

Sonder un signal différentiel avec un oscilloscope

Jean-Michel Friedt, 27 avril 2025

enseignant à l'Université de Franche-Comté, chercheur à FEMTO-ST/temps-fréquence

Un signal différentiel est caractérisé par la propagation sur deux fils supposés proches, pour subir les mêmes perturbations électromagnétiques, de potentiels opposés pour propager une information, et ces potentiels ne sont pas référencés à une masse mais l'un par rapport à l'autre. Un oscilloscope ne peut observer qu'un potentiel référencé à sa masse (puisque les normes interdisent "normalement" de déconnecter la masse de la terre pour la rendre flottante), et même si la solution de soustraire la mesure de deux voies pour analyser le signal différentiel et désormais disponible sur oscilloscopes numériques, d'énormes oscillations du secteur à 50 Hz polluent la mesure différentielle. Nous proposons un circuit dédié, faible coût et facile à assembler, pour convertir le signal différentiel en signal référencé.

Thomas Lavarenne propose dans ces pages [1] une étude détaillée des signaux portés par Ethernet [2] 10 et 100 Mb/s, mais pour acquérir ces signaux il utilise une sonde différentielle dédiée, outil que tout électronicien n'a pas forcément dans la boîte à outils sur son oscilloscope. Afin de pallier cette déficience, nous proposons un montage simple d'amplificateur différentiel, avec la seule subtilité qui consiste à trouver des amplificateurs opérationnels suffisamment rapides pour laisser passer les quelques dizaines de MHz qu'observe Thomas sur ses spectres. Parmi les candidats abordable, faciles à sourcer et obtenus pour ces tests comme échantillons gratuits auprès d'Analog Devices, les ADA4857-1 avec 750 MHz de bande passante en format SOIC faciles à souder sans matériel spécialisé, ou ADA4817-1 avec son GHz de bande passante, semblent parfaitement convenir. Pour les amateurs (ou pas) mieux équipés, les versions -2 en boîtier un peu plus difficiles à manipuler comportent deux amplificateurs opérationnels identiques et permettront donc de sonder avec un seul circuit les deux paires différentielles des câbles Ethernet CAT5.

1 L'amplificateur différentiel

Le montage d'amplificateur différentiel fait partie des grands classiques des montages à amplificateur opérationnel, et habituellement un tel amplificateur (aussi dit d'instrumentation) s'achète assemblé en configuration de deux suiveurs suivis du montage différentiel. Ce circuit est classiquement utilisé pour sonder des hautes tensions ou un pont de Wheatstone, par exemple avec le vénérable AD622 dont le schéma interne est fourni en figure 16 de sa documentation technique [3]. Cependant avec ses quelques centaines de kHz de bande passante, nous n'irons pas loin pour sonder les signaux Ethernet. Il faut donc revenir aux bases (e.g. [4], et Fig. 1, gauche) :

- l'entrée inverseuse est configurée comme pour tout amplificateur inverseur avec une boucle de rétroaction sur la sortie et un pont diviseur entre l'entrée et la sortie pour déterminer le gain d'amplification,
- plus original, l'entrée non-inverseuse n'est pas à la masse mais amène le second signal de la paire différentielle, lui aussi divisé par le même pont de résistances mais cette fois référencé à la masse.

Attention : le circuit proposé a été uniquement testé pour observer les signaux Ethernet 10 et 100Mb, et ne doit en aucun cas être utilisé pour des mesures de signaux vitaux (électrocardiogramme) ou sous haute tension sans une compréhension des implications du manque d'isolation d'un amplificateur unique sans les suiveurs de l'amplificateur d'instrumentation habituel.

Quand toutes les résistances du circuit sont identiques, nous avons

$$V_{\text{sortie}} = V_2 - V_1$$

qui est bien le rôle attendu d'un convertisseur de signaux différentiels (V_1 et V_2) pour produire un signal référencé à la masse V_{sortie} . Pour rappel, nombre de signaux rapides sont propagés en paires différentielles pour garantir une meilleure immunité aux perturbations électromagnétiques qui sont supposées affecter de la même façon les deux brins et donc ne pas être visibles sur la différence.

