فهرست

مقدمه ـ معرفی : آمادگی برای عیب‌یابی ۱۱

بخش اول : مرتب‌سازی منزل ۱۵

فصل ۱ ـ مقایسه تلفنی : آشنایی با مفاهیم مقدماتی شبکه ۱۷

کارت‌های رابط شبکه ۱۸

تهاجم MAC ۱۹

مسیریاب‌ها ۲۱

پروتکل‌ها ۲۳

اهمیت TCP/IP ۲۳

DLC ۲۵

IPX/SPX ۲۵

بسته‌ها ۲۶

داخل اسم چیست؟ ۲۸

DNS ۲۸

WINS ۳۰

خلاصه ۳۰

کارگاه ۳۱

پرسش و پاسخ ۳۱

آزمون ۳۲

پاسخ به سؤالات آزمون ۳۲

فصل ۲ ـ نمی‌توانید بیش از اندازه مستندات، پول یا سرگرمی داشته باشید ۳۳

راهبری یک مجموعه شبکه‌ای بد ۳۳

فواید مستندسازی ۳۳

نقشه‌های منطقی/عملیاتی ۳۴

نقشه‌های فیزیکی ۳۵

برچسب‌زدن کابل‌ها و ابزارها ۳۸

مستندسازی جزئیات/توضیحات ۴۱

خلاصه ۴۱

کارگاه ۴۲

پرسش و پاسخ ۴۲

آزمون ۴۲

پاسخ به سؤالات آزمون ۴۲

بخش دوم : استراتژی‌های عیب‌یابی «جعبه سیاه» ۴۳

فصل ۳ ـ روش دلتا: شناسایی تغییر شبکه ۴۵

فاکتور انگشت شصت ۴۵

مواظب فروشنده باشید ۴۶

عوامل خارجی ۴۷

نسبت ریسک به سود ۴۸

خلاصه ۴۹

کارگاه ۴۹

پرسش و پاسخ ۴۹

آزمون ۵۰

پاسخ به سؤالات آزمون ۵۰

فصل ۴ ـ روش ناپلئون: تفرقه‌بیانداز ـ و ـ حکومت‌کن ۵۱

بازی اعداد ۵۱

واترلوی عملیات شبکه متوقف است ۵۲

جستجو در بخش ۵۴

تقسیم کار ۵۶

خلاصه ۵۸

کارگاه ۵۹

پرسش و پاسخ ۵۹
آزمون ۵۹
پاسخ‌های سؤالات آزمون ۶۰

فصل ۵ ـ روش خیابان سسمی : یکی از چیزها شبیه بقیه نیست ۶۱
سرویس‌دهنده‌ها و مسیریاب‌ها ۶۱
اشیاء کاربری ۶۲
آن را ساده نگهدارید ۶۳
هدف‌گیری ۶۴
خلاصه ۶۸
کارگاه ۶۹
پرسش و پاسخ ۶۹
آزمون ۶۹
پاسخ سؤالات آزمون ۶۹

فصل ۶ ـ روش SOAP : دادهٔ درونی، دادهٔ ظاهری، تجزیه و تحلیل و طرح ۷۱
دکتر شبکه ۷۱
فقط واقعیت‌ها ۷۲
SOAP در دنیای واقعی ۷۳
آیا با یک ویروس سروکار داریم؟ ۷۴
مشاوره ۷۴
خلاصه ۷۶
کارگاه ۷۷
پرسش و پاسخ ۷۷
آزمون ۷۷
پاسخ سؤالات آزمون ۷۸

فصل ۷ ـ روش سیمون ساده ۷۹
یک نفر قبلاً مشکل شما را حل کرده است ۷۹
جستجو برای پشتیبانی در تمامی محل‌های صحیح ۸۰
مشکلی تکنیکی در راه انجمن اتفاق افتاد ۸۳
بلیط بازی ۸۵
همبستگی ۸۶
خلاصه ۸۹
کارگاه ۸۹
پرسش و پاسخ ۸۹
آزمون ۹۰
پاسخ به سؤالات آزمون ۹۰

بخش سوم : مواظبت و تغذیهٔ اسباب شبکه ۹۱

فصل ۸ ـ «مبانی سخت‌افزار»: چگونه استادکار سخت‌افزار شویم؟ ۹۳
چیزهایی که باید در مورد PC بدانید ۹۳
BIOS ۹۴
PC های نشاندار در مقابل PC های عمومی ۹۴
نصب و دعا ۹۵
تمیزسازی ۹۶
جلسهٔ تعویض ۹۷
کابل همان شبکه است ۹۹
استفاده از مولتی‌متر ۱۰۰
اتمام سوخت در بزرگراه اطلاعات ۱۰۱
ویندوز ۱۰۲
System Resource Meter ۱۰۳
کاربران غیر ویندوز ۱۰۵
یونیکس ۱۰۵
نِت‌ور ۱۰۷
خلاصه ۱۰۷
کارگاه ۱۰۸
پرسش و پاسخ ۱۰۸
آزمون ۱۰۸
پاسخ به سؤالات آزمون ۱۰۸

فصل ۹ ـ مبانی اِترنِت ۱۰۹
تبعیت از قوانین: تا هنگامی‌که در شبکهٔ ما زندگی می‌کنید... ۱۰۹

تصادمها ۱۱۰
قاب‌دار و تقسیم‌شده ۱۱۱
سرعت اجرا ۱۱۲
اِترنِت ۱۰۰ مگابیتی ۱۱۲
کارناوال کابل‌کشی ۱۱۳
پایین، پایین، پایین ۱۱۶
خلاصه ۱۱۷
کارگاه ۱۱۸
پرسش و پاسخ ۱۱۸
آزمون ۱۱۸
پاسخ به سؤالات آزمون ۱۱۸

فصل ۱۰ ـ مبانی حلقه ـ نشانه ۱۱۹

قواعد را دنبال کنید : به اشتراک گذارده
و لذت ببرید! ۱۲۰
بلای خطا : هنگامی‌که NAUN شخص، محل ۱۲۱
یا چیز شناخته‌شده‌ای نیست ۱۲۱
انواع خطا ۱۲۲
تحلیل‌گران نشانه ۱۲۳
دیدگاه فیزیکی ۱۲۵
اندازهٔ بسته‌ها ۱۲۶
خرابی ۱۲۶
خلاصه ۱۲۷
کارگاه ۱۲۸
پرسش و پاسخ ۱۲۸
آزمون ۱۲۸
پاسخ به سؤالات آزمون ۱۲۸

فصل ۱۱ ـ مبانی شبکه در ویندوز ۱۲۹

بومی‌سازی ۱۳۰
NetBEUI ۱۳۰
حوزهٔ بزرگ ۱۳۳
سنگ‌نبشته‌های TCP/IP ۱۳۶
DHCP ۱۳۶
تحلیل نام در TCP/IP ۱۳۸
پیکربندی ایستگاه‌کاری ۱۴۱
Network در Control Panel ۱۴۱
مقیدسازی ۱۴۳
فرمانروایی و تسلط ۱۴۶
winipcfg ۱۴۶
دستورات اطلاعاتی ۱۴۷
net ۱۴۷
نظارت بر سیستم ۱۴۸
خلاصه ۱۵۰
کارگاه ۱۵۰
پرسش و پاسخ ۱۵۰
آزمون ۱۵۰
پاسخ به سؤالات آزمون ۱۵۱

فصل ۱۲ ـ مبانی شبکه در یونیکس ۱۵۳

دیدگاه کلی ۱۵۳
سرویس‌گیرنده/سرویس‌دهنده ۱۵۳
پیکربندی یونیکس ۱۵۴
دیمون‌های دوست‌داشتنی ۱۵۵
برقراری سوکت ۱۵۹
بازی اسامی ۱۶۱
nslookup ۱۶۱
مکان قطبی ۱۶۲
خلاصه ۱۶۳
کارگاه ۱۶۴
پرسش و پاسخ ۱۶۴
آزمون ۱۶۵
پاسخ به سؤالات آزمون ۱۶۵

فصل ۱۳ ـ مبانی شبکه در نت‌ور ۱۶۷

شبکهٔ NDS ۱۶۷
مبانی Das ۱۶۹
NLM ها ۱۶۹
سکوت فهرست ۱۷۲
«دوستتان»، ABEND ۱۷۴

ناظر بزرگ شاهد است ۱۷۵
ترس به خود راه ندهید؛ Monitor اینجا است! ۱۷۷
مشکلات پروتکلی ۱۷۹
IPX/SPX ۱۸۰
سرویس‌دهنده یا مسیریاب ۱۸۰
TCP/IP ۱۸۱
بازی TCPCON ۱۸۱
خلاصه ۱۸۲
کارگاه ۱۸۳
پرسش و پاسخ ۱۸۳
آزمون ۱۸۳
پاسخ به سؤالات آزمون ۱۸۴

فصل ۱۴ ـ مبانی مسیریاب و سوئیچ ۱۸۵
تئوری و عملی ۱۸۵
تئوری مسیریاب ۱۸۸
جداول مسیریابی ۱۸۹
دو میلی ثانیه از زندگی یک بسته ۱۹۰
مسیریاب‌های پویا ۱۹۱
مسیریابی در صلح و صفا: پروتکل‌های مسیریابی ۱۹۲
وارسی مسیرها ۱۹۴
تئوری سوئیچ ۱۹۵
توقف و سوئیچ ۱۹۶
اخبار انتشاری ۱۹۶
درخت‌های نجات‌بخش ۱۹۷
تنهٔ درختان ۱۹۷
خلاصه ۱۹۹
کارگاه ۱۹۹
پرسش و پاسخ ۱۹۹
آزمون ۲۰۰
پاسخ به سؤالات آزمون ۲۰۱

فصل ۱۵ ـ مبانی دیوار آتش و سرویس‌دهندهٔ پروکسی ۲۰۳
رموز فوق سری ۲۰۳
TCP در مقابل UDP ۲۰۴
مسیریاب‌های فیلترکننده بسته ۲۰۵
تقویت فیلتر بسته ۲۰۶
نوع پروکسی ۲۰۸
تنها نرم‌افزار اضافه کنید ۲۰۹
پیکربندی پروکسی ۲۰۹
مشکل پروکسی ۲۱۰
همان بازی نام: DNS و دیوارهای آتش ۲۱۱
خلاصه ۲۱۲
کارگاه ۲۱۳
پرسش و پاسخ ۲۱۳
آزمون ۲۱۴
پاسخ به سؤالات آزمون ۲۱۴

بخش چهارم: در خندق‌ها ۲۱۵

فصل ۱۶ ـ ثبات عمیق، زیباست: نجات از مشکل ۲۱۷
استانداردسازی دستی ۲۱۸
عصر ابزار قدرتمند ۲۱۹
الگوهای کاربری ۲۱۹
اسکریپت‌های ورود به سیستم در سطح کاربر ۲۲۰
اسکریپت‌های ورود به سیستم گروهی/سازمانی ۲۲۰
اسکریپت‌های کمکی ۲۲۱
پروفایل‌های میکروسافت ۲۲۲
ارسال انبوه ۲۲۳
سیاست محافظت: ابزار سرپرستی خودکار ۲۲۵
سیاست‌ها ۲۲۵
برنامه‌های کاربردی در یک نگاه ۲۲۶

