# Technical Note

| | |
|---|---|
| *date:* Nov 3, 2005 | *subject:* **LCLS Control System Network Requirements** |
| *from:* Doug Murray<br>x2235 | |
| *department:* LCLS Controls | |

*Linac Coherent Light Source* • *Stanford Synchrotron Radiation Laboratory*



The LCLS Controls Group has requirements for network access, during the construction of the LCLS, and for the Accelerator itself once operational (the production, or operations network.)

Requirements are organized as Functional, Non-functional, Schedule and Cost. Functional requirements specify what the network must do; non-functional requirements specify qualities that the network must have. Capacity, bandwidth and speed are examples of non-functional requirements. Schedule and Cost requirements are estimates based on current information, and in many cases are yet to be determined.

## Functional Requirements

1. The SCCS Group at SLAC shall be responsible for the design details and installation of the physical LCLS network as specified in this document. All design and installation details shall be reviewed by the LCLS Controls Group regularly as work proceeds.
2. The LCLS network shall support four conceptual subnets, each having distinct requirements. They are referred to as **Development**, **Test**, **Access Control** and **Operations**.
3. **Development subnet**; the LCLS network shall support a Development subnet for engineering and testing of components to be used in the LCLS accelerator.
    1. The development subnet shall isolate development activities from other SLAC network activity.
    2. Activity on the LCLS development network shall not interfere with normal activities on the rest of the SLAC network.
    3. The development subnet shall be accessible to offices in Building 280A, where the LCLS Controls Group currently reside, but also to a few specific Lab areas within SLAC, to be determined as work proceeds.
    4. The development subnet shall be accessible to desktop computers, laptop computers and single-board computers used by the LCLS Controls Group.
        1. The LCLS Controls Group shall be able to do day-to-day work on their desktop computers. Specifically, they shall have full access to resources on the SLAC network, and the Internet in general, from specific desktop or laptop computers residing on the development subnet, subject to the network policies in place at SLAC.
        2. Desktop and laptop computers shall be assigned DHCP or static IP addresses, as per standard SLAC policy.
        3. The LCLS Controls Group shall have the ability to add any reasonable number of single board computers to the development subnet. These computers shall not be directly accessible from the Internet, nor shall they be able to access anything outside the development subnet. They are considered to be in an Internet-Free Zone.
        4. Single board computers on the development subnet shall be assigned static IP addresses, according to standard SLAC policy.
    5. The development subnet shall contain a development server, which is accessible from all desktop, laptop and single board computers on that development subnet.
        1. The development server shall be physically accessible to members of the LCLS Controls Group, currently those located in Building 280A.

2. Certain specific individuals shall have administrative (root) privilege on the development server, either as a root password or through a "sudo all" capability.
3. The development server shall be accessible from Internet through a secure channel. It is not required to be directly accessible from the Internet; it may be accessed indirectly via an intermediate login host.
4. The development server shall provide TFTP-based file transfers. TFTP service shall only be made available to IOCs on the development subnet. TFTP service shall not be visible outside of the development subnet.
5. The development server shall provide NFS mounted directories as an NFS server, only to IOCs on the development subnet. The NFS mount service shall not be visible outside the development subnet.
6. The development server shall provide full access to AFS.
7. The development server shall provide all development tools, including compilers, debuggers, version control and other software deemed necessary by the LCLS Controls Group.
8. The SCCS Group shall specify a backup strategy for the development server.

4. **Testing subnet**; the LCLS network shall support a separate conceptual Testing subnet, on which LCLS Controls engineers can deploy test equipment intended for primary accelerator operations.
    1. The test subnet shall isolate any and all anomalous network activity to that subnet.
    2. Network test equipment shall reside on this subnet to accommodate testing.
    3. The Testing subnet is not required to have direct access to the Internet or other SLAC public networks.
        1. The Testing subnet shall be accessible from, and have access to, the Development network.
    4. The testing subnet shall provide a set of predefined IP addresses that can be temporarily assigned to network-enabled devices. As a footnote, it is important that an effective policy be implemented to manage the allocation and usage of these temporary addresses.

