Cyber Defense Organization

Spring 2019 - Networking, A Functional Focus

PLEASE SIGN IN >>>>
https://bit.ly/2I0fCRM

Updates!

NECCDC Updates!

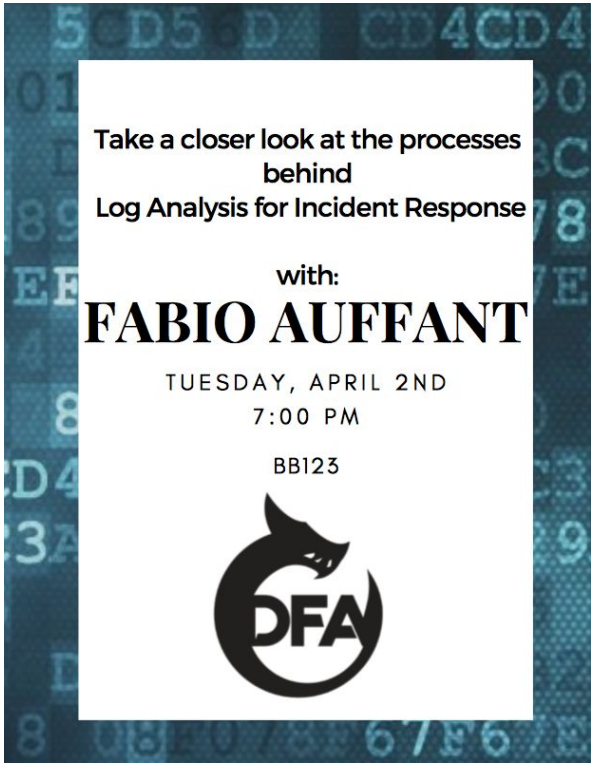
Other Events!

April 11th General Keith Alexander

April 12-13th NYC Women In Computing

April 12th Pentesting workshop - Training hours

April 17th Makerspace Open House



Other Events!

KEYNOTE

WiCyS
women in cybersecurity
UNIVERSITY AT ALBANY STUDENT CHAPTER

Victoria Kisekka

Dr. Victoria Kieskka is an assistant professor in the Information security and Digital Forensics department at the university with years of experience in Cybersecurity, Computer Science and Digital Forensics.

PROFESSIONAL PHOTOS WILL BE TAKEN AFTER! DRESS ACCORDINGLY.

Thursday March 29th @ BB002 6:30

FOOD WILL BE PROVIDED

Take a closer look at the processes behind
Log Analysis for Incident Response

with:

FABIO AUFFANT

TUESDAY, APRIL 2ND
7:00 PM

BB123

DFA

Discord Shenanigans

Upcoming Competitions

Central New York Hackathon

- Beginner
- 25 People Registered! ... out of 100 total
- DATES: Friday, April 5th, 4p to 9p
  Saturday, April 6th, 9a to 5p

Upcoming Competitions

University at Buffalo Lockdown v7

- Defensive cyber security competition
- Red vs Blue format
- Beginner to intermediate skill level
- April 27, 2019

Two teams
12 people total

Workshop!

Table of Contents

1. Basics
2. OSI Model Understanding
3. Network Devices
4. Important Network Protocols
5. Network Errors

Basics (Question)

- What does a computer need on the network?
- Answers
  a. IP Address
  b. MAC Address
  c. Subnet Mask
  d. Default Gateway

Basics (Abbreviations)

Damn IT!

- LAN (Local Area Network)
  - Where you are sitting now
- WAN (Wide Area Network)
  - Internet

Basics (Cont.)

