Campus Area Network Design Proposal

Christopher Iwen

DeVry University

Author Note

This paper was prepared for Netw 207

taught by Professor R. Gulledge

**Table of Contents**

Table of Contents pg. 2

Request for Proposal pg. 3 – 4

Horton Hall Diagram pg. 5

Nassua Residence Diagram pg. 5

Laffin Hall Diagram pg. 6

Campus Area Network Diagram pg. 7

Bill of Materials Spreadsheet pg. 8

Security Narrative pg. 9 – 13

Justification pg. 13

Campus Area Network VLSM pg. 14 - 17

**Request for Proposal:**

Customer goals:

* To connect 1050 current users across three buildings on campus and make the network scalable to accommodate 1365 users without over taxing the infrastructure and degrading the quality of education Farmingdale State college can provide for its students.1
* To stay competitive with other colleges offering the same degree programs.
* To offer convenience for the students and faculty alike by having everything they need available at their fingertips anytime they are online.
* To offer strong collaboration tools and incentives to expand the reach and education of students and professors.
* To garner more prestige for the school as their students become the market standard.

Customer constraints:

* Interference with student and faculty's daily life.
* Limited space to fit everything into.
* Building codes and inspections or laws.
* The overall cost and success of the setup is a major concern, but with an overall budget of 2 million dollars we should be able to get top quality equipment and have everything done in a timely manner so that the buildings are ready for use next school session.
* We don’t want to disrupt day to day business activities on the campus. Thankfully the buildings themselves are gutted and not currently occupied so that part can be done at any time of the day. The trenching, which is going to tear up the ground, will need to be done before the end of the project. Most of this is in student walkway areas that can be covered with temporary bridges. There will be a small section of roadway that must be dug up to lay the cables. The path we have laid out will only affect a small parking area between Gleeson Hall and Whitman Hall. We will make this the area that gets trenched last and fixed first to minimize the disturbance to students and faculty.

User and administrative applications:

* Cloud storage for the student and faculty
* Printing services at each of the buildings.
* Email server and accounts for each student and faculty member.
* Wi-Fi in the lobby of each building and in the class rooms for the convenience students, professors, and visitors.
* DHCP services set up in Horton Hall to give out ip addresses to everyone on the intranet.
* NAT overload to facilitate connection of all these users to the internet with a limited number of public ip addresses.
* DNS setup so that network users can get to webpages using a url.
* Desktop virtualization with all the applications a student or professor might need on a remote server like Citrix.

Technical goals:

* Redundancy without loops
* Small failure domains (simplified troubleshooting)
* Equipment needs to be able to handle to combined bandwidth of everything connecting through it.
* Set up a central location for administration
* Allow for future growth starting with 1050 users and expanding to 1365 in the near future.
* Security (security badges, pin numbers, cameras)

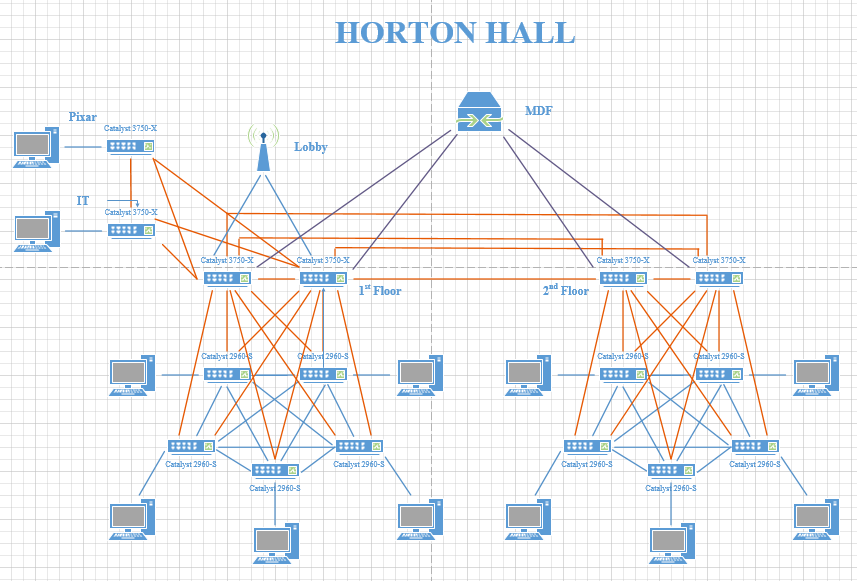
Technical constraints:

