CHABOT-LAS POSITAS COMMUNITY COLLEGE DISTRICT

INFORMATION TECHNOLOGY MASTER PLAN

ITS DETAILED SPECIFICATIONS

Updated 2007

This document presents the 2007 update on the state of the Information Technology Infrastructure at all three CLPCCD sites: the District Office, Chabot College and Las Positas College. This document has been assembled from the collective inputs of District ITS staff and College Computer Services departments. The information herein includes detailed descriptions of servers, desktops, network cabling, wireless, network switches and routers, as updated from the original configurations documented in the 2005 ITMP and the 2006 update.

Given the level of detail that is presented, this information, if used improperly, could place CLPCCD in a vulnerable position with respect to viruses and other threats that could debilitate the IT infrastructure. As such, this document will be circulated to a limited set of District IT and College Computer Services staff, and is considered "For ITS Limited Distribution only" to those individuals who have a need to know this information in performance of their daily jobs.

Issued: December 2004
Updated: March 2005
Updated: May 2006
Updated: September 2007

Overview of Current IT Environment

Over the past year, the District ITS and Computer Services departments have participated in the design of the new building and upgrade projects. This document summarizes the key areas of upgrade.

5.0 Conduit Infrastructure

As the design of the new Measure B Bond buildings has been evolved, a number of conflicts with the existing Telecommunications infrastructure were identified. The programming requirements of the new buildings prioritized the placement and functions of the new buildings. As described in the Facilities Master Plan, new buildings were being placed on existing conduit routes and vaults. Production cabling that runs in these existing conduits would be destroyed, cutting off the voice/data and possibly fire alarm services to the buildings on campus. In addition, the Chabot conduits were congested and not adequate to support the cabling that would be needed for the new buildings and connectivity.

CLPCCD District ITS noted the priority of the building requirements and participated in addressing these design requirements with the following initiatives.

Site proofing – In May of 2005 CLPCCD District ITS engaged the services of GeoTech Locating to identify, verify and document the Communications conduits and vaults on the Chabot and LPC Campuses. The results were a detailed set of CAD drawings that showed the pathway utilization and cable routing. From these results, CLPCCD District ITS presented a summary of the conduit rerouting requirements to DMJM Program Management and CLPCCD Bond Construction Management.

Building Construction Document Review – CLPCCD District ITS participated in the design review of projects on the CC and LPC campus to evaluate the building site plans and identify specific impacts on the infrastructure. Any construction that would introduce demolition or loss of service to voice/data connectivity on campus was documented and brought to the attention of the Architect/Engineer design team for modification.

Conduit Design Sessions – CLPCCD District ITS participated in several design sessions to discuss alternative conduit routing that would provide a new pathway to the buildings being impacted. This included working with teams from Interface Engineering, P2S Engineering, Sandis and other A&E firms to come up with a satisfactory design.

Detailed discussions of the specific areas covered by these initiatives is included in the following paragraphs.

5.1 Chabot Campus – Conduit Redesign

At the Chabot campus, the proofing project quickly identified that the existing conduits and vaults were full, in disrepair and unable to support new connectivity. It was clear that there was a need to replace the infrastructure with new vaults and conduits, rather than trying to salvage the current system. The Chabot campus needed the addition of new conduits and vaults for the following purposes: 1) the construction of new buildings (Instructional Office Building, Community and Student Services Center, Chabot Portables) and modernization of buildings (300, 500, 800, 900) which will provide new copper and fiber backbones to these locations, and 2) new single mode cabling which will be installed to all the remaining buildings on campus. In addition, the

construction of the Community and Student Services Center and Instructional Office Building would destroy an existing conduit bank that provided connectivity to Buildings 900/1000, 1100 and 1200/1300.

With the decision to build a Central Plant on the Chabot campus, a utility loop for the hot/cold and domestic water was designed. IT conduits would be built in a joint trench parallel to the water service. A backbone loop of eight (8) four-inch IT conduits was designed to circle the campus. Three (3) four-inch building conduits would extend from the IT loop into each building. Twelve (12) four-inch conduits would be constructed to provide new access to the Building 300 MDF. Six (6) four-inch conduits would be built to provide additional access to the Building 200 MPOE. These requirements were provided as a set of design guidelines, illustrated in a color-coded marked-up site plan drawing presented to the architect team. Project Manual Specification sections were also provided, which described the conduit design requirements, referencing the TIA/EIA 568B, 569B, 758A and other applicable standards, and NEC/CFC code requirements. A key component of the IT design was the penetration of the new conduits within a 50 foot distance of the telecom room. It is a fire code requirement that the fiber/copper cables be not exposed for more than 50 feet from point of first exposure in the building.

As the design project progressed, the IT conduit design became the basis of design and construction for the IT conduit expansion at Chabot. This project was awarded as a design-build contract to Southland Inc. Redwood City Electric was engaged as a subcontractor to Southland for the design of the IT infrastructure.

