AP/ITEC 2210 3.0 A: System Administration Fall 2023

Instructor: Jamon Camisso
ITEC 2210 Chat: mattermost.itec2210.ca
Email: jamon@yorku.ca
Website: https://eclass.yorku.ca/

Date/Time: Wednesday, 19:00-22:00
Location: Zoom / ACE 003
Office hours: Via Mattermost any time

Class 4 - TCP/IP - Internet

- Midterm:
  - October 18, online during our 7-10pm time slot
  - We'll be using Zoom to collaborate on answers
  - Hopefully a change from the usual midterm tedium

Class 4 - TCP/IP - Internet

- Lab 1/Assignment 1:
  - Clock is ticking. October 11 @ 23:59 due date.

Class 5 - Naming things

- Readings (this week)
  - PSNA sections:
    - 39-39.3
    - 39.5-39.8
    - 40-40.2
- Readings (after midterm for those who want to read ahead)
  - PSNA chapter 44 - “Everyone hates backups”

Class 5 - Naming things

- Definitions:
- “A **Namespace** is a set of names that have a common purpose”
  - Examples: accounts, printers, FQDNs, /etc/services
- “A **Nameservice** associates attributes with each name in a given namespace”
  - Examples: a directory service associates user IDs, home directories, and file ownership with an account

Class 5 - Naming things

- **Namespaces**
  - Two concepts: an **abstract** idea of a namespace
    - All multiuser operating systems have the concept of unique identifiers for users
  - The book sticks to **concrete** (actual) datasets for the most part. For example:
    - All real life sets of usernames will differ (unless they contain identical users)

Class 5 - Naming things

- **Namespaces**
  - Can be designed to be **flat** or **hierarchical**
  - Examples:
    - WINS namespace(for NetBIOS) on Windows is flat, 1 machine, 1 name, no hierarchy
    - UIDs in Linux/Unix systems are flat - just simple numbers

Class 5 - Naming things

- **Namespaces**
  - LDAP/Active Directory data can be flat or hierarchical
    - Everyone can live at the top level of a directory tree
    - Or an organization can be subdivided into branches, and each user has a place in their unit
    - (Note LDAP/AD are nameservices that implement the abstract idea of a ‘directory’ namespace)

Class 5 - Naming things

- **Namespaces**
  - Learn to spot where namespaces are being used
    - York Passport, your username is part of a namespace
  - Linking namespaces together can reduce duplication, work to maintain data, and keep things better organized across an organization
    - And provide a better user experience!

Class 5 - Naming things

- **Namespaces need rules**
  - Have a policy - naming, duration, location, visibility
  - Need a process for adding, changing, deleting names
  - Centralize management for each, or all namespaces
    - Despite passport being a free for all in terms of attribute selection (your name), it is centralized and controls access to most services at York

Class 5 - Naming things

- **Namespace name rules**
  - What kinds of names are allowed?
  - What kinds are not?
  - How are names selected?
  - How to avoid collisions?
  - Is renaming allowed? If so, when?

Class 5 - Naming things

- **Namespace names**
  - Different namespace hierarchies can sometimes determine how names are chosen
  - Hierarchical namespaces can be flattened, e.g. every computer with a unique name in a DNS namespace
  - Example, my (old) Bell IP address reverse DNS name:
  - bas4-oshawa95-70-31-58-31.dsl.bell.ca

Class 5 - Naming things

- **Namespace names**
  - DNS namespace: bas4-oshawa95-70-31-58-31.dsl.bell.ca
  - .ca, cTLD (country top level domain)
  - bell (second level)
  - dsl (third level)
  - bas4-oshawa95-70-31-58-31 (4th level, flat, but hierarchy)

Class 5 - Naming things

- **Choosing names**
  - Thematic - name servers after planets, stars
    - Berry bearing plants (there are more than you think!)
    - Even Pokemon
  - Functional - name corresponds to function:
    - gateway1, resolver-internal, ww1, ww2, db1, db2 etc.
    - Doesn’t so much work for users and their roles

