DrayTek

Syslog, Debug & Wireshark traces

Inhoudsopgave

Logging voor Support

Wanneer er problemen zijn met bepaalde functies van een DrayTek product is het handig om te achterhalen waardoor deze problemen worden veroorzaakt. Voor probleem-analyse is verstandig om debug/log-informatie te achterhalen zodat dit verzamelt kan worden.

Middels onderstaande mogelijkheden kan logging worden verkregen:
- Syslog
- Telnet / Web Console
- Wireshark

Syslog

Syslog is een feature waarmee de router activiteit kan worden bijgehouden. Syslog wordt gebruikt om configuratie instellingen van de router te controleren, zoals Firewall en VPN log gegevens. Tevens is Syslog een goed hulpmiddel bij het oplossen van problemen. De Syslog tool van DrayTek is gratis te downloaden op onze website. Deze tool is alleen bruikbaar op Windows systemen.

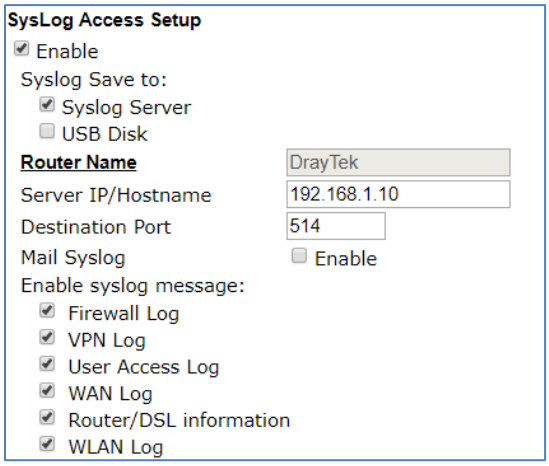
Welke Syslog mogelijkheden hebt u?

Syslog kunt u op 3 manieren gebruiken:

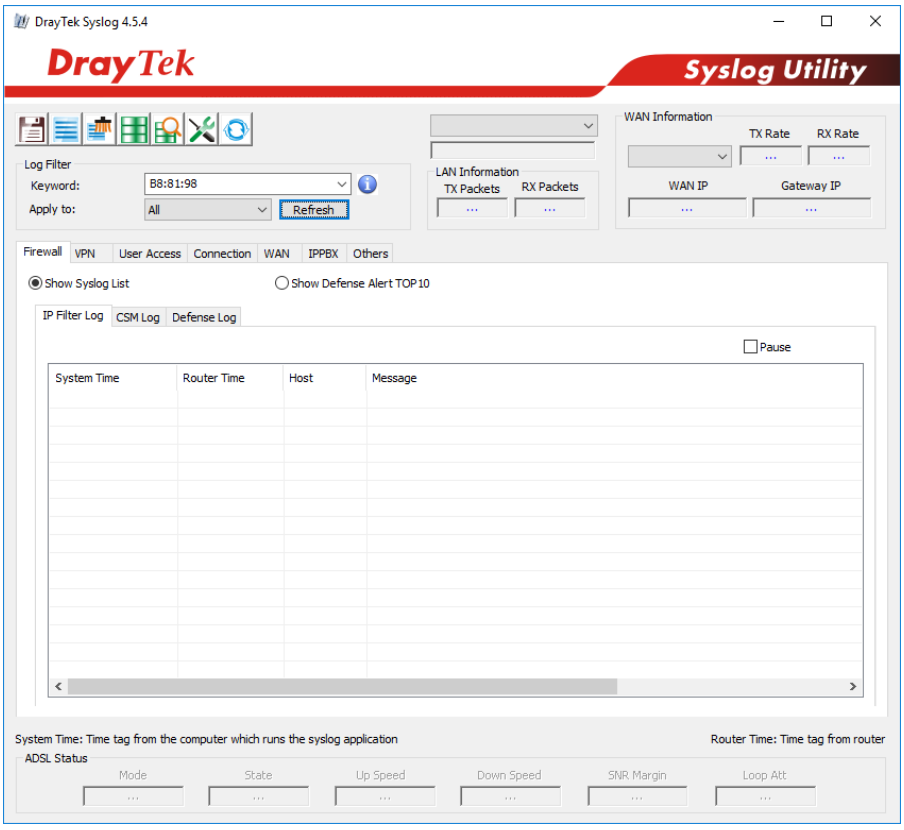
1. Syslog wegschrijven naar een IP-adres
2. Syslog wegschrijven naar een USB stick welke is aangesloten op de USB poort van de DrayTek.
3. Syslog live bekijken in de Web User Interface van de DrayTek.

Syslog wegschrijven naar een IP-adres

Ga in het hoofdmenu van de DrayTek naar 'System Maintenance >> Syslog / Mail Alert'. Selecteer onder Syslog Access Setup de optie **Enable**. Vul bij **Server IP Address** het IP-adres in van de PC/laptop waarop u Syslog wil gebruiken. Vul bij **Destination Port** het poortnummer in welke u voor Syslog wilt gebruiken. Standaard is dit poort **514**.



