Homework 3

Name: Anusha Balasubramanian
UID: U01305952
Email id: ab19533n@pace.edu

Part 1:

I tried to investigate network access control scheme at my Previous Work Place.

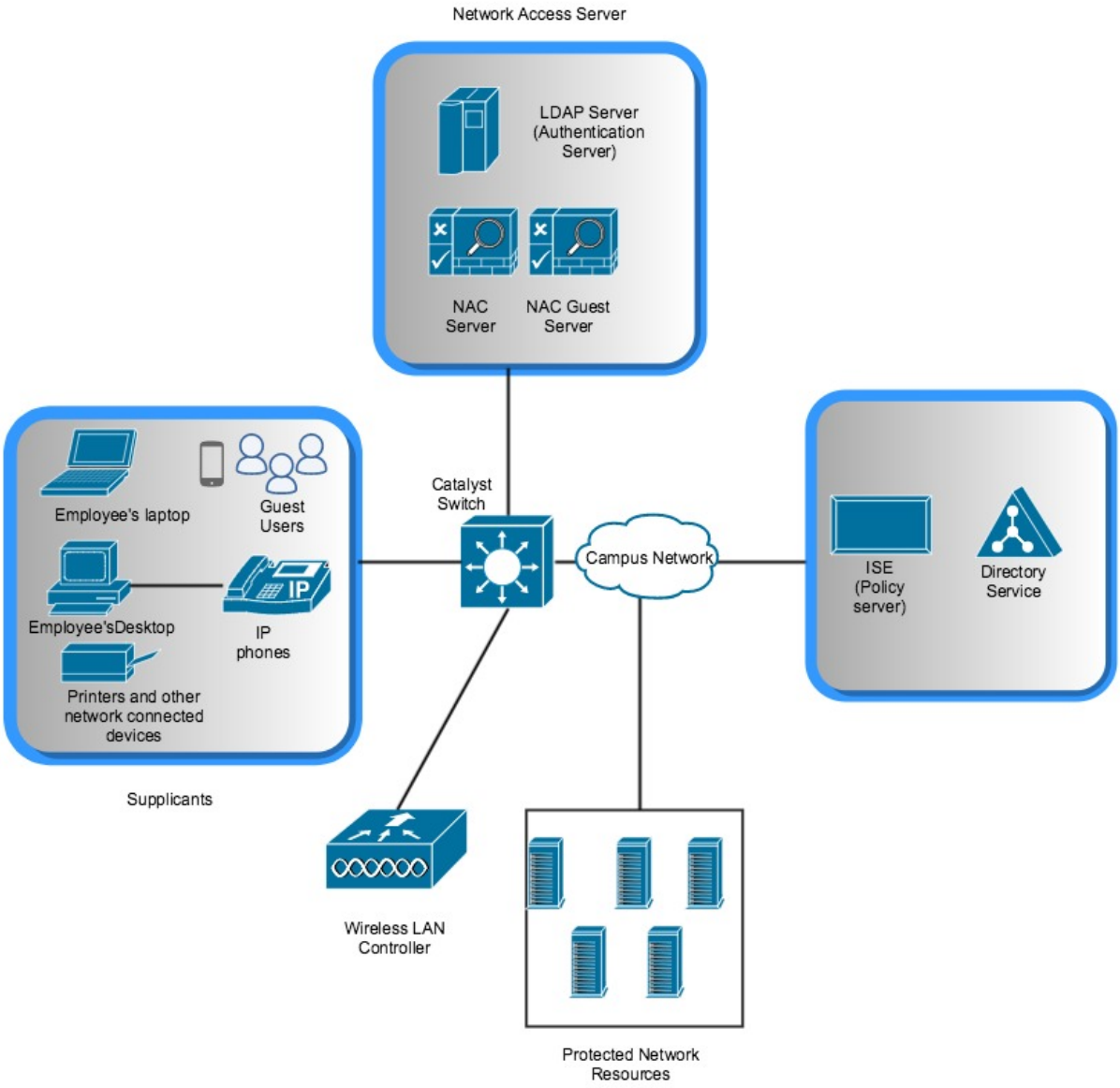
Overview about network access at my place of research:

My workplace uses CISCO's clean access to to provide network access control.
We have a desktop, IP phone and laptops as organization assets.
Our laptops can connect through WIFI and usingLAN cable.

We also have two different connections in WIFI based on the requirement.

1. Corp-wifi: In-order to connect to the "corp-wifi" we need to first connect our laptop to LAN and perform authentication. Once Authentication is done, employees can connect their laptop's to the "corp-wifi" and can freely move around. Employees have equal access permissions like the access they have through LAN network.
2. Guest-wifi: We use this for connecting our smart phones and other devices that we own. This is protected by password and its common to everyone in organization. It has various restrictions. This is also provided to guests who come in for events like hackathon.

Below mentioned is the network access control mechanism diagram. I have created this through gliffy.com



Terminologies:

NAC Server: The NAC Server enforces access privileges based on endpoint compliance and user authentication. A user cannot gain access to the network until they authenticate and the device meets defined posture requirements.

NAC Manager: This is a centralized, web-based console for establishing roles, checks, rules, and policies.

NAC Guest Server: The NAC Guest Server streamlines the provisioning, notification, management, and reporting of guest users on wireless networks.

ISE (Identity Services Engine): ISE provides profiling capabilities that can discover, analyze, and classify in real time all the endpoints connecting to the network. ISE comes with hundreds of built-in profiles for devices such as IP phones, printers, mobile devices (IPads, IPhones), scanners, and more, making it possible to identify the type of device connecting to the network. ISE provides the administrator full visibility into everything connected to the network in real time. It allows the administrator to control the access privileges associated with each type of endpoint.

LDAP: Light weight Directory Access protocol

When the computer first connects to the network, NAC server checks and enforces necessary authentication for the computer. The authentication is successfully done by LDAP server where a TCP connection and authentication session is established with LDAP server through a simple bind (username and password). And on successful authentication, the ISE (policy server) issues the required access permissions that is required for the computer. Once this is done the computer will be part of directory to access network resources.
Every computer in-order to connect to corp network, uses either wired or wireless network. Wireless LAN controller lets laptop connect to "corp -wifi" network (through wifi). In this case, the laptop is checked against the ISE and directory service for its permission. The user doesn't have to authenticate again. LDAP helps in achieving this. Once authentication is done, these systems are marked for LDAP authorization. So when the same system connects through wifi only the authorization check is done. Also LDAP helps in providing authentication integration with single sign on.
In case of guest wifi, the user id and password (Authentication information) is checked by LDAP server, which in-turn takes help from ISE to provide access rights for guest users.

All these devices are considered a campus network including the protected network servers

References:

http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html
http://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html
http://www.cisco.com/c/en/us/products/collateral/security/nac-appliance-clean-access/product_data_sheet0900aecd802da1b5.html
www.wikipedia.com