Security Vulnerabilities in IEEE-1588 (PTPv2)

William Kluge
William.Kluge1@marist.edu

Casimer DeCusatis
Casimer.DeCusatis@Marist.edu

Paul Wojciak
wojciak@us.ibm.com

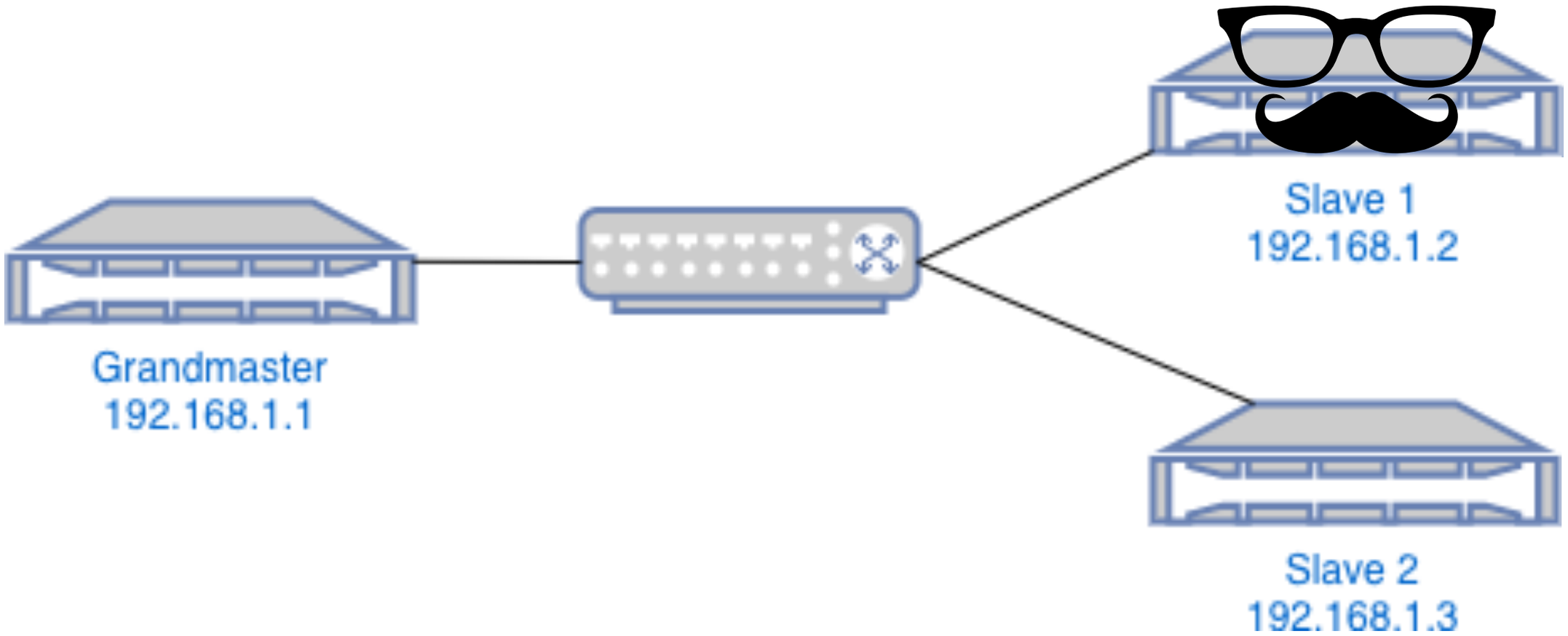
John Houston
jhouston@us.ibm.com

Marist College
School of Computer Science and Mathematics
Poughkeepsie, NY 12601

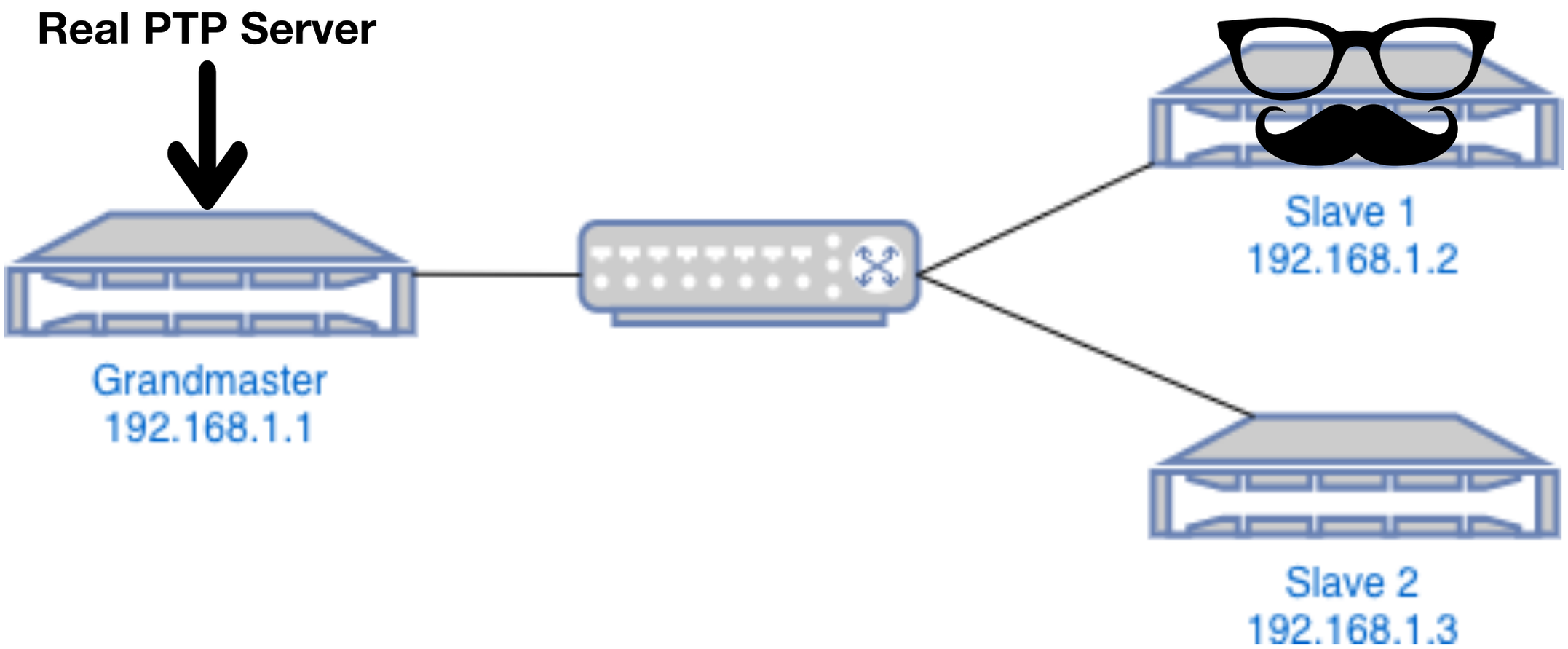
What's the damage?

- **Manipulated bank records**
- **Incorrect access to posts**
- **Falsified logs**

