CommView®

Programme de surveillance et d'analyse réseau pour MS Windows

Guide de l'utilisateur

Introduction

À propos de CommView

CommView est un programme conçu pour contrôler les activités des réseaux Internet et des réseaux Local Area Network (LAN), capable de capturer et d'analyser les paquets de réseau. CommView réunit les informations sur les données qui passent par une connexion modem à accès commuté ou une carte Ethernet, puis décode les données analysées.

Avec CommView, vous pouvez visionner la liste des connexions réseau, ainsi que les statistiques IP vitales, puis examiner les paquets individuellement. Les paquets sont décodés au niveau le plus bas, accompagnés d'une analyse complète des protocoles les plus communs. Un accès entier aux données non traitées est aussi fourni. Les paquets capturés peuvent être enregistrés, afin d'enregistrer les fichiers pour fins d'analyse future. Un système flexible de filtres permet l'abandon de paquets dont vous n'avez pas besoin, ou de la capture de seulement ceux que vous souhaitez capturer. Des alarmes configurables peuvent vous notifier à propos d'événements importants, tels que des paquets suspects, une utilisation élevée de la bande passante ou des adresses inconnues.

CommView est un outil utile pour les administrateurs de LAN, les professionnels en sécurité, les administrateurs de réseau ou toute personne souhaitant avoir une image nette du trafic circulant sur un ordinateur ou un segment LAN. Cette application est conçue pour les utilisateurs d'Internet, ainsi que pour les petits et moyens réseaux, et peut opérer sur n'importe quel système Windows 95/98/Me/NT/2000/XP/2003 ou Windows XP édition 64-bit pour processeurs AMD Opteron et Athlon64. CommView requiert une carte Ethernet, une carte réseau sans fil Ethernet ou une carte de réseau en anneau à jeton prenant en charge le pilote NDIS 3.0 standard, ou une connexion par modem à accès commuté standard.

CommView procure le décodage complet des protocoles suivants : ARP, BCAST, BGP, BMP, CDP, DAYTIME, DDNS, DHCP, DIAG, DNS, EIGRP, FTP, G.723, GRE, H.225, H.261, H.263, H.323, HTTP, HTTPS, ICMP, ICQ, IGMP, IGRP, IMAP, IPsec, IPv4, IPv6, IPX, HSRP, LDAP, MS SQL, NCP, NDS, NetBIOS, NFS, NLSP, NNTP, NTP, OSPF, POP3, PPP, PPPoE, RARP, RADIUS, RDP, RIP, RIPX, RMCP, RPC, RSVP, RTP, RTCP, RTSP, SAP, SER, SIP, SMB, SMTP, SNA, SNMP, SNTP, SOCKS, SPX, SSH, TCP, TELNET, TFTP, TIME, TLS, UDP, VTP, WAP, WDOG, YMSG, 802.1Q, 802.1X.

En supplément, notre nouvelle technologie de contrôle à distance permet aux utilisateurs de CommView de capturer le trafic de réseau sur n'importe quel ordinateur où Remote Agent opère, sans tenir compte de l'emplacement physique de l'ordinateur. Afin de prendre avantage de cette caractéristique unique, vous devez installer CommView Remote Agent, un addiciel à CommView à prix abordable.

Quoi de neuf

Version 5.0

- Les paquets sont mappés vers l'application qui les a reçus ou émis (fonctionnalité disponible sous Windows2000/XP/2003).
- Horodatage haute résolution (jusqu'à la microseconde, disponible sous Windows NT/2000/XP/2003).
- Nouveau format de journal compact et ouvert.
- Matrices graphiques représentant les conversations entre machines hôte.
- De nouveaux modules de décodage ont été ajoutés: MS SQL, LDAP, et YMSG. Les décodages de SMB et ICQ ont été améliorés.
- Support de Windows XP édition 64-bit pour processeurs AMD Opteron et Athlon64.
- Les connexions multiples d'agents distants sont maintenant supportées.
- Générateur de paquets amélioré incluant l'ajout de modèles prédéfinis.
- Les rapports HTML peuvent inclure des graphiques.
- Nouveaux types d'alarmes.
- Moins d'utilisation du CPU.

Version 4.1

- Vous pouvez maintenant capturer les paquets de boucle envoyés de/vers des adresses IP locales, par exemple 127.0.0.1 (cette fonctionnalité est disponible sous Windows NT/2000/XP/2003).
- Le programme peut journaliser les adresses Web visitées.
- De nouveaux protocoles de décodage ont été ajoutés : IMAP, NNTP, SSH, TLS.
- Une interface de module d'extension ouverte vous permet d'implémenter votre propre protocole de décodage.
- Les fenêtres de Reconstruction de session TCP peuvent maintenant décompresser le contenu Web GZIP, puis afficher les images envoyées par l'entremise de sessions TCP.
- Les fenêtres de Reconstruction de session TCP vous permettent maintenant de sauter vers la session TCP suivante entre deux hôtes, n'importe lesquels (dans les versions précédentes, vous ne pouviez sauter à la session suivante entre les deux hôtes sélectionnés).
- Le programme notifie maintenant toute modification apportée à la liste des adaptateurs réseau.
- La capture est automatiquement redémarrée après une hibernation ou un suspension de Windows.
- Les cartes de réseau en anneau à jeton sont maintenant prises en charge (cette fonctionnalité est disponible sous Windows 2000/XP/2003).
- Les trames géantes sont maintenant prises en charge.
- Vous pouvez faire en sorte que le programme génère des statistiques des données précapturées, en plus des statistiques en temps réel.
- La fonctionnalité d'alarme améliorée vous permet de passer des variables aux applications en exécution ou aux messages d'alarme.
- Quelques autres améliorations mineures.

Version 4.0

- Alarmes : Vous pouvez configurer le programme, afin d'être alerté à propos de certaines occurrences de paquets, comme des adresses MAC inconnues, et ainsi de suite.
- De nouveaux modules de décodage de protocoles ont été ajoutés : DAYTIME, DDNS, H.323 (H.225, Q.850, Q.931, Q.932), HTTPS, NTP, RMCP, RTP/RTCP (G.723, H.261, H.263), SNTP, TIME.
- Interface multilingue.
- Un module de décodage personnalisé peut être utilisé avec le programme.
- De nouveaux paramètres de lignes de commande vous permettent de charger des ensembles de règles automatiquement et/ou des adaptateurs ouverts.
- Les fenêtres de reconstruction de sessions TCP possèdent maintenant la fonction << Rechercher >>.
- Des modèles de paquet TCP, UDP et ICMP dans le Générateur de paquets.
- Une nouvelle fonction << Décoder sous >> qui peut être utilisée pour décoder des protocoles pris en charge et utilisant des ports non standard.
- De nombreuses nouvelles options configurables.

Version 3.4

- Des nouveaux modules de décodage de protocoles ont été ajoutés : BGP, EIGRP, IGRP, IPsec, GTP, HSRP, NFS, OSPF, RADIUS, RIP, SNA, VTP, WAP, 802.1Q, 802.1X.
- De nouveaux outils de gestion de fichiers journaux vous permettent de partager/concaténer les fichiers CCF qui ont été ajoutés.
- Les fenêtres de reconstruction de sessions TCP permettent maintenant de sauter à la session suivante entre les deux hôtes.
- De nouvelles caractéristiques dans la fenêtres Statistiques : bascule de bits par seconde à octets par secondes, indicateur de l'utilisation de la bande passante, graphiques de protocole IP ou de sous-protocole par nombre d'octets ou par nombre de paquets.
- Un mode non-espion optionnel.
- L'importation de fichiers capturés dans MS NetMon et NAI Sniffer pour les formats de Windows.
- La surbrillance de syntaxe dans la fenêtre de formule avancée.
- Une amélioration du support des thèmes de Windows XP.

- Une réparation de bogues importante dans la fonction hex de règles avancées; cette fonction ne s'effectuait pas correctement pour les modèles d'octet incluant 0x00.

Version 3.3

- Des règles avancées qui permettent de créer des filtres complexes en utilisant la logique booléenne simple, une syntaxe facile à comprendre.
- De nouveaux modules de décodage de protocoles ont été ajoutés : FTP, TFTP, SOCKS (v. 4,5), TELNET.
- Encore une autre amélioration de la performance.
- De nouvelles caractéristiques du Générateur de paquets : prise en charge de la fonctionnalité glisser-déposer pour n'importe quel format de paquet, la génération de paquets à haute vitesse (plus de 5,000 paquets/sec) et la capacité d'envoyer plusieurs paquets différents au moyen d'un simple clic de souris.
- Option de concaténation des fichiers journaux en un seul fichier lorsque le programme arrête la capture.
- Nouveaux formats d'exportation : fichiers séparés par des points-virgules avec ou sans données hexadécimales.
- Vous pouvez maintenant enregistrer les paquets sous différents formats (CCF, ENC, et ainsi de suite) directement, sans avoir à charger d'abord les fichiers capturés dans l'Éditeur de fichiers journaux.
- Les tables d'hôtes LAN peuvent maintenant traiter plus de 1 000 adresses MAC et IP.
- Une option << Taille >> des colonnes est disponible dans la liste de paquets.
- Vous pouvez définir les adresses réseau et les masques de sous-réseau pour les adresses IP que vous voulez traiter par le programme localement.
- Plusieurs améliorations mineures et réparations de bogues.

Version 3.2

- De nouveaux modules de décodage de protocoles ont été ajoutés : SNMP (v. 1,2,3), IPv6, ICQ, GRE, RDP.
- Une amélioration majeure de la performance lorsque ouvrant/important : les fichiers sont chargés jusqu'à 25 fois plus rapidement.
- Un usage moins grand du processeur.
- Des statistiques NIC étendues, telles que les collisions et erreurs CRC, sont disponibles.
- La possibilité d'appliquer des règles aux données pré-capturées dans l'Éditeur de fichiers journaux.
- Un dialogue Rechercher un paquet amélioré.

Version 3.1

- De nouveaux modules de décodage de protocoles ont été ajoutés : DHCP, DNS, HTTP, POP3, RTSP, SMTP.
- Une nouvelle et unique technologie de contrôle à distance.
- La possibilité d'ajouter jusqu'à 4 protocoles conventionnels au registre de sous-protocoles IP.
- La possibilité d'importer des fichiers capturés en format Tcpdump (libcap).
- Plus d'options de configuration ajoutées.
- Plusieurs améliorations mineures et réparations de bogues.

Version 3.0

- Un nouveau module de décodage de protocoles; prenant maintenant en charge ARP, BCAST, BMP, DIAG, ICMP, IGMP, IPv4, IPX, NCP, NDS, NetBIOS, NLSP, PPP, PPPoE, RARP, RIPX, RSVP, SAP, SER, SMB, SPX, TCP, UDP, WDOG. Plus de protocoles à venir sous peu.
- Support pour les adaptateurs d'Ethernet (802.11b) sans fil.
- Le programme est prêt pour Windows XP (testé avec RC1).
- Le Générateur de paquets peut maintenant envoyer des paquets via une connexion par modem à accès commuté sur Windows 2000/XP.
- Un décodeur de protocoles et un correcteur de somme de contrôle ont été ajoutés au Générateur de paquets.
- L'option d'exécuter plusieurs instances de CommView pour contrôler plusieurs adaptateurs simultanément.
- Les statistiques IP peuvent être incluses dans le Rapport de statistiques.
- Un nouvel hôte de LAN par table d'adresses IP a été ajouté à la fenêtre Statistiques.
- La fenêtre Reconstruction de sessions TCP permet d'exclure/inclure les données basées sur la direction du paquet.
- La possibilité de filtrer les paquets selon les flags TCP.
- Le programme peut être exécuté en mode invisible.
- La possibilité de partager les données de CommView avec votre propre application utilisant une interface TCP/IP simple.
- L'onglet Paquets vous permet de sélectionner plusieurs paquets.

Version 2.6

- Les alias peuvent être assignés aux adresses IP.
- Des règles courantes peuvent être appliquées à la fenêtre Statistiques et à son onglet Rapport.
- Décodage de PPPoE.
- La fenêtre Reconstruction de sessions TCP, maintenant non-modale, vous permet d'avoir plusieurs fenêtres ouvertes avec différentes sessions.
- Des améliorations mineures à l'interface et autres réparations de bogues.

Version 2.5

- Un support complet de la fonctionnalité glisser-déposer : vous pouvez maintenant glisser les statistiques IP, les paquets individuels et les graphiques, puis les déposer sur votre bureau ou dans n'importe quel dossier. Vous pouvez glisser les fichiers capturés (CCF, ENC ou BFR) et les déposer dans l'application.

- Un Graphique de distribution de la taille du paquet et des Tables d'hôtes LAN ont été ajoutés à la fenêtre Statistiques.
- Génération de rapport automatique ou manuelle : toutes les données statistiques peuvent être sauvées en HTML ou en rapports délimités par des points-virgules. (Voir l'onglet << Rapport >> de la fenêtre Statistiques.)
- La fenêtre Reconstruction de sessions TCP vous permet maintenant de visionner les données en HTML et en EBCDIC, en plus des formats ASCII et HEX.

Version 2.4

- Reconstruction de session TCP.
- Les alias peuvent être assignés aux adresses MAC.
- Identificateur de fournisseur NIC.
- Plus de colonnes sont disponibles dans les onglets << Statistiques IP >> et << Paquets >>.
- Les colonnes des onglets << Paquets >> et << Statistiques IP >> peuvent être masquées.
- Les paquets ARP/RARP sont décodés.
- Les jokers peuvent être utilisées dans les règles d'adresses IP.
- L'option << Les deux >> pour la capture de règles est disponible, en addition aux options << De >> et << À >>.
- Les onglets avec règles actives sont maintenant disposés en caractère gras.
- Les données sortantes des paquets peuvent être suspendues/reprises.
- Plusieurs alternatives de mise en page des statistiques IP sont disponibles.
- Autres améliorations mineures.

Version 2.3

- Support des connexions par modem à accès commuté sous Windows 2000.

Version 2.2

- Les entêtes de MAC, IP, et TCP/UDP/ICMP sont colorées.
- Le contenu de l'onglet Statistiques IP peut être enregistré en fichier HTML.
- L'ajout du Générateur de paquets vous permet d'envoyer des paquets.
- Les configurations de règles peuvent être enregistrées/chargées.
- Les règles en texte peuvent maintenant respecter la casse.
- Le dialogue Rechercher le contenu d'un paquet est amélioré.
- Bogue réparé : les problèmes avec le démarrage du pilote sur les systèmes localisés de Windows 2000 ont été résolus.

Version 2.1

- Éditeur de fichiers journaux : Vous pouvez maintenant charger et explorer les fichiers capturés, tout comme vous le faites avec les données capturées en temps réel.
- Vous pouvez importer et exporter des fichiers capturés de/à NIC Observer ou de fichiers en format NAI Sniffer.
- Les nunméros de ports peuvent être affichés en noms de service.
- Une nouvelle option << Sauter vers >> vous permet de retrouver rapidement des paquets allant/venant d'une adresse IP donnée.
- Quelques améliorations à l'interface.
- Bogue réparé : les versions précédentes montraient une somme de contrôle UDP incorrecte.

Version 2.01

- Support de Windows 2000.

Version 2.0 Final

- Performance améliorée sur les systèmes Windows NT.
- Quelques bogues trouvés dans 2.0 Beta ont été réparés.

Version 2.0 Beta

- Support de Windows NT.
- Plus d'informations statistiques.

Version 1.0 Final

- Nouvelles fonctions : Rechercher un paquet et Aller au numéro de paquet.
- Nouveaux filtres : Capturer/ignorer les paquets basés sur les adresses MAC et la direction des paquets.
- Statistiques : Histogrammes de paquets par seconde et octets par seconde, graphiques de distribution de protocoles et de sous-protocoles IP.
- Bogue réparé : Le filtre texte dans la version 1.0 Beta pouvait parfois capturer les paquets qui ne contenaient pas de texte spécifique; ce problème a été réglé.

Licence d'utilisation

Veuillez lire attentivement les conditions et modalités suivantes avant d'utiliser ce logiciel. Votre utilisation de ce logiciel indique votre consentement à cette licence d'utilisation. Si vous n'êtes pas d'accord avec les conditions de cette licence, vous devez enlever ce logiciel de vos périphériques de stockage et cesser l'utilisation de ce produit.

Copyright
Ce logiciel est légalement déposé 1999-2004 par TamoSoft. CommView est une marque de commerce déposée de TamoSoft. L'utilisation et les droits réservés de ce logiciel sont gouvernés par des traités internationaux de droits réservés et légalement déposés. TamoSoft. conserve les titres complets et les droits de ce logiciel et de cette documentation, et en aucun cas l'accord de licence ne diminue les droits de propriété intellectuelle de TamoSoft. Vous ne devez pas redistribuer les codes d'enregistrement procurés—sur papier, éléctroniquement, ou sous toute autre forme.

Version d'évaluation
Ce logiciel n'est pas gratuit. Vous êtes de ce fait licencié pour utiliser ce logiciel pour fins d'évaluation, sans frais pour une période de 30 jours. Utiliser ce logiciel après cette période d'évaluation viole les lois de droits réservés et peut résulter en de sévères pénalités civiles et criminelles.

Version enregistrée (licenciée)
Une copie enregistrée de ce logiciel peut être utilisée par un seule personne qui utilise personnellement ce logiciel sur un ou plusieurs ordinateurs, ou elle peut être installée sur une station de travail simple utilisée non-simultanément par plus d'une personne, mais pas les deux. La Licence Personnelle impose des restrictions sur l'utilisation et les fonctionnalités du logiciel. La liste de ces limitations est sujette à modification sans préavis. Cette liste est disponible sur le site internet de Tamosoft. Ce logiciel peut être installé sur un serveur de réseau, munie d'une licence séparée, appropriée pour l'utilisation de ce logiciel et reçue par TamoSoft. pour chacun des terminaux ayant accès à ce logiciel.

Avis de non-responsabilité
TAMOSOFT NE GARANTI PAS QUE LE PRODUIT EST SANS ERREURS. CE LOGICIEL EST FOURNI << TEL QUEL >> SANS GARANTIE D'AUCUNE SORTE, SOIT EXPRIMÉE OU IMPLIQUÉE, INCLUANT, MAIS NON-LIMITÉE AUX, LES GARANTIES DE MARCHANDAGE OU DE FONCTIONNALITÉ POUR DES FINS PARTICULIÈRES. EN AUCUN CAS TAMOSOFT. NE SERA RESPONSABLE ENVERS VOUS POUR TOUT DOMMAGE, INCLUANT LES DOMMAGES ACCIDENTELS OU INDIRECTS, RÉSULTANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI AVISÉ(E) DE LA POSSIBILITÉ DE TELS DOMMAGES. VOUS CONSENTEZ ET ACCEPTEZ QUE VOUS AVEZ LU CETTE LICENCE, QUE VOUS L'AVEZ COMPRISE ET QUE VOUS ACCEPTEZ D'ÊTRE OBLIGÉ(E) PAR SES TERMES.

Loi Gouvernante
Cette Licence d'utilisation sera gouverné par les lois de la Nouvelle-Zélande.

Distribution
Ce logiciel peut être distribué gratuitement dans sa forme originale non-modifiée et non-enregistrée. La distribution doit inclure tous les fichiers de sa distrbution originale. Les distributeurs ne peuvent charger aucun frais pour sa distribution. Toute personne distribuant ce logiciel pour quelque sorte de rémunération doit d'abord nous contacter pour une autorisation.

Autres Restrictions
Vous ne pouvez pas modifier, faire de l'inginérie inverse, décompiler ou désassembler ce logiciel en aucune façon, incluant changer ou enlever tout message ou fenêtre.

Utilisation de CommView

Aperçu

L'interface du programme consiste en cinq onglets qui vous permettent de visionner les données et d'exécuter des actions variées avec les paquets capturés. Pour commencer à capturer les paquets, sélectionnez un adaptateur de réseau à partir de la liste du menu déroulant sur la barre d'outils, puis cliquez sur le bouton **Démarrer la capture** ou sélectionnez **Fichier = > Démarrer la capture** à partir du menu. Si le trafic du réseau passé par l'adaptateur de réseau est sélectionné, CommView va commencer à afficher les informations.

Main Menu

Fichier

Démarrer/Arrêter la capture – démarrer/arrêter la capture des paquets.
Suspendre/Reprendre les données de paquet – suspendre/reprendre les données de paquets en temps réel sur le 2ème onglet.
Mode de surveillance à distance – afficher/masquer la barre d'outils de la surveillance à distance .
Enregistrer les Dernières Connexions IP sous – permet d'enregistrer le contenu de l'onglet des Dernières Connexions IP en tant que fichier HTML formaté CSV (les champs séparés par des virgules).
Enregistrer le fichier journal de paquets sous –permet d'enregistrer le contenu de l'onglet Paquets sous différents formats. Utilisez l'onglet Journalisation pour les options avancées d'enregistrement.
Editeur de fichiers journaux – ouvre une nouvelle fenêtre de l'Éditeur de fichiers journaux .
Effacer les Dernières Connexions IP – efface la liste des Dernières Connexions IP (1er onglet).
Effacer la mémoire tampon de paquets – efface le contenu de la mémoire tampon du programme et de la liste de paquets (2ème onglet).
Données de performance – affiche les statistiques de la performance du programme : le nombre de paquets capturés et abandonnés par le logiciel de pilotage. Cette commande n'est pas disponible sous Windows 95/98/Me.
Quitter – ferme le programme.

Recherche

Rechercher un paquet – affiche un dialogue qui vous permet de rechercher les paquets correspondant à un texte spécifique.
Aller au numéro de paquet – affiche un dialogue qui vous permet de sauter à un paquet au moyen du numéro spécifié.

Affichage

Statistiques – affiche une fenêtre avec des statistiques de transfert de données et des statistiques de distribution de protocole.
Référence de port – affiche une fenêtre avec des informations de référence sur le port.
Répertoire du fichier journal – ouvre le repértoire où les fichiers journaux sont enregistrés par défaut.
Dernières connexions IP – afficher/masquer les colonnes de l'onglet Dernières Connexions IP.
Colonnes de paquets – afficher/masquer les colonnes de l'onglet Paquets.

Outils

Générateur de paquets – ouvre la fenêtre du Générateur de paquets (non disponible sous Windows 95/98/Me)..
Reconstructeur de session TCP – vous permet de reconstruire une session TCP en partant du paquet sélectionné; ouvre une fenêtre qui affiche la conversation complète entre deux hôtes.
Identificateur de fournisseur NIC – ouvre une fenêtre où vous pouvez identifier un fournisseur d'adaptateurs réseau par adresse MAC.
Planificateur – vous permet d'ajouter ou de supprimer des tâches de .

Paramètres

Polices – affiche le sous-menu pour configurer les polices des éléments de l'interface.
Alias MAC – ouvre une fenêtre où vous pouvez assigner des alias faciles à mémoriser aux adresses MAC.
Alias IP – ouvre une fenêtre où vous pouvez assigner des alias faciles à mémoriser aux adresses IP.
Options – ouvre la fenêtre Options où des options supplémentaires avancées peuvent être configurées.
Langue – vous permet de modifier la langue de l'interface. Assurez-vous de bien relancer le programme une fois que vous avez modifié la langue. Le fichier d'installation de CommView peut ne pas contenir toutes les langues disponibles pour l'interface. Cliquez sur le menu **Autres Langues** pour accéder à la page de téléchargement de notre site internet ou vous pourrez télécharger le fichier correspondant à votre langue, si celle-ci est disponible pour la version actuelle du logiciel.
Installer le pilote par accès commuté – installe un pilote pour la capture des paquets sur les adaptateurs par accès commuté. Cet élément n'est disponible que sous Windows 2000/XP/2003 ; Windows 95/98/ME/NT ne requiert pas ce pilote. Cet élément est invisible si le pilote est installé.
Installer le pilote par boucle – installe un pilote pour la capture de paquets par boucle, c'est-à-dire des paquets envoyés de/vers des adresses IP locales, comme 127.0.0.1. Cet élément n'est disponible que sous Windows NT/2000/XP/2003 ; Windows 95/98/ME ne prend pas en charge la capture par boucle. Cet élément est invisible si le pilote est installé. Vous serez invité à redémarrer l'ordinateur lorsque ce pilote aura été installé.
Installer le pilote par anneau à jeton – installe un pilote pour la capture de paquets sur les adaptateurs par anneau à jeton. Cet élément n'est disponible que sous Windows 2000/XP/2003. Sous Windows 95/98/ME/NT, CommView ne prend pas en charge les adaptateurs par anneau à jeton. Cet élément est invisible si le pilote est installé.

