LIS4482 Design Project - Tallahassee Cares

James Kaiser, Samuel Schweitzer, Josiah Granger, Matthew Jackson

Who is Tallahassee Cares?

Tallahassee Cares is our (fictional) non-profit organization that primarily focuses on aggregating the resources and efforts of local mission partners to combat, rectify, hopefully eliminate homelessness in the Tallahassee area. They focus on connecting local businesses with each other for the purpose of collaborative effort, as collective effort will always be more effective than individual efforts. Due to the nature of the work done by Tallahassee Cares, their team consists primarily of volunteers that work one or two half days a week

This time frame and engagement is consistent with existing nonprofits, such as Georgia's Thomas County C.A.R.E.S.

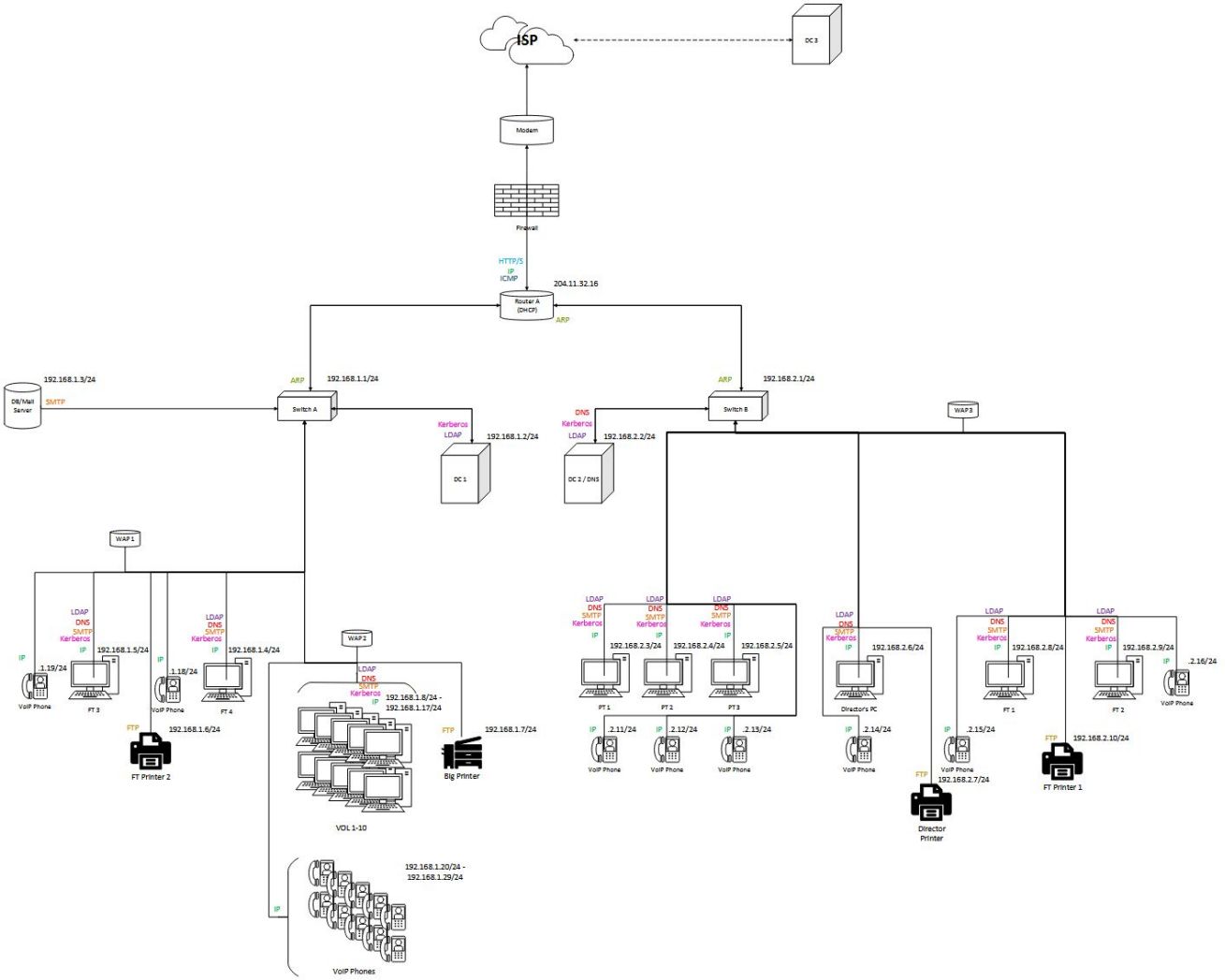
Network Details

Network Summary

Our network will consist primarily of the existing devices left behind by the small business previous inhabiting our office space alongside new server equipment. Give the hardware left behind, our group has assumed our project takes place somewhere around the late 2009 time period, just before the sunsetting of windows 2000 but just after the release of Windows 7 to account for both operating systems to be present in the same environment. We use a Active Directory environment with two on-site domain controllers with one off-site disaster recovery domain controller. This network will utilize four total network printers, four servers, three wireless access points, and eighteen total workstations. A single server will act as both the email and file sharing server, and the second domain controller will also act as the network's DNS server.

Network Breakdown

- Begins at the ISP’s modem, which then connects to a business-owned firewall
- Moves from firewall to network router, then to two network switches.
- Switch A
  - Domain Controller 1 (Primary Domain Controller)
  - Email/file server
  - 12 desktops and VoIP phones
  - 2 printers, 1 of which is a scanner
  - 2 wireless access points
- Switch B
  - Domain Controller 2/DNS server
  - 6 desktops and VoIP phones
  - 2 printers
  - 1 wireless access point


ISP
DC 3
Modem
Firewall
HTTP/S
IP
ICMP
204.11.32.16
Router A
(DHCP)
ARP
192.168.1.3/24
DB/Mail
Server
SMTP
ARP
192.168.1.1/24
Switch A
Kerberos
LDAP
192.168.1.2/24
DC 1
DNS
Kerberos
LDAP
192.168.2.2/24
DC 2 / DNS
ARP
192.168.2.1/24
Switch B
WAP 3
WAP 1
LDAP
DNS
SMTP
Kerberos
IP
192.168.1.5/24
.1.19/24
VoIP Phone
FT 3
.1.18/24
VoIP Phone
FT 4
192.168.1.4/24
FTP
192.168.1.6/24
FT Printer 2
WAP 2
192.168.1.8/24 -
192.168.1.17/24
VOL 1-10
FTP
192.168.1.7/24
Big Printer
192.168.1.20/24 -
192.168.1.29/24
VoIP Phones
192.168.2.3/24
192.168.2.4/24
192.168.2.5/24
PT 1
PT 2
PT 3
.2.11/24
.2.12/24
.2.13/24
VoIP Phone
VoIP Phone
VoIP Phone
192.168.2.6/24
Director's PC
.2.14/24
VoIP Phone
FTP
192.168.2.7/24
Director
Printer
.2.15/24
VoIP Phone
192.168.2.8/24
FT 1
192.168.2.9/24
FT 2
.2.16/24
VoIP Phone
FTP
192.168.2.10/24
FT Printer 1

