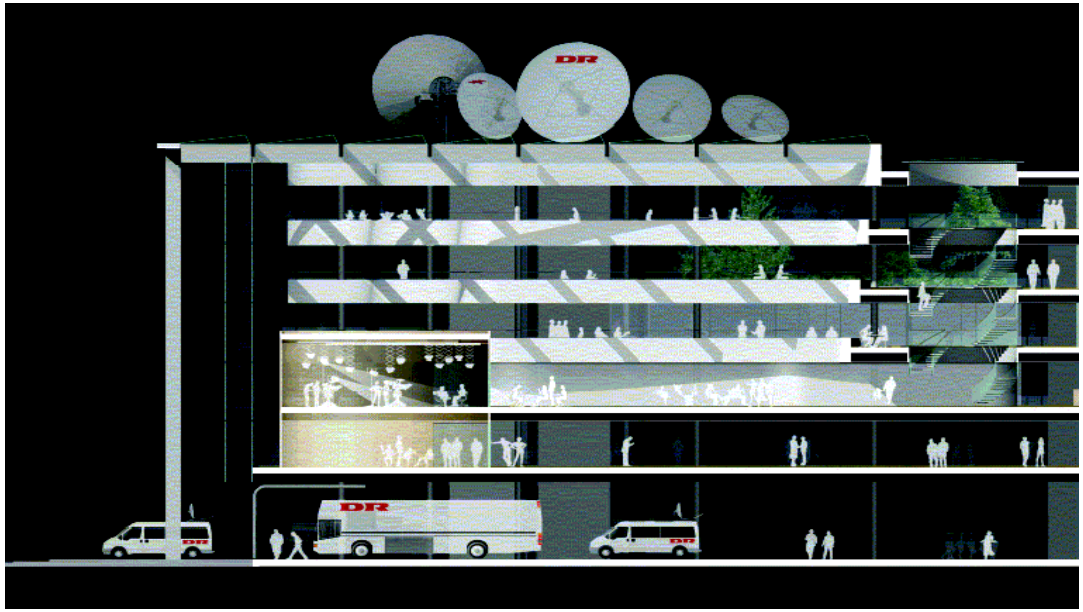
## *A case study:*

# *Protecting DRs broadcasting network*

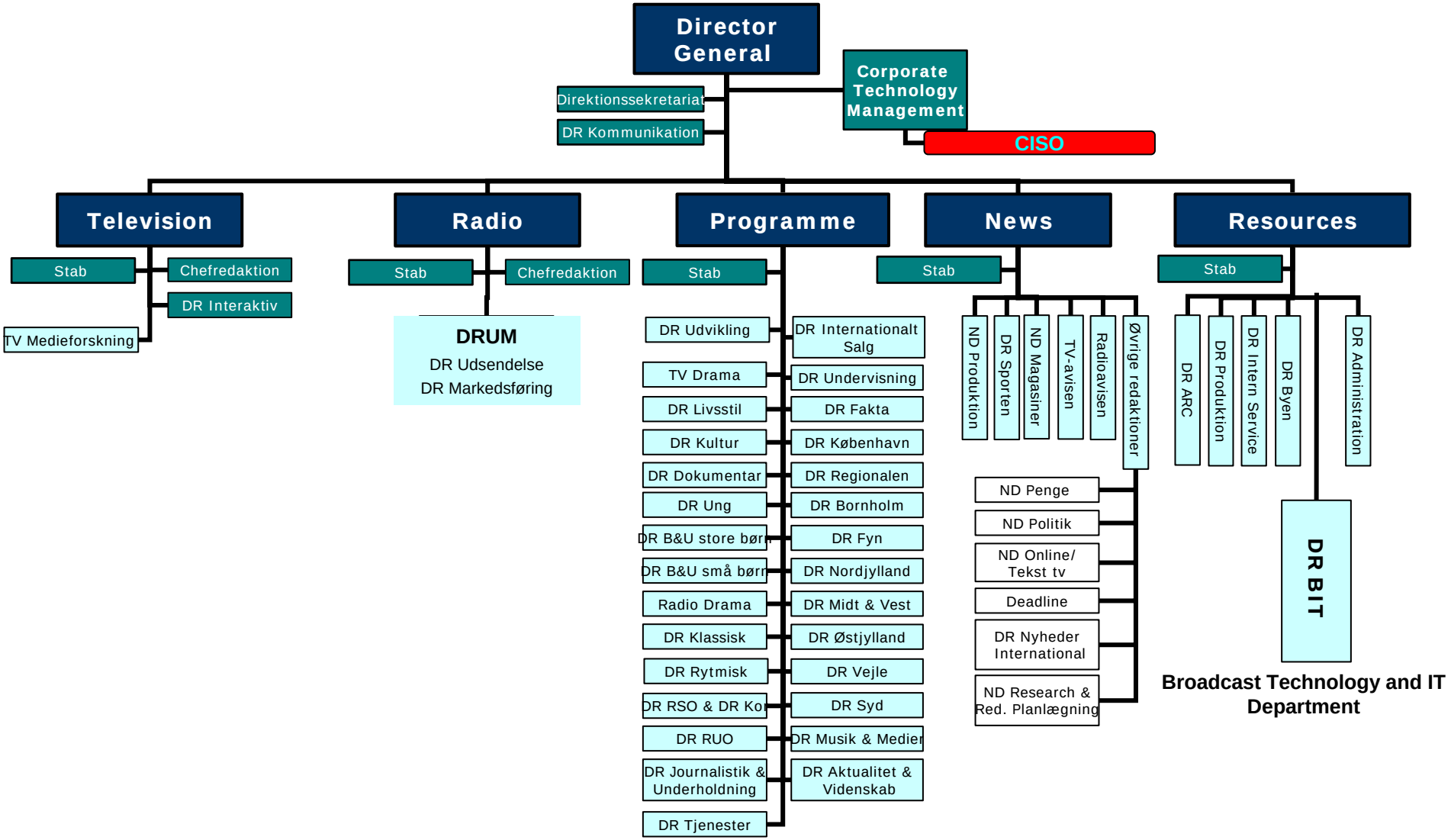

***Søren Olsen***

*CISO (Chief Security Information Officer)*


***EBU Networks 2005 - 22. June 2005 – Geneva***



# DRs Organisation



# Strategies and policies

- IT Security Policy (based on BS7799)
- IT Security Policy for use of Internet and e-mail
- IT Security Handbook (191 requirements/rules)