Règles

Enregistrer les règles actuelles sous – vous permet d'enregistrer les règles actuelles de configuration à un dossier.
Charger les règles de – vous permet de charger des règles de configuration préalablement enregistrées dans un dossier.
Réinitialiser tout – efface toutes les règles existantes (si lieu).

Aide
Contenu – affiche l'aide de CommView.
Rechercher l'aide sur ... – affiche l'index d'aide de CommView.
Manuel d'apprentissage en ligne – lance votre navigateur internet pour accéder au manuel d'apprentissage en ligne de CommView.
À propos – affiche les informations à propos du programme.

Presque tous les éléments de l'interface possèdent un menu sensible au contexte (pop-up), lequel peut être invoqué en cliquant sur le bouton droit de la souris. Plusieurs commandes sont également disponibles seulement à travers ces menus.

Le premier onglet est utilisé pour afficher les informations détaillées sur les connexions réseau (protocole IP seulement) de votre ordinateur. Pour plus d'informations, consultez le chapitre Dernières Connexions IP.

Le second onglet est utilisé pour afficher les paquets de réseau capturés et les informations détaillées sur un paquet sélectionné. Pour plus d'informations, consultez le chapitre Paquets.

Le troisième onglet vous permet de enregistrer des paquets capturés dans des dossiers. Pour plus d'informations, consultez le chapitre Journalisation.

Le quatrième onglet est pour configurer les règles qui vous permettent de capturer/ignorer des paquets, basés sur des critères variés, tel que les adresse IP ou le nombre de port. Pour plus d'informations, consultez le chapitre Règles.

Le cinquième onglet vous permet de créer des alarmes pour vous alerter lors d'événements importants, comme des paquets suspects, une utilisation élevée de la bande passante, des adresses inconnues, et ainsi de suite. Pour de plus amples informations, consultez le chapitre Alarmes.

Vous pouvez modifier certaines des configurations, tells que les fontes, les couleurs, ainsi que la taille de la mémoire tampon en sélectionnant **Paramètres** à partir du menu. Pour plus d'informations, consultez le chapitre Configuration des options.

Sélectionner un périphérique réseau à surveiller

La surveillance de votre connexion réseau commence par la sélection du périphérique que vous voulez surveiller. Choisir le bon périphérique est crucial pour arriver aux résultats escomptés. Nous avons essayé de rendre CommView aussi simple et convivial que possible, les seules étapes nécessaires pour commencer la surveillance de votre réseau consistent à sélectionner un périphérique dans la liste déroulante de la barre d'outils et à cliquer sur le bouton **Démarrer la capture**.

Alors que les technologies réseaux se développent, de plus en plus de périphériques différents apparaissent sur le marché: WiFi, xDsl, et ainsi de suite. CommView supporte la plupart d'entre eux; néanmoins, chaque type de connexion réseau possède des particularités que vous devez connaître en vue d'effectuer une surveillance efficace.

Enumérons ensemble la liste des périphériques réseau les plus répandus et regardons de quelle manière CommView se comporte et devrait être configuré.

Durant l'installation, CommView détecte les périphériques réseau disponibles sur votre système. Une des étapes du script d'installation vous proposera d'installer un pilote de Connexion Distante. Vous devez cliquer sur **Oui** si vous désirez surveiller une connexion via un modem RTC (réseau téléphonique commuté) ou xDSL, ou utiliser PPPoE/VPN avant tout autre type de connexion réseau. Si vous cliquez **Non**, vous pourrez toujours installer le pilote ultérieurement en allant dans le menu **Paramètres => Installer le Pilote de Connexion Distante**. Durant l'installation de ce pilote, vos liens réseau seront temporairement indisponibles.

Lorsque l'installation est terminée, lancez CommView et cliquez sur la liste déroulante dans la barre d'outils. Vous pourrez y voir le périphérique de connexion en Boucle Locale (non disponible sous Windows 98/ME), votre périphérique de connexion au Réseau Local (si vous en possédez un), et le périphérique de Connexion Distante (si vous avez choisi d'installer le pilote de Connexion Distante).

Examinons ensemble à quoi correspondent ces entrées au niveau du matériel installé dans votre ordinateur et des types de connexions réseau disponibles.

Si vous êtes connecté au réseau via un **périphérique Ethernet** ordinaire, sélectionnez le dans la liste déroulante et commencez la surveillance. CommView supporte, virtuellement, tout périphérique Ethernet 10, 100 ou 1000 Mbit disponible sur le marché.

Si vous utilisez un modem pour vous connecter au réseau, sélectionnez le **périphérique de Connexion Distante**. Notez que vous pourrez seulement voir les paquets entrants et sortants (et non ceux en transit) dans CommView. Ce n'est pas une limitation de CommView. C'est ce qui caractérise toute connexion de type point-à-point; seul deux hôtes, un hôte local et un hôte distant, participent à la connexion. Si vous utilisez ICS, vous allez capturer tous les paquets en direction ou en provenance des clients ICS.

Si vous voulez utiliser CommView pour surveiller un réseau sans fil aux normes 802.11 a, b ou g, sélectionnez le **périphérique Wi-Fi**. Les pilotes génériques ne peuvent pas utiliser les périphériques Wi-Fi en mode passif (promiscuous); CommView affichera les paquets entrants et sortants, de même que les paquets multipoints/diffusés. Les en-têtes de paquets 802.11 ne seront pas affichées. Si vous recherchez une solution de surveillance en mode passif pour les réseaux de type 802.11 a/b/g, essayez CommView pour WiFi qui utilise votre périphérique en mode de surveillance passive vous permettant ainsi de capturer le traffic en provenance d'autres stations et points d'accès sans fil. CommView pour WiFi peut être téléchargé depuis le site internet de TamoSoft.

Si vous êtes connecté au réseau via un modem **xDSL** avec une **interface USB**, vous pourrez certainement surveiller cette connexion avec CommView. Officiellement, nous ne supportons pas les interfaces USB dans CommView, le mieux est donc de tester. Dans la plupart des cas, la connexion actuelle au réseau sera établie à partir d'une liaison PPPoE, auquel cas vous devrez sélectionner le périphérique de Connexion Distante pour pouvoir capturer le traffic sur le réseau.

Si votre **modem xDSL** possède une **interface Ethernet**, mais que la connexion actuelle se fait au travers d'une liaison PPPoE, sélectionnez le périphérique de Connexion Distante pour surveiller le traffic réseau à destination ou en provenance de votre ordinateur, et les paquets multipoints/diffusés. Si vous sélectionnez votre périphérique Ethernet, vous serez capable de capturer tous les paquets sur le LAN, néammoins ils seront encapsulés PPPoE et ainsi être cryptés.

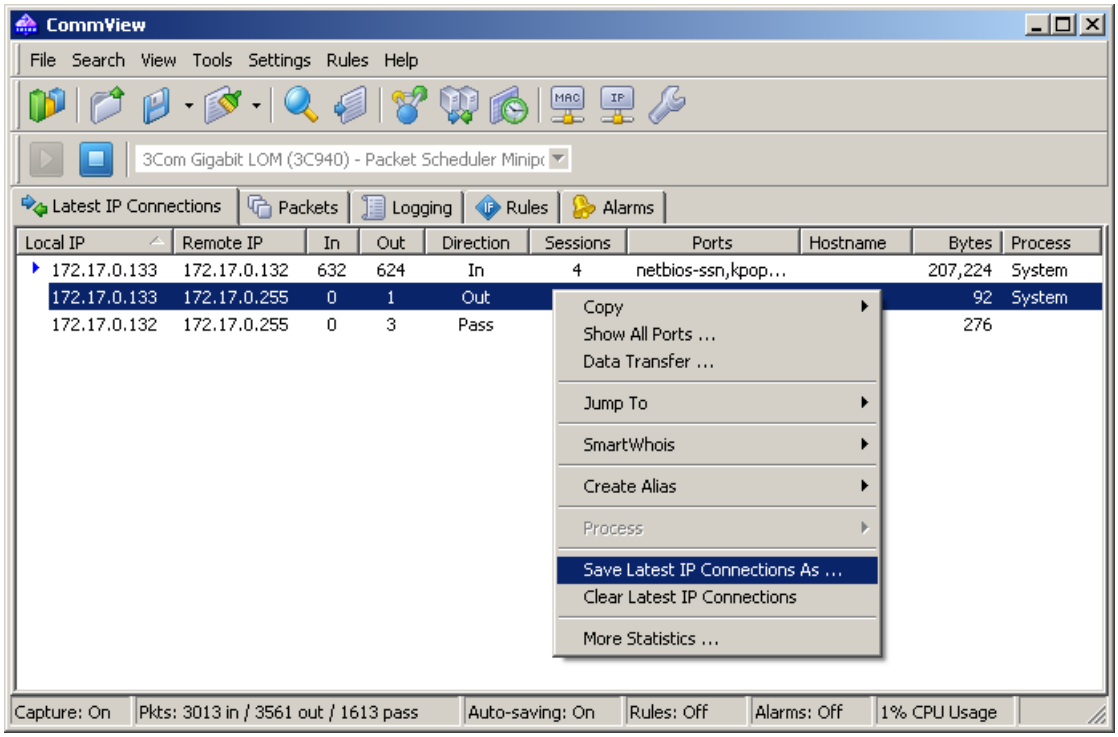
Si vous êtes connectés au réseau via une liaison sécurisé **VPN**, la surveillance de votre périphérique réseau Ethernet vous permettra seulement de capturer des paquets cryptés. Dans ce cas vous devrez surveiller le périphérique de Connexion Distante pour capturer les données actuellement transmises.

Si vous possédez plusieurs périphériques réseau **reliés en Pont** dans votre ordinateur, surveiller le Pont montrera le traffic entrant et sortant de chaque périphérique appartenant au Pont, les paquets multipoints/diffusés, et les paquets redirigés vers un autre Pont.

La surveillance du **périphérique de Boucle Locale** vous montrera le traffic local envoyé ou reçu via TCP/IP par les programmes tournant sur votre ordinateur. Si vous avez des programmes actifs qui échangent des données localement, vous ne verrez aucun traffic en surveillant le périphérique de Boucle Locale. Notez que le Générateur de Paquets ne fonctionnera pas avec ce périphérique. Pour plus d'information, veuillez consulter le chapitre Capture du Traffic en Boucle Locale.

Dernières Connexions IP

Ce onglet est utilisé pour afficher les informations détaillées à propos des connexions réseau (protocole IP seulement) de votre ordinateur. Pour commencer à capturer des paquets, sélectionnez **Fichier = > Démarrer la capture** à partir du menu ou cliquez le bouton approprié sur la barre d'outils.



La définition de chaque colonne est expliquée ci-dessous :

IP locale – affiche l'adresse IP locale. Pour les paquets entrants, c'est l'adresse de destination IP; pour les paquets sortants et transitants, c'est l'adresse source IP.
IP à distance – affiche l'adresse à distance IP. Pour les paquets entrants, c'est l'adresse source IP; pour les paquets sortants et transitants, c'est l'adresse de destination IP.
Entrant – affiche le nombre de paquets reçus.
Sortant – affiche le nombre de paquets envoyés.
Direction – affiche la direction de la session. La direction est déterminée selon la direction du premier paquet reçu de et envoyé à l'adresse à distance IP.
Sessions – affiche le nombre de sessions TCP/IP établies. Si aucune connexion TCP n'a été établie (la connexion a échoué, ou le protocole est UDP/IP ou ICMP/IP), cette valeur est de zéro.
Ports – liste les ports d'ordinateurs à distance utilisés durant la connexion TCP/IP ou la tentative de connexion. Cette liste peut être vide si le protocole n'est pas TCP/IP. Les ports peuvent être affichés en valeurs numériques et en noms de service correspondants. Pour plus d'informations, consultez le chapitre Configuration des options.
Nom d'hôte – affiche le nom d'hôte de l'ordinateur à distance. Si le nom d'hôte ne peut être résolu, cette colonne est vide.
Octets – affiche le nombre d'octets transmis durant la session.
Denier paquet – affiche l'heure du dernier paquet envoyé/reçu durant la session.
Processus – indique le processus local qui a envoyé ou reçu les paquets durant la session. Cette colonne est uniquement disponible sous Windows 2000/XP/2003. Le mappage des paquets vers les processus qui les ont émis ou reçus fonctionne uniquement pour les paquets entrants et sortants, CommView ne pouvant être conscient des processus tournant sur d'autres ordinateurs émettant ou recevant des paquets. Naturellement, comme il peut y avoir plusieurs applications sur l'ordinateur local qui échangent des données avec le même ordinateur distant, l'onglet des **Dernières Connexions IP** montre uniquement le dernier processus ayant reçu ou émis des données pour cette même paire d'adresses IP. Si vous désirez mapper un paquet donné vers le processus qui l'a émis ou reçu, vous pouvez voir l'information au niveau de l'onglet **Paquets**, dans le volet de décodage de l'en-tête. CommView peut afficher le répertoire du processus qui a émis ou reçu les paquets, cochez la case **Afficher le Chemin Complet** dans le menu **Paramètres => Options**, onglet **Général** pour activer cette fonctionnalité.

Vous pouvez afficher ou masquer les colonnes individuellement en cliquant l'élément approprié dans le menu **Affichage** => **Colonnes des Dernières Connexions IP**.

Commandes du menu

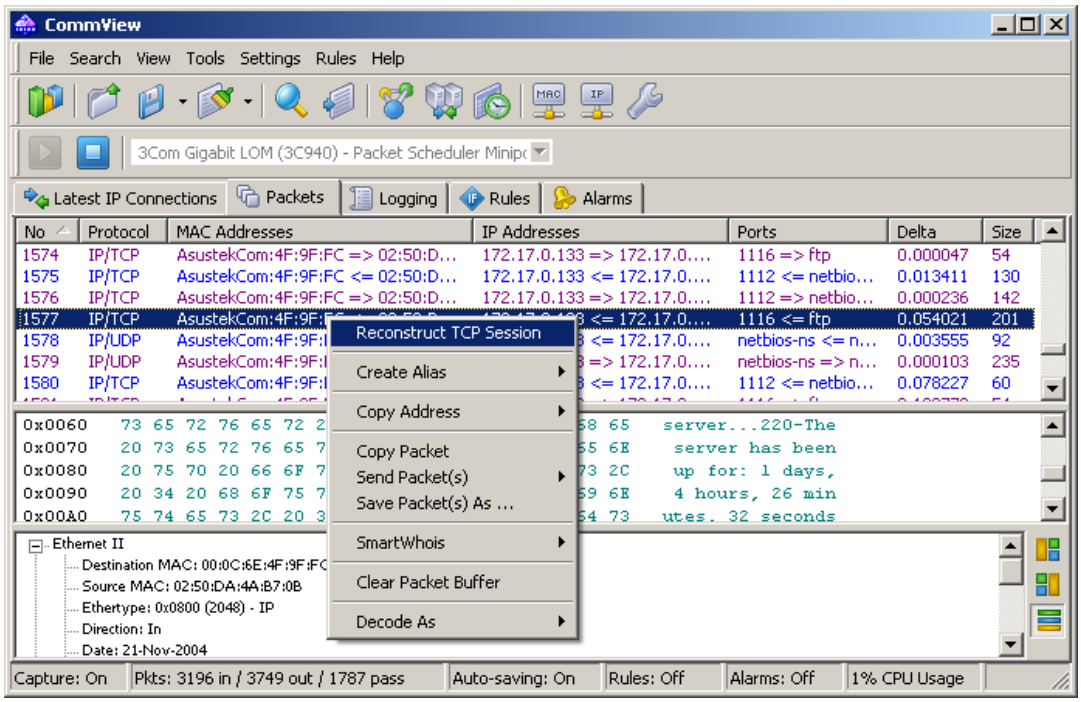
En cliquant le bouton droit de la souris sur la liste des Dernières Connexions IP, un menu apparaît et conporte les commandes suivantes :

Copier – copie l'adresse IP locale, l'adresse à distance IP ou le nom d'hôte sur le presse-papiers.

Afficher tous les ports – affiche une fenêtre avec une liste complète des ports utilisés lors de la communication entre la paire sélectionnée d'adresses IP. Ceci est très utile lorsque plusieurs ports ont été utilisés, et qu'ils ne correspondent pas à la colonne sélectionnée.
Transfert de données – affiche une fenêtre avec les informations à propos du volume de transfert de données entre la paire d'adresses IP sélectionnée et l'heure du dernier paquet.
Sauter vers – vous permet de sauter rapidement au premier/dernier paquet avec l'adresse source ou destination IP sélectionnée; le programme affichera l'onglet Paquets et positionnera le curseur de la souris au paquet correspondant aux critères.
SmartWhois – envoie l'adresse à distance IP source ou destination sélectionnée à SmartWhois, si ce dernier est installé sur votre système. SmartWhois est une application autonome développée par notre compagnie et capable d'obtenir les informations à propos de n'importe quelle adresse IP ou nom d'hôte dans le monde entier. Elle procure automatiquement les informations associées à une adresse IP, comme le domaine, le nom de réseau, le pays, l'état ou la province, ainsi que la ville. Ce programme peut être téléchargé à partir de notre site.
Créer un alias – ouvre une fenêtre où vous pouvez assigner des alias faciles à mémoriser aux addresses IP.
Processus – vous permet d'obtenir des informations supplémentaires ou d'agir sur le processus qui a envoyé ou reçu les paquets dans la session sélectionnée (Windows 2000/XP/2003 uniquement). Vous pouvez **Terminer** un processus, afficher la fenêtre **Propriétés du Fichier**, ou **Afficher le Chemin Complet** du fichier éxecutable.
Enregistrer les Dernières Connexions IP sous – vous permet de enregistrer le contenu de l'onglet Statistiques IP dans un fichier HTML formaté CSV.
Effacer les Dernières Connexions IP – efface la table.
Plus de statistiques -- affiche une fenêtre avec des statistiques de transfert de données et de distribution de protocole.

Paquets

Cet onglet est utilisé pour répertorier tous les paquets réseau capturés et afficher les informations détaillées à propos d'un paquet sélectionné.



La **table supérieure** répertorie la liste des paquets capturés. Utilisez cette liste pour sélectionner un paquet que vous voulez afficher et analyser. Lorsque vous sélectionnez un paquet en cliquant dessus, d'autres volets affichent des informations à propos du paquet sélectionné.

La définition de chaque colonne est expliquée ci-dessous :

No – un numéro unique par paquet.
Adresses MAC – affiche les adresses source et destination MAC et la direction des paquets.

Exemples :

22:22:22:22:22:22 => 33:33:33:33:33:33 est un paquet entrant de 22:22:22:22:22:22 à 33:33:33:33:33:33.

22:22:22:22:22:22 <= 33:33:33:33:33:33 est un paquet entrant de 33:33:33:33:33:33 à 22:22:22:22:22:22.

44:44:44:44:44:44 <=> 55:55:55:55:55:55 est un paquet transitant de 44:44:44:44:44:44 à 55:55:55:55:55:55.

55:55:55:55:55:55 <=> 44:44:44:44:44:44 est un paquet transitant de 55:55:55:55:55:55 à 44:44:44:44:44:44.

Par défaut, CommView affiche les adresses MAC dans un mode mixte, donc les adresses sont du type CompaqComp:22:22:22 ou ZyxelCommu:33:33:33. Les trois premiers octets de l'adresse MAC identifient le fabricant du périphérique réseau utilisant cette adresse, et CommView affiche le nom abrégé du fabricant plutôt que la valeur hexadécimale des trois premiers octets.

Adresses IP – affiche les adresses source et destination IP (lorsqu'applicable) et la direction des paquets.
Ports – affiche les ports source et destination (lorsqu'applicable) et la direction des paquets. Les ports peuvent être affichés en valeurs numériques ou comme noms des service correspondants. Pour plus d'informations, consultez le chapitre Configuration des options.
Heure / Delta – affiche l'heure absolue ou delta des paquets. L'heure delta est la différence entre l'heure absolue des deux derniers paquets. Vous pouvez passer de l'heure absolue à l'heure delta en cliquant **Affichage** =>**Colonnes de paquets** =>**Afficher l'heure comme**.
Taille – affiche la taille des paquets en octets. Cette colonne n'est pas visible par défaut.

Les colonnes individuelles peuvent être affichées ou masquées en cliquant l'élément correspondant du menu **Affichage** =>**Colonnes de paquets**. Le paquet sortant peut être suspendu en cliquant **Fichier** =>**Suspendre les données de paquet**. En mode suspendu, les paquets sont capturés, mais ne sont pas affichés, sur l'onglet **Paquets**. Ce mode est utile lorsque vous êtes interessé(e) seulement dans les statistiques, plutôt que dans les paquets individuels. Pour reprendre le déploiement des paquets en temps réel, cliquez **Fichier** =>**Reprendre les données de paquet**.

Le **panneau du milieu** affiche le contenu brut du paquet, à la fois en notation hexadécimale et en texte clair. En texte clair, les caractères non-imprimables sont remplacés par des points. Quand plusieurs paquets sont sélectionnés dans la table du haut, le

panneau du milieu affiche le nombre de paquets sélectionnés, la taille totale, et l'intervalle de temps entre le premier et le dernier paquet.

Le **volet inférieur** déploie les informations de décodage des paquets pour le paquet sélectionné. Cette information comprend des données vitales qui peuvent être utilisées par des professionnels de réseau. Cliquer le bouton droit de la souris sur le volet invoque le menu contextuel (pop-up) qui vous permet de réduire/développer tous les dossiers, ou bien de copier tous les dossiers ou seulement ceux sélectionnés. Vous pouvez modifier la position de la fenêtre Décodeur en cliquant sur un des trois boutons du volet inférieur (vous pouvez avoir une fenêtre Décodeur alignée sur le bas, la droite ou la gauche).

Commandes du menu

Cliquer le bouton droit de la souris sur la liste de paquets ouvre un menu avec les commandes suivantes :

Reconstruire la session TCP – vous permet de reconstruire une session TCP en partant du paquet sélectionné; une fenêtre ouvre et affiche la conversation complète entre deux hôtes.
Créer un alias – ouvre une fenêtre où vous pouvez assigner un alias facile à mémoriser à l'adresse MAC ou IP sélectionnée.
Copier l'adresse – copie l'adresse source MAC, l'adresse de destination MAC, l'adresse source IP ou l'adresse de destination IP au presse-papiers.
Copier le paquet – copie les données indéfinies du paquet sélectionné sur le presse-papiers.
Envoyer le(s) paquet(s) – affiche la fenêtre Générateur de paquets qui vous permet de renvoyer le paquet sélectionné ou un groupe de paquets. Vous pouvez aussi modifier le contenu du paquet avant de l'envoyer.
Enregistrer le(s) paquet(s) sous – enregistre le contenu du(des) paquet(s) sélectionné(s) dans un fichier. Le dialogue Enregistrer sous vous permet de sélectionner le format à être utilisé lorsque vous enregistrez des données de la liste déroulante.
SmartWhois – transmet l'adresse IP source ou destination du paquet sélectionné à SmartWhois si celui-ci est installé sur votre système. SmartWhois est une application autonome, développée par notre compagnie, capable d'obtenir des informations sur toute adresse IP ou nom d'hôte dans le monde entier. Elle fournie automatiquement les informations associées à une adresse IP, comme le domaine, le nom du réseau, le pays, l'état ou la région, et la ville. Le logiciel peut être téléchargé depuis notre site.
Effacer la mémoire tampon de paquets – efface le contenu de la mémoire tampon du programme. La liste de paquets sera effacée, puis vous ne serez plus capable d'afficher les paquets précédemment capturés par le programme.
Décoder sous – pour les paquets TCP et UDP, vous permet de décoder des protocoles pris en charge qui utilisent des ports non standard. Par exemple, si votre serveur SOCKS est exécuté sur le port 333, au lieu du port 1080, vous pouvez sélectionner un paquet qui appartient à la session SOCKS et utiliser cette commande de menu pour faire en sorte que CommView décode tous les paquets du port 333 en tant que paquets SOCKS. De tels réassignations de port-protocole ne sont pas permanents et dureront jusqu'à ce que le programme soit fermé. Prenez note que vous ne pouvez pas écraser des pairs de port-protocole standard , par exemple, vous ne pouvez pas faire en sorte que CommView décode les paquets du port 80 en tant que paquets TELNET.