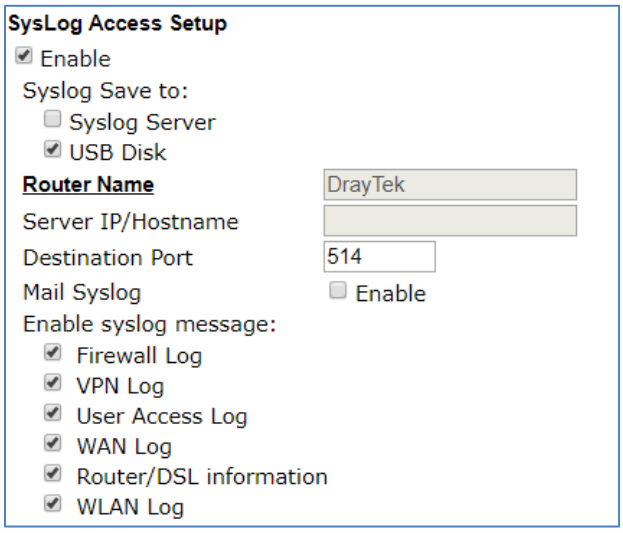
Belangrijk: *De standaard Windows Firewall blokkeert dit type verkeer, schakel voordat u gebruik gaat maken van de Syslog Utility de firewall daarom tijdelijk uit.*



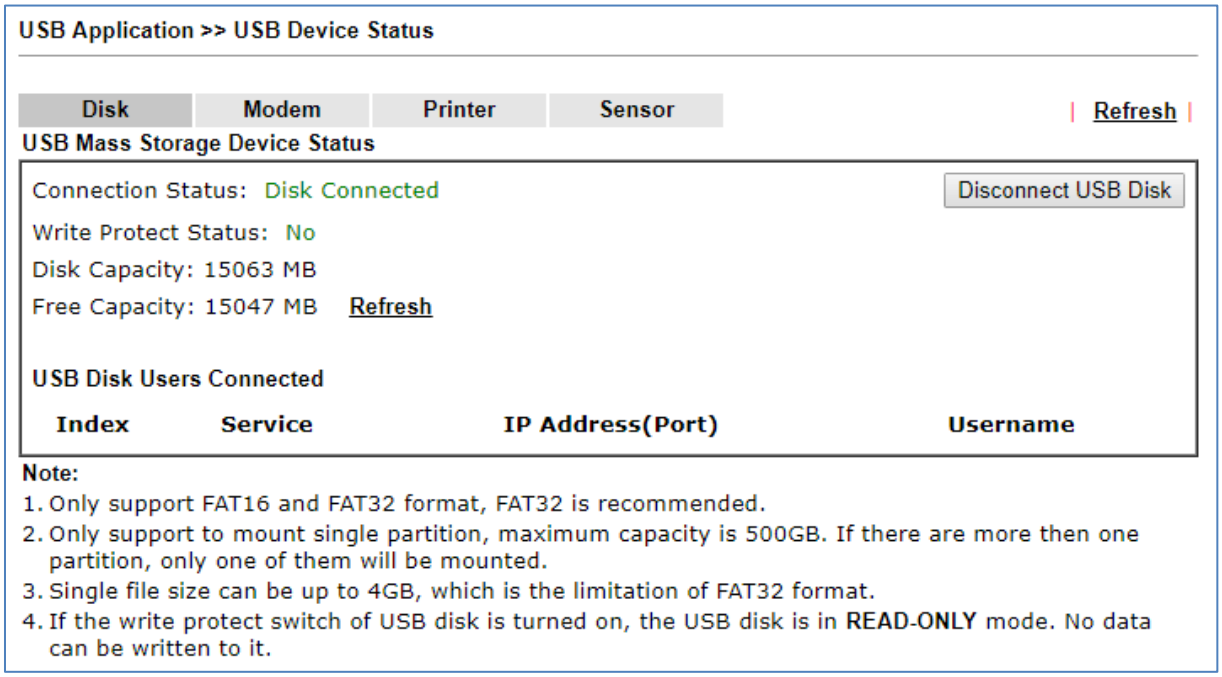
Syslog wegschrijven naar een USB stick

Door een vinkje te plaatsen bij USB Disk zorgt u ervoor dat de DrayTek de Syslog informatie opslaat op de aangesloten USB stick.

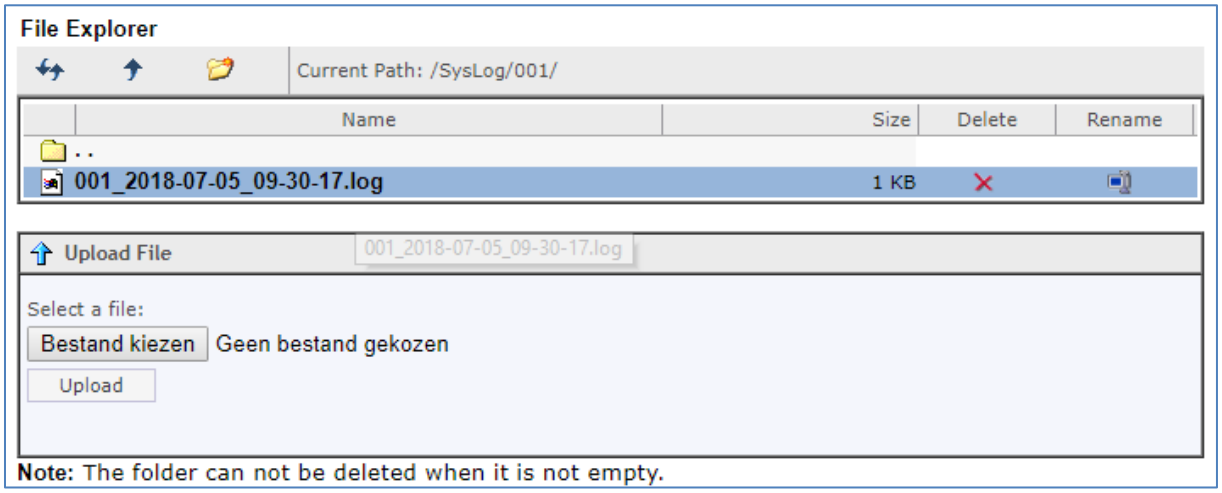
Belangrijk: Alleen bestandssysteem FAT16 & FAT32 worden ondersteund, het is dus niet mogelijk een USB stick met bestandssysteem NTFS te gebruiken.



