

802.420

Eddie, Dale, Terence

Overview

- Purpose
- Features
- Design
- Implementation

Purpose

- Ethernet repeater
- Analytics
- Traffic shaping
- Network reliability / diagnostics

Features

- Monitor Traffic Categories / Sources
- Blocking / Throttling / Expediting traffic streams
- Monitor connectivity (ping / bandwidth / fragmentation)
- Detect suspicious port scans (nmap)
- Smarter drop policies
- VGA display - traffic streams and stats
- Keyboard controller to select streams
- Simple Piezo-speakers for notifications

Monitor Traffic

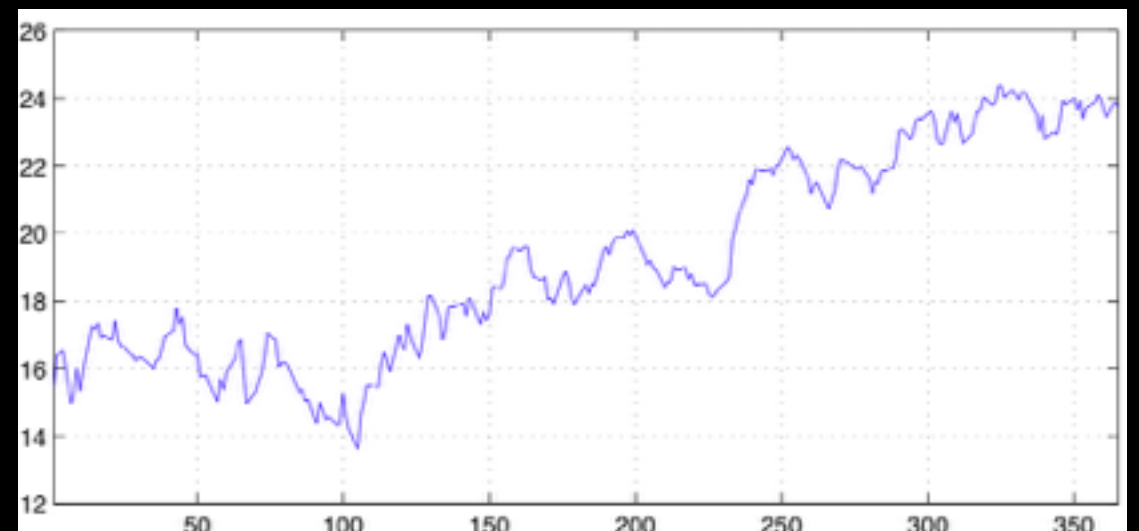
World of Warcraft - 50ms ping

Bandwidth Usage [Mbps]:

Priority - High

Buffer Size - Low

Drop Policy - RED



Blocking / Throttling/ Expediting

North Korean Source

ece545.com

≡ reddit.com

Security

• Welcome to CityPower Grid Rerouting •
Authorized Users only!
New users MUST notify Sys/Ops.
login:

EDIT01 sshnuke
rcr ebx, 1
bsr ecx, ecx
shrd ebx, edi, CL
shrd eax, edx, CL
[nobile]
[nobile]

Port	State	Service
80/tcp	open	http
81/tcp	open	hosts2-ns

10 # nmap -v -ss -O 10.2.2.2
11 Starting nmap V. 2.54BETA25
13 Insufficient responses for TCP sequencing (3), OS detection may be less
13 accurate
14 Interesting ports on 10.2.2.2:
44 (The 1539 ports scanned but not shown below are in state: closed)
51 Port State Service
51 22/tcp open ssh
58 No exact OS matches for host
68
68
24 Nmap run completed -- 1 IP address (1 host up) scanned
50 # sshnuke 10.2.2.2 -rootpw="210N0101"
Connecting to 10.2.2.2:ssh ... successful.
Re Attempting to exploit SSHv1 CRC32 ... successful.
IP Resetting root password to "210N0101".
System open: Access Level <9>
Mn # ssh 10.2.2.2 -l root
root@10.2.2.2's password: █

