

LGi2A

LNR 29 - Brest - France

Mise en place d'une DMZ

Le groupe LGi2A (Laboratoires Gouvernementaux pour l'industrie Agro-Alimentaire) est issu du regroupement de plusieurs laboratoires en Europe. En France, ce réseau de laboratoires dépend directement du ministère de l'agriculture et de la pêche.

Formation : BTS SIO (Service Informatique aux Organisation)
option A : SISR (Solutions d'Infrastructure, Systèmes et Réseaux)

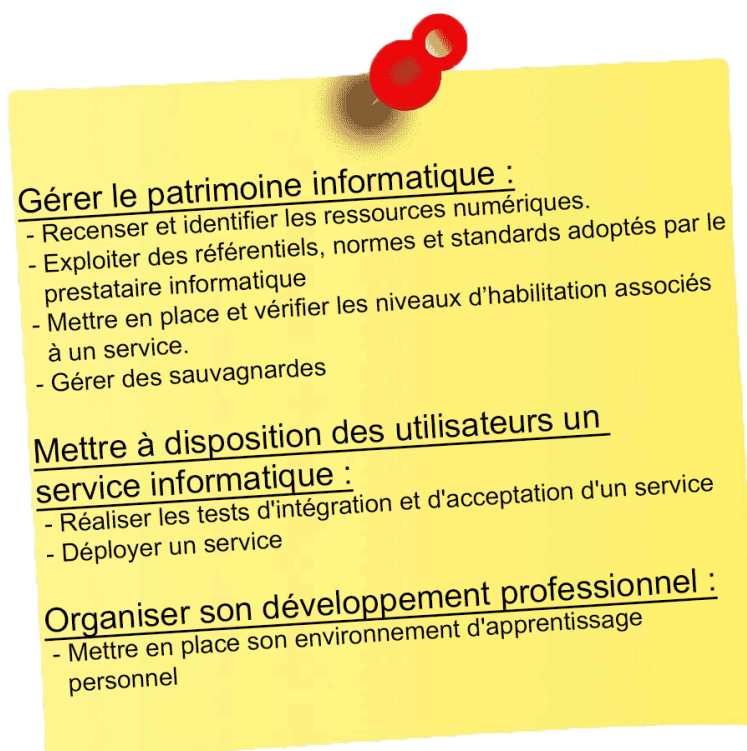
Session 2024



Fiche d'activité

Contexte	LG12A
Situation professionnelle	Mise en œuvre du routage Inter-vlans à l'aide d'un commutateur de niveau 3
Activité	Installer, tester et déployer un élément d'infrastructure
Pré-requis	Plan d'adressage IP, norme 802.1Q, Agrégation ou Trunk, protocoles de routage.
Ressources fournies	Solution d'infrastructure Cahier des charges techniques Plan d'adressage et de nommage Éléments d'infrastructure à configurer (Commutateur Catalyst 3560/3750)
Résultats attendus	Le dossier de choix et l'argumentaire technique sont rédigés et prennent en compte des préoccupations éthiques et environnementales. Les éléments d'infrastructure (switch de niveau 2 et niveau 3) sont installés et configurés Les éléments d'infrastructure permettant d'assurer la continuité de service (serveur TFTP) sont installés et configurés

Validation de compétences



Sommaire

Fiche d'activité.....	2
Validation de compétences.....	2
Sommaire.....	3
Fiche d'activité.....	4
Mise en situation.....	5
Expression des besoins.....	6
IDENTIFICATION DES RISQUES ASSOCIES A UNE INTERCONNEXION AVEC INTERNET.....	7
Étape 1 : Recommandations ANSSI concernant l'interconnexion d'un système d'information à.....	7
Étape 2 : Définition d'Internet.....	7
Étape 3 : Vulnérabilité d'un réseau informatique connecté à Internet.....	7
Étape 4 : Identification des risques.....	8
Étape 5 : Définition d'une zone démilitarisée (DMZ).....	9
MISE EN ŒUVRE DE LA DMZ SUR LE ROUTEUR FILTRANT.....	9
Etap 1 : Affichage de la configuration sur le routeur filtrant R1.....	9
Etap 2 : Création du nouveau vlan 3 nommé DMZ.....	11
Etap 3 : Affectation d'une adresse IP et d'un masque.....	11
Etap 4 : Affectation des interfaces disponibles au vlan « DMZ ».....	12
Etap 5 : Affichage et vérification des modifications apportées.....	12
Etap 6 : Enregistrement de la configuration courante dans la mémoire NVRAM.....	13
DETERMINATION DES TESTS NECESSAIRES A LA VALIDATION DE LA LIAISON LAN-DMZ.....	13
Etap 1 : Interconnexion d'un équipement sur la DMZ.....	13
Etap 2 : Configuration des propriétés TCP/IP l'équipement.....	13
Etap 3 : Tests de connectivité entre l'équipement et le routeur filtrant.....	14
Etap 4 : Affichage de la table de routage sur le routeur filtrant et interprétation.....	15
Étape 5 : Tests de connectivité entre la DMZ et les vlans du LNR.....	16
DETERMINATION DES TESTS NECESSAIRES A LA VALIDATION DE LA LIAISON DMZ-WAN.....	17
Etap 1 : Tests de connectivité entre la DMZ et les LNR partenaires.....	17
Etap 2 : Modification(s) à apporter si nécessaire.....	17
Etap 3 : Renouveler les tests de connectivité.....	18
Etap 4 : Tests de connectivité entre la DMZ et Internet.....	19
Etap 5 : Conclusion sur l'accès Internet.....	19
MISE EN PLACE D'UNE GESTION DE CONFIGURATIONS VIA UN SERVEUR TFTP.....	20
Etap 1 : Démarrage et configuration du serveur TFTP.....	20
Etap 2 : Vérification de la connectivité au serveur TFTP.....	20
Etap 3 : Copie du fichier de configuration initiale sur le serveur TFTP.....	21
Etap 4 : Vérification du transfert vers le serveur TFTP.....	21
Etap 5 : Sauvegarde des configurations de chaque équipement.....	22
Etap 6 : Procédure de restauration des différentes configurations.....	22