Bij USB Application >> USB Device Status kunt u terug vinden of de aangesloten USB stick door de DrayTek wordt herkent.

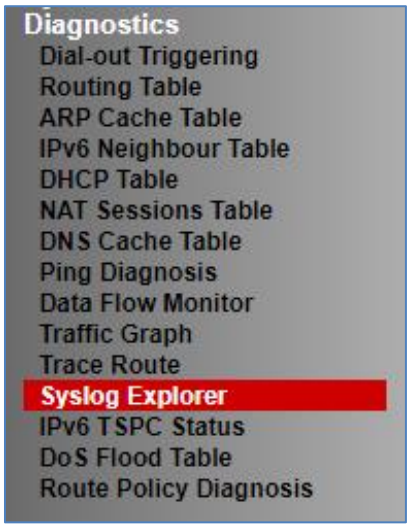


De DrayTek zal een directory aanmaken op de USB stick, in deze directory kunt u de Syslog bestanden terug vinden. Deze Syslog bestanden kunt u downloaden door naar USB Application >> File Explorer te gaan.

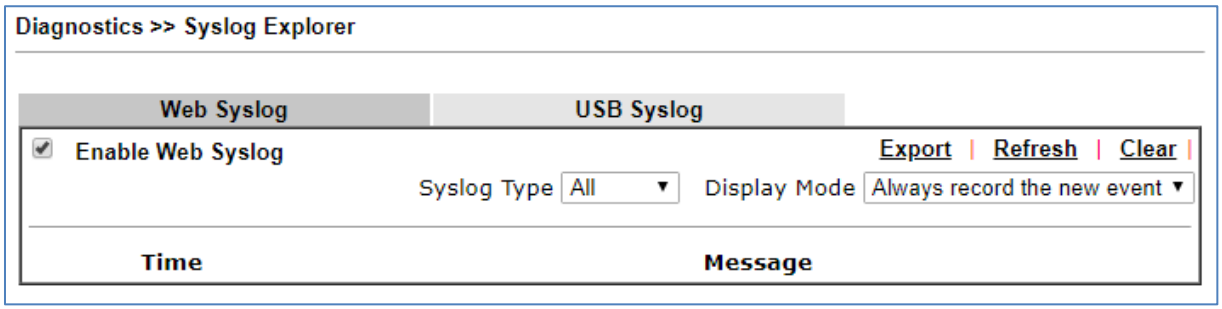


Syslog live bekijken

Syslog kun je tevens live uitlezen bij Diagnostics >> Syslog Explorer.



Door Syslog in te schakelen kunt u de log informatie live uitlezen, deze informatie kunt u eventueel exporteren. Daarnaast hebt u de mogelijkheid om het Type Syslog aan te passen.

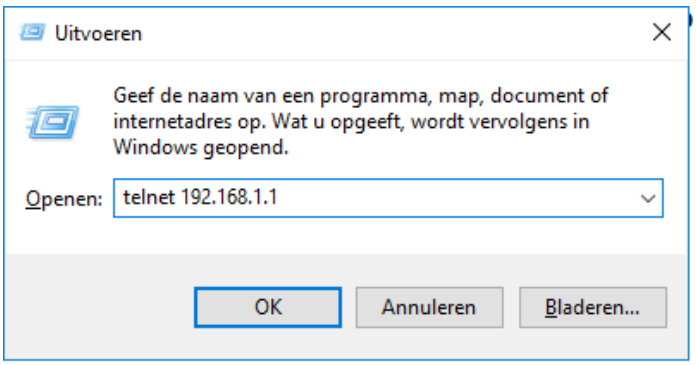


Telnet/Web Console

De meeste DrayTek producten hebben naast hun grafische interface (WUI) ook een Command Line interface.

Verbinding maken d.m.v. Telnet
Klik met uw rechtermuisknop op de Windows Startknop en kies vervolgens voor **Uitvoeren**.

In het scherm dat hierdoor verschijnt typt u achter Openen: '**telnet 192.168.1.1**'. Hierbij is het IP-adres het adres van uw router(in ons voorbeeld 192.168.1.1). Klik vervolgens op **OK**.



