

מדריך

רשתות
לטכנאי PC
ולמנהלי רשת

מהד' 4

דורון סיון

שמות מסחריים

שמות המוצרים והשירותים המוזכרים בספר הינם שמות מסחריים רשומים של החברות שלהם. הוצאת הוד-עמי עשתה כמיטב יכולתה למסור מידע אודות השמות המסחריים המוזכרים בספר זה ולציין את שמות החברות, המוצרים והשירותים. שמות מסחריים רשומים (registered trademarks) המוזכרים בספר צוינו בהתאמה.

הודעה חשובה

בנוסף, קרא בעיון את המבוא לספר זה.

ספר זה מיועד לתת מידע אודות מוצרים שונים. נעשו מאמצים רבים לגרום לכך שהספר יהיה שלם ואמין ככל שניתן, אך אין משתמעת מכך אחריות כלשהי.

תוכן הספר וההפניות לספרים, לתוכנות, לאתרים ולמקורות מידע המוזכרים בו מסופקים "כמו שהם (as is)". השימוש בכל אלה הוא על אחריותו הבלעדית של המשתמש. הוצאת הוד-עמי והמחבר אינם אחראים כלפי יחיד או ארגון עבור כל אובדן או נזק ישיר או עקיף, אשר ייגרם, אם ייגרם, מהשימוש בספר ו/או בתוכנות ו/או באתרים ו/או כל מקור מידע או תוכנה המוזכרים בספר, ובכלל זה (רשימה חלקית): הפרעה במתן שירות, אובדן מידע, אובדן זמן, אובדן רווח וכד'.

המשתמש רשאי להשתמש בתוכנות המוזכרות בספר ו/או לפנות לאתרים ו/או למקורות מידע אחרים על אחריותו. כל אלה הם בבעלות ובאחריות החברות המייצרות, משווקות ומציגות אותם. הוד-עמי והמחבר אינם גובים תשלום עבור השימוש בתוכנות ובמידע ממקורות אחרים המוזכרים בספר. הוד-עמי והמחבר אינם מספקים תמיכה בהתקנה ו/או ההפעלה של התוכנות ו/או בגישה לאתרים ומידע אחר. מחלקת התמיכה בהוצאת הוד-עמי תגיש עזרה רק עבור מקרים של אי בהירות של הסבר בספר או שיבוש דפוס. כל שאלה לגבי תוכנה ו/או אתר ו/או מקור מידע כלשהם יש להפנות אל מפתח/יוצרי/משווקי התוכנה ו/או אל בעלי האתרים ו/או מקורות המידע.

הוצאת הוד-עמי והמחבר עשו כל מאמץ שתוכן הספר יהיה אמין ושלם. עם זאת, ההוצאה והמחבר אינם טוענים לאמינות ולשלמות של התכנים המוצגים בספר זה, ובמיוחד דוחים כל אחריות, ובכלל זה טענה להתאמה של הנאמר בספר למקרה ספציפי כלשהו. לא ניתן ליצור או להרחיב אחריות על ידי מידע שיווקי ו/או פרסומי כלשהו. ייתכן שההצעות ו/או ההמלצות הניתנות בספר לא יתאימו לכל מצב ומקרה. הספר משווק ונמכר תוך הבנה שההוצאה והמחבר אינם מספקים שירותים שונים הכרוכים בשימוש בספר, אלא לשם הבנת הכתוב ותיקון שיבושי לשון. לקבלת שירות מקצועי יש לפנות אל בעלי המקצוע בתחום. הן ההוצאה והן המחבר אינם אחראים לכל אובדן או נזק ישיר או עקיף, אשר ייגרם, אם ייגרם, מהשימוש בספר ו/או בתוכנות ו/או באתרים ו/או כל מקור מידע או תוכנה המוזכרים בספר. אין בכוונת ההוצאה ו/או המחבר להמליץ או להעדיף תוכנה ו/או אתר ו/או מקור מידע כלשהם. רק המשתמש הוא שיחליט כיצד לנהוג על פי המוצג בספר. המשתמש צריך להיות ער לעובדה שאתרי האינטרנט הינם דינמיים ועלולים להיסגר, לשנות את התכנים שלהם וכד'. ההוצאה והמחבר אינם אחראים לשינויים אשר עלולים לחול באתרים המוזכרים בספר, ועל כן להיות שונים ממה שהוצג בספר.

אין להשאל ו/או לעשות שימוש מסחרי ו/או להעתיק, לשכפל, לצלם, לתרגם, להקליט, לשדר, לקלוט ו/או לאחסן במאגר מידע בכל דרך ו/או אמצעי מכני, דיגיטלי, אופטי, מגנטי ו/או אחר - בחלק כלשהו מן המידע ו/או התמונות ו/או האיוורים ו/או כל תוכן אחר הכלולים ו/או שצורפו לספר זה, בין אם לשימוש פנימי או לשימוש מסחרי. כל שימוש החורג מציטוט קטעים קצרים במסגרת של ביקורת ספרותית אסור בהחלט, אלא ברשות מפורשת בכתב מהמוציא לאור.

מדריך

רשתות
לטכנאי PC
ולמנהלי רשת

מהד' 4

דורון סיון



עריכה ועיצוב: שרה עמיהוד, יצחק עמיהוד, מירי אלעני
עיצוב עטיפה: שרון רז

לשם שטף הקריאה כתוב ספר זה בלשון זכר בלבד. ספר זה מיועד לגברים
ונשים כאחד ואין בכוונתנו להפלות או לפגוע בציבור המשתמשים/ות.

(C)

כל הזכויות שמורות

הוצאת הוד-עמי בע"מ

ת.ד. 6108 הרצליה 46160

דואר אלקטרוני: info@hod-ami.co.il

אתר אינטרנט: www.hod-ami.co.il

הודפס בישראל אפריל 2007

All Rights Reserved

HOD-AMI Ltd.

