BUT R&T -Semestre 3

CONCEVOIR UN RÉSEAU INFORMATIQUE SÉCURISÉ MULTI-SITES

SAÉ3.Cyber03 - Présentaion

Présenté par NJIMI Faysa,
DYSHEVYY Bohdan,
HERBRECHT-BOURGOIN Clément,
BENSGHIR Khawla

Responsable : KWIATKOWSKI Laurent

Site **EST** Dep **D**

Découpage en Sous-Réseaux

Infrastructure IP

Adresse IP de départ : **192.168.32.0/21**

5 Vlans >>> **5** sous-réseaux

On rajoute 3 bits dans la partie réseau.

/21 /24

192.168.XXXX X|XXX| 0000 0000

0010 0000 >>> 192.168.32.0 /24
0010 0001 >>> 192.168.33.0 /24
0010 0010 >>> 192.168.34.0 /24
0010 0100 >>> 192.168.36.0 /24
0010 0101 >>> 192.168.37.0 /24

Découpage en Sous-Réseaux

192.168.32.0/21 en 5 sous-réseaux (/24)
pour 5 VLAN

Sous-Réseaux

Sous-Réseaux pour les VLAN 2,3,4,6 & 7 :
VLan 2 : 192.168.32.0 à 192.168.32.254
VLan 3 : 192.168.33.0 à 192.168.33.254
VLan 4 : 192.168.34.0 à 192.168.34.254
VLan 6 : 192.168.36.0 à 192.168.36.254
VLan 7 : 192.168.37.0 à 192.168.37.254

Autres Réseaux

Réseau 10.10.32.0/28
10.10.32.0 à 10.10.32.15

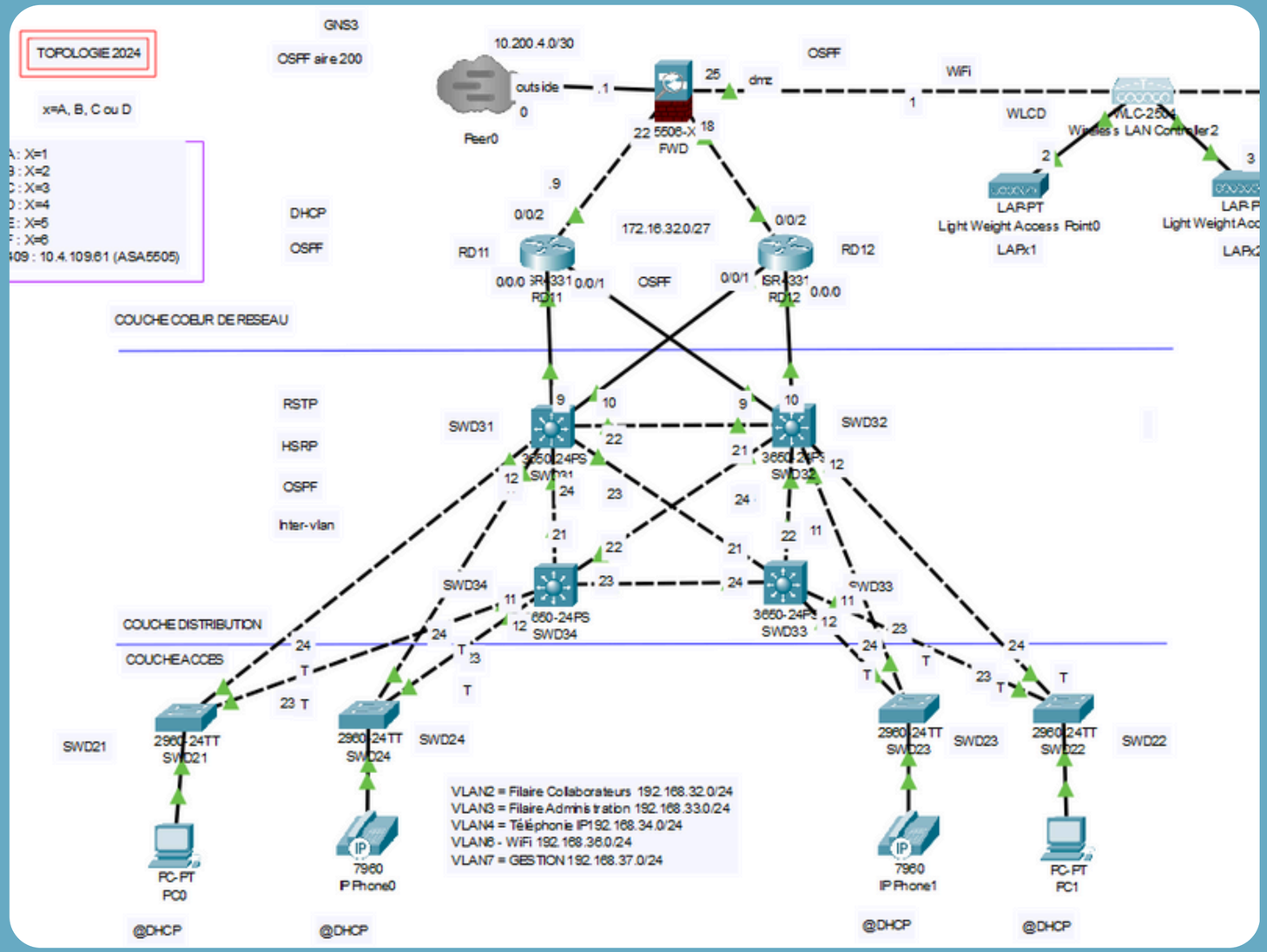
Réseau 172.16.32.0/27
172.16.32.0 à 172.16.32.31

