TEST PROJECT

Startech's Days 2018

Finale

Métier : Gestion Réseau IT
Epreuve réalisée par : Patrick WERY
Employeur : Technobel

RESUME DE L'ÉPREUVE

Le travail à réaliser intègre dans un environnement réseau Cisco, des éléments d'infrastructure Microsoft et GNU-Linux.

Les compétiteurs doivent mettre en place un réseau contenant des switchs et routeurs Cisco donnant accès à une connexion centralisée représentant internet.

Un ordinateur fonctionnant sous Windows Server 2016 offre un environnement Virtuel Hyper-V dans lequel se trouvent 3 serveurs et 1 client. Les compétiteurs doivent configurer les machines virtuelles sur l'hôte.

L'hôte Hyper-V sera pré-créés afin de maximiser le temps disponible pour les autres tâches de configuration.

DESCRIPTIF DU PROJET ET DES TACHES À EFFECTUER

Tache 1 :
Vous allez dépanner le réseau présenté dans le fichier Packet tracer.

Tache 2 :
Câblage d'une topologie réseau en respect des informations fournies sur un schéma topologique et configuration du réseau commuté.

Tache 3 :
Configurations des paramètres de couche 3 incluant la mise en place du routage inter-vlan, du routage dynamique et d'une configuration NAT

Tache 4 :
Configuration d'un environnement Microsoft Windows avec mise en place d'un Active Directory, configuration d'objet du domaine et ajout de Rôles et de fonctionnalités.

Tache 5 :
Configuration d'un environnement GNU/Linux sur base de la distribution CENTOS 7 et intégration du système libre dans un environnement Microsoft

Tache 6 :
Configuration de paramètres de sécurités supplémentaires tels que des Group Policy Object et Radius.

Tache 7 :
Mise en place d'un contrôle de Traffic réseau a l'aide de liste de contrôle d'accès, de monitoring et de restriction DHCP

Tache 8 :
Cette tache va consister à sauvegarder toutes vos configurations sur un server centralisé au moyen du protocole TFTP

INSTRUCTIONS POUR LES CANDIDATS

Attention à bien lire l'énoncé au complet avant de commencer l'épreuve. Cela vous permettra d'avoir une meilleure vue d'ensemble de ce qui est demandé et permettra d'effectuer les tâches dans l'ordre.

Tache 1 : Dépannage d'une topologie réseau existante

Dépannez la topologie qui vous est présentée sur le Packet tracer.

Tache 2 : Mise en place d'un réseau commuté et câblage d'une topologie selon le schéma fournis

A. Câblage de la topologie

A l'aide du schéma de topologie fournis ainsi que des câblages préparés sur votre espace de travail, vous allez devoir procéder au câblage de votre Labo ; respectez le schéma scrupuleusement.

B. Configuration de base des équipements réseaux

Votre deuxième tâche est la configuration de base des équipements réseaux. Il vous faudra tout configurer comme précisé dans le tableau. Toute dérive (changement des informations par rapport à ce qui est fournis) sera considérée comme fausse.

Voici les différents éléments à configurer **sur chaque équipement**

Tâche ou élément de configuration	Spécification
Définissez le nom d'hôte	Référez-vous au schéma topologique
Désactivez la recherche DNS inverse	
Définissez le mot de passe d'accès à la console	Startechconpasswd
Activez la synchronisation de lignes	Sur le port console
Définissez un mot de passe crypté d'accès au mode d'exécution privilégie	Startechenpasswd
Définissez la longueur minimum des mots de passe	12 caractères
Chiffrez tous les mots de passes en clair de la configuration	
Activer les sessions d'accès à distance	• 5 session maximum (les autres doivent être interdites) • Mot de passe : startechvtypasswd
Définissez un utilisateur qui sera administrateur	Utilisateur : Startechadmin Password : Adminpassword
Définissez un utilisateur	Utilisateur : Startechuser Password : Userpassword
Fermer la session après 20 minutes et 10 secondes d'inactivité	Aussi bien pour les sessions locales que distantes
Bloque la connexion pendant 45 secondes si 3 tentatives de login infructueuses arrivent endéans les 3 minutes	Uniquement sur les routeurs
Définir la bannière de connexion	Startech 2018 – Accès interdit !
Utilisation du protocole SSH	• Utilisez le domaine : startech2018.loc • Utiliser la version 2 de SSH • Seul SSH doit être autorisé (pas de telnet) • Utilisez une clé rsa de 1500 bits • L'adresse IP sera définie dans la tâche 3

