

Case Studies, Lessons Learned

Ing. Tijl Deneut
Researcher XiaK, Ghent University
Lecturer Applied Computer Sciences Howest



Case Study Overview

3 soorten cases

- Troubleshooting
 - “Onze systemen sluiten af, waarom?”
- Implementatie
 - “We willen ons netwerk aanpassen, kan u helpen?”
- Security
 - “Is dit veilig en waarom niet?”

Troubleshooting Case Studies

Usually, we start capturing network data and with the resulting PCAP files, we try to find the problem and provide recommendations

Example Case Studies:

1. Cogeneration (*WKK*) generates false positive messages: alarms were received about emergency buttons pressed that weren't pressed

Presented on 2015-05-07

2. PLC switches to STOP Mode every day because of abnormal large TCP packets being broadcasted

Presented on 2016-03-15

Troubleshooting Case Studies

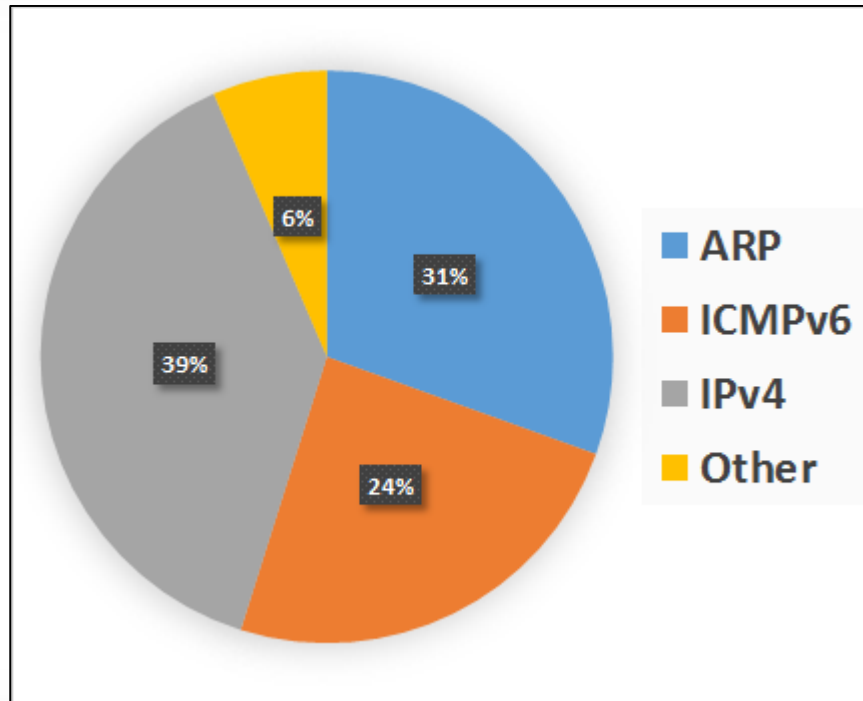
Doorgaans, starten we met het capteren van netwerkdata, met de resulterende PCAP-files onderzoeken we het probleem en geven feedback.

Voorbeelden van Case Studies:

1. Warmtekrachtkoppeling genereert *false positive* berichten: er worden alarmberichten ontvangen betreffende ingedrukte noodstoppen die nooit zijn ingedrukt
Gepresenteerd op GGV van 2015-05-07
2. PLC gaat in STOP Mode op het zelfde moment elke dag, door broadcasts van abnormaal grote TCP pakketten
Gepresenteerd op GGV van 2016-03-15

Lessons Learned Troubleshooting

Een gemeenschappelijke factor was de aanwezigheid van veel onnodig verkeer



Implementatie Case Studies

Het algemene geval: bedrijven die migreren van een bepaalde netwerk lay-out naar een andere.

Naast assistentie, verzorgen we ook datacaptaties **voor** de migratie en vergelijken deze met captaties **na** de migratie.

Voorbeeld Case:

- Migratie van een plat netwerk naar een volledig VLAN'ed netwerk met interVLAN routing

Presented today

Implementatie Case Study

Voestalpine / Sadeef, Bruggesteinweg 220, Hooglede



- Voestalpine (multinational)
- SadeF (lokale vestiging)

