



CREER UN MONDE NUMERIQUE

Appliquer les règles de sécurité

Table des matières

Introduction :	Erreur ! Signet non défini.
1. Premier pka :	Erreur ! Signet non défini.
1.1 Configurer le serveur FTP :	Erreur ! Signet non défini.
1.2 Vérifier le service http :	Erreur ! Signet non défini.
1.3 Configurer le serveur DNS :	Erreur ! Signet non défini.
1.4 Configuration du serveur NTP :	Erreur ! Signet non défini.
1.5 Configurer le serveur AAA :	Erreur ! Signet non défini.
2. Second pka :	Erreur ! Signet non défini.
1.6 Charger des fichiers à l'aide du FTP :	Erreur ! Signet non défini.
1.7 Accéder à un routeur d'entreprise à distance à l'aide de Telnet.	Erreur ! Signet non défini.
1.8 Accéder à un routeur d'entreprise à distance avec Telnet :	Erreur ! Signet non défini.
1.9 Accéder à un routeur d'entreprise à distance :	Erreur ! Signet non défini.
3. Troisième pka :	Erreur ! Signet non défini.
1.10 Localiser les informations d'identification du compte FTP de l'ordinateur portable de Mary :	Erreur ! Signet non défini.
1.11 Charger des données confidentielles par FTP :	Erreur ! Signet non défini.
1.12 Localiser les informations d'identification FTP de bob :	Erreur ! Signet non défini.
4. Quatrième pka :	Erreur ! Signet non défini.
1.13 Télécharger les fichiers clients sur le pc de Mike :	Erreur ! Signet non défini.
1.14 Télécharger les fichiers clients du serveur de sauvegarde des fichiers sur le pc de Mike :	Erreur ! Signet non défini.
1.15 Vérifier l'intégrité des fichiers clients avec le hash :	Erreur ! Signet non défini.
1.16 Vérifier l'intégrité des fichiers sensibles à l'aide du HMAC :	Erreur ! Signet non défini.
5. Cinquième pka :	Erreur ! Signet non défini.
1.17 Configurer le WEP pour Healthcare at Home:	Erreur ! Signet non défini.
1.18 Configurer le protocole WPA2 RADIUS pour le siège social de Metropolis Bank :	Erreur ! Signet non défini.
6. Sixième pka :	Erreur ! Signet non défini.
1.19 Envoyer du trafic FTP non chiffré :	Erreur ! Signet non défini.

Introduction :

Ce TP a pour objectif de me familiariser avec la configuration et l'administration des principaux services réseau tels que le FTP, le DNS, le NTP, le serveur web et les services de messagerie. À travers des scénarios cisco, il me permet de comprendre le rôle et l'importance de chaque service. Ce TP, permet d'acquérir des compétences pratiques dans le déploiement, de gestion des accès et de sécurisation des services.

1. Premier PKA :

1.1 Configurer le serveur FTP :

The screenshot shows the 'FTP/Web' configuration window in Cisco Packet Tracer. The 'Services' tab is active. The 'FTP' service is enabled (On). Under 'User Setup', a new user 'Bob' is being added with the password 'cisco123'. The permissions 'Write', 'Read', 'Delete', 'Rename', and 'List' are all checked. The 'Add' button is highlighted.

	Username	Password	Permission
1	cisco	cisco	RWDNL
2	Mary	cisco123	RWDNL
3	Bob	cisco123	RWDNL

J'active le service FTP en sélectionnant l'option "On". Cela permet d'autoriser les connexions FTP sur le système. Ensuite, j'ajoute un utilisateur avec le nom "Bob" et le mot de passe "cisco123". Je coche les permissions "Write", "Read", "Delete", "Rename", et "List" pour lui donner un contrôle complet sur les fichiers. Cette configuration est utile pour permettre à l'utilisateur Bob de gérer les fichiers sans restriction. Enfin, je clique sur "Add" pour sauvegarder les informations de cet utilisateur.

	Username	Password	Permission
1	Bob	cisco123	RWDNL
2	Mary	cisco123	RWDNL
3	cisco	cisco	RWDNL
4	Mike	cisco123	RWDNL

Cette liste récapitule les utilisateurs enregistrés pour le service FTP, avec leurs noms d'utilisateur, mots de passe, et permissions. Par exemple, l'utilisateur "Bob" a le mot de passe "cisco123" et des permissions complètes (RWDNL). Cela permet de vérifier rapidement les droits assignés à chaque utilisateur et de s'assurer qu'ils sont configurés correctement pour leurs besoins.

- a) Un service FTP transfère des fichiers entre un client et un serveur via un réseau en utilisant un protocole standardisé.
- b) Ce type de service décide qui peut lire, écrire, supprimer, renommer et lister les fichiers de la banque. Ça permet d'éviter que des informations sensibles contenues dans les fichiers soient accessibles par tout le monde et évite une diffusion de ses données et évite que des hackers puissent s'en servir contre des clients pour leur soutirer de l'argent.
- c) Les autorisations RWDNL sur un serveur FTP définissent les actions qu'un utilisateur peut effectuer sur les fichiers et répertoires :

R pour read : lire ou télécharger un fichier depuis le serveur.

W pour write : écrire ou téléverser un fichier sur le serveur.

D pour delete : supprimer des fichiers ou des répertoires.

N pour rename : renommer des fichiers ou des répertoires.

L pour list : lister les fichiers et répertoires sur le serveur.

Ces droits sont appelés permissions utilisateur. Les permissions utilisateur servent à définir et contrôler les actions qu'un utilisateur peut effectuer sur un système, un fichier ou une ressource. Dans le contexte d'un serveur FTP, elles définissent qui peut lire, écrire, supprimer ou gérer les fichiers et répertoires.

- d) Les droits ne sont pas spécifiques au service FTP. Ils reflètent une logique universelle de gestion des permissions dans les systèmes informatiques.

Systèmes de fichiers (OS)

Exemples : Windows et Linux.

Droits équivalents :

R : Lire un fichier ou un répertoire.

W : Modifier ou créer des fichiers.

X : Exécuter un fichier ou accéder à un répertoire (Linux).

D : Supprimer un fichier ou un répertoire.

List : Lister le contenu d'un répertoire.

Ces droits gèrent les accès utilisateur dans des environnements partagés.

Bases de données

Exemple : PostgreSQL.

Droits équivalents :

SELECT : Lire les données.

INSERT : Ajouter ou modifier des données.

DELETE : Supprimer des données.

RENAME : Renommer des tables ou des colonnes.

SHOW : Lister les bases, tables ou colonnes.

Les permissions permettent un contrôle précis des interactions des utilisateurs avec les données.

Partage de fichiers en réseau

Exemple : SMB.

Droits équivalents :

Lecture seule : Accéder aux fichiers partagés.

Lecture/Écriture : Modifier ou ajouter des fichiers.

Supprimer : Effacer des fichiers partagés.

Lister le contenu : Voir les fichiers disponibles dans un dossier partagé.

Ces droits sont courants pour les ressources partagées au sein d'un réseau local ou d'une organisation.

Applications web et cloud

Exemple : Google Drive.

Droits équivalents :

Lecture : Consulter les fichiers ou documents.

Édition : Modifier ou créer des fichiers.

Suppression : Supprimer des fichiers.

Partage : Gérer les droits d'accès pour d'autres utilisateurs.

Ces permissions sont utilisées pour la collaboration et la gestion des droits d'accès au contenu.

Contrôle d'accès dans les systèmes d'information

Exemple : Active Directory.

Droits équivalents :

Accès en lecture : Consulter les informations d'un utilisateur ou d'un groupe.

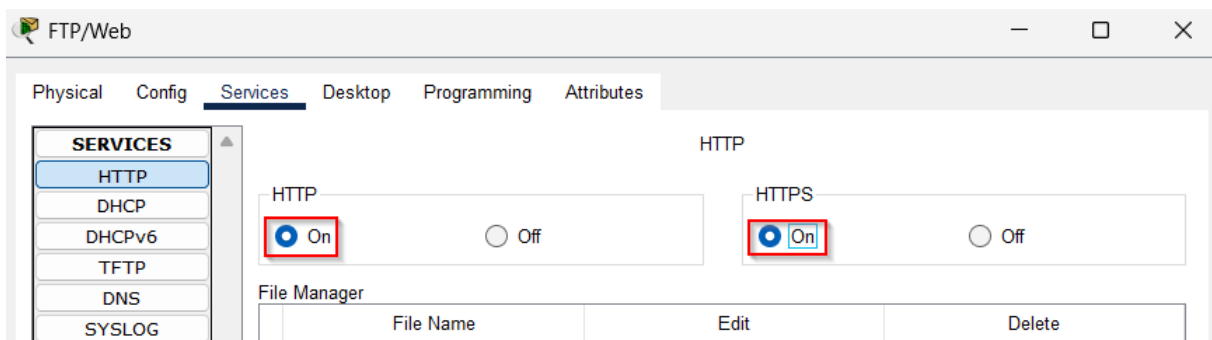
Modification : Mettre à jour les attributs des utilisateurs.

Suppression : Supprimer des comptes ou des groupes.

Ces droits gèrent l'authentification et les autorisations dans une organisation.

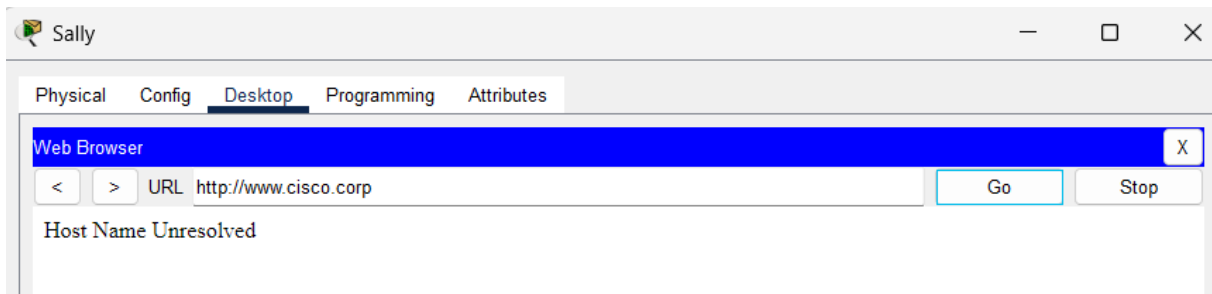
Configurer le serveur web :

Activer le service http :

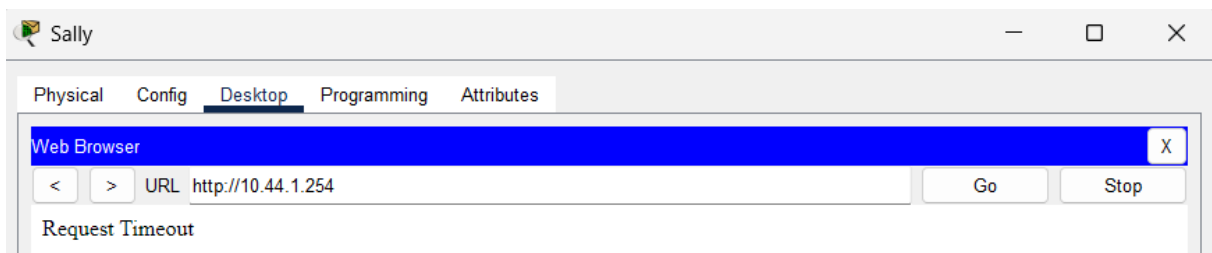


J'active les options HTTP et HTTPS en sélectionnant "On" pour chacune. Cela permet de prendre en charge les connexions HTTP et HTTPS pour les services web. Activer HTTPS est particulièrement important pour sécuriser les communications via un chiffrement SSL/TLS.

1.2 Vérifier le service http :

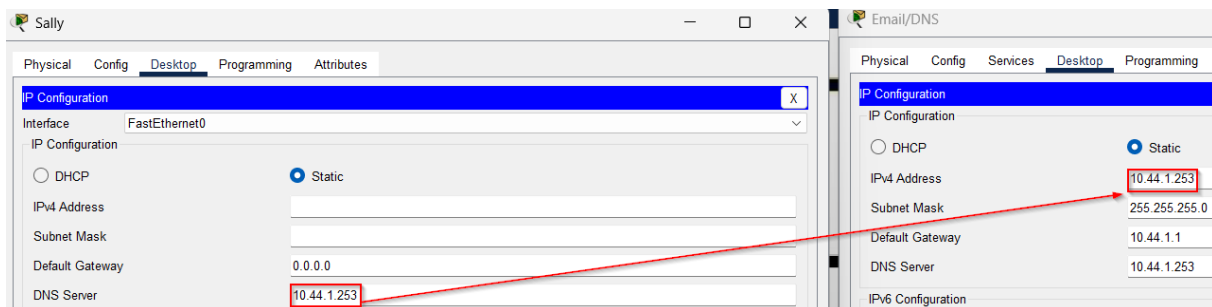


J'essaie d'accéder à l'URL `http://www.cisco.corp`, mais le message "Host Name Unresolved" s'affiche. Cela signifie que le serveur DNS n'est pas configuré ou qu'il ne peut pas résoudre le nom de domaine en adresse IP.



J'entre l'adresse IP `10.44.1.254` dans le navigateur, mais je reçois un message "Request Timeout". Cela indique que la connexion à cette adresse IP échoue, probablement en raison d'un problème de configuration réseau ou d'un service inactif à cette adresse.

a)

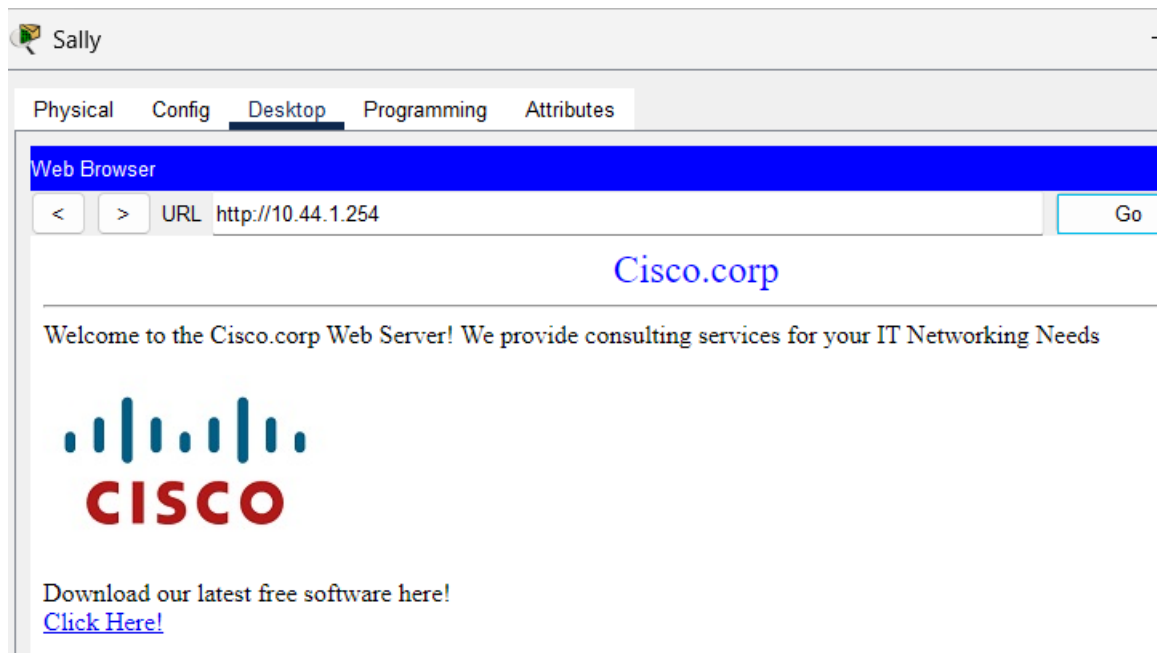


L'adresse DNS par défaut est bien la même que celle du serveur DNS. Mais Sally n'a pas de passerelle par défaut ni d'adresse IP.

```
C:\>ipconfig /renew

IP Address.....: 10.44.1.4
Subnet Mask.....: 255.255.255.0
Default Gateway...: 10.44.1.1
DNS Server.....: 10.44.1.253
```

`Ipconfig /renew` permet de renouveler l'adresse IP, le masque de sous-réseau, la passerelle par défaut et le serveur DNS.



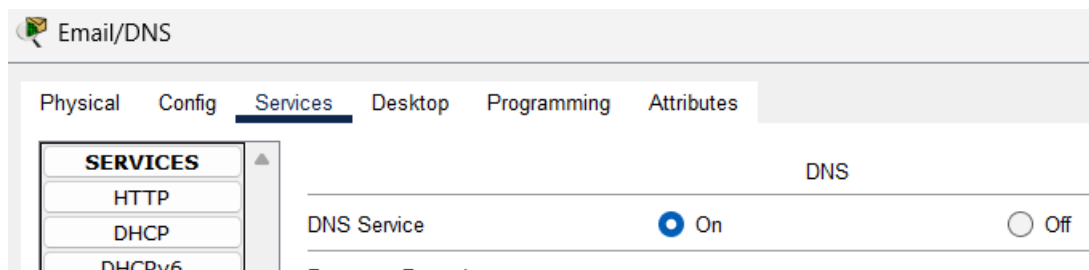
J'accède au serveur web en utilisant l'URL `http://10.44.1.254`. La page s'affiche correctement, confirmant que le service HTTP est actif et que la configuration réseau est correcte.

Evaluation :

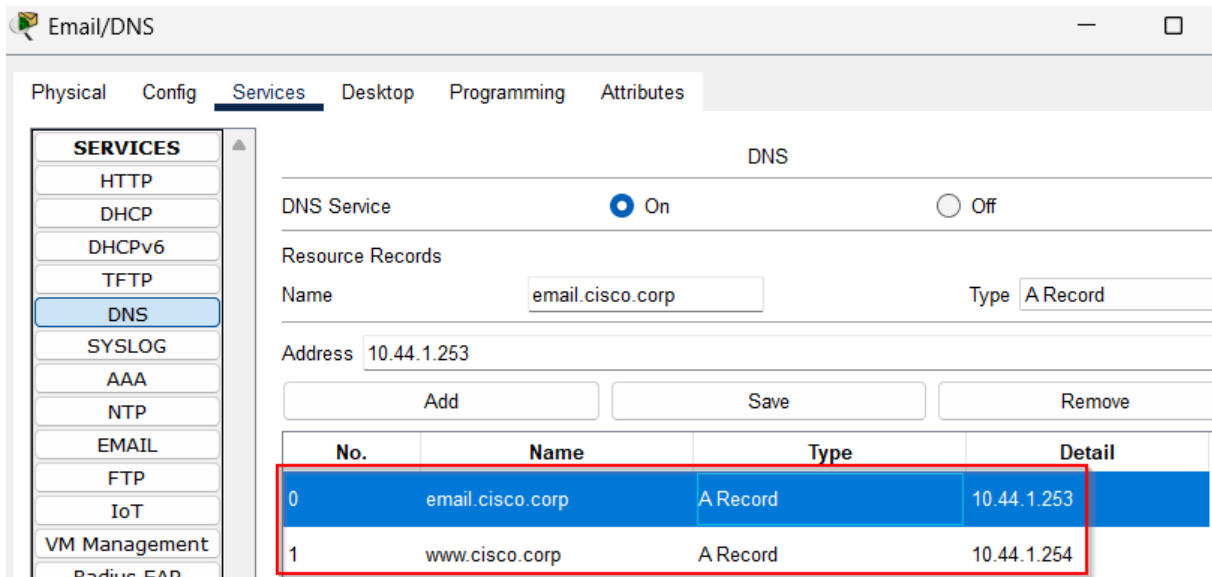
a) Les serveurs FTP/Web, Email/DNS et NTP/AAA sont sur le même réseau, une attaque sur un serveur pourrait se propager facilement aux autres. Il faudrait les segmenter pour éviter que les hackers aient accès à tous les serveurs au lieu d'un seul s'ils sont séparés.

Il n'y a pas de serveur redondant des services FTP/Web, Email/DNS et NTP/AAA pour une disponibilité en cas de panne de l'un des serveurs.

