



Collège LaSalle
Montréal

INSTALLATION ET ADMINISTRATION DES RÉSEAUX (LEA.99)

Rapport de projet

DÉPLOIEMENT D'UN RÉSEAU D'ENTREPRISE MULTIPLATEFORMES

420-DR3-AS
(Cisco)

Cezar Gurulea
2235092

27 novembre 2023

Sommaire

1. Introduction	
• Remerciement	3
2. Conception du réseau	
• Topologie	5
• VLSM	6
3. Configuration de la branche de Dublin	
• VLANs	11
• VTP	12
• STP	13
• EtherChannel	14
• DHCP	15
Configuration des servers	
• Site <i>www.local.com</i>	17
• FTP et TFTP	18
• DNS	19
• AAA (Tacacs+, RADIUS)	19
• ACL	20
4. Configuration du routeur du Dublin	
• Routage OSPF	21
• Routage EIGRP	24
• PPP	27
• ZPF	29
5. Configuration de la branche d'Edinburgh	
• HSRP	31
6. Configuration de la branche du Cork	
• DHCP	35

7. Configuration de la branche du Galway-Limerick	
• VPN IPSec -----	37
• HDLC -----	41
• DHCP Galway server -----	41
• DHCP Limerick server -----	42
• WLC -----	43
8. Configuration de la branche d'ISP	
• NAT -----	48
• Test AAA -----	50
9. Configuration de la branche de la branche d'Internet	
• Site <i>www.groupe.com</i> -----	52
10. Problèmes rencontrés, méthodes de dépannage et recommandations -----	54
11. Glossaire de termes techniques -----	57
12. Conclusion -----	59

Remerciement

Chers Professeurs, du Collège LaSalle

A l'approche de la fin de notre parcours au collège, je tiens à exprimer ma profonde gratitude envers chacun d'entre vous. Votre dévouement, votre passion pour l'enseignement et votre engagement envers notre éducation ont laissé une empreinte indélébile dans nos vies.

Tout au long de la formation, vous avez été bien plus que des enseignants pour nous. Vous avez été des guides, des mentors et des modèles inspirants. Vos encouragements ont été les bouées de sauvetage dans les moments difficiles, et vos leçons vont bien au-delà des manuels scolaires. Vous nous avez enseigné la valeur du travail acharné, de la persévérance et de l'intégrité.

Votre passion pour vos matières respectives a allumé en nous la flamme de la curiosité et a nourri notre soif de connaissances. Chaque leçon était une aventure, chaque défi était une opportunité de grandir, grâce à vous.

Au-delà de l'enseignement académique, vous avez contribué à notre développement personnel. Vos conseils éclairés, votre soutien constant et vos encouragements ont renforcé notre confiance en nous et ont façonné notre vision du monde.

Alors que nous nous apprêtons à franchir cette étape importante de nos vies, nous emportons avec nous bien plus que des connaissances académiques. Nous emportons les leçons de vie précieuses que vous nous avez enseignées.

Merci du fond du cœur pour votre dévouement inlassable et votre impact positif sur notre éducation. Nous ne vous oublierons jamais et porterons vos enseignements avec nous tout au long de notre parcours.

Avec respect et reconnaissance,
Cezar Gurulea.

Introduction

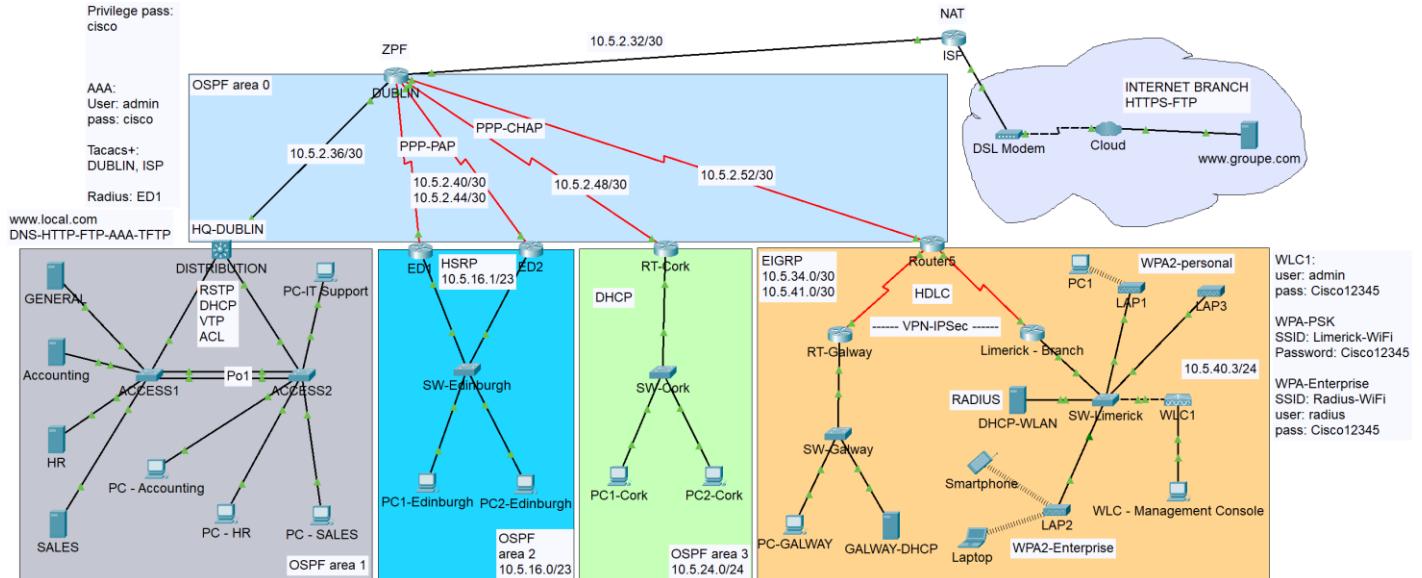
Bienvenue dans la présentation d'un projet de réseau pour une organisation étendue, comprenant plusieurs branches à Dublin, Edinburgh, Cork, Galway et Limerick. Le réseau assigné, 10.5.0.0/16, a été subdivisé en différents sous-réseaux pour optimiser l'utilisation des adresses IP et garantir la scalabilité du réseau. Ce projet se distingue par la complexité de la branche de Dublin, avec ses 5 VLANs dédiés à chaque département, ainsi qu'une salle serveurs abritant divers services tels que le web, AAA, FTP, TFTP, DNS, etc. L'objectif central de ce réseau est d'assurer une gestion efficace des ressources tout en permettant une expansion aisée des sous-réseaux.

Chaque branche est conçue de manière à répondre aux besoins spécifiques de son emplacement. Dublin, en tant que hub central, joue un rôle crucial en connectant toutes les branches, y compris l'accès à Internet. Nous explorerons en détail la configuration des commutateurs, routeurs, serveurs DHCP, pare-feu et autres éléments clés déployés dans chaque branche pour assurer le bon fonctionnement du réseau. Les protocoles tels que OSPF, HSRP, EIGRP, et la mise en œuvre de technologies telles que PPP, IPsec, NAT, et bien d'autres, seront également examinés.

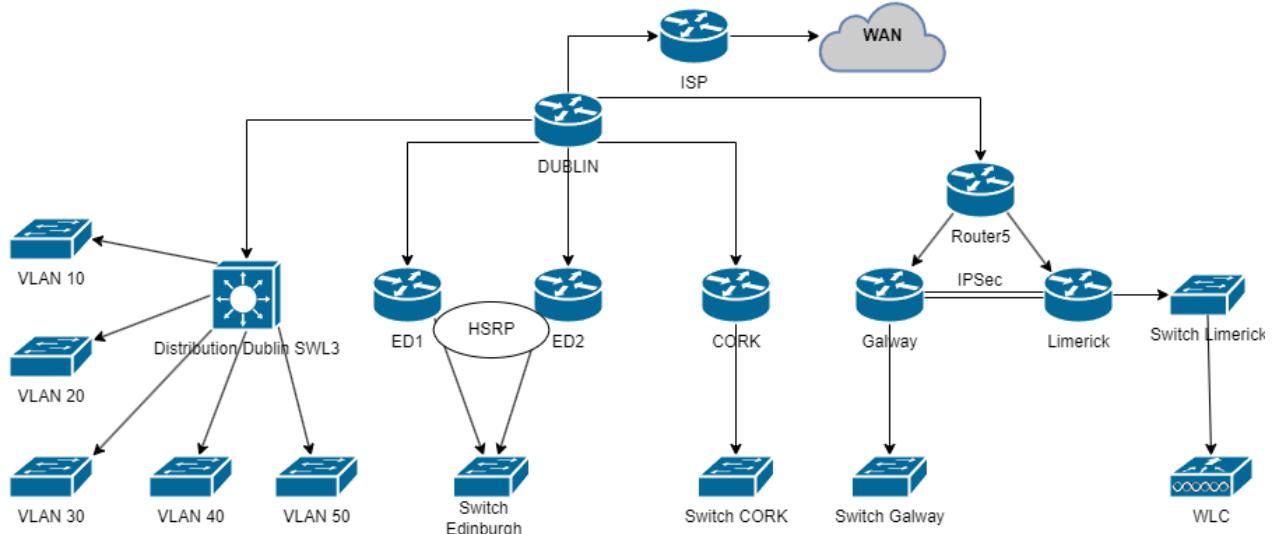
Ce projet vise à fournir une infrastructure réseau robuste, sécurisée et évolutive pour répondre aux besoins d'une organisation moderne. Nous commencerons par une vue d'ensemble, suivie d'une analyse détaillée de chaque composant du réseau, démontrant ainsi comment ces éléments convergent pour créer un système cohérent et fonctionnel.

Conception du réseau

- La topologie physique



- La topologie logique



Le tableau VLSM

Nom de réseau	VLAN	Nombre d'adresses d'hôtes nécessaires	Adresse réseau	Masque de sous-réseau	Nombre maximum d'hôtes possibles	Adresse de passerelle par défaut
IT	10	20	10.5.2.0	255.255.255.224 /27	30	10.5.2.1
ACCOUNTING	20	50	10.5.1.128	255.255.255.192 /26	62	10.5.1.129
HR	30	40	10.5.1.192	255.255.255.192 /26	62	10.5.1.193
SALES	40	200	10.5.0.0	255.255.255.0 /24	254	10.5.0.1
GENERAL	50	100	10.5.1.0	255.255.255.128 /25	126	10.5.1.1
Edinburgh	-	500	10.5.16.0	255.255.254.0 /23	510	10.5.16.1
Cork	-	250	10.5.24.0	255.255.255.0 /24	254	10.5.24.1
Galway	-	500	10.5.32.0	255.255.254.0 /23	510	10.5.32.1
Limerick	-	200	10.5.40.0	255.255.255.0 /24	254	10.5.40.1
Dublin-ISP	-	2	10.5.2.32	255.255.255.252 /30	2	Point to point
Dublin-HQ	-	2	10.5.2.36	255.255.255.252 /30	2	Point to point
Dublin-ED1	-	2	10.5.2.40	255.255.255.252 /30	2	Point to point
Dublin-ED2	-	2	10.5.2.44	255.255.255.252 /30	2	Point to point
Dublin-Cork	-	2	10.5.2.48	255.255.255.252 /30	2	Point to point
Dublin-Router5	-	2	10.5.2.52	255.255.255.252 /30	2	Point to point
Router5-Galway	-	2	10.5.34.0	255.255.255.252 /30	2	Point to point
Router5-Limerick	-	2	10.5.41.0	255.255.255.252 /30	2	Point to point
WAN	-	2	200.1.5.0	255.255.255.252 /30	2	Point to point
Cork ipv6	-	-	fc00::1::	/64	2^{64}	FE80::1
Galway ipv6	-	-	fc00::2::	/64	2^{64}	FE80::2

Nom du routeur: DISTRIBUTION

Nom de réseau	Description et but	Type/numéro d'interface/so us-interface	VLAN	Encapsulatio n	Réseau	Adresse IP de l'interface	Masq ue
Sales	Département des ventes	Vlan 40	40	dot1Q 40	10.5.0.0	10.5.0.1	/24
General	Servers HTTP/AAA/etc.	Vlan 50	50	dot1Q 50	10.5.1.0	10.5.1.1	/25
Accounting	Service de la comptabilité	Vlan 20	20	dot1Q 20	10.5.1.128	10.5.1.129	/26
HR	Ressources humaines	Vlan 30	30	dot1Q 30	10.5.1.192	10.5.1.193	/26
IT	Administrateurs IT	Vlan 10	10	dot1Q 10	10.5.2.0	10.5.2.1	/27
Dublin-HQ	Lien vers le routeur Dublin	G0/1	-	-	10.5.2.36	10.5.2.38	/30

Nom du routeur: DUBLIN

Nom de réseau	Description et but	Type/numéro d'interface/sous-interface	VLAN	Encapsulation	Réseau	Adresse IP de l'interface	Masque
Dublin-ISP	Lien vers ISP	G0/0/0	-	-	10.5.2.32	10.5.2.33	/30
Dublin-HQ	Lien vers la distr. Dublin	G0/0/1	-	-	10.5.2.36	10.5.2.37	/30
Dublin-ED1	Lien vers Edinburgh 1	S0/1/0	-	PPP-PAP	10.5.2.40	10.5.2.41	/30
Dublin-ED2	Lien vers Edinburgh 2	S0/1/1	-	PPP-PAP	10.5.2.44	10.5.2.45	/30
Dublin-Cork	Lien vers Cork	S0/2/0	-	PPP-CHAP	10.5.2.48	10.5.2.49	/30
Dublin-Router5	Lien vers Router5	S0/2/1	-	PPP-CHAP	10.5.2.52	10.5.2.53	/30

Nom du routeur: ED1

Nom de réseau	Description et but	Type/numéro d'interface/sous-interface	VLAN	Encapsulation	Réseau	Adresse IP de l'interface	Masque
Dublin-ED1	Lien vers Dublin	S0/1/0	-	PPP-PAP	10.5.2.40	10.5.2.42	/30
Edinburgh	Virtual router HSRP	G0/0/1	-	-	10.5.16.0	10.5.16.2	/23

Nom du routeur: ED2

Nom de réseau	Description et but	Type/numéro d'interface/sous-interface	VLAN	Encapsulation	Réseau	Adresse IP de l'interface	Masque
Dublin-ED2	Lien vers Dublin	S0/1/0	-	PPP-PAP	10.5.2.44	10.5.2.46	/30
Edinburgh	Virtual router HSRP	G0/0/1	-	-	10.5.16.0	10.5.16.3	/23

Nom du routeur: Cork

Nom de réseau	Description et but	Type/numéro d'interface/sous-interface	VLAN	Encapsulation	Réseau	Adresse IP de l'interface	Masque
Dublin-Cork	Lien vers Dublin	S0/1/0	-	PPP-CHAP	10.5.2.48	10.5.2.50	/30
Cork	Branche Cork	G0/0/1	-	-	10.5.24.0	10.5.24.1	/24

Nom du routeur: Router5

Nom de réseau	Description et but	Type/numéro d'interface/sous-interface	VLAN	Encapsulation	Réseau	Adresse IP de l'interface	Masque
Dublin-Router5	Lien vers Dublin	S0/1/1	-	PPP-CHAP	10.5.2.52	10.5.2.54	/30
Galway	Lien vers Galway	S0/1/0	-	HDLC	10.5.34.0	10.5.34.1	/30
Limerick	Lien vers Limerick	S0/2/0	-	HDLC	10.5.41.0	10.5.41.1	/30

Nom du routeur: Galway

Nom de réseau	Description et but	Type/numéro d'interface/sous-interface	VLAN	Encapsulation	Réseau	Adresse IP de l'interface	Masque
Router5	Link to Router5	S0/1/0	-	HDLC	10.5.34.0	10.5.34.2	/30
Galway	Branche Galway	G0/0/1	-	-	10.5.32.0	10.5.32.1	/23