Approved by Executive Board and Main Works Committee

# Digitalisation

DR NYHEDER

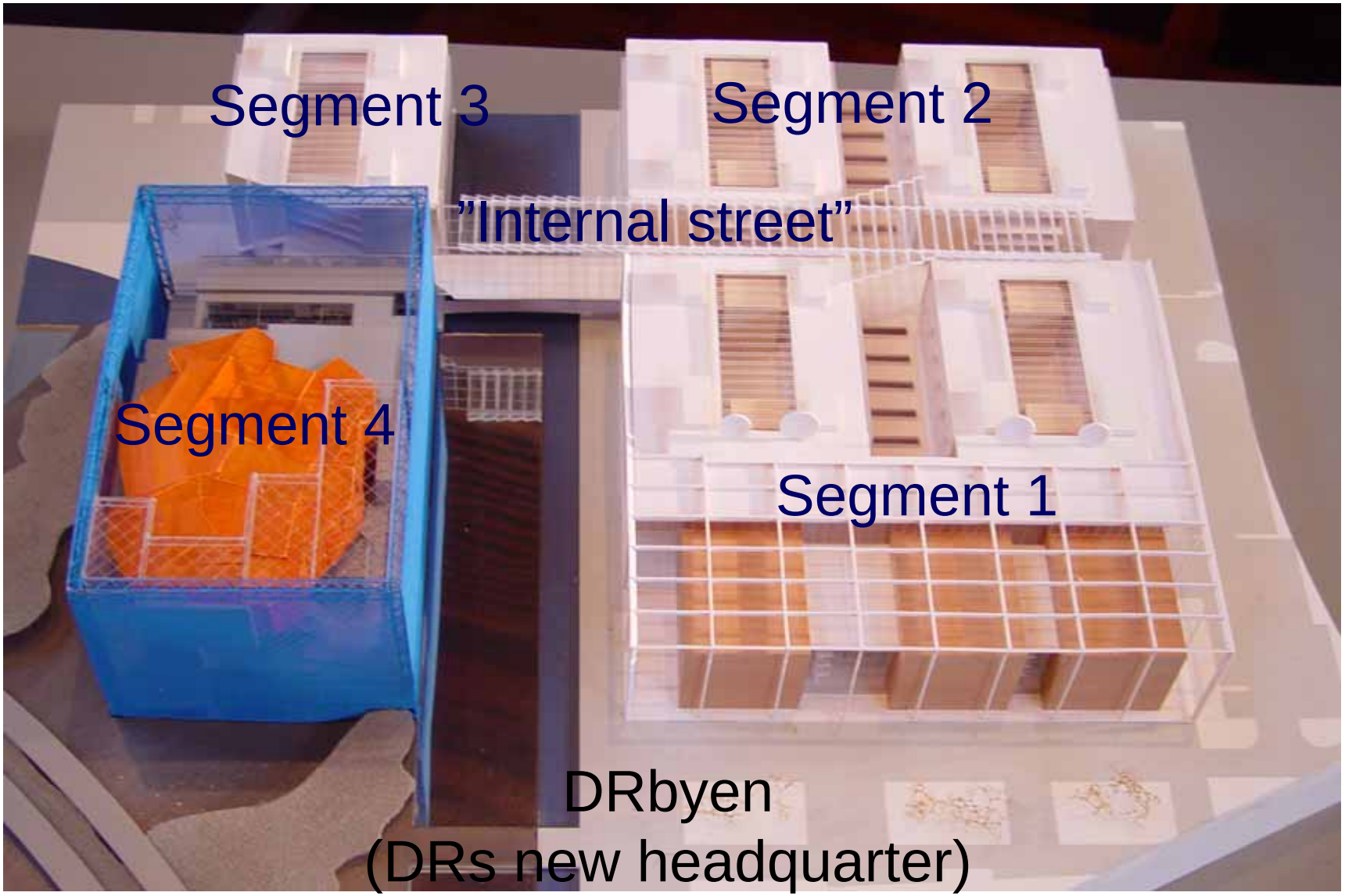
DR 1

DR 2

RADIOAVISEN

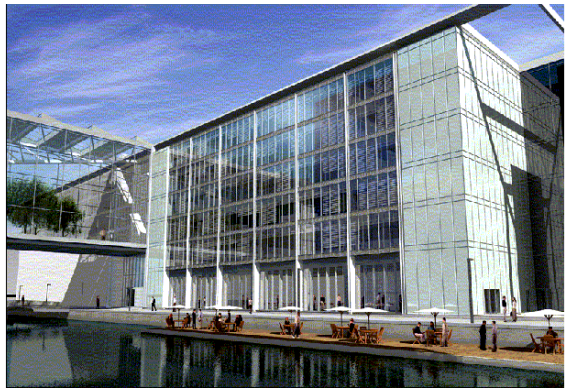
# The new DRnet design

# Practical experience of security design

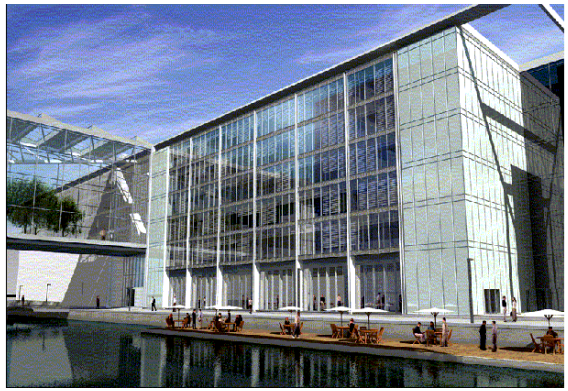


# Need of communication

- IT-communication to workstations
- IT-communication to servers
- Synchronic connection of production equipment
- Steering signals to equipment
- Technical monitoring
- Wireless communication
- WAN to other DR location
- Internal broadcasting
- Telephony
- Intercom
- BMS-system (Building Management)



# Main requirement



- Performance
- 10.000 user ports with gigabit on cobber
- 500 server ports with gigabit on cobber
- WLAN
- Stratified architecture with non blocking switch equipment
