

Network Troubleshooting and Analysis

Objective:

The objective of this lab is to gain a deeper understanding of the tools and concepts required for troubleshooting and analyzing a network.

References:

A portion of the network layout was provided with the lab.

Equipment/Programs Used:

Dell Inspiron 8600 Laptop
GFI LanGuard Network Scanner
Various networking devices provided in the lab
Switches, hubs, servers, routers, workstations
3COM Network Manager

Procedures:

The procedures of this lab will be organized into the following sections:

1. Analyze the network in the lab.
2. What are the IP addresses of all of the boxes?
3. What is the network topology?
4. What is the connectivity map? ie what can see what?
5. What are the port configurations on the boxes?
6. What is broken in the network?
7. What tools are necessary to analyze an unknown network's state?
8. Would it be possible to manage this network as it is currently configured?
9. Document a strategy for analyzing a network using what you have learned.
10. Propose a default configuration of devices that would enable one to begin to manage this network.
11. How could you protect the network devices from discovery and attack from the normal users of the infrastructure? (Note: If you can't ping it you can't hack it.)

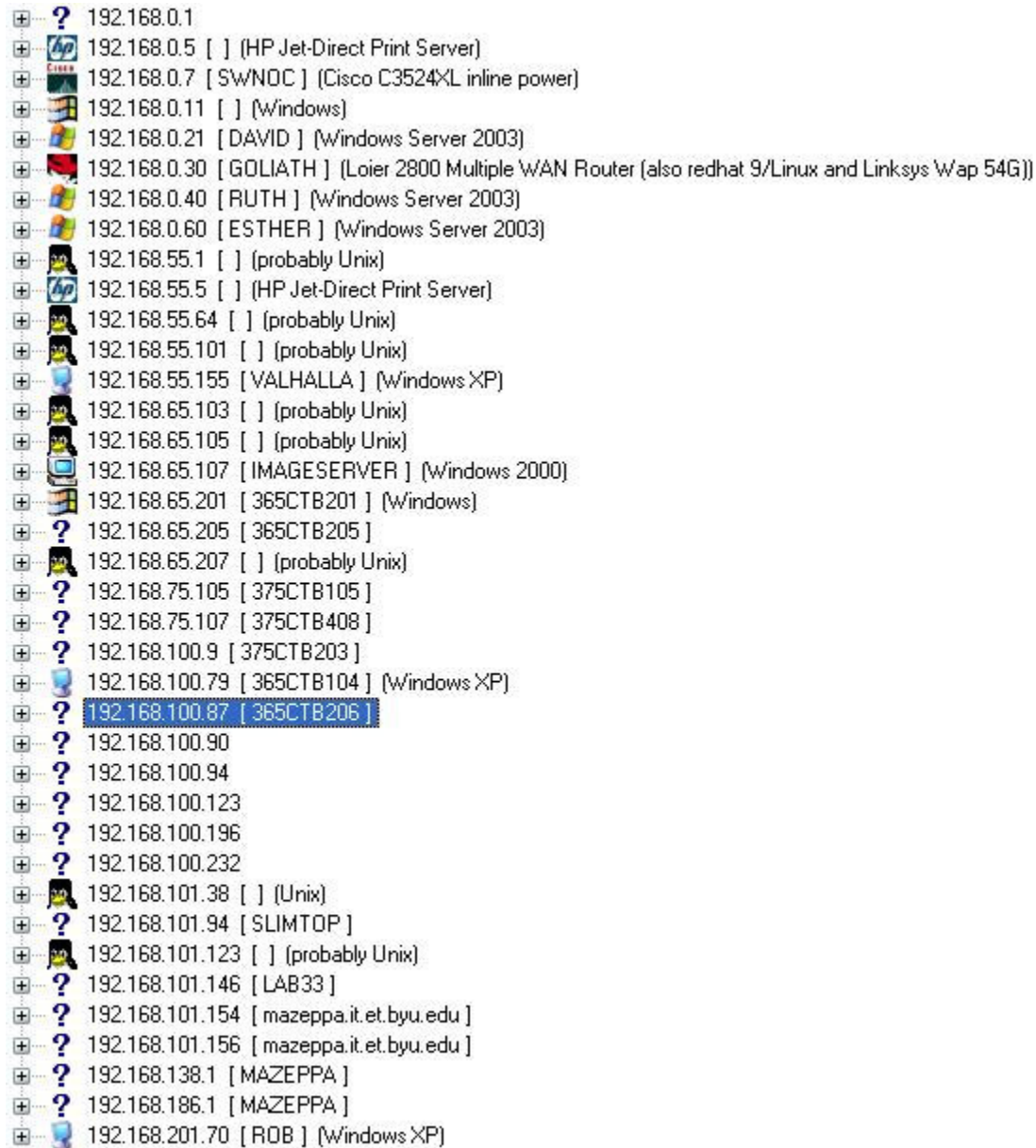
1. Analyze the network in the lab

Because this step is an ambiguous statement of what the other steps in this lab should accomplish, no actual actions were taken.

2. What are the IP addresses of all of the boxes?

There are several ways of discovering the IP addresses of 'all' of the boxes in the network. For this lab, GFI Languard was used to scan the address range from 192.168.0.1 through 192.168.0.255. Languard uses ping sweeps, as well as netbios

and snmp sweeps to attempt to discover the boxes in a network. An image showing the various IP addresses discovered is provided below.



