Securing & Future Proofing OT/IT Environments

ATS GROEP

Powered by experience,
driven by passion

a member of luminus

Agenda

- 09h30 - 09h40 - Welkom & Introductie
- 09h40 - 10h20 - Evolutie IT
- 10h20 - 10h50 - Pauze
- 10h50 - 11h00 - Evolutie OT
- 11h00 - 11h20 - NIS2 - Waarom-Wie-Wat
- 11h20 - 11h45 - NIST Framework
- 11h45 - 12h30 - Claroty Demo
- 12h30 - Slotwoord & Lunch met vragen

Welkom - Waarom

- **NIS2**
- Verouderde Topologie/Technologie
- Meer geconnecteerd richting IT / Cloud
- Cyberaanvallen / Lokale resistentie
- Wat kunnen ATS / APS / Claroty betekenen

Welkom - Termen

- IT Information Technology (administratie/printers/ERP)
- OT Operational Technology (PLC/Scada/MES)
- NIS Network and information systems

Welkom - Wie

APS

BU Automation

CLAROTY

Welkom - APS

- Fiber / Koper
- Actieve / Passieve IT componenten
- IT Monitoring / Management / Protection software

Welkom - ATS NV – BU Automation

- Actieve OT componenten
- OT Infrastructure
- OT Monitoring / Management / Protection software

BU Automation

Welkom - Claroty

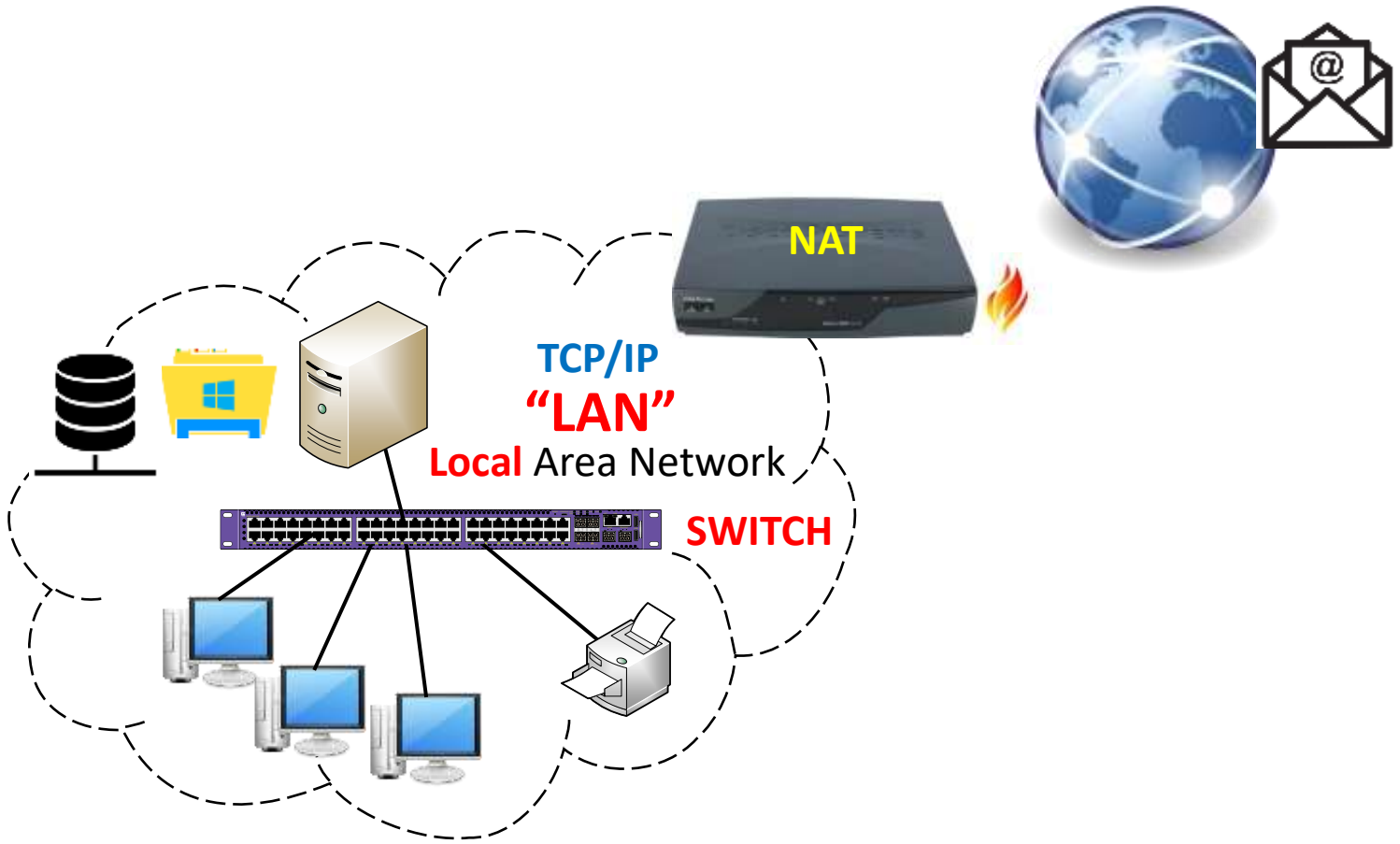
- CTD - Continuous Thread Detection
- SRA - Secure Remote Access

Welkom - APS

Marnix Snijers

Manager Technical IT Services

marnix.snijers@aps.be



Local Area Network

IEEE 802.3

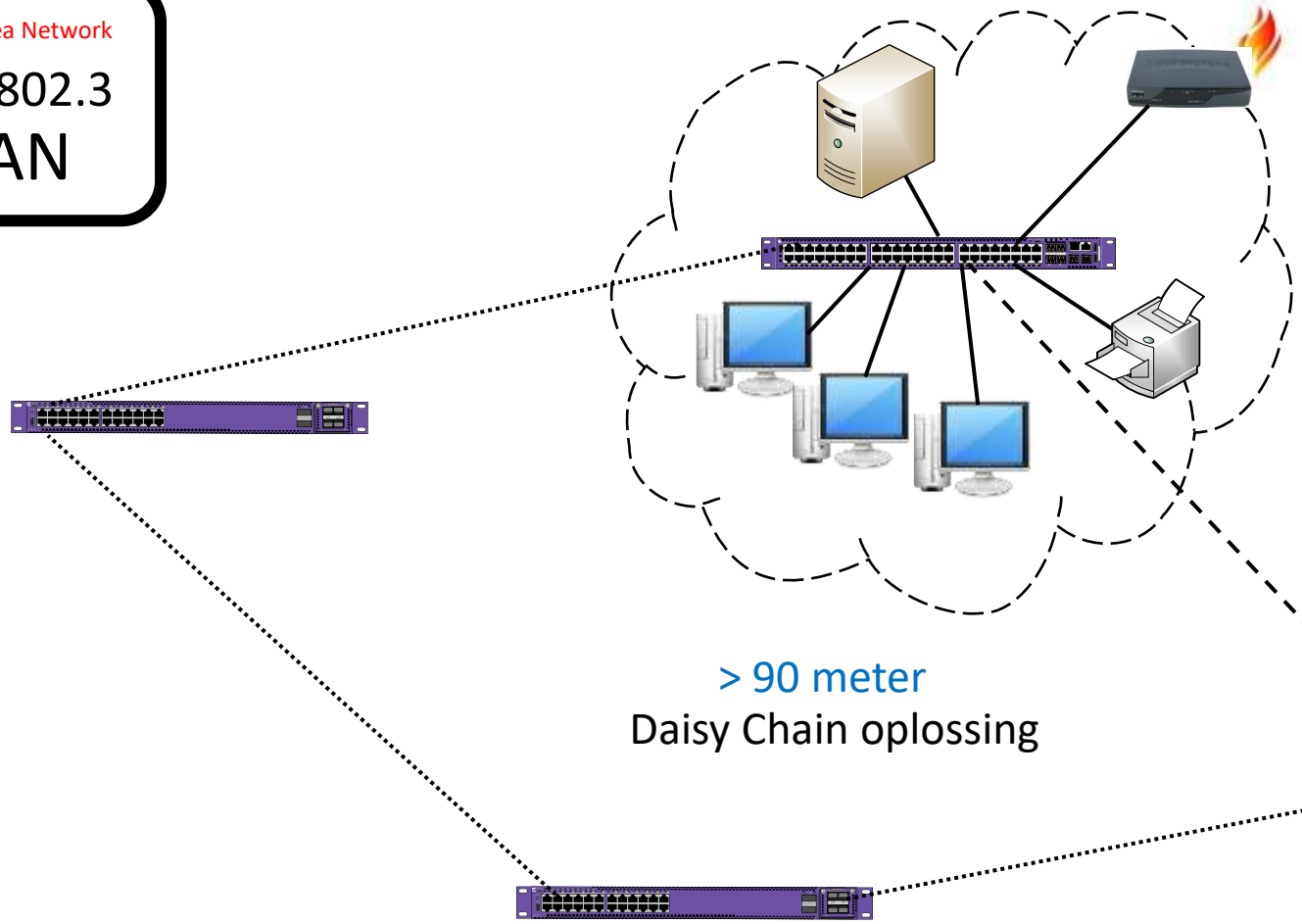
LAN

IT De eerste uitbreidingen - Extra netwerknoden steken de kop op …

Local Area Network

IEEE 802.3

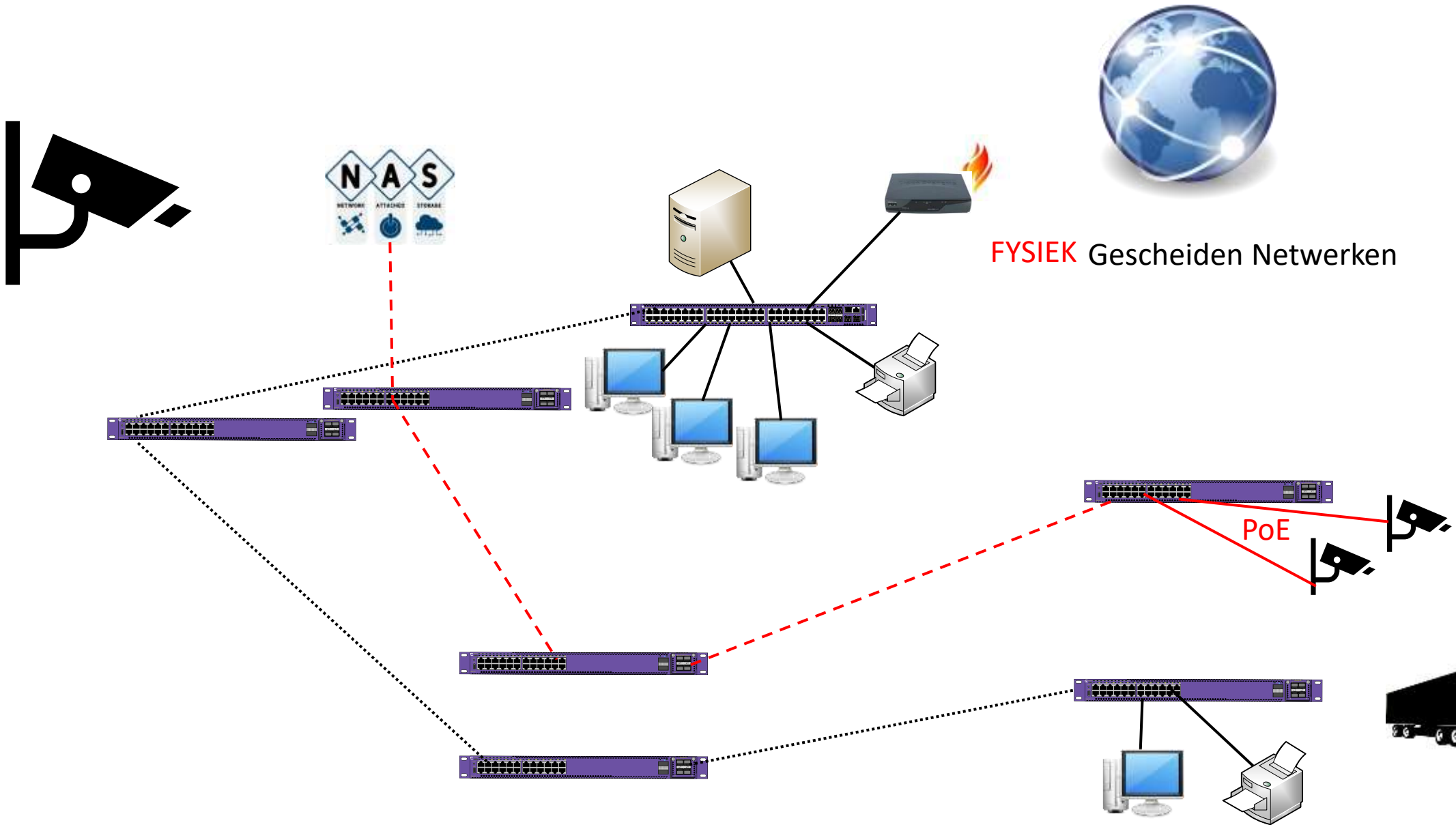
LAN



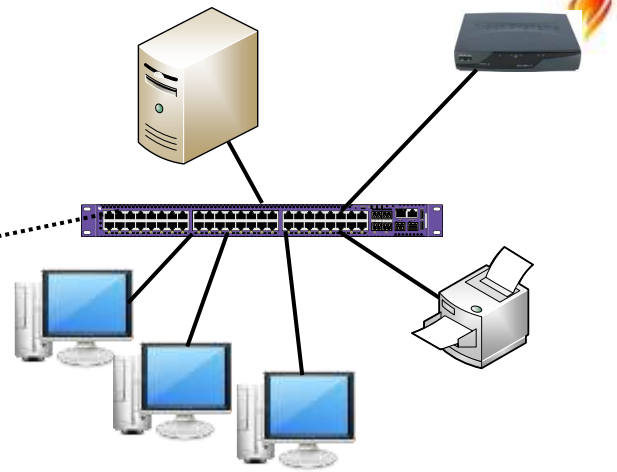
> 90 meter

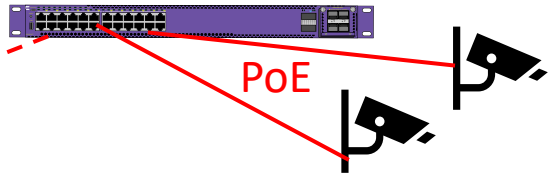
Daisy Chain oplossing

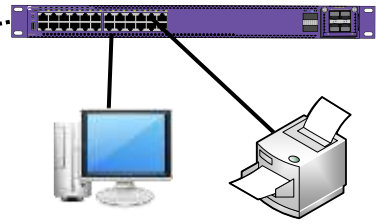
Camera’s … maar niet samen - Gescheiden netwerken … Over multiple Hardware