Nom du routeur: Limerick

Nom de réseau	Description et but	Type/numéro d'interface/sous-interface	VLAN	Encapsulation	Réseau	Adresse IP de l'interface	Masque
Router5	Link to Router5	S0/1/0	-	HDLC	10.5.41.0	10.5.41.2	/30
Limerick	Branche Limerick	G0/0/0	-	-	10.5.40.0	10.5.40.1	/24

Nom du routeur: ISP

Nom de réseau	Description et but	Type/numéro d'interface/sous-interface	VLAN	Encapsulation	Réseau	Adresse IP de l'interface	Masque
Dublin-ISP	Link to ISP	G0/0/0	-	-	10.5.2.32	10.5.2.34	/30
ISP-WAN	WAN	G0/0/1	-	-	200.1.5.0	200.1.5.2	/30

Nom du point d'accès sans fil: LAP1

Type d'interface/port	Description et but	Nom de réseau	Réseau	SSID	Sécurité - Clé WPA2	Adresse IP de l'interface ou plage IP	Masque
Port 0 (Wired)	Lien vers WLC	Limerick	10.5.40.0	-	-	10.5.40.10 DHCP	/24
Port 1 (Wireless)	Wi-Fi PSK	Limerick	10.5.40.0	Limerick-WiFi	Cisco12345	DHCP	/24

Nom du point d'accès sans fil: LAP2

Type d'interface/port	Description et but	Nom de réseau	Réseau	SSID	Sécurité - Clé WPA2	Adresse IP de l'interface ou plage IP	Masque
Port 0 (Wired)	Lien vers WLC	Limerick	10.5.40.0	-	-	10.5.40.11 DHCP	/24
Port 1 (Wireless)	Wi-Fi Radius	Limerick	10.5.40.0	Radius-WiFi	Cisco12345	DHCP	/24

Nom du point d'accès sans fil: LAP3

Type d'interface/port	Description et but	Nom de réseau	Réseau	SSID	Sécurité - Clé WPA2	Adresse IP de l'interface ou plage IP	Masque
Port 0 (Wired)	Lien vers WLC	Limerick	10.5.40.0	-	-	10.5.40.12 DHCP	/24
Port 1 (Wireless)	Wi-Fi PSK	Limerick	10.5.40.0	Limerick-WiFi	Cisco12345	DHCP	/24

Nom du commutateur de distribution: Dublin_SWL3

Adresse IP	VLAN
10.5.0.1	40
10.5.1.1	50
10.5.1.129	20
10.5.1.193	30
10.5.2.1	10

Numéro de port	Description et but	Vitesse	Duplex	VLAN autorisé	Switchport Type	Encapsulation
F0/1	Trunk interface	100 Mbps	Full duplex	2-1000	Trunk	Dot1Q
F0/2	Trunk interface	100 Mbps	Full duplex	2-1000	Trunk	Dot1Q
F0/3-24	Blackhole	-	-	-	-	-
G0/1	Lien vers Dublin	1 Gbps	Full duplex	-	-	-
G0/2	Blackhole	-	-	-	-	-

Nom du commutateur d'accès: ACCESS1

Type d'interface/sous-interface/Port/Numéro	Description et but	Vitesse	Duplex	Réseau	VLAN	Switchport Type
Po1	EtherChannel	-	Full duplex	EtherChannel	2-1000	Trunk
F0/1	Lien vers Dublin SWL3	100 Mbps	Full duplex	Dublin	2-1000	Trunk
F0/2	EtherChannel	100 Mbps	Full duplex	EtherChannel	2-1000	Trunk
F0/3	EtherChannel	100 Mbps	Full duplex	EtherChannel	2-1000	Trunk
F0/4-20	Blackhole	-	-	-	999	-
G0/1-2	Blackhole	-	-	-	999	-
F0/21	GENERAL Vlan	100 Mbps	Full duplex	GENERAL	50	Access

F0/22	ACCOUNTING Vlan	100 Mbps	Full duplex	ACCOUNTING	20	Access
F0/23	HR Vlan	100 Mbps	Full duplex	HR	30	Access
F0/24	SALES Vlan	100 Mbps	Full duplex	SALES	40	Access

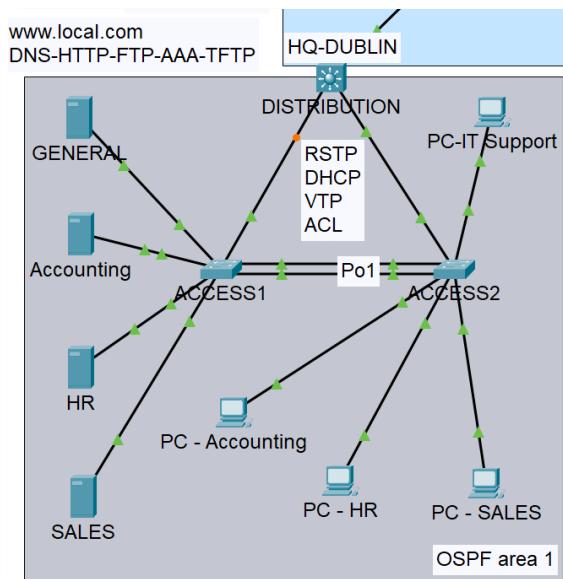
Nom du commutateur d'accès: ACCESS1

Type d'interface/sous-interface/Port/Numéro	Description et but	Vitesse	Duplex	Réseau	VLAN	Switchport Type
Po1	EtherChannel	-	Full duplex	EtherChannel	2-1000	Trunk
F0/1	Lien vers Dublin SWL3	100 Mbps	Full duplex	Dublin	2-1000	Trunk
F0/2	EtherChannel	100 Mbps	Full duplex	EtherChannel	2-1000	Trunk
F0/3	EtherChannel	100 Mbps	Full duplex	EtherChannel	2-1000	Trunk
F0/4-20	Blackhole	-	-	-	999	-
G0/1-2	Blackhole	-	-	-	999	-
F0/21	ACCOUNTING Vlan	100 Mbps	Full duplex	ACCOUNTING	20	Access
F0/22	HR Vlan	100 Mbps	Full duplex	HR	30	Access
F0/23	SALES Vlan	100 Mbps	Full duplex	SALES	40	Access
F0/24	IT Vlan	100 Mbps	Full duplex	IT	10	Access

Configuration de la branche de Dublin

- La topologie physique de la branche Distribution-Dublin

Il y a trois commutateurs, un du niveau 3 et deux autres du niveau 2. Le commutateur de Distribution est destiné au routage, à la gestion des VLAN et aux accès externes. ACCESS1 est situé dans la salle des serveurs, respectivement les serveurs de la branche y sont connectés. Les ordinateurs et autres périphériques sont connectés en ACCESS2. Il existe une connexion Ethernet



- VLAN - Au sein de la branche, il existe cinq VLANs, accompagnés d'un VLAN (BlackHole) dédié à la sécurisation des ports non utilisés sur les commutateurs.

VLAN	Name	Status	Ports
1	default	active	
10	IT	active	
20	ACCOUNTING	active	
30	HR	active	
40	SALES	active	
50	GENERAL	active	
999	BLACKHOLE	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/2

Les VLANs dans le commutateur de distribution Dublin

VLAN	Name	Status	Ports
1	default	active	
10	IT	active	
20	ACCOUNTING	active	Fa0/22
30	HR	active	Fa0/23
40	SALES	active	Fa0/24
50	GENERAL	active	Fa0/21
999	BLACKHOLE	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Gig0/1, Gig0/2

Les VLANs dans le commutateur ACCESS1

VLAN	Name	Status	Ports
1	default	active	
10	IT	active	Fa0/24
20	ACCOUNTING	active	Fa0/21
30	HR	active	Fa0/22
40	SALES	active	Fa0/23
50	GENERAL	active	
999	BLACKHOLE	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Gig0/1, Gig0/2

Les VLANs dans le commutateur ACCESS2

- Les VLANs sont configurés sur le commutateur de distribution Dublin_SWL3, puis diffusés aux autres commutateurs via **VTP** (VLAN Trunking Protocol).

Ci-dessous nous voyons le résultat du VTP

```
Dublin_SWL3#sh vtp status
VTP Version capable      : 1 to 2
VTP version running      : 1
VTP Domain Name          : www.local.com
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0001.C757.3C00
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 10.5.2.1 on interface VI10 (lowest numbered VLAN interface found)

Feature VLAN :
-----
VTP Operating Mode       : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 11
Configuration Revision    : 18
MD5 digest               : 0xB7 0x19 0x41 0xDB 0xA5 0xF 0x6F 0x75
                           0x98 0x82 0x7A 0x68 0xB8 0x97 0x1A 0x2B
```

```
ACCESS1#sh vtp status
VTP Version capable      : 1 to 2
VTP version running      : 1
VTP Domain Name          : www.local.com
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0001.C77B.B100
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00

Feature VLAN :
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 255
Number of existing VLANs   : 11
Configuration Revision    : 42
MD5 digest               : 0xEB 0x69 0x4F 0xC8 0xCE 0x78 0xA3 0xFD
                           0x77 0x3B 0xA3 0x6D 0xCA 0xD 0x5A 0x1F
ACCESS1#
```

```
ACCESS2#sh vtp status
VTP Version capable      : 1 to 2
VTP version running      : 1
VTP Domain Name          : www.local.com
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0090.2131.0D00
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00

Feature VLAN :
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 255
Number of existing VLANs   : 11
Configuration Revision    : 42
MD5 digest               : 0xEB 0x69 0x4F 0xC8 0xCE 0x78 0xA3 0xFD
                           0x77 0x3B 0xA3 0x6D 0xCA 0xD 0x5A 0x1F
```

- Rapid Spanning-Tree (**RSTP**)

Pour éviter les boucles, j'ai configuré le spanning-tree dans tous les commutateurs.

```
Dublin_SWL3#sh spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for:
Extended system ID      is enabled
Portfast Default         is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default        is disabled
EtherChannel misconfig guard is disabled
UplinkFast               is disabled
BackboneFast              is disabled
Configured Pathcost method used is short

Name          Blocking Listening Learning Forwarding STP Active
-----
VLAN0010           2       0       0       1       3
VLAN0020           2       0       0       1       3
VLAN0030           2       0       0       1       3
VLAN0040           2       0       0       1       3
VLAN0050           2       0       0       1       3
VLAN0999           2       0       0       1       3

-----
7 vlans            12      0       0       6      18
```

```
ACCESS1#sh spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for:
Extended system ID      is enabled
Portfast Default         is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default        is disabled
EtherChannel misconfig guard is disabled
UplinkFast               is disabled
BackboneFast              is disabled
Configured Pathcost method used is short

Name          Blocking Listening Learning Forwarding STP Active
-----
VLAN0010           6       0       0       2       8
VLAN0020           5       0       0       3       8
VLAN0030           5       0       0       3       8
VLAN0040           5       0       0       3       8
VLAN0050           5       0       0       3       8
VLAN0999           6       0       0       2       8

-----
7 vlans            32      0       0      16      48
```

```

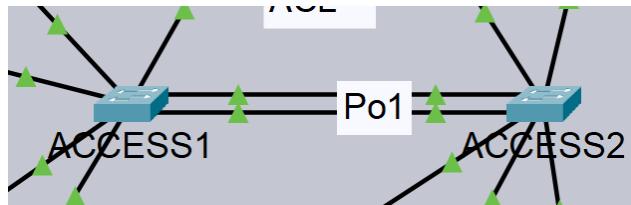
ACCESS2#sh spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: IT ACCOUNTING HR SALES GENERAL BLACKHOLE
Extended system ID      is enabled
Portfast Default        is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default       is disabled
EtherChannel misconfig guard is disabled
UplinkFast              is disabled
BackboneFast             is disabled
Configured Pathcost method used is short



| Name           | Blocking  | Listening | Learning | Forwarding | STP Active |
|----------------|-----------|-----------|----------|------------|------------|
| VLAN0010       | 5         | 0         | 0        | 3          | 8          |
| VLAN0020       | 5         | 0         | 0        | 3          | 8          |
| VLAN0030       | 5         | 0         | 0        | 3          | 8          |
| VLAN0040       | 5         | 0         | 0        | 3          | 8          |
| VLAN0050       | 6         | 0         | 0        | 2          | 8          |
| VLAN0999       | 6         | 0         | 0        | 2          | 8          |
| <b>7 vlans</b> | <b>32</b> | <b>0</b>  | <b>0</b> | <b>16</b>  | <b>48</b>  |


```

- Pour optimiser le débit au sein du VLAN, la bande passante du lien entre Access1 et Access2 est élargie en mettant en place un **EtherChannel**.



```

ACCESS1#sh etherchannel
    Channel-group listing:
    -----
Group: 1
-----
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP
ACCESS1#
ACCESS1#sh int pol status
Port      Name          Status      Vlan      Duplex   Speed Type
Po1           Po1      connected   trunk     auto     auto

```

```

ACCESS2#sh etherchannel
      Channel-group listing:
-----
Group: 1
-----
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
ACCESS2#
ACCESS2#sh int pol status
Port      Name          Status       Vlan      Duplex  Speed Type
Po1           connected    trunk     auto     auto

```

- DHCP

Un serveur DHCP a été instauré dans la filiale pour les VLANs configurés sur Dublin_SWL3. Des adresses ont été exclues de la plage DHCP afin d'être assignées de manière statique aux serveurs.

```

hostname Dublin_SWL3
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
ip dhcp excluded-address 10.5.0.1 10.5.0.10
ip dhcp excluded-address 10.5.1.1 10.5.1.10
ip dhcp excluded-address 10.5.1.129 10.5.1.134
ip dhcp excluded-address 10.5.1.193 10.5.1.199
ip dhcp excluded-address 10.5.2.1 10.5.2.6
!
ip dhcp pool VLAN40-SALES
  network 10.5.0.0 255.255.255.0
  default-router 10.5.0.1
  dns-server 10.5.1.2
ip dhcp pool VLAN20-ACCOUNTING
  network 10.5.1.128 255.255.255.192
  default-router 10.5.1.129
  dns-server 10.5.1.2
ip dhcp pool VLAN30-HR
  network 10.5.1.192 255.255.255.192
  default-router 10.5.1.193
  dns-server 10.5.1.2
ip dhcp pool VLAN10-IT
  network 10.5.2.0 255.255.255.224
  default-router 10.5.2.1
  dns-server 10.5.1.2
ip dhcp pool VLAN50-GENERAL
  network 10.5.1.0 255.255.255.128
  default-router 10.5.1.1
  dns-server 10.5.1.2
!
!
ip routing

```

On voit ici le résultat de la configuration DHCP sur les ordinateurs. On voit que les adresses sont correctement attribuées par le serveur DHCP.

PC - HR		PC - Accounting		
Physical	Config	Desktop	Programming	Attributes
IP Configuration				
Interface FastEthernet0				
IP Configuration				
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static	<input checked="" type="radio"/> DHCP	<input type="radio"/> Static	
IPv4 Address	10.5.1.200	IPv4 Address	10.5.1.135	
Subnet Mask	255.255.255.192	Subnet Mask	255.255.255.192	
Default Gateway	10.5.1.193	Default Gateway	10.5.1.129	
DNS Server	10.5.1.2	DNS Server	10.5.1.2	

PC - SALES		PC-IT Support		
Physical	Config	Desktop	Programming	Attributes
IP Configuration				
Interface FastEthernet0				
IP Configuration				
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static	<input checked="" type="radio"/> DHCP	<input type="radio"/> Static	
IPv4 Address	10.5.0.11	IPv4 Address	10.5.2.7	
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.224	
Default Gateway	10.5.0.1	Default Gateway	10.5.2.1	
DNS Server	10.5.1.2	DNS Server	10.5.1.2	

La configuration manuelle des serveurs suit.