CLPCCD District ITS worked with Swinerton, Southland and RCE to review and enhance the design for the conduits so that they conformed to the design standards and CLPCCD's requirements. This has included reviewing the building penetrations, conduit sweeps and bends, the vault sizes and configurations and other design parameters. For cost reasons, Chabot Program Management (Doug Horner) asked if the IT building penetrations could be placed in the same locations as the water penetrations, i.e. at the building mechanical rooms. CLPCCD District ITS was in agreement with this approach, providing it would not adversely affect the pathway for future cable installation.

In some buildings, the new point of conduit penetration fits within the 50-foot rule. In other buildings, this will require a conduit extension from the point of penetration, to the telecom room. Also by code requirements, the conduits will need to be made of rigid or intermediate conduit material. Doug's estimation was that the conduit extension would be less costly than the in-ground conduit extension (priced at $2,000 per foot). By TIA 569B requirements, there cannot be more than cumulatively 180 degrees of bend between pull boxes, and the first pullbox determines the start of the 50 foot measurement.

The design-build process led to some fluidity of the resultant construction process. What was presented on drawings did not necessarily get built as such during the construction process. This led to some reworks as inspections revealed bends that did not conform to TIA conduit design guidelines. Additionally the congested nature of the campus underground, and the perimeter of the new building construction limits the locations where the utilities could be laid.

Phase 1 of the conduit infrastructure is scheduled for completion in February of 2008. This phase includes the following buildings: 200, 300, 500, 800, 900/1000, 1100 and 1200/1300.

Following the completion of this phase of construction, CLPCCD District ITS will bid for the installation of single mode fiber for buildings 1100 and 1200/1300. This backbone is needed

because the construction of the IOB and CSSC will disrupt the existing fiber runs to these buildings. These buildings need to be converted to new fiber backbones through the new conduits prior to the commencement of the construction of these buildings. It is expected that the installation of the new single mode backbones to service these buildings will occur immediately following the availability of the Phase 1 conduits.

As later phases of the conduit construction occur, the campus will be equipped with a new set of conduits extending around the campus, and into the buildings. CLPCCD ITS' goal is to then install new zero water peak single mode fiber to all remaining buildings, and fully convert off the aging 62.5 multimode fiber, to Gigabit LX connectivity over single mode. In keeping with the directions documented in the original CLPCCD Infrastructure Upgrade document (dated 2005), CLPCCD District ITS plans a future installation of two fiber backbones to each building, routing the fiber in diverse routes, back to the core switches located in buildings 200 and 300 on campus.

5.2 Las Positas Campus – Conduit Redesign

At the Las Positas Campus, significant building expansion is planned. These projects do have substantial impact on the current voice/data infrastructure.

College Center for the Arts (CCA) Amphitheatre

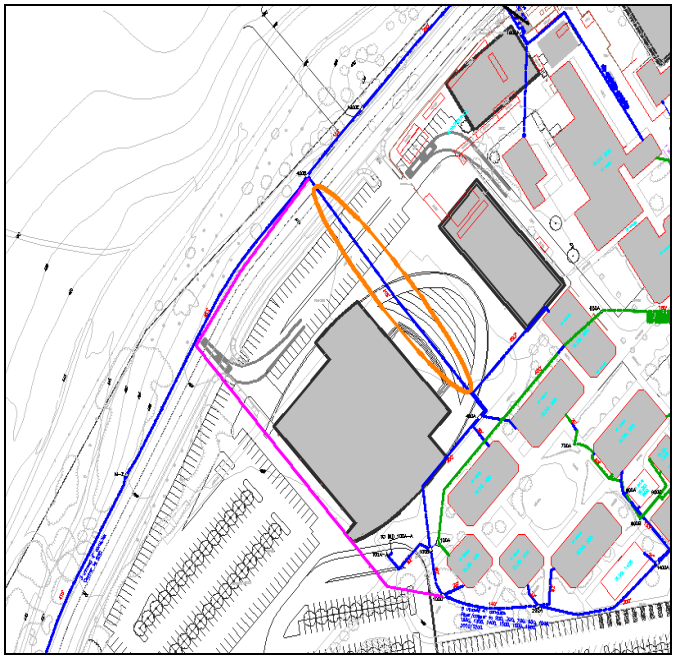
With the decision to build the College Center for the Arts in the existing soccer fields, it became clear that the location and structure of the Amphitheatre would disrupt the current voice/data cabling that serviced most of the buildings on campus. The 1998 bond project installed a bank of fourteen (14) four-inch conduits from a vault in the north loop road, underneath the east end of the soccer field, to a new vault placed on the north side of building 400. This conduit bank was extended around the south side of the campus to deliver new multi-mode fiber, single mode fiber and copper backbone cables from building 1900 to the following buildings on campus: 100, 200, 300, 400, 500, 600, 700, 900, 1000, 1100, 1200, 1300, 1400, 1500, 1600, 1800, and 2000/2100. All of these backbone cables will be destroyed by the Amphitheatre construction.