IT Wifi noden & challenges - Een verdere opdeling blijkt noodzakelijk







Nood aan
Gescheiden
Netwerken
over zelfde
infrastructuur

Challenges

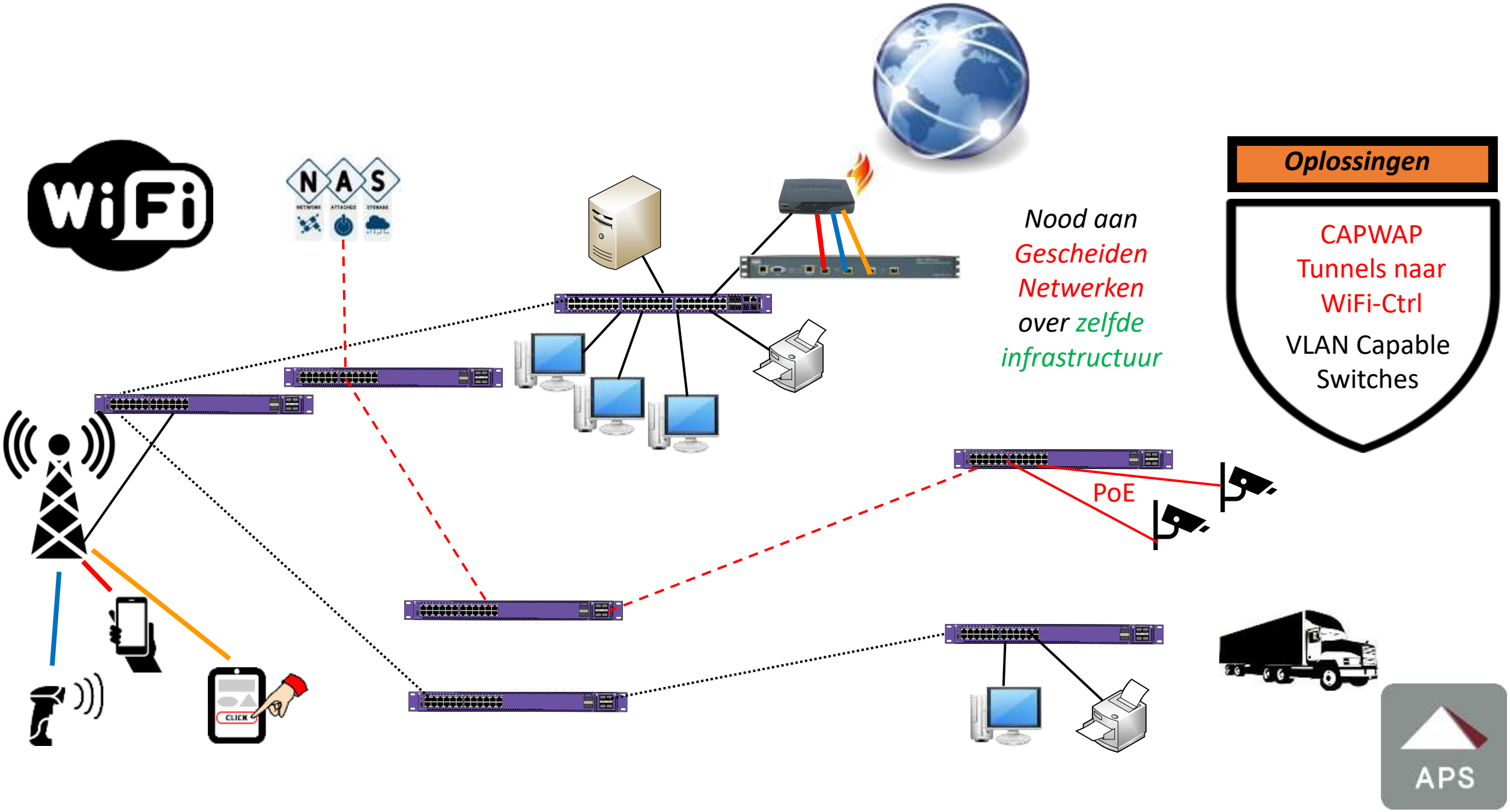
Guest Access

Picking Scanners

Tablets TD

APS

IT Wifi noden & challenges - Een verdere opdeling blijkt noodzakelijk



Nood aan
Gescheiden
Netwerken
over zelfde
infrastructuur

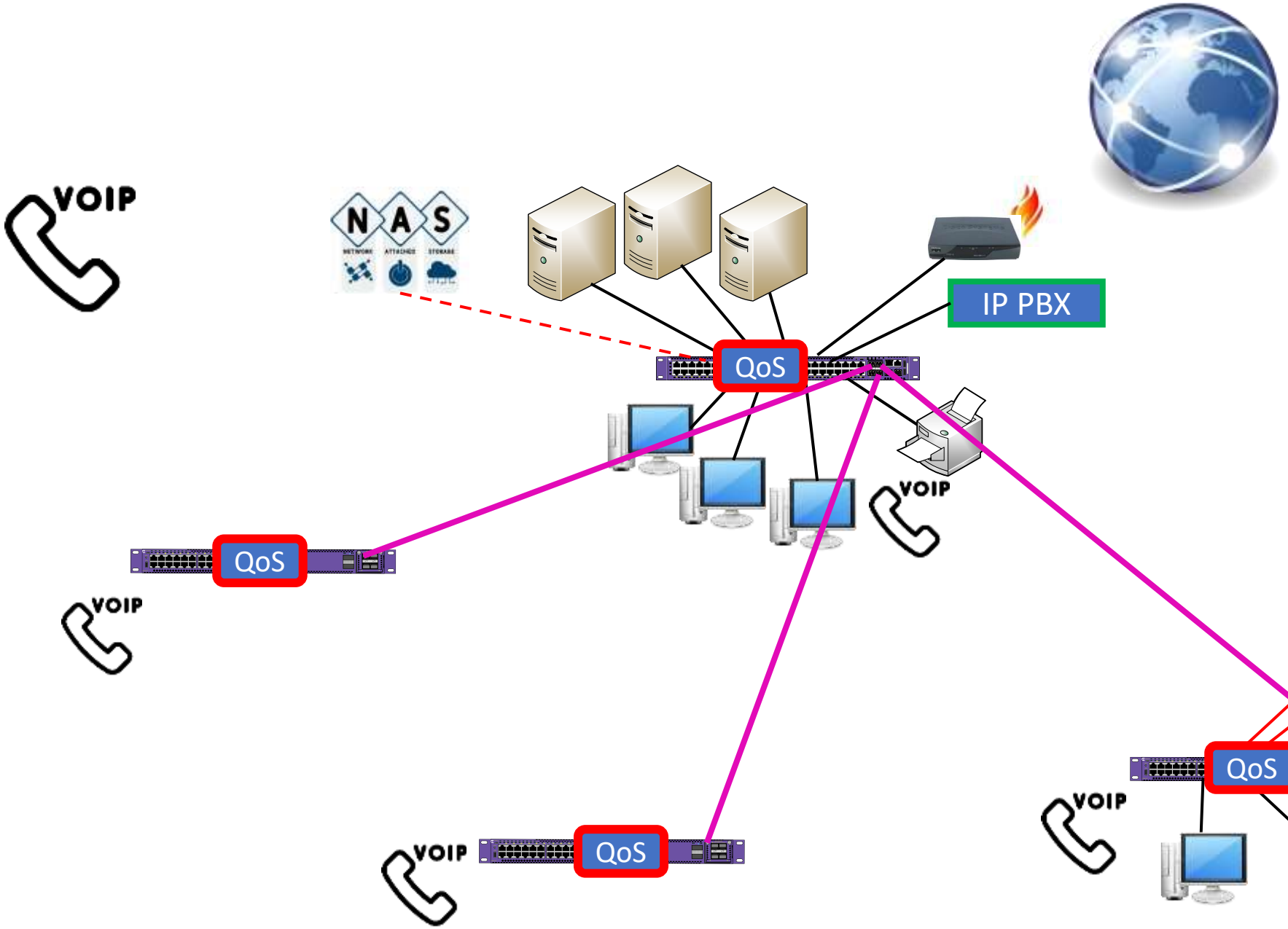
Oplossingen

CAPWAP
Tunnels naar
WiFi-Ctrl

VLAN Capable
Switches

APS

VoIP … veeleisender voor het LAN - Need for Speed – meer convergentie



Daisy Chain -> Ster netwerk

Koper -> Fiber Uplinks

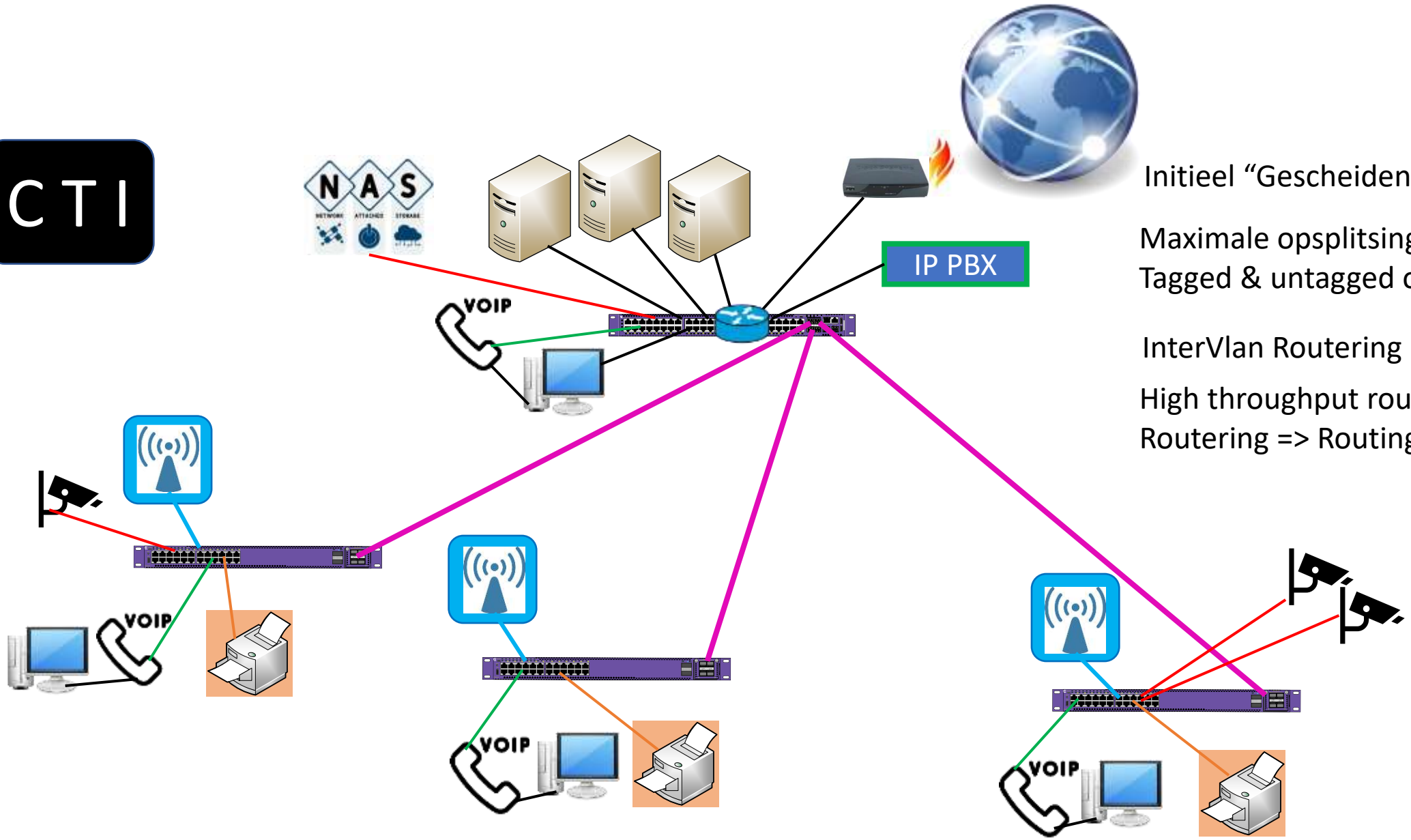
VLANs voor scheiding

VoIP -> QoS

Meer Servers -> meer bandbreedte

APS

CTI



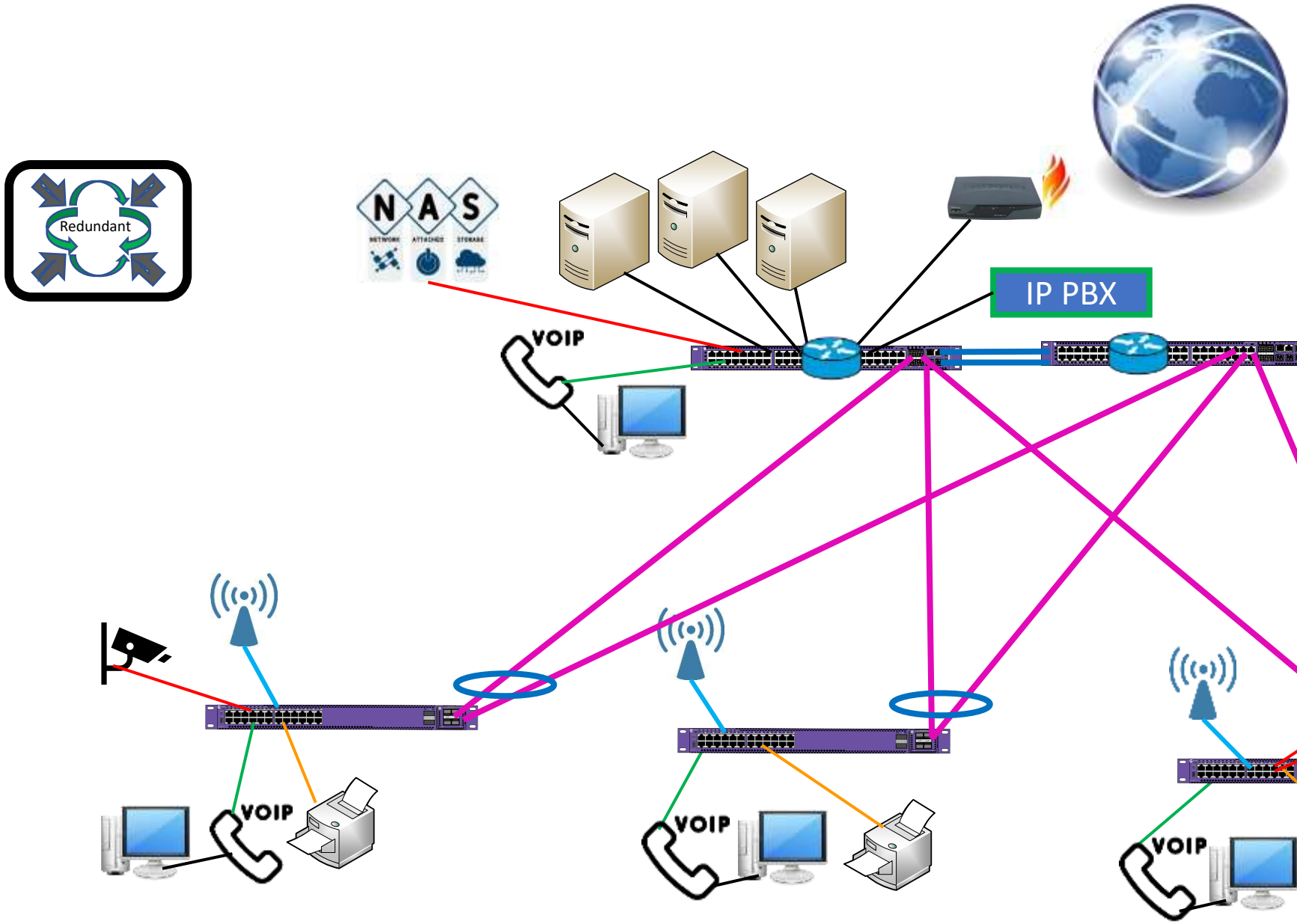
Initieel “Gescheiden” netwerken …

Maximale opsplitsing in (V)LANs
Tagged & untagged over één poort

InterVlan Routering => Firewall

High throughput routering nodig
Routering => Routing switches

“Always ON” networking - Vermijden van Single points of failure … by design



Bouwen van dubbele (up)linken

Ontdubbelen van routing core(s)

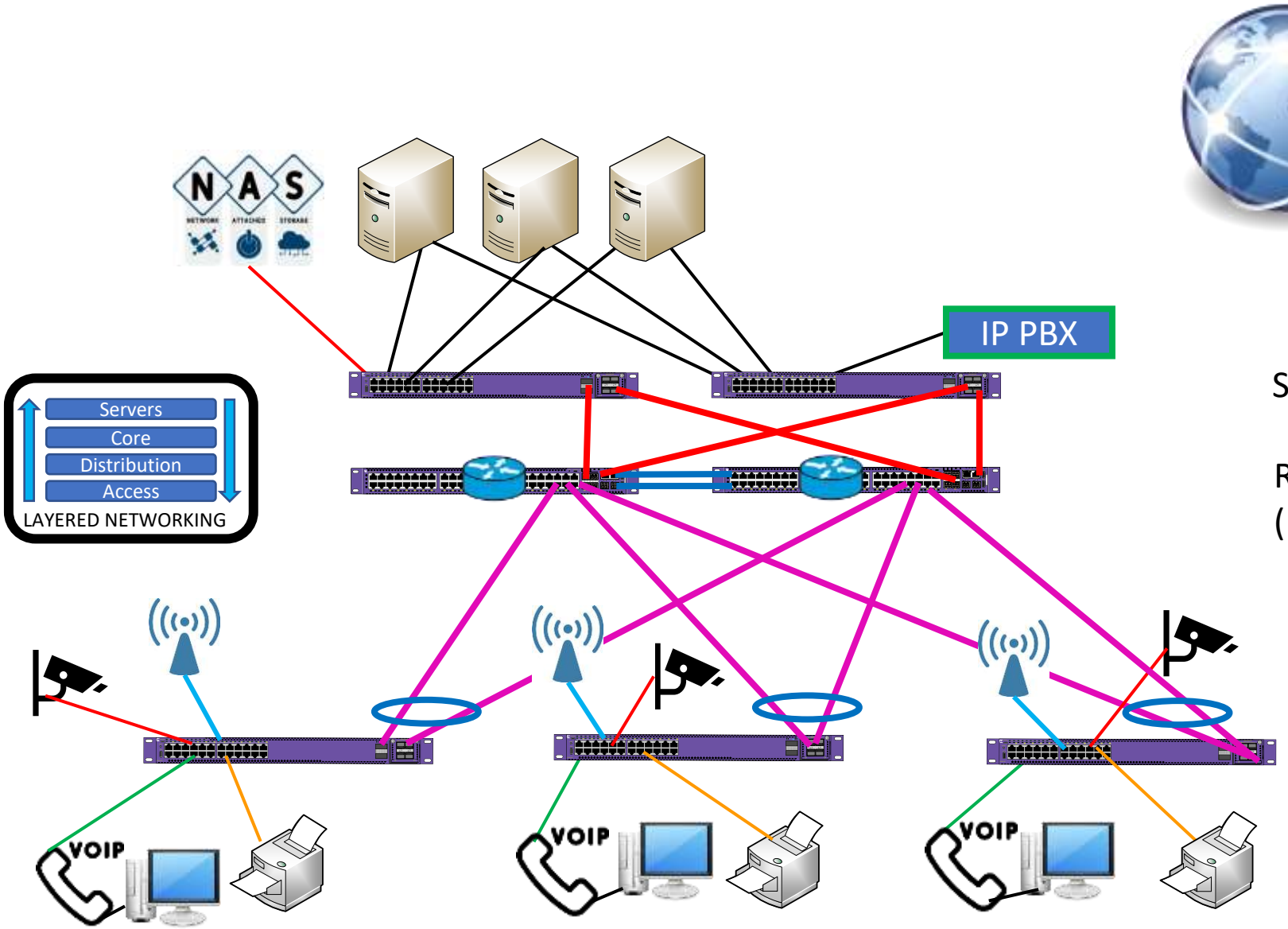
Virtuele Cluster Core(s)

Active-active uplinks

Active-active routers

APS

“Noord – Zuid” communicatie - Layered networking



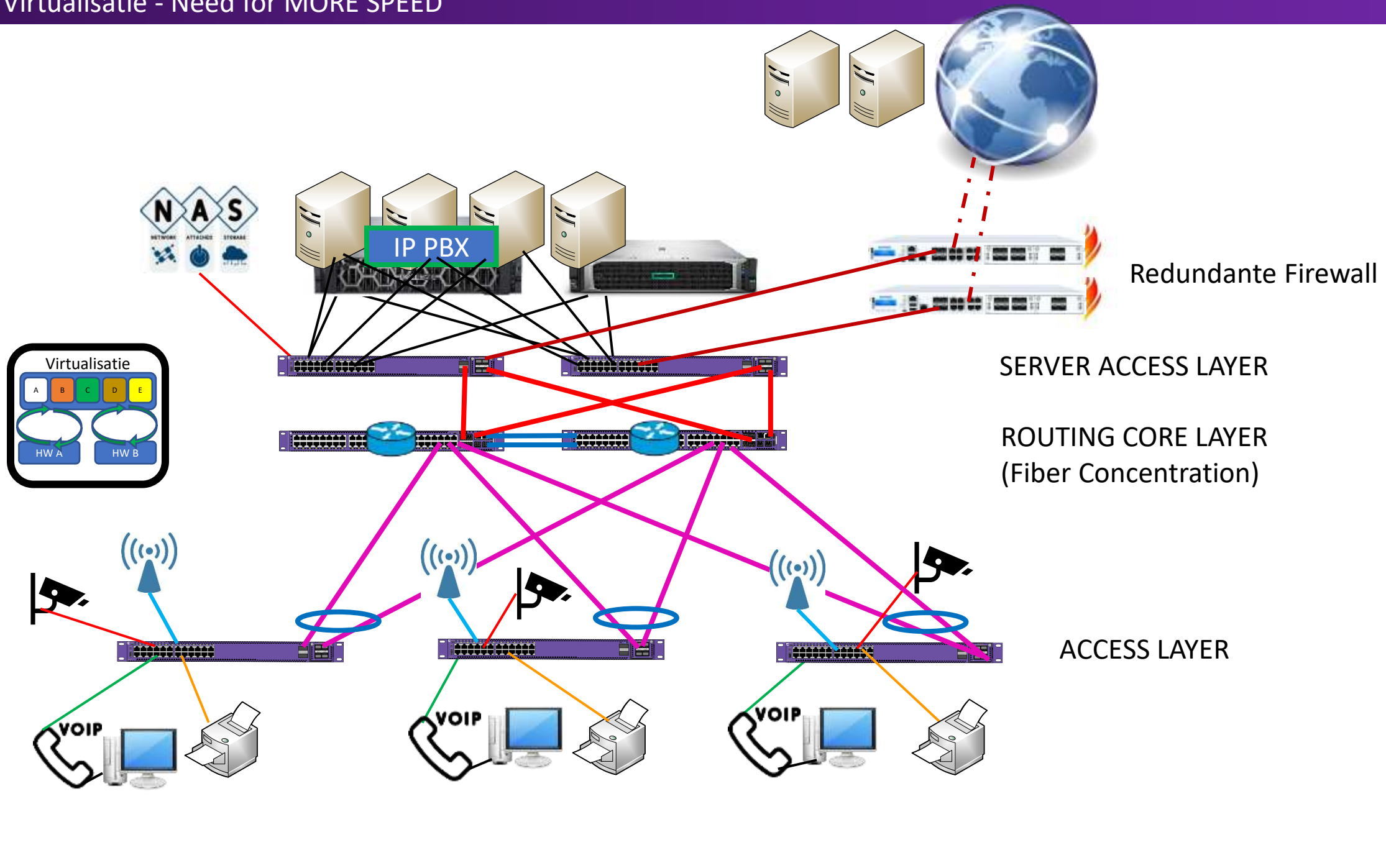
SERVER ACCESS LAYER

ROUTING CORE LAYER
(Fiber Concentration)

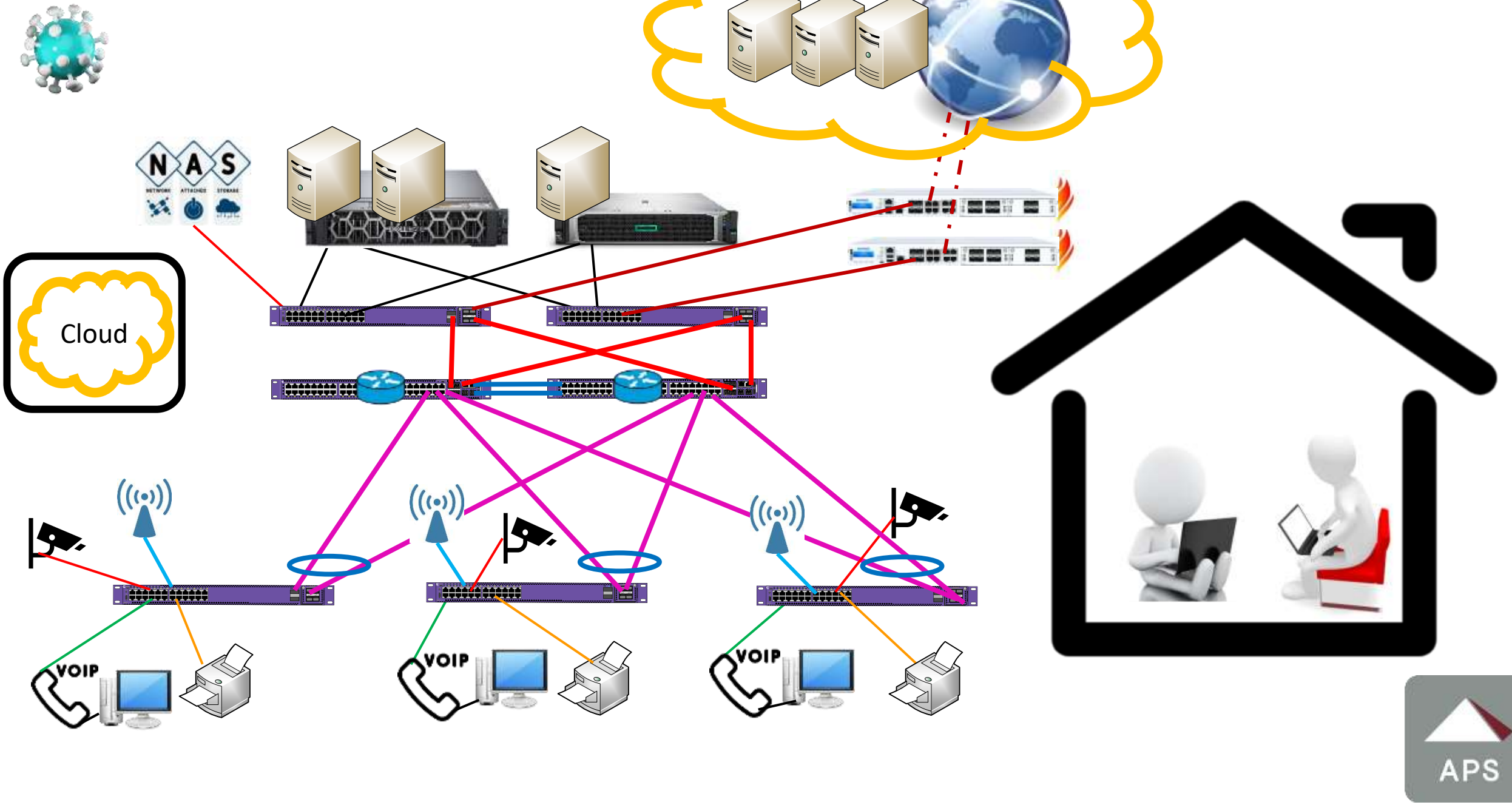
ACCESS LAYER

Security features
Multicast
VLANs
PoE
FO uplinks
10/100/1000
Multirate 2,5/5/10G

Virtualisatie - Need for MORE SPEED



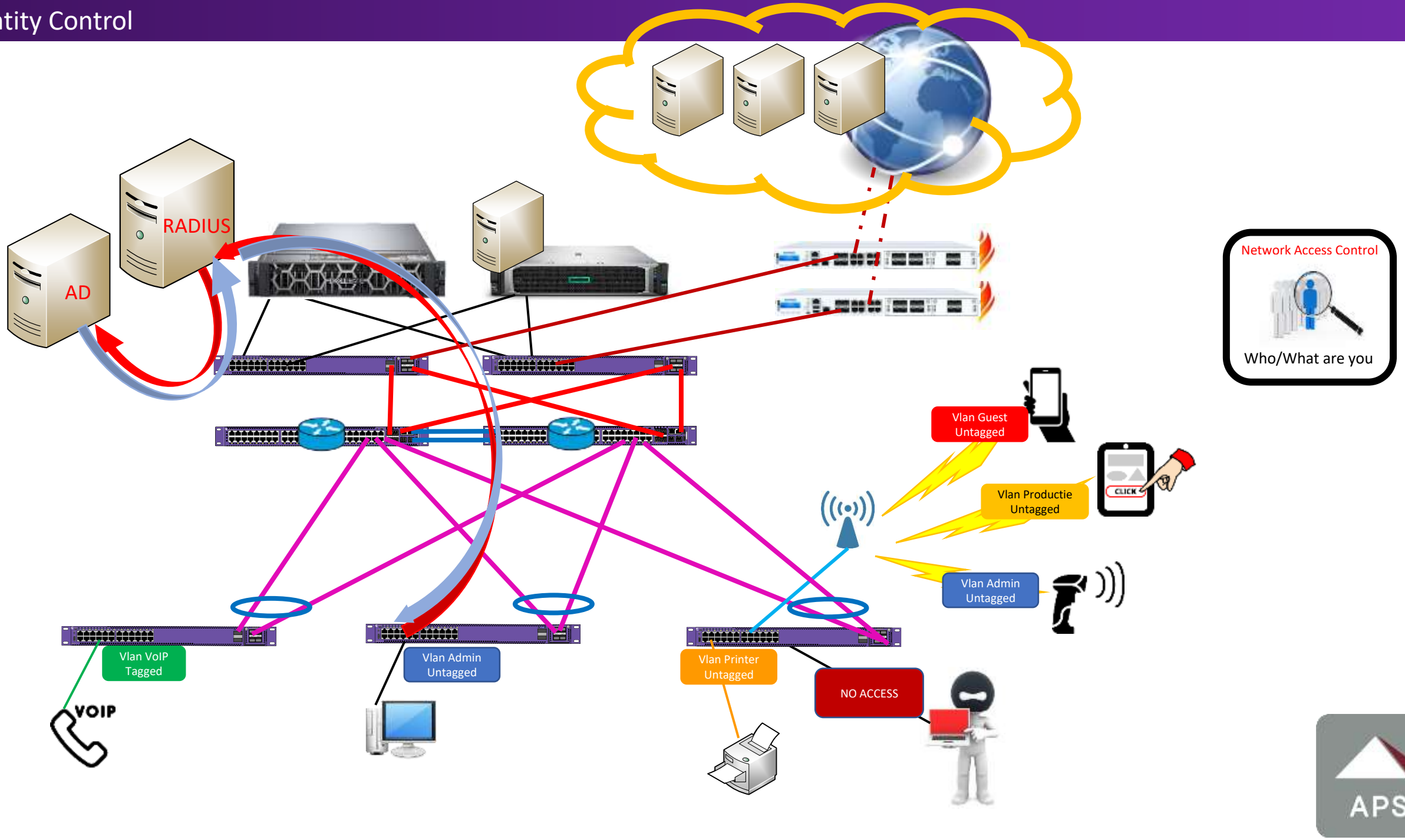
Covid19… => Versnelde Cloud Migratie



Network Access Control

Who/What are you ?

Identity Control



NAC… evolueert naar SDN - Automatisatie op basis van Authenticatie

Network Access Control

Who/What are you

Software Defined Networking

SDN

Where do you belong ?