Fiche d'activité

Contexte	LGi2A
Situation Professionnelle	Mise en œuvre d'une DMZ sur un équipement de sécurité (routeur filtrant) répondant aux besoins en matière de sécurité informatique du groupe LGi2A
Compétences	Bloc 2 <ul style="list-style-type: none"> • Etudier l'impact d'une évolution d'un élément d'infrastructure et rédiger les spécifications techniques • Déterminer et préparer les tests nécessaires à la validation de la solution d'infrastructure retenue • Installer et configurer des éléments d'infrastructure • Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure • Tester l'intégration et l'acceptation d'une solution d'infrastructure • Administrer sur site et à distance des éléments d'une infrastructure
Savoirs organisationnels	<p>Maintenir la documentation technique du réseau (schéma physique et logique)</p> <p>Rédaction d'une note de service</p> <p>Adopter une démarche structurée de diagnostic selon les couches réseau.</p>
Savoirs	<p>Connaissance du modèle OSI et de l'architecture TCP/IP</p> <p>Connaissance du rôle et des fonctions des équipements de sécurité (pare-feu et proxy)</p> <p>Connaissance de la technologie des équipements d'interconnexion</p> <p>Connaissance des topologies physique et logique des réseaux</p>
Pré-requis	Bonnes pratiques, plan d'adressage IP, routage statique et routage dynamique (RIPv2, OSPF), table de routage, NAT Overload, ACL, analyse de trames.
Ressources Fournie	<p>Solution d'infrastructure</p> <p>Cahier des charges technique</p> <p>Plan d'adressage et de nommage</p> <p>Éléments d'infrastructure à configurer (Routeur Cisco série 881)</p> <p>Logiciel de simulation (Packet Tracer)</p>
Résultats attendus	<p>Élément d'infrastructure installé et configuré</p> <p>Maquette de la solution</p> <p>Rédaction de notes destinées au DSI précisant les modifications à effectuer</p> <p>Compte-rendu, fichiers de configuration et de simulation,</p> <p>Mise à jour des schémas</p>

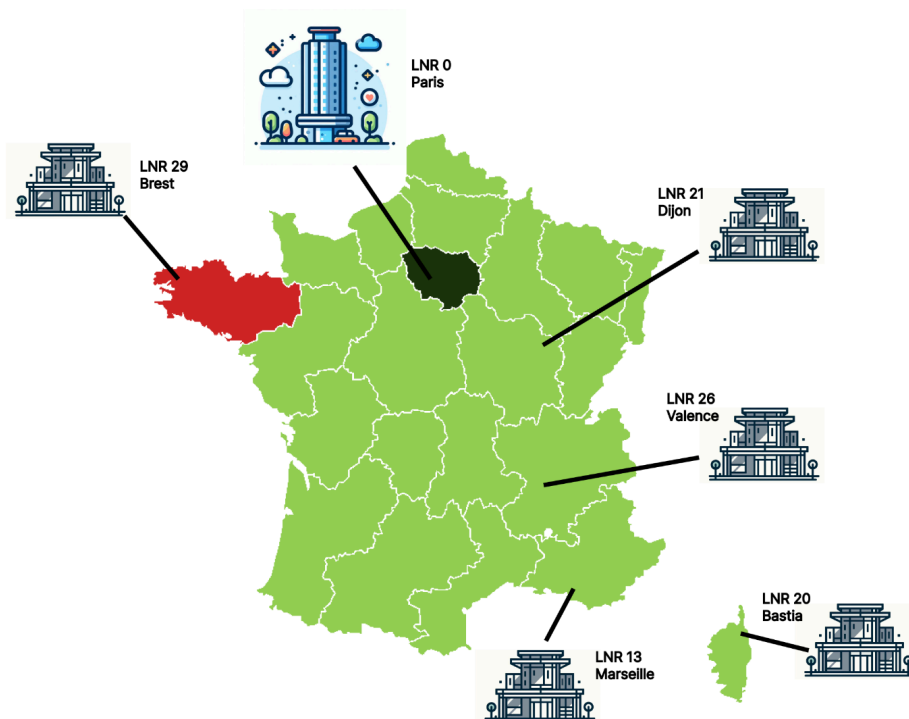
Mise en situation

Nous allons opérer dans le LNR 29 à Brest :

La France figure parmi les premiers pays producteurs et exportateurs de produits agricoles et agroalimentaires. Le maintien et l'amélioration de la compétitivité des filières françaises par rapport aux concurrents de l'Union européenne et des pays tiers sont des défis majeurs. Pour les relever, une vision et une stratégie à l'horizon 2025, partagées par l'ensemble des acteurs des différentes filières sont une nécessité.

