Campus Research Network Management

Feb 2008
Version 2

1. PURPOSE AND INTENDED AUDIENCE

1. The Campus Research Network (CRN) is a special purpose network on the campus of the University of Florida that was established in 2005 with a Major Research Instrumentation grant[1] from NSF to complement the campus network for special research purposes. The CRN connections are 10 Gbps to 20 Gbps at this time.
2. The CRN is **not** a faster campus network[2] offering the same services. It offers special network services that for some reason cannot be provided by the campus network, such as latency, bandwidth, protocol, or when the requested service might be disruptive to the campus network, such as testing experimental protocols.
3. Research projects are eligible to connect to and use the CRN only if there is a compelling reason to expect that the research will not be as successful if it is conducted on the campus network, or if there is reason to expect that the campus network could be adversely impacted by the research activity.
4. If in the future the campus network can offer the all such required services, including failsafe protocols to provide test environments, the CRN will be obsolete and will be dismantled. In other words, by design, the CRN shall not compete with the campus network to become a parallel general purpose network.
5. Therefore, only a very small number of people will interact with the CRN directly. As a further result, every new connection to CRN and every new use must be considered on a case by case basis.
6. This document defines and explains the general principles and guidelines for managing the CRN. It specifies how the CRN fits into the UF IT infrastructure and complies with all UF campus IT policies.

2. REQUIREMENTS

1. Modern research involves experimental instruments and computational applications that may require moving large amounts of data to specialized high performance computing and storage servers for processing. The technology at this time may impose stringent requirements on latency, bandwidth or protocols that make it impractical or impossible to move the data across a general purpose network.

[1] Principal investigators: Sanjay Ranka, Paul Avery, Alan George, Sam Trickey, Peter Sheng.
[2] In this document "campus network" includes all networks operated and managed by all service organizations on the UF campus, including CNS, HealthNet, CLASnet, and other organizations, providing network services to all buildings including wireless services inside and outside buildings.

2. Although this situation may change as technology evolves, it currently leads to the need to connect some special servers by fast, special purpose networks that are much faster than the networks that connect desktops and laptops to file, e-mail and web servers and to these special servers. The use of special protocols may be required as well to achieve the required performance and functionality.
3. Thus, it makes sense to build a fast research network separate from the general purpose campus network. The creation of a separate, special purpose, dedicated, not-open network allows deployment and use of special protocols.
4. In the future, it will be necessary to consider moving large amounts of restricted data over this network. At this time, all data accessible on the CRN is unrestricted data.[3] Extra protocols and precautions will need to be determined and implemented for restricted data to be moved across the CRN. Since the CRN is designed for special purposes only, each use much be considered on a case by case basis and the solution will depend on the precise nature of the data. It is inconsistent with the nature of the CRN that it ever could be allowed to transport generic restricted data.
5. Connections to the CRN shall be performed by authorized personnel only. No port on the CRN shall be made available for direct access to the UF public.
6. Every CRN connection will be managed and monitored for security in coordination by the system administrators of the server room, the HPC Center, CNS, and the network provider of the building in which the server room is located, this being CNS or HealthNet or CLASnet, etc.
7. The ISM of the relevant units will review requests for connections to CRN and changes of scope in the activity or the nature of the data at each connected machine room. In particular, HSC Security shall review all requests for connections of server rooms located in buildings for which HealthNet is the network service provider to the CRN.

3. PRINCIPLES AND ARCHITECTURE

1. The CRN shall be managed by the HPC Center under the direction and supervision by the ITAC-HPC committee which shall be a faculty driven committee. Details on governance and operation of the HPC Center can be found at http://www.hpc.ufl.edu.
2. Only individual server rooms, usually machine rooms with specialized servers for research, shall be provided with a connection to the CRN to connect specific computer systems. Offices or class rooms or non-computer laboratory rooms are not eligible to be connected to the CRN.
3. It is likely that the campus network provides network ports to these machine rooms. However, no computer system shall be connected to both networks and provide a bridge between the CRN and the campus network. Wireless access points shall not be connected to the CRN. For example, when administrators connect laptops to the CRN inside a machine room for the purpose of trouble shooting and other administrative tasks, they shall be careful to disable the wireless network adapter on the laptop.
4. The CRN connects to the UF campus network and the Florida Lambda Rail in SSRB. Traffic between the machines on the CRN and any laptop, desktop, or server on the

[3] This includes the data of the Interdisciplinary Center for Biotechnology Research (ICBR).

campus network must go to SSRB first to enter CRN. This will ensure that all security and protection mechanisms in place will continue to protect the laptops and desktops and servers on the campus network.

