BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

ANNEXE VII-1-A : Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation :**
Nom, prénom : SAUVAGET--TIGHERSTINE Aymeric	**N° candidat :**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date :** 16 / 04 / 2026

Organisation support de la réalisation professionnelle

Intitulé de la réalisation professionnelle
PPE – Access List Réseau (Cisco)

Période de réalisation : 2025-2026 **Lieu :** Promeo CFAI Picardie - Beauvais
Modalité : ☒ **Seul(e)** ☐ **En équipe**

Compétences travaillées
- ☐ Concevoir une solution d'infrastructure réseau
- ☐ Installer, tester et déployer une solution d'infrastructure réseau
- ☐ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[1] (ressources fournies, résultats attendus)
Topologie réseau réalisée sur Packet Tracer afin de prévoir la connectivité des appareils et le plan d'adressage
Routeurs et switchs Cisco physiques en salle informatique

Description des ressources documentaires, matérielles et logicielles utilisées[2]
Accès à internet pour l'explication du sujet et à l'IA pour résoudre les problèmes rencontrés en fonction des messages d'erreur.
Utilisation des cours, labs et présentations effectuées au cours de l'année.
Packet Tracer a été utilisé pour la topologie du réseau et la configuration des appareils

Modalités d'accès aux productions[3] et à leur documentation[4]
Les productions et leur documentation sont accessibles sur le site suivant :
https://asauvagettigherstine.promeo-capnumerique.fr

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.
[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.
[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.
[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

ANNEXE VII-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

Sauvaget--Tigherstine Aymeric

PPE – Access List Réseau (Cisco)

Section BTS SIO 26

Table des matières

Contexte

L'administrateur d'un centre de formation souhaite renforcer la sécurité du réseau en rajoutant des règles ayant pour objet de réguler le trafic.

Le but est de limiter l'activité des différents réseaux (étudiants, enseignants, local).

Les ACL représentent donc une solution à implémenter afin de sécuriser le réseau à partir de règles définies en fonction de ce que l'administrateur souhaite restreindre ou permettre.

Présentation des ACL

Les ACL sont des règles permettant de filtrer le trafic réseau selon certains critères, tels que l'IP source/destination ou le port. Ces règles servent à sécuriser le réseau en fonction de ce que l'on souhaite mettre en place et empêcher.

Fonctionnement général

Une ACL examine les paquets et décide de leur sort selon les règles configurées. Les équipements réseau (routeurs, pare-feu, switch) comparent chaque paquet aux entrées de l'ACL, dans l'ordre, jusqu'à trouver une correspondance.
Une ACL peut filtrer selon :

- Adresse IP source ou destination
- Plage d'adresses ou hôte unique
- Protocole (HTTP, ICMP, FTP…)
- Masques génériques (wildcard mask) pour définir des plages d'adresses
- Critères avancés (ToS, DSCP…)

Types d'ACL

1. ACL Standard : Filtrages simples basées sur **l'adresse IP source**

2. ACL Étendue

- Filtrent selon des critères définis :
    - IP source et destination
    - Protocole
    - Ports
    - Type de trafic
- Permettent un contrôle beaucoup plus précis.

Composants d'une ACL

- **Numéro de séquence** : ordre des règles
- **Nom ou numéro d'ACL**
- **Action** : *permit* ou *deny*
- **Protocole** : IP, TCP, UDP, ICMP…
- **Adresse source + masque générique**
- **Adresse destination + masque générique**
- **Ports** (pour les ACL étendues)

Placement des ACL

- Sur les **routeurs de périphérie** pour filtrer le trafic entrant/sortant
- Exemple : entre **Internet ↔ DMZ** ou **DMZ ↔ réseau interne**
- Chaque emplacement a une configuration adaptée au niveau de protection souhaité

