


Manuel d'utilisation du programme

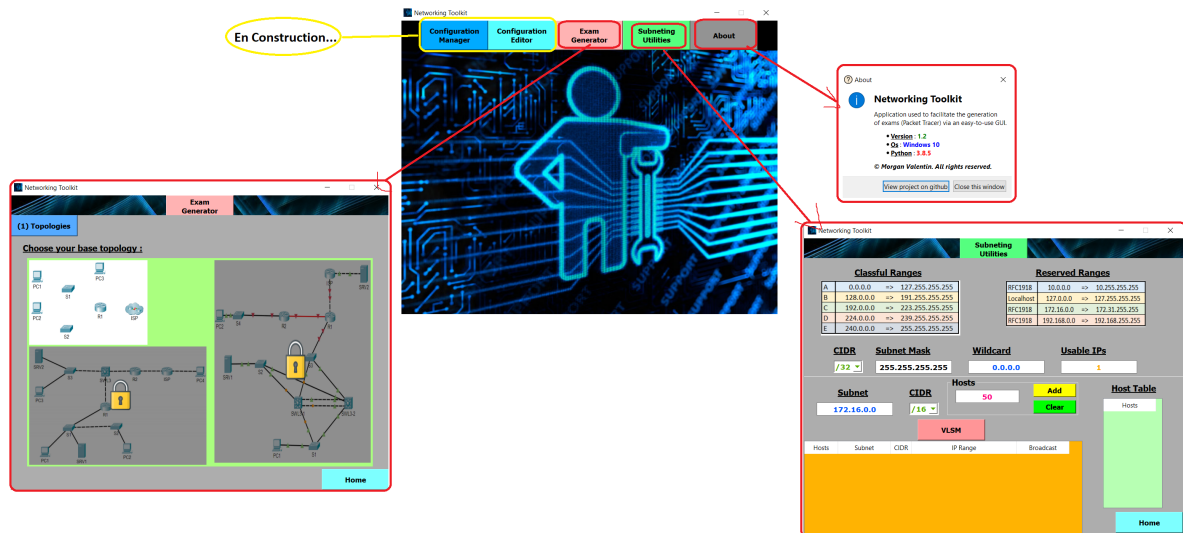
- [Procédures d'installation](#)
- [Utilisation](#)
 - [Générateur examens de niveau 1](#)
 - Choisir la topologie
 - (2) Main Configuration
 - (3) Connectivity
 - (4) Addons
 - (5) Fichiers Générés
 - [Calculatrice réseau](#)

Procédures d'installation

1. Aller sur le repos GitHub du projet : [github](#)
2. Téléchargez la dernière version :
 - Version **1.4** : [release windows v1.4.zip](#)
 -  Cette version inclus **UNIQUEMENT** le générateur d'examen de niveau 1 !
3. (Optionnel) Vérifier l'intégralité du fichier [Voir section du github](#)
4. Extraire les fichiers :
 - Vous devriez avoir 1 dossier `img` contenant les images du programme et le programme sous format exécutable (`.exe`).
5. Double cliquer sur l'exécutable pour démarrer le programme.

PS : Cette exécutable contient toutes les librairies python ainsi que les différents modules utilisées.