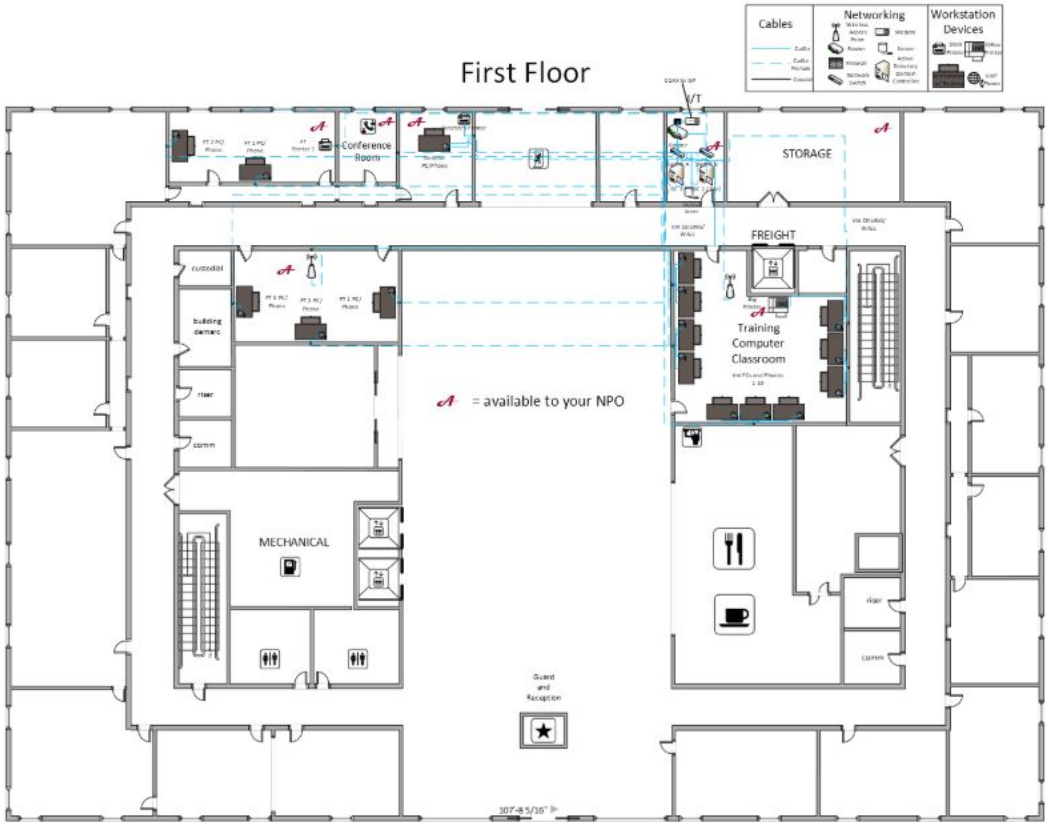
Network Protocols Used

- IP for addressing
- DHCP for dynamic client addressing
- DNS for internal and external name resolution
- HTTPS for web browsing
- SMTP for secure email services
- SMB for file sharing
- Kerberos for network authentication
- LDAP for directory query and management
- WPA2 for wireless encryption