Class 5 - Naming things

- **Choosing names**
  - Descriptive:
    - NetBIOS shared folder ‘\accounts\receivable\2017’
    - Linux partition ‘/dev/disk/by-label/BACKUPS’
    - Recall my IP, bas4-oshawa95 - functional and geographically descriptive
  - Formulaic:
    - Usernames first.last, initial.last, last.initial, etc. etc.
    - Docker containers (adjective, name)
    - Ubuntu releases (adjective, animal - warty warthog)

Class 5 - Naming things

- **Choosing names**
  - Hybrid:
    - Often geographical and functional, e.g. my Bell IP
    - bas4-oshawa95 - bas4 must be something functional on Bell's end
    - Maybe equipment related or phone infrastructure etc, likely maps to a specific DSLAM in Oshawa, and probably identifies the switch port or router

Class 5 - Naming things

- **Choosing names**
  - No method:
    - First come first served
    - York Passport

Class 56 - Naming things

- **Choosing names**
  - Book mentions a caveat about formulaic names:
    - Encoding too much information can make things fragile
    - Moving machines with geographical names can be hard, especially if you don't have a renaming policy
    - It is rare to find a machine with no dependencies on its name, be it DNS, hostname, or applications

Class 5 - Naming things

- **Choosing names**
  - With DNS names, CNAMEs can point to hosts, so that the host server can be changed, but the service name is not
  - Careful with logs and aliases, usually you want the actual hostname, not the aliased service name in the logs
  - Intruders will spot inconsistent names and target the anomalous machines, usually they’re important ones

Class 5 - Naming things

- **Name lifecycles**
  - When do names expire (if at all?)
  - How do you handle contractors?
  - Who gets public IP addresses?
  - Have you planned for longevity?

Class 5 - Naming things

- **Name reuse**
  - Policy should be in place to determine how soon a name can be reused
    - (Presuming of course that you allow reuse)
  - Hostnames are one thing, email reuse is quite another
  - Many people will leave and come back to an organization
    - Usually they are the only ones allowed to reuse an email name

Class 5 - Naming things

- **Name use**
  - A namespace can be used by multiple nameservices
    - A login user ID can be used across multiple systems
  - Thus, for each namespace, you need to determine:
    - **Scope** - where will it be used?
    - **Consistency** - under what circumstances are attributes kept consistent across nameservices?
    - **Authority** - which nameservice is authoritative?

Class 5 - Naming things

- **Name use**
  - **Consistency -** which attributes are kept consistent across nameservices where some are common attributes?
  - Useful measures of consistency are **level** and **strength**
    - High level would be everywhere a name is used, all attributes are common to every service
    - e.g multiple separate Active Directory servers with mostly the same data, like dev, beta, prod SSO sites

Class 5 - Naming things

- **Name use**
  - **Low consistency** - useful where there are multiple security models with different levels of privilege
  - Example: requiring 2FA logins when using a VPN, but not at a workstation. The authentication attributes for an account differ
  - More common: separate passwords for the same user, depending on the service

Class 5 - Naming things

- **Name use**
  - **Strong consistency** - attributes cannot be different across multiple nameservices
  - Example: HR database periodically syncing to systems
  - This is quite common, and if you don't know a service relies on HR systems, it leads to head scratching
  - Very common for everything but passwords to come from HR systems

Class 5 - Naming things

- **Name use**
  - **Weak consistency** - attributes can be different across multiple nameservices
  - Example: multiple methods of changing a password, which aren't synced with each other
  - User can have same ID, but different passwords
  - Local server passwords can override LDAP depending on server configuration