خلاصه ۲۲۷
کارگاه ۲۲۷
پرسش و پاسخ ۲۲۷
آزمون ۲۲۸
پاسخ به سؤالات آزمون ۲۳۰

فصل ۱۷ ـ از کجا شروع کنم؟ ۲۳۱
تعیین حوزه ناقص : «در آغاز ...» ۲۳۱
شیرجه به درون جزییات ۲۳۲
جمع‌بندی یک راه حل : تکنیک‌های اولیه
مدیریت تماس تلفنی ۲۳۳
مشکلات پروتکلی ۲۳۴
TCP/IP ۲۳۴
IPX/SPX ۲۳۹
خلاصه ۲۴۰
کارگاه ۲۴۰
پرسش و پاسخ ۲۴۰
آزمون ۲۴۱
پاسخ به سؤالات آزمون ۲۴۲

فصل ۱۸ ـ «افراد مختلف بسیار در همسایگی شما»: عیب‌یابی عمقی کاربردی ۲۴۳
تعاریف سرویس‌ها ۲۴۳
سرویس‌های فایل و چاپ ۲۴۳
محاسبات سرویس‌گیرنده/سرویس‌دهنده ۲۴۴
مشکلات فایل و چاپ ۲۴۵
نمی‌توانم چاپ کنم! ۲۴۶
انبوه فایل ۲۵۱
سرویس‌گیرنده/سرویس‌دهنده ۲۵۸
وضعیت آدرس سوکت ۲۵۸
سرویس‌های متبسم ۲۵۹
خلاصه ۲۶۴
کارگاه ۲۶۴
پرسش و پاسخ ۲۶۴
آزمون ۲۶۵
پاسخ به سؤالات آزمون ۲۶۶

فصل ۱۹ ـ عیب‌یابی اینترنت/اینترانت ۲۶۷
تعاریف ۲۶۷
اینترانت = داخلی ۲۶۷
آشفتگی مجازی ۲۶۸
شناسایی اینترنت ۲۶۸
هفت سال آزگار... ۲۷۲
در اینجا دوباره Ping می‌کنم ۲۷۲
مشکلات DNS ۲۷۳
مشکلات مسیریابی ۲۷۸
عیب‌یابی در اینترانت ۲۸۰
سرویس‌دهندهٔ وِب ۲۸۰
مشکل در پُست الکترونیکی؟ ۲۸۲
مشکلات شماره‌گیری ۲۸۳
خلاصه ۲۸۴
کارگاه ۲۸۵
پرسش و پاسخ ۲۸۵
آزمون ۲۸۵
پاسخ به سؤالات آزمون ۲۸۶

فصل ۲۰ – عیب‌یاب‌های شبکه تنها می‌خواهند سرگرمی داشته باشند ۲۸۷
پیداکردن دیوار آتش ۲۸۸
مطالبی در مورد Socks ۲۸۹
AOL Instant Messenger ۲۹۱
AOL NetMail ۲۹۱
ICQ ۲۹۲
RealPlayer ۲۹۳
استراتژی بازی ۲۹۵
خلاصه ۲۹۵
کارگاه ۲۹۵
پرسش و پاسخ ۲۹۵
آزمون ۲۹۶
پاسخ به سؤالات آزمون ۲۹۶

فصل ۲۱ ـ برایم از شبکه‌ات بگو : تحلیل‌گران شبکه ۲۹۷
تحلیل‌گر شبکه چیست؟ ۲۹۷
عملکرد عمومی ۲۹۸
شبکه‌درمانی : تکنیک‌هایی برای استفاده از تحلیل‌گر ۳۰۲
بسته‌های فیلترشده ۳۰۲
تسخیر عمومی ۳۰۷
تجزیه و تحلیل مناسب ۳۰۸
عتیقه‌جات کاربردی ۳۰۹
تشخیص ایستگاه ۳۰۹
حلقه شکسته ۳۱۰
محدودیت‌ها و راه‌حل‌ها ۳۱۱
خلاصه ۳۱۳
کارگاه ۳۱۳
پرسش و پاسخ ۳۱۳
آزمون ۳۱۴
پاسخ به سؤالات آزمون ۳۱۴

فصل ۲۲ ـ ابزار مدیریت شبکه ۳۱۵
ناظر بزرگ مشغول نظارت است ۳۱۵
MIB ۳۱۶
RMON ۳۱۸
مدیریت شبکه غیراستاندارد ۳۱۹
مراجع واقعی ۳۲۱
خلاصه ۳۲۲
کارگاه ۳۲۲
پرسش و پاسخ ۳۲۲
آزمون ۳۲۳
پاسخ به سؤالات آزمون ۳۲۴

فصل ۲۳ ـ شبکه کُند است! دریافت پاسخی صریح به سؤالی مبنایی ۳۲۵
عوامل محدودکننده ۳۲۵
عرض‌باند و توان عملیاتی ۳۲۶
تأخیر ۳۲۶
کارایی پروتکل و برنامه کاربردی ۳۲۷
محدودیت‌های سرویس‌دهنده ۳۲۹
دو بار اندازه‌گیری، یک بار برش ۳۲۹
سربار اشتراک ۳۳۰
اتمام سوخت سرویس‌دهنده ۳۳۰
خط پایه ۳۳۲
ایجاد خط پایه به صورت خودکار ۳۳۲
تلاش انجام کار به صورت دستی ۳۳۳
خلاصه ۳۳۶
کارگاه ۳۳۷
پرسش و پاسخ ۳۳۷
آزمون ۳۳۷
پاسخ به سؤالات آزمون ۳۳۸

فصل ۲۴ ـ مهندسی معکوس شبکه ۳۳۹
ردیابی کابل ۳۳۹
کشف TCP/IP ۳۴۰
پیکربندی مسیریاب ۳۴۰
سرویس‌دهنده‌ها ۳۴۲
انجام خودکار برای افراد ۳۴۴
مرور TCP/IP ۳۴۵
اکتشاف IPX/SPX ۳۴۵
خلاصه ۳۴۸
کارگاه ۳۴۸
پرسش و پاسخ ۳۴۸
آزمون ۳۴۹
پاسخ به سؤالات آزمون ۳۴۹

ضمیمه ـ واژه‌نامه ۳۵۱

فهرست راهنما ۳۷۱

مقدمه

معرفی: آمادگی برای عیب‌یابی

مثل جراحی که برای عمل جراحی قلب آماده می‌شوند، متبحران شبکه نیز باید با سالها آموزش و تجربه آماده حمله به مشکل شبکه‌ای پیچیده باشند. ممکن است آنها ابزار پیچیده و گرانقیمتی را به‌کار برده به پروتکل‌های شبکه به عنوان زبان دومشان صحبت کنند. خیلی ترسناک است!

با این وجود، برای حل بیشتر مشکلات شبکه‌ای، نیازی به مدرک علوم فضایی نیست. در واقع، همان طور که خودتان بدون تماس با آقای زیراکس تجمع کاغذ در دستگاه فتوکپی را پاک می‌کنید، یا کارتریج تونر را تعویض می‌نمایید؛ به همان شکل مشکل سیستم پُست الکترونیکی خود را هنگام بروز خرابی برطرف می‌سازید. چرا نه؟ شما هوش دارید و با داشتن درک مقدماتی از نحوه کارکرد این مؤلفه‌ها، می‌توانید مثل هر کس دیگری به نتیجه‌های منطقی دست یابید. می‌توانید با مراجعه کمتر به مشاور خود، در هزینه‌ها صرفه‌جویی کنید.

آیا استادان شبکه برای حل بیشتر مشکلات شبکه‌ای به ابزار گرانقیمتی نیاز دارند؟ در واقع، خیر. کسانی که به چنین ابزاری بیش از هوش و قدرت استنتاج خود تکیه می‌کنند، عیب‌یاب‌های خیلی خوبی نیستند. تمایل آنها به جای ارائه راه حل‌های نیازمندیهای شما، روی جمع‌آوری ابزار جالب تمرکز یافته است.

بیشتر حرفه‌ای‌های شبکه‌ای واقعاً خوب، قادر هستند به واسطه تواناییهای بصیرتی و حس استنتاج قوی و قدیمی خود، به خوبی چنین ابزاری را به‌کار بیندازند. و از آن گذشته، بیشتر اوقات آنها حتی به وسیله گرانقیمتی برای عیب‌یابی مسأله نیاز ندارند. چرا؟ زیرا آنها اصول عیب‌یابی «جعبه سیاه» را درک کرده‌اند، اصولی که شما می‌توانید در بخش دوم این کتاب، «استراتژی‌های عیب‌یابی جعبه سیاه» فرابگیرید. البته، این افراد اصول پایه‌ای شبکه‌سازی کامپیوتر را نیز می‌دانند، اما این اصول هم در واقع کاملاً ساده هستند. خبر جدیدی است، چرا که بدان معناست که بیشتر اوقات برای گرفتن نتایج مشابه نیازی به صرف ۱۰۰۰۰ دلار برای خرید تحلیل‌گر شبکه نیست.

عیب‌یابی جعبه سیاه

عیب‌یابی «جعبه سیاه» اشارت دارد بر تلقی‌کردن یک سیستم پیچیده به مجموعه‌ای از سیستم‌های ساده‌تر. هر قطعه یا جز در «جعبه سیاه اسرارآمیز»، جعبه‌ای است که درون خود چیزهای مخفی‌ای دارد که باعث می‌شوند آن طور که می‌بینیم رفتار کند. این چیزهای مخفی، هنگامی که از «سطح بالا» کار عیب‌یابی را صورت می‌دهید، اهمیتی ندارند. یعنی، اهمیت نمی‌دهید چرا یکی از قطعات سیستم به صورتی که هست، رفتار می‌کند؛ مطلب مهم چیزی است که رخ می‌دهد. بسیار شبیه به برنامه‌نویسی شیءگرا، عیب‌یابی جعبه سیاه نیز به شما اجازه می‌دهد کار بیشتری را در زمان کمتری به انجام برسانید، چرا که دیگر نگران جزئیات کوچک نخواهید بود!

برای مثال، با اینکه ممکن است هیچ چیز در مورد داخل دستگاه پمپ بنزین اتومبیل ندانید (و اهمیتی هم ندارد

که بدانید)، با این وجود ممکن است به آن به عنوان دلیل خرابی‌های گهگاه اتومبیل خود ظنین باشید. از آنجا که آن را یک جعبه سیاه تلقی می‌کنید، با جایگزین‌کردن یک پمپ بنزین سالم شک خود را بررسی کنید، و اگر سیستم اتومبیل به صورت مناسب کارکرد، آنگاه متوجه می‌شوید که علت خرابی چه بوده است. بعد از یکی دو روز درست کارکردن ماشین، پی می‌برید که در واقع پمپ بنزین علت خرابی بوده است ـ بدون آنکه بدانید اجزا داخلی آن چگونه کار می‌کنند. عیب‌یابی جعبه سیاه روشی است برای افراد پرمشغله که بتوانند تقریباً هر نوع مشکل قابل تصوری را حل نمایند.