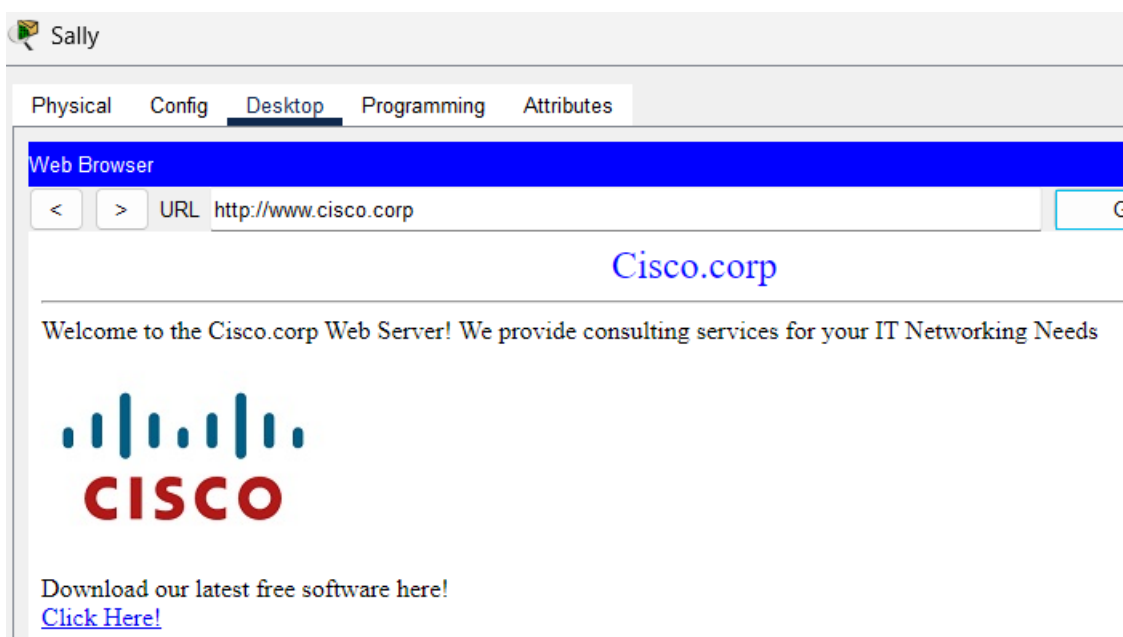
1.3 Configurer le serveur DNS :



J'active le service DNS en sélectionnant l'option "On". Ça permet de résoudre les noms de domaine en adresses IP. Cette activation est essentielle pour que les noms comme "www.cisco.corp" puissent être traduits en adresses réseau.



Je configure deux enregistrements DNS . Le premier associe le nom email.cisco.corp à l'adresse IP 10.44.1.253. Le second relie www.cisco.corp à l'adresse IP 10.44.1.254. Ces enregistrements permettent de rediriger les requêtes DNS vers les adresses IP appropriées pour accéder aux services correspondants.



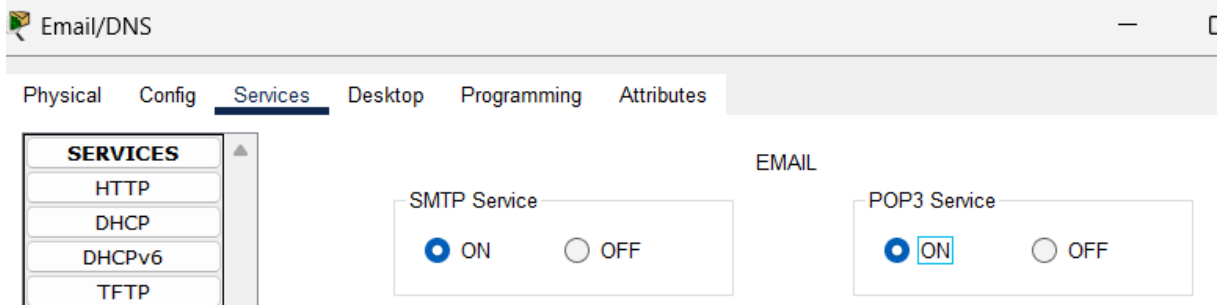
Je teste l'URL http://www.cisco.corp après la configuration DNS. La page s'affiche correctement, confirmant que le serveur DNS fonctionne bien et que le nom de domaine est résolu en adresse IP. Cela prouve que la configuration DNS est tout à fait opérationnelle.

a) On a fait le lien entre le nom de domaine et l'adresse IP 10.44.1.254 Le DNS comprends que 10.44.1.254 et doit amener au même endroit.

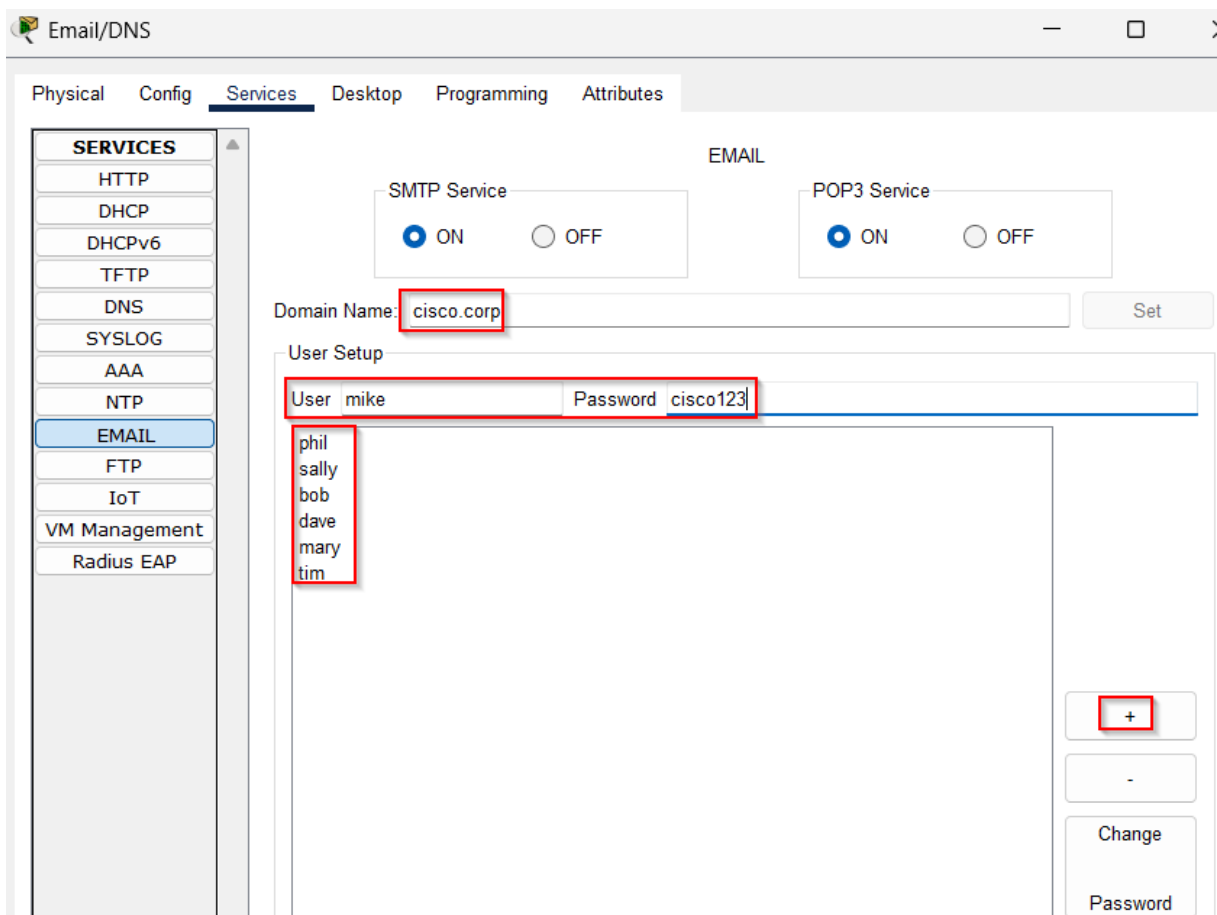
b) Le service DNS traduit les noms de domaine en adresses IP pour permettre la communication sur un réseau.

c) Metropolis Bank peut se servir du DNS pour que ce soit plus facile à écrire et à retenir pour arriver sur les sites voulu plus rapidement.

Configuration du serveur messagerie :

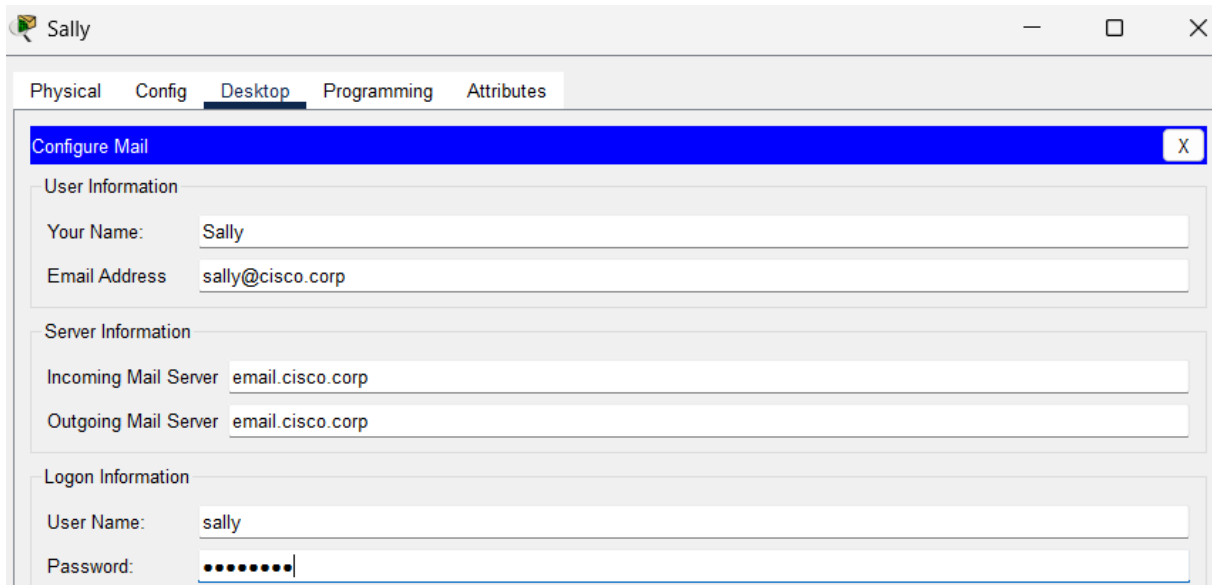


J'active les services SMTP et POP3 en sélectionnant "ON" pour les deux. Le service SMTP permet d'envoyer des emails, tandis que POP3 est utilisé pour recevoir les messages. Ces services sont nécessaires pour configurer une communication email complète au sein du réseau.



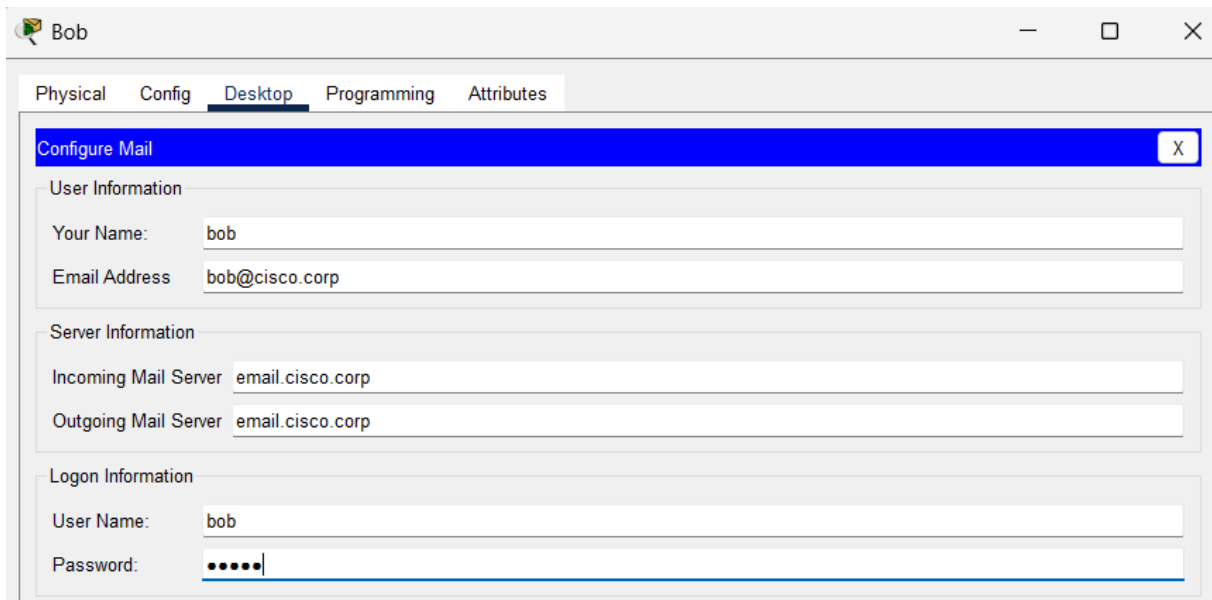
Je configure le service email. J'ajoute le nom de domaine cisco.corp et je crée un utilisateur "mike" avec le mot de passe "cisco123". En cliquant sur le bouton "+" après avoir entré ces

informations, j'ajoute cet utilisateur à la liste. Cette configuration permet à plusieurs utilisateurs d'avoir des comptes email personnalisés liés au domaine.



The screenshot shows a window titled 'Sally' with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, and a 'Configure Mail' dialog box is open. The dialog has three sections: 'User Information', 'Server Information', and 'Logon Information'. In 'User Information', 'Your Name' is 'Sally' and 'Email Address' is 'sally@cisco.corp'. In 'Server Information', both 'Incoming Mail Server' and 'Outgoing Mail Server' are 'email.cisco.corp'. In 'Logon Information', 'User Name' is 'sally' and 'Password' is masked with dots.

Je configure un client email pour Sally. J'entre son nom, son adresse email (sally@cisco.corp), ainsi que les informations des serveurs entrant (POP3) et sortant (SMTP), tous deux configurés à email.cisco.corp. Enfin, je renseigne le nom d'utilisateur "sally" et son mot de passe. Cela permet à Sally d'envoyer et de recevoir des emails via le domaine configuré.



The screenshot shows a window titled 'Bob' with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, and a 'Configure Mail' dialog box is open. The dialog has three sections: 'User Information', 'Server Information', and 'Logon Information'. In 'User Information', 'Your Name' is 'bob' and 'Email Address' is 'bob@cisco.corp'. In 'Server Information', both 'Incoming Mail Server' and 'Outgoing Mail Server' are 'email.cisco.corp'. In 'Logon Information', 'User Name' is 'bob' and 'Password' is masked with dots.

Je configure le client email pour Bob. Les étapes sont similaires : je saisis son nom, son adresse email (bob@cisco.corp), les informations des serveurs email (entrant et sortant) et ses identifiants de connexion. Cette configuration assure que Bob peut également utiliser son compte pour gérer ses emails.

a) Pour activer un service de messagerie, on doit utiliser SMTP et POP3, car ces deux protocoles ont des rôles différents mais complémentaires. SMTP sert à envoyer les emails, que ce soit entre un client (comme un PC) et le serveur ou entre plusieurs serveurs de messagerie. De son côté, POP3 permet de récupérer les emails reçus en les téléchargeant depuis le serveur vers le client. Par exemple, dans une entreprise comme Metropolis Bank, un employé utilise SMTP pour envoyer un email à un collègue, et POP3 pour lire les emails qu'il a reçus. Donc, les deux protocoles sont indispensables pour que le service fonctionne correctement.

b) SMTP et POP3 ne sont pas les seuls protocoles utilisés pour gérer les emails.

IMAP permet de lire les messages directement sur le serveur sans les télécharger,

SSL/TLS sécurisent les connexions entre le client et le serveur en chiffrant les données.

SPF vérifier que l'email provient d'un serveur autorisé par le propriétaire du domaine.

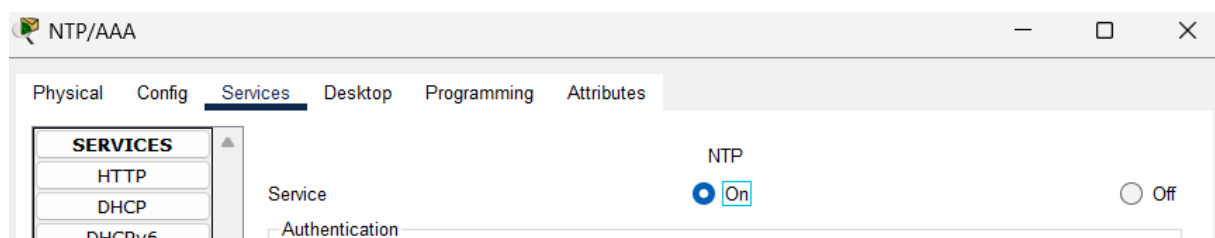
DKIM ajoute une signature numérique à chaque email pour garantir qu'il n'a pas été altéré pendant son envoi.

DMARC combine SPF et DKIM pour renforcer la sécurité et éviter les attaques de type phishing ou usurpation d'identité.

Chaque protocole a donc un rôle bien précis pour garantir une gestion complète et sécurisée des emails.

c) Metropolis Bank peut utiliser les mails pour envoyer une confirmation de transaction à son client lors d'un transfert de banque.

1.4 Configuration du serveur NTP :



J'active le service NTP (Network Time Protocol) en sélectionnant "On".

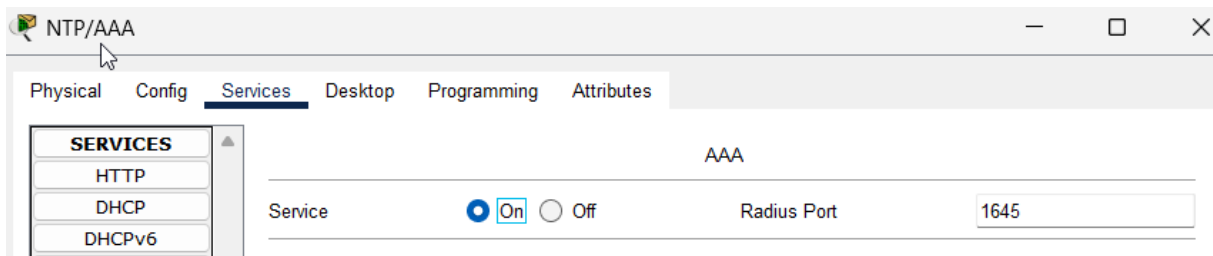
a) NTP (Network Time Protocol) échange de données temporelles (comme l'heure), corrige des décalages et synchronise les appareils. Il permet de synchroniser l'heure exacte entre les équipements réseau et les serveurs.

AAA (Authentication, Authorization, Accounting) : Service qui contrôle l'accès des utilisateurs en vérifiant leur identité, en définissant leurs permissions, et en enregistrant leurs activités.

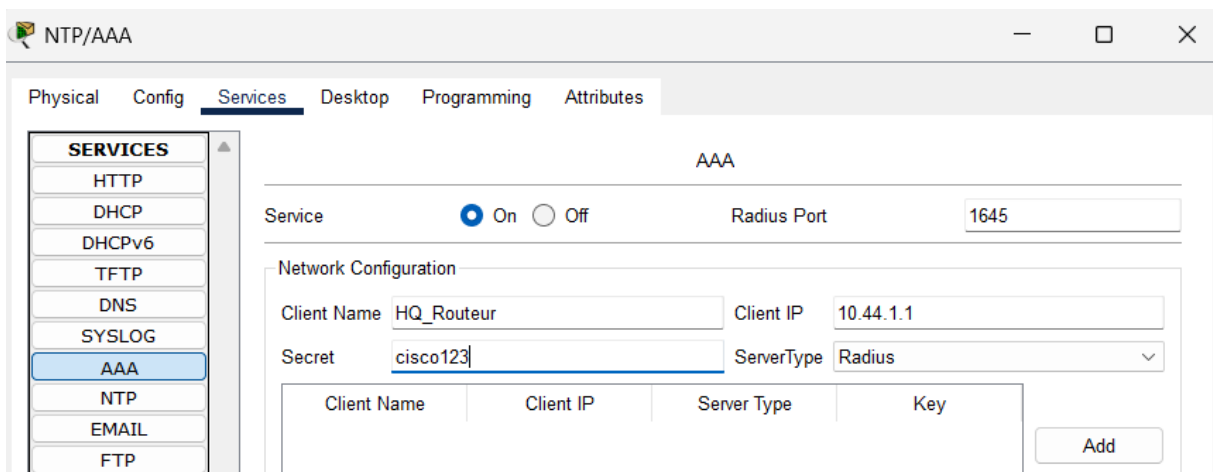
b) Le service NTP peut être utilisé pour synchroniser l'horloge de son ordinateur ou de ses appareils connectés avec un serveur de temps précis. Cela est particulièrement utile lors de soumissions de devoirs ou d'examens en ligne, où les délais sont stricts et basés sur une heure précise. Une horloge non synchronisée pourrait entraîner un retard injustifié ou des problèmes d'enregistrement, ce que NTP permet d'éviter en assurant une exactitude temporelle.

