Computer Networks and Data Systems

Introduction

Official Course Description

- TDC 463 Network Interconnection Technologies

  "A detailed discussion of the upper layers of network architectures. Network protocol organization will be discussed using TCP/IP as an example. IP addresses, subnetting, supernetting, and CIDR. Routing algorithms. Transport layer protocols. Application layer protocols. Introduction to IPv6."

Prerequisites

- TDC 405 Voice and Data Network Fundamentals

  "This course provides an introduction to voice and data networking technologies, including public and private voice services, Ethernet and Internet data technologies, network security, business applications and network management. The structure, regulation, and history of the telecom and data network industry will be discussed as well."

- TDC 413 Introduction to Lan and Wan

  "This course covers the principles of local area network (LAN) and wide area network (WAN) technologies including structured cabling, protocols, network devices, and network operating systems. Students will learn the theories and practices of designing, provisioning, and deploying LAN and WAN in an enterprise environment. Assigned lab exercises involving LAN/WAN configuration and troubleshooting will help reinforce various concepts."

Phrases that shouldn’t scare you

- I've exhausted this /24, I need more addresses
- My MAC address is 00:01:54:32:AC:59
- Download the pcap and load it into Wireshark
- Check the RFC and see what it says
- Bridges are switches, L3 switches are routers
- The ARP cache entry timed out
- TCP port 23 is blocked by an ACL

Phrases you may not get, but will

- They rolled out anycast for their DNS service
- It has been mitigated, our ISP supports RTBH
- The e2e argument doesn't say that
- A lot of networks still don't do BCP 38
- I found some additional C&C's with passive DNS
- Your ISP will SWIP some to you
- Do not block TCP port 53
- NAT sucks

Important web pages

https://aharp.iorc.depaul.edu/teaching/tdc463/fall2017

https://D2L.depaul.edu

https://iorc.depaul.edu/cgi-bin/mailman/listinfo/nextgen

- aharp is where I'll put public course materials
- D2L for submissions, quizzes, grades, and news
- nextgen is where the cool kids hang out

Textbook / References

- Officially required:
  - Internetworking with TCP/IP, 6th edition, Comer
- Unofficially:
  - You could use a comparable book
- We'll draw from multiple sources
  - Standards
  - Research papers
  - Conference talks
  - My published / unpublished work

Assignments and Grading

- Homework each week (30% of grade)
  - Elaborate / multiple answer format
- On line quiz each week (30% of grade)
  - 5 multiple choice questions, 1 answer each
  - 2-hour window to complete once started
- Take-home final (40%)
  - Elaborate, comprehensive
- HWs*.3 + Quizzes*.3 + Final*.4 ≈ % grade
- Note: 3 lowest HWs and 3 lowest quizzes dropped

Someone will ask me anyway, but

- NO late homework accepted
- NO late quiz accepted
- NO make up homework given
- NO make up quiz given

jtk

- I prefer: jtk@depaul.edu
- Voice / SMS: +1 312 493-0305
- I am often available M-F 9a-5p by appointment
- More about me:
  https://aharp.iorc.depaul.edu

Numbering Systems

- Decimal, ten digits (symbols): 0, 1, 2, 3 … 9
- Binary, two digits: 0, 1
- Hexadecimal has sixteen: 0, 1, 2 … 9, a, b … f
- Consider an alien with a total of three finger

Bases and Column Placement

- Decimal: base 10
  - Ones (10^0), tens (10^1), hundreds (10^2)
- Binary: base 2
  - Ones (2^0), twos (2^1), fours (2^2)
- Hexadecimal: base 16
  - Ones (16^0), sixteens (16^1), two hundred fifty-sixes (16^2)
- Consider:
  - 10 in base10, base2, and base16

Demo: consider a packet capture

- Wireshark or tcpdump in-class example

What happens when you click

https://aharp.iorc.depaul.edu

URL interpretation

- Parse the URI
- It is an HTTP GET
- For aharp.iorc.depaul.edu
- What do we do with that?

