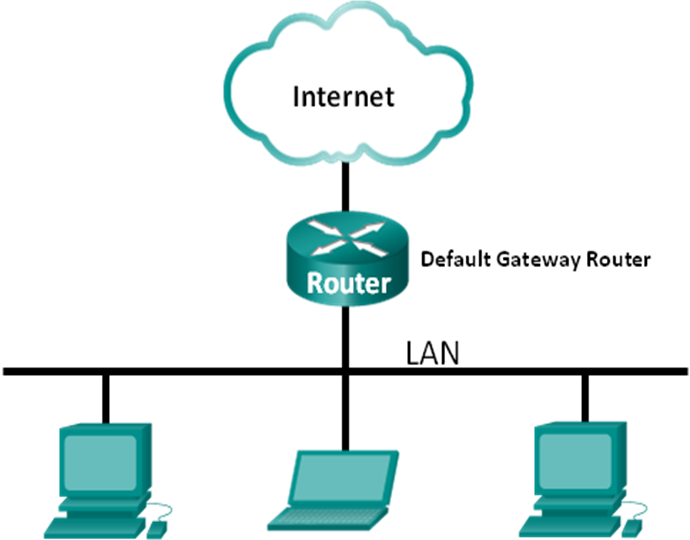
Übung - Anzeigen von Netzverkehr mit Wireshark

1. Topologie



1. Lernziele

Teil 1: (Optional) Herunterladen und Installieren von Wireshark

Teil 2: Erfassen und analysieren von lokalen ICMP-Daten in Wireshark

* Datenerfassung von Ping-Verkehr zu lokalen Hosts starten und stoppen
* IP- und MAC-Adressinformationen in erfassten PDUs ermitteln

Teil 3: Erfassen und analysieren von Remote-ICMP-Daten in Wireshark

* Datenerfassung von Ping-Verkehr zu Remote-Hosts starten und stoppen
* IP- und MAC-Adressinformationen in erfassten PDUs ermitteln
* Warum sich MAC-Adressen für Remote-Hosts von MAC-Adressen lokaler Hosts unterscheiden

1. Hintergrund / Szenario

Wireshark ist ein Software-Protokoll-Analysator oder eine "Paket-Sniffer"-Anwendung zur Fehlersuche, Analyse, Software- und Protokollentwicklung sowie Ausbildung im Netzwerk. Sobald Datenströme über das Netzwerk hin und her wandern, "fängt" der Sniffer jede Protokolldateneinheit (PDU) ein und kann gemäß der entsprechenden RFC oder sonstigen Spezifikationen deren Inhalt dekodieren und analysieren.

Wireshark ist ein nützliches Werkzeug für alle, die mit Netzwerken arbeiten und kann mit den meisten Übungen in den CCNA-Kursen zur Datenanalyse und Fehlersuche verwendet werden. Diese Übung enthält Anweisungen zum Herunterladen und Installieren von Wireshark, auch wenn es möglicherweise bereits installiert ist. In dieser Übung werden Sie Wireshark nutzen, um ICMP-Datenpaket, IP-Adressen und Ethernet-Frame-MAC-Adressen zu erfassen.

1. Erforderliche Ressourcen

* 1 PC (Windows 7, Vista oder XP mit Internet-Zugang)
* Zusätzliche PCs in einem lokalen Netzwerk (LAN) werden verwendet, um auf Ping-Anfragen zu antworten.

1. Erfassen und analysieren von lokalen ICMP-Daten in Wireshark

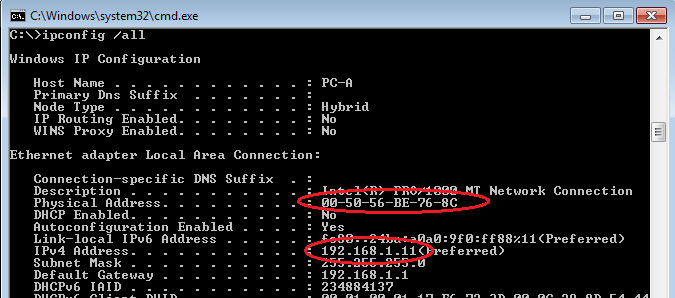
In Teil 2 dieser Übung werden Sie einen Ping an einen anderen PC in dem LAN senden und ICMP-Anfragen und Antworten in Wireshark erfassen. Sie werden außerdem in den erfassten Rahmen nach spezifischen Informationen suchen. Diese Analyse soll klären, wie Paket-Header verwendet werden, um Daten zu ihrem Bestimmungsort zu transportieren.