- Availability (100%)
- No single point of failure
- No service window
- Fast convergence
- Possibility to built out the capacity 4 times up
- End-to-end quality of service (QoS)
- Layer 3 segmentation
- Possibility to manage instantly (round trip delay < 10ms)
- Access security

# - and requirement equipment connecting

**Communication may not be based on broadcasting**

**Equipment connecting, may not be depending on forwarding layer 2 broadcasts between layer 3 segmental (IP subnets).**

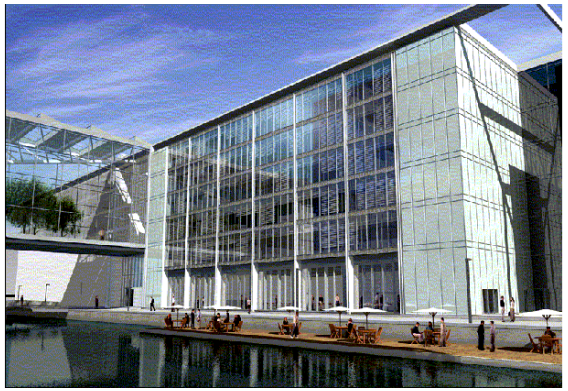
**Equipment connecting, may not be depending on forwarding layer 2 multicasts between layer 3 segmental (IP subnets).**

**802.1x**

**PoE via 802.1af**

**QoS/CoS via 802.1Q/802.1p**

**WLAN WI-FI certificated**



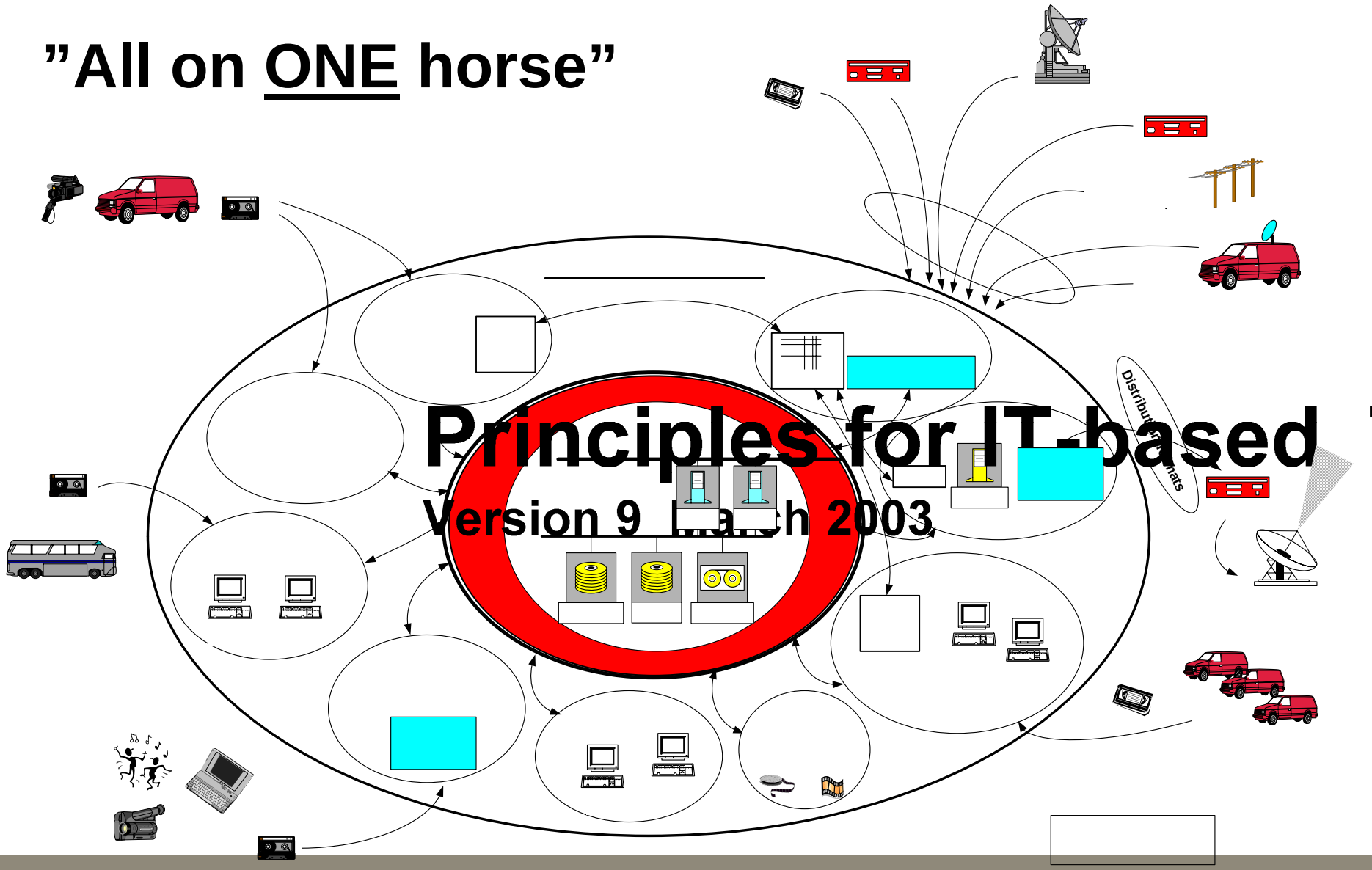
# Only ONE protocol – IP ?

