2010 Western Regional Collegiate Cyber Defense Competition Team Packet

Version 2.0

Opening Keynote Speaker: TBD

Closing Keynote Speakers: TBD

For more information contact Dr. Dan Manson at dmanson@csupomona.edu or visit the Western Regional CCDC web site at http://www.wrccdc.org.

TABLE OF CONTENTS

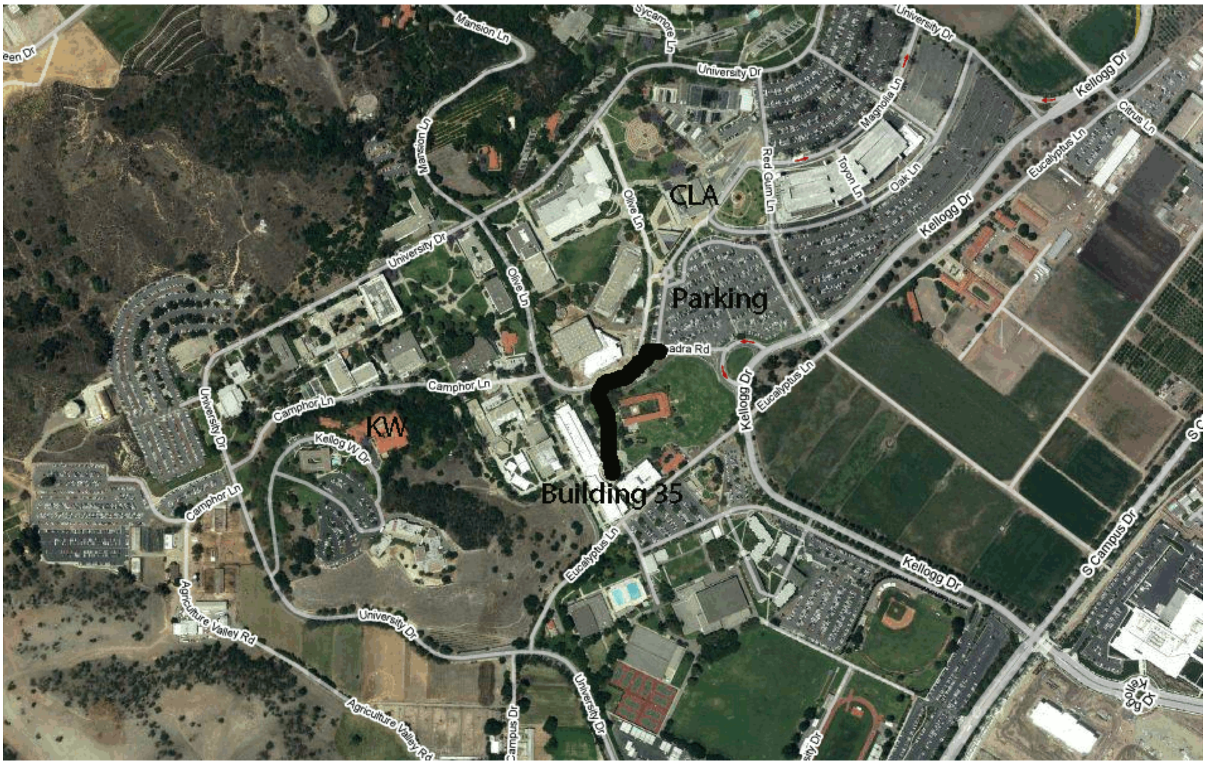
On behalf of the Center for Information Assurance (CIA), Regional Information Systems Security Center (RISSC) and Cal Poly Pomona, I would like to welcome you to the third Western Regional Collegiate Cyber Defense Competition (CCDC). We hope that you will find this regional competition a challenging experience. The winning team from this regional competition will advance to the National Collegiate Cyber Defense Competition (CCDC) at the University of Texas at San Antonio (UTSA).