RTF CONTROL
ACCESS GRANTED

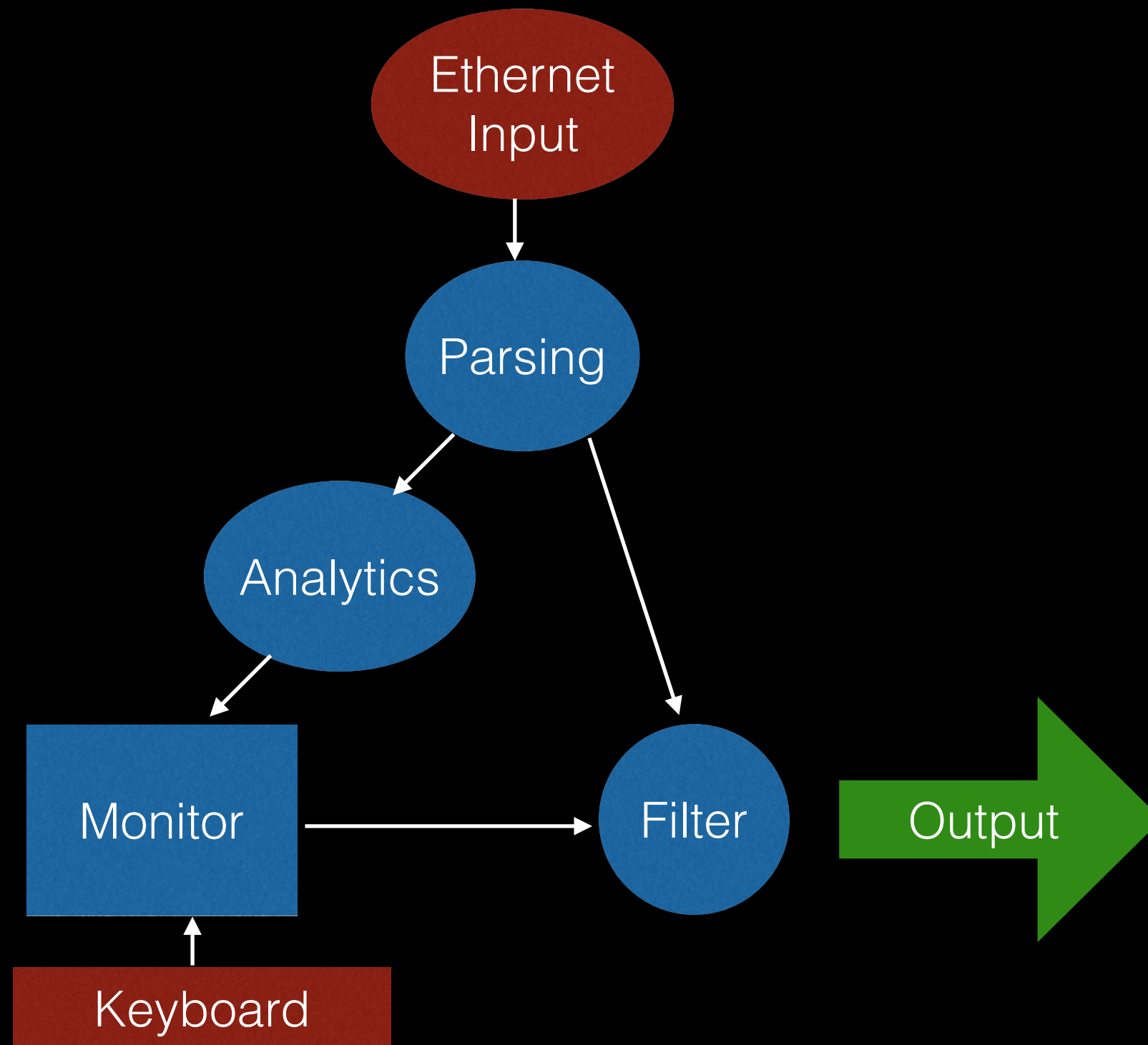
1:501

56

Tail Drop vs RED

Global TCP Synchronization

Design

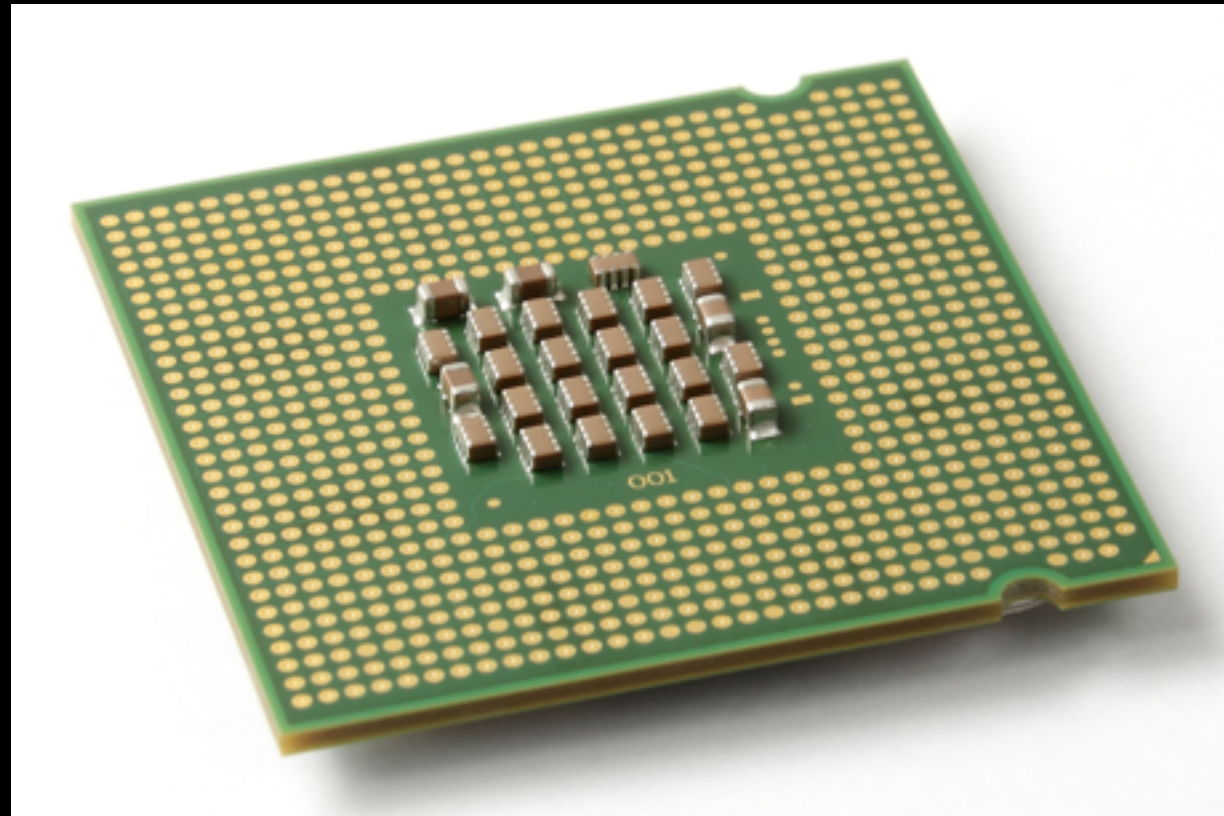


Implementation

802.3 Ethernet packet and frame structure									
Layer	Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interpacket gap
	7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46(42) ^[b] –1500 octets	4 octets	12 octets
Layer 2 Ethernet frame	← 64–1518(1522) octets →								
Layer 1 Ethernet packet	← 72–1526(1530) octets →								

Lex and Parse

Analytics



Filter



Expected Challenges

- Delimiting and parsing packets quickly is non-trivial
- 1 Gbps
- Reconstructing packets

Questions?