2 Circuit et routage sous KiCAD

Un circuit aussi simple ne pose aucun problème de schéma ou de routage (Fig. 1), si ce n'est de bien penser que nous propagerons des signaux à près de 100 MHz donc au minimum un plan de masse convenablement relié au plan des signaux par nombre de vias, même sur un circuit deux couches, est nécessaire. Par ailleurs, les amplificateurs opérationnels rapides ont une fâcheuse tendance à trouver quelque-part dans leur bande passante une condition de Barkhausen [5] d'oscillation, et donc de bons découplages (ici 10 et 100 nF) et un condensateur sur la boucle de rétroaction visent à atténuer toute velléité d'oscillation intempestive.

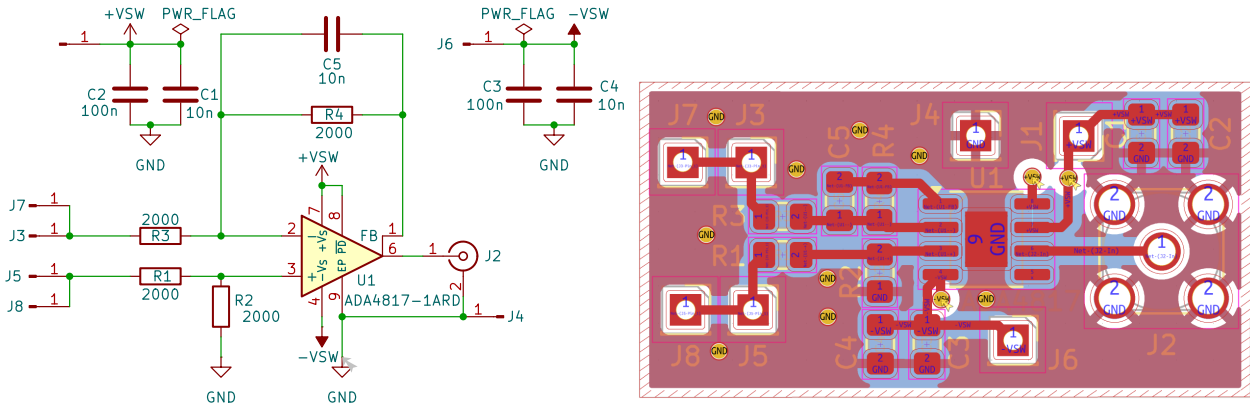


FIGURE 1 – Schéma et circuit contenant l'amplificateur opérationnel rapide en configuration d'amplificateur différentiel rapide.

Deux points de connexion sont prévus pour chaque signal différentiel (J8 et J5 d'une part, J7 et J3 d'autre part) afin de facilement connecter les deux bouts du câble Ethernet CAT5 coupé en deux puisque le circuit se connecte en parallèle. Le signal de mise hors tension est connecté à un via flottant qui peut être relié par un fil soit à la tension positive d'alimentation, soit la tension négative selon qu'un ADA4817 (PD# inactif en connectant à $+V_S$) ou un ADA4857 (PD inactif en connectant à $-V_S$) est utilisé.

3 Observation des signaux Ethernet

Un oscilloscope, toute de même de qualité radiofréquence et idéalement avec une bonne profondeur mémoire pour post-traiter les acquisitions, est connecté en sortie de l'amplificateur différentiel. Les observations (Fig. 2) dans le domaine temporel (gauche) et en diagramme de l'œil pour faire ressortir les symboles, est conforme aux observations de Thomas avec ses sondes professionnelles. Le diagramme de l'œil s'obtient en sélectionnant un mode de persistance des traces – ici une centaine de millisecondes – et en déclenchant la synchronisation sur un niveau entre deux transitions (flèche à droite de la capture d'écran).