P.O.B. 6108, Herzliya

ISRAEL, 2007

מסת"ב 965-361-376-6 ISBN

הספר מוקדש בחום ואהבה לאשתי דליה
ולילדיי עופר, נעה ועמית

תוכן עניינים מקוצר

25	מבוא
27	פרק 1: ניהול רשתות תקשורת
149	פרק 2: TCP/IP
225	פרק 3: נתבים ורכזות
331	פרק 4: LINUX
431	פרק 5: Windows 2003
587	פרק 6: תוספות וחידושים בשרתי Windows
599	אינדקס

תוכן עניינים

25 **מבוא**

27 **פרק 1: ניהול רשתות תקשורת**

28 מהי רשת תקשורת ומהם המודלים התומכים בה

28 שרת מרכזי

28 רשת שוויונית (Peer To Peer)

29 דוגמאות לשירותי רשת ועבודה מול לקוחות

32 היתרונות בהתקנת רשת תקשורת

33 עיבוד מרכזי (רשת מרוכזת)

33 עיבוד מבוזר (רשת מבוזרת)

34 רשתות בעלות תשתיות שונות

35 מודל שבע השכבות – הצורך בתקינה והכרה של גופים בינלאומיים

37 מבנה מודל שבע השכבות

38 השכבה הפיסית (1) – Physical Layer

38 טופולוגיות פיסיות

38 Bus – אפיק

39 Star – כוכב

40 Ring – טבעת

41 Mesh – סריג

41 ציוד תקשורת

41 ציוד לחיבור ברשת

42 כרטיסי רשת

42 מודם

42 Repeater – משחזר

43 רכזות פסיביות

44 רכזות אקטיביות (Hubs)

44 רכזות מיתוג (Switch)

44 שידור ספרתי או שידור אנלוגי

46 Amplitude Modulation – AM

46 Frequency Modulation – FM

46 Phase Modulation – PM

47	סיכום
47	ריבוב
48	BroadBand
49	BaseBand
50	T1/E1 מרכב
50	PDH מרכב
50	SDH מרכב
51	ריבוב WDM
52	Data Link Layer – (2) שכבת עורק הנתונים
52	LLC
53	Media Access Control – MAC (בקרת גישה לתווך)
54	משטרי גישה לתווך
55	כתובות
57	Network Layer – (3) שכבת הרשת
57	Logical Network Address
58	שיטות מיתוג
58	Circuit Switching – מיתוג מעגלי
59	Packets Switching – מיתוג מנות
60	שיטות לגילוי מסלולי ניתוב
61	פקודות שימושיות
64	Transport Layer – (4) שכבת התעבורה
68	הסבר על TCP ו-UDP
71	Session Layer – (5) שכבת השיח
72	Presentation Layer – (6) שכבת התצוגה
72	Application Layer – (7) שכבת היישום
73	סיכום מודל שבע השכבות
75	סקירת פרוטוקולים נפוצים
75	מודל Internet
77	שיטות חיווט ותקנים אלוטטיים
77	Coax Cable – כבל קואקס
79	דוגמה לשימוש בכבל קואקס לחיווט לפי תקן 10Base2
80	(TP) Twisted Pair – זוג שזור
80	UTP – כבל שזור לא מסוכך
81	STP – כבל שזור מסוכך
82	סיב אופטי
82	אופן העברת האותות
83	Multimode

83 Single Mode
84 סיכום
85 מדיה אלוטית
85 Radio Wave – גלי רדיו
86 Micro Wave – גלי מיקרו
87 Infrared – אינפרא-אדום
88 תקשורת אלוטית – יישום בשטח
89 Bluetooth
90 Wi-Fi
91 נקודות חשובות בהתקנת הרשת
92 Access Point – רכזת מיתוג אלוטית
92 כרטיסי רשת
93 Routers – נתבים אלוטיים
93 WiMAX
94 פרוטוקולים להעברת נתונים ברשת מקומית
94 Ethernet
96 Ethernet-ב חיווט
96 10Base תקני חיווט
96 10Base2
97 100BaseT
100 100BaseTx Fast Ethernet
101 Gigabit Ethernet
101 10 Gigabit Ethernet
101 מבנה המנה ב-Ethernet
102 Token-Ring
104 החיווט ב-Token Ring מתבצע בעזרת רכזת MAU (Multi station Access Unit)
105 תחזוקה והתמודדות עם תקלות
106 Ethernet
106 Token-Ring
106 סיכום
107 רכזות מהירות ומתגים
109 רכזות – הסבר מתקדם
110 רשתות עירוניות (MAN) ומרחביות (WAN)
111 Fiber Distributed Data Interface – FDDI
113 Asynchronous Transmission Mode – ATM
114 תהליך יצירת קשר
115 שילוב ATM ברשתות LAN

116	קו נל"ץ – נקודה לנקודה
117	ספרנת
118	רשת מיתוג מנות – X.25
120	מבנה מסגרת
122	ממסר מסגרת – Frame Relay
123	מבנה המסגרת
123	אופן הפעולה
124	התקנת רשת Frame Relay
126	תקשורת לוויינים
126	MPLS
129	IPVPN
130	טכנולוגיות חיבור של משתמשים מרוחקים
130	ADSL
131	קצת מידע טכני
132	חיבור ADSL דרך תשתית אנלוגית
132	חיבור ADSL דרך תשתית ISDN
133	טכנולוגיית כבלים
133	אופן הפעולה
134	פרוטוקול התקשורת ISDN
136	חיבור לרשת ISDN
136	Basic Rate Interface – BRI
138	Primary Rate Interface – PRI
138	התקנה פיסית של הרשת
138	ניתוח המערכת
139	התקנת הכרטיסים
142	פרוטוקולי קישור שימושיים באינטרנט והכרת VPN
142	PPP
142	שימוש בתעלות (Tunnels)
144	VPN
148	SSL
149	פרק 2: TCP/IP
150	מודל OSI בהשוואה למודל TCP/IP
151	פירוט פרוטוקולי TCP/IP
151	פירוט היישומים בכל שכבה
152	שכבת היישום
152	דוגמאות לפרוטוקולים השייכים לשכבת היישום