حتی اگر به فروشنده‌ای اتکا کنید (این کار را خواهید کرد؛ حتی حرفه‌ای‌ها هم این کار را می‌کنند!)، با دانستن آنکه چه کار می‌کنید، می‌توانید تحلیل مشکلات‌تان را سرعت بخشد. تصور کنید که با نصب‌کننده‌های شبکه‌ای و عیب‌یاب‌های حرفه‌ای ـ یعنی «فروشنده» ـ شریک شده‌اید. می‌توانید مشکلات ساده را حل کنید و مثل قهرمانان به نظر برسید و کارهای خیلی سخت را برای آنان باقی بگذارید.

نسبت کاربران به افراد حرفه‌ای و کارآزموده شبکه بسیار پایین است، و خیلی اوقات یک نفر (شاید شما)، به عنوان عیب‌یاب شبکه غیررسمی و البته بدون پرداخت اضافی، وامانده خواهید شد. پس باید با تکنولوژی‌ها و تکنیک‌های مختلف کنار بیایید.



نکته : *البته، حتی اگر آنقدرها هم خوش‌شانس نباشید، این احتمال وجود دارد که کارتان به نحو گسترده‌ای به تواناییهای شبکه‌ای‌تان بستگی داشته باشد. چه شغل‌تان، مثل برنامه‌نویسی یا مدیریت اطلاعات کمکی به شبکه وابسته باشد و چه مثل مهندسی و پزشکی، این طور نباشد، این حقیقت وجود دارد که برای انجام کار خود به به‌اشتراک‌گذاری اطلاعات نیاز دارید. اگر بتوانید بیشتر مشکلات شبکه‌ای را خودتان حل کنید، می‌توانید در کارهای خود سرعت بسیار زیادی را به وجود آورید.*

آیا برای به‌وجودآوردن این حالت، باید خودتان به استادکار شبکه تبدیل شوید؟ مسلم است که نه. موضوعات و سطوحی از جزییات مطرح نشده در این کتاب وجود دارند که برای یک مدیر، طراح یا مهندس شبکه حرفه‌ای‌بودن، باید آنها را بدانید. اما جزییات برای کسی که می‌خواهد عیب‌یابی جعبه سیاه را انجام دهد، از اهمیت اساسی برخوردار نیستند و اشکالی ندارد که مخفی هم باقی بمانند ـ البته، تا اندازه‌ای که بتوانید به تبادل اطلاعات لازم با شخص مسؤول پشتیبانی شبکه پردازید، در این کتاب فراخواهید گرفت.

مفاهیم ساده ـ اما ـ قدرتمندی را خواهید دید که حرفه‌ای‌ها هم بر آنان متکی هستند. علاوه بر اصول شبکه، حتی حرفه‌ای‌ترین عیب‌یاب‌ها نیز به موارد زیر نیازمند است:

- مستندات محصول
- مستندات سایت
- کتب و لوازم اضافی
- توانایی مشاهده و استنتاج
- عیب‌یابی جعبه سیاه
- پشتیبانی سایر افراد

برای آنکه با سرعت به چارچوب کاری واژه‌های مصطلح در شبکه آشنا شوید، در فصل ۱ با «مقایسه تلفنی» آشنا خواهید شد. بعد از آن، به خوبی خواهید توانست با مؤلفه‌های شبکه کنار بیایید و راحت باشید؛ مهمتر از آن، اصول و واژگان اصلی شبکه را فراخواهید گرفت. این به شما اجازه می‌دهد روش جریان‌یابی یک مکالمه شبکه‌ای را از آغاز تا پایان درک کنید و شروع کنید به یادگیری و فهم آنکه چرا شبکه‌تان خراب شده است. اگر با اصول و اصطلاحات شبکه آشنایی دارید، می‌توانید از این قسمت صرف‌نظر کنید و یک‌راست به روشهای عیب‌یابی شیرجه بروید.

عیب‌یابی هر شبکه، به ویژه شبکه‌ای بزرگ، مثل حل یک معماست، اگر با اصول کارکرد شبکه آشنا باشید و بدانید که کدام قطعات به کدام دیگری بستگی دارند (بسیار شبیه آنکه در یک معمای جورجین قطعات کناری را در ابتدا جاسازی می‌کنید) و با روش بایسته جریان اطلاعات آشنا باشید، یافتن مشکل کار چندان سختی نخواهد بود. بعد از تعیین ناحیه‌ای کلی برای مشکل، می‌توانید از تکنیک‌های مقدماتی عیب‌یابی برای پیداکردن قطعه خاص مشکل‌زا بهره بجویید.

اجازه دهید معمایی واقعی که در عیب‌یابی به‌کار می‌آید، مطرح نمائیم. فرض کنید شما معلم هستید؛ مشکل‌تان این است که سه دانش‌آموز دارید که مشکلاتی را در کلاس ایجاد می‌کنند. احتمالاً دو تکنیک قدرتمند عیب‌یابی جعبه سیاه، «تفرقه بینداز ـ و ـ حکومت کن» و «روش دلتا» را به‌کار خواهید بست.

متوجه می‌شوید که یکی از دانش‌آموزان، تازه به این شهر آمده است و این تنها تغییری است که در کلاس‌تان، که قبلاً آرام بود، رخ داده است. او را با درنظرگرفتن آنکه وی سبب اصلی است از گروه جدا می‌کنید. با ایجاد فاصله از دو دانش‌آموز دیگر، متوجه می‌شوید که آشوب به نقطه دیگری از کلاس منتقل می‌گردد. پس به این ترتیب دانش‌آموز مذکور را به عنوان دلیل شلوغی شناسایی می‌کنید و دانش‌آموزان دیگر را از این فرض کنار می‌گذارید. از همین‌جا، مقداری تجربه برای مقابله با مشکلات شبکه برای خود اندوختید.

اجازه دهید مشکلی مشابه با مشکل کلاس درس را مورد بررسی قرار دهیم. فرض کنید افرادی برای نصب یک PC جدید به دفتر کارتان می‌آیند. آنها می‌آیند، نصب می‌کنند و همه چیز مرتب به نظر می‌رسد. روز بعد، هیچ کس نمی‌تواند نامه الکترونیکی خود را ارسال کند! یکی از آنان می‌گوید باید سرویس‌دهنده پُست الکترونیکی را از دوباره ساخت، اما شما هوشمندانه به این نکته توجه می‌کنید که تنها چیزی که از دیروز تغییر کرده، نصب PC جدید است. با اصرار شما PC جدید را از شبکه بیرون می‌برند و ناگهان همه چیز درست می‌شود. با انجام بررسی، مشخص می‌شود که کابل شبکه PC جدید، خرابی دارد و مشکل ایجادشده، در سرویس‌دهنده پُست الکترونیکی تأثیر می‌گذارد. کابل شبکه تعویض می‌شود. شما قهرمان شده‌اید و از خطرات بازسازی سرویس‌دهنده پُست الکترونیکی نیز جلوگیری کرده‌اید.

البته، همیشه به این راحتی نیست. بسیاری اوقات، تشخیص اینکه چه چیزی تغییر کرده یا حتی آنکه چه کسی تغییر را به وجود آورده مشکل است. متأسفانه، از آنجا که در شبکه همه چیزها به هم ارتباط دارند، هر چیزی می‌تواند منبع مشکل باشد. به دلیل آنکه همه چیزها در شبکه جای می‌گیرند، متهم‌کردن شبکه کار آسانی است. در واقع بسیاری اوقات، باید مشکلی را حل کنید که ارتباطی با شبکه ندارد!

کلام آخر این است، برای شروع عیب‌یابی هر مسأله به دانسته‌های کمی در مورد همه چیزها نیاز دارید. آن‌گاه کافی است این دانسته‌ها را به هم ربط داده و کار لازم برای حل مسأله را انجام دهید. و موفق هم خواهید شد!

بخش اول

مرتب‌سازی منزل

فصل ۱ : «مقایسه تلفنی» :
آشنایی با مفاهیم مقدماتی شبکه
فصل ۲ : «نمی‌توانید بیش از اندازه مستندات،
پول یا سرگرمی داشته باشید»

فصل ۱

مقایسه تلفنی: آشنایی با مفاهیم مقدماتی شبکه

تلاش برای درک قطعات و بخشهای سازنده شبکه‌ای کامپیوتری، حتی برای افرادی که در زمینه دیگری در کامپیوتر کارکشته هستند، می‌تواند با ترس همراه باشد. اگر از قبل با واژگان و مفاهیم شبکه آشنایی دارید، می‌توانید از مطالعه این فصل صرف نظر کنید و سراغ جاهای بزرگتر و بهتری بروید؛ در غیر این صورت، در اینجا راه خوبی برای ایجاد ارتباط با اصول تکنولوژی شبکه در اختیارتان قرار گرفته است.

مد نظر قراردادن وسیله‌ای که از قبل آن را می‌شناسید، روش خوبی برای یادگیری سریعتر است. یادگیری زبان ویژه کمک مؤثری است، اما حتی اگر بتوانید از سخنان تخصصی استفاده کنید، در صورت نداشتن چیزی مشابه که بتوانید واژه‌های جدید را با آن مقایسه نمایید؛ باز هم دچار ضعف خواهید بود.



اخطار : *مقایسه‌های واژه‌ای ذیل، نسبی هستند. آنها به صورت کامل با هم یکی نیستند. آگاه باشید که چنین تصوری را در ذهن خود ایجاد نکنید.*

بنابراین، ممکن است مورد توجه قراردادن این مطلب که شبکه‌های کامپیوتری بسیار شبیه به شبکه تلفنی عمومی هستند، به کمک‌تان بیاید. یا وجود تفاوت‌های بسیار در باطن، شباهتهای کافی در ظاهر وجود دارند که به شما کمک کنند مفهوم خوبی از چگونگی کارکرد واقعی شبکه را درک نمایید. در فرضیه‌مان، فراخوانی‌های شبکه‌ای بسیار شبیه به مکالمات تلفنی هستند. شکل ۱-۱ مقایسه‌ای کلی بین یک شبکه اطلاعاتی و سیستم تلفنی را نشان می‌دهد. همچنین، در این بخش فهرستی مرجع ارائه می‌شود:

واژهٔ شبکه‌ای	معادل تلفنی
NIC (کارت رابط شبکه[1])	تلفن منزل شما.
رسانه (کابل) شبکه[2]	خط تلفن.
آدرس	شماره تلفن (167.195.162.5 ترسناکتر از 1-212-818-5555 نیست).
مسیریاب[3] یا دروازه[4]	تجهیزات دفتر مرکزی شرکت تلفن که «کُدهای ناحیه‌ای» مختلف را متصل می‌سازد.