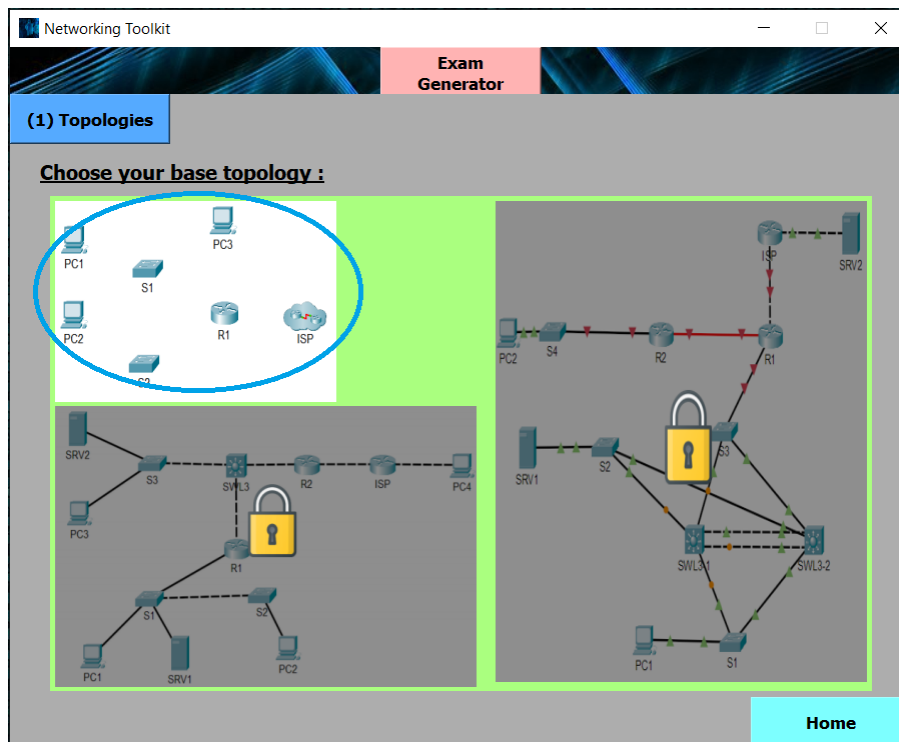
Utilisation

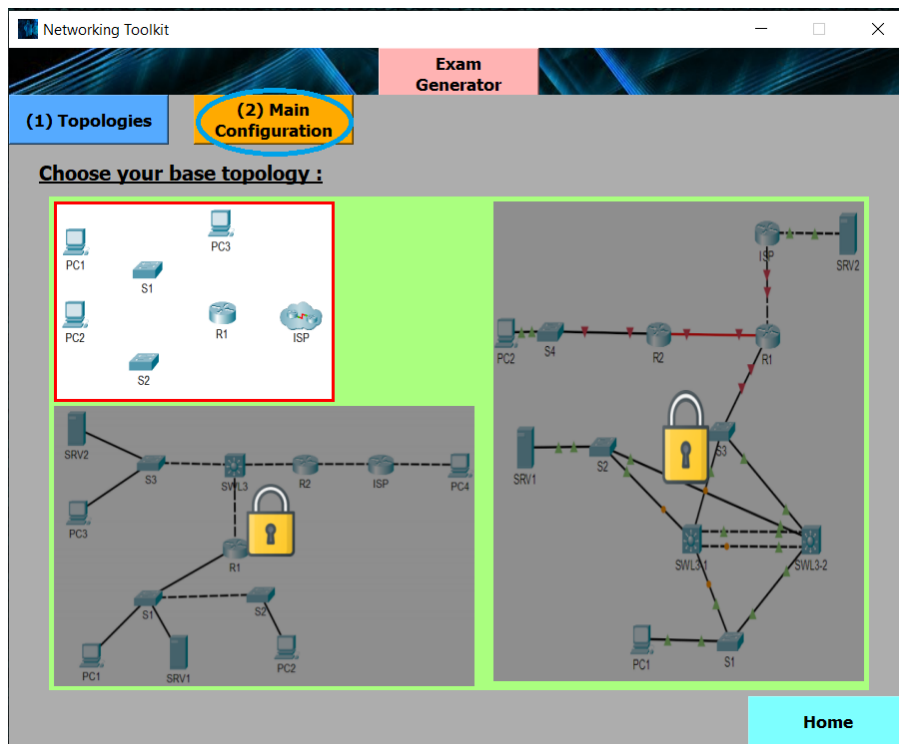


Générateur d'examens de niveau 1

1. Choisir la topologie

PS : Une seule topologie est actuellement disponible.





- Une fois la topologie sélectionnée, celle-ci se voit encadré en rouge et un bouton apparaît.
- Cliquer sur le bouton pour continuer.