GENERAL		Accounting		
Physical	Config	Services	Desktop	Program
IP Configuration				
IP Configuration				
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static	<input type="radio"/> DHCP	<input checked="" type="radio"/> Static	
IPv4 Address	10.5.1.2	IPv4 Address	10.5.1.130	
Subnet Mask	255.255.255.128	Subnet Mask	255.255.255.192	
Default Gateway	10.5.1.1	Default Gateway	10.5.1.129	
DNS Server	10.5.1.2	DNS Server	10.5.1.2	

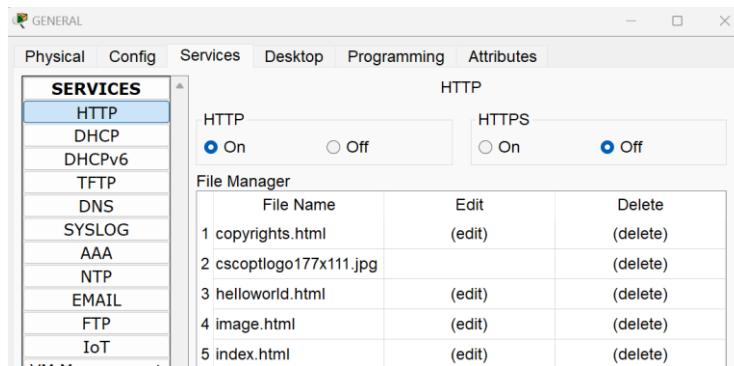
The image contains two side-by-side windows from the PC-IT software. Both windows have a top navigation bar with tabs: Physical, Config, Services, Desktop, Programming, and Attributes. The left window is titled 'HR' and the right one is titled 'SALES'. Under the 'IP Configuration' section, both show the same settings:

	HR	SALES
IP Configuration	IP Configuration	
IPv4 Address	10.5.1.194	10.5.0.2
Subnet Mask	255.255.255.192	255.255.255.0
Default Gateway	10.5.1.193	10.5.0.1
DNS Server	10.5.1.2	10.5.1.2

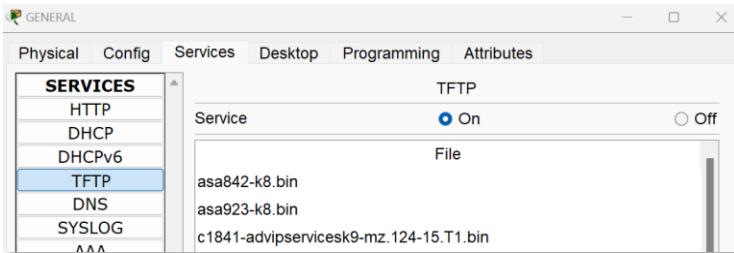
- Configuration du serveur GENERAL

Les services HTTP, FTP, TFTP, DNS, AAA sont implémentés sur le serveur GENERAL

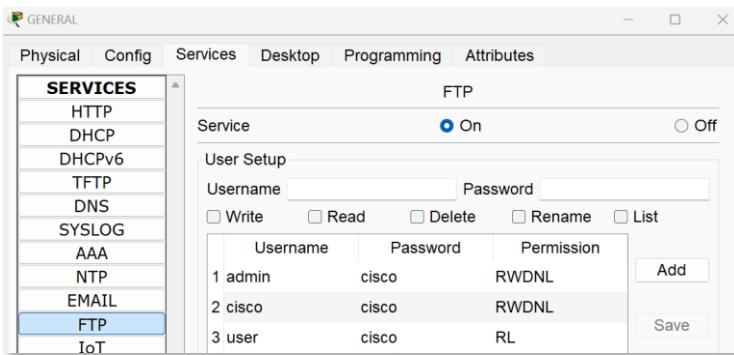
Le site **www.local.com** est configuré au niveau local et peut être consulté à partir de n'importe quel dispositif dans l'entreprise. À des fins de test, l'accès a été réalisé depuis le PC-IT.



- TFTP



- FTP

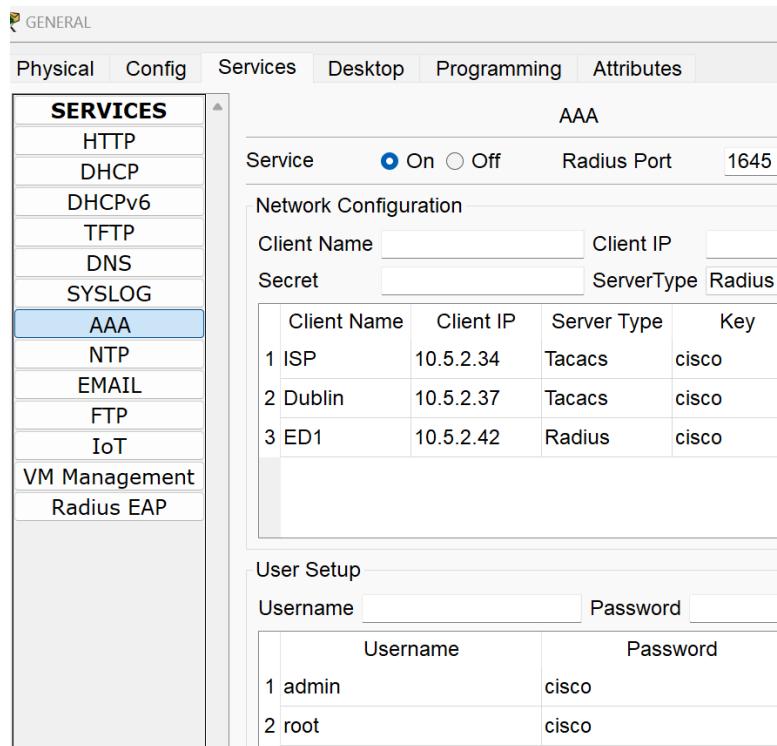
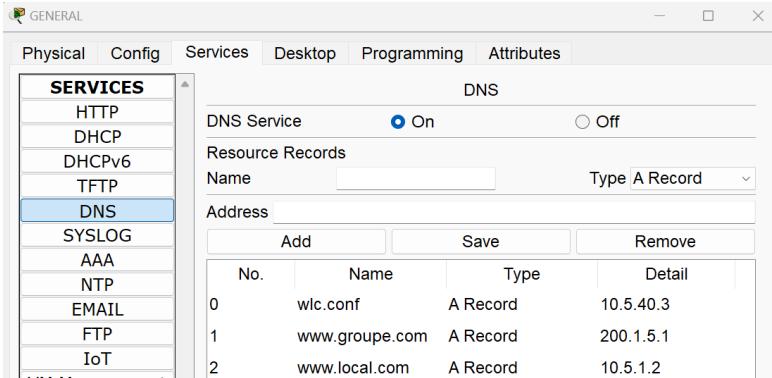


Dans l'exemple fourni, le serveur FTP a été configuré avec trois utilisateurs, dont deux bénéficient de privilèges complets tandis que le troisième dispose uniquement de droits de lecture.

```
PC-IT Support
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ftp 10.5.1.2
Trying to connect...10.5.1.2
Connected to 10.5.1.2
220- Welcome to PT Ftp server
Username:admin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 10.5.1.2:
0   : asa842-k8.bin                               5571584
1   : asa923-k8.bin                               30468096
2   : c1841-advipsericesk9-mz.124-15.T1.bin    33591768
3   : c1841-ipbasek9-mz.123-14.T7.bin          13832032
4   : c1841-ipbasek9-mz.124-12.bin              16599160
5   : c1900-universalk9-mz.SPA.155-3.M4a.bin    33591768
6   : c2600-advipsericesk9-mz.124-15.T1.bin    33591768
7   : c2600-i-mz.122-28.bin                      5571584
8   : c2600-ipbasek9-mz.124-8.bin                13169700
```

- DNS - Le serveur DNS est configuré pour www.local.com, qui est un site interne, pour www.groupe.com, qui est public, et pour le contrôleur WLC afin de faciliter l'accès à la page de configuration.



- Le serveur AAA est paramétré pour trois routeurs distincts. Deux sont configurés avec une autorisation Tacacs+, tandis que le troisième utilise le protocole Radius. Après avoir réalisé la configuration des routeurs, nous examinerons le résultat à la **page 49**.

- ACL - L'accès entre les VLANs est sécurisé par des listes de contrôle d'accès (ACL). Le département IT a un accès global, tandis que les autres départements ne peuvent pas accéder au département informatique. Pour accéder au serveur WEB (www.local.com) et au DNS, les ports 80 et 443 sont ouverts.

```
Dublin_SWL3#sh ac
Extended IP access list 101
 10 permit tcp 10.5.0.0 0.0.0.255 10.5.2.0 0.0.0.31 established
 20 permit icmp 10.5.0.0 0.0.0.255 10.5.2.0 0.0.0.31 echo-reply
 30 deny ip 10.5.0.0 0.0.0.255 10.5.2.0 0.0.0.31
 40 permit tcp 10.5.1.0 0.0.0.127 10.5.2.0 0.0.0.31 established
 50 permit icmp 10.5.1.0 0.0.0.127 10.5.2.0 0.0.0.31 echo-reply
 60 permit tcp host 10.5.1.2 10.5.2.0 0.0.0.31 eq www established
 70 permit udp host 10.5.1.2 eq domain 10.5.2.0 0.0.0.31
 80 deny ip 10.5.1.0 0.0.0.127 10.5.2.0 0.0.0.31
 90 permit tcp 10.5.1.128 0.0.0.63 10.5.2.0 0.0.0.31 established
100 permit icmp 10.5.1.128 0.0.0.63 10.5.2.0 0.0.0.31 echo-reply
110 deny ip 10.5.1.128 0.0.0.63 10.5.2.0 0.0.0.31
120 permit tcp 10.5.1.192 0.0.0.63 10.5.2.0 0.0.0.31 established
130 permit icmp 10.5.1.192 0.0.0.63 10.5.2.0 0.0.0.31 echo-reply
140 deny ip 10.5.1.192 0.0.0.63 10.5.2.0 0.0.0.31
150 permit ip any any
```

PC - Accounting

Physical	Config	Desktop	Programming	Attributes
Command Prompt				
C:\>ping 10.5.2.7				
Pinging 10.5.2.7 with 32 bytes of data:				
Reply from 10.5.1.129: Destination host unreachable.				
Reply from 10.5.1.129: Destination host unreachable.				
Reply from 10.5.1.129: Destination host unreachable.				
Reply from 10.5.1.129: Destination host unreachable.				
Ping statistics for 10.5.2.7:				
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)				
C:\>ping 10.5.1.200				
Pinging 10.5.1.200 with 32 bytes of data:				
Reply from 10.5.1.200: bytes=32 time=1ms TTL=127				
Reply from 10.5.1.200: bytes=32 time<1ms TTL=127				
Reply from 10.5.1.200: bytes=32 time<1ms TTL=127				
Reply from 10.5.1.200: bytes=32 time<1ms TTL=127				
Ping statistics for 10.5.1.200:				
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)				
Approximate round trip times in milli-seconds:				
Minimum = 0ms, Maximum = 1ms, Average = 0ms				
C:\>ping 10.5.0.11				
Pinging 10.5.0.11 with 32 bytes of data:				
Reply from 10.5.0.11: bytes=32 time<1ms TTL=127				
Reply from 10.5.0.11: bytes=32 time<1ms TTL=127				
Reply from 10.5.0.11: bytes=32 time<1ms TTL=127				
Reply from 10.5.0.11: bytes=32 time<1ms TTL=127				
Ping statistics for 10.5.0.11:				
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)				
Approximate round trip times in milli-seconds:				
Minimum = 0ms, Maximum = 0ms, Average = 0ms				

PC - IT Support

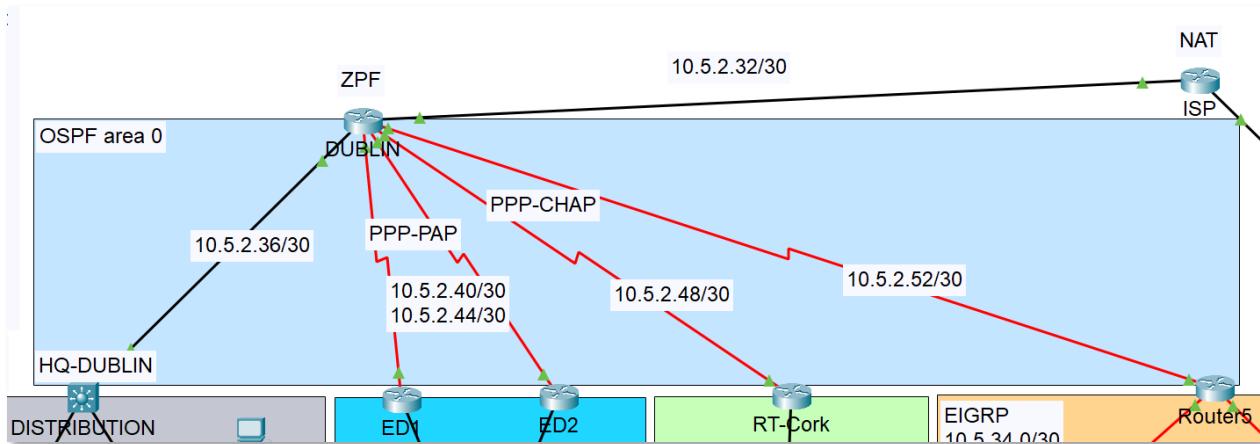
Physical	Config	Desktop	Programming	Attributes
Command Prompt				
C:\>ping 10.5.1.200				
Pinging 10.5.1.200 with 32 bytes of data:				
Request timed out.				
Reply from 10.5.1.200: bytes=32 time<1ms TTL=127				
Reply from 10.5.1.200: bytes=32 time=8ms TTL=127				
Reply from 10.5.1.200: bytes=32 time<1ms TTL=127				
Ping statistics for 10.5.1.200:				
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),				
Approximate round trip times in milli-seconds:				
Minimum = 0ms, Maximum = 8ms, Average = 2ms				
C:\>ping 10.5.1.135				
Pinging 10.5.1.135 with 32 bytes of data:				
Request timed out.				
Reply from 10.5.1.135: bytes=32 time<1ms TTL=127				
Reply from 10.5.1.135: bytes=32 time<1ms TTL=127				
Reply from 10.5.1.135: bytes=32 time<1ms TTL=127				
Ping statistics for 10.5.1.135:				
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),				
Approximate round trip times in milli-seconds:				
Minimum = 0ms, Maximum = 0ms, Average = 0ms				
C:\>ping 10.5.0.11				
Pinging 10.5.0.11 with 32 bytes of data:				
Request timed out.				
Reply from 10.5.0.11: bytes=32 time<1ms TTL=127				
Reply from 10.5.0.11: bytes=32 time<1ms TTL=127				
Reply from 10.5.0.11: bytes=32 time<1ms TTL=127				
Ping statistics for 10.5.0.11:				
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),				
Approximate round trip times in milli-seconds:				
Minimum = 0ms, Maximum = 0ms, Average = 0ms				
C:\>ping 10.5.1.193				
Pinging 10.5.1.193 with 32 bytes of data:				
Reply from 10.5.1.193: bytes=32 time<1ms TTL=255				
Reply from 10.5.1.193: bytes=32 time<1ms TTL=255				

Configuration du routeur du Dublin

- Routage OSPF

Afin d'assurer une fiabilité optimale et de respecter une norme universelle, le protocole de routage OSPF est déployé. Il bénéficie de la prise en charge de tous les fabricants d'équipements réseau, facilitant ainsi la modification et l'expansion du réseau de manière aisée.

Configuration OSPF accomplie.