CLPCCD District ITS worked with DMJM Program Management and P2S Engineering to identify a new conduit route that would replace the conduit path across the existing soccer fields. A route was chosen through the horticulture area and basketball courts to intersect with an existing vault by building 1300. The bid package with CAD drawings and specifications was prepared and ready for bidding in the fall of 2006. A portion of the design was incorporated into the construction of the Multi-Disciplinary (MD) Building. This allowed the MD building to be connected into the campus voice and data network through a new route. The remaining P2S design elements were to be bid as a separate construction package. With the decision to build a Central Plant on the LPC site, additional conflicts arose with this new routing that was detailed in the P2S package. Specifically, the IT Building was rotated to accommodate the space requirements of the Central Plant building. This then placed the IT Building in conflict with the proposed path for the P2S conduit rerouting. Adjusting the P2S routing to avoid the IT building was not possible because of 1) uncertainties with the Central Plant building footprint and 2) negative impact to the Horticulture program. The P2S design was determined to be abandoned.

CLPCCD Facilities construction then engaged the services of Sandis to perform a comprehensive review of the site utilities. This project was to identify all utilities needing to be rerouted (gas, electrical, water, storm drain, communication) and then make recommendations for redesign of these utilities. CLPCCD ITS supplied proofing documentation and met several times with the

Sandis design team, to provide information on the conflicts as they pertain to the communications conduits.

After looking at several alternate paths, it seems that the conduit routing impacted by the Amphitheatre would be best rerouted, by extending the path to the west end of the CCA building, in a route parallel to the original route. This means that new conduit would be constructed along the loop road, using existing vaults, and new conduit/vault infrastructure would route across the proposed CCA parking lot towards existing MH100C. This is drawn schematically in magenta on the following diagram. Note that the blue route circled in orange is the path the existing path that will be dug up during the Amphitheatre construction.



Proposed Communications Conduit rerouting by College Center for the Arts

The required new cabling is as follows:

Building	Fiber	Copper	Vault Feed
100	24-strand SMF	100 pair *	MH100-C
200	24-strand SMF	25 pair	MH100-C
300	24-strand SMF	25 pair	MH100-C
400	24-strand SMF	25 pair	MH100-C
500	24-strand SMF	25 pair	MH100-C
600	24-strand SMF	25 pair	MH100-C
700	24-strand SMF	100 pair *	MH100-C
800	24-strand SMF	50 pair *	MH1900-D
900	24-strand SMF	25 pair	MH100-C
1000	24-strand SMF	25 pair	MH100-C
1200	24-strand SMF	25 pair	MH1900-D
1300	24-strand SMF	50 pair	MH100-C

1400	24-strand SMF	25 pair	MH100-C
1500	24-strand SMF	100 pair *	MH100-C
1600	24-strand SMF	25 pair	MH100-C
1800	24-strand SMF	50 pair	MH1900-D
2000/2100	24-strand SMF	200 pair	MH1900-D

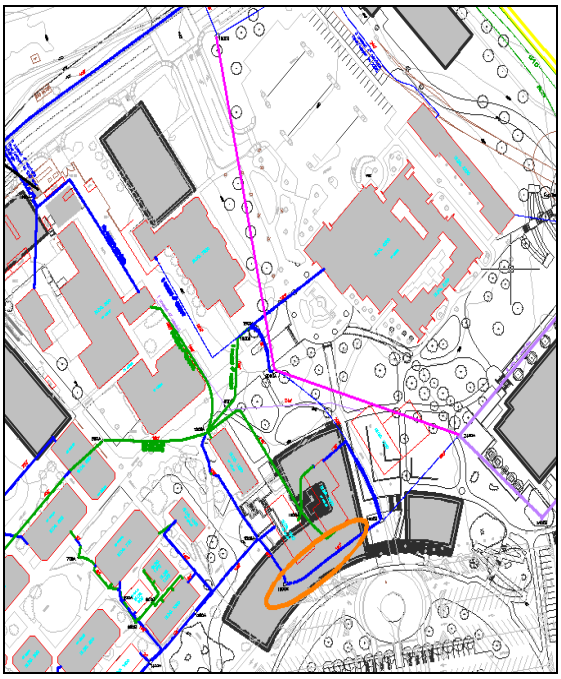
* Increased above current provisioning

A complete infrastructure will be constructed including: cable, terminations (fiber patch panels, voice protectors), service loops, cable management. This new conduit route (in magenta, above), and the required cabling infrastructure will be added to the CCA project to ensure that no excavation for the Amphitheatre is performed before the new conduits and cabling are in place, and converted into production.

