

****

**Vorlesung Rechnernetze**

**AIN 5**

**Laborübung**

**Socket Monitoring**

**Prof. Dr. Dirk Staehle**

Die Abgabe erfolgt durch Hochladen der bearbeiteten Word-Datei in Moodle.

**Bearbeitung in Zweier-Teams**

**Team-Mitglied 1: Böcker Jona**

**Team-Mitglied 2: Stöhr Tobias**

# Einleitung

In diesem Laborversuch lernen Sie, wie Sie eine Übersicht bekommen, mit welchen Rechnern im Internet Anwendungen auf ihrem PC kommunizieren. Die gängigen Betriebssysteme stellen das Tool „netstat“ zur Anzeige der geöffneten Sockets zur Verfügung. Eine komfortablere Anzeige bietet unter Windows z.B. das freie Tool „CurrPorts“ von NirSoft (<https://www.nirsoft.net>) und unter Linux NetActView (<http://netactview.sourceforge.net/download.html>, Achtung: weder geladen noch getestet, Download auf eigenes Risiko).

Verwenden Sie für diese Übung wenn möglich ihrem privaten Laptop/PC und nicht den Labor-PC. Eine Analyse der geöffneten Sockets ihres privaten PCs ist für Sie vermutlich interessanter. Achten Sie bei der Arbeit im Team darauf, dass hier Informationen über ihren privaten PC sichtbar werden. Wenn Sie das nicht möchten, sollte jedes Team-Mitglied die Übung selbständig durchführen.

# Monitoring von Sockets

In diesem Versuch sollen Sie analysieren, mit wem ihr PC kommuniziert und welche Prozesse bzw. Programme für diese Kommunikation verantwortlich sind. Erstellen Sie dazu eine Liste der Programme, die Sockets geöffnet haben und finden Sie heraus, mit wem diese Programme kommunizieren. Nutzen Sie hierzu bevorzugt CurrPorts. In CurrPorts lässt sich unter Options einstellen, welche Sockets angezeigt werden. Machen Sie davon Gebrauch, um die gewünschten Ports darzustellen.

Beantworten Sie die folgenden Fragen:

1. Wie viele Sockets sind insgesamt geöffnet?

140

1. Wie unterscheiden sich die Einträge von TCP und UDP Sockets?   
   (Vorgriff auf Kapitel 4.2 der Vorlesung)

TCP Sockets hat ausführlichere Infos (State, Remote Port, Remote Port Name, Remote Address)

1. Was bedeuten die Einträge in der Spalte „State“ bei TCP Sockets?   
   (Vorgriff auf Kapitel 4.3 der Vorlesung)   
   Infos in der Vorlesung oder z.B. hier (eher willkürliche Auswahl):
   1. <https://www.computerweekly.com/de/tipp/Netzwerk-Analyse-mit-Netstat-So-finden-Sie-offene-Ports-und-Malware>
   2. <https://www.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.halu101/constatus.htm>
   3. <https://de.wikipedia.org/wiki/Transmission_Control_Protocol>

LISTEN: Der Server wartet auf eingehende Verbindungen von Clients. In diesem Zustand lauscht der Server auf einem bestimmten Port und wartet darauf, dass eine eingehende Verbindung ankommt.

SYN\_SENT: Der Client hat eine Verbindungsanfrage (SYN) an den Server gesendet und wartet auf eine Bestätigung (ACK) vom Server.

SYN\_RECEIVED: Der Server hat die SYN-Anfrage des Clients erhalten und hat mit einem SYN-ACK geantwortet, was bedeutet, dass er die Verbindungsanfrage akzeptiert hat und auf die Bestätigung des Clients wartet.

ESTABLISHED: Die Verbindung wurde erfolgreich hergestellt. Daten können jetzt zwischen Client und Server ausgetauscht werden. Dies ist der Hauptzustand, während Daten über die Verbindung übertragen werden.

FIN\_WAIT\_1: Der Client hat die Verbindung beendet und wartet auf eine Bestätigung oder eine Bestätigung vom Server, dass er die Verbindung ebenfalls beendet.

FIN\_WAIT\_2: Der Client hat seine Datenübertragung abgeschlossen und wartet auf eine Bestätigung vom Server, um die Verbindung endgültig zu beenden.

1. Wie viele Server Ports hat ihr Rechner geöffnet (state=Listening)? Auf diesen Ports (und den UDP Ports) kann ihr Rechner von außen kontaktiert werden.

35

1. Wie viele Sockets (ESTABLISHED) werden neu geöffnet, wenn Sie die Messung nach einer Minute erneut durchführen bzw. die Ergebnisse aktualisieren?  
   (In CurrPorts AutoRefresh ausschalten und einen manuellen Refresh durchführen)

35 zu 34, es wurde nur ein Port geschlossen.

1. Sehen Sie zahlreiche Sockets mit IP-Adresse 127.0.0.1? Finden Sie heraus, wofür diese IP Adresse benutzt wird und blenden Sie alle Sockets mit dieser Adresse aus.

Es ist die IP-Adresse für den localhost (virtueller Server der auf dem eigenen Rechner läuft)

Filter: exclude:both:tcpudp:127.0.0.1

1. Bestimmen sie anhand der Portnummer und der Portliste für einige interessante/unbekannte Prozesse, mit welchem Protokoll diese kommunizieren. Die Zuweisung von Portnummer zu Protokollen finden Sie z.B. hier:
   1. Offiziell (IANA): <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt>
   2. Wikipedia: <http://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports>
   3. Häufigste Dienste: <https://isc.sans.edu//services.html>

443: HTTPS

80 und 8080: HTTP

25: SMTP

143: IMAP

# Details über die Kommunikationspartner ihres PCs

Das Tool „IPNetInfo“ von NirSoft dient dazu, die zu einer IP Adresse öffentlich verfügbare Information abzurufen und darzustellen. Nachdem Sie IPNetInfo gestartet haben, können Sie es direkt aus CurrPorts aufrufen. Markieren Sie dazu einen oder mehrere Sockets und clicken Sie die rechte Maustaste oder drücken Ctrl+I. Unter Linux habe ich leider kein komfortables Tool gefunden. Sie können entweder den Befehl „whois“ verwenden oder eine Web-Seite nutzen, auf der Sie einzelne IP-Adressen eingeben können.

Analysieren Sie jetzt, mit welchen Servern/Rechnern die Prozesse auf ihrem PC kommunizieren. Generieren Sie dazu mit Hilfe von IPnetInfo in Excel eine Gesamtübersicht der Kommunikationspartner ihres Rechners.

1. Finden Sie über WireShark heraus, wie das Programm „IPnetInfo“ die Informationen erhält. Welcher Server wird kontaktiert? Welches Protokoll wird verwendet?

Verwendete Protokolle: WHOIS, DNS

Kontaktierte IP WHOIS: 199.5.26.46

Kontaktierte IP DNS: 141.37.11.1 🡪 dns-01.htwg-konstanz.de

WHOIS fragt die entsprechende Domain oder IP bei einem verteilten Datenbanksystem an und liefert Informationen über die Adresse oder Domain.

1. Im welchem Netz befindet sich der Web-Server, der in der ersten WireShark-Aufgabe aufgerufenen Web-Seite?

Hostname:

whois.arin.net → 199.212.0.46

IP-Bereich:

199.5.0.0 - 199.5.255.255

Internetanbieter:

ARIN Operations

Organisation:

ARIN Operations

1. Welche Informationen finden Sie über die HTWG?

Hostname:

dns-01.htwg-konstanz.de → 141.37.11.1

IP-Bereich:

141.32.0.0 - 141.63.255.255

Internetanbieter:

BelWue University Network

Organisation:

BelWue University Network

# Sockets beim Laden einer Web-Seite

In der WireShark-Übung haben Sie bereits herausgefunden, wie Sie die Anzahl der geöffneten Sockets beim Download einer Web-Seite wie z.B. [www.spiegel.de](http://www.spiegel.de) feststellen können.

Mit CurrPorts geht das jetzt einfacher und mit mehr Informationen. Sie können die Sockets auch direkt dem Prozess (ihrem Browser) zuordnen und Informationen über die Remote IP-Adresse erhalten.

1. Bestimmen Sie die Anzahl Sockets, die geöffnet werden, wenn Sie [www.spiegel.de](http://www.spiegel.de) herunterladen.
   1. Wenn es Sie interessiert: vergleichen Sie die Anzahl der Sockets mit und ohne Ad-Blocker

343 neue Sockets

1. Was ist die maximale Anzahl von Sockets pro Remote-IP-Adresse?

124 Sockets für den HTWG DNS-Server (141.37.11.1)

1. Welche Remote-Ports werden verwendet?

443 (HTTPS)

53 (DNS)

1. Wie viele verschiedenen Firmen können Sie die Remote-Hosts zuordnen (am Besten über Contact Name in IPNetInfo)?

24 verschiedene Firmen

1. Laden Sie eine andere populäre Web-Seite und vergleichen Sie die Liste der kontaktierten Firmen.

Facebook.com kontaktiert nur google LLC und Microsoft