The image shows a list of discovered network devices. Each entry includes an icon, an IP address, and a NetBIOS name in brackets. The IP address 192.168.100.87 is highlighted with a blue selection box. The list includes various devices such as HP Jet-Direct Print Servers, Cisco routers, and Windows/Linux servers.

IP Address	NetBIOS Name	OS / Device Type
192.168.0.1	[]	[]
192.168.0.5	[]	(HP Jet-Direct Print Server)
192.168.0.7	[]	(Cisco C3524XL inline power)
192.168.0.11	[]	(Windows)
192.168.0.21	[DAVID]	(Windows Server 2003)
192.168.0.30	[GOLIATH]	(Loier 2800 Multiple WAN Router (also redhat 9/Linux and Linksys Wap 54G))
192.168.0.40	[RUTH]	(Windows Server 2003)
192.168.0.60	[ESTHER]	(Windows Server 2003)
192.168.55.1	[]	(probably Unix)
192.168.55.5	[]	(HP Jet-Direct Print Server)
192.168.55.64	[]	(probably Unix)
192.168.55.101	[]	(probably Unix)
192.168.55.155	[VALHALLA]	(Windows XP)
192.168.65.103	[]	(probably Unix)
192.168.65.105	[]	(probably Unix)
192.168.65.107	[IMAGE SERVER]	(Windows 2000)
192.168.65.201	[365CTB201]	(Windows)
192.168.65.205	[365CTB205]	[]
192.168.65.207	[]	(probably Unix)
192.168.75.105	[375CTB105]	[]
192.168.75.107	[375CTB408]	[]
192.168.100.9	[375CTB203]	[]
192.168.100.79	[365CTB104]	(Windows XP)
192.168.100.87	[365CTB206]	[]
192.168.100.90	[]	[]
192.168.100.94	[]	[]
192.168.100.123	[]	[]
192.168.100.196	[]	[]
192.168.100.232	[]	[]
192.168.101.38	[]	(Unix)
192.168.101.94	[SLIMTOP]	[]
192.168.101.123	[]	(probably Unix)
192.168.101.146	[LAB33]	[]
192.168.101.154	[mazeppa.it.et.byu.edu]	[]
192.168.101.156	[mazeppa.it.et.byu.edu]	[]
192.168.138.1	[MAZEPPA]	[]
192.168.186.1	[MAZEPPA]	[]
192.168.201.70	[ROB]	(Windows XP)

This list not only shows the IP address, but also provides the NetBIOS name where one was able to be discovered. LanGuard also makes an attempt to discover what OS is running on the discovered device.

