Travaux pratiques 3.4.3 : Services et protocoles de messagerie

Schéma de topologie

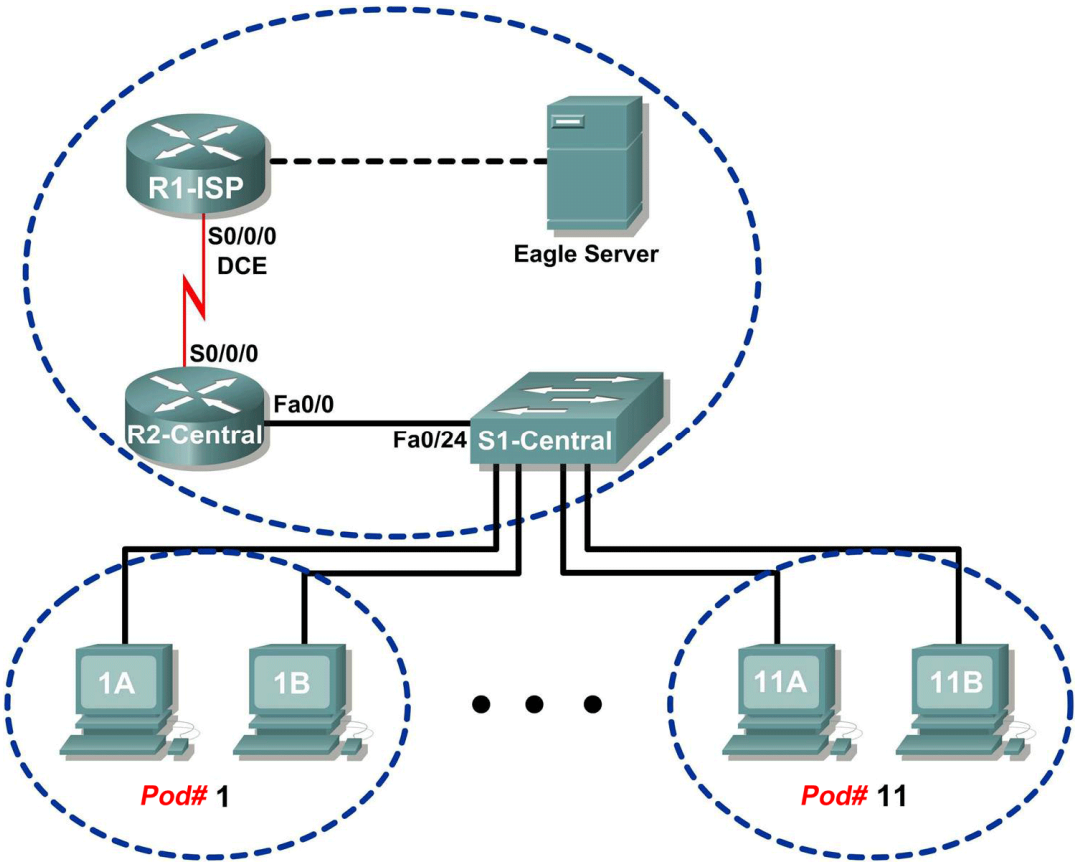


Tableau d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	S/O
	Fa0/0	192.168.254.253	255.255.255.0	S/O
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	S/O
	Fa0/0	172.16.255.254	255.255.0.0	S/O
Eagle Server	S/O	192.168.254.254	255.255.255.0	192.168.254.253
	S/O	172.31.24.254	255.255.255.0	S/O
host*Pod*#A	S/O	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod*#B	S/O	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	S/O	172.16.254.1	255.255.0.0	172.16.255.254

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Objectifs pédagogiques

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Configurer l'ordinateur hôte pod du service de messagerie
- Capturer et analyser la communication de messagerie électronique entre l'ordinateur hôte pod et un serveur de messagerie

Contexte

La messagerie électronique est l'un des services réseau les plus populaires utilisant le modèle client/serveur. Le client de messagerie électronique est configuré sur l'ordinateur d'un utilisateur, puis configuré pour se connecter à un serveur de messagerie. La plupart des fournisseurs de services Internet donnent des instructions pas à pas pour utiliser des services de messagerie électronique. Par conséquent, l'utilisateur type peut ne pas être familiarisé aux complexités des services de messagerie ou des protocoles utilisés.

Dans les environnements réseau où le client MUA doit se connecter à un serveur de messagerie sur un autre réseau pour envoyer et recevoir les courriels, les deux protocoles suivants sont utilisés.