Software Defined Networking

SDN

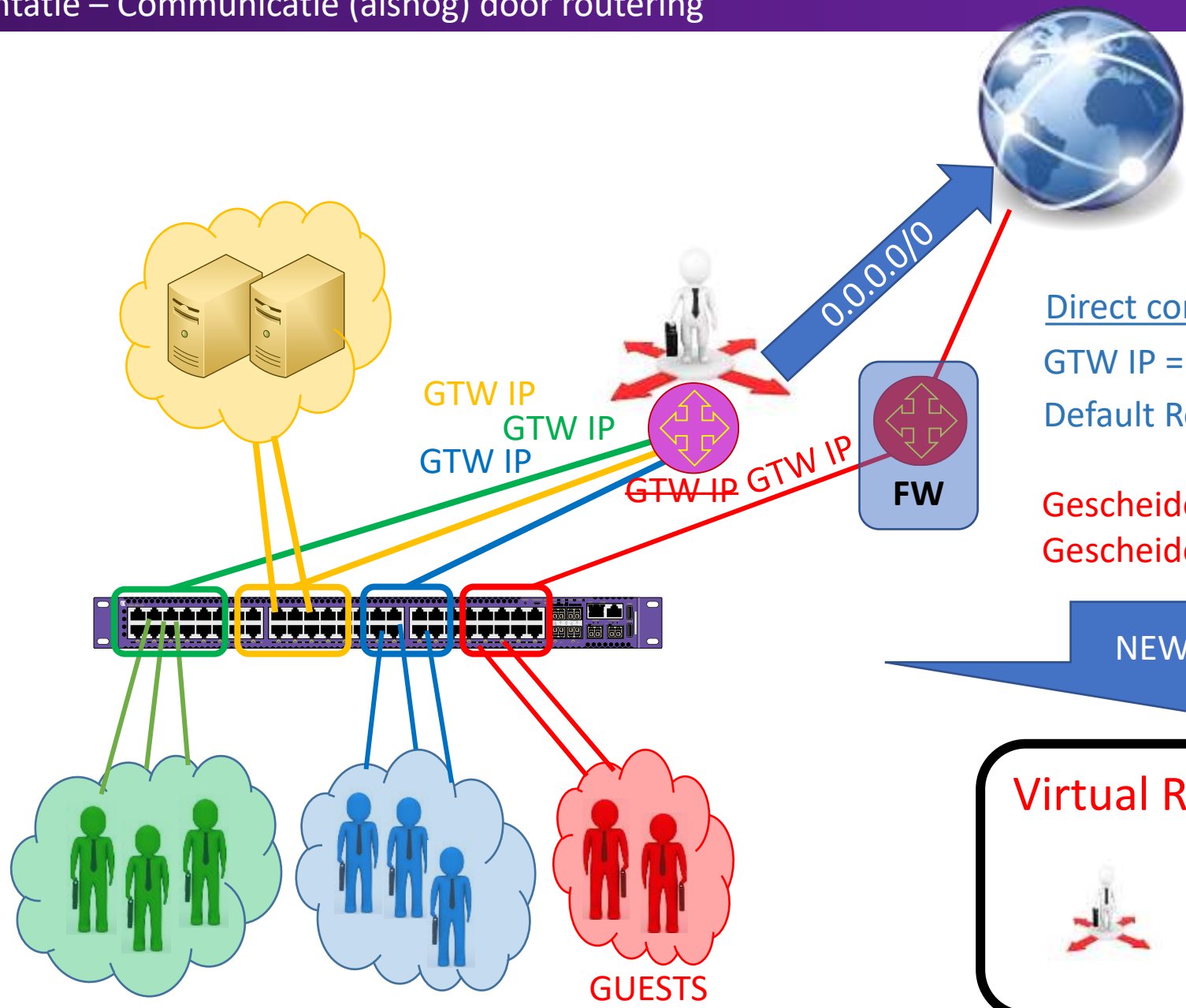
Reducing
HUMAN ERROR
In configurations

BETTER
Nework Uptime

FASTER
Network config

APS

VLAN Segmentatie – Communicatie (alsnog) door routering



Direct connected Networks routeren

GTW IP = Address Resolution (ARP-tabellen)

Default Route => ongekende netwerken

Gescheiden ROUTER functionaliteit

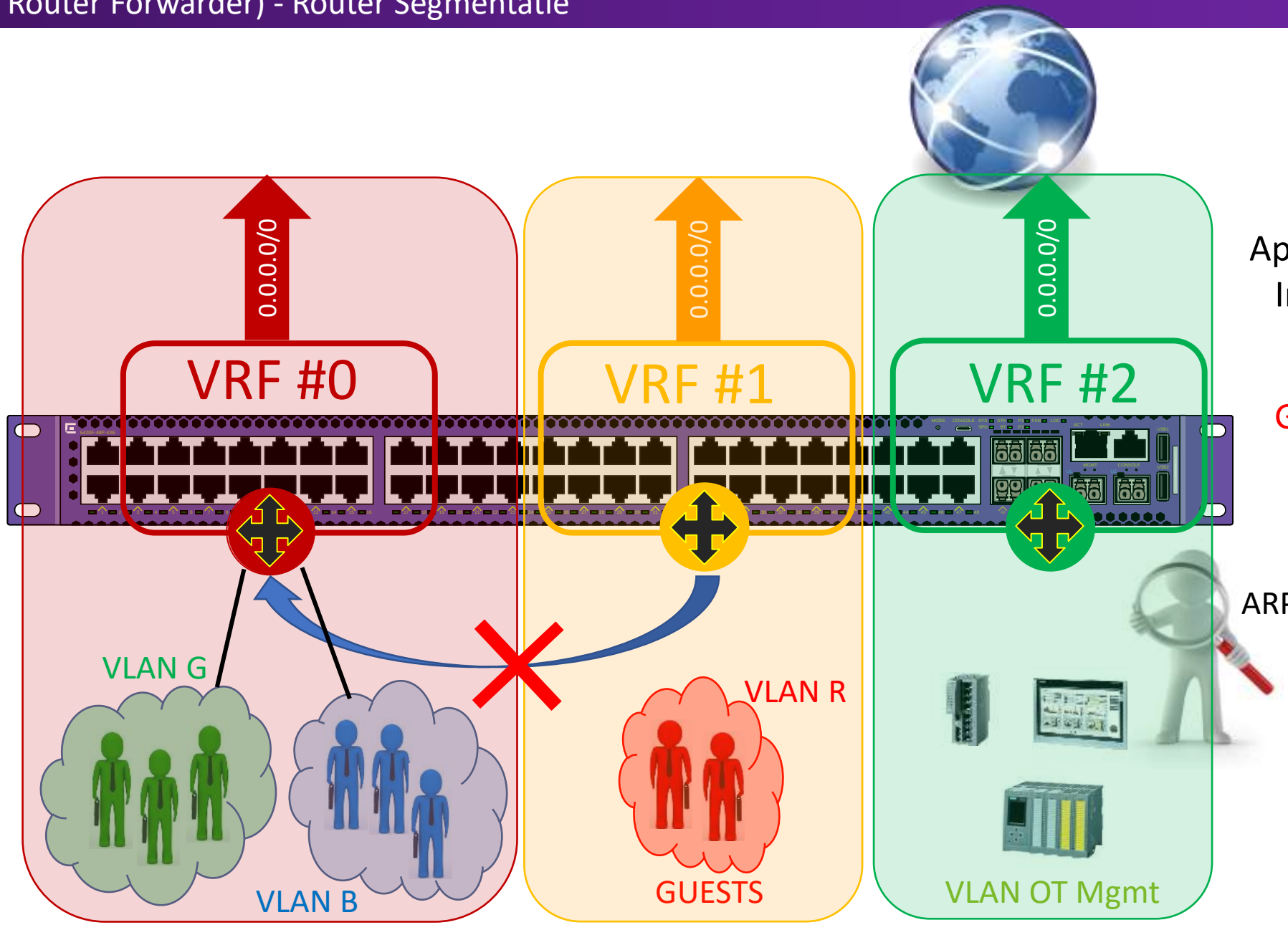
Gescheiden Hardware

NEW Technologies

Virtual Router Forwarder

VRF

VRF (Virtual Router Forwarder) - Router Segmentatie



Aparte (Virtuele) Routers
In dezelfde Hardware

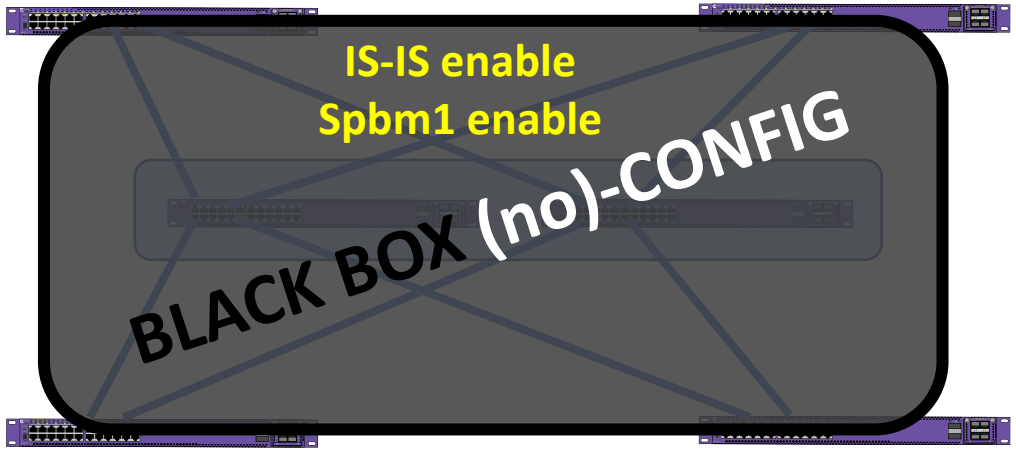
VRF #0 = default
Global Routing Table

ARP tabellen

Virtual Router Forwarder
VRF
Waar routeren?

APS

SPBm (Shortest Path Bridging) Mac - Black Box Backbone – No VLAN config



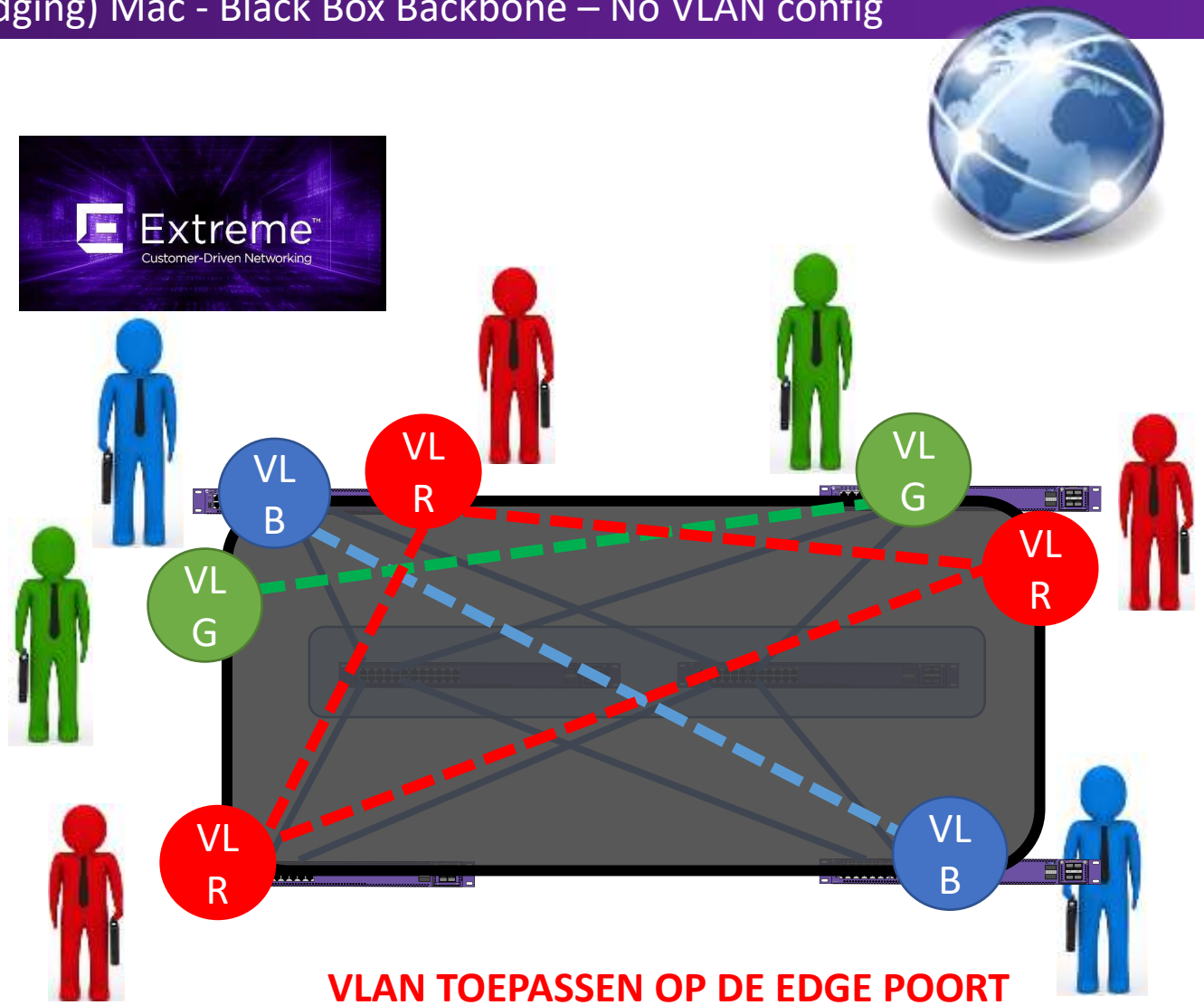
VL G

VL R

VL B

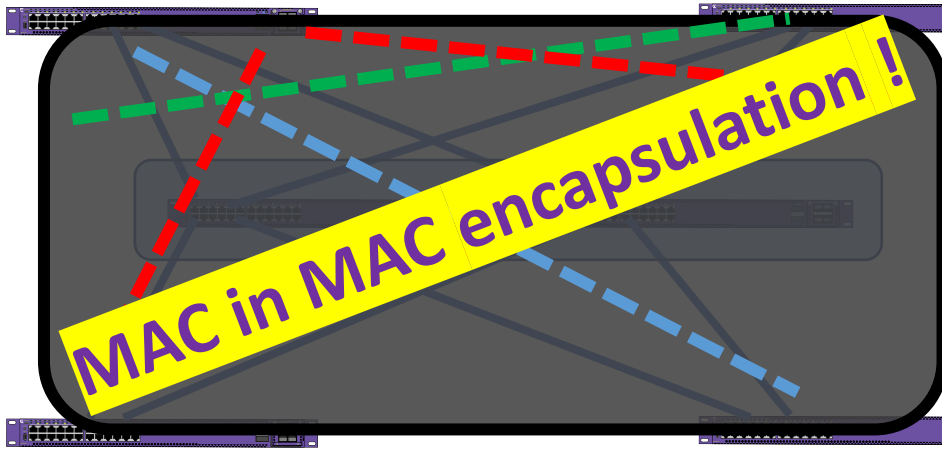
APS

SPBm (Shortest Path Bridging) Mac - Black Box Backbone – No VLAN config



VLAN TOEPASSEN OP DE EDGE POORT
AUTOMATISCHE CONFIG VAN BACKBONE

SPBm (Shortest Path Bridging) Mac - Black Box Backbone – No VLAN config



GEEN IP HOP-By-HOP info
BLACK-BOX info for unwanted individuals

SPBm (Shortest Path Bridging) Mac - Black Box Backbone – Key Elements

IEEE Standard **802.1aq** (SPB)

Shortest **P**ath **B**ridging is a protocol intended to simplify the creation and configuration of networks

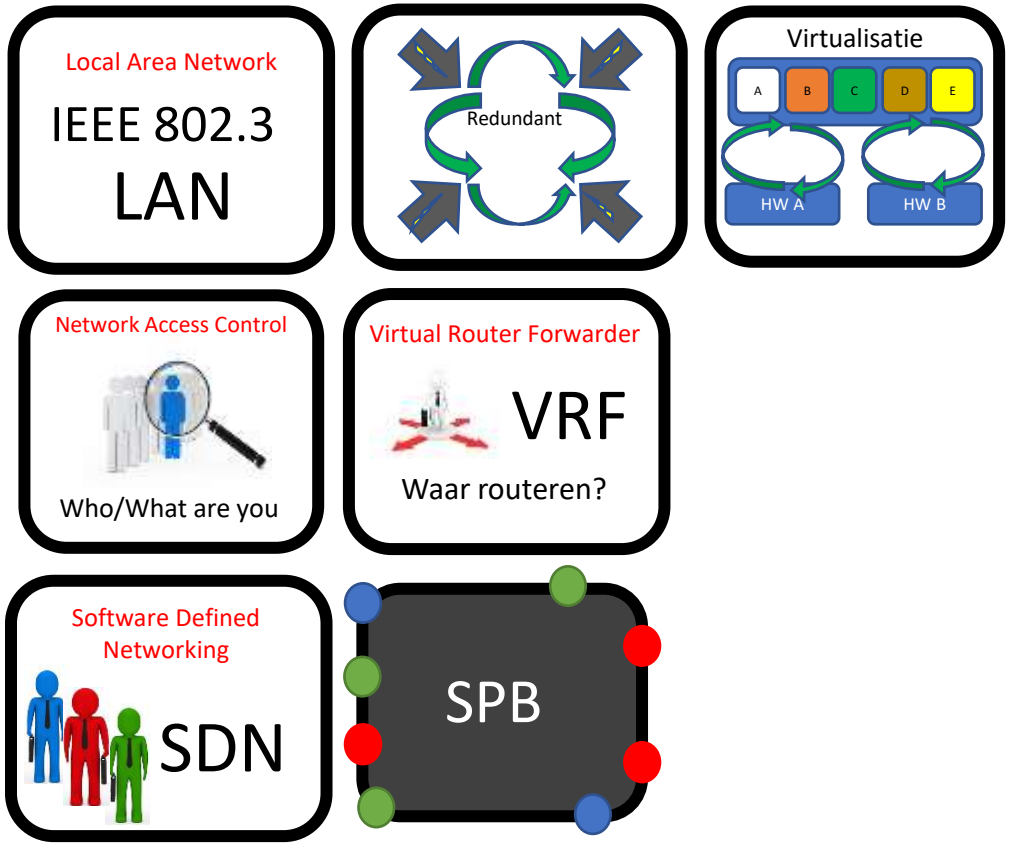
i-SID (Internal **S**ervice **ID)** (1 tot 16Miljoen)

2 Backbone VLAN **(4051-4052)**

IS-IS (Link State Protocol**)**
No Spanning Tree Protocol
Multilink **Loopfree** Backbone

Extreme™
Customer-Driven Networking

APS



Renewal Rate van Hardware in IT : gemiddeld 7 jaar

Bij iedere Renewal =

- Hogere Snelheden 10/100 -> 10/100/1000
  100/1000/10G
  100/1000/10G/25G
  10G/25G/100G