1- Network Interface Card 2- Network Media 3- router
4- gateway

ادامهٔ جدول صفحه قبل

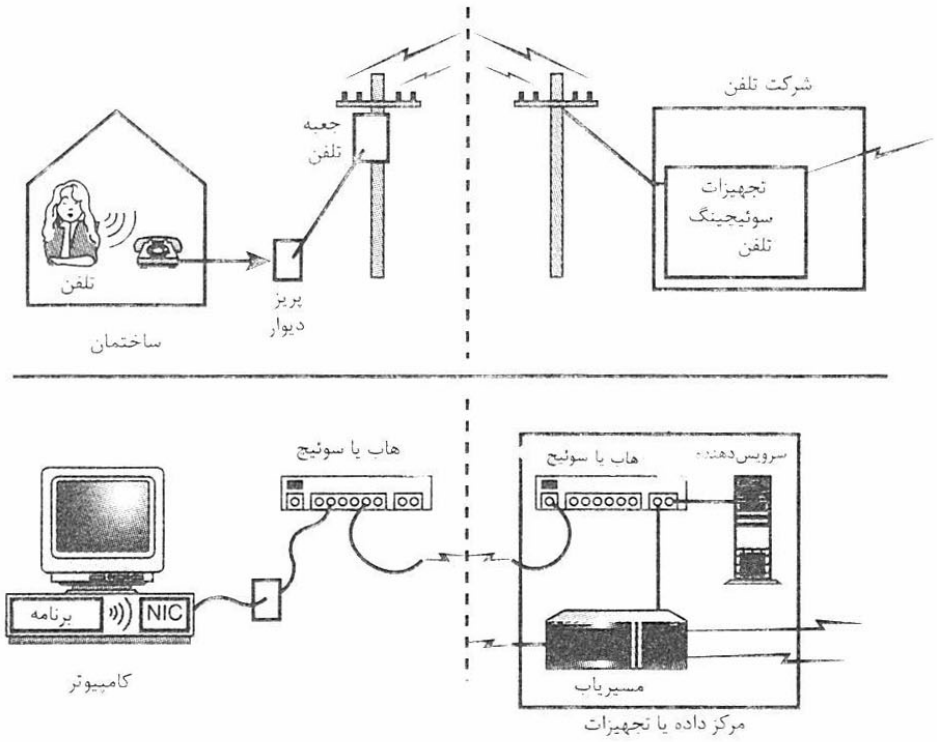
واژهٔ شبکه‌ای	معادل تلفنی
سوئیچ یا پل[1]	جعبه تلفن محلی که خطوط خصوصی و «خطوط جمعی» (هاب‌ها) را متصل می‌سازد.
هاب یا تمرکزدهنده[2]	خطوط جمعی اشتراکی در ناحیه‌ای عمومی.
پروتکل	زبان. تنها در صورتی می‌توانید با شخص دیگری ارتباط برقرار کنید که هر دو، زبان مور استفاده را درک نمایید. برای هر نوع مکالمه می‌توان هر زبان دلخواهی را به‌کار گرفت، اه برخی زبانها در موقعیت‌های خاصی بهتر هستند (ایتالیایی برای اپرا، فرانسوی برای شعرهای عاشقانه و غیره).
بسته[3] یا قاب[4]	جمله‌ای از مکالمه (یک ایده از مکالمه و نه کل آن).
سوکت	انشعاب. فرض کنید که می‌خواهید با آقای جونز که در شرکت XYZ کار می‌کند، صحبت نمایید. معمولاً، با شرکت XYZ تماس می‌گیرید و درخواست اتصال به انشعاب وی را می‌نمایید.
برنامه یا سرویس	موجودیتی در آن سوی خط تلفن، که می‌تواند اطلاعات، یا سرویس دریافتی از جانب شما را در طی مکالمه فراهم آورد. هنگام صحبت با آقای جونز، می‌توانید از وی در مورد قیمت ابزار مکانیکی خاصی سؤال کنید و یا بخواهید که تکنسین‌هایی را برای راه‌اندازی دستگاه‌تان گسیل دارد. تنها برخی از سرویس‌ها می‌توانند با بیش از یک پروتکل کار کنند ـ همان گونه که همه افراد اغلب با یک یا دو زبان صحبت می‌کنند.
سرویس‌های فهرست (DNS،[6] WINS[5])	دفتر تلفن «الکترونیک». به جای به خاطرسپردن شماره آقای جونز، به سادگی عمل جستجو و شماره‌گیری خودکار را به انجام می‌رسانید.

کارت‌های رابط شبکه

همان گونه که قبلاً ذکر شد، دستگاه تلفن و کارت رابط شبکه (NIC) در کامپیوتر بسیار شبیه به هم هستند. هردوی آنها، به موجودیت‌های مستقلی (شما، در مورد دستگاه تلفن و کامپیوتر، در مورد NIC) کمک می‌کنند که با دیگران صحبت کنند. همچنین، هم تلفن و هم کارت شبکه، برای موجودیتی که با آن ارتباط ایجاد می‌شود، و نوع تراکنش انجام‌شده، نامرئی هستند.

گوئی تلفن، قطعه‌ای فیزیکی از سخت‌افزاری است که شما را قادر می‌سازد از طریق تجهیزات شرکت تلفن با همسایه خود و یا آن سوی دنیا صحبت کنید. این موضوع در صورت NIC هم صدق می‌کند. NIC می‌تواند با NIC های همان خط و NIC های خطوط مختلف با استفاده از تجهیزات سوئیچ‌کردن که به خط متصل است، صحبت نماید.

1- bridge 2- concentrator 3- packet 4- frame
5- Windows Internet Naming Services 6- Domian Name Service



شکل ۱-۱ : مقایسه تقریبی شبکه اطلاعاتی و سیستم تلفن.

تهاجم MAC

همان‌گونه که هر شهروند، شماره تلفن منحصر به فردی دارد، NIC کامپیوتر هم دارای یک شماره منحصر به فرد است. البته، برخلاف گوشی تلفن، دارای شماره‌ای است که در کارخانه روی آن حک شده و به آن آدرس حک‌شده[1] یا BIA گفته می‌شود. این آدرس به اندازه کافی طولانی است و بنابراین تریلیون‌ها آدرس ممکن در دسترس قرار دارند. برای راحتی کار، آدرس دارای شکل فشرده‌ای است که با ۶ بایت شانزدهی نمایش داده می‌شود.



یادداشت : *بعضی افراد به آدرس BIA، آدرس MAC[2] می‌گویند.*

کلمه شانزدهی ممکن است یادآور ریاضیات باشد. در واقع، در اینجا با روش متفاوتی برای شمارش سروکار داریم - به جای آنکه ارقام ۹-۰ (دهدهی) باشند، از ارقام 0-F (شانزدهی) استفاده می‌کنیم. به خاطر در اختیارداشتن گزینه‌های رقمی بیشتر (۱۶ به جای ۱۰)، می‌توانیم اعداد را در شکل فشرده‌تری بیان کنیم. زیاد نگران این قضیه نباشید، تمامی آنچه که لازم است بدانید آن است که هر بایت از دورقم شانزدهی تشکیل یافته و از ۶ بایت برای تبیین آدرس MAC استفاده می‌شود. در حقیقت، به نظر نمی‌رسد که 00-00-10-2b-5c-8d خیلی طولانی‌تر از 1-800-555-1212 باشد، این طور نیست؟

IEEE گستره‌های آدرس‌های MAC را توزیع می‌کند (برای مثال، شرکت Proteon Inc تمامی شماره‌های آغازگرشونده

1- burned-in address 2- Media Access Control

با 93-00-00 را در اختیار دارد). این بدان معناست که با نگاه‌کردن به سه بایت اول آدرس MAC می‌توان سازنده کارت شبکه را تشخیص داد. این ارقام OUI (شناسه منحصر به فرد سازمانی[1]) نام دارد و هنگام عیب‌یابی مشکلات بخصوصی مفید واقع می‌شود.



یادداشت : *مؤسسه مهندسین برق و الکترونیک (IEEE؛ که آی‌تریپل‌ایی تلفظ می‌شود)، سازمانی است که علاوه بر فعالیتهای دیگر، استانداردهای الکترونیک را تدوین می‌نماید. یکی از نقش‌های IEEE، نظارت بر آدرس‌های MAC می‌باشد. به خاطر تعدد تولیدکنندگان شبکه‌ای، واقعاً مهم است که آدرس‌های MAC را بتوان ردیابی نمود. در غیر این صورت، ممکن است دو تولیدکننده متفاوت تصادفاً کارت‌های شبکه‌ای با آدرس یکسان تولید کنند که در صورت به‌کارگیری آن دو کارت در یک شبکه، مشکلاتی بروز می‌کند. وقوع این امر، با وجود آدرس‌های MAC بسیار، امکان‌پذیر است. هر آدرس MAC، در شش‌رقم شانزدهی قالب‌بندی شده است (یا آدرس ۴۸ بیتی، اگر بخواهیم از اصطلاحات دودویی استفاده کنیم). این فضای آدرسی ۲۸۱ تریلیون آدرس ممکن را در اختیار می‌گذارد ـ دقیقاً ۲۸۱,۴۷۴,۹۷۶,۷۱۰,۶۵۶ ـ این مقدار ترکیبات هنگفتی را در اختیار می‌گذارد. این عدد را با سیستم تلفنی آمریکا مقایسه کنید، که در آن تنها ۹ تریلیون شماره موجود است.*

کاربرد OUI

به مفیدبودن OUI، در تجربه‌ای با مشکلات تناوبی در برنامه‌ای کاربردی جدید، برخورد کردم. فروشنده برنامه مشکل را به کارت شبکه مربوط دانست و فروشنده کارت‌های شبکه هم توصیه کرد برای رفع مشکل «آخرین و فوق‌العاده‌ترین» راه‌اندازهای کارت‌های شبکه را به‌کار بگیرم. با آغاز به‌کارگیری مجموعه کوچکی از آن راه‌اندازها، با مشکلات شبکه‌ای اساسی روبه‌رو شدم و متوجه شدم مشکلات تنها در کارت‌هایی است که به تازگی به‌روز درآورده شده‌اند (از طریق بررسی OUI های ارائه شده توسط برنامه تحلیل‌گر شبکه (network analyzer). به‌روزدرآوری‌های جدید را بازگشت دادم و مشکلات شبکه رفع شدند و برای حل مشکل اولیه به فروشنده برنامه مراجعه نمودم. دانستن OUI می‌تواند مفهوم قابل استفاده‌ای باشد.