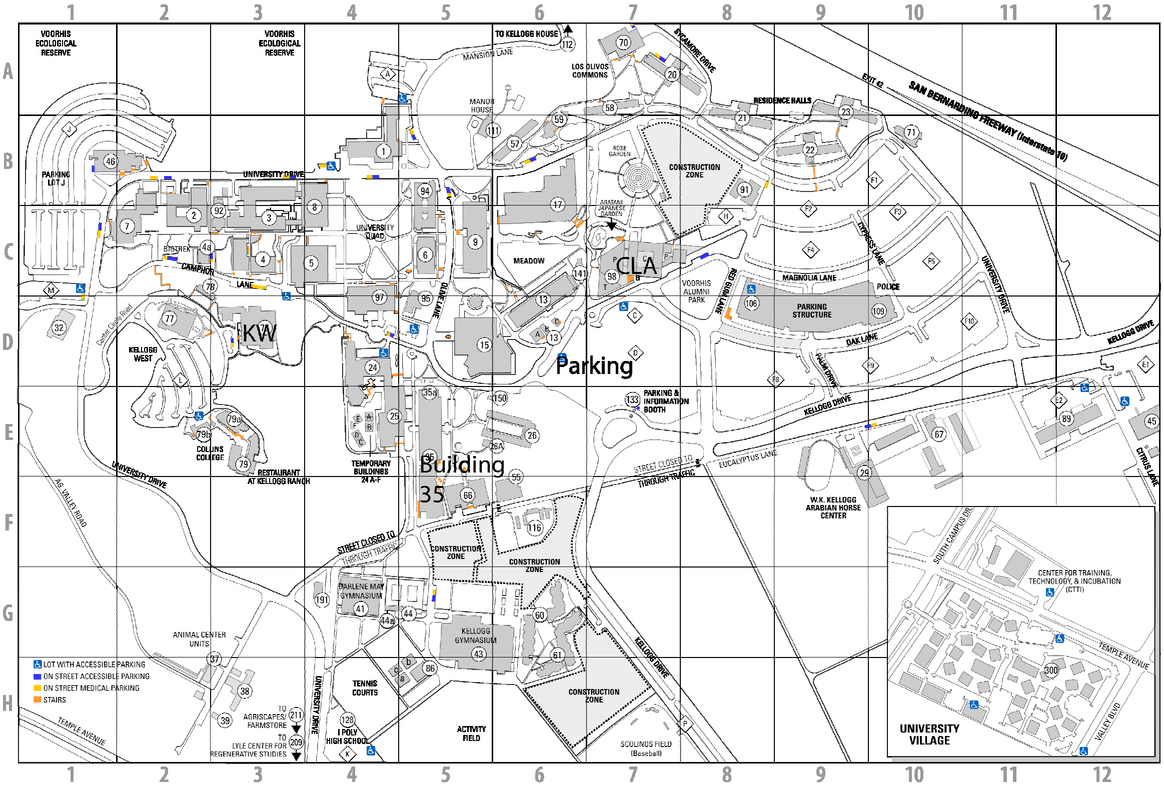
We are excited to be able to host this event. We are also very thankful for our industry and professional association sponsors. Our staff, volunteers, and sponsors have tried to make this an interesting, exciting, and challenging competition. The competition is receiving increased attention from government and industry and we expect this attention to continue to grow. This is the third Western Regional CCDC, last year we grew from four teams to six teams. This year several state competitions and eight regional competitions are expected. The eventual goal is to have eight to ten regional competitions with the winner from each being invited to the national championship. We encourage you to provide comments and feedback to help us improve future events. We wish the best of luck to each of you and your teams!

Daniel Manson, Ph.D
Director
Center for Information Assurance

Campus Map

On Friday you will park in the visitor lot next to the CLA Building. From the front of the CLA Building, follow the signs to the Bronco Student Center (Building 35) for registration. The Competition will be in Building 35. Lodging will be at Kellogg West (KW).