- Betere Redundantie
- Extra Software features
- Meer automatisatie

Meer Security features

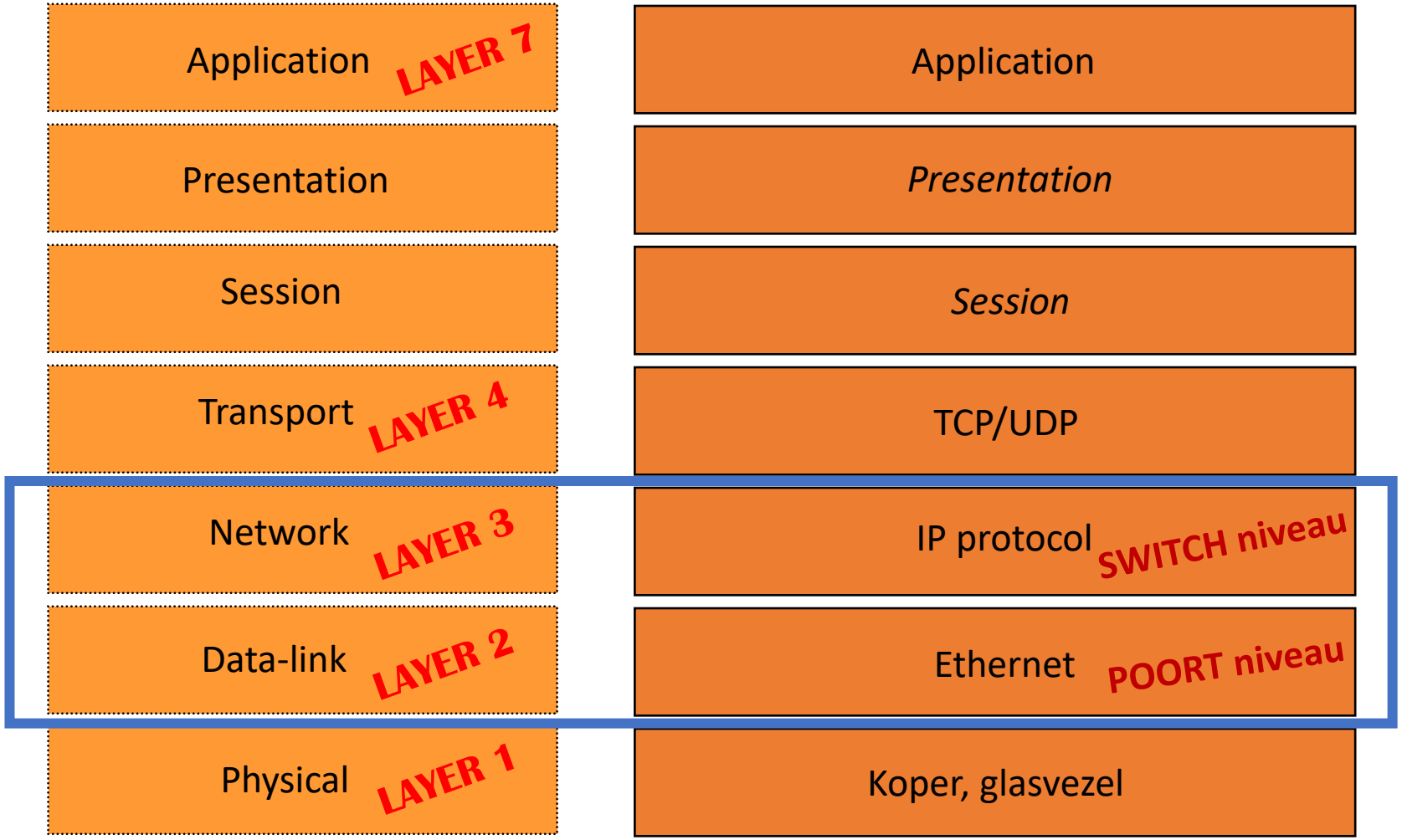
Extreme™ Customer-Driven Networking

APS

Local Area Network
IEEE 802.3
LAN

Meer Security features ... @ Switch level

OSI - model



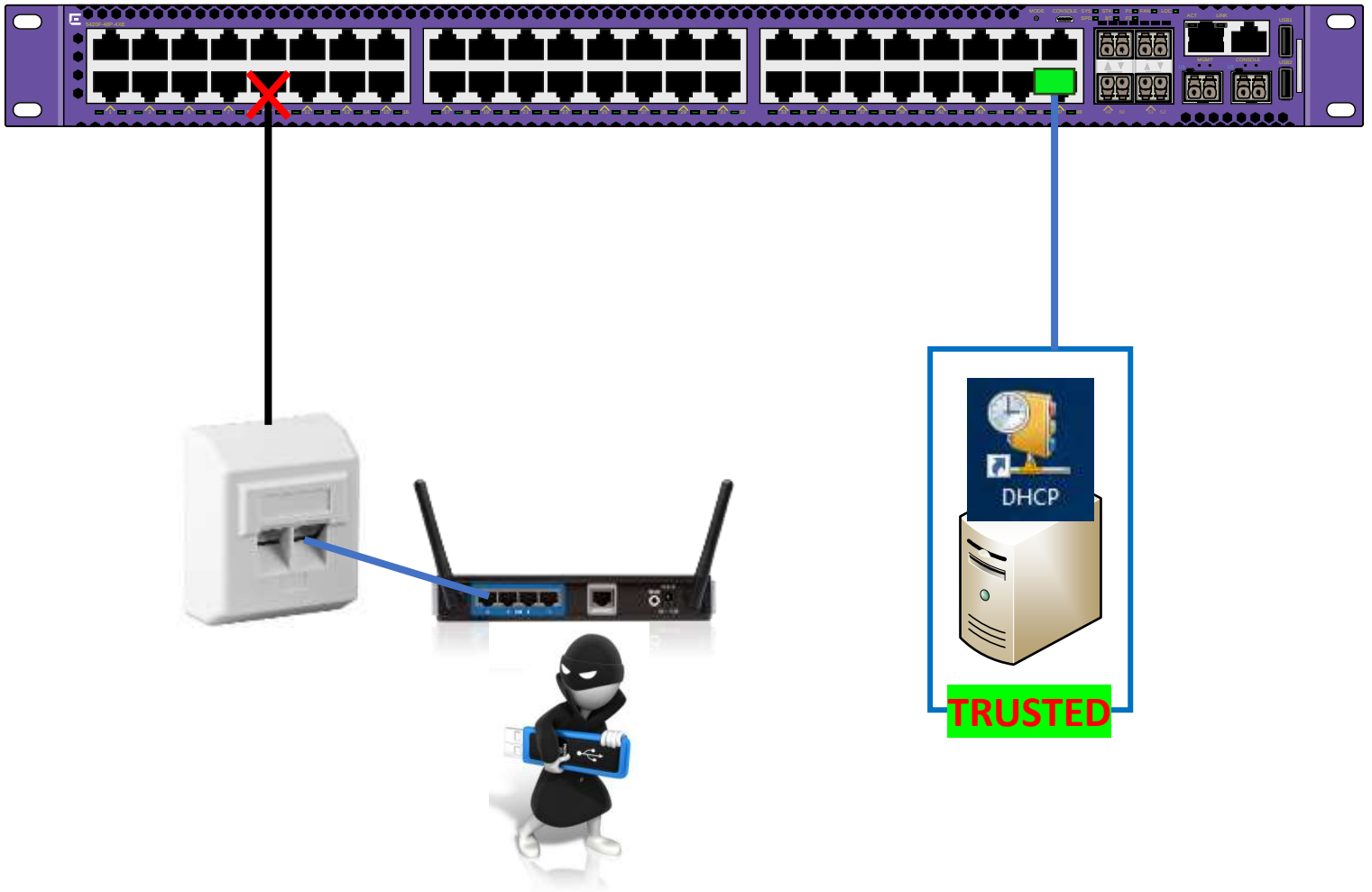
Extreme™
Customer-Driven Networking

APS

Port Based

L2 Security

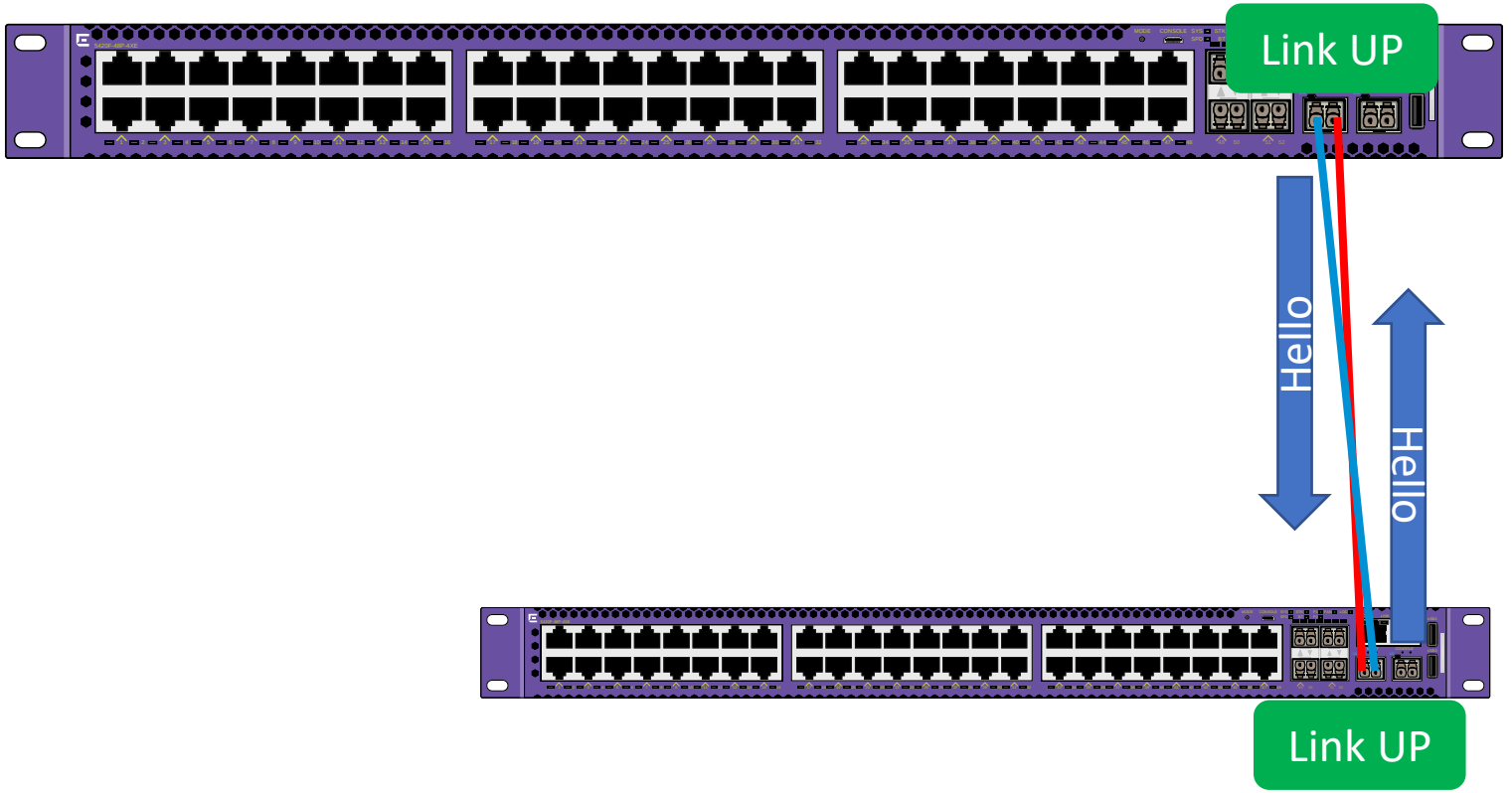
Dynamic **H**ost **C**ontrol **P**rotocol