C. Configuration des VLANs

Votre Tâche consistera à mettre en place les fonctionnalités de couche 2 de votre réseau. Les différents éléments à configurer sont les suivants :

Tableau des VLANs :

VLAN	Nom	Sous-Réseau
10	IT	10.200.10.0/24
20	HR	10.200.20.0/24
100	SRV	10.200.100.0/24
110	Management	10.200.110.0/24
99	Natif	---
999	UnusedPorts	---

Vous allez maintenant sur chaque Switch configurer les VLANs et attribuer chaque port aux VLANs approprié.
Pour ce faire, vous allez utiliser le protocole VTP, C'est S3750 qui sera serveur VTP, S2960-1 et S2960-2 seront quant à eux clients VTP. Le domaine VTP est **Startechforever**, le mot de passe est **Cisco**, la version à utiliser est la version **2**.
Vous voyez dans le tableau ci-dessus que le vlan Natif est changé (veillez donc à le faire) et que les ports inutilisés doivent être déplacés dans le van 999.
Pour les interfaces en Trunk, veuillez noter que les interfaces remontant au Switch 3750 sont en Etherchannel. L'Etherchannel est à monter avec les paramètres appropriés, à savoir :

- Utilisation du protocole Standard de l'IEEE (803.3ad)
- L'Etherchannel doit être dans un état de négociation actif (échange de messages propre au protocole permettant la gestion de cet Etherchannel)

Chaque Trunk ne devra autoriser que les VLANs créés ci-dessus.
L'interface Fa0/24 des switchs S2960-1 et S2960-2 est un Trunk, ainsi que l'interface G0/0/12 du switch S3750 ; Pour cette interface particulière, le vlan natif sera le vlan 10 (IT).
Pour chacun des switchs, voici les informations d'attribution des ports aux VLANs :

Switch	Port	Vlan
S3750	G0/0/3-4	999
	G0/0/6-11	999
	G0/0/15-16	999
	G0/0/18-23	999
	G0/0/24	100
S2960-1	F0/1-4	10
	F0/5-8	20
	F0/9-23	999
S2960-2	F0/1-8	20
	F0/9-16	100
	F0/17-23	999

N'oubliez pas pour chacun des switchs de définir l'IP de management suivant les informations fournie sur le schéma de topologie (⚠ à placer dans le bon vlan).

D. Configuration de la sécurité des ports

Il ne nous reste plus qu'à définir les paramètres de sécurité supplémentaires pour les Switch d'accès :

- Chaque port ne devra accepter qu'une seule adresse MAC par port
- Cette adresse MAC sera apprise de manière dynamique et rémanente.
- Sur le S2960-1, éteindre la liaison en cas de non-respect
- Sur S2960-2, bloquer le trafic en infraction, en générant des Logs.
- Tous les ports inutilisés, en plus d'être placés dans un autre vlan (999) devront être arrêtés

- Il faut vous arranger pour que les ports éteins par la sécurité de port se rallument après 2 minutes et 30 secondes sans que l'administrateur n'ait besoin de venir le faire manuellement

E. Configuration du Spanning-tree

Vous allez configurer les équipements de sorte que S3750 soit root bridge pour tous les VLANs.
La version du protocole à utiliser est le RSTP.
Vous devez vous arranger pour que l'interface f0/24 de s2960-2 soit utilisée pour joindre le root bridge (pont racine).
Tous les ports d'accès doivent être configurés pour laisser passer le trafic immédiatement après le branchement du câble

Tache 3 : Configuration des paramètres de couche 3

A. Configuration du routage Inter-Vlan

Le routage Inter-Vlan sera effectué par le S3750. A cette fin, le Switch utilisera la première adresse IP de chaque réseau pour son interface de couche 3 permettant le routage entre ces VLANs.