- Advantage:
  - Well known and wide spread.
  - Easy communication between different equipment.
  - Only one type of network.
  - 100 % flexibility.
  - Simplified maintenance.
- Disadvantage:
  - Not instantly.
  - Not widespread in the broadcast world.

# Only ONE IP network ?

- Advantage:
  - 100 % wide spread.
  - Reach data everywhere.
  - Only one workplace.
  - 100 % flexibility.
  - Not double up regarding cabling & electronic equipment.
- Disadvantage:
  - 100 % wide spread – single point of failure.
  - Not 100% separation.

”All on ONE horse”




# Principles for IT-based T

Version 9 March 2003

# Fact

## IP based communication:

- Asynchrony data transmission
- IP telephony
- Connection to SAN
- Wireless communication (WLAN)

Not IP based

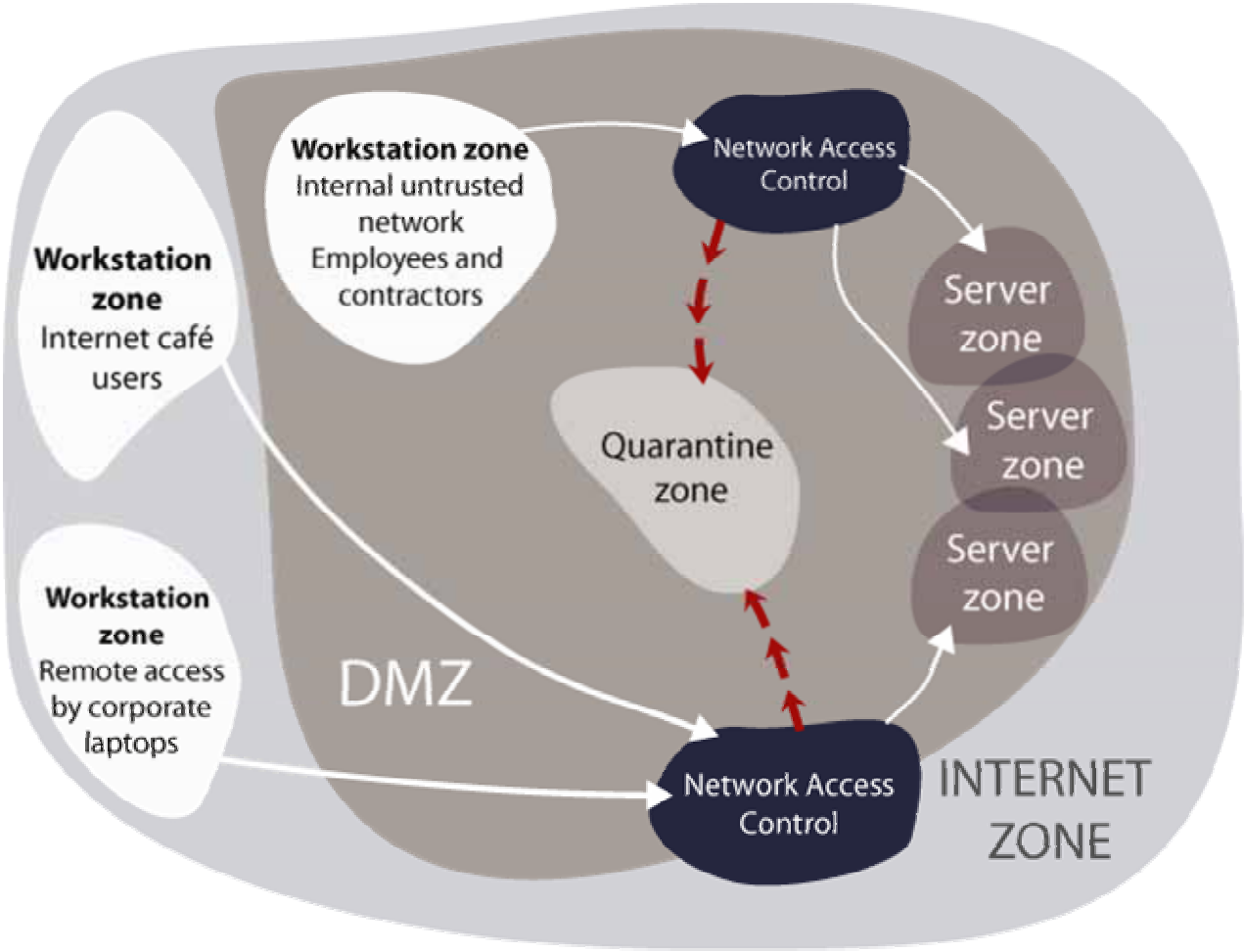
- TV-studioinfrastructure (SDI)
- Audio infrastructure (AES)
- Intercom
- Internal broadcasting