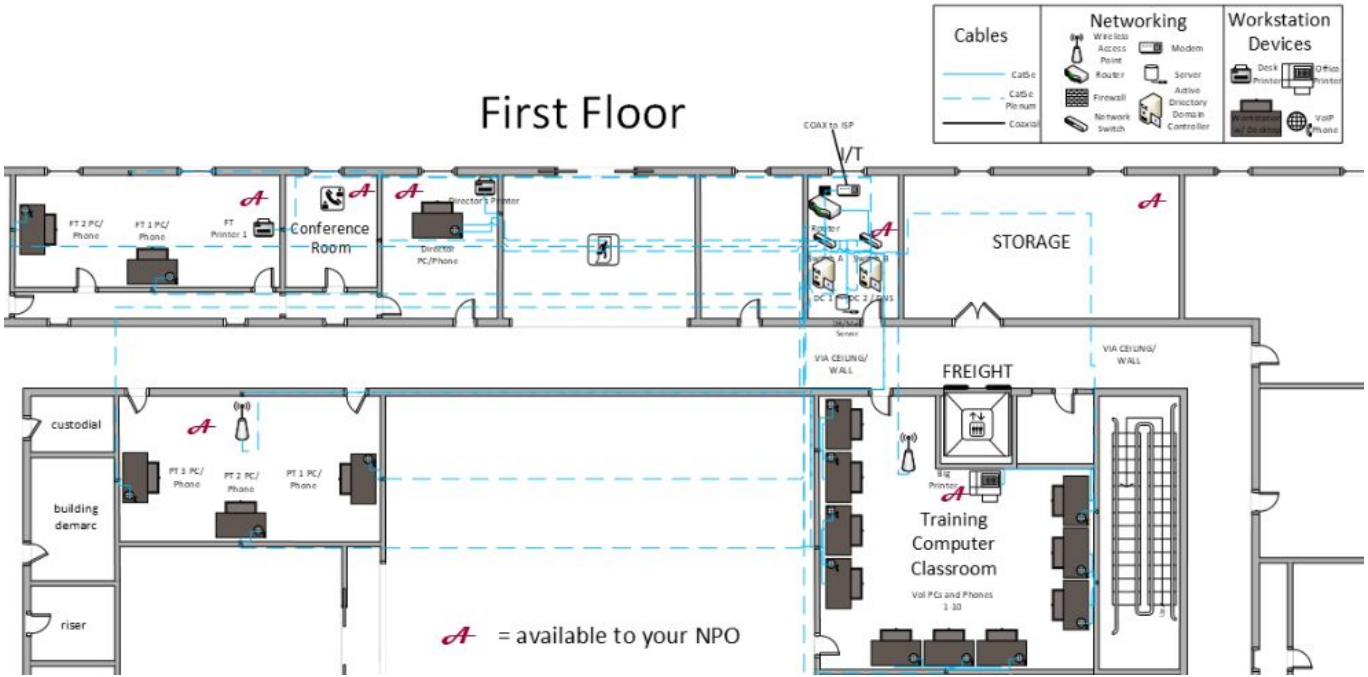
Physical Device Placement

- All network devices that do not need regular physical access (modem, router, switches, servers) will be located in the first floor IT room, which will remain locked at all times.
- Each workstation will consist of one desktop and one VoIP phone connected to a wall data jack via cat5 cable.
- 10 workstations will be installed in the computer lab room, one in the first floor office, one in the fifth floor office, three in the part time office, and one in the director’s office.
- One wireless access point will be installed in the computer lab room, one in the part time office, and one in the fifth floor office.
- One desktop printer will be installed in the first floor office, one in the fifth floor office, and one in the director’s office
- A large office printer/scanner will be installed in the computer lab room to facilitate bulk printing and scanning