Following construction of the new conduits and cabling, CLPCCD District ITS and College Computer Services will perform the voice and data conversion off the old cabling infrastructure and onto the new cabling infrastructure. The most laborious part of this will be the individual cross-connects for each telephone connection, which will take a minimum of 20 minutes per telephone to move and verify.

LPC Student Administrative Services Building

Concurrent with the Sandis analysis effort, preliminary designs were released for the LPC Student Administrative Services building. This building will be constructed on the south side of campus, in the area currently occupied by buildings 1500 and 1600. This new building will compromise MH1500-A, MH1500-B, MH1600-A and MH1600-B and their associated conduit paths. (Conduit path shown below circled in orange.) These routes currently service cabling to buildings 1500, 1600, 1800 and 2000/2100. Concurrent with the CCA construction, a new set of conduits is being designed to provide a pathway across campus from the north side of the loop road, into vaults MH2000A and possibly MH2400A.

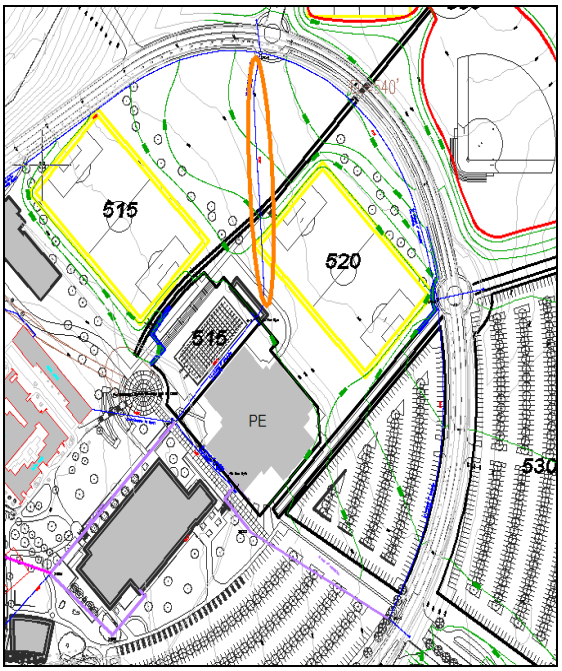


Proposed Communications Conduit rerouting by Student Administrative Services Building

This path must be designed in conjunction with the future renovation projects which will be modifying the landscaping and sidewalk features of this area. While the pathway shown above is just diagrammatic, when this is designed, it is prudent to place new vaults along the path to provide future connectivity to Building 2000 when the remodel/expansion of that building occurs. Early programming indicates that: 1) Building 2000 will be expanded along its north boundary, 2) new Telecom Rooms and backbone cabling will be provisioned and 3) the Building 2000 voice/data cabling will be completely replaced.

New Route to Physical Education Complex (PE)

The PE backbone cabling routes a conduit path that goes diagonally through the undeveloped land on the east side of campus. This routing was built with the 1998 remodel, with the intent that it would service future buildings on each side of the conduit path. With the design of the new soccer facility, these conduits will be demolished (conduit path shown below circled in orange).



Communications Conduit rerouting by PE

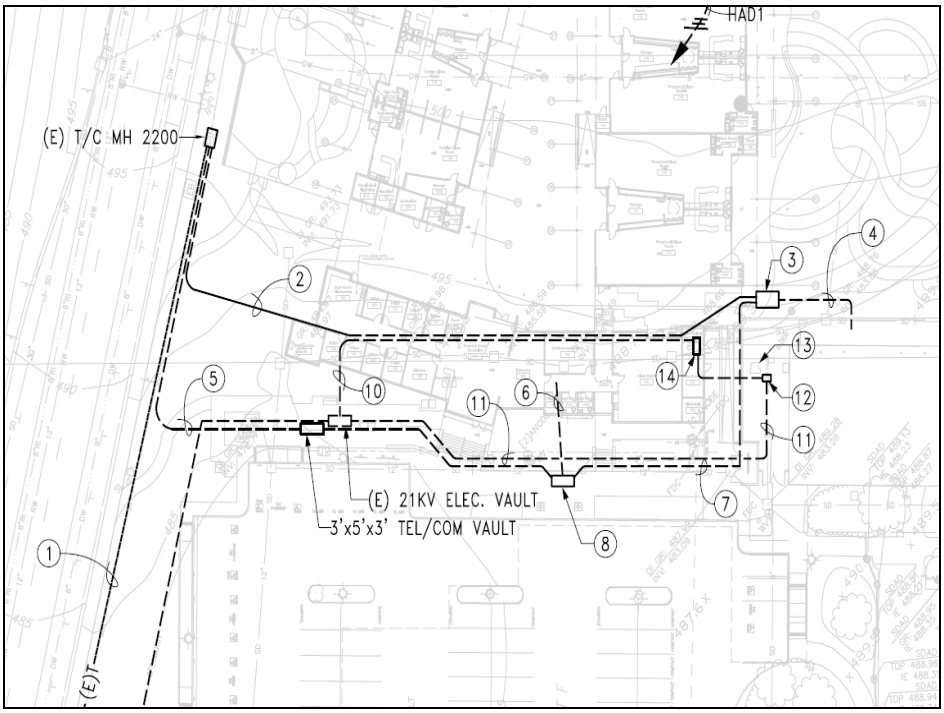
To provide an alternate path to the PE Building, a new conduit bank was installed between the outer loop road and the southwest corner of the PE building. This routing was constructed as part of the Multi-Disciplinary (MD) building project, and current provides a pathway for the MD Building backbones. An interim link that cascades the PE building from the MD building is in place to keep PE in service when the conduits in the diagonal route are demolished. Since the interim cabling is limited in the number of connections it can support, the long term solution is to run new dedicated copper and fiber backbones into the PE building using the routing from the outer loop road to the southwest corner of the PE building.