1 2 3 4 5 6 7 8 9 10 11 12
A B C D E F G H
VOORHIS ECOLOGICAL RESERVE
TO KELLOGG HOUSE
MANSION LANE
LOS OLIVOS COMMONS
SYCAMORE DRIVE
RESIDENCE HALLS
EXIT 42
SAN BERNARDINO FREEWAY (Interstate 10)
MANOR HOUSE
PARKING LOT J
UNIVERSITY DRIVE
ROSE GARDEN
CONSTRUCTION ZONE
ARATANI JAPANESE GARDEN
UNIVERSITY QUAD
BISTREK
CAMPUS LANE
MEADOW
CLA
VOORHIS ALUMNI PARK
RED GUM LANE
MAGNOLIA LANE
CYPRESS LANE
POLICE
PARKING STRUCTURE
OAK LANE
KELLOGG DRIVE
KW
KELLOGG WEST
OLIVE LANE
Parking
PALM DRIVE
PARKING & INFORMATION BOOTH
KELLOGG DRIVE
EUCALYPTUS LANE
STREET CLOSED TO THROUGH TRAFFIC
COLLINS COLLEGE
RESTAURANT AT KELLOGG RANCH
TEMPORARY BUILDINGS 24 A-F
Building 35
W.K. KELLOGG ARABIAN HORSE CENTER
CITRUS LANE
AG VALLEY ROAD
STREET CLOSED TO THROUGH TRAFFIC
CONSTRUCTION ZONE
CONSTRUCTION ZONE
DARLENE MAY GYMNASIUM
KELLOGG GYMNASIUM
ANIMAL CENTER UNITS
SOUTH CAMPUS DR.
CENTER FOR TRAINING, TECHNOLOGY, & INCUBATION (CTTI)
TEMPLE AVENUE
LOT WITH ACCESSIBLE PARKING
ON STREET ACCESSIBLE PARKING
ON STREET MEDICAL PARKING
STAIRS
TENNIS COURTS
CONSTRUCTION ZONE
KELLOGG DRIVE
TO AGRISCAPES/ FARMSTORE
TO LYLE CENTER FOR REGENERATIVE STUDIES
I POLY HIGH SCHOOL
ACTIVITY FIELD
SCOLINOS FIELD (Baseball)
UNIVERSITY VILLAGE
VALLEY BLVD
TEMPLE AVENUE
UNIVERSITY DRIVE

Competition Schedule

Friday – March 26

9:00 AM	Registration opens outside Ursa Major Room in Bronco Student Center (Building 35)
12:00 PM	Lunch – Opening Keynote – Competition Instructions in Ursa Major Room in Bronco Student Center
1:00 PM	Competition Day 1 begins in Ursa Major Room in Bronco Student Center
5:00 PM	Dinner at Bronco Student Center – Evening Keynote
7:00 PM	Competition continues
10:00 PM	Competition ends for Friday

Saturday – March 27

9:00 AM	Competition continues – Breakfast available
12:30-1:30 PM	Lunch available
6:00-7:00 PM	Dinner available
9:00 PM	Competition ends for Saturday