Class 5 - Naming things

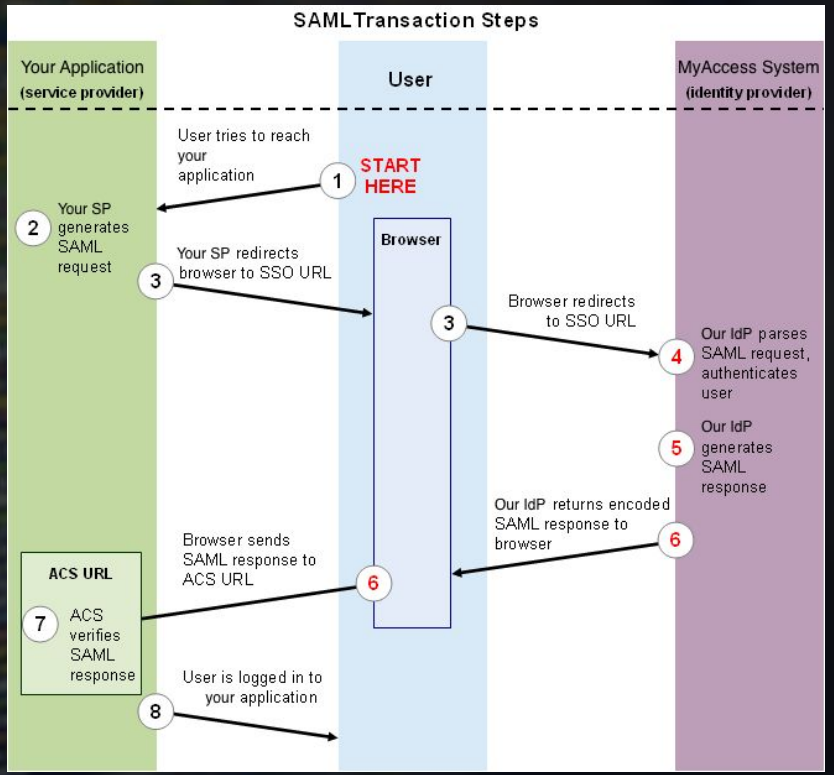
- **Name use**
  - **Federated Identity**
  - Identity attributes are linked across various systems
  - You'll come across things like
    - Identity Provider (IdP)
    - Identity (Access) Management (IAM, IdM)
    - SP (Service provider)
    - RP (Relying Party)

Class 5 - Naming things

- **Name use**
  - **Federated Identity**
  - Single Sign On (SSO) is one subset of federation
    - SAML protocol (Security Assertion Markup Language)
      - Usually you'll see Shibboleth used here
    - OAuth 2.0 - spec for authorization **RFC 6749**
      - Use this to access APIs or services with tokens
    - OpenID, OpenID Connect
      - Use this to authenticate a user
      - Connect integrates with OAuth