Réseau 10.200.4.0/30
10.200.4.0 à 10.200.4.3

Plan d'Adressage IP

	@ Réseau	Masque	@ Diffusion	@ IP Disponibles	Nb Hôtes
VLAN 2	192.168.32.0	/24	192.168.32.255	192.168.32.1-254	254
VLAN 3	192.168.33.0	/24	192.168.33.255	192.168.33.1-254	254
VLAN 4	192.168.34.0	/24	192.168.34.255	192.168.34.1-254	254
VLAN 6	192.168.36.0	/24	192.168.36.255	192.168.36.1-254	254
VLAN 7	192.168.37.0	/24	192.168.37.255	192.168.37.1-254	254

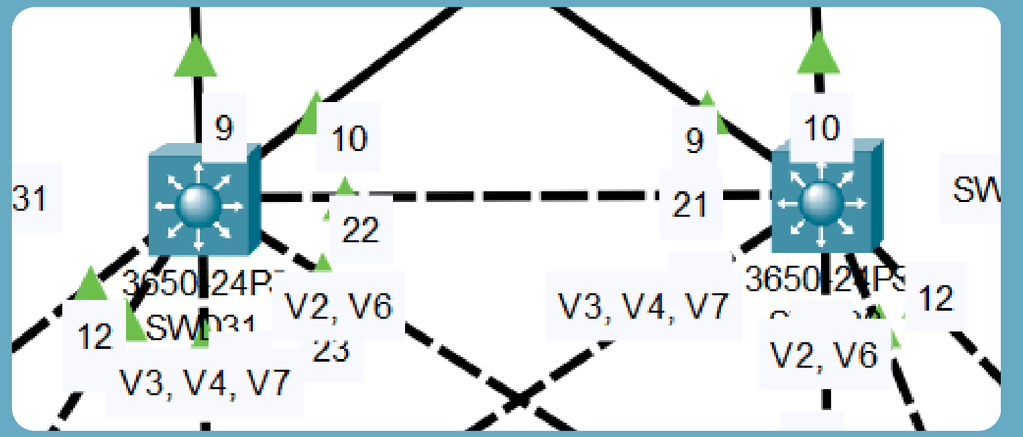
Vue d’ensemble



Mise en place de RSTP

Sur **SWD31** :
spanning-tree mode rapid-pvst
spanning-tree vlan 3,4,7 priority 24576