VLACP link failure detection

Port Based

L2 Security

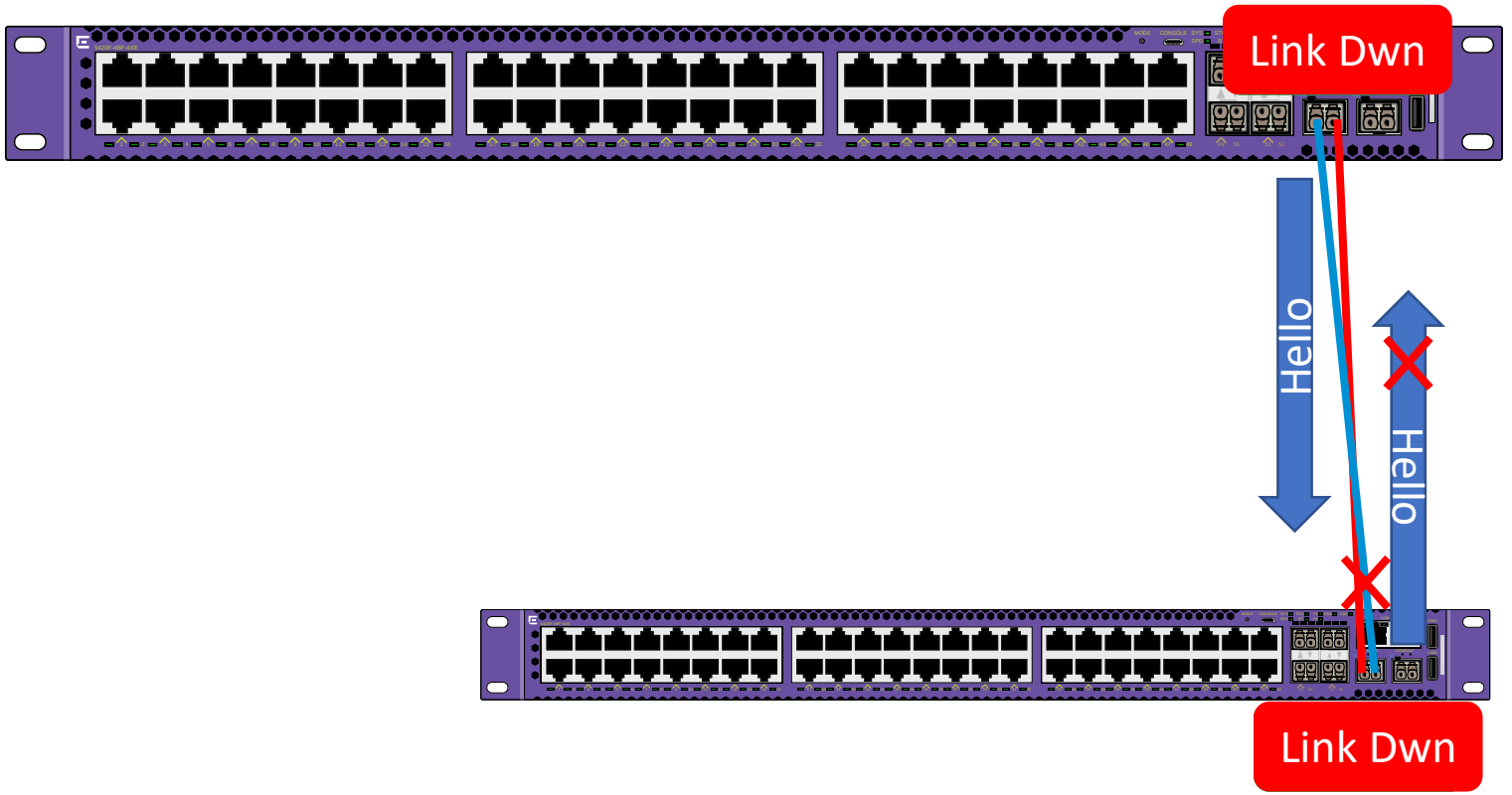


DHCP Snooping

VLACP link failure detection

Port Based

L2 Security



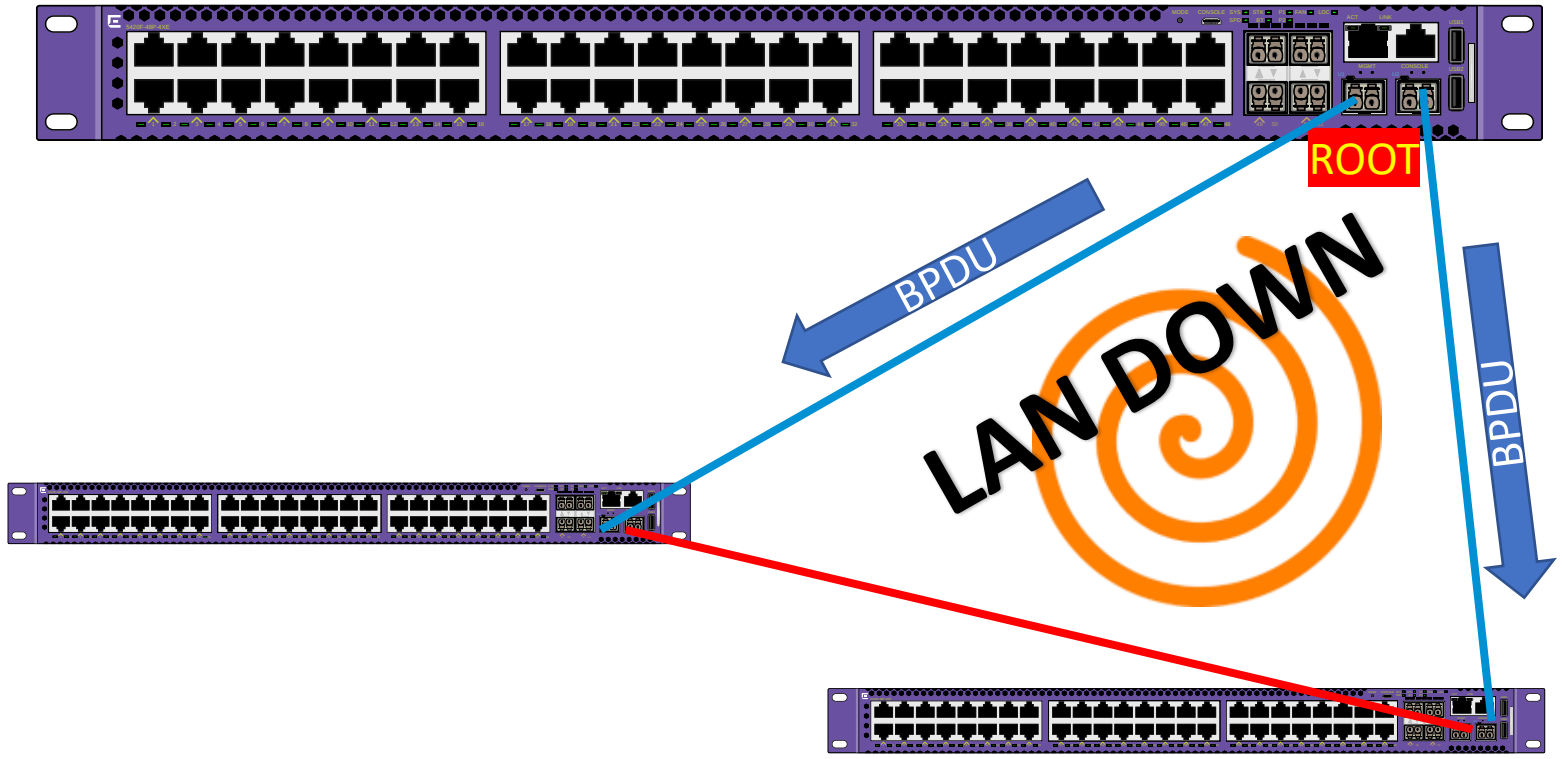
DHCP Snooping

Port Based

L2 Security

Bridge **P**rotocol **D**ata **U**nits

Spanning **T**ree **P**rotocol **802.1D**



DHCP Snooping

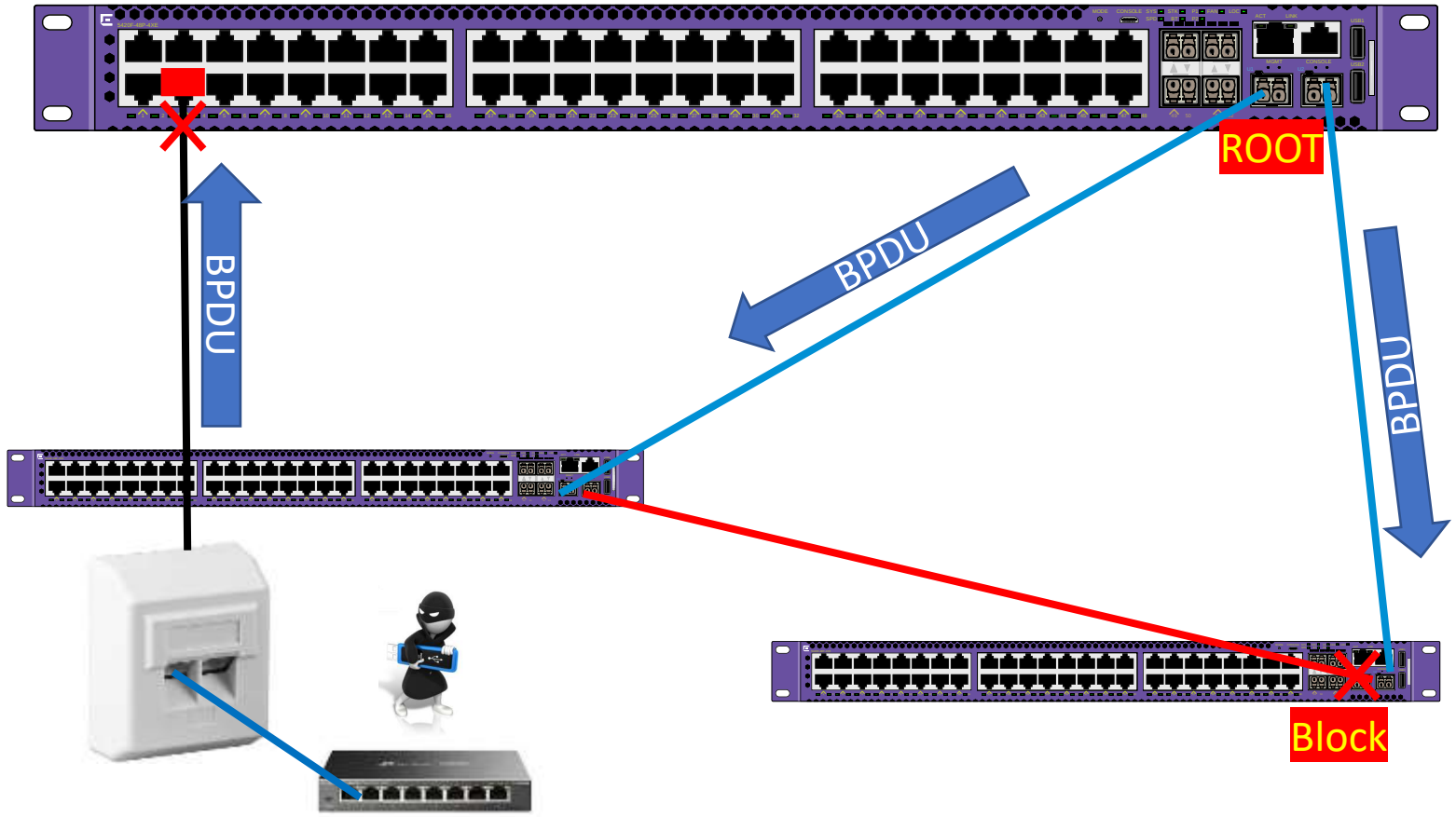
VLACP link failure detection

Port Based

L2 Security

Bridge **P**rotocol **D**ata **U**nits

Spanning **T**ree **P**rotocol **802.1D**



DHCP Snooping

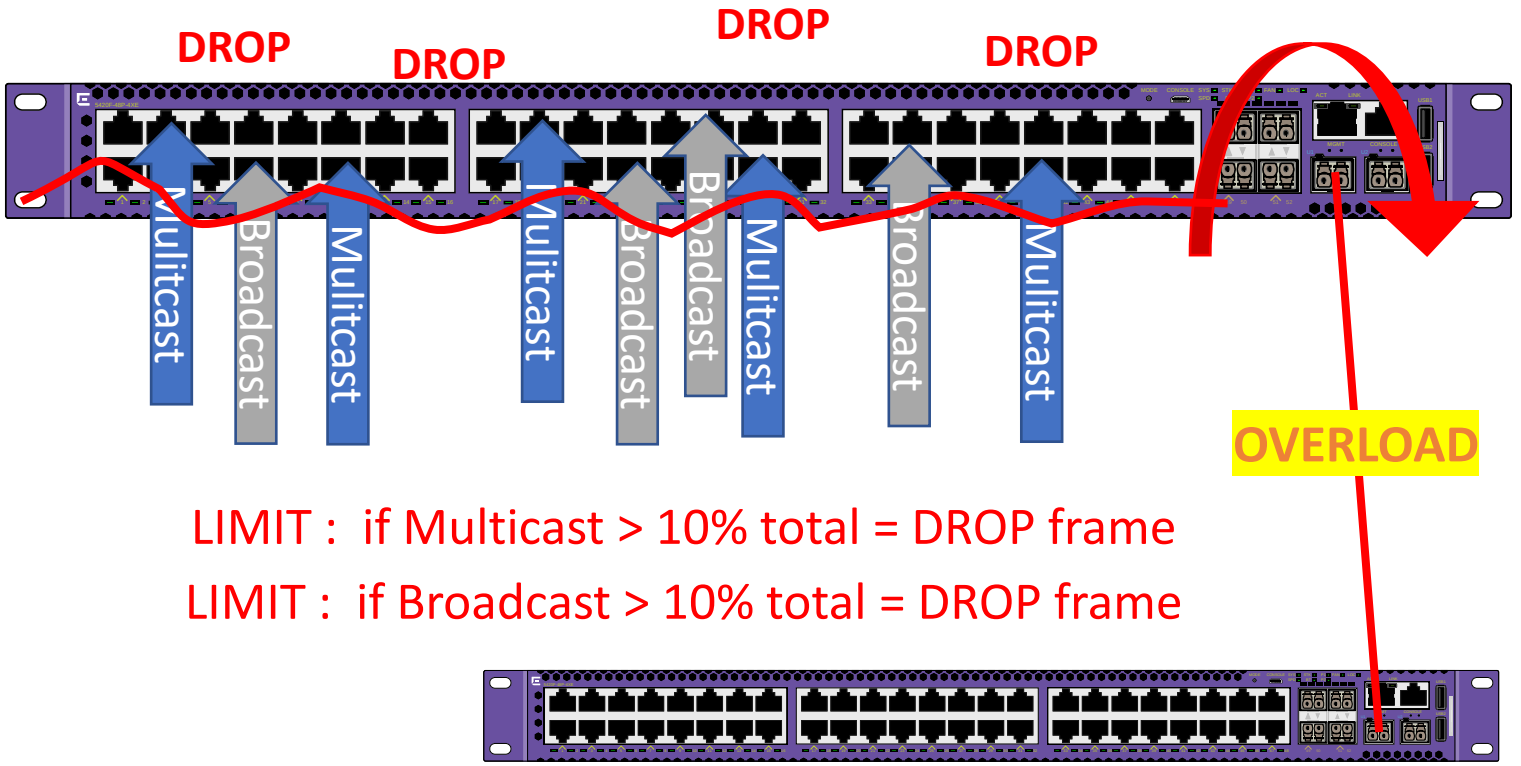
VLACP link failure detection

Port Based

L2 Security

Multicast Frames -> Dedicated Receivers

Broadcast Frames -> Iedereen is Receiver



LIMIT : if Multicast > 10% total = DROP frame

LIMIT : if Broadcast > 10% total = DROP frame

DHCP Snooping BPDU guard

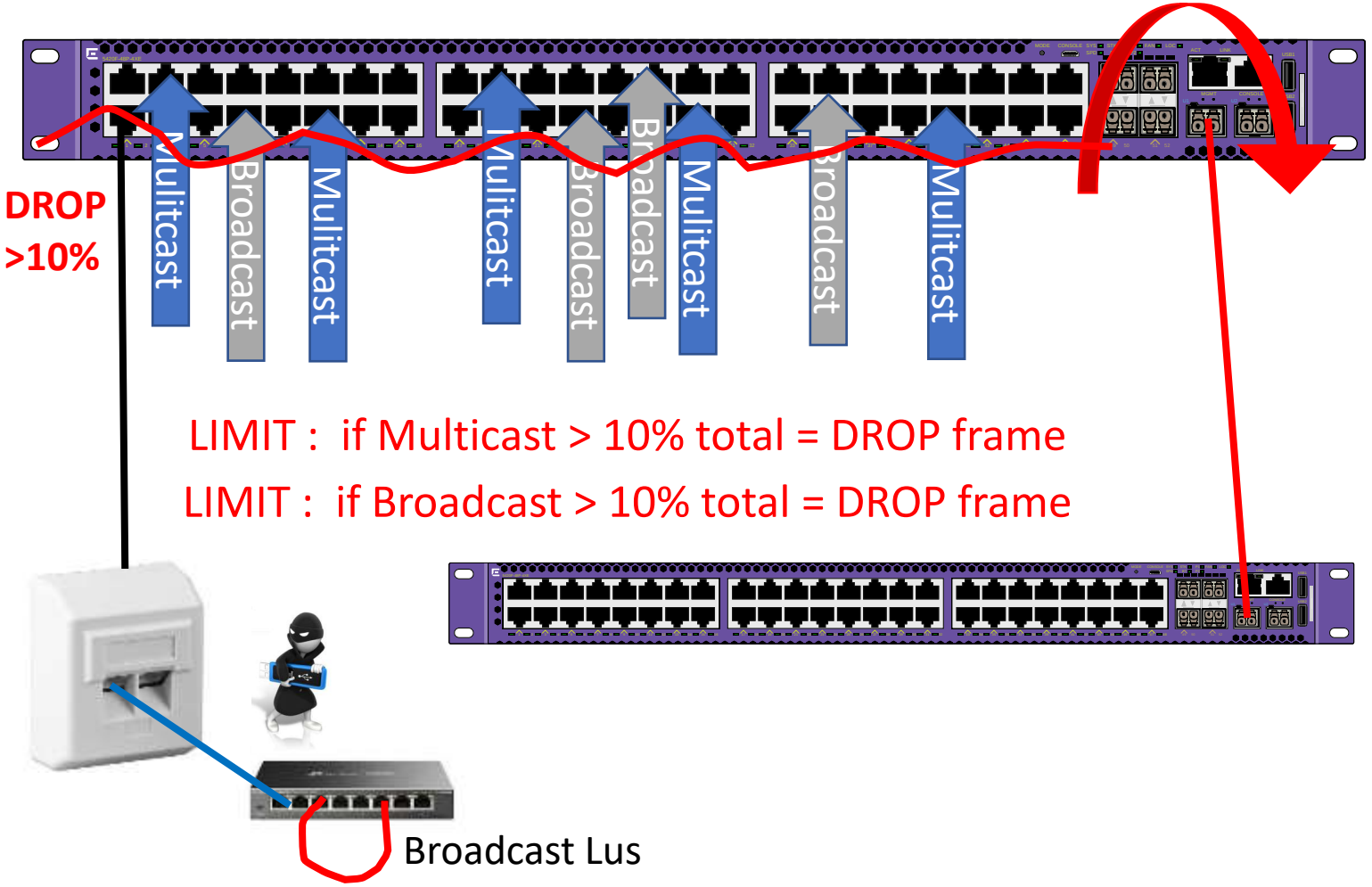
VLACP link failure detection

Port Based

L2 Security

Multicast Frames -> Dedicated Receivers

Broadcast Frames -> Iedereen is Receiver

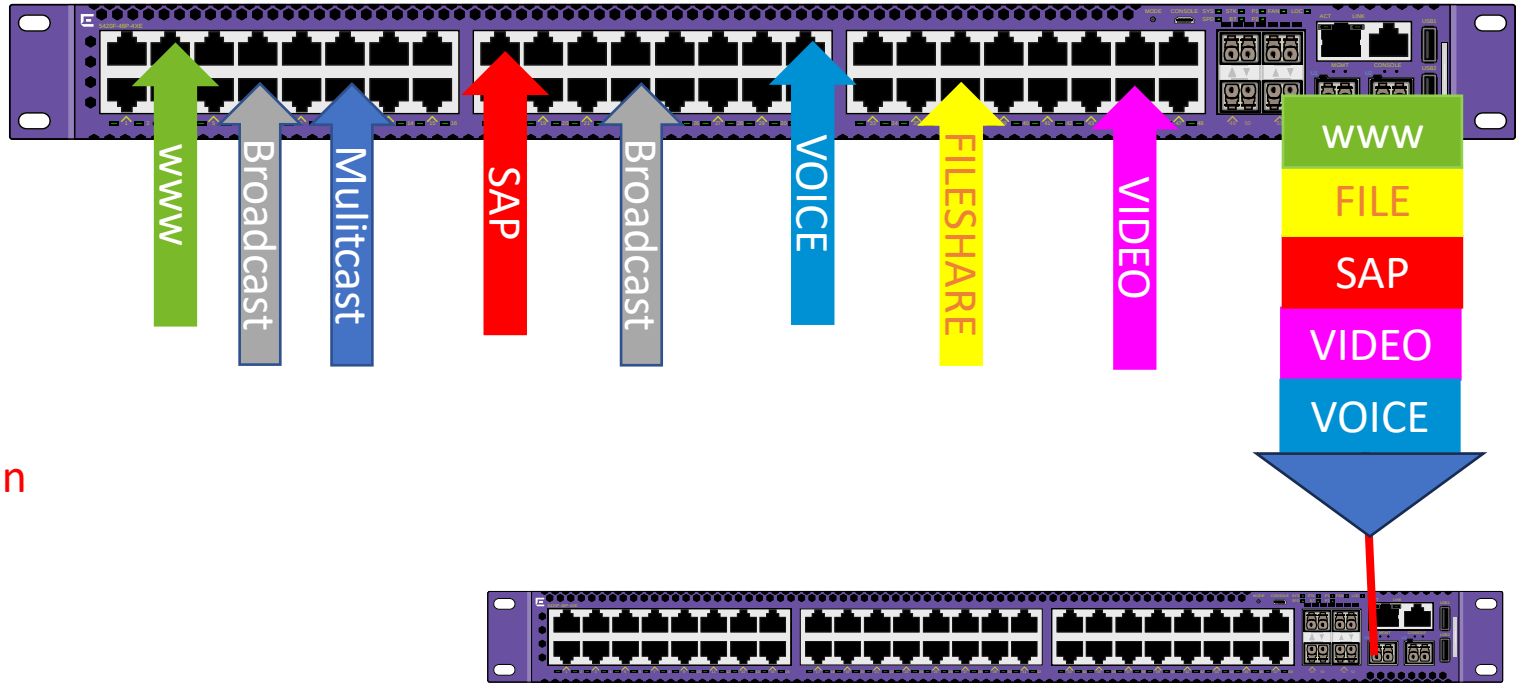


DHCP Snooping BPDU guard Storm Control

VLACP link failure detection

Port Based

L2 Security



Voorrang geven aan bepaalde protocollen

Voorrang geven aan bepaalde poorten

Advanced QoS

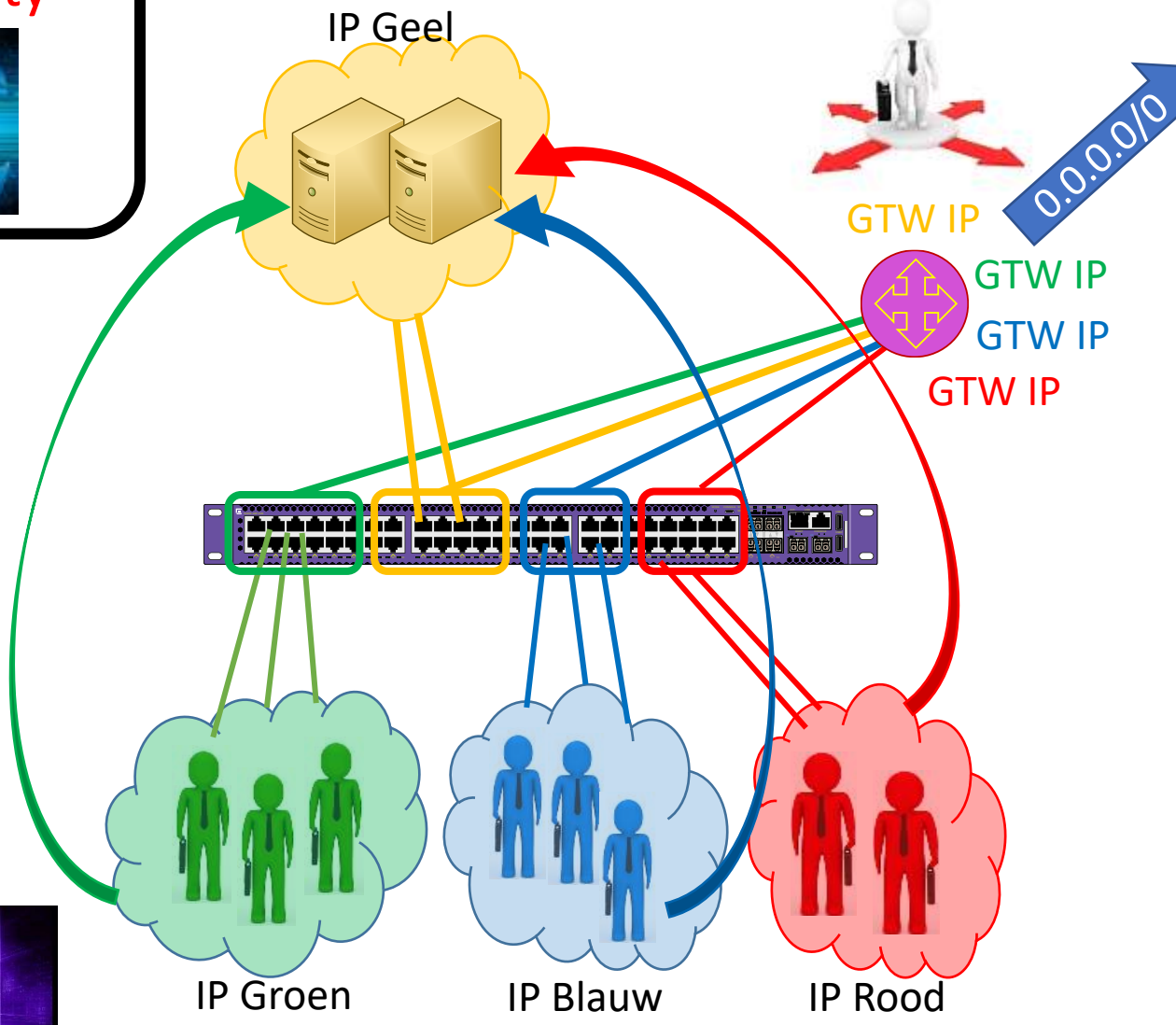
Vergt Layer 3 features

DHCP Snooping BPDU guard Storm Control

VLACP link failure detection QoS

Switch Based

L3 Security



Access Control List

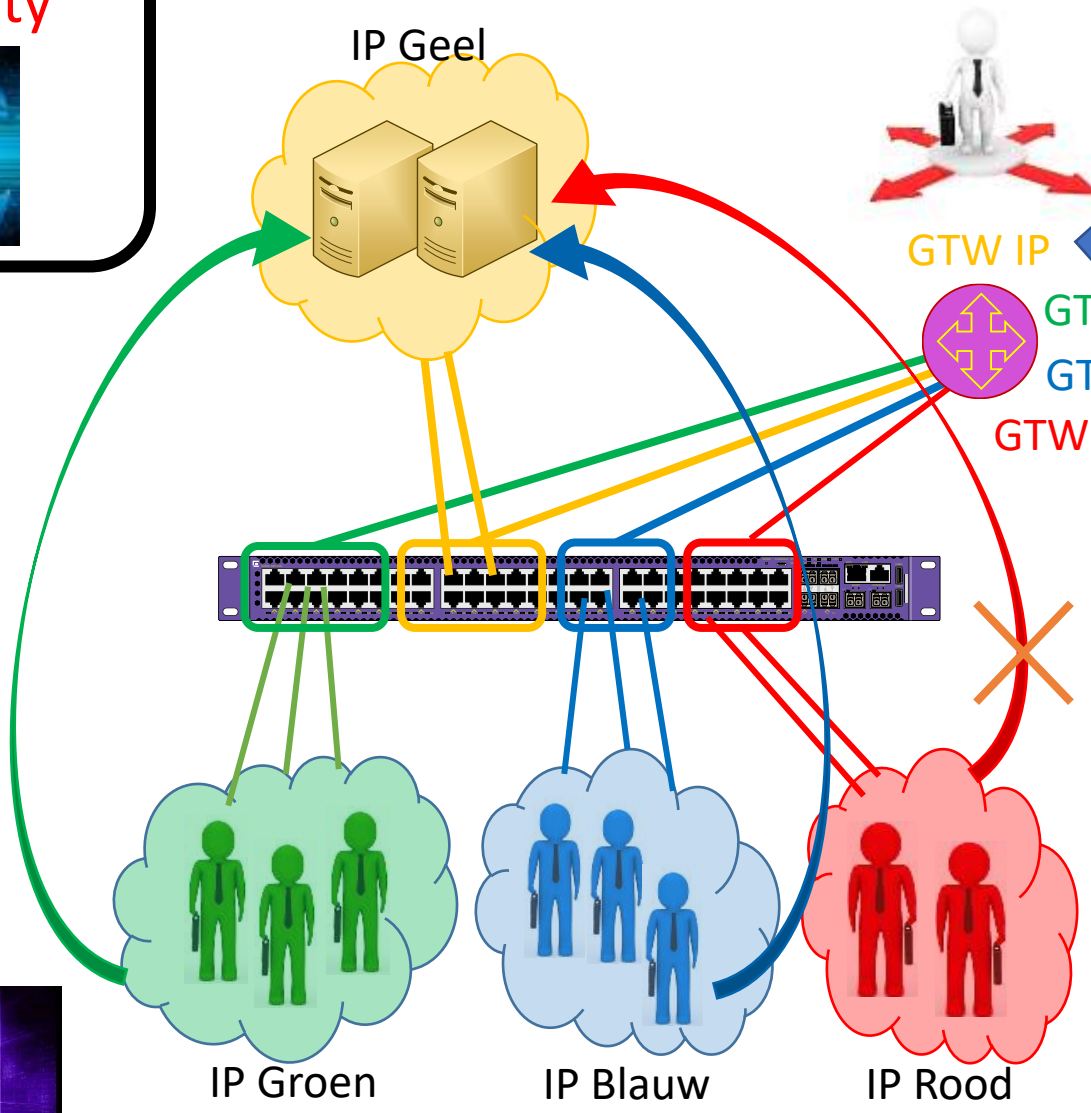
Any <-> Any : ALLOW

Extreme Customer-Driven Networking

APS

Switch Based

L3 Security



Access Control List

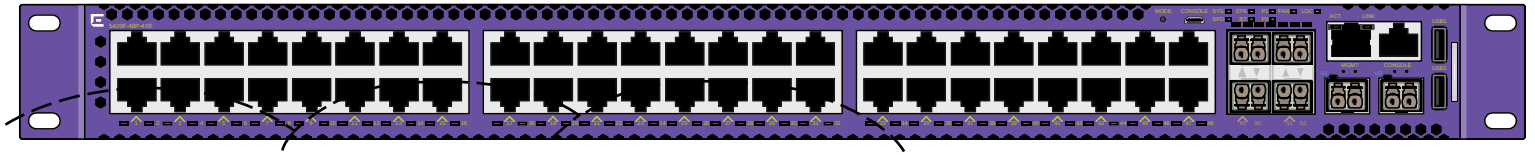
Top-down

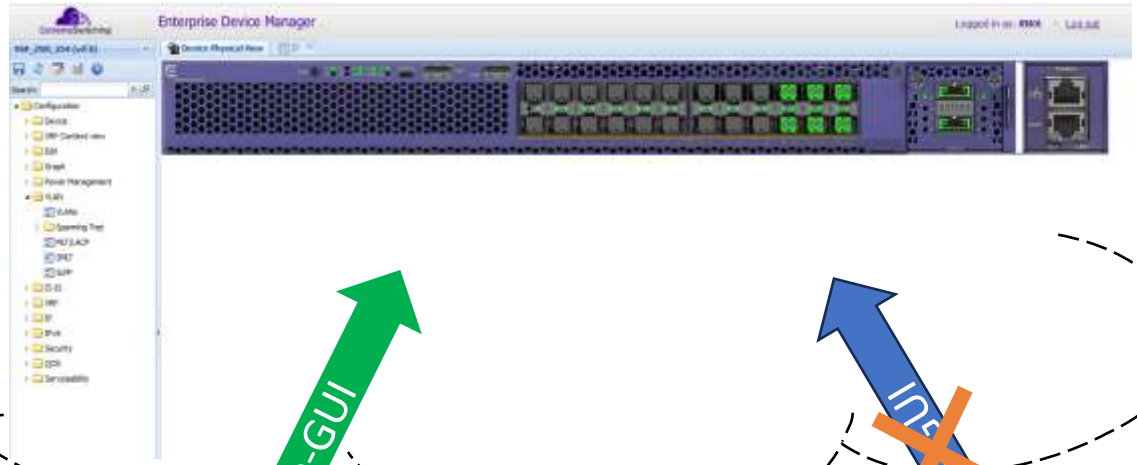
IP Rood <-> IP Geel : DENY

Any <-> Any : ALLOW

Switch Based

L3 Security





Web-GUI

Web-GUI

IP Groen

IP Blauw

IP Manager

IP Groen <-> Mgmt : ALLOW

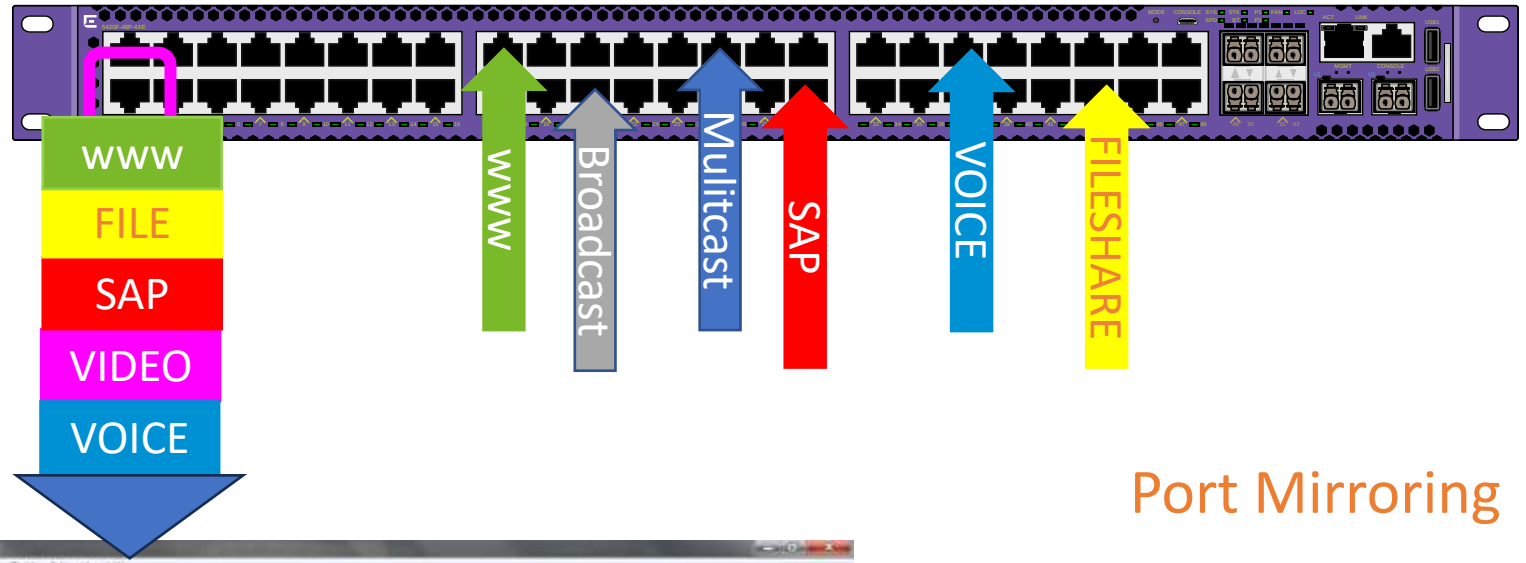
Any <-> Any : DENY

Extreme™ Customer-Driven Networking

APS

Switch Based

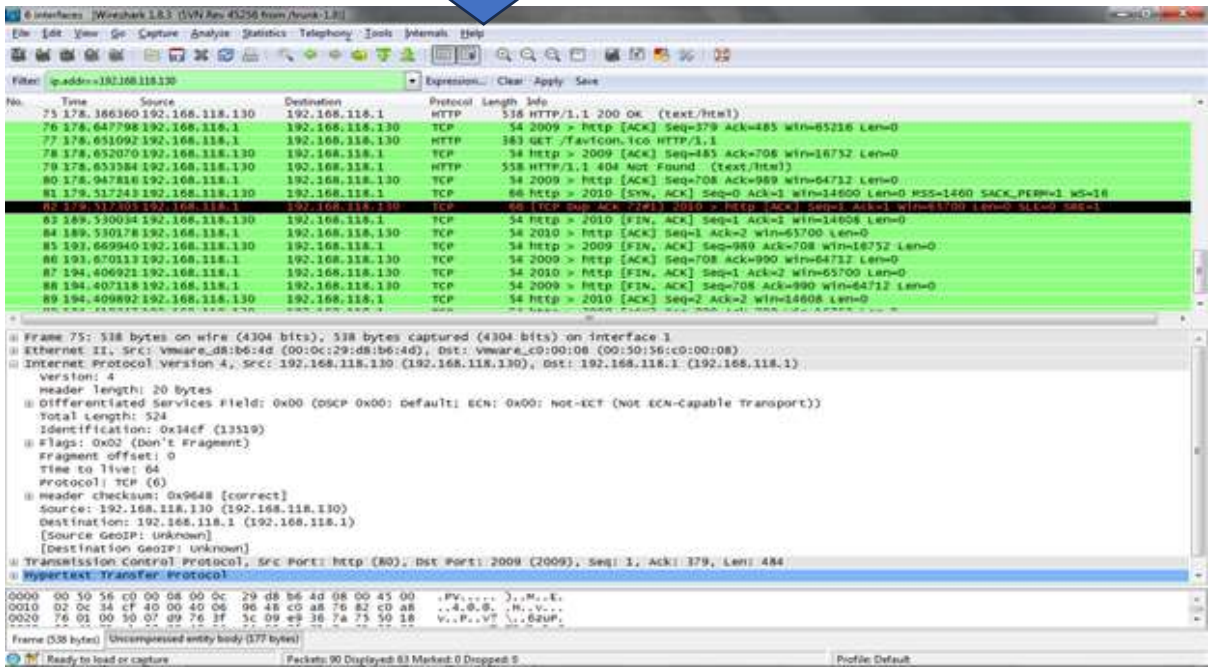
L3 Security



WIRESHARK

CLAROTY

Extreme
Customer-Driven Networking



Port Mirroring

Copy Ports x,y,z -> Port 2
Copy Vlan x,y,z -> Port 2

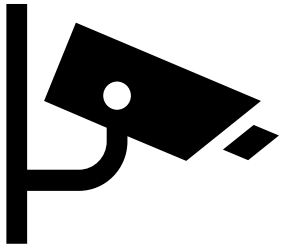
APS

IT … van toen tot gisteren - Vele stapjes naar een hybride oplossing

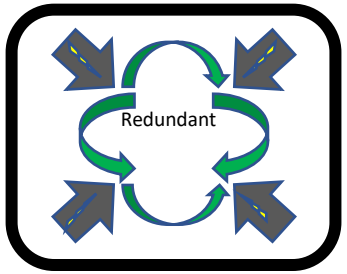
Local Area Network

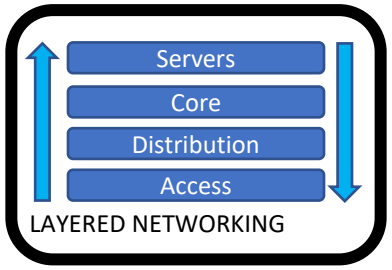
IEEE 802.3

LAN



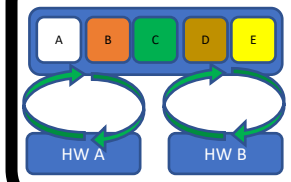
CTI





LAYERED NETWORKING

Virtualisatie

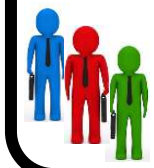


Cloud

Network Access Control

Who/What are you

Software Defined Networking

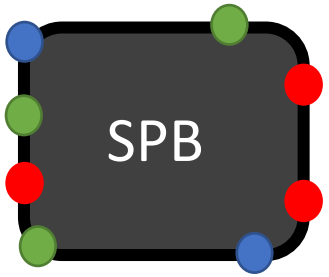


SDN

Virtual Router Forwarder

VRF

Waar routeren?