- DUBLIN

```
router ospf 1
  router-id 1.1.1.1
  log-adjacency-changes
  network 10.5.2.36 0.0.0.3 area 0
  network 10.5.2.52 0.0.0.3 area 0
  network 10.5.2.48 0.0.0.3 area 0
  network 10.5.2.44 0.0.0.3 area 0
  network 10.5.2.40 0.0.0.3 area 0
  network 10.5.2.32 0.0.0.3 area 0
!
```

```

DUBLIN#sh ip ospf neighbor

Neighbor ID      Pri   State            Dead Time    Address          Interface
8.8.8.8          1     FULL/DR         00:00:31     10.5.2.34       GigabitEthernet0/0/0
2.2.2.2          1     FULL/DR         00:00:31     10.5.2.38       GigabitEthernet0/0/1
3.3.3.1          0     FULL/ -         00:00:39     10.5.2.42       Serial0/1/0
3.3.3.2          0     FULL/ -         00:00:31     10.5.2.46       Serial0/1/1
4.4.4.4          0     FULL/ -         00:00:31     10.5.2.50       Serial0/2/0
5.5.5.5          0     FULL/ -         00:00:31     10.5.2.54       Serial0/2/1
DUBLIN#sh ip ospf border-routers
OSPF Process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 2.2.2.2 [1] via 10.5.2.38, GigabitEthernet0/0/1, ABR, Area 0, SPF 1
i 8.8.8.8 [1] via 10.5.2.34, GigabitEthernet0/0/0, ASBR, Area 0, SPF 1
i 3.3.3.1 [64] via 10.5.2.42, Serial0/1/0, ABR, Area 0, SPF 64
i 5.5.5.5 [64] via 10.5.2.54, Serial0/2/1, ASBR, Area 0, SPF 64
i 4.4.4.4 [64] via 10.5.2.50, Serial0/2/0, ABR, Area 0, SPF 64
i 3.3.3.2 [64] via 10.5.2.46, Serial0/1/1, ABR, Area 0, SPF 64
DUBLIN#

```

- Distribution Dublin

```

Dublin_SWL3#sh ip ospf neighbor

Neighbor ID      Pri   State            Dead Time    Address
1.1.1.1          1     FULL/BDR        00:00:38     10.5.2.37

```

- ED1

```

router ospf 1
  router-id 3.3.3.1
  log-adjacency-changes
  network 10.5.2.40 0.0.0.3 area 0
  network 10.5.16.0 0.0.1.255 area 2
.

```

```

ED1#sh ip ospf neighbor

Neighbor ID      Pri   State            Dead Time    Address
1.1.1.1          0     FULL/ -         00:00:31     10.5.2.41
3.3.3.2          1     FULL/DR        00:00:33     10.5.16.3

```

- ED2

```
router ospf 1
  router-id 3.3.3.2
  log-adjacency-changes
  network 10.5.2.44 0.0.0.3 area 0
  network 10.5.16.0 0.0.1.255 area 2
```

```
ED2#sh ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address
1.1.1.1	0	FULL/ -	00:00:39	10.5.2.45
3.3.3.1	1	FULL/BDR	00:00:39	10.5.16.2

- Cork

```
router ospf 1
  router-id 4.4.4.4
  log-adjacency-changes
  network 10.5.2.48 0.0.0.3 area 0
  network 10.5.24.0 0.0.0.255 area 3
```

```
CORK#sh ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address
1.1.1.1	0	FULL/ -	00:00:32	10.5.2.49

- Router5 (Galway-Limerick) a été configuré avec une combinaison d'OSPF et EIGRP, car les réseaux de Galway et Limerick sont exclusivement en EIGRP. La redistribution est mise en œuvre pour assurer l'interopérabilité entre les protocoles de routage OSPF et EIGRP.

```

router eigrp 1
  eigrp router-id 5.5.5.5
  redistribute ospf 1 metric 1544 2000 255 1 1500
  passive-interface default
  no passive-interface Serial0/1/0
  no passive-interface Serial0/1/1
  no passive-interface Serial0/2/0
  network 10.5.34.0 0.0.0.3
  network 10.5.41.0 0.0.0.3
  auto-summary
!
router ospf 1
  router-id 5.5.5.5
  log-adjacency-changes
  redistribute eigrp 1 metric 1 subnets
  passive-interface default
  no passive-interface Serial0/1/1
  network 10.5.2.52 0.0.0.3 area 0

```

```
ROUTER5#sh ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address
1.1.1.1	0	FULL/ -	00:00:31	10.5.2.53

```
ROUTER5#sh ip eigrp neighbors
```

IP-EIGRP neighbors for process 1

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	10.5.41.2	Se0/2/0	14	01:39:26	40	1000	0	35
1	10.5.34.2	Se0/1/0	14	01:39:24	40	1000	0	35

- Galway

```
router eigrp 1
  eigrp router-id 5.5.5.1
  passive-interface default
  no passive-interface Serial0/1/0
  network 10.5.34.0 0.0.0.3
  network 10.5.32.0 0.0.1.255
  auto-summary
```

IP-EIGRP interfaces for process 1							
Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes	
Se0/1/0	1	0/0	1236	0/10	0	0	

IP-EIGRP neighbors for process 1							
H	Address	Interface	Hold (sec)	Uptime (ms)	SRTT	RTO	Q Cnt Seq Num
0	10.5.34.1	Se0/1/0	10	05:12:50	40	1000	0 61

- Limerick

```
router eigrp 1
  eigrp router-id 5.5.5.2
  passive-interface default
  no passive-interface Serial0/1/0
  network 10.5.41.0 0.0.0.3
  network 10.5.40.0 0.0.0.255
  auto-summary
```

IP-EIGRP interfaces for process 1							
Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes	
Se0/1/0	1	0/0	1236	0/10	0	0	

IP-EIGRP neighbors for process 1							
H	Address	Interface	Hold (sec)	Uptime (ms)	SRTT	RTO	Q Cnt Seq Num
0	10.5.41.1	Se0/1/0	13	05:15:11	40	1000	0 61

- ISP

```
router ospf 1
  router-id 8.8.8.8
  log-adjacency-changes
  network 10.5.2.32 0.0.0.3 area 0
  default-information originate
```

ISP#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address
1.1.1.1	1	FULL/BDR	00:00:32	10.5.2.33

Dans cette illustration, nous pouvons observer les résultats du routage OSPF sur l'ensemble du réseau, en examinant l'exemple de la base de données du routeur DUBLIN.

```
DUBLIN#sh ip ospf database
      OSPF Router with ID (1.1.1.1) (Process ID 1)

      Router Link States (Area 0)
Link ID      ADV Router      Age      Seq#      Checksum Link
1.1.1.1      1.1.1.1      1554      0x80000015 0x00b4fb 10
5.5.5.5      5.5.5.5      1589      0x8000000b 0x0014f0 2
4.4.4.4      4.4.4.4      1586      0x8000000b 0x0cc49 2
3.3.3.1      3.3.3.1      1584      0x8000000b 0x00181a 2
3.3.3.2      3.3.3.2      1584      0x8000000b 0x00988f 2
8.8.8.8      8.8.8.8      1555      0x8000000b 0x00f3ae 1
2.2.2.2      2.2.2.2      1550      0x8000000b 0x001bb0 1

      Net Link States (Area 0)
Link ID      ADV Router      Age      Seq#      Checksum
10.5.2.34    8.8.8.8      1555      0x80000009 0x00ed7b
10.5.2.38    2.2.2.2      1550      0x80000009 0x00e5ad

      Summary Net Link States (Area 0)
Link ID      ADV Router      Age      Seq#      Checksum
10.5.24.0    4.4.4.4      1582      0x80000009 0x0043db
10.5.16.0    3.3.3.2      1579      0x80000019 0x009a82
10.5.16.0    3.3.3.1      1579      0x80000019 0x0a07d
10.5.2.0     2.2.2.2      1545      0x80000029 0x0077c4
10.5.1.128   2.2.2.2      1545      0x8000002a 0x00ba21
10.5.1.192   2.2.2.2      1545      0x8000002b 0x003664
10.5.0.0     2.2.2.2      1545      0x8000002c 0x0042d9
10.5.1.0     2.2.2.2      1545      0x8000002d 0x003861

      Summary ASB Link States (Area 0)
Link ID      ADV Router      Age      Seq#      Checksum
5.5.5.5      3.3.3.2      1539      0x8000001a 0x001392
5.5.5.5      3.3.3.1      1539      0x8000001a 0x00198d
8.8.8.8      3.3.3.2      1529      0x8000001b 0x000ec9
8.8.8.8      3.3.3.1      1529      0x8000001b 0x0014c4

      Type-5 AS External Link States
Link ID      ADV Router      Age      Seq#      Checksum Tag
10.5.34.0    5.5.5.5      1598      0x80000009 0x001c6d 0
10.5.41.0    5.5.5.5      1598      0x80000009 0x00ceb3 0
0.0.0.0      8.8.8.8      1594      0x80000009 0x001c8e 1
10.5.40.0    5.5.5.5      1593      0x80000009 0x00eb94 0
10.5.32.0    5.5.5.5      1589      0x80000009 0x003f4a 0
DUBLIN#
```

- PPP - Les liaisons entre Dublin, Édinbourg, Cork et Galway-Limerick ont été sécurisées au moyen des connexions PPP (Point-to-Point Protocol).
- PPP-CHAP Dublin

```
interface Serial0/2/0
  description CORK
  ip address 10.5.2.49 255.255.255.252
  zone-member security IN
  encapsulation ppp
  ppp authentication chap
  clock rate 2000000
!
interface Serial0/2/1
  description GALWAY-LIMERICK
  ip address 10.5.2.53 255.255.255.252
  zone-member security IN
  encapsulation ppp
  ppp authentication chap
  clock rate 2000000
!
```

- PPP-CHAP Cork

```
interface Serial0/1/0
  description DUBLIN
  ip address 10.5.2.50 255.255.255.252
  encapsulation ppp
  ppp authentication chap
```

- PPP-CHAP Router5 (Galway-Limerick)

```
interface Serial0/1/1
  description DUBLIN
  ip address 10.5.2.54 255.255.255.252
  encapsulation ppp
  ppp authentication chap
```

- PPP-PAP Dublin

```
interface Serial0/1/0
description ED1
ip address 10.5.2.41 255.255.255.252
zone-member security IN
encapsulation ppp
ppp authentication pap
ppp pap sent-username DUBLIN password 0 cisco
clock rate 2000000
!
interface Serial0/1/1
description ED2
ip address 10.5.2.45 255.255.255.252
zone-member security IN
encapsulation ppp
ppp authentication pap
ppp pap sent-username DUBLIN password 0 cisco
clock rate 2000000
```

- PPP-PAP ED1

```
interface Serial0/1/0
description DUBLIN
ip address 10.5.2.42 255.255.255.252
encapsulation ppp
ppp authentication pap
ppp pap sent-username ED1 password 0 cisco
```

- PPP-PAP ED2

```
interface Serial0/1/0
description DUBLIN
ip address 10.5.2.46 255.255.255.252
encapsulation ppp
ppp authentication pap
ppp pap sent-username ED2 password 0 cisco
```

- ZPF - L'entreprise a besoin d'une protection externe, et pour cela sans un pare-feu bien configuré elle n'est pas sécurisée. Mais pour avoir accès au site www.local.com, les ports 80 et 443 sont ouverts, ainsi que pour le ftp, afin que les webmasters aient accès, par une ACL.

```

class-map type inspect match-any IN_PROTOCOLS
match protocol dns
match protocol ftp
match protocol http
match protocol https
match protocol icmp
match protocol pop3
match protocol smtp
match protocol telnet
match protocol udp
match protocol ssh
class-map type inspect match-any OUT_IN_WWW
match access-group 101
!
policy-map type inspect IN_TO_OUT
  class type inspect IN_PROTOCOLS
    inspect
!
policy-map type inspect OUT_TO_IN
  class type inspect OUT_IN_WWW
    inspect
!
!
zone security IN
zone security OUT
zone-pair security IN_TO_OUT source IN destination OUT
  service-policy type inspect IN_TO_OUT
zone-pair security OUT_TO_IN source OUT destination IN
  service-policy type inspect OUT_TO_IN
!
!
```

```

interface GigabitEthernet0/0/0
  description ISP
  ip address 10.5.2.33 255.255.255.252
  zone-member security OUT
  duplex auto
  speed auto
!
interface GigabitEthernet0/0/1
  description Dublin-SwL3
  ip address 10.5.2.37 255.255.255.252
  zone-member security IN
  duplex auto
  speed auto
!
interface GigabitEthernet0/0/2
  no ip address
  zone-member security IN
  duplex auto
  speed auto
  shutdown
!
```

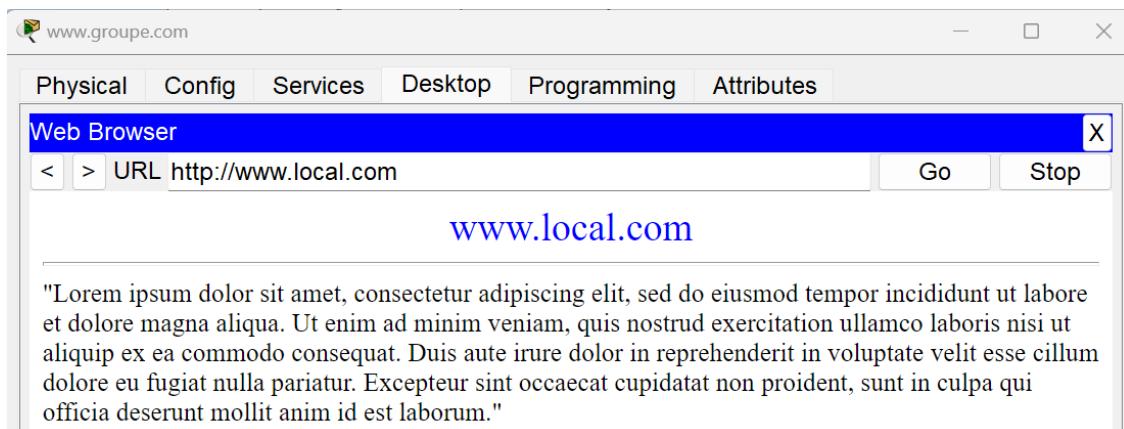
- ACL

```

!
access-list 101 permit tcp any host 10.5.1.2 eq 443
access-list 101 permit tcp any host 10.5.1.2 eq ftp
access-list 101 permit tcp any host 10.5.1.2 eq www
!
```

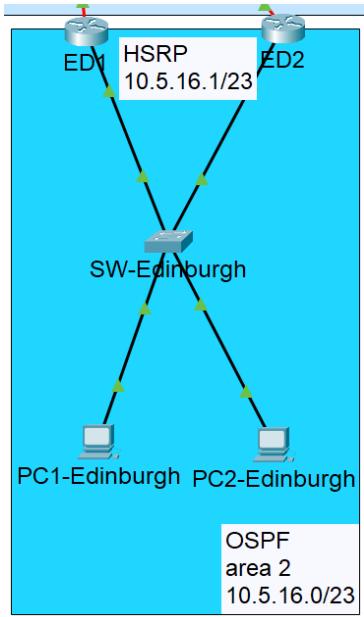
Le résultat du travail du pare-feu. L'accès au site www.local.com est confirmé, et les essais de ping, à la fois de l'intérieur vers l'extérieur et en sens inverse, sont démontrés sur l'illustration. www.groupe.com est le serveur d'extérieur.

Fire	Last Status	Source	Destination	Type	Colo
	Failed	www.groupe.com	PC - SALES	ICMP	
	Successful	PC - SALES	www.groupe.com	ICMP	



Configuration de la branche d'Edinburgh

- HSRP



Le site d'Edinburgh a instauré une redondance via le protocole HSRP. La priorité est attribuée en faveur du routeur ED1 par rapport au routeur ED2.

- ED1