5. **Access Control subnet**; often referred to as the DMZ subnet, shall provide the only mechanism to access the operations network. The operations network is described under requirement 6 below.
    1. Only those devices in the Access Control subnet shall have access to the Operations network.
    2. There shall be an SSH Server on the Access Control subnet, which provides the only means by which an individual outside of the control room or accelerator halls can gain login access to the Operations network.
        1. A subset of SLAC User IDs shall be recognized and enabled by the SSH server, to allow remote login to the Operations network.
    3. There shall be a Web server located on the Access Control subnet, which shall provide open web-based access to most of the measured data being cached from the Operations network.
        1. The Web pages from this server shall not be accessible outside of SLAC.
    4. There shall be an EPICS Gateway server on the Access Control subnet, which will provide software running outside the Operations network with access to specific control and monitor points within the Operations network.
        1. The EPICS Gateway server shall recognize a subset of SLAC User IDs from specific hosts and provide them remote programmatic access to the Operations network.
        2. Only software running under an authenticated User ID shall be allowed control system access through the EPICS Gateway server.
    5. There shall be offline data servers available on the Access Control subnet. The majority of programmatic access to the control system data shall access that data on this server.

Specifically, this server shall maintain a regularly updated cache of accelerator controls data.

6. **Operations network**; the LCLS network shall support a separate dedicated network for the commissioning and operation of the LCLS accelerator.
    1. The operations network shall be completely self-contained. Specifically, it shall be able to perform all control system functions and provide all services without a physical connection to any other network.
    2. The operations network shall provide redundant network switching and connectivity support. For example, certain key pieces of network equipment shall be duplicated such that a failure of one key component will cause a second to come into effect.
    3. The operations network shall be populated by network devices having IP addresses in the Class A reserved space of 10.X.X.X.
        1. The SCCS Group shall provide the specific network range in which the IP addresses shall reside. Specifically, the second number in the dotted decimal notation shall be provided by the SCCS Group, effectively specifying a Class B range of addresses. For example, operations network IP addresses may be specified by the SCCS Group to be in the range of 10.10.0.X to 10.10.255.X.
        2. The third and fourth set of numbers in the dotted decimal notation shall be assigned by the LCLS Controls Group. The third set of addresses shall refer to subnets having related functionality or geography. For example, 10.11.100.X might refer to the Injection line components, and 10.11.300.X might refer to LTU components.
        3. The SCCS Group has the option of specifying an address allocation strategy beyond what is described here. For instance, there could be a policy to reserve IP addresses in a certain range for network diagnostic equipment.
        4. All MAC addresses and IP addresses in use within the operations network shall be recorded and made available to the SCCS Group. Ideally, this will allow easy identification of misbehaving network or computer equipment, or unwanted interaction of network equipment with elements outside the network.
    4. The operations network shall be centered in the Main Control Center (MCC) and connect all areas of the LCLS accelerator facility.

    The diagram in Figure 1 is meant to represent the LCLS accelerator facility, and the labeled, highlighted rectangles indicate where Operations network access is required. Those locations will house the IOCs and related instrumentation. Refer to requirements 6.4.5 through 6.4.20 below.

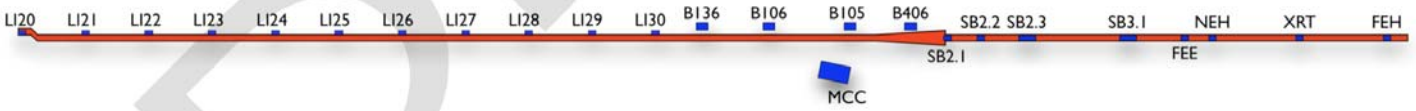


*Figure 1. LCLS Accelerator Areas and Anticipated IOC Locations*

The 'B' refers to an existing Building, 'SB' refers to Support Building (new construction), and XRT refers to the X-ray tunnel of the XTOD area.

1. All operations network nodes shall have the ability to communicate with any other node on the operations network.
2. Each IOC shall have its primary ethernet connection on a specific subnet.
3. Certain dual-homed IOCs shall have their secondary ethernet connection on a different subnet from their primary one, but on the same operations network. For example, the following 2 IOCs have primary connections to different subnets, but they are both on a dedicated subnet (VLan) for Fast Feedback. In practice, there could be any number of IOCs having their primary or secondary ethernet ports (but not both) connected to a Fast Feedback dedicated VLan.