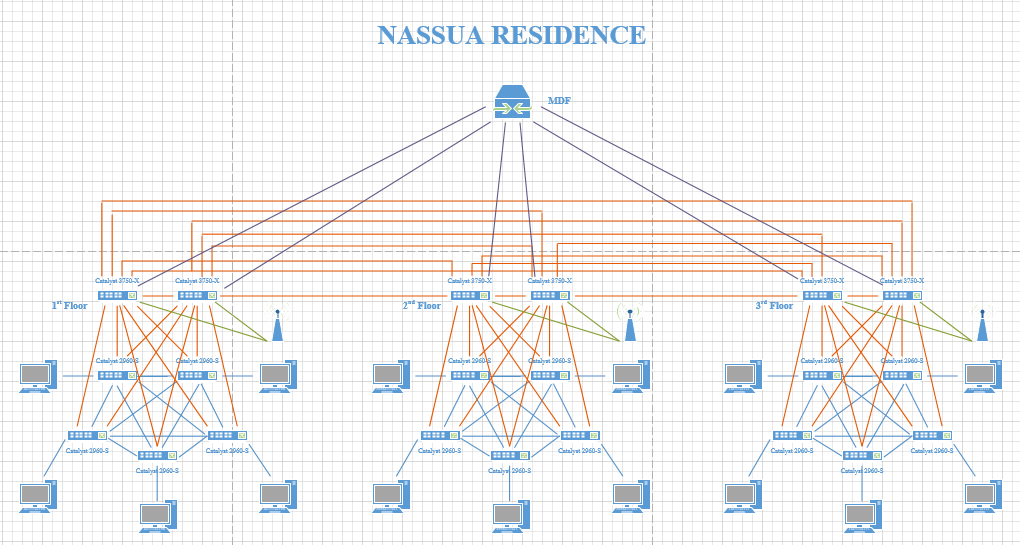
* Space for equipment to have a secure room in each building, and room to run the wires through the ceiling.
* Security: badges, pin numbers, cameras, passwords, sticky mac, bdpu guard, firewalls, ACL’s
* Server room:

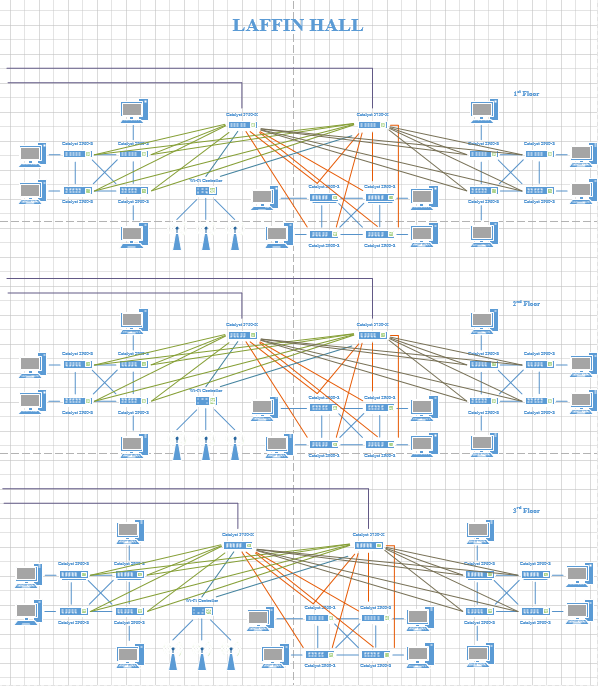
Finger print reader and pin number for outside door. Video cameras on both sides of the server room door, and only one way in and out of the server room. Everything in the sever room is locked behind cages that requires a physical key to open.