Sur **SWD32** :
spanning-tree mode rapid-pvst
spanning-tree vlan 2,6 priority 24576



Mise en place de HSRP

- **Tolérance aux pannes :**
- **Équilibrage de charge :**
- **Surveillances en cas de panne:**

SWD31

```
.
interface Vlan3
 mac-address 0060.7040.8c02
 ip address 192.168.33.1 255.255.255.0
 ip helper-address 172.16.32.1
 standby version 2
 standby 3 ip 192.168.33.254
 standby 3 priority 101
 standby 3 preempt
 standby 3 track fa 0/9
 standby 3 track fa 0/10
 standby 3 track fa 0/22
!
interface Vlan4
 mac-address 0060.7040.8c03
 ip address 192.168.34.1 255.255.255.0
 ip helper-address 172.16.32.1
 standby version 2
 standby 4 ip 192.168.34.254
 standby 4 preempt
!
interface Vlan5
 mac-address 0060.7040.8c04
 no ip address
!
interface Vlan6
 mac-address 0060.7040.8c05
 ip address 192.168.36.1 255.255.255.0
 ip helper-address 172.16.32.1
 standby version 2
 standby 6 ip 192.168.36.254
 standby 6 priority 101
 standby 6 preempt
```

SWD32

```
interface Vlan4
 mac-address 00d0.ff6d.2a03
 ip address 192.168.34.2 255.255.255.0
 ip helper-address 172.16.32.13
 standby version 2
 standby 4 ip 192.168.34.254
 standby 4 priority 101
 standby 4 preempt
 standby 4 track fa 0/9
 standby 4 track fa 0/10
 standby 4 track fa 0/22
!
interface Vlan6
 mac-address 00d0.ff6d.2a04
 ip address 192.168.36.2 255.255.255.0
 ip helper-address 172.16.32.13
 standby version 2
 standby 6 ip 192.168.36.254
 standby 6 preempt
!
interface Vlan7
 mac-address 00d0.ff6d.2a05
 ip address 192.168.37.2 255.255.255.0
 ip helper-address 172.16.32.13
 standby version 2
 standby 7 ip 192.168.37.254
 standby 7 priority 101
 standby 7 preempt
 standby 7 track fa 0/9
 standby 7 track fa 0/10
 standby 7 track fa 0/22
```

Mise en place de OSPF

RD11

```
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 redistribute static subnets
 network 172.16.32.0 0.0.0.3 area 0
 network 172.16.32.4 0.0.0.3 area 0
 network 172.16.32.20 0.0.0.3 area 0
```

RD12

```
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 redistribute static subnets
 network 172.16.32.8 0.0.0.3 area 0
 network 172.16.32.12 0.0.0.3 area 0
 network 172.16.32.16 0.0.0.3 area 0
```

FWD

```
router ospf 1
 log-adjacency-changes
 network 172.16.32.24 255.255.255.252 area 0
 network 172.16.32.20 255.255.255.252 area 0
 network 172.16.32.16 255.255.255.252 area 0
 network 10.200.4.0 255.255.255.252 area 200
```

SWD31

```
router ospf 1
 log-adjacency-changes
 network 192.168.32.0 0.0.0.255 area 0
 network 192.168.33.0 0.0.0.255 area 0
 network 192.168.34.0 0.0.0.255 area 0
 network 192.168.36.0 0.0.0.255 area 0
 network 192.168.37.0 0.0.0.255 area 0
 network 172.16.32.0 0.0.0.3 area 0
 network 172.16.32.8 0.0.0.3 area 0
```

SWD32

```
router ospf 1
 log-adjacency-changes
 network 192.168.32.0 0.0.0.255 area 0
 network 192.168.33.0 0.0.0.255 area 0
 network 192.168.34.0 0.0.0.255 area 0
 network 192.168.36.0 0.0.0.255 area 0
 network 192.168.37.0 0.0.0.255 area 0
 network 172.16.32.12 0.0.0.3 area 0
 network 172.16.32.4 0.0.0.3 area 0
```