CLPCCD ITS is proceeding with a cabling project to replace the PE backbones. This project will provide new fiber and copper backbones to the PE 115 Telecom Room. The cables will follow the loop road conduit path

New Route to Building 2200

When the CDC construction project begins, the conduits routing backbone cabling to Building 2200 will be demolished (Shown with note (2) on diagram below). An interim cabling to Building 2200 through old multimode fiber is in production through an alternate path that will not be affected by the construction.

The CDC project will provide new conduits and fiber/copper from MH2200A in a non-conflicting route to both the CDC and 2200 Buildings as shown below:



5.3 WAN UPGRADES AT CLPCCD

CLPCCD relies on AT&T T-1 service for private network connectivity to its sites. This includes the following links:

Chabot to LPC – This link is comprised of three T-1s, providing a total of 4.5 Mbps bandwidth. This link is heavily used by LPC for administrative access to Banner resources.

Chabot to District Office – This link is comprised of one T-1, providing a total of 1.5 Mbps bandwidth. This link is heavily used by the District Office for administrative access to Banner resources and Internet access. This link is almost always saturated and users complain about slow response time.

LPC to District Office –This link is comprised of one T-1, providing a total of 1.5 Mbps bandwidth. This link is used by LPC to access DO applications, and is also configured for routing of videoconferencing traffic between Chabot and the District Office. It also provides a redundant route in the event that the dedicated line between Chabot and the DO is disrupted.

As part of the Measure B Bond Construction projects, a number of new servers and applications have been added to the network. These include 1) archival of CAD drawings and documents, 2) FTP download of files, 3) remote video monitoring of construction projects and 4) Prolog Construction Management software. Most of the information stored by these applications is centralized at the CLPCCD District Office locations, thus increasing the WAN utilization and

prolonging response times beyond previous levels. This necessitates upgrades to the WAN links as soon as possible.

CLPCCD District ITS has approached the need for WAN upgrades through multiple upgrade steps. The short-term upgrade approach has included the following implementations:

Router Upgrades – Originally deployed in the late 1990s, the core 7507 router on the Chabot campus has been replaced with state-of-the art Cisco router equipment. Controlling the VLAN routing at Chabot campus, the 6509 router provides packet throughput in excess of 400 million pps. The 3825 WAN router controls the T-1 links to the LPC and District Office. The net improvement in routing is more than 100 times that possible with the old equipment. Router upgrades have also been installed at LPC (3825) and District Office (2811) locations.

Additional T-1 to the District Office – To provide immediate relief for the saturated line and slow response times, CLPCCD District ITS has installed a second T-1 line. This doubles the bandwidth to 3 Mbps. In addition to the added capacity, CLPCCD District ITS has implemented traffic management to more precisely route the traffic so that the mission-critical access to Banner is not compromised.

Fiber Upgrade – The most significant performance gains are to be realized by upgrading from the multiple T-1 technology to a Fiber based Ethernet connection. OptEMAN is a recent product offering from AT&T that offers this type of connectivity. The OptEMAN service is provisioned on a fiber connection, to an AT&T switch, using a copper RJ-45 connection to the customer equipment. OptEMAN speeds can be configured in stepwise increments from 5Mbps through 1 Gbps and the links “look” like standard VLAN connections. OptEMAN offers the following benefits for CLPCCD:

- The interface to the CLPCCD network is a standard RJ-45 FastEthernet or Gigabit connection. This does not require any special interfaces for the CLPCCD equipment.
- OptEMAN can be deployed at different speeds appropriate for the size and connectivity requirements of the sites. Chabot can be allocated higher bandwidth commensurate with the concentrated access to the Banner servers. The OptEMAN speeds can be incremented as the traffic needs required.
- Since all three CLPCCD sites are provisioned with fiber, we know that the service can be installed. Note: The District Office site is not using the fiber. It was provisioned by the previous tenant. However, since the AT&T fiber terminal is there, it does show that AT&T will be able to support fiber connectivity into the DO building.