```
interface GigabitEthernet0/0/1
description SW-Edinburgh
ip address 10.5.16.2 255.255.254.0
duplex auto
speed auto
standby version 2
standby 1 ip 10.5.16.1
standby 1 priority 150
standby 1 preempt
```

- ED2

```
interface GigabitEthernet0/0/1
description SW-Edinburgh
ip address 10.5.16.3 255.255.254.0
duplex auto
speed auto
standby version 2
standby 1 ip 10.5.16.1
```

```

ED1#sh standby brief
                  P indicates configured to preempt.
                  |
Interface   Grp  Pri P State      Active           Standby        Virtual IP
Gig0/0/1     1    150 P Active    local            10.5.16.3      10.5.16.1
ED1#
ED1#
ED1#sh standby
GigabitEthernet0/0/1 - Group 1 (version 2)
  State is Active
    7 state changes, last state change 00:00:17
    Virtual IP address is 10.5.16.1
    Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
    Hello time 3 sec, hold time 10 sec
      Next hello sent in 2.42 secs
    Preemption enabled
    Active router is local
    Standby router is 10.5.16.3, priority 100 (expires in 6 sec)
    Priority 150 (configured 150)
    Group name is hsrp-Gig0/0/1-1 (default)
ED1#

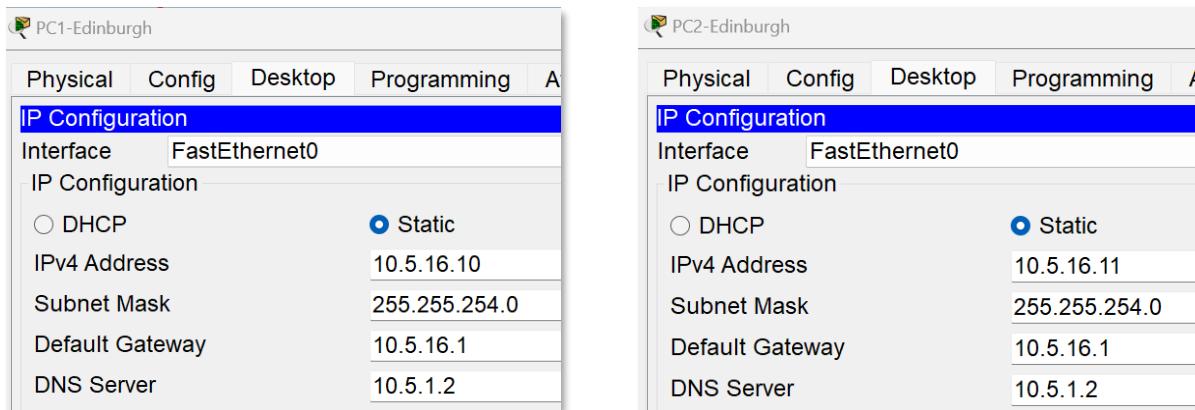
```

```

ED2#sh standby brief
                  P indicates configured to preempt.
                  |
Interface   Grp  Pri P State      Active           Standby        Virtual IP
Gig0/0/1     1    100  Standby   10.5.16.2      local          10.5.16.1
ED2#
ED2#
ED2#sh standby
GigabitEthernet0/0/1 - Group 1 (version 2)
  State is Standby
    8 state changes, last state change 00:00:40
    Virtual IP address is 10.5.16.1
    Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
    Hello time 3 sec, hold time 10 sec
      Next hello sent in 0.653 secs
    Preemption disabled
    Active router is 10.5.16.2, priority 150 (expires in 9 sec)
      MAC address is 0000.0C9F.F001
    Standby router is local
    Priority 100 (default 100)
    Group name is hsrp-Gig0/0/1-1 (default)
ED2#

```

Les terminaux sont configurés avec des adresses IP statiques, car aucun serveur DHCP n'est en place.



Dans l'exemple illustré, le protocole on teste le protocole HSRP s'il est bien configuré. Il est clair que le flux de trafic traverse le routeur ED1, identifié par l'adresse IP 10.5.16.2.

```

PC2-Edinburgh
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 200.1.5.1

Pinging 200.1.5.1 with 32 bytes of data:

Request timed out.
Reply from 200.1.5.1: bytes=32 time=82ms TTL=125
Reply from 200.1.5.1: bytes=32 time=72ms TTL=125
Reply from 200.1.5.1: bytes=32 time=69ms TTL=125

Ping statistics for 200.1.5.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 69ms, Maximum = 82ms, Average = 74ms

C:\>tracert 200.1.5.1

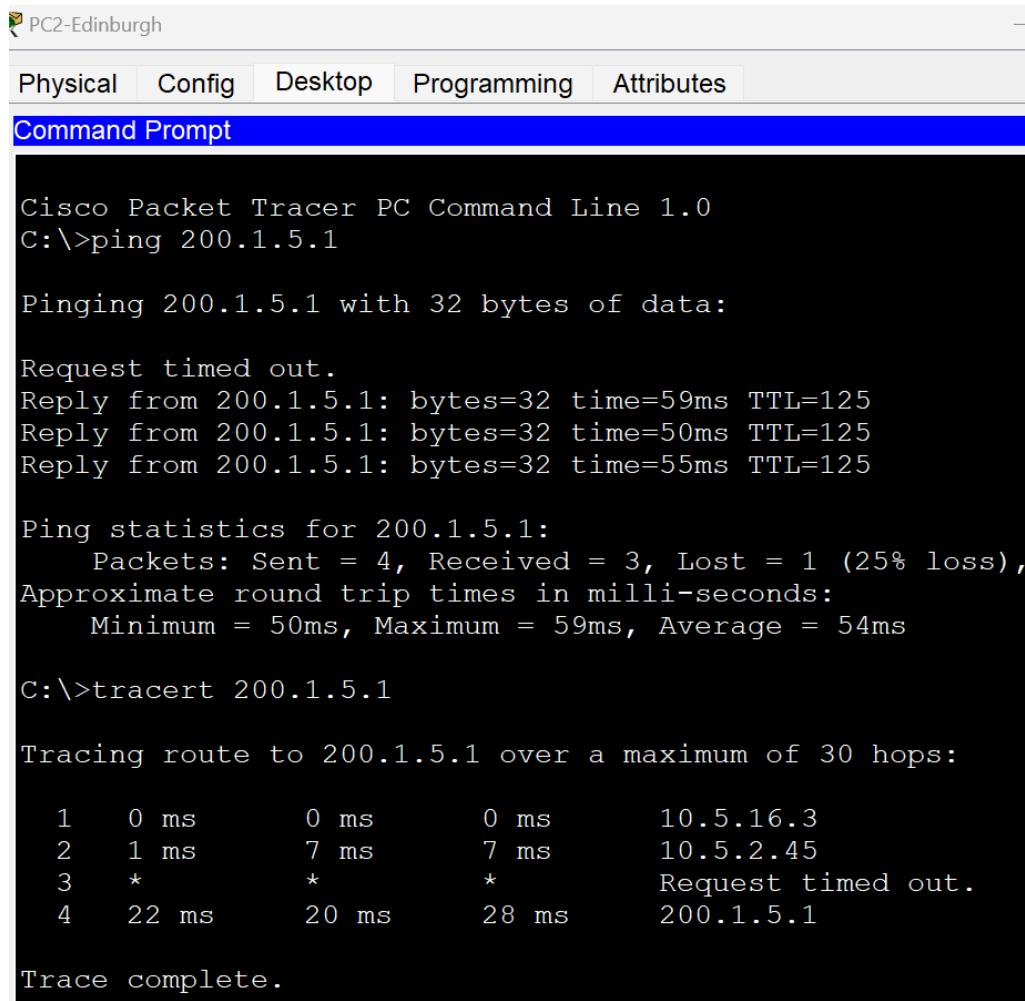
Tracing route to 200.1.5.1 over a maximum of 30 hops:

    1    0 ms      0 ms      0 ms      10.5.16.2
    2    9 ms      9 ms     15 ms     10.5.2.45
    3    *          *          *          Request timed out.
    4   29 ms     15 ms     23 ms     200.1.5.1

Trace complete.

```

En déconnectant ED1 on teste à nouveau et on voit que le trafic traverse ED2, qui a IP 10.5.16.3 .
On trouve que la redondance fonctionne.



The screenshot shows a window titled "PC2-Edinburgh" with a toolbar at the top containing icons for Physical, Config, Desktop, Programming, and Attributes. The "Command Prompt" tab is selected, highlighted in blue. The main area displays the output of a ping and tracert command.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 200.1.5.1

Pinging 200.1.5.1 with 32 bytes of data:

Request timed out.
Reply from 200.1.5.1: bytes=32 time=59ms TTL=125
Reply from 200.1.5.1: bytes=32 time=50ms TTL=125
Reply from 200.1.5.1: bytes=32 time=55ms TTL=125

Ping statistics for 200.1.5.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 50ms, Maximum = 59ms, Average = 54ms

C:\>tracert 200.1.5.1

Tracing route to 200.1.5.1 over a maximum of 30 hops:

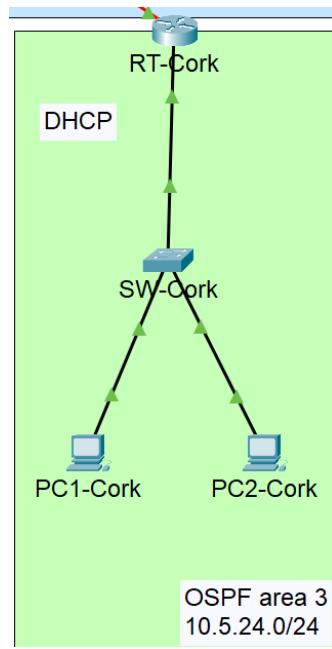
  1  0 ms      0 ms      0 ms      10.5.16.3
  2  1 ms      7 ms      7 ms      10.5.2.45
  3  *          *          *          Request timed out.
  4  22 ms     20 ms     28 ms      200.1.5.1

Trace complete.
```

Configuration de la branche du Cork

Au sein de cette branche, la configuration inclut un serveur DHCP pour IPv4 ainsi qu'un adressage IPv6 simple via SLACC.

```
ip dhcp excluded-address 10.5.24.1
!
ip dhcp pool CORK
network 10.5.24.0 255.255.255.0
default-router 10.5.24.1
dns-server 10.5.1.2
```



```
interface GigabitEthernet0/0/1
description SW-CORK
ip address 10.5.24.1 255.255.255.0
duplex auto
speed auto
ipv6 address FE80::1 link-local
ipv6 address FC00:0:0:1::1/64
```

```
CORK#sh ipv6 interface
GigabitEthernet0/0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    FC00:0:0:1::1, subnet is FC00:0:0:1::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
```

```

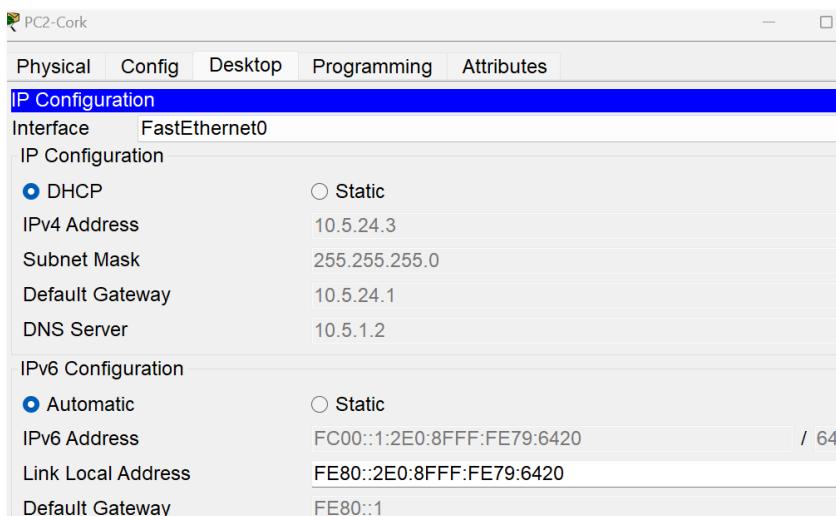
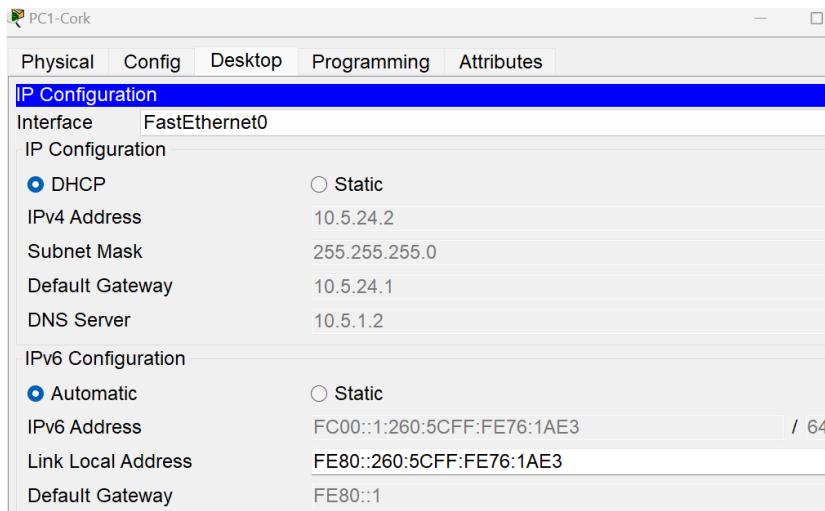
CORK#sh ip dhcp pool

Pool CORK :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)        : 0 / 0
  Total addresses                 : 254
  Leased addresses                : 2
  Excluded addresses              : 1
  Pending event                   : none

  1 subnet is currently in the pool
  Current index      IP address range          Leased/Excluded/Total
  10.5.24.1           10.5.24.1       - 10.5.24.254    2      / 1      / 254
CORK#

```

Les ordinateurs ont bien reçu les adresses appropriées.



Les branches de Galway et Limerick bénéficient d'une connexion tunnel VPN IPsec.

Les configurations des routeurs Galway et Limerick suivent.

