Objective:

The objective of this visit was to analyze the existing network infrastructure with the intention of unearthing any vulnerabilities or inconsistencies that might exist. This analysis was performed from both within the network and from the outside looking in.

Background:

Dr. Example's office consists of one building with a standard communications closet. It will be our goal to discover the topology of the physical and logical networks and the existing infrastructure and interconnects.

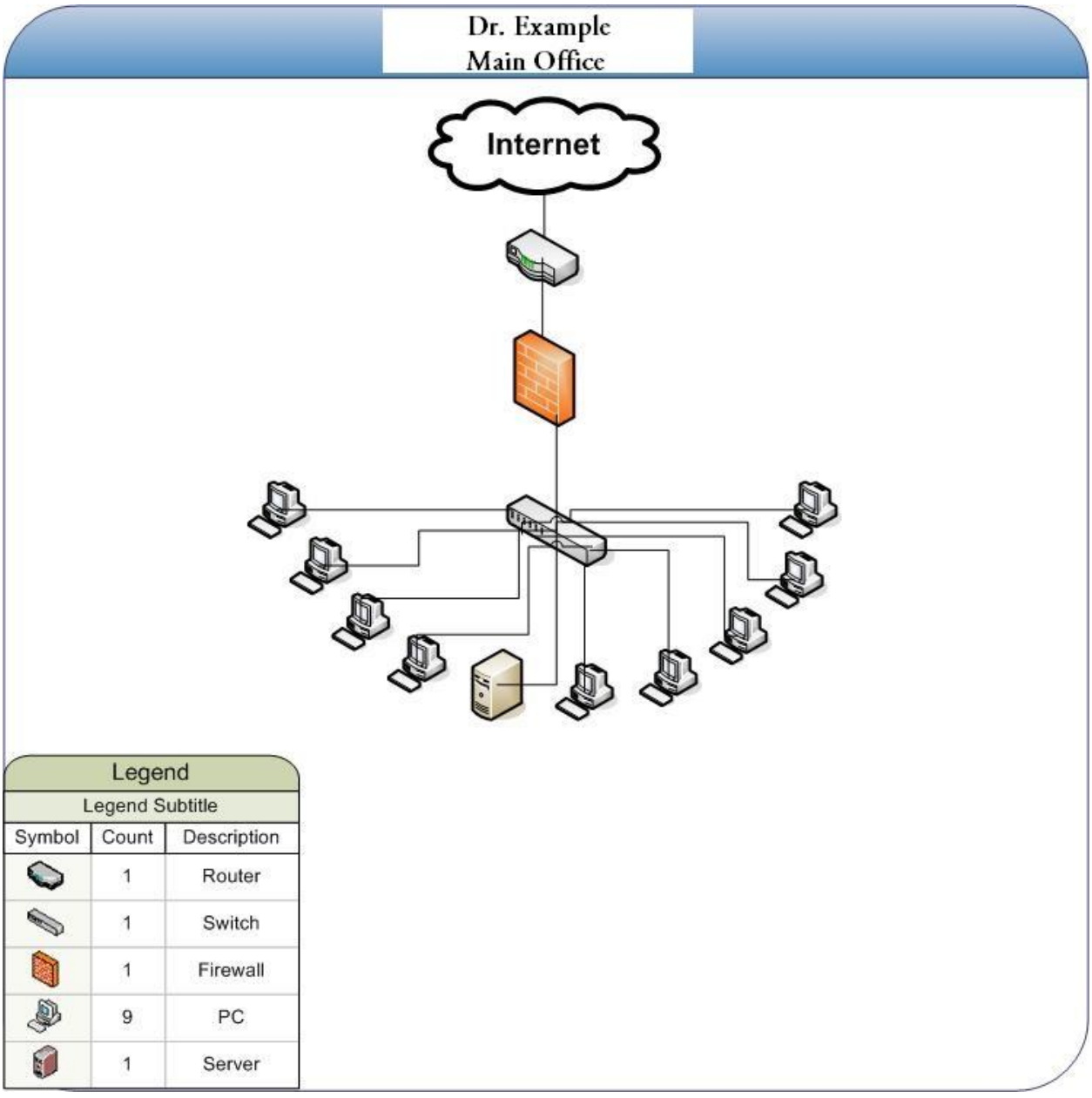
Review (Main Building):