Vous pouvez aussi glisser-déposer le(s) paquet(s) sélectionné(s) sur le bureau.

Journalisation

Cet onglet est utilisé pour enregistrer les paquets capturés dans un fichier sur le disque. CommView enregistre les paquets dans son propre format avec l'extension . NCF. L'ancien format (.CCF) continue d'être supporté pour des raisons de compatibilité ascendante; néanmoins, vous ne pourrez plus sauvegarder dans ce format. Vous pouvez ouvrir et afficher ces fichiers en tout temps en utilisant l'Éditeur de fichiers journaux ou vous pouvez simplement double-cliquer sur tout fichier NCF ou CCF pour le charger et le décoder.

NCF est un format ouvert; veuillez vous référer au chapitre Format des Fichiers Journaux de CommView pour une description détaillée du format NCF.

Enregistrement et gestion

Utilisez ce cadre pour enregistrer manuellement les paquets capturés dans un fichier et pour concaténer/diviser les fichiers de capture.

Il est possible d'enregistrer tous les paquets actuellement stockés dans le tampon ou de n'enregistrer qu'une partie de ces derniers selon une plage donnée. Les champs **À** et **De** vous permettent de définir la plage requise selon les numéros de paquet, tel qu'illustré sur l'onglet Paquets. Cliquez sur **Enregistrer sous ...** pour sélectionner un nom de fichier.

Pour concaténer manuellement plusieurs fichiers NCF en un seul fichier plus volumineux, cliquez sur le bouton **Concaténer fich.journaux**. Pour découper les fichiers NCF qui sont trop volumineux en plus petits fichiers, cliquez sur le bouton **Partager fich. journaux**. Par la suite, le programme vous guidera à travers le processus et vous serez en mesure de saisir la taille souhaitée des fichiers résultants.

Enregistrement automatique

Cochez cette case pour que le programme enregistre automatiquement les paquets capturés au fur et à mesure qu'ils arrivent. Utilisez le champ **Taille maximum du répertoire** pour limiter la taille totale des documents capturés stockés dans le **Répertoire de fichiers journaux**. Si la taille totale des documents excède la limite, le programme va automatiquement supprimer les plus anciens documents du répertoire. Le champ **Taille Moyenne du Fichier Journal** vous permet de spécifier la taille approximative voulue pour chaque fichier journal. Lorsque le fichier journal atteint la taille spécifiée, un nouveau fichier est automatiquement créé. Pour changer le Répertoire de Journaux par défaut, cliquez sur le bouton dans Sauvegarder les Fichiers Sous et sélectionnez un répertoire différent.

Un fichier journal contenant 500 paquets est d'une taille approximative de 500 kilobytes.

IMPORTANT : Si vous désirez conserver un fichier de capture important durant une longue période de temps, ne le gardez pas dans le Répertoire de fichiers journaux par défaut : il y a des chances qu'ils soit automatiquement supprimé, au fur et à mesure que de nouveaux fichiers seront enregistrés. Déplacez ce document dans un dossier different pour le préserver.

Veuillez noter que le programme n'enregistre pas chaque paquet individuellement dès son arrivée. Cela signifie que si vous affichez le fichier journal en temps réel, il se peut qu'il ne contienne pas les derniers paquets. Pour que le programme recopie immédiatement la mémoire tampon dans le fichier journal, cliquez sur **Arrêter la capture** ou décochez la case **Enregistrement automatique**.

Pour les utilisateurs de niveau avancé : Pour modifier la valeur par défaut de 500 paquets par fichier, modifiez la clé de registre suivante : HKEY_CURRENT_USER\Software\CommView\Main\PacketsPerFile. Rappelez-vous de fermer CommView avant d'éditer cette clé.

Journalisation des accès WWW

Cochez si cette cas pour activer la journalisation des sessions http. Utilisez le champ **Taille maximum de fichier size** pour limiter la taille du fichier-journal. Si la taille du fichier-journal excède la limite, le programme supprimer automatiquement les vieux enregistrements du fichier. Pour modifier le nom et le chemin d'accès du fichier par défaut, cliquez sur la case **Enregistrer les fichiers vers** et sélectionnez un nom de fichier différent. Les fichiers-journaux peuvent être générés au format **HTML** ou **TXT**. Cliquez sur **Configure** pour modifier les options de journalisation par défaut. Vous pouvez modifier le numéro de port utilisé pour les accès HTTP (la valeur par défaut de 80 pourrait ne pas fonctionner si votre ordinateur est caché derrière un serveur mandataire), puis exclure certains types de données (habituellement, la journalisation de tout autre type autre que les pages HTML est pratiquement itnuile, ainsi il est judicieux d'exclure les adresses Web des images du fichier-journal).

Affichage des fichiers journaux

L'Éditeur de fichiers journaux est un outil pour afficher et explorer les documents capturés créés par CommView et plusieurs autres analyseurs de paquets. Il comporte la même fonctionnalité de l'onglet Paquets sur la fenêtre principale du programme, mais contrairement à l'onglet Paquets, l'Éditeur de fichiers journaux déploie les paquets chargés à partir des dossiers sur le disque, au lieu des paquets capturés en temps réel.

Pour ouvrir l'Éditeur de fichiers journaux, cliquez **Fichier => Éditeur de fichiers journaux** du menu principal du programme, ou double-cliquez simplement sur n'importe lequel des dossiers capturés par CommView et précédemment enregistrés. Vous pouvez ouvrir autant de fenêtres d'Éditeur de fichiers journaux que vous le souhaitez, et chacune d'elle peut être utilisée pour explorer un ou plusieurs dossiers enregistrés.

L'Éditeur de fichiers journaux peut être utilise pour l'exploration des fichiers de capture créés par d'autres analyseurs de paquets et pare-feu personnels. La version actuelle peut importer des fichiers dans les formats de Network Instruments Observer®, Network General Sniffer® pour DOS/Windows, Microsoft® NetMon, WildPackets EtherPeek™ et AiroPeek™, et Tcpdump (libcap). Ces formats sont également utilisés par un certain nombre d'applications de tierce-partie. L'Éditeur de fichiers journaux offre la capacité d'exporter les données de paquet en créant des fichiers en format Network Instruments Observer®, Network General Sniffer® pour DOS/Windows, Microsoft® NetMon, WildPackets EtherPeek™ et AiroPeek™, et Tcpdump (libcap), ainsi qu'au format natif CommView.

Utiliser l'Éditeur de fichiers journaux est similaire à utiliser l'onglet Paquets de la fenêtre principale; veuillez consulter le chapitre Paquets si vous avec besoin d'informations détaillées.

Menu de l'Éditeur de fichiers journaux

Fichier

Charger les fichiers journaux CommView – ouvre et charge un ou plusieurs dossiers capturés CommView.
Importer les fichiers journaux – vous permet d'importer des dossiers capturés créés par d'autres analyseurs de paquets.
Exporter les fichiers journaux – vous permet d'exporter les paquets affichés pour capturer des dossiers dans plusieurs formats.
Effacer la fenêtre – efface la liste de paquets.
Générer des statistiques – fait en sorte que CommView génère des statistiques sur les paquets chargés dans l'Éditeur de fichiers journaux. Optionnellement, il est possible de réinitialiser les données statistiques précédemment recueillies qui sont affichées dans la fenêtre **Statistiques**. Veuillez prendre note que cette fonction n'affichera que la distribution de paquets selon un horaire établi. Elle est limitée à l'affichage des totaux, des tableaux de protocoles et d'hôtes LAN.
Fermer la fenêtre – ferme la fenêtre.

Recherche

Rechercher un paquet – affiche un dialogue qui vous permet de trouver des paquets correspondant à un texte spécifique.
Aller au paquet numéro – affiche un dialogue qui vous permet de sauter à un paquet à l'aide d'un numéro spécifié.

Règles

Appliquer les règles en cours – applique vos règles courantes pour les paquets affichés dans l'Éditeur de fichiers journaux. En résultat, lorsque vous utilisez cette commande, le programme va supprimer les paquets qui ne correspondent pas aux règles courantes. Notez que ceci ne modifiera pas le dossier sur le disque.
Du fichier ... - fait la même chose que la commande **Appliquer les règles en cours**, mais vous permet d'utiliser les règles d'un dossier .RLS précédemment enregistré plutôt que l'ensemble de règles actuelles.

Règles

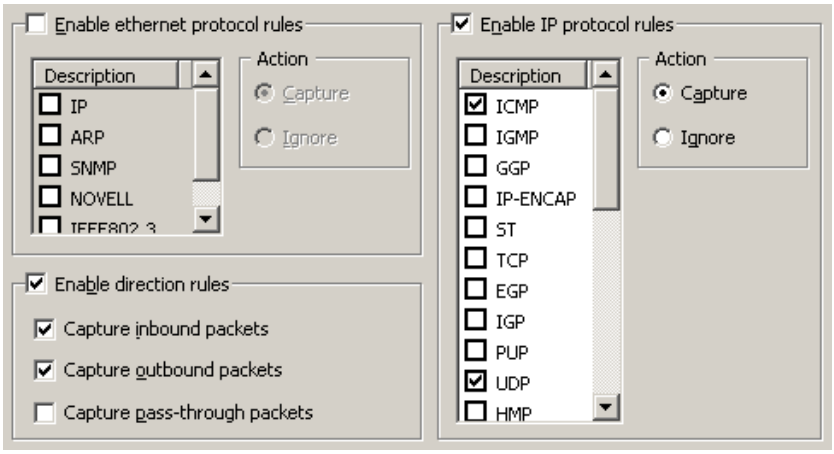
Cet onglet vous permet de configurer des règles pour capturer des paquets. Si une ou plusieurs règles sont configurées, le programme filtre les paquets en se basant sur ces règles et affiche seulement les paquets qui correspondent à ces règles. Notez que CommView n'est pas un pare-feu, et que lorsque vous utilisez ces règles, les paquets sont toujours procédés par le système d'exploitation; ils ne sont seulement pas affichés et enregistrés par CommView. Si une règle est configurée, le nom de l'onglet correspondant est affiché en police à caractère gras.

Vous pouvez enregistrer vos configuration(s) de règles dans un dossier et les charger en utilisant **Règles** du menu du programme.

Puisque le trafic LAN peut souvent générer un nombre élevé de paquets, il est recommandé d'utiliser des règles pour filtrer vers l'extérieur les paquets inutiles. Ceci peut considérablement réduire le nombre de ressources du système consommées par le programme. Si vous désirez activer/désactiver une règle, sélectionnez la branche approprié sur le côté gauche de la fenêtre (par exemple, **Adresses IP** ou **Ports**), et cochez ou décochez la case décrivant la règle (**Activer les règles d'adresses IP** ou **Activer les règles de port**). Il y a sept types de règles qui peuvent être utilisés :

Protocoles & Direction

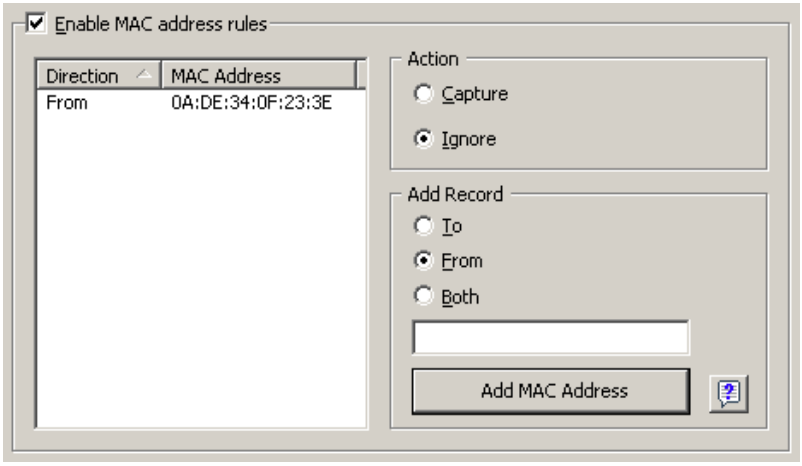
Vous permet d'ignorer ou de capturer des paquets basés sur l'Ethernet (Layer 2), les protocoles IP (Layer 3) ou sur la direction des paquets.



Cet exemple affiche comment faire pour que le programme capture seulement les paquets ICMP et UDP entrants et sortants. Tous les autres paquets de la famille IP seront ignorés; tous les paquets transitants seront également ignorés.

Adresses MAC

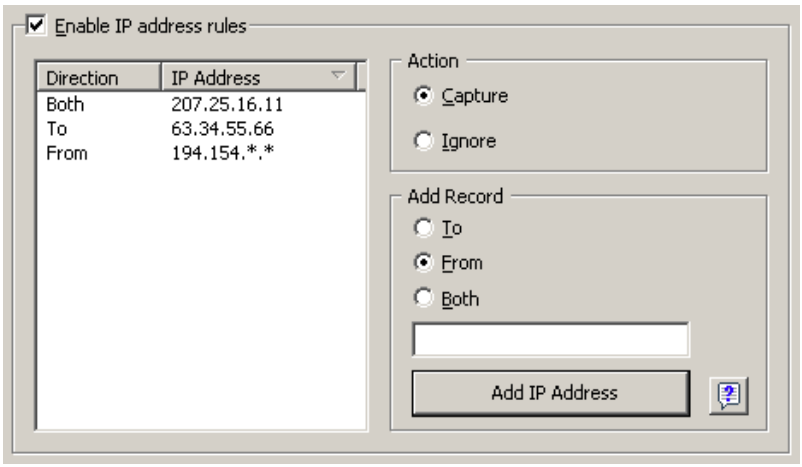
Vous permet d'ignorer ou de capturer les paquets basés sur les addresses MAC (matériel). Entrez une adresse MAC dans le champ **Ajouter un enregistrement**, sélectionnez la direction (**De, À,** ou **Les deux**), puis cliquez **Ajouter une adresse MAC**. La nouvelle règle va être affichée. Maintenant, vous pouvez sélectionner l'action à prendre lorsqu'un nouveau paquet est procédé : le paquet peut être ou bien capturé, ou bien ignoré. Vous pouvez aussi cliquer sur le bouton Alias MAC pour obtenir une liste des alias; double-cliquez sur l'alias que vous souhaitez ajouter, puis l'adresse MAC correspondante apparaîtra dans la boîte d'entrée.



Cet exemple affiche comment faire pour que le programme ignore les paquets qui viennent de 00:07:95:D9:3B:EF. Tous les paquets venant d'adresses MAC différentes seront capturés.

Adresses IP

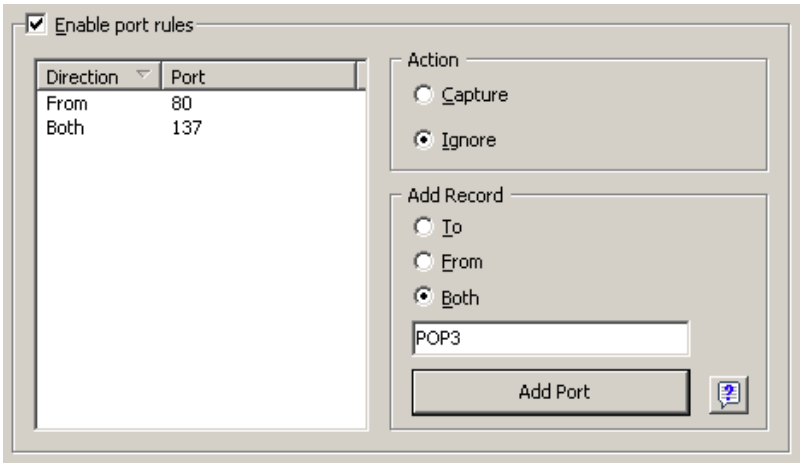
Vous permet d'ignorer ou de capturer les paquets basés sur les addresses IP. Entrez une adresse IP dans le champ **Ajouter un enregistrement**, sélectionnez la direction (**De, À,** ou **Les deux**), puis cliquez **Ajouter une adresse IP**. Vous pouvez utiliser des jokers (wildcards) pour spécifier des blocs d'adresses IP. La nouvelle règle va être affichée. Maintenant, vous pouvez sélectionner l'action à prendre lorsqu'un nouveau paquet est procédé : le paquet peut être ou bien capturé, ou bien ignoré. Vous pouvez aussi cliquer sur le bouton Alias IP pour obtenir une liste des alias; double-cliquez sur l'alias que vous souhaitez ajouter, puis l'adresse IP correspondante apparaîtra dans la boîte d'entrée.



Cet exemple déaffiche comment faire pour que le programme capture les paquets qui vont à 63.34.55.66, qui vont vers et viennent de 207.25.16.11 et viennent de toutes les adresses comprises entre 194.154.0.0 et 194.154.255.255. Tous les paquets venant d'adresses différentes ou allant vers d'autres adresses seront ignorées. Puisque les adresses IP sont utilisées dans protocole IP, une telle configuration va faire en sorte que le programme ignore automatiquement les paquets non IP.

Ports

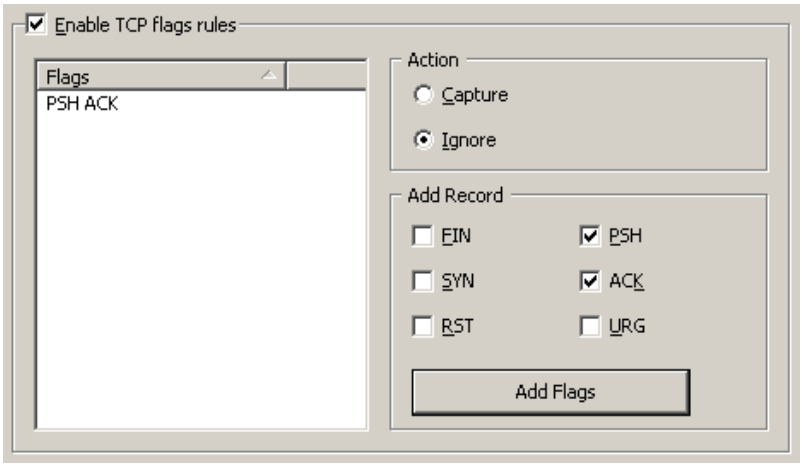
Vous permet d'ignorer ou de capturer les paquets basés sur les ports. Entrez un nombre de port dans le champ **Ajouter un enregistrement**, sélectionnez la direction (**De, À,** ou **Les deux**), puis cliquez **Ajouter un port**. La nouvelle règle va être affichée. Maintenant, vous pouvez sélectionner l'action à prendre lorsqu'un nouveau paquet est procédé : le paquet peut être ou bien capturé, ou bien ignoré. Vous pouvez aussi cliquer sur le bouton **Référence de port** pour obtenir une liste de tous les ports connus; double-cliquez sur le port que vous souhaitez ajouter et son nombre apparaîtra dans la boîte d'entrée. Les ports peuvent aussi être entrés en texte; par exemple, vous pouvez taper en *http* ou *pop3*, puis le programme convertira le nom du port en valeur numérique.



Cet exemple illustre comment faire pour que le programme ignore les paquets qui viennent du port 80 et vont et viennent du port 137. Cette règle évitera que CommView n'affiche le trafic entrant HTTP, aussi bien que le trafic de noms de service entrant et sortant NetBIOS. Tous les paquets venant et allant de ports différents seront capturés.

Flags TCP

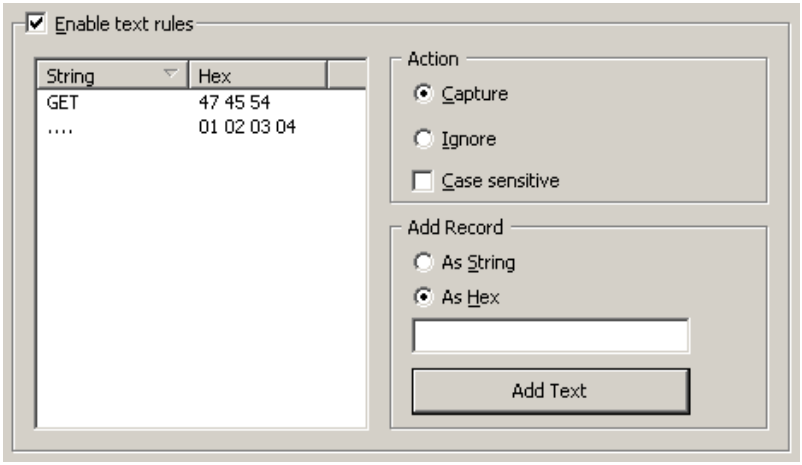
Vous permet d'ignorer ou de capturer des paquets basés sur les flags TCP. Cochez un flag ou une combinaison de flags dans le champ **Ajouter un enregistrement**, puis cliquez **Ajouter un flag**. La nouvelle règle va être affichée. Maintenant, vous pouvez sélectionner l'action à prendre lorsqu'un nouveau paquet entrant avec flags TCP est procédé : le paquet peut être capturé ou ignoré.



Cet exemple illustre comment faire pour que le programme ignore les paquets TCP avec le flag PSH ACK. Tous les paquets avec des flags TCP différents seront capturés.

Texte

Vous permet de capturer des paquets contenant un certain texte. Entrez une chaîne de texte dans le champ **Ajouter un enregistrement**, sélectionnez le type de l'information entrée (**Comme chaîne** ou **Comme Hex**), puis cliquez **Ajouter du texte**. La nouvelle règle va être affichée. Vous pouvez entrer une chaîne en texte ou en valeur hexadécimale. La dernière méthode devrait être utilisée lorsque vous voulez entrer des caractères imprononçables : tapez seulement des valeurs à caractères hexadécimaux, séparées par des espaces, tel que montré ci-dessous. Maintenant, vous pouvez sélectionner l'action à prendre lorsqu'un nouveau paquet est procédé : le paquet peut être capturé ou ignoré.



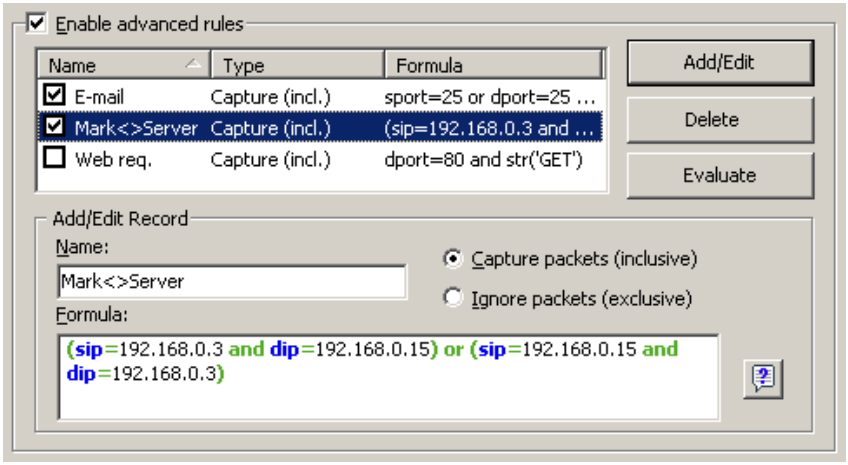
Cet exemple illustre comment faire pour que le programme capture seulement les paquets contenant "GET" ou des données hexadécimales 01 02 03 04. Cochez la case **Respecter la casse**, si vous désirez que les règles respectent la casse. Tous les autres paquets ne contenant pas le texte ci-dessus mentionné seront ignorés.

