CSC437 Network Information

Each student in CSC437 is assigned a server. Much like in a large corporate environment, these servers have various network interfaces. These interfaces are connected to the core network that has already been configured by your network team. Here's the information on how to access your server from your admin machine:

Your Server

You will be assigned a server number as well as a team number. This information will be important when determining what IP addresses and VLANs you need to configure.

Network Interfaces

Your server technically has five network interfaces, however one of them is inactive. Only four are usable, the fifth interface is for management. You can see the details below:

ThinkServer System Manager (TSM_Interface)

https://172.16.85.1XX where XX is your server number.

This interface allows you to directly interface with your server. It's a virtual KVM console. You can use this interface to install an OS directly on your hardware, power on your server, or restart it if you're having problems. You'll log in to this interface using your DSU username & password, you may need to accept a self-signed cert in your browser. Use FireFox, it works best with the Java console.

To mount an ISO on your server (if you need to install/reinstall the servers OS), you'll need to use the TSMCLI application and run the script called Mount-ISO.ps1 on your desktop.

Nic0

This is an access interface which will automatically be assigned an IP address. You will only use this interface to access an NFS server which contains ISO files. You can only mount this NFS server as *read only.*

Server information: 172.16.87.2/NFS/

Nic1

This is an interface that has several trunked VLANs as well as a native VLAN. For CSC437, we will not use the native VLAN.

Two trunks exist on this network interface:

- Team_LAN, the network shared between your servers. The VLAN-ID is '*3649+ your team number*'. So if your team number was 45, you'd use VLAN 3694.
- NFS_Share, the network where you will access your shared storage. The VLAN ID is 3695 for everyone. Information on the server/directory to mount will be distributed in class.
- WAN, this is the WAN for our CSC437 class. We will treat it as if it's a true WAN connection, delivered to us by an ISP. In order to gain internet access, we'll have to deploy a router/firewall connected to this network.

Nic3

This interface is directly connected to your partner's server. There are no switches or other infrastructure in between, you should have a line-rate gigabit connection. This is a great interface to use as a dedicated vMotion interface.

Nic4

This interface isn't used and should appear as disconnected… since it's not plugged into anything…

The Network

The network for this class is a very large & complicated one that encompasses both the Beacom Institute of Technology's Academic Server Room, the Information Assurance Lab, and the DSU edge network. All in all, roughly 30 miles of CAT6, a few thousand VLANS, plenty of fiber optics, routers, switches, and some occasional NSX Software Defined Networking all work together to get your lab-based servers out to the internet.

This part of the guide basically takes a tour of what a packet will see when leaving the ASR and heads for the internet.

Beacom Institute of Technology ASR

Most of the servers used for CSC437 live in the ASR. Each server uses uplinks to a virtual chassis of 6X Juniper EX4300's. Each 4300 has two 40GB link in a round robin fashion, giving the ASR and 80GB backplane throughout the room. When accessing ISOs, a server located in the ASR is used that has dual 10GB network interfaces. When needing to route traffic externally (either to the internet or to your hosted admin machines), the ASR has redundant 10GB uplinks to the Information Assurance Lab core.

Beacom College's Information Assurance Lab

The IA Lab is located in the Science Center and consists of several connections before your traffic can get to the internet. This description primarily pretains to student traffic, as other types of traffic may take a different path, depending on the security level associated with it.

IA Core

When any traffic arrives from the ASR it first enters the IA Lab's core which consists of 8 Juniper QFX5100 switches. Each of these switches has either two or four 40GB connections, making the backplane vary from 80 to 160GB in speed. All in all, the IA Lab core has an estimated 2.56Tbps throughput performance (which isn't something we come close to for CSC437!).

PA-500

Almost all student traffic is treated with a low security level at this point and is therefore passed to a pair of Palo Alto PA500 firewalls. These firewalls act as a redundant pair and host the captive portal as well as the first round of traffic analysis, tagging, and categorization. The IA Core connects to the PA-500 Cluster via four aggregated ethernet interfaces (etherchannel, for the Cisco folks), giving a 4GB redundant uplink.