152	Host to Host	השכבה
158	Internet-	שכבת ה-
160		שכבת הגישה לרשת
160		כתובות IP
161		Class A
161		Class B
162		Class C
163		קצת על חישובים בינאריים
165	Subnet Mask	(מסכת רשת משנה)
166	Default Gateway	
169		חלוקה פנימית של הרשת
169	Mask	(מיסוך)
172		דוגמה 1
175		דוגמה 2
179		כתובות פיסיות וכתובות לוגיות
181		השימוש בכתובות פנימיות
183	TCP/IP	תחזוקה ב-
184		סקירת מושגים ושרתים
184	IP Address	
185	Subnet Mask	
185	Default Gateway	
185	DNS	
185	Host	
186	WINS	
187	LMHOSTS	
187	DHCP	
189	NT/9x	סדר האתחול ברשת (המשתמשת בפרוטוקול TCP/IP)
189	Windows XP/2000/2003	סדר האתחול ברשת
193		רשימת פקודות
193	PING	
193	ARP	
194	NETSTAT	
194	NBTSTAT	
195	IPCONFIG	
196	TRACERT	
196	ROUTE	
196	NSLOOKUP	

196	נוהל בדיקות
196	שלב ראשון
197	שלב שני
199	IPv6
200	הכרת בסיס הספירה ההקסדצימלי
201	שיטת הכתובות של IPv6
203	Aggregatable Global Unicast Addresses
203	כתובות חיצוניות – Global
204	כתובות לשימוש פנימי
205	אופן הקצאת הכתובות לארגונים תוך שימוש בשדה NLA
205	דוגמה לחלוקה של שדה TLA
206	אופן חלוקת הרשת הארגונית לתת-רשתות תוך שימוש בשדה SLA
206	הגדרת כתובות עבור Interface
207	אופן הקצאת כתובות לפי תקן IEEE EUI-64
208	שימוש ב-Multicast
209	סיכום קידומות
210	עבודה מול הנתב
211	תרגום שמות לכתובות IP
212	ניתוב בעולם IPv6
212	פרוטוקולי ניתוב דינמיים פנים ארגוניים
213	פרוטוקולי ניתוב דינמיים בין ארגונים
213	תאימות בין מערכות
213	סוגי תאימות לכתובות
214	אם המערכת תומכת בשתי התבניות, כיצד הכתובות מתקשרות לתבניות אלו? ...
215	התייחסות ל-Windows
216	Vista/Longhorn
217	חזרה על נושא הכתובות עם התייחסות להגדרות
217	ארבע סוגי כתובות מסוג Unicast
217	צפייה בהגדרות
219	כתובת Anycast
219	דוגמה לקישור בין עמדות תוך שימוש ב-ISATAP
223	דוגמה לניתוח פלט של הפקודה IPConfig
225	פרק 3: נתבים ורכזות
226	נתבי כבלים/ADSL
228	נתבי Cisco
228	מבנה הנתב

230	סוגי כבלים
231	נוהל האתחול של הנתב
233	הכרת נוהל השימוש בנתב
235	Privileged Mode
237	Global Configuration Mode
237	Interface Configuration Mode
238	SubInterface Configuration Mode
239	תחזוקה
239	סדר איתור ואתחול IOS
239	סדר הטענת קבצי קונפיגורציה
240	הודעות שגיאה
240	דריסת סיסמה
241	טבלת מצבי Configuration Register
243	עבודה מול שרת TFTP
243	שחזור מערכת הפעלה
245	עבודה עם Notepad-1 Terminal
247	Cisco Discovery Protocol – CDP
247	סיכום נוהל העבודה
248	הגדרות ניתוב
248	ניתוב סטטי
250	ניתוב דינמי
250	הכרת הפרוטוקולים
251	סקירת פרוטוקולים
252	עדיפויות בין פרוטוקולים
253	נהלי הגדרות כלליים
254	הגדרת שימוש בפרוטוקול RIP
255	פקודות שימושיות
257	מה ההבדל בין RIP לבין RIP2 ?
257	הודעות מערכת
257	הגדרת שימוש בפרוטוקול IGRP
258	בקרה
259	הגדרת שימוש בפרוטוקול OSPF
260	תמיכה בסוגי רשתות
261	אימות בפרוטוקול OSPF
261	תקלות ובעיות
261	פרוטוקול הניתוב EIGRP
262	הגדרות

263	Access List
267	Telnet-ל התייחסות
267	NAT
268	הגדרות עבור NAT
268	הגדרות עבור Pool
269	PAT
270	סקירת מושגים בתחום WAN
270	השכבה הפיסית
271	שכבת ערוק הנתונים
271	PPP
272	שלבי יישום PPP בנתבי CISCO
273	הגדרות שרת הגישה עבור Frame Relay
274	הצעדים הדרושים להגדרות Frame Relay
276	הגדרות Frame Relay ברשת עם מספר נתבים
278	ניטור ובקרה
278	דוגמה מפורטת לחיבור הנתב לרשת פנימית ולרשת Frame Relay
279	שלב ההגדרות
282	סיכום המידע על נתב סיסקו
284	סקירת נתבי CISCO
284	תמיכה בסוגי LAN
284	תמיכה ברשתות מרחביות (WAN)
285	התקנת נתב CISCO 1005 צעד אחר צעד
286	התקנת הנתב
286	חזית הנתב
287	גב הנתב
287	חיווט
289	שלב ההתקנה
289	הכנת הנתב לאתחול
290	אתחול הנתב והגדרות
292	בדיקה
293	הגדרות של Switch
293	הגדרות
295	מצבים אפשריים של מתג
295	אופן עבודת המתג
297	Spanning Tree Protocol – STP
298	הגדרת רכזת
299	הגדרות מתקדמות