Avancées

Les règles avancées sont les règles les plus puissantes et les plus flexibles vous permettant de créer des filtres complexes en utilisant la logique booléenne. Pour une aide détaillée sur l'utilisation des règles avancées, veuillez consulter le chapitre Règles avancées.

Règles avancées

Les règles avancées sont les règles les plus puissantes et les plus flexibles vous permettant de créer des filtres complexes en utilisant la logique booléenne. L'utilisation des règles avancées requiert une compréhension de base des mathématiques et de la logique, mais la syntaxe des règles est tout de même facile à comprendre.



Aperçu

Pour ajouter une nouvelle règle, vous devriez entrer un nom arbitraire dans le champ **Nom**, sélectionner l'action (**Capturer / Ignorer**), entrer une **Formule** en utilisant la syntaxe décrite ci-dessous, puis cliquer **Ajouter / Modifier**. Votre nouvelle règle sera ajoutée à la liste et deviendra active immédiatement. Vous pouvez ajouter autant de règles que vous le désirez, mais seulement les règles dont la case à côté de son nom est cochée seront actuellement actives. Vous pouvez activer/désactiver les règles en cochant/décochant les cases correspondantes ou en supprimant complètement les règles en utilisant le bouton **Supprimer**. Si plus d'une règle est active, vous pouvez évaluer le résultat de celles-ci combinées en cliquant sur le bouton **Évaluer**. Veuillez noter que l'activation de règles multiples sont combinées en utilisant l'opérateur logique OR, par exemple si vous avez trois règles actives, RÈGLE1, RÈGLE2, et RÈGLE3, la règle résultant est RÈGLE1 OR RÈGLE2 OR RÈGLE3.

Vous pouvez utiliser les règles avancées en conjonction avec les règles de base décrites dans le chapitre précédent, mais si vous vous sentez confortable avec la logique booléenne, c'est une bonne idée d'utiliser seulement les règles avancées, puisqu'elles offrent beaucoup plus de flexibilité. Les règles de base sont combinées avec les règles avancées en utilisant l'opérateur logique AND.

Description de la Syntaxe

dir – Direction des paquets. Les valeurs possibles sont *in* (entrants), *out* (sortants et *pass-through* (transitants).

etherproto – Protocole Ethernet, les 13ème et 14ème octets d'un paquet. Les valeurs acceptables sont des nombres (par exemple *etherproto=0x0800* pour IP) ou des alias communs (par exemple *etherproto=ARP*, lequel est équivalent à 0x0806).

ipproto – Protocole IP. Les valeurs acceptables sont des nombres (par exemple *ipproto!=0x06* pour TCP) ou des alias communément utilisés (par exemple *ipproto=UDP*, lequel est équivalent à 0x11).

smac – Adresses MAC source. Les valeurs acceptables sont des adresses MAC à notation hexadécimale (par exemple *smac=00:00:21:0A:13:0F*) ou des alias définis par l'utilisateur.

dmac – Adresses MAC de destination.

sip – Adresses IP source. Les valeurs acceptables sont des adresses IP à notation avec points (par exemple *sip=192.168.0.1*), des adresses IP avec des jokers (par exemple *sip!=*.*.*.255*), des adresses de sous-réseau (par exemple *sip=192.168.0.4/255.255.255.240* ou *sip=192.168.0.5/28*), des plages d'adresses IP (par exemple *sip from 192.168.0.15 to 192.168.0.18* ou *sip in 192.168.0.15 .. 192.168.0.18*) ou des alias définis par l'utilisateur.

dip - Adresses IP de destination.

sport – Port source pour les paquets TCP et UDP. Les valeurs acceptables sont des nombres (par exemple *sport=80* for HTTP), des plages (par exemple *sport from 20 to 50* ou *sport in 20..50* pour tout numéro de port compris entre 20 et 50) ou des alias définis par le système d'exploitation (par exemple *sport=ftp*, lequel est équivalent à 21). Pour la liste des alias pris en charge par votre système d'exploitation, cliquez **Affichage => Référence de port**.

dport – Port de destination pour les paquets TCP et UDP.

flag – Flag TCP. Les valeurs acceptables sont des nombres (par exemple *0x18* pour PSH ACK) ou un ou plusieurs des caractères suivants : *F* (FIN), *S* (SYN), *R* (RST), *P* (PSH), *A* (ACK), et *U* (URG), ou le mot-clé *has*, lequel veut dire que le flag contient une certaine valeur. Exemples d'utilisation : *flag=0x18*, *flag=SA*, *flag has F*.

size – Taille des paquets. Les valeurs acceptables sont des nombres (par exemple *size=1514*) ou des plages (par exemple *size from 64 to 84* ou *size in 64..84* pour toute taille comprise entre 64 et 84).

str – Contenu des paquets. Utilisez cette fonction pour indiquer que le paquet doit contenir une certaine chaîne. Cette fonction comporte trois arguments : string, position, et case-sensitivity. Le premier argument est une chaîne, par exemple *'GET'*. Le deuxième argument est un nombre qui indique la position de la chaîne (décalage) dans le paquet. La valeur de décalage est de base zéro, c'est-à-dire que si vous recherchez le premier octet du paquet, la valeur de décalage doit être *0*. Si la valeur de décalage n'est pas importante, utilisez *–1*. Le troisième argument indique la sensibilité à la casse et peut être soit *false* (insensible à la casse) ou *true* (sensible à la casse). Les deuxième et troisième arguments sont optionnels; si omis, la valeur de décalage est de *–1* par défaut et la sensibilité à la casse est *false* par défaut. Exemples d'utilisation : *str('GET',-1,false)*, *str('GET',-1)*, *str ('GET')*.

hex – Contenu des paquets. Utilisez cette fonction pour indiquer que le paquet doit contenir un certain modèle hexadécimal d'octet. Cette fonction possède deux arguments : hex pattern et position. Le premier argument est une valeur hexadécimale, par exemple *0x4500*. Le deuxième argument est un nombre qui indique la position du modèle (décalage) dans le paquet. La valeur de décalage est de base zéro, c'est-à-dire que si vous recherchez le premier octet du paquet, la valeur de décalage doit être *0*. Si la valeur de décalage n'est pas importante, utilisez *–1*. Le deuxième argument est optionnel; si omis, la valeur de décalage est de *–1* par défaut. Exemples d'utilisation : *hex(0x04500, 14)* , *hex(0x4500, 0x0E)*, *hex (0x010101)*.

bit – Contenu des paquets. Utilisez cette fonction pour determiner si le bit spécifié à la position de décalage donnée est à 1. Dans ce cas, la fonction retourne *true* (vrai). Si le bit spécifié est à 0, ou se situe au delà des limites du paquet, la fonction retourne *false* (faux). Le premier argument est l'indice du bit dans l'octet; les valeurs autorisées vont de 0 à 7. La valeur 0x01 indique que le bit 0 est à 1, tous les autres bits étant à 0. Le deuxième argument est un nombre indiquant la position (de décalage) de l'octet dans le paquet. La position de décalage est basée par rapport à la position zéro, c'est-à-dire que si vous voulez le premier octet du paquet, la position de décalage doit être *0*. Les deux arguments sont obligatoires. Exemple d'utilisation: *bit(0, 14)*, *bit(0, 0x0E)*.

Les mots-clés décrits ci-dessous peuvent être utilisés avec les opérateurs suivants :

and – Conjonction booléenne.
or - Disjonction booléenne.
not – Négation booléenne.
= - Égalité arithmétique.
!= - Inégalité arithmétique.
<> - Inégalité arithmétique.
> - Plus grand que - Arithmétique.
< - Moins grand que - Arithmétique.
( ) – Parenthèses, Opérateur de contrôle pour les règles prioritaires.

Tous les nombres peuvent être à notation décimale ou hexadécimale. Si vous voulez utiliser la notation hexadécimale, le nombre doit être précédé par *0x*, c'est-à-dire que vous pouvez utiliser soit *15* ou *0x0F*.

Exemples

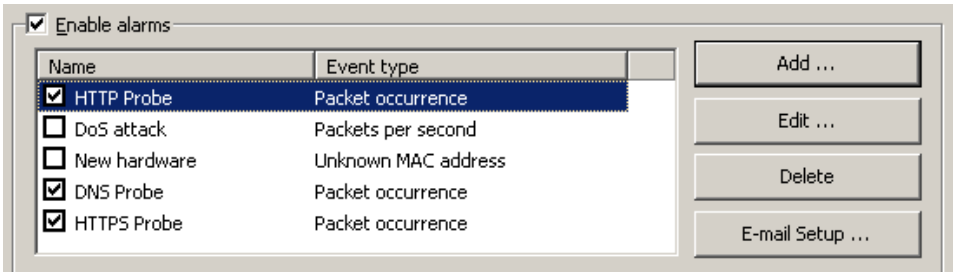
Vous trouverez ci-dessous un certain nombre d'exemples illustrant la syntaxe des règles. Chaque règle est suivie par nos commentaires sur la fonction de chacune d'elles. Les règles sont montrées en rouge. Les commentaires sont séparés des règles par deux barres obliques.

- dir!=pass // Capture seulement les paquets entrants et sortants. Les paquets transitants à travers d'autres stations de travail sur le LAN sont ignorés.
- (smac=00:00:21:0A:13:0E or smac=00:00:21:0A:13:0F) and etherproto=arp // Capture les paquets ARP envoyés par deux ordinateurs, 00:00:21:0A:13:0E et 00:00:21:0A:13:0F.
- ipproto=udp and dport=137 // Capture les paquets UDP/IP envoyés au numéro de port 137.
- dport=25 and str('RCPT TO:', -1, true) // Capture les paquets TCP/IP ou UDP/IP qui contiennent ""RCPT TO:" et dont le port de destination est 25.
- not (sport>110) // Capture tout, excepté les paquets dont le port source est plus grand que 110
- (sip=192.168.0.3 and dip=192.168.0.15) or (sip=192.168.0.15 and dip=192.168.0.3) // Capture seulement les paquets IP envoyés entre deux machines, 192.168.0.3 et 192.168.0.15. Tous les autres paquets sont discartés.
- ((sip from 192.168.0.3 to 192.168.0.7) and (dip = 192.168.1.0/28)) and (flag=PA) and (size in 200..600) // Capture les paquets TCP dont la taille est comprise entre 200 et 600 octets et venant des adresses IP comprises entre 192.168.0.3 - 192.168.0.7, dont l'adresse IP de destination est dans le segment 192.168.1.0/255.255.255.240, et où le flag TCP est PSH ACK.
- Hex(0x0203, 89) and (dir<>in) // Capture les paquets qui contiennent 0x0203 à la valeur de décalage 89, où la direction des paquets n'est pas entrante.

Alarmes

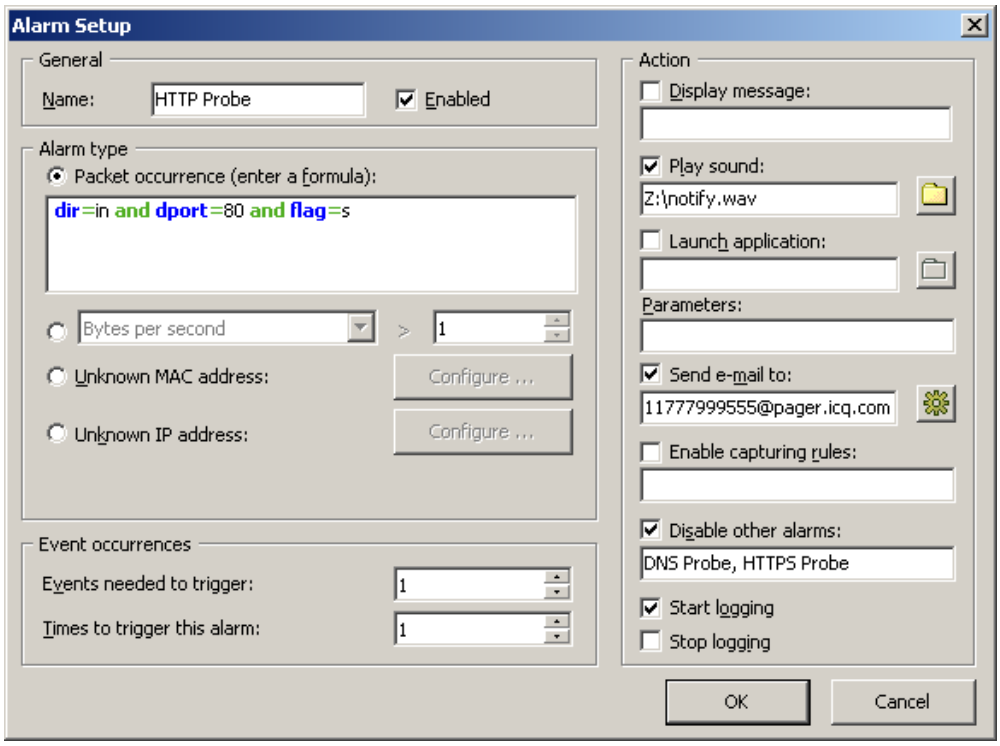
Cet onglet vous permet de créer des alarmes pour vous notifier à propos d'importants événements, tels que des paquets suspects, une utilisant élevée de la bande passante, des adresses inconnues, et ainsi de suite. Les alarmes sont très utiles dans une situation où vous avez besoin de surveiller le réseau pour des événements suspects, par exemple des modèles d'octet distinct dans les paquets capturés, des scans de ports ou des connexions périphériques matérielles inattendues.

Les alarmes sont gérées au moyen de la liste d'alarmes illustrée ci-dessous :



Chaque ligne représente une alarme individuelle, et le crochet situé à côté du nom d'alarme indique que l'alarme est actuellement active. Lorsqu'une alarme est déclenchée, le crochet disparaît. Pour réactiver une alarme désactivée, cochez la case située à côté de son nom. Pour désactiver toutes les alarmes, décochez la case **Activer les alarmes**. Pour ajouter une nouvelle alarme ou pour modifier une alarme existante, utilisez les boutons situés à la droite de la liste d'alarmes. Le bouton **Configuration email** devrait être utilisé pour entrer les informations à propos de votre serveur SMTP, si vous planifiez utiliser les options de notification par email (voyez ci-dessous).

La fenêtre de configuration d'email est illustrée ci-dessous :



Le champ **Nom** devrait être utilisé pour la description de la fonction de l'alarme. Cochez la case **Activé** si vous souhaitez que l'alarme que vous ajoutez/modifiez soit activée, une fois que vous en avez terminé avec sa configuration. Cette case à cocher équivaut à celle affichée dans la liste d'alarmes. Le cadre **Type d'alarme** vous permet de sélectionner un des sept types d'alarme :

- **Occurrence de paquet** : L'alarme sera déclenchée une fois que CommView aura capturé un paquet correspondant à la formule donnée. La syntaxe de la formule est pareille à la syntaxe utilisée pour les Règles avancées, décrite en détails dans le chapitre Règles avancées.
- **Octets par seconde** : L'alarme sera déclenchée une fois que le nombre d'octets par seconde aura excédé la valeur spécifiée. Notez que vous devriez entrer la valeur en octets, ainsi, si vous désirez que l'alarme soit déclenchée lorsque le taux de transfert de données aura excédé 1MOctet par seconde, la valeur entrée devrait être 1000000.
- **Paquets par seconde** : L'alarme sera déclenchée une fois que le nombre de paquets par seconde aura excédé la valeur spécifiée.

- **Diffusés par seconde**: L'alarme sera déclenchée dès que le nombre de paquets diffusés aura dépassé la valeur spécifiée.

- **Multipoints par seconde**: L'alarme sera déclenchée dès que le nombre de paquets multipoints aura dépassé la valeur spécifiée.

- **Adresse MAC inconnue** : L'alarme sera déclenchée une fois que CommView aura capturé un paquet avec une adresse MAC source ou destination inconnue. Utilisez le bouton **Configurer** pour entrer les adresses MAC connues. Ce type d'alarme est utile pour la détection de nouveaux périphériques matériels non autorisés connectés à votre LAN.

- **Adresse IP inconnue** : L'alarme sera déclenchée une fois que CommView aura capturé un paquet avec une adresse IP source ou destination inconnue. Utilisez le bouton **Configurer** pour entrer les adresses IP connues. Ce type d'alarme est utile pour la détection de connexions IP non autorisées derrière une pare-feu corporatif.

Le champ **Nbre événements avant déclenchement** vous permet de spécifier le nombre de fois que l'événement attendu doit survenir avant que l'alarme ne soit déclenchée. Par exemple, si vous spécifier la valeur de 3, l'alarme ne sera pas déclenchée jusqu'à ce que l'événement survienne trois fois. Si vous modifiez une alarme existante, le compteur d'événements interne sera réinitialisé.

Le champ **Nbre de déclenchements de cette alarme** vous permet de spécifier le nombre de fois que votre alarme peut être déclenchée avant sa désactivation. Par défaut, cette valeur équivaut à 1, ainsi l'alarme sera désactivée après la première occurrence de l'événement. En augmentant cette valeur, vous ferez en sorte que CommView déclenche l'alarme plusieurs fois. Si vous modifiez une alarme existante, le compteur de déclenchements interne sera réinitialisé.

La cadre **Action** vous permet de sélectionner les actions à prendre lorsque l'événement d'alarme survient. Les actions suivantes sont disponibles :

- **Afficher le message** : Affiche une boîte de message non modale avec le texte spécifié. Cette action permet l'utilisation de variables qui doivent être remplacés par les paramètres correspondants du paquet contenant l'alarme déclenchée. Ces variables sont ci-dessous répertoriées :
  %SMAC% -- adresse MAC source.
  %DMAC% -- adresse Mac de destination.
  %SIP% -- adresse IP source.
  %DIP% -- adresse IP de destination.
  %SPORT% -- port source.
  %DPORT% -- port de destination.
  %ETHERPROTO% -- protocole Ethernet.
  %IPPROTO% -- protocole IP.
  %SIZE% -- taille de paquet.
  %FILE% -- le chemin d'accès vers un fichier temporaire contenant le paquet capturé.

  Par exemple, si votre message est « Paquet SYN reçu de %SIP% », dans la fenêtre contextuelle actuelle, le texte %SIP% sera remplacé par l'adresse IP source du paquet ayant déclenché l'alarme. Si vous utilisez la variable %FILE%, un fichier .CCF sera créé dans le dossier temporaire. Il en va de votre responsabilité de supprimer le fichier après qu'il ait été procédé ; CommView ne le supprimer en aucun cas. Vous ne devriez pas utiliser de variables su l'alarme est déclenchée par les valeurs **Octets par seconde** ou **Paquets par seconde**, puisque ces types d'alarme ne sont pas déclenchés par des paquets individuels.

- **Émettre le son** : Joue le fichier WAV spécifié.

- **Lancer l'application** : Exécute le fichier EXE ou COM spécifié. Utilisez le champ optionnel **Paramètres** pour entrer les paramètres de ligne de commande. Vous pouvez utiliser les variables décrites dans la section **Afficher le message** précédente comme paramètres de ligne de commande si vous souhaitez que votre application reçoive et procède les informations à propos du paquet ayant déclenché l'alarme.

- **Envoyer email à** : Envoie un email à l'adresse email spécifiée. Vous DEVEZ configurer CommView pour qu'il utilise votre serveur SMTP avant l'envoi d'un email. Utilisez le bouton **Configuration d'email** situé à côté de la liste d'alarme pour entrer les paramètres de votre serveur SMTP et envoyer un message email d'essai. Habituellement, un message email peut aussi être utilisé pour envoyer des alertes à votre application de messagerie instantanée, votre cellulaire ou votre téléavertisseur. Par exemple, pour envoyer un message à un utilisateur ICQ, vous devriez entrer son adresse email ainsi : ICQ_USER_UIN@pager.icq.com, où ICQ_USER_UIN est le numéro d'identification ICQ unique de l'utilisateur, qui permet les messages EmailExpress dans les options de ICQ. Veuillez vous reporter à la documentation de votre messager instantanée ou de votre téléphone cellulaire pour de plus amples informations.

- **Activer la capture de règles** : Active les Règles avancées; vous devriez entrer le(s) nom(s) de règle. Si plusieurs règles doivent être activées, séparez-les avec une virgule ou un point-virgule.

- **Désactiver autres alarmes** : Désactive les autres alarmes; vous devriez entrer le(s) nom(s) d'alarme. Si plusieurs alarmes doivent être activées, séparez-les avec une virgule ou un point-virgule.

- **Démarrer l'enreg. Au fich. Journal** : Active l'enregistrement automatique (consultez le chapitre Journalisation); CommView commencera à déverser les paquets vers le disque dur.

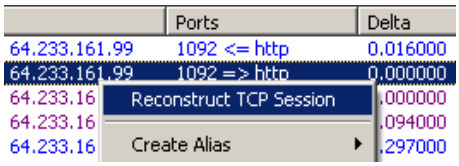
- **Arrêter l'enreg. Au fich. Journal** : Désactive l'enregistrement automatique.

Cliquez sur **OK** pour enregistrer vos paramètres et fermer la boîte de dialogue de configuration d'alarme.

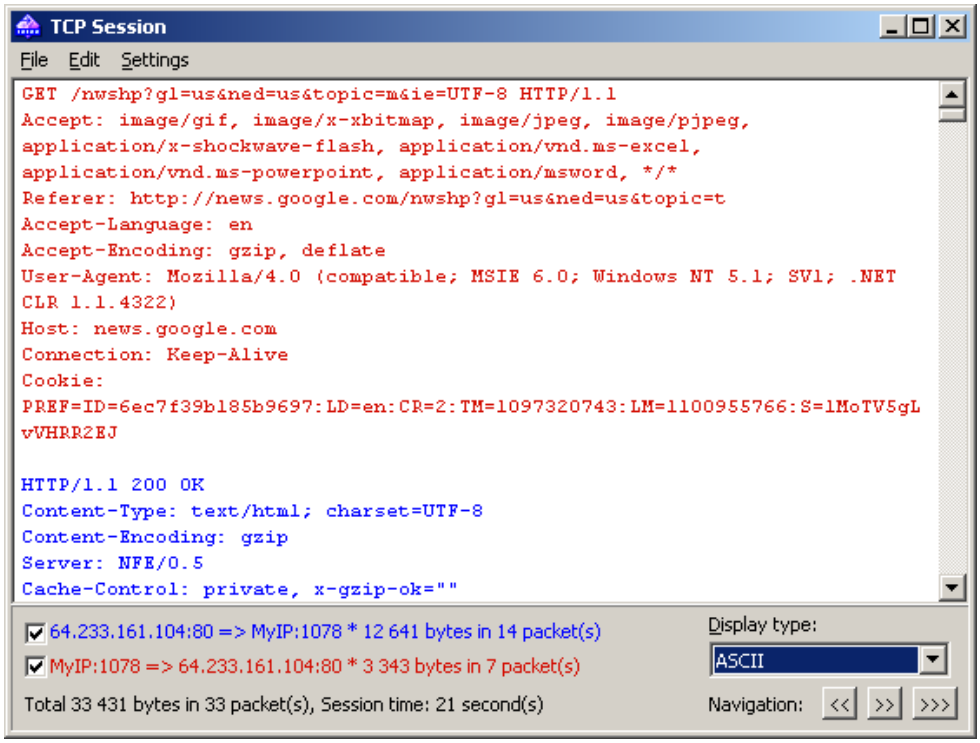
Tous les événements et actions reliés aux alarmes seront listés dans la fenêtre **Fichier journal d'événements** située en dessous de le liste d'alarmes.