Mise en place de DHCP

RD12

```
hostname RD11
!
ip dhcp excluded-address 192.168.32.1 192.168.32.9
ip dhcp excluded-address 192.168.32.254
ip dhcp excluded-address 192.168.33.1 192.168.33.9
ip dhcp excluded-address 192.168.33.254
ip dhcp excluded-address 192.168.34.1 192.168.34.9
ip dhcp excluded-address 192.168.34.254
ip dhcp excluded-address 192.168.36.1 192.168.36.9
ip dhcp excluded-address 192.168.36.254
ip dhcp excluded-address 192.168.37.1 192.168.37.9
```

```
ip dhcp pool VLAN4
 network 192.168.34.0 255.255.255.0
 default-router 192.168.34.4
 dns-server 8.8.8.8
!
ip dhcp pool VLAN6
 network 192.168.36.0 255.255.255.0
 default-router 192.168.36.6
 dns-server 8.8.8.8
!
ip dhcp pool VLAN7
 network 192.168.37.0 255.255.255.0
```

RD11

```
ip dhcp excluded-address 192.168.32.1 192.168.32.9
ip dhcp excluded-address 192.168.32.254
ip dhcp excluded-address 192.168.33.1 192.168.33.9
ip dhcp excluded-address 192.168.33.254
ip dhcp excluded-address 192.168.34.1 192.168.34.9
ip dhcp excluded-address 192.168.34.254
ip dhcp excluded-address 192.168.36.1 192.168.36.9
ip dhcp excluded-address 192.168.36.254
ip dhcp excluded-address 192.168.37.1 192.168.37.9
```

```
ip dhcp pool vlan2
 network 192.168.32.0 255.255.255.0
 default-router 192.168.32.2
 dns-server 8.8.8.8
 domain-name gtr.tp
!
ip dhcp pool vlan3
 network 192.168.33.0 255.255.255.0
 default-router 192.168.33.3
 dns-server 8.8.8.8
 domain-name gtr.tp
```

SWD31

```
interface Vlan3
 mac-address 00d0.ff6d.2a02
 ip address 192.168.33.2 255.255.255.0
 ip helper-address 172.16.32.13
 standby version 2
 standby 3 ip 192.168.33.254
 standby 3 preempt
```

(•) DHCP	( ) Static
IPv4 Address	192.168.33.6
Subnet Mask	255.255.255.0
Default Gateway	192.168.33.3
DNS Server	8.8.8.8

Sécurisation

Attaques
VLan spoofing
VLan hopping
BPDU storm
DHCP starvation
DHCP spoofing

```
ip dhcp snooping
ip dhcp snooping vlan 2,3,4,6,7
ip dhcp snooping limit rate 100
```

```
spanning-tree bpduguard enable
```

Mise en place de ACL

```
access-list allow_ping extended permit icmp 192.168.32.0 255.255.255.0 172.16.32.24
255.255.255.252 echo
access-list allow_ping extended permit icmp 192.168.33.0 255.255.255.0 172.16.32.24
255.255.255.252 echo
access-list allow_ping extended permit icmp 192.168.34.0 255.255.255.0 172.16.32.24
255.255.255.252 echo
access-list allow_ping extended permit icmp 192.168.36.0 255.255.255.0 172.16.32.24
255.255.255.252 echo
access-list allow_ping extended permit icmp 192.168.37.0 255.255.255.0 172.16.32.24
255.255.255.252 echo
access-list allow_ping extended permit icmp 172.16.32.0 255.255.255.224 172.16.32.24
255.255.255.252 echo
```