Domain name look up

- Does the browser have the name cached?
- Let us assume the answer is no
- Browser issues a gethostbyname() or equivalent
- We embark on a resolution sub-process...

What is involved in resolving?

- Does hosts(.txt) have aharp.iorc.depaul.edu in it
- Are we a stub, forwarder or full resolver?
- Assume we're a stub, who do we talk to?
  - And how did we get that information?
  - That was probably derived from boot strap
- OK, let's format an **A** query. What about **AAAA**?
  - Maybe do both?

OK, let's send the query!?!?

- Not so fast!
- Put the DNS message in... UDP? Ya should work
- OK, IP datagram, sending to DNS resolver, easy
- From... my IP address? Uhm, am I connected?
- OK, send it on the wire?!?!

Send IP directly on the wire?

- MTU OK? Checksum, set TTL, etc... OK go, go!
- Wait, what L2 destination? Is it a local host?
- Oh, gotta talk to a router... OK lets do that.
  - How do I know who that is? Argh...
  - That was probably part of boot strap
  - Check ARP cache, maybe do ARP?
- OK, got it, get this into Ethernet and off we go...
- Done yet? Not even close

Here ya go router!

- OK, Ethernet daddr is to the router.
  - Wha...? is that right
- Yep, unless your mask is broken
  - What the @?!# is a mask?
- Presume it's non-local, router gets it, now what?
- Router has a decision to make.
- Forwarding/policy decision, re-encap, ARP, etc...
- At least no DNS... I think

Skip ahead, DNS server has query!

We haven't even gotten to HTTPS request yet!

DNS server processing

- Process query
  - Can we?
  - Do I know about this name? Cache or auth?
  - How do I go about finding out?
- If not auth and not cached, how many more steps?
- Quite a few maybe
- ...skip ahead …skip ahead ...skip ahead

Time warp...

- Sending TCP packet
  - UDP for DNS, now TCP? What gives?
- Gotta setup a connection, the 3-way handshake
  - Connection? Isn't IP connectionless?!?!
- Exchange options, sequence numbers
- Timers, congestion control, sliding window, oh my!
- Is it time for HTTP now?

Crypto is fun

- I have to do a TLS handshake now?
- What algorithms do we each support?
- How do strangers even encrypt to each other?
- Check the server certificate's CA chain?
- What if I have no trusted path to the CA?
- How did I get a list of trusted CAs to begin with?

This isn't a cake walk

- Its hard to learn how this all works even after year's of experience, never mind a short networks course
- But we'll try our best...
- I left out a whole bunch of stuff. This slide deck could have been hundreds of pages long, easily! ..and that's without pictures
- Someone else's version of a related idea:

  https://github.com/alex/what-happens-when

Some Fundamental Questions

Speaking of cake… Layering

- Why or why not layer?
- Abstraction and recursion
- Are you sick of the OSI model yet?
- TCP/IP protocol suite (and model?)
- Models versus running code

Addressing

- Assignment
- Static / hard coded issues
- Issues with dynamic and transient usage
- Fixed versus variable length
- Hierarchy and aggregation
- Centralized, distributed, and/or delegated?

Routing / forwarding

- Source-based versus network-based
- Distance-vector versus link-state
- Policy requirements
- Unfriendly / uncooperative / byzantine concerns
- Scaling issues

Naming

- Name versus ID versus Locator
- How do you name things?
- How do you discover names?
- One root to rule them all?
- Privacy, performance, and security issues

Packetization Challenges

- Fragmentation
- Error detection and control
- Sequencing
- Flow control
- Congestion control and avoidance
- Authentication, authorization, and accounting
- Class/Quality of service guarantees

Internetwork Security

- Placement of security services
- Defense-in-depth, belt-and-suspenders
- From obscurity to strong crypto
- From anarchy to totalitarianism
- Ease-of-use
- Isolation versus open
- Privacy and anonymity
- Trust

Standards

- Access and transparency
- Vendors and competing interests
- Intellectual property concerns
- Design by committee syndrome

If time permitting

- An overview of the DePaul University net
- ...and more about a real TCP/IP network