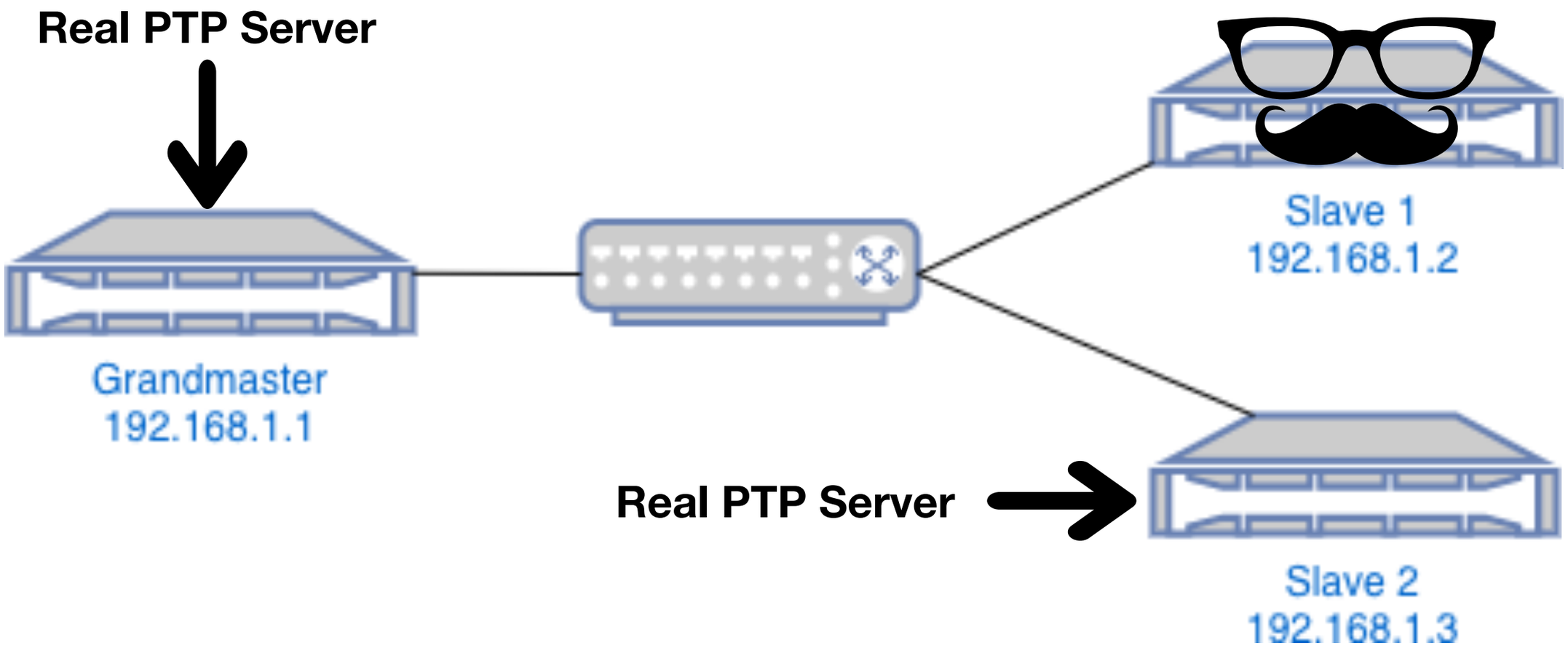
PTP Environment



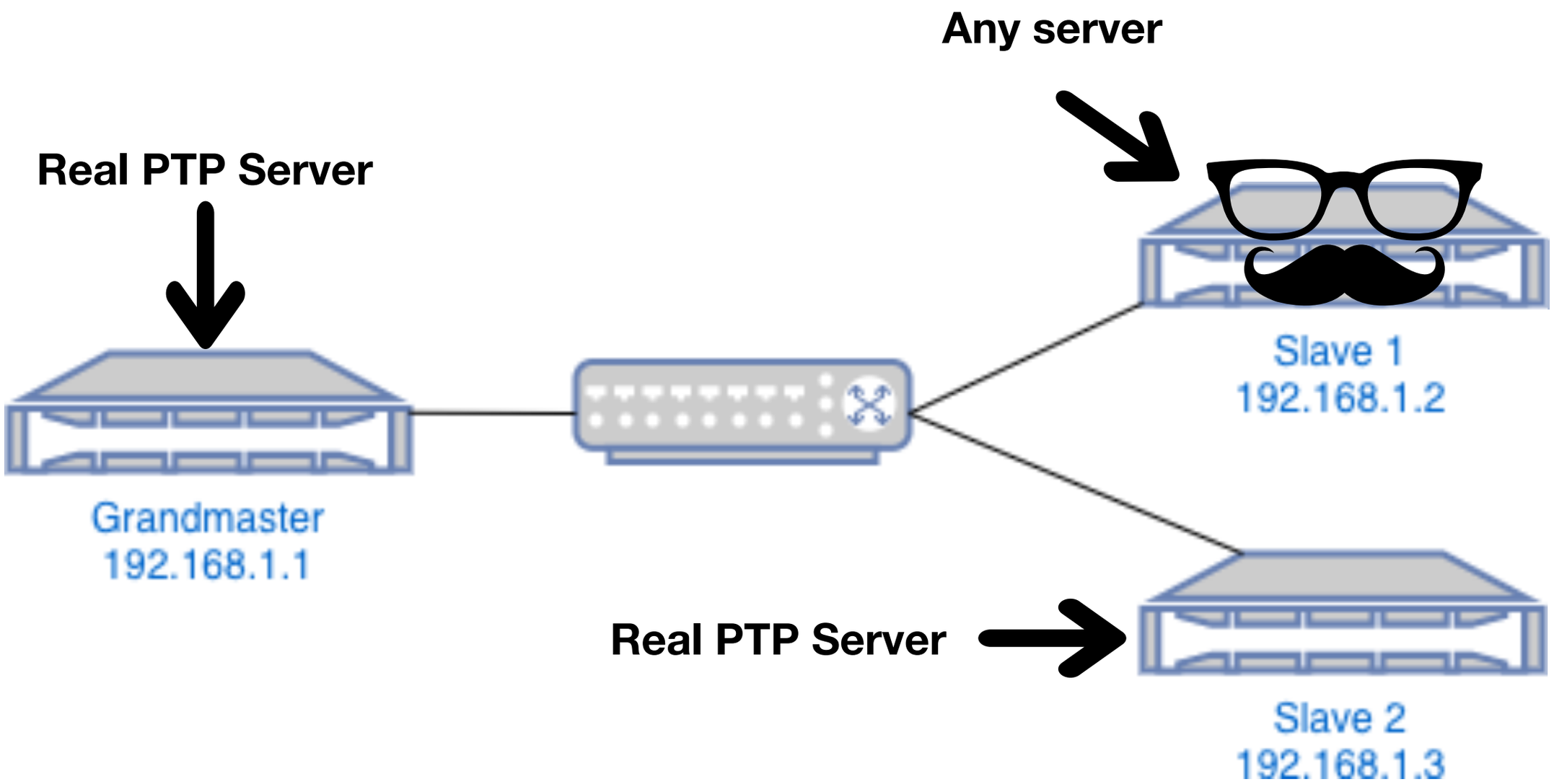
PTP Environment



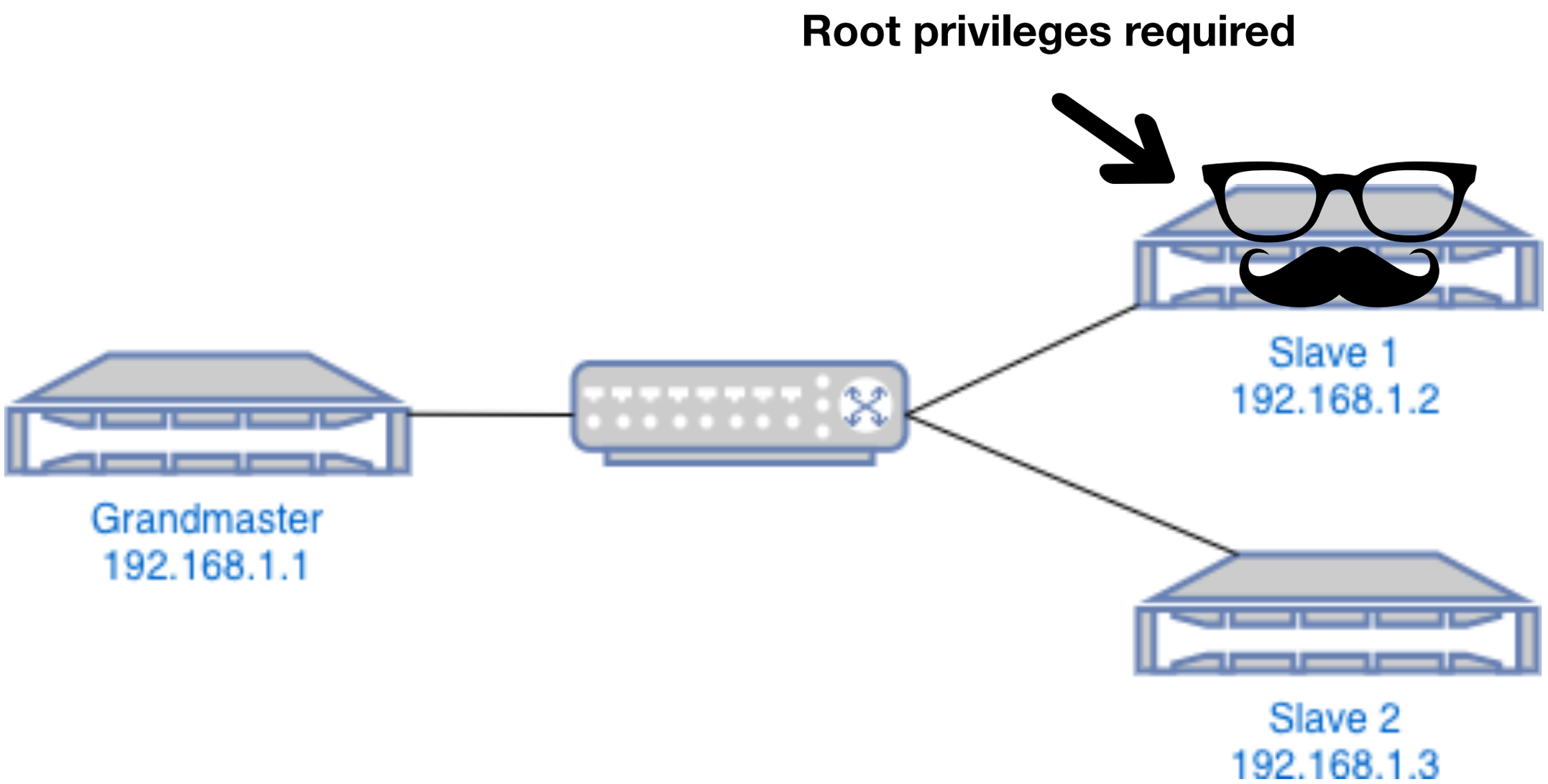
PTP Environment



PTP Environment



PTP Environment

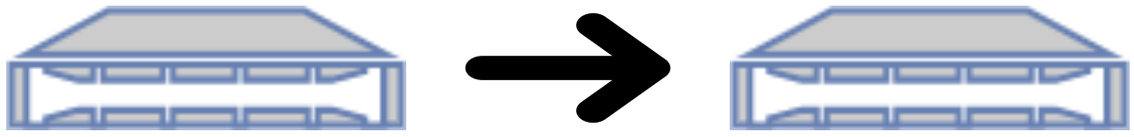


Rouge Slave Software

Python

Scapy

PTP Packets - Announce



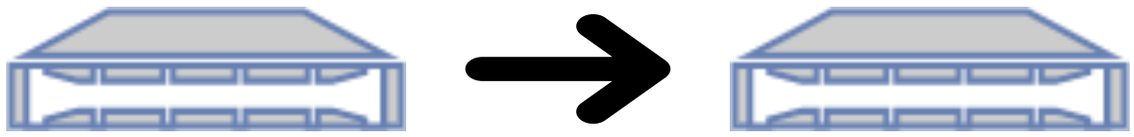
Grandmaster **Slaves**

```
▼ Precision Time Protocol (IEEE1588)
  ▶ 0000 .... = transportSpecific: 0x0
    .... 1011 = messageId: Announce Message (0xb)
    .... 0010 = versionPTP: 2
    messageLength: 64
    subdomainNumber: 0
  ▶ flags: 0x0008
  ▶ correction: 0.000000 nanoseconds
    ClockIdentity: 0xa0369ffffe1f62ac
    SourcePortID: 1