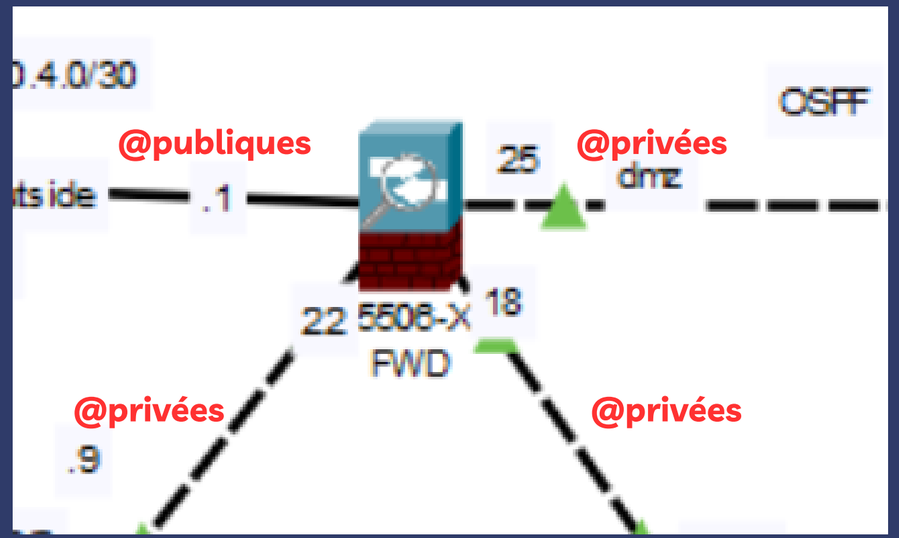
```
access-list allow_echo_reply extended permit icmp 172.16.32.24 255.255.255.252
192.168.32.0 255.255.255.0 echo-reply
access-list allow_echo_reply extended permit icmp 172.16.32.24 255.255.255.252
192.168.33.0 255.255.255.0 echo-reply
access-list allow_echo_reply extended permit icmp 172.16.32.24 255.255.255.252
192.168.34.0 255.255.255.0 echo-reply
access-list allow_echo_reply extended permit icmp 172.16.32.24 255.255.255.252
192.168.36.0 255.255.255.0 echo-reply
access-list allow_echo_reply extended permit icmp 172.16.32.24 255.255.255.252
192.168.37.0 255.255.255.0 echo-reply
access-list allow_echo_reply extended permit icmp 172.16.32.20 255.255.255.252
192.168.32.0 255.255.255.0 echo-reply
access-list allow_echo_reply extended permit icmp 172.16.32.24 255.255.255.252
172.16.32.0 255.255.255.224 echo-reply
```

```
access-group allow_ping out interface DMZ
access-group allow_echo_reply in interface DMZ
```

Mise en place de NAT

On active NAT masquerading

```
nat (inside, outside) after-auto source dynamic any interface
```



Mise en place de SSH

```
RD11(config)#username admin privilege 15 secret RocsicvtyD1112345
RD11(config)#!
RD11(config)#line vty 0 15
RD11(config-line)# transport input ssh
RD11(config-line)# login local
RD11(config-line)# exec-timeout 10
RD11(config-line)#!
RD11(config-line)#ip ssh version 2
RD11(config)#ip ssh time-out 60
RD11(config)#ip ssh authentication-retries 3
```

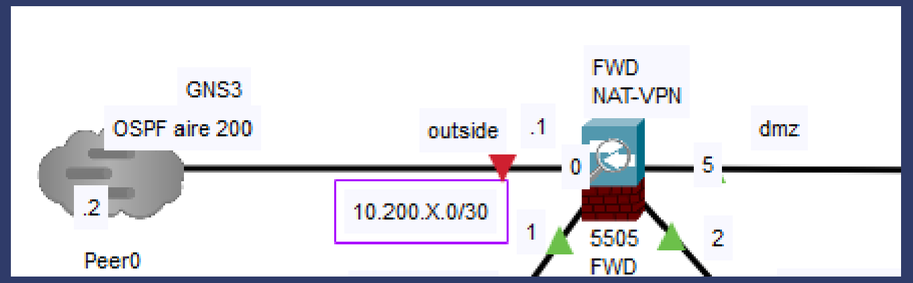
```
SWD31#ssh -l admin 172.16.32.1

Password:
Unauthorized access to this device is prohibited !
RD11#
```