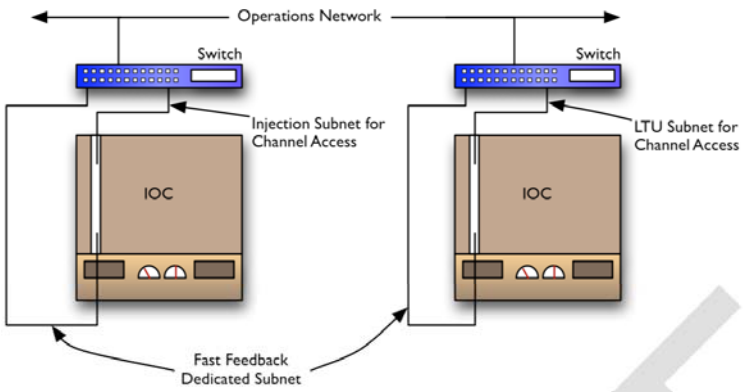


*Figure 2. Multi-homed IOCs with a Dedicated Connection*

4. Each area of the LCLS Accelerator having one or more IOCs shall also have a terminal server and a power management unit. Figure 3 below shows an example of IOC connections. Note that the terminal server and power management units are network devices connected to the ethernet switch, and ultimately to the Operations network.

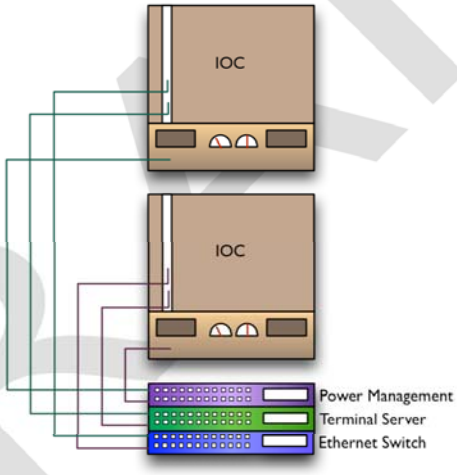


*Figure 3. Typical IOC Managed Connections*

5. The operations network shall provide service to IOCs and other network devices in the klystron gallery above the LCLS injector area at sectors 20 and 21 with at least 96 network ports.
6. The operations network shall provide service to the LCLS control system racks situated in the klystron gallery at each sector from 22 to sector 30 with at least 48 network ports at each sector.
7. The operations network shall provide service to Building 136, immediately east of sector 30 with at least 24 network ports. This shall serve equipment between Sector 30 and the first section of the Beam Switchyard (BSY) area.
8. The operations network shall provide service to Building 106 with at least 24 network ports, to provide access to equipment in the central BSY area.
9. The operations network shall provide service to Building 105 with at least 24 network ports, to provide access to equipment in the east BSY area, before the LTU area.
10. The operations network shall provide service to Building 406 with at least 24 network ports to provide access to equipment in the first part of the LTU area.

11. The operations network shall provide service to the LCLS Support Building 2.1, with at least 24 network ports to provide access to equipment in the LTU area.
12. The operations network shall provide service to the LCLS Support Building 2.2, with at least 24 network ports to provide access to equipment in the LTU area.
13. The operations network shall provide service to the LCLS Support Building 2.3, with at least 48 network ports to provide access to equipment in the LTU area and the west end of the Undulator Hall.
14. The operations network shall provide service to the LCLS Support Building 3.1, with at least 48 network ports to provide access to equipment in the east end of the Undulator Hall and to the Beam Dump area.
15. The operations network shall provide service to the Front End Enclosure (FEE) of the XTOD, with at least 24 network ports to provide access to equipment in that area.
16. The operations network shall provide service to the near hall of the XTOD with at least 24 network ports.
17. The operations network shall provide service to the X-ray tunnel of the XTOD with at least 24 network ports.
18. The operations network shall provide service to the far hall of the XTOD with at least 24 network ports.
19. The operations network shall provide service to the main control room for operator control consoles with at least 24 network ports.
20. The operations network shall provide service to various servers located in a server room in the MCC building with at least 24 network ports.