B. Configuration du routage dynamique et statique

Afin de pouvoir accéder à internet, vous allez devoir créer des routes statiques par défaut sur S3750. Il vous est demandé d'envoyer le trafic sur R2900 (il a la meilleure bande passante) mais de garder un chemin de secours vers R2800 si jamais la première route devenait inaccessible.
Pour ce faire, vous allez devoir dans un premier temps configurer le réseau sur les interfaces G0/0/5 & G0/0/17. La première adresse du réseau sera attribuée à chaque interface de notre S3750
R800 aura lui aussi, pour ses interfaces fa1 et fa2 la première IP du réseau. L'interface fa3 obtiendra ses informations grâce à un serveur DHCP fournis par votre FAI
Pour le routage Dynamique à mettre en place, il faudra utiliser le protocole EIGRP. Voici les différentes informations nécessaires à sa configuration.

- Le numéro de système autonome est le 51
- Le routeur ID de chaque routeur est le suivant (et sera configuré grâce à une interface de bouclage) :
  - R800 : 8.8.8.80
  - R2800 : 8.8.8.28
  - R2900 : 8.8.8.29
- Vous devez configurer les routeurs pour échanger tous leurs réseaux directement connectés
- Vous propagerez une route par défaut vers internet grâce au protocole EIGRP

C. Configuration du NAT

Afin de permettre à chacun d'accéder aux ressources internet, il va vous être demandé de configurer votre Routeur d'extrémité afin qu'il supporte la fonction NAT. Voici ce qu'il vous est demandé de faire :

- Vous allez configurer votre Routeur pour qu'il puisse faire du PAT (appelé aussi NAT avec surcharge)
- Tous les réseaux du LAN doivent être autorisés à accéder à internet sauf le réseau de management

Il est également demandé que vous créez un Nat statique permettant d'accéder à votre serveur Web (qui sera créé plus tard). Pour ce faire, vous utiliserez l'adresse IP suivante : 5.5.0.**X**
(Si le X ci-dessus n'est pas défini, demandez à un membre du jury)

Tache 4 : Configuration d'un environnement Microsoft Windows

Sur votre machine SRV-2016-1, vous allez créer trois machines virtuelles serveurs qui hébergeront chacune un Windows serveur. Regardez bien dans le tableau afin de sélectionner la bonne version de serveur lors de l'installation.
Voici les différentes informations dont vous allez avoir besoin pour configurer vos VMs :

Infos	VM1	VM2	VM3
Système d'exploitation	Windows Server 2016 desktop experience	Windows Server 2016 core	Windows Server 2012R2
Fonction	Domain Controller	Domain Controller	Member Server
IP	10.200.100.100	10.200.100.200	10.200.110.100
Processeurs	2	2	2
RAM	4096	4096	4096
Préinstallé / préconfiguré	Non / Non	Oui / Non	Oui / Non
Nom de la machine	DC1	DC2-core	MS1
Password	Pa$$w0rd	Pa$$w0rd	Pa$$w0rd

Il va vous falloir installer l'OS sur VM1. Les ISO des systèmes se trouvent sur le bureau de votre machine hôte.
Pour les VMs, il va falloir créer la mise en réseau dans le gestionnaire Hyper-V. Rappelez-vous que c'est un TRUNK qui est relié au serveur, il vous faudra donc configurer les connexion réseau de chacune des Machines virtuelles sur le bon VLAN ☺ (plusieurs méthodes existent, choisissez celle que vous préférez).
L'hôte quant à lui utilisera l'IP renseignée sur le schéma.