2. "(2) Main Configuration"

Networking Toolkit

Exam Generator

(1) Topologies (2) Main Configuration

Local subnet (LAN) : 192.168.0.0 /24

Subnet to ISP (WAN) : 200.0.0.0 /24

DNS Domain : formation.local

VLSM

LAN Name : LAN A

Number of hosts : 50

Clear Add

Name	Hosts
------	-------


Save Changes Home

- (1) : C'est le schéma du réseau.
- (2) : Les données générales du réseau
 - LAN => C'est le réseau de base qui sera ensuite "coupé" en d'autres sous-réseau (via VLSM)
 - WAN => C'est le réseau entre R1 et ISP
 - DNS Domain => Permettra par la suite de mettre en place un accès distant chiffré (SSH)
- (3) : Le système de VLSM
 - Pour chaque sous-réseau, il faut indiquer le nom du sous réseau et le nombre d'hôtes souhaités.
 - Se configure 1 par 1. Il faut donc mettre par exemple "LAN A" et "50" puis ensuite cliquer sur "Add" pour l'ajouter au tableau.
 - PS : Il n'est pas possible d'avoir 2 réseau avec le même nom !
PPS : Si jamais vous avez fait une bêtise, cliquer sur le bouton "Clear" qui effacera tout de la table.
- (4) : La table VLSM
 - Cette table à pour but de montrer ce qui est encodé dans le programme.
 - Mais tant que vous n'avez pas cliquer sur "Save Changes", vous pouvez toujours revenir en arrière.

- **(5) : "Save Changes"**

- Une fois que vous avez mis toutes les informations désirées, cliquer sur ce bouton pour passer à la suite.
- Ce bouton va sauvegardé les données et faire apparaître le prochain bouton.

- **(6) : "Home"**

- Permet de retourner à la page d'accueil du programme.
- Utilité ?
 - Permet d'aller dans la section "Subnetting utilities" pour effectué un calcul de sous réseau pour ensuite revenir dans l'onglet "Exam Generator"
-  Attention, si c'est pour relancer le générateur d'examen, il est vivement conseillé de redémarrer le programme.

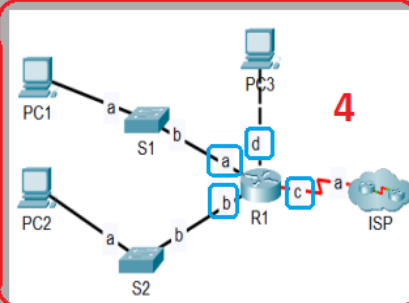
3. "(3) Connectivity"

Networking Toolkit

Exam Generator

(1) Topologies (2) Main Configuration (3) Connectivity

Device	Hostname	Subnet	Ip Rule
PC1 :	PC1	LAN A	1st IP Available
PC2 :	PC2	LAN B	1st IP Available
PC3 :	PC3	LAN C	1st IP Available



Device	Interface	Subnet	Ip Rule	Action
S1 :	(a) F0/1	LAN A	Last IP -1	To LAN A
S2 :	(a) F0/1	LAN B	Last IP -1	To LAN B
R1 :	(a) G0/0	LAN A	Last IP Available	To LAN A
	(b) G0/1	LAN B	Last IP Available	To LAN B
	(c) S0/0/0	WAN	200.0.0.1	To ISP
	(d) E0/0/0	LAN C	Last IP Available	To PC3
ISP	(a) S0/0/0	WAN	200.0.0.2	To R1



