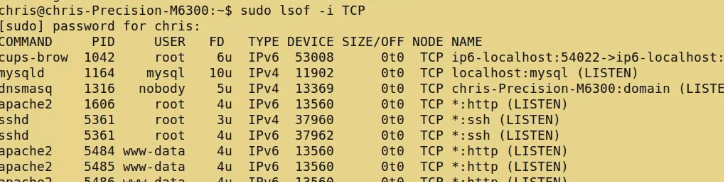
# Linux Network Programming

### Setting the Scene : Demonstrations: lsof and nmap

lsof עומד עבור list open files ואפשר להשתמש בו לבדוק פורטים פתוחים ב TCP במכונה עליה רצה הפקודה

(כמובן, אם רוצים לבדוק מחשב מרוחק אז אפשר להתחבר אליו בעזרת ssh <remoteIp> ולתת שם את הפקודה)

דוגמא



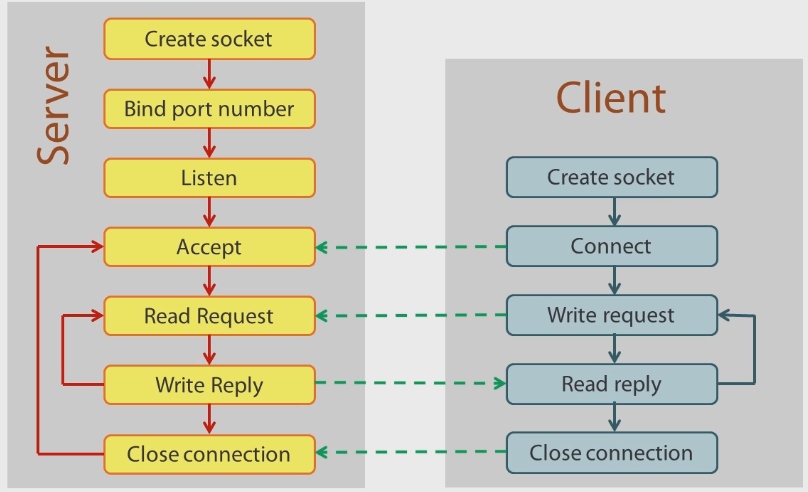
בעוד ש lsof מסתכל על המכונה מבפנים, nmap מסתכל על המכונה מבחוץ.

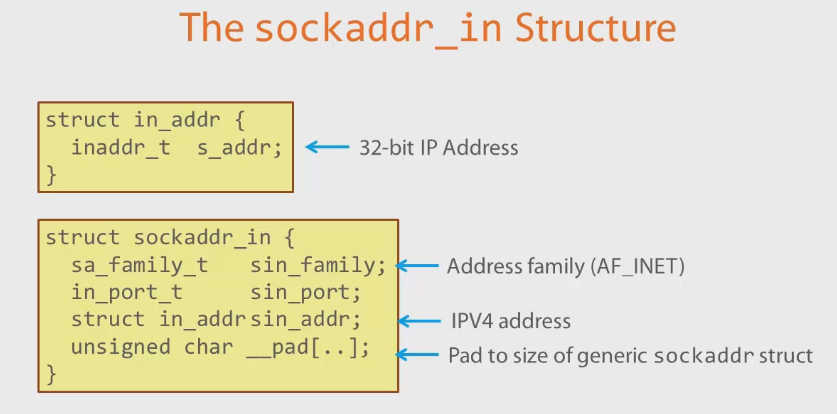
nmap <remoteIp> יתן את שמות הפורטים הפתוחים במכונה המרוחקת.

הערה: מאחר ורוב הפורטים הם מיוחדים לאפליקציות ידועות, הוא מראש כותב את שם ה service במקום לציין את מספר הפורט. זה נכון גם ל lsof ועל כן בתמונה הנ"ל המחרוזת **\*:ssh** פירושה שהמכונה מאזינה בכל כרטיסי הרשת על פורט 22.

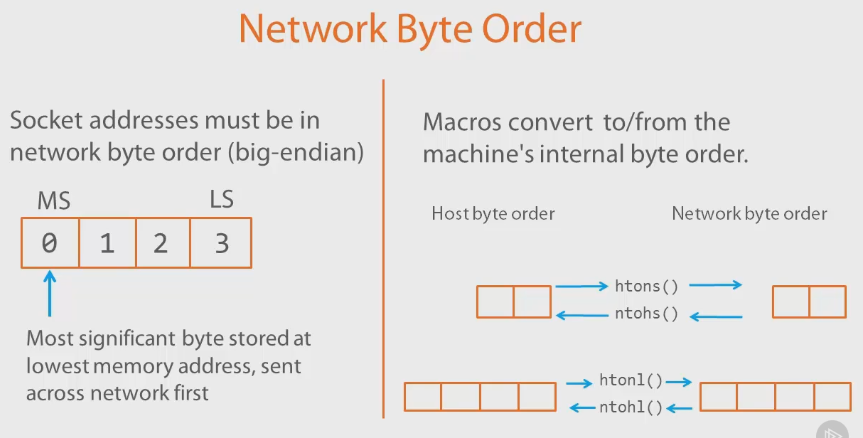
### Writing TCP-based Servers : TCP server: Operations and System Calls

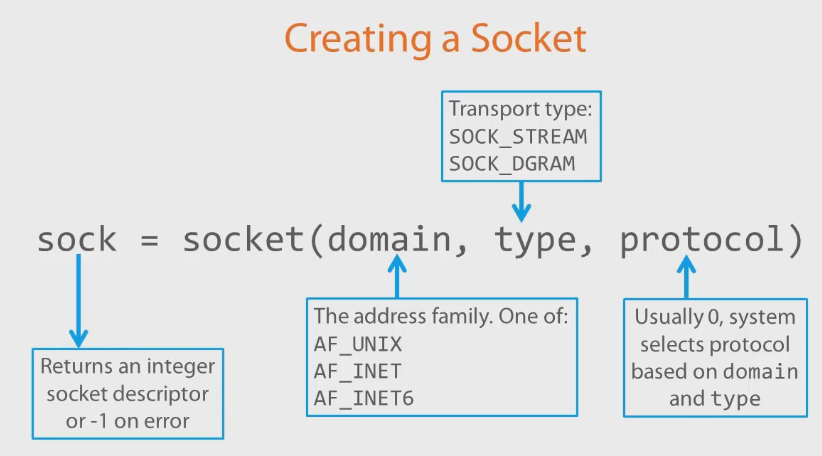
המהלך בכללותו הינו כדלקמן



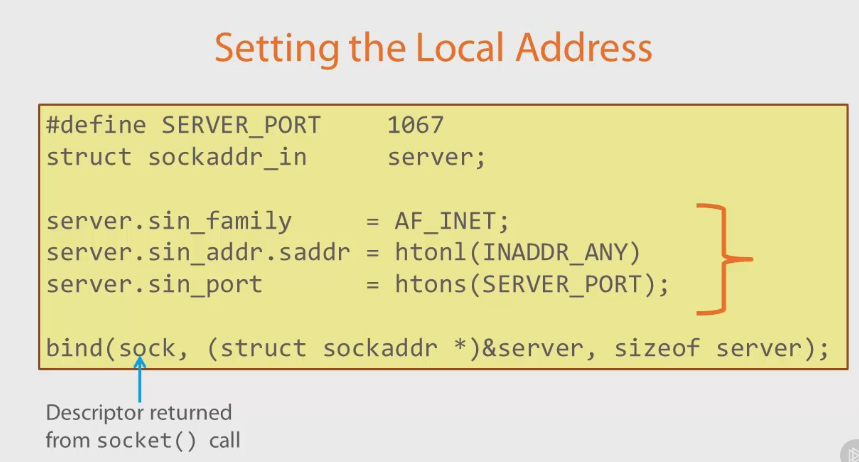


הרשת עובדת ב BigEndian ועל כן במכונות אינטל צריך להמיר את הכתובות. המתודות htons וחברותיה (יש כמה גרסאות בהתאם לטיפוסי המידע) עושות את ההמרה הנדרשת. במכונות שהן בעצמן BigEndian מתודות אלה לא עושות דבר.