3. What is the network topology?

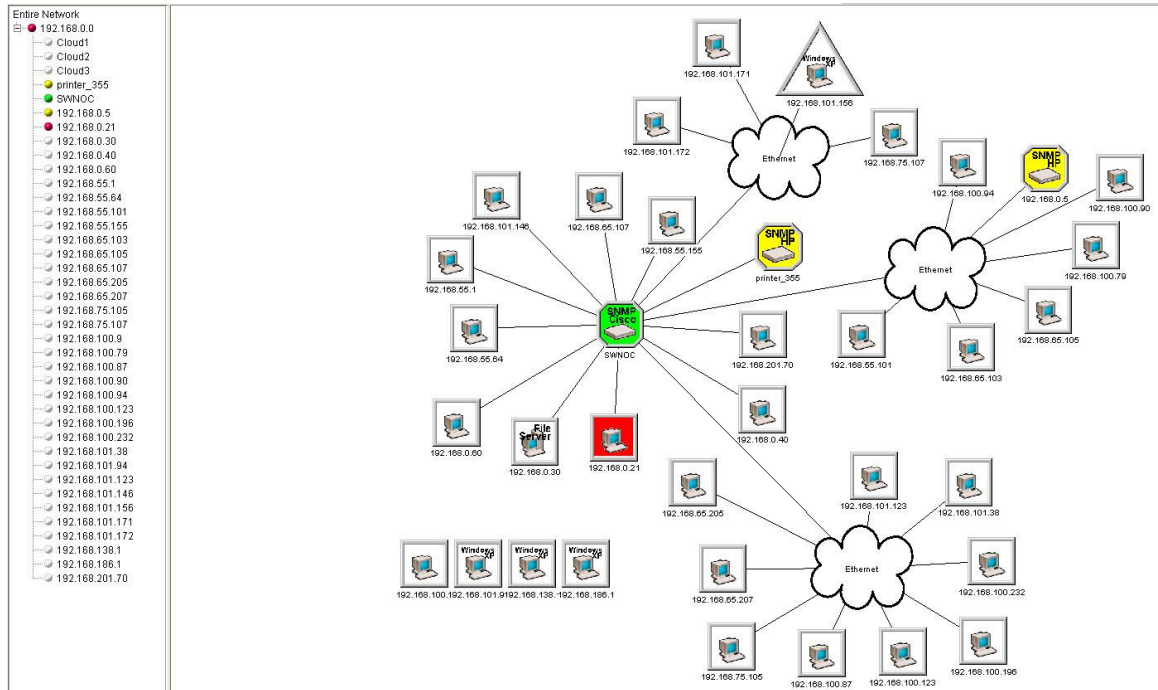
This question is referring to the actual physical topology of the network. In order to discover the physical topology, it was necessary to trace the network cables and come up with a layout of the physical network. The tracing began with the workstations in

room 385 and then led through the labs up to the NOC. Because the lab students were not expected to enter the NOC, a layout of the equipment there was provided.

A map of the physical topology of the network is included as an MS Visio file along with the lab documentation, and therefore is not included here.