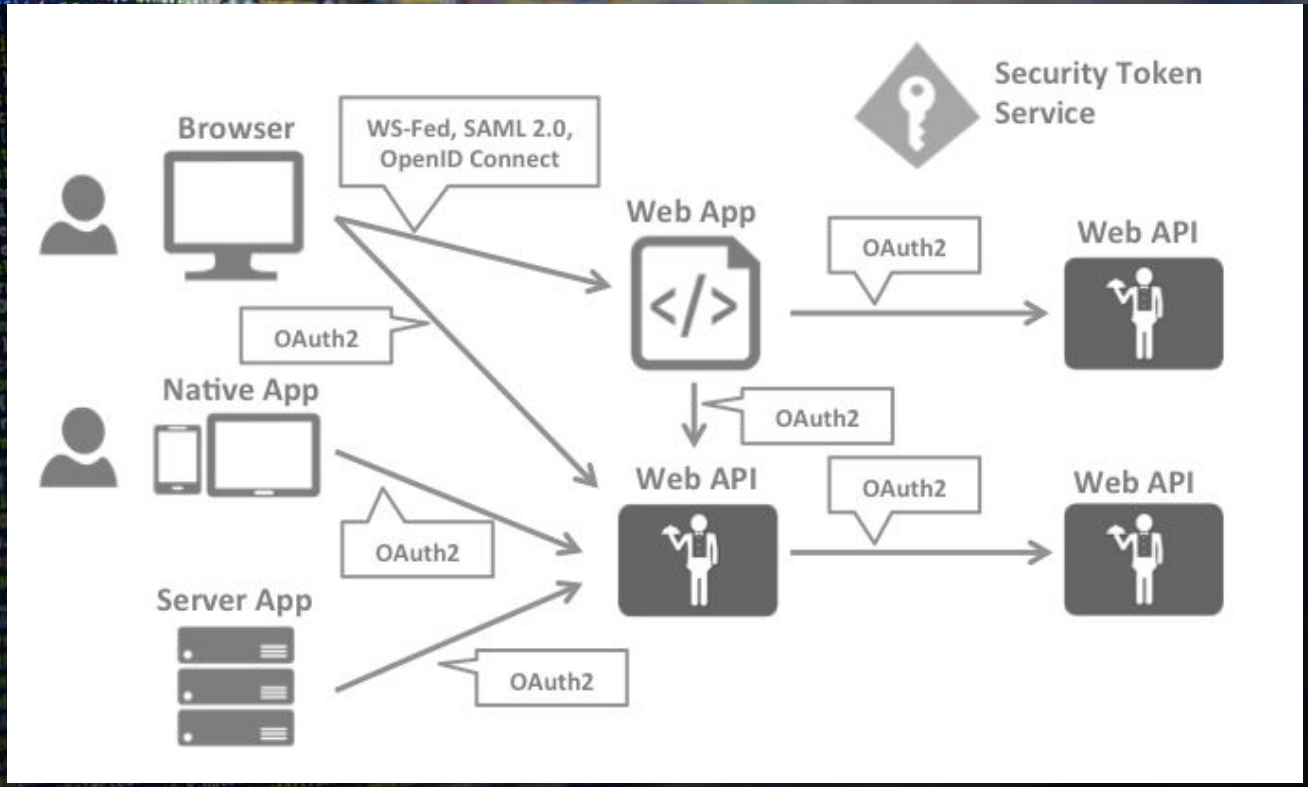
Class 5 - Naming things

- Name use
  - SAML example



https://wiki.library.ucsf.edu/display/IAM/How+It+Works%3A+MyAccess%2C+SAML+and+Shibboleth

Class 5 - Naming things



https://identityserver.github.io/Documentation/docsv2/overview/bigPicture.html

Class 5 - Naming things

- **Nameservices**
- “A nameservice is a an instantiation of a namespace that associates particular attributes with names in the namespace and makes this information available to other systems and end users using some particular protocol or set of protocols.
- “Examples of nameservices include DNS, DHCP, LDAP, Active-Directory, the HR directory” PSNA p.711

Class 5 - Naming things

- **Nameservices**
- Which data will be stored in this nameservice?
  - Passwords? PII? These are attributes associated with a namespace, which are provided or used by the service
- Which namespaces does this nameservice use?
  - User IDS? Emails? Hostnames?

Class 5 - Naming things

- **Nameservices**
- What are the consistency requirements for the data?
  - Can the data be changed on different systems?
  - Are some attributes shared and synced across systems?
  - Can queries to subordinates be passed to the primary**?
  - Can an attribute be updated in one place and propagate across systems? E.g. one primary to another like AD/DC

Class 5 - Naming things

- **Nameservices**
- Which nameservice is authoritative for data with a strong consistency requirement?
  - If you have LDAP & AD, which is the primary?
- How is the data stored in this nameservice accessed?
  - Public DNS, or private occasional SQL queries?
- What is the data capacity limit for this nameservice?
  - Throughput, disk usage, performance bottlenecks?

Class 5 - Naming things

- **Nameservice reliability - DNS**
- "Domain Name Service (DNS) is used by nearly every client and service that exists" PSNA p.714
- **RFCs 1034 and 1035, http://www.zytrax.com/books/dns/**
- 'Client' is a device that queries a DNS service. A client can be a laptop, physical server, phone etc.
- 'DNS server' is a nameservice (Bind, NSD, AD/DNS, PowerDNS) that provides data for/from DNS namespaces

Class 5 - Naming things

- **Nameservice reliability - DNS**
- Clients query DNS resolvers (local, or remote service), which in turn query DNS servers and returns namespace data
- Redundant resolvers are desirable in case one goes down - you still have working DNS resolution
- Resolvers can be setup using Anycast so that if one fails, clients don’t notice at all

Class 5 - Naming things

- **Anycast resolvers**
- **1.1.1.1** is resolver
- Clients query 1.1.1.1
- Resolver queries its closest or best upstream DNS server