Initialement basé en Île-de-France, LGi2A regroupe de plus en plus de laboratoires sur le territoire afin de proposer une large étendue de prestations à nos collaborateurs jusque dans les départements et territoires d'Outre-mer. Du fait de sa clientèle, issue de l'industrie agroalimentaire et de la distribution, LGi2A est en mesure de prendre en charge tous types de produits de consommation et d'y associer une palette de services.

Faisant partie du département informatique de LGi2A, un des réseaux de ces laboratoires m'a été confié. J'administre le réseau du laboratoire de Brest correspondant au LNR 29. Ma mission est de configurer ce LNR pour qu'il puisse communiquer avec le reste du réseau que d'autres techniciens gèrent



Bâtiment situé à Brest :



Expression des besoins

Au terme de la mission précédente, chaque LNR (Laboratoire National de référence) du groupe LGi2A a désormais accès à Internet.

Les LNR ont ainsi identifié le digital (ou numérique) comme un levier clé. En effet, Internet offre des possibilités à la fois riches et nouvelles pour la recherche dans le domaine de l'Agro-alimentaire et surtout répondre à leurs principaux défis : créer de la valeur pour leurs chercheurs, satisfaire la demande alimentaire croissante, accompagner les évolutions de leurs consommateurs (vente en ligne, e-commerce) et ainsi renforcer la compétitivité, ...

Mais si Internet va transformer et nettement améliorer la recherche et les transactions commerciales, ce vaste réseau et les technologies qui lui correspondent vont ouvrir la porte à un nombre croissant de menaces relatives à la sécurité contre lesquelles les entreprises comme le groupe LGi2A doivent se prémunir.

Il faut donc sécuriser notre réseau.

IDENTIFICATION DES RISQUES ASSOCIES A UNE INTERCONNEXION AVEC INTERNET

On rappelle que chaque LNR du groupe LGi2A, héberge des services, donc des serveurs Internet comme le serveur web, le serveur de messagerie, le serveur de partage de données (CLOUD)...

Chaque LNR a donc une "porte" ouverte vers internet et autorise donc les internautes à entrer sur ses serveurs Internet. Il y a donc des risques de divers types suite à cette ouverture sur l'extérieur.

Étape 1 : Recommandations ANSSI concernant l'interconnexion d'un système d'information à

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a élaboré des recommandations pour sécuriser l'interconnexion d'un système d'information (SI) avec Internet.

Ces recommandations visent à définir une architecture de passerelle d'interconnexion qui puisse faire face aux menaces courantes. Principalement destiné aux architectes et administrateurs réseau, le guide de l'ANSSI propose des principes pour la création d'une zone démilitarisée (DMZ) et la séparation des réseaux internes et externes.

Il insiste également sur l'importance d'une passerelle d'interconnexion sécurisée pour protéger le système d'information des attaques provenant d'Internet.

Pour plus de détails, vous pouvez consulter le guide complet sur les recommandations relatives à l'interconnexion d'un système d'information à Internet sur le site de l'ANSSI.

Étape 2 : Définition d'Internet

Les réseaux Internet sont des réseaux mondiaux interconnectés permettant à des millions d'ordinateurs de communiquer entre eux. Le protocole de communication utilisé est le TCP/IP (Transmission Control Protocol/Internet Protocol). Il trois types de services fondamentaux d'Internet sont le World Wide Web (WWW) pour l'accès aux sites web, le courrier électronique (e-mail) pour la communication, et le transfert de fichiers (FTP) pour le partage de données.

Étape 3 : Vulnérabilité d'un réseau informatique connecté à Internet

Les menaces sur la confidentialité et l'intégrité des données d'une entreprise comprennent l'interception de données sensibles, le vol d'identifiants, et l'accès non autorisé aux données. Les ennemis potentiels incluent les pirates informatiques, les concurrents malveillants, les employés mécontents, et les espions industriels.

Étape 4 : Identification des risques

Les intrusions les plus courantes venant d'Internet comprennent les attaques par force brute, les attaques par déni de service (DDoS), le phishing, les injections SQL, et l'exploitation de vulnérabilités logicielles. Chaque vecteur de menace exploite des failles spécifiques dans les systèmes et les applications pour accéder de manière non autorisée aux données ou perturber les services.


```

!
interface FastEthernet0
description cote_LAN
switchport access vlan 2
no ip address
!
interface FastEthernet1
no ip address
!
interface FastEthernet2
no ip address
!
interface FastEthernet3
no ip address
!
interface FastEthernet4
description cote_WAN
ip address 192.168.217.129 255.255.255.0
ip nat outside
ip virtual-reassembly in
duplex auto
speed auto
!