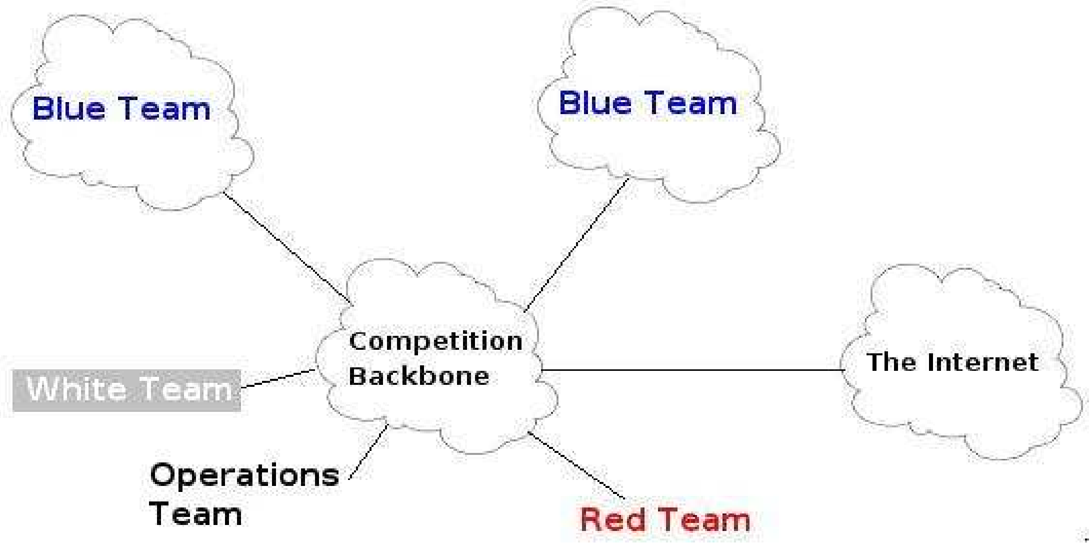
Sunday – March 28

8:30 AM	Competition Continues - Breakfast available
10:00 AM	Competition ends
10:30 AM	Keynote Speakers
11:30 AM	Feedback sessions
12:00 PM	Lunch
12:30 PM	Awards

Competition Overview

The Western Regional Collegiate Cyber Defense Competition is one of a collection of cyber security competitions held around the USA each year, in the early spring. Schools send teams to represent them to the competition, and the winner from each regional competition goes on to a national competition usually held in April.

Each collegiate team is what is called a 'BLUE' team. They are provided with a complete and working enterprise, though the enterprise is not secured. Each enterprise will be identical for all BLUE teams and will consist of a number of computers and network appliances. The computers will run various operating systems and a variety of services.



After the initial time to secure the enterprise is complete, a RED team of experts from academia and industry begin to attack the BLUE teams, looking for vulnerabilities. If a vulnerability is discovered in one BLUE team site, it is checked for in all other BLUE team

sites. Then, it is reported to a WHITE team. The WHITE team are the competition judges and scorers.

In addition to the RED team attacks, the WHITE team is monitoring BLUE team service availability, with the help of a final Operations team. The Operations team's responsibility is to automatically check whether service level requirements of the BLUE teams are being met and to generate normal (non-attack) traffic to all BLUE team sites. The Operations team is also charged with maintenance of the competition network, up to the BLUE team network borders. The BLUE teams are responsible for their own enterprise networks.

The competition runs from 1 to 10 pm on Friday continuing at 9 am through 9 pm on Saturday and 8:30 – 10 am on Sunday. Sunday morning is used for final scoring and speeches. At a luncheon on Sunday, a winner is announced and awards are given to the winning team.

During the competition, the WHITE team 'injects' requirements into the workflow of the BLUE teams. All BLUE teams receive the same 'injects' at the same time, to keep the playing field level. 'Injects' can be of any type, from requiring a report to management, to removing one or more team members (simulating illness, for instance) to changing the requirements of the enterprise.

To win the competition, a BLUE team must be able to balance service level responsibilities with external attacks and internal demands.

The competition is designed to test each student team’s ability to secure a networked computer system while maintaining standard business functionality. The scenario involves team members simulating a group of new employees that have been brought in to manage and protect the IT infrastructure at a small to medium sized IT services/reseller. The teams

are expected to manage the computer network, keep it operational, and control/prevent any unauthorized access. Each team will start the competition with a set of identically configured systems.

Objective

The objective of the competition is to measure each team's ability to maintain secure computer network operations in a simulated business environment. This is not just a technical competition, but also one built upon the foundation of business operations. A technical success that impacts the business operation will result in a lower score as will a business success which results in security weaknesses. A detailed business scenario will be distributed along with technical specifications prior to the exercise to allow teams to develop their team and capabilities.

Team Identification

- **Blue Team - student teams consisting of graduate and undergraduate students from an academic institution who will compete in the WRCCDC.**

- **Red Team - comprise of unbiased informational security professionals from commercial, military, or governmental organizations who have volunteered their time and skills to assist in the assessment of a team's ability to defend their network and services. The red team is responsible for providing a credible, realistic threat to the network and services where they will probe, scan, and attempt to penetrate or disrupt each team's daily operations throughout the competition.**

- **White Team – a group of information technology and information security academics and professionals who will serve as room judges and referees in the various competition rooms. Each competing team will have a White Team member on a rotational basis that will assess the competition team's ability to maintain their**

networks and service availability based upon a business inject and a scoring instrument.

To provide an equitable, fair and even playing field:

- **Each team will begin with an identical set of hardware and software: Each team will be given an existing network with 4-6 servers and 2-3 clients they must secure and maintain.**
- **Each team will be located on a dedicated internal network: To remove the variables associated with VPNs and propagation delay each team's network will be connected to a competition network allowing equal bandwidth and access for scoring and red team operations. This also allows tight control over competition traffic.**
- **Each team will be given the same set of business requirements that must be provided and corporate standards which must be adhered to.**
- **Each team will be challenged with required business injects (tasks) at the same time during the course of the competition. Team must adhere to corporate standards while performing injects and mitigating any resulting security threat.**
- **Only team members, White Team members and others designated by the CCDC coordinator will be allowed inside their competition room.**
- **Each team will be assigned their own room during the competition and only the members of the certified student team will be allowed inside during the competition. This eliminates the potential influence of coaches or mentors during the competition.**
- **A non-biased Red Team will be used: A commercially experienced Red Team will be used during the competition.**

Competition Systems

- **Each student team will be given identical hardware and software installations to configure and support.**

- **Student teams will be provided the system architecture and initial set-up prior to the event to permit planning.**

- **Student teams are not allowed to bring in any additional hardware or software into the competition area which includes team rooms and white team areas.**

- **Student teams may not connect any outside equipment to the competition network or the competition systems.**

- **Student teams should not assume any system is properly functioning or secure; they are assuming recently hired administrators and are assuming responsibility for each of their systems.**

- **Student teams must maintain specific services on the "public" DNS servers and host names assigned to their team – for example if a team's web service is provided to the "world" on www.team1.ccdc.com at an IP of 10.1.1.10, the web service must remain available at that DNS name and IP throughout the competition. Moving services from one public IP to another is not permitted without a change request from corporate which is to be expected from time to time throughout the competition.**

- **Each team must maintain and protect their individual public and private DNS servers. The public network includes competition DNS Root servers strictly off limits to teams. These DNS Root servers have delegated zones to each competing team's public DNS servers where the host records for a team's public servers and services such as mail routing are kept.**

- **Student teams may alter their local addressing scheme in the "ccdc.local" network for NAT/PAT configurations but are warned that many of the services on the local network are bastion hosts being accessed from the public network. Changing IP local addresses may cause public service availability to fail affecting services level to customers and in turn may reduce a team's score. Extreme caution should be taken as scoring will not pause.**

Competition Rules

- **Each team will consist of up to eight (8) members.**
- **Each team member must be a full-time student of the institution the team is representing and must not be currently employed in the IT industry (security operations, network administrator, system administrator, programmer, network operations, help desk, etc.) as a salaried employee or as an hourly employee for more than 20 hours per week.**
- **Team members must qualify as full-time students as defined by the institution they are attending - typically this means the team member must be enrolled in 12 or more semester credit hours for undergraduates and 9 or more semester credit hours for graduate students during the semester the competition is held.**
- **Each team may have no more than two (2) graduate students as team members.**
- **Each team may have one advisor present at the competition – this may be faculty/staff member of the institution or a team sponsor. The advisor may not assist or advise the team during the competition.**
- **All team members will wear badges identifying team affiliation at all times during competition hours.**
- **Each team will designate a Team Captain for the duration of the competition to act as the team liaison between the competition staff and the teams before and during the competition.**