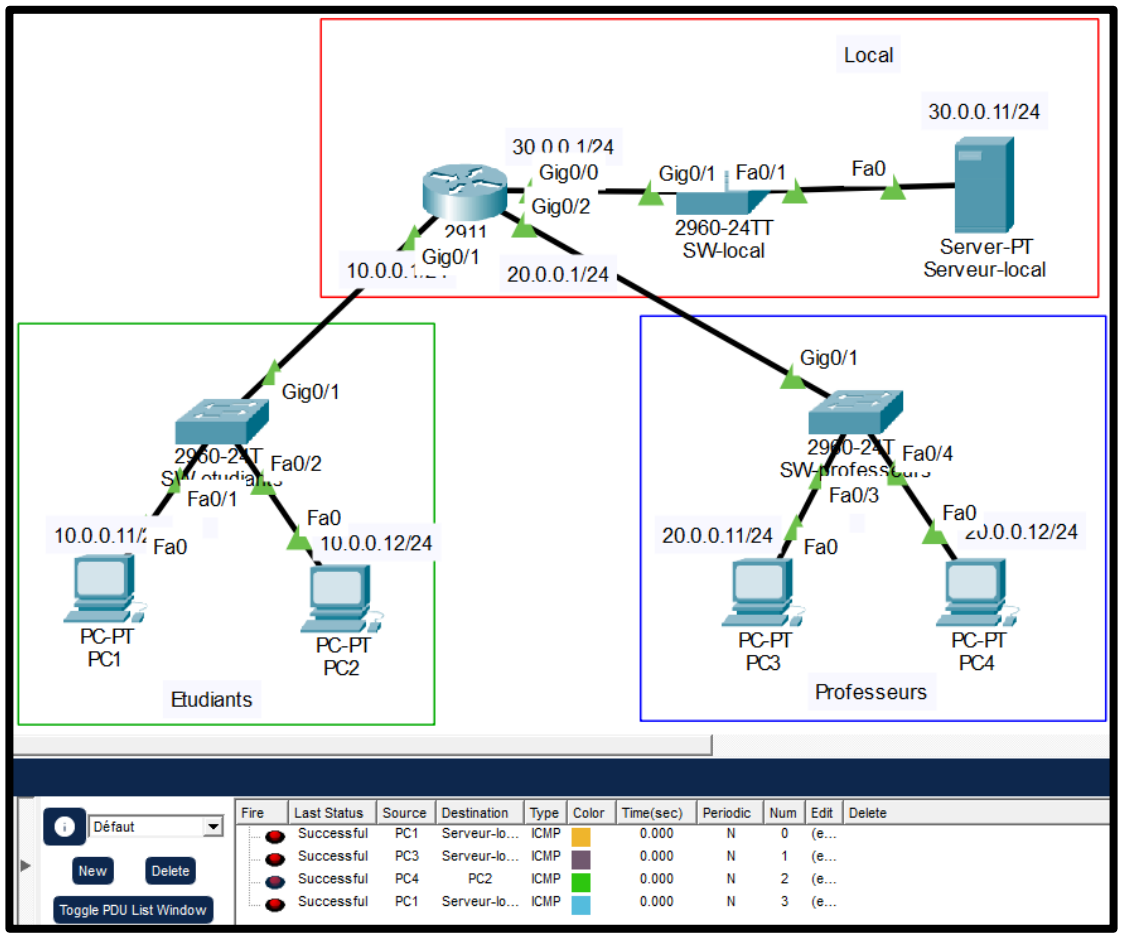
Par principe, une ACL standard se placera toujours au plus proche de la destination et une ACL étendue se placera toujours au plus proche de la source.

Avantages

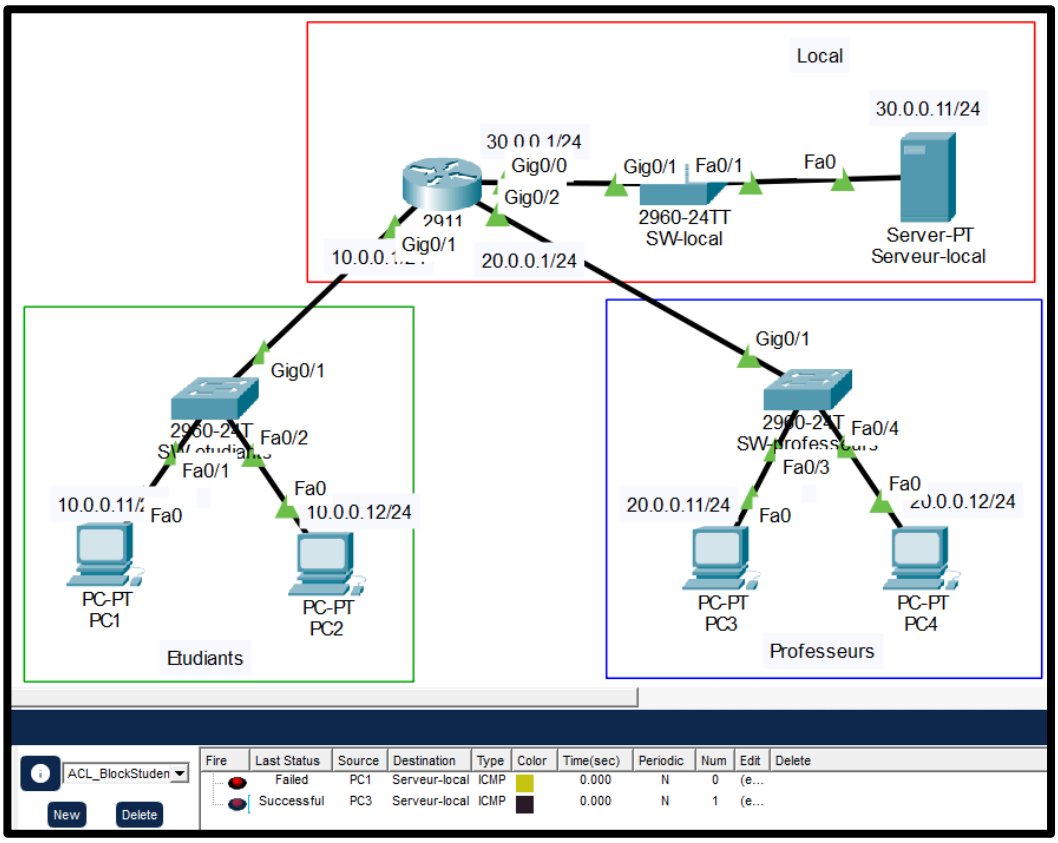
- Contrôle précis du trafic à la main des administrateurs
- Prévention des risques d'accès non autorisés
- Complément utile aux pare-feux et VPN