```

Afficher la table de routage.

```

Router1_Brest>en
Password:
Router1_Brest#show vlan
% Ambiguous command: "show vlan"
Router1_Brest#show route
% Ambiguous command: "show route"
Router1_Brest#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override

Gateway of last resort is 192.168.217.254 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 192.168.217.254, FastEthernet4
     10.0.0.0/8 is variably subnetted, 15 subnets, 4 masks
R     10.0.0.0/8 [120/1] via 192.168.217.126, 00:00:20, FastEthernet4
          [120/1] via 192.168.217.121, 00:00:07, FastEthernet4
          [120/1] via 192.168.217.113, 00:00:20, FastEthernet4
C     10.31.162.252/30 is directly connected, Vlan2
L     10.31.162.253/32 is directly connected, Vlan2
R     10.31.170.0/24 [120/1] via 10.31.162.254, 00:00:24, Vlan2
R     10.31.171.0/24 [120/1] via 10.31.162.254, 00:00:24, Vlan2
R     10.31.172.0/24 [120/1] via 10.31.162.254, 00:00:24, Vlan2
R     10.31.173.0/24 [120/1] via 10.31.162.254, 00:00:24, Vlan2
R     10.31.180.0/24 [120/1] via 10.31.162.254, 00:00:24, Vlan2
R     10.31.181.0/24 [120/1] via 10.31.162.254, 00:00:24, Vlan2
R     10.31.182.0/24 [120/1] via 10.31.162.254, 00:00:24, Vlan2
R     10.31.183.0/24 [120/1] via 10.31.162.254, 00:00:24, Vlan2
R     10.31.184.0/24 [120/1] via 10.31.162.254, 00:00:24, Vlan2
R     10.31.185.0/24 [120/1] via 10.31.162.254, 00:00:24, Vlan2
R     10.31.186.0/24 [120/1] via 10.31.162.254, 00:00:24, Vlan2
R     10.31.187.0/24 [120/1] via 10.31.162.254, 00:00:24, Vlan2
     192.168.217.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.217.0/24 is directly connected, FastEthernet4
L     192.168.217.129/32 is directly connected, FastEthernet4
Router1_Brest#

```

Etape 2 : Création du nouveau vlan 3 nommé DMZ

On configure le nouveau vlan pour la DMZ en mode « **config** » on marque « **vlan 3** » puis on lui attribue un nom « **name DMZ** ».

```
Router1_Brest#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router1_Brest(config)#vlan 3
Router1_Brest(config-vlan)#name DMZ
Router1_Brest(config-vlan)#
```

Etape 3 : Affectation d'une adresse IP et d'un masque.

On définit une adresse IP sur l'interface vlan.

Peripherique	Reference	Interface		Adresse ip	Masque
R1_Brest	Cisco 881	LAN	FA 0	10.31.162.253	255.255.255.0
		DMZ	FA 1	172.30.29.254	255.255.255.0
			FA 2		
			FA 3		
		WAN	FA 4	192.168.217.129	255.255.255.0

Interface vlan 3
ip address « IP du vlan » « masque de sous réseau »

```
Router1_Brest(config-if)#ip address 172.30.29.254 255.255.255.0
Router1_Brest(config-if)#
```

On ajoute une « **description DMZ** »

```
Router1_Brest(config)#interface v
Router1_Brest(config)#interface vl
Router1_Brest(config)#interface vlan 3
Router1_Brest(config-if)#des
Router1_Brest(config-if)#description DMZ
Router1_Brest(config-if)#
```

Etape 4 : Affectation des interfaces disponibles au vlan « DMZ »

On affecte les 3 interfaces non utilisées au vlan « **DMZ** »

```
Router1_Brest(config)# interface range fastEthernet 1-3
Router1_Brest(config-if-range)# switchport access vlan 3
```

Etape 5 : Affichage et vérification des modifications apportées

Voici la configuration que l'on obtient

```
!
interface FastEthernet0
  description cote_LAN
  switchport access vlan 2
  no ip address
!
interface FastEthernet1
  switchport access vlan 3
  no ip address
!
interface FastEthernet2
  switchport access vlan 3
  no ip address
!
interface FastEthernet3
  switchport access vlan 3
  no ip address
!
interface FastEthernet4
  description cote_WAN
  ip address 192.168.217.129 255.255.255.0
  ip nat outside
  ip virtual-reassembly in
  duplex auto
  speed auto
!
interface Vlan1
  no ip address
!
interface Vlan2
  ip address 10.31.162.253 255.255.255.252
  ip nat inside
  ip virtual-reassembly in
!
interface Vlan3
  description DMZ
  ip address 172.16.29.254 255.255.255.0
!
```

Etape 6 : Enregistrement de la configuration courante dans la mémoire NVRAM.

On enregistre la configuration.

```
Router1_Brest(config-if-range)#e
Router1_Brest#write
Building configuration...
[OK]
```