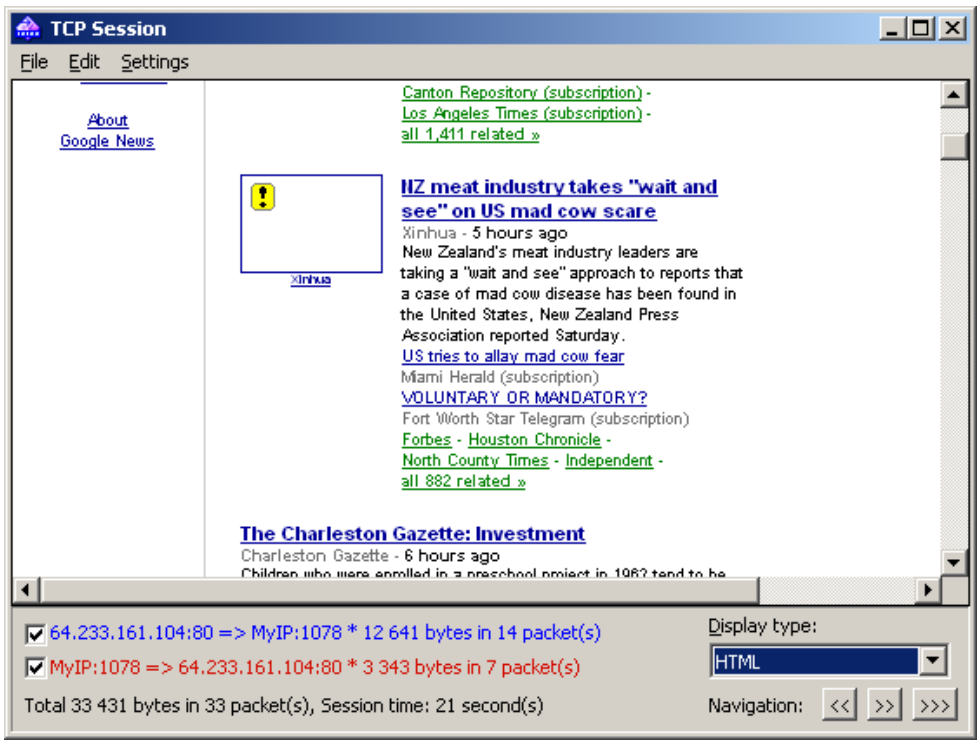
Reconstruction de sessions TCP

Cet outil vous permet d'afficher la conversation TCP entre deux hôtes. Pour reconstruire une session TCP, vous devriez premièrement sélectionner un paquet TCP à partir de l'onglet Paquets. Si vous voulez reconstruire entièrement la session, il est recommandé de sélectionner le premier paquet dans la session; autrement, la reconstruction pourrait commencer au milieu de la << conversation >>. Après, localisez et sélectionnez le paquet, cliquez dessus avec le bouton droit de la souris et sélectionnez **Reconstruire la session TCP** à partir du menu contextuel (pop-up), tel que montré ci-dessous :

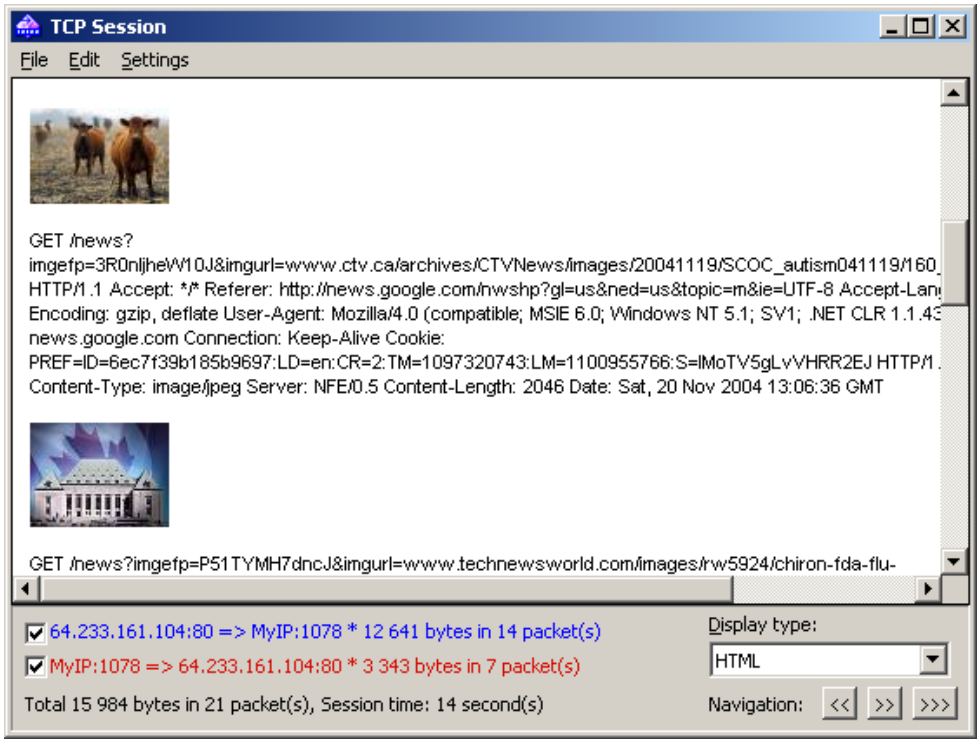


La reconstruction de sessions opère mieux pour les protocoles à base textuelle, tels que POP3, Telnet, ou HTTP. Bien sûr, vous pouvez aussi reconstruire le téléchargement d'un large document compressé, mais CommView peut alors prendre un long moment à reconstruire plusieurs megaoctets de données, et l'information obtenue serait inutile dans la plupart des cas. Un exemple de session contenant des données HTML affichée en modes ASCII et HTML est illustrée ci-dessous :





En mode d'affichage HTML, les pages HTML n'incluent jamais les graphiques, puisque les images du protocole http sont transférées séparément des données HTML. Pour afficher les images, il est normalement nécessaire de naviguer vers la session TCP suivante. Un exemple de session HTTO contenant des données images et affichée en mode HTML est illustrée ci-dessous :



Par défaut, CommView tente de décompresser le contenu Web GZIP et de reconstruire les flots de données binaires. Si vous souhaitez désactiver cette fonctionnalité, utilisez l'onglet **Décodage** de la boîte de dialogue **Options** du programme.

Vous pouvez filtrer vers l'extérieur les données qui sont venues de l'une des directions, en décochant une des cases à cocher du volet inférieur. Les données entrantes et sortantes sont marquées par différentes couleurs pour votre convenance. Si vous désirez modifier l'une de ces couleurs, cliquez **Paramètres** =>**Couleurs**, et choisissez une couleur différente. Vous pouvez activer ou désactiver le renvoi de ligne automatique en utilisant l'élément **Renvoi de ligne automatique** du menu **Paramètres**.

Le menu déroulant **Type d'affichage** vous permet d'afficher les données dans les formats **ASCII** (données texte nature), **HEX** (données hexadécimales), **HTML** (pages web et images) et **EBCDIC** (données d'encodage d'ordinateurs centraux IBM). Veuillez prendre note que visualiser ces données en format HTML ne reproduit pas nécessairement exactement le même résultat que celui

que vous pouvez voir dans le navigateur Web (par exemple, vous ne serez pas capable de voir les graphiques incorporés); toutefois, le résultat devrait vous donner une petite idée de l'apparence de la page originale.

Vous pouvez choisir le type d'affichage par défaut pour la fenêtre de Reconstruction de Session TCP dans l'onglet **Decodage** de la boîte de dialogue **Options** du programme.

Les boutons de **Navigation** vous permettent de rechercher le tampon de la session TCP précédente ou suivante. Le premier bouton d'avancement (>>) recherchera la session suivante entre deux hôtes qui ont été impliqués dans la première session reconstruite. Le second bouton d'avancement (>>>) recherchera la session suivante entre deux hôtes, n'importe lesquels. Si vous avez de multiples sessions dans la mémoire tampon entre deux hôtes, et que vous désirez les voir une à la fois, il est recommandé de commencer la reconstruction à partir de la première session, puisque le bouton « précédent » - **<<** ne peut pas naviguer au-delà de la session qui a été reconstruite en premier.

Les données obtenues peuvent être enregistrées en format binaire, texte, ou RTF (rich text file) en cliquant **Fichier =>Enregistrer sous** ... . Vous pouvez également rechercher une chaîne dans la session en cliquant **Modifier => Rechercher**... .

Statistiques et rapports

Cette fenêtre (**Affichage => Statistiques**) affiche les statistiques vitales réseau de votre ordinateur ou segment LAN, telles que le taux de paquets par seconde, le taux d'octets par seconde, les protocoles Ethernet, et les graphiques de distribution de sous-protocoles et protocoles IP. Vous pouvez copier n'importe lequel de ces graphiques au presse-papiers en double-cliquant sur un graphique. Les protocoles Ethernet, les graphiques en camembert des protocoles et sous-protocoles IP peuvent être orientés en utilisant les petits boutons au coin inférieur droit pour une meilleure visibilité des tranches des graphiques.

Les données affichées sur chaque page peuvent être enregistrées en format bitmap ou en texte délimité par des virgules en utilisant le menu contextuel (pop-up) ou la fonctionnalité glisser-déposer. La page Rapport permet que CommView génère automatiquement des rapports conventionnels en HTML ou en format texte délimité par des virgules.

Les statistiques réseau peuvent être collectionnées en utilisant toutes les données transitantes sur votre adaptateur réseau ou en utilisant les règles qui sont actuellement configurées. Si vous souhaitez que les compteurs de statistiques procèdent seulement les données (paquets) qui correspondent aux règles configurées et ignorent toutes les autres données, vous devriez cocher la case **Appliquer les règles actuelles**.

Général
Affiche des histogrammes de Paquets par seconde et d'Octets/Bits par seconde, un graphique de l'utilisation de la bande passante (le trafic par seconde divisé par la vitesse de liaison du modem ou du NIC), ainsi que tous les compteurs de paquets et d'octets.

Protocoles
Affiche la distribution des protocoles Ethernet, tels que ARP, IP, SNAP, SPX, etc. Utilisez la liste déroulante **Diagramme par** pour sélectionner une des deux méthodes de calcule disponibles : par nombre de paquets ou par nombre d'octets.

Protocoles IP
Affiche la distribution des protocoles IP. Utilisez la liste déroulante **Graphique par** pour sélectionner une des deux méthodes de calcul disponibles : par nombre de paquets ou par nombre d'octets.

Sous-protocoles IP
Déploie la distribution des principales applications de niveau de sous-protocoles IP : HTTP, FTP, POP3, SMTP, Telnet, NNTP, NetBIOS, HTTPS, et DNS. Pour ajouter plus de protocoles, cliquez sur le bouton **Personnaliser**. Ce dialogue vous permet de définir jusqu'à 8 protocoles conventionnels. Vous devriez entrer un nom de protocole, sélectionner le type de protocole (TCP/UDP), puis le numéro de port. Utilisez la liste déroulante **Graphique par** pour sélectionner une des deux méthodes de calcul disponibles : par nombre de paquets ou par nombre d'octets.

Tailles
affiche le graphique de distribution de la taille d'un paquet.

Hôtes (MAC) LAN
Répertorie les hôtes LAN par adresses MAC et affiche les statistiques de transfert de données. Vous pouvez assigner des alias aux adresses MAC. Si vous avez trop de paquets multipoints sur votre réseau et que la table d'hôtes par adresses MAC est surchargée, vous pourriez vouloir grouper les adresses multipoints en une seule ligne nommée GroupeMultipoint. Vous pouvez activer cette fonction en cochant la case **Grouper les adresses multipoints**. Veuillez noter que seuls les paquets arrivés après que cette option ait été activée seront groupés en conséquence; les paquets reçus auparavant ne seront pas affectés.

Hôtes (IP) LAN
Répertorie les hôtes LAN actifs par adresses IP et affiche les statistiques de transfert de données. Puisque les paquets IP capturés par le programme peuvent originer d'un nombre illimité d'adresses IP (à la fois de votre LAN interne et externe), par défaut cet onglet ne déploie aucune statistique. Pour afficher les statistiques, vous devriez d'abord configurer la plage d'adresses IP à être contrôlées en cliquant **Ajouter/Définir des plages**. Normalement, ces plages devraient appartenir à votre LAN, et configurer le programme pour contrôler une certain plage d'adresses IP permet l'utilisation des statistiques. Vous pouvez entrer n'importe quel nombre de plages, mais le nombre total d'adresses IP à être contrôlées ne peut excéder 1,000. Pour supprimer une plage, cliquez sur le bouton droit de la souris sur la liste des plages et sélectionnez la commande de menu appropriée. Vous pouvez assigner des alias aux adresses IP.

Matrices par MAC
Cette page affiche la matrice graphique des conversations entre hôtes en fonction de leur adresse MAC. Les hôtes représentés par leur adresse MAC sont placés sur le cercle, et les sessions sont représentées par des lignes connectées aux hôtes. Déplacer la souris sur un hôte met en valeur toutes les connexions que cet hôte a eu avec les autres. Vous pouvez changer le nombre des paires d'hôtes les plus actives affichées dans la matrice en changeant la valeur du champ **Paires les plus actives**. Pour changer le nombre des dernières paires d'adresses examinées par le programme, modifiez la valeur du champ **Dernières paires à prendre en compte**. Si votre segment réseau possède plusieurs paquets diffusés ou multipoints qui remplissent la matrice, vous pouvez ignorer de tels paquets en cochant les cases **Ignorer diffusés** et **Ignorer multipoints**.

Matrices par IP
Cette page affiche la matrice graphique des conversations entre hôtes en fonction de leur adresse IP. Les hôtes représentés par leur adresse IP sont placés sur le cercle, et les sessions sont représentées par des lignes connectées aux hôtes. Déplacer la souris sur un hôte met en valeur toutes les connexions que cet hôte a eu avec les autres. Vous pouvez changer le nombre des paires d'hôtes les plus actives affichées dans la matrice en changeant la valeur du champ **Paires les plus actives**. Pour changer le nombre des dernières paires d'adresses examinées par le programme, modifiez la valeur du champ **Dernières paires à prendre en compte**. Si votre segment réseau possède plusieurs paquets diffusés ou multipoints qui remplissent la matrice, vous pouvez ignorer de tels paquets en cochant les cases **Ignorer diffusés** et **Ignorer multipoints**.

Erreurs
Affiche les informations sur les erreurs Ethernet obtenues directement de l'adaptateur. Ci-dessous sont indiquées les explications des types d'erreur :

Rx CRS Errors
Le nombre de cadres reçus avec erreur circular redundancy check (CRC-vérification circulaire de redondance) ou frame check sequence (FCS-vérification de séquence de cadres).
Rx Alignment Errors
Le nombre de cadres reçus avec erreurs d'alignements.
Rx Overrun
Le nombre de cadres non reçus dû à une surcharge d'erreurs sur le NIC.
Tx One Collision
Le nombre de cadres transmis avec succès après exactement une collision.
Tx More Collisions
Le nombre de cadres transmis avec succès après plus d'une collision.
Tx Deferred
Le nombre de cadres transmis avec succès après que le NIC diffère une transmission au moins une fois.
Tx Max Collisions
Le nombre de cadres non transmis dû aux collisions excessives.
Tx Underrun
Le nombre de cadres non transmis dû à une sous-utilisation d'erreurs sur le NIC.
Tx Heartbeat Failure
Le nombre de cadres transmis avec succès sans détection du Collision-Detect Heartbeat.
Tx Times CRS Lost
Le nombre de fois que le signal CRS a été perdu durant la transmission de paquets.
Tx Late Collisions
Le nombre de collisions détectées après la fenêtre normale.
Rx Frames w/Errors
Le nombre de cadres qu'un NIC reçoit mais qui n'indique pas les protocoles dû aux erreurs.
Rx Frames w/o Errors
Le nombre de cadres qu'un NIC reçoit sans erreur et indique les protocoles reliés.
Tx Frames w/Errors
Le nombre de cadres qu'un NIC échoit à transmettre.
Tx Frames w/o Errors
Le nombre de cadres qui sont transmis sans erreur.

Veuillez noter que :

- Les connexions par modem d'accès commuté ne sont pas prises en charge, seulement le matériel de cartes Ethernet.
- Votre adaptateur peut ne pas prendre en charge tous les champs listés. Quelques marchands fabriquent des NICs qui procurent toute l'information requise, d'autres pas.
- Contrairement à d'autres données dans la fenêtre Statistiques, les données sur l'onglet **Erreurs** ne peuvent pas être réinitialisées lorsque vous cliquez sur le bouton **Réinitialiser**. Le compteur est initialisé lorsque votre ordinateur démarre.
- Cet onglet n'est pas pris en charge sous Windows 95.

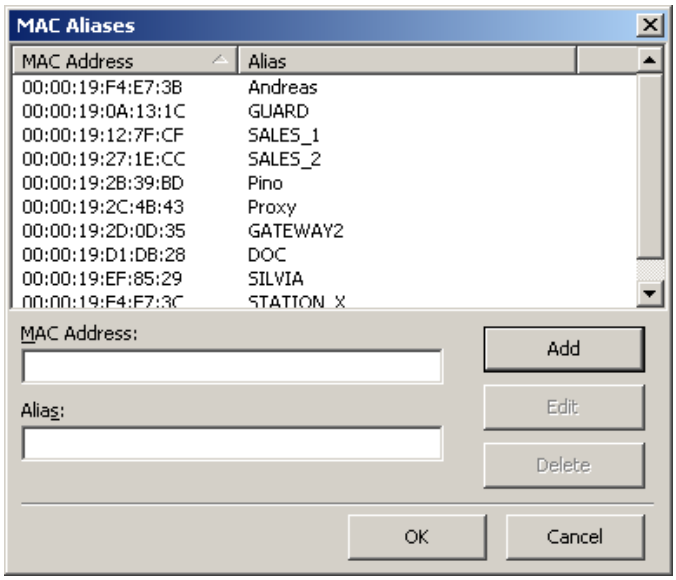
Rapport
Cet onglet vous permet que CommView génère automatiquement des rapports conventionnels en HTML (incluant images de graphiques et graphes) ou en format texte délimité par des virgules.

Il est possible de faire en sorte que le programme génère des statistiques sur les données précapturées, en plus des statistiques en temps réel. Pour ce faire, chargez un fichier de capture dans l'Éditeur de fichiers journaux et cliquez sur **Fichier => Générer des statistiques**. Optionnellement, vous pouvez réinitialiser les statistiques précédemment recueillies qui sont affichées dans la fenêtre **Statistiques**. Veuillez prendre note que cette fonction n'affichera que la distribution de paquets selon un horaire établi. Elle est limités à l'affichage des totaux, des tableau de protocoles et d'hôtes LAN.

Utilisation d'alias

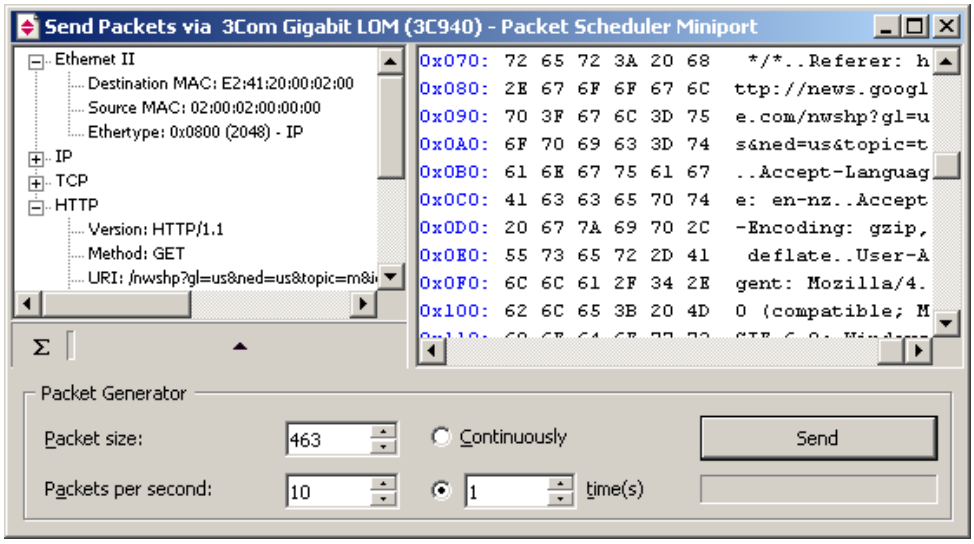
Les alias sont des noms faciles à mémorer et humainement lisibles que CommView substituera pour une adresse MAC ou IP, lorsque sont affichés les paquets sur les onglets Pacquts et Statistiques. Ceci peut rendre les paquets plus facilement reconnaissables et analysables. Par exemple, 00:00:19:2D:0D:35 devient GATEWAY2, et ns1.earthlink.com devient MyDNS.

Pour ajouter un alias MAC, cliquez le bouton droit de la souris sur un paquet et sélectionnez **Créer un alias en utilisant une adresse MAC source** ou **en utilisant une adresse MAC destination** à partir du menu contextuel (pop-up). Une fenêtre va apparaître où le champ de l'adresse MAC est déjà rempli, et vous n'aurez qu'a y ajouter un alias. Alternativement, vous pouvez cliquer **Paramètres** => **Alias MAC** et remplir l'adresse MAC et les champs Alias manuellement. Pour supprimer un alias ou effacer la liste entière des alias, cliquez le bouton droit de la souris sur la fenêtre Alias et sélectionnez **Supprimer l'enregistrement** ou **Effacer tout**. Ceci s'applique aussi à la creation d'alias IP. Lorsqu'un nouvel alias IP est créé en cliquant de la droite sur un paquet, le champ d'alias est préalablement rempli avec le nom d'hôte correspondant (si disponible) et peut être modifié par l'utilisateur.



Générateur de paquets

Cet outil vous permet d'éditer et d'envoyer des paquets via votre carte réseau. Il est disponible seulement sous Windows NT/2000/XP/2003. Pour ouvrir le Packet Generator, cliquez **Outils => Générateur de paquets**, ou sélectionnez un paquet de l'onglet **Paquets**, cliquez le bouton droit de la souris sur ce dernier, puis sélectionnez la commande **Envoyer le(s) paquet(s)**.



Veuillez prendre note que le Générateur de paquets ne peut et ne devrait pas être utilisé pour l'envoi de flots de données TCP au niveau de l'application, c'est-à-dire qu'il ne peut traiter l'incrémentation des valeurs SEQ ou ACK, ajuster les sommes de contrôles et la taille des paquets automatiquement, et ainsi de suite. Si vous devez envoyer un flot de données TCP, vous devriez utiliser une application Winsock spécifiquement conçue à ces fins. Le Générateur de paquets est un outil pour la relecture de données précapturées, l'essai des pare-feu et des systèmes de détection d'intrusion, ainsi que pour la performance d'autres tâches spécifiques nécessitant la préparation manuelle de paquets.

Le Générateur de paquets vous permet de changer le contenu du paquet et d'avoir le décodage du paquet affiché dans la fenêtre de gauche, lorsque vous l'éditez. Vous pouvez créer des paquets de toutes sortes; vous avez le contrôle total sur le contenu des paquets. Pour les paquets IP, TCP, UDP et ICMP, vous pouvez automatiquement corriger le(s) sommes de contrôle (checksums(s)) en cliquant sur le bouton **Sigma**.

Vous pouvez aussi cliquer sur le bouton avec une flèche pour afficher la liste des patrons de paquet prédéfinis disponibles. Le programme est fourni avec les patrons **TCP**, **UDP** et **ICMP**; les utiliser est souvent plus rapide que de saisir les codes hexadécimaux dans la fenêtre de l'éditeur. Ces patrons contiennent les paquets TCP, UDP et ICMP typiques, mais vous voudrez probablement éditer plusieurs champs du paquet et utiliser des valeurs plus représentatives suivant vos besoins, comme les adresses réelles MAC et IP, les numéros de ports, les nombres SEQ et ACK, etc. Vous pouvez utiliser vos propres patrons à la place de ceux prédéfinis. Vous pouvez glisser-déposer un paquet depuis l'onglet des Paquets de CommView vers la section des patrons de la fenêtre du Générateur de Paquets. Si vous déposez plusieurs paquets dans la section des patrons, seul le premier sera utilisé comme patron. Une entrée nommée Nouveau Patron apparaitra dans la liste des patrons. Vous pouvez renommer un patron en cliquant dessus avec le bouton droit dans la liste et en sélectionnant **Renommer**. Si vous devez effacer un patron, cliquez dessus avec le bouton droit et sélectionnez **Effacer** depuis le menu déroulant. Sélectionner un patron dans la liste charge le paquet qu'il contient dans la fenêtre de l'éditeur où il pourra être édité avant envoi.