* 1. Interface-Adressen Ihres PCs abrufen

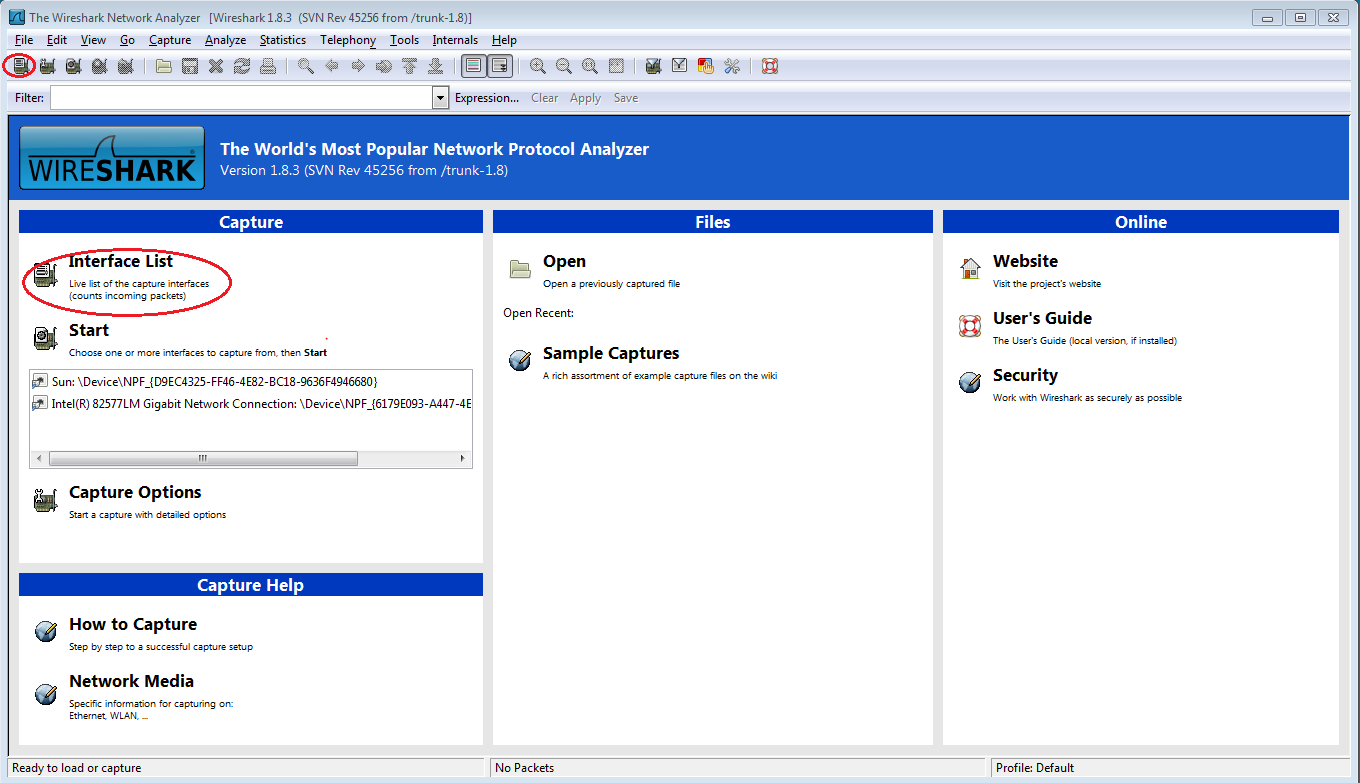
Für diese Übung müssen Sie die IP-Adresse Ihres PCs und die physikalische Adresse seiner Netzwerkkarte (NIC), auch MAC-Adresse genannt, abrufen.

* + 1. Öffnen Sie das Befehlsfenster, geben Sie **ipconfig /all** ein und drücken Sie die Eingabetaste.
    2. Notieren Sie die IP-Adresse und (physikalische) MAC-Adresse Ihrer PC-Schnittstelle.

IP: 10.151.131.24 MAC: D4C9EFE138C2

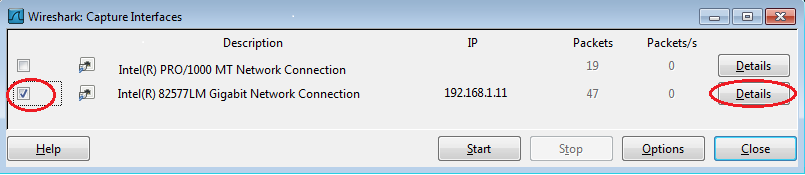


* + 1. Fragen Sie einen Teamkollegen nach der IP-Adresse seines PCs und geben Sie ihm die IP-Adresse Ihres PCs. Geben Sie an dieser Stelle noch nicht Ihre MAC-Adresse weiter.
  1. Wireshark starten und mit dem Erfassen von Daten beginnen
     1. Auf Ihrem PC klicken Sie auf die Schaltfläche Windows **Start**, um Wireshark als eines der Programme in dem Pop-up-Menü zu sehen. Doppelklicken Sie auf **Wireshark**.
     2. Nachdem Wireshark gestartet ist, klicken Sie auf **Interface List**.

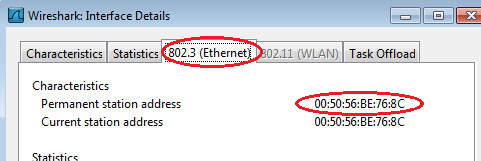


**Hinweis**: Durch Klicken auf das erste Schnittstellensymbol in der Symbolleiste öffnet sich auch die Schnittstellenliste.

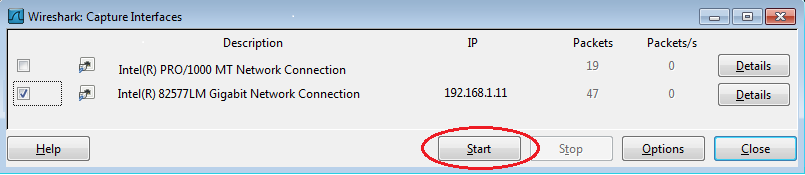
* + 1. Im Fenster Wireshark: Capture Interfaces klicken Sie auf das Kontrollfeld neben der Schnittstelle, die mit Ihrem LAN verbunden ist.