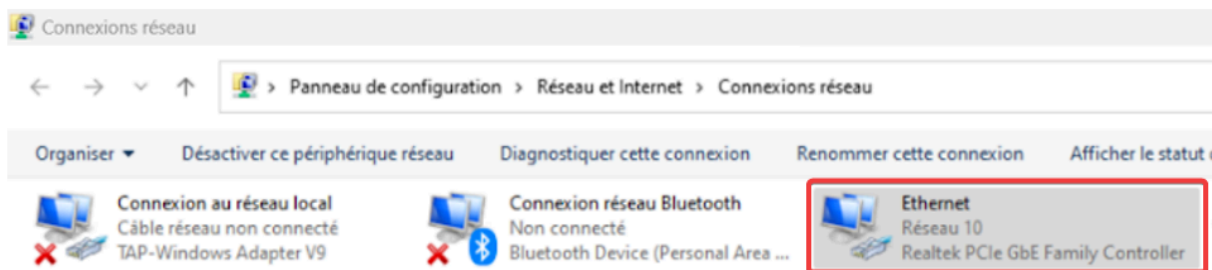
DETERMINATION DES TESTS NECESSAIRES A LA VALIDATION DE LA LIAISON LAN-DMZ

Etape 1 : Interconnexion d'un équipement sur la DMZ

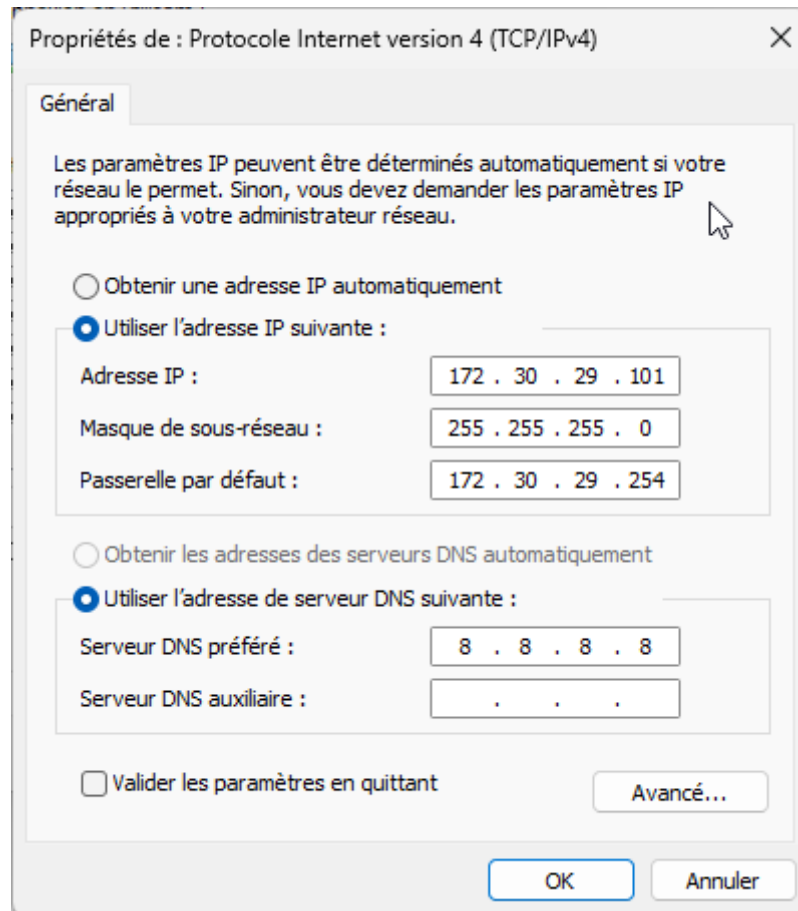
On interconnecte le serveur d'infrastructure ESXI3-VILLE-LNR au routeur filtrant (A défaut, on pourra utiliser un poste client).

Etape 2 : Configuration des propriétés TCP/IP l'équipement

On paramètre les propriétés TCP/IP du client



On y ajoute une IP en « **172.30.29.- /24** » la passerelle « **172.30.29.254 (ip du vlan)** »



Etape 3 : Tests de connectivité entre l'équipement et le routeur filtrant.

On effectue un test de connectivité entre l'équipement et le routeur filtrant.

```
C:\Users\cleme>ping 10.31.162.253

Envoi d'une requête 'Ping' 10.31.162.253 avec 32 octets de données :
Réponse de 10.31.162.253 : octets=32 temps=1 ms TTL=255
Réponse de 10.31.162.253 : octets=32 temps=1 ms TTL=255
Réponse de 10.31.162.253 : octets=32 temps=2 ms TTL=255
Réponse de 10.31.162.253 : octets=32 temps=1 ms TTL=255
```

```
C:\Users\cleme>ping 192.168.217.129

Envoi d'une requête 'Ping' 192.168.217.129 avec 32 octets de données :
Réponse de 192.168.217.129 : octets=32 temps=2 ms TTL=255
Réponse de 192.168.217.129 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.217.129 : octets=32 temps=2 ms TTL=255
Réponse de 192.168.217.129 : octets=32 temps=15 ms TTL=255
```


Etape 4 : Affichage de la table de routage sur le routeur filtrant et interprétation

On affiche la table de routage.

```
Gateway of last resort is 192.168.217.254 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 192.168.217.254, FastEthernet4
    10.0.0.0/8 is variably subnetted, 15 subnets, 4 masks
R   10.0.0.0/8 [120/1] via 192.168.217.126, 00:00:23, FastEthernet4
    [120/1] via 192.168.217.121, 00:00:04, FastEthernet4
    [120/1] via 192.168.217.113, 00:00:24, FastEthernet4
C   10.31.162.252/30 is directly connected, Vlan2
L   10.31.162.253/32 is directly connected, Vlan2
R   10.31.170.0/24 [120/1] via 10.31.162.254, 00:00:14, Vlan2
R   10.31.171.0/24 [120/1] via 10.31.162.254, 00:00:14, Vlan2
R   10.31.172.0/24 [120/1] via 10.31.162.254, 00:00:14, Vlan2
R   10.31.173.0/24 [120/1] via 10.31.162.254, 00:00:14, Vlan2
R   10.31.180.0/24 [120/1] via 10.31.162.254, 00:00:14, Vlan2
R   10.31.181.0/24 [120/1] via 10.31.162.254, 00:00:14, Vlan2
R   10.31.182.0/24 [120/1] via 10.31.162.254, 00:00:14, Vlan2
R   10.31.183.0/24 [120/1] via 10.31.162.254, 00:00:14, Vlan2
R   10.31.184.0/24 [120/1] via 10.31.162.254, 00:00:14, Vlan2
R   10.31.185.0/24 [120/1] via 10.31.162.254, 00:00:14, Vlan2
R   10.31.186.0/24 [120/1] via 10.31.162.254, 00:00:14, Vlan2
R   10.31.187.0/24 [120/1] via 10.31.162.254, 00:00:14, Vlan2
C   172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
L   172.30.29.0/24 is directly connected, Vlan3
    172.30.29.254/32 is directly connected, Vlan3
R   192.168.217.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.217.0/24 is directly connected, FastEthernet4
L   192.168.217.129/32 is directly connected, FastEthernet4
```