Save Changes Home

- (1) : Représente les champs pour mettre le nom d'hôtes des différentes machines (Hostname).
- (2) : Menu déroulant pour indiquer dans quelle réseau/sous-réseau l'appareil en question se trouve.
 - Ce menu est constitué des sous-réseau sauvegardé de la page précédente + le réseau "WAN" (entre ISP et R1)
- (3) : Menu déroulant comprenant la règle au niveau de l'adressage IP.
 - "1st IP Available" => Indique qu'il faut donner la **1ère IP disponible** à cette appareil (PC1 par exemple).
 - "2nd IP Available" => Indique qu'il faut donner la **2ème IP disponible**.
 - "Last-1 IP Available" => Indique qu'il faut donner l'**avant-dernière IP disponible**.
 - "Last IP Available" => Indique qu'il faut donner la **dernière IP disponible**.
- (4) : Schéma réseau avec des lettres utilisées pour représenté les interfaces disponibles.
- (5) : Menu déroulant avec les interfaces disponibles pour l'appareil en question.
- (6) : Permet de préciser quelle interface vous êtes en train de configurer.
 - Exemple 1 : R1 : (a) G0/0 => R1 vers S1 (interface a) utilisera l'interface GigabitEthernet0/0 (G0/0)
 - Exemple 2 : R1 : (d) E0/0/0 => R1 vers PC3 (interface d) utilisera l'interface Ethernet0/0/0 (E0/0/0)

- **(7) : Description**
 - Permet de mettre une description pour savoir de quoi il s'agit.
- **(8) : "Save Changes"**
 - Une fois que vous avez tout configuré comme vous le souhaitez, appuyer sur ce bouton afin de sauvegarder les données et de passer à la suite.
 - PS : ⚠ 2 boutons vont s'affichés par la suite : "(4) Addons" et "(5) Generate my exam !".

4. "(4) Addons"

- (0) : Il faut bien cliquer sur le bouton "(4) Addons" qui signifie "suppléments".
 - Contient le nécessaire de sécurité de base, SSH et la possibilité d'ajouter **une** route statique/ par défaut.
- (1) : Le mot de passe secret.
- (2) : Le mot de passe pour accéder à la ligne console et distante.
- (3) : Coché si vous voulez chiffré les mots de passes (fortement conseillé).
- (4) : Coché si vous voulez utilisez SSH.
- (5) : Champs où il faut y indiquer le nom d'utilisateur et le mot de passe à utiliser lors des connections via SSH.
 - Uniquement visible si la case "SSH ?" est cochée.
- (6) : La bannière affiché lors d'une connexion à l'appareil.
- (7) : Le même menu sauf qu'il concerne les switchs.
 - Il n'est malheureusement PAS possible de configurer la sécurité des switchs individuellement.
 - Utilité ?
 - Par exemple d'autorisé SSH sur R1 mais pas sur les switchs, avoir des mots de passes différents.

- **(8)** : Champ pour insérer le réseau que l'on souhaite accéder.
- **(9)** : Le masque de sous-réseau du réseau que l'on souhaite accéder.
- **(10)** : Menu déroulant qui comprends l'interface de sortie du routeur (R1) et l'adresse IP de l'ISP.
 - Permet de choisir si l'on souhaite utilisé l'interface de sortie de R1 ou bien mettre l'adresse IP de l'ISP pour encoder la route statique.
- **(11)** : Cocher cette case si vous voulez que la route soit sauvegardé
 -  Rappel : Qu'une seule route statique est possible.
- **(12)** : Comme d'habitude, appuyer sur ce bouton pour enregistrer les modifications.
- **(13)** : Appuyer sur ce bouton pour générer les 2 fichiers de sorties.
 - "solution.txt" et "packet-tracer.yaml"
 -  PS : Ces 2 fichiers seront générer directement sur le bureau.