299	שריון כתובת MAC קבועה בפורט מסוים ברכות.
300	הוספת מרכיב אבטחה
301	רשת מקומית וירטואלית – VLAN
304	הגדרות הנתב בעת שימוש ב-VLAN
306	איפוס סיסמה ברכות
306	ביצוע Mirror לפורט
307	הגדרת נתבים בעזרת הכלי הגרפי ConfigMaker
310	אבטחת מידע
311	שמירה
312	שרטוט רשת
313	סיכום ביניים
313	שרתי Windows 2003 כנתבים
315	עדכון נתבים
316	ניתוב דינמי
317	התקנת נתב על שרת 2003
319	OSPF
320	ניתוב סטטי
321	הגדרת ניתוב סטטי בדרך גרפית
324	סינון תעבורה
324	DHCP ברשת המכילה נתבים
326	בעיות אופייניות
329	עדכון מספר השער בעמדה

331..... פרק 4: LINUX

333	Red-Hat
333	SuSE
334	דרישות החומרה להתקנת מערכת לינוקס
335	תהליך ההתקנה של מערכת Red-Hat 9
337	תהליך ההתקנה של מערכת SuSE 9.1
337	טעינה כפולה עם Windows
338	סקירה כללית של המערכת
341	גישה להתקנים
342	כוננים קשיחים
346	מערכות הקבצים
346	ממשק משתמש גרפי – GUI
347	זיהוי חומרה
348	סקירת פקודות

348	מידע אודות הפעלה נכונה של הפקודות
349	פקודות שכוחות
349	פקודות הקשורות למשתמשים
349	פקודות הקשורות למערכת הקבצים
351	יצירת חשבונות משתמש וקבוצה
354	כניסה למערכת
355	יצירת חשבונות באמצעות הממשק הגרפי
356	עבודה כמשתמש אחר
357	הקניית זכויות של ביצוע פעולות System למשתמש
357	הגבלת נפח האחסון של המשתמש
358	מערכת ההרשאות
359	צבעי הקבצים והתיקיות
360	קביעת המשתמשים שההרשאות מתייחסות אליהן
360	chown
360	Chgrp
361	אופן הגדרת הרשאות
361	שיטת מספור בינארית
363	הגדרת הרשאות בעזרת אותיות
363	הקצאת הרשאות בדרך גרפית
365	מתגים ופקודות בנושא קבצים ותיקיות
366	הדפסה
366	הפעלה דרך שורת הפקודה
366	הפעלה דרך הממשק הגרפי
368	התקנת תוכנות
368	rpm
369	תחזוקת rpm
370	התקנה מהתקליטור
370	התקנה דרך הממשק הגרפי של המערכת
370	tar.gz
371	deb
372	העורך VI
373	Script (סקריפט)
376	Process (תהליך)
378	קביעת עדיפות
379	מודולי תוכנה
381	תקשורת במערכת לינוקס
381	שילוב TCP/IP בלינוקס

381	תחזוקה מרוחקת על ידי SSH
382	הקצאת כתובת IP למחשב
385	הגדרת המחשב כנתב
385	הגדרת מסלולי ניתוב
385	הגדרת המחשב כנתב
385	הגדרה זמנית כנתב, עבור ResHat ועבור SuSE
385	הגדרה קבועה כנתב
386	שיתוף קבצים ותיקיות – NFS
386	אופן העבודה
386	בצד של המחשב שמשותף משאב
387	בצד של המחשבים האחרים (לקוחות)
388	קישור בין סביבת לינוקס לסביבת Windows
389	גישה מעמדת לינוקס אל עמדת Windows
389	גישה מעמדת Windows אל עמדת לינוקס
392	תמיכה ביישומי Microsoft
392	Run Level –1 Services
394	יצירת קישורים
397	הפקודה chkconfig
398	פריצת סיסמת Root ב- Red-Hat וב-SuSE
399	Apache – שרת האינטרנט
400	הפעלת השירות
401	עריכת ההגדרות
401	שרת FTP
403	ביצוע פקודות דרך ממשק טקסט
403	שינוי מאפייני ברירת מחדל
404	שירותי רשת
404	שרת DHCP
405	שרת DNS
406	IPtables – חומת אש
409	איפוס חוקים והורדת השירות
409	שמירת ההגדרות
410	התוכנה YaST למשתמשי SuSE
411	הממשק Webmin
414	סדר אתחול המערכת
415	LILO
417	GRUB
418	תחזוקה

418	יצירת דיסקט אתחול
418	יצירת דיסקט הצלה / טעינה מרשת
419	הודעות הקשורות ל-LILO
420	בעיות בתצוגה
420	kernel panic הודעות
420	עדכון Kernel
421	כיצד לעדכן את ה-Kernel
425	צפייה בקבצי היומן של המערכת
427	Logrotate
429	נספח פקודות
431	פרק 5: Windows 2003
432	<u>Active Directory –1 Windows 2003 Server</u>
432	פירוט הגרסאות ודרישות החומרה
433	סיבות למעבר ממערכת Windows 2000
434	שיפורים של Active Directory
434	התקנה או שדרוג של המערכת
435	שדרוג Windows 2000 ל- Windows 2003
435	תאימות עם גרסאות Windows קודמות
435	התקנת שרת חדש
436	שדרוג Windows Server 2003 לבקר Domain
439	Domain Modes
440	אופן המעבר בין המצבים השונים
441	Active Directory
442	מבנה Active Directory
444	הבנת מבנה Active Directory
446	Trust
447	חמשת התפקידים של Active Directory
447	תפקידים ברמת Forest
448	תפקידים ברמת Domain
448	העברת תפקידים בין בקרי דומייין (DC)
449	העברה בעזרת ntdsutil
449	הגדרת משתמשים וקבוצות
451	Organizational Unit
452	יצירת חשבון משתמש
457	יצירת קבוצה
459	סוגי קבוצות

461	שיתוף משאבים
461	שיתוף – Share
462	הרשאות Security
464	שילוב הרשאות Share
465	פרסום דרך Active Directory
467	DFS
469	הגבלת נפח דיסק בעזרת Quotas
471	Terminal Server
472	התקנת Terminal Services
474	התקנת Terminal Services Client Software
476	הגדרת תוכנות ב-Terminal Services והרצתן
476	חיבור מרוחק
479	גיבויים
481	סוגי גיבוי
484	Group Policy
490	שיקולי הורשה, ובדיקת ה-GPO האפקטיבי
492	הרשאות GPO
493	קביעת מדיניות עבור עמדות ישנות
494	עדכונים אוטומטיים בעזרת WSUS
496	כלי ניהול ותחזוקה
496	ביצועים – Performance
497	ניהול משאבי המחשב – Computer Management
500	פעולות תחזוקה הקשורות לאתחול המערכת
504	שירותי רשת
504	ניתוב
505	הוספת שירותי תקשורת
506	DHCP
508	DNS
510	חיבור עמדת XP
512	<u>שרת דואר Exchange 2003</u>
512	הקמה ואבטחה
513	דרישות חומרה להתקנה
513	דרישות תוכנה להתקנה
514	התקנת המערכת (שרת + לקוחות)
516	קצת על Outlook
518	ניהול שרת Exchange
519	השרתים הלוגיים המותקנים

521	יצירת תיקיות ציבוריות
522	Mailbox Store
526	יצירת חשבון למשתמש
528	חשבון דואר לקבוצה
531	Recipient
532	גישה לחשבון הדואר
536	גיבוי המערכת ותחזוקה שוטפת
537	בקרה על המערכת
540	חלוקת סמכויות
542	אבטחה
543	מערכת Exchange 5.5 בהשוואה ל- Exchange 2003
545	ניהול תיקיות
546	שדרוג המערכת
547	<u>שרת האינטרנט IIS 6.0</u>
548	WWW
550	Web site
550	Performance
551	Home Directory
552	Directory Security
553	FTP
557	יצירת אתר מאובטח
562	<u>ניטור רשת וגיבויים</u>
562	ניטור רשת
563	SNMP
563	ארכיטקטורת הניהול
564	מבנה מערכת סטנדרטית
566	בניית איור התואם את מצב המחשוב בארגון
566	תחזוקה
568	גיבויים
569	תוכנת גיבוי מול ניהול אמצעי אחסון
570	ומה עם זמן הגיבוי?
570	ארכיטקטורות גיבוי
570	אחסון מחובר ישירות – DAS
570	אחסון מחובר לרשת – NAS
571	רשתות אחסון אזוריות – SAN
571	iSCSI
572	Cluster

572	זמינות גבוהה על ידי שכפול
572	Snapshot
573	גיבוי חם וגיבוי קר
573	סבב מדיה
574	סיכום השיקולים המנחים ברכישת ארכיטקטורת הגיבוי בארגון
574	תוכנות גיבוי מקצועיות כוללות שלושה מרכיבים
574	דוגמה לנוהל גיבוי מקובל בארגונים קטנים
576	כתיבת סקריפטים ב-VBScript
577	אופן ההרצה של הסקריפט
577	מעט רקע – הפונקציה
578	פונקציות ואובייקטים נפוצים
580	חיבור לכונני רשת
580	דוגמה – מיפוי כונן רשת
581	דוגמה – הסרת מיפוי כונן רשת
581	הוספת אובייקטים ב-Active Directory
581	הוספת OU
582	מחיקת OU
582	יצירת חשבון משתמש
583	מחיקת חשבון משתמש
583	צירוף משתמשים לקבוצה
584	הסרת המשתמש doron מקבוצת support
584	קביעת מפקח ל-OU
585	העברת משתמשים בין OU
585	צפייה ברשימת חברי הקבוצה

פרק 6: תוספות וחידושים בשרתי Windows

587	R2
589	SP2
590	Longhorn
597	סיכום

אינדקס

מבוא

תחום התקשורת ההולך ומתרחב, הוביל ליצירת מקצוע בעל התמחות מיוחדת בשם "מנהל רשת". כמנהל רשת עליך להתמצא בנושאים רבים, החל מתשתיות הרשת וכלה במערכות הפעלה ויישומי רשת.

ספר זה עוסק בתחום הרשתות ומנסה לתת מענה לחלק גדול מצרכי מנהל הרשת בארגון, ולאנשי מקצוע אחרים בתחום המחשוב.

הספר מחולק לשלושה חלקים, שבכל אחד מהם יש חלוקה נוספת לפי נושאים:

⊙ **תשתית** - הכרת סוגי חיווט, ציוד תקשורת ושיקולים בבחירת החומרה. הפרק הראשון מכסה את הנושא ועל כן הוא פרק חיוני בספר. הוא כולל, מלבד היכרות מעמיקה עם תשתיות שונות, גם מידע חשוב בתחום רכזות ונתבים. בנושאים אלה עוסקים פרקים 1 ו-2.

⊙ **TCP/IP** - ידע מעמיק בפרוטוקול TCP/IP הינו כיום תנאי הכרחי לעבודה השוטפת. בפרק השני תכירו לעומק את מגוון הפרוטוקולים המאוגדים תחת פרוטוקול האם הקרוי TCP/IP, כולל התקן החדש שקרוי IPv6. בנוסף ניתן בפרק 3 הסבר מפורט על ציוד התקשורת של חברת Cisco. הידע שיירכש בלימוד זה יוכל לסייע בהכנה למבחן ההסמכה היוקרתית CCNA של Cisco. בנושאים אלה עוסק פרק 3.

⊙ **מערכת הפעלה לרשת** - איזו מערכת הפעלה לבחור, Windows או Linux, וכיצד ניתן לשלב ביניהן? בפרקים 4, 5 ו-6 ניתן הסבר על מערכות הפעלה אלו ועל שרתים מסוגים שונים, כמו שרתי קבצים וקבצי דואר. בפרקים אלה יש הסברים על נושאים נוספים, כמו Active Directory וכתובת סקריפט. ניתן גם ללמוד על חבילות התוכנה הנפוצות של לינוקס הקרויות RedHat ו-SuSE. פרק 4 יכול לשמש בסיס טוב להכנה למבחן MCP היוקרתית של Microsoft על שרת Windows 2003. פרק 5 יכול לשמש בסיס טוב להכנה למבחן ההסמכה הבינלאומי LPI עבור Linux. פרק 6 עוסק בחידושים ובגרסאות החדשות של שרתי Windows.