5. There shall be physical connection point (i.e. RJ45 wall jacks, or "walk-up" taps) located at specific points in the LCLS accelerator equipment areas.
    1. Only mobile computers and laptops configured by the LCLS Controls Group shall be usable in the LCLS accelerator equipment areas. Other computers will not be recognized nor allowed access to control system functionality on the Operations network, nor will they have access to the Internet or other SLAC services through the Operations network.
    2. Many locations in the LCLS accelerator equipment areas shall have "walk-up" taps. This includes the injection vault, klystron gallery, Linac tunnel, BSY, LTU and undulator areas, the XTOD areas and the X-ray beamlines. Their numbers are yet to be determined, but they will be part of the port allocation described above for each of those areas.
6. Secure and restricted wireless access shall be provided.
    1. Wireless access shall be available throughout the LCLS accelerator, including the injection vault, klystron gallery, Linac tunnel, BSY, LTU and undulator areas, the XTOD areas and the X-ray beamlines.
    2. Wireless transceivers shall not be permanently mounted in the accelerator areas. There shall be a small pre-determined number of portable pre-configured transceivers used for commissioning and maintenance purposes.
    3. Wireless access shall only be available to people having SLAC accounts, who also have LCLS Control System accounts. See Requirement 7.1 below.
7. Access to the operations network shall be restricted to a well-known set of users.
    1. Certain individuals shall be able to login directly to control consoles. These users shall have a standard SLAC computer account, and their LCLS Controls account shall have a user ID consistent with their ID on the SLAC network.
    2. Certain *types* of users shall be able to login directly to control consoles in the control room. For instance, there shall be provision for general operator login in the control room, with potentially limited abilities.
    3. Other users may retrieve data and interact with certain control system software through an EPICS Gateway service, which acts as a proxy. Gateway servers reside on the access control subnet, as stated in requirement 5.4 above.

8. The operations network shall be completely isolated, without access from any other SLAC subnet except for the **Access Control** subnet. Refer to requirement 5, above and a short-term requirement described in requirement 7 below.
    1. No access to the operations network shall be granted to any device other than one residing on the Access Control subnet.
    2. Certain SLAC services shall be made available to the operations network. Specifically, cable, drawing, support and technical databases shall be accessible from any operator computer in the Operations network.
    3. Printing shall be possible from the operations network, and forwarding to printers outside of the operations network shall be possible.
9. Several computers shall reside in the operations network for use as file or compute servers.
    1. No server shall have network connections to any network outside of the operations network.
    2. At least one server shall provide a copy of the development environment with a complete set of development tools.

7. **Temporary SLC-aware IOC Connection**; short-term access to the PEP/Linac Accelerator Control Network shall be provided, to allow the existing MCC Control System to control SLC-aware IOCs.
    1. Access to the LCLS operations network shall be provided to a specific PEP Proxy server. This PEP Proxy server shall have access only to a specific set of IOCs on the LCLS operations subnet.
    2. The VMS computer currently used for accelerator controls shall have secure access to a file server located in the LCLS operations network.

## Non-functional Requirements

1. **Development subnet**; all network devices on the development subnet shall have the ability to communicate at speeds up to 100 Mbps.
2. **Test subnet**; all network devices on the test subnet shall have the ability to communicate at speeds up to 100 Mbps.
3. **Access Control subnet**; all network devices on the access control subnet shall have the ability to communicate at speeds up to 1000 Mbps.
    1. Connections to other subnets in the LCLS network, or in the larger SLAC network shall have the ability to communicate at 100 Mbps.
    2. Connections to the Operations network from the Access Control subnet shall have the ability to communicate at speeds up to 1000 Mbps.
4. **Operations network**; all network devices on the operations network shall have the ability to communicate at speeds up to 1000 Mbps.

## Schedule Requirements

1. The Development subnet shall be implemented in several stages to accommodate LCLS Controls Group development work.
    1. The Development server shall be physically installed by November 1, 2005.
    2. The Development server shall be setup and configured by December 1, 2005.
    3. Developers shall be able to configure IOCs, build software and do basic IOC tests on the development subnet by December 1, 2005.
2. The Test subnet shall be implemented as needs arise, but not before December 31, 2005.
3. The Operations network shall be implemented according to a detailed schedule (see separate document) with specific milestones.
    1. Network access to the injector area building at sector 20 shall be available by May 15, 2006.
    2. Network access to the klystron galleries for each sector from 21 through 30 shall be available by December 2007.