Annexes

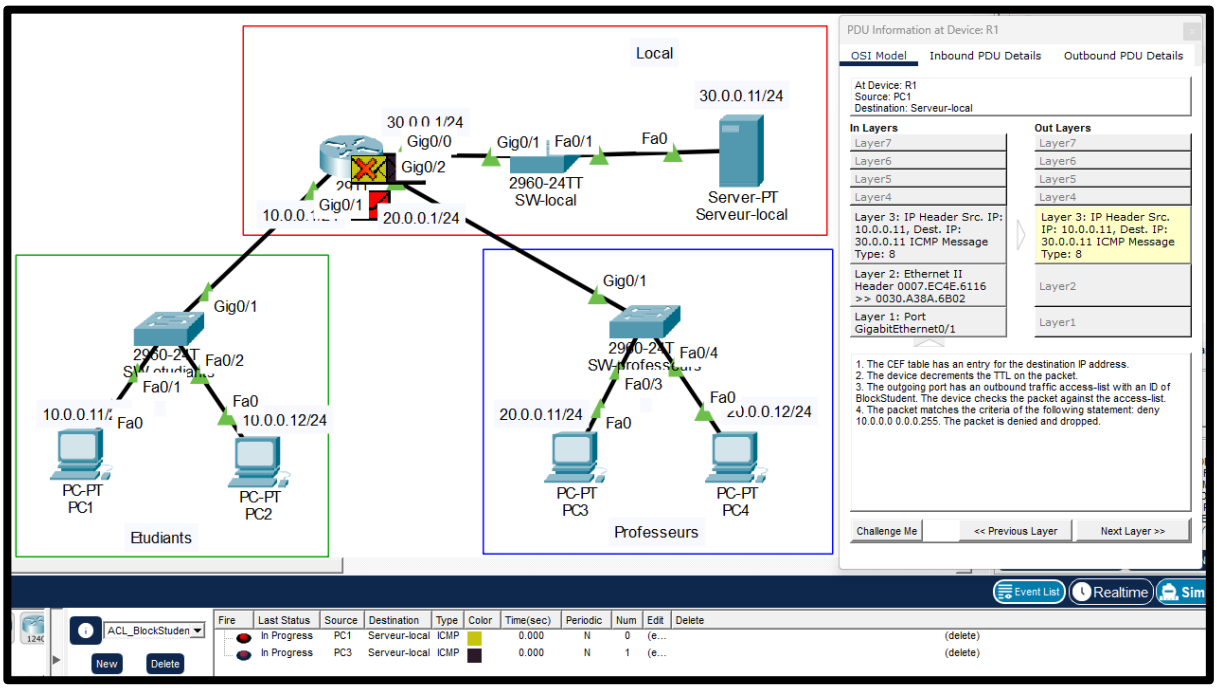
- Configuration de base



- ACL BlockStudents

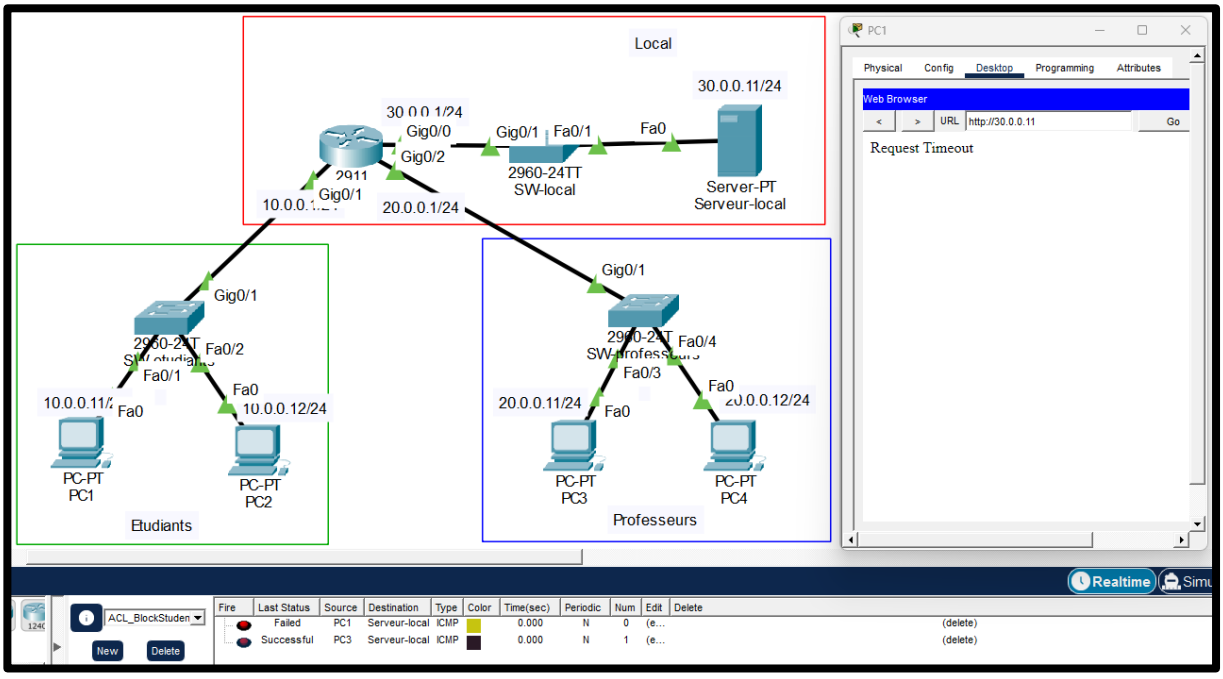