IP Address

- Address of the Computer within its network
- “Home Address”
- Ex: 192.168.1.124

Subnet Mask

- Defines what network you are apart of
- “Zip Code”
- Ex: 255.255.255.0

MAC Address

- Physical address of the device
- Given when created in factory
- “Social Security Number”
- Ex: 00-14-22-01-23-45

Default Gateway

- Exit point of the network, Connection to the internet
- “Post Office”
- Ex: 192.168.1.1

Windows Example

```
C:\WINDOWS\system32>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : 8B2GQD2
   Primary Dns Suffix  . . . . . . . : nyscifa.research.lab
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : nyscifa.research.lab

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (2) I219-LM
   Physical Address. . . . . . . . . : 18-66-DA-2C-57-25
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.0.18(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Lease Obtained. . . . . . . . . . : Friday, March 29, 2019 11:05:24 AM
   Lease Expires . . . . . . . . . . : Saturday, March 30, 2019 11:07:33 AM
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DNS Servers . . . . . . . . . . . : 192.168.0.5
                                       192.168.0.8
                                       169.226.1.100
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Where are:

IP Address?
Subnet Mask?
MAC Address?
Gateway?

Lets Go to Packet Tracer!

https://tinyurl.com/2019NetworkingCDOWorkshop

Important Info for Hands on

HeadQuarters

