



FLR

Florida LambdaRail

FLORIDA'S 100 GIGABIT RESEARCH & EDUCATION NETWORK

FLORIDA LAMBDA RAIL REGIONAL SCIENCE DMZ

Overview. The FLR Regional Science DMZ follows the ESnet Science DMZ model as the standard for recommended best practices (<http://fasterdata.es.net/science-dmz/>). A Science DMZ is a portion of the network, built at or near the campus or laboratory's local network perimeter that is designed such that the equipment, configuration, and security policies are optimized for high-performance scientific applications rather than for general-purpose business systems or "enterprise" computing. Important Note: The FLR Regional Science DMZ/Research & Education Network (RENnet) peers with a number of other layer 3 platforms including Internet2, ESnet, and CENIC's Pacific Research Platform.

FLR Science DMZ Architecture and Characteristics – Main Points.

- Creates a new Research Virtual Routing and Forwarding (VRF) on the FLR transport network.
- Designed to support Intensive Science Applications and High Performance Computing.
- Offers L3 peering and L2 circuits.
- Provides a method for FLR members to separate research and science applications from the Campus enterprise and commodity traffic.
- Allows for a smaller routing domain and security perimeter.
- Will:
 - Peer directly with FLR member Science DMZs to provide optimal low latency connectivity between sites engaged in research.
 - Utilize the Internet2 AL2S network to create point-to-point circuits across Internet2 to peer with remote Science DMZs.
 - Contain a subset of routes to other qualified Science DMZ networks or high-performance Data Transfer Nodes.
 - Connect and extend to other Science DMZs or Regional Science DMZ's.
- Will not:
 - Contain the Internet routing table or the Internet2 routing table.

Guidelines to connect a Campus Science DMZ to the FLR Regional Science DMZ include:

- A Campus has created a Campus Science DMZ that is physically or virtually separated from the enterprise network and should only be used for research, science applications, or HPC-related traffic.
- The size of the Campus Science DMZ network will vary based on the needs and applications of that campus. It could be as large as a fully distributed backbone with many endpoints or as small as a single Data Transfer Node.
- No general purpose workstations or devices should exist on the Campus Science DMZ.
- Security architecture of the Campus Science DMZ network should not include general purpose non-optimized firewalls in the data path. Note: The state engine in firewalls will negatively affect the performance and optimization of intensive science applications and large data transfers. Firewalls which are optimized for large science flows may be acceptable.
- A Campus Science DMZ network:
 - should be a limited and specific subset of the Campus's IP space. IPv4 and IPv6 are supported.
 - will have a separate physical or virtual connection to the FLR Regional Science DMZ.
 - should be able to BGP peer with the FLR Regional Science DMZ.
 - may peer with the Campus Enterprise network or have other additional peering connections (FLR R&E net, Internet, private peers, etc.), but should not transit other traffic to the FLR Regional Science DMZ.
 - should implement at least one PerfSonar monitoring system within their Science DMZ.

What's Next?

- Additional Campus Science DMZs connect to the Regional Science DMZ.
- Campus Researchers use Campus Science DMZ.
- Researchers connect to each other through the Campus, Regional, Internet2 AL2S and planned National Research Platform infrastructure.
- FLR Engineering/NOC:
 - The FLR NOC will work with FLR Partner Institutions and Affiliates to design and/or validate a Campus Science DMZ for connectivity to the FLR Regional Science DMZ.
 - Work with Internet2 Engineers to establish a research VRF across the Internet2 network.
 - Connect the FLR Regional Science DMZ to the Internet2 research VRF.

Update. The following table provides an update to the progress being made to connect campus science DMZs to the Regional Science DMZ.

Campus	100G	Science DMZ	FLR MPLS (OF/SDN)	FLR Regional Science DmZ 10G/100G Connection
Florida Atlantic University		X	X	
Florida Gulf Coast University			X	
Florida Institute of Technology			X	
Florida International University		X	X	
Florida State University	X	X	X	100G
Nova Southeastern University	In Progress		X	
University of Central Florida		X	X	
University of Florida	X	X	X	100G
University of Miami	X	X	X	
University of North Florida			X	
University of South Florida		X	X	10G
University of West Florida			X	

Some potential questions (Q) with responses (R)

Q: Can FLR Partner Institutions and Affiliates without a Campus Science DMZ or Campus Research Network connect to the FLR Science DMZ?

R: Yes. Previous guidelines provide that a Campus Science DMZ could be as large as a fully distributed backbone with many endpoints or as small as a single Data Transfer Node. As such a campus researcher who may be conducting astrophysics research on an HPC node could work with campus IT leadership and networking engineers to build a research VRF that adheres to the FLR Regional Science DMZ connection guidelines.

Q: Who can I contact to connect to the FLR Regional Science DMZ?

R: Please contact FLR Chief Network Architect, Chris Griffin, email Chris.griffin@flrnet.org or Sr. Network Engineer, Ryan Vaughn, email Ryan.Vaughn@flrnet.org