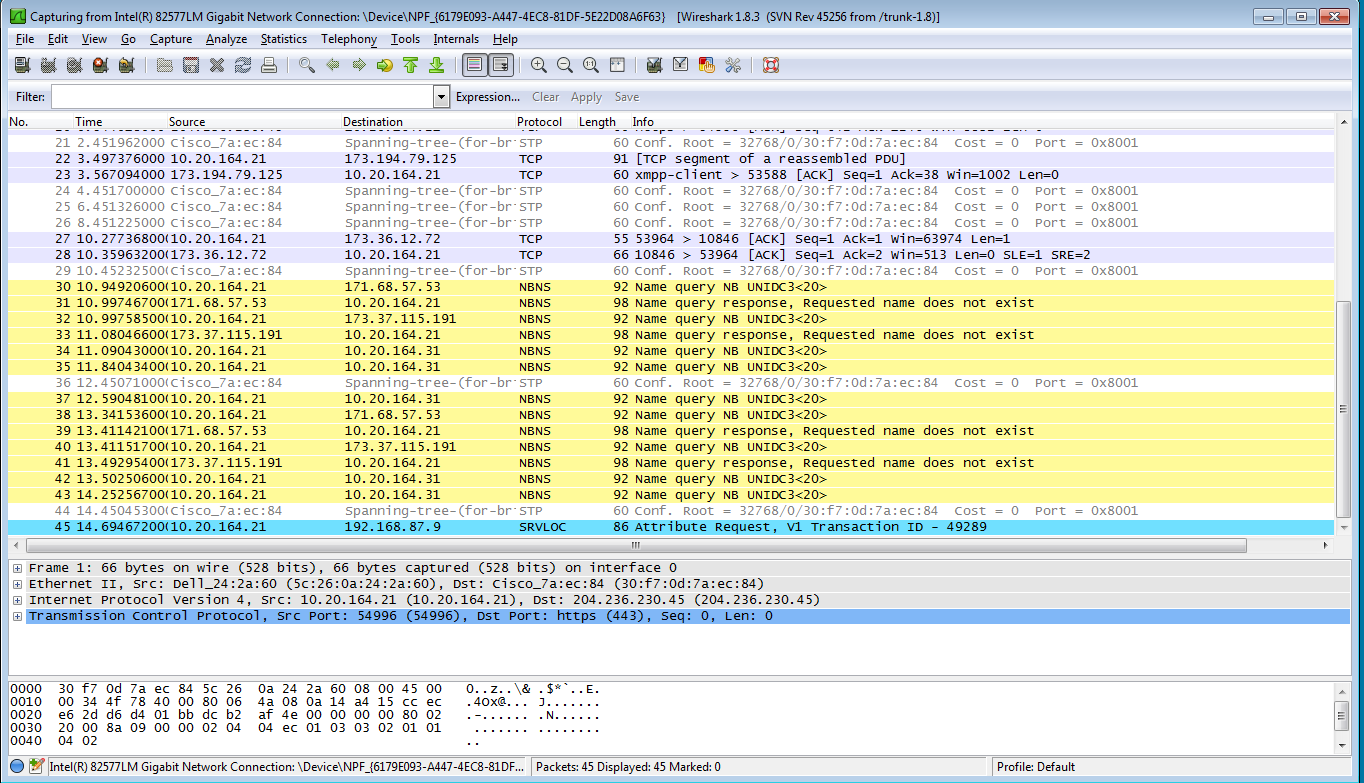
**Hinweis**: Falls mehrere Schnittstellen aufgeführt sind und Sie unsicher sind, welche Schnittstelle Sie aktivieren sollen, klicken Sie auf die Schaltfläche **Details** und dann auf die Registerkarte **802.3 (Ethernet)**. Stellen Sie sicher, dass die MAC-Adresse mit der Adresse übereinstimmt, die Sie in Schritt 1b notiert haben. Nach Verifizieren der richtigen Schnittstelle schließen Sie das Fenster Interface Details.



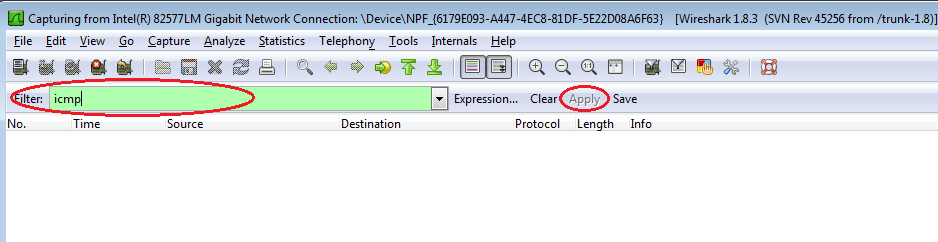
* + 1. Nachdem Sie die richtige Schnittstelle aktiviert haben, klicken Sie auf **Start**, um mit der Datenerfassung zu beginnen.



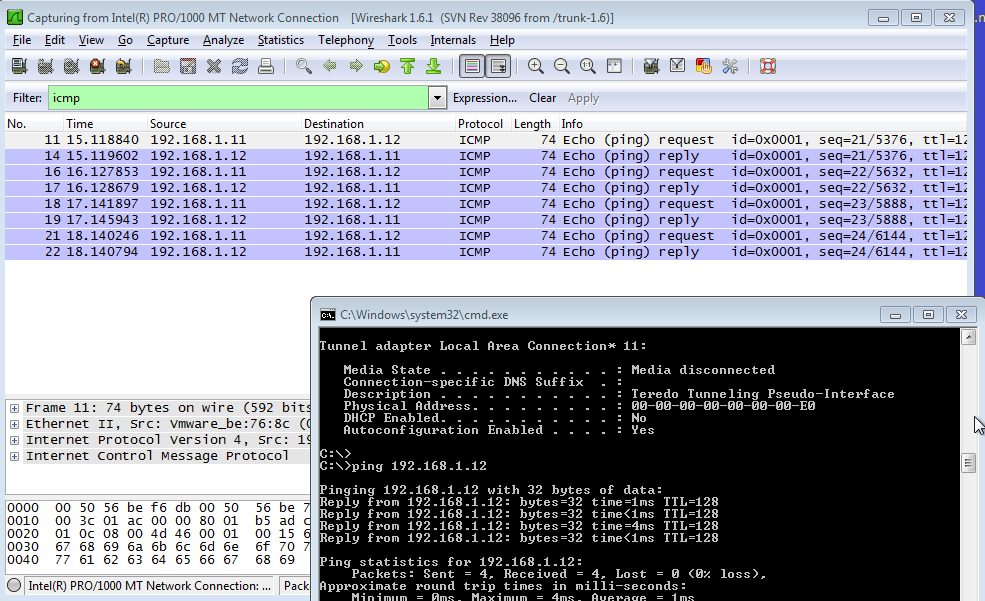
Informationen beginnen, über den oberen Abschnitt in Wireshark herunterzurollen. Die Datenzeilen erscheinen in verschiedenen Farben beruhend auf dem Protokoll.



* + 1. Diese Informationen können sehr schnell vorbeirollen, je nachdem, welche Kommunikation zwischen Ihrem PC und dem LAN gerade stattfindet. Wir können einen Filter anwenden, damit es einfacher wird, die von Wireshark erfassten Daten anzusehen und damit zu arbeiten. In dieser Übung interessieren wir uns nur für die Anzeige von ICMP (ping)-PDUs. Geben Sie **icmp** im Filterfeld oben von Wireshark ein und drücken Sie die Eingabetaste oder klicken Sie auf die Schaltfläche **Apply**, um nur ICMP (ping)-PDUs anzuzeigen.

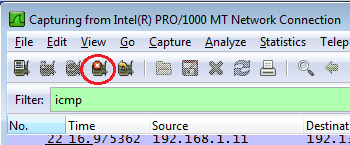


* + 1. Dieser Filter führt dazu, dass alle Daten im oberen Fenster verschwinden, Sie erfassen jedoch immer noch den Verkehr auf der Schnittstelle. Gehen Sie zurück in das vorher geöffnete Befehlseingabefenster und senden Sie einen Ping an die IP-Adresse, die Sie von Ihrem Teamkollegen erhalten haben. Beachten Sie, dass wieder Daten im oberen Fenster von Wireshark erscheinen.



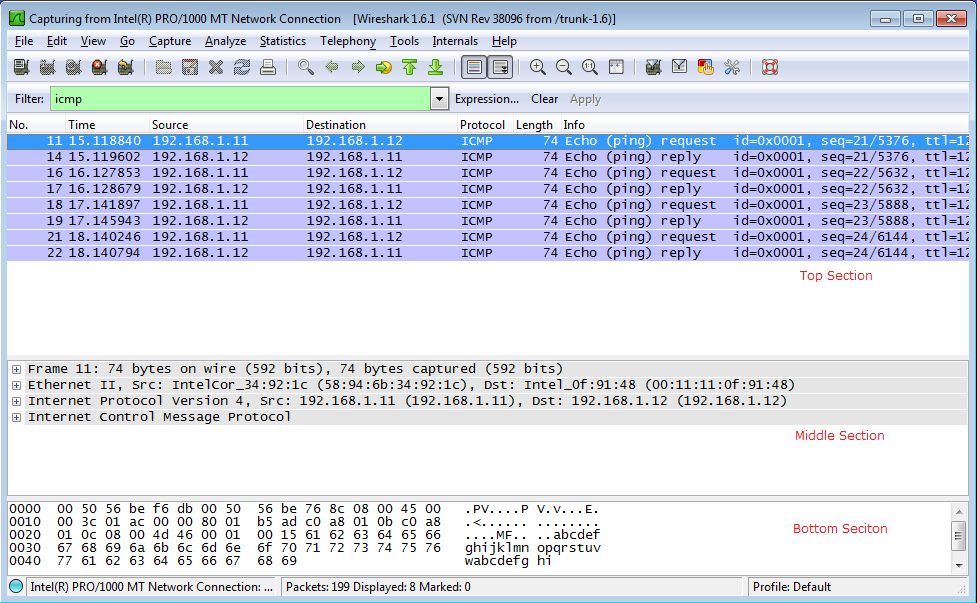
**Hinweis**: Falls der PC Ihres Teamkollegen nicht auf Ihre Pings antwortet, blockiert möglicherweise die Firewall auf dessen PC diese Anfragen. Lesen Sie bitte nach unter Anhang A: ICMP-Verkehr durch eine Firewall zulassen für weitere Informationen, wie man ICMP-Verkehr durch die Firewall unter Windows 7 zulässt.

* + 1. Beenden Sie die Datenerfassung, indem Sie auf das Symbol **Stop Capture** klicken.

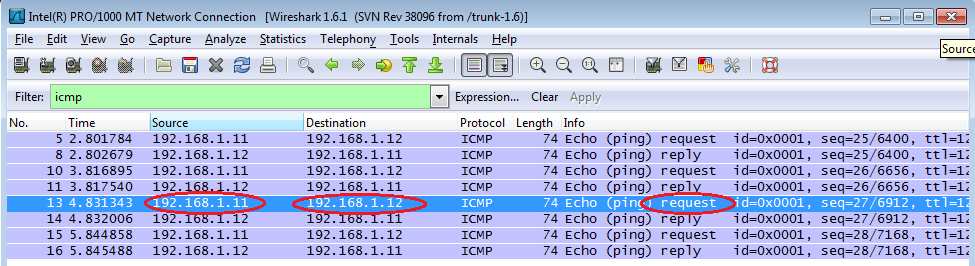


* 1. Die erfassten Daten prüfen

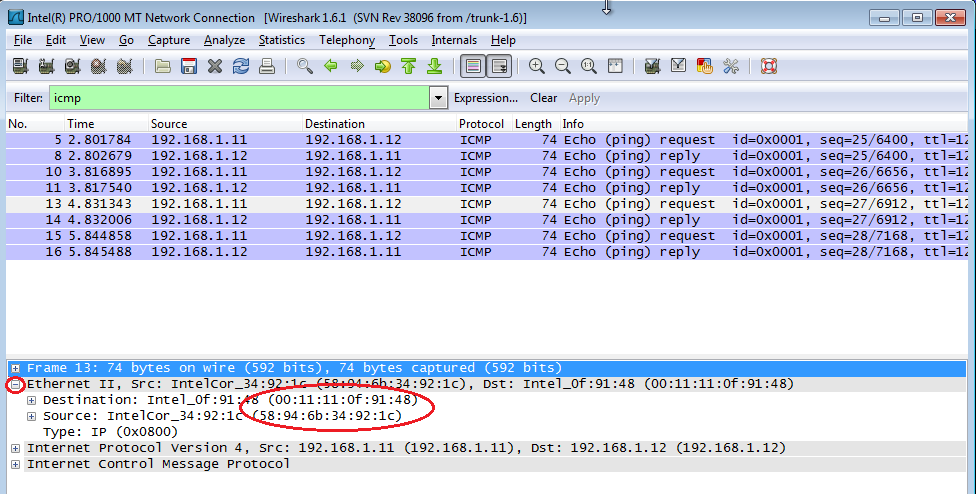
In Schritt 3 prüfen Sie die Daten, die durch die Ping-Anfragen vom PC Ihres Teamkollegen generiert wurden. Wireshark-Daten werden in drei Abschnitten angezeigt: 1) Der obere Abschnitt zeigt die Liste der erfassten PDU-Rahmen mit einer Zusammenfassung der aufgeführten IP-Paketinformationen, 2) der mittlere Abschnitt listet PDU-Informationen für den Rahmen auf, der im oberen Teil des Bildschirms ausgewählt ist und separiert einen erfassten PDU-Rahmen nach dessen Protokollschichten und 3) der untere Abschnitt zeigt die Rohdaten für jede Schicht. Die Rohdaten werden sowohl hexadezimal als auch dezimal angezeigt.



* + 1. Klicken Sie auf die ersten ICMP-Request-PDU-Rahmen im oberen Bereich von Wireshark. Beachten Sie, dass die Source-Spalte die IP-Adresse Ihres PCs enthält und die Destination-Spalte die IP-Adresse des von Ihnen gepingten PCs Ihres Teamkollegen enthält.



* + 1. Bei markiertem PDU-Rahmen im oberen Abschnitt navigieren Sie in den mittleren Abschnitt. Klicken Sie auf das Pluszeichen links neben der Ethernet-II-Zeile, um die Ziel- und Quell-MAC-Adressen anzuzeigen.



Stimmt die MAC-Quelladresse mit der Schnittstelle Ihres PCs überein? Ja

Stimmt die MAC-Zieladresse in Wireshark mit der MAC-Adresse Ihres Teamkollegen überein?

Ja

Wie wird die MAC-Adresse des gepingten PCs von Ihrem PC erhalten?

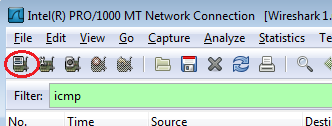
ARP Protokoll

**Hinweis**: In dem vorhergehenden Beispiel einer erfassten ICMP-Anfrage sind die ICMP-Daten in einer IPv4-Paket-PDU (IPv4-Header) gekapselt, die wiederum in einer Ethernet II-Rahmen-PDU (Ethernet II-Header) für die Übertragung in dem LAN gekapselt sind.

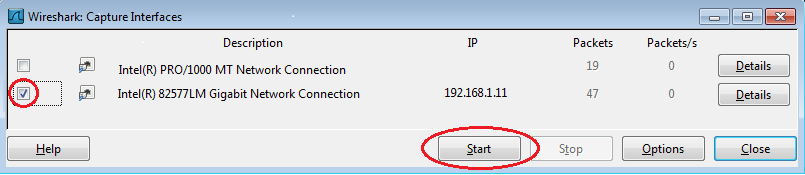
1. Erfassen und analysieren von Remote-ICMP-Daten in Wireshark

In Teil 3 werden Sie Pings an Remote-Hosts (Hosts außerhalb des LANs) senden und die generierten Daten aus diesen Pings untersuchen. Sie werden dann ermitteln, wie sich diese Daten von den in Teil 2 geprüften Daten unterscheiden.

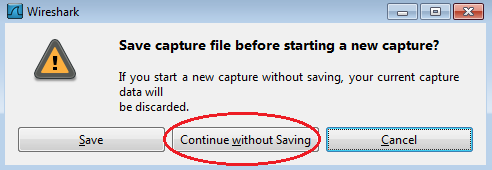
* 1. Erfassen von Daten auf der Schnittstelle starten
     1. Klicken Sie auf das Symbol **Interface List**, um die Liste der PC-Schnittstellen erneut anzuzeigen.



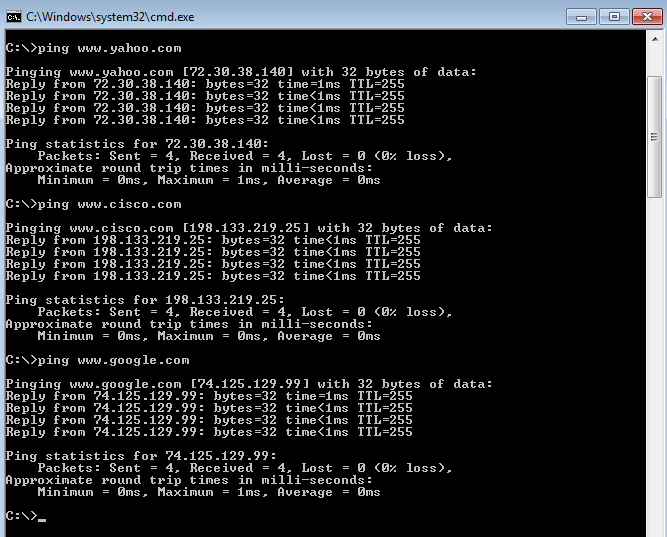
* + 1. Stellen Sie sicher, dass das Kontrollkästchen neben der LAN-Schnittstelle aktiviert ist und klicken Sie dann auf **Start**.



* + 1. Ein Fenster fordert Sie auf, die zuvor erfassten Daten vor dem Beginn einer neuen Datenerfassung zu speichern. Es ist nicht notwendig, diese Daten zu speichern. Klicken Sie auf **Continue without Saving**.

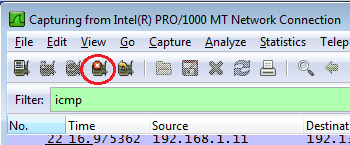


* + 1. Bei aktivierter Erfassung senden Sie einen Ping an die folgenden drei Website-URLs:
       1. www.yahoo.com
       2. www.cisco.com
       3. www.google.com



**Hinweis**: Wenn Sie die aufgeführten URLs anpingen, beachten Sie, dass der Domain Name Server (DNS) die URL in eine IP-Adresse übersetzt. Notieren Sie die für jede URL erhaltene IP-Adresse.

* + 1. Sie können das Erfassen von Daten stoppen, indem Sie auf das Symbol **Stop Capture** klicken.



* 1. Daten von den Remote-Hosts prüfen und analysieren
     1. Überprüfen Sie die erfassten Daten in Wireshark, prüfen Sie die IP- und MAC-Adressen der drei Standorte, die Sie gepingt haben. Tragen Sie die IP- und MAC-Zieladressen für alle drei Standorte in der jeweilige Lücke ein.

1. Standort: IP: \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_ MAC: \_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_

2. Standort: IP: \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_ MAC: \_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_

3. Standort: IP: \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_ MAC: \_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_

* + 1. Was ist an dieser Information wichtig?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Wie unterscheiden sich diese Informationen von denen, die Sie in Teil 2 erhalten haben?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Reflexion

Warum zeigt Wireshark die tatsächliche MAC-Adresse des lokalen Hosts, nicht aber die tatsächliche MAC-Adresse für die Remote-Hosts?

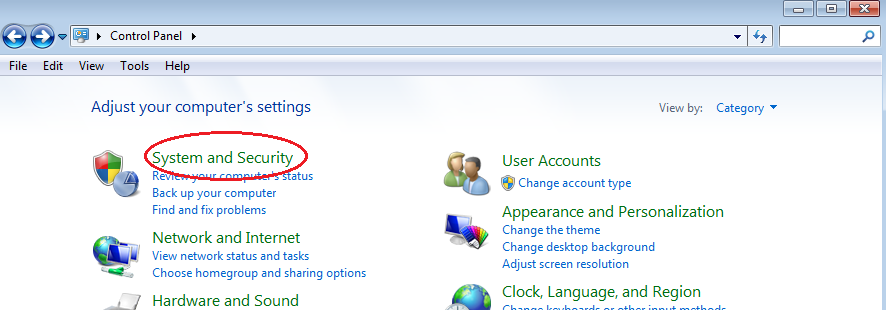
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

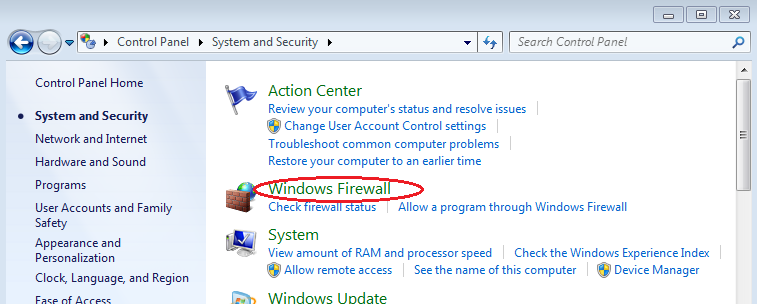
1. Anhang A: ICMP-Verkehr durch eine Firewall zulassen

Falls die Kollegen Ihres Teams Ihren PC nicht anpingen können, blockiert die Firewall möglicherweise diese Anfragen. Dieser Anhang beschreibt, wie eine Regel in der Firewall zum Erlauben von Ping-Anfragen generiert wird. Er beschreibt außerdem, wie diese neue ICMP-Regel nach Beendigung dieser Übung wieder deaktiviert wird.

* 1. Neue Eingangsregel generieren, die ICMP-Datenverkehr durch die Firewall zulässt
     1. Klicken Sie in der Systemsteuerung auf die Option **System and Security**.



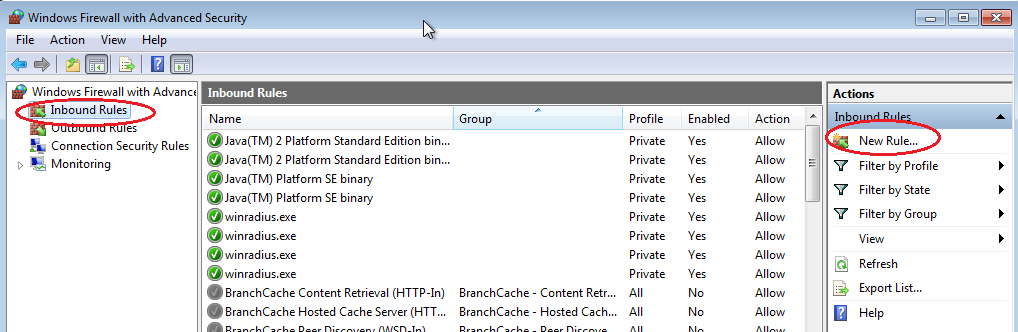
* + 1. Klicken Sie im Fenster System and Security auf **Windows Firewall**.



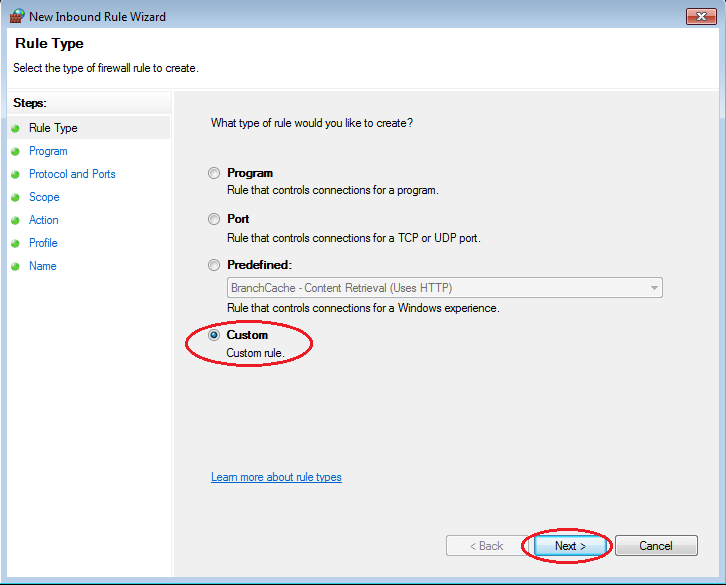
* + 1. In der linken Hälfte des Fensters Windows Firewall klicken Sie auf **Advanced settings**.



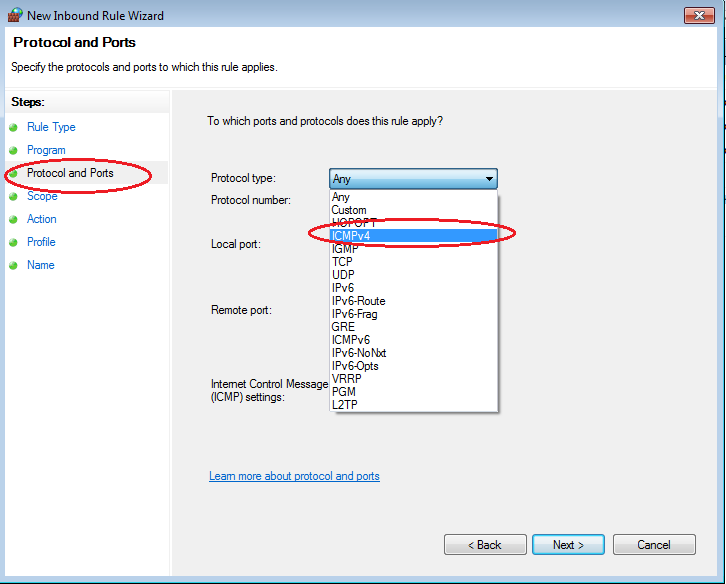
* + 1. Im Fenster Advanced Security wählen Sie die Option **Inbound Rules** auf der linken Seitenleiste und klicken Sie dann **New Rule…** auf der rechten Seitenleiste.



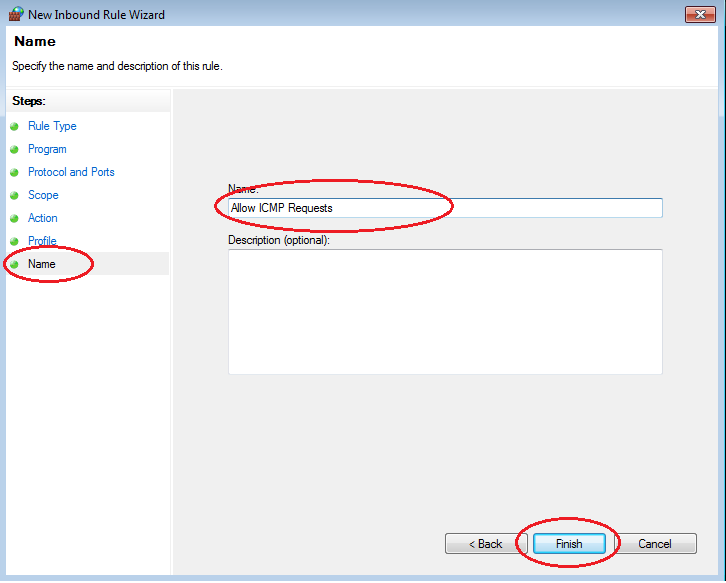
* + 1. Damit wird der Assistent New Inbound Rule gestartet. Im Bildschirm Rule Type klicken Sie auf das Optionsfeld **Custom** und dann auf **Next**



* + 1. In der linken Hälfte klicken Sie auf die Option **Protocol and Ports** und wählen Sie mit dem Protokolltyp-Drop-down-Menü **ICMPv4** und klicken Sie dann auf **Next**.