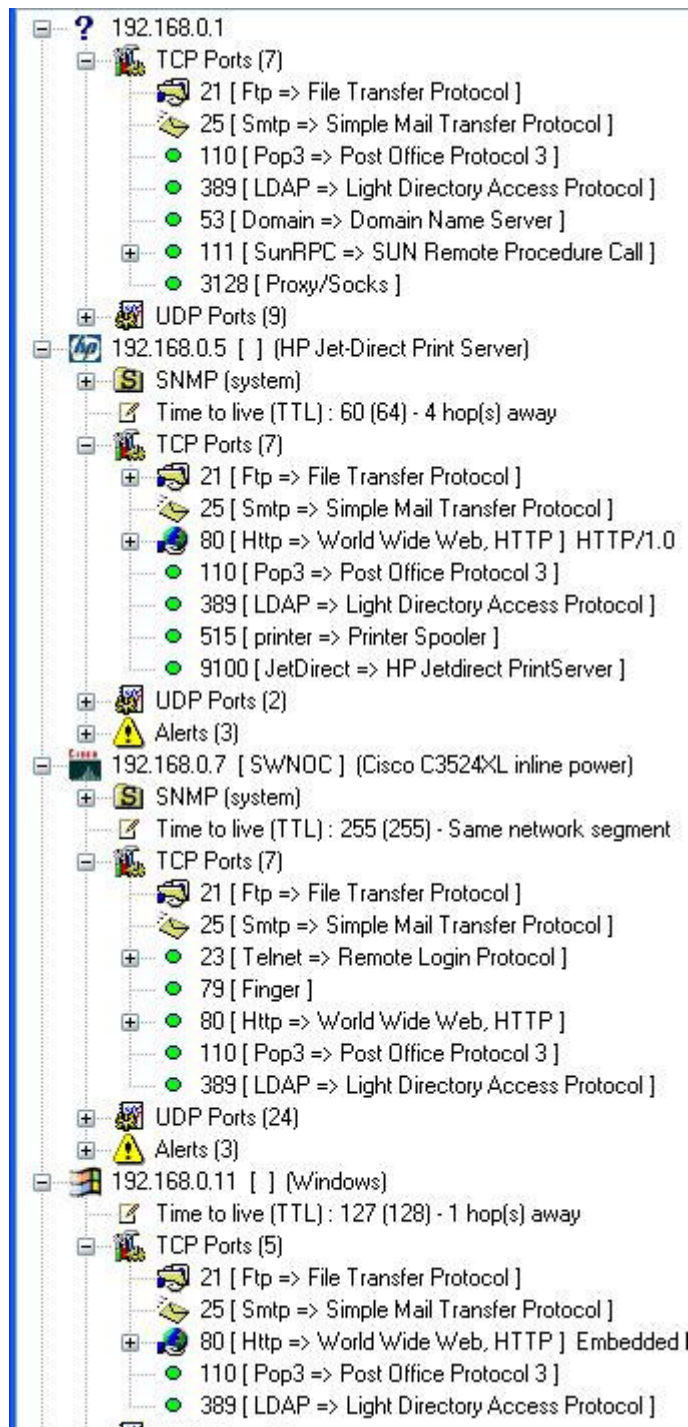
4. What is the connectivity map? ie what can see what?

The connectivity map was obtained using the Network Monitoring and Discovery software created by 3COM. The trial version of this software was downloaded from their website. The software asked for the range of the network to scan, and was provided with the 192.168.0.1 – 192.168.0.255 range. The software took approximately 2-3 hours to complete scanning all 65,000+ IP addresses. The final connectivity map is provided below.



5. What are the port configurations on the boxes?

This information was provided by using LanGuard. After finding all of the IP addresses in step two of this lab, the software then scanned for port configurations on the various devices. Because most of the devices were work stations with the same port configurations, a complete list is not provided. However, a screenshot of the more interesting devices is provided here.



It is clear that each device has a distinct port configuration. Some of the devices are running services such as web or ftp.

6. What is broken in the network?

In order to answer this question it was first necessary to define the term 'broken.' The professor responded that 'broken' simply means that the device does not respond how it is expected to respond.

According to this definition, there are several devices that would appear 'broken'. The CISCO 6000 switch is functional to the point that it is routing correctly, but SNMP queries or ECHO requests do not return valid results. Several of the Hubs and Switches in the labs act in a similar manner. Also, although GOLIATH is functional and has SNMP enabled, an SNMP walk will not turn up any useful information. There are also 4 workstations that did not answer correctly to some of the requests to discover the connectivity map. For this reason, these four workstations are shown as being disconnected from the network in the provided connectivity map.

7. What tools are necessary to analyze an unknown network's state?

There are several tools that are necessary and useful in analyzing an unknown network. Any type of network discovery tool (that is of good quality) will assist in discovering connectivity of devices. Network analysis tools that can monitor traffic and flow of information are also useful in determining weak/strong points on a network. Also, if one has physical access to the devices, in order to truly understand the state of the network it is also necessary to physically discover how the devices are configured, and which ones are functioning properly.

8. Would it be possible to manage this network as it is currently configured?

Unless both physical and remote access to the lab were not available, it is always possible to manage a network. However, some networks make management somewhat easier than others. The current IT network is somewhat difficult to manage, because many of the devices are not functioning properly, or have management protocols such as SNMP disabled. However, there are some devices in the lab that can be easily managed through SSH or RPC. Therefore the lab is not set up to be completely manageable, but it seems to be improving.