    sequenceId: 865
    control: Other Message (5)
    logMessagePeriod: 1
    originTimestamp (seconds): 0
    originTimestamp (nanoseconds): 0
    originCurrentUTCOffset: 36
    priority1: 0
    grandmasterClockClass: 248
    grandmasterClockAccuracy: Accuracy Unknown (0xfe)
    grandmasterClockVariance: 65535
    priority2: 0
    grandmasterClockIdentity: 0xa0369ffffe1f62ac
    localStepsRemoved: 0
    TimeSource: INTERNAL_OSCILLATOR (0xa0)
```

Accuracy_Unknown
Accurate to within 25 ns
…

INTERNAL_OSCILLATOR
ATOMIC_CLOCK
GPS
…

PTP Packets - Sync and Follow-up

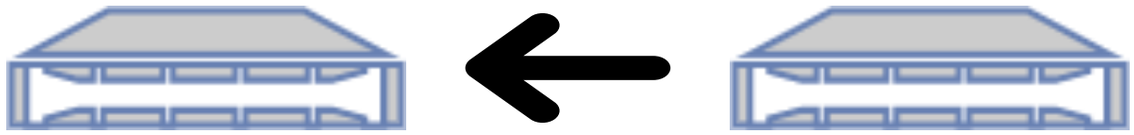


Grandmaster **Slaves**

```
▼ Precision Time Protocol (IEEE1588)