# Security elements

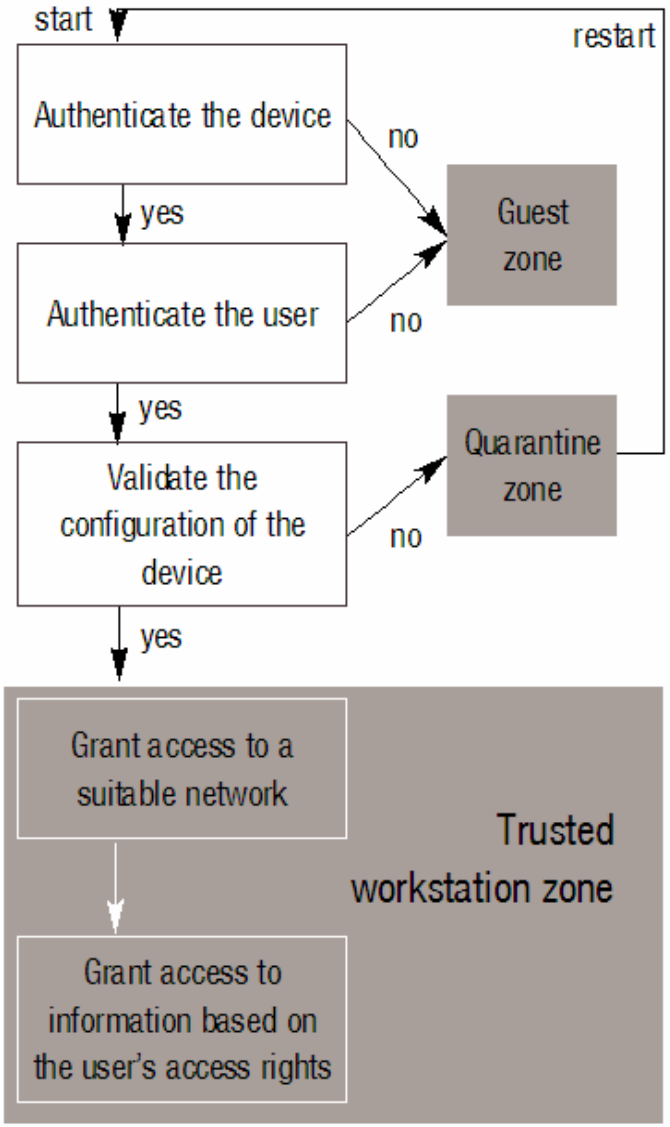
# NAC/NAP

Only those devices that meet a minimum set of security criteria can attach to the DRnet.

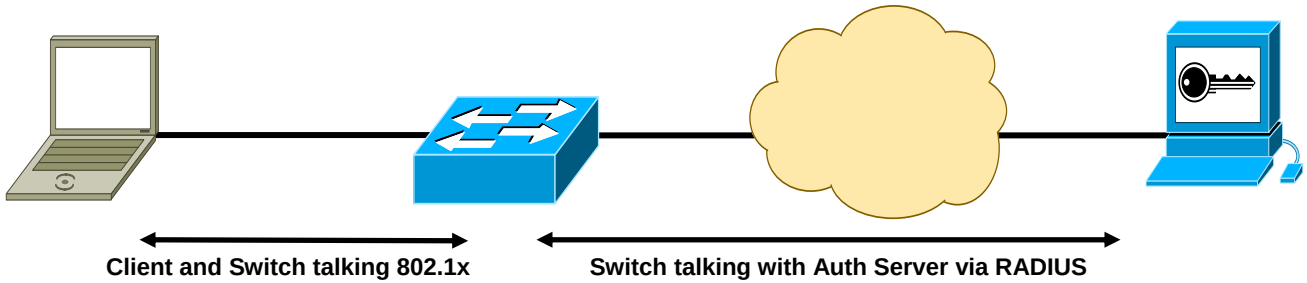
Non-compliant devices can be updated to meet the minimum set of security criteria.