- Le protocole SMTP a été défini en août 1982 par le document RFC 821 et a depuis fait l'objet de nombreuses modifications et améliorations. Le document RFC 2821 d'avril 2001 regroupe et met à jour les documents RFC précédents relatifs au courriel. Le serveur SMTP écoute le port TCP 25. Il est utilisé pour envoyer les courriels du client de messagerie électronique au serveur de messagerie électronique, diffuser les courriels aux comptes locaux et les relayer entre les serveurs SMTP.
- Le protocole POPv3 (Post Office Protocol version 3) est utilisé lorsqu'un client de messagerie externe souhaite recevoir les courriels à partir du serveur de messagerie électronique. Le serveur POPv3 écoute le port TCP 110.

Les versions antérieures des deux protocoles ne doivent pas être utilisées. En outre, il existe des versions sécurisées des deux protocoles qui utilisent la technologie SSL/TSL dans le cadre de la communication.

Les courriels sont exposés à diverses failles de sécurité informatique. Les attaques de courrier indésirable saturent les réseaux de courriels inutiles et non sollicités. Il en résulte une consommation excessive de la bande passante et des ressources réseau. Les serveurs de messagerie électronique ont connu de nombreuses failles qui laissaient l'ordinateur exposé aux menaces.

Scénario

Au cours de ces travaux pratiques, vous allez configurer et utiliser une application cliente de messagerie pour vous connecter aux services réseau d'Eagle Server. Vous surveillerez les communications à l'aide du logiciel Wireshark et analyserez les paquets capturés.

Un client de messagerie électronique tel qu'Outlook Express ou Mozilla Thunderbird sera utilisé pour établir la connexion au service réseau d'Eagle Server. Les services de messagerie électronique SMTP d'Eagle Server sont préconfigurés avec des comptes utilisateur capables d'envoyer et de recevoir des courriels externes.

Tâche 1 : configuration de l'ordinateur hôte pod du service de messagerie

Les travaux pratiques doivent être configurés comme illustré dans le schéma de topologie et dans le tableau d'adressage logique. Si ce n'est pas le cas, demandez de l'aide auprès de votre formateur.

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Étape 1 : téléchargement et installation de Mozilla Thunderbird

Si Thunderbird n'est pas installé sur l'ordinateur hôte pod, vous pouvez le télécharger à l'adresse eagle-server.example.com. Reportez-vous à la figure 1. L'URL de téléchargement est la suivante : `ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter3`.

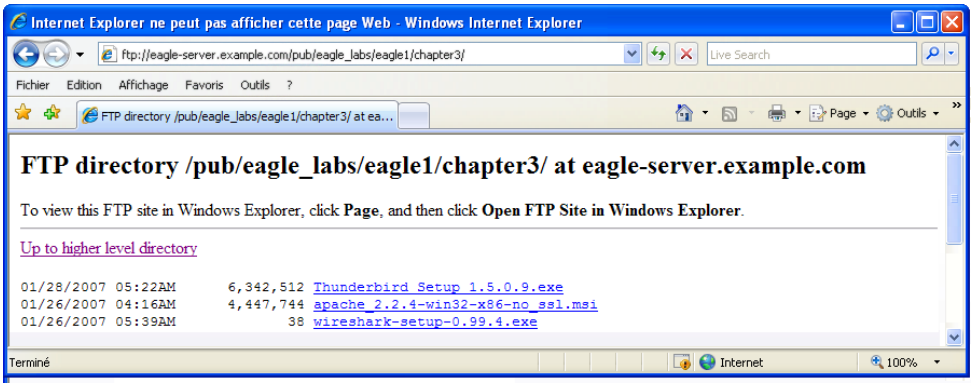


Figure 1. Page de téléchargement de Thunderbird sur FTP

1. Cliquez avec le bouton droit sur le nom de fichier de Thunderbird, puis enregistrez le fichier sur l'ordinateur hôte pod.
2. Une fois le fichier téléchargé, double-cliquez sur le nom de fichier et installez Thunderbird avec les paramètres par défaut.
3. Une fois terminé, démarrez Thunderbird.

Étape 2 : configuration de Thunderbird afin de recevoir et d'envoyer des courriels

1. Au démarrage de Thunderbird, les paramètres de compte de messagerie doivent être configurés. Renseignez les informations du compte comme suit :

Champ	Valeur
Account Name (Nom du compte)	Le nom du compte se base sur l'ordinateur hôte pod. 22 comptes sont configurés sur Eagle Server, marqués ccna[1..22]. Si cet hôte pod se trouve sur l'hôte A de Pod1, le nom du compte est `ccna1`. Si cet hôte pod se trouve sur l'hôte B de Pod3, le nom du compte est `ccna6`. Etc.
Your Name (Nom)	Utilisez le même nom que ci-dessus.
E-mail address (Adresse e-mail)	*votre_nom*`@eagle-server.example.com`
Type de serveur entrant que vous utilisez	`IMAP`
Serveur entrant (SMTP)	`eagle-server.example.com`
Serveur sortant (SMTP)	`eagle-server.example.com`

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

2. Vérifiez les paramètres de compte dans **Tools (Outils) > Account Settings (Paramètres de compte)**. Reportez-vous à la figure 2.