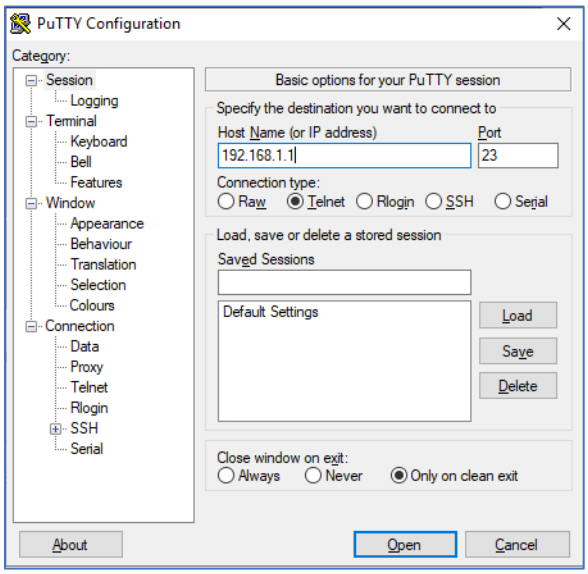
U krijgt vervolgens een login scherm te zien waarin u op basis van de admin credentials van de DrayTek kunt inloggen.

Als u succesvol bent ingelogd krijgt een prompt > te zien. Zoals op onderstaande afbeelding te zien is.

Met behulp van het commando "**?**" kunt u zien welke commando's beschikbaar zijn. Op basis van de commando's die op pagina 10 staan kunt u bepaalde logging uit de DrayTek halen. Deze informatie kan handig zijn indien u tegen bepaalde problemen aanloopt.

Belangrijk

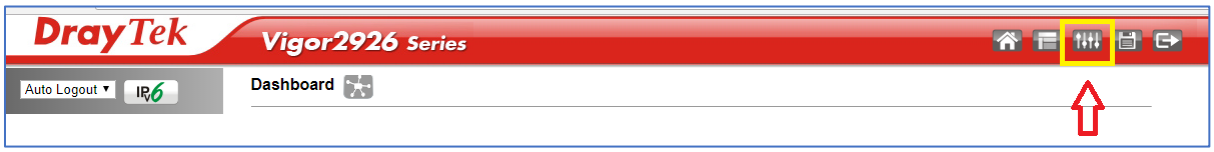
Wanneer u geen Telnet verbinding kunt maken kunt u ervoor kiezen om gebruik te maken van een software programma genaamd ‘Putty’. Deze opensource software kunt u gratis downloaden op de volgende URL: https://www.putty.org/



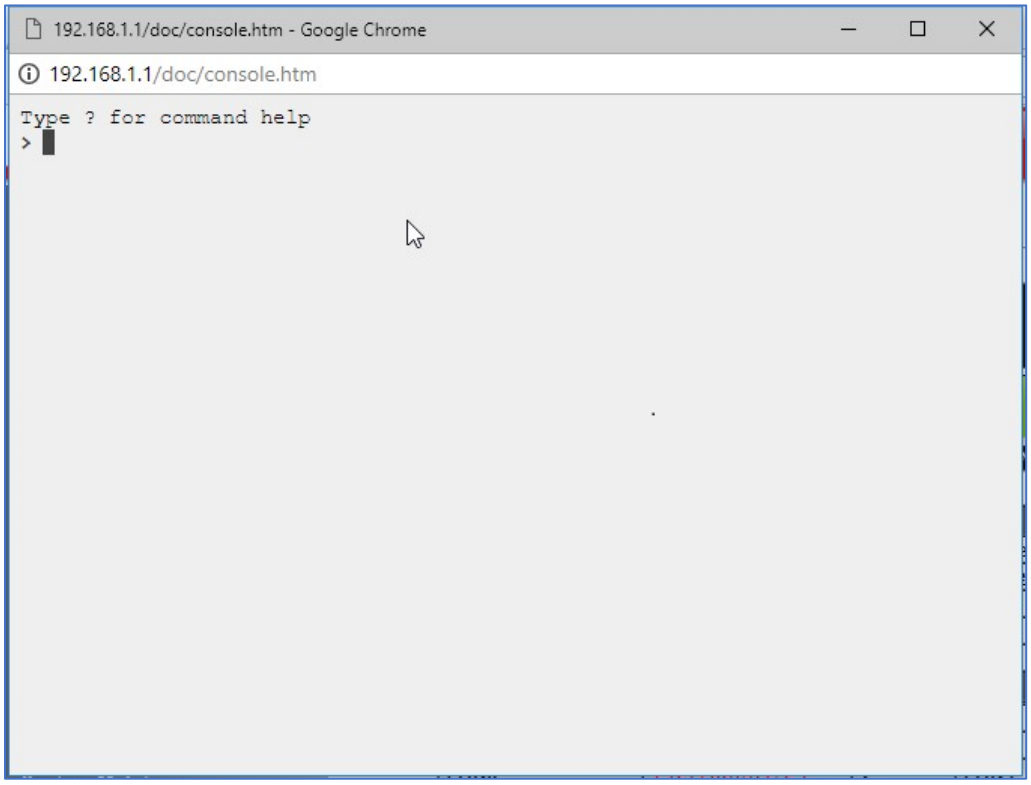
Web Console

De meeste Draytek modem/routers ondersteunen de **Web Console** feature**.** Dit is een Telnet functie die in de WUI (webpagina) van de DrayTek zit. Op die manier kunt u rechtstreeks vanuit de Web User interface een Telnet verbinding opzetten met de DrayTek.

De Web Console vindt u rechtsbovenin wanneer u ingelogd bent in de Web User Interface.



Wanneer u deze optie aanklikt zal er een popup scherm worden geopend.



In de Webconsole van de DrayTek kunnen niet alle commando's worden uitgevoerd. Commando's die veel informatie opvragen kunnen niet via de Webconsole worden uitgevoerd, hiervoor adviseren wij gebruik te maken van de telnet verbinding of Putty.