A. Configuration des Domain Controller

Pour configurer les Domain Controller, vous allez avoir besoin d'un nom de domaine. Pour ce faire, utilisez les instructions ci-dessous.
Le nom de domaine à utiliser est à composer à l'aide de votre nom et prénom :
Les 3 premières lettres de votre prénom suivi des 3 premières lettres de votre nom de famille terminé par l'extension « .loc »

➔ Exemple : charles DUPUIS : chadup.loc

B. Configuration du DHCP

Il vous est demandé de mettre en place un serveur DHCP, celui-ci se situera sur le server DC2-CORE.
Un pool doit être créé pour tous les VLANs à l'exception du vlan 100.
Les Pools DHCP devront distribuer les IP de 10 à 99 pour chacun des Pool, Les paramètres DNS, Passerelle par défaut et serveur de temps (voir les informations de celui-ci au point 7C) devrons également être distribuées aux clients.
Le bail sera de 8h pour chaque VLAN, les noms de Pool DHCP seront : « POOL+VLANID » où vous remplacerez VLAN ID par l'ID de VLAN. (Ex : POOL50)

C. Configuration de l'Active Directory

Dans l'AD, vous allez créer une structure d'unité organisationnelle afin de pouvoir y placer tous vos utilisateurs et vos ordinateurs.
Cette structure sera sur plusieurs niveaux :

- Niveau 1 : XXX_users / XXX_Computers
  (remplacer XXX par votre domaine [sans l'extension])
- Niveau 2 : Pour les utilisateurs, voir le tableau ci-dessous
  Pour les ordinateurs : Serveurs / Clients
- Niveau 3 : Pour les Ordinateurs Clients et Serveurs : Windows / Linux

Voici maintenant la liste des utilisateurs et leur OU (Remplacer les X de l'UPN par votre nom de domaine) :

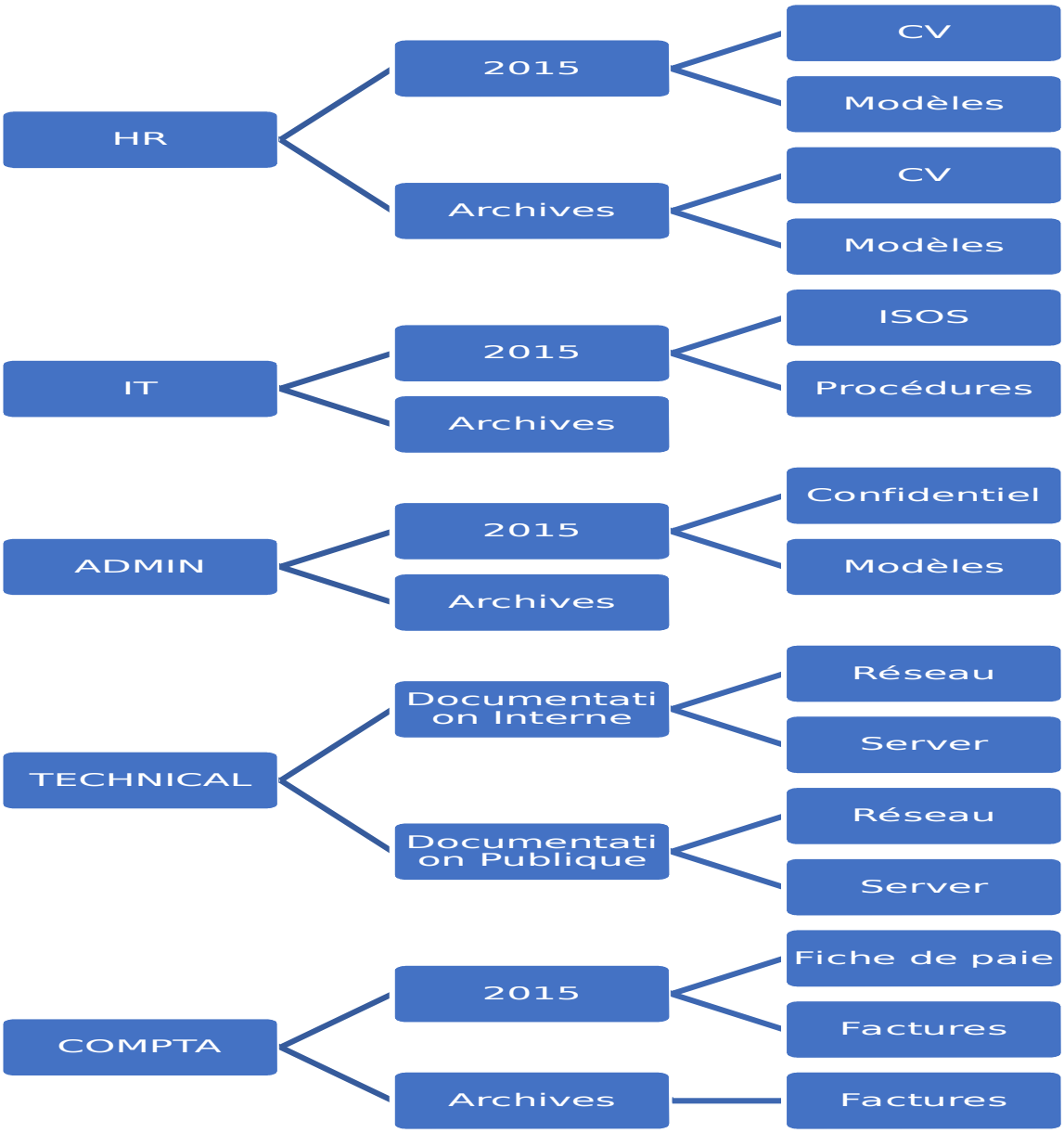
Nom	Prénom	Username	UPN	Groupe	OU
Mauve	Guy	guy.mau	guy.mau@XXXXXX	Admin	Admin
Biffe	Rose	ros.bif	ros.bif@ XXXXXX	Admin	Admin