בספר זה ניסיתי להעניק ללומד המקצועי ולקורא המתעניין מניסיוני הרב כמרצה בתחום התקשורת וכאיש שטח. הנושאים מועברים בסגנון של הרצאות והקשרים שתואמים את הפעילות המעשית, והשתדלתי למסור את כל המידע שדרוש לדעתי לבחירת הציוד והמערכות, ולתחזוקתן. על כן, לצד מידע תיאורטי עשיר ניתן למצוא בספר מאות תמונות מסך שיוכלו לסייע בהמחשת ההסברים ולפני המגע הישיר במערכות החומרה והתוכנה של עולם התקשורת.

תודה להורי, לאה וויליאם סיטבון, על השקעתם בי; תודה לשרון סיטבון על ההגהה בנושא VBScript; תודה לרון סיון על הסיוע בסעיף הגיבויים.

דורון סיון

הארות והערות ניתן לשלוח לכתובת: doronsivan@walla.co.il

ספר זה שייך לסדרה בת שלושה ספרים:

- ⊙ מדריך חומרה ותוכנה לטכנאי PC, מהד' 4. 2006.
- ⊙ מדריך רשתות לטכנאי PC ולמנהלי רשת, מהד' 4 (ספר זה).
(ספר קודם: המדריך השלם לטכנאי PC - רשתות תקשורת, מהד' 3.)
- ⊙ מדריך אבטחת מידע והגנה מפני האקרים. 2006.

בספר תמצא הפניות לספרים בשם מקוצר: "ספר החומרה" ו"ספר האבטחה". הכוונה לספרים המפורטים כאן, כולם בהוצאת הוד-עמי.

פירוט על ספרי ההוצאה תוכל למצוא באתר הוד-עמי www.hod-ami.co.il

5

Windows 2003

פרק זה עוסק בשרתים שונים של Windows, דוגמת Domain Controller, שרת אינטרנט, שרת דואר ועוד. כמו כן תהיה התייחסות לתחזוקת השרתים ולביצוע פעולות באופן אוטומטי בעזרת סקריפטים.

מפאת כמות החומר, חולק הפרק ל-5 תת-פרקים, אשר סדר הלימוד והעיון בהם אינו מקרי, אלא מומלץ על ידי המחבר עבור הקורא והלומד.

⊙ החלק הראשון עוסק ב- Windows 2003 Server וכולל לימוד מעמיק של **.Active Directory**

⊙ החלק השני עוסק בשרת הדואר **Exchange 2003**.

⊙ החלק השלישי עוסק בהכרת שרת האינטרנט שמגיע עם השרת.

⊙ החלק הרביעי עוסק בבקרת רשתות והכרת כלי גיבוי מתקדמים.

⊙ בחלק החמישי תלמד לבצע פעולות שוטפות ברשת תוך שימוש ב-**VBScript**.

תוכל למצוא בסעיפים השונים התייחסויות למערכות החדשות של Microsoft Exchange 2007.

Active Directory – Windows 2003 Server

מערכת הפעלה זו הוכרזה רשמית באפריל 2003. היא מקובלת מאוד וכנראה תהיה בשטח זמן רב, עד להתבססות של מערכת ההפעלה החדשה של מיקרוסופט. למערכת Windows 2003 יש ארבע גרסאות (ולמעשה חמש, כפי שתראה בהמשך). שלוש ממשיות את הקו שננקט במערכת Windows 2000 והרביעית מיועדת לתפקיד שרת Web בלבד.

תחילה נכיר את הגרסאות הקיימות ואת הסיבות שבעטיין כדאי לשדרג את גרסת 2000 לגרסה זו. אחר כך נכיר את המערכת באופן מעמיק כדי לרכוש את המיומנויות הדרושות להתקנתה בארגון.

פירוט הגרסאות ודרישות החומרה

דרישות החומרה אשר מוצגות להלן הן המינימום המומלץ על ידי היצרנית Microsoft. דרישות אלו מספיקות להתקנת מערכת ההפעלה, אך כדי לעבוד איתה בפועל רצוי להתקין את מערכת ההפעלה במערכת מחשב חזקה בהרבה.

גרסאות Windows Server 2003 הן:

Windows Server 2003 Standard Edition ☉

מיועדת לארגון קטן, או לשימוש כשרת בעל תפקיד מוגדר, כגון: שרת קבצים והדפסה או שרת אבטחה. דרישות המינימום המומלצות הן מעבד Pentium III 550MHz, זיכרון RAM בן 256MB, נפח דיסק פנוי לפחות 1.5GB. מערכת הפעלה זו תומכת בעד 4 מעבדים. כמוכן שדרישות אלה נראות כיום מגוחכות, פנטיום 3 לא נמכר יותר ולא מומלץ שרת עם פחות מ- 2GB.

Windows Server 2003 Enterprise Edition ☉

מיועדת לארגון בינוני עד גדול וליישומים "כבדים" כגון: שרת דואר, מסחר אלקטרוני, מסדי נתונים וכדומה. לפיכך, המערכת קיימת הן בגרסת 32bit והן בגרסת 64bit. דרישות המינימום המומלצות כאן הן מעבד Pentium III 733MHz, זיכרון RAM בן 256MB (הזיכרון המקסימום לגרסה 32bit הוא 32GB, ולגרסה 64bit הוא 512GB). מערכת הפעלה זו תומכת בעד 8 מעבדים.

Windows Server 2003 Datacenter Edition ☉

מיועדת למערכות גדולות ומורכבות, בהן נדרש טיפול בבסיסי מידע גדולים ומיחוסת חשיבות רבה למהירות הביצוע וליציבות המערכת. דרישות המינימום כאן הן מעבד Pentium III 733MHz, זיכרון RAM בן 1GB (המקסימום לגרסה 32bit הוא זיכרון בן 64GB, ולגרסה 64bit (מעבדי איטניום) – 512GB). מערכת הפעלה זו תומכת במינימום 8 מעבדים ועד 64 מעבדים. נפח מינימלי של דיסק קשיח 1.5GB למערכת 32bit ו- 2GB למערכת 64bit.

Windows Server 2003 Web Edition ☉

מיועד לאחסון אתרי אינטרנט, יישומי Web ושירותי XML. מומלץ מעבד Pentium III 550MHz, זיכרון RAM בן 256MB, נפח דיסק פנוי לפחות 1.5GB. המערכת תומכת בלוחות של עד 2 מעבדים.

הערה!



הגרסה החמישית היא Windows Small Business Server 2003 (SBS). זהו שרת Standard Edition אשר מצורפים לו שרתים ארגוניים אחרים (דואר, פקס, SQL וכדומה) ואשר מיועד למלא צרכים של ארגונים בגודל קטן עד בינוני. לשרת זה יש מספר מוגבל של משתמשים שיכולים להתחבר אליו בו-זמנית. הוא מגיע בשתי מהדורות, Premium-1 Standard, אשר ההבדלים ביניהן הם מספר השרתים הנוספים המצורפים בחבילה.

סיבות למעבר ממערכת Windows 2000

המערכת Windows 2003 יציבה ומהירה יותר מגרסת 2000. מבחינת אנשי IT הוסיפה Microsoft למערכת יכולות ניהול חדשות שמקלות על ניהול השרת. בין הכלים והיכולות החדשות, נמצא את RSoP (Resultant Set of Policy) שמאפשר למנהל הרשת לבחון את השפעת ה-GPO (Group Policy).

שירות נוסף הוא Volume Shadow Copy Restore, אשר מאפשר למנהל הרשת שמירת מידע קריטי שניתן יהיה לגשת אליו למטרות שחזור. ניתן להחיל את השירות גם על עמדות Windows XP Professional, בתנאי שיותקן בהן Volume Shadow Copy Service Client For XP, שנמצא בתקליטור ההתקנה של Windows Server 2003. השירות החדש יכול להתבצע באופן אוטומטי במהלך עבודה על הקבצים, והדבר מאפשר גיבוי נוח שיכול לסייע במקרים רבים של אבדן מידע. בנוסף, נוהל הגיבוי מצטבר (Incremental), רק השינויים מועברים, ולכן אין העמסה מיותרת בשרת וברשת.

נקודה נוספת, היא היכולת לבצע את רוב עבודות התחזוקה משורת הפקודה, כפי שמקובל על מנהלי רשתות לינוקס ו-UNIX. מנהלי רשתות Windows רגילים להשתמש בתפריטים, אולם לעבודה משורת הפקודה יתרונות רבים: דרושים פחות משאבי מערכת וקל להתחבר למחשב מרוחק ולתחזק אותו. Microsoft קראה לכלי זה Windows Management Instrumentation Command Line, אולם אל תיתן לשם הארוך לבלבל אותך, הממשק נוח מאוד ואף ניתן להרחבה על ידי סקריפטים מוכנים.

אבטחת המידע לא נשכחה ולא הוזנחה. תמיכה מלאה בתקן 802.1X מעניקה אימות שרק עמדות מורשות יכולות להתחבר למערכת. יתרון זה יבוא לידי ביטוי ברשתות מקומיות (LAN) אלחוטיות, אולם יאפשר גם בקרת גישה למערכות מחוטות. התמיכה בהתקנים אלחוטיים שופרה באופן משמעותי.

כמו כן בוצע שדרוג במערכת IIS. מערכת IIS 6.0 תומכת ביישומי Web ושירותי XML Web. בנוסף, המערכת מבודדת בין האתרים המאוחסנים בשרת כדי שתקלה באחד מהם לא תשפיע על האחרים. הדבר תורם כמובן ליציבות ולביצועים טובים יותר.

שיפורים של Active Directory

- ⊙ ניתן לערוך מאפיינים של כמה משתמשים בו-זמנית.
- ⊙ ניתן לעבוד בשיטת 'גרור ושחרר' (Drag and Drop), לדוגמה לגרור משתמש לקבוצה.
- ⊙ הוספת כלי ניהול ל- Active Directory משורת הפקודה. דוגמאות יוצגו בהמשך.
- ⊙ הוספת בקרי Domain באמצעות Backup Media.
- ⊙ Global Catalog – כזכור, כאשר משתמש נכנס למערכת (מבצע login), המערכת מאתרת את ה- Global Catalog, כדי לקבל מידע אודות החברות של המשתמש בקבוצה מסוג Universal. דבר זה עלול להשפיע על הביצועים בארגון גדול, שבו פעולת הכניסה נפרסת על פני כל הרשת המרחבית (WAN). במערכת החדשה נשמר מידע זה ברמת ה- Domain Controller, ולכן משך פעולת הכניסה יהיה קצר יותר.
- ⊙ ניתן לשנות שם של בקר Domain. השינוי יכול לכלול NetBIOS name ושל DNS name בכל הרמות. לכן, למרות שהדבר אפשרי הוא עדיין מסובך ולא מומלץ, מכיוון שניאלץ לבצע הגדרות רבות בהמשך.
- ⊙ יצירת Forest Trusts. פעולה זו מסייעת בפישוט ניהול של מערכות גדולות, שיש בהן מספר Forests. זה נושא חשוב כיום בעידן של מיזוגים בין חברות.
- ⊙ גמישות בעבודה מול הסכמה (schema), אשר מתבטאת במספר אופנים. לדוגמה, נטרול מאפיינים שאינם רלוונטיים.

טיפ



במערכות NT הוענקה, כנריות מחול, הרשאת Anonymous Users - Read. כדי לשמור על תאימות נוחה, מומלץ, הן Windows 2000 והן Windows 2003, לצרפם לקבוצה Pre Windows 2000 Compatible Access. בזמן התקנת Active Directory (כלומר, dcpromo), ניתן לבחור זאת על ידי בחירה באפשרות Permissions Compatible With Pre-Windows 2000 Server Operating System. אם יש בעיה עם יישום מסוים, צריך את הקבוצה Everyone מאותו Domain אל הקבוצה Pre Windows 2000 Compatible Access Security.