اخطار : *OUI تنها سازنده تراشه را بیان می‌کند، نه سازنده‌ای که بُرد را جمع کرده است. ساخت ریزتراشه گرانقیمت است، اما کنار هم قراردادن تراشه‌ها روی یک برد مداری که NIC خواهد شد ارزانتر تمام می‌شود. به خاطر این تفاوت هزینه، بسیاری از فروشندگان، از تراشه‌های فروشنده‌های دیگر برای کارت‌های شبکه خود استفاده می‌کنند، برای مثال، Emalex در فهرست OUI از 00-00-c9 استفاده می‌نماید، proteon Inc نیز بُردهای شبکه‌ای با این OUI تولید نموده است.*



اخطار : *در پاسخ به هرگزینه پیکربندی شبکه که می‌پرسد آیا می‌خواهید آدرس MAC یک کارت NIC را بازنویسی کنید، بگویید خیر! این گزینه برای سرپرستان باتجربه درنظرگرفته شده است و در صورت عدم استفاده صحیح می‌توانند مشکل‌زا باشد.*

1- organization unique identifier

مسیریاب‌ها

از آنجا که هر کارت شبکه دارای آدرس MAC متفاوتی است، به هر گروه شبکه‌ای عددی تخصیص داده می‌شود. این شماره شبکه‌ای، که «ناحیه» شبکه را تعیین می‌کند، شبیه به کُد ناحیه‌ای تلفن است. شماره‌های ناحیه‌ای شبکه‌ای مختلف از طریق مسیریاب به هم متصل می‌شوند، که همان گونه که از نام آن قابل برداشت است، بسته‌ها را از یک ناحیه شبکه‌ای (حوزه مسیریابی) به ناحیه‌ای دیگر مسیرگردانی می‌کند.

می‌توانید تصور کنید مسیریاب در شبکه تلفن، آن بخشی از تجهیزات است که شما را از شهرتان به شهر دیگر متصل می‌کند. مسیریاب‌ها اغلب شبکه‌های مجزای جغرافیایی را به هم وصل می‌کنند. (این موضوع همیشه صادق نیست، اما نقش مدللی از این وسیله را تبیین می‌کند). دقیقتر که بگوییم، هر مسیریاب به بیش از یک شماره شبکه‌ای متصل می‌شود و کمک می‌کند فراخوانی‌های شبکه‌ای به همانجایی که می‌خواهند، بروند (با فرض آنکه زبان موجود در فراخوانی شبکه، توسط مسیریاب پشتیبانی می‌شود).



***یادداشت** : در اینجا مقایسه دیگر کارا نیست: سوئیچ‌های تلفنی هیچ کاری با مکالمه روی خط ندارند، اما در مورد مسیریاب‌ها این طور نیست. این فکر ممکن است مفید باشد که مسیریاب‌ها، همسایگانی دوست‌داشتنی هستند که پیغام شما را منتقل می‌کنند (در صورتی که همزبان‌تان باشند).*

البته، سیستم تلفنی به تجهیزاتی در همسایگی شما و تجهیزات مفصل‌تری در شرکت تلفن نیاز دارد. این حالت برای شبکه هم وجود دارد. دو نوع «چسب» شبکه‌ای، شما را به شبکه همسایه‌تان متصل می‌کنند:

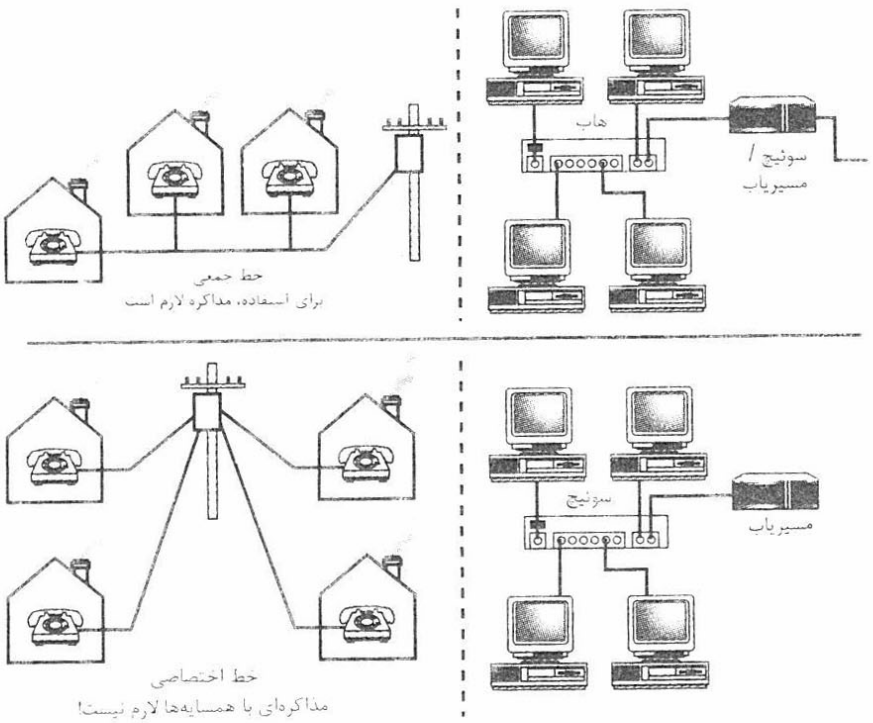
- هاب‌ها (متمرکزکننده‌ها)
- سوئیچ‌ها

هاب، خط جمعی مشترک همسایگی (نظیر آنچه که برای کلبه جنگلی استفاده می‌کنید) است. کاربرد آن به خاطر کاهش هزینه در ارائهٔ کانال به هر کارت شبکه برای صحبت‌کردن می‌باشد. هاب، محلی است که تمام NIC ها در «خط جمعی» (یا بخش = سگمنت) به هم وصل می‌شوند. سیم تک‌تک NIC ها به هاب متصل می‌شود که در آن همگی به یک سیستم مشترک متصل می‌گردند.



***یادداشت** : از این اتصال فیزیکی عمومی اغلب با عنوان گذرگاه (bus) یاد می‌شود. واژه bus به معنی اتوبوس است. هر شرکت‌کننده که بخواهد از این اتصال عمومی استفاده کند، سوار اتوبوس می‌شود و یا از آن پیاده می‌گردد.*

از آنجا که NIC ها از یک گذرگاه عمومی استفاده می‌کنند، هر NIC می‌تواند به NIC های دیگر «گوش فرادهد». NIC ها قواعد توکاری را برای استفاده از این ناحیه مشترک به‌کار می‌برند که در فصول ۹ و ۱۰ بررسی خواهند شد. در حال حاضر، کافی است بدانید که در کارخانه به هر NIC یاد داده شده است که چگونه به خوبی با دیگران کار کند و از کابل اشتراکی استفاده نماید ـ البته، بیشتر اوقات. بدانید که اگر یک کارت شبکه از این قواعد پیروی نکند، ممکن است در کل سگمنت اشتراکی مشکلاتی را ایجاد نماید (شکل ۲-۱ تفاوت بین خطوط تلفنی و سگمنت‌های شبکه‌ای اشتراکی و اختصاصی را روشن می‌سازد).



شکل ۲-۱ : تفاوت بین خطوط اشتراکی و اختصاصی.



یادداشت *: کامپیوترهای شبکه‌های قدیمی، نظیر لامپ‌های قدیمی که در اعیاد استفاده می‌شدند، از طریق یک سیم به یکدیگر متصل می‌شدند. بنابراین، یک خرابی فیزیکی در سیم باعث اشکال در تمامی کامپیوترهایی می‌شد که بعد از آن بخش خراب قرار داشتند. استفاده از بخش‌هایی مبتنی بر هاب این اشکال را مرتفع می‌کند، چرا که هر کامپیوتر دارای اتصال فیزیکی مخصوص به خود است و هاب آنها را به هم متصل می‌کند. روش جدیدتر اشتراک سیم، توپولوژی ستاره نام دارد، چرا که شبیه به ستاره است. متد قدیمیتر، توپولوژی گذرگاه (باس) نام دارد ـ خطی از یک PC به PC دیگر.*

تکنولوژی جدیدی به نام سوئیچینگ این امکان را فراهم می‌سازد که هر کارت شبکه خط خصوصی خود را داشته باشد؛ البته، شبکه‌های مبتنی بر هاب بسیاری هنوز وجود دارند (و به نظر نمی‌رسد که به این زودی از کار کنار روند). تکنولوژی سوئیچینگ را با آشنایی بیشتر با عیب‌یابی شبکه، مهیج خواهید یافت. نظیر هاب‌ها که مشکل «لامپ عید» را از پیش‌پای برداشتند، سوئیچ‌ها به کاربران اجازه می‌دهند که از بسیاری مشکلات شبکه‌های اشتراکی رهایی یابند. به جای آنکه کامپیوتر برای دستیابی به حق صحبت در هنگام نیاز، رقابت کند، می‌تواند تا زمانی که کامپیوتر مقابل در دسترس است، هر زمان که بخواهد انتقال اطلاعات را صورت دهد. رقابتی با کامپیوترهای دیگری در دسترسی به سیم وجود ندارد و هر کامپیوتر اتصال خود را داراست.

این حالت چگونه کار می‌کند؟ هسته سوئیچ به آدرس‌های MAC دو کامپیوتری که می‌خواهند ارتباط برقرار کنند، نگاه می‌کند و یک کانال خصوصی سریع برای آنها باز می‌کند. هاب تنها یک کانال عمومی دارد، اما سوئیچ تعداد زیادی کانال و توانایی تغییر مکالمات بین آنها را یکجا در خود جای داده است. اگر سوئیچ به اندازه کافی سریع باشد (سوئیچ با سرعت مخابراتی)، ایستگاههای کاری متصل به آن که با یکدیگر صحبت می‌کنند، تحت تأثیر ایستگاههای کاری دیگر که آنها نیز با سرعت بالا به‌کار انتقال مشغول هستند، قرار نخواهند گرفت.

با اینکه قیمت هاب‌ها خیلی پایین هستند، هزینه سوئیچ‌ها نیز رو به کاهش است؛ می‌توانید منتظر این تکنولوژی برای کاربرد در شبکه‌های محلی در آینده‌ای نزدیک باشید. با اینکه هاب‌های اشتراکی خاصیت خود را دارا هستند (برای مثال، درک مکالمات روی یک خط اشتراکی آسان است، که این خود برای عیب‌یابی خوب است)، این حقیقت که از شبکه‌های سوئیچ مشکل‌دارتر هستند، در جای خود محفوظ باقی می‌ماند (شبکه‌های سوئیچی بسیار سریعتر و قابل اطمینان‌تر هستند). با ارزانترشدن سوئیچ‌ها، می‌توان منتظر کاربرد آنها به جای هاب بود.

پروتکل‌ها

کامپیوتر از طریق کارت شبکه‌اش «صحبت می‌کند»، اما تکنولوژی به پایه‌ای نرسیده که بتواند به انگلیسی صحبت نماید و به جای آن، از زبان مقدماتی‌تری ـ پروتکلی با NetBEUI یا IPX/SPX استفاده می‌کند. می‌توانید این گونه تصور کنید که این پروتکل‌ها، همان زبان مورد استفاده در تلفن می‌باشند؛ همان گونه که آلمانی یا فرانسوی صحبت‌کردن شما، تفاوتی برای تلفن ایجاد نمی‌کند، برای کارت شبکه هم اهمیتی ندارد که کامپیوتر و برنامه‌های آن از TCP/IP یا IPX/SPX استفاده می‌نمایند.