Vérification de l'ACL BlockStudents

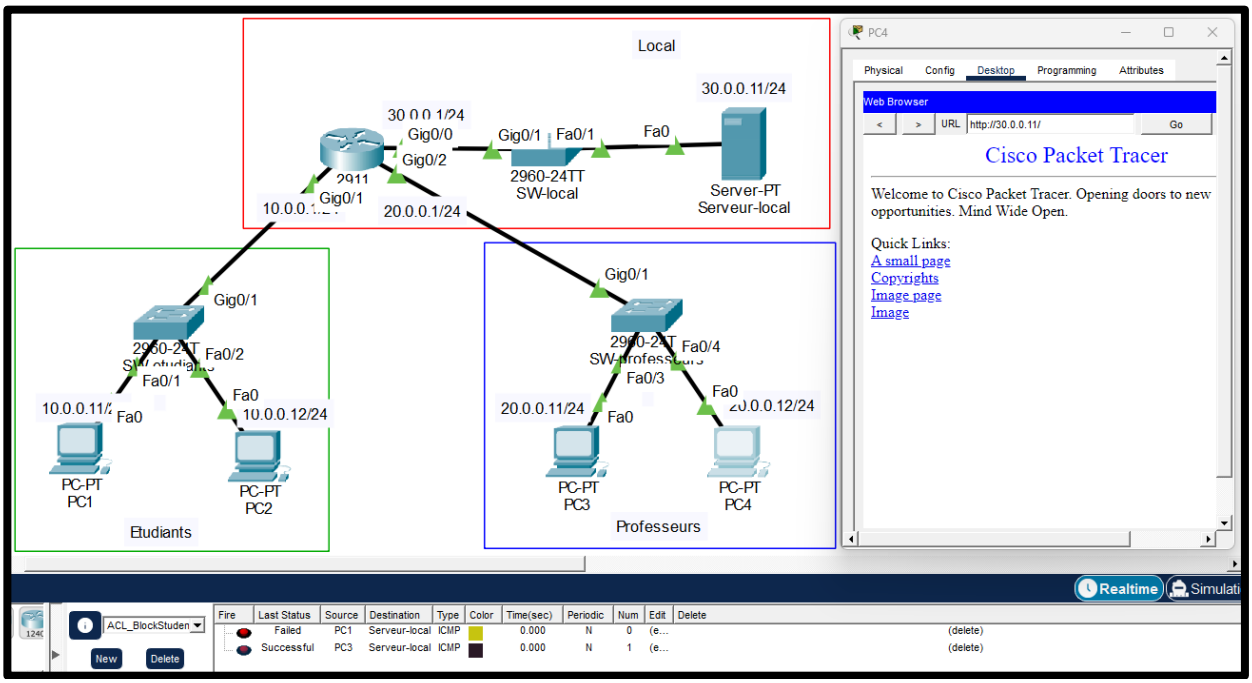


- Accès au serveur WEB

Du PC1 (étudiants) vers le serveur web.