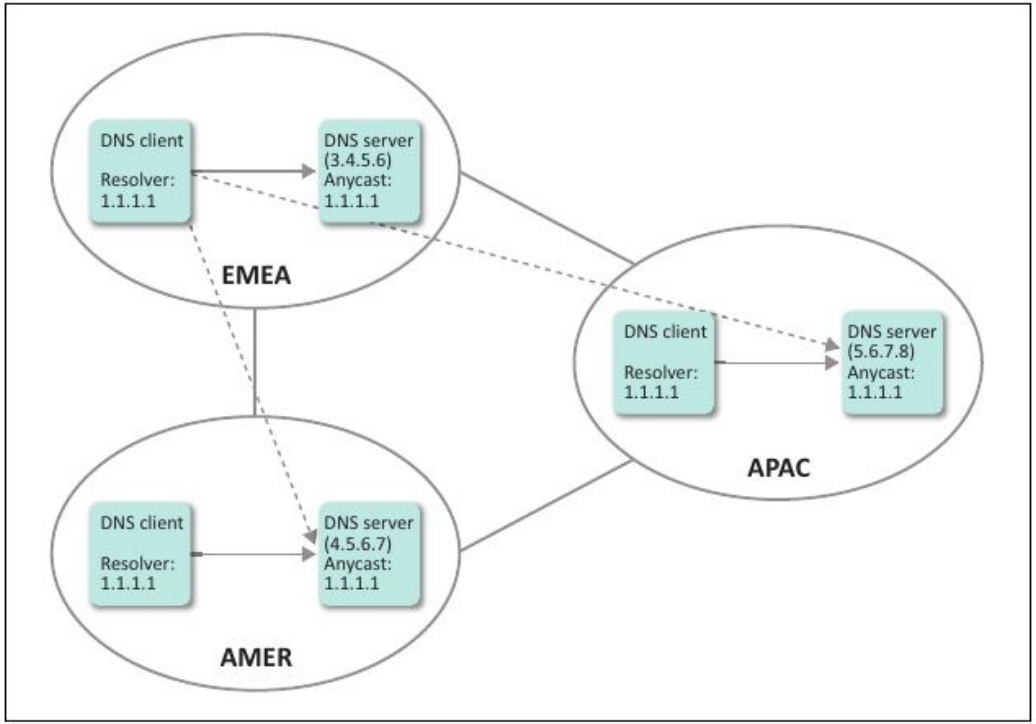


Figure 40.1: Multi-region DNS anycast

Class 5 - Naming things

- **Nameservice reliability - DNS**
- DNS resolvers are configured with the locations of **root** DNS servers, all 13 of them
  - 13 is misleading, because each root host uses Anycast,
  - While there are 13 logical {a,m}.root-servers.net, each can be comprised of hundreds of machines anywhere in the world
- Resolvers, or DNS caching servers need to bootstrap the list of top level resolvers only, any other data can be looked up

Class 5 - Naming things

- **Nameservice reliability - DNS**
- DNS resolvers will algorithmically determine the best root servers from their list to use based on response times, and bias those that are faster
- Leads to distributed load-balancing across the global cluster of root servers, usually nearest neighbour
- If the closest is unavailable, resolver will find the next best because of anycast, and no one notices (except operators!)

Class 5 - Naming things

- **Nameservice reliability - DNS**
- Multiple redundant strategies for authoritative DNS servers
  - Multi-primary, updates sync across primaries
  - Primary/Secondary, updates propagate to 2ndaries
  - Primary/Primary + store & forward, updates propagate to main primary, then to others - any primary can become main primary in the event of an outage