Since OptEMAN provides superior speeds, it is more costly than then current T-1 services. However the “net” bandwidth to be gained is less costly than the equivalent bank of multi-linked T-1s that would provide comparable bandwidth. Also, OptEMAN can easily be reconfigured for to rebalance speeds at different sites. This will become very useful when the Data Center moves to the LPC site and the bandwidth will need to be rebalanced.

Implementation plans are in progress for the following OptEMAN configuration:

Chabot: 20 Mbps
LPC: 10 Mbps
District: 10 Mbps

The estimated deployment window is early 2008.

5.4 WIRELESS INITIATIVES

CLPCCD District ITS has worked with its student, faculty and administrative representatives at the Chabot and Las Positas College to establish a direction for the use and management of wireless networking. Since each campus operates independently from each another, there will be variances in the implementation details, schedules and locations particular to each campus.

CLPCCD Wireless Directions

CLPCCD does not view wireless network as a replacement for traditional cabling and high-speed switching infrastructure. Rather, the initiatives for wireless network at CLPCCD sites have the following goals:

- Wireless networking will provide flexible connectivity for student access in open classrooms and congregation areas inside of buildings.
- Wireless networking will augment the instructional environment at the Colleges, over and above the capabilities already in place in classrooms and computer labs.
- Wireless networks will be designed and enabled to ensure sufficient performance is available.
- Wireless connectivity will be configured with appropriate security and authentication methods, so that CLPCCD ITS will at all times be aware of the level and type of wireless connections in use.
- Wireless networks will only be implemented when CLPCCD ITS is able to appropriately monitor activity, intrusion and performance of the wireless networks.

In one of the Measure B Bond projects, CLPCCD has installed new state-of-the-art Gigabit network switches. This infrastructure replaces old hub/switch equipment that has been in use for 5-7 years. The new network equipment offers advanced capabilities for connection and management of network traffic, including power-over-ethernet (POE) ports, quality of service (QOS), high availability, intrusion detection and network authentication.

The CLPCCD Wireless Initiative is project that will build on the new switching infrastructure, in conjunction with comprehensive security and good operation/management techniques to offer CLPCCD's students, faculty and staff a safe and high-performing wireless computing environment.

CLPCCD Wireless Working Group

A CLPCCD working group developed four classes of service after discussing the security and access issues for wireless. The classes recognize the relative sensitivity of data on the network and their usage. The four classes are:

1. OPEN
2. INSTRUCTIONAL
3. ADMIN
4. RESTRICTED

The Open class has the least number of restrictions, but also provides the least access. It is designed to only provide Internet access. Anyone could configure his or her system to operate without intervention by IT. This is the model currently used in the college library. No college-related data is available in this class.

The Instructional class provides access to machines on the college's instructional network where all student computers are connected. Connection to the network requires intervention by IT staff to properly program the wireless client to access the network traffic. This model is currently used in the mobile cart used on the campuses. Only college instructional information is available – no Banner student data can be accessed.

The Admin class is designed to carry traffic for our student information system, Banner. It provides the greatest security requiring both setup by IT and data encryption. At present Admin class wireless installations are not in place.

The final class is Restricted, which is designed for special applications such as HVAC and security control, which if compromised could cause failure in physical plant. At present there are no Restricted class wireless installations.

For IT, the freedom of untethered operation has been offset by fears of loss of control of operating networks. Wireless networks are typically viewed with suspicion because of the "out-of-site" connection to network this technology provides. The concern is that any random person could connect to the network and use it without permission. The team discussed these concerns at great length and came to some logical conclusions.

First, CLPCCD does not house any defense secrets on any of our systems – especially the Instructional ones. CLPCCD ITS/CS should temper the need for control by the knowledge of the data that is being secured. Further, systems are in place to guard sensitive data on the machines wired network. This is needed because CLPCCD already allows random persons to connect to the instructional networks using wired connections. The working group conclusions were to implement wireless technologies to provide ubiquitous access to enterprise data, application, and services. An analysis of what is feasible and reasonable for this ubiquitous access must be performed.

Early Wireless Deployments

As with most networks, there is always a population of end-users who are "early-adopters", demanding the implementation of new technologies, well in advance of having support mechanisms in place for their correct operation. Wireless access points, readily purchasable at a local computer store, and laptops that come wireless-enabled, compound that situation, since users may feel empowered to implement their own network connectivity. There is significant vulnerability introduced when a rogue access point is connected to an administrative network port, particularly when physical cable connections and door locks were the method to previous limit access to a network jack. An insecure access point, default configured without WEP encryption or changes to the admin password, is a guaranteed way of inviting unauthorized access onto the network.

