

MUSC Information Services Infrastructure

- **Overview**
- **Data Center**
- **Network Configuration**
- **Desktop Management**
- **Information Security Measures**



OCIO
Information Services

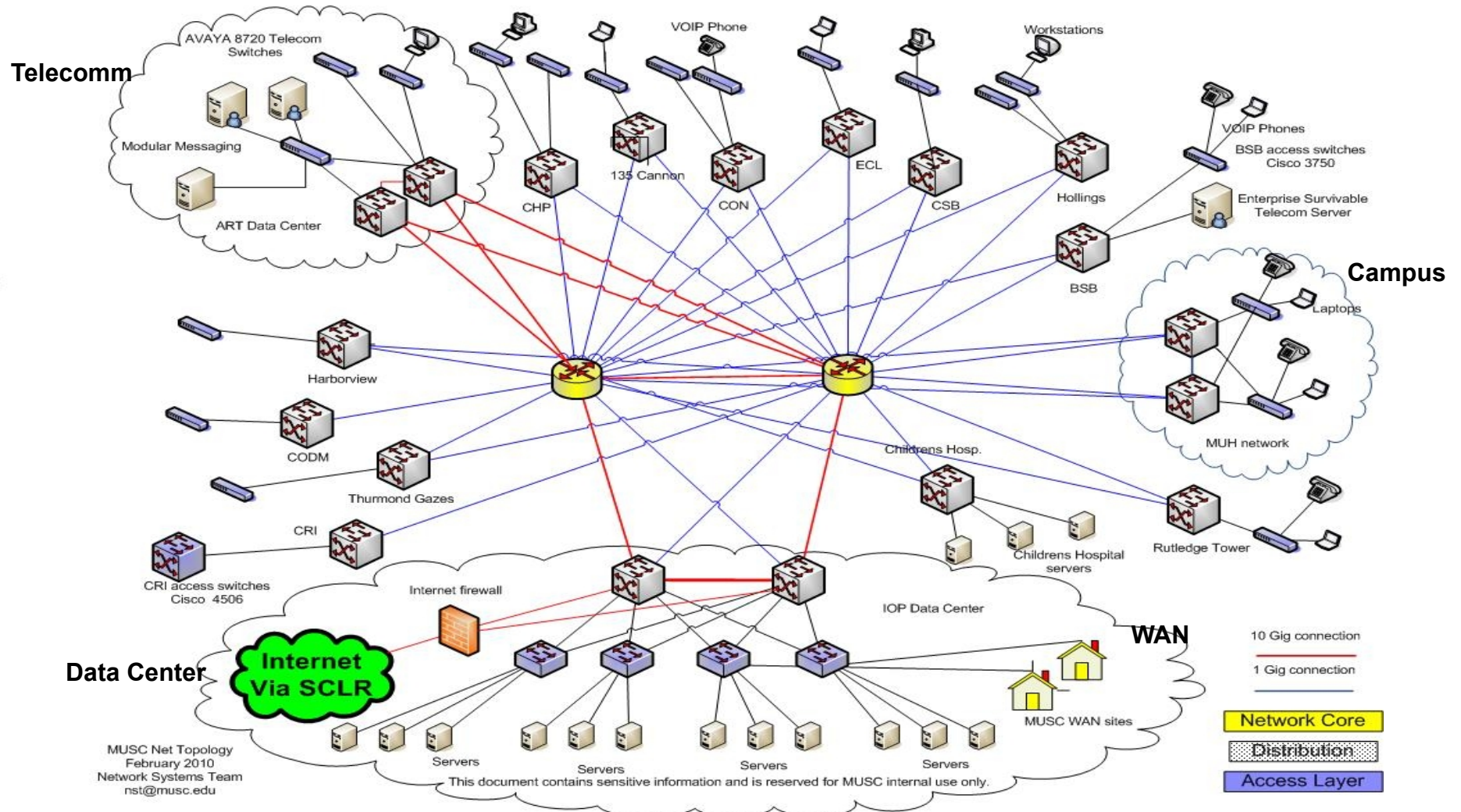
MUSC Information Services Overview

108 Buildings

26 Acres

37 WAN Sites

99.98% System Availability



MUSC Campus Data Center

6,750 Square Feet of Raised Floor

- **911 Physical Production Servers**
- **175 Virtual Production Servers**
- **375 Terabytes of Centrally-Managed Disk Storage**
- **1.7 Petabytes (1,700 TB) of Data Stored on Tape**
- **20 Terabytes dedicated research storage**

MUSC Network Configuration

Wired Network

- 40,000 ports
- 25,000 active devices
- 3 Layer Network
 - Cisco 3750 switches at Access Layer
 - Cisco 4500 and 6500 switches in Distribution layer
 - Cisco 6500 E Series in Core Layer
- 10 Gb Core and Data Center Connections
- 1 Gb to desktop
- 200 mbps internet connection
- 800 mbps internet 2 connection

Wireless Network

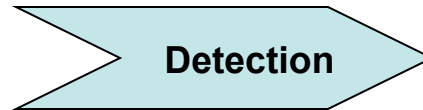
- 3,000 daily wireless clients
- 930 Cisco Access Points 802.11 A, B, G
- 72 Aruba Access Points 802.11 N
- 1 Interwireless Distributed Antenna System (DAS) in new hospital (ART)

MUSC Desktop Management

14,740 Workstations

- **9,740 Centrally Managed Desktop PC's**
 - **Application updates distributed through HP Client Automation**
 - **System update distributed through Window Server Update Services (WSUS)**
 - **System Center Configuration Manager (SCCM) distributes new OS**
- **3,500 Non-Managed PC's**
- **1,500 Mac's**

Information Security Prevention



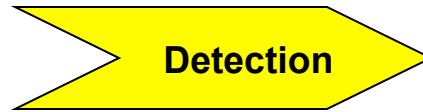
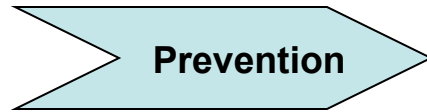
Present (Prevention)

- Border Router
- Internet Border Firewall
- Business Partner Firewall
- Intrusion Prevention System
- Firewall Service Module
- Guest Network
- SPAM filter
- Laptop Encryption
- Tape Encryption
- Anti Virus/Malware
- Identity Management
- Erase Data Storage Media Devices
- Server Admin Access Logs
- Data Center Access Control
- Email Encryption

Future

- Network Registration
- Single Sign-On
- Penetration Assessment
- Multi-Factor Authentication
- Patch Management
- Vulnerability Testing & Mgmt
- Intrusion Prevention Upgrade
- Awareness and Training Program

Information Security Detection & Response



Present (Detection)

- Alerts
- Network Taps
- Snort Detection
- Argus Network Monitoring
- MS Operations Manager
- Airwave Diagnoses
- Video Surveillance

Present (Incident Response)

- Notification
- Network Taps
- Video Recording
- Splunk to Search Logs
- Isolate the Threat
- Corrective Action

Future

- Centralized Logs

Future

- Forensic Tools
- Preserve Data

South Carolina Light Rail

- 16, 10 Gb Lambdas (160 Gb)
- 7x24x365 NOC support
- Full network redundancy
- Layer 3 Network
- Connectivity to NLR via SoX

SC Light Rail

SCLR Services

- Virtual Private LAN Service
- Layer 3 Virtual Private Network Service
- SCLR Common Peering

Other Resources

- Redundant Connections to Internet2
- Redundant Connection to NLR
- TransitRail
- SURA
- TeraGrid
- Redundant Tier 1 ISP
- 24x7x365 NOC services

MUSC Information Services Infrastructure

Questions?