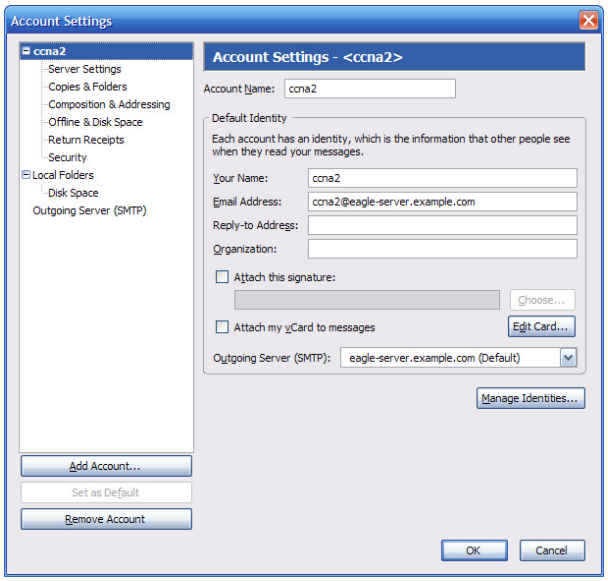


Figure 2. Paramètres de compte Thunderbird

3. Dans le panneau de gauche de l'écran Account Settings (Paramètres de compte), cliquez sur **Server Settings (Paramètres du serveur)**. Un écran semblable à celui de la figure 3 s'affiche.

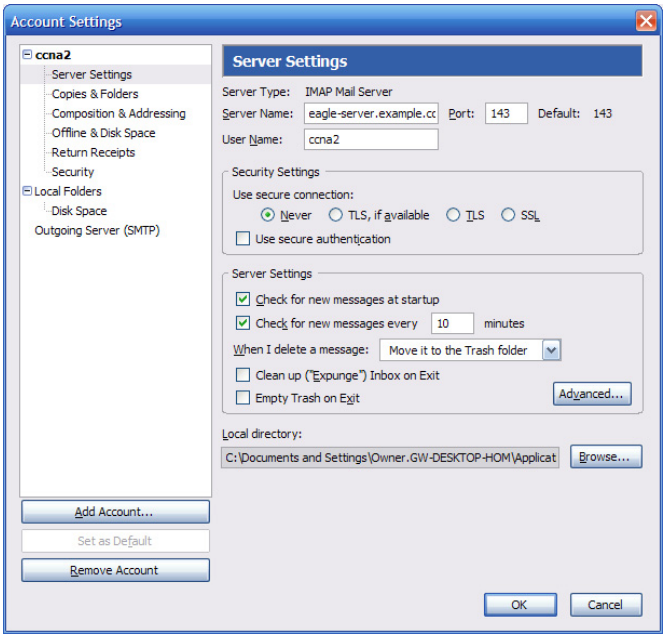


Figure 3. Écran Server Settings (Paramètres du serveur) de Thunderbird

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

La figure 4 illustre une configuration correcte du serveur sortant (SMTP).

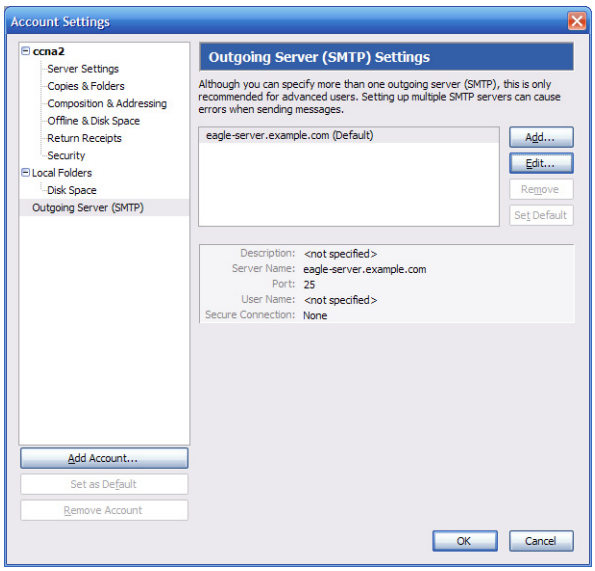


Figure 4. Écran Outgoing Server (SMTP) Settings (Paramètres du serveur sortant (SMTP))

Quelle est la fonction du protocole SMTP et quel est le numéro de port TCP bien connu ?