Commando's die nuttig voor support zijn:

>sys ver dbg	**(crashlog)**
>vdsl status	**(informatie over de vdsl verbinding)**
>adsl status	**(informatie over de adsl verbinding)**
>voip debug show	**(log voor de VoIP op de V modellen)**

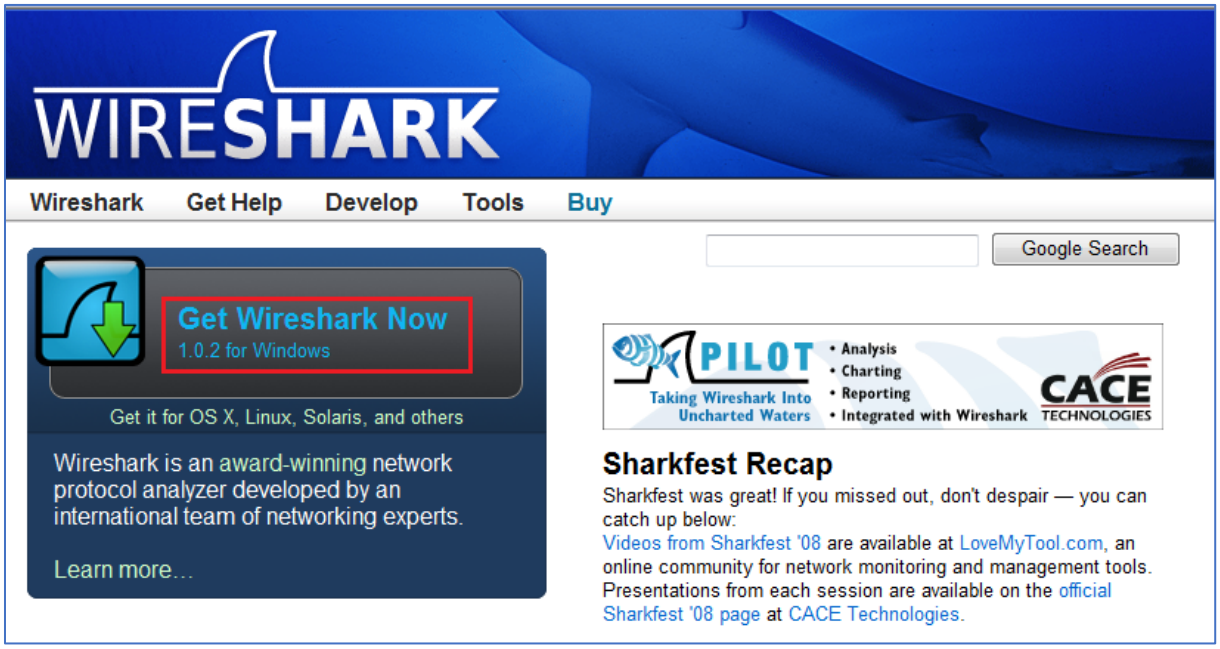
Wireshark

Het computerprogramma **Wireshark** is een **'packet sniffer'** en **'protocol analyzer'**, een programma dat gebruikt wordt om gegevens op een computernetwerk op te vangen en te analyseren. **Wireshark** is de opvolger van **Ethereal**.

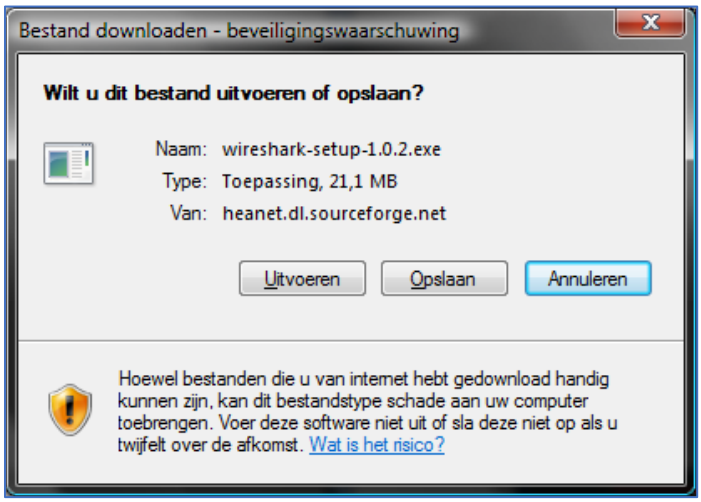
Met Wireshark kan de gebruiker zien welke data over het netwerk wordt verstuurd door de netwerkkaart in 'promiscuos mode' te zetten. **Wireshark** beeldt niet zomaar het netwerkverkeer af, maar begrijpt de structuur van de talrijke netwerkprotocols. Op deze manier kan de software de verschillende protocols weergeven en de inhoud van elk veld tonen.

De interface van **Wireshark** toont een lijst van **'gevangen'** pakketten, evenals de inhoud van het geselecteerde pakket. Handig is dat u met regels bepaalde pakketten een andere kleur kunt geven of met filters de lijst opschoont. Uiteraard kunt u de analyse beperken tot bepaalde protocollen. **Wireshark** beschikt over verschillende exportmogelijkheden: tekst, PostScript of XML.

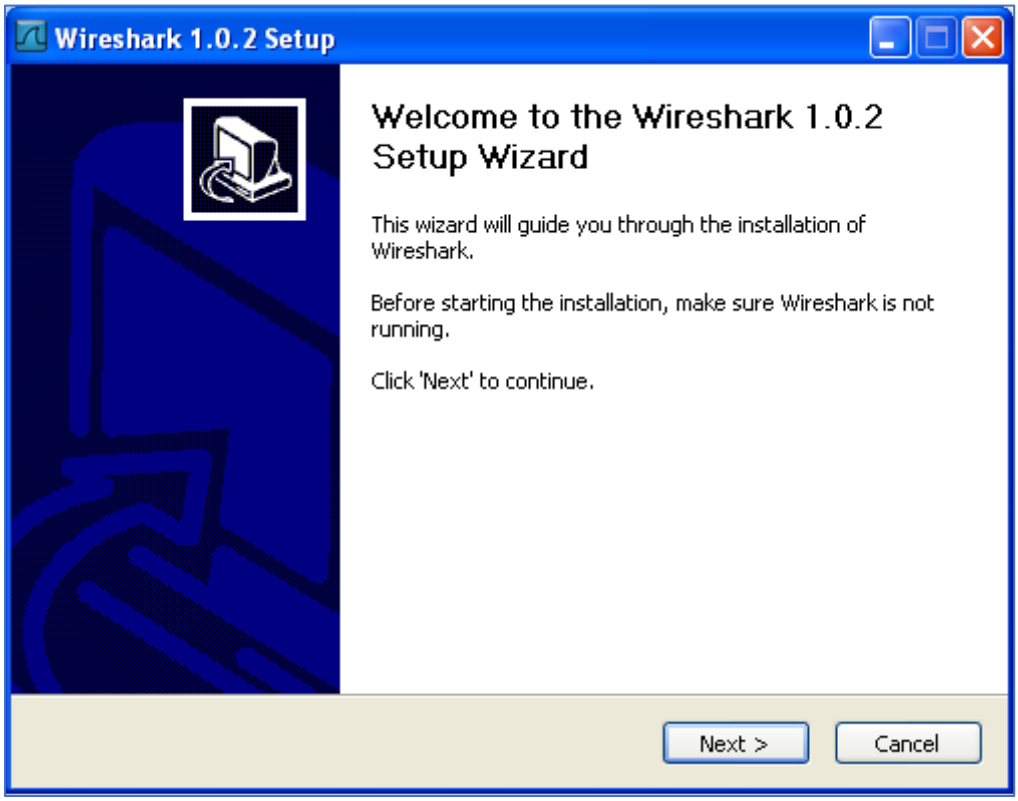
Belangrijk:
Om een Wireshark Trace te kunnen maken kunt u het beste gebruik maken van de LAN Port Mirror. Dit is een feature in de DrayTek die u in kunt schakelen. Op pagina 15 kunt u meer informatie vinden over het inschakelen van LAN Port Mirror.



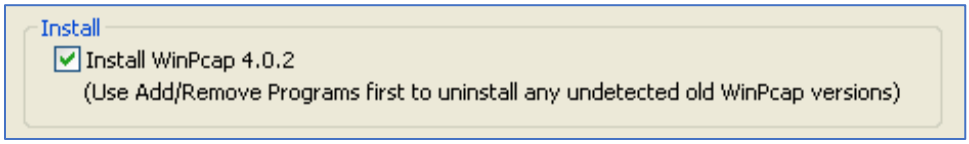
Wireshark is gratis te downloaden op www.wireshark.org. Wanneer u naar deze site gaat kunt u op **'Get Wireshark Now'** klikken, let er wel op dat dit alleen voor Windows gebruikers is. Wanneer u een ander besturingssysteem gebruikt kunt u op **'Get it for OS X, Linux, Solaris, and others'** klikken.



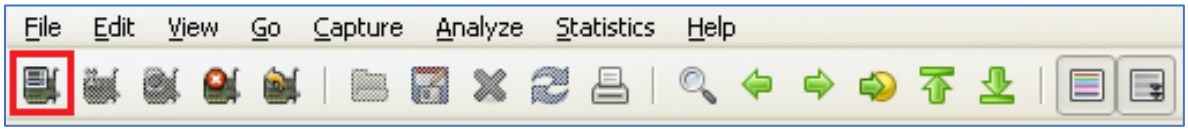
Vervolgens doorloopt u de Install Wizard van **Wireshark**. Hierbij kunt u nog een aantal dingen aanpassen.



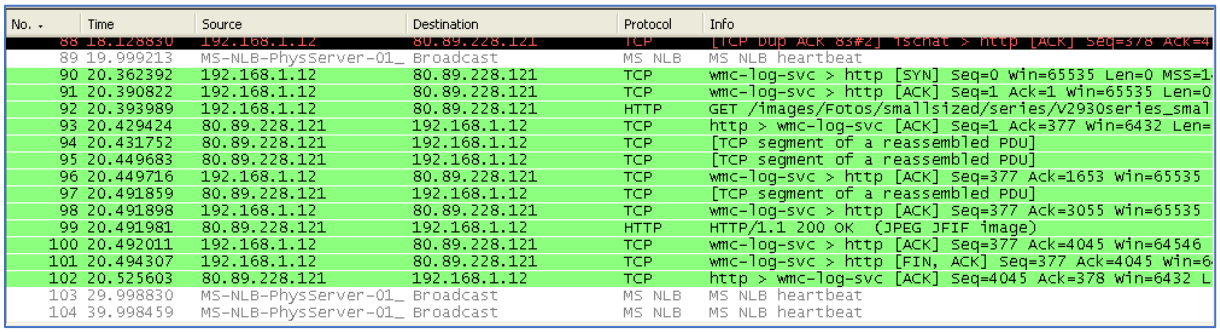
Tijdens de installatie wordt er gevraagd of u **WinPCap** wilt installeren, dit is noodzakelijk omdat **Wireshark** dit programma nodig heeft. **WinPCap** analyseert het gegevensverkeer onder netapparaten met de reeks geïntegreerde uitleenverzamelingen in **WinPCap**, een klein programma waarvan de inhoud door andere toepassingen wordt vereist om een perfecte functionering te krijgen.



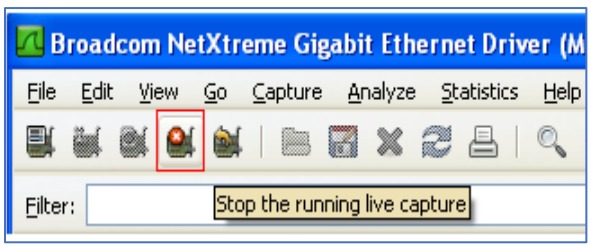
Na het installeren van beide programma's kunt u **Wireshark** gaan gebruiken. Na het openen van **Wireshark** krijgt u een leeg scherm te zien met een aantal menu opties. Om een capture te starten klikt u op het meest linker icoontje, onder de Filter dropdown list.



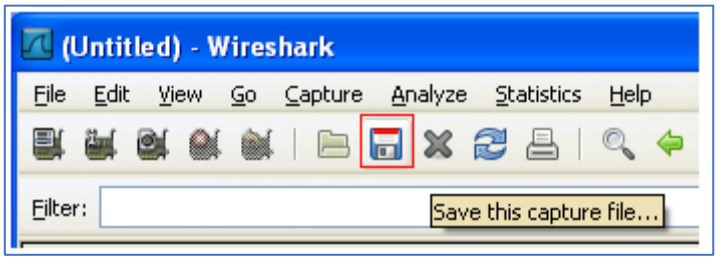
Vervolgens kunt u aangeven van welke interface u captures wilt maken, tevens heeft u hier de mogelijkheid om enkele **Details** of **Options** te bekijken. Klik op **Start** om de capture te starten.



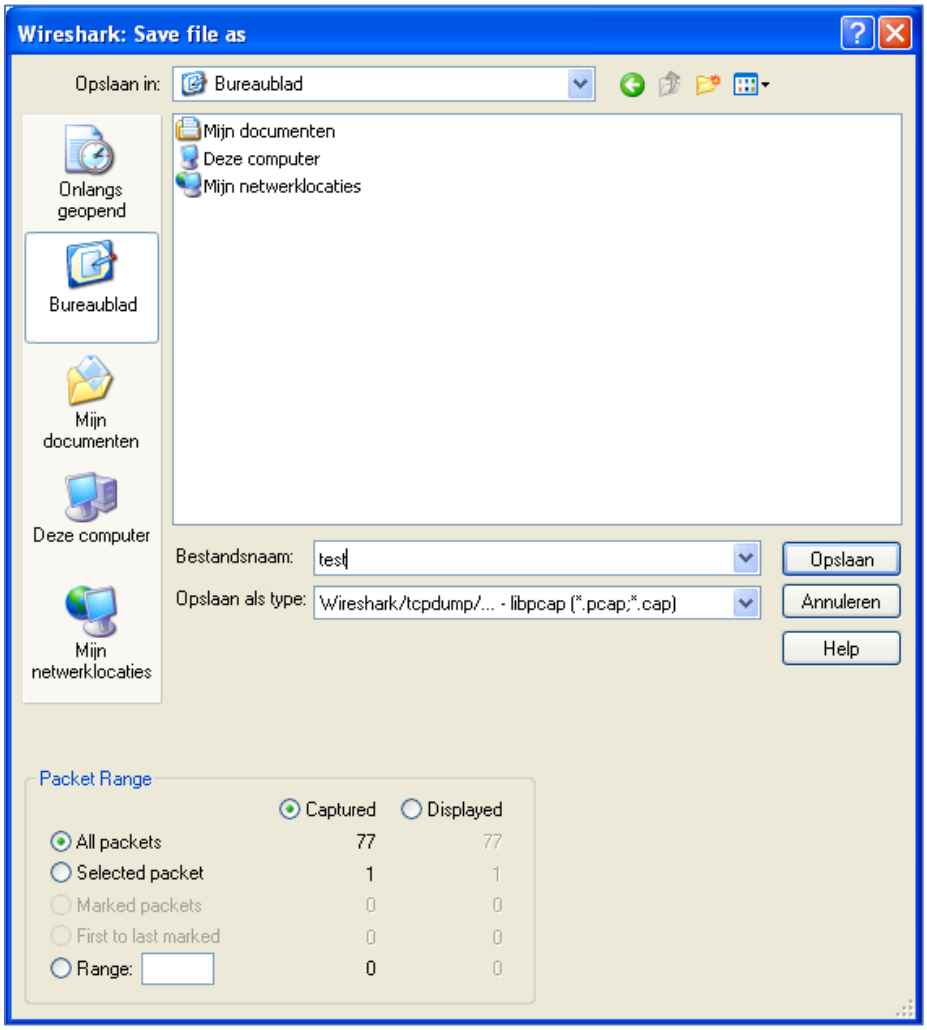
Vervolgens wordt al het verkeer vastgelegd zoals u kunt zien in bovenstaande afbeelding. Wanneer u genoeg gegevens hebt vastgelegd en u dit wilt opslaan stopt u de capture. Dit kunt u doen door op het 4e icoontje te klikken, zoals aangegeven in onderstaande afbeelding.



Om al deze gegevens op te slaan klikt u op het diskette icoontje.



Hier kunt u aangeven onder welke naam, waar en hoe u het u het bestand wilt opslaan.

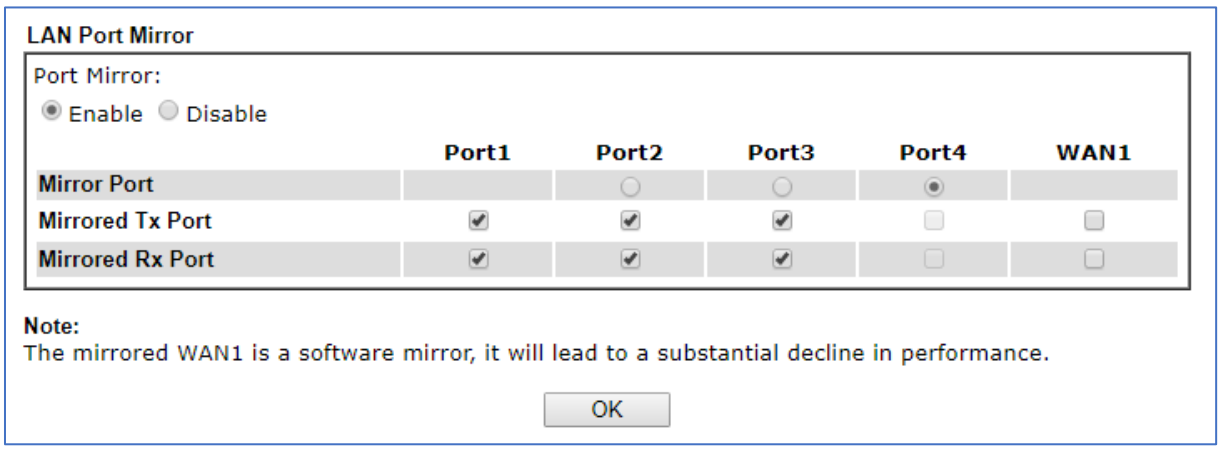


Dit bestand kunt u dan naar de DrayTek support sturen voor analyze.

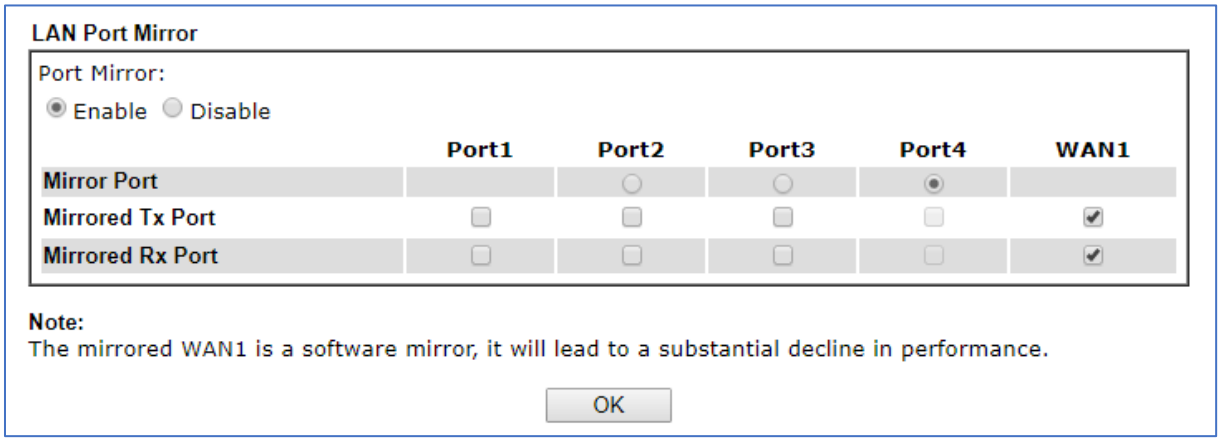
LAN Port Mirror

Middels LAN Port Mirror kunt u aangeven welke LAN of WAN poorten u wilt mirroren. De Mirror Port is de poort waarop u een PC/Server kunt aansluiten waarop u Wireshark gebruikt. De Mirrored TX of Rx Port is de poort waar u een Wireshark trace van wilt maken.

In onderstaande afbeelding sluiten we op LAN poort 4 een PC aan met Wireshark, wanneer de Wireshark trace word gestart zal deze van LAN poorten 1,2 en 3 een capture maken.



In onderstaande afbeelding maken we een capture van de WAN1 interface van de DrayTek. De PC met Wireshark is nog steeds aangesloten op LAN poort 4.



Voorbehoud
We behouden ons het recht voor om deze en andere documentatie te wijzigen zonder de verplichting gebruikers hiervan op de hoogte te stellen. Afbeeldingen en screenshots kunnen afwijken.