- Galway

```
interface Serial0/1/0
description Router5
ip address 10.5.34.2 255.255.255.252
crypto map VPN-MAP
```

IPSec nécessite une ACL. L'exemple d'ACL du Galway

```
!
access-list 110 permit ip 10.5.32.0 0.0.1.255 10.5.40.0 0.0.0.255
!
```

```
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 5
!
crypto isakmp key ciscovpn address 10.5.41.2
!
!
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
  description $ VPN connection to Limerick router $
  set peer 10.5.41.2
  set transform-set VPN-SET
  match address 110
!
```

- Limerick

```
interface Serial0/1/0
description Router5
ip address 10.5.41.2 255.255.255.252
crypto map VPN-MAP
!
```

L'exemple d'ACL du Limerick

```
!
access-list 110 permit ip 10.5.40.0 0.0.0.255 10.5.32.0 0.0.1.255
!
```

```
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 5
!
crypto isakmp key ciscovpn address 10.5.34.2
!
!
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
  description $ VPN connection to Galway router $
  set peer 10.5.34.2
  set transform-set VPN-SET
  match address 110
!
```

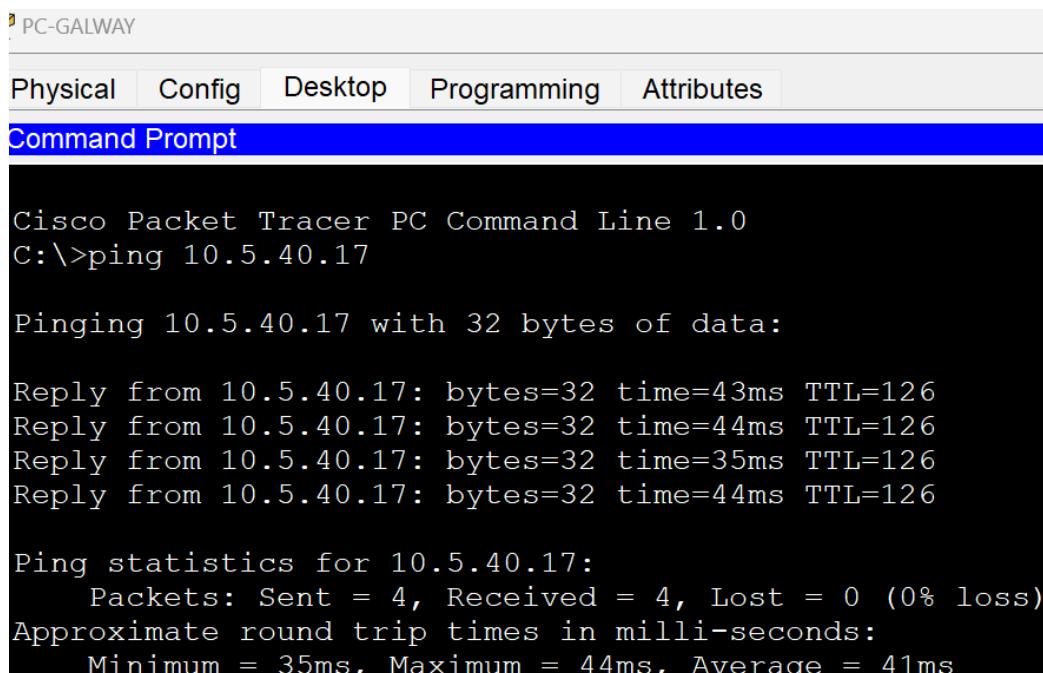
Dans les illustrations suivantes, la connexion est établie. Mais il faut la vérifier

```
GALWAY#sh crypto map
Crypto Map VPN-MAP 10 ipsec-isakmp
  Peer = 10.5.41.2
  Extended IP access list 110
    access-list 110 permit ip 10.5.32.0 0.0.1.255 10.5.40.0 0.0.0.255
  Current peer: 10.5.41.2
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N) : N
  Transform sets={
    VPN-SET,
  }
  Interfaces using crypto map VPN-MAP:
    Serial0/1/0
```

```
LIMERICK#sh crypto map
Crypto Map VPN-MAP 10 ipsec-isakmp
  Peer = 10.5.34.2
  Extended IP access list 110
    access-list 110 permit ip 10.5.40.0 0.0.0.255 10.5.32.0 0.0.1.255
  Current peer: 10.5.34.2
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={
    VPN-SET,
  }
Interfaces using crypto map VPN-MAP:
  Serial0/1/0
```

Afin de vérifier le bon fonctionnement du tunnel, il est nécessaire de générer du trafic sur le réseau, par exemple, en effectuant un ping entre les terminaux de Galway et ceux de Limerick.

Fire	Last Status	Source	Destination	Type	Color
●	Successful	PC-G...	Smartphone	ICMP	■
●	Successful	Laptop	PC-GALWAY	ICMP	■



On constate qu'il y avait des paquets encapsulés et désencapsulés.

```
GALWAY#sh crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN-MAP, local addr 10.5.34.2

    protected vrf: (none)
    local ident (addr/mask/prot/port): (10.5.32.0/255.255.254.0/0/0)
    remote ident (addr/mask/prot/port): (10.5.40.0/255.255.255.0/0/0)
    current_peer 10.5.41.2 port 500
        PERMIT, flags={origin_is_acl,}
    #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
    #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

    local crypto endpt.: 10.5.34.2, remote crypto endpt.:10.5.41.2
    path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
    current outbound spi: 0x34AB044F(883622991)

    inbound esp sas:
        spi: 0x3BDC279E(1004283806)
            transform: esp-aes esp-sha-hmac ,
            in use settings ={Tunnel, }
            conn id: 2001, flow_id: FPGA:1, crypto map: VPN-MAP
            sa timing: remaining key lifetime (k/sec): (4525504/3586)
            IV size: 16 bytes
            replay detection support: N
            Status: ACTIVE
```

```
LIMERICK#sh crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN-MAP, local addr 10.5.41.2

    protected vrf: (none)
    local ident (addr/mask/prot/port): (10.5.40.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (10.5.32.0/255.255.254.0/0/0)
    current_peer 10.5.34.2 port 500
        PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
    #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 10.5.41.2, remote crypto endpt.:10.5.34.2
    path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
    current outbound spi: 0x3BDC279E(1004283806)

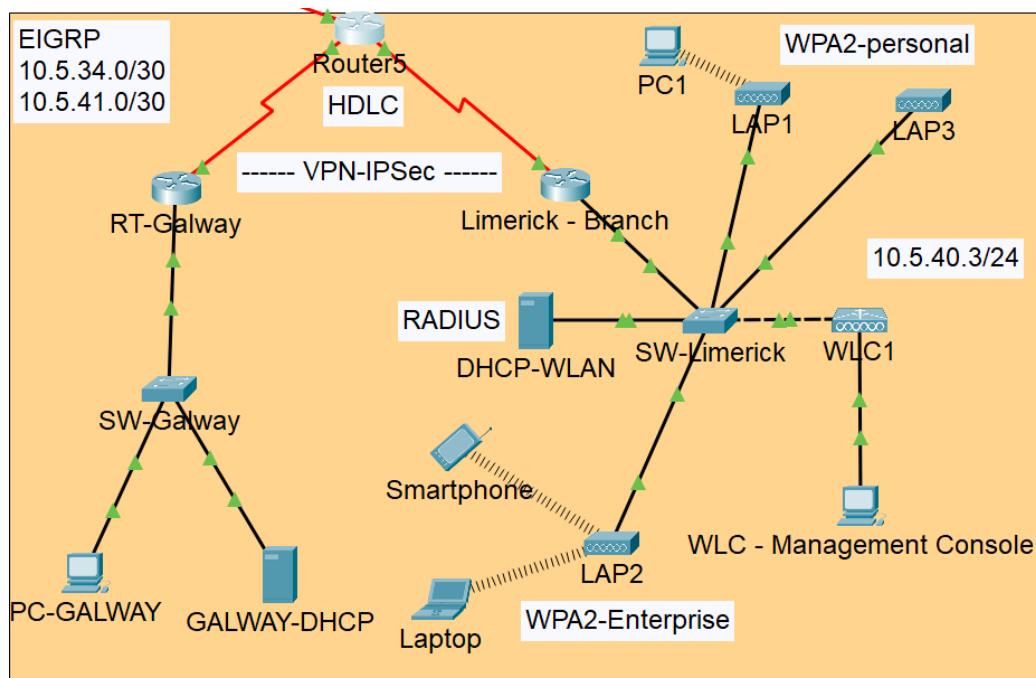
    inbound esp sas:
        spi: 0x34AB044F(883622991)
            transform: esp-aes esp-sha-hmac ,
            in use settings ={Tunnel, }
            conn id: 2001, flow_id: FPGA:1, crypto map: VPN-MAP
            sa timing: remaining key lifetime (k/sec): (4525504/3467)
            IV size: 16 bytes
            replay detection support: N
            Status: ACTIVE
```

- L'encapsulation HDLC est configurée entre Router5 et Galway, ainsi qu'entre Router5 et Limerick, afin de renforcer le contrôle des connexions série (point à point) et d'assurer une correction des erreurs de trafic.

```
GALWAY#sh interfaces s0/1/0
Serial0/1/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Description: Router5
  Internet address is 10.5.34.2/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
```

```
LIMERICK#sh int s0/1/0
Serial0/1/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Description: Router5
  Internet address is 10.5.41.2/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
```

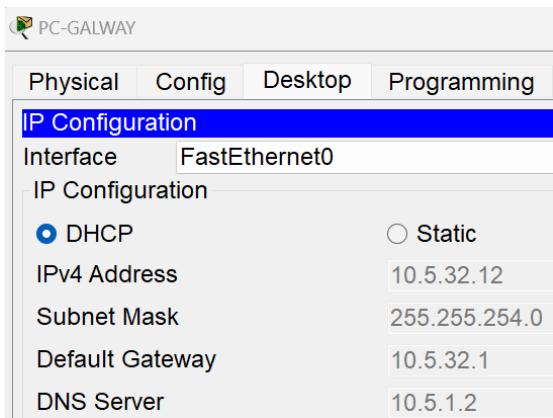
Les branches Galway et Limerick



- Dans la branche de **Galway**, un serveur DHCP basique a été mis en place.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User
serverPool	10.5.32.1	10.5.1.2	10.5.32.12	255.255.254.0	500

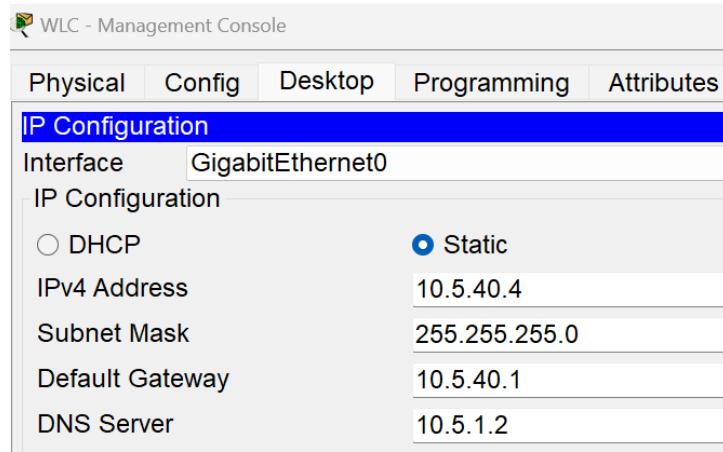
On observe respectivement que le serveur DHCP fonctionne correctement, l'ordinateur a obtenu une adresse IP.



- Dans la succursale de **Limerick**, un serveur DHCP avec AAA a été déployé, lequel partagera les adresses via un WLC également, pour avoir des connexions sans fils.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	10.5.40.1	10.5.1.2	10.5.40.10	255.255.255.0	246	10.5.1.2	10.5.40.3

- La configuration du WLC est la suivante. On le configure en utilisant une adresse statique.



Web Browser < > URL <https://10.5.40.3/frameMonitor.html>

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAG

Monitor

- Summary
- Access Points
- Cisco CleanAir
- Statistics
- CDP
- Rogues
- Clients
- Sleeping Clients
- Multicast
- Applications
- Local Profiling

Controller Summary

Management IP Address	10.5.40.3 , ::/128
Software Version	8.3.111.0
Field Recovery Image Version	7.6.101.1
System Name	WLC1
Up Time	3 hours, 12 minutes, 29 seconds
System Time	Sun Nov 12 01:08:41 2023
Redundancy Mode	N/A
Internal Temperature	+31 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	
CPU(s) Usage	0%
Individual CPU Usage	0%/1%, 0%/0%
Memory Usage	46%
Fan Status	3800 rpm

Access Point Summary

	Total	Up	Down	
802.11a/n/ac Radios	3	3	0	Detail
802.11b/g/n Radios	3	3	0	Detail
Dual-Band Radios	0	0	0	Detail
All APs	3	3	0	Detail

Client Summary

Current Clients	3	Detail
Excluded Clients	0	Detail
Disabled Clients	0	Detail

Radius server

The screenshot shows the 'AAA' configuration page in the Cisco WLC interface. The left sidebar lists various services: HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA (selected), NTP, EMAIL, FTP, IoT, VM Management, and Radius EAP. The main area is titled 'AAA' and contains the following sections:

- Service:** Radio button is set to 'On'. **Radius Port:** 1645.
- Network Configuration:**
 - Client Name:** [Input field]
 - Client IP:** [Input field]
 - Secret:** [Input field] **ServerType:** Radius
 - Table:**

Client Name	Client IP	Server Type	Key
1 WLC1	10.5.40.3	Radius	Cisco12345
- User Setup:**
 - Username:** [Input field] **Password:** [Input field]
 - Table:**

Username	Password
1 radius	Cisco12345

Deux réseaux WiFi ont été établis, Limerick-WiFi avec l'authentification WPA2-PSK, et Radius-WiFi avec l'authentification Radius, en utilisant le serveur Radius configuré précédemment.

	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
<input type="checkbox"/>	1	WLAN	Limerick-WiFi	Limerick-WiFi	Enabled	[WPA2][Auth(PSK)]
<input type="checkbox"/>	2	WLAN	Radius-WiFi	Radius-WiFi	Enabled	[WPA2][Auth(802.1X)]

Ici, on trouve la configuration IP du serveur Radius sur le WLC.

The screenshot shows the 'Security' tab in the Cisco WLC configuration interface, specifically the 'AAA Servers' section. The tabs at the top are General, Security, QoS, Policy-Mapping, Advanced, Layer 2, Layer 3, and AAA Servers (selected). The main area displays the following configuration:

- Select AAA servers below to override use of default servers on this WL**
- Radius Servers**
- Radius Server Overwrite interface:** Enabled
- Authentication Servers:** Enabled. **IP:** 10.5.40.2, **Port:** 1645.
- Accounting Servers:** Enabled. **IP:** None.
- EAP:** Enabled.

RADIUS Authentication Servers

Auth Called Station ID Type	IP Address			
Use AES Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)			
MAC Delimiter	Hyphen			
Framed MTU	1300			
Network User	Management	Server Index	Server Address(Ipv4/Ipv6)	Port
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	*	10.5.40.2

Sur le réseau, il y a trois points d'accès répartis en deux groupes : l'un dédié à Radius (WPA2-Enterprise) et l'autre à WPA2-PSK. Les LAP1 et LAP3 sont configurés pour WPA2-PSK, tandis que le LAP2 via l'authentification Radius.