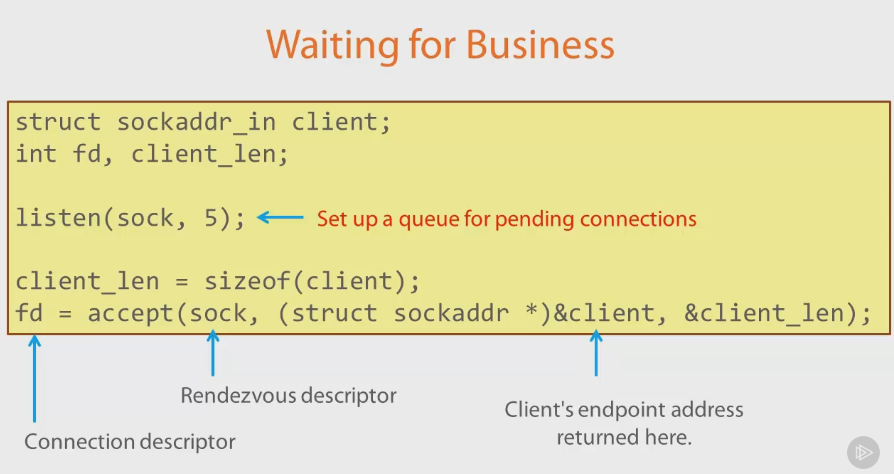


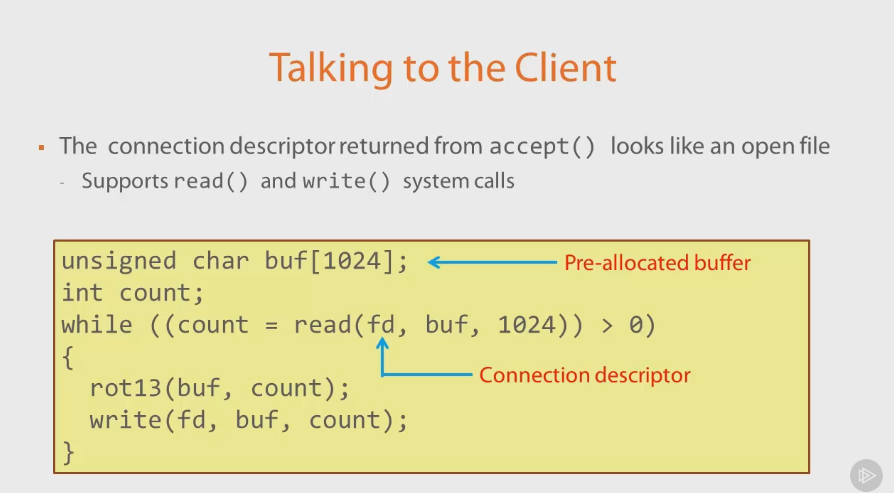
הערה: AF\_UNIX משמש לתקשורת בין תהליכים על אותה מכונה והם מקבילים ל named pipes של unix.



Bind מחזיר 0 להצלחה ו -1 לכשלון.

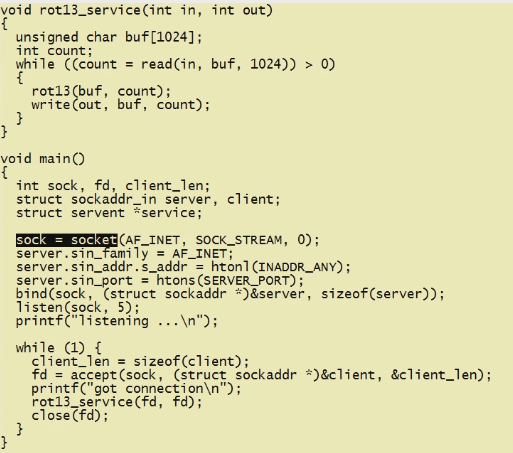
ה cast בשורה האחרונה נועד לשמור על כלליות.





Write מחזיר בחזרה דרך אותו סוקט הודעה אל הלקוח. שים לב שלאחר יצירת הקשר הסוקטים כבר לא משחקים. משתמשים ב fd !

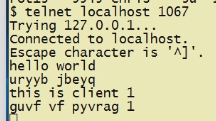
הקוד הבא מאחד את כל השקפים הנ"ל.



המתודה rot13 עושה פעולה מסוימת על הטקסט ומחזירה מחרוזת באותו אורך.

אע"פ שהתכנית מסוגלת בפוטנציה לקבל חמש בקשות התקשרות, בפועל היא כתובה כך שאינה יכולה לקבלם במקביל, מאחר ולאחר כל בקשה היא סוגרת את הקשר ונכנסת להמתנה להתקשרות נוספת, המספר 5 הוא כאן חסר משמעות.

כדי לבחון את התכנית אין צורך לכתוב קליינט יעודי. אפשר פשוט להשתמש בטלנט.



מנסים ליצור קשר עם תהליך על המחשב המקומי. יש לציין פורט מפני שהוא שונה מברירת המחדל (ככלל, לא להשתמש בפורטים קטנים מ 1024 כי הם שמורים ובלינוקס צריך גם זכויות של סופר יוזר להשתמש בהם)

המשתמש הקליד hello world

והתהליך המרוחק החזיר מחרוזת מעורבלת

שוב המשתמש הקליד this is client 1

והתהליך המרוחק החזיר מחרוזת מעורבלת

כדי לסיים נקליד בחלון הטלנט ^] ואז נחזור לשורת הפקודה

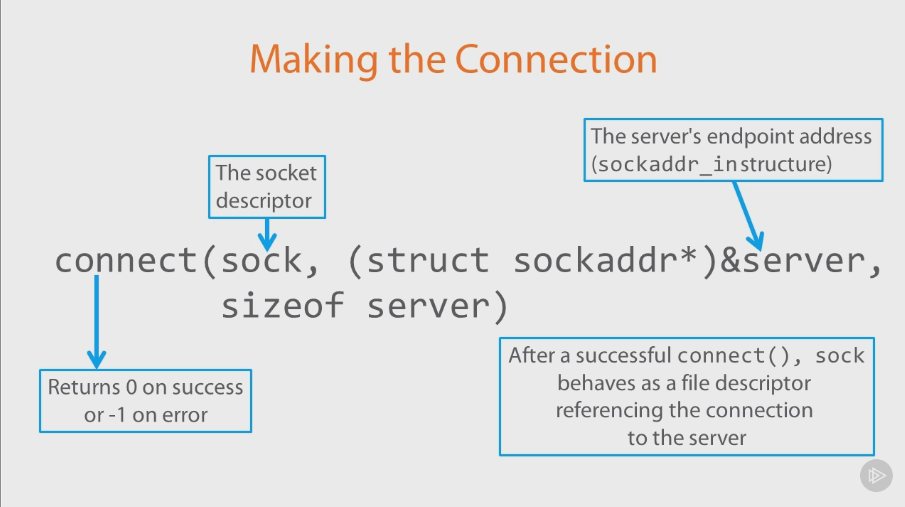
ושם נקליד close

אנו אמורים לקבל הודעה: connection closed

## Linux Network Programming

### Writing TCP-based Clients

#### : The Traditional Resolvers: gethostbyname() and getservbyname()

הקליינט רשאי לבצע bind לפורט. במידה והוא לא יעשה זאת, יבחר עבורו פורט אוטומטית (בדרך כלל אפשרות מועדפת).

# ICMP

שני סוגים של ICMP

Query ו Error

לדוגמא. קיבלתי את הודעתך בהצלחה.

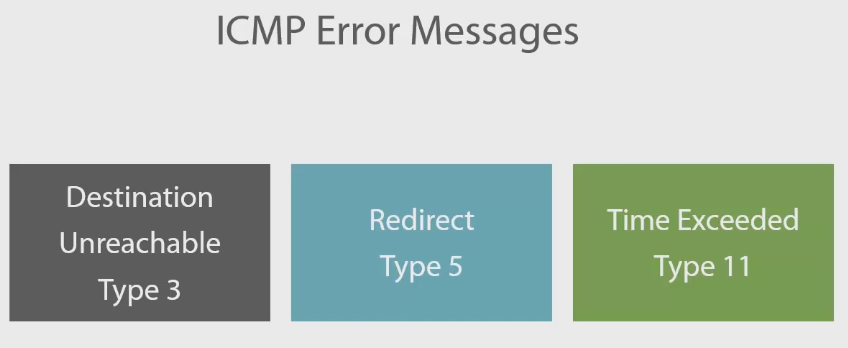
לא הצלחתי להעביר את הודעתך ליעדה משום כך וכך.

שני סוגי Query.

Time, Echo

לכל סוג הודעת ICMP יש מספר בתחום 0-255 אשר מזהה אותה.

לדוגמא, אלה שלש סוגי תשובות שגיאה:



# Linux commands

פקודות שונות

|  |  |  |
| --- | --- | --- |
| קונפיגורצית רשת |  | Ip addr show |
| default gateway |  | Ip route |
| **- get list of all network interfaces** |  | **netstat –i** |
| **the routing table** |  | **netstat –r** |
| **– translate ip to name and vice versa** |  | **host** |
|  |  | **id** |
| -  list all groups that a user is in |  | **groups** |
|  |  | **Who** |
| **The command w on many Unix-like operating systems provides a quick summary of every user logged into a computer,[1] what each user is currently doing, and what load all the activity is imposing on the computer itself. The command is a one-command combination of several other Unix programs: who, uptime, and ps -a.** |  | **W** |
| **Show list of last logged in users** |  | **Last** |
|  |  | sudo useradd –m Orit  sudo passwd Orit |
| הוספת משתמש לקבוצה קיימת |  | usermod –a –G secret-group Orit |
| מחזיר את רשימת ההתקנים המותקנים כולל mount-point |  | df - h |
| רשימת ההתקנים אף אם אינם מותקנים |  | lsblk |
|  | t tcp  n don’t translate ports  l listening only | netstat |
| List partitions |  | fdisk –l /dev/sda |
|  |  |  |

LPI: Linux Essentials (010-150)

The Linux Operating System : Networking

### Security and File Permissions : Controlling User Accounts

/etc/shadow

/etc/passwd

**/etc/group** file -  list all users groups.

Ls –l output: