CS 640 Introduction to Computer Networks Fall 2007
http://www.cs.wisc.edu/~akella/CS640/F07

Programming Assignment 4: Network Operator Interview

Assigned: December 1, 2007 Due: December 11, 2007, 11:59pm

1 Introduction

So far this semester, you have mainly seen the "theoretical" side of computer networking, with some glimpses into the practice of networking via programming assignments. Getting many of the protocols to work well in practice ad offer predictable and reasonable performance is not very straight-forward. Network operators employ specific tricks, and in some cases, hacks, to improve the performance and to fit the specific needs of their networks. In the final project, instead of having you do yet another programming assignment, we would like to have you talk to DoIT network engineers about specific operational issues, and understand what it takes to get various aspects of a network running seamlessly. In the end, we hope you will write a short paper on the best common practices for a specific topic (see below), and also discuss how things can be improved relative to status quo.

There are four different topics:

1. Traffic engineering and network management
2. Wireless network design, configuration, and management.
3. Network and end-host security, anomaly detection
4. Email management and spam filtering.

Each group should send a rank ordered list of the four topics, starting with the most preferred to the least preferred. We will these ordering to inform our assignment of groups to topics. You will know your assignments by Monday, Nov 26. So you need to get us your preferences soon, otherwise you will be assigned randomly.

2. General Procedure for Each Group

Each group has to set up 3 meetings over time to meet with the specific network operator related to the topic assigned to you. In the first meeting, you will discuss the general questions about the specific set-up and approached used by the network operators in UW-Madison. In the second meeting, you will discuss a specific problem related to the assigned topic. In the final meeting, you will propose some ideas to improve the current approach to the problem and the operator will give you his or her comment on your proposals. At the end, each group hands in a **three-page** paper about the interview. Please use 11pt font, times roman. No hand-written papers will be accepted.

3. Topics for Specific Areas

For each topic we have set up a set of contents you should have to discuss in each meeting – these are guidelines. Feel free to set your own agenda for the meetings. Your questions and discussion with the operator is not limited to this set. In fact, we encourage you to think out of the box and come up with questions not outlined below. However, we must emphasize that the basic set of issues you discuss and the depth you exhibit will used to evaluate your success in this assignment.

Traffic engineering and network management

In the first meeting, you can collect the general information related to traffic engineering and network management by asking the following questions

- How do they monitor and troubleshoot network incidents?
- Which tools do they use for network management?
- How do they perform root-cause analysis of problems (what is root cause analysis, BTW)?
- Visualization of network data, such as large anomalous flows, peer-to-peer traffic, traffic spikes etc.

In the second meeting, you can discuss ***effective traffic engineering***:

- What applications types do they see on their networks?
- How do they rate limit users?
- What mechanism do they use to provide QoS?
- How do they handle traffic surges?
- How do they handle different content types (multicast video vs regular HTTP), routing weights, and so on?
- How do they tune the network setting?

In the final meeting, you can propose some ideas on how to improve the network management and traffic engineering in UW-Madison and get comments from the operator on the suitability of your solutions and potential loopholes.

Wireless network design, configuration, and management

In the first meeting, you can collect the general information related to wireless network design, configuration, and management by asking the following questions

1. How is the wireless network setup in UW-Madison?
2. What is DOIT's role in wireless network setup in UW-Madison?
3. What is the design of the wired network back end? How are packets routed to the access points?

4. What incidents have they had trouble-shoot in the past? How did they trouble-shoot?

In next meetings, you need to discuss ***configuration and management***

1. What mechanisms do they use for managing and monitoring APs?
2. Whether they perform load-balancing at all (and why not), channel assignment, transmit power assignment etc.
3. How do they handle mobility, authentication, diversity of clients (laptops, PDAs, iPhones)?

In the final meeting, you need to propose some ideas on how to improve wireless network design and management and get comments from the operator on the suitability of your solutions and potential loopholes.

Network and end-host security, and anomaly detection

In the first meeting, you can collect information related to network and end-host security, and anomaly detection by asking the following questions

1. What mechanisms do they use to secure the network?
2. What mechanisms do they use within the network and what functionality do they install in end-hosts (or expect end-hosts to implement)?
3. What is the role of proxies, filters and firewalls, authentication?
4. What are recent attacks they faced? How do they deal with attacks? What are the worst-case down times the network has seen due to attacks? What caused the down time?

In the next meeting, you can discuss ***anomaly detection, intrusion detection and prevention*** :

1. What mechanisms do they use for identifying typical anomalies and intrusions? Extent of false positives?
2. How do they update the mechanisms?
3. How do they keep network and end-hosts patched and up-to-date? How to deal with legacy systems?
4. What known loopholes exist in the techniques they use and how do they hope to cope with them?

In the final meeting, you can propose some ideas to improve the network and end-hosts security engineering and get comments from the operator on the suitability of your solution and potential loopholes.