- **If the member of a qualifying team is unable to attend the national competition, that team may substitute another student in their place provided the substitute meets all stated eligibility requirements.**
- **All teams are connected to a central router and scoring system.**
- **Each student team will start the competition with identically configured systems.**
- **A Red Team will attempt to infiltrate or disrupt each team's daily operations throughout the competition.**
- **Team members will not be allowed to communicate written or verbally with the Red team members throughout the competition unless requested by the chief judge.**
- **Student team members will not initiate any contact with members of the Red Team during the hours of live competition. All team members must wear badges or other identification given identifying team affiliation at all times.**
- **Student team members will not initiate any contact with other student teams in the competition area during the hours of live competition.**
- **Student team members will not enter another team's competition workspace.**
- **The competition will run over a three day period. (Friday 1:00 pm to 9 pm, Saturday 9 am to 9 pm and Sunday 8:30 am – 1 pm). Registration will occur on Friday between 9:00 am – 11:45 am**

Scoring

- **All teams are connected to a central router and scoring system.**

- **Scoring will be based on keeping required services up, controlling/preventing unauthorized access, and completing business tasks that will be provided throughout the competition.**

- **The White Team is responsible for monitoring the network, implementing scenario events, and refereeing. A White Team member along with each team captain will verify service functionality prior to competition scoring. Scores will be maintained by the White Team, but will not be shared until the end of the competition. There will be no running totals provided during the competition.**

- **Protests by any team will be presented by the Team Captain to the competition officials as soon as possible. The competition Chief Judge will be the final arbitrator for any protest or questions arising before, during, or after the competition.**

- **Any team action that interrupts the scoring system is exclusively the fault of that team and will result in a lower score. Should any question arise about specific scripts or how they are functioning, the Team Captain should immediately contact the competition officials to address the issue.**

- **Any team that tampers with or interferes with the scoring or operations of another team's systems will be disqualified.**

- **Team captains are encouraged to work with the contest staff to resolve any questions or disputes regarding the rules of the competition or scoring methods before the competition begins.**

- **No cell phones, PDAs, memory sticks, CDROMs, electronic media, or other similar electronic devices are allowed in the room during the competition unless provided by competition officials. All cellular calls must be made and received in the designated area. Any violation of these rules will result in disqualification of the team member and point penalties assigned to the appropriate team.**