SRX5100

While technically traffic would bounce back to the IA Core, it essentially goes directly to the IA Lab's edge firewalls, two SRX4100 firewalls, for additional traffic classification, policy enforcement, etc. These firewalls act as a redundant pair and currently have two 10GB interfaces (each connected to the IA Core (40GB total). In addition, each firewall has a 10GB

connection to each other in order to keep their state table in sync in the event of a hardware failure. Each firewall is located in a separate location and have diverse uplinks for extra redundancy.

DSU Edge Network

The IA Lab (and therefore ASR) are a DMZ off of the DSU network, but before we get to the internet we have to hit one more step through the DSU security appliances.

PA5220

Once traffic leaves the IA SRX it heads for DSU's edge firewall over one of four 10GB interfaces. DSU's edge firewall consists of two PA5220's acting as a highly available pair. As with all other firewalls, additional traffic classification, logging, and analysis take place here.

MX240

Finally, we're done enforcing security policies! Once we've passed DSU's edge PA5220's, traffic leaving the DSU network is handed to DSU's MX240 routers. Currently this takes place over two 40GB QSFP+ interfaces. Soon this will be upgraded as DSU's edge firewall will be upgraded. The MX240's handle DSU's BGP advertisements to the world as well as make routing decisions, depending on which "internet" your packet is destined for.

State of South Dakota

DSU houses one of the internet exchanges, routing internet for the State of South Dakota.

MX480

The DSU edge routers actually hop over to the Bureau of Information Technology's dual MX480 routers over dual 100GB network connections. Depending on the destination of your traffic, it may make one of the two following connections, either to "The Internet" or to "Internet2". More details below!

The Internet

In DSU's datacenter you'll find routers from midcontinent communications. These routers provide one of two internet links for DSU and for the State of South Dakota REED Network (Research Education and Economic Development Network). The second uplink exists in Pierre. If the traffic is destined for a location that we can't find on Internet2, your packet will head down this slower link which is capped at around ~4GB. You can tell if your traffic went this direction if during a traceroute/tracert you see references to midco.net in the router names.

Internet2- The Better Internet

Internet2 is exactly what it sounds like, a secondary network, basically Internet 2.0. It consists primarily with educational institutions connected over super high speeds for the sake of making large data transfers. However, several commercial entities have connected onto I2, so a lot of time your traffic will head over these links.

SDN Communications: The Infinera

SDN Houses a large Infinera router in the DSU datacenter. It hosts 4X redundant connections out to the REED network, all of which head to Sioux Falls. At the moment, these connections are 10GB but will be moving to 100GB sometime in 2019.

East Core

The East Core, located in Sioux Falls houses connections across the state, including to the EROS Datacenter, DSU, USD, SDSU, Northern, and to the Pierre & West Core. The East Core handles the Eastern South Dakota REED traffic as well as traffic destined for Internet2. Depending

where on I2 your packet may be destined, it'll transit to one of two Internet2 Networks: Great Plains or Northern Lights.

Great Plains Network

GPN tends to be where the majority of our I2 traffic goes, but it can vary from day to day. When leaving the REED State Connector, we transit to the GPN core located in Kansas City. Our link technically goes from Sioux Falls to Nebraska, then hops onto the 100GB connection to GPN's MX960 core (unless you arrive at your destination while transiting Nebraska). You can tell if your traffic takes this route, do a traceroute/tracert to your destination and you see greatplains.net before hitting internet2.edu.

Northern Lights/Northern Tier

If your I2 traffic is destined for the Northern United States, you'll head north from Sioux Falls typically to NSU (although a secondary path exists for redundancy). Once at NSU, you'll head into North Dakota passing through Fargo, then onto Northern Lights/Northern Tier. You can see if your traffic went this way, do a traceroute/tracert to your destination, if you see northernlights.gigapop.net, then you're on the Northern Lights network.