AP Groups

AP Group Name	AP Group Description
Limerick-WiFi	PSK
Radius-WiFi	Radius
default-group	

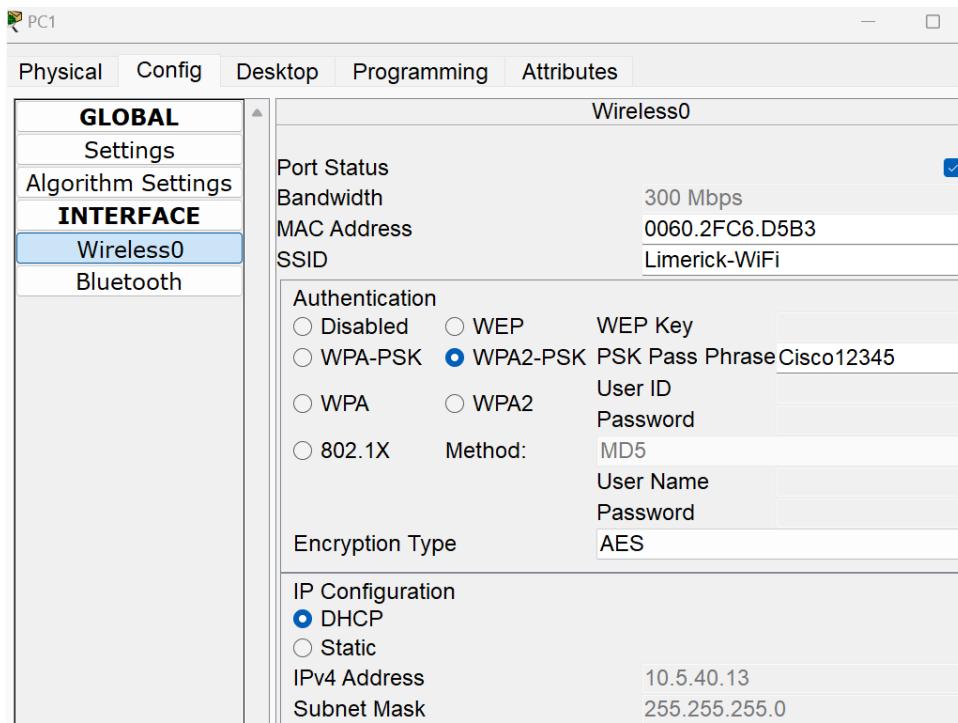
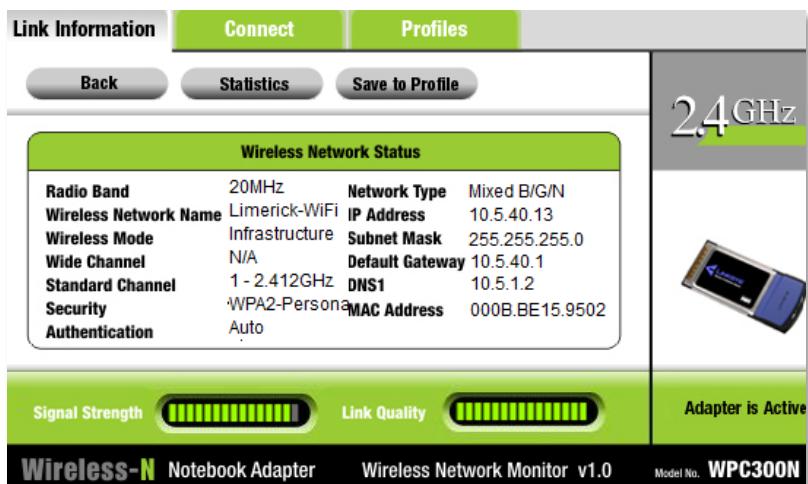
Ap Groups > Edit 'Limerick-WiFi'

General	WLANS	RF Profile	APs	802.11u	Location	Ports/Module
APs currently in the Group				Add APs to the Group		
<input type="checkbox"/> AP Name Ethernet MAC <input type="checkbox"/> LAP3 0090.2B7E.5001 <input type="checkbox"/> LAP1 000B.BE15.9501				<input type="checkbox"/> AP Name Group Name <input type="checkbox"/> LAP2 Radius-WiFi		

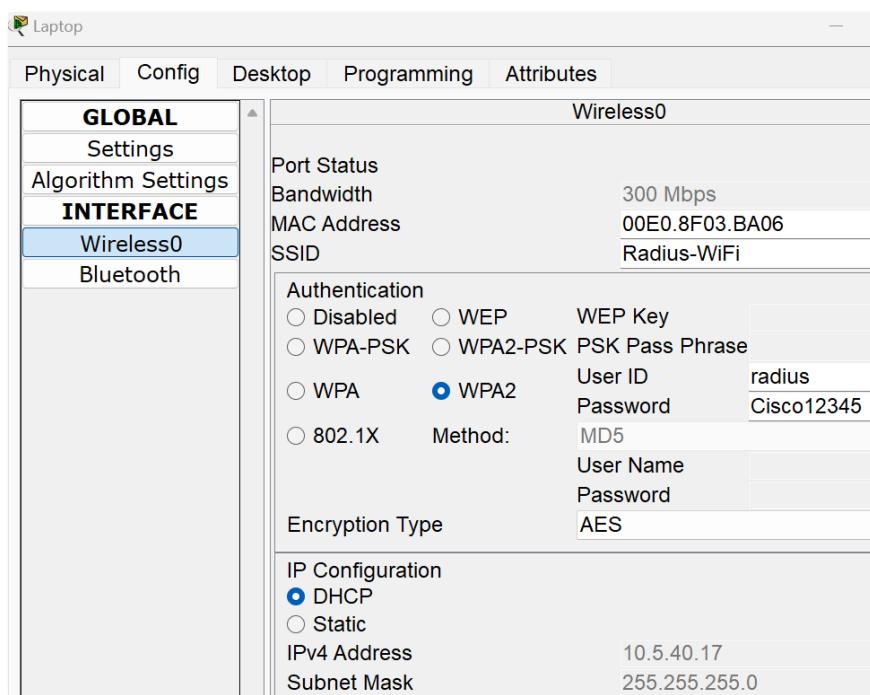
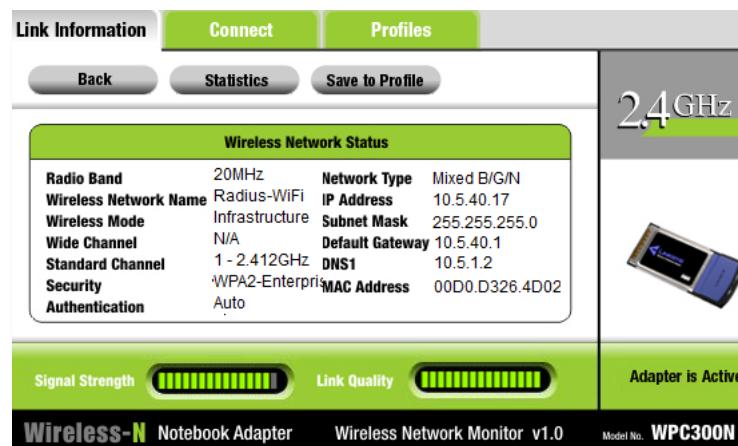
Ap Groups > Edit 'Radius-WiFi'

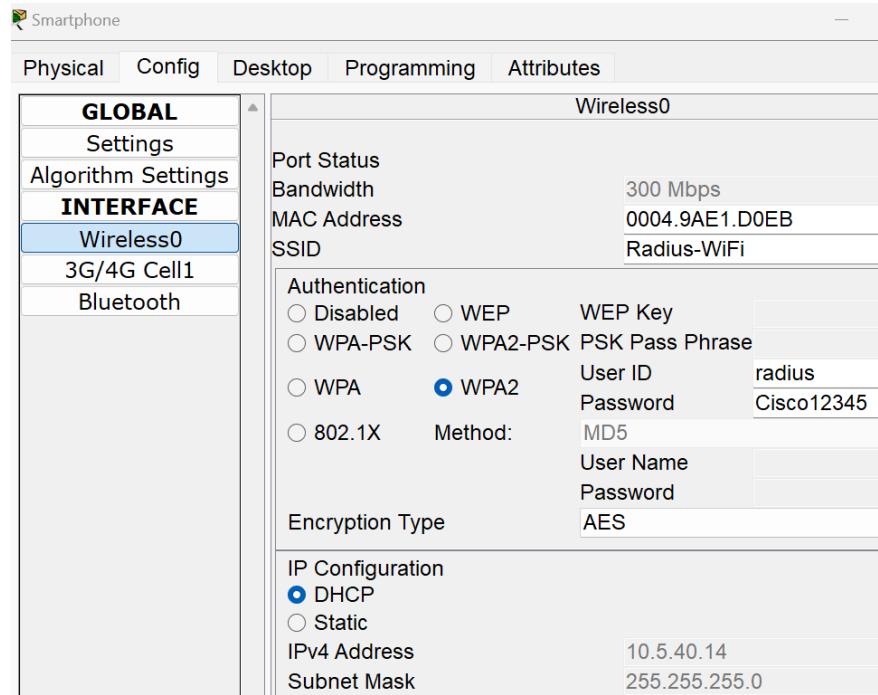
General	WLANS	RF Profile	APs	802.11u	Location	Ports/Module
APs currently in the Group				Add APs to the Group		
<input type="checkbox"/> AP Name Ethernet MAC <input type="checkbox"/> LAP2 00D0.D326.4D01				<input type="checkbox"/> AP Name Group Name <input type="checkbox"/> LAP3 Limerick-WiFi <input type="checkbox"/> LAP1 Limerick-WiFi		

On test d'abord la connexion à Limerick-WiFi, qui utilise une authentification WPA2-PSK. On connecte l'ordinateur au point d'accès LAP1.



Ensuite, on procède au test de l'authentification Radius en connectant à la fois l'ordinateur portable et le smartphone au point d'accès LAP2.





- NAT - Pour sécuriser et anonymiser le réseau à l'extérieur, nous utiliserons le NAT et le PAT. Cependant, pour le serveur www.local.com, nous utiliserons un NAT statique afin de permettre l'accès à la page web depuis l'extérieur.

```
ip nat inside source list 1 interface GigabitEthernet0/0/1 overload
ip nat inside source static 10.5.1.2 200.1.5.2
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/1
!
ip flow-export version 9
!
!
access-list 1 permit 10.5.0.0 0.0.255.255
```

```
interface GigabitEthernet0/0/0
description DUBLIN
ip address 10.5.2.34 255.255.255.252
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/0/1
description ISP
ip address 200.1.5.2 255.255.255.252
ip nat outside
duplex auto
speed auto
!
```

Afin de vérifier le fonctionnement du NAT, nous allons générer du trafic, en effectuant des pings et en accédant à www.groupe.com.

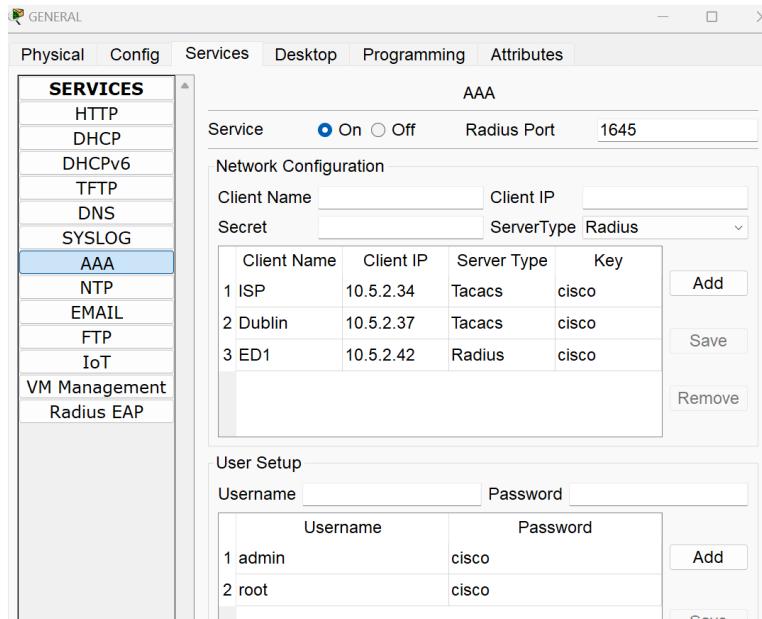
Fire	Last Status	Source	Destination	Type	Co
●	Successful	SALES	www.groupe.com	ICMP	■
●	Successful	GENERAL	www.groupe.com	ICMP	■
●	Successful	Laptop	www.groupe.com	ICMP	■



Les adresses IP ont été traduites avec succès, une adresse IP publique a été attribuée, 200.1.5.1

```
ISP#sh ip nat statistics
Total translations: 7 (1 static, 6 dynamic, 6 extended)
Outside Interfaces: GigabitEthernet0/0/1
Inside Interfaces: GigabitEthernet0/0/0
Hits: 57 Misses: 28
Expired translations: 21
Dynamic mappings:
ISP#
ISP#
ISP#sh ip nat translations
Pro Inside global      Inside local        Outside local       Outside global
icmp 200.1.5.2:2       10.5.1.2:2        200.1.5.1:2       200.1.5.1:2
icmp 200.1.5.2:3       10.5.40.14:3      200.1.5.1:3       200.1.5.1:3
---  200.1.5.2          10.5.1.2          ---             ---
tcp  200.1.5.2:1025    10.5.1.194:1025   200.1.5.1:80     200.1.5.1:80
tcp  200.1.5.2:1026    10.5.1.194:1026   200.1.5.1:443   200.1.5.1:443
tcp  200.1.5.2:1027    10.5.1.194:1027   200.1.5.1:443   200.1.5.1:443
tcp  200.1.5.2:80       10.5.1.2:80        200.1.5.1:1025  200.1.5.1:1025
```

- Le test AAA avec Radius et Tacacs+



- Dublin – Tacacs+

```
aaa new-model
!
aaa authentication login default group tacacs+ local
!
```

```
!
tacacs-server host 10.5.1.2
tacacs-server key cisco
!
!
!
line con 0
  login authentication default
!
line aux 0
!
line vty 0 4
  login authentication default
  transport input ssh
!
```

On teste l'authentification Tacacs+ sur le routeur Dublin. L'authentification a réussi.

The screenshot shows a terminal window with the title "PC-IT Support". The tabs at the top are "Physical", "Config", "Desktop", "Programming", and "Attributes". The active tab is "Command Prompt". The command entered is "C:\>ssh -l admin 10.5.2.37". The password is entered twice. The output shows the interface status:

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	10.5.2.33	YES	NVRAM	up	up
GigabitEthernet0/0/1	10.5.2.37	YES	NVRAM	up	up
GigabitEthernet0/0/2	unassigned	YES	NVRAM	administratively down	down
Serial0/1/0	10.5.2.41	YES	NVRAM	up	up
Serial0/1/1	10.5.2.45	YES	NVRAM	up	up
Serial0/2/0	10.5.2.49	YES	NVRAM	up	up
Serial0/2/1	10.5.2.53	YES	NVRAM	up	up
Vlan1	unassigned	YES	unset	administratively down	down

DUBLIN#

- ED1 - Radius

```
aaa new-model
!
aaa authentication login default group radius local
!
```

```
radius server GENERAL
  address ipv4 10.5.1.2 auth-port 1645
  key cisco
radius server 10.5.1.2
  address ipv4 10.5.1.2 auth-port 1645
  key cisco
!
!
!
line con 0
  login authentication default
!
line aux 0
!
line vty 0 4
  login authentication default
  transport input ssh
```

On teste l'authentification Radius sur le routeur Dublin. L'authentification a réussi.