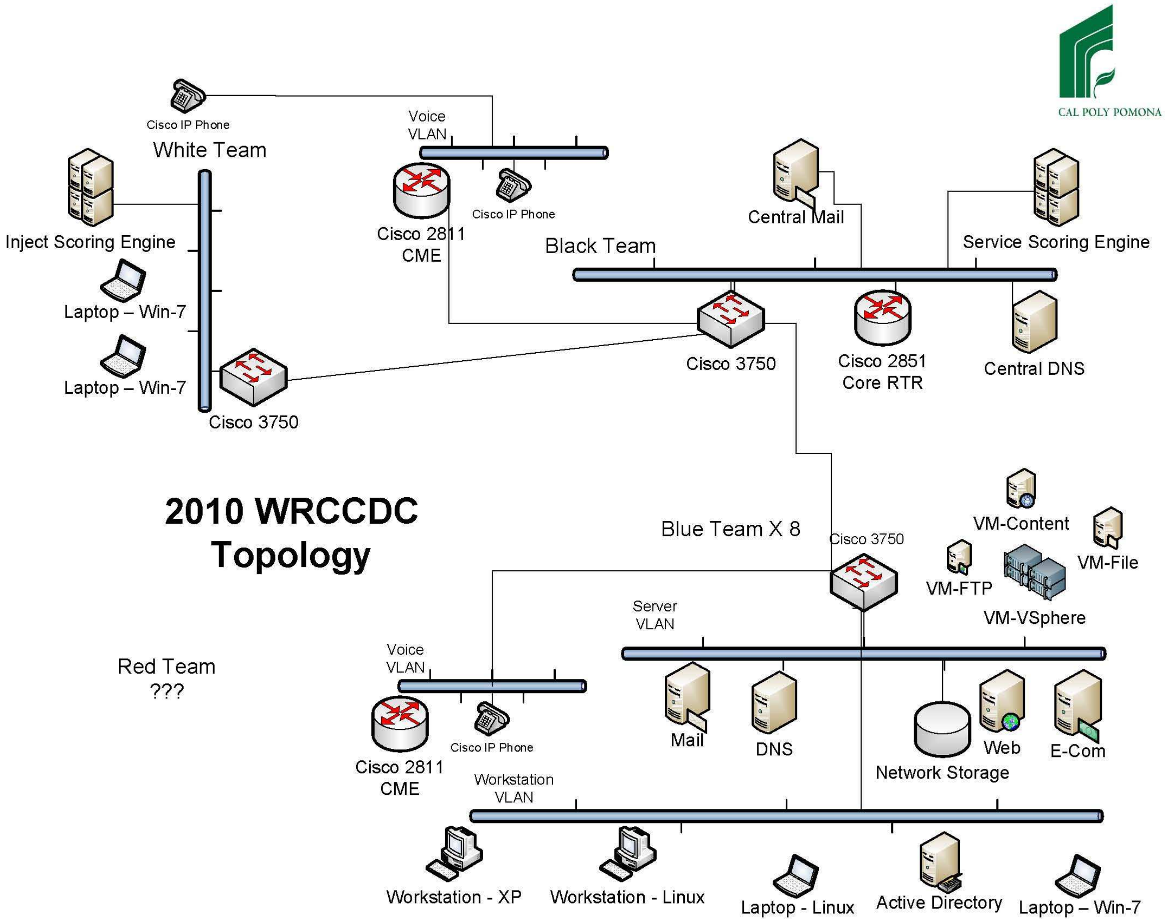
Network Description

The competition network will be completely standalone with no external connectivity. All networks will be connected to a central router that will be maintained by the Gold Team.

The anticipated equipment list per team room will be:

- 6 servers
- 3 clients
- 1 printer
- 2 IP phones
- 1 switch
- 1 router
- Firewall (TBD)
- 1 Network Storage Device

The anticipated topography is shown below. Note that the final topography and system configuration may be different.



Each team network will be connected to the central router through their own individual router. Monitored Internet access will be allowed through a proxy.

Each team will be provided with a CD folder set containing the software, drivers, and data necessary to perform a complete disaster recovery for each site. (Note: The exact composition of this folder will be distributed at competition time.)

Functional Services

Certain services are expected to be operational at all times or as specified throughout the competition. In addition to being up and accepting connections, the services must be functional and serve the intended business purpose. At random intervals, certain services will be tested for function and content where appropriate.

HTTP

A request for a specific web page will be made. Once the request is made, the result will be stored in a file and compared to the expected result. The returned page must match the expected content for points to be awarded.

HTTPS

A request for a page over SSL will be made. Again, the request will be made, the result stored in a file, and the result compared to the expected result. The returned page needs to match the expected file for points to be awarded.

SMTP/POP3

Email will be sent and received through a valid email account via SMTP. This will simulate an employee in the field using their email. Each successful test of email functionality will be awarded points.

SSH

An SSH session will be initiated to simulate a vendor account logging in on a regular basis to check error logs. Each successful login and log check will be awarded points.

SQL

An SQL request will be made to the database server. The result will be stored and compared against an expected result. Each successfully served SQL request will be awarded points.

DNS

DNS lookups will be performed against the DNS server. Each successfully served request will be awarded points.

Business Tasks

Throughout the competition, each team will be presented with identical business task requests. Points will be awarded based upon successful completion of each business task or part of a task group. Tasks will vary in nature and points will be weighted based upon the difficulty and time sensitivity of the assignment. Tasks may contain multiple parts with point values assigned to each specific part of the tasking. Some examples:

- **Opening an FTP service for a 2 hours interval for a specific user:**
- **Configuring SSH access on a system:**
- **Creating/enabling new user accounts:**
- **Installing new infrastructure hardware:**

Each business tasking will have point values assigned and a specific time period in which the assignment must be completed.