  ▶ 0000 .... = transportSpecific: 0x0
    .... 0000 = messageId: Sync Message (0x0)
    .... 0010 = versionPTP: 2
    messageLength: 44
    subdomainNumber: 0
  ▶ flags: 0x0200
  ▶ correction: 0.000000 nanoseconds
    ClockIdentity: 0xa0369ffffe1f62ac
    SourcePortID: 1
    sequenceId: 36720
    control: Sync Message (0)
    logMessagePeriod: 0
    originTimestamp (seconds): 0
    originTimestamp (nanoseconds): 0
```

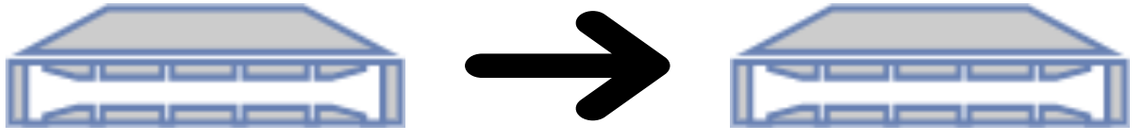
```
▼ Precision Time Protocol (IEEE1588)
  ▶ 0000 .... = transportSpecific: 0x0
    .... 1000 = messageId: Follow_Up Message (0x8)
    .... 0010 = versionPTP: 2
    messageLength: 44
    subdomainNumber: 0
  ▶ flags: 0x0000
  ▶ correction: 3213615.000000 nanoseconds