Vous pouvez aussi placer des fichiers NCF avec les patrons de votre choix dans le sous-répertoire TEMPLATES (patrons) du dossier principal de l'application. Si CommView trouve des fichiers NCF (ou juste l'un d'entre eux) dans le sous-répertoire TEMPLATES (patrons), il va les lister parmi les patrons disponibles dans la liste déroulante. Ces fichiers NCF devraient contenir un seul paquet par fichier, mais si vous utilisez un fichier qui en contient plusieurs, CommView chargera seulement le premier.

Une fois que vous avez édité un paquet, utilisez les contrôles ci-dessous pour l'envoyer :

Taille du paquet – modifie la taille d'un paquet.
Paquets par seconde – contrôle la vitesse à laquelle les paquets seront envoyés. Soyez certain de ne pas envoyer de paquets trop rapidement si vous avez une connexion lente. Par exemple, envoyer un paquet de 1 000 octets 5 000 fois par seconde est plus que ce que votre ordinateur 10Mbit NIC ne peut supporter.
Continuellement – sélectionnez cette option si vous désirez que le Générateur de paquets envoie des paquets continuellement jusqu'à ce que vous cliquiez sur **Arrêter**.
Fois – sélectionnez cette option si vous désirez que le Générateur de paquets envoie un paquet un nombre donné de fois.
Envoyer/Arrêter – cliquez ce bouton lorsque vous êtes prêt(e) à envoyer des paquets ou lorsque vous désirez arrêter d'en envoyer.

Travailler avec plusieurs paquets

Vous pouvez utiliser le Générateur de paquets pour envoyer plusieurs paquets à la fois. Pour ce faire, sélectionnez seulement les paquets que vous voulez envoyer dans la liste et invoquez le Générateur de paquets en utilisant le menu du bouton droit de la

souris, ou glissez-déposez les paquets sélectionnés vers la fenêtre du Générateur de paquets. Alternativement, vous pouvez glisser-et-déposer des fichiers capturés dans tous les formats pris en charge directement dans la fenêtre du Générateur de paquets. Lorsque plusieurs paquets sont envoyés, l'éditeur de paquets et l'arborescence décodeur deviennent invisibles.

Enregistrer des paquets édités

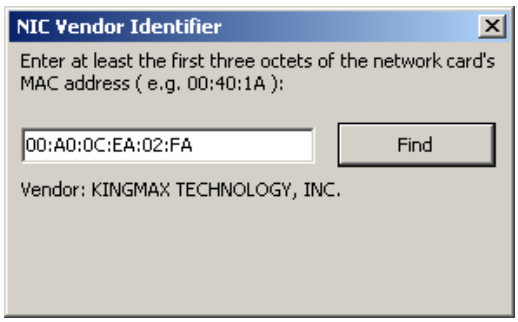
Si vous éditez un paquet et que vous voulez l'enregistrer, simplement glisser l'arborescence décodeur sur le bureau ou dans tout autre dossier, puis un nouveau fichier en format NCF contenant le paquet sera créé. Le nom du fichier est toujours PACKET.NCF. Vous pouvez aussi glisser le paquet vers la fenêtre des patrons. Si vous devez éditer et envoyer plusieurs paquets, modifiez-les un par un, en le glissant chaque fois sur votre Bureau et en le renommant. Après quoi, ouvrez une nouvelle fenêtre Éditeur de fichiers journaux, glissez-déposez les paquets modifiés du Bureau vers l'Éditeur de fichiers journaux, sélectionnez-les en utilisant le bouton Maj., puis invoquez le Générateur de paquets en utilisant le menu contextuel.

ATTENTION :

1. N'utilisez pas le Générateur de paquets, à moins que vous ne sachiez exactement quel effet vous souhaitez rencontrer. Envoyer des paquets peut produire des résultats imprévisibles, et nous recommandons fortement l'abstention de l'utilisation de cet outil, à moins que vous ne soyiez un administrateur de réseau expérimenté.
2. Il devrait y avoir au moins un ordinateur opérant sur votre LAN, en plus de votre propre ordinateur, lorsque vous utilisez cet outil. Autrement, vous expérimenterez des délais sévères dans l'envoi des paquets.
3. Cet outil ne peut être utilisé pour envoyer des paquets via les adaptateurs RAS sous Windows NT.

Identificateur de fournisseur NIC

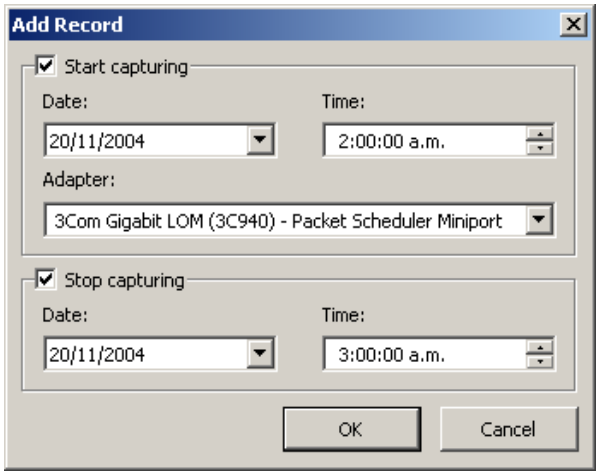
Les premières 24 bits d'une adresse MAC de votre carte réseau identifie uniquement le marchand de la carte réseau. Ce nombre de 24-bits est appelé le OUI ("Organizationally Unique Identifier"). L'Identificateur de fournisseur NIC est un outil qui vous permet de rechercher un nom de fournisseur par adresse MAC. Pour rechercher un nom de marchand, cliquez **Outils** => **Identificateur de fournisseur NIC**, entrez une adresse MAC, puis cliquez **Rechercher**. Le nom du fournisseur sera alors affiché. Par défaut, CommView remplace les trois premiers octets de l'adresse MAC par le nom du fournisseur du périphérique dans l'onglet **Paquets**. Ce comportement peut être modifié en décochant la case **Afficher le nom du fournisseur dans l'adresse MAC** via l'onglet Général de la boîte de dialogue **Options** du programme.



La liste des fournisseurs est contenue dans le fichier MACS.TXT, situé dans le dossier d'application de CommView. Vous pouvez éditer cette liste manuellement pour ajouter/modifier de l'information.

Planificateur

Vous pouvez utiliser cet outil pour créer et éditer les tâches de capture planifiée. Ceci est pratique lorsque vous souhaitez que CommView démarre et/ou arrête la capture et que vous n'êtes pas dans les environs, par exemple, durant la nuit ou les week-ends. Pour ajouter une nouvelle tâche, cliquez **Outils** => **Planificateur**, puis cliquez sur le bouton **Ajouter**.



Utilisez le cadre **Démarrer la capture** pour spécifier la date et l'heure auxquelles CommView démarrera la capture. Utilisez la liste déroulante **Adaptateur** pour spécifier l'adaptateur qui devrait être utilisé. Utilisez la cadre **Arrêter la capture** pour spécifier la date et l'heure auxquelles CommView arrêtera la capture. Vous n'avez pas nécessairement besoin de cocher les cases **Démarrer la capture** et **Arrêter la capture**. Si vous ne cochez que la première case, la capture continuera jusqu'à ce que vous l'arrêtiez manuellement. Si vous ne cochez que la seconde case, alors vous aurez à démarrer la capture manuellement, mais CommView l'arrêtera automatiquement à la date et à l'heure spécifiées.

Si CommView capture déjà des paquets au moment où la tâche planifiée est due et que l'adaptateur que vous avez spécifié est différent de celui qui est actuellement surveillé, CommView arrêtera la capture, basculera vers l'autre adaptateur spécifié, puis redémarrera la capture.

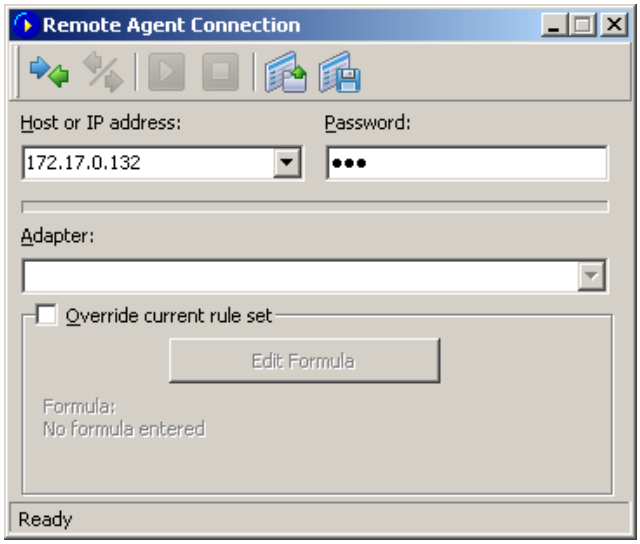
Il est important de comprendre que les tâches planifiées ne peuvent être exécutées que si CommView est en exploitation.

Utilisation de Remote Agent

CommView Remote Agent (agent distant) est un produit compagnon qui peut être utilisé pour contrôler le trafic de réseau à distance. Tout ce que vous avez à faire est d'installer Remote Agent sur l'ordinateur ciblé, et ensuite utiliser CommView pour vous connecter à Remote Agent. Une fois que vous êtes connecté et authentifié, vous pouvez commencer à contrôler à distance comme si vous y étiez.

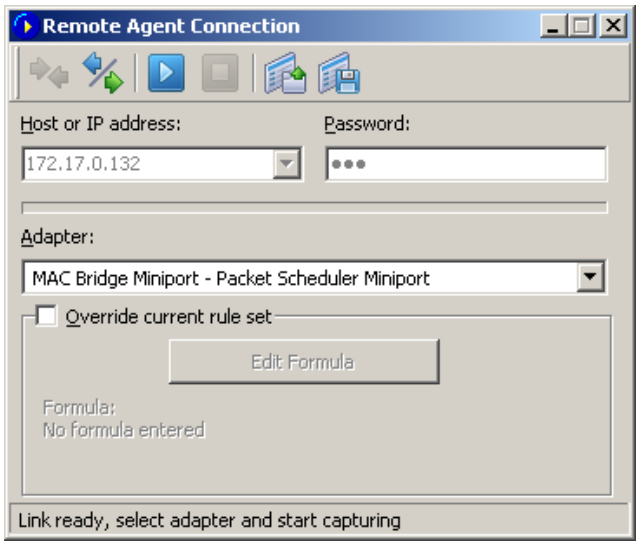
Important : le chapitre décrit comment utiliser CommView pour se connecter à Remote Agent et capturer le trafic à distance. Pour une information détaillée sur l'installation et la configuration de Remote Agent, veuillez vous référer au fichier d'aide inclus avec Remote Agent. Il est hautement recommandé que vous lisiez attentivement la documentation de Remote Agent avant d'en faire l'utilisation. CommView Remote Agent peut être téléchargé de notre site.

Pour passer au mode de contrôle à distance, cliquez **Fichier** => **Mode de surveillance à distance**. Une barre d'outils additionnelle apparaîtra dans la fenêtre principale de CommView à côté de la barre d'outils principale. Si vous êtes derrière un pare-feu ou un serveur proxy, ou utilisez un port non-standard de Remote Agent, vous pourriez avoir besoin de cliquer sur le bouton **Paramètres réseau avancés** pour changer le numéro du port et/ou entrer les configurations de serveur proxy SOCKS5.



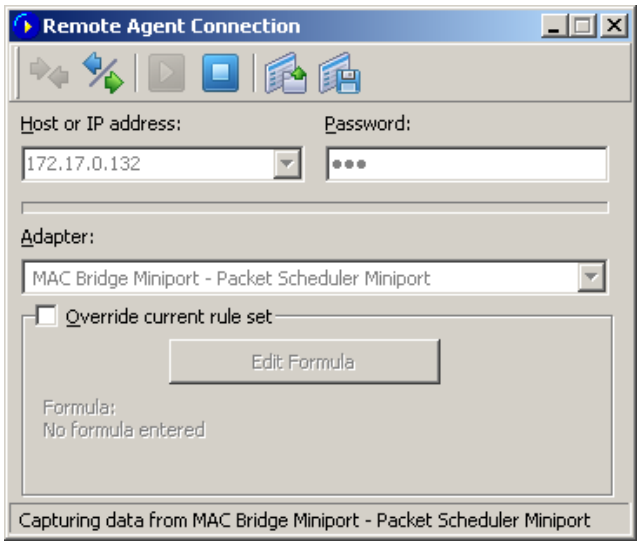
Cliquez sur le bouton **Nouvelle Connexion d'Agent Distant** pour établir une nouvelle connexion, ou cliquez sur le bouton **Charger un Profile d'Agent Distant** de la boîte à outils pour charger un profile de connexion d'agent distant précédemment sauvegardé. Un profile antérieur peut aussi être chargé à partir de la fenêtre Nouvelle Connexion d'Agent Distant.

Une fenêtre apparaîtra ou vous pourrez saisir l'adresse IP de l'ordinateur sur lequel tourne CommView Remote Agent, le mot de passe de la connexion et cliquer sur le bouton **Se Connecter**, et si le mot de passe est correct, une connexion sera établie. Vous verrez alors le message *Link Ready (lien prêt)*, puis la boîte de selection du périphérique listera les périphériques d'ordinateurs distants.



Il est temps de configurer les règles de capture en utilisant l'onglet **Règles**. Il est très important de configurer ces règles correctement pour que le volume du trafic entre Remote Agent et CommView n'excède pas la limite de la bande passante sur l'une ou l'autre des connexions, sinon vous allez expérimenter des délais de fonctionnement sensibles. Soyez sûr(e) de filtrer les paquets

inutiles (voir ci-dessous pour plus de détails sur ce sujet). Vous pouvez aussi appliquer un ensemble de règles de capture personnalisées sur cette connexion et contourner les règles courantes définies dans CommView en cochant la case **Contourner l'ensemble de règles courant**, cliquer sur le bouton **Editer Formule** et saisir les formules des règles dans le champ en dessous. La syntaxe de la formule est la même que celle utilisée dans Règles Avancées. Dès que vous êtes prêt à commencer la surveillance, sélectionnez le périphérique réseau à partir de la liste et cliquez sur le bouton **Commencer la Capture** de la boîte à outils. CommView vous permet de sauvegarder les réglages de la Connexion d'Agent Distant dans un profile de connexion pour y accéder ultérieurement de manière simple et rapide. Cliquez sur le bouton **Sauvegarder Profile d'Agent Distant** de la boîte à outils dans la fenêtre Nouvelle Connexion d'Agent Distant et saisissez un nom pour le fichier.



CommView commencera à capturer le trafic d'ordinateur à distance comme si c'était le trafic de votre réseau local; il n'y a virtuellement aucune différence entre l'utilisation de CommView localement ou à distance. Lorsque vous en avez terminé avec le contrôle à distance, simplement cliquez sur le bouton **Arrêter la capture** de la barre d'outils. Vous pouvez alors modifier l'adaptateur et vous déconnecter de Remote Agent en cliquant sur le bouton **Déconnecter** de la barre d'outils. Pour retourner au mode standard, cliquez **Fichier** => **Mode de surveillance à distance**, puis la barre d'outils supplémentaire disparaîtra.

Veuillez noter que CommView peut travailler avec plusieurs Agents Distants simultanément. Vous pouvez ouvrir plusieurs connexions distantes, chacune ayant ses propres réglages et un ensemble indépendant de règles, et collecter le traffic depuis les segments réseau distants dans une seule instance de CommView.

Capture de trafic par boucle

CommView vous permet de capture le trafic par boucle. Cette fonctionnalité est disponible sous Windows NT/2000/XP/2003. Pour commencer à surveiller le périphérique de boucle locale, sélectionnez le depuis la liste déroulante dans la barre d'outils.

Les paquets par boucle sont les paquets reçus/envoyés vers le même ordinateur, c'est-à-dire des paquets de retour. Typiquement, il n'existe virtuellement pas de trafic par boucle sur un ordinateur standard. Néanmoins, le trafic par boucle est largement utilisé par les développeurs logiciels pour le déboguage d'applications relatives aux réseaux. Ainsi, la fonctionnalité de capture de trafic par boucle de CommView est principalement orientée à ce groupe d'utilisateurs.

Lorsque vous capturez du trafic par boucle, les paquets paraissent exactement comme tout autre paquet réseau, sauf que les sommes de contrôle ne sont pas computées. Veuillez porter une attention spéciale aux particularités suivantes lors de la capture de trafic par boucle :

- CommView capture le trafic par boucle sur toutes les adresses IP locales. Celui-ci comprend toujours 127.0.0.1/255.0.0.0, mais pourrait également inclure les adresses IP de vos adaptateurs Ethernet, par exemple 192.168.0.1.
- Les paquets ICMP ne peuvent pas être capturés. Les autres protocoles IP peuvent l'être (TCP, UDP, etc.).
- Seuls les paquets reçus/envoyés avec succès sont capturés. Par exemple, si une tentative de connexion n'est pas réussie en raison du port de destination fermé, vous ne verrez ainsi aucun paquet SYN / RST.
- Les sessions sont silencieusement fermées ; aucun paquet FIN n'est capturé.

Configuration des Options

Vous pouvez configurer quelques-unes des options du programme en sélectionnant **Paramètres** du menu.

Polices

Utilisez cette entrée du menu pour modifier la police du texte de l'interface, des paquets et du décodeur de paquets. Pour changer la couleur du texte des paquets, utilisez le menu **Options** (ci-dessous).

Options

Général

Démarrage automatique de la capture – cochez cette case si vous désirez que CommView commence à capturer les paquets immédiatement après le lancement du programme. Pour les systèmes avec de multiples adaptateurs, vous devriez aussi sélectionner l'adaptateur qui doit être utilisé à partir de la liste déroulante.

Réseau

Désactiver la résolution DNS – cochez cette case si vous ne voulez pas que CommView exécute un reverse DNS lookups des adresses IP. Si vous la cochez, la colonne **Nom d'hôte** sur l'onglet **Dernières Connexions IP** sera vide.

Convertir les valeurs de port numérique en noms de service – cochez cette case si vous voulez que CommView affiche les noms de service au lieu des nombres. Par exemple, si cette case est cochée, port **21** est montré comme **ftp**, et port **23** comme **telnet**. Le programme convertit les valeurs numériques en noms de service en utilisant le dossier SERVICES installé par Windows. Dépendemment de la version de votre Windows, le dossier SERVICES est localisé dans différents fichiers : avec Windows 95/98/Me vous pouvez le trouver dans le fichier \Windows, et avec Windows NT/2000/XP/2003, vous le trouvez dans le fichier \Winnt\system32\drivers\etc. Vous pouvez éditer ce fichier manuellement si vous désirez ajouter plus de ports/noms de service.

Convertir les adresse MAC en alias – substitue les adresses MAC pour des alias sur l'onglet **Paquets**. Les Alias peuvent être assignés aux adresses MAC en utilisant la commande de menu **Paramètres => Alias MAC**.

Convertir les adresses IP en alias – substitue les adresses IP pour des alias sur les onglets **Paquets** et **Statistiques**. Les Alias peuvent être assignés aux adresses IP en utilisant la commande de menu **Paramètres =>Alias IP**.

Convertir les adresses IP en noms d'hôte dans l'onglet << Paquets >> – cochez cette case si vous voulez que CommView affiche les noms d'hôte résolus au lieu d'adresses IP dans l'onglet **Paquets**. Si cette case est cochée, alors CommView tentera d'abord de trouver un alias pour l'adresse IP donnée. Si aucun alias n'est trouvé ou que la case précédente (**Convertir les adresse IP en alias**) n'est pas cochée, CommView fera une requête à la masque DNS interne pour le nom d'hôte. Si aucun nom d'hôte n'est trouvé, l'adresse IP sera affichée sous forme numérique.

Afficher le nom du fournisseur dans l'adresse MAC – par défaut, CommView remplace les trois premiers octets de l'adresse MAC par le nom du fournisseur du périphérique dans l'onglet **Paquets**. Décochez cette case si vous voulez changer ce comportement.

Utiliser le mode non-espion – par défaut, CommView place l'adaptateur de réseau en mode espion, ce qui veut dire que le programme capture tout le trafic du segment local du LAN. Cocher cette case fait basculer le mode de CommView à non-espion, lequel vous utilisez quelques fois, par exemple si la politique IT de votre compagnie ne vous permet pas le contrôle espion de paquets, ou alors lorsque vous désirez réduire l'utilisation du CPU dans une situation où vous êtes seulement intéressé dans vos propres paquets entrants et sortants et devez filtrer à l'extérieur de multiples paquets transitants.

Notifier lorsque la liste d'adaptateurs a été modifiée – cochez cette case si vous souhaitez que CommView affiche un message dans la zone de notification système lorsque le nombre d'adaptateurs réseau actifs a été modifié.

Afficher le chemin complet du processus – cochez cette case si vous voulez voir le chemin complet du processus qui envoi/reçoit des paquets dans l'onglet **Dernières Connexions IP** et sur le volet de décodage de l'en-tête du paquet dans l'onglet **Paquets** (par exemple, "C:\Files\Program.exe" est le chemin complet de "Program.exe").

Afficher les noms de périphérique standards – cocher cette option permet à CommView d'afficher le nom des périphériques, dans la liste déroulante de la barre d'outils, tels qu'ils apparaissent dans la page des connexions réseau de Windows.

Utilisation de la mémoire

Affichage

Paquets maximum dans la mémoire tampon – configure le nombre maximum de paquets que le programme stocke dans la mémoire et peut afficher dans la liste de paquets (2ème onglet). Par exemple, si vous configurez cette valeur à 3000, seulement les 3000 derniers paquets seront stockés dans la mémoire et la liste de paquets. Le plus haut cette valeur atteint, le plus de ressources informatiques le programme consomme.

Notez que si vous souhaitez avoir accès à un nombre élevé de paquets, il est recommandé que vous utilisiez les caractéristiques d'enregistrement automatique (consultez Journalisation pour plus d'informations) : cette caractéristique vous permet de supprimer tous les paquets d'un fichier journal sur un disque dur.

Maximum de lignes dans les Dernières Connexions IP - configure le nombre de lignes que le programme affiche dans l'onglet Dernières Connexions IP. Lorsque le nombre de connexions excède la limite, les connexions qui ont été inoccupées pour la plus longue période de temps sont supprimées de la liste.

Mémoire tampon pilote (Windows NT/2000/XP/2003 seulement) – configure la taille du pilote de la mémoire tampon. Cette caractéristique affecte la performance du programme : le plus de mémoire est allouée pour le pilote de la mémoire tampon, le moins de paquets le programme échappe. Pour un trafic bas de LANs et de connexions par modem d'accès commuté, la taille de la mémoire tampon n'est pas critique. Pour les trafic élevés de LANs, vous pourriez vouloir augmenter la taille du mémoire tampon si le programme échappe des paquets. Pour verifier le nombre de paquets échappés, utilisez la commande de menu **Fichier => Données de performance** lorsque la capture est en cours.

Dernières Connexions IP

Affichage logique– vous permet de sélectionner la mise en page des Dernières Connexions IP qui convient le mieux à vos besoins. Sélectionner un item à partir de la liste déroulante va afficher la description logique de celui-ci. Dans la plupart des cas, il est recommandé d'utiliser la logique **Smart** par défaut.

Définir les adresses IP locales – vous devriez utiliser cet outil si vous contrôlez un trafic LAN avec plusieurs paquets transitants et un mélange d'adresses IP entrantes et sortantes. Dans une telle situation, CommView ne << connaît >> pas quelles adresses IP devraient être traitées localement et lesquelles pourraient renverser l'adresse IP dans les colonnes IP locale et IP à distance. Cet outil vous permet de définir les adresses de réseau locales et les masques de sous-réseau pour assurer que la fenêtre Dernières Connexions IP fonctionne correctement. Ceci fonctionnera seulement si vous utilisez la logique **Smart** par défaut.