Source	Aude	aud.sou	aud.sou@ XXXXXX	HR	HR
Tograf	Laure	lau.tog	lau.tog@ XXXXXX	HR	HR
Haux	Claude	cla.hau	cla.hau@ XXXXXX	IT	IT
Erne	Maud	mau.ern	mau.ern@ XXXXXX	IT	IT
Némar	Jean	jea.nem	jea.nem@ XXXXXX	Compta	Compta
Luation	Eva	eva.lua	eva.lua@ XXXXXX	Technical	Technical

Rappel : Lors de la création d'utilisateur, il faut utiliser la méthode **AGDLP** également appelée **IGDLA**

D. Configuration du Member server

Vous allez configurer le serveur 2012R2 en serveur membre du domaine.
Le member Server, une fois bien ajouté dans le domaine vous servira de serveur de fichiers. Il vous est demandé de filtrer l'affichage dans le dossier de manière à ce que les utilisateurs connectés ne puissent voir que les éléments auxquels ils ont accès.
Voici la structure des Dossier à créer dans un dossier nommé « Partage » à la racine de votre disque C et partagé sous le nom « Share » :



Voici les autorisations effectives à régler sur ces dossiers partagés :

- Chaque utilisateur doit pouvoir accéder en modification au dossier de son groupe
- Les utilisateurs du groupe Admin ont les droits en lecture & écriture sur tous les dossiers
- Tous ont le droit en lecture dans le sous-dossier Documentation Publique du dossier Technical. Cependant seul les gens des OU « Technical » & « Admin » peuvent accéder en lecture et écriture dans le dossier « documentation interne ».

E. Configuration du client Windows

Vous allez à présent configurer le client Windows. Celui-ci doit être entré dans le domaine, veillez à ce qu'il porte le nom convenu sur le schéma. Ses paramètres IP doivent être obtenu en DHCP.
Cette machine doit se situer dans la bonne OU, veillez y.
Connectez-vous à l'aide de différents utilisateurs pour vérifier le fonctionnement du pc en domaine.

Tache 5 : Configuration d'un environnement GNU/Linux

A. Installation et configuration du serveur Linux-SVR

A l'aide de la clé USB fournie, vous allez installer le système linux Centos 7. Cette installation se fera sans interface graphique. Vous utiliserez l'intégralité du disque dur. Il vous est demandé de partitionner le système comme suit :

Partition	Taille
/	20 GB
/boot	5 GB
/home	100 GB
/var	Tout l'espace disponible sur le disque
SWAP	2GB

La langue d'installation doit être Français avec un clavier Belge. Le mot de passe Root est « Secret » ; un utilisateur « startech » avec le mot de passe « Startech2018 » sera créé. Cet utilisateur sera administrateur du système.
Vous allez configurer votre pc avec l'adresse IP fixe renseignée sur le schéma de topologie. Ensuite, vous vous arrangerez pour qu'il utilise le dépôt de paquet local qui est accessible via l'adresse : http://172.30.10.250/repo/
Vous allez à présent installer un serveur apache afin de mettre en place un site web. Une fois apache installé, vous allez mettre en place un site web ; ce site est déjà fait, il est stocké sur un serveur distant. Il vous est demandé de récupérer celui-ci est de le mettre en ligne.
Pour récupérer votre site WEB, vous allez devoir monter un partage NFS. Le dossier nfs est accessible via le chemin d'accès suivant : 172.30.10.1**X0**:nfs
(Si le X ci-dessus n'est pas défini, demandez à un membre du jury [si x=1 ip = 172.30.10.110])

B. Installation du client Linux

Sur le laptop, vous installerez également CentOS via la clé USB. Cette fois-ci, vous allez installer l'interface graphique.
Vous utiliserez toujours le dépôt http://172.30.10.250/repo/ comme dépôt de paquets. Votre pc récupèrera son IP en DHCP.
Vous allez ensuite installer les paquets suivants :
sssd, realmd, oddjob, oddjob-mkhomedir, adcli, samba-common, samba-common-tools, krb5-workstation, openldap-clients, policycoreutils-python.

A présent, vous allez ajouter votre machine dans l'Active Directory et vous connecter avec un utilisateur du domaine afin de vérifier le bon fonctionnement de votre configuration.

Tache 6 : Configurations de paramètres de sécurités supplémentaire

A. Configuration de GPOs

Vous allez configurer les Polices de sécurité suivantes :

- Il est demandé d'installer automatiquement le logiciel 7zip a l'ouverture de session
- Sur les postes clients, nous ne voulons pas voir apparaitre le nom du dernier utilisateur connecté
- Empêcher l'utilisation d'internet explorer 10 et inférieur

Vérifiez le fonctionnement de ces GPOs grâce à la machine Client Windows

B. Configuration du serveur radius

Il vous est à présent demandé de configurer un serveur Radius sur le MS1 afin de permettre l'authentification des utilisateurs sur les équipements réseaux. Il est demandé que le serveur Radius soit pris comme facteur d'authentification principal et que la base de données locale ne soit utilisée que si le radius n'est pas accessible. La clé partagée pour le radius est « Startech2018 ».

Tache 7 : Mise en place d'un contrôle du trafic réseau.

A. Configuration des Access List

Voici les différentes Access List que vous allez créer :

1. **Une liste d'accès standard nommée Admin-MGMT**

Cette liste doit permettre uniquement aux réseau IT d'accéder à distance en SSH a tous les équipements réseau.
Il est également permis d'accéder en SSH à partir d'un autre équipement Cisco de la topologie.

2. **Une liste de contrôle d'accès étendue numérotée 111**

Cette liste doit permettre à chaque Vlan d'accéder à internet et au réseau des serveurs
Elle doit également interdire tout autre type de trafic inter-VLAN

B. Configuration du monitoring

Afin de configurer le monitoring de manière constructive, il va falloir commencer par mettre tous nos équipements réseau a la bonne date et à la bonne heure. Nous utiliserons pour ce faire un serveur NTP.