Le service AAA permet d'accéder en toute sécurité à une plateforme éducative en ligne. Lorsqu'il se connecte, le système vérifie son identité (authentification) à l'aide de ses identifiants, détermine les ressources auxquelles il a droit (autorisation), comme les cours ou documents liés à sa filière, et enregistre toutes ses activités (accounting), comme les dates de connexion et les actions effectuées. Ce processus garantit une sécurité renforcée et une traçabilité complète des interactions sur la plateforme.

1.5 Configurer le serveur AAA :



J'active le service AAA en sélectionnant "On". Je configure également le port RADIUS sur 1645, qui est le port standard utilisé pour les communications avec un serveur RADIUS. Cette configuration prépare le système à utiliser un serveur RADIUS pour gérer l'authentification et l'autorisation des utilisateurs.



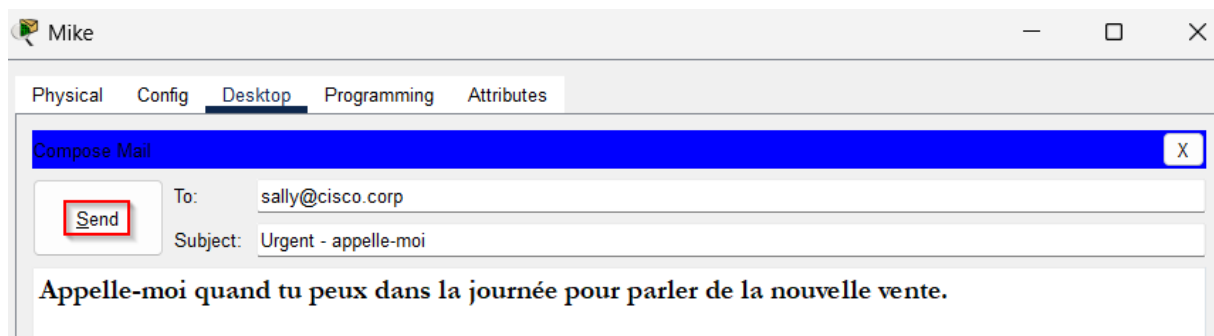
Je configure les paramètres réseau pour le service AAA. Je définis le nom du client comme "HQ_Routeur", l'adresse IP du client sur 10.44.1.1, et le type de serveur sur "Radius". Je spécifie également une clé secrète "cisco123" pour sécuriser les échanges entre le serveur et le client. Enfin, en cliquant sur "Add", j'enregistre ces paramètres pour permettre au serveur AAA de gérer l'authentification des utilisateurs à partir de ce routeur.

- a) Le service AAA (Authentication, Authorization, Accounting) gère l'accès sécurisé aux systèmes en vérifiant l'identité des utilisateurs, leurs permissions, et en traçant leurs actions.
- b) Associer AAA à un serveur de messagerie garantit une gestion sécurisée et centralisée des accès aux comptes de messagerie. Cela permet d'authentifier les utilisateurs avant qu'ils n'accèdent à leurs e-mails, de limiter les actions autorisées (par exemple, en fonction du rôle ou de l'appareil), et d'enregistrer toutes les activités (comme l'envoi ou la consultation d'e-mails), renforçant ainsi la traçabilité et la sécurité des communications.
- c) Metropolis Bank peut utiliser AAA avec son serveur de messagerie pour garantir que seuls les employés autorisés accèdent à leur boîte professionnelle. Par exemple, un conseiller bancaire peut se connecter uniquement depuis les appareils approuvés par la politique de sécurité de la banque.

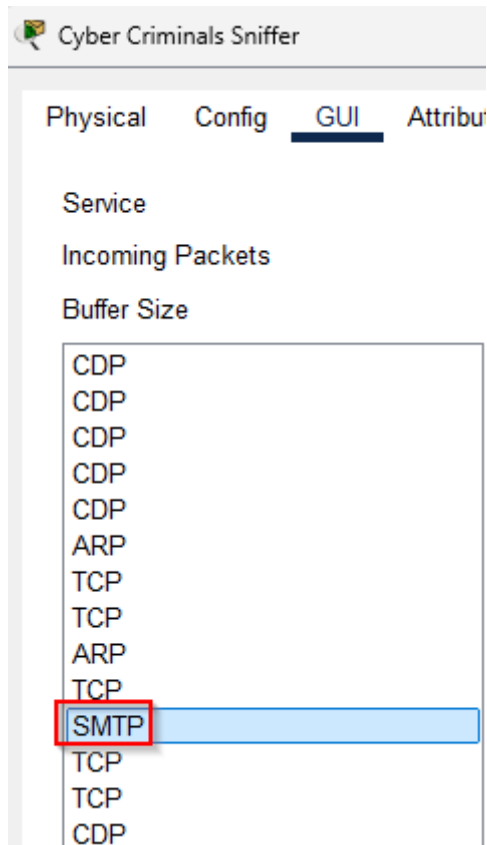
2. Second PKA :

1.6 Charger des fichiers à l'aide du FTP

Envoie de mail entre utilisateurs :



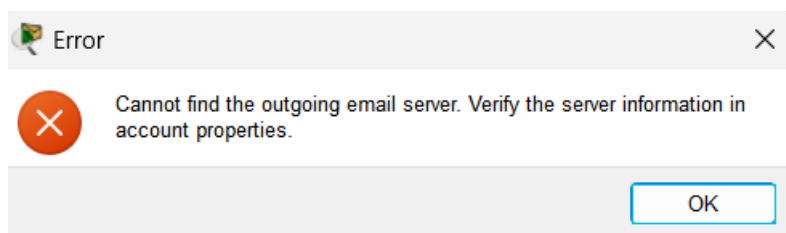
Dans cette capture, l'utilisateur Mike rédige un email adressé à Sally (sally@cisco.corp) avec pour objet "Urgent - appelle-moi" et un message demandant à être contacté. En cliquant sur "Send", il tente d'envoyer ce message.



Le protocole utilisé pour l'envoi est SMTP. On le voit en utilisant l'analyseur de trafic Cyber Criminal Sniffer sur le port 1. Mais sur le mail de Sally on voit que c'est le POP3 qui est utilisé :

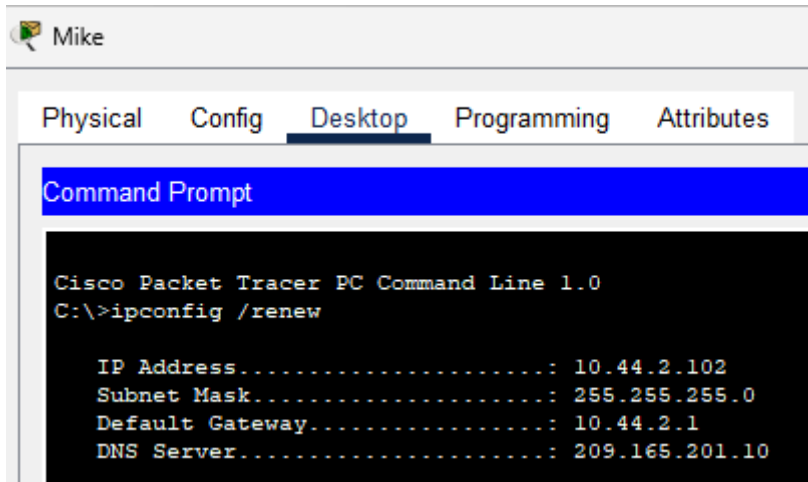
```
Receiving mail from POP3 Server email.cisco.corp
DNS resolving. Resolving name: email.cisco.corp by querying to DNS Server:
10.44.1.253 DNS resolved ip address: 10.44.1.253
Receive Mail Success.
```

Ce message confirme que le serveur POP3 (email.cisco.corp) a bien résolu l'adresse IP via le DNS (10.44.1.253) et que le courrier a été reçu avec succès. Cela prouve que la configuration DNS et POP3 est fonctionnelle.



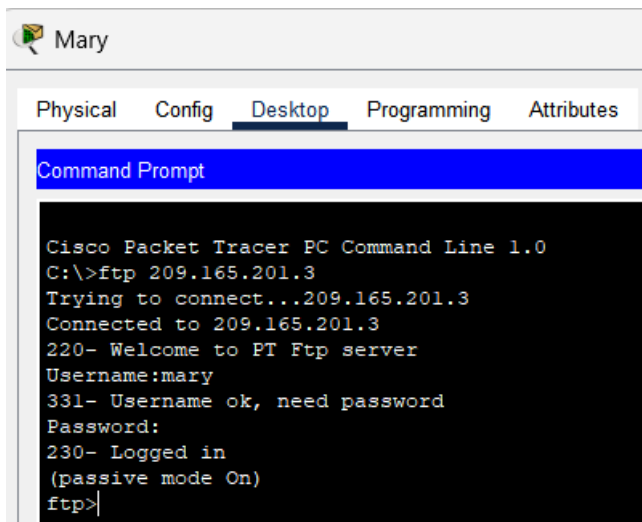
Une erreur est affichée, indiquant que le serveur d'email sortant (SMTP) ne peut pas être trouvé.

Il faut faire un ipconfig /renew sur le pc de Sally comme dans le PKA 1 et sur le PC de Mike pour donner l'adresse IP, une passerelle par défaut et un serveur DNS à jour :



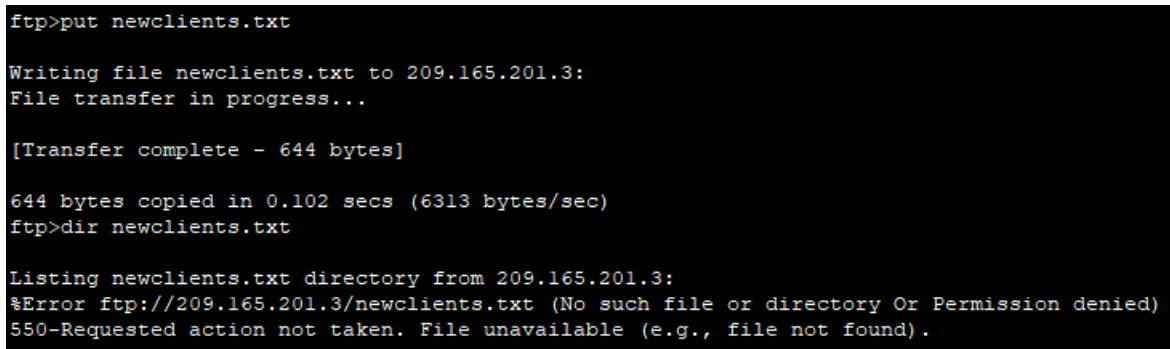
```
Mike
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /renew

IP Address.....: 10.44.2.102
Subnet Mask.....: 255.255.255.0
Default Gateway...: 10.44.2.1
DNS Server.....: 209.165.201.10
```



```
Mary
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 209.165.201.3
Trying to connect...209.165.201.3
Connected to 209.165.201.3
220- Welcome to PT Ftp server
Username:mary
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

L'utilisateur Mary se connecte à un serveur FTP situé à l'adresse IP 209.165.201.3. Après avoir saisi son nom d'utilisateur et son mot de passe, elle se connecte avec succès en mode passif. Cela permet d'accéder aux fichiers hébergés sur le serveur.



```
ftp>put newclients.txt
Writing file newclients.txt to 209.165.201.3:
File transfer in progress...

[Transfer complete - 644 bytes]

644 bytes copied in 0.102 secs (6313 bytes/sec)
ftp>dir newclients.txt
Listing newclients.txt directory from 209.165.201.3:
%Error ftp://209.165.201.3/newclients.txt (No such file or directory Or Permission denied)
550-Requested action not taken. File unavailable (e.g., file not found).
```

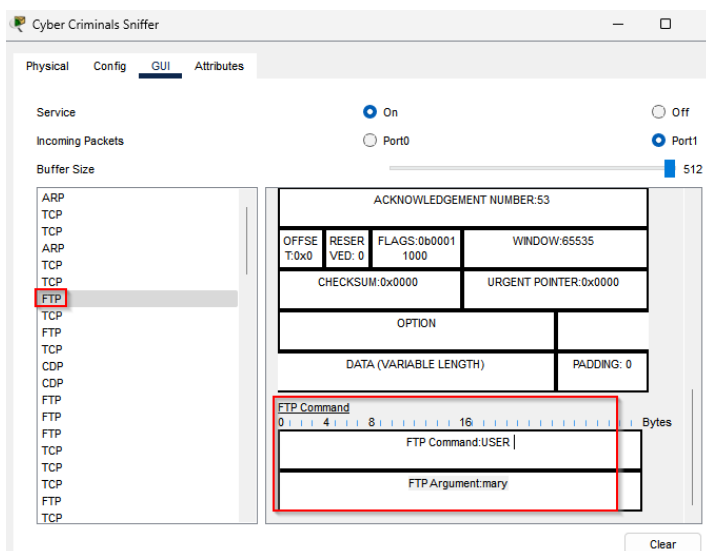

Dans cette capture, Mary transfère un fichier nommé newclients.txt vers le serveur FTP à l'adresse IP 209.165.201.3. Le transfert est complet avec 644 octets transférés. Cependant, une tentative de lister le fichier avec dir échoue avec une erreur, indiquant une permission ou une localisation incorrecte.

```
ftp>dir

Listing /ftp directory from 209.165.201.3:
 0 : BankData.txt                               1553
 1 : asa842-k8.bin                             5571584
 2 : c1841-advipservicesk9-mz.124-15.T1.bin    33591768
 3 : c1841-ipbase-mz.123-14.T7.bin            13832032
 4 : c1841-ipbasek9-mz.124-12.bin             16599160
 5 : c2600-advipservicesk9-mz.124-15.T1.bin    33591768
 6 : c2600-i-mz.122-28.bin                    5571584
 7 : c2600-ipbasek9-mz.124-8.bin              13169700
 8 : c2800nm-advipservicesk9-mz.124-15.T1.bin  50938004
 9 : c2800nm-advipservicesk9-mz.151-4.M4.bin   33591768
10 : c2800nm-ipbase-mz.123-14.T7.bin          5571584
11 : c2800nm-ipbasek9-mz.124-8.bin            15522644
12 : c2950-i6q412-mz.121-22.EA4.bin          3058048
13 : c2950-i6q412-mz.121-22.EA8.bin          3117390
14 : c2960-lanbase-mz.122-25.FX.bin           4414921
15 : c2960-lanbase-mz.122-25.SEE1.bin        4670455
16 : c2960-lanbasek9-mz.150-2.SE4.bin         4670455
17 : c3560-advipservicesk9-mz.122-37.SEE1.bin 8662192
18 : newclients.txt                           644
19 : pt1000-i-mz.122-28.bin                   5571584
20 : pt3000-i6q412-mz.121-22.EA4.bin        3117390
```

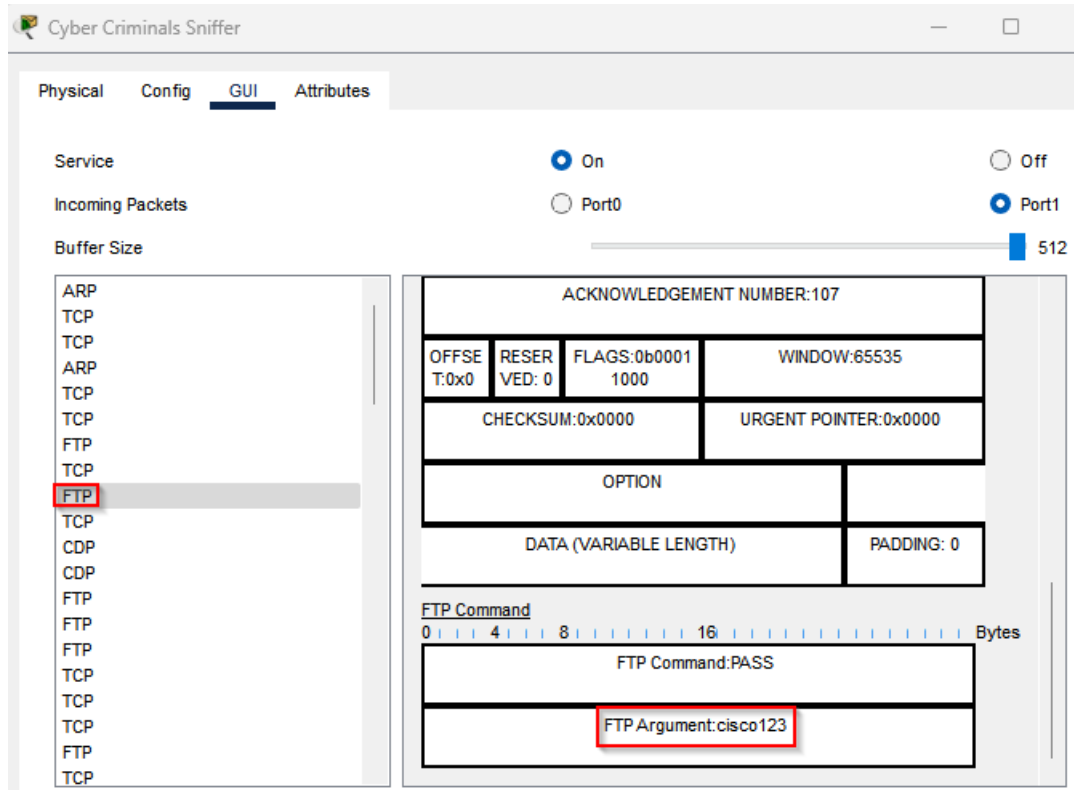
J'ai donc utilisé la commande dir pour lister le contenu du répertoire FTP. Le fichier newclients.txt apparaît correctement dans la liste avec une taille de 644 octets, confirmant que le fichier a bien été transféré et est disponible sur le serveur.

1.7 Accéder à un routeur d'entreprise à distance à l'aide de Telnet



Dans cette capture, Cyber Criminals Sniffer analyse un paquet FTP. On a capturé un paquet FTP avec USER mary.

b) Dans la commande FTP Command: USER, l'argument contient le nom d'utilisateur utilisé pour l'authentification (mary).



On peut voir dans le deuxième paquet FTP le mot de passe en clair utilisé pour se connecter à la session de mary.

1.8 Accéder à un routeur d'entreprise à distance avec Telnet :

```
C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 209.165.201.2: bytes=32 time=131ms TTL=253
Reply from 209.165.201.2: bytes=32 time=133ms TTL=253
Reply from 209.165.201.2: bytes=32 time=129ms TTL=253
Reply from 209.165.201.2: bytes=32 time=121ms TTL=253

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 121ms, Maximum = 133ms, Average = 128ms
```

La commande ping est utilisée pour tester la connectivité avec l'adresse IP 209.165.201.2. Les réponses reçues montrent que la communication est fonctionnelle, avec un temps de latence moyen de 128 ms, confirmant que le périphérique cible est accessible sur le réseau.