Du PC4 (professeurs) vers le serveur web.

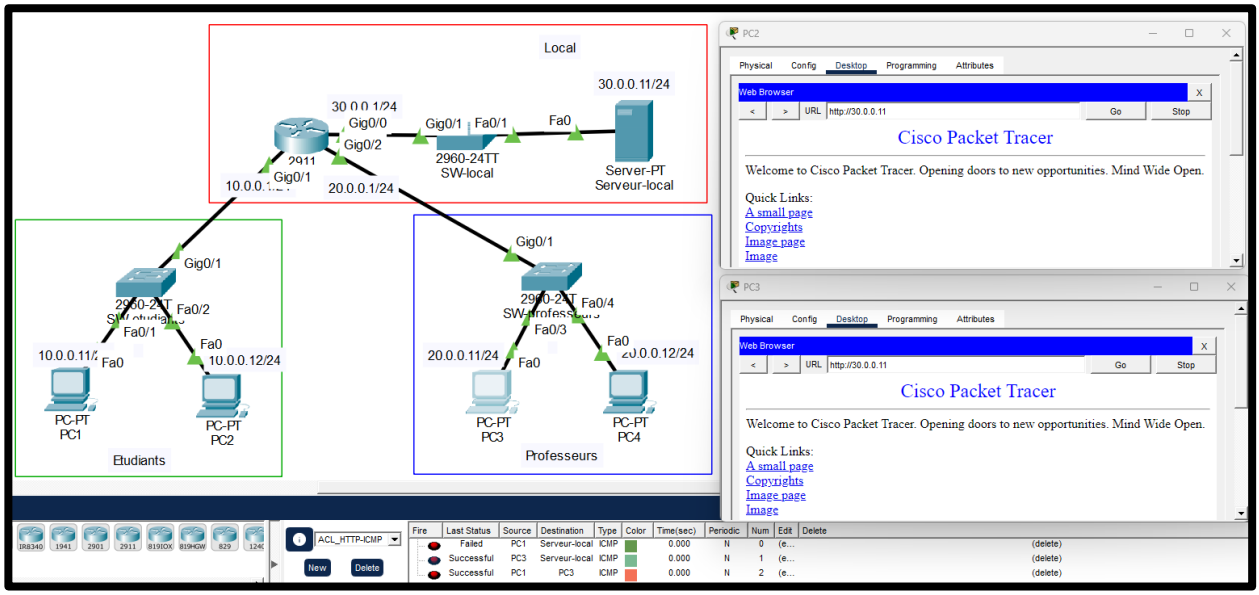


- ACL HTTP-ICMP

Il va falloir affiner les ACL, en :
- désactivant l'ACL BlockStudent
- permettant : ping entre 10. et 20. ; accès au serveur web depuis 10. et 20.

- **Rendu final :**

- 10. et 20. peuvent communiquer entre eux et joindre le serveur web
- 10. ne peut pas ping le serveur web contrairement à 20.



Commandes pour les ACL

- BlockStudent

R1(config)#ip access-list standard BlockStudent
R1(config-std-nacl)#deny 10.0.0.0 0.0.0.255
R1(config-std-nacl)#permit any
R1#show access-lists
Standard IP access list BlockStudent
10 deny 10.0.0.0 0.0.0.255
20 permit any
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip access-group BlockStudent out

- HTTP-ICMP

R1(config)#ip access-list extended ACL_HTTP-ICMP
R1(config-ext-nacl)#permit icmp 10.0.0.0 0.0.0.255 20.0.0.0 0.0.0.255
R1(config-ext-nacl)#permit tcp 10.0.0.0 0.0.0.255 host 30.0.0.11 eq www
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#ip access-group ACL_HTTP-ICMP in
R1#show access-lists
Extended IP access list ACL_HTTP-ICMP
10 permit icmp 10.0.0.0 0.0.0.255 20.0.0.0 0.0.0.255
20 permit tcp 10.0.0.0 0.0.0.255 host 30.0.0.11 eq www
interface GigabitEthernet0/1
ip access-group ACL_HTTP-ICMP in