Class 5 - Naming things

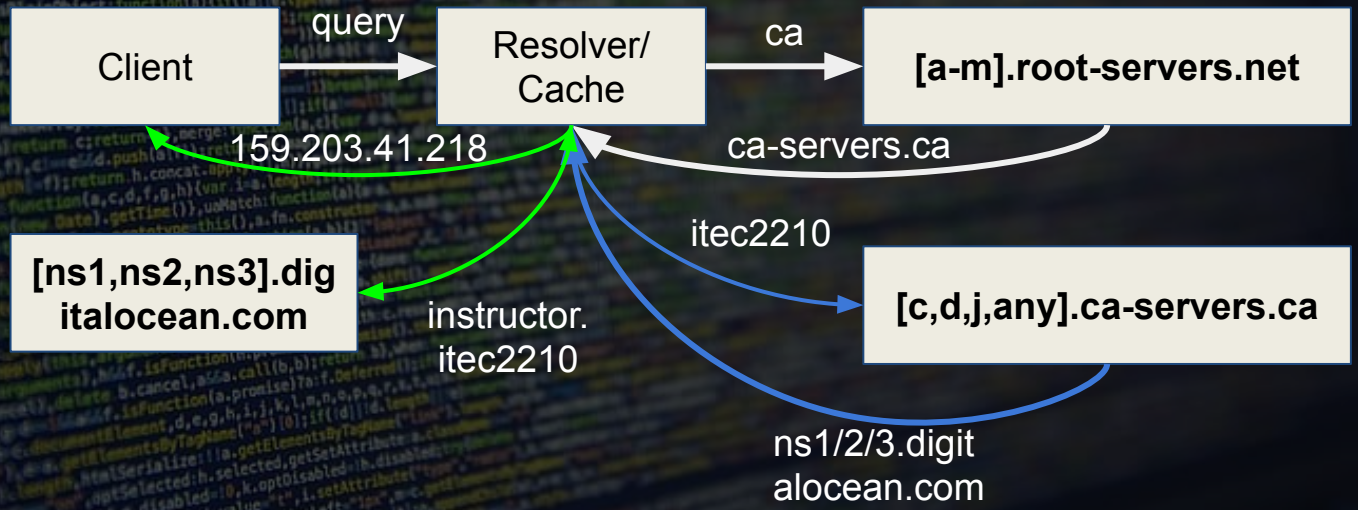
- **Nameservice reliability - DNS**
- Multi-primary
  - What happens if there's a network partition? Split brain
  - Hard to unify updates on each side when connection is restored
  - Benefit is high throughput for updates, e.g. if you're a big registrar, you don't want a single point of failure
- Primary/Secondary, updates propagate to secondaries
  - If primary is offline, no updates can occur, but queries still work

Class 5 - Naming things

- **Nameservice reliability - DNS**
- Name resolution flows like this:
  - Client requests '**instructor.itec2210.ca**' from resolver
  - Resolver breaks domain into pieces from **left to right**
  - If resolver doesn't have a cached record, it queries one of its preconfigured root servers for rightmost zone, **ca**
  - Root responds with location of **ca** nameservers
  - Resolver queries **ca** nameserver for **itec2210.ca** nameservers
  - **ca nameserver** responds with location of nameserver for **itec2210** inside the ca country top level zone (cTLD)
  - **ns1.digitalocean.com** nameserver responds with **A** record, or yet another **NS** to query