3. Network access to the Linac BSY and LTU areas shall be available by April 2008.
4. Network access to the Undulator hall, beam dump and Front-end enclosure areas shall be available by June 2008.
5. Network access to the Front-end enclosure of the XTOD area shall be available by June 2008.
6. Network access to the Near Hall of the XTOD area shall be available by June 2008.
7. Network access to the Far Hall of the XTOD area shall be available by September 2008.
8. Network access to the X-ray transport lines of the XTOD area shall be available by November 2008.

### Cost Requirements

1. The total cost of the development subnet equipment shall be the responsibility of the SCCS group and the LCLS Controls Group.
    1. The cost of cables, switches and other network related hardware for the development subnet shall be the responsibility of the SCCS Group, according to current SLAC computing policy.
    2. The cost of servers, desktop computers, laptops and single board computers for the development subnet shall be the responsibility of the LCLS Controls Group.
2. The total cost of the test subnet shall be the responsibility of the LCLS Controls Group.
3. The total cost of the Access Control subnet equipment shall be the combined responsibility of the SCCS group and the LCLS Controls Group.
    1. The cost of cables and ethernet switches for the access control subnet shall be the responsibility of the SCCS Group, according to current SLAC computing policy.
    2. The cost of other network equipment such as terminal servers, remote power management units, as well as computers such as servers, desktop computers, laptops and single board computers for the access control subnet shall be the responsibility of the LCLS Controls Group.
4. The total cost of the Operations network equipment shall be the responsibility of the LCLS Controls Group.

### Suggestions for Implementation

The diagram in Figure 4 shows a conceptual layout of the required network. The four networks described above are shown; the **operations network**, and the **development**, **test** and **access control** (DMZ) subnets.

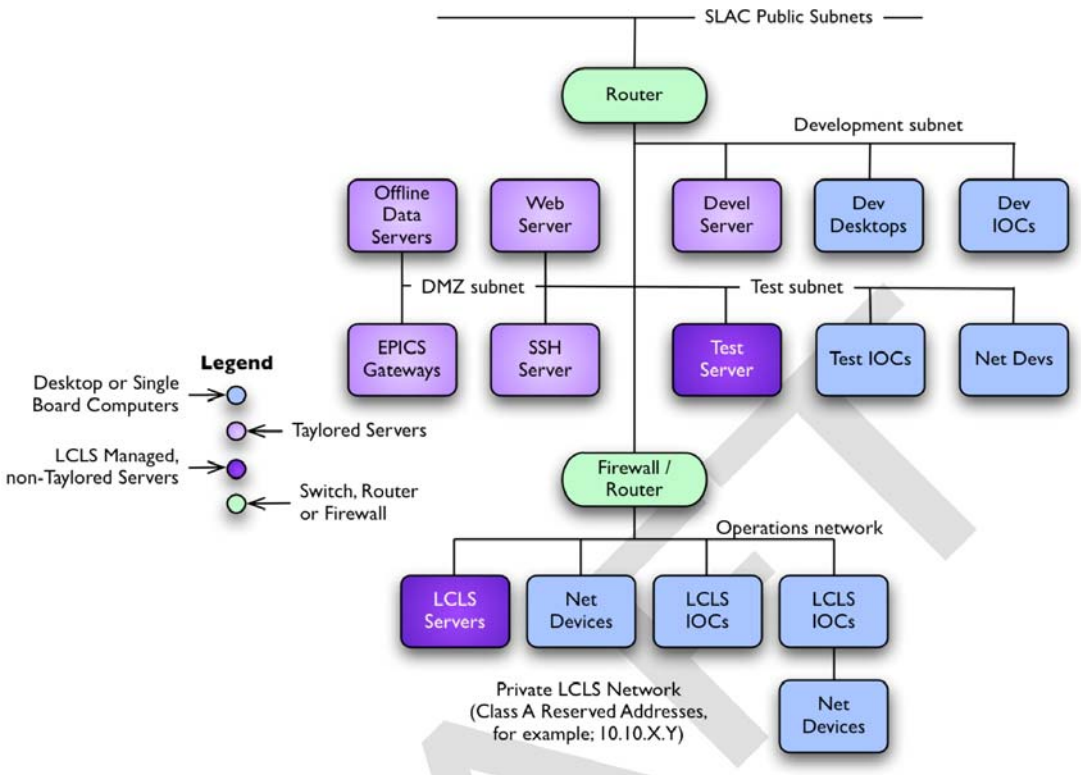


*Figure 4. The LCLS Conceptual Network*

Although the development, test and access control subnets are conceptually on the same level, they may in practice be on completely different subnets, separated by layers of network equipment.