Mise en place de MDP

	SWD 21	SWD 22	SWD 23	SWD 24	SWD 31	SWD 32	SWD 33	SWD 34	RD 11	RD 12	FWD
Console	Socsi cW21 12345	Socsi cW22 12345	Socsi cyW2 31234 5	Socsic W241 2345	Mocs icLS3 1123 45	Mocsi cLS32 12345	Mocsi cLS33 12345	Mocs icLS3 4123 45	Roc sic D11 123 45	Roc sicD 121 234 5	Focsi cWD 1123 45
Privilege	Sssal cW21 12345	Sssal cW22 12345	Sssal cW23 12345	Sssalc W241 2345	Mssa lcLS3 1123 45	Mssal cLS32 12345	Mssal cLS33 12345	Mssa lcLS3 4123 45	Rss alc D11 123 45	Rss alcD 121 234 5	Fssal cWD 1123 45
SSH	Socsi cvtyW 21123 45	Socsi cvtyW 22123 45	Socsi cvtyW 23123 45	Socsic vtyW2 41234 5	Mocs icvtyL S311 2345	Mocsi cvtyLS 32123 45	Mocsi cvtyL S331 2345	Mocs icvty3 4123 45	Roc sicv tyD 111 234 5	Roc sicvt yD1 212 345	Focsi cvty WD1 1234 5

Mise en place de VPN IPsec



IKE

```
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
```

```
crypto ikev1 policy 10
 hash sha
 authentication pre-share
 group 2
 lifetime 3600
 encryption des
```

```
tunnel-group 10.200.5.1 type ipsec-l2l
tunnel-group 10.200.5.1 ipsec-attributes
 ikev1 pre-shared-key SAEdept-DE
!
tunnel-group 10.200.6.1 type ipsec-l2l
tunnel-group 10.200.6.1 ipsec-attributes
 ikev1 pre-shared-key SAEdept-DF
!
tunnel-group 10.4.109.166 type ipsec-l2l
tunnel-group 10.4.109.166 ipsec-attributes
 ikev1 pre-shared-key SAEdept-D409
```

Cryptomap

```
crypto map VPN-MAP 10 match address VPN-DE
crypto map VPN-MAP 10 set peer 10.200.5.1
crypto map VPN-MAP 10 set ikev1 transform-set ESP-DES-SHA
!
crypto map VPN-MAP 20 match address VPN-DF
crypto map VPN-MAP 20 set peer 10.200.6.1
crypto map VPN-MAP 20 set ikev1 transform-set ESP-DES-SHA
!
crypto map VPN-MAP 30 match address VPN-D409
crypto map VPN-MAP 30 set peer 10.4.109.166
crypto map VPN-MAP 30 set ikev1 transform-set ESP-DES-SHA
!
crypto map VPN-MAP interface outside
!
! --- Activer IKEv1 sur l'interface outside ---
crypto ikev1 enable outside
```

Mise en place de VPN IPsec

```
object network LOCAL_NETWORK
 subnet 192.168.32.0 255.255.248.0
 subnet 172.16.32.0 255.255.255.224
!
object network REMOTE_DE
 subnet 192.168.40.0 255.255.248.0
 description reseau local dept-E
!
object network REMOTE_DF
 subnet 192.168.48.0 255.255.248.0
description reseau local dept-F
object network REMOTE_D409
 subnet 192.168.100.0 255.255.255.0
 description paillasse prof salle 409
```

ACL

```
access-list VPN-DE extended permit ip object LOCAL_NETWORK object REMOTE_DE
access-list VPN-DF extended permit ip object LOCAL_NETWORK object REMOTE_DF
access-list VPN-D409 extended permit ip object LOCAL_NETWORK object REMOTE_D409
```