First Floor Physical Network Diagram



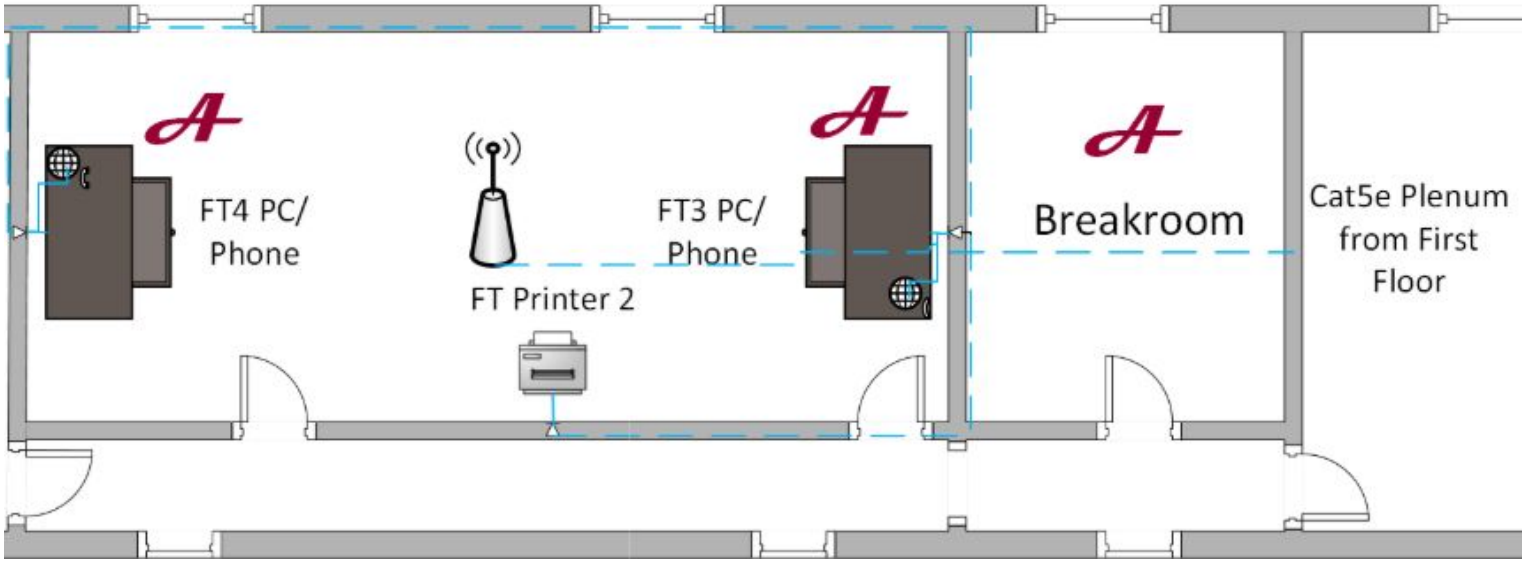
First Floor Physical Network Diagram



Fifth Floor Physical Network Diagram



Fifth Floor Physical Network Diagram



Network Security

Network Administration

- Due to the size of the enterprise, one full-time IT professional would be sufficient to maintain and administer the network. Given the number of volunteers, a high volume of helpdesk tickets can be expected, but actual network administration emergencies should stay at a minimum
- A part-time IT assistant may be deemed necessary depending on the volume of tickets.
- Intrusion detection and prevention will be performed by Snort's free Community Ruleset installed to the domain controllers.
    - While this is less all-seeing than more professional IPSs, given the nature of Tallahassee Cares as a small nonprofit, this should be more than sufficient
- Windows Defender will be used for virus protection

Network Security Policy

- All major changes to the network will be approved by both the IT professional and director to ensure dual control is maintained
- Access to file server directories and printers will be given in a role-based system via Active Directory. This will ensure employees and volunteers are given access to vital materials in the file sharing drive without being given access to potentially sensitive information such as HR data or network administration materials
- Domain password requirements will favor complexity over frequent changes to avoid rapid password fatigue and decreased security
    - I.e. 10-15 characters with at least one special character and one numeric character, but only changed every six months
- Executable and installer downloads can only be performed by IT staff to ensure harmful software is not improperly introduced to the network environment

Physical Security Policies

- In order to protect sensitive information, all offices will be locked outside of working hours with a key only available to employed staff.
- Upon end of day, the last employee to leave will close and lock all office doors to ensure security is maintained.
- Upon violation of the above policies, additional training will be given to whichever employee committed the violation
- Bitlocker will be used encrypt business hard drives to prevent information leaks in the form of hard drive theft.
    - Bitlocker encryption keys will be saves to a server directory accessible by all IT employees and the director in the case of a recovered stolen hard drive or hardware failure

Handling Security Violations