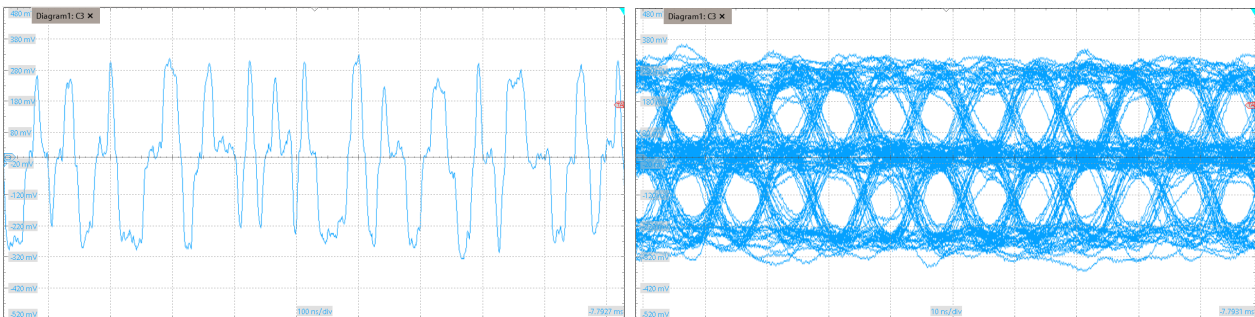


FIGURE 2 – Captures d'écran sur oscilloscope Rohde & Schwarz RTO2034 sur une voie configurée pour traiter la bande complète de 3 GHz, chargée sous 50 Ω .

4 Décodage des signaux Fast Ethernet (100Mb)

Le programme Python proposé par Thomas fonctionne fort bien, sous réserve de sélectionner une fréquence d'échantillonnage multiple du bit-rate du signal Fast Ethernet, à savoir 125 MHz. En configurant l'oscilloscope Rohde & Schwarz RTO2034 pour acquérir 500 MS/s, avec sa profondeur mémoire de 10 Mpoints, nous pouvons enregistrer une durée de 20 ms. Afin de garantir une trame dans l'observations, nous allons demander (ping) toutes les 10 ms à l'oscilloscope d'adresse IP 192.168.1.201, depuis notre ordinateur portable, s'il est présent : `ping -i 0.01 192.168.1.201`. Le fichier acquis et traité indique :

```
Preamble: 55555555555555d5
DEST MAC: 20c6eb67cd3e
SOURCE MAC: 00e03305f474
ETHERTYPE: 0800
DATA: 450000540f0600008001a77dc0a801c9c0a8010c00003e91003218b060c7f76700000000878a
0a000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f303132
333435363759693f93
```

dans laquelle nous retrouvons la description des champs Ethernet et d'un paquet ICMP (RFC0792) tel que décrits dans [6] et correctement analysé par Thomas, en accord avec les informations des deux interlocuteurs puisque sur l'ordinateur portable, `ifconfig eth0` indique

```
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 192.168.1.12 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::22c6:ebff:fe67:cd3e prefixlen 64 scopeid 0x20<link>
    ether 20:c6:eb:67:cd:3e txqueuelen 1000 (Ethernet)
```

avec l'adresse MAC argument du champ `ether`, et `netdiscover` indique

```
192.168.1.201 00:e0:33:05:f4:74 2 120 E.E.P.D. GmbH
```

correspond bien à l'adresse MAC d'un fournisseur allemand. La charge utile est un paquet IPv4 (0x45 pour IPv4 avec un entête de 5 mots de 32 bits) de longueur totale 0x0054=84 octets et de nature ICMP (0x01 après le temps de vie du paquet initialisé à 0x80 sauts), à destination de l'IP 192.168.1.201 (0xC0A801C9) en provenance de 192.168.1.12 (0xC0A8010c). Le contenu du paquet ICMP commençant à 0x00003e91... indique un type *echo reply* (initié par ping) suivi d'un code cyclique de validation (CRC).