```
C:\>telnet 209.165.201.2
Trying 209.165.201.2 ...Open

User Access Verification

Username: admin
Password:
HQ_Router#show users
  Line      User      Host(s)      Idle      Location
*390 vty 0   admin     idle         00:00:00  209.165.201.11

  Interface  User      Mode      Idle      Peer Address
HQ_Router#
```

Ici, la commande telnet est utilisée pour établir une connexion à l'adresse IP 209.165.201.2. Une fois connecté, l'utilisateur admin s'authentifie et exécute la commande show users, qui liste les utilisateurs connectés à ce moment. Cette étape est utile pour vérifier l'activité sur le routeur et s'assurer que seuls les utilisateurs autorisés y accèdent.

1.9 Accéder à un routeur d'entreprise à distance :

```
C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 209.165.201.2: bytes=32 time=120ms TTL=253
Reply from 209.165.201.2: bytes=32 time=114ms TTL=253

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 114ms, Maximum = 120ms, Average = 117ms
```

Cette capture montre un test de connectivité avec la commande ping vers l'adresse IP 209.165.201.2. Les deux premières requêtes échouent avec un "Request timed out", tandis que les deux suivantes réussissent.

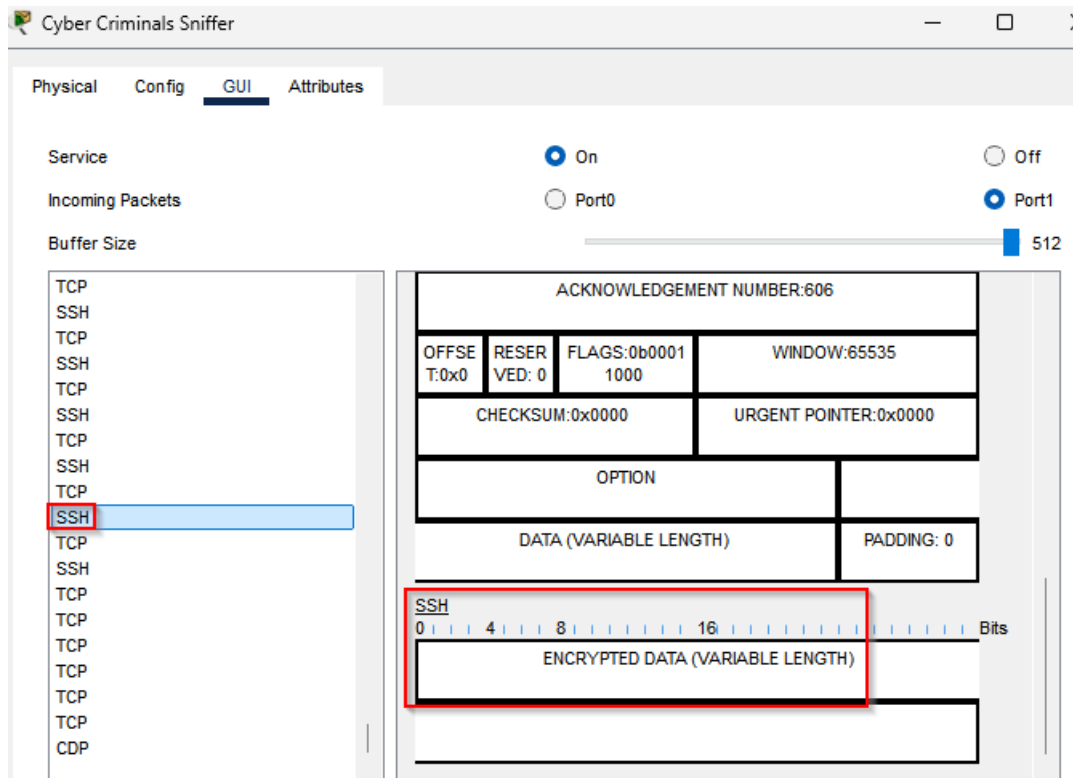
```
C:\>ssh -l admin 209.165.201.2

Password:
HQ_Router#show users
  Line      User      Host(s)      Idle      Location
 390 vty 0   admin     idle         00:02:57  209.165.201.11
*391 vty 1   admin     idle         00:00:00

  Interface  User      Mode      Idle      Peer Address
HQ_Router#
```

La commande ssh -l admin 209.165.201.2 est utilisée pour établir une connexion SSH sécurisée avec le routeur à l'adresse IP spécifiée. Après authentification avec succès, la commande show users est exécutée pour afficher les utilisateurs connectés. Cela montre deux sessions administratives actives, provenant de différentes adresses IP.

a) SSH est plus sécurisé que Telnet car tout est crypté sur le sniffer :



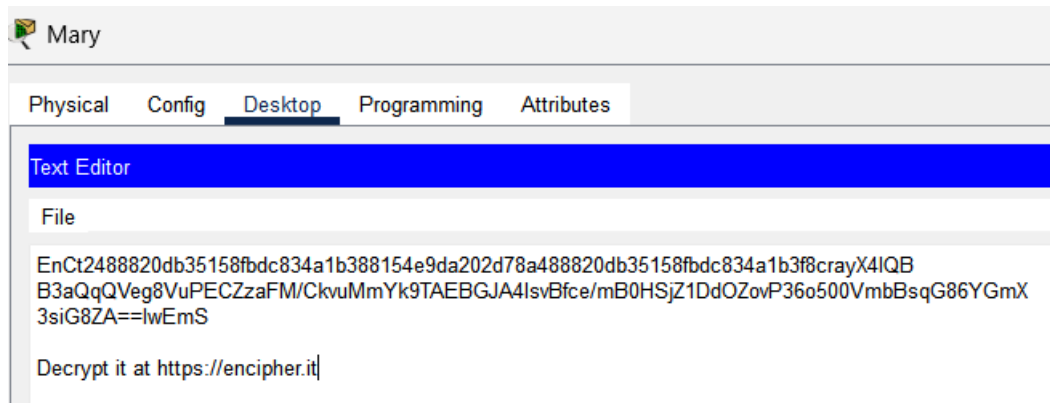
Dans cette capture, l'outil de sniffing réseau capture un paquet SSH. Contrairement au FTP, les données capturées sont chiffrées (indiquées par "ENCRYPTED DATA"). Cela démontre que SSH protège les informations sensibles, comme les identifiants et les commandes, contre l'interception.

```
HQ_Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
HQ_Router(config)#enable secret cisco
```

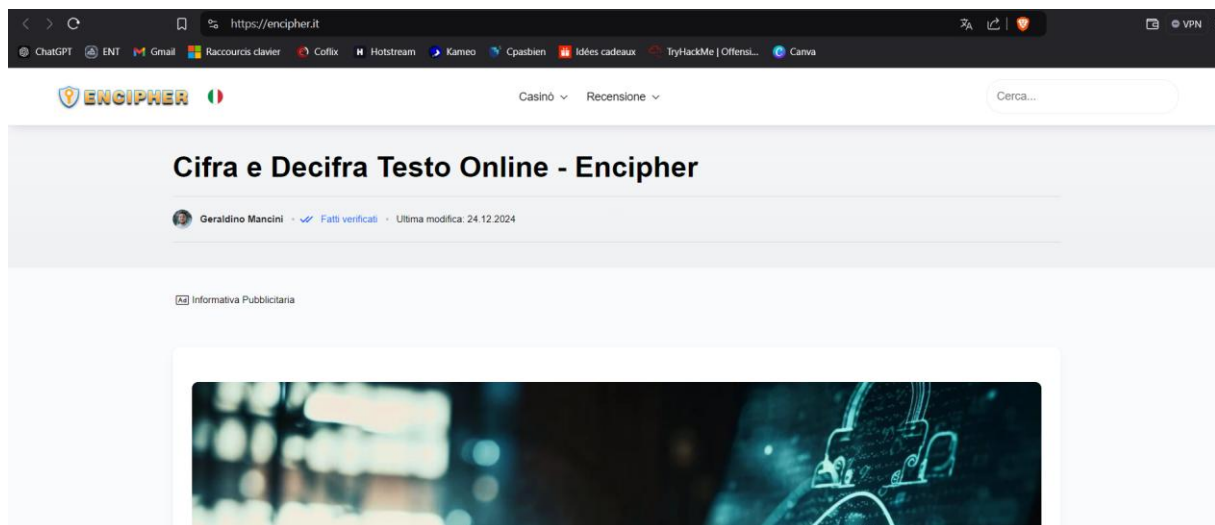
Cette capture montre une commande de configuration sur le routeur. La commande enable secret cisco est utilisée pour configurer un mot de passe chiffré pour accéder aux privilèges administratifs. Cela renforce la sécurité en empêchant l'accès non autorisé aux niveaux élevés de configuration.

3. Troisième PKA :

1.10 Localiser les informations d'identification du compte FTP de l'ordinateur portable de Mary :

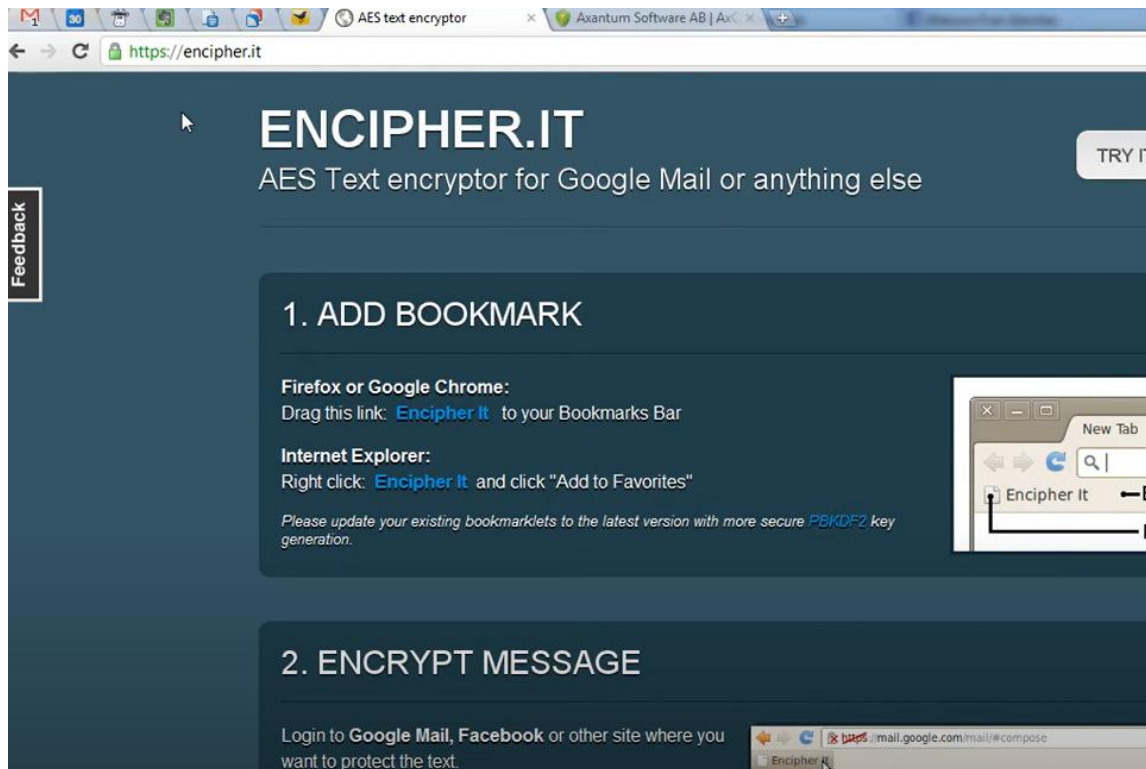


On voit le fichier crypté.



Le site renvoi a un article italien ou je sans page blanche pour coller le texte.

J'ai recherché le site et il ressemblait à ça auparavant :



Il est indiqué dans l'article que c'est du chiffrement AES :



J'ai donc cherché un site internet qui déchiffrait du AES et j'ai trouvé
<https://www.codeeeee.com/fr/encrypt/aes.html>

Codeeeee [Accueil](#) [Formatage JSON](#) [Hachage▼](#) [Encodage et décodage▼](#) [Cryptage](#)

[Accueil](#) / [Cryptage et Décryptage](#) / Cryptage et Décryptage AES

Outil de chiffrement/déchiffrement AES en ligne

Veuillez saisir le contenu à chiffrer/déchiffrer

```
EnCt2488820db35158fdbc834a1b388154e9da202d78a488820db35158fdbc834a1b3f8crayX4IQB  
B3aQqQVeg8VuPECZzaFM/CkvuMmYk9TAEBGJA4lsvBfce/mB0HSjZ1DdOZovP36o500VmbBsqG8  
6YGmX  
3siG8ZA==lwEmS
```

Mot de passe

maryftp123

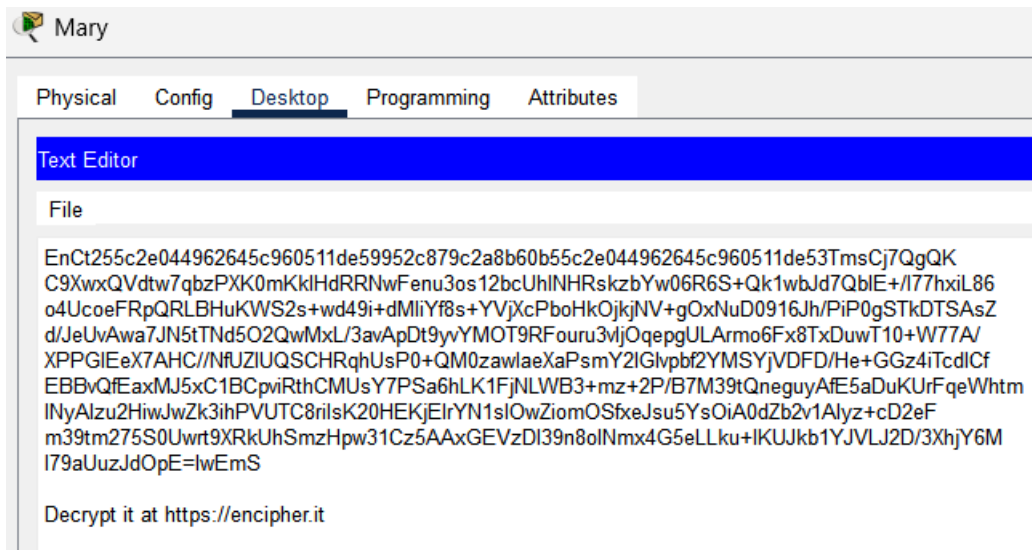
Crypter

Décrypter

Malheureusement, il affichait un message d'erreur à chaque fois que j'essayai de le décrypter :

Échec du déchiffrement, veuillez vérifier
que le texte chiffré et le mot de passe sont
corrects

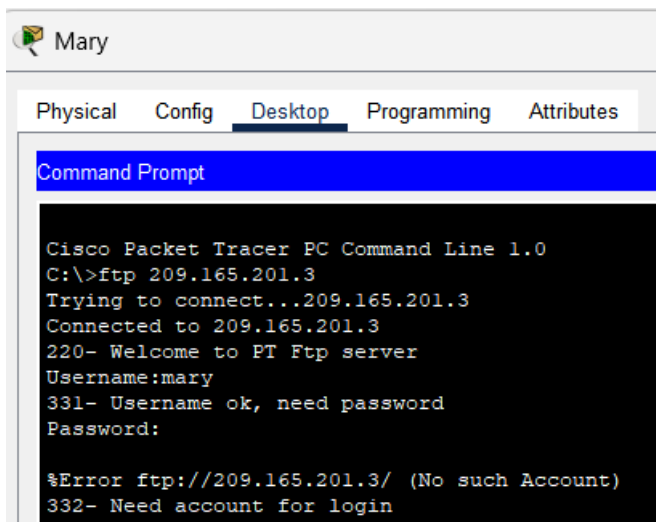
1.11 Charger des données confidentielles par FTP :



On a le même problème qu'en haut. Impossible de le déchiffrer.

a) L'hacker verrait comme dans la capture du haut, une suite de chiffres et de lettres incompréhensible. Il ne pourra donc pas lire les données.

J'ai tout de même testé avec des mots de passe courant comme cisco123 :



Sans succès.

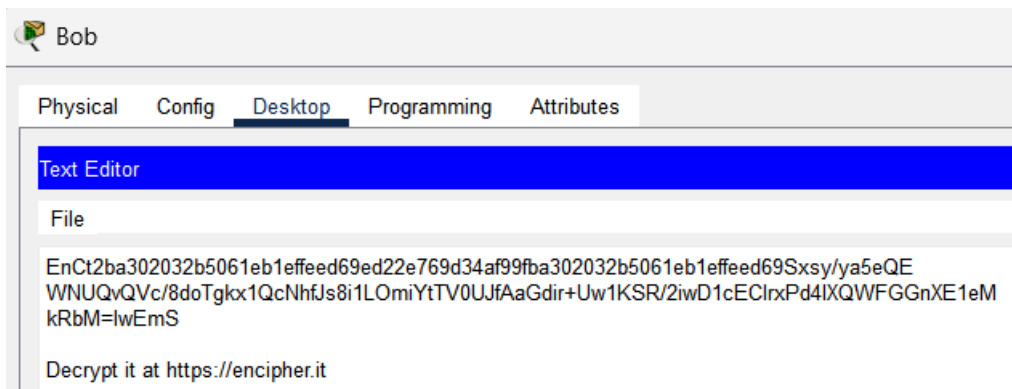
Et avec maryftp123 :


```
C:\>ftp 209.165.201.3
Trying to connect...209.165.201.3
Connected to 209.165.201.3
220- Welcome to PT Ftp server
Username:mary
331- Username ok, need password
Password:

%Error ftp://209.165.201.3/ (No such Account)
332- Need account for login
```

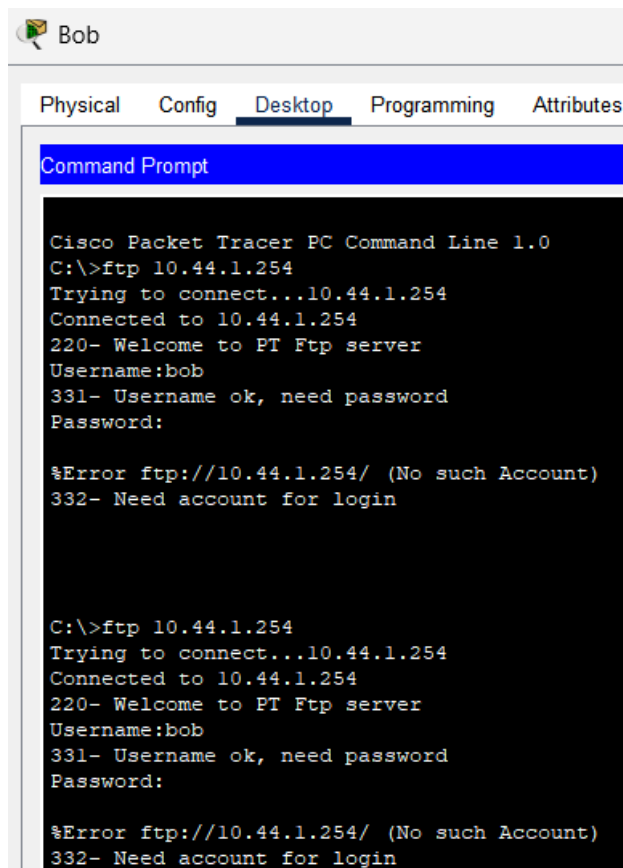
Ça ne marchait pas non plus. J'ai réussi qu'à trouvé le nom d'utilisateur (le plus simple).

1.12 Localiser les informations d'identification FTP de bob :



Il est impossible pour moi de le décrypter

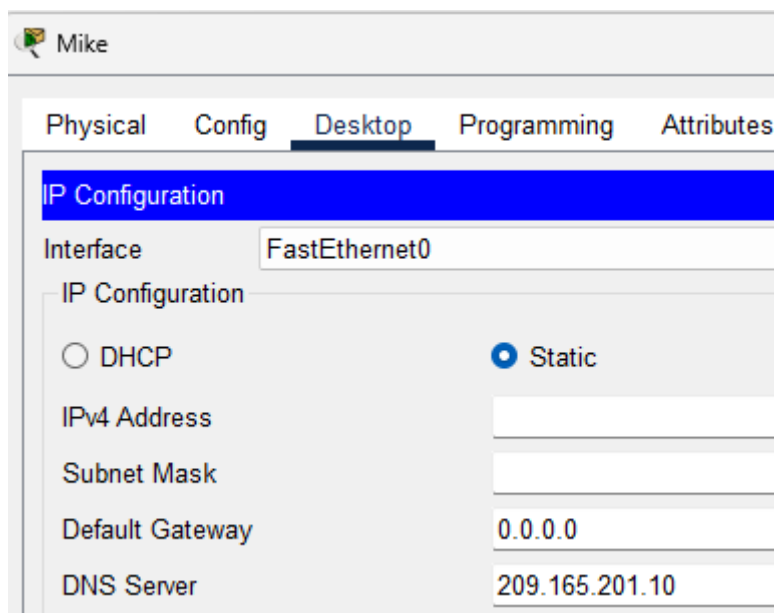
J'ai quand même essayé de me connecter sur la session ftp de bob avec les mots de passe cisco123 et bobftp123 :



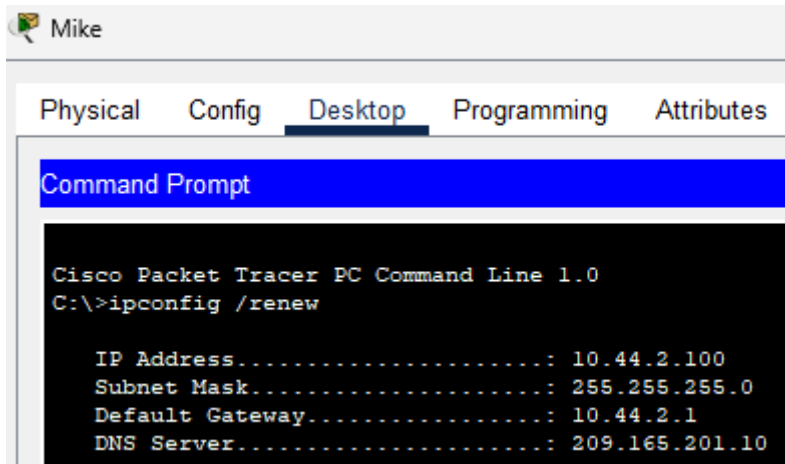
Sans succès, j'ai juste trouvé son nom d'utilisateur, ce qui est vraiment très facile.

4. Quatrième PKA :

1.13 Télécharger les fichiers clients sur le pc de Mike :



Mike n'a pas de passerelle par défaut, je vais donc utiliser la commande ipconfig /renew pour que les informations se mettent à jour :

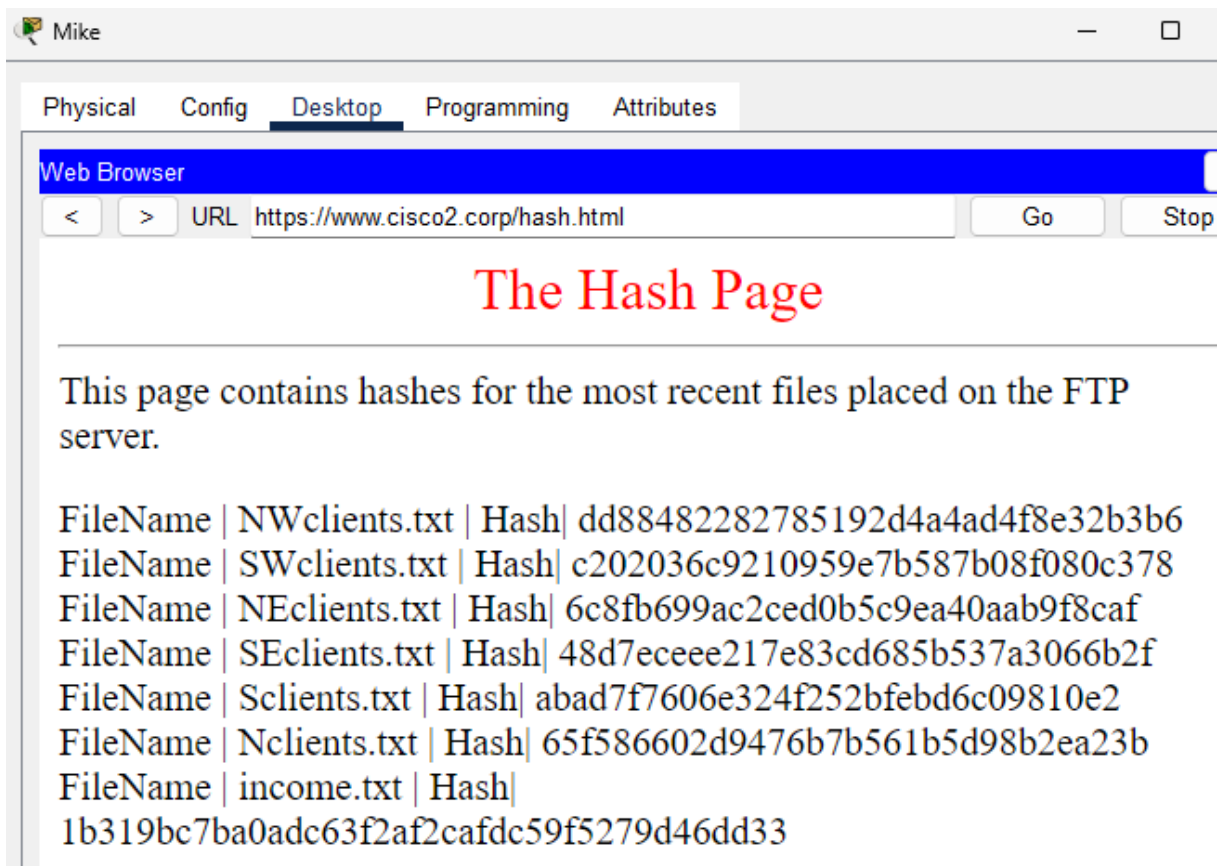


Il faut aussi faire un ipconfig /renew sur le pc de Sally pour avoir une passerelle par défaut, comme dans le PKA 1.

```
Sending mail to Sally@cisco.corp , with subject : De la plus haute importance
Mail Server: email.cisco.corp
DNS resolving. Resolving name: email.cisco.corp by querying to DNS Server:
209.165.201.10 DNS resolved ip address: 209.165.201.4
Send Success.
```

Le mail pour avertir Sally a été envoyé avec succès.

1.14 Télécharger les fichiers clients du serveur de sauvegarde des fichiers sur le pc de Mike :



Dans cette capture, une page web sur l'URL <https://www.cisco2.corp/hash.html> affiche des hachages associés aux fichiers récents placés sur le serveur FTP. Chaque fichier (par exemple, NWclients.txt) est lié à son hachage unique. Cela permet de vérifier l'intégrité des fichiers en comparant leurs hachages avant et après leur transfert.

Le protocole est https comme dans l'url.

Les noms et hashes des fichiers clients sur le serveur de sauvegarde sont :

FileName	NWclients.txt	Hash	dd88482282785192d4a4ad4f8e32b3b6
FileName	SWclients.txt	Hash	c202036c9210959e7b587b08f080c378
FileName	NEclients.txt	Hash	6c8fb699ac2ced0b5c9ea40aab9f8caf
FileName	SEclients.txt	Hash	48d7ecccc217e83cd685b537a3066b2f
FileName	Scclients.txt	Hash	abad7f7606e324f252bfebd6c09810e2

FileName | Nclients.txt | Hash| 65f586602d9476b7b561b5d98b2ea23b

FileName | income.txt | Hash| 1b319bc7ba0adc63f2af2cafde59f5279d46dd33

```
ftp>dir

Listing /ftp directory from www.cisco2.corp:
 0  : NEclients.txt                584
 1  : NWclients.txt                584
 2  : Nclients.txt                 698
 3  : SEclients.txt                 598
 4  : SWclients.txt                 650
 5  : Sclients.txt                 781
 6  : asa842-k8.bin                5571584
 7  : cl841-advipservicesk9-mz.124-15.T1.bin 33591768
 8  : cl841-ipbase-mz.123-14.T7.bin 13832032
 9  : cl841-ipbasek9-mz.124-12.bin 16599160
10  : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
11  : c2600-i-mz.122-28.bin        5571584
12  : c2600-ipbasek9-mz.124-8.bin 13169700
13  : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
14  : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
15  : c2800nm-ipbase-mz.123-14.T7.bin 5571584
16  : c2800nm-ipbasek9-mz.124-8.bin 15522644
17  : c2950-i6q412-mz.121-22.EA4.bin 3058048
18  : c2950-i6q412-mz.121-22.EA8.bin 3117390
19  : c2960-lanbase-mz.122-25.FX.bin 4414921
20  : c2960-lanbase-mz.122-25.SE1.bin 4670455
21  : c2960-lanbasek9-mz.150-2.SE4.bin 4670455
22  : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
23  : income.txt                   203
24  : pt1000-i-mz.122-28.bin       5571584
25  : pt3000-i6q412-mz.121-22.EA4.bin 3117390
```

Ici, la commande ftp dir liste le contenu du répertoire FTP situé sur www.cisco2.corp. On retrouve les fichiers mentionnés sur la page précédente, tels que NEclients.txt, NWclients.txt, etc., avec leurs tailles respectives. Cela confirme la présence des fichiers sur le serveur FTP.

```
ftp>get NEclients.txt

Reading file NEclients.txt from www.cisco2.corp:
File transfer in progress...

[Transfer complete - 584 bytes]

584 bytes copied in 0.051 secs (11450 bytes/sec)
ftp>get NWclients.txt
```

Dans cette capture, la commande ftp get est utilisée pour télécharger le fichier NEclients.txt depuis le serveur FTP. Le transfert est complété avec succès, et 584 octets sont copiés. Cela confirme que l'accès en lecture fonctionne correctement pour ce fichier.

```
1/1/1970    1:0 PM          584      NEclients.txt
1/1/1970    1:0 PM          584      NWclients.txt
1/1/1970    1:0 PM          698      Nclients.txt
1/1/1970    1:0 PM          598      SEclients.txt
1/1/1970    1:0 PM          650      SWclients.txt
1/1/1970    1:0 PM          781      Sclients.txt
2/7/2106    7:28 PM          26      sampleFile.txt

3921 bytes      7 File(s)
```

Cette capture montre une commande pour vérifier le contenu local du répertoire après les téléchargements. Les fichiers, tels que NEclients.txt et NWclients.txt, sont listés avec leurs tailles respectives, confirmant que les téléchargements ont bien été effectués et enregistrés localement.

1.15 Vérifier l'intégrité des fichiers clients avec le hash :

Online hash calculator

[Home](#) / [Online tools](#) / [Hash calculator](#)

Calculates the hash of string using various algorithms.

Grant K. Dyer|mattis.semper.duit@luctusut.edu|Est Foundation|I9Z 9AZ
Tamekah O. Petty|odio.Phasellus.at@magnatellusfaucibus.co.uk|Posuere Cubilia Limited|45-937
Adam H. Buck|sagittis@enim.edu|Pede Blandit Congue Company|647129
Calvin V. Hays|elit.a@vitaedolor.net|Nunc Nulla Vulputate LLP|00078
Zane Casey|luctus@mauris.com|Iaculis Incorporated|72240
Rudyard W. Dalton|lorem@Nuncullamcorpervelit.co.uk|Auctor Nunc PC|626714
Lamar Q. Allen|aliquet@sagittisNullamvitae.org|Et Rutrum Corp.|44736
Michelle Sloan|dolor.sit.amet@seddictum.edu|Nisi PC|00312
Haley E. Bass|nec@eu.com|Lorem Associates|00079
Larissa G. Swanson|vulputate@diamnuncullamcorper.com|Ut Limited|0626QT

Algorithm: md2 ▼

Hash this!

Result: 65f586602d9476b7b561b5d98b2ea23b

Cette capture montre l'utilisation d'un calculateur de hachage en ligne. L'utilisateur entre un texte ou un contenu pour générer son hachage à l'aide de l'algorithme sélectionné (ici, MD2). Le résultat produit (65f586602d9476b7b561b5d98b2ea23b) peut être utilisé pour vérifier l'intégrité ou la validité des données.

Hachage des fichiers :

NEclients.txt : 6c8fb699ac2ced0b5c9ea40aab9f8çaf

NWclients.txt : 8ecf9ea9fd8044b4c8568a3ed9b0fd34, ce n'est pas le même hachage que sur la capture plus haut :

Nclients.txt : 65f586602d9476b7b561b5d98b2ea23b

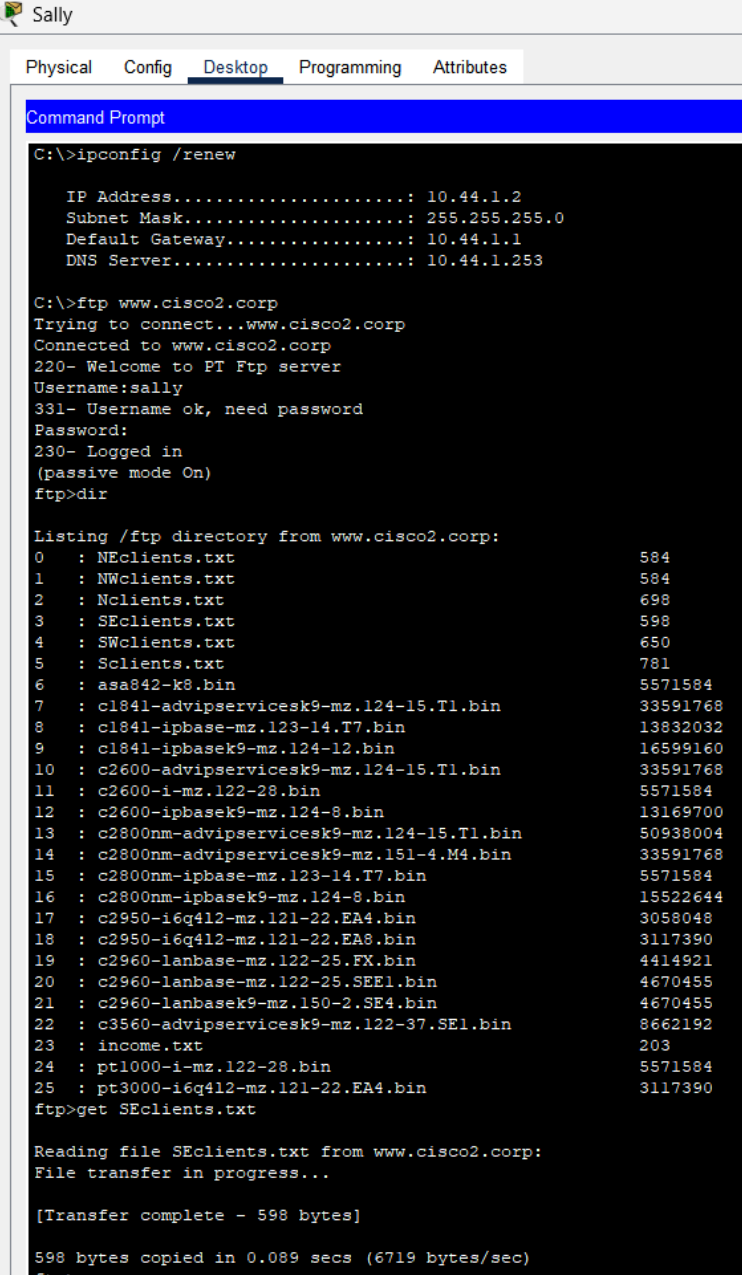
SEclients.txt : e2236dacdda7126e81af5b79d9çaa20b ce n'est pas le même hachage que sur la capture :

SWclients.txt : 815ça6a9dd4f3749334d72d4b7d99c14, ce n'est pas le même hachage que sur la capture :

FileName | SWclients.txt | Hash| c202036c9210959e7b587b08f080c378

Sclients.txt : 9d5ae45f46d266e4e7354261ed0fe3cc

Comme il y a plusieurs hachs modifier, j'ai donc pris SEclients.txt :



```
Sally
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ipconfig /renew

IP Address. . . . .: 10.44.1.2
Subnet Mask. . . . .: 255.255.255.0
Default Gateway. . . . .: 10.44.1.1
DNS Server. . . . .: 10.44.1.253

C:\>ftp www.cisco2.corp
Trying to connect...www.cisco2.corp
Connected to www.cisco2.corp
220- Welcome to PT Ftp server
Username:sally
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from www.cisco2.corp:
0  : NEclients.txt                584
1  : NWclients.txt                584
2  : Nclients.txt                698
3  : SEclients.txt                598
4  : SWclients.txt                650
5  : Sclients.txt                781
6  : asa842-k8.bin                5571584
7  : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
8  : c1841-ipbase-mz.123-14.T7.bin 13832032
9  : c1841-ipbasek9-mz.124-12.bin 16599160
10 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
11 : c2600-i-mz.122-28.bin        5571584
12 : c2600-ipbasek9-mz.124-8.bin  13169700
13 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
14 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
15 : c2800nm-ipbase-mz.123-14.T7.bin 5571584
16 : c2800nm-ipbasek9-mz.124-8.bin 15522644
17 : c2950-i6q412-mz.121-22.EA4.bin 3058048
18 : c2950-i6q412-mz.121-22.EA8.bin 3117390
19 : c2960-lanbase-mz.122-25.FX.bin 4414921
20 : c2960-lanbase-mz.122-25.SE11.bin 4670455
21 : c2960-lanbasek9-mz.150-2.SE4.bin 4670455
22 : c3560-advipservicesk9-mz.122-37.SE11.bin 8662192
23 : income.txt                  203
24 : pt1000-i-mz.122-28.bin      5571584
25 : pt3000-i6q412-mz.121-22.EA4.bin 3117390
ftp>get SEclients.txt

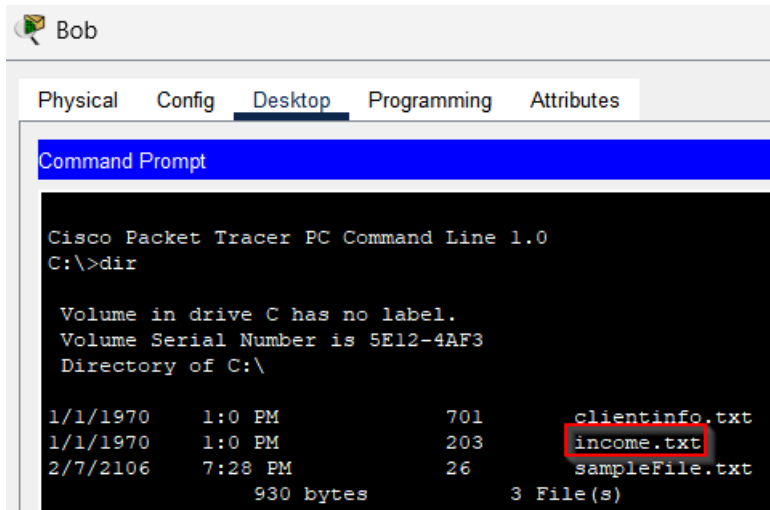
Reading file SEclients.txt from www.cisco2.corp:
File transfer in progress...