Port Based

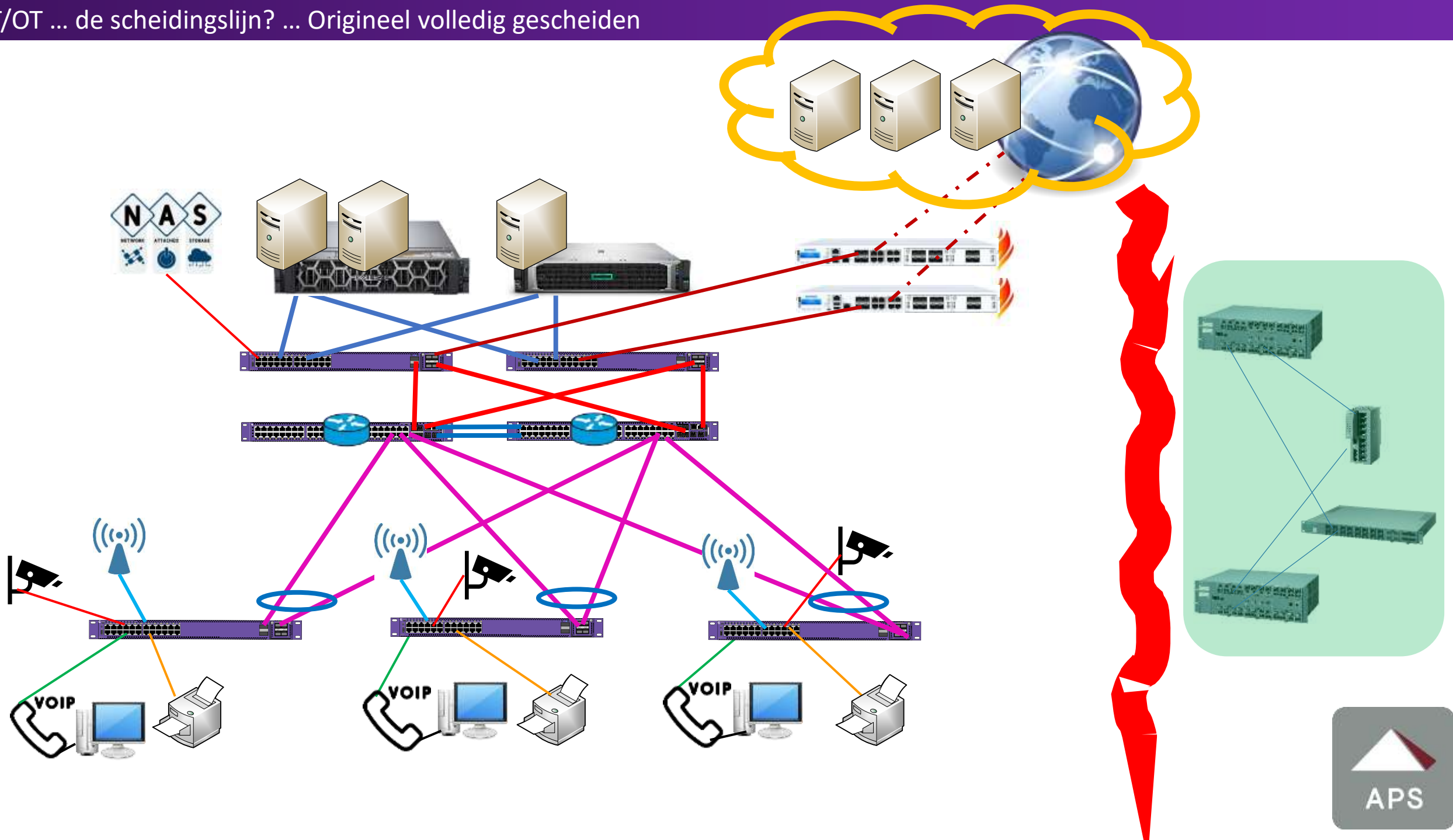
L2 Security

Switch Based

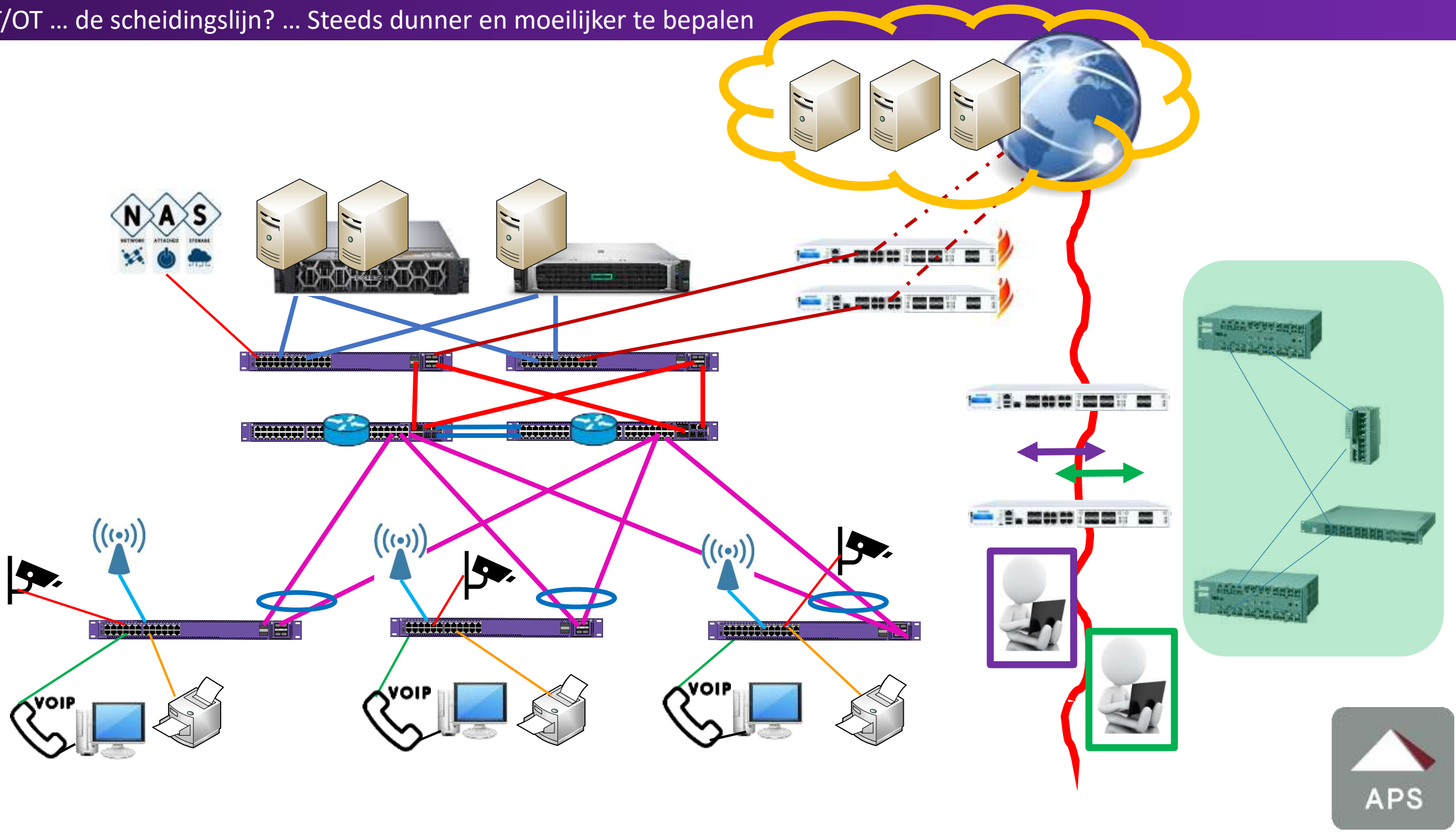
L3 Security

APS

IT/OT … de scheidingslijn? … Origineel volledig gescheiden



IT/OT … de scheidingslijn? … Steeds dunner en moeilijker te bepalen



All Professional Services NV

Brandstraat 4
Lokeren, Oost Vlaanderen 9160
Belgium
Phone: +32 93404060

Capabilities

Wired

Wireless

Cloud & Applications

Level

Diamond

GRAND MASTER

PartnerWorks CERTIFIED

Specializations

ExtremeWireless

Master Cloud & Applications

Master Edge

Master Campus

Cloud, Management & Automation

ExtremeSwitching

Security & Access Control

Extreme™ Customer-Driven Networking

Keynote sessie

14h00 Extreme Networks – intrinsieke security met SPBm LAN infrastructuur

16h00 APS nv - Flexibiliteit met Blown Fiber Backbone

BU Automation

Sammy Van den Meersschaut

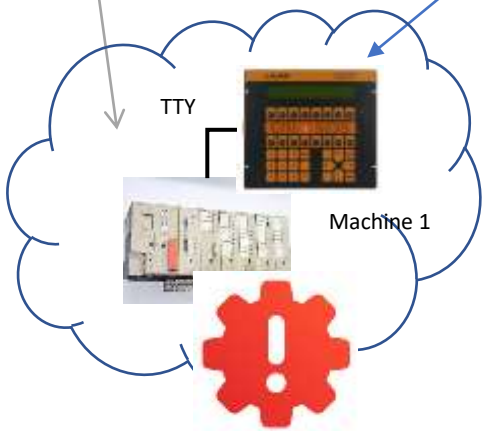
Application Manager

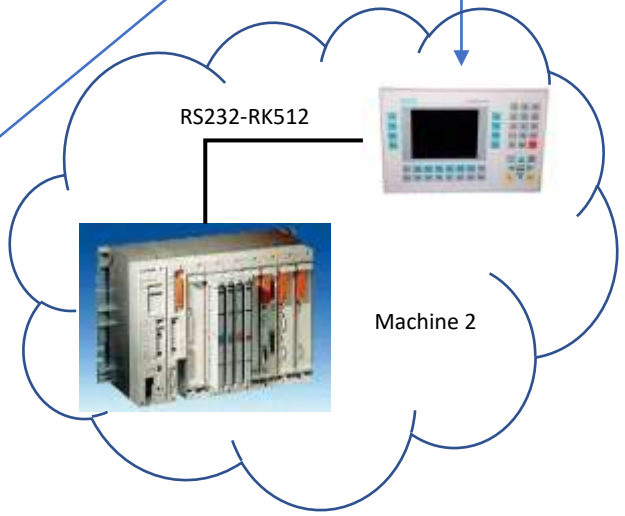
sammy.van.den.meersschaut@atsgroep.be

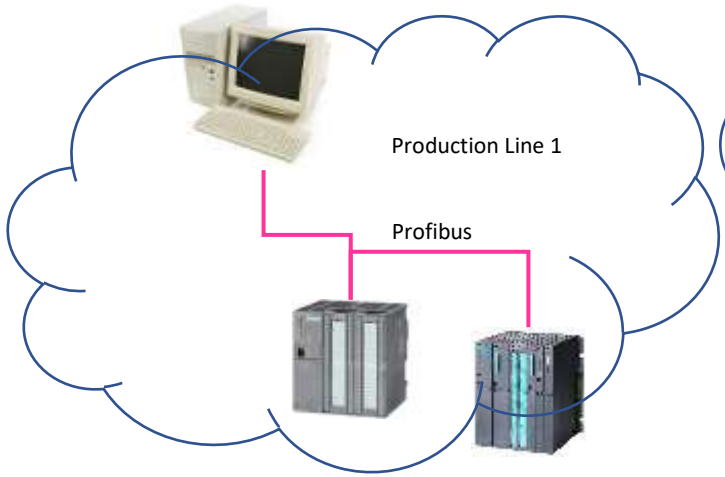
BU Automation

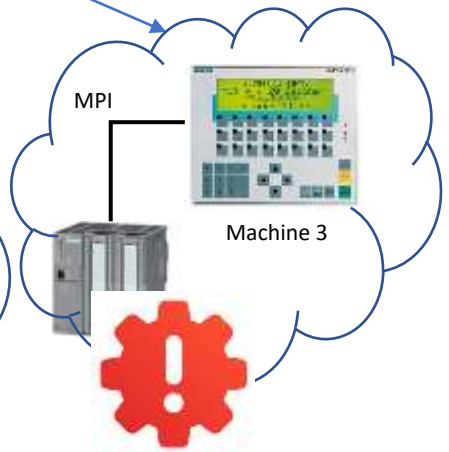
OT Evolutie - 1ste Moderne machines / PLC / HMI

Recepten / Parameters / Productieplanning

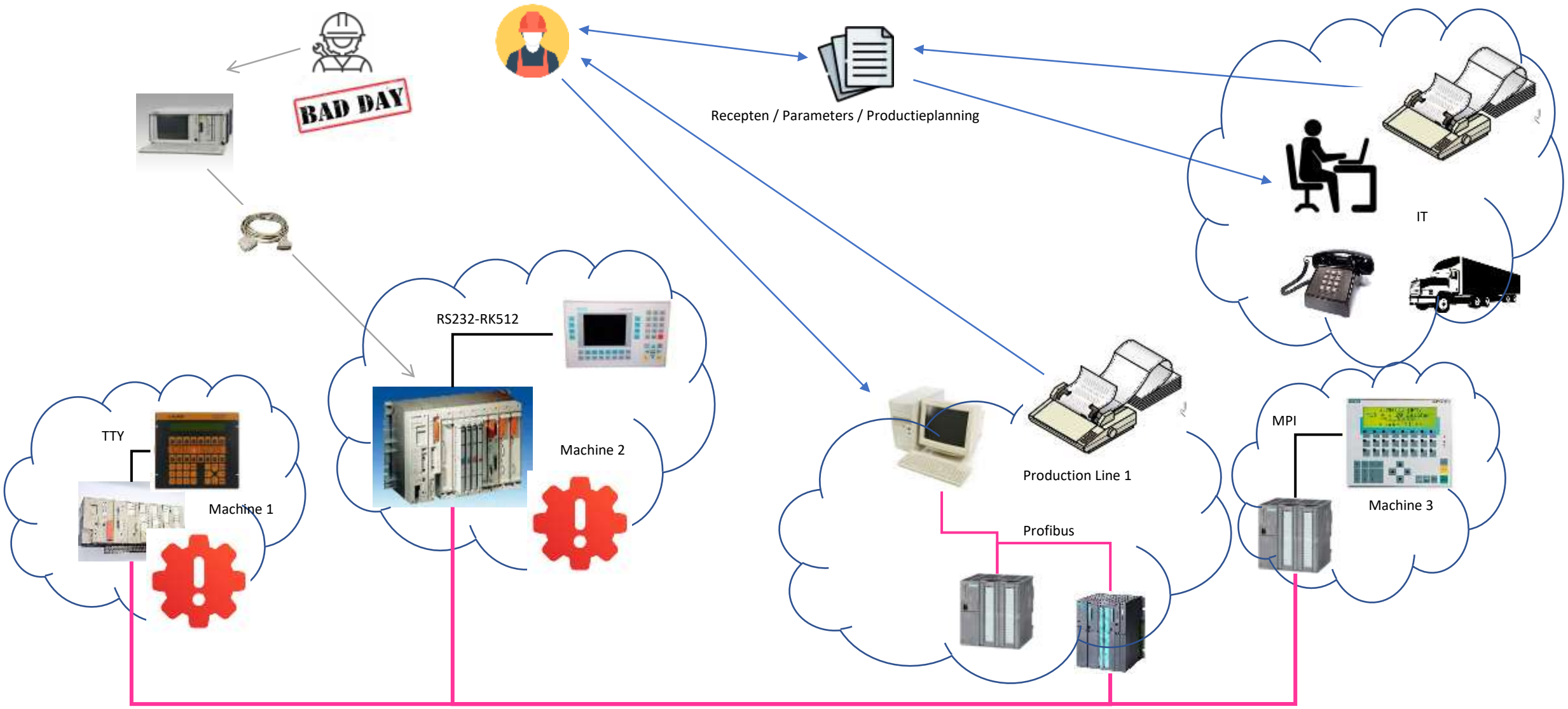




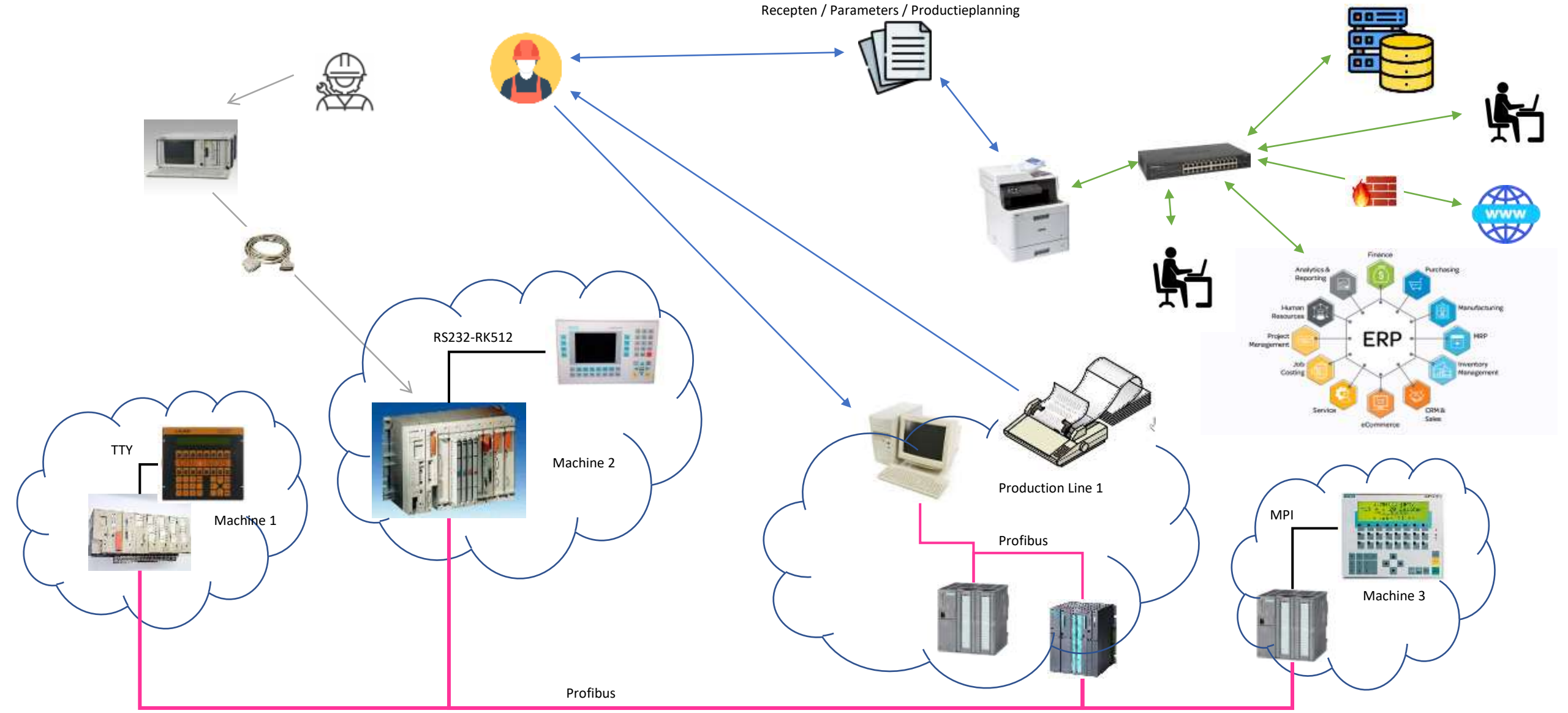




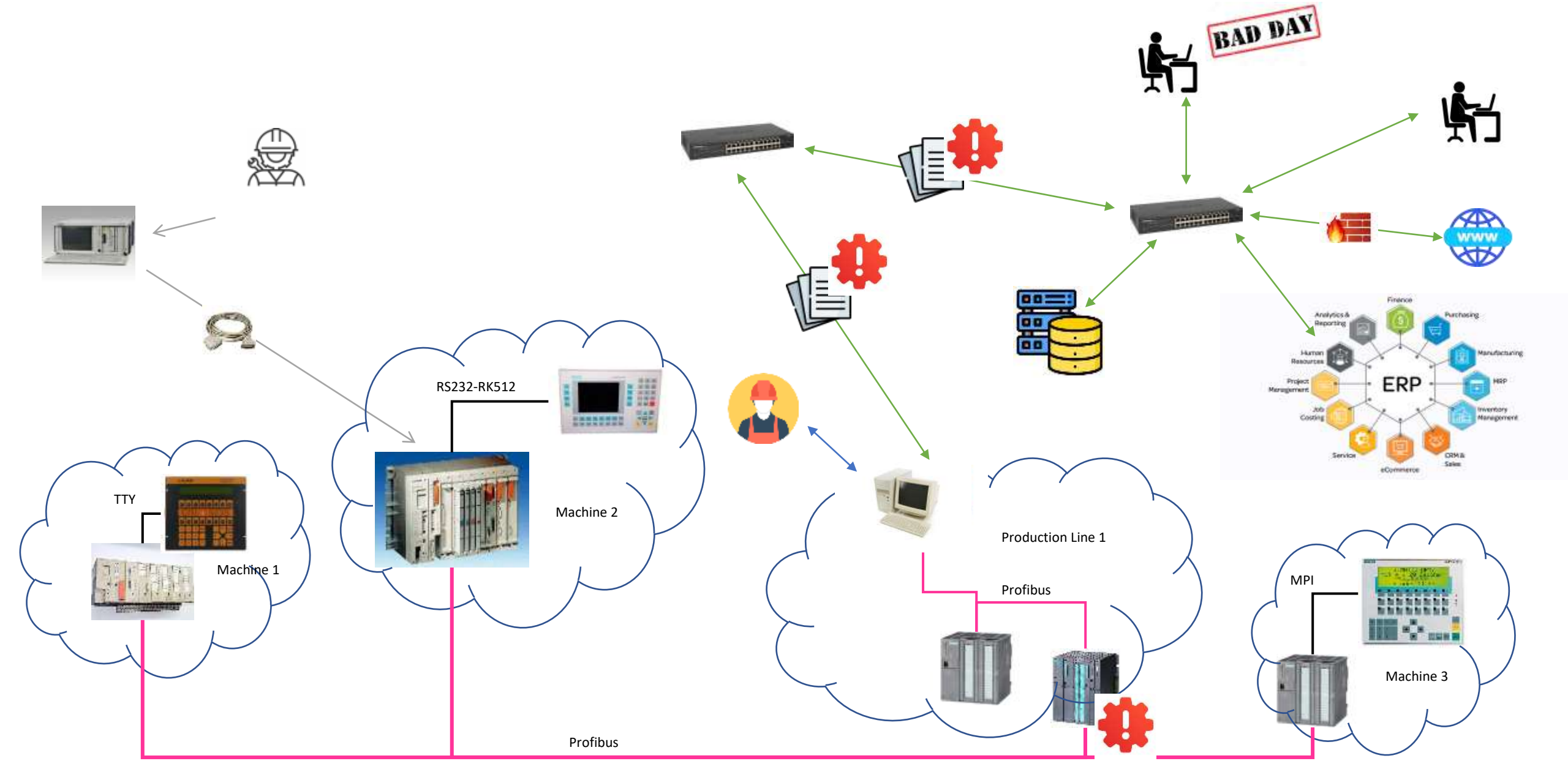
OT Evolutie - Lokale OT netwerken



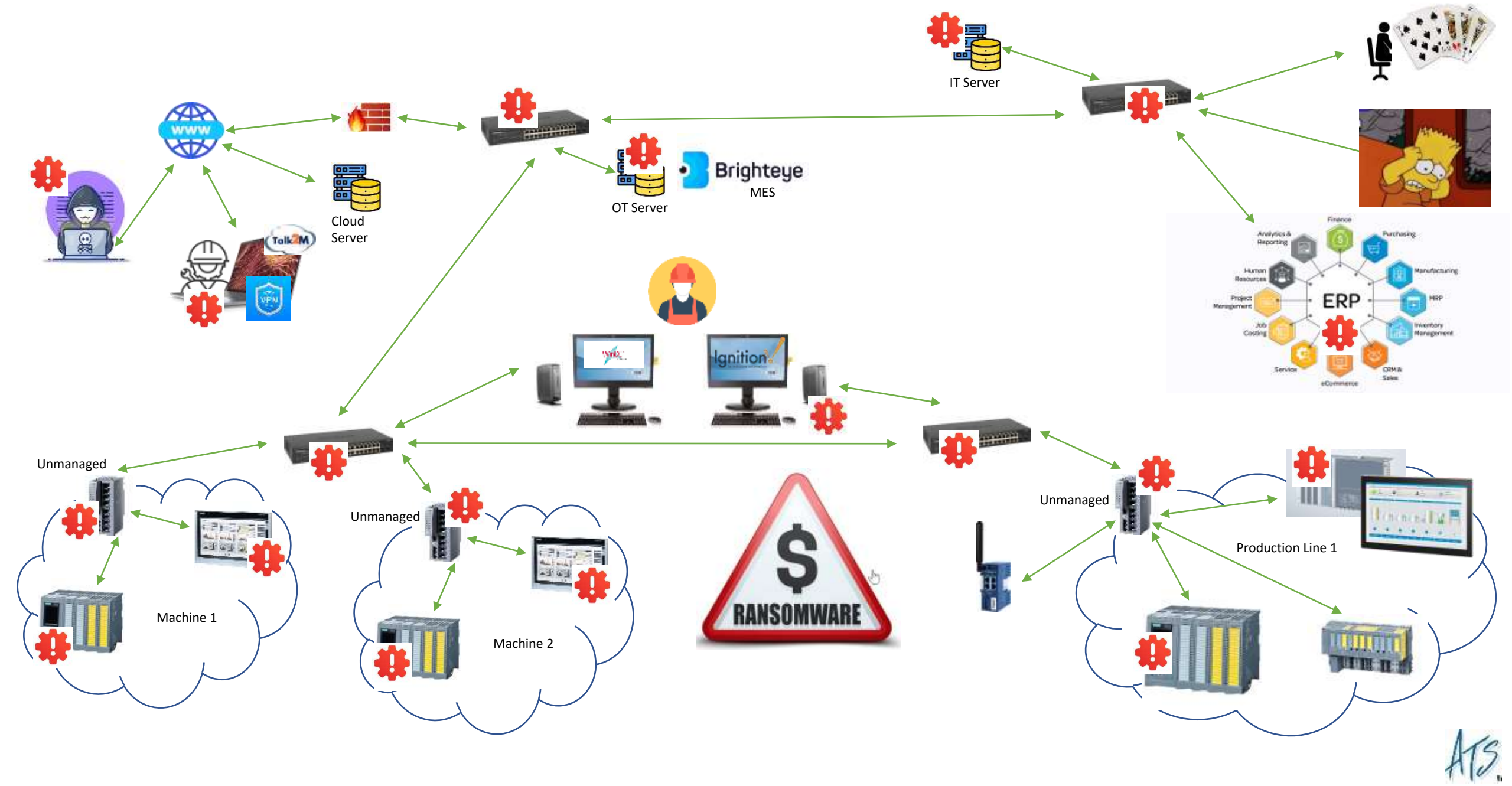
OT Evolutie - Modernisering IT



OT Evolutie - IT/OT Link



OT Evolutie - IOT Factory



Situatie

- Gesegmenteerd netwerk?
- Visibiliteit? Wat is er? Hoeveel is er? Welke trafiek? Welke poorten?
- Gecontroleerde toegang?
- Detectie van potentiële dreigingen?
- Full Managed / Monitored Network?
- Redundantie?
- Performantie?
- Veilig?
- Volgens de Regels?
- Stabiel?