# Principles – access granting process



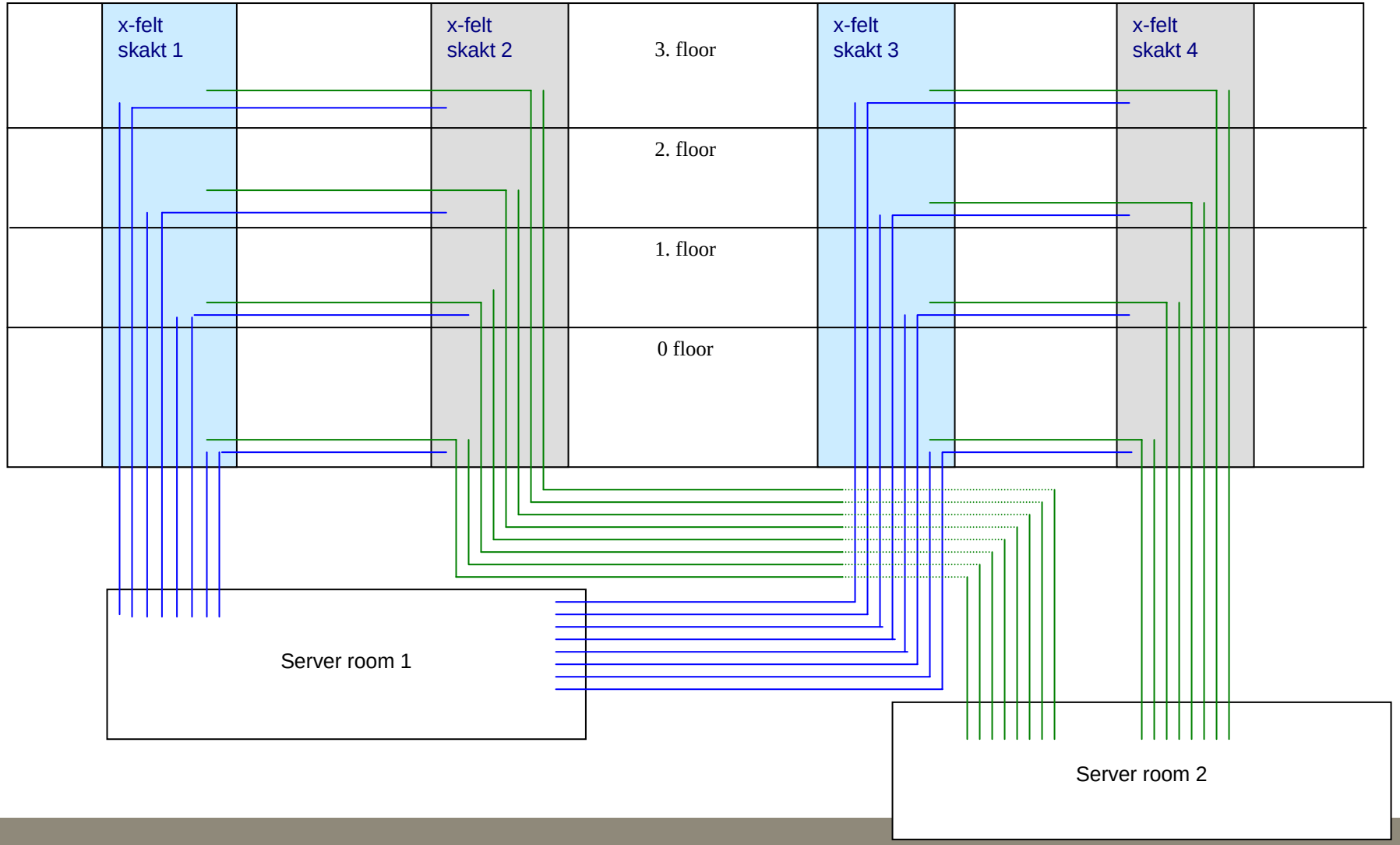
# Identity based networking services (IBNS)




## Design:

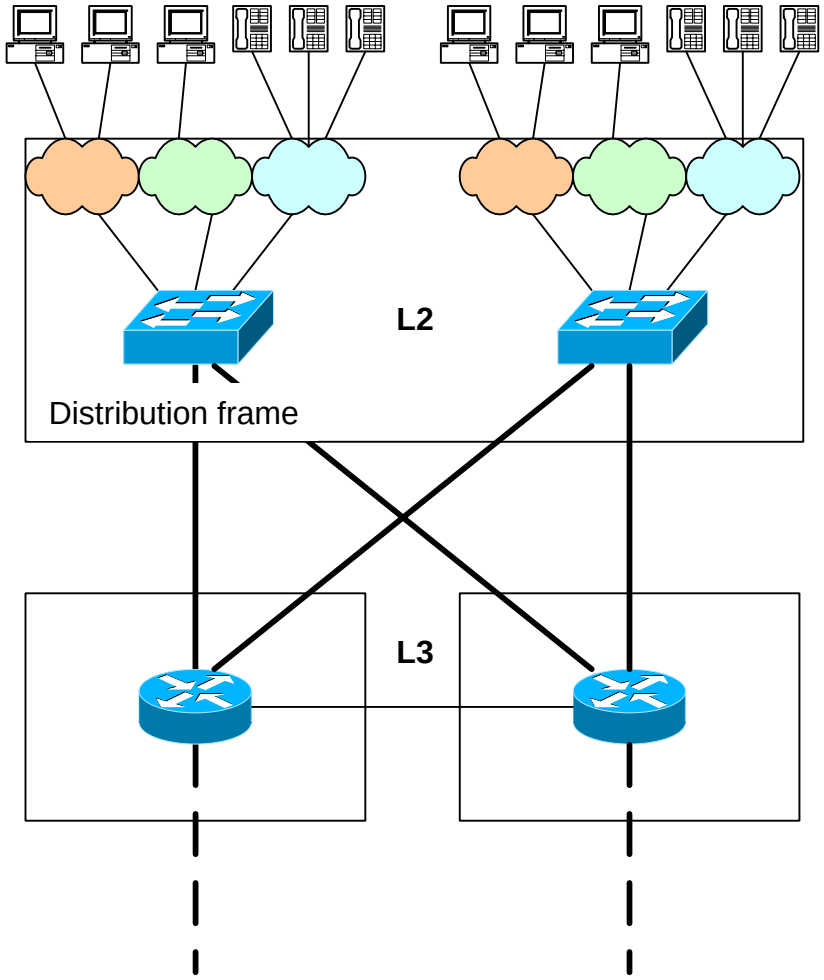
- 802.1x enables in all user Access switches, but can disables specific ports or group of ports (e.g. printers).
- 802.1x enables NOT in server access switches