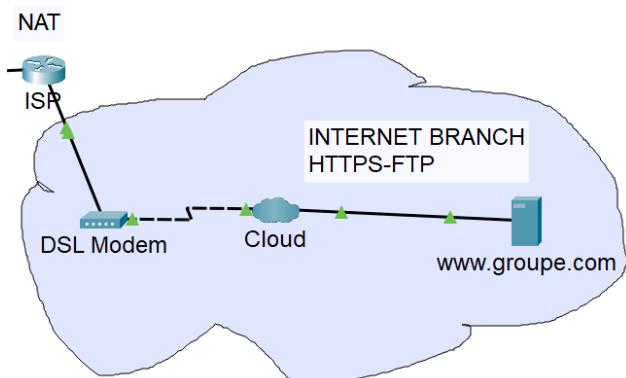
The screenshot shows a terminal window titled "PC-IT Support". The tabs at the top are "Physical", "Config", "Desktop", "Programming", and "Attributes". The active tab is "Command Prompt". The command entered was "C:\>ssh -l admin 10.5.16.2". The password was provided, and the connection was successful. The output shows the interface configuration:

```
C:\>ssh -l admin 10.5.16.2

Password:
ED1>en
Password:
ED1#sh ip int br
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0/0 unassigned      YES NVRAM administratively down down
GigabitEthernet0/0/1 10.5.16.2       YES NVRAM up             up
GigabitEthernet0/0/2 unassigned      YES NVRAM administratively down down
Serial0/1/0          10.5.2.42       YES NVRAM up             up
Serial0/1/1          unassigned     YES NVRAM administratively down down
Vlan1               unassigned     YES unset   administratively down down
ED1#exit

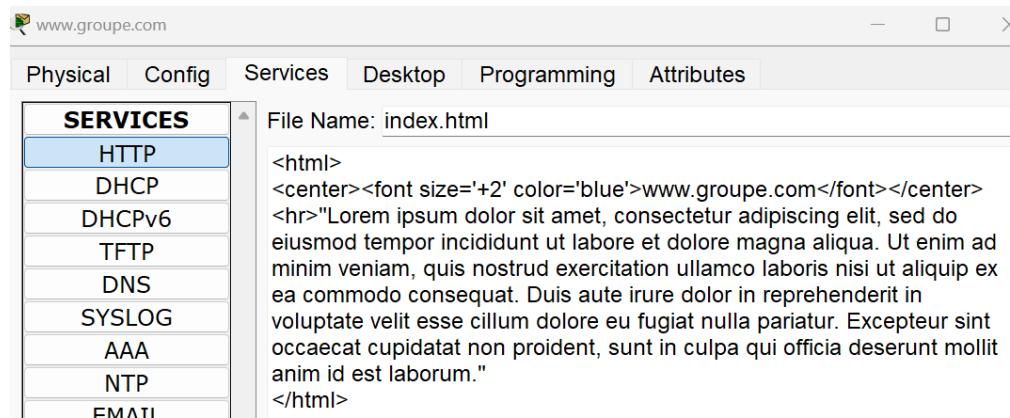
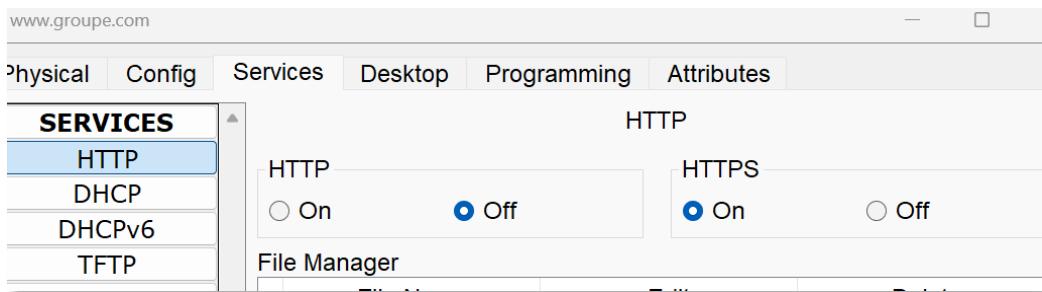
[Connection to 10.5.16.2 closed by foreign host]
```

Configuration de la branche de la branche d'Internet



The screenshot shows a configuration interface for the website "www.groupe.com". The tabs at the top are "Physical", "Config", "Services", "Desktop", and "Program". The active tab is "IP Configuration". The configuration details are as follows:

Setting	Value
DHCP	<input type="radio"/>
Static	<input checked="" type="radio"/>
IPv4 Address	200.1.5.1
Subnet Mask	255.255.255.252
Default Gateway	200.1.5.2
DNS Server	200.1.5.1



- Le test du site www.groupe.com

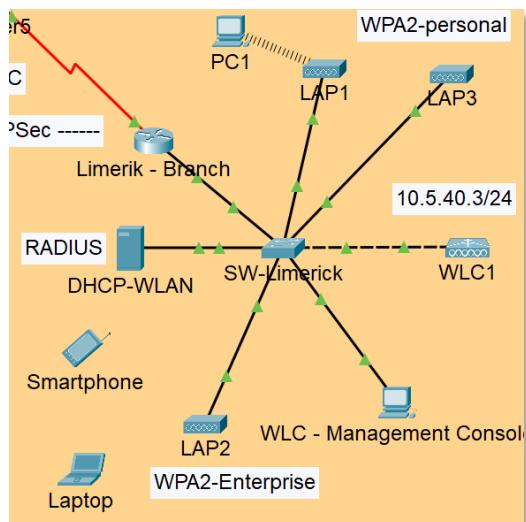
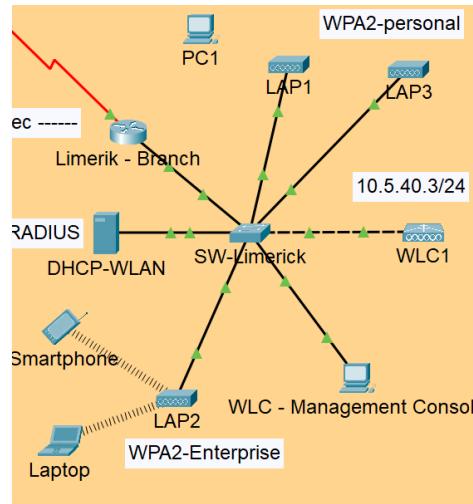


Problèmes rencontrés, méthodes de dépannage et recommandations.

La principale difficulté rencontrée était liée au simulateur Packet Tracer. Souvent, les terminaux ne se connectaient pas aux points d'accès, même si la configuration était correcte. Parfois, la configuration du WLC disparaissait, revenant à la configuration initiale d'usine. La solution a été de reconfigurer le WLC.

Quelques exemples de ces problèmes sont illustrés ci-dessous.

Dans cette illustration, PC1 ne parvient pas à se connecter au point d'accès LAP1.



Sur cette illustration, la connexion Radius ne fonctionne pas, le portable et le téléphone ne parviennent pas à se connecter à LAP2.

Voici quelques exemples d'erreurs rencontrées dans l'application :

Problème de Connexion des Terminaux :

- Symptôme: Les terminaux, comme PC1, ne parviennent pas à se connecter aux points d'accès, même avec une configuration correcte.
- Cause potentielle : Des problèmes avec la fonctionnalité de connexion des terminaux dans Packet Tracer.

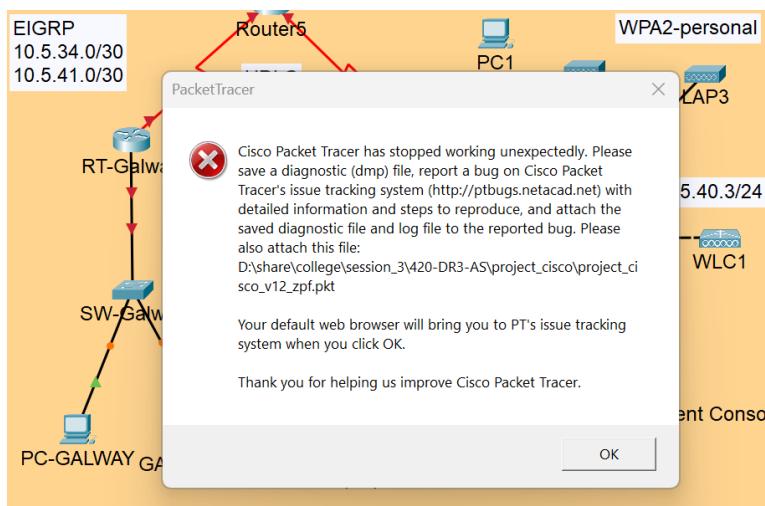
Perte de Configuration dans le WLC :

- Symptôme: La configuration du WLC disparaît parfois, revenant à la configuration d'usine.
- Cause potentielle : Problèmes de stabilité ou de sauvegarde de la configuration dans Packet Tracer.

Échec de la Connexion Radius :

- Symptôme: Les périphériques tels que le portable et le téléphone échouent à se connecter à LAP2 via la connexion Radius.
- Cause potentielle : Problèmes avec la configuration ou la gestion de l'authentification Radius dans Packet Tracer.

Ces exemples illustrent des difficultés qui peuvent survenir lors de l'utilisation de Packet Tracer, et peuvent être liés à des limitations ou des bugs dans l'application. Dans de tels cas, il peut être utile de consulter la documentation de Packet Tracer ou de rechercher des solutions en ligne.



Parfois, j'ai rencontré ce type d'erreurs.

Évidemment, j'ai signalé et envoyé les fichiers de capture (dump) à Cisco.

Networking
Cisco Academy

Thank you for taking the time to report a Cisco Packet Tracer defect. Include as much detail as you can to give us the best chance to fix the issue. For curriculum file related issues, please use the chatbot, support desk, or contact your instructor.

Before we begin, we'd like to know, how satisfied are you with Cisco Packet Tracer?

Extremely unsatisfied Extremely satisfied

0	1	2	3	4	5	6	7	8	9	10
<input type="radio"/>										

What is the nature of this defect?

- Crash or freeze that cannot be avoided
- Crash or freeze when utilizing a specific feature
- Incorrect Behavior
- Graphical error
- Suggestion

```
dump.dmp.log
```

```
1 sYz85ntpy1MMhem1PapKeVaqxbT+5oRj+Ze6stFbIx+00f6rov
2 mLzzVM/Bqu8xcggv02oYaM1T7/sBH7NKCN8zW3ks4YK3FVT1XO
3 DqXZf01U6z3hcfchm6vBSgDMGXeWwH8TBFOMeIzDnxdsI8KUkE
4 ZQJfbPoP8F+1D4f+hjoMHBE1JB5eNMTxqeYDIph6ExyxMSboYE
5 P/Z3JHQv3HojcgvgoYoRlAUUHjo8Ds1vGtw9SL0jqpBTKXg9VS
6 f7wz2Xgu207iw9V/Mb18kwUUHjo8Ds1vGtw9SL0jqpBT0HAzUy
7 hd/PUJxs3utDNDstnD/cSpaNYA5p1FndvdiVlkUE2zXvWE8hQW
8 SuA1Gnowac7Zuh4tFdo2z9io4uyDTuuwfWLTSbjQYApSX6eSw/v
9 kdw8kixMICacE15ZAcIK9CMpJf53FH0iOF+5Xw0pBz3pj0QQS1
10 t4aASmhQIYPMsZvKaH0axQu5z6Ti7ocw45WkosIcPzy03P7ExJ
11 FUBFq81YqzjI1YTIH0g9mDFPwX812d99kd/s8Mzr8TRFJbKxQM
12 azdEu8ypvPstm9NYFEa94CJ6APihBX8KLH8pfQjh9Fk0SgT8Yx
13 Bzt6quUZincEod3b6Bd9P3f2DwhLiRj17HYhuJy/thLkqqsm3L
14 909tCDR8F7uEeTdCvqT/NdSp7uGaD6LXR60LY3hHXsaV8Kw/w
15 v1wSRfCC8wR0M5ntwmuSbj1chw5KU7TZxV9CqbkSyhxxSyQVnS
16 p8FmvsjpaHWsg8kvEWcmiNgtIfvaxIoh0xiKTx4jNiNDat/q31
17 uDQKTdELJ0g9KvyJaWgFqNxtd4c5W3LJvzuAd8AuF8SKzIjR2
18 /wxVSkIfvSLBitHsZBdZE1I2VO0gj3PgN5F2d41Uvj3bjamzo8
19 KnH0rQ4uHzfLiIXtW8TE6hMvgSF8EX7Bd6McCPwRzTTCVwgvMC
20 VbGjaY82TBrbE+UJiZsnXrWuA7/LpuLgmzrbi7KGoFYBxzcz636
21 6uRHRSBOI 0XT0kI al 0xF7X11ehlw7HwHPTwai16PY8OVHV7TV3f
```

length : 364.80 Ln : 1 Col : 1 Pos : 1 | Windows (CR LF) | UTF-8 | INS | .

Glossaire de termes techniques

- AAA (Authentication, Authorization, and Accounting) - ensemble de protocoles de sécurité gérant l'authentification, l'autorisation et la comptabilité des utilisateurs dans les réseaux informatiques.
- ACL (Access Control List) - liste de règles qui contrôle l'accès aux ressources réseau en spécifiant les autorisations ou restrictions basées sur des critères tels que les adresses IP, les ports et les protocoles.
- Commutateur (Switch) - dispositif réseau qui relie et dirige le trafic entre les appareils au sein d'un réseau local (LAN) en utilisant les adresses MAC.
- DHCP (Dynamic Host Configuration Protocol) automatise l'attribution des configurations réseau, comme les adresses IP, en fournissant dynamiquement ces paramètres aux dispositifs sur un réseau.
- DNS (Domain Name System) - traduit les noms de domaine en adresses IP pour simplifier l'accès aux ressources en ligne.
- EIGRP (Enhanced Interior Gateway Routing Protocol) - protocole de routage avancé de Cisco, offrant une configuration simple, une convergence rapide et une métrique basée sur plusieurs facteurs pour déterminer les meilleures routes.
- EtherChannel agrège plusieurs liens physiques entre deux commutateurs en un seul canal logique pour améliorer la bande passante et fournir une redondance en cas de défaillance.
- FTP (File Transfer Protocol) - protocole de transfert de fichiers entre un client et un serveur, avec des fonctionnalités avancées et l'authentification par nom d'utilisateur et mot de passe.
- HDLC (High-Level Data Link Control) est un protocole de liaison de données utilisé pour la communication série, définissant le format des trames, le contrôle de flux et la détection d'erreurs.
- NAT (Network Address Translation) - traduit les adresses IP entre les réseaux, permettant à plusieurs dispositifs d'utiliser une seule adresse IP publique pour accéder à Internet.
- OSPF (Open Shortest Path First) - protocole de routage, basé sur l'algorithme SPF, adapté aux réseaux de grande envergure. Il offre une convergence rapide, une hiérarchie par zones et utilise une métrique basée sur la largeur de bande.

- Packet Tracer - logiciel de simulation réseau de Cisco, utilisé pour concevoir, configurer et dépanner des réseaux virtuels. Il est largement employé dans l'éducation pour l'apprentissage des technologies réseau.
- PPP (Point-to-Point Protocol) établit des connexions point à point, couramment utilisé pour les connexions à distance via divers supports de communication, offrant une encapsulation standardisée des protocoles réseau.
- Routeur - dispositif réseau qui connecte et achemine les données entre différents réseaux, opérant au niveau de la couche réseau du modèle OSI.
- Serveur - dispositif informatique ou logiciel fournissant des services ou des ressources à d'autres appareils dans un réseau.
- STP (Spanning Tree Protocol) évite les boucles dans les réseaux Ethernet en bloquant sélectivement des liens redondants pour assurer une topologie sans boucle.
- Switch - dispositif réseau qui relie et dirige le trafic entre les appareils au sein d'un réseau local (LAN) en utilisant les adresses MAC.
- TFTP (Trivial File Transfer Protocol) - protocole de transfert de fichiers simple et rapide, sans authentification.
- VPN IPSec - connexion sécurisée sur Internet en établissant un tunnel crypté pour assurer la confidentialité, l'intégrité et l'authentification des données.
- VLSM (Variable Length Subnet Mask) - technique de sous-réseautage qui permet de créer des sous-réseaux avec des masques de longueur variable.
- VTP (VLAN Trunking Protocol) automatise la gestion des VLAN en propageant dynamiquement les informations de configuration VLAN d'un serveur VTP vers les commutateurs clients du réseau.
- WLC (Wireless LAN Controller) est un contrôleur centralisé qui gère les points d'accès sans fil dans un réseau, fournissant une gestion unifiée des fonctionnalités sans fil.
- ZPF (Zone-Based Policy Firewall) est une fonctionnalité de sécurité Cisco qui organise le réseau en zones logiques pour appliquer des politiques de filtrage du trafic spécifiques à chaque zone.

Conclusion

Grâce à ce projet, j'ai pu mettre en pratique toutes les connaissances acquises au cours de mes études au collège. Cela m'a donné l'occasion d'ancre des concepts dans ma mémoire à travers des mises en pratique, des recherches et des résolutions de problèmes complexes.

Le projet a été un défi pour optimiser le réseau, appliquer les protocoles appropriés et bien sûr, concevoir de manière optimale l'infrastructure du réseau.

J'ai principalement appliqué des protocoles standard compatibles avec différents fabricants d'équipements réseau pour assurer la scalabilité et la facilité de modification de la topologie du réseau, comme le protocole OSPF, qui permet le routage dynamique entre les équipements CISCO et d'autres.

La sécurité a été un aspect crucial, car toute organisation doit protéger ses données personnelles et commerciales à des fins éthiques, morales et légales. Ainsi, un pare-feu, diverses listes de contrôle d'accès (ACL), le NAT, le VPN IPSec, etc., ont été configurés.

En conclusion, l'organisation dispose maintenant d'un réseau optimisé et sécurisé.

27 novembre 2023