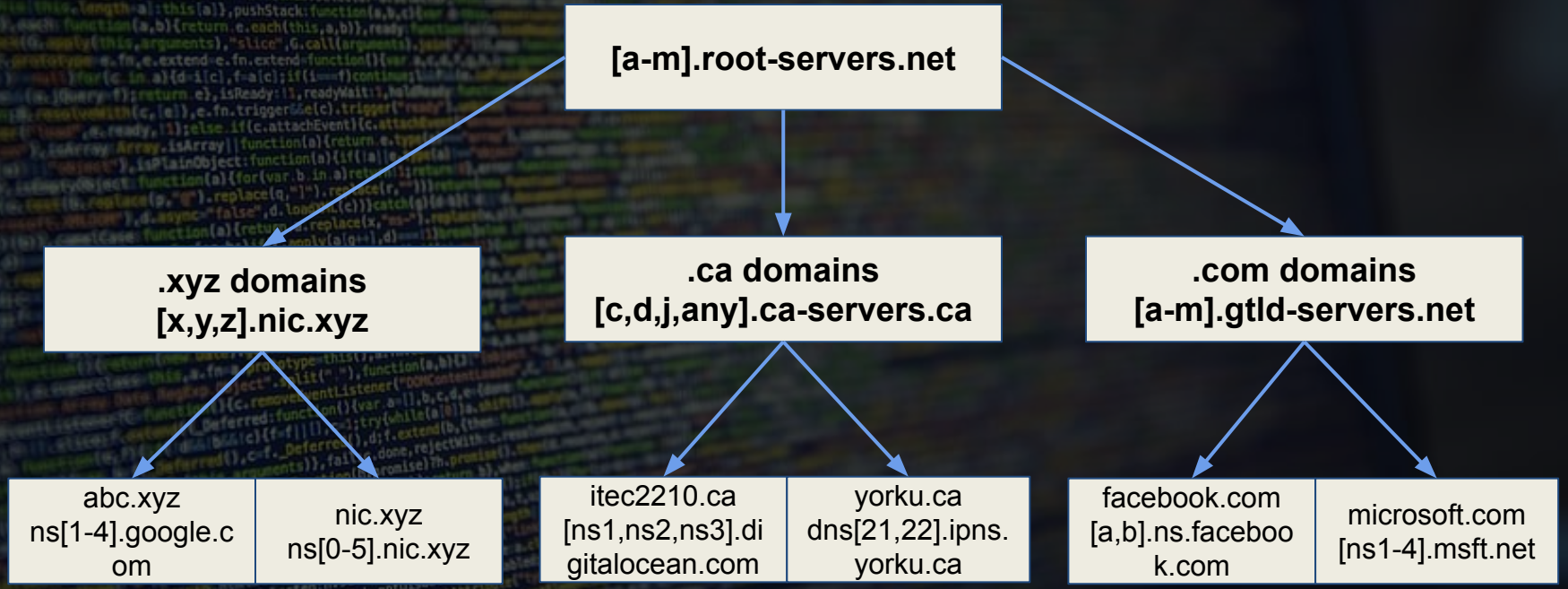
Class 5 - Naming things

- **Nameservice reliability - DNS**
- Query for instructor.itec2210.ca would look like this



Class 5 - Naming things

- DNS namespace and nameserver tree looks like this



Class 5 - Naming things

- **Nameservice experimenting - DNS queries**
- Try it out on your VMs:
  - dig NS yorku.ca # ask for nameservers for yorku.ca
  - dig NS itec2210.ca # ask for nameservers for itec2210.ca
  - dig A itec2210.ca # ask for IP address for itec2210.ca
  - dig A +trace yorku.ca # start at root of DNS and walk tree
  - dig A +trace itec2210.ca # start at root of DNS and walk tree
  - dig NS com; dig NS ca; dig NS net; # etc. etc. etc.
  - whois yorku.ca
  - whois itec2210.ca

Class 5 - Naming things

- DNS root hints and zones
  - https://www.internic.net/domain/named.root
  - https://www.internic.net/domain/root.zone
  - https://data.iana.org/TLD/tlds-alpha-by-domain.txt

Class 5 - Naming things

Class 5 - Naming things

- **Midterm preparation**
  - 90 minutes, *REMOTE*. 7-10pm window - eClass
  - 30 marks of your total grade in the course
  - Notes are OK, 1 single sided page. Be honest and reasonable. Academic integrity applies here.

Class 5 - Naming things

- **Midterm format**
  - 20 of 30 marks multiple choice based
    - 20 multiple choice questions worth 1 mark each
    - Questions will ask for 1 answer only. Choose the best one
  - 10 of 30 marks long answer (bullet and sentences ok)
    - 2 questions worth 5 marks each

Class 5 - Naming things

- **Midterm material**
  - Anything from slides, eClass, or assigned readings up to and including this class
  - Focus attention on areas where we've spent a lot of time - full Class on troubleshooting, cloud and virtualization, TCP/IP, and service launch, namespaces

Class 5 - Naming things

- **Midterm material**
  - We looked in detail at OSI & TCP/IP models, though not so much at other protocols or higher layers in the stack
  - We didn't spend any time on IPv6

Class 5 - Naming things

- **Midterm example multiple choice**
- VLANs are useful for (select best answer):
  - A) Increasing bandwidth between servers
  - **B) Isolating traffic on shared physical networks**
  - C) Making sure VPN traffic is fully encrypted
  - D) Creating Software Defined overlay networks

Class 5 - Naming things

- **Midterm example long answer**
- Describe a multi-star network topology:
  - Multiple datacentres
  - Satellite networks connected to each datacentre
  - Usually geographically separated
  - Each datacentre has connections to at least 2 others
  - Internal networks can use any topology, CLOS, TOR