- Default Gateway: 192.168.1.1
- Subnet Mask: 255.255.255.0
- DNS Server: 192.168.1.100

Remote Office

- Default Gateway: 172.16.3.1
- Subnet Mask: 255.255.255.0
- DNS Server: 192.168.1.100

OSI Model & Packets

7 Layers of the OSI Model

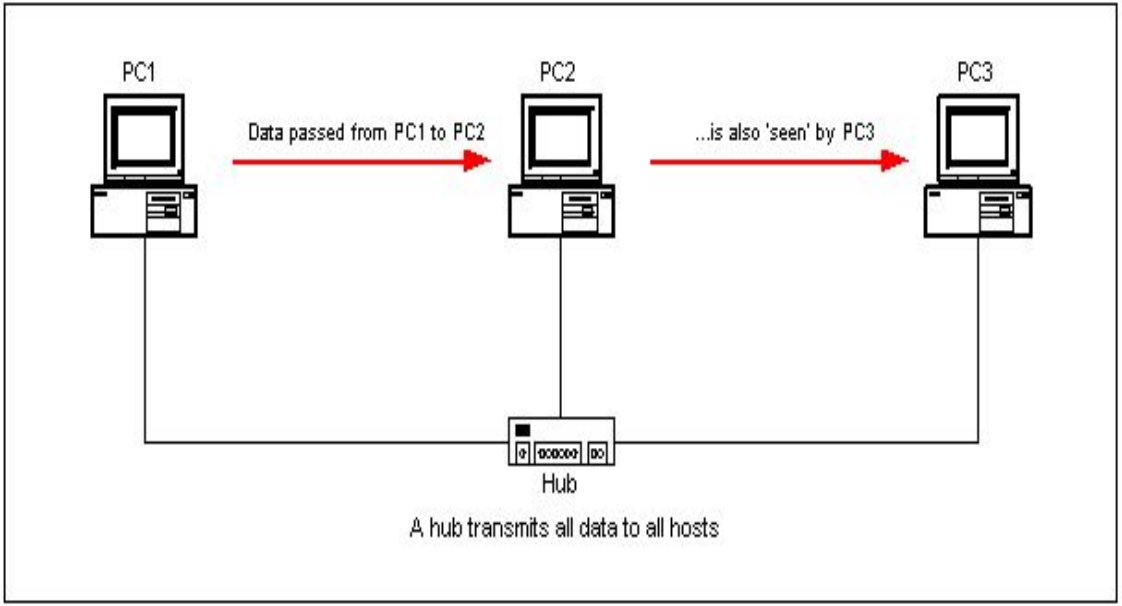
Application	• End User layer • HTTP, FTP, IRC, SSH, DNS
Presentation	• Syntax layer • SSL, SSH, IMAP, FTP, MPEG, JPEG
Session	• Synch & send to port • API's, Sockets, WinSock
Transport	• End-to-end connections • TCP, UDP
Network	• Packets • IP, ICMP, IPSec, IGMP
Data Link	• Frames • Ethernet, PPP, Switch, Bridge
Physical	• Physical structure • Coax, Fiber, Wireless, Hubs, Repeaters

Encapsulation

Network Devices

1. **Switch**
    a. Layer 2 device
    b. Uses Destination MAC Address of the Packet Sent
    c. Uses a MAC table
        i. Maps the MAC Address of the computer to the port it is connected on
2. **Hubs**
    a. Layer 1 Device
    b. Takes the packet sent, Shoves out all ports except the one sent on
3. **Routers**
    a. Layer 3 Device
    b. Holds Default Gateway
    c. Uses Destination IP Address
    d. Uses Routing table to route the Packets to their needed destination
4. **Endpoint devices**
    a. Servers
        i. Tend to serve data for users
        ii. Examples
    b. Computers
        i. Device that you are using

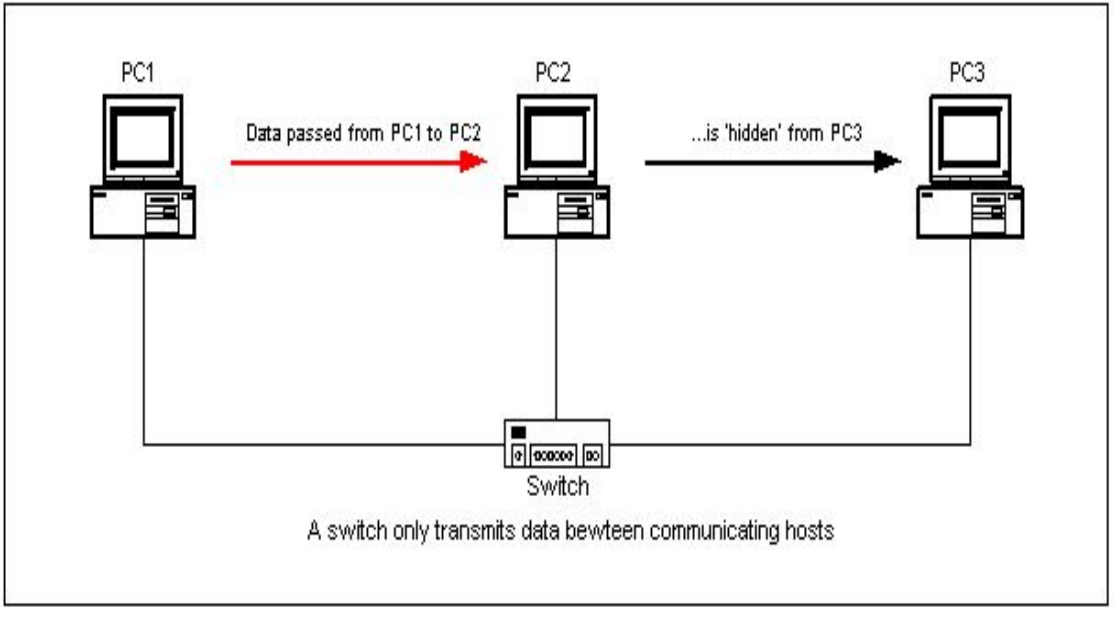
Hub



Layer 1 Device

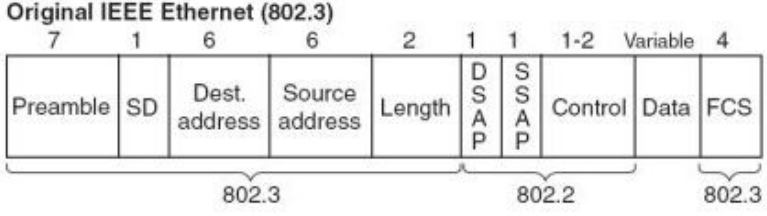