5. Fichiers générés

1. "solution.txt"

```
-----  
SUBNETS  
-----  
  
LAN B (100) : 192.168.0.1 => 192.168.0.126 /25 (255.255.255.128)  
  
LAN A (50) : 192.168.0.129 => 192.168.0.190 /26 (255.255.255.192)  
  
LAN C (10) : 192.168.0.193 => 192.168.0.206 /28 (255.255.255.240)  
  
-----  
PC1 (LAN A)  
-----  
IP : 192.168.0.129  
Mask : 255.255.255.192  
Gateway : 192.168.0.190  
-----  
PC2 (LAN B)  
-----  
IP : 192.168.0.1  
Mask : 255.255.255.128  
Gateway : 192.168.0.126  
-----  
PC3 (LAN C)  
-----  
IP : 192.168.0.193  
Mask : 255.255.255.240  
Gateway : 192.168.0.206  
  
-----  
S1  
-----  
en  
conf t  
host S1  
enable secret class  
  
banner motd #You are accessing a restricted system#  
  
line console 0  
    password cisco  
    login  
exit  
  
line vty 0 15  
    password cisco  
    login  
exit  
  
service password-encryption
```

```
int vlan1
  description To LAN A
  ip add 192.168.0.189 255.255.255.192
  no shut
exit
```

```
ip default-gateway 192.168.0.190
end
wr
```

S2

```
en
conf t
host S2
enable secret class
```

```
banner motd #You are accessing a restricted system#
```

```
line console 0
  password cisco
  login
exit
```

```
line vty 0 15
  password cisco
  login
exit
```

```
service password-encryption
```

```
int vlan1
  description To LAN B
  ip add 192.168.0.125 255.255.255.128
  no shut
exit
```

```
ip default-gateway 192.168.0.126
end
wr
```

R1

```
en
conf t
host R1
enable secret class
```

```
banner motd #You are accessing a restricted system#
```

```
ip domain-name formation.local
crypto key generate rsa general-keys modulus 1024
username username password password
```

```
line console 0
  password cisco
  login
exit

line vty 0 4
  password cisco
  transport input ssh
  login local
exit

line vty 0 15
  password cisco
  login
exit

service password-encryption

int G0/0
  description To LAN A
  ip add 192.168.0.190 255.255.255.192
  no shut
exit

int G0/1
  description To LAN B
  ip add 192.168.0.126 255.255.255.128
  no shut
exit

int S0/0/0
  description To ISP
  ip add 200.0.0.1 255.255.255.252
  no shut
exit

int E0/0/0
  description To PC3
  ip add 192.168.0.206 255.255.255.240
  no shut
exit

ip route 0.0.0.0 0.0.0.0 S0/0/0
end
wr
```

1. "packet-tracer.yaml"

Network:

PC1:

Default Gateway: 192.168.0.190

Ports:

F0:

IP: 192.168.0.129

Link:

Connects to: F0/1

Type: 0 0

Mask: 255.255.255.192

PC2:

Default Gateway: 192.168.0.126

Ports:

F0:

IP: 192.168.0.1

Link:

Connects to: F0/1

Type: 0 0

Mask: 255.255.255.128

PC3:

Default Gateway: 192.168.0.206

Ports:

F0:

IP: 192.168.0.193

Link:

Connects to: F0/1

Type: 0 0

Mask: 255.255.255.240

R1:

Banner MOTD: You are accessing a restricted system

Console Line:

Login: 1

Password: cisco

DNS:

Ip Domain Name: formation.local

Enable Secret: class

Host Name: R1

Ports:

E0/0/0:

Description: To PC3

IP: 192.168.0.206

Link to PC3:

Connects to F0: 'True'

Type: 0 0

Mask: 255.255.255.240

Port Status: 1

G0/0:

Description: To LAN A

IP: 192.168.0.190

Link to S1:

Connects to F0/1: 'True'

Type: 0 0

Mask: 255.255.255.192

Port Status: 1

G0/1:

```
Description: To LAN B
IP: 192.168.0.126
Link to S2:
  Connects to F0/1: 'True'
  Type: 0 0
Mask: 255.255.255.128
Port Status: 1
S0/0/0:
  Description: To ISP
  IP: 200.0.0.1
  Link to ISP:
    Connects to S0/0/0: 'True'
    Type: 0 0
  Mask: 255.255.255.252
  Port Status: 1
Routes:
  Static Routes:
    Route0: 0.0.0.0-0-Serial0/0/0
Security:
  Crypto Key Set: Check this case
  Modulus Bits: 1024
Service Password Encryption: 1
Startup config: 1
User Names:
  Username: username password
VTY Lines:
  VTY Line 0:
    Login: 2
    Password: cisco
    Transport Input: 2
  VTY Line 15:
    Login: 2
    Password: cisco
    Transport Input: 2
S1:
  Banner MOTD: You are accessing a restricted system
  Console Line:
    Login: 1
    Password: cisco
  Default Gateway: 192.168.0.190
  Enable Secret: class
  Host Name: S1
  Ports:
    F0/1:
      Link to R1:
        Connects to G0/0: 'True'
        Type: 0 0
    Vlan1:
      IP: 192.168.0.189
      Mask: 255.255.255.192
      Port Status: 1
  Service Password Encryption: 1
  Startup config: 1
  VTY Lines:
    VTY Line 0:
      Login: 1
      Password: cisco
    VTY Line 15:
```

```
    Login: 1
    Password: cisco
S2:
Banner MOTD: You are accessing a restricted system
Console Line:
    Login: 1
    Password: cisco
Default Gateway: 192.168.0.126
Enable Secret: class
Host Name: S2
Ports:
    F0/1:
        Link to R1:
            Connects to G0/1: 'True'
            Type: 0 0
    Vlan1:
        IP: 192.168.0.125
        Mask: 255.255.255.128
        Port Status: 1
Service Password Encryption: 1
Startup config: 1
VTY Lines:
    VTY Line 0:
        Login: 1
        Password: cisco
    VTY Line 15:
        Login: 1
        Password: cisco
```

Calculatrice réseau

Classful Ranges

A	0.0.0.0 => 127.255.255.255
B	128.0.0.0 => 191.255.255.255
C	192.0.0.0 => 223.255.255.255
D	224.0.0.0 => 239.255.255.255
E	240.0.0.0 => 255.255.255.255

Reserved Ranges

RFC1918	10.0.0.0 => 10.255.255.255
Localhost	127.0.0.0 => 127.255.255.255
RFC1918	172.16.0.0 => 172.31.255.255
RFC1918	192.168.0.0 => 192.168.255.255

1 **CIDR** **2** **Subnet Mask** **Wildcard** **Usable IPs**

1 **/32** **255.255.255.255** **0.0.0.0** **1**

3 **Subnet** **CIDR**

172.16.0.0 **/16**

Hosts **200** **Add** **Clear**

4

VLSM **6**

Hosts	Subnet	CIDR	IP Range	Broadcast
100	172.16.0.0	/25	172.16.0.1 => 172.16.0.126	172.16.0.127
50	172.16.0.128	/26	172.16.0.129 => 172.16.0.190	172.16.0.191
3	172.16.0.192	/29	172.16.0.193 => 172.16.0.198	172.16.0.199

7

Host Table

Hosts

50

100

3

5

Home

- **(1)** : En fonction du CIDR, va générer en (2) :
 - Le masque de sous-réseau
 - Le masque de sous réseau inversé
 - Le nombre d'adresses IP disponibles (et utilisables)
- **(3)** : Mettre le réseau et le CIDR correspondant (va permettre des calculs de VLSM)
- **(4)** : Mettre le nombre d'hôtes souhaité et à chaque fois cliquer sur "Add" pour ajouter un nombre d'hôte dans la table.
 - Par exemple, j'ai mis 50 puis "Add", 100 puis "Add" et enfin 3 et "Add" afin d'avoir 50-100-3 dans la table.
PS : L'ordre n'a pas d'importance, le programme s'occupe de remettre dans l'ordre les nombres et de mener à bien les calculs de VLSM.
- **(5)** : La table des hôtes - permet d'avoir un visuel sur ce que le programme va prendre en compte.
- **(6)** : En appuyant sur ce bouton, cela va démarrer le calcul de VLSM et injecter la solution dans la table (7).
 - Fonction caché : En appuyant une 2ème fois sur le bouton, va nettoyer la table.
- **(7)** : La table VLSM contenant la solution du calcul de VLSM.