اهمیت TCP/IP

خبر خوب آن است که برای عیب‌یابی، لازم نیست چیز زیادی در مورد پروتکل‌ها بدانید ـ بیشتر اوقات، مشکل شما ربطی به پروتکل ندارد؛ چرا که پروتکل‌ها ساده و به خوبی تعریف شده‌اند. برای مثال، ۲۰ سال از به‌کارگیری TCP/IP می‌گذرد (زمانی بس عظیم در دنیای کامپیوتر)، و اضافات صورت پذیرفته در آن ناچیز بوده است. این یعنی برخلاف برنامه‌های کاربردی رومیزی، TCP/IP این شانس را داشته که به ثبات برسد.

این موضوع در کنار فاکتورهای دیگر، TCP/IP (شکل کوتاه‌شده پروتکل کنترلی انتقال/پروتکل اینترنت[1]) را زبان جهانی پروتکل‌های شبکه گردانیده است. اینترنت TCP/IP را در زمره وسایل خانگی قرار داده است، یعنی به احتمال زیاد چیزهایی در مورد TCP/IP می‌دانید. برای مثال می‌دانید که اسم میزبان در TCP/IP چیزی نظیر myhost.mycompany.com و آدرس TCP/IP عددی مشابه 167.195.160.6 می‌باشد.

این آدرس با سه نقطه اعشار چیست؟ مگر قبلاً نگفته‌ایم که آدرس یک عدد شانزدهی ۶ بایتی است؟ خوب، در مورد کارت‌های شبکه این طور است، اما در مورد پروتکل‌های اوضاع فرق می‌کند. همان گونه که تلفظ شماره تلفن به زبان فرانسوی اندکی متفاوت است، تفاوتی در آدرس شبکه‌ای هنگام «تلفظ» آن با TCP/IP و آدرس MAC وجود دارد. هردو آنها برای منظورهای خویش، «شماره تلفن» کارت شبکه محسوب می‌شوند؛ این تنها به زبانی که در حال به آن صحبت می‌شود دارد.

آدرس‌های TCP/IP از چهار عدد بین 0 تا 254 که در سیستم آشنا و دوست‌داشتنی دهدهی بیان شده‌اند. تشکیل یافته است. این آدرس‌ها را اغلب سرپرست شبکه تخصیص می‌دهد. یکی از وظایف سرپرست، تخصیص آدرس‌های منحصر به فرد به تک‌تک کامپیوترهای شبکه می‌باشد.

1- Transmission Control Protocol/Internet Protocol



یادداشت : *چرا باید دو آدرس مختلف وجود داشته باشند؟ از آنجا که OUI واحدبودن آدرس‌های تضمین کرده، چرا تنها آدرس TCP/IP را به صورت دهدهی بیان نکنیم؟ در قدیم، کارتهای شبکه فا آدرس‌های MAC توزیعی IEEE واحد بودند؛ برخی باید به ۲۵۴ آدرس بسنده کنند! به همین خاط استفاده از آدرس MAC برای آدرس TCP/IP در شبکه‌ای بزرگ عملی نبود، بنابراین طراحان TCP/IP روشی برای ترجمه آدرس MAC به مقداری بزرگ و واحد، اختراع نمودند این کار با وجود آدرس‌ها MAC امروزی لازم نیست، اما میراث قدیمی تا به امروز پابرجا مانده است.*



اخطار : *آدرس‌های تکراری TCP/IP می‌توانند کار برنامه‌های وابسته به TCP/IP را مختل کنند. اگ آدرس‌های TCP/IP را خودتان تخصیص می‌دهید، مواظب باشید که از آدرس‌های واحد و منحصر فرد استفاده نمایید.*



نکته : *برنامه‌های سرویس‌دهنده DHCP (پروتکل پیکربندی پویای میزبان[1]) می‌توانند به صورت خودکار آدرس‌های IP را به کامپیوترها تخصیص دهند. اگر شماره تلفن‌تان هر چند روز تغییر کند، چ کار می‌کنید؟ DHCP فرآیند آدرس‌دهی را خودکار می‌سازد و خطاهای تکراری را حذف می‌نماید. د فصل ۱۱ اطلاعات کلی در مورد عیب یابی DHCP ملاحظه خواهید نمود.*

TCP/IP، نظیر شماره تلفن، دارای شماره شبکه (یا «کُد ناحیه‌ای») می‌باشد. البته، برخلاف شماره تلفن، «کُد ناحیه‌ای» بخش اعظم عدد را به خود تخصیص داده است. بخش کوچکتر شماره (که بدان گره یا شماره میزبان گفته می‌شود)، همان شماره تلفن محلی است. به بخش اول آدرس که با «کُد ناحیه‌ای» متناظر است، شماره شبکه گفته می‌شود. از آنجا که لازم نیست شماره شبکه TCP/IP، طول ثابتی داشته باشد، این کار توسط ماسک شبکه صورت می‌پذیرد. این ماسک عددی است که با کمک ریاضیات، طول شماره شبکه را تعیین می‌نماید.

خوشبختانه، بیشتر شبکه‌های TCP/IP کوچک دارای ماسک یکسان هستند، بنابراین محاسبه شماره شبکه به جای انجام محاسبات دودویی، از طریق مثال صورت می‌پذیرد.

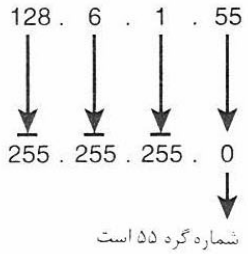


نکته : *پرکاربردترین استفاده از ماسک شبکه در عیب یابی، در طی بررسی صحت پیکربندی می‌باشد. از آنجا که ماسک شبکه اشتباه می‌تواند باعث بدکارکردن هر ایستگاه‌کاری گردد، حصول اطمینان از یکی‌بودن ماسک شبکه کلیه PCهای یک بخش از اهمیت ویژه‌ای برخوردار است.*

در مورد یک ماسک شبکه که تمامی اعداد آن 255 است، این محاسبه آسان است. کافی است شماره IP را به همراه ماسک شبکه در زیر آن روی کاغذ بنویسیم؛ هر عدد که با 255 تطابق دارد، شماره شبکه است. اعداد باقی‌مانده، شماره گره را تشکیل می‌دهند (شکل ۳-۱ مثالی را نشان می‌دهد).

سرویس‌دهنده‌ای که شماره IP آن 192.168.5.10 و ماسک شبکه آن 255.255.255.0 است را در نظر بگیرید. در اینجا شماره شبکه 192.168.5.0 و شماره گره 10 می‌باشند. از آنجا که اغلب شبکه‌های TCP/IP ساده به این صورت کار می‌کنند، نحوه کار با اعداد دودویی برای ماسک‌های شبکه‌ای غیرمعمول را می‌توانیم برای کسانی که از مشقت لذت می‌برند، باقی گذاریم.

1- Dynamic Host Configuration Protocol



شکل ۳-۱ : برای یافتن شماره گره در جایی که شماره‌های ماسک همگی ۲۵۵ هستند، شماره‌های شبکه که با 255 متناظر هستند را بلوک (ماسک) نمایید. نتیجه، شماره گره می‌باشد.

با اینکه مفهوم ماسک‌های شبکه و شماره‌های شبکه ممکن است در وهله اول گنگ و نازیبا به نظر برسد، اما واقعاً لازم است بدانید کدام بخش از آدرس TCP/IP تان شماره شبکه است. به این صورت می‌توانید آن را یادداشت کرده و در هنگام لزوم عیب‌یابی نمایید. با عادت‌کردن به این مفاهیم، آنها را مشکل نخواهید یافت (این بهایی است که برای قادربودن به «تماس و شماره‌گیری همسایه خود» می‌پردازید).

DLC

برخی از پروتکل‌ها نمی‌توانند برای تماس با همسایگان به‌کار روند. آیا این پروتکل‌ها خوب نبوده‌اند؟ آیا این به خاطر تنبیه آنهاست؟ نه، آنها خیلی باهوش نیستند و به طور عمده بر پایه توانایی کارت شبکه در صحبت با شبکه محلی عمل می‌کنند. این پروتکل‌ها تنها می‌توانند با سایر آدرس‌های MAC صحبت کنند و با عنوان پروتکل‌های DLC (کنترل پیوند داده[1]) شناخته می‌شوند. این پروتکل‌ها قابلیت مسیریابی ندارند، که بدان معناست که آنها تنها می‌توانند با ایستگاههای همان شبکه صحبت کنند. می‌توانید DLC را به سیستم «چهارشماره‌ای» در برخی از هتل‌ها تشبیه کنید (بدون توانایی فشردن ۹ برای تماس با خارج از محدوده هتل).

NetBEUI شرکت میکروسافت، مثالی از یک پروتکل DLC می‌باشد. NetBEUI شکل کوتاه‌شده رابط توسعه یافته کاربر *NetBIOS*[2] است که در آن NetBIOS مخفف عبارت «سیستم ورودی خروجی پایه برای شبکه[3]» می‌باشد. در اصل، NetBEUI بهبودیافته NetBIOS است. NetBIOS یک پروتکل ساده شبکه‌ای است که توسط IBM و میکروسافت در محصولات اولیه اشتراک فایل که در DOS کار می‌کردند، به‌کار گرفته می‌شد. NetBEUI ویندوز NT، ۹۸ و ۹۵ شکل توسعه‌یافته آن است که در ویندوز ۹۵ به‌کار گرفته شده است.



***نکته :** کاربران ویندوز ۹۵/۹۸ همیشه از من می‌پرسند، چرا نمی‌توانم گروههای کاری سایر افراد را در شبکه ببینم؟» این اغلب به خاطر آن است که آنها از ویندوز 9x خود که از NetBEUI برای اشتراک فایل‌ها استفاده می‌کند، می‌خواهند که گروههای کاری در آن سوی مسیریابی را ملاحظه کنند. این مشکل را می‌توان با افزودن پروتکلی با قابلیت مسیریابی، نظیر IPX/SPX حل نمود (TCP/IP را نیز می‌توان به‌کار برد، اما پیکربندی آن پیچیده‌تر است).*

IPX/SPX

IPX/SPX علاوه بر اینکه پروتکلی با قابلیت مسیریابی است، از نقطه نظر کاربر نیز پروتکلی آسان به‌شمار می‌رود. به جای

1- data link control 2- NetBIOS Extended User Unterface

3- Network Basic Input Output System

سروکارداشتن با ماسک‌های شبکه و پیداکردن شماره‌های شبکه‌ای، تنها کافی است به سرویس‌دهنده (یا مسیریاب) در شبکه نگاه کنید تا شماره شبکه را دریافت کنید. این شماره، عددی است دلخواه ولی واحد که در مبنای شانزده به‌کار برده می‌شود. آدرس گره نیز به سادگی آدرس MAC مربوط به کارت شبکه می‌باشد. شکل کامل آدرس به همراه «کُد ناحیه‌ای» نظیر این است:

0000001D: 000093552899

که یعنی شماره شبکه 1D و شماره گره 93552899 که به هیچ گونه محاسبه‌ای نیاز ندارد. از آن گذشته، هیچ گونه پیکربندی آدرسی در ایستگاه‌کاری لازم نیست، چرا که آدرس مستقیماً از آدرس MAC کارت استخراج می‌شود. متأسفانه، از آنجا که IPX/SPX (ابداع شده توسط ناول، سازنده نت‌ور) تا حدودی پروتکلی خصوصی محسوب می‌شود، هیچ گاه در بازار در حد TCP/IP ظاهر نشده است. از طرف دیگر و با اینکه میکروسافت IPX/SPX را به عنوان پروتکل‌های پشتیبانی‌کننده از اشتراک فایل و چاپ در ویندوز ۹۵ و NT پشتیبانی نموده است، به خاطر قدرت روزافزون اینترنت و در نتیجه TCP/IP، IPX/SPX به هنگام بازیکن ذخیره و دست دوم باقی خواهد ماند.