CLPCCD ITS has remained adamant that the network connectivity is the responsibility of the CLPCCD District and its Network Analyst, and unauthorized wireless connectivity is strictly disabled through the use of port configurations and real-time monitoring.

To date, limited span 802.11b wireless networks have been enabled by CLPCCD ITS at each campus. At Chabot College, the wireless access points are located in the (1) library, (2) physics labs, (1) on a mobile cart with laptops [NSF Project], and (1) for Chabot ITS testing located in room 310A, [normally off]. The Library AP is configured as an "OPEN" access point (no WEP), on a separate VLAN, and only offers limited access to the Internet. The Library wireless network offers no access to school resources that are not normally available through an Internet connection. The mobile care and physics lab networks are "INSTRUCTIONAL". The Chabot ITS AP is development.

At LPC, the wireless networks are used by students and faculty to gain access to server applications and the Internet. There are currently 3 wireless access points sanctioned and used on the instructional networks. These wireless access points are located in the (1) library, (1) Science with directional antenna, and (1) in room 803 computer lab. The access point in the Library is configured with SSID LPC-LRC and no WEP key. As such, "OPEN" access from Library visitors is available, although the wireless network is secured to only grant Internet access and no access to any LPC networks. Limited wireless has been expanded to other buildings on campus so students can take advantage of the free Internet access.

All of these wireless networks are protected behind the CLPCCD firewall, but laptops connecting to these wireless networks are not protected from each other. No tools are enabled to browse the wireless computers before granting access, to ensure that they are patched to an adequate level, or equipped with virus protection/personal firewalls. As such, wireless student laptops are vulnerable to attacks from other laptops which may share the same wireless network and possibly be infected with a virus. To date, there has been no occurrence of virus infection or hacking from the wireless networks, but the threat is still there. CLPCCD regularly monitors the use of the wireless networks for performance and utilization.

Next Step Wireless Directions

CLPCCD District ITS has set a direction to keep wireless networking services at the College campuses as a District provisioned and operated service, as done with the wired network. Many vendors are advertising wireless services that they will deploy at a customer site. In analyzing third party outsourcing services such as "FreedomLink" from SBC, these solutions are not considered viable options because of several reasons, including:

- Infrastructure upgrade requirements – Service providers require a level of cabling connectivity that is not universally available across the campuses.
- Intrusiveness to CLPCCD's private network – Since these service providers install access point locations that connect to the CLPCCD network infrastructure, their wireless network activity could impact the performance of CLPCCD's private network.
- Contract Limitations – Service providers demand an "exclusive" provisioning that precludes CLPCCD from deploying additional wireless services.
- Student Value – Many of these providers have a low-ball initial contract offerings that limit the access provided to students to a few web sites. Higher priced contracts increase access but often are not price advantageous compared to what is provided.

CLPCCD is developing a more detailed strategy to define wireless access requirements and operating procedures. While the working group called for ubiquitous wireless access, the practicality of implementing end-to-end connectivity from anywhere on campus has narrowed the actual scope of the wireless environment. In particular, CLPCCD has examined the construction aspects of wireless laptop networking and defined the following directions:

1) As part of the modernization of existing facilities and new construction funded by the Measure B bond, all classrooms, conference rooms, theatre halls and inside assembly areas will be wired to support wireless connectivity. This includes the placement of data jacks and electrical outlets dispersed throughout the ceiling structure, in sufficient density to support access points that offer connectivity to the population of students/attendees who may congregate in each specific room space. Note that while the cabling/power will be provided, each room will be evaluated on an individual basis before being equipped with working access point hardware.

2) No provision has been made to install electrical outlets distributed to student seats to support recharging of wireless computers in the classroom. The cost for installing electrical outlets is exceedingly high and it is impossible to accurately estimate the density of outlets that should be designed into a classroom. Support of a teacher's workstation and podium in each classroom will be provided.

3) Wireless networking will be provisioned to inside buildings only. The concept of having pervasive wireless access so students can lounge outside on the lawns and access the network from the hillsides is very idealistic. Operating a computer out of doors leads introduces may issues such as 1) glare on the screen thereby reducing visibility, 2) dirt and other contaminants that are windborne and deposited on keyboards and 3) lack of electrical power. Because of the wide-open spaces on the Chabot and LPC campuses, it would take a great density of wireless access-points, externally mounted to the building façade in order to "beam" appropriate signal strength to outdoor areas. This is a sizable cost to implement and presents a difficult maintenance environment. Once the wireless networks inside the buildings are deployed and functional, services to the building exteriors may be reevaluated in conjunction with technological advances and new products.