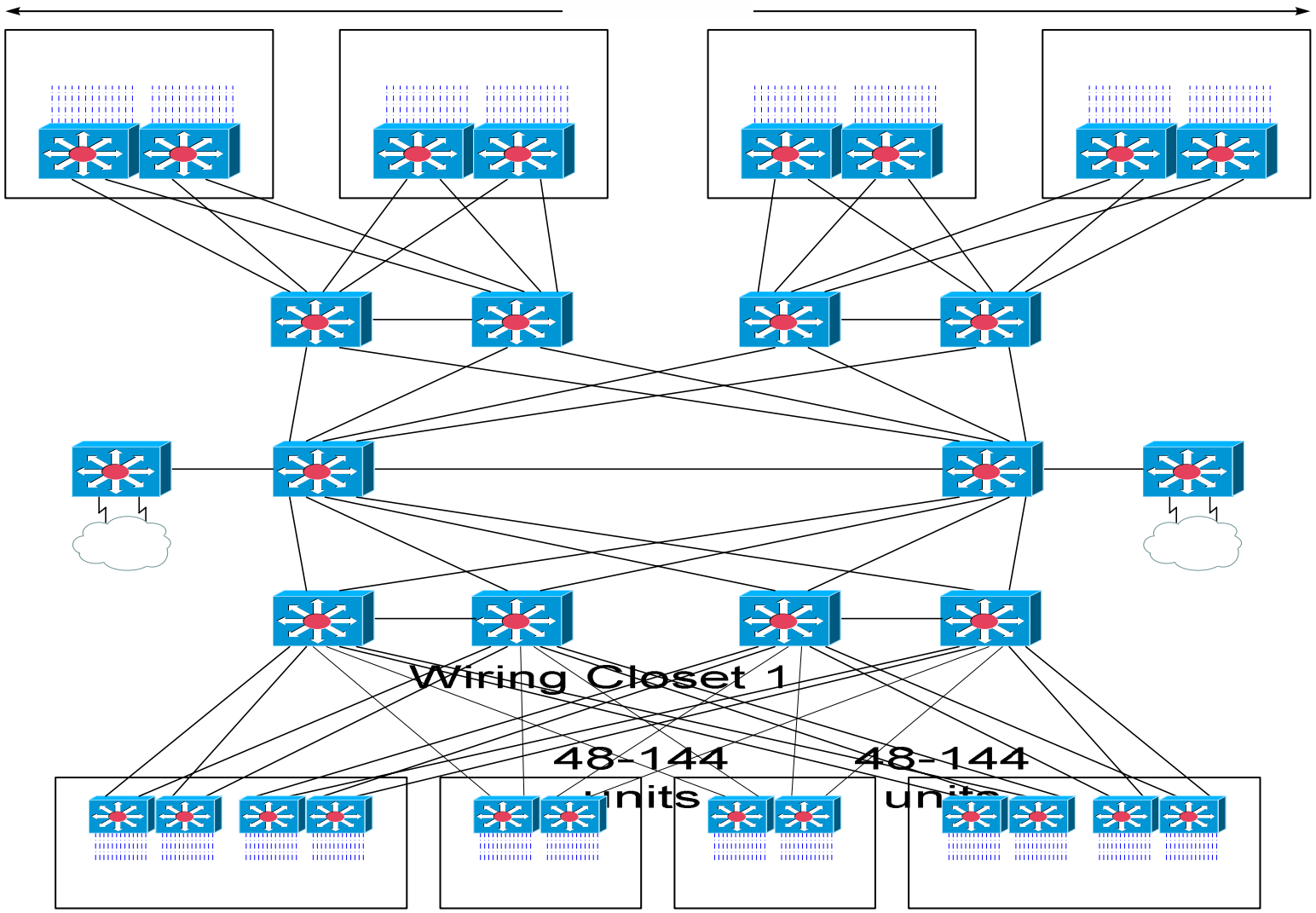
# Redundant


x-felt
skakt 1
x-felt
skakt 2
3. floor
x-felt
skakt 3
x-felt
skakt 4
2. floor
1. floor
0 floor
Server room 1
Server room 2

# Principle for access-layer

- Layer 3 border in distribution
- Redundant in first step
- No wide spread VLAN
- Security
  - IBNS (802.1x)
  - PortFast
  - BPDU Guard
  - RootGuard
  - EtherChannel Guard
  - Uni-Diredtional Link Detection
  - Loop Guard
  - Port Security
  - DHCP Snooping (planned)
  - Dynamic Arp Inspection (planned)
  - IP Source Guard (planned)

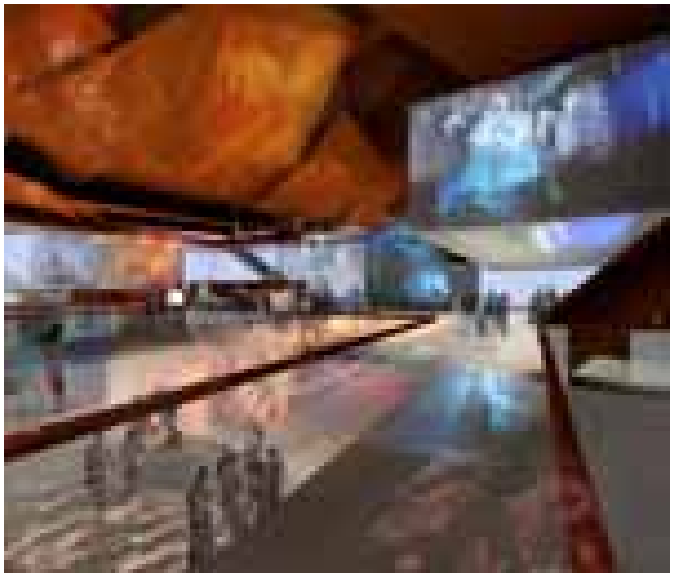



Wiring Closet 1
48-144
48-144

# QoS/Cos

(examples)

