.

**Communication**
- Work with IT Council to develop a communication plan that prepares the campus for this eventual transition. This would include periodic updates on the service offerings and provide campus with an overview of this technology.
- Conduct forums as part of the ongoing Tier II community event series to discuss the VoIP deployment on campus.

**Policy & Standards**
- Develop a set of service guidelines that include quality of service (QoS) and other technical standards necessary to support VoIP deployment as a real alternative to circuit

---

\(^3\) VoIP, for purposes of this discussion, is applying voice service onto the data network.
switched telephony. Standards to include network viability requirements and analysis programs.

- Create a standard set of supportable voice features that transfer from the circuit switched arena to the data network with minimal impact to customers.
- Create documentation for Tiers I – III of the 4-Tiered support model.

**Required Involvement**

**Governance & Authority**
The Office of the Associate Vice Chancellor for Academic and Campus Technology.

**Required Departmental Involvement & Responsibilities**

- ITS Networking to configure and provision regions of the campus network to handle VoIP deployment.
- ITS Networking to provide the interface between the campus network and existing phone systems.
- ITS support Tiers I, II and III to be prepared to support VoIP customer.

**Expected Costs**

**Annual IT Infrastructure Investment**
Initial VoIP test already funded. During the course of the next four years, we will be doing small-scale deployments that are within existing cost recovery models. No additional annual funding expenditures are expected since the test period is well within the expected life of the campus phone system.

**Operating and Maintenance**
Ongoing costs to be recovered through service fees.

**Personnel**
No new personnel expected to support the deployment. However, some training will be required for voice service personnel to support the new technology.

**Funding**
Cost recovery models consistent with existing campus voice services delivery will be developed.

**Timing**
Program begins with FY 02-03 for the VoIP test on campus. Testing and evaluation should be completed by spring 2003. Deployment of VoIP to new remote sites will happen as appropriate while continuing to examine the technology in preparation for next generation phone system.
3.4 Telephony – Service Integration and Mobility (Section II of II)

Recommendation: Make it easier for campus customers to access voice related technologies and services.

Discussion of the Recommendation

Current Situation
Voice services on campus are limited to telephone sets physically connected to the campus PBX system. These services on the voice network do not support freedom of movement about campus. Increasingly, campus customers are using carrier-based mobility technologies such as cell phones and two-way radios. These technologies are not integrated with the set of campus voice services currently available. Customers are required to go to the technology in order to get the services they need rather than the technology coming to the customer. This situation applies to basic telephony, voice mail, as well as administrative services.

Rationale
Campus customers have noted a lack of compatible voice service offerings that support mobility and service integration. In an effort to bring technology to customers, ITS should support the voice communications tools that customers need while responding to rapidly changing technology. The campus should design such a strategy to provide improved access to all members of the university community including those with disabilities.

Specific Recommendations Include
- Cordless telephone set offerings for mobility within all campus buildings
- Mobility features support for cell phones, which will allow customers to use their cell phones to receive campus calls simultaneously with their campus telephones.
- Voice activated (hands-free) control of telephone and voice mail features.
- Desktop computer access to telephone and voice mail features.
- Investigate and deploy integrated voice mail and email on the desktop.
- Provide additional web based resources to assist customers with service changes while automating simple requests with proper authentication.

Steps

Implementation
- Develop cost effective and scalable solutions that include short- and long-range telephony options for campus customers.
- Research wireless telephony opportunities that may integrate with campus wireless LAN planning.
- Develop and provide voice-activated technologies that integrate with existing campus telephony offerings.
- Enhance the web interface for telephone service requests so that simple requests can be processed automatically.
- Explore and develop integration of desktop voice mail access with current email access.

Communication
- Develop a communication plan that includes mobility solutions as part of Tier II community events, and other customer forums, as well as disability access.
• Create a communication plan, which regularly provides campus customers with updates regarding service improvements and additional feature offerings.

**Policy & Standards**

• Create a plan that incorporates FCC and other regulations regarding the deployment of wireless solutions. Integrate this plan with campus spectrum management.
• Incorporate campus Environmental, Health and Safety (EH&S) guidelines regarding radio frequency emissions.

**Required Involvement**

**Governance & Authority**
The Office of the Associate Vice Chancellor for Academic and Campus Technology.

**Required Departmental Involvement & Responsibilities**

• ITS for installation, provisioning and maintenance of equipment on an ongoing basis that is consistent with development of wireless LAN on campus.
• ITS support Tiers I-III to be prepared to support the customer.
• ITS CAUS Group for email support and integration.
• ITS Networking Group for the development of these services.
• Environmental, Health and Safety (EH&S) for review of acceptable levels of transmission energy.

**Expected Costs**

**Annual IT Infrastructure Investment**
No annual infrastructure increase is planned other than an estimated $100,000 investment during the FY 05-06 for integration of the campus voice mail and email.

**Operating and Maintenance**
Costs for operating and maintenance are expected to be within normal operating funds.

**Personnel**
No new FTE are required to support the development or ongoing maintenance of this activity. Provide training to personnel on the safe deployment and operation of wireless equipment.

**Funding**
Funding for most services can be obtained through ongoing cost recovery activities with the exception of voice mail and email integration, for which institutional funding should also be pursued.

**Timing**

• FY 02-03: Evaluate mobility features and technologies. Deployment of web based service request form.
• FY 03-04: Development of automation services. Deployment of small-scale solutions.
• FY 04-05: Deployment of automation services and development of integration.
• FY 05-06: Deployment of integration of voice mail and email.