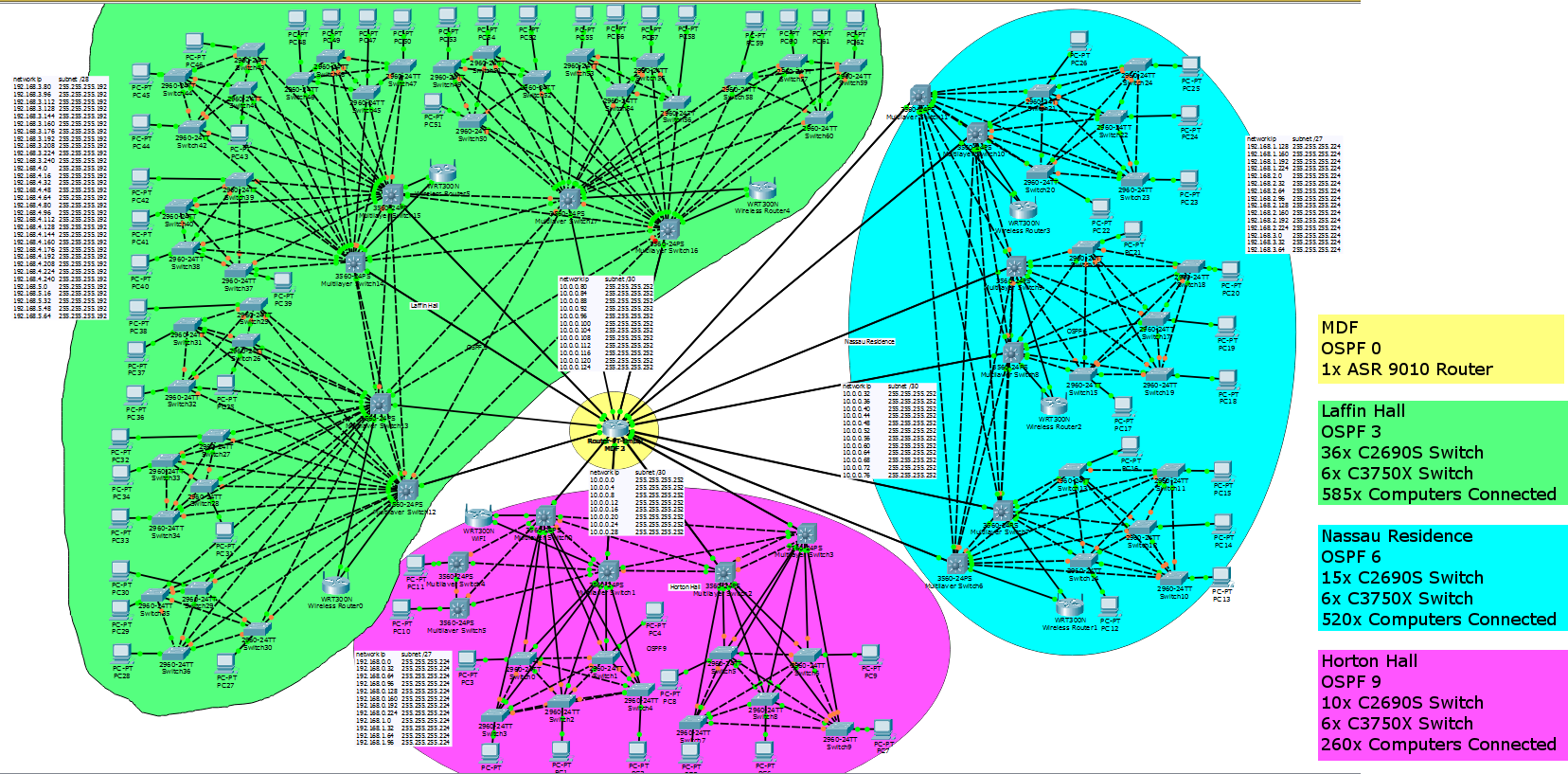
* Security Room:

Security room is in front of the server room with one way glass wrapping around the security room. Chip readers connected to any terminal that can SSH into the servers, acl’s to restrict all other ip’s from creating remote connections to the server room. The chip reader requires the card to be in to operate the computer. As soon as the card is removed the computer locks down. Only computers in the security room can SSH into the server room.









**Bill of Materials Spreadsheet:**



**Security Narrative:**

One of the most important things we will be doing is setting up access control lists on every Layer 3 device blocking any connection originating from outside the network. Assuming the gateway ip address is 192.168.1.1 an example of this would be #access-list 101 permit tcp any 192.168.1.1 255.255.255.255 established #access-list 101 deny tcp any any. We will also be using ACL’s to turn off all unused ports to prevent intruders from exploiting a service that we aren’t even using.

We will be setting up separate OSPF areas for the DMZ, the backbone, and each building. The DMZ will contain the Email server, citrix server, cloud storage, and HTTP server all on separate VLAN’s. The cloud storage will be running a Linux OS and scanning all incoming files for virus using the Clam Anti-virus tool. Linux is the best OS to do the job because most viruses are made for Windows and won’t have any effect at all on the Linux server. The webserver will force all connections to use HTTPS for more security. This means if someone is capturing packets on our network they will still need to decrypt the data to to make any use of it. Just inside the DMZ we will have our network DHCP server, private DNS server, and Database server containing usernames and passwords for students and faculty. The passwords are required to be at least 10 characters in length and include at least one uppercase, one lowercase, one number, and one special character. All users will be required to change their passwords every 60 days, and the password cannot be reused. The command #access-list 1 deny 192.168.1.1 255.255.255.255 will be used to create an ACL that will protect these device from any connections originating from the gateway. This means that only connections originating from inside the network will be able to have access to our DHCP, DNS, and Login Database. The DHCP server will also try to set the DNS addresses to our DNS server. Having our own DNS server assures that no one inside our network will be sent to a malicious website via a DNS redirect hack. It also means that we can simply remove listings for urls that we don’t want people going to, and unless they have another DNS setup the webpage will be unreachable.

We will setup the Gateway to deny pings (config)#access-list 102 deny icmp any any (config)#access-list 102 permit ip any any (config-if)#ip access-group 102 in. The DMZ itself will have two firewalls protecting the network, one on the outside and one on the inside of the DMZ.

We will be using Network Address Translation overload ( more commonly known as Port Address Translation) on our edge router to hide the actual IP addresses on our network, using the command #ip nat inside source list 1 interface serial 0/0/0 overload. Each 3750 switch will be setup to act as a router on a stick and will also be preforming PAT. This means that anyone snooping on the inside of our network will still have a difficult time figuring out what IP addresses are connected and mapping the entire network. By doing this we make it a little harder for the attacker to target and take over computers on campus.

All unused ports will be shutdown to prevent anyone from hooking a device to them, and being granted network access. We will have a total of 70 VLANS. Each 2960 switch will have its own VLAN setup to prevent devices connected to other switches from being able to directly communicate with computers that it shouldn’t. Two 3750 will also be setup to have VLANs, one for the Pixar offices and one for the Security/ IT office. We will also have one VLAN in each building for the Wi-Fi access points to connect to. By segregating the network this much we limit the number of devices that hackers can gain contact with. All 2960 switches, except Nassau Residence, will have sticky mac addresses set up on every port that is not connected to another switch using the command #switchport port-security mac-address sticky. These ports will also have BPDU guard setup to prevent someone from connecting a switch to them. The ports connected to other switches will all be configured as trunk ports to handle traffic from each VLAN in case of a network device failure and for load balancing. Because Nassau is a residence we assume that new devices will get plugged into the network all the time so we won’t be limiting the number of Mac addresses available on each port.

Each buildings switches will be cross connected for redundancy. This means that if one networking device goes down then only the end devices connected to it will lose connectivity. All other devices will still have a connection through other switches and will be able to route around the problem. We will be using Spanning Tree Protocol on every switch to prevent switching loops form happening.

Our campus wide Wi-Fi will have two SSID’s. The first one will be hidden from the public and exist only for students and faculty. The information for the hidden SSID will be available from our IT/ Security department and will allow full access to the intranet. Connection to this network will require a valid username and password that is unique to each individual and are only given to students and faculty. The public SSID will be broadcast and open for use by anyone on the campus. The public SSID will only allow access to the internet, not to local network services. We will be heavily logging all activity on the network to help us block or prosecute anyone using it for devious purposes. Once connected to the network the user will be redirected to a webpage requiring them to accept our terms of use. This should prevent intruders from having an easy way onto our private network, and give us some idea of who did what and how to prevent it in the future.

For Physical security we will have cameras on each floor monitoring entrances, exits, hallways, and stairwells. All students and faculty will be required to carry photo id badges with rfid chips to gain access to buildings. The lobby of each building will have a security guard to monitor camera footage, and keep shady people out, as well as prevent tampering with devices.

Our security room will have one way windows lining the offices so that they can see who is coming without being seen in case of camera failure. The cameras in the hallway will monitor everyone who comes and goes, including who enters the security office. The Main Distribution Frame (MDF) equipment is kept in a locked room inside the security room. The security room requires an rfid card and finger print reader to gain access. Once inside the security room the door to the MDF room will have an electronic lock with keypad and inside it will have cages with pad locks protecting the switches and routers from physical tampering. This means in order to gain access to the MDF room you have to pass multiple checks against who you are, what you know, and what you have. There will be several cameras inside the MDF room monitoring everything that goes on. One of these cameras will be inside the cage making it harder for an intruder to physically tamper with all the cameras, even once he is inside the MDF room. All security computers in every building will also require a chipped card to be inserted to a card reader, if the card is removed the computer locks down. These chips will be part of the security team’s normal badge but will not be part of the faculty and student’s badges. Chip readers will also be connected to any terminal that can SSH into the servers. ACL’s will be used to restrict all other IP’s from creating remote connections to the server room. Telnet will not be allowed anywhere on our network.

That does it for our current security plan. We believe this is a good way to secure the network. But this doesn’t mean that we will stop there. We will continually monitor the network and run our own pen testing to make sure everything is up to date and secured now and in the future.

**Justification:**

The network will be comprised of mostly C2960 and C3750X switches connecting up to one central ASR9010 routers. The ASR9010 will provide internet connection for the whole campus. Each C3750X switch will connect to two different blades in the ASR9010 router using single mode fiber for high speeds, long distances, and network redundancy. This way if one port or one blade in the ASR9010 router goes down the building will not completely lose connectivity.

All of the C2960 switches come with 1 Gb Ethernet ports connecting to the computers and each other for redundancy. However the throughput will not allow all connections to run at 1 Gb each. Instead our goal is about 100 Mb for each computer in Laffin Hall and Horton Hall. This should be plenty of speed for regular school and office work, while allowing a few individuals to still get higher speeds when needed. However, Nassau residence will have more throughput to allow for students streaming movies, music, and constant social media updates. Since it is unlikely that everyone will be using up all the bandwidth at the same time it is more likely that each student will be able to use their max bandwidth when that student needs it. This also means that when students are touring the empty dorms they can hook up their laptops and see amazing download speeds enticing them to join our university.

Each C2960 switch will have two 1Gb ports to the C3750X switches. The C3750X switches will have two 10 Gb uplinks to the ASR9010 router and 1 Gb connections to each other C3750X switch in the building for redundancy.

**Campus Area Network VLSM:**

Horton Hall has 260 computers with 26 ip's connected to each Cisco 2960 switch

Network IP Subnet /27

192.168.0.0 255.255.255.224

192.168.0.32 255.255.255.224

192.168.0.64 255.255.255.224

192.168.0.96 255.255.255.224

192.168.0.128 255.255.255.224

192.168.0.160 255.255.255.224

192.168.0.192 255.255.255.224

192.168.0.224 255.255.255.224

192.168.1.0 255.255.255.224

192.168.1.32 255.255.255.224

192.168.1.64 255.255.255.224

192.168.1.96 255.255.255.224

Cisco 3750X

Network IP Subnet /30

10.0.0.0 255.255.255.252

10.0.0.4 255.255.255.252

10.0.0.8 255.255.255.252

10.0.0.12 255.255.255.252

10.0.0.16 255.255.255.252

10.0.0.20 255.255.255.252

10.0.0.24 255.255.255.252

10.0.0.28 255.255.255.252

Nassau Residence has 585 computers with 40 ip's connected to each 2960 switch.

Network IP Subnet /27

192.168.1.128 255.255.255.224

192.168.1.160 255.255.255.224

192.168.1.192 255.255.255.224

192.168.1.224 255.255.255.224

192.168.2.0 255.255.255.224

192.168.2.32 255.255.255.224

192.168.2.64 255.255.255.224

192.168.2.96 255.255.255.224

192.168.2.128 255.255.255.224

192.168.2.160 255.255.255.224

192.168.2.192 255.255.255.224

192.168.2.224 255.255.255.224

192.168.3.0 255.255.255.224

192.168.3.32 255.255.255.224

192.168.3.64 255.255.255.224

Cisco 3750X

Network IP Subnet /30

10.0.0.32 255.255.255.252

10.0.0.36 255.255.255.252

10.0.0.40 255.255.255.252

10.0.0.44 255.255.255.252

10.0.0.48 255.255.255.252

10.0.0.52 255.255.255.252

10.0.0.56 255.255.255.252

10.0.0.60 255.255.255.252

10.0.0.64 255.255.255.252

10.0.0.68 255.255.255.252

10.0.0.72 255.255.255.252

10.0.0.76 255.255.255.252

Laffin Hall has 520 computers with only 17 ip's connected to each 2960 switch.

Network IP Subnet /28

192.168.3.80 255.255.255.192

192.168.3.96 255.255.255.192

192.168.3.112 255.255.255.192

192.168.3.128 255.255.255.192

192.168.3.144 255.255.255.192

192.168.3.160 255.255.255.192

192.168.3.176 255.255.255.192

192.168.3.192 255.255.255.192

192.168.3.208 255.255.255.192

192.168.3.224 255.255.255.192

192.168.3.240 255.255.255.192

192.168.4.0 255.255.255.192

192.168.4.16 255.255.255.192

192.168.4.32 255.255.255.192

192.168.4.48 255.255.255.192

192.168.4.64 255.255.255.192

192.168.4.80 255.255.255.192

192.168.4.96 255.255.255.192

192.168.4.112 255.255.255.192

192.168.4.128 255.255.255.192

192.168.4.144 255.255.255.192

192.168.4.160 255.255.255.192

192.168.4.176 255.255.255.192

192.168.4.192 255.255.255.192

192.168.4.208 255.255.255.192

192.168.4.224 255.255.255.192

192.168.4.240 255.255.255.192

192.168.5.0 255.255.255.192

192.168.5.16 255.255.255.192

192.168.5.32 255.255.255.192

192.168.5.48 255.255.255.192

192.168.5.64 255.255.255.192

Cisco 3750X

Network IP Subnet /30

10.0.0.80 255.255.255.252

10.0.0.84 255.255.255.252

10.0.0.88 255.255.255.252

10.0.0.92 255.255.255.252

10.0.0.96 255.255.255.252

10.0.0.100 255.255.255.252

10.0.0.104 255.255.255.252

10.0.0.108 255.255.255.252

10.0.0.112 255.255.255.252

10.0.0.116 255.255.255.252

10.0.0.120 255.255.255.252

10.0.0.124 255.255.255.252

MDF:

ASR 9010 will be connected to the 3750 switches using fiber and the following VLSM scheme.

Network IP Subnet /30

10.0.0.0 255.255.255.252

10.0.0.4 255.255.255.252

10.0.0.8 255.255.255.252

10.0.0.12 255.255.255.252

10.0.0.16 255.255.255.252

10.0.0.20 255.255.255.252

10.0.0.24 255.255.255.252

10.0.0.28 255.255.255.252

10.0.0.32 255.255.255.252

10.0.0.36 255.255.255.252

10.0.0.40 255.255.255.252

10.0.0.44 255.255.255.252

10.0.0.48 255.255.255.252

10.0.0.52 255.255.255.252

10.0.0.56 255.255.255.252

10.0.0.60 255.255.255.252

10.0.0.64 255.255.255.252

10.0.0.68 255.255.255.252

10.0.0.72 255.255.255.252

10.0.0.76 255.255.255.252

10.0.0.80 255.255.255.252

10.0.0.84 255.255.255.252

10.0.0.88 255.255.255.252

10.0.0.92 255.255.255.252

10.0.0.96 255.255.255.252

10.0.0.100 255.255.255.252

10.0.0.104 255.255.255.252

10.0.0.108 255.255.255.252

10.0.0.112 255.255.255.252

10.0.0.116 255.255.255.252

10.0.0.120 255.255.255.252

10.0.0.124 255.255.255.252