_____

_____

Tâche 2 : capture et analyse de la communication de messagerie électronique entre l'ordinateur hôte pod et un serveur de messagerie

Étape 1 : envoi d'un courriel non capturé

1. Demandez à un autre participant son nom de courriel.
2. Utilisez ce nom pour composer et envoyer un message amical au participant.

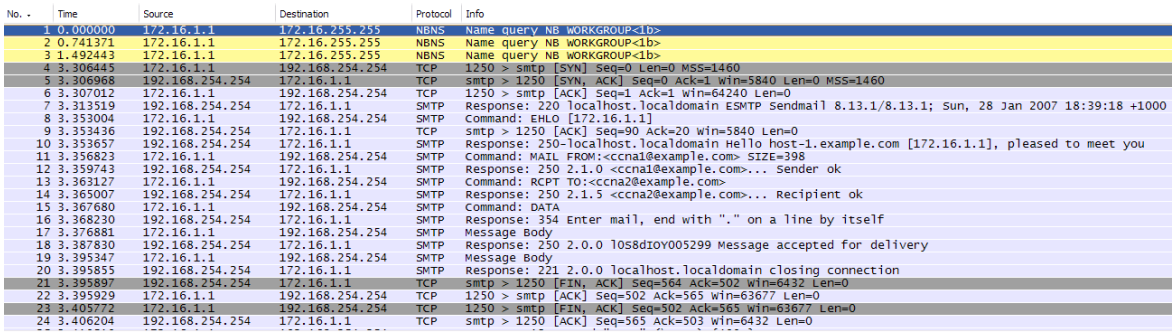
Étape 2 : lancement de la capture à l'aide de Wireshark

Lorsque vous êtes certain du déroulement correct de l'opération en envoi et en réception, démarrez une capture Wireshark. Les résultats s'affichent par type de paquet.

Étape 3 : analyse d'une session de capture de protocole SMTP à l'aide de Wireshark

1. Utilisez à nouveau ce client de messagerie pour envoyer et recevoir un courriel à destination/en provenance d'un autre participant. Cette fois-ci, les transactions seront capturées.
2. Une fois un courriel envoyé et reçu, arrêtez la capture Wireshark. La figure 5 présente une capture partielle Wireshark d'un courriel sortant à l'aide de SMTP.

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.1	172.16.255.255	NBNS	Name query NB WORKGROUP<1b>
2	0.741371	172.16.1.1	172.16.255.255	NBNS	Name query NB WORKGROUP<1b>
3	1.492443	172.16.1.1	172.16.255.255	NBNS	Name query NB WORKGROUP<1b>
4	3.306445	172.16.1.1	192.168.254.254	TCP	1250 > smtp [SYN] Seq=0 Len=0 MSS=1460
5	3.306968	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
6	3.307012	172.16.1.1	192.168.254.254	TCP	1250 > smtp [ACK] Seq=1 Ack=1 Win=64240 Len=0
7	3.313519	192.168.254.254	172.16.1.1	SMTP	Response: 220 localhost.localdomain ESMTP Sendmail 8.13.1/8.13.1; Sun, 28 Jan 2007 18:39:18 +1000
8	3.353004	172.16.1.1	192.168.254.254	SMTP	Command: EHLO [172.16.1.1]
9	3.353436	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [ACK] Seq=90 Ack=20 Win=5840 Len=0
10	3.353657	192.168.254.254	172.16.1.1	SMTP	Response: 250-localhost.localdomain Hello host-1.example.com [172.16.1.1], pleased to meet you
11	3.356823	172.16.1.1	192.168.254.254	SMTP	Command: MAIL FROM:<ccna1@example.com> SIZE=398
12	3.359743	192.168.254.254	172.16.1.1	SMTP	Response: 250 2.1.0 <ccna1@example.com>... Sender ok
13	3.363127	172.16.1.1	192.168.254.254	SMTP	Command: RCPT TO:<ccna2@example.com>
14	3.365007	192.168.254.254	172.16.1.1	SMTP	Response: 250 2.1.5 <ccna2@example.com>... Recipient ok
15	3.367680	172.16.1.1	192.168.254.254	SMTP	Command: DATA
16	3.368230	192.168.254.254	172.16.1.1	SMTP	Response: 354 Enter mail, end with "." on a line by itself
17	3.376881	172.16.1.1	192.168.254.254	SMTP	Message Body
18	3.387830	192.168.254.254	172.16.1.1	SMTP	Response: 250 2.0.0 l0S8dIOY005299 Message accepted for delivery
19	3.395347	172.16.1.1	192.168.254.254	SMTP	Message Body
20	3.395855	192.168.254.254	172.16.1.1	SMTP	Response: 221 2.0.0 localhost.localdomain closing connection
21	3.395897	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [FIN, ACK] Seq=564 Ack=502 Win=6432 Len=0
22	3.395929	172.16.1.1	192.168.254.254	TCP	1250 > smtp [ACK] Seq=502 Ack=565 Win=63677 Len=0
23	3.405772	172.16.1.1	192.168.254.254	TCP	1250 > smtp [FIN, ACK] Seq=502 Ack=565 Win=63677 Len=0
24	3.406204	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [ACK] Seq=565 Ack=503 Win=6432 Len=0