- In the event of a network breach, the vulnerability will be swiftly found and offending softwares will be removed or updated to avoid continued impacts.
- In the event of a fault due to social engineering, the offending employee will be assigned training on social engineering prevention and information security. These trainings must be completed prior to returning to normal operation.
- IT staff will perform random phishing penetration tests in the form of fake phishing attempts. Employees who fail these will be treated as though they had succumbed to a real phishing attempt.

Disaster Recovery

- In the event of a disaster that renders the entire building inoperable, a third domain controller will be placed in an off-site location to ensure the domain is not lost.
- A nightly backup of the business's file server will be sent to this offsite domain controller to assist in data recovery if the file server is rendered inoperable.
- To combat smaller instances of hardware failure, all network equipment belonging to the company will have a backup ready and available in the IT room. This will consist of a backup switch and router. All network infrastructure will be secured with universal power supplies in the case of power outages. Furthermore, extra Client Access Licenses will be procured to assist in easy desktop replacement.
- Tallahassee Cares will also have active liability, cybersecurity, and property insurance in the case of a disaster or incident.

Budgeting

Hardware Needed

- 2 Cisco 2600 Routers
- 3 Cisco 2960S-48 Port
- 1 Cisco ASA 5505 Firewall
- 1000ft Cat5e Plenum
- 500 ft Cat5e Non-Plenum
- 3 Dell Poweredge 2650
- 2 APS Back-UPS 500
- 3 Netgear WG103
- 18 4-plug wall data jacks
- 100 RJ45 cord caps
- 2 Server Racks
- 10 power strips
- 18 VoIP Phones

Software Licenses Needed

- 10 Windows 2000 to Windows XP License Upgrades
- 10 Microsoft Office Licenses
- 3 Windows Server 2008 R2 Standard Licenses
- 20 pack of Windows Server Client Access Licenses

Labor

- Cat5e Plenum cable routing
  - Performed by contracted professionals
- Network setup
  - Performed by full time IT professional
- Workstation setup
  - Performed by volunteers

Subscriptions

- 18 Nextiva VoIP phone subscriptions
- Internet Plan
- Data center/backup rent
- Insurance
  - Cyber security
  - Liability
  - Property

Final Budget and Cost

Final Budget (Including existing materials):

$35,130.00

Total Savings from Current Equipment:

$16,300.00

Total Cost to Tallahassee Cares:

$18,830.00 with a Monthly Upkeep of **$730.00**

THANK YOU!

Questions?