Mise en place de Téléphonie IP

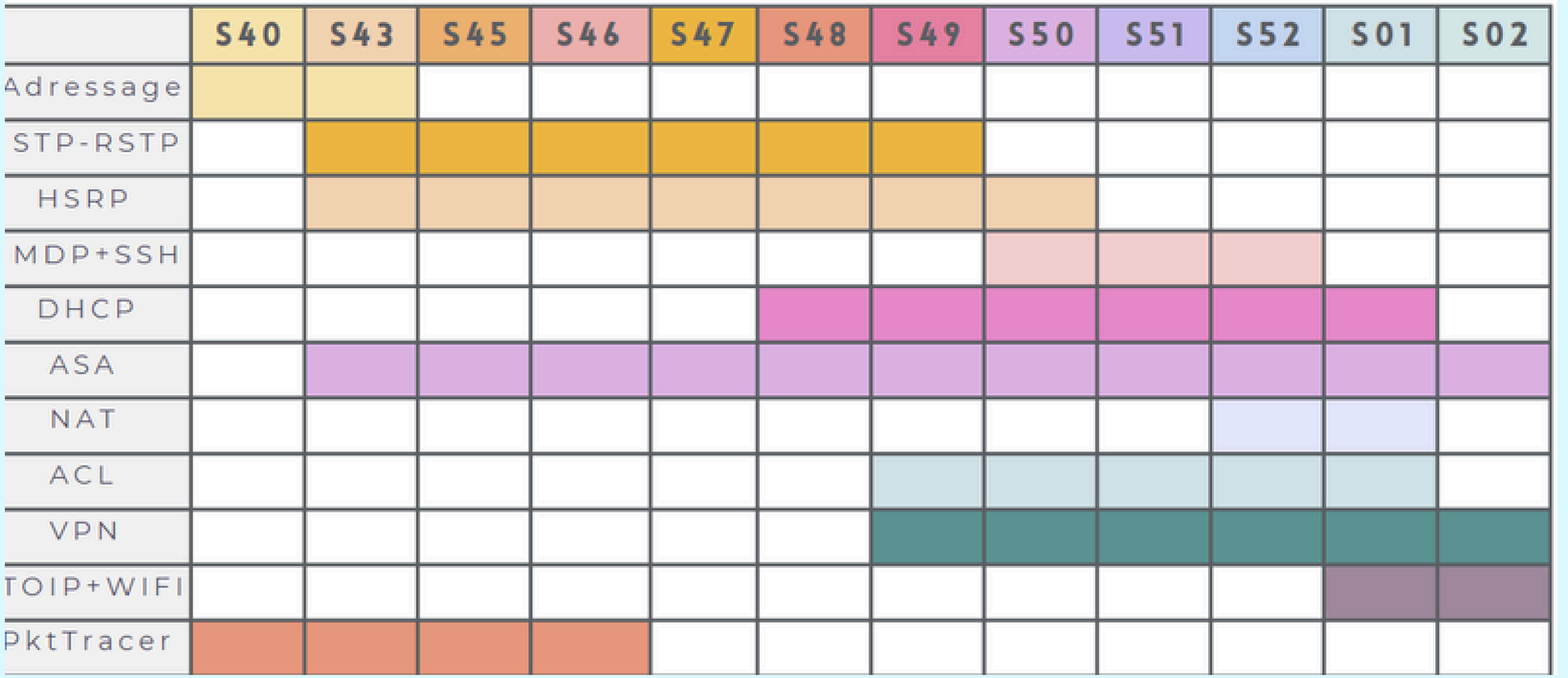
```
interface FastEthernet0/21
 description Vlan for ToIP
 switchport mode access
 switchport access vlan 4
 switchport voice vlan 1
 mls qos trust cos
 spanning-tree portfast
 no shut
```


```
ip helper-address 10.4.109.166
```

Répartition

	Clément	Bohdan	Faysa	Khawla
Adressage	x	x	x	x
STP-RSTP	x		x	
HSRP	x	x	x	
MDP + SSH	x			x
DHCP			x	x
ASA	x	x	x	x
NAT		x	x	
ACL	x	x	x	
VPN		x	x	
ToIP + WIFI		x		x

GANTT


S40
S43
S45
S46
S47
S48
S49
S50
S51
S52
S01
S02
Adressage
STP-RSTP
HSRP
MDP+SSH
DHCP
ASA
NAT
ACL
VPN
TOIP+WIFI
PktTracer

MERCI DE NOUS AVOIR ÉCOUTÉ

BUT R&T -Semestre 3