5. In general, complex computing machinery on the CRN shall not present all its network interfaces to the outside, i.e. the campus network or the Florida Lambda Rail, or even to the entire CRN. For example, the HPC center cluster nodes are not visible on the CRN, just a small number of server nodes allow a limited number of ports and protocols to be visible. These provide services to the campus or need services from the campus or the Internet. Often the primary protocols visible on the CRN for which the existence and use of the CRN is essential are special protocols on special ports such as the Lustre parallel files system.

4. IMPLEMENTATION

1. The switches on the CRN are monitored by CNS.
2. The security of the CRN shall be implemented by the HPC Center and CNS in coordination with the HSC Security and HealthNet or the network service organization of the building that contains the machine room connected to the CRN.
3. Access controls shall be applied where appropriate to maintain the highest level of securrity compatible with the need to move data and offer services.
4. At each location a small amount of public IP space (usually a /27 or /28) and a larger block of private IP space (usually a /22 or a /21) within the campus block 10.13.x.x/16 is allocated. Larger allocations are approved on a case by case basis. Typically these netblocks are on two different vlans. These vlans are routed by the edge device (6506, 6509, Force10 S50, 4948).
5. The CRN has connectivity to the campus network via a 10Gbps cross connect in the CNS machine room. It also has direct connectivity to the Ultralight network via a 10Gbps wave over FLR. Only specific CRN prefixes are advertised to Ultralight and only those prefixes may be reached via Ultralight. Otherwise, all external connectivity comes from UF's external network connections including the Internet, Internet2, National LambdaRail, and Florida LambdaRail Layer 3 networks.
6. All traffic from the external network (with the exception of Ultralight) is subject to the same base level of security that protects the rest of campus including blocking netbios, snmp, tftp, etc. Additional security is implemented by the various CRN participants on the edge network nodes themselves. Additionally, all private IP from the CRN leaving campus is NATed at the campus boundary and subject to stateful security rules which block unsolicited return traffic.
7. Additional security measures to protect restricted data that may need to traverse parts of the CRN are being investigated.

5. CRN MACHINE ROOM LIST

This list will be maintained by the HPC Center to accurately reflect the security aspects of CRN as a whole. Because rooms are connected to CRN for a special purpose, there are special considerations and authorizations for each room.

1. **SSRB machine room:** Central hub of CRN connection to campus network and Florida Lambda Rail.
2. **NPB 2250 Physics machine room**: This room houses Phase IIb HPC cluster with InfiniBand fabric and storage server. Nodes and servers have UF-private IP numbers, the login node and the web server both have public UF IP.
3. **NPB 1114 QTP machine room**: Houses Tier2 cluster with UF public IP to share storage on OSG. Also houses Ethernet-only part of Phase IIb cluster, which is connected by a 10Gbps fiber link to the part of the cluster in NPB 2250. Also house QTP clusters which are connected to campus network and not to CRN.
4. **LAR 121 HPC machine room**: Expansion for HPC Center systems to be completed in Mar 2008.
5. **LAR 320 HSC machine room**: Small test cluster connected to CRN. Dedicated fiber to NPB 2250 carries IB extension traffic.
6. **BEN 312 ACIS machine room**: No systems connected in Feb 2008.
7. **CSE 310 CISE machine room:** No systems connected in Feb 2008.
8. **WEIL 514 Coastal Engineering machine room**: Connection to be completed in Feb 2008.
9. **GCRC 173 ICBR machine room**: Connection to be completed in Feb 2008. This room houses the storage server that will hold the data received from the 454 analyzer and provided high-speed access over CRN to the HPC clusters in NPB 2250 and in LAR 121. Only unrestricted data will be allowed. ICBR will get an IP assignment of campus-private IP for the UF-public addresses of the file servers. The cluster nodes are on private IP that remains internal to GCRC 173. As a result, the servers can be reached from CRN and from the campus network and the desktops of the ICBR staff, but they cannot be reached from outside UF. ACLs will be put in place at the SSRB router to prevent access to NAT from the servers.
10. **College of Medicine Data Processing Center machine room:** The current location (Farm Bureau Building) is off campus. Therefore this room cannot be connected to the CRN at this time. Once the center starts using a room on campus, connection will be considered. Connecting that room will require specifying security requirements and limitations on selected data. The task force that wrote this management document will investigate the specific needs for connecting this room to the CRN. This will involved determining which data needs to be processed by the HPC cluster and then define security model to accomplish this without compromising the SAS70 certification of the machine room[4] and the operation.

[4] The HSC has a security standard for machine rooms: HSC Security Standard PS0002.02 https://security.health.ufl.edu/plicies/policies_b/PS0002.02%20-%20Physical%20Security%20of%20Server%20Rooms%20Standard.pdf.