The diagram in Figure 5 shows a few of the components from the existing SLAC/PEP control system, and specifically the linkage implied from requirement 7.1 above.

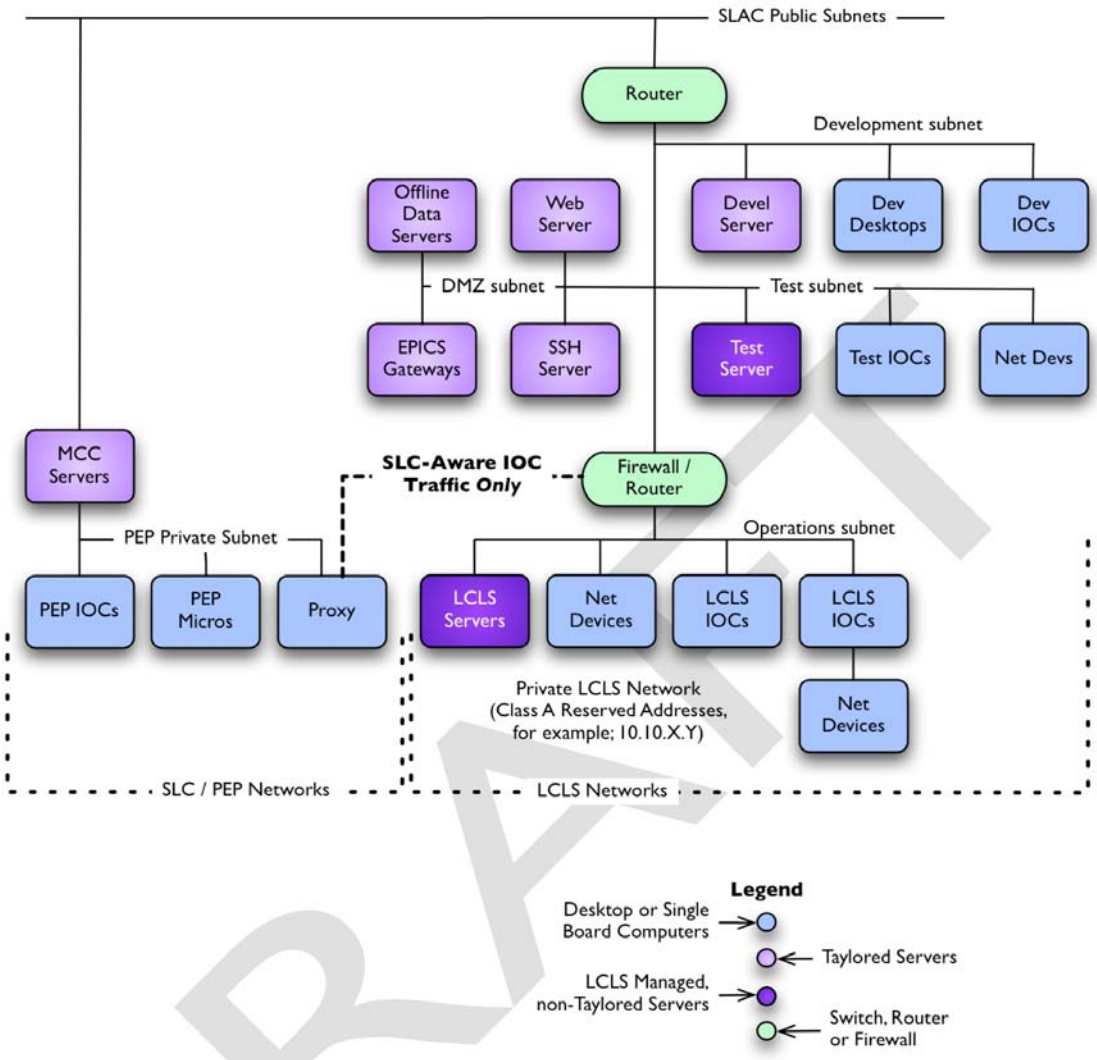


*Figure 5. The SLC/PEP Connection From The LCLS*