Figure 5. Capture SMTP

3. Sélectionnez la première capture SMTP dans la fenêtre Wireshark supérieure. Dans la figure 5, il s'agit de la ligne 7.
4. Dans la seconde fenêtre Wireshark, développez l'enregistrement Simple Mail Transfer Protocol.

   Il existe différents types de serveurs SMTP. Les pirates malveillants peuvent obtenir des informations vitales par la simple connaissance du type et de la version du serveur SMTP.

Nom et version du serveur SMTP ?

_____

Les applications de client de messagerie électronique envoient des commandes aux serveurs de messagerie électronique et ceux-ci renvoient les réponses. Lors de chaque premier échange SMTP, le client de messagerie électronique envoie la commande **EHLO**. La syntaxe peut cependant varier entre les clients. La commande peut également apparaître sous la forme **HELO** ou **HELLO**. Le serveur de messagerie électronique doit répondre à la commande.

Quelle est la réponse du serveur SMTP à la commande EHLO ?

_____

Les échanges suivants entre le client et le serveur de messagerie électronique contiennent des informations sur le courriel. À l'aide de la capture Wireshark, remplissez les réponses du serveur de messagerie électronique aux commandes du client de messagerie électronique :

Client de messagerie électronique	Serveur de messagerie électronique
MAIL FROM:<ccna1@excmaple.com>	
RCPT TO:<ccna2@example.com>	
DATA	
(le corps du message est envoyé)	

Que contient le corps du dernier message du client de messagerie électronique ?

_____

Comment le serveur de messagerie électronique répond-il ?

_____

_____

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Tâche 3 : confirmation

Utilisez un ordinateur disposant d'un accès à Internet. Jetez un coup d'œil au nom et à la version du serveur SMTP pour en déduire les failles et menaces connues. Une version plus récente est-elle disponible ?

Tâche 4 : remarques générales

La messagerie électronique est probablement le service réseau le plus utilisé. La compréhension du flux du trafic avec le protocole SMTP vous permettra de comprendre comment le protocole gère la connexion des données client/serveur. La messagerie électronique peut également connaître des problèmes de configuration. Le problème se situe-t-il au niveau du client de messagerie ou du serveur de messagerie ? Une façon simple de tester le fonctionnement du serveur SMTP consiste à utiliser la ligne de commande Windows de l'utilitaire Telnet pour établir une connexion Telnet avec le serveur SMTP.

1. Pour tester le fonctionnement du serveur SMTP, ouvrez la fenêtre de ligne de commande Windows et démarrez une session Telnet avec le serveur SMTP.

```
C:\>telnet eagle-server.example.com 25
220 localhost.localdomain ESMTP Sendmail 8.13.1/8.13.1; Sun, 28 Jan
2007 20:41:0
3 +1000
HELO eagle-server.example.com
250 localhost.localdomain Hello [172.16.1.2], pleased to meet you
MAIL From: ccna2@example.com
250 2.1.0 ccna2@example.com... Sender ok
RCPT To: instructor@example.com
250 2.1.5 instructor@example.com... Recipient ok
DATA
354 Please start mail input.
e-mail SMTP server test...
.
250 Mail queued for delivery.
QUIT
221 Closing connection. Good bye.
Connection to host lost.
C:\>
```

Tâche 5 : nettoyage

Si l'installation de Thunderbird a eu lieu sur l'ordinateur hôte pod pour ces travaux pratiques, il se peut que le formateur souhaite la suppression de l'application. Pour supprimer Thunderbird, cliquez sur **Démarrer > Panneau de configuration > Ajout/Suppression de programmes**. Faites défiler la liste jusqu'à **Thunderbird**, puis cliquez sur **Supprimer**.

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.