5 Décodage des signaux Fast Ethernet (100Mb) dans les deux sens

L'amplificateur opérationnel que nous avons choisi se décline en une version à deux voies, le ADA4817-2, aussi obtenu comme échantillon gratuit auprès d'Analog Devices. Ce boîtier LFCSP à 16 connexions est un peu plus délicat à assembler (Fig. 3), mais avec une bonne binoculaire et la capillarité de l'étain aidant pour éviter les courts-circuits entre broches adjacentes, le brasage manuel se fait sans trop de problèmes au fer à souder. Le bénéfice est de maintenant pouvoir connecter les deux paires différentielles et donc observer le trafic dans les deux sens entre interlocuteurs. Cependant, nous constatons que les acquisitions sont significativement plus bruitées avec ce montage qu'avec l'amplificateur unique, probablement par un manque de blindage et d'isolation entre les deux voies portant les signaux à 125 Mb/s.

Les fichiers contenant 100 Méchantillons sont sauvegardés en format binaire, avec 4 octets/échantillon représenté comme nombre à virgule flottante. Le Rohde & Schwarz RTO2034 sauvegarde en entrelaçant les deux voies si un seul fichier binaire contient les échantillons de deux voies : chaque fichier sauvegardé fait donc la modique taille de 800 MB! Afin de traiter au mieux ces fichiers, Thomas optimise le script d'analyse en resynchronisant le mot de brouillage lorsque la trame débrouillée ne correspond pas à l'état au repos, et surtout accélère considérablement l'analyse pour extraire les trames des énormes fichiers. Ainsi, toujours au cours d'un échange de paquets ICMP toutes les 10 ms, une voie enregistre à l'indice 6,351688 ms de la première voie acquise à 1 G'échantillons/s la trame

```
Preamble: 55555555555555d5
DEST MAC: 00e03305f474
SOURCE MAC: 20c6eb67cd3e
ETHERTYPE: 0800
DATA: 45000054cd4e40004001e8d4c0a8010c0a801c908000e90004601aa46ae0b680000000d396030000000001011
12131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f30313233343536370b1ed159
```