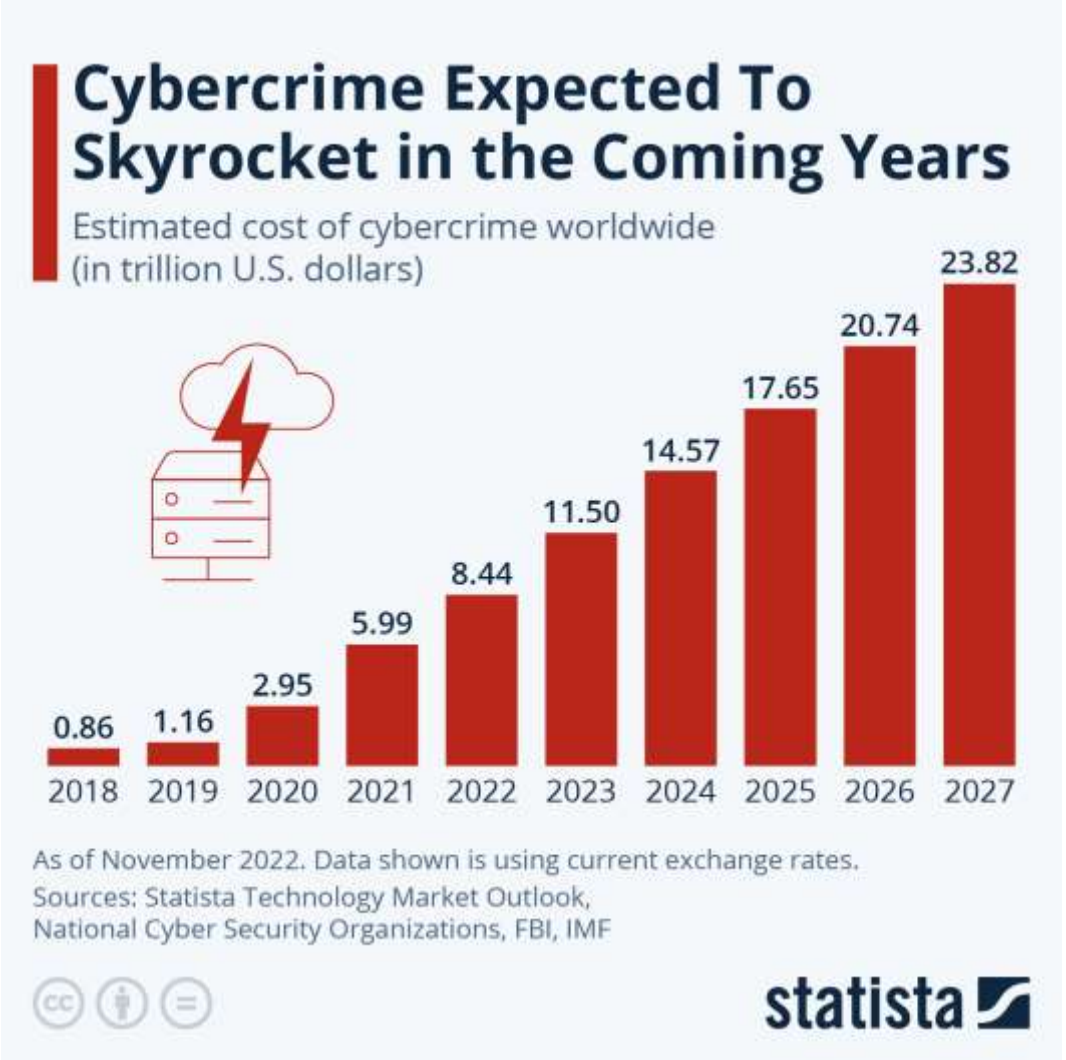
Uitdagingen

- Alles is geconnecteerd
- Beveiligen en toch werkbaar blijven
- Omgaan met groeiende complexiteit
- Vraag naar Bandbreedte
- Continue Optimalisatie
- Verantwoorden investering = €€€€ / $$$$
- Overzicht behouden - Visibiliteit

Bedreigingen

- DDoS Aanval (Distributed denial of service)
- Kwaadwillige Software (Virus)
- Privacy
- Phishing (voordoen als)
- Data integriteit – Ransomeware (manipulatie van data)
- Interne aanvallen (menselijke fouten)
- Security kwetsbaarheden (gekende veiligheidslekken aanvallen)
- OT Attacks (stuxnet)
- Toestel/Traject Falen

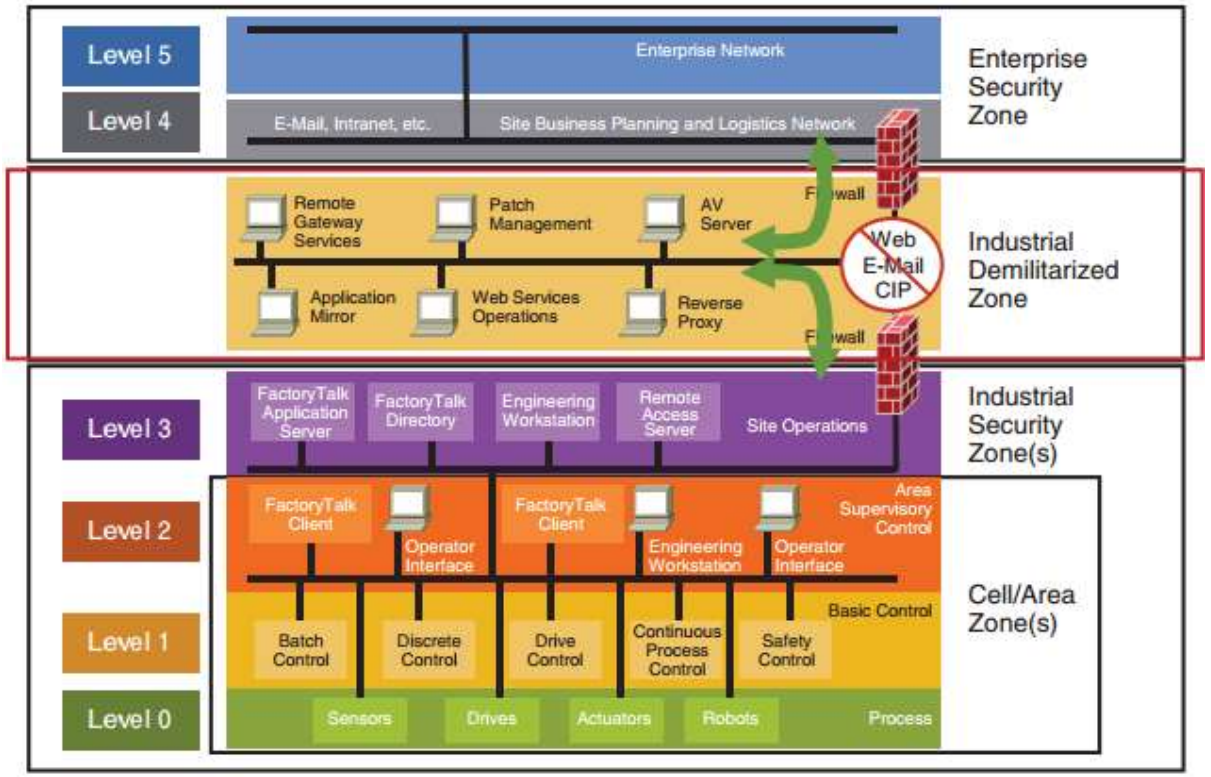
Bedreigingen



Gevolgen

- Downtime
- ~~€€€€€€€€€€~~ / $$$$$$$$$
- Verlies van Data / Productie
- Bankroet
- Ramp

Wetgeving / Richtlijnen



Richtlijnen

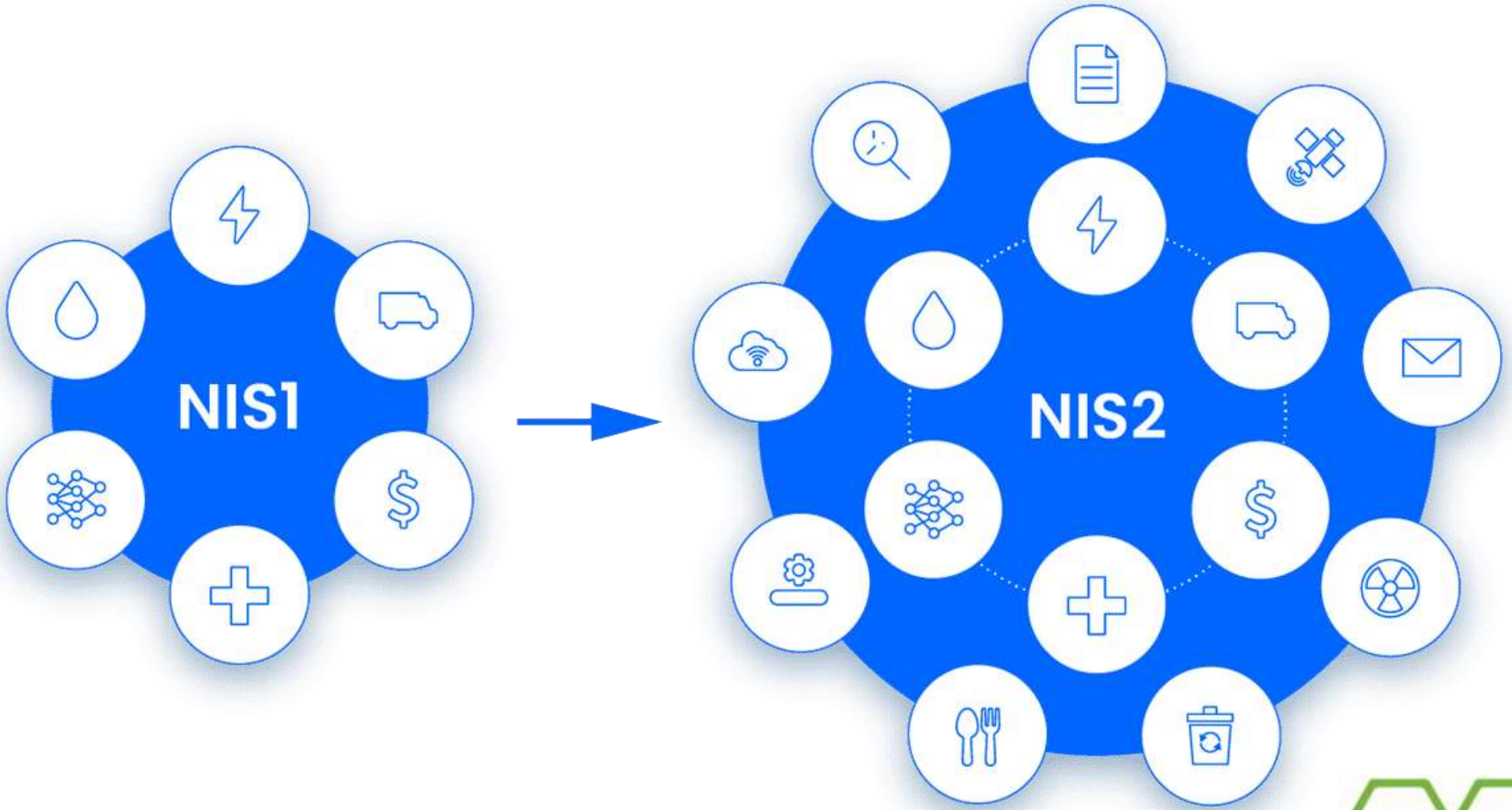
- **ISO 27001** is een ISO standaard waarin wordt beschreven hoe Informatiebeveiliging procesmatig ingericht zou kunnen worden
- De **IEC 62443**-standaard is bedoeld om Industrial Automation & Control Systems (IACS) te beveiligen. Het biedt een systematische en praktische aanpak die elk aspect van cyberbeveiliging voor industriële systemen omvat.
- De **NIST** Cybersecurity Framework kan een organisatie helpen bij het starten of verbeteren van hun cyberbeveiligingsprogramma. Gebaseerd op praktijken waarvan bekend is dat ze effectief zijn, kan het organisaties helpen hun cyberbeveiligingshouding te verbeteren

Wetgeving NIS2 - Doel

Wettelijk technische verplichtingen om het algemene niveau van cyberbeveiliging in de EU te verhogen

- Risico op cyberaanval verminderen
- Data beveiligen
- Gevolgen van een aanval reduceren

Wetgeving NIS2 - Wie



Wetgeving NIS2 - Wie

Supply Chain

bedrijven welke producten en diensten toeleveren aan de essentiële en belangrijke entiteiten

Sector	Subsector	Jurisdiction	NIS-1 & CER entities (+ equivalent)	Large entities (more than 250 employees **or** more than 50 million revenue)	Medium (more than 50 employees **or** more than 10million revenue)	Small & Micro
Annex I: Sectors of high criticality						
1. **Energy**	Electricity; district Heating &cooling; Gas; Hydrogen; oil;	The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as essential or important by national authorities** due to sole service, significant impact, essential to society
2. **Transport**	Air; Water; Rail; Road					
	Special case: Public Transport: **only** if identified as CER					
3. **Banking**	Credit institutions **(attention: DORA lex specialis)**					
4. **Financial Market Infrastructure**	Trading venues, central counterparties **(attention: DORA lex specialis)**					
5. **Health**	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency					
	Special case: entities holding a distribution authorization for medicinal products: **only** if identified as CER					
6. **Drinking Water**						
7. Waste Water	(only if it is an essential part of their general activity)					
8. **Digital Infrastructure**	Qualified trust service providers			Essential		
	DNS service providers (excluding root name servers)	**One stop**: Only the MS where they have their main establishment		Essential		
	TLD name registries					
	Providers of public electronic communications networks	Member State in which they **provide their services**		Essential		Important, except if identified as essential based on National risk assessment
	Non-qualified trust service providers	The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as essential or important**
	Internet Exchange Point providers					
	Cloud computing service providers	**One stop**: Only the MS where they have their main establishment				
	Data centre service providers					
	Content delivery network providers					
8a. ICT-service management	Managed (Security) Service Providers					
9. Public Administration entities	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security).	MS that established them		Essential		
	Of regional governments: risk based. (Optional for Member States: of local governments)			Important, except if identified as essential by Member State		
10. Space	Operators of ground-based infrastructure (by MS)	The Member State(s) where it is established		Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as essential or important**
Annex II: other critical sectors						
1. Postal and courier services		The Member State(s) where it is established	Essential	Important, except if identified as essential by Member State		Not in Scope, **except if identified as essential or important by national authorities** due to sole service, significant impact, essential to society
2. Waste Management	(only if principal economic activity)					
3. Chemicals	Manufacture, production, distribution					
4. Food	Production, processing and distribution					
5. Manufacturing	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)					
6. Digital providers	online marketplaces, search engines, social networking	**One stop**: Only the MS where they have Main establishment				
7. Research	Research organisations **(excluding education institutions)**	Member State(s) where established				

Wetgeving NIS2 – Toezicht lidstaten

Essentiële entiteiten	Belangrijke entiteiten
Proactief	Reactief - Vermoeden dat niet voldaan is
Audits	Audits
Verzoek om informatie	Verzoek om informatie
Meldingsplicht incidenten	Meldingsplicht incidenten

Wetgeving NIS2 - Sancties

Administratieve Boetes	
Essentiële entiteiten	Belangrijke entiteiten
10 000 000 €	7 000 000 €
2% van jaarlijkse omzet	1,4% van jaarlijkse omzet

Bestuurdersaansprakelijkheid bij Essentiële entiteiten

Wetgeving NIS2 - Deadline

Deadline België : 17/10/2024

CENTRE FOR CYBER SECURITY BELGIUM

https://ccb.belgium.be/en

NIST Framework

Information Security Management
ISO
27001
Certified

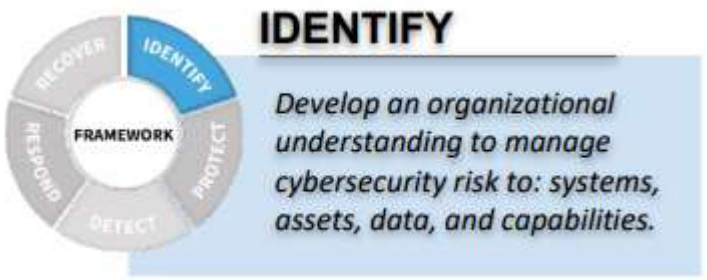
IEC®
62443-3-3

International
Electrotechnical
Commission

NIST Framework – Wat is ter beschikking

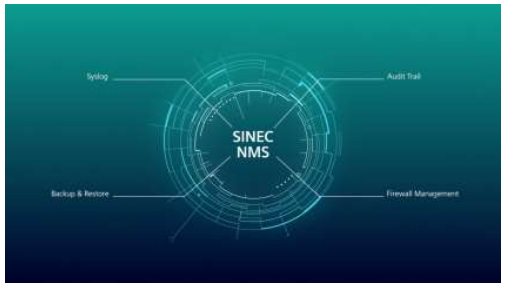
- Fysieke/Virtuele Scheiding IT/OT
- VLAN separatie
- Redundantie
- Toegangcontrole Lokaal (Radius/NAC) & Remote (SRA)
- Firewalls
- Managed switches
- NMS – Network Management System
- RMM/EPP - Endpoint Protection / Management / Monitoring / Patching
- CTD – Continuous Thread detection (Visibiliteit)
    - Poorten – Firmware/Updates/Versies – trafiek – netwerk - wie met wie - protocollen - afwijkingen
- Domain controllers - Policy enforcement - Active Directory – SSO – MFA
- Backup

NIST Framework - Oplossingen



- Welke Fysieke toestellen en systemen? Intern extern
- Welke data wordt gebruikt, door wie, waar wordt de data bewaard?
- Welke communicatie & data flows?
- maatregelen / regels vooropstellen en documenteren
- Kwetsbaarheden identificeren met gebruik van externe bronnen
- Controle van leveranciers en andere 3e partijen

CLAROTY



Extreme networks

NIST Framework - Oplossingen

Intune

ninjaOne

CLAROTY

- Beheer fysieke/externe/digitale toegang tot netwerk/assets
- Authenticatie - MFA
- Encryptie
- Backups – DR plan
- EPP-updates
- Gebruikers bewust maken … opnieuw en opnieuw

VEEAM

2FA
TWO-FACTOR AUTHENTICATION

Windows Defender

Bitdefender

SentinelOne

NIST Framework - Oplossingen

ninjaOne

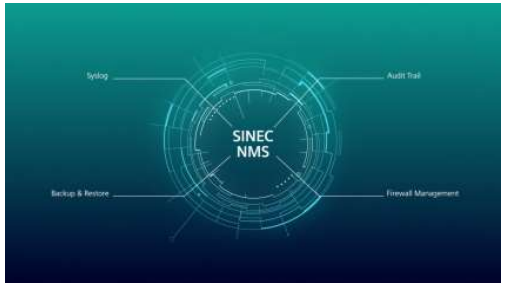
Intune

Zoek continue naar ongeoorloofde users of devices.

Zorg voor monitoring en logging en bewaar de logs om terug te kunnen gaan in de tijd.

Ken de te verwachten trafiek flows in je netwerk.

Wees alert als er onverwachte zaken of abnormale trafiek gedetecteerd wordt



Windows Defender

CLAROTY

Bitdefender

SentinelOne

NIST Framework - Oplossingen

RESPOND

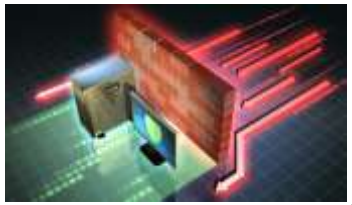
Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Maak een response planning (wie doet wat) zorg eventueel voor hulp van 3rd party

Zorg voor een communicatieplan (overheid, partners, contractors, pers …)

Communiceer duidelijk met belangrijkste partners (uitwisseling van laatste data)

Analyseer, voer plan uit en maak update van de plannen volgens wat je meemaakt



CLAROTY

Bitdefender

SentinelOne

Windows Defender

NIST Framework - Oplossingen

Communiceer duidelijk en tijdig, beheers de reputatieschade

Communiceer duidelijk met belangrijkste partners (uitwisseling van alleen de benodigde en correcte data)

Voer recover plan uit en herstel de geleden schade en verbeter de uitvoeringsplannen volgens lessons learned

NIST Framework - ATS

Virtuele of Fysieke Scheiding?

- Waar zit de kennis?
- Wie heeft de resources?
- Hoe dynamisch kan IT / OT schakelen?
- Wat buiten werkuren?
- Compatibiliteit & garanties QoS bv. Profinet F(i)RT?
- Prioriteiten IT / OT?
    - Beschikbaarheid / Security / Updates / Omgeving / Omschakeltijden
- Verantwoordelijkheden?