[Transfer complete - 598 bytes]

598 bytes copied in 0.089 secs (6719 bytes/sec)
ftp>
```

Je Sally renouvelle l'adresse IP de Sally avec `ipconfig /renew`, obtenant une configuration réseau correcte. Elle se connecte ensuite au serveur FTP `www.cisco2.corp` et liste les fichiers disponibles. Elle télécharge avec succès le fichier `SEclients.txt`, comme indiqué par le message de transfert complété de 650 octets.

1.16 Vérifier l'intégrité des fichiers sensibles à l'aide du HMAC :



J'utilise la commande `dir` pour afficher les fichiers dans son répertoire local. Le fichier `income.txt` est présent avec une taille de 203 octets, confirmant qu'il est accessible pour d'autres opérations, comme la vérification d'intégrité ou le traitement.

a)HMAC : 1b319bc7ba0adc63f2af2cafdc59f5279d46dd33 :

Copy-paste the string here

INCOME
2016
2015
\$
\$

Secret key

cisco123

Digest algorithm

SHA1

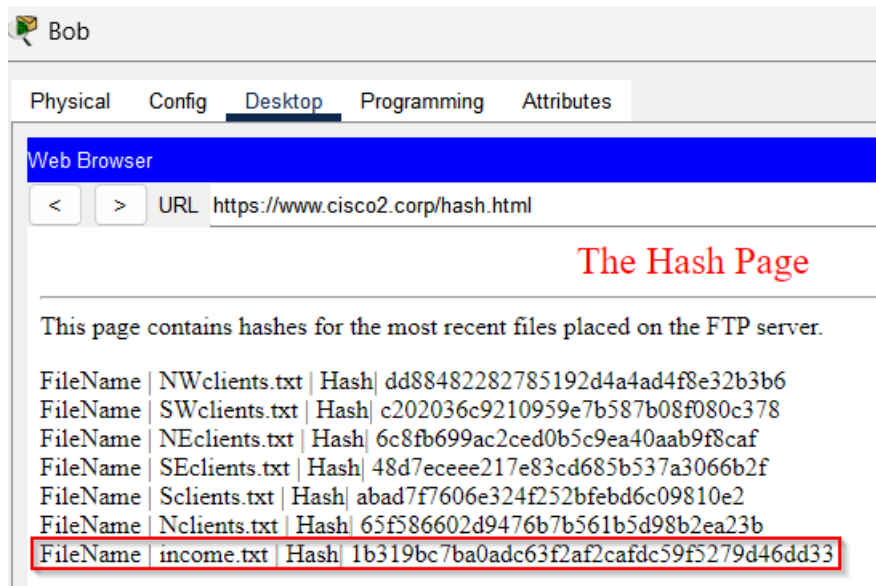
Compute HMAC

-Computed HMAC-

1b319bc7ba0adc63f2af2cafdc59f5279d46dd33

Dans cette capture, un HMAC (Hash-based Message Authentication Code) est calculé pour le contenu du fichier income.txt à l'aide de la clé secrète cisco123 et de l'algorithme SHA1. Le résultat est 1b319bc7ba0adc63f2af2cafdc59f5279d46dd33.

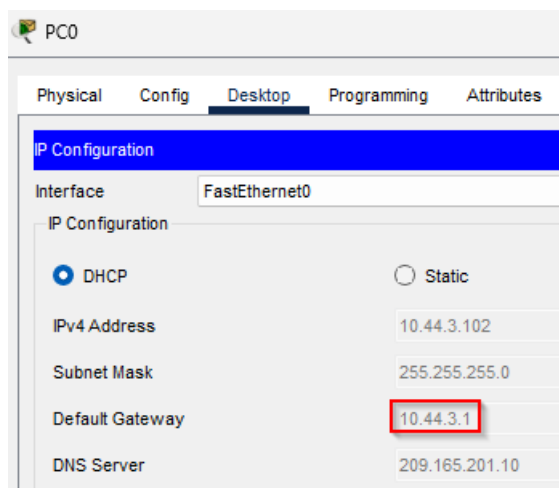
b) HMAC est plus sûr qu'un hash basique car il utilise une clé secrète en complément des données à hacher. Cette clé rend le résultat du HMAC unique et empêche un attaquant de recréer ou de manipuler le message sans la connaître, même s'il a accès à la fonction de hachage. Contrairement à un hash simple qui ne vérifie que l'intégrité des données (s'assurer qu'elles n'ont pas été modifiées), HMAC garantit également leur authenticité en prouvant qu'elles proviennent d'une source légitime, c'est-à-dire celle qui possède la clé. De plus, HMAC est résistant à des attaques comme la force brute ou les collisions, car l'ajout de la clé complique énormément le processus de falsification. Cette robustesse fait qu'HMAC est couramment utilisé dans des protocoles sécurisés comme HTTPS, VPN ou pour l'authentification des API, où l'intégrité et l'authenticité des données sont essentielles.



Le hachage correspond bien à celui qu'on a trouvé en dessus.

5. Cinquième PKA :

1.17 Configurer le WEP pour Healthcare at Home:



Dans cette capture, la configuration réseau de l'ordinateur "PC0" est définie sur DHCP. L'appareil a sa passerelle par défaut de 10.44.3.1

a)

Web Browser
URL http://10.44.3.1/Wireless_Basic.asp

Wireless-N Broadband Router

Wireless Setup Wireless Security Access Restrictions Applications & Gaming Administration
Basic Wireless Settings Wireless Security Guest Network Wireless MAC Filter

Basic Wireless Settings

Network Mode: Mixed

Network Name (SSID): Home

Radio Band: Auto

Wide Channel: Auto

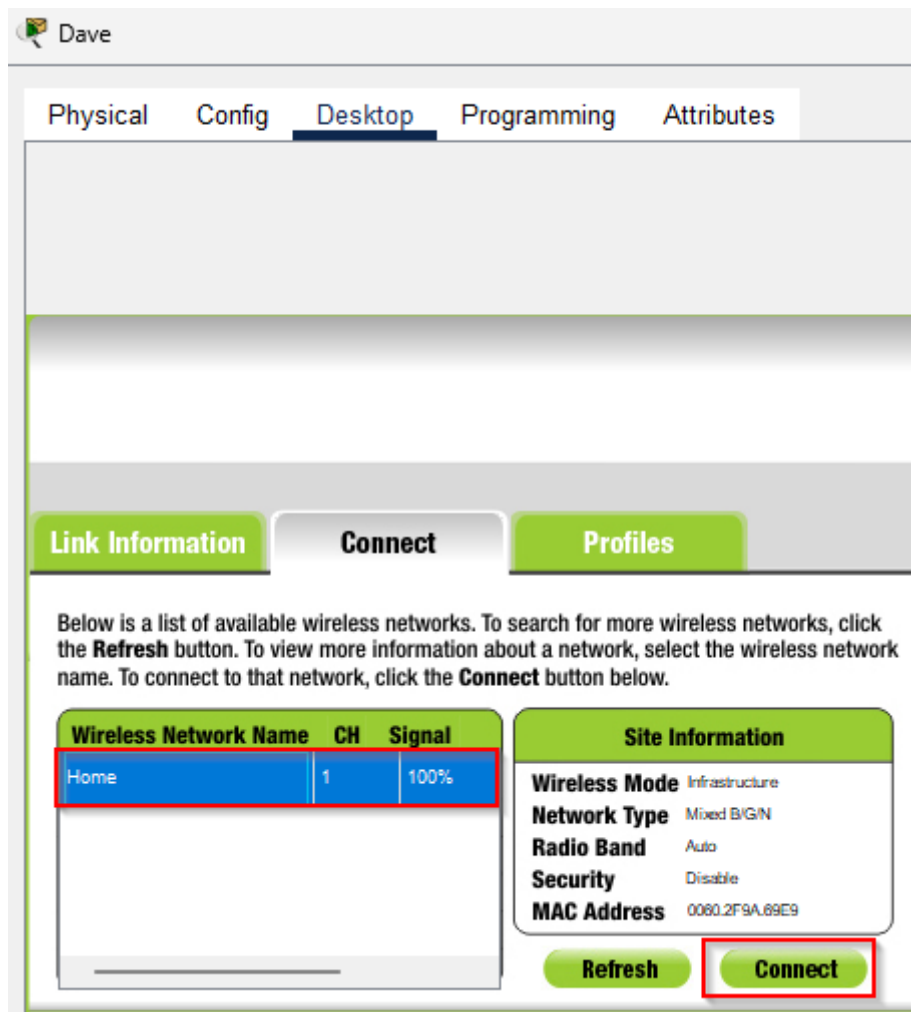
Standard Channel: 1 - 2.412GHz

SSID Broadcast: ☒ Enabled ☐ Disabled

Cette capture montre la configuration des paramètres Wi-Fi d'un routeur. Le SSID du réseau est défini sur "Home", avec le mode réseau réglé sur "Mixed" pour prendre en charge différents types de clients. Le SSID broadcast est activé (Enabled), permettant aux périphériques de détecter le réseau sans fil automatiquement. Cette configuration assure la compatibilité et la visibilité du réseau.

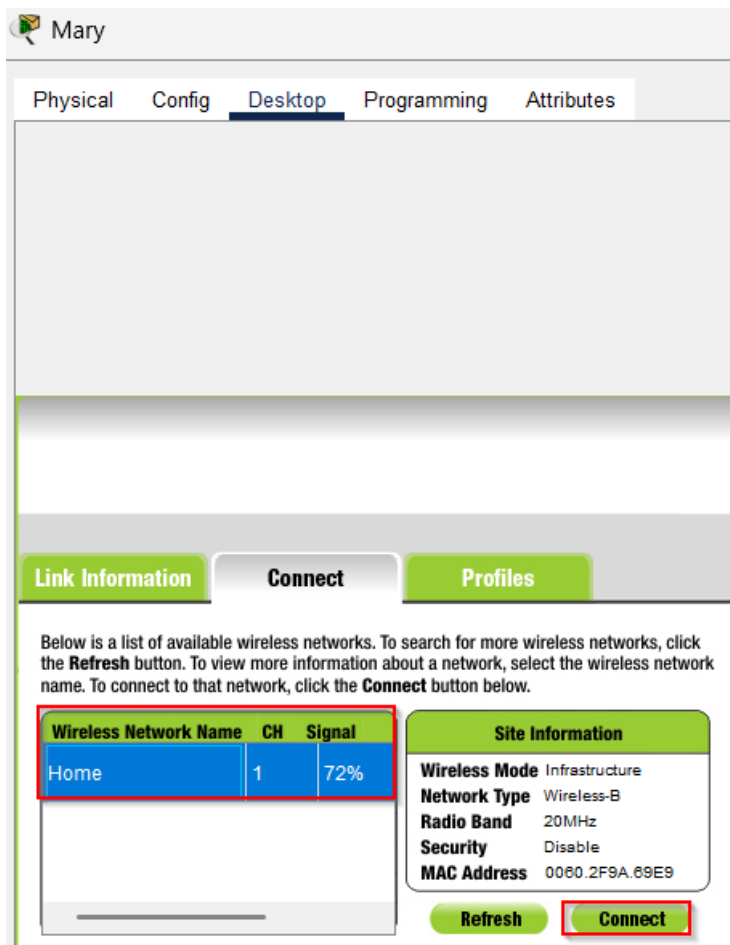
b) Le WEP utilise l'algorithme RC4 pour chiffrer les données mais les clés de chiffrement sont statiques (en analysant le trafic, on peut déduire la clé). Si une clé est compromise, tout le réseau est vulnérable tant que la clé n'est pas changée manuellement. Il est donc facile de craquer les clés.

Dave :



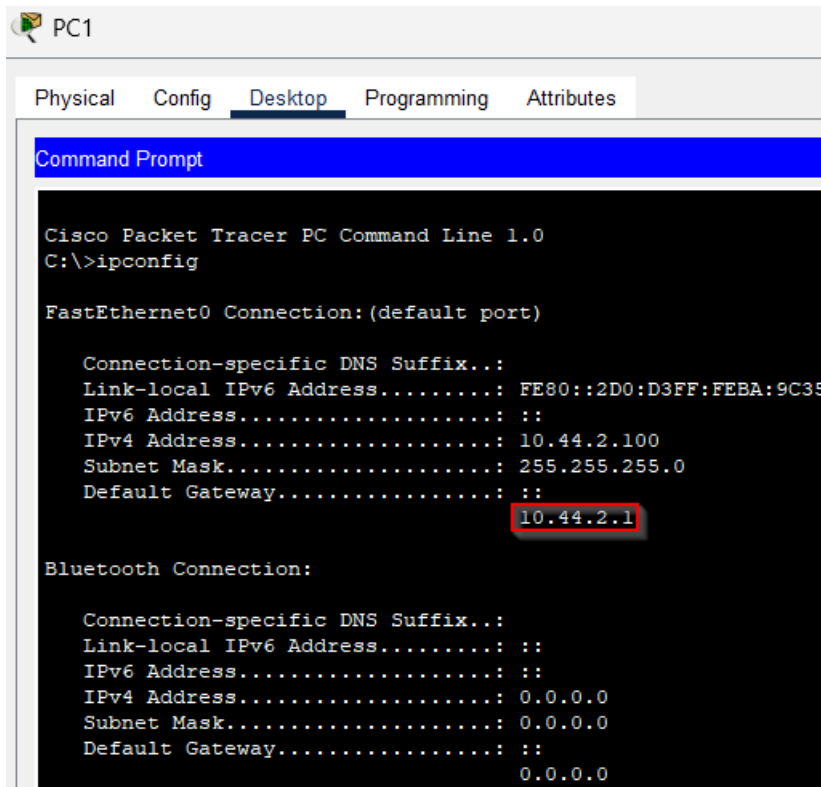
Je configure le pc de Dave en sçannant les réseaux sans fil disponibles et trouve le réseau "Home" avec un signal de 72%. Elle sélectionne ce réseau et clique sur "Connect" pour s'y connecter. La configuration montre que la sécurité du réseau est désactivée, ce qui peut représenter un risque en termes de sécurité.

Mary :

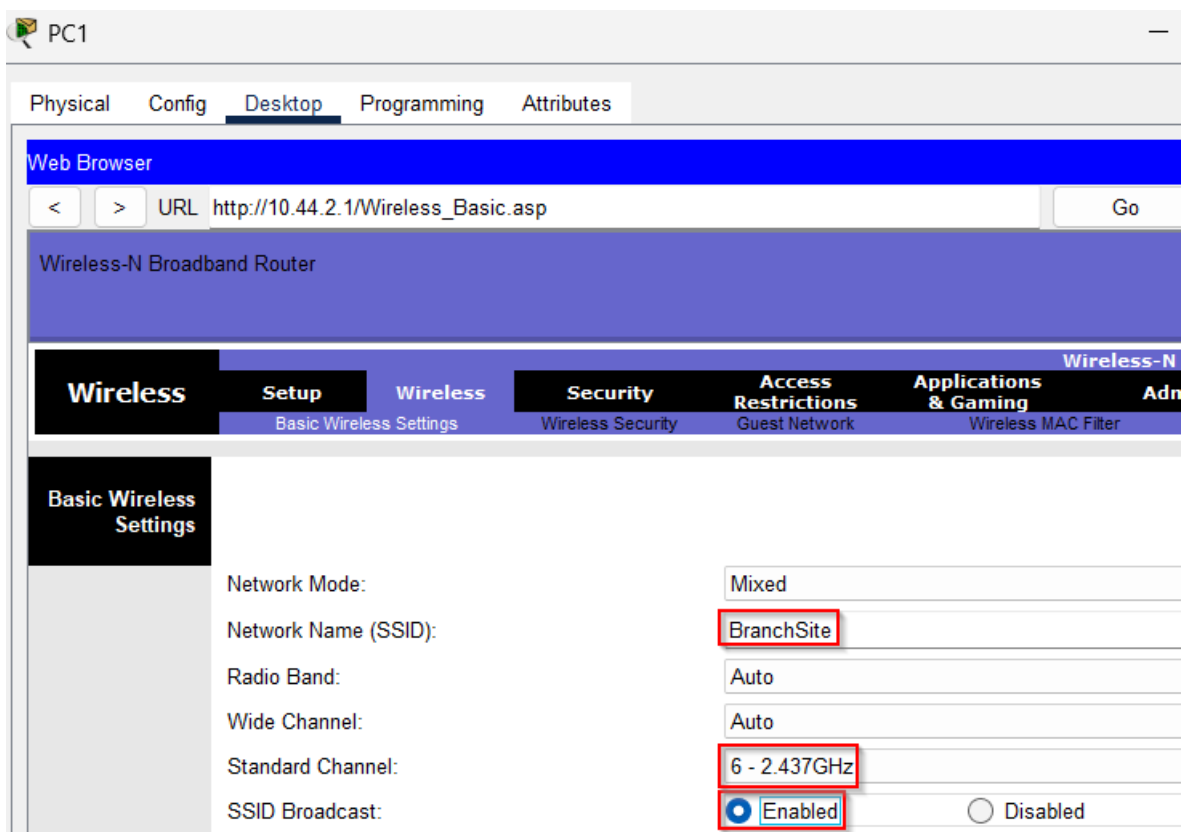


De manière similaire, je configure le pc de Mary détecte le même réseau sans fil "Home", mais avec un signal plus fort de 100%. Il clique également sur "Connect" pour établir une connexion. Les paramètres du réseau indiquent un mode mixte B/G/N avec une sécurité désactivée, ce qui pourrait être amélioré pour éviter les connexions non autorisées.

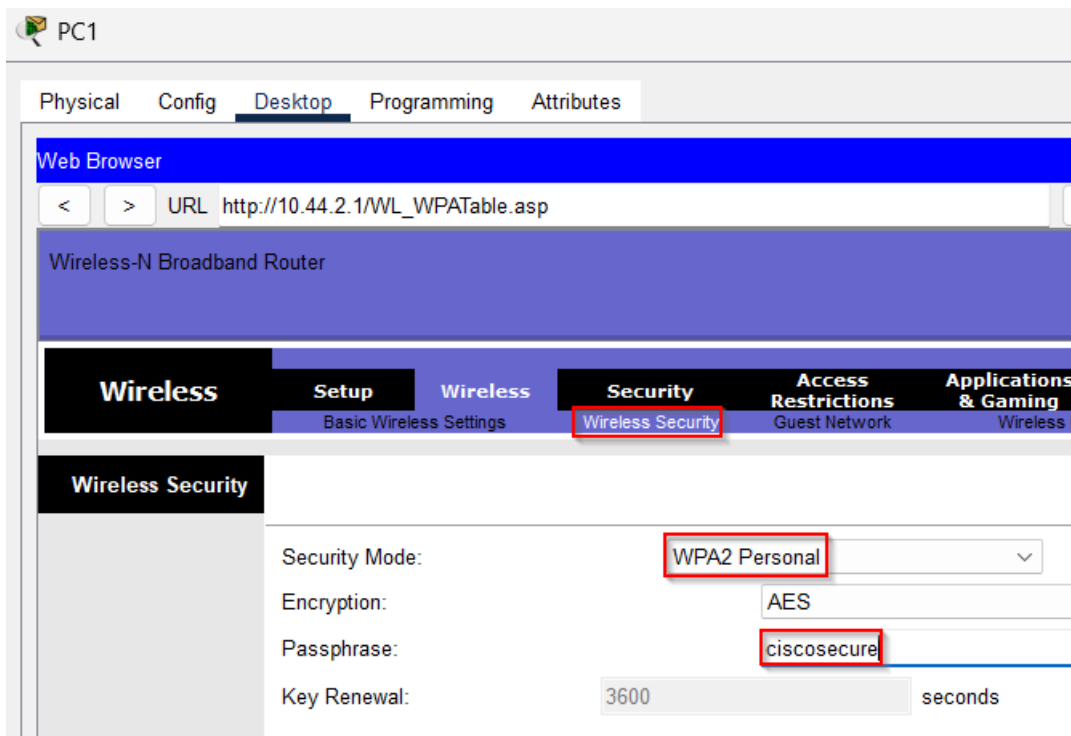
Configurer le WPA2 PSK pour la succursale de Gotham Healthçare :



Dans cette capture, la commande ipconfig montre que l'ordinateur "PC1" a une configuration réseau correcte avec une passerelle par défaut de 10.44.2.1.

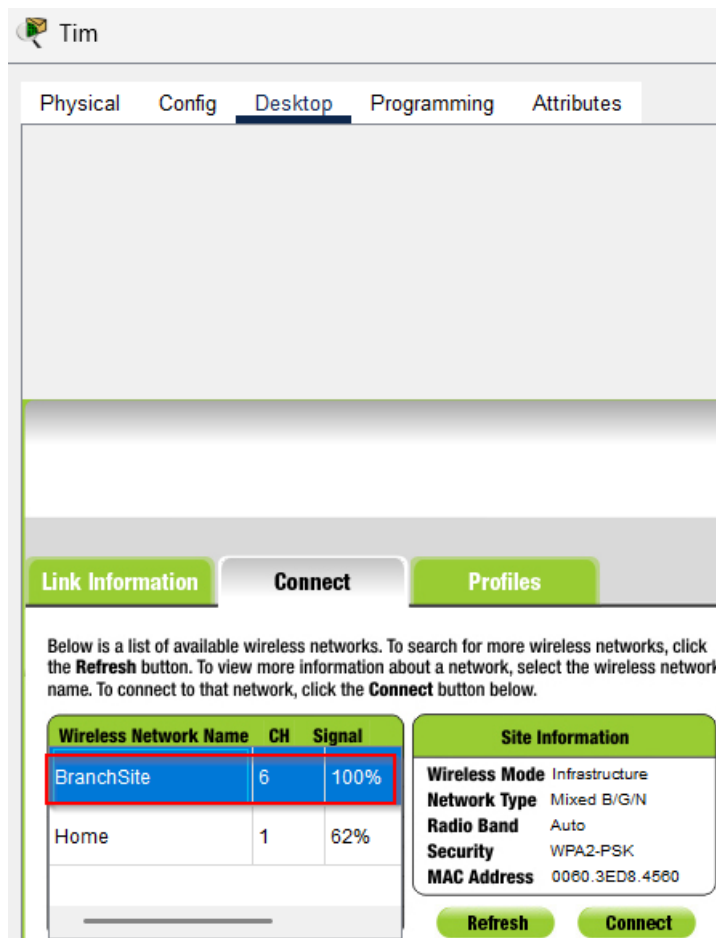


Ici, les paramètres sans fil du routeur sont configurés via l'interface web accessible à l'adresse http://10.44.2.1/Wireless_Basic.asp. Le SSID du réseau est défini sur "BranchSite", avec un mode réseau "Mixed" et un canal standard fixé à "6 - 2.437GHz". L'option SSID Broadcast est activée, rendant le réseau visible pour les appareils à proximité.

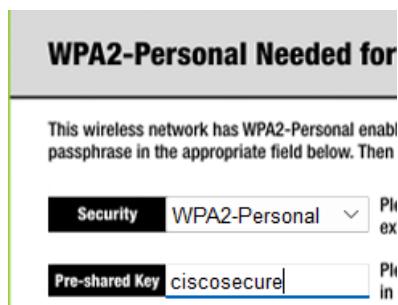


Dans l'onglet "Wireless Security", la sécurité du réseau sans fil est configurée. Le mode de sécurité choisi est "WPA2 Personal" avec un chiffrement AES pour assurer une connexion sécurisée. Une passphrase (ciscosecure) est définie pour authentifier les utilisateurs, renforçant la protection contre les accès non autorisés.

Tim :

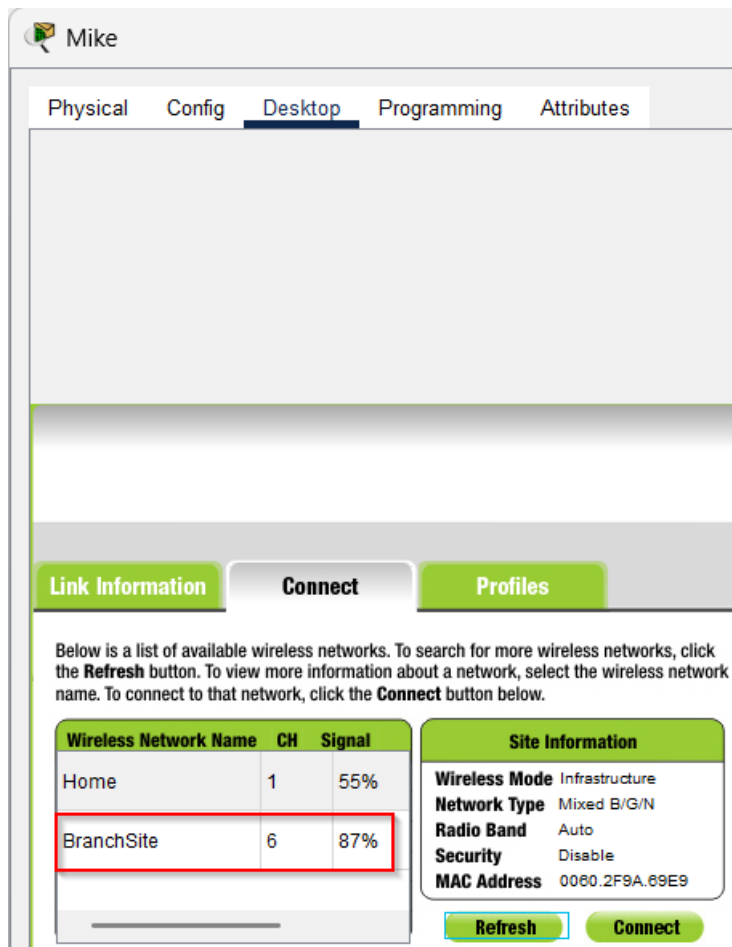


Je scanne les réseaux disponibles et détecte le réseau "BranchSite" avec un signal de 100%. Il sélectionne ce réseau et clique sur "Connect" pour s'y connecter. La configuration montre que la sécurité WPA2-PSK est activée, garantissant une connexion sécurisée pour les utilisateurs autorisés.

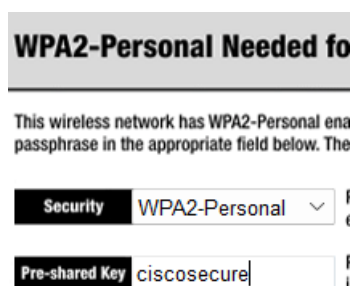


Dans cette capture, je saisis la clé de sécurité prépartagée (Pre-shared Key) ciscosecure pour me connecter à un réseau sans fil protégé par le mode de sécurité WPA2-Personal. Cela garantit que seuls les utilisateurs disposant de la clé correcte peuvent accéder au réseau, renforçant ainsi la sécurité des communications.

Mike :

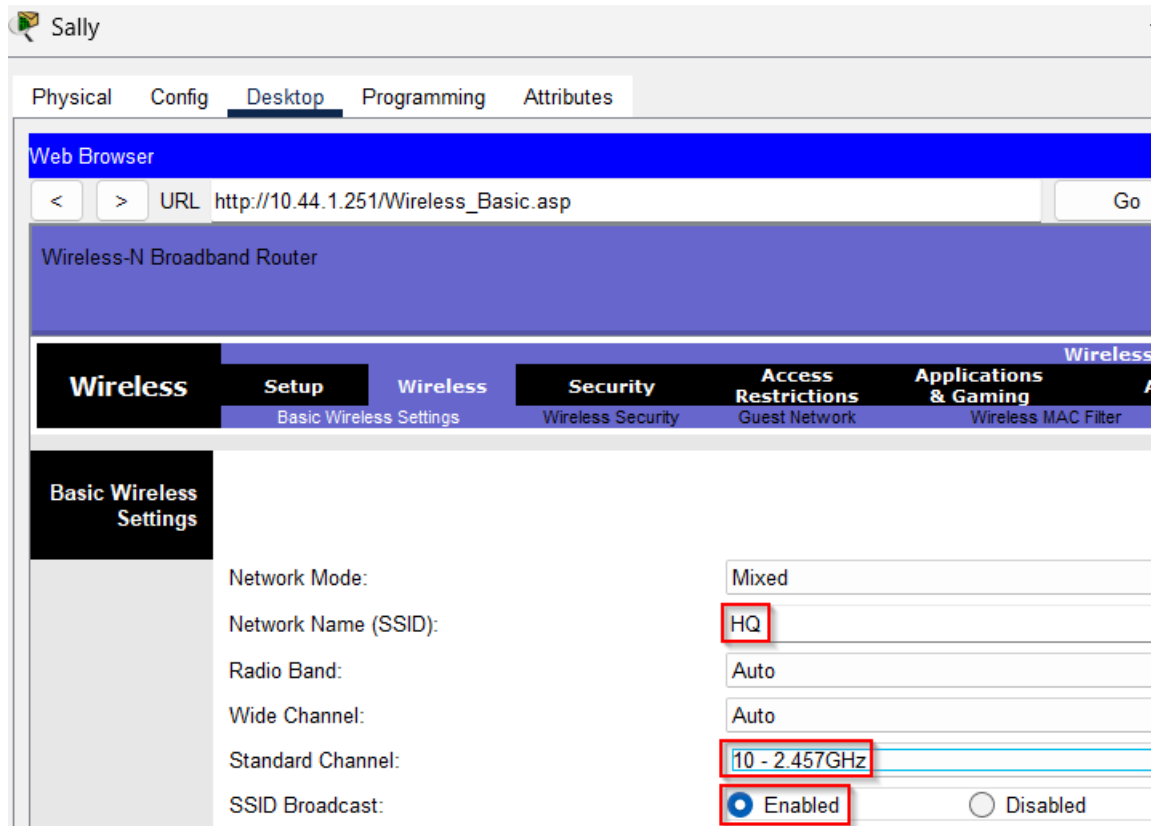


Je scanne les réseaux disponibles et détecte le réseau "BranchSite" avec un signal de 100%. Il sélectionne ce réseau et clique sur "Connect" pour s'y connecter. La configuration montre que la sécurité WPA2-PSK est activée, garantissant une connexion sécurisée pour les utilisateurs autorisés.



Dans cette capture, je saisis la clé de sécurité prépartagée (Pre-shared Key) ciscosecure pour se connecter à un réseau sans fil protégé par le mode de sécurité WPA2-Personal. Cela garantit que seuls les utilisateurs disposant de la clé correcte peuvent accéder au réseau, renforçant ainsi la sécurité des communications.

1.18 Configurer le protocole WPA2 RADIUS pour le siège social de Metropolis Bank :



Dans cette capture, la configuration du routeur pour le réseau sans fil "HQ" est affichée. Le mode réseau est "Mixed" pour prendre en charge plusieurs types de clients, le canal standard est fixé à "10 - 2.457GHz" pour éviter les interférences, et la diffusion du SSID est activée (Enabled) pour rendre le réseau visible aux utilisateurs.

Web Browser

< > URL http://10.44.1.251/WL_WPATable.asp Go

Wireless-N Broadband Router

Wireless Setup Wireless Security Access Restrictions Applications & Gaming

Basic Wireless Settings Wireless Security Guest Network Wireless MAC Filter

Wireless Security

Security Mode: WPA2 Enterprise

Encryption: AES

RADIUS Server: 10 . 44 . 1 . 252

RADIUS Port: 1645

Shared Secret: ciscosecure

Key Renewal: 3600 seconds

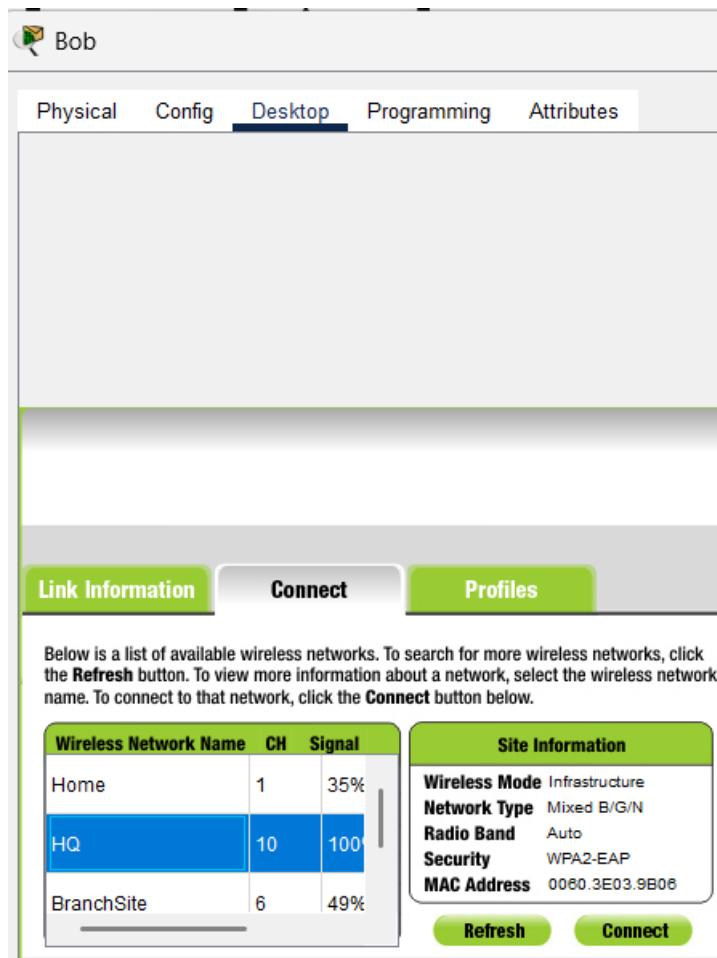
L'onglet "Wireless Security" montre que la sécurité du réseau "HQ" est configurée avec le mode "WPA2 Enterprise". Un chiffrement AES est utilisé pour une protection renforcée. Le serveur RADIUS est défini à l'adresse 10.44.1.252 avec le port 1645, et le secret partagé est ciscosecure. Cette configuration assure une authentification centralisée et sécurisée.

The screenshot shows the NTP/AAA configuration window. On the left is a 'SERVICES' sidebar with options: HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA (selected), NTP, EMAIL, FTP, IoT, VM Management, and Radius EAP. The main area is titled 'AAA' and has tabs for Physical, Config, Services, Desktop, Programming, and Attributes. The 'Services' tab is active, showing 'Service' as 'On' and 'Radius Port' as '1645'. Below this is the 'Network Configuration' section, which includes a red-bordered box containing 'Client Name' (HQ), 'Client IP' (10.44.1.251), 'Secret' (ciscosecure), and 'ServerType' (Radius). Below this box is a table with columns 'Client Name', 'Client IP', 'Server Type', and 'Key'. The table has two rows: '1 HQ_Router' with IP '10.44.1.1' and '2 HQ' with IP '10.44.1.251'. To the right of the table are 'Add', 'Save', and 'Remove' buttons. Below the network configuration is the 'User Setup' section, which includes a red-bordered box containing 'Username' (phil) and 'Password' (philwashere). Below this box is a table with columns 'Username' and 'Password'. The table has three rows: '1 admin' with password 'cisco123', '2 bob' with password 'secretninjabob', and '3 phil' with password 'philwashere'. To the right of the table are 'Add' and 'Save' buttons.