    ClockIdentity: 0xa0369ffffe1f62ac
    SourcePortID: 1
    sequenceId: 36724
    control: Follow_Up Message (2)
    logMessagePeriod: 0
    preciseOriginTimestamp (seconds): 1538688324
    preciseOriginTimestamp (nanoseconds): 162897187
```

PTP Packets - Delay Request



Grandmaster **Slaves**

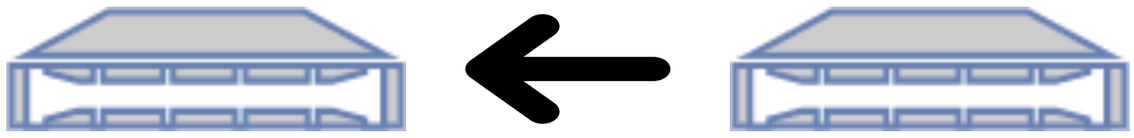
PTP Packets - Delay Response



Grandmaster **Slaves**

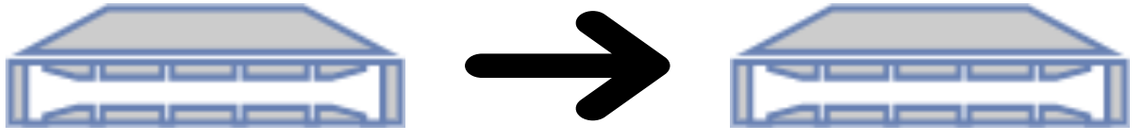
PTP's security does not look at these. They are only for timing.

PTP Packets - Delay Request



Grandmaster **Slaves**

PTP Packets - Delay Response



Grandmaster **Slaves**

PTP's security does not look at these. They are only for timing.