1. **Configuration du serveur de temps**

Voici les différents éléments que vous allez configurer pour le NTP :

- Chaque équipement réseau devra se synchroniser avec R800
- R800 sera votre serveur de temps
- R800 aura comme Strate la valeur 5
- R800 sera client du serveur 5.5.0.253

2. **Configuration du monitoring avec Syslog**

Voici les différents éléments de configuration :

Tâche ou élément de configuration	Spécification
Configurez chaque équipement afin d'utiliser Syslog	L'adresse IP du serveur Syslog est : 10.200.10.100
Niveau de sévérité	Information (6)
Options des messages	Utilisation des numéros de séquence et de l'horodatage
	Chaque routeur doit utiliser son IP de bouclage pour être identifié sur le syslog
	Le switch S3750 utilisera son IP du réseau de management pour être identifié sur le syslog

Le serveur Syslog est tftpd32 présent sur la machine SRV-2016-1. (Allez à l'onglet Syslog)

C. Restriction DHCP

Il vous est demandé de configurer les équipements réseau afin de ne permettre que le serveur DHCP légitime de répondre aux requêtes des clients. Cette mesure est mise en place afin de s'assurer que c'est bien notre serveur qui est le seul à pouvoir donner des IP aux équipements du réseau.

Tache 8 : Sauvegarde centralisée de la configuration des routeurs et switchs

Vous allez à présent sauvegarder toutes les configurations du matériel réseau de chacun des équipements sur le serveur central : 172.30.10.X.
(Si le X ci-dessus n'est pas défini, demandez à un membre du jury [si x=1 ip = 172.30.10.110])

MATERIEL A EMPORTER PAR LE CANDIDAT

Tout le matériel nécessaire à l'épreuve est fourni sur place.

MATERIEL INTERDIT LORS DE LA COMPETITION

Il est interdit d'utiliser tout ce qui peut troubler votre travail : GSM, Radio, MP3.

L'usage d'accessoires connectés sur les ports USB ou autres (clé USB sous toute formes, disque dur, GSM, tablette, …) est proscrit

L'utilisation de tout documents relatifs au domaine couvert par l'épreuve, sous quelque forme que ce soit, est totalement et formellement interdite

PROCEDURE DE NOTATION

- Organisation et gestion du travail 10 %
- Conception 15 %
- Configuration des équipements de réseau 25 %
- Installation et configuration de systèmes d'exploitation 25 %
- Résolution des problèmes 25 %