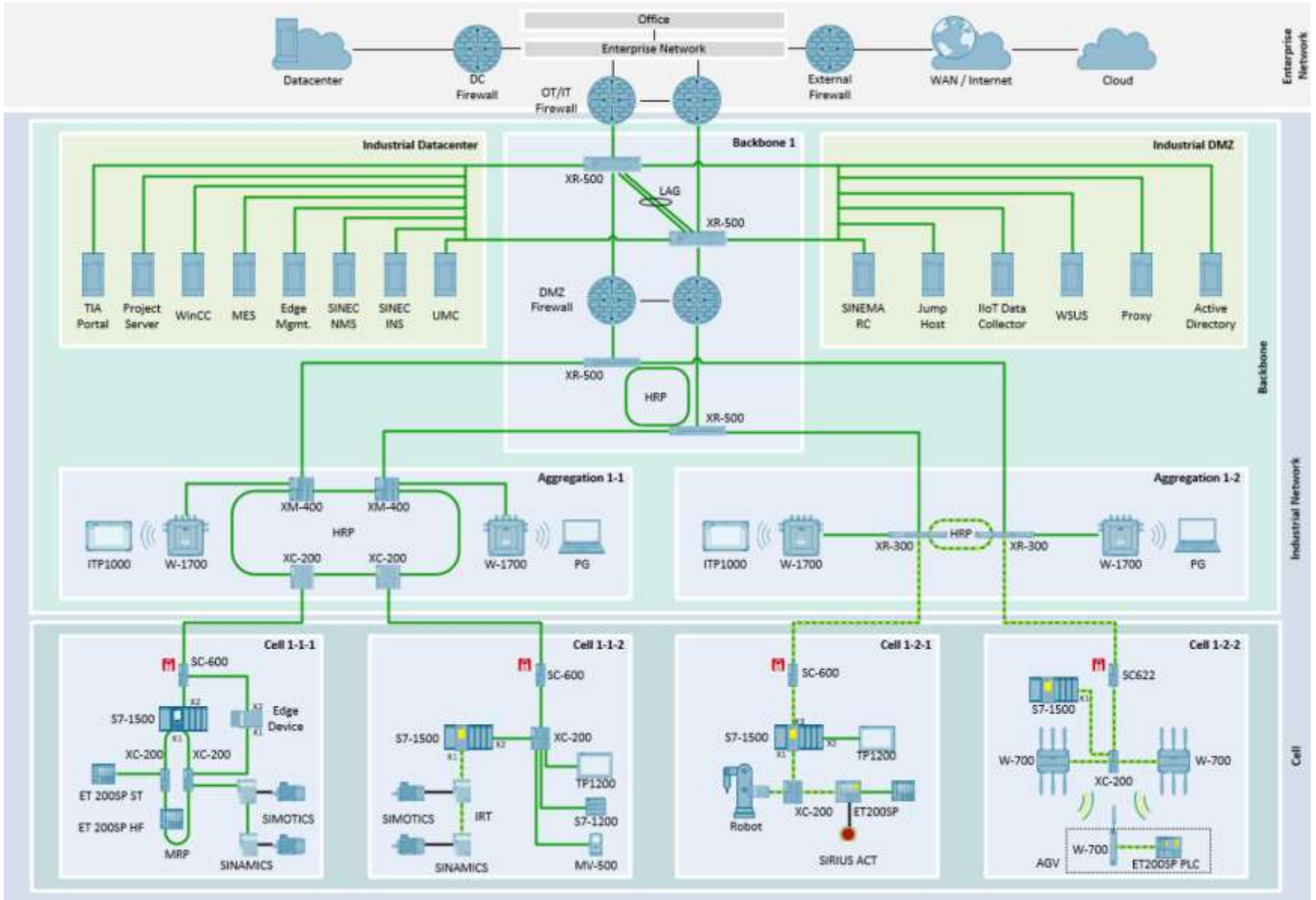
QoS – Realtime Verkeer

PCP	Priority	Acronym	Traffic types
1	0 (lowest)	BK	Background
0	1	BE	Best Effort
2	2	EE	Excellent Effort
3	3	CA	Critical Applications
4	4	VI	Video, < 100 ms latency and jitter
5	5	VO	Voice, < 10 ms latency and jitter
6	6	IC	Internetwork Control
7	7 (highest)	NC	Network Control

QoS - IEEE 802.1Q

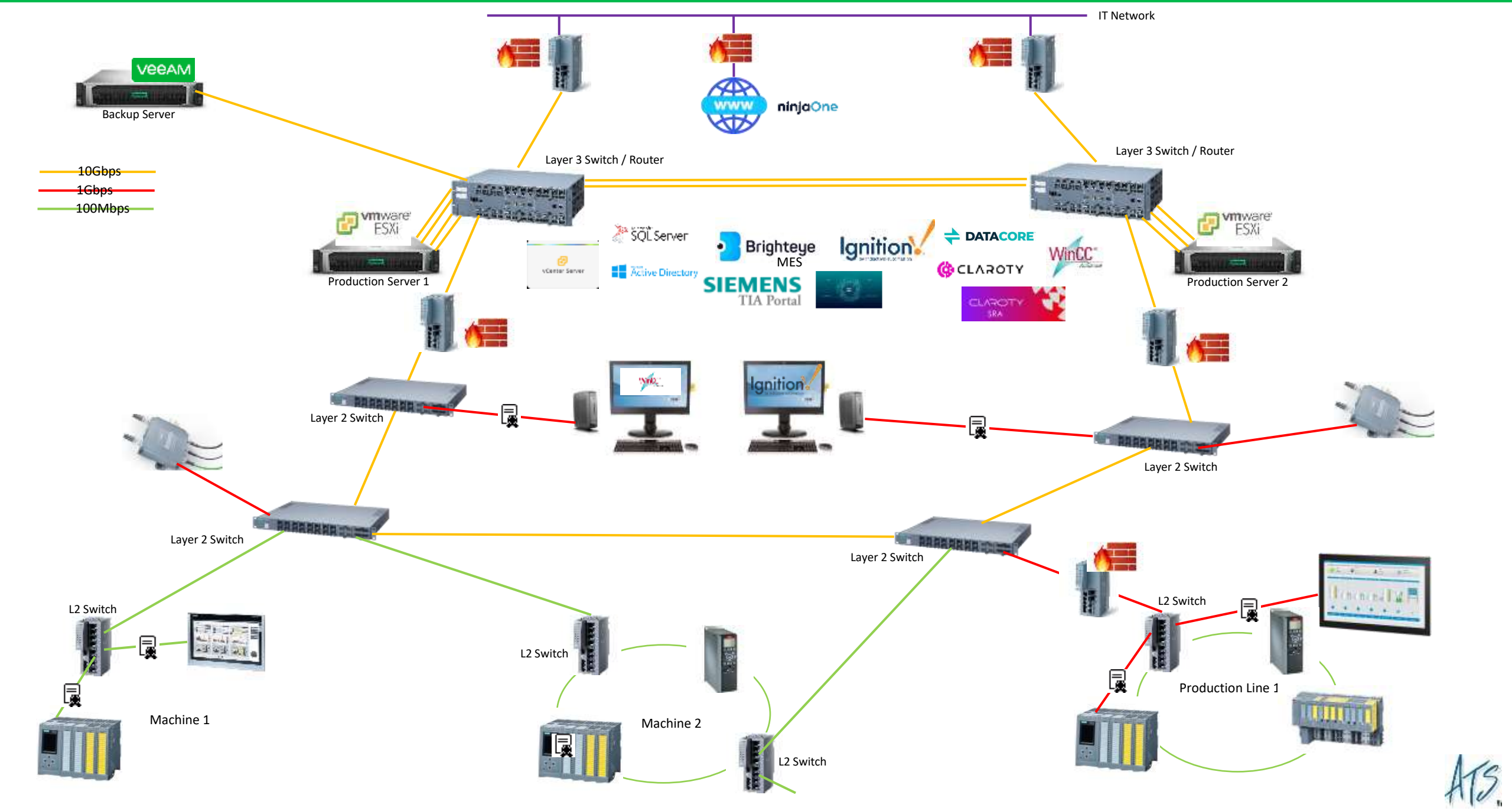
802.1D user priority	802.1D designation	802.11e access category	802.11aa transmit queue	Description
7	Network Control (NC)	VO	VO	Both time- and safety-critical, consisting of traffic needed to maintain and support the network infrastructure
6	Voice (VO)	VO	A_VO	Time-critical, characterized by less than 10 ms delay
5	Video (VI)	VI	VI	Time-critical, characterized by less than 100 ms delay
4	Controlled Load (CL)	VI	A_VI	Non-time-critical but loss sensitive, such as streaming multimedia or business-critical traffic; usually used for applications that require reservation mechanisms or admission control decisions
3	Excellent Effort (EE)	BE	BE	Also non-time-critical but loss sensitive; for best-effort services delivered to the most important customers
0	Best Effort (BE)	BE	BE	Non-time-critical and loss insensitive. This is the most common traffic type, predominant in today's networks
2	Spare (—)	BK	BK	
1	Background (BK)	BK	BK	Non-time-critical and loss insensitive, but of lower priority than best effort; includes bulk transfers and other data transfer that are permitted on the network but that should not impact the use of the network by other users and applications

OT Netwerk – Fysiek (Siemens Template)

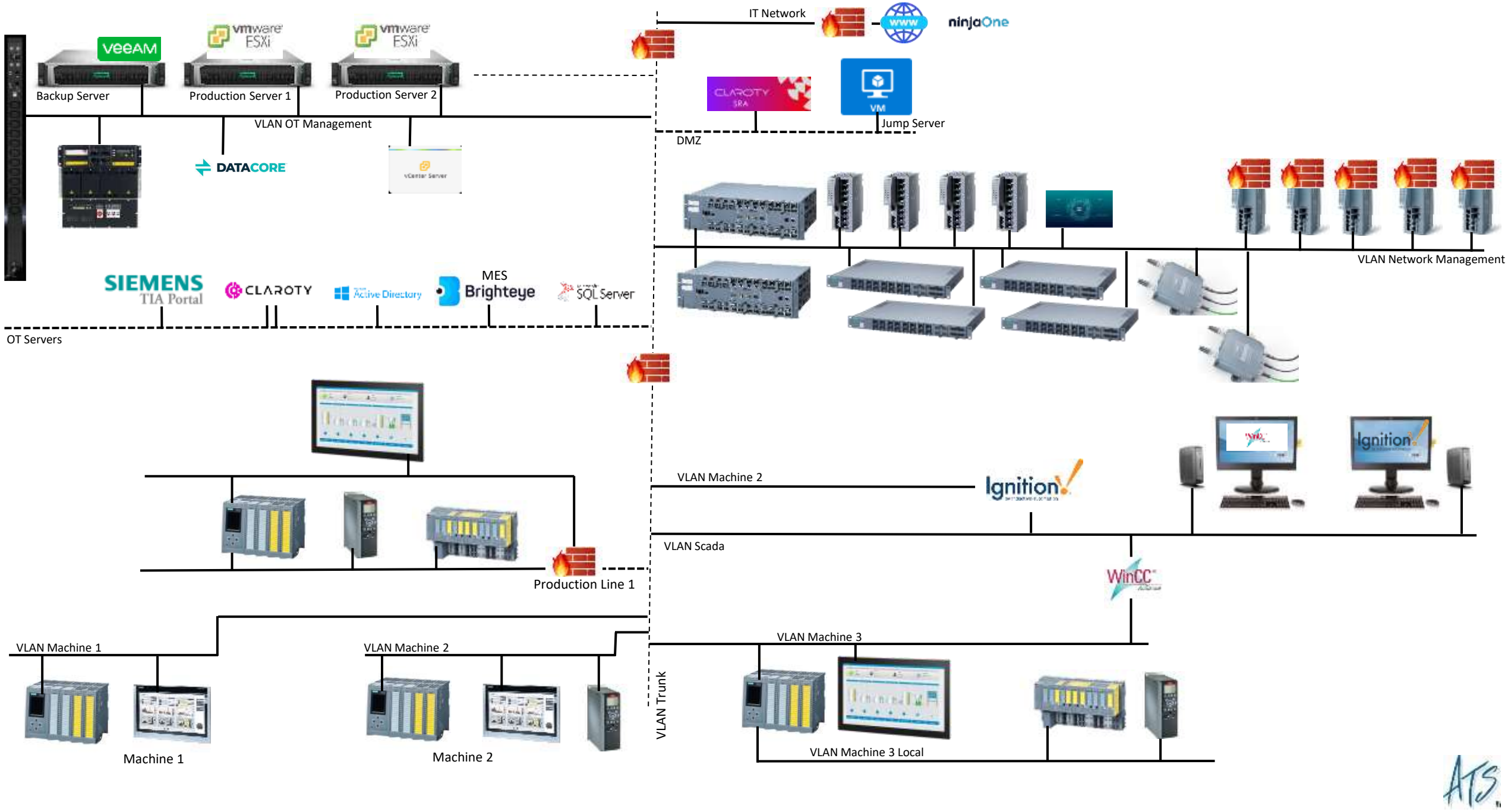


[Network concept for discrete manufacturing - ID: 109802750 - Industry Support Siemens]

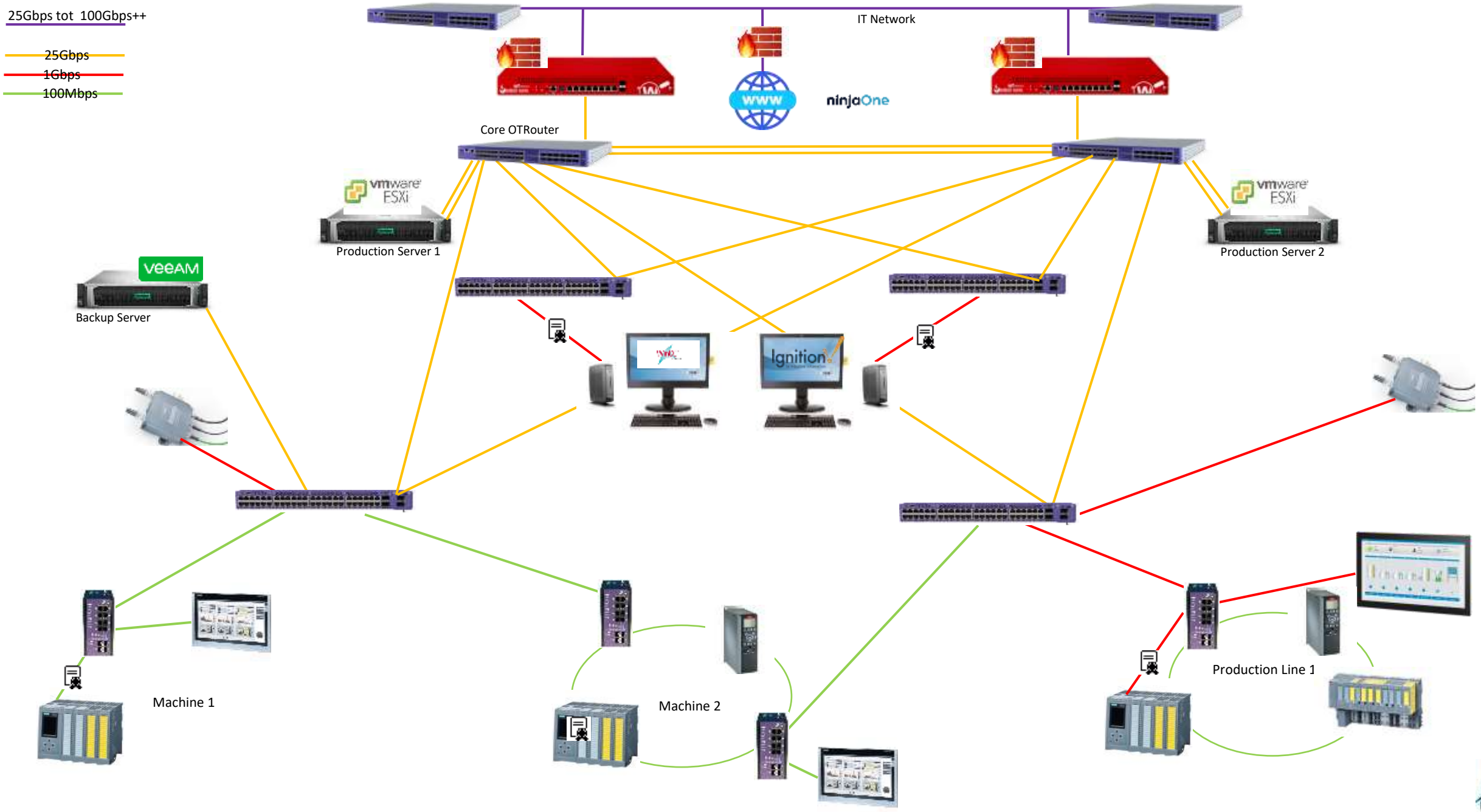
OT Netwerk – Fysiek Voorbeeld



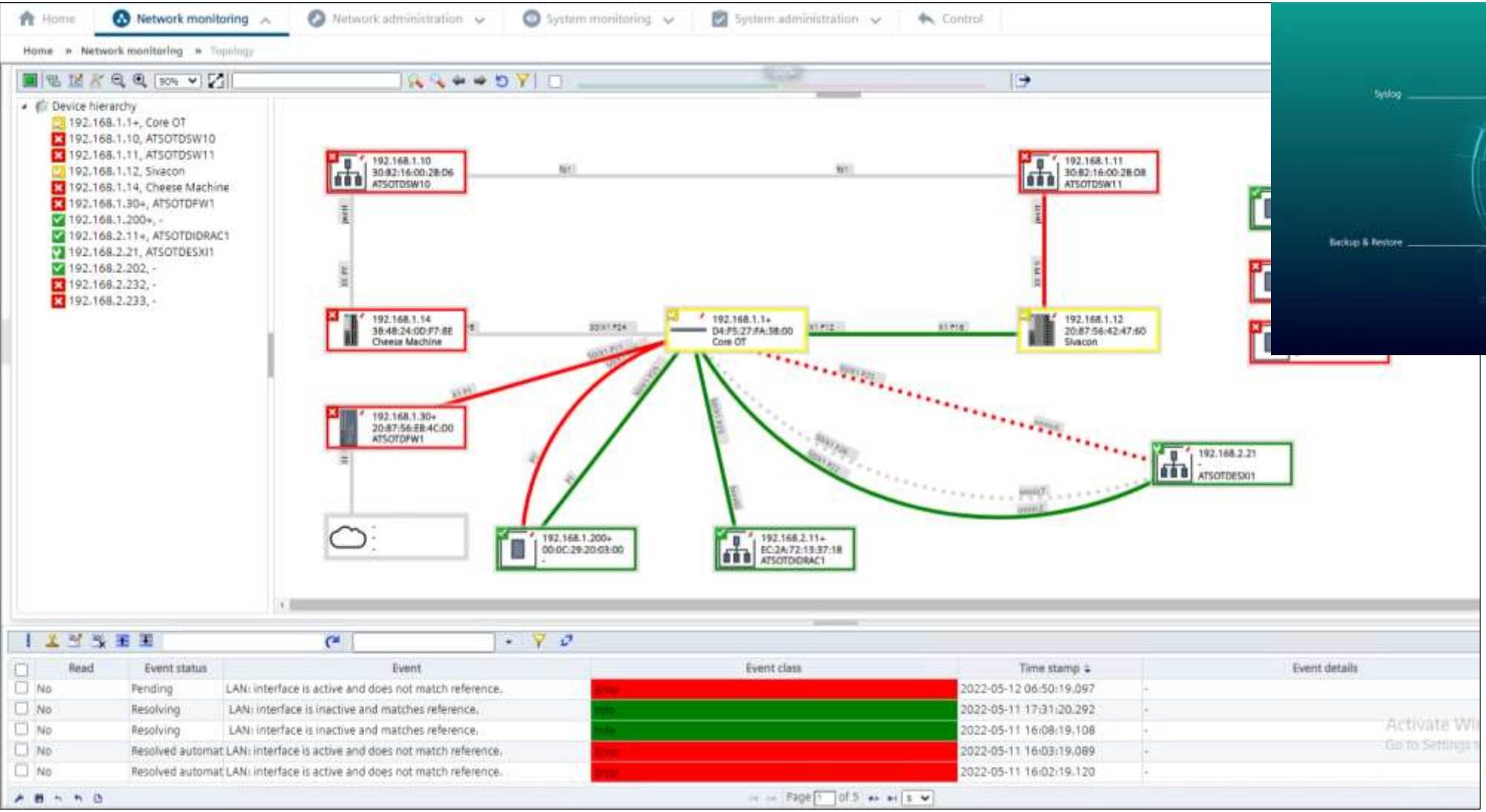
OT Netwerk – Logisch Voorbeeld

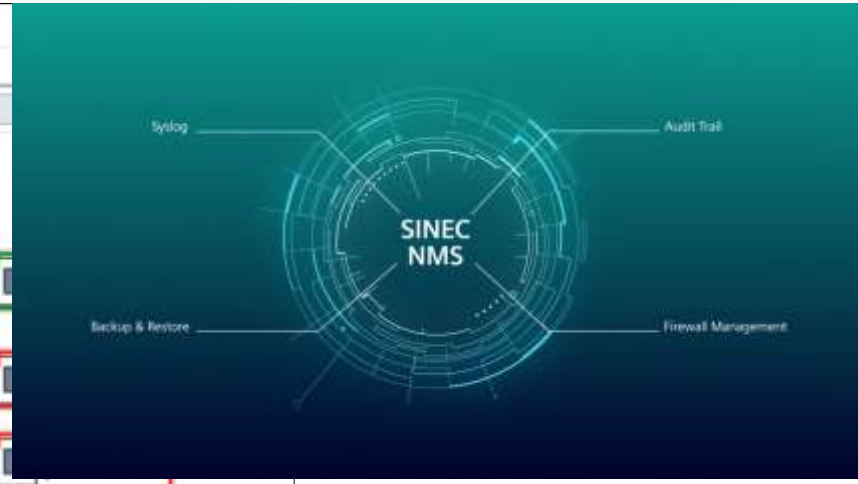


OT Netwerk – VRF Virtueel gescheiden OT Netwerk

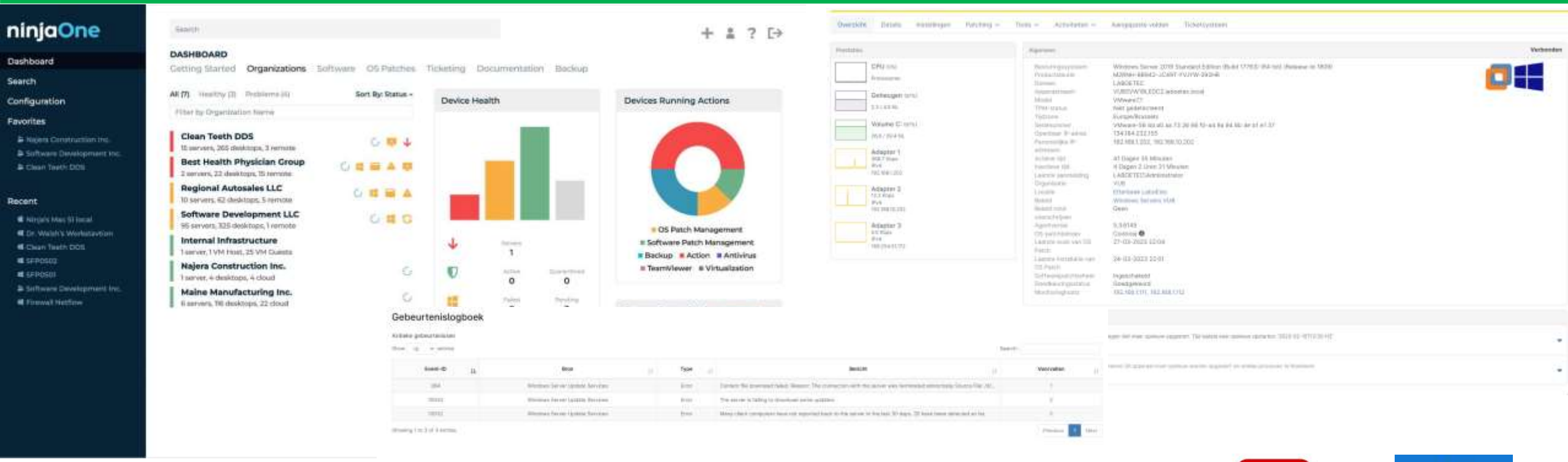


OT Netwerk - NMS





OT Netwerk – RMM - EPP



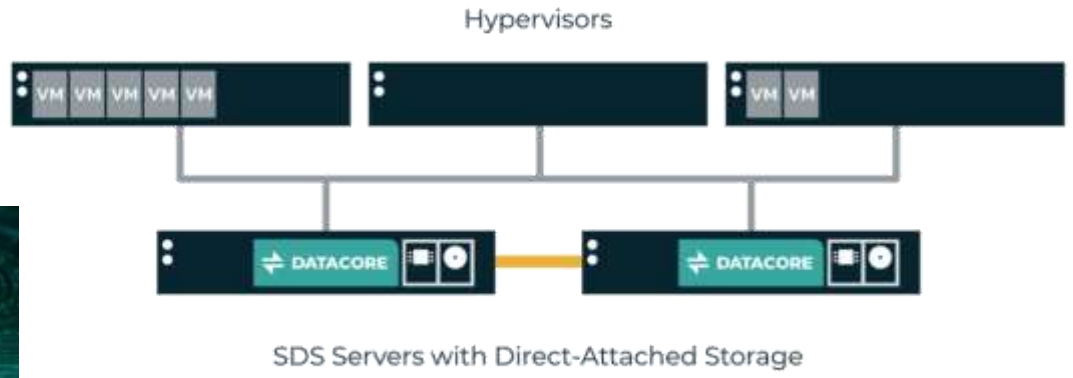
SentinelOne

Bitdefender

Windows Defender

OT Netwerk – Redundante HA Infrastructuur

DATACORE



SDS Servers with Direct-Attached Storage

OT Netwerk – Siemens Certified Partner

Claroty

Erwin Schürmann

Solution Engineer

erwin.s@claroty.com

CLAROTY

xDome

Claroty xDome is a highly flexible, modular SaaS-based solution that supports your entire industrial cybersecurity journey.

Edge

As one of our five flexible asset discovery methods, Claroty Edge grants full visibility into your industrial environment in minutes.

SRA

Claroty Secure Remote Access (SRA) delivers frictionless, reliable, and secure remote access for internal and third-party industrial personnel.

CTD

Claroty Continuous Threat Detection (CTD) is a robust solution that delivers comprehensive cybersecurity controls for industrial environments.

A.T.S. nv, BU Automation & APS nv

Sammy Van den Meersschaut, A.T.S. nv BU Automation

OT Netwerkspecialist

sammy.van.den.meersschaut@atsgroep.be

Marnix Snijers, APS nv

IT Netwerkspecialist

marnix.snijers@aps.be

ATS Groep

Karel De Roosestraat 15

B-9820 Merelbeke

www.atsgroep.be