We verified this by spoofing the correct delays.

Typical PTP Interactions

```
192.168.1.1       224.0.1.129       PTPv2       50473   106 Announce Message
192.168.1.1       224.0.1.129       PTPv2       34172    86 Sync Message
192.168.1.1       224.0.1.129       PTPv2       34172    86 Follow_Up Message
192.168.1.1       224.0.1.129       PTPv2       34173    86 Sync Message
192.168.1.1       224.0.1.129       PTPv2       34173    86 Follow_Up Message
192.168.1.3       224.0.1.129       PTPv2          16    86 Delay_Req Message
192.168.1.1       224.0.1.129       PTPv2          16    96 Delay_Resp Message
192.168.1.1       224.0.1.129       PTPv2       50474   106 Announce Message
192.168.1.1       224.0.1.129       PTPv2       34174    86 Sync Message
192.168.1.1       224.0.1.129       PTPv2       34174    86 Follow_Up Message
192.168.1.3       224.0.1.129       PTPv2          17    86 Delay_Req Message
192.168.1.1       224.0.1.129       PTPv2          17    96 Delay_Resp Message
192.168.1.1       224.0.1.129       PTPv2       34175    86 Sync Message
192.168.1.1       224.0.1.129       PTPv2       34175    86 Follow_Up Message
192.168.1.3       224.0.1.129       PTPv2          18    86 Delay_Req Message
192.168.1.1       224.0.1.129       PTPv2          18    96 Delay_Resp Message
```

Source IP

Destination (multicast)

Sequence ID

Message Type

Average Offset: -0.042 ns

Attacks Reviewed

Announce Denial of Service (DoS)

Spam announce packets at the slave.

Master Spoof

Pretend to be the actual grandmaster and send fake data to slaves.

Atomic Master Takeover*

Fake the entire PTP Process as a clock with an atomic time source.

*E. Itkin and A Wool, “A security analysis and revised security extension for the precision time protocol” - same attack, different results

Announce DoS

192.168.1.1	224.0.1.129	PTPv2	63854	106	Announce Message
192.168.1.1	224.0.1.129	PTPv2	55201	106	Announce Message
192.168.1.1	224.0.1.129	PTPv2	55200	106	Announce Message
192.168.1.1	224.0.1.129	PTPv2	55199	106	Announce Message
192.168.1.1	224.0.1.129	PTPv2	55198	106	Announce Message
192.168.1.1	224.0.1.129	PTPv2	55197	106	Announce Message
192.168.1.1	224.0.1.129	PTPv2	55196	106	Announce Message
192.168.1.3	224.0.1.129	PTPv2	3177	86	Delay_Req Message
192.168.1.1	224.0.1.129	PTPv2	55195	106	Announce Message
192.168.1.1	224.0.1.129	PTPv2	55194	106	Announce Message
192.168.1.1	224.0.1.129	PTPv2	55193	106	Announce Message
192.168.1.1	224.0.1.129	PTPv2	55051	106	Announce Message
192.168.1.1	224.0.1.129	PTPv2	55050	106	Announce Message

Spoofed IP

“Valid” Sequence IDs

Average Offset During Attack: 137.8 ms

Average Offset After Attack: -86.1 ms

Announce DoS - Graph

Master Spoof

192.168.1.1	224.0.1.129	PTPv2	9471	106	Announce Message
192.168.1.1	224.0.1.129	PTPv2	13905	86	Sync Message
192.168.1.1	224.0.1.129	PTPv2	13905	86	Follow_Up Message
192.168.1.1	224.0.1.129	PTPv2	13760	86	Sync Message
192.168.1.1	224.0.1.129	PTPv2	13760	86	Follow_Up Message
192.168.1.1	224.0.1.129	PTPv2	9471	106	Announce Message
192.168.1.1	224.0.1.129	PTPv2	13905	86	Sync Message
192.168.1.1	224.0.1.129	PTPv2	13905	86	Follow_Up Message
192.168.1.1	224.0.1.129	PTPv2	13760	86	Sync Message
192.168.1.1	224.0.1.129	PTPv2	13760	86	Follow_Up Message

Spoofed IP

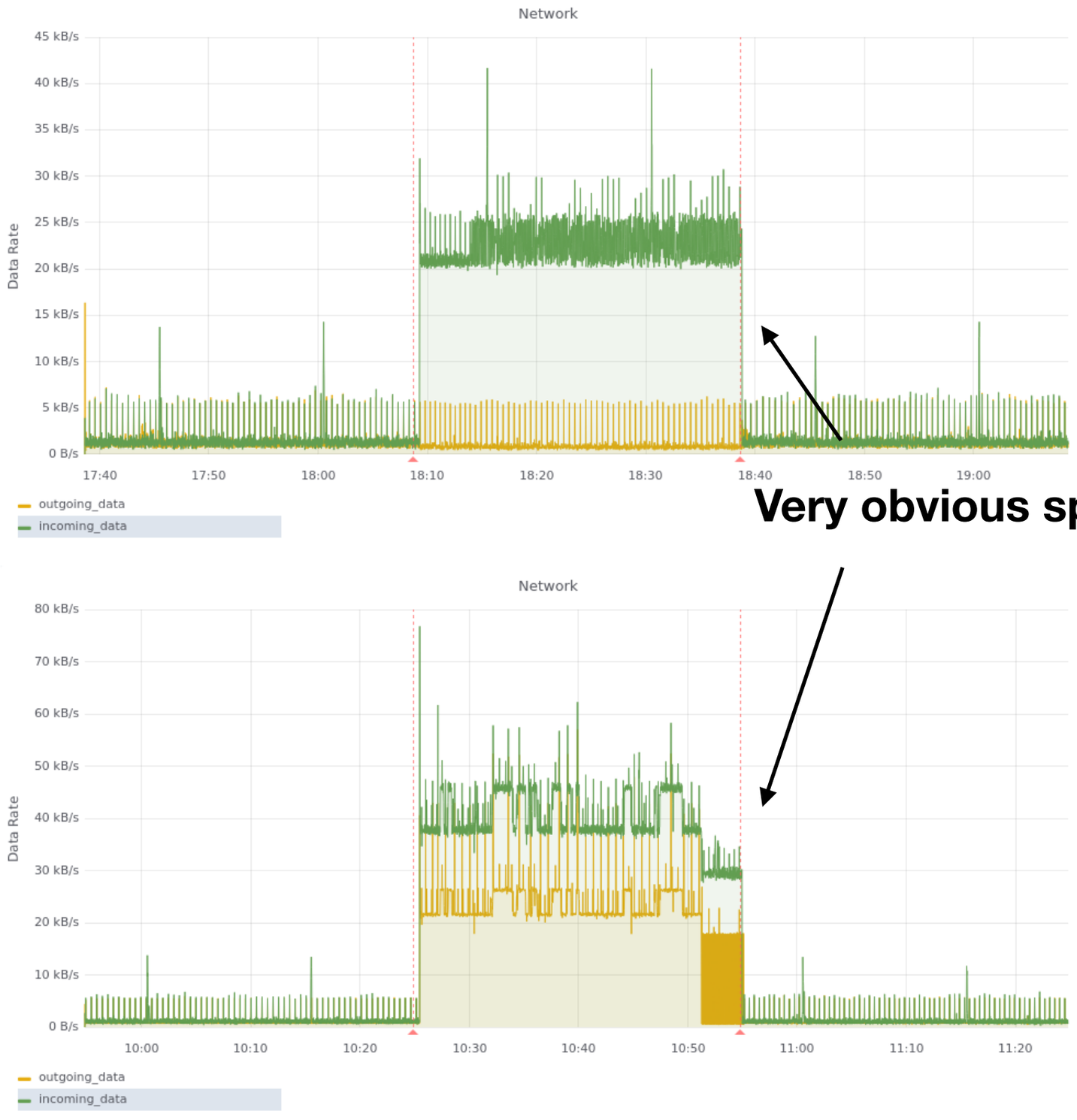
Sequence IDs mimic master

Average Offset During Attack: -23.83 min

Average Offset After Attack: 1330.15 min

Master Spoof - Graph

The Disadvantage of DoS Style Attacks



Very obvious spikes and drops

Atomic Master Takeover

192.168.1.2	224.0.1.129	PTPv2	310	106	Announce Message
192.168.1.2	224.0.1.129	PTPv2	620	86	Sync Message
192.168.1.2	224.0.1.129	PTPv2	620	86	Follow_Up Message
192.168.1.3	224.0.1.129	PTPv2	2437	86	Delay_Req Message
192.168.1.2	224.0.1.129	PTPv2	2437	96	Delay_Resp Message
192.168.1.3	224.0.1.129	PTPv2	2438	86	Delay_Req Message
192.168.1.2	224.0.1.129	PTPv2	2438	96	Delay_Resp Message
192.168.1.2	224.0.1.129	PTPv2	621	86	Sync Message
192.168.1.2	224.0.1.129	PTPv2	621	86	Follow_Up Message
192.168.1.3	224.0.1.129	PTPv2	2439	86	Delay_Req Message
192.168.1.2	224.0.1.129	PTPv2	2439	96	Delay_Resp Message