Client Name	Client IP	Server Type	Key
1 HQ_Router	10.44.1.1	Radius	cisco123
2 HQ	10.44.1.251	Radius	ciscosecure

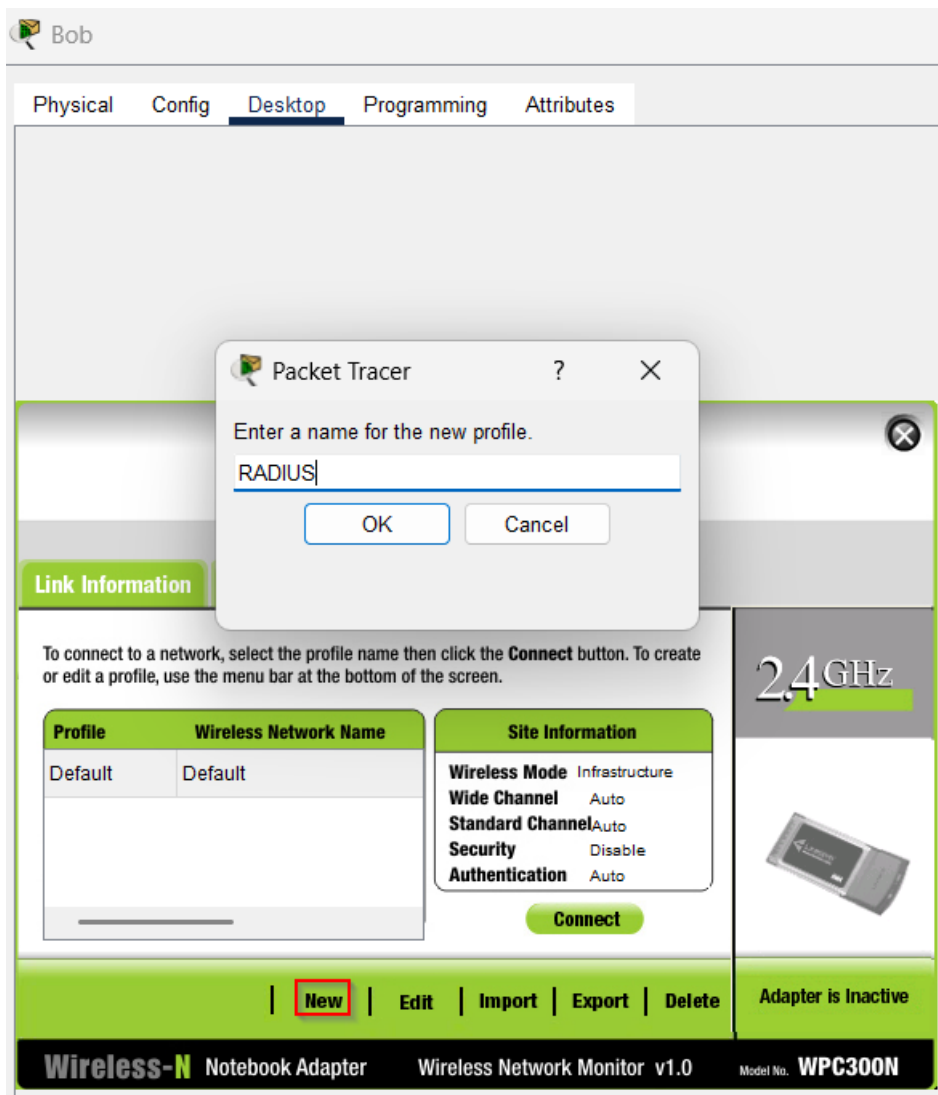
Username	Password
1 admin	cisco123
2 bob	secretninjabob
3 phil	philwashere

Dans les paramètres AAA, le serveur RADIUS est configuré avec le nom de client "HQ", une adresse IP de client 10.44.1.251, et un type de serveur "Radius". Le secret partagé utilisé est ciscosecure. De plus, des utilisateurs tels que "phil" et "bob" avec les mots de passes secretninjabob et philwashere sont définis, permettant leur authentification via le serveur RADIUS.



Je scanne les réseaux disponibles et détecte le réseau "HQ" avec un signal fort de 100% sur le pc de bob. Le réseau utilise WPA2-EAP pour la sécurité, nécessitant une authentification via un serveur RADIUS. Bob peut se connecter au réseau en fournissant les informations appropriées pour l'authentification.

Connection de bob :



Dans cette capture, je crée un nouveau profil de connexion pour le réseau en cliquant sur le bouton "New". J'entre le nom du profil "RADIUS" pour identifier ce réseau spécifique, car il utilise l'authentification RADIUS. Cela facilite la gestion des paramètres réseau associés à ce profil.

Creating a Profile

Wireless Mode

Please choose the Wireless Mode that best suits your needs.

☒ Infrastructure Mode

Select Infrastructure Mode if you want to connect to a wireless router or access point.

☐ Ad-Hoc Mode

Select Ad-Hoc Mode if you want to connect to another wireless device directly without using a wireless router or access point.

Please enter the wireless network name (SSID) for your wireless network.

The wireless network name is shared by all devices in a wireless network and is case-sensitive.

Wireless Network Name HQ

Ici, je configure le mode du réseau sans fil en sélectionnant "Infrastructure Mode" car je veux me connecter à un routeur ou point d'accès centralisé. Ensuite, je renseigne le nom du réseau (SSID) "HQ" pour identifier le réseau cible.

The screenshot shows the 'Creating a Profile' screen with the 'Wireless Security' section active. A dropdown menu for 'Security' is set to 'WPA2-Enterprise'. To the right, there is explanatory text about WEP, WPA-Personal, WPA2-Personal, and WPA-Enterprise/RADIUS. At the bottom right, there are 'Back' and 'Next' navigation buttons.

Creating a Profile

Wireless Security

Security WPA2-Enterprise ▾

Please select the wireless security method used by your existing wireless network.

WEP stands for Wired Equivalent Privacy.

WPA-Personal, also known as Pre-shared Key, is a security standard stronger than WEP encryption.

WPA2-Personal is the newer version with stronger encryption than WPA-Personal.

WPA-Enterprise, WPA2-Enterprise and **RADIUS** use Remote Authentication Dial-In User Service (RADIUS).

| Back | Next

Dans cette étape, je choisis "WPA2-Enterprise" comme méthode de sécurité, car elle offre un niveau de sécurité avancé grâce à l'authentification via un serveur RADIUS. Ce mode est plus sécurisé que WPA-Personal.

This screenshot shows the 'Wireless Security - WPA2 Enterprise' configuration screen. It contains several fields: 'Authentication' (PEAP), 'Login Name' (bob), 'Password' (masked), 'Server Name' (empty), 'Certificate' (Trust Any), and 'Inner Authen.' (TOKEN CARD). Each field has a corresponding instruction. The 'Login Name' and 'Password' fields are highlighted with a red box. Navigation buttons 'Back' and 'Next' are at the bottom right.

Creating a Profile

Wireless Security - WPA2 Enterprise

Authentication PEAP ▾ Please select the authentication method that you use to access your network.

Login Name bob Enter the Login Name used for authentication.

Password Enter the Password used for authentication.

Server Name Enter the Server Name used for authentication. (Optional)

Certificate Trust Any ▾ Please select the certificate used for authentication.

Inner Authen. TOKEN CARD ▾ Please select the inner authentication method used inside the PEAP tunnel.

| Back | Next

Je configure les détails d'authentification pour WPA2-Enterprise. J'entre le nom d'utilisateur "bob" et le mot de passe correspondant pour m'authentifier auprès du serveur RADIUS. Je sélectionne également PEAP comme méthode d'authentification et "Trust Any" pour accepter tout certificat, car il s'agit d'un environnement de test. Ces options garantissent une connexion sécurisée au réseau.

Confirm New Settings

Profile Settings			
Wireless Network Name	HQ	IP Address	Auto
Wireless Mode	Infrastructure	Subnet Mask	Auto
Network Mode	Mixed Mode	Default Gateway	Auto
Radio Band	Auto	DNS1	Auto
Wide Channel	Auto	DNS2	
Standard Channel	Auto		
Security	WPA2 Enterprise		
Authentication	Auto		

Je configure un profil nommé "HQ" pour le réseau sans fil avec un mode de réseau "Infrastructure". J'ai choisi le mode "Mixed Mode" pour permettre la compatibilité avec divers appareils, tandis que le canal et les paramètres de bande radio sont laissés sur "Auto" pour une configuration dynamique optimale. La sécurité est configurée en WPA2 Enterprise, ce qui offre un niveau de sécurité avancé en utilisant le serveur RADIUS pour l'authentification.

Connexion de Phil :

Phil

Physical Config **Desktop** Programming Attributes

Confirm New Settings

Profile Settings			
Wireless Network Name	HQ	IP Address	Auto
Wireless Mode	Infrastructure	Subnet Mask	Auto
Network Mode	Mixed Mode	Default Gateway	Auto
Radio Band	Auto	DNS1	Auto
Wide Channel	Auto	DNS2	
Standard Channel	Auto		
Security	WPA2 Enterprise		
Authentication	Auto		

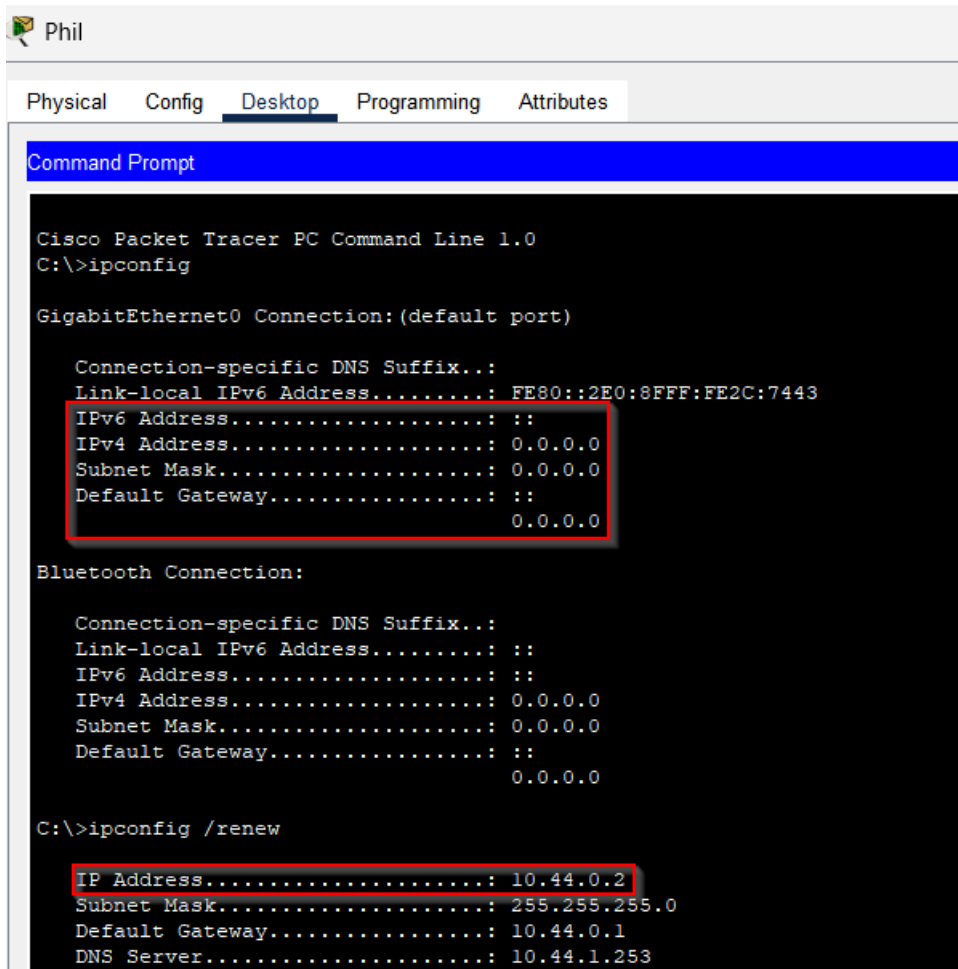
Je valide les paramètres de profil pour le réseau sans fil. Ces paramètres incluent le SSID "HQ", le mode infrastructure, et la sécurité WPA2 Enterprise. Les paramètres réseau comme l'adresse IP, le masque de sous-réseau, et les DNS sont définis sur "Auto" pour permettre une configuration dynamique via le serveur DHCP. Cette approche simplifie la gestion tout en maintenant la sécurité et la compatibilité.

a) Dans le contexte d'une grande entreprise, le protocole WPA2 RADIUS est largement préférable à WPA2 PSK en raison de ses nombreux avantages en termes de sécurité et de gestion. Tout d'abord, WPA2 RADIUS offre une sécurité renforcée, car chaque utilisateur ou appareil possède des identifiants uniques, comme un login et un mot de passe ou un certificat. En cas de compromission, seul le compte concerné est impacté, contrairement à WPA2 PSK où une clé partagée entre tous les utilisateurs rend le réseau vulnérable si cette clé est compromise. De plus, WPA2 RADIUS permet une gestion centralisée des accès via un serveur RADIUS, souvent intégré avec un annuaire comme Active Directory. Cela simplifie la création, la modification ou la suppression des accès et permet une personnalisation fine des droits selon les utilisateurs ou groupes.

Un autre avantage majeur de WPA2 RADIUS est la traçabilité. Chaque connexion est enregistrée dans les journaux du serveur, ce qui permet de suivre les activités réseau pour des besoins de conformité réglementaire ou d'analyse d'incidents. À l'inverse, WPA2 PSK ne permet pas de tracer individuellement les utilisateurs, car tous partagent la même clé. De plus, WPA2 RADIUS est particulièrement adapté aux environnements à grande échelle, où de nombreux utilisateurs et appareils se connectent. La gestion fine des sessions réduit les conflits et améliore la sécurité. Enfin, WPA2 RADIUS permet l'intégration avec des politiques avancées comme la mise en quarantaine des appareils non conformes ou la segmentation réseau (VLAN), ce qui est impossible avec WPA2 PSK. Ces caractéristiques font de WPA2 RADIUS une solution incontournable pour les grandes entreprises, tandis que WPA2 PSK reste limité à des environnements simples ou personnels.

6. Sixième PKA :

1.19 Envoyer du trafic FTP non chiffré :



The screenshot shows a Cisco Packet Tracer PC Command Line window for a device named 'Phil'. The 'Desktop' tab is selected. The Command Prompt displays the following commands and output:

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

GigabitEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address . . . . .: FE80::2E0:8FFF:FE2C:7443
IPv6 Address . . . . .: ::
IPv4 Address . . . . .: 0.0.0.0
Subnet Mask . . . . .: 0.0.0.0
Default Gateway . . . . .: ::
                                0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address . . . . .: ::
IPv6 Address . . . . .: ::
IPv4 Address . . . . .: 0.0.0.0
Subnet Mask . . . . .: 0.0.0.0
Default Gateway . . . . .: ::
                                0.0.0.0

C:\>ipconfig /renew

IP Address . . . . .: 10.44.0.2
Subnet Mask . . . . .: 255.255.255.0
Default Gateway . . . . .: 10.44.0.1
DNS Server . . . . .: 10.44.1.253
```