At the office there is a standard communications closet with one server running Server 2003 Small Business. There are two front desk machines, six operatory machines and Dr. Example's office machine. There are two network printers on the network. The cabling structure for the network comes from each jack into the 24 port patch panel and then into the switch. The cable internet is plugged directly into the sonicwall. The sonicwall is the default gateway, dhcp server and firewall for the entire network.
The domain is being scarcely used. The following machines are on the domain: Server (the domain controller), Operatory1, Owner (this should be renamed Operatory2) and Doctor1. The following machines belong to various workgroups: Office1, Office2, Operatory3, Operatory4, Operatory, and Operatory6.

Basic Network Information:

Class: A
Network: 192.168.16.X
Netmask: 255.255.255.0
Gateway: 192.168.16.1
DHCP Server: 192.168.16.1
DNS Server: (using cable modem dns)
ISP: Cable Company LLC
Number of Devices: ~13

Network Diagram:



94143 Bayou Drive, Diamondhead, MS 39525 • Phone: 601.569.1770

Concerns (listed in priority order):

- **No Backup Solution**
  - **Explanation: Currently all of the data is being stored on the server in the R:/ drive. If the server should fail than all data would be lost without hopes of recovery.**
  - **Recommendation: Purchase a NAS Black Armor to do network backups of the server. This will protect you from machine failure.**
  - **Optional Recommendation: Purchase a subscription to online backup software to back up your most crucial data in the event the whole building is destroyed. (Hurricane, Fire, Tornado, etc.)**

- **No Common Antivirus Solution**
  - **Explanation: Several machines are using some type of antivirus, but they are either not updated or expired. Some machines do not have any antivirus at all.**
  - **Recommendation: Order a 12 license subscription to Avast and use your domain controller to manage the antivirus for you. With this in place it will force all updates for you and if a machine reports an infection then the server will force it to run a scan.**

- **No Battery Backup on Equipment**
  - **Explanation: Currently there is no battery backup on the network equipment or the server to protect against power failure. This could cause data loss if you are working on a file that exists on the server and a power outage should occur.**
  - **Recommendation: Install an APC UPS 750 at both locations.**

- **No Domain Control**
  - **Explanation: The server is set up to be a domain controller yet several of the machines at the office have not been joined to the domain.**
  - **Recommendations: Join the machines to the domain.**

- **No Centralized Windows Update System**
  - **Explanation: Windows updates help to fix the "holes" in windows security. It patches windows to fix bugs and potential threats to Servers and PCs alike. Without a centralized manager for windows updates you cannot confirm that all of your machines are in fact up to date.**
  - **Recommendation: Download, Install and Configure WSUS (Windows Software Update Server). This will manage all updates from the server and force them to all PCs on the network and joined to the domain. It is free to use with a Server Operating System**

- **Not Using Local DNS**
  - **Explanation: On a domain network it is crucial to use a local DNS server. Your existing server is not utilizing this role. Without using this feature you will experience significantly delayed logon times to your machines on the domain.**
  - **Recommendation: Configure the DNS server role and change the settings in the Sonicwall to use the server as the domain server when it hands out IP addresses.**

- **Mounting of Server**
  - **Explanation: The server is currently strapped to the side of a desk. I noticed that if you move it, it will swing freely. If the server is jarred at the wrong time this could cause significant data loss or hard drive failure.**
  - **Recommendation: I recommend moving the server to another location so that it can stand flat. The ideal place to put it would be in the communications room away from idle hands.**