CONSIGNES DE SECURITE

Néant

DIVERS

Néant

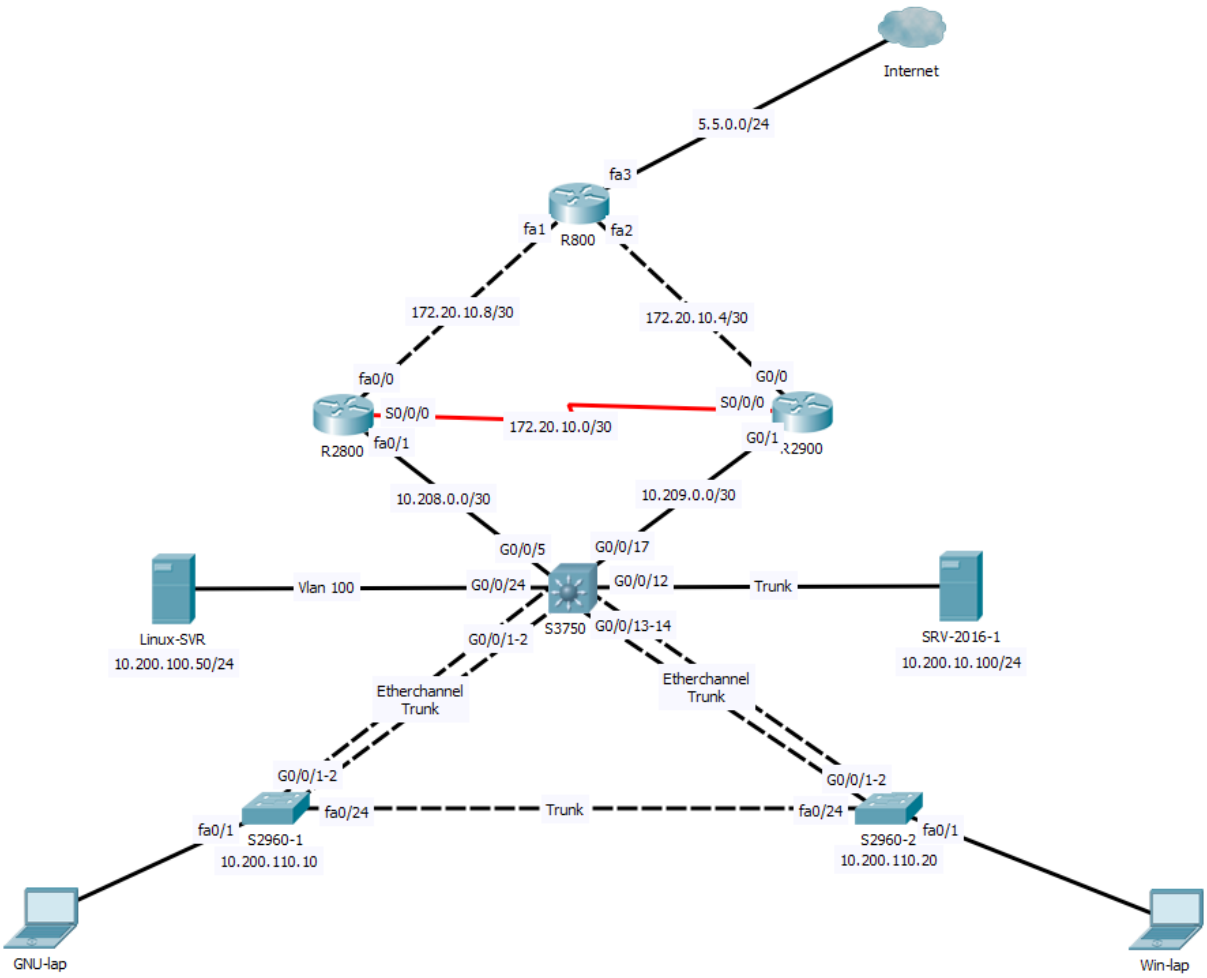
ANNEXES :

- STD2018_TP_Gestion_Réseau_IT_Finale_Annexe_1-Préparation.docx
- STD2018_TP_Gestion_Réseau_IT_Finale _Annexe_2-Topologie.png
- STD2018_TP_Gestion_Réseau_IT_Finale _Annexe_3-Troubleshoot.pka

EST-CE QUE CE DOCUMENT, ANNEXES Y COMPRIS, PEUVENT-ILS ÊTRE ENVOYÉS AUX CANDIDATS AVANT L'ÉPREUVE?

UNE PARTIE

Seule l'annexe 1 reprenant les sujets traités par l'épreuve peut etre divulguée. Le reste doit rester confidentiel


Internet
5.5.0.0/24
fa3
fa1
R800
fa2
172.20.10.8/30
172.20.10.4/30
fa0/0
G0/0
S0/0/0
S0/0/0
172.20.10.0/30
R2800
fa0/1
G0/1
R2900
10.208.0.0/30
10.209.0.0/30
G0/0/5
G0/0/17
Linux-SVR
10.200.100.50/24
Vlan 100
G0/0/24
S3750
G0/0/12
Trunk
SRV-2016-1
10.200.10.100/24
G0/0/1-2
G0/0/13-14
Etherchannel
Trunk
Etherchannel
Trunk
G0/0/1-2
G0/0/1-2
fa0/1
fa0/24
S2960-1
10.200.110.10
Trunk
fa0/24
S2960-2
10.200.110.20
fa0/1
GNU-lap
Win-lap