On peut y voir que la route a bien été créée.

Le routeur filtrant est capable de transmettre un paquet reçu à un des Vlans de notre LNR.

```
Router1_Brest>ping 10.31.170.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.31.170.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Router1_Brest>ping 10.31.186.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.31.186.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Router1_Brest>ping 10.31.171.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.31.171.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Router1_Brest>
```

Étape 5 : Tests de connectivité entre la DMZ et les vlans du LNR.

On effectue un test de connectivité entre l'équipement et un poste situé dans un des VLAN

```
C:\Users\cleme>ping 10.31.170.254

Envoi d'une requête 'Ping' 10.31.170.254 avec 32 octets de données :
Réponse de 10.31.170.254 : octets=32 temps=1 ms TTL=254
Réponse de 10.31.170.254 : octets=32 temps=1 ms TTL=254
Réponse de 10.31.170.254 : octets=32 temps<1ms TTL=254
Réponse de 10.31.170.254 : octets=32 temps<1ms TTL=254

Statistiques Ping pour 10.31.170.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\cleme>|
```


DETERMINATION DES TESTS NECESSAIRES A LA VALIDATION DE LA LIAISON DMZ-WAN

Etape 1 : Tests de connectivité entre la DMZ et les LNR partenaires.

Le test vers Valence a échoué, effectivement aucune ACL et route static a été créé pour pouvoir faire la liaison, nous devons créer des routes statiques car le routeur essaie d'aller vers tous les réseaux LGI2A 113, 126... sans jamais trouver. tout cela est dû au limite du protocole RIP il faut le diriger via les route static

```
C:\Users\cleme>ping 10.31.74.1

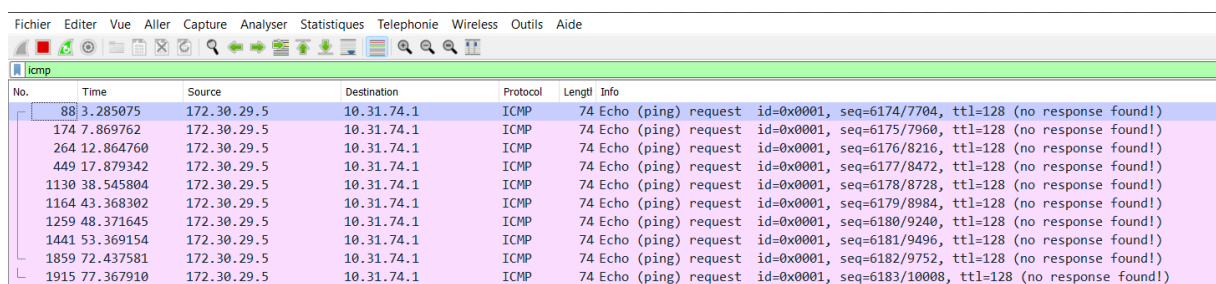
Envoi d'une requête 'Ping' 10.31.74.1 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 10.31.74.1:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),

C:\Users\cleme>
```

Etape 2 : Modification(s) à apporter si nécessaire

On peut voir via Wireshark que le ping echoue.



No.	Time	Source	Destination	Protocol	Length	Info
88	3.285075	172.30.29.5	10.31.74.1	ICMP	74	Echo (ping) request id=0x0001, seq=6174/7704, ttl=128 (no response found!)
174	7.869762	172.30.29.5	10.31.74.1	ICMP	74	Echo (ping) request id=0x0001, seq=6175/7960, ttl=128 (no response found!)
264	12.864760	172.30.29.5	10.31.74.1	ICMP	74	Echo (ping) request id=0x0001, seq=6176/8216, ttl=128 (no response found!)
449	17.879342	172.30.29.5	10.31.74.1	ICMP	74	Echo (ping) request id=0x0001, seq=6177/8472, ttl=128 (no response found!)
1130	38.545804	172.30.29.5	10.31.74.1	ICMP	74	Echo (ping) request id=0x0001, seq=6178/8728, ttl=128 (no response found!)
1164	43.368302	172.30.29.5	10.31.74.1	ICMP	74	Echo (ping) request id=0x0001, seq=6179/8984, ttl=128 (no response found!)
1259	48.371645	172.30.29.5	10.31.74.1	ICMP	74	Echo (ping) request id=0x0001, seq=6180/9240, ttl=128 (no response found!)
1441	53.369154	172.30.29.5	10.31.74.1	ICMP	74	Echo (ping) request id=0x0001, seq=6181/9496, ttl=128 (no response found!)
1859	72.437581	172.30.29.5	10.31.74.1	ICMP	74	Echo (ping) request id=0x0001, seq=6182/9752, ttl=128 (no response found!)
1915	77.367910	172.30.29.5	10.31.74.1	ICMP	74	Echo (ping) request id=0x0001, seq=6183/10008, ttl=128 (no response found!)

La modification a apporté sont les suivantes

Ajout de la ACL 10.31.64.0 0.0.31.255, on ajoute egalement une IP route 172.30.26.0 255.255.255.0 FA/04 192.168.217.126

Du coter de Valence ils doivent ajouter l'ACL 10.31.160.0 0.0.31.255 pour nous joindre,

```

interface Vlan3
description DMZ
ip address 172.30.29.254 255.255.255.0
ip nat inside
ip virtual-reassembly in
!
router rip
version 2
network 10.0.0.0
network 172.30.0.0
network 192.168.217.0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip nat pool ovrl 192.168.217.129 192.168.217.129 prefix-length 24
ip nat inside source list 20 pool ovrl overload
ip nat inside source list 21 pool ovrl overload
ip nat inside source list 22 pool ovrl overload
ip nat inside source list 23 pool ovrl overload
ip nat inside source list 24 pool ovrl overload
ip route 0.0.0.0 0.0.0.0 FastEthernet4 192.168.217.254
ip route 10.29.160.0 255.255.224.0 FastEthernet4 192.168.217.113
ip route 10.31.64.0 255.255.224.0 FastEthernet4 192.168.217.126
ip route 172.30.26.0 255.255.255.0 FastEthernet4 192.168.217.126
!
access-list 20 permit 10.31.160.0 0.0.31.255
access-list 21 permit 10.31.64.0 0.0.31.255
access-list 22 permit 172.30.29.0 0.0.0.255
access-list 23 permit 10.29.160.0 0.0.31.255
access-list 24 permit 172.30.26.0 0.0.0.255

```

Etape 3 : Renouveler les tests de connectivité.

Cette fois l'inter-sites fonctionne

```

C:\Users\cleme>ping 10.31.74.1

Envoi d'une requête 'Ping' 10.31.74.1 avec 32 octets de données :
Réponse de 192.168.217.126 : octets=32 temps=1 ms TTL=125
Réponse de 192.168.217.126 : octets=32 temps=1 ms TTL=125
Réponse de 192.168.217.126 : octets=32 temps=1 ms TTL=125
Réponse de 192.168.217.126 : octets=32 temps=1 ms TTL=125

Statistiques Ping pour 10.31.74.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms

C:\Users\cleme>

```

Etape 4 : Tests de connectivité entre la DMZ et Internet.

On effectue un test de connectivité entre l'équipement situé dans la DMZ et le serveur google.

```
C:\Users\cleme>ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=3 ms TTL=114
Réponse de 8.8.8.8 : octets=32 temps=2 ms TTL=114
Réponse de 8.8.8.8 : octets=32 temps=5 ms TTL=114
Réponse de 8.8.8.8 : octets=32 temps=2 ms TTL=114

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 5ms, Moyenne = 3ms

C:\Users\cleme>|
```

Etape 5 : Conclusion sur l'accès Internet

Conclure sur la mise en œuvre de la DMZ.

Pour conclure l'accès à internet et ok car l'ACL pour communiquer avec le site et relier avec un NAT POOL donc il permet la communication avec internet

```
C:\Users\cleme>ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=3 ms TTL=114
Réponse de 8.8.8.8 : octets=32 temps=3 ms TTL=114
Réponse de 8.8.8.8 : octets=32 temps=2 ms TTL=114
Réponse de 8.8.8.8 : octets=32 temps=2 ms TTL=114

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms

C:\Users\cleme>|
```

MISE EN PLACE D'UNE GESTION DE CONFIGURATIONS VIA UN SERVEUR TFTP

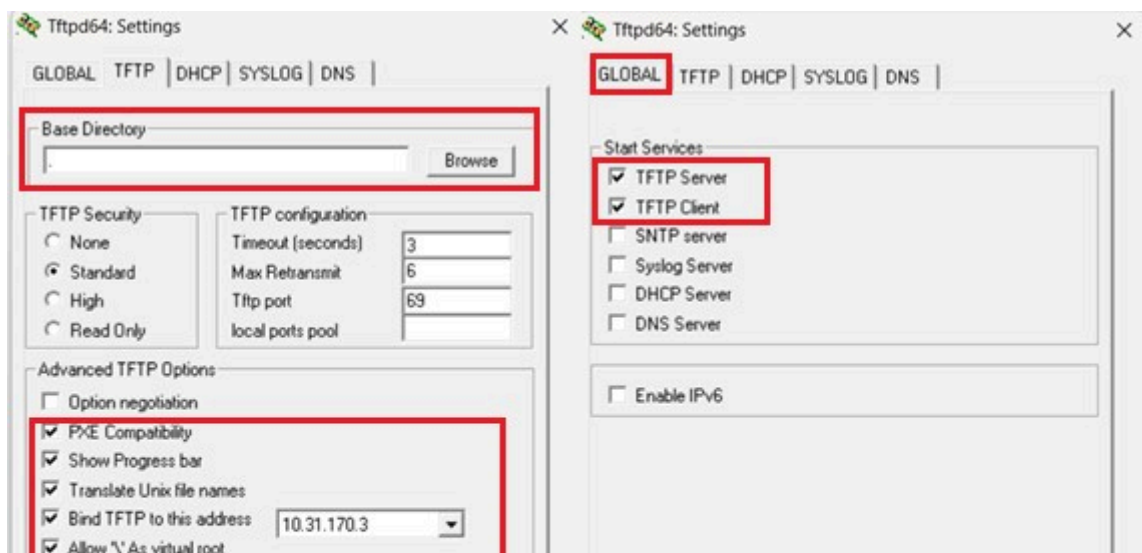
Etape 1 : Démarrage et configuration du serveur TFTP

Une fois tftpd64 : <https://pjo2.github.io/tftpd64/> installé sur votre machine

On démarre le logiciel Tftpd64 et on se rend dans les paramètres (settings).



On active uniquement les paramètres suivants



Etape 2 : Vérification de la connectivité au serveur TFTP

On vérifie que le serveur TFTP fonctionne correctement et que l'on peut envoyer une requête ping à partir du commutateur vers le serveur TFTP.

```
SW0_29>ping 10.31.170.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.31.170.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW0_29>ping 10.31.170.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.31.170.3, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

SW0_29>
```

Etape 3 : Copie du fichier de configuration initiale sur le serveur TFTP

On entre la commande "copy running-config startup-config" pour s'assurer que le fichier de configuration est bien enregistré, puis on sauvegarde le fichier sur le serveur TFTP en utilisant la commande appropriée.

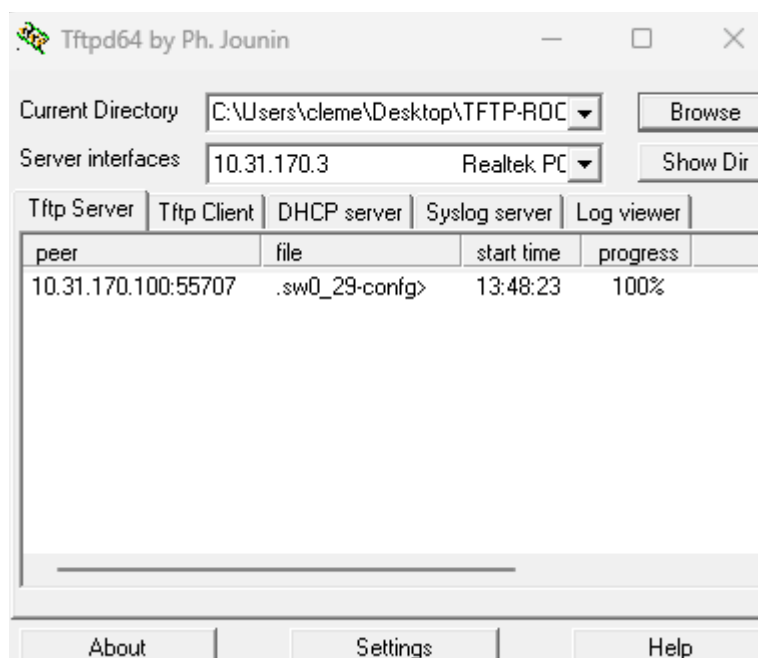
```
copy startup-config tftp
10.31.170.3
```

```
[OK]
SW0_29#copy startup-config tftp
Address or name of remote host []? 10.31.170.3
Destination filename [sw0_29-config]?
!!
4484 bytes copied in 0.051 secs (87922 bytes/sec)
SW0_29#
```

Etape 4 : Vérification du transfert vers le serveur TFTP

On vérifie que le transfert vers le serveur TFTP s'effectue correctement et que le fichier apparaît correctement dans le dossier de destination.

Le fichier se nomme sw0_29-config



Etape 5 : Sauvegarde des configurations de chaque équipement.

On assure la maintenance préventive de chacun des équipements mis en œuvre pour permettre une restauration rapide en cas de panne fatale (maintenance corrective).

Les configurations à sauvegarder sont : **vlan.dat** et **sw0_29-config**

On réitère l'opération sur tous les commutateurs afin d'avoir toutes les sauvegardes nécessaires.

```
[OK]
SW0_29#copy startup-config tftp
Address or name of remote host []? 10.31.170.3
Destination filename [sw0_29-config]?
!!
4484 bytes copied in 0.051 secs (87922 bytes/sec)
SW0_29#
```

Etape 6 : Procédure de restauration des différentes configurations

En cas de remplacement d'urgence du commutateur "cœur de réseau", voici une procédure pour restaurer nos configurations :

Pour commencer, on prépare le nouveau commutateur en le connectant au réseau de la même manière que le commutateur défectueux. On applique les paramètres de base, tels que l'adresse IP, correspondant à ceux du commutateur défectueux.

Ensuite, on procède à la restauration de nos configurations en utilisant notre serveur TFTP. On copie les sauvegardes des configurations et des VLANs du commutateur défectueux vers le nouveau commutateur :

```
copy tftp:config.text flash:config.text
Address or name of remote host []? « adresse IP »
Destination filename [config.dat]? [entrée]

copy tftp:vlan.dat flash:vlan.dat
Address or name of remote host []? « adresse IP »
Destination filename [vlan.dat]? [entrée]
```