In the original image, red boxes highlight the initial zeroed-out IP configuration and the renewed IP configuration details.

Dans cette capture, je commence par exécuter la commande `ipconfig`. Les informations initiales montrent que l'interface réseau GigabitEthernet0 ne dispose d'aucune configuration IPv4 ou IPv6, les adresses et les masques sont à zéro. J'exécute ensuite la commande `ipconfig /renew`, ce qui force le renouvellement de la configuration IP via DHCP. Cette action attribue une adresse IPv4 dynamique (10.44.0.2) avec un masque de sous-réseau (255.255.255.0) et une passerelle par défaut (10.44.0.1).

```
C:\>ftp 209.165.201.20
Trying to connect...209.165.201.20
Connected to 209.165.201.20
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put PublicInfo.txt

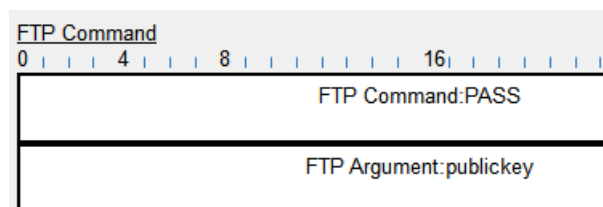
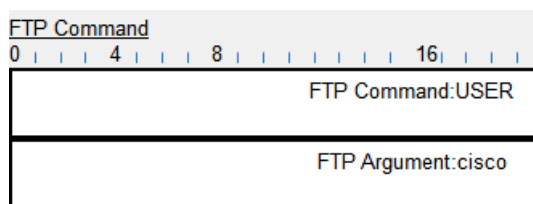
Writing file PublicInfo.txt to 209.165.201.20:
File transfer in progress...

[Transfer complete - 346 bytes]

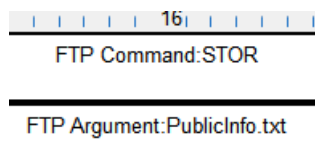
346 bytes copied in 0.008 secs (43250 bytes/sec)
ftp>
```

Ici, je me connecte à un serveur FTP à l'adresse 209.165.201.20. Après l'authentification réussie avec le nom d'utilisateur et le mot de passe, je passe en mode passif pour le transfert. Ensuite, j'upload un fichier nommé PublicInfo.txt sur le serveur en utilisant la commande put. Le transfert est complété avec succès en une fraction de seconde, confirmant que la connexion et la configuration FTP fonctionnent correctement.

a)

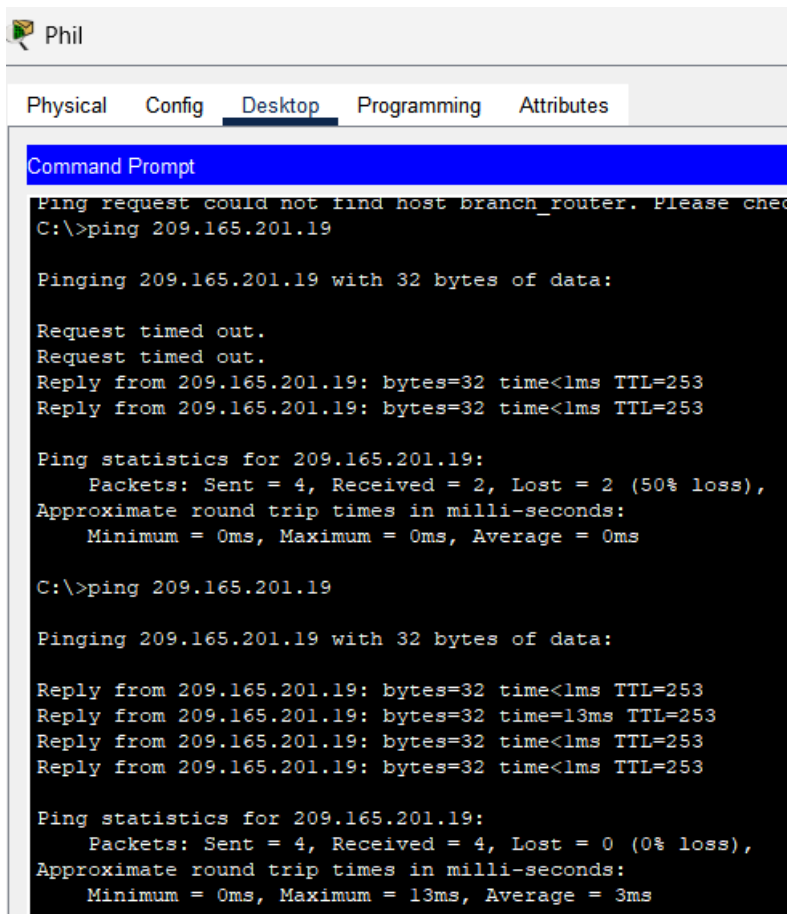


Il y a l'identifiant et le mot de passe pour se connecter au ftp.



Le fichier PublicInfo.txt apparait aussi.

1.20 Configurer le VPN :



```
Phil
Physical Config Desktop Programming Attributes
Command Prompt
Ping request could not find host branch_router. Please check the name and number.
C:\>ping 209.165.201.19

Pinging 209.165.201.19 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 209.165.201.19: bytes=32 time<1ms TTL=253
Reply from 209.165.201.19: bytes=32 time<1ms TTL=253

Ping statistics for 209.165.201.19:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

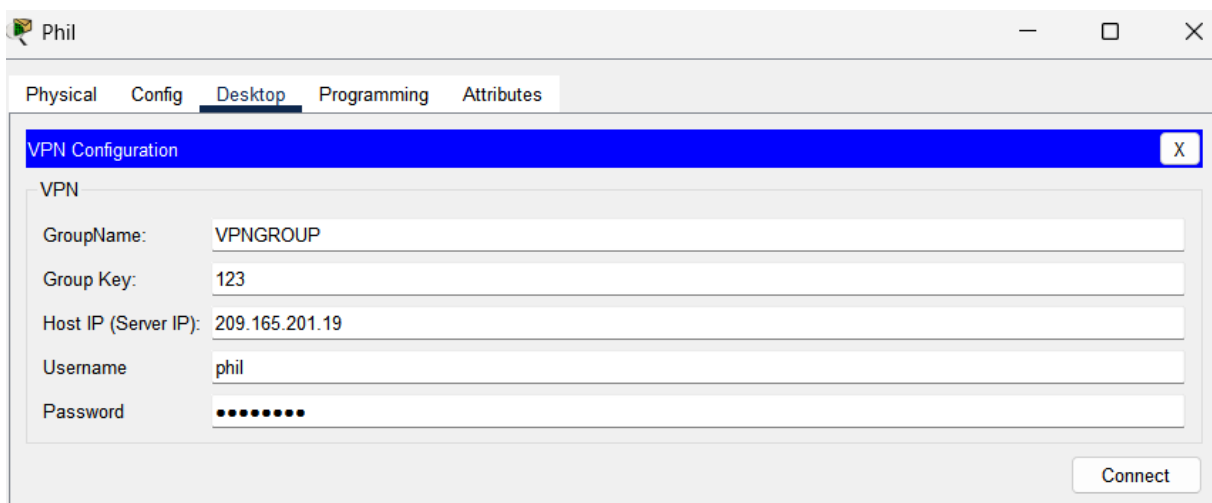
C:\>ping 209.165.201.19

Pinging 209.165.201.19 with 32 bytes of data:

Reply from 209.165.201.19: bytes=32 time<1ms TTL=253
Reply from 209.165.201.19: bytes=32 time=13ms TTL=253
Reply from 209.165.201.19: bytes=32 time<1ms TTL=253
Reply from 209.165.201.19: bytes=32 time<1ms TTL=253

Ping statistics for 209.165.201.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

Dans cette capture, je teste la connectivité avec l'adresse IP 209.165.201.19 en utilisant la commande ping. La première tentative montre une perte de 50 % des paquets. Une seconde tentative confirme une connexion stable avec 0 % de perte.



Phil

Physical Config Desktop Programming Attributes

VPN Configuration

VPN

GroupName: VPNGROUP

Group Key: 123

Host IP (Server IP): 209.165.201.19

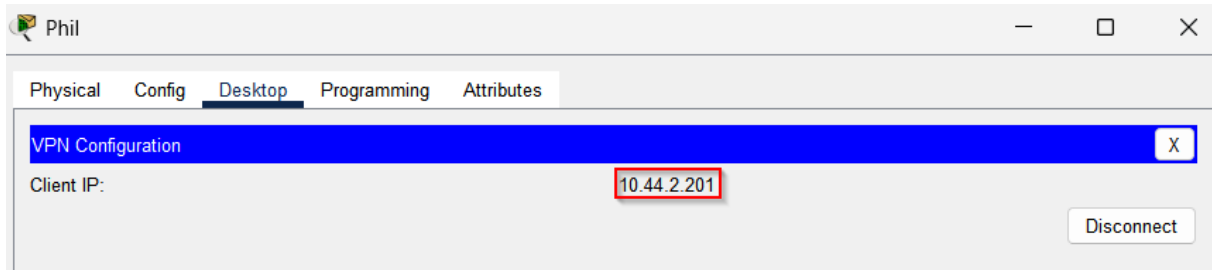
Username: phil

Password:

Connect

Ici, je configure une connexion VPN. Je saisis les informations nécessaires : le nom de groupe (VPNGROUP), la clé de groupe (123), l'adresse IP du serveur VPN (209.165.201.19), ainsi

que le nom d'utilisateur et le mot de passe. Après avoir rempli ces champs, je clique sur "Connect" pour établir la connexion. Ces étapes sont cruciales pour sécuriser les communications via un tunnel VPN.



Cette capture montre que la connexion VPN est réussie. Une adresse IP de client VPN (10.44.2.201) a été attribuée. Cela confirme que je suis connecté au réseau VPN et que mon trafic réseau passe maintenant par ce tunnel sécurisé.

1.21 Envoie du trafic FTP chiffré :

```
C:\>ipconfig

GigabitEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2E0:8FFF:FE2C:7443
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 10.44.0.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                   10.44.0.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                   0.0.0.0
    Tunnel Interface IP Address . . . .: 10.44.2.201
```

Il y a une nouvelle ligne, « Tunnel Interface IP Address » qui est apparue

La Tunnel Interface IP Address correspond à une adresse IP assignée à une interface réseau virtuelle utilisée pour établir une connexion tunnel. Les données sont encapsulées et transmises de manière sécurisée à travers un réseau public grâce au tunnel sécurisé.

```
C:\>ftp 209.165.201.19
Trying to connect...209.165.201.19

%Error ftp://209.165.201.19/ (Ftp peer reset)

(Disconnecting from ftp server)
```

Je n'arrive pas à me connecter au ftp.

7. Conclusion :

Ce TP m'a permis de me familiariser avec les principaux services réseau et d'acquérir des compétences pratiques dans leur configuration et leur sécurisation. Chaque étape m'a apporté une meilleure compréhension des protocoles, ainsi que des enjeux liés à la gestion des accès et à la protection des données. J'ai également constaté l'importance d'une segmentation réseau efficace et d'une sécurisation renforcée pour limiter les risques en cas d'attaques.

8. Sources :

<https://learn.microsoft.com/fr-fr/windows-server/administration/windows-commands/ipconfig>

<https://www.youtube.com/watch?v=M7tlt3M2riQ&t=62s>

<https://fr.wikipedia.org/wiki/HMAC>

<https://www.it-connect.fr/serveur-de-fichiers-les-permissions-ntfs-et-de-partage/>

<https://contenthub.netacad.com/legacy/CyberEss/1.1/en/course/files/1.5.3.5%20Packet%20Tracer%20-%20Creating%20a%20Cyber%20World.pdf>

<https://www.linuxtricks.fr/wiki/droits-sous-linux-utilisateurs-groupes-permissions>

<https://blog.netwrix.fr/2019/02/28/differences-entre-autorisations-de-partage-et-autorisations-ntfs/>