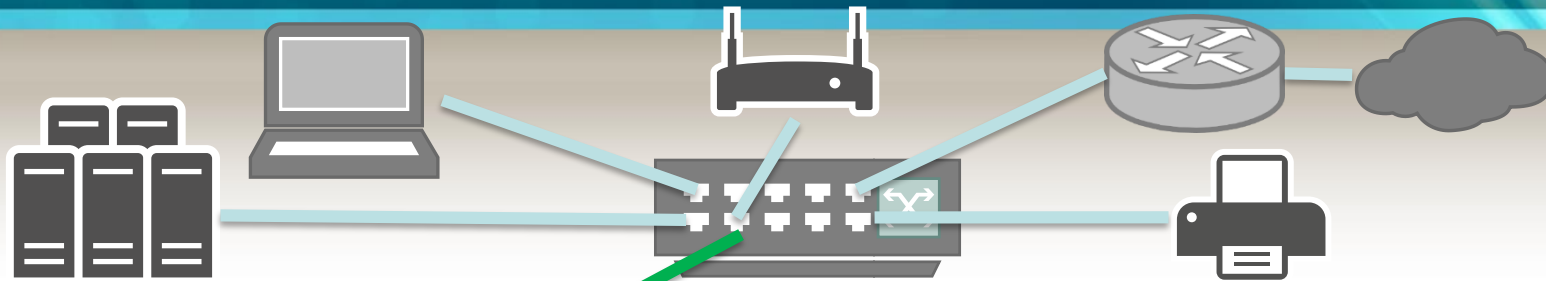
- Middelgrote tot grote onderneming
 - 552 werknemers (2015) in SadeF alleen
 - 48500 werknemers in de Voestalpine Group
- Pure metaalbewerking, in de brede zin van de betekenis:
 - Fietsbruggen, auto-onderdelen, zonne-energie installaties, vloeren, poorten ...

Netwerk Lay-Out Pre Migratie

- Zeer gelijkaardig aan dat van het FicTile demobedrijf: een grotendeels plat netwerk.
 - Dit houdt in: elk toestel kan rechtstreeks communiceren met elk ander toestel. Zonder bescherming.
- Routers waren niet toegelaten door de IT dienst
- Het 'management' van de IP adressen gebeurde op één Excel sheet.

Concreet, migratie van dit:

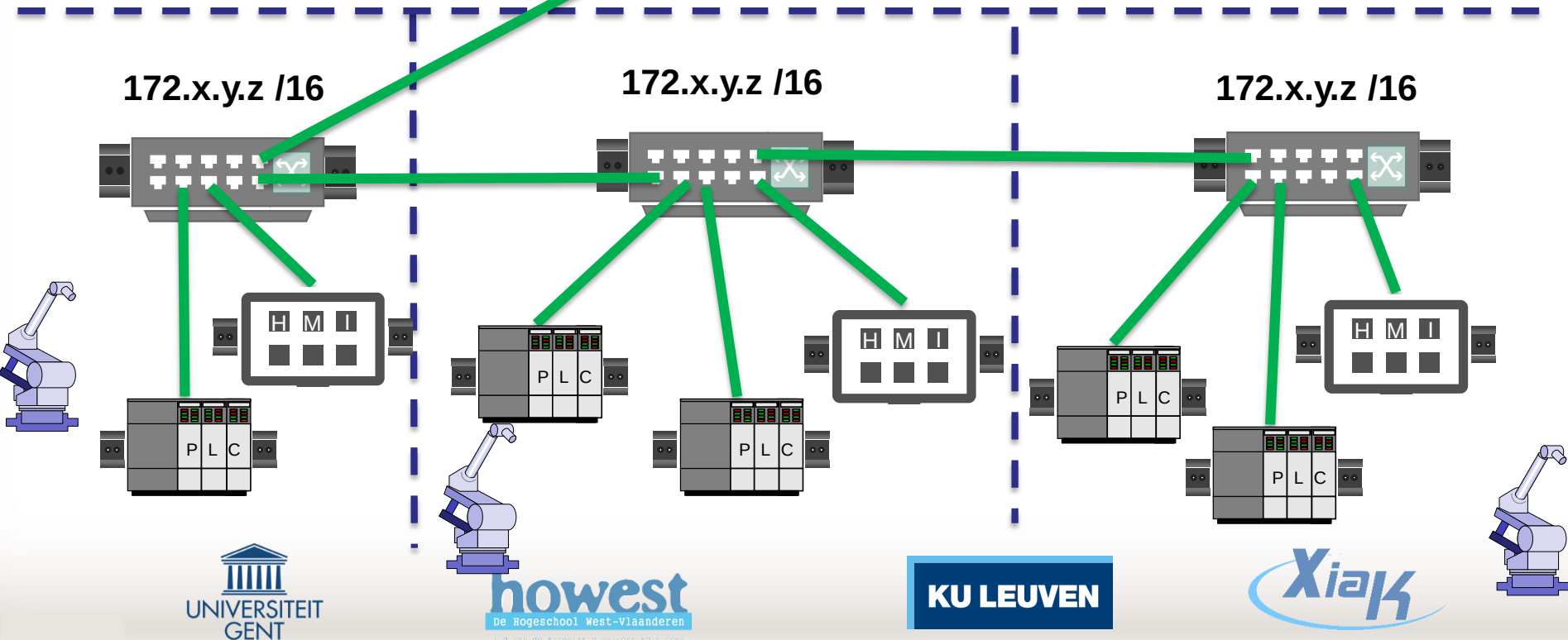
Office / datacenter



172.x.y.z /16

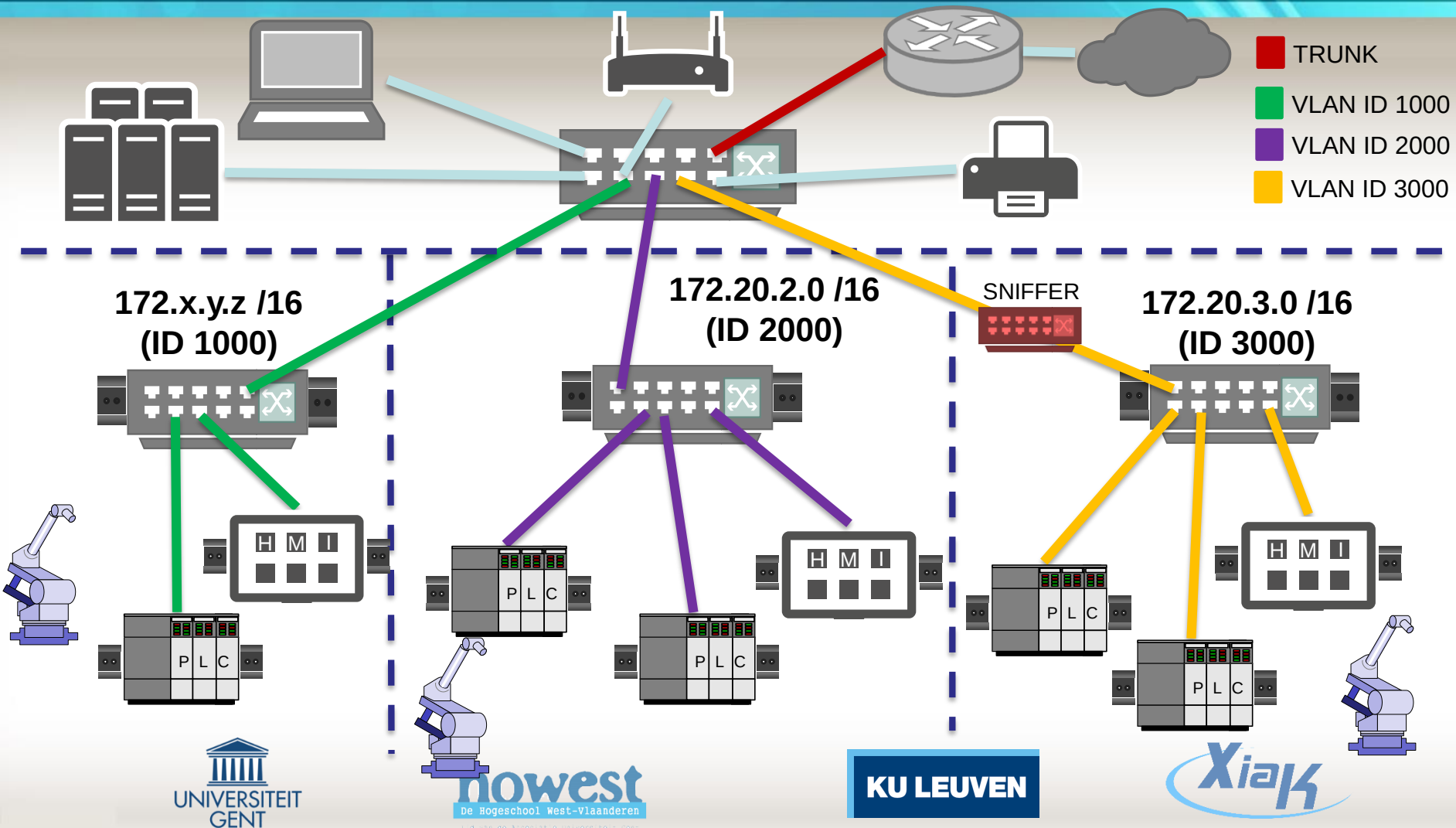
172.x.y.z /16

172.x.y.z /16



Naar dit:

Office / datacenter



Verzamelde (ruwe) data

Statistieken i.v.m. data verzameld aan de **ingang** van één (grote) machine over een periode van **exact** 24 uur

- 90% daling in totale aantal pakketten
- 90.2% daling in gemiddeld aantal pakketten/sec
- 207.9% stijging in gemiddelde pakketgrootte, met als gevolg een betere netwerk I/O
- 69.7% daling in gemiddeld gebruikte bandbreedte
- 75.7% daling in grootte van de ARP tabellen
- 99.4% daling in aantal broadcast pakketten

Lessons Learned

Segmentatie Resultaten