البته به این زودی هم کنار نخواهد رفت. اگر IPX/SPX در دم و دستگاهتان پیدا می‌شود، آشنایی با آن ارزشمند خواهد بود. جزئیات را می‌توانید در فصل ۱۳ ملاحظه کنید.

بسته‌ها

یک بلوک ساختمانی دیگر در هر شبکه (با همان اهمیت گلبول‌های قرمز در دستگاه گردش خون) بسته می‌باشد (که برخی اوقات قاب خوانده می‌شود). بسته کوچکترین واحد ارتباطی در شبکه است، بسیار شبیه به آنکه جمله کوچکترین واحد در یک مکالمه می‌تواند محسوب شود (با اینکه کلمات خود به تنهایی واحدهای کوچکتری هستند، اما واحدهایی کامل محسوب نمی‌شوند. برای مثال، تنها گفتن کلمه «شام» به کسی نمی‌تواند معنی خاصی داشته باشد، مشخص نیست که می‌خواهید وی را به شام دعوت کنید، او را برای شام بپزید و یا هر دو از خیر شام بگذرید!).

در هر لحظه تنها یک بسته می‌تواند در سیم وجود داشته باشد، که این امر هنگامی که چندین کاربر در شبکه بخواهند چندین وظیفه را به انجام برسانند، مشکل به نظر می‌رسد. برای مثال، فرض کنید قطعات مکالمه زیر به ترتیب ذکرشده در ذیل روی رسانه انتقالی ظاهر شوند:

«استیسی، من جاناتان هستم. چطوره که برای شام مقداری نان بخرم؟»

«جاناتان، من لئو هستم. مایلم که خانه بیایی تا با هم بازی کنیم.»

«جاناتان، من استیسی هستم، لطفاً سر راه منزل نان بخر.»

«لئو، من جاناتان هستم، بزودی به خانه می‌رسم و با کمال میل بازی خواهم کرد.»

«استیسی، جاناتان هستم، این کار را انجام خواهم داد.»

دنبال‌کردن این کلمات مشکل است، نه؟ خوشبختانه، شبکه‌ها از روش سوئیچینگ بسته استفاده می‌کنند. ایده به‌کار رفته در این روش ساده است. از آنجا که لازم است مکالمات به نظر برسند، هر قطعه از مکالمه حاوی اطلاعاتی بر نگهداری رد اینکه چه کسی به چه کسی صحبت می‌کند، می‌باشد. به این ترتیب، آنچه که مکالمه‌ای اشتباه به نظر

می‌رسید، به دو مکالمه منطقی تبدیل می‌شود:

«استیسی، من جاناتان هستم. چطوره که برای شام مقداری نان بخرم؟»

«جاناتان، من استیسی هستم، لطفاً سر راه منزل نان بخر.»

استیسی، جاناتان هستم، این کار را انجام خواهم داد.»

«جاناتان، من لئو هستم. مایلم که خانه بیایی تا با هم بازی کنیم.»

لئو، من جاناتان هستم، بزودی به خانه می‌رسم و با کمال میل بازی خواهم کرد.»

از آنجا که هر بسته، آدرس (یا «شماره تلفن») طرف مقابل را دارد و نیز به خاطر آنکه در هر کامپیوتر ممکن است بیش از یک برنامه بخواهد مکالمه را صورت دهد، مفهوم جدیدی به نام سوکت مطرح می‌گردد که بسیار مشابه انشعاب تلفن عمل می‌کند. بنابراین، همان گونه که با شرکت آلفا تماس می‌گیرید و می‌خواهید با فردی با شماره داخلی 412 صحبت کنید، کامپیوترتان هم در یک فراخوانی شبکه‌ای، آدرسی شبکه‌ای را صدازده و شماره سوکت را مورد پرس‌وجو قرار می‌دهد.

اغلب شماره سوکت بعد از علامت (:) و به دنبال آدرس به نمایش درمی‌آید. برای مثال، هنگامی که مرورگر وِب http://www.co.chatham.ga.us را پیمایش می‌کند، در واقع به 167.195.1609:80 اشاره می‌شود (یا سوکت 80 از آدرس 167.195.160.9). سوکت 80، استانداردی است که برای سرویس‌های وِب HTTP خوانده می‌شود (پروتکل انتقالی فوق متن[1]).



یادداشت : *HTTP اسم سرویسی است که اغلب در سوکت 80 توسط برنامه‌ای مقیم در آن ارائه می‌شود. البته، HTTP به مجموعه‌ای از قواعد که تراکنش‌های وِب (آنچه که سرویس‌دهنده‌ها و مرورگرهای وِب تلاش می‌کنند انجام دهند) را میسر می‌سازند نیز گفته می‌شود.*

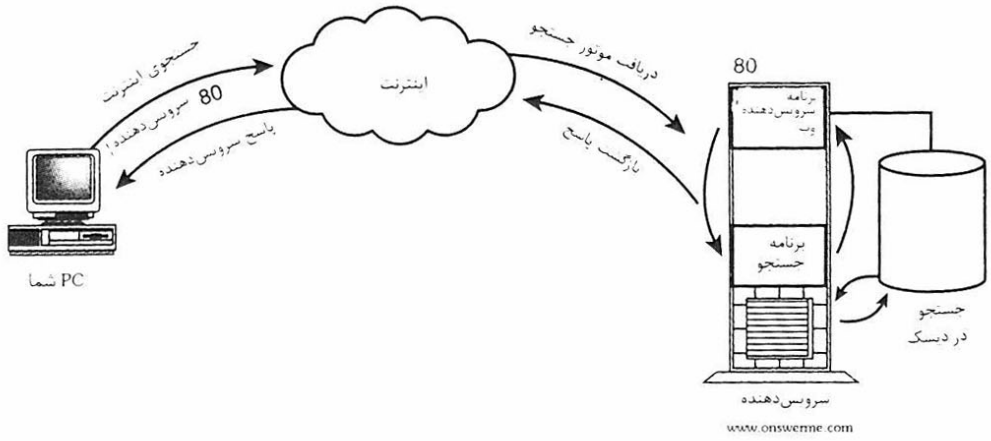
این مهم است که درک کنیم دو تعریف از HTTP وجود دارد: اسم سوکت («سوکت 80، سوکتی است که به صورت معمول برای HTTP استفاده می‌گردد») و خود پروتکل («تمامی سرویس‌دهنده‌های وِب به منظور عملکرد خالی از خطا باید از پروتکل HTTP تبعیت نمایند»). بسیاری از پروتکل‌ها و سرویس‌های دیگر نیز معانی دوگانه دارند ـ برای مثال SMTP هم به سوکت ۲۵ اشاره می‌کند (که اغلب برای سرویس‌های پستی استفاده می‌شود) و هم پروتکل انتقالی پستی ساده[2] محسوب می‌شود.

از آنجا که سوکت معادل انشعاب تلفن است، برنامه‌ای که به فراخوانی پاسخ می‌دهد، نظیر شخصی است که می‌خواهید با وی صحبت کنید (شکل ۴-۱ را ببینید). برنامه می‌تواند هنگامی که «صحبت» می‌کنید، کارها را برایتان انجام دهد ـ یا اطلاعات لازم را ارائه کند و یا فرآیندی را شروع کند که می‌خواهید صورت پذیرد. برخی درخواستها می‌توانند ترکیبی از هردو باشند: هنگامی که در اینترنت جستجو می‌کنید، از برنامه آن سوی خط می‌خواهید که جستجویی را انجام دهد و پاسخ را ارسال کند.

درست نظیر مردم، برخی برنامه‌ها (که به خاطر سرویس ارائه‌شده، سرویس دهنده نام گرفته‌اند)، که در طرف دیگر خط قرار گرفته‌اند، تنها به یک زبان صحبت می‌کنند. برای مثال، سرویس‌دهنده‌های استاندارد وِب تنها به TCP/IP صحبت می‌کنند. البته، همان طور که قبلاً نیز اشاره شد، سرویس‌های اشتراک فایل و چاپ میکروسافت می‌تواند هر چیزی را مورد استفاده قرار دهد: TCP/IP، IPX/SPX و NetBEUI. نظیر آموزش زبانی جدید به یک شخص، ایجاد توانایی پشتیبانی چندگانه پروتکل‌ها مستلزم تلاش بیشتر است و اگر قرار به پرداخت بهای بیشتر برای برنامه نباشد، اکثر برنامه‌ها یک پروتکل را انتخاب می‌کنند. محبوب‌ترین پروتکل برنامه‌های مدرن کدام است؟ درست حدس زده‌اید: TCP/IP.

1- Hypertext Transmission Protocol

2- Simple Mail Transfer Protocol



شکل ۴-۱ : سوکت معادل انشعاب تلفن است.

داخل اسم چیست؟

احتمالاً، در طی پاراگراف‌های قبلی از خود پرسیده‌اید، «چگونه www.co.chatham.ga.us به 167.195.160.9 ترجمه می‌گردد؟ از آن گذشته، چرا اصولاً از اسامی استفاده می‌کنیم؟ ما که می‌توانیم با شماره تلفن‌ها کار کنیم، چرا تنها از شماره ؟ استفاده نمی‌کنیم؟ اینها سؤالات خوبی هستند. پاسخ سؤال اخیر آن است که تنها به خاطر آنکه افراد می‌توانند با اعداد کا کنند، دلیل آن نیست که آنها ترجیح می‌دهند با اعداد سروکار داشته باشند. به خاطرسپردن کدامیک راحت‌تر است 1-800-NETWORK یا 1-800-638-9675؟ مشخص است که بیشتر افراد بهتر می‌توانند اسامی را به خاطر آورند. در واقع اسامی هنگام کار با شبکه بهتر هستند، چرا که آدرس‌های عددی ممکن است در حین انتقال یا پیکربندی مجدد تغییر کنند، در حالی که اسامی سمبولیک ثابت باقی می‌مانند.