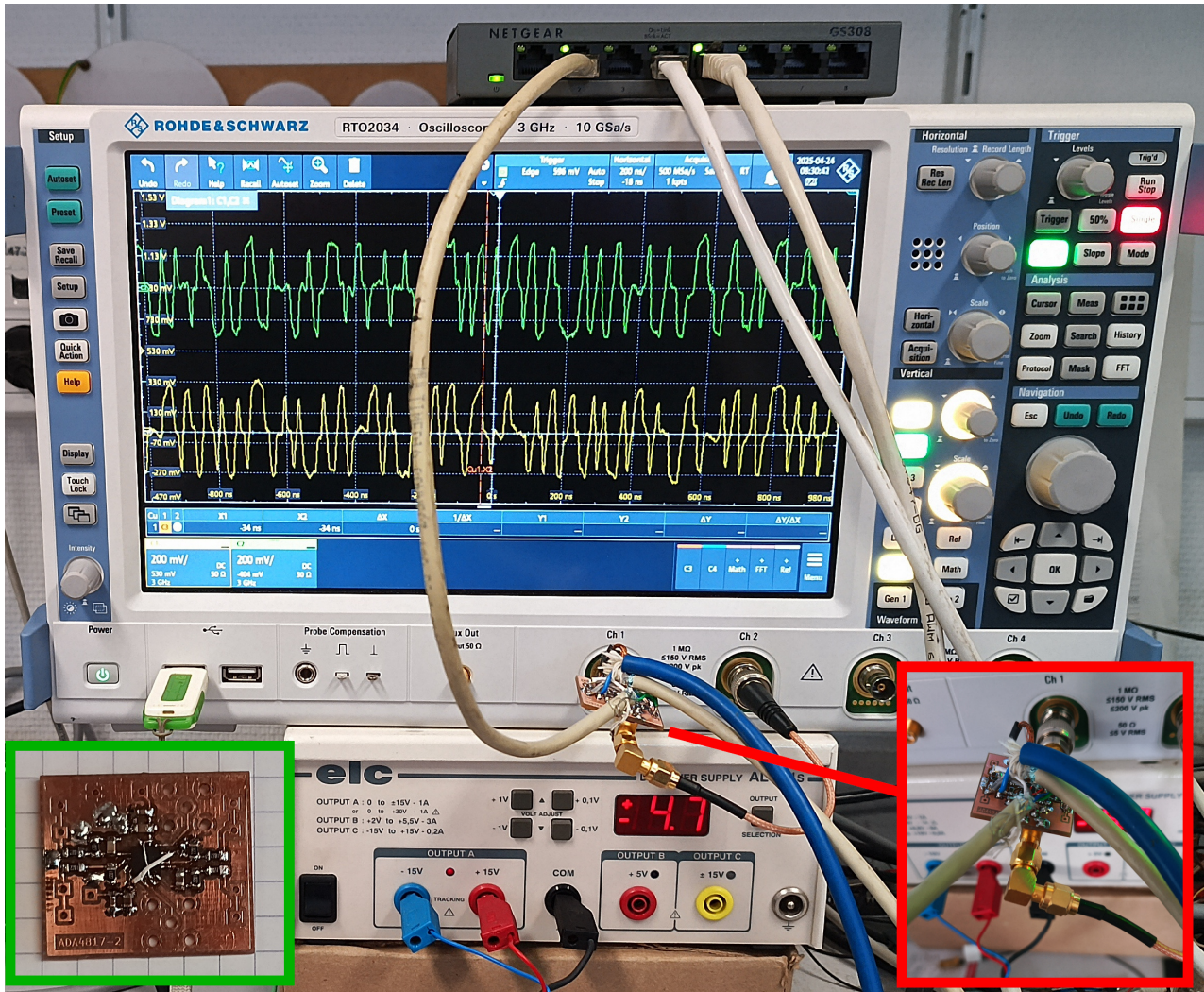


FIGURE 3 – Montage expérimental avec le double amplificateur-opérationnel ADA4817-2 (encadré rouge) convertissant les deux signaux différentiels du câble Fast Ethernet en deux signaux référencés à la masse de l'oscilloscope. Le Rohde & Schwarz RTO2034 a été sélectionné pour sa bande passante, avec des fréquences d'échantillonnage de 500 MS/s ou 1 GS/s pour 4 ou 8 échantillons/bit, et surtout sa profondeur mémoire de 100 Méchantillons, ou 200 ms de durée d'acquisition. Les trois niveaux des deux signaux sont clairement visibles à l'écran. Le circuit de gauche, en cours d'assemblage, est placé sur une feuille graduée tous les 5 mm.

de 192.168.1.12 vers 192.168.1.201, suivi du paquet ICMP commençant par 08 pour demander une réponse (*Echo Request*) dans la séquence 0x1AA4, auquel la réponse ne tarde pas à venir à l'indice 6,465856 ms de l'enregistrement de la seconde voie :

```
Preamble: 55555555555555d5
DEST MAC: 20c6eb67cd3e
SOURCE MAC: 00e03305f474
ETHERTYPE: 0800
DATA: 450000d46b78000080014b0bc0a801c9c0a8010c0001690004601aa46ae036800000000d396030000000001011
12131415561718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637b2b65b39
```

donc, $(6,465856 - 6,351688) = 0,1142$ ms plus tard ou $114 \mu\text{s}$, toujours un paquet ICMP mais cette fois de type 0 donc *Echo Reply* de la séquence 0x1AA4.

Alors que nous étudions les trames, quelle ne fut pas la surprise d'observer

```
Preamble: 55555555555555d5
DEST MAC: 011b19000000
SOURCE MAC: e06ca6000e58
ETHERTYPE: 88f7
DATA: 0002002c00000200000000000000000000000000e06ca6fff000e54000553820000000063ef9fb612569c6f00008d001757
```


3. `sed 's/.\{2\}/& /g'` insère un espace tous les deux caractères qui représentent un octet
4. `sed 's/^/0000 /g'` insère en début de chaîne (^) une adresse "0000"
5. `text2pcap - -` convertit la chaîne ASCII sur stdin en format PCAP sur stdout
6. `tshark -v -x -r - lit (-r)` sur stdin pour décoder la trame et en afficher le contenu.