9. Document a strategy for analyzing a network using what you have learned.

A good strategy for analyzing a network is to begin at the bottom of the OSI model and work up. This means physically following the network and mapping out the physical connectivity of all devices. Keeping good notes of the devices will save a great amount of time later on.

It would then be wise to begin a connectivity map to see how the network 'sees itself'. This will provide information about the various DMZs in the network, the VLANs that exist, and especially how the 'virtual' network differs from the 'physical' network. This comparison will also help to determine what devices may not be functioning properly.

Upon completing the connectivity map, some sort of network scanning tool should be used to discover the port configurations, and other services that are being run on the network. This information will help to provide important information on services that are available, and possibly what services can or should be disabled for security purposes. This will also provide insight into possible methods for management.

10. Propose a default configuration of devices that would enable one to begin to manage this network.

The default configuration would depend on what type of device it is that is being connected. For example, a workstation should begin by having all services locked down while initially connected to the network. Once the workstation has been updated with OS patches, virus protection, and a firewall, then the necessary services can be enabled. It may be useful to install a remote desktop client such as VNC or Remote Desktop, although this is not completely necessary to have this sort of access to a workstation. A server should begin much the same way, until it has had proper firewalling and other security protection. Then, by having SSH enabled on the server, one can remotely configure the services that should be running, and provide a secure and easy way to manage the server. Routers/Switches should be configured with secure SNMP so that once it is plugged into the network, it can be managed from a central location. Some of these devices provide a web client that allows for remote management as well. If this is not a major security risk to the network, then leaving the web client enabled will allow for easier management of the device.

11. How could you protect the network devices from discovery and attack from the normal users of the infrastructure? (Note: If you can't ping it you can't hack it.)

This depends on the definition of 'normal'. There are several ways to discover that a device exists, and a 'ping' is only one of these methods. For Linux devices, not having NetBIOS mapping is another way to protect from being discovered. Also, disabling SNMP will help prevent a device from surfacing on a scan. The only way to truly protect a device, is to not allow access to it at all. This is highly unreasonable. Therefore, using software firewalling and physical firewalling are both good ways to BEGIN securing a device. However, it cannot stop there. If a service is unnecessary, it should be turned off. Also, an administrator must be certain to continually apply the latest patches for the OS and services running on the device. Otherwise an attacker may use a service exploit to gain access to a device. There is no way to allow services to run, and stay 100% secure. The use of methods described above, and other methods, will at least allow for greater security.

Results:

Using GFI LanGuard Network Scanner, the 3COM Network Discovery tool, and by physically analyzing the layout of the network, a topology map of the network was successfully created. The physical topology map is included as a separate file with the write-up. The connectivity map is included in the procedures section of the write-up. Many devices were discovered, and the layout of the devices, as well as the services on them was analyzed. All questions and problems outlined in the lab were successfully completed and are documented in the procedures section of the write-up.

Analysis:

The physical network was fairly simple to obtain by following the cables of the devices. The largest portion of the lab was located in the NOC and was thus provided by the System Administrator. By analyzing the differences between the physical network and the connectivity map, it was clear that some devices in the network are not functioning properly. It was also clear that many devices are 'locked down' so as to provide little information about how they are configured. Several of the machines were

running unnecessary services, while others were lacking the services required to manage them (such as SNMP). This particular arrangement is one that would be fairly difficult to manage and keep control of.

Conclusions:

This lab was very valuable in learning several tools that can be used to help in the discovery and management of a network. By combining the features provided in various tools, one can fairly quickly make an assertion as to the condition and state of an unknown network. Both the physical and connectivity maps of the network are necessary in order to truly manage and understand how the network is functioning.

This lab also raised some interesting thoughts on security. Several of the network devices did not show up in the connectivity map at all, despite the fact that they are physically a part of the network. This helps to reduce the risk of being hacked, simply because an attacker would not recognize the existence of the device. Also, this lab pointed out several weak points in the network. This included, but is not limited to, unnecessary services, and unprotected write-access to SNMP devices.

Overall this lab was extremely valuable in gaining an understanding of network discovery and troubleshooting techniques. The formulation of a standard, yet flexible management policy is vital in order to truly administer to a network.