התקנה או שדרוג של המערכת

ניתן לבצע התקנה חדשה, אך עם זאת, במקרה של מערכת קיימת, סביר שתוצאה לבצע שדרוג. כך ניתן לחסוך בהתקנה מחדש של יישומים, יצירת משתמשים והגדרות הניהול.

שדרוג Windows 2000 ל- Windows 2003

מערכת Windows 2003 כוללת ארבע גרסאות שרת, לעומת שלוש הגרסאות הקיימות בסביבת Windows 2000 Server. לפיכך, אפשרויות השדרוג הן מקבילות, למעט גרסת Web Edition, שאינה קיימת במערכת ההפעלה Windows 2000.

אפשרויות השדרוג הן:

ל- Windows Server 2003	מ- Windows 2000 Server
Standard Edition	Windows 2000 Server
Enterprise Edition	Windows 2000 Advanced Server
Datacenter Edition	Windows 2000 Datacenter Server
Web Edition	לא קיימת גרסת Web

תאימות עם גרסאות Windows קודמות

ניתן להפעיל עמדות Windows 95/98/NT, אבל מומלץ להתקין בהן את תוכנת הלקוח DSCClient, שניתן למצוא בתיקייה Clients שבתקליטור ההתקנה של Windows. אם תוכנת הלקוח לא תהיה מותקנת בעמדות אלו, המערכת תיראה בעיניהם כ- Windows NT Domain. נקודה זו חשובה גם ברשתות שפועלות בסביבת Windows 2000. תוכנת הלקוח הזו משדרגת את יכולת האבטחה של העמדה, ומאפשרת לעמדה להכיר ב- Active Directory. נקודה זו חשובה מאוד למנהל רשת בארגונים גדולים. ללא תוכנה זו, עמדה הפועלת בסביבת Windows 95/98 תוכל לגשת למשאבים רק ב-Domain שלה וב-Domains שנמצאים עמה ביחסי אמון (Trust). כל הרעיון של Domain Tree אינו מובן להן, ואין להן גישה למשאבים שנמצאים בו. לכן, אם העמדות הן מסוג Windows 2000/XP, התמיכה קיימת בהן באופן טבעי, ועבור האחרות - חובה להתקינה.

התקנת שרת חדש

עבור לתיקייה I386 שבתקליטור ההתקנה והקלד את הפקודה winnt. אם במערכת מותקן בקר SCSI, עליך להקיש F6 בתחילת ההתקנה (כאשר בשורת המצב של תוכנית ההתקנה מופיעה הדרישה לכך), ולוודא שהדרייבר הנכון עבור בקר SCSI זה כבר מוגדר. אם טרם נעשה, עליך להתקין את הדרייבר באופן ידני. לאחר שתבחר בהתקנה ותסכים לתנאי הסכם השימוש בתוכנה, תתבקש לבחור את המחיצה להתקנת מערכת ההפעלה. אם בחרת מחיצה מסוג FAT, תופיע השאלה אם להמיר את המחיצה למערכת הקבצים NTFS. במקרה של שרת בארגון, מומלץ לאשר את ההמרה, אך אם זו התקנה ביתית ובמערכת זו מותקנת מערכת הפעלה נוספת, כגון Windows 98 שאינה תומכת ב-NTFS, אתה עשוי להצטער על בחירה זו, מכיוון שלא תהיה למערכת ההפעלה הקודמת (Windows 98 בדוגמה שלפנינו) גישה למחיצה זו.

חשוב לדעת שלא ניתן להתחרט. המעבר לאחור (מ-NTFS חזרה ל- FAT/FAT32) נעשה רק על ידי פירמוט מחדש של המחיצה. בהמשך תהליך ההתקנה תבוצע סקירה למרכיבי המחשב, כאשר אתה עשוי להיות מופתע מהכמות האדירה של דרייברים המובנים (Built In) שמותקנים במערכת.

בהמשך תהליך ההתקנה, תתבקש לציין שם משתמש, שם ארגון וסיסמת מנהל מערכת. לאחר שתציין את אזור הזמן יגיע תור רכיבי הרשת. בשלב זה יאוטר כרטיס הרשת ותציין את ה- Domain שתשייך אליו את המערכת החדשה. אם זהו Domain חדש, השאר אותו ברמת שרת רגיל שחבר בקבוצת עבודה (Workgroup).

בסיום התהליך יבוצע שוב אתחול, והפעם תיכנס למערכת לאחר שתזדהה בתור Administrator.

שדרוג Windows Server 2003 ל-Domain

זו פעולה חשובה, ולכן אפרט זאת. יש הבדל עקרוני בין שרת לבין DC (Domain Controller). מבחינות רבות השרת הוא עמדה לכל דבר. השרת מבצע כניסה ל-Domain, בדיוק כמו XP. ההבדל היחיד הוא בכך שהוא מסוגל להריץ יישומים ש-XP אינו יכול להריץ. כדי ליצור Domain, אחד השרתים חייב לתפקד כבקר Domain. לשם כך לוקחים שרת ומבצעים פעולה שנקראת קידום (Promotion) למעמד של בקר Domain, וכך 'נבנה' שם הפקודה dcpromo. לאחר שתבצע זאת לפי ההנחיות בהמשך, תצטרך לעבור בין כל העמדות ולציין בהגדרות TCP/IP את כתובת שרת DNS, שבדרך כלל תהיה כתובת השרת שהוא DC (כלומר, המחשב שקודם למעמד בקר Domain). לאחר מכן תצטרך להגדיר דרך מאפייני המחשב שלי את המחשב כחבר ב-Domain (פעולה הנקראת Join to Domain). רק אז המחשב יוכל להצטרף ל-Domain בעת האתחול.

במסכים הבאים מופיעים בפירוט שלבי הפיכת שרת לבקר Domain.

לאחר שתקליד דרך **Start** ← **Run** את הפקודה dcpromo, יופיע אשף ההתקנה. השאלה הראשונה תהיה האם זהו Domain חדש, או שמערכת זו מצטרפת ל-Domain קיים.

Active Directory Installation Wizard

Domain Controller Type
Specify the role you want this server to have.

Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?

Domain controller for a new domain
Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.

Additional domain controller for an existing domain