Thomas a intégré l'analyse des trames Ethernet dans le script Python, mais cette démonstration vise surtout à illustrer la puissance du *pipe* et la philosophie d'unix d'un outil pour une fonction, dont se privent les utilisateurs d'interfaces graphiques intégrant mal toutes les fonctions en bridant leurs logiciels aux séquences de traitements imposées par chaque menu ou icône.

6 Conclusion

Compte tenu de sa taille (Fig. 4) et sa fonction, ce circuit n'est pas sans rappeler les produits du catalogue ANT de la NSA dans lequel un certain nombre de circuits compacts et passifs visent à faire fuiter les informations produites par un ordinateur au travers d'une télé-alimentation et communication sans fil par un RADAR à onde continue. Au lieu de se brancher sur un câble vidéo, il semble tout à fait envisageable de télé-alimenter ce circuit pour lui faire rayonner sous forme d'onde radiofréquence les données transmises par Ethernet. La consommation de ± 5 mA sur chaque polarité pour l'ADA4857-1 ne semble pas incompatible avec une source distante d'alimentation.

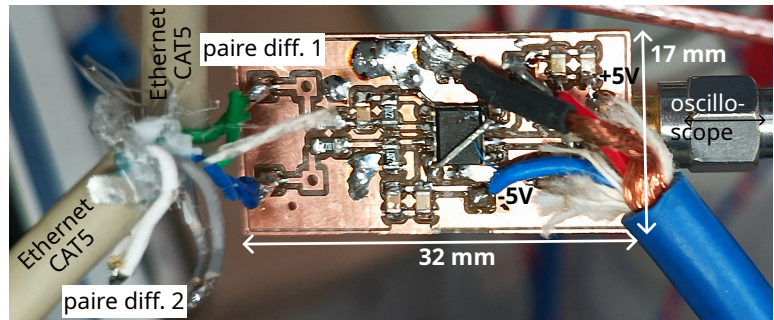


Figure 4: Montage final avec un amplificateur opérationnel alimenté de façon bipolaire pour convertir un signal différentiel en signal référencé à la masse, ici avec un ADA4857-1. Le câble sacrifié pour cette mesure a été assemblé manuellement et ne respecte pas le code couleur des signaux.

La gravure anglaise du circuit imprimé a été réalisée par le service commun électronique de l'institut FEMTO-ST. Le dépôt contenant le logiciel de traitement et les fichiers de conception des circuits imprimés pour KiCAD sont disponibles à <https://github.com/tlavarenne/Ethernet-Hackable>.

Références

- [1] T. Lavarenne, *Ethernet à la loupe : de la couche physique au décodage des trames*, Hackable **XX** (2025)
- [2] K. Hafner & M. Lyon, *Where wizards stay up late : The origins of the Internet*, Simon and Schuster p.155 (1998)
- [3] <https://www.analog.com/media/en/technical-documentation/data-sheets/AD622.pdf>
- [4] *The Differential Amplifier* à https://www.electronics-tutorials.ws/opamp/opamp_5.html ou P. Horowitz & W. Hill, *The art of electronics* 2nd Ed. Cambridge University Press (1989), p.185
- [5] E. Rubiola, *Phase noise and frequency stability in oscillators* chap. 3, Cambridge University Press (2008)
- [6] W.R. Stevens, *TCP/IP Illustrated Vol. 1 – The Protocols (2nd Ed.)*, Addison & Wesley (2012)
- [7] <https://en.wikipedia.org/wiki/EtherType#Values> ou <https://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.xhtml>
- [8] <https://macaddress.io/>
- [9] *White Rabbit Switch by Creotech* à <https://creotech.pl/product/white-rabbit-switch-wrs/>
- [10] <https://gitlab.com/ohwr/project/ppsi/-/blob/49833dde2fcbed69df4191cb4901d1f533e0e009/include/ppsi/constants.h#L182>
- [11] M. Lipiński & al., *White Rabbit : a PTP Application for Robust Sub-nanosecond Synchronization*, IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication (2011), Fig. 2