Couleurs

Couleur de paquet – configure la couleur pour afficher les paquets sur l'onglet Paquets selon la direction du paquet (entrant, sortant, transitant). Pour modifier la couleur, sélectionnez la direction du paquet à partir de la liste déroulante et cliquez sur le rectangle coloré.

Colorer les en-têtes de paquets – cochez cette case si vous désirez que CommView colore le contenu des paquets. Si cette case est cochée, le programme déploie les huit premières couches de paquets en utilisant différentes couleurs. Pour modifier la couleur, sélectionnez le type d'en-tête pour lequel vous désirez changer la couleur et cliquez sur le rectangle coloré.

Surbrillance de syntaxe de formule – personnalisez les couleurs pour la surbrillance de mots-clés de formules dans la fenêtre de syntaxe avancée Règles avancées.

Couleur de séquence d'octet sélectionné – définit les couleurs de la police et du fond de la séquence d'octet qui a été sélectionnée dans l'arborescence de décodage. Par exemple, lorsque vous sélectionnez le dossier d'arborescence << TCP >>, la partie correspondante du paquet sera mis en surbrillance en utilisant ces couleurs.

Décodage

Toujouts tout développer tous les dossiers dans la fenêtre Décodeur – cochez cette case si vous voulez que tous les dossier de la fenêtre Décodeur soient automatiquement développés, lorsque vous sélectionnez un nouveau paquet dans la liste de paquets.

Décoder jusqu'au premier niveau seulement dans l'exportation ASCII – cette option affecte le format de décodage utilisé lorsque vous exportez un paquet de fichier journal ou un paquet individuel en dossier ASCII avec décodage. Si cette case est cochée, seulement les dossiers de tête vont être enregistrés. Par exemple, si vous enregistrez un paquet TCP/IP lorsque cette option est désactivée, tout *Type of service* sous-dossier est enregistré. Lorsque cette option est activée, ces sous-dossiers ne sont pas enregistrés. Cocher cette case faiten sorte que les fichiers ASCII sortants sont moins détaillés et plus compacts.

Ignorer sommes de contrôle incorrectes pour reconstr. Sessions TCP – cette option affecte la façon dont CommView traîte les paquets TCP/IP malformés lors de reconstructions de sessions TCP. Par défaut, cette option est activée, et les paquets avec des sommes de contrôle (checksums) incorrectes sont discartés dans le processus de reconstruction. Si vous désactivez cette option, les paquets avec des sommes de contrôle (checksums) incorrectes seront discartés et non affichés dans la fenêtre de reconstruction de sessions TCP. Attention aux utilisateurs de carte Gigabit : tous les paquets sortants auront une somme de contrôle (checksum) incorrecte si la caractéristique << checksum offload >> est présente. Si vous désactivez cette option, il est probable que vous verrez seulement la moitié de la session TCP reconstruite. Ceci s'applique également à la reconstruction de sessions par boucle, puisque les paquets par boucle sont defines par une somme de contrôle de zéro.

Décompresser le contenu GZIP – cochez cette case si vous souhaitez que CommView convertisse le contenu http compressé au format GZIP en texte lisible dans les fenêtres de Reconstructions de session TCP. Le contenu GZIP n'est décompressé que lors le type d'affichage de la fenêtre est défini à « ASCII ».

Reconstruire les images – cochez cette case si vous souhaitez que CommVire convertisse les flots de données http binaires représentant des images en images affichables au format JPG, BMP, PNG et GIF dans les fenêtres de Reconstruction de session TCP. Les images ne sont affichées que lorsque le type d'affichage de la fenêtre est défini à « HTML ». Les images ne sont jamais affichées dans les pages HTML auxquelles elles appartiennent, puisqu'elles sont transférées par le serveur dans une session HTTP séparée.

Type d'affichage par défaut – sélectionnez le type d'affichage, à partir de la liste déroulante, que vous désirez appliquer par défaut pour la fonctionnalité de Reconstruction de Session TCP. Les choix disponibles sont ASCII, HEX, HTML et EBCDIC.

Divers

Masquer de la barre des tâches sur réduction - cochez cette case si vous ne voulez pas voir le bouton de programme sur la barre d'outils de Windows lorsque vous minimisez le programme. Si cette case est cochée, utilisez l'icône de plateau du programme pour sa restitution après sa minimisation.

Permettre plusieurs instances de l'application – cochez cette case si vous voulez avoir plusieurs instances de CommView opérant simultanément, pour être capable de capturer le trafic passant à travers différents adaptateurs. Cette option n'est pas disponible sous Windows 95.

Inviter à confirmer lors de la fermeture de l'application – cochez cette case si vous désirez que le programme vous demande une confirmation lorsque vous quittez.

Défilement automatique de la fenêtre des données de paquet - si cette case est cochée, le programme examine le texte de la fenêtre de données de paquet automatiquement lorsque vous sélectionnez un nouveau paquet de la liste de paquets (mais seulement si le texte ne correspond pas à celui dans la fenêtre). Ceci est utile lorsque vous voulez voir le contenu d'un long paquet sans examiner manuellement la fenêtre.

Défilement automatique de la liste de paquets au dernier paquet - si cette case est cochée, alors le programme défile automatiquement la liste de paquets de l'onglet **Paquets** jusqu'au dernier paquet reçu.

Tri automatique des nouveaux enregistrements dans les dernières connexions IP - si cette case est cochée, le programme trie automatiquement les nouveaux enregistrements sur l'onglet Statistiques IP selon les critères de tri définis par l'utilisateur (par exemple, ordre ascendant des adresses à distance IP).

Contrôle d'utilisation intelligente du processeur – si cette case est cochée, le programme essaie de diminuer l'utilisation du processeur lors de la capture d'un taux élevé de trafic en diminuant la qualité et la fréquence des rafraîchissements d'écran.

Exécuter au démarrage de Windows – si cette case est cochée, le programme est automatiquement lancé chaque fois que vous lancez Windows.

Exécuter avec une fenêtre réduite – si cette case est cochée, le programme est lancé minimisé et la fenêtre principale n'est pas affichée jusqu'à ce que vous cliquiez sur l'icône de plateau ou le bouton de la barre d'outils.

Extensions

Cet onglet est utilisé par les plugiciels de tierce partie pour la performance des tâches de configuration. Veuillez vous reporter à la section Échange de données avec votre application pour de plus amples informations.

Rechercher un paquet

Ce dialogue (**Recherche => Rechercher un paquet**) vous permet de trouver les paquets correspondant à un texte spécifique. Entrez une chaîne de recherche, sélectionnez le type d'information entrée (**Chaîne** ou **Hex**), puis cliquez **Chercher suiv.**. Le programme recherchera les paquets qui correspondent aux critères de recherches et les déploiera dans l'onglet Packets.

Vous pouvez entrer une chaîne de texte, en valeur hexadécimale ou en adresse IP. Une chaîne hexadécimale devrait être utilisée lorsque vous voulez entrer des caractères non-prononçables : tapez seulement les valeurs de caractères hexadécimaux séparées par des espaces, e.g. AD 0A 02 78 04.

Cochez **Respecter la casse** pour une recherche sensible à la casse. Cochez **Au décalage** pour rechercher une chaîne qui commence à un certain décalage. Notez que l'indicateur décalage est hexadécimal et à base zéro (i.e. si vous recherchez le premier byte du paquet, la valeur décalage sera de 0).

Référence de port

Cette fenêtre déploie une table des nombre de ports et des noms de service correspondants. Cette référence est obtenue à partir du fichier SERVICES installé par Windows. En fonction de la version de Windows, le fichier SERVICES est situé dans différents dossiers : Dans Windows 98/Me, vous pouvez le trouver dans le dossier **\Windows**, et dans Windows NT/2000/XP/2003, vous le trouvez dans le dossier **\system32\drivers\etc**. Vous pouvez éditer ce fichier manuellement, si vous désirez ajouter plus de ports/noms de service. CommView lit ce fichier au démarrage, les changements apportés au fichier seront donc affichés seulement après le redémarrage du programme.

Foire aux questions

Dans ce chapitre, vous pouvez trouver les réponses à quelques-unes des questions les plus fréquemment demandées. Le plus récent FAQ est toujours disponible au http://www.tamos.com/products/commview/faq.php .

Q. Est-ce que CommView peut être utilisé pour capturer le trafic d'un adaptateur (RAS) par modem d'accès commuté?
A. Oui, Windows 98/Me/NT/2000/XP/2003.

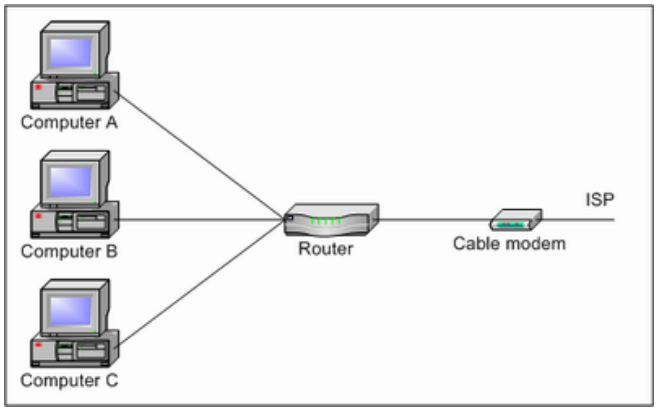
Q. Qu'est-ce que CommView "voit" exactement lorsqu'installé sur un ordinateur connecté sur un LAN?
A. CommView active le mode confus de la carte-réseau et peut capturer le trafic de réseau sur le segment du LAN. En d'autres mots, il capture normalement et analyse les paquets adressés à tous les ordinateurs sur le segment, pas seulement à ceux où le programme opère. Il y a certaines limitations pour les adaptateurs sans fil Ethernet (vous pouvez contrôler seulement le trafic entrant/sortant) et les réseaux commutés (consultez la prochaine question de ce FAQ sur les commutateurs).

Q. Je suis connecté sur un LAN à travers un commutateur, et lorsque je lance CommView, il capture seulement les paquets envoyés vers et venant de ma machine. Je ne peux voir le trafic sur les autres machines. Pourquoi?
A. Contrairement aux concentrateurs, les commutateurs préviennent les sondeurs (sniffing) confus. Dans un environnement en réseau avec commutateur, CommView (ou tout autre analyseur de paquets) est limité à la capture de paquets radiodiffusés et multidiffusés, , puis pour le trafic envoyé ou reçu par l'ordinateur sur lequel CommView opère. Cependant, les plus modernes commutateurs (switches) supportent le "port miroir", lequel est une caractéristique qui vous permet de configurer le commutateur (switch) pour rediriger le trafic qui a cours sur certains ports ou tous les ports à un port de contrôle désigné sur le commutateur (switch). En utilisant cette caractéristique, vous serez capable de contrôler le segment entier du LAN. Veuillez s'il-vous-plaît vous référer à la documentation incluse avec votre commutateur (switch) pour connaître la disponibilité de cette caractéristique, ainsi que les instructions de configuration. Les manufacturiers de matériel de réseau nomment cette caractéristique différemment. Ci-dessous se trouve une courte liste de références de matériel par trois manufacturiers majeurs – Cisco, 3COM et Intel qui supportent le port miroir.

Manufacturier	Nom utilisé pour la caractéristique port miroir	Modèles de commutateurs avec support du port miroir
Cisco	Switched Port Analyzer (SPAN)	Cisco Catalyst 1900 Series Switches Cisco Catalyst 4500 Family Switches Cisco Catalyst 6000 Family Switches
3COM	Roving analysis port (RAP)	3Com SuperStack 3 Switch 4400
Intel	Port mirroring	Intel Express 460T Intel Express 480T

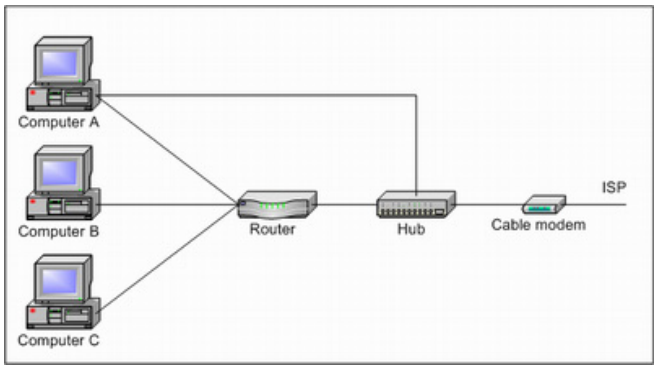
Q. Ok, je suis connecté sur un LAN au moyen d'un concentrateur multiport, mais je ne peux voir le trafic des autres machines encore, comme si c'était un commutateur. Pourquoi?
A. Il existe deux raisons possibles : Soit vous avez un concentrateur multiport qui est déjà libellé en tant que concentrateur multiport, mais qu'à l'intérieur se trouve un commutateur (quelques fournisseurs comme Linksys font de même), ou que vous avez un concentrateur multivitesse, dans lequel cas vous ne pouvez voir le trafic des stations opérant à une vitesse différente de celle de votre carte réseau (par exemple, si vous avez une carte réseau 10Mbit, vous ne pouvez voir le trafic généré par les cartes réseau 100 Mbit).

Q. J'ai un LAN local connecté à Internet par l'entremise d'un routeur Broadband, et je ne puis voir que mon propre trafic. Est-il possible de capturer le trafic des autres machines de mon LAN local ?
R. Oui. Une configuration de réseau local est illustrée ci-dessous :



Puisque votre routeur fonctionne en tant que commutateur, un ordinateur sur votre LAN ne peut voir que son propre trafic (et les diffusions des autres ordinateurs). Toutefois, vous pouvez installez un concentrateur entre le routeur et Internet. Ensuite, installez

le second NIC dans votre ordinateur, puis connectez ce NIC à ce concentrateur. Le second NIC n'a pas à être relié à aucun protocole ou à posséder d'adresse IP. Ce serait complètement passif, pous des fins de surveillance seulement. Vous pouvez ensuite utiliser CommView pour capturer les données du second NIC. Cette configuration est illustrée ci-dessous.



Assurez-vous d'installer un concentrateur réel, puisque certains concentrateurs ne sont qu'étiquetés en tant que concentrateurs, mais sont en fait des commutateurs (certains distributeurs comme Linksys le font). Procurez-vous un concentrateur miniature et bon marché. L'un de seconde main fera amplement l'affaire.

Q. Est-ce que CommView peut capturer des données à partir d'un adaptateur de réseau qui n'a pas d'adresse IP?
A. Oui. En fait, l'adaptateur de réseau n'a pas besoin d'être relié à TCP/IP ou à tout autre protocole. Dans une situation où vous tentez de trouver la problématique d'un réseau, il se peut qu'il soit nécessaire de brancher l'ordinateur qui opère CommView à un port ou àun concentrateur disponible. Dans de tels cas, vous n'avez pas besoin de deviner l'adresse IP disponible dans le segment LAN, tout ce dont vous avez besoin de faire est de délier l'adaptateur de réseau du TCP/IP et de commencer à capturer. Avec Windows 2000/XP/2003, ouvrez Control Panel => Network Connexions, cliquez le bouton droit de la souris sur l'icône de connexion, sélectionnez Properties, puis décochez les cases correspondant aux protocoles que vous ne voulez pas voir reliés au NIC. Avec Windows 9x Control Panel => Network, sélectionnez TCP/IP => Your NIC item, cliquez Remove, puis redémarrez la machine.

Q. J'ai lancé le programme et cliqué "Start Capture", mais aucun paquet n'est affiché. Pourquoi?
A. Il y a deux raisons possibles : Vous avez soit sélectionné un adaptateur de réseau inutilisé, ou fait une erreur lors de la configuration des règles de capture. Désactivez les règles et voyez ce qui se produit. Dans tous les cas, même lorsque les règles de capture sont activées, la barre de statut du programme devrait afficher le nombre total de paquets, il faudrait donc verifier ceci avant de paniquer.

Q. J'ai remarqué que les sommes de contrôle (checksums) IP/TCP/UDP des paquets entrants sont incorrectes. Pourquoi donc?
A. Les nouveaux adaptateurs de réseau Gigabit ont une caractéristique appelée TCP/UDP/IP "checksum offload", laquelle permet à l'adaptateur de réseau de calculer les sommes de contrôle (checksums) des paquets, tout en augmentant la performance du système en diminuant l'utilisation du CPU. Puisque CommView intercepte les paquets avant qu'ils n'atteignent l'adaptateur de réseau, la somme de contrôle apparaît incorrecte. Ceci est normal et la seule chose que cela puisse affecter est la reconstruction de sessions TCP, et seulement si vous avez modifié l'option par défaut "Ignore incorrect checksums" (consultez Configuration des options pour plus d'information).

Q. Est-ce que CommView peut d'exécuter sur des ordinateur multi-processeurs ?
A. Oui, il le peut.

Q. Ma connexion réseau est via un modem-câble/xDSL. Est-ce que CommView sera capable de contrôler le trafic dessus?
A. Si votre modem a une interface dual USB/Ethernet et que vous pouvez la connecter sur une carte Ethernet, CommView sera certainement capable de capturer le trafic sur celui-ci. S'il n'a qu'une interface USB, la meilleure chose à faire est de l'essayer.

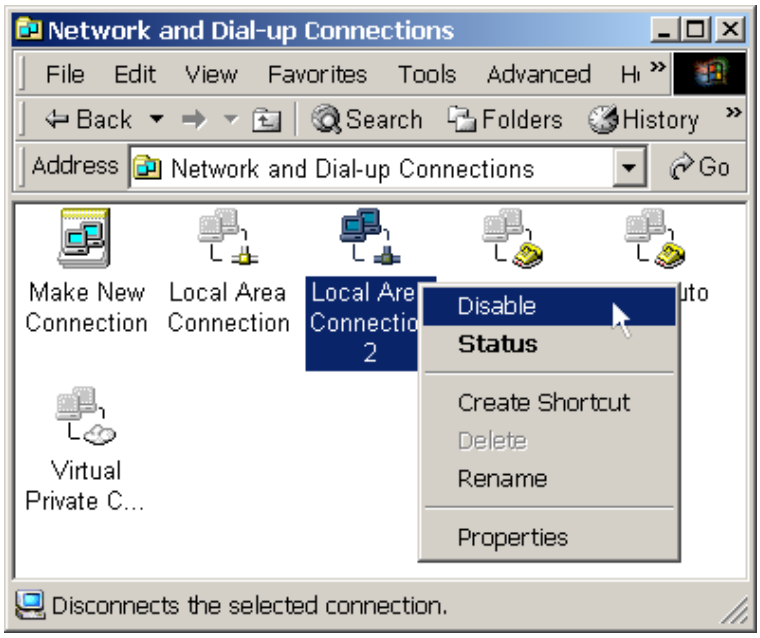
Q. Mon logiciel de pare-feu m'avertit que CommView "tente d'accéder à l'Internet". Je suis au courant que certains sites sont capables de pister les utilisateurs en collectionnant l'information envoyée par leur programme via Internet. Pourquoi est-ce que CommView "tente d'accéder à l'Internet"?
A. Ce qui alerte votre pare-feu est la tentative de convertir les adresses IP en noms d'hôtes. Puisque CommView doit contacter votre serveur DNS pour faire une requête DNS, ceci active inévitablement l'alarme. Vous pouvez désactiver cette caractéristique (Settings => Options => Disable DNS resolving), mais dans ce cas, l'onglet Dernières Connexions IP ne sera plus capable de afficher les noms d'hôtes. Les requêtes DNS sont les seuls types de connexions que CommView peut potentiellement effectuer. Il n'y a pas d'autres activités cachées. Nous ne vendons pas de logiciel d'espionnage.

Q. Sous Windows 2000/XP/2003, j'y suis souvent connecté comme utilisateur sans privilèges administratifs. Est-ce que je dois me déconnecter, puis me reconnecter comme administrateur pour être capable d'opérer CommView?
A. Non, vous pouvez ouvrir le fichier de CommView, cliquer avec le bouton droit de la souris sur le fichier CV.exe tout en appuyant sur la touche Shift, puis sélectionner "Run As" du menu contextuel (pop-up). Entrez le nom d'utilisateur et le mot de passe de l'administrateur dans la fenêtre contextuelle (pop-up), puis cliquez OK pour opérer le programme.

Q. Je possède Windows NT, et je vois plusieurs entrées "Remote Access WAN Wrapper" dans la liste d'adaptateurs. Lequel dois-je sélectionner pour que CommView capture mes paquets RAS?
A. Tout dépend de votre système. La chose la plus facile à faire est de les essayer un par un, et dans la plupart des cas, n'importe lequel d'entre eux va fonctionner. Avec un des adaptateurs Remote Access WAN Wrapper, vous pourriez faire face à un effet indésirable : CommView capture et déploie les paquets, mais les paquets ne sont pas délivrés à vos applications en réseau (par

exemple, le délai d'attente des connexions est échu, etc.). Si vous avez ce problème, arrêtez seulement de capturer et sélectionnez un différent Remote Access WAN Wrapper à partir de la liste.

Q. Je possède Windows 2000, et lorsque je désinstalle le programme, je reçois ce message : "CommView will now uninstall the drivers. Click "OK" to continue. This can take between 10 and 60 seconds." Mais alors, rien n'arrive!
A. Ceci peut se produire s'il y a des connexions actives en réseau lorsque vous désinstallez le programme. Vous devriez temporairement désactiver toutes les connexions actives tel que démontré ci-dessous :



Dès que la(les) connexion(s) est(sont) désactivée(s), CommView résumera le processus de désinstallation. Lorsque la désinstallation sera complétée, vous pourrez réactiver les connexions.

Q. Je possède Windows 2000 Terminal Server, et j'ai un problème pour lancer CommView via un Terminal Services client.
La seule limitation est qu'un périphérique peut être ouvert par un seul utilisateur au même moment. En d'autres termes, deux utilisateurs (locaux ou distants) ne peuvent capturer le trafic à partir d'un même périphérique en lançant deux instances de CommView sur le même serveur.

Q. CommView peut-il surveiller un périphérique réseau lorsqu'il tourne sous Microsoft Virtual PC ?
A. Oui. La seule limitation est que le mode passif (promiscuous) n'est pas disponible pour les interfaces virtuelles, donc vous serez limité à la capture de vos propres paquets et des paquets diffusés uniquement.

Q. Lorsque je contrôle ma connexion par modem d'accès commuté, je ne vois aucun paquet PPP durant l'installation de la session (CHAP, LCP, etc). Est-ce normal?
A. Désolé, les paquets PPP ne peuvent être capturés que sous Windows 95/98/NT/ME, CommView ne capture pas de tels paquets sous Windows 2000/XP/2003. Veuillez prendre note que tous les autres paquets PPP qui suivent le processus d'approbation initial sont capturés.

Q. Puis-je changer les cartes PC sur mon portatif pendant que CommView opère?
A. Non, il est plus sécuritaire de fermer CommView, ensuite changer ou brancher/débrancher votre carte, puis redémarrer le programme. La liste d'adaptateurs va être automatiquement mise à jour.

Q. Je suis sur un LAN avec un volume de trafic élevé, et j'ai remarqué que CommView augmente la charge du CPU et/ou devient moins réceptif. Que puis-je y faire?
A. La meilleure façon d'optimiser la performance du programme est d'utiliser des règles pour filtrer vers l'extérieur les paquets que vous n'avez pas besoin de contrôler. Par exemple, envoyer un fichier de 50 Meg entre deux machines sur votre LAN peut générer approximativement 40,000 paquets NetBIOS avec un taux de transfert de données de 1Mbytes par seconde, lequel peut être une charge lourde pour l'application. Mais normalement, vous n'avez pas besoin de visionner tous les paquets NetBIOS envoyés, vous pouvez donc configurer CommView pour capturer les paquets IP seulement. CommView a un système flexible de filtres, et vous pouvez configurer l'application pour afficher seulement les paquets dont vous avez réellement besoin. Si vous êtes interessé(e) dans les informations de statistiques seulement (ces diagrammes verts, graphiques circulaires, et tables d'hôtes), vous pouvez utiliser la commande de menu "Suspend packet output", qui vous permet d'avoir les données statistiques sans déploiement de paquet en temps réel. Aussi, consultez le chapitre Capture d'un trafic de grand volume pour plus d'informations.