* + 1. In der linken Hälfte klicken Sie auf die Option **Name** und geben Sie im Feld Name **Allow ICMP Requests** ein. Klicken Sie auf **Finish**.

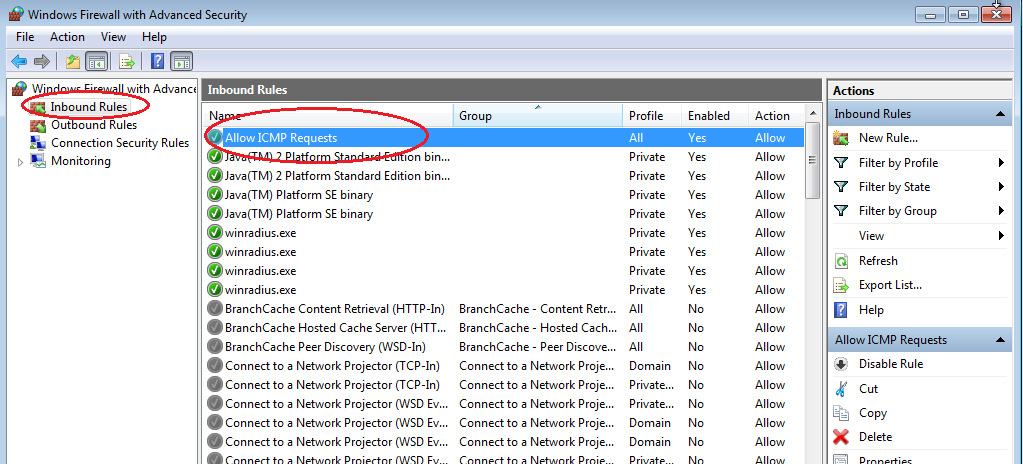


Diese neue Regel sollte Ihren Teamkollegen ermöglichen, Pings von Ihrem PC zu empfangen.

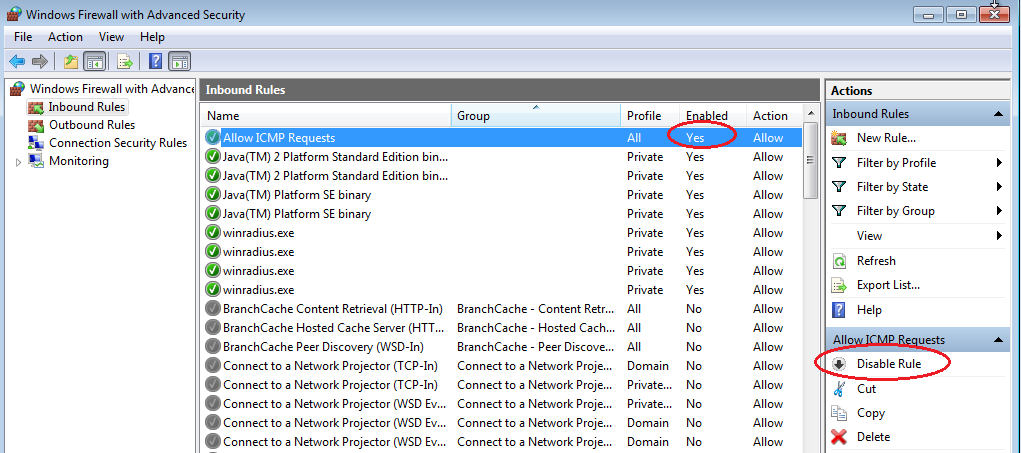
* 1. Die neue ICMP-Regel deaktivieren oder löschen

Nachdem die Übung abgeschlossen ist, möchten Sie die in Schritt 1 erstellte Regel vielleicht deaktivieren oder sogar löschen. Mit der Option **Disable Rule** können Sie die Regel zu einem späteren Zeitpunkt wieder aktivieren. Durch Löschen der Regel wird die Regel dauerhaft aus der Liste Inbound Rules entfernt.

* + 1. Im Fenster Advanced Security klicken Sie in der linken Hälfte auf **Inbound Rules** und suchen Sie die Regel, die Sie in Schritt 1 generiert haben.



* + 1. Zum Deaktivieren der Regel klicken Sie auf die Option **Disable Rule**. Wenn Sie diese Option wählen, sehen Sie, wie sich diese Option ändert in **Enable Rule**. Sie können zwischen Disable Rule und Enable Rule hin und her schalten; der Status der Regel wird auch in der Enable-Spalte und in der Inbound Rule-Liste angezeigt.



* + 1. Zum dauerhaften Löschen der ICMP-Regel klicken Sie auf **Delete**. Wenn Sie diese Option wählen, müssen Sie diese Regel erneut generieren, um ICMP-Antworten zuzulassen.