Wireless-Equipped Computer Equipment for Faculty

CLPCCD District ITS in conjunction with the College Computer Services departments provide desktop computers for faculty use. These desktops are imaged with a standard set of applications and installed in faculty offices. To date, there is limited momentum to move towards laptop computers as the preferred computing platform. A fixed number of laptop computers are available from loaner pools at each campus, and checked in/out as requested. Faculty which currently own their own laptops and bring them to campus, are integrated onto the network as needed.

The direction toward laptops is an important part of the wireless strategy because veritably all of the manufacturers include 802.11b/g cards as part of the laptop hardware. As faculty move towards preferring laptops, network mobility requirements will increase, requiring the implementation of seamless wireless roaming from office to classroom. Wireless deployments will be planned to match the connectivity requirements of the faculty.

Wireless Design Objectives

Moving forward with the classes of wireless networking formulated by the working group, the following technical directions are set:

Use of 802.11b/g/n – In the past several years, wireless technology has begun to favor of 802.11g networks at 54 Mbps, because of the increased speed over 802.11b networks at 11 Mbps. The 802.11g networks still operate in the 2.4 GHz "open" spectrum range, and can be in conflict with legacy wireless communications. However, manufacturers have not embraced the more proprietary 5 GHz 802.11a technology and laptops are usually equipped with 802.11b/g functionality. CLPCCD does not want to force the purchase of an 802.11a card onto students who will be using the wireless network, nor do they want to assume responsibility for the configuration and operational support of student laptops. As such, 802.11b/g technology will be the standard used for all future deployments. Development of the 802.11n standard, which will be forthcoming in 2-3 years, will further enhance speed and performance on the wireless networks.

Use of encryption – In keeping with the security approach described above, CLPCCD will implement varying levels of encryption on the different classes of network.

Open – On the Open network, no encryption will be used. To limit easy access, the SSID will not be broadcast, and users will need to enter the SSID into their configurations to gain access. This network is considered a "hostile" network and will continue to have access equivalent to an Internet connection from home or any off-campus wireless "hot-spot". Typical users of this network are students who bring their own computers to school or other campus visitors. Campus locations include the Libraries, student lounges and cafeterias.

Instructional - Wireless access via SSIDs configured for the Instructional networks will be configured with 128-bit WEP encryption keys. SSIDs will also be hidden and entered into the configuration with the WEP key. Typical users of this network are mobile laptop carts, selected CLPCCD managed laptop computers.

Admin – Administrative computers will be configured with the highest level of encryption. This includes the rotating WEP keys and hidden SSIDs. See also authentication section below. Typical locations are the District Office, Board Rooms and limited administrative areas.

Restricted – The deployment of wireless for Restricted networks is under review. While wireless access could be advantageous to the maintenance workforce, the locations where wireless access is needed include places like boiler rooms, mechanical rooms and electrical rooms. These areas often contain heavy machinery that emit a great deal of electrical interference. The likelihood that wireless connections would be functional in these areas is slim.

Authentication – Wireless authentication will be implemented for all networks except the Open network. This will require that prospective wireless network users sign-on and identify themselves before being granted access to the wireless network. Use of RADIUS Authentication has been prototyped. The long term goal is to integrate the authentication to the Novell NDS or Banner database for real-time student and employee verification. This goal is synergistic with a long-term direction to single authentication on the wired network. However the complexities of

multiple directory services (NDS, LDAP), user databases and formats introduce significant barriers which must be overcome in order to achieve a seamless "single sign-on" authentication.

Monitoring – An important element of network maintenance is real-time monitoring of performance and access. CLPCCD will continue to provision an "Open" wireless network that is available to transient students and visitors. This opens up the possibility that hackers and virus-infected computers could be connected to CLPCCD's network and introduce network traffic that will be damaging to network users. A critical element to maintaining a functional network is the early detection of traffic anomalies and intrusion activities. As such, CLPCCD will augment its current suite of network monitoring tools with those that are customized for the wireless network environment. Tools include capabilities such as wireless client monitoring and notification, rogue access point detection, etc. CLPCCD will be assessing monitoring tools in conjunction with access point product selection.

Tactical Steps

1) Formation of a District/College committee who will:

    a. Review previous statements and discussions on wireless directions
    b. Review current wireless environments to discuss pros/cons, what is working/what doesn't work, end-user feedback, etc.
    c. Assemble new needs from faculty and admin users
    d. Evaluate College directions to provisioning student access (Free? Assessed? Ongoing support model? Help Desk?)
    e. Ratify direction and strategy
    f. Identify/quantify deployment locations for each campus
    g. State of technology review (Wireless hardware, tools, probes).
    h. Vendor presentations and analysis
    i. Hand off the District for :
        i. Design of wireless networks in each building.
        ii. Identify wiring needs for data and power support of APs.
        iii. Preparation of Bid(s)
    j. Solution Bid(s), award and deployment.

Progress towards accomplishing these steps is anticipated during 2008.