Q. Quelques fois, lorsque je lance CommView, je vois l'icône hourglass, mais l'application ne démarre pas. Pourquoi?
A. Soyez certain que vous n'avez pas ouvert la fenêtre de Connexion Properties dans les connexions par modem d'accès commuté de réseau commuté. Vous ne devriez pas ouvrir cette fenêtre lorsque CommView démarre. Lorsque la fenêtre sera fermée, CommView continuera automatiquement à se charger.

Q. Existe-t-il des conflits connus avec tout autre logiciel?

A. Actuellement, nous connaissons des conflits avec les programmes suivants :

- SoftIce par Numega : Possibles pannes de système.
- PGPNet 7.0 par NAI : Il existe un conflit de logiciel de pilotage de bas niveau résultant en un Écran Bleu de la Mort sous Windows 2000 si PGPNet est relié à une connexion par modem d'accès commuté.
- Sygate Personal Firewall : Un conflit de pilote résultant en un Écran Bleu de la Mort sous Windows 2000/XP si vous tentez de surveiller l'adaptateur d'accès commuté et que vous utilisez CommView 3.3 ou antérieur. Si vous surveillez une carte Ethernet, vous n'êtes pas affecté. Ce problème a été résolu dans CommView 3.4.

Si vous croyez que vous avez découvert un conflit avec une application ci-dessus non mentionnée, nous apprécirions que vous nous en fassiez part.

Q. Dois-je être un professionnel pour utiliser ce programme?
A. Non. Nous espérons que même les utilisateurs inexpérimentés vont trouver ce programme utile. Vous n'avez pas besoin d'utiliser toutes ses caractéristiques. Par exemple, même les novices peuvent être interessés à avoir une image nette des connexions LAN à partir et venant de leur ordinateur ou trouver que ce programme installé hier est en fait un Trojan qui envoie vos mots de passe de connexion par modem d'accès commuté à une certaine adresse de courriel.

Q. Où puis-je trouver un bon FAQ sur la capture de paquets et d'analyse de protocoles?
A. Visitez ces sites :

Sniffing (network wiretap, sniffer) FAQ

Protocols.com

CommView Tutorial

Utilisation avancée

Capture d'un trafic de grand volume

Lorsque la capture de données d'un segment de réseau large et occupé est en cours, vous devriez garder en tête que procéder des milliers de paquets par seconde peut considérablement augmenter l'usage de votre CPU et rendre l'application moins réceptive. Le meilleur moyen d'optimiser la performance du programme est d'utiliser des règles pour filtrer vers l'extérieur les paquets que vous n'avez pas besoin de contrôler. Par exemple, envoyer un fichier de 50 Meg entre deux machines sur votre LAN peut générer approximativement 40,000 paquets NetBIOS, avec une vitesse de transfert de données de 1Mbytes par seconde, laquelle peut être une charge lourde pour l'application. Mais normalement, vous n'avez pas besoin de visionner chacun des paquets NetBIOS envoyés, et vous pouvez donc configurer CommView pour capturer les paquets IP seulement. CommView a un système de filtres flexible, et vous pouvez configurer l'application pour afficher seulement les paquets dont vous avez réellement besoin. Aussi, si vous n'êtes interessé(e) qu'en les informations statistiques (ces histogrammes verts, graphiques circulaires et tables d'hôtes), vous pouvez utiliser la commande de menu "Suspend packet output", laquelle vous permet d'obtenir les données statistiques sans déploiement de paquets en temps réel.

Les facteurs qui améliorent la performance du programme :

- Un CPU rapide (Pentium IV recommandé)
- Volume RAM (128 et plus recommandé)
- Un système d'exploitation construit sur la technologie NT (Windows 2000/XP/2003 recommandé)
- Utilisation de règles pour filtrer vers l'extérieur le trafic inutile

Travailler avec Plusieurs Instances

CommView peut capturer des paquets de plusieurs périphériques réseau simultanément. Cette option est activée en cochant la case **Permettre plusieurs instances de l'application** dans **Settings => Options => Divers**. Veuillez s'il-vous-plaît prendre note que vous ne pouvez pas ouvrir le même adaptateur dans deux différentes instances du programme. La même limitation s'applique au serveur terminal : deux utilisateurs (locaux ou à distance) ne peuvent capturer le trafic du même adaptateur en opérant sur deux instances de CommView sur le même serveur.

Opérer CommView en Mode Invisible

Il y a deux façons d'opérer CommView en processus caché :

1. Lancez CommView avec l'interrupteur "hidden", i.e. :

   CV.EXE hidden

2. Si CommView opère déjà, vous pouvez le masquer/voir en utilisant le "raccourci-clavier". Pour masquer l'application, pressez ALT+SHIFT+h. Pour voir l'application, pressez ALT+SHIFT+u.

Rappelez-vous que vous ne pouvez pas complètement masquer toute application dans Windows. Lorsque CommView opère en mode invisible, il n'est pas listé dans la liste de tâches (celle qui est invoquée en pressant ALT+CTRL+DEL) sous Windows 98/ME, mais on peut encore le voir en utilisant tout accessoire qui liste les processus en cours. Sous Windows NT/2000/XP/2003, cet accessoire fait partie de Task Manager.

Paramètres de lignes de commande

Vous pouvez utiliser les paramètres de lignes de commande pour exécuter les opérations suivantes lorsque le programme est lancé :

- Charger et activer une définition de règle à partir d'un fichier. Utilisez le paramètre "/ruleset" suivie par le nom du fichier et le chemin d'accès complet, par exemple :

  CV.EXE /ruleset "C:\Program Files\CommView\Rules\POP3Rules.rls"

  Si un nom de fichier ou son chemin d'accès contient des espaces, il doit être mis entre guillemets (" ").

- Ouvrir un adaptateur et commencer à capturer. Utilisez le paramètre "/adapter" suivie par le nom de l'adaptateur, par exemple :

  CV.EXE /adapter "Intel(R) PRO/1000 T Desktop Adapter"

  Le nom de l'adaptateur doit être mis en guillemets (" "). Puisque les noms d'adaptateur sont habituellement longs, vous pourriez vouloir copier ces derniers à partir de la boîte de sélection d'adaptateur du programme, au lieu de l'entrer manuellement. Pour copier le nom d'adaptateur, sélectionnez l'adaptateur dans la boîte de sélection d'adaptateur, puis appuyez sur Ctrl-C.

- Utiliser le dossier spécifié pour enregistrer les fichiers journaux. Utilisez le paramètre /logdir suivi du chemin complet du dossier, par exemple

  CV.EXE /logdir "C:\Program Files\CommView\Logs"

Vous pouvez utiliser tous ces paramètres simultanément.

Échanger des Données avec Votre Application

CommView propose une interface TCP/IP simple qui vous permet de traiter les paquets capturés avec votre propre application en temps réel. A partir de la version 5.0 vous pouvez aussi utiliser cette interface pour envoyer des paquets (de manière similaire à la fonctionnalité de Génération de paquets dans CommView).

Veuillez noter que le format des données a changé par rapport aux versions précédentes de CommView. Le paramètre TS a aussi été supprimé sachant que toutes les informations à propos d'un paquet, incluant l'horodatage, sont maintenant envoyées dans l'en-tête.

Comment ça fonctionne
CommView devrait être lancé avec un argument de ligne de commande spécial, « MIRROR », qui indique au programme de miroiter les paquets capturés vers une adresse IP et un port TCP de votre choix.

Exemples :
CV.EXE mirror:127.0.0.1:5555 // miroite les paquets à l'adresse de retour, TCP port 5555
CV.EXE mirror:192.169.0.2:10200 // miroite les paquets à 192.169.0.2, TCP port 10200

Lorsque CommView est lancé avec un commutateur (switch) comme celui-ci, il essaie de se connecter à une session TCP, en se branchant à une adresse spécifiée et un nombre de port. Ceci veut dire que vous devriez déjà avoir votre application lancée et en train d'écouter le port spécifié. Si CommView ne peut établir une connexion, il continuera d'essayer de se connecter toutes les 15 secondes. La même chose se produit lorsqu'une connexion est interrompue : CommView tentera de se reconnecter toutes les 15 secondes. Si la connexion est établie avec succès, CommView envoie les paquets qu'il capture à l'adresse IP spécifiée dès qu'ils arrivent, en temps réel.

Format des Données

Les données sont transmises dans le format NCF. Veuillez vous référer au chapitre Format des Fichiers Journaux de CommView pour une description de ce format.

Envoyer des paquets

Les paquets peuvent non seulement être reçus par votre application, mais aussi envoyés comme si vous utilisiez le Générateur de paquets. Les données peuvent être envoyées à CommView en utilisant la même connexion TCP à partir de laquelle vous recevez les données. Le format des données est simple: vous devez envoyer la taille du paquet (un entier non-signé sur deux octets au format little-endian) suivie par le paquet lui-même. Si le périphérique n'est pas ouvert ou ne supporte pas l'injection de paquet, le paquet sera écarté de manière transparente.

Projets Échantillons
Deux applications simples de démonstration, qui écoutent les connexions entrantes, extraient les paquets du flux, et affichent les données brut, sont disponibles.

- http://www.tamos.com/products/commview/samp_mirr_c5.zip. Projet Visual Studio avec le code source C++.
- http://www.tamos.com/products/commview/samp_mirr_d5.zip. Projet Delphi avec le code source en Pascal. Si vous voulez compiler ce projet, vous aurez besoin de la fameuse suite de composants ICS de François Piette disponible à http://www.overbyte.be.

Bande Passante (Bandwidth)
Lorsque vous miroitez des données d'un ordinateur à distance, soyez certain(e) que que le lien entre CommView et l'ordinateur sur lequel les données sont miroitées est assez rapide pour transférer toutes les données capturées. 500 Kbytes/sec, et que votre lien ne peut traiter que 50 Kbytes/sec, vous allez inévitablement avoir des "embouteillages de trafic", ce qui pourrait résulter en des problèmes variés (par exemple, Winsock peut seulement arrêter l'envoi de données sous certaines versions Windows). Si vous recherchez une solution plus flexible qui incluerait des caractéristiques de mémoire tampon intelligente et de contrôle à distance, considérez l'utilisation de CommView Remote Agent.

Décodage personnalisé

CommView vous permet d'utiliser deux types de vos propres décodeurs personnalisés.

Décodeur simple

Si vous implémentez ce type de décodeur, les données résultantes de votre décodeur seront affichées dans la colonne supplémentaire de l'onglet **Paquets**. Votre décodeur doit être un fichier DLL de 32 bits nommé << Custom.dll >> exportant la seule procédure nommée << Decode >>. Le prototype de cette procédure est montrée ci-dessous dans les langages C et Pascal :

```
extern "C" {
  void __stdcall Decode(unsigned char *PacketData, int PacketLen, char *Buffer, int BufferLen);
}

procedure Decode (PacketData: PChar; PacketLen: integer; Buffer: PChar; BufferLen: integer); stdcall;
```

La DLL doit être située dans le dossier d'application de CommView. Lorsque vous lancez CommView, ce dernier recherche pour << Custom.dll >> dans le dossier de l'application et le charge dans sa mémoire. Si le point d'entrée de << Decode >> est trouvé, CommView ajoute une nouvelle colonne nommée << Personnalisé >> à la liste de paquets.

Lorsqu'un nouveau paquet est capturé et est sur le point d'être affiché, CommView appelle la procédure << Decode >> et passe le contenu du paquet à la DLL. La procédure << Decode >> doit traiter les données du paquet et copier les résultats dans la mémoire tampon spécifiée. Le premier argument est le pointeur aux données du paquet, le second argument est la longueur des données, le troisième argument est le pointeur à la mémoire tampon où les résultats du décodage doivent être copiés et le quatrième argument est la taille de la mémoire tampon (actuellement toujours 1024 octets). La mémoire tampon est allouée et libérée par CommView, alors ne tentez pas de la réallouer ou de la libérer. Les résultats que vous avez copiés dans la mémoire tampon seront affichés sous forme de chaîne dans la colonne << Personnalisé >>.

Votre procédure doit être suffisamment rapide pour traiter des milliers de paquets par seconde ; autrement, elle pourrait ralentir l'application. N'oubliez pas d'utiliser la convention d'attribution de noms STDCALL.

Deux démos DLL sont disponibles. Elles démontrent une opération fort simple : les données résultantes de la fonction « Decode » sont le code hex du dernier octet du paquet. Votre propre décodeur peut être aussi complexe que désiré.

- http://www.tamos.com/products/commview/cust_decoder_c.zip. Projet Visual Studio avec code source C++.
- http://www.tamos.com/products/commview/cust_decoder_d.zip. Projet Delphi avec code source en Pascal.

Décodeur complexe

Si vous implémentez ce type de décodeur, les données résultantes de votre décodeur seront affichées en tant qu'éléments supplémentaires dans l'arborescence du décodeur de paquets. Pour des informations à propos de ce décodeur, veuillez télécharger le fichier suivant :

http://www.tamos.com/products/commview/complex_decoder_c5.zip

Ce type de décodeur ne peut être écrit qu'au moyen de Microsoft Visual C++, puisqu'il est créé avec des classes C++.

Support technique

Un support technique relatif aux décodeurs est offert dans la « meilleure mesure ». Nous pourrions ne pas être en mesure de répondre à vos questions connexes à la programmation.

Format des fichiers journaux de CommView

CommView et CommView pour WiFi utilisent le format de données décrit ci-dessous pour écrire les paquets capturés dans les fichiers .NCF. C'est un format ouvert que vous pouvez utiliser aussi bien pour traiter les fichiers journaux générés par CommView dans votre application, que pour échanger des données directement avec votre application (cette méthode est décrite dans le fichier d'aide).

Les paquets sont enregistrés de manière consécutive. Une en-tête de 24 octets, dont la structure est donnée ci-dessous, précède le corps de chaque paquet. Tous les champs de l'en-tête dont la taille excède 1 octet sont au format little-endian.

<table>
<tr><th>Nom du champ</th><th>Taille (octets)</th><th>Description</th></tr>
<tr><td>Taille des données</td><td>2</td><td>La taille du corps du paquet qui suit l'en-tête</td></tr>
<tr><td>Taille des donnée source</td><td>2</td><td>La taille originale du corps du paquet qui suit l'en-tête (sans compression). Si aucune compression n'est utilisée, la valeur de ce champ est égale à la valeur du champ précédent.</td></tr>
<tr><td>Version</td><td>1</td><td>Version du format du paquet (0 pour l'implementation actuelle)</td></tr>
<tr><td>Année</td><td>2</td><td>Date du paquet (année)</td></tr>
<tr><td>Mois</td><td>1</td><td>Date du paquet (mois)</td></tr>
<tr><td>Jour</td><td>1</td><td>Date du paquet (jour)</td></tr>
<tr><td>Heures</td><td>1</td><td>Heure du Paquet (heures)</td></tr>
<tr><td>Minutes</td><td>1</td><td>Heure du Paquet (minutes)</td></tr>
<tr><td>Secondes</td><td>1</td><td>Heure du Paquet (secondes)</td></tr>
<tr><td>Microsecondes</td><td>4</td><td>Heure du Paquet (microsecondes)</td></tr>
<tr><td>Drapeaux</td><td>1</td><td>Bits des drapeaux:
<table>
<tr><td>Support</td><td>0...3</td><td>Type de support pour le paquet (0 - Ethernet, 1 - WiFi, 2 - Token Ring)</td></tr>
<tr><td>Décrypté</td><td>4</td><td>Le paquet a été décrypté
(applicable uniquement aux paquets WiFi)</td></tr>
<tr><td>Cassé</td><td>5</td><td>Le paquet était corrompu, c'est à dire avait une valeur CRC non valide (applicable uniquement aux paquets WiFi)</td></tr>
<tr><td>Compressé</td><td>6</td><td>Le paquet est emmagasiné sous une forme compressée</td></tr>
<tr><td>Reservé</td><td>7</td><td>Reservé</td></tr>
</table></td></tr>
<tr><td>Niveau du Signal</td><td>1</td><td>Niveau du Signal en pourcentage
(applicable uniquement aux paquets WiFi)</td></tr>
<tr><td>Taux</td><td>1</td><td>Taux de transmission des données en Mbps (megabits par seconde) multiplié par 2
(applicable uniquement aux paquets WiFi)</td></tr>
<tr><td>Bande</td><td>1</td><td>Bande de transmission. 0x01 pour 802.11a, 0x02 pour 802.11b, 0x04 pour 802.11g, 0x08 pour 802.11a-turbo, 0x10 pour 802.11 SuperG.
(applicable uniquement aux paquets WiFi)</td></tr>
<tr><td>Canal</td><td>1</td><td>Numéro du canal
(applicable uniquement aux paquets WiFi)</td></tr>
<tr><td>Direction</td><td>1</td><td>Direction du paquet. 0x00 pour les paquets en transit, 0x01 pour entrant, 0x02 pour sortant
(non applicable aux paquets WiFi)</td></tr>
<tr><td>Reservé</td><td>2</td><td>Reservé</td></tr>
<tr><td>Données</td><td>...</td><td>Corps du paquet (non modifié, tel que transmis sur le support). Si le drapeau de compression est positionné, les données sont compressées en utilisant la librarie gratuite Zlib 1.1.4. La taille de ce champ est enregistrée dans le champ Taille des données.</td></tr>
</table>

La taille totale de l'en-tête est de 24 octets.
Si les paquets sont emmagasinés dans une forme compressée, le champ « Taille des données » contient la taille après compression, alors que le champ « Taille des données source » contient la taille originale des données. Si un paquet n'est pas compressé, les deux champs contiennent la même valeur.

Information

Comment se Procurer CommView

Ce programme est une version d'évaluation de 30 jours. Ci-dessous se trouvent les prix pour le programme entièrement fonctionnel et sans restriction :

Type de Licence	**Prix, US$**
Licence Entreprise de CommView 1 utilisateur (à usage professionnel, commercial)	**499.00**
Licence Personnelle de CommView 1 utilisateur (à usage privé, non commercial)	**99.00**

- La licence la moins dispendieuse, **Licence Personnelle**, vous donne le droit d'utiliser le programme à la maison pour des fins non commerciales. Si vous utilisez CommView pour contrôler votre réseau maison, le nombre maximum d'hôtes dans votre LAN que cette licence vous permet ne peut excéder cinq.

- La licence la plus dispendieuse, **Licence Entreprise**, vous donne droit d'utiliser le programme n'importe où pour des fins commerciales ou non commerciales.

Une copie licenciée de CommView peut être utilisée par une seule personne qui utilise le logiciel personnellement sur un ou plusieurs ordinateurs ou le logiciel peut être installé sur une seule station de travail utilisée non simultanément par plus d'une personne, mais pas les deux. Visitez notre site web pour les prix sur les licences pour multiples usagers si vous avez besoin de faire l'achat de ce produit pour plus d'un utilisateur.

En tant qu'utilisateur enregistré, vous recevrez :

- Une copie du logiciel entièrement fonctionnelle et sans restriction
- Des mises à jour gratuites qui seront lancées durant l'année suivant la date d'achat
- De l'information sur les mises à jour et les nouveau produits
- Un support technique gratuit

Nous acceptons les commandes par cartes de crédit, les commandes par téléphone et télécopieur, les chèques, les commandes par mandat ou ordre et les transferts de fonds. Les prix, les termes et les conditions sont sujets à changement sans aucune forme de préavis : veuillez s'il-vous-plaît visiter notre site web pour les dernières offres de produits et les derniers prix.

http://www.tamos.com/order/

Contactez-nous

Web

http://www.tamos.com

E-mail

sales@tamos.com (Questions reliées aux ventes)
support@tamos.com (Toutes les autres questions)

Courrier postal et Télécopieur

Adresse postale :

PO Box 1385
Christchurch 8015
New Zealand

Fax : +64 3 359 0392 (Nouvelle-Zélande)
Fax : +1 917 591-6567 (États-Unis)

Autres Produits par TamoSoft

SmartWhois

SmartWhois est un accessoire utilitaire pour obtenir de l'information sur toute adresse IP, nom d'hôte ou de domaine dans le monde entier. Contrairement à d'autres utilitaires whois standards, il délivre automatiquement l'information associée à une adresse IP ou à un domaine, peu importe où il est géographiquement enregistré. En seulement quelques secondes, vous obtenez toute l'information que vous désirez connaître sur un utilisateur : domaine, nom de réseau, pays, état ou province et ville. Même si l'adresse IP ne peut pas être convertie en nom d'hôte, SmartWhois n'échouera pas!

Plus d'informations

Essential NetTools

Essential NetTools est un kit d'outils de réseau utile pour diagnostiquer les réseaux et contrôler les connexions réseau de votre ordinateur. C'est un véritable couteau d'armée suisse pour toute personne intéressée dans un kit d'outils de réseau puissant pour usage quotidien. Le programme inclut un utilitaire NetStat qui affiche les connexions réseau de votre ordinateur et ouvre les ports et les cartes à cette propre application. Il contient aussi un scanner NetBIOS rapide, un outil d'audition NetBIOS pour vérifier la sécurité LAN, ainsi qu'un contrôle de connexions externes aux ressources partagées de votre ordinateur, puis un contrôle de processus qui déploie l'information sur tous les programmes et services opérant sur votre ordinateur. D'autres outils utiles sont aussi inclus, tells que Ping, TraceRoute, et NSLookup. Des accessoires additionnels incluent un générateur de rapports en HTML, en texte, et en format délimité par des virgules et une interface conventionnelle. Le programme est un remplacement puissant et facile à utiliser pour les utilitaires Windows tels que nbtstat, netstat, et NetWatcher. Il incorpore plusieurs accessoires avancés que les outils standards Windows ne peuvent offrir.

Plus d'informations

DigiSecret

DigiSecret est une application sécuritaire et facile à utiliser pour l'encryptage et la partage de fichiers. Elle utilise des algorithmes d'encryptage forts et prouvés pour créer des archives encryptées, des fichiers auto-extractibles EXE, et partager des fichiers avec vos associés et vos amis. DigiSecret inclut aussi un compresseur de fichier puissant et intelligent; vous n'avez maintenant plus besoin de fichiers .zip lorsque vous pouvez avoir encrypté ou compressé les fichiers DigiSecret. Le programme est integré avec le Shell de Windows, et vous pouvez performer des opérations sur des fichiers en cliquant le bouton droit de la souris sur ceux-ci. Le programme supporte aussi entièrement les opérations de glisser-déposer.

Plus d'informations

CommTraffic

CommTraffic est un utilitaire réseau pour la cueillette, le traitement et l'affichage des statistiques de trafic et d'utilisation réseau, y compris des réseaux LAN et par accès commuté. Il affiche les statistiques de trafic et d'utilisation réseau de chaque ordinateur du segment. Le logiciel présente une interface très attrayante et personnalisable, ainsi qu'une icône de menu optionnelle apparaissant dans la zone de notification système, laquelle affiche les statistiques réseau générales. Vous pouvez par ailleurs l'utiliser pour générer des rapports qui reflètent le volume du trafic réseau et les dépenses reliées à la connexion Internet (si présente). CommTraffic prend virtuellement en charge tout plan de tarifs que votre ISP pourrait utiliser, comme celui basé sur le temps de connexion, le volume du trafic, l'heure du jour, et d'autres mesures. Vous pouvez définir des alarmes qui vous indiqueront lorsqu'un certain critère (par exemple, le volume du trafic, les dépenses) a été atteint. Un assistant de configuration vous guidera à travers l'installation et détectera automatiquement les paramètres de votre réseau ou connexion.

Plus d'informations