ترجمه اسم ـ به ـ آدرس (که جستجوی نام یا تحلیل نام نیز نامیده می‌شود)، از طریق سرویس‌های نام رخ می‌دهد. سرویس‌های نام، معادل شبکه‌ای کتابچه الکترونیکی اسامی دفتر تلفن می‌باشند. در واقع، این سرویس‌ها بسیار راحت‌تر از دکمه‌های تماس سریع تلفن عمل می‌کنند. برای مثال، تصور کنید که به تلفن بگویید «مادر» و آنگاه دستگاه شماره مادرتان را برایتان بگیرد.

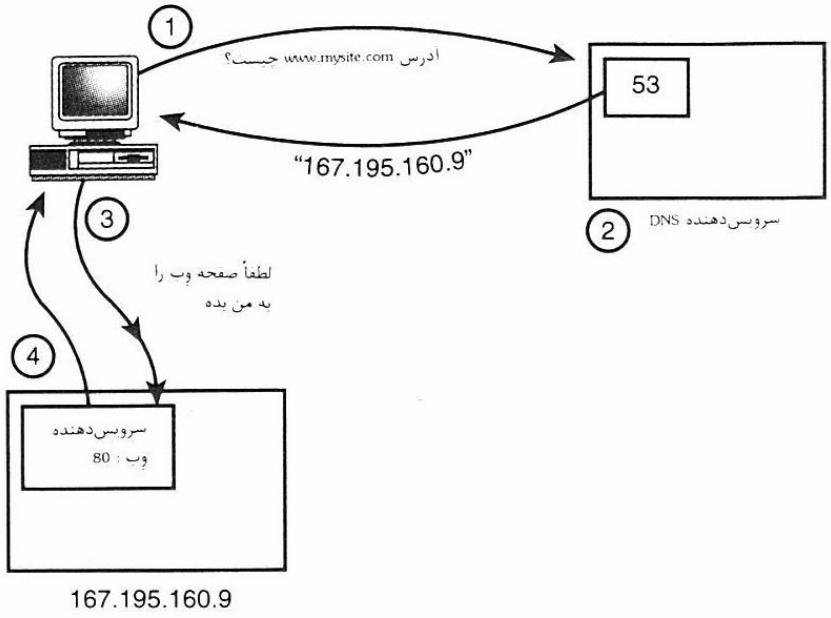
DNS

سرویس‌های نام به صورت یک سرویس در هر سرویس‌دهندهٔ نامی کار می‌کنند؛ یعنی، برنامه‌ای خاص در سرویس‌دهنده نام اجرا می‌شود که با ارائه نامی به آن، آدرس متناظر را بازمی‌گرداند. مثل دکمه‌های سریع گوشی تلفن، باید اسامی و آدرس‌های IP را وارد مجموعه اطلاعات برنامه نمود.

در مورد سرویس‌های نام TCP/IP، با وجود قدرتمندبودن و توانایی کار با میلیونها و میلیونها نام، روش کاربرد آنها کاملاً هم به شکل نصب و اجرا[1] نیست. DNS (سرویس نام حوزه[2]) که آن را هنگام گشت و گذار در وِب مورد استفاده قرار می‌دهید، در صورت پیکربندی درست به صورت خودکار و به زیبایی کار می‌کند و www.co.chatham.ga.us را به 167.195.160.9 تبدیل می‌نماید. البته لازم است که شماره دقیق سرویس‌دهنده DNS خود را بدانید. برخلاف اطلاعات تلفن،

1- plug-and-play 2- Domain Name Service

سرویس‌دهنده‌های DNS همگی آدرس‌های مختلفی دارند؛ بررسی صحت درستی سرویس‌دهنده DNS مربوط به ایستگاه‌کاری، ممکن است گام مهمی در عیب‌یابی باشد (شکل ۵-۱).



شکل ۵-۱ : تحلیل نام در DNS.

به خاطر داشته باشید که اکثر سایت‌های کوچکتر که از TCP/IP استفاده می‌کنند، از DNS بهره نمی‌برند. به جای آن، هر ایستگاه‌کاری دارای یک فایل "hosts" محلی است که آدرس‌ها و اسامی میزبان مورد نظر ایستگاه‌کاری را در خود نگه می‌دارد. (تصور کنید که این فایل مثل دفتر تلفن شخصی شماست و با فهرست تلفن‌های شرکت‌تان مقایسه کنید). همان گونه که حدس می‌زنید، این کار با زیادشدن تعداد ایستگاههای کاری مشکل می‌شود، مگر آنکه فهرست آدرس‌های مورد نظر تغییر نکند. با رشد سایت‌ها و با اتصال آنها به اینترنت سرویس‌دهنده‌های DNS به‌کار می‌آیند. می‌توانید تصور کنید یک فایل منفرد حاوی تمامی سرویس‌دهنده‌های اینترنت چقدر بزرگ است؟ خوشبختانه، هر سرویس‌دهنده DNS برای یک قلمرو DNS بخصوص تنها مسؤول اطلاعات خویش است.



***یادداشت** : هر قلمرو DNS (میدان دید مسؤولیت برای اسم‌گذاری) می‌تواند بسیار بزرگ باشد ـ برای مثال، com. میلیونها زیر قلمرو دارد jotto.com,yahoo.comو غیره)؛ از سوی دیگر، قلمرو ممکن است کوچک باشد ـ برای مثال feldman.org تنها یک میزبان (www.feldman.org) داشته و فاقد زیرقلمرو می‌باشد.*

با آسانترشدن مدیریت سرویس‌دهنده‌های DNS و عضویت بلامنازع برای دسترسی به اینترنت، با گذشت زمان، آنها را در مجموعه‌های کوچک بیش از پیش خواهید دید. ذکر این نکته ضروری است که هر سرویس‌دهنده DNS تنها مسؤول قلمرو خویش می‌باشد، بنابراین اگر نمی‌توانید به آدرس بخصوصی (مثلاً، yahoo.com) دسترسی داشته باشید، اما می‌توانید به سایت دیگری (مثل jotto.com) متصل شوید، ممکن است سرویس‌دهنده نام برای آن ناحیه غیرفعال باشد. این امر در اینترنت به ندرت اتفاق می‌افتد، چرا که سازمان‌دهندگان DNS سرویس‌دهنده‌های DNS پشتیبان برای هر قلمرو را الزامی داشته‌اند. مشکلات DNS بیشتر در اینترانت سازمانی کوچکتر رخ می‌دهد، بخصوص اگر امکانات سازمان در یک جا متمرکز شده باشند.



نکته : *به خاطر داشته باشید که در صورت شکسته‌شدن و خراب‌شدن دکمه‌های تماس سریع ه می‌توانید خودتان با شماره‌ای تماس بگیرید. به طرز مشابهی، اگر نمی‌توانید با اسم به سایتی م شوید، شماره آن را امتحان کنید. برای مثال، می‌توانید به جای http://www.co.chatham.ga.us http://167.195.160.6 متصل شوید. در صورت کارکرد این ترفند، متوجه می‌شوید که مشکل ارتباط با سرویس‌دهنده‌های نام وجود دارد.*

WINS

میکروسافت که نمی‌خواست به DNS بسنده کند، سرویس نام دیگری را به نام WINS (سرویس نام اینترنت ویندوز[1]) ب ویندوز ابداع نمود. WINS یک سرویس نام مخصوص ویندوز برای TCP/IP می‌باشد و برای شبکه‌ای‌کردن کامپیوتر ویندوزی که از لحاظ جغرافیایی دور از هم قرار گرفته‌اند، به‌کار می‌رود (اغلب در شبکه محلی استفاده نمی‌شود). NS علاوه بر راهنمای اسامی سرویس‌دهنده‌ها، اسامی گروههای کاری و حوزه‌های NT را نگهداری می‌کند.

بعید است که WINS در نسل بعدی ماشینهای ویندوز وجود داشته باشد (گواینکه هنوز در ویندوز ۹۸ وجود دار میکروسافت درصدد است از سرویس‌های خودکار نام و سرویس‌های فهرست استفاده کرده و سرویس‌های نام TCP/IP با سرویس‌های اسم کاربر و رمز عبوری درهم آمیزد. نام این تکنیک، فهرست فعال[2] خواهد بود.

تصور فهرست، نظیر مفهوم سرویس‌های نام است، اما یک گام فراتر می‌رود: به جای تحلیل نام به یک عد سرویس‌های فهرست، جزییات بسیاری از داده در شبکه را ارائه می‌کنند. در اصل، سرویس‌های فهرست به کاربران اجاز می‌دهند از همه جا به جای یک سرویس‌دهنده بخصوص، به کل شبکه وارد شوند؛ سرویس‌دهنده‌های شبکه برای تخصیص حقوق امنیتی و غیره به سرویس‌های فهرست وابسته هستند.

این حالت به خاطر آنکه سرپرستان شبکه دیگر نیازی ندارند که اطلاعات اسم کاربر و رمز عبور را د سرویس‌دهنده‌های چندگانه به‌روز درآیند جالب است. به جای آن کار، این امکان وجود دارد که به‌روزدرآوری‌ها از یک نقطه صورت پذیرفته و در شبکه توزیع گردد. با اینکه هدف از این کار ساده‌سازی و آسانترشدن عیب‌یابی است، باید مواظب پیاده‌سازی‌های اولیه باشید. حتی DNS شرکت ناول ـ که «بهترین» سرویس فهرست لقب گرفته (چندین سال است که به‌کار برده می‌شود و به از آن پشتیبانی وسیعی به عمل می‌آید) ـ مشکلات عدیده‌ای داشت.

در آینده از یکی از سرویس‌های فهرست ـ خواه از آن میکروسافت ناول یا Acme باشد ـ استفاده خواهید نمود.

خلاصه

این فصل معرفی تقریباً کاملی دارد از مفاهیم شبکه‌ای که با آنها برخورد خواهید داشت. البته آن طور که آنها می‌گویند، مشکلات در جزییات خود را نشان می‌دهند. این فصل پایه خوبی را می‌سازد که می‌توانید اطلاعات عیب‌یابی خود را بر آن بنا نهید.

و اینها نکاتی هستند که باید به خاطر بسپارید:

- کارت شبکه نظیر تلفن، کامپیوتر را به دنیای خارج ارتباط می‌دهد. همچنین شناسه واحد خود (آدرس MAC) را داراست.
- بسیاری LAN براساس باس اشتراکی یا «خط جمعی» پایه‌ریزی شده‌اند. نظیر خطوط جمعی واقعی، خرابیها و

1- Windows Internet Name Service

2- Active Directory

مشکلات توسط کسانی که خارج از نوبت صحبت می‌کنند، ایجاد می‌گردد.

- بخش‌ها را می‌تواند از طریق سوئیچ‌ها به هم متصل نمود. همچنین از مسیریاب می‌توان برای مسیریابی بسته‌ها (جمله‌های یک مکالمه شبکه‌ای) به/از شماره‌های شبکه‌ای مختلف استفاده نمود.
- پروتکل‌های شبکه‌ای را می‌توان به زبانهای تکلم تشبیه نمود. برنامه‌ها نظیر آدمها نمی‌توانند که همه زبانها صحبت کنند، بنابراین لازم است قبل از عیب‌یابی برنