Network Security and Availability – Executive Summary

Purpose

The purpose of this executive overview is to provide a non-technical high level view of network security and availability enhancements implemented by the Information Technology Department during 2014 and 2015.

802.1x Network Security

The Information Technology Department strives to ensure that all authorized users are protected from foreign parties gaining access to the network. One way that security is implemented is on a port by port basis. When there is a cable running from the back of your desktop computer to a wall-jack, that wall-jack is directly connected to a port on a piece of networking equipment called a switch.

Previously those switch ports were secured by means of a technology called "port-security". The way that security feature works is when a device plugs into a port it leaves a signature that is unique to the device. That signature is called a MAC Address. Every piece of computing equipment that connects to a network has a unique MAC Address. Port-Security saves a copy of that MAC Address and identifies the computing device that is plugged into a specific port. If a foreign device, or to say a foreign MAC Address is seen, it disables the port.

This is a very simple way of guaranteeing only the devices that should connect to a port are allowed access. But, it also creates challenges. When employees move offices and take their phone or computer to plug into the network through a new wall-jack, port-security does not know this is authorized and will disable the ports anyway. This then has to be manually cleared by the Information Technology Department Network team, and creates a time-gap for users as they will now wait until it is addressed. The same goes even if a user isn't moving, but gets a new IP phone, or computer that will plug into their existing wall-jacks. Not to mention, it requires even more configurations by the Networking team if an unauthorized device needs access; as in a vendor that needs to plug into a wall-jack to gain Internet connectivity for a presentation.

A solution to bring additional security and fully automate the process of moving users to new offices, upgrading the equipment in their current office, and allowing foreign hosts like vendors access to the Internet was the 802.1x protocol. With this protocol we are now able to automatically determine if a device belongs to the City and regardless of what wall-jack it plugs into it will be granted full access to the inside network. Vendors and other foreign hosts can also plug into any wall-jack and gain Internet access without being allowed to the sensitive inside network that is for City employees only. This is all fully automated by a series of authorizations that happen between the computing device, the switch, and a pair of redundant servers in the datacenter.

The 802.1x solution has greatly increased the City's ability to make moves, changes, and grant vendors and others the ability to get to their resources while maintaining the highest level of security.

Virtualized Network Enhancement

The Information Technology Department is responsible for the voice and data communications in the City. Whenever a City employee makes a phone call, enters their timesheet on JDE, or surfs the Internet, it is the

City network that makes that connection possible. Many of the tasks performed by employees throughout the organization rely on reliable end to end connectivity.

A day to day objective for the Networking team is to ensure reliability and availability for all connectivity in the City. The primary way users get connected to resources is through some form of cabling. Even wireless devices attach to access points that need to eventually find their way to a cable to get connected. Some cabling is copper, or what we call Cat5E cable, and can be seen connecting a desktop computer to a wall jack. Other cabling is glass, or fiber optic, and is what interconnects the floors of buildings and spans through the City connecting each location back to City Hall and all of its resources.

The City has many different responsibilities and some of them need to be securely separated from each other. For example, the water department needs to be very secure as any malicious attack on their network could affect the quality of the Public's water supply. In other instances it is the City worker that needs to be protected; such as from the Public Library patrons and their Internet usage.

Previously the solution to keep all of these various networks separated was to just run individual fiber optic that was dedicated to one network or the other. This created a vast amount of redundant fiber throughout the City, but all of it was being underutilized. Wouldn't it be nice if all this fiber was available for all of the networks? That was the challenge the Networking Team was charged with solving.

Utilizing advanced networking techniques the team was able to "virtualize" the network. This virtualization allowed every network in the City to use all of the redundant fiber securely and efficiently. Now instead of the Water Department, Library, or other City Departments relying on their own dedicated fiber optic to connect to their resources, they could use any of the redundant connections. Instead of a piece of network hardware having to be dedicated to one network, any could take advantage of it. This enhancement greatly increased the reliability and availability of resources, regardless of the network involved.

The benefits didn't stop there either. Once this was in place, functionality that was once previously unavailable was now possible. The Library now has City resources delivered directly through the network similar to the other City Departments. The resources needed by the Water Department, Library, and City users was now able to be provided in a redundant fashion through the City's virtualized servers. Through the virtual network, the City's Disaster Recovery data center capabilities were enhanced in functionality and ability to provide the resources in case of an emergency. The benefits realized from the virtualization project have been numerous, offering enhanced services, more efficient use of fiber resources, and high network availability.

Internet Load Balance Implementation

The City leases connections with CenturyLink and Comcast to provide inbound and outbound internet connectivity. There is a 20 Mbps synchronous connection, meaning that both the upload and download speed is the same. This is used primarily for users on the Public Internet when connecting to the City's resources; for example the City website. There are also three asynchronous connections, or differing upload and download speed, with 50 Mbps upload and 10 Mbps download that are used primarily for all employee connections to the Internet.

In the past the three asynchronous connections were utilized in a single-use fashion. There was one located at City Hall for most of the City's Internet traffic. There was one connection at College Hill Library, as well as Irving Street Library. Each Library had the benefit of a private connection to the Internet based at their location, while the rest of the City utilized the one at City Hall.

Through some creative design and advanced networking techniques, the Network Team was able to send all of the City's Internet traffic out all three asynchronous connections simultaneously in a perfectly load balanced way. This increased the collective whole of all users connected to the Internet's bandwidth, while simultaneously tripling the availability.

With this newly configured technology there was also a "health-check" mechanism that verifies the availability of each Internet connection and ensures that a good connection is available. If one of the connections is unavailable or unhealthy due to a provider issue or service, it is automatically removed as a choice in the load balance group. As soon as the unhealthy connection regains its availability, it is automatically placed back into the group of choices.

This load balance scheme with built in health-check has allowed the City to provide the very best in Internet availability and reliability. Because of its robustness and its full automation, the only time the Internet is unavailable is for scheduled service by the Information Technology Department. Since the time the load balancing enhancements were incorporated into the network, the City has experienced 99%+ Internet uptime.