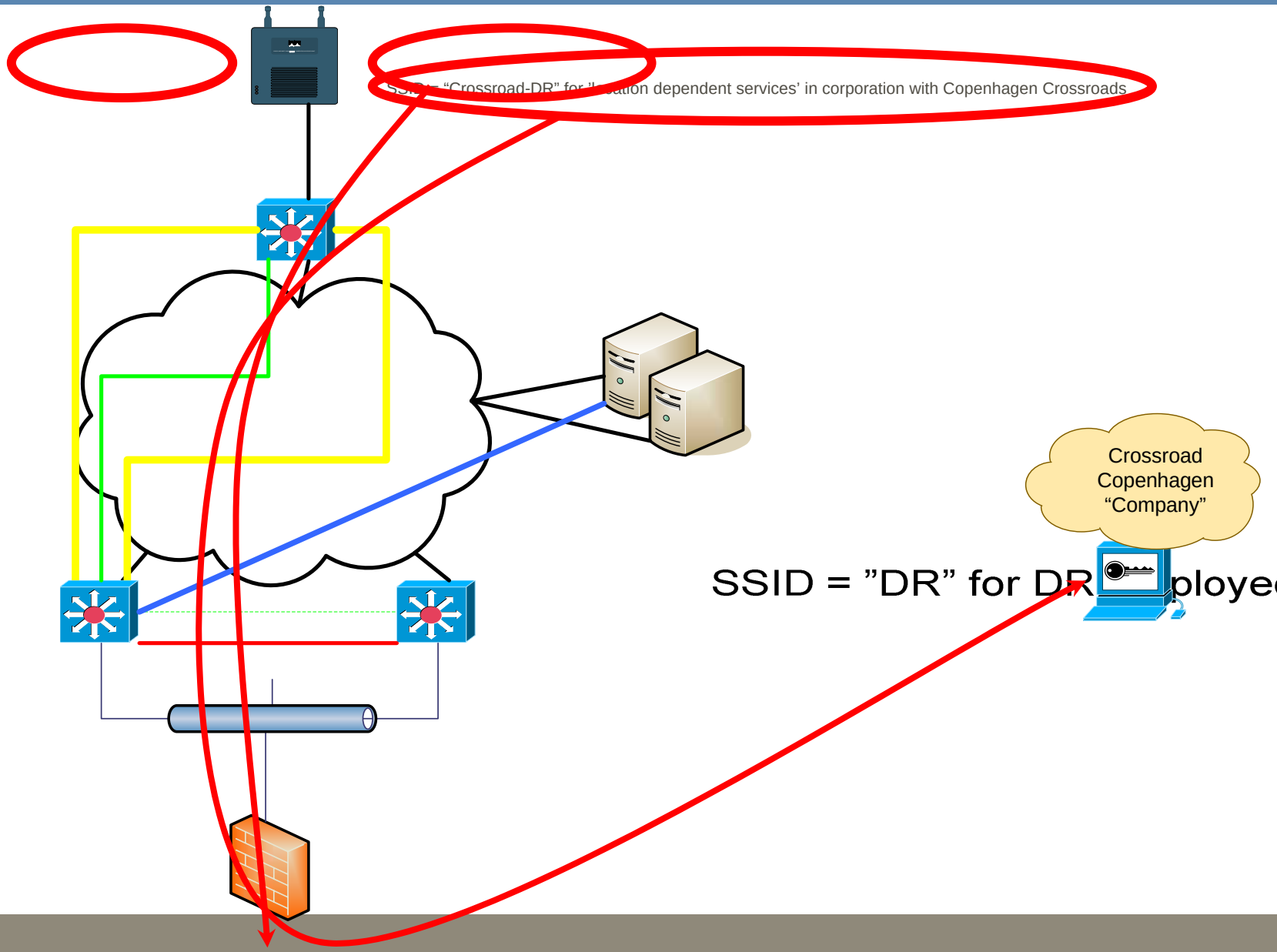
| Traffic class | DSCP |
|---|---|
| Internetwork | 48 |
| Real-time (voice) | 46 |
| Interactive video | 34 |
| Streaming | 32 |
| Mission critical data | 25 |
| Call signalling | 24 |
| Transactional data | 18 |
| Management | 16 |
| Bulk data | 10 |
| Scavenger | 8 |
| Best effort | 0 |



DSCP = Differentiated Services Code Point

# WLAN

- **Cisco AP1200**
- **100 %  all over the headquarter (700+ AP)**
- **No telephone**
- **EAP-TLS/Radius to authentication against WIN AD**
- **WLSM steering the traffic**
- **WLSE steering AP – upgrade, configuration, rouge AP**


SSID = "Crossroad-DR" for "location dependent services' in corporation with Copenhagen Crossroads
Crossroad
Copenhagen
"Company"
SSID = "DR" for DR ployee

# Question & answers

**Søren Olsen**
*CISO (Chief Security Information Officer)*
**snol@dr.dk**
**+45 3520 2872**