Takes the packet sent, Shoves out all ports except the one sent on

Switch

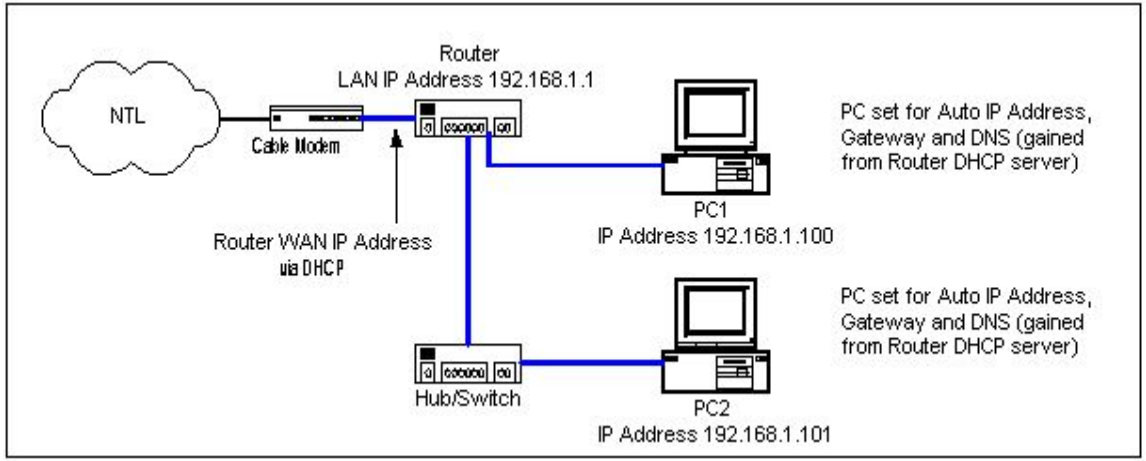


Layer 2 device

1. Uses Destination MAC Address of the Packet Sent
2. Uses a MAC table
   a. Maps the MAC Address of the computer to the port it is connected on



Router



Routers

a. Layer 3 Device
b. Holds Default Gateway
c. Uses Destination IP Address
d. Uses Routing table to route the Packets to their needed destination

Important Network Protocols

User Datagram Protocol (UDP)

- Sends the data and forgets it
- Relies on other sources to fix data loss

Transport Control Protocol (TCP)

- Establishes a channel for communication
- Has established rules
- Three way Handshake

Address Resolution Protocol (ARP)

- Resolves IP Address to MAC Address
- Allows Communication to other Devices

Domain Name Service (DNS)

- Resolves URLs to IP Address
- Allows for using “www.google.com“

Back to Packet Tracer!

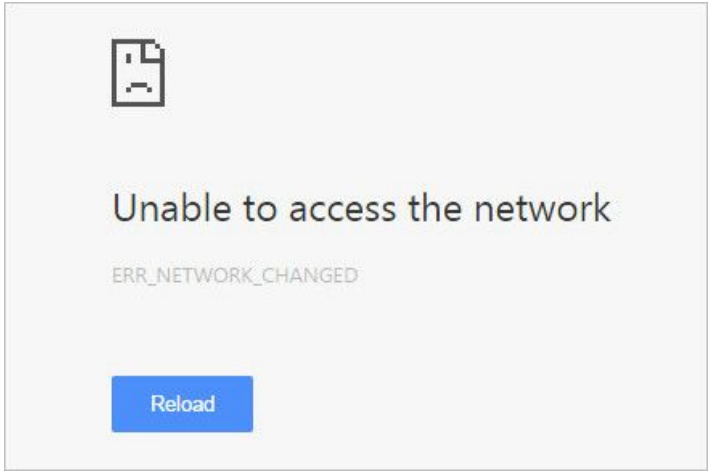
Dealing with Network Errors

How do you usually find them?

- They are reported by co-workers/teammates

Troubleshooting Process

- Ping, Traceroute gather info
- Go Back to the basics
- Move slowly up to more complex Issues



Major CDO Update! (Teaser =)

Cya Next week!

If you have any good memes send them to the email below.

wcsmith@albany.edu

Log Analysis - April 2nd.

Talk to Liam or Eric to Pay for the TShirt!

Follow us on Twitter? Add on myInvolvement?

MyInvolve

Twitter

Discord

https://discord.gg/9Dh6R5R