Slave is communicating with fake master

Full sync sequence

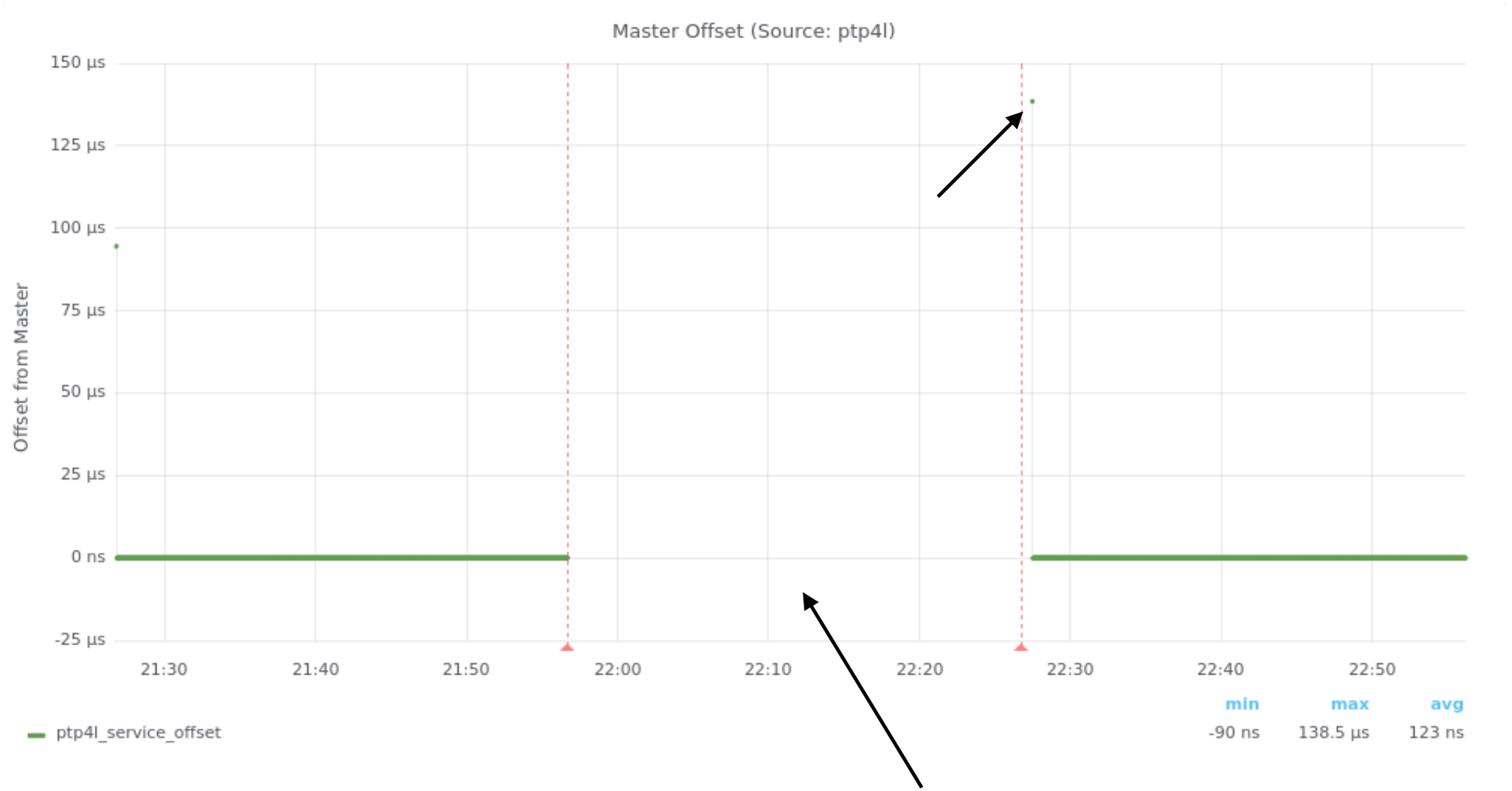
Atomic Master Takeover - The Master Packet

```
▼ Precision Time Protocol (IEEE1588)
  ▶ 0000 .... = transportSpecific: 0x0
    .... 1011 = messageId: Announce Message (0xb)
    .... 0010 = versionPTP: 2
    messageLength: 64
    subdomainNumber: 0
  ▶ flags: 0x0008
  ▶ correction: 0.000000 nanoseconds
    ClockIdentity: 0xa0369ffffe1f6570
    SourcePortID: 1
    sequenceId: 310
    control: Other Message (5)
    logMessagePeriod: 1
    originTimestamp (seconds): 0
    originTimestamp (nanoseconds): 0
    originCurrentUTCOffset: 0
    priority1: 0
    grandmasterClockClass: 248
    grandmasterClockAccuracy: The time is accurate to within 25 ns (0x20)
    grandmasterClockVariance: 65535
    priority2: 0
    grandmasterClockIdentity: 0xa0369ffffe1f6570
    localStepsRemoved: 0
    TimeSource: ATOMIC_CLOCK (0x10)
```

Extremely accurate

Best time source

Atomic Master Takeover - Graph



Average Offset During Attack: N/A

Average Offset After Attack: 148 ns

Acts like packets are being dropped

The Current State of PTP

- Works great in ideal conditions
- Vulnerable
  - Even basic attacks destroy integrity
- Unreliable
  - Not always able to recover
  - Useless log output under stress
- No field verification

What's next?

Research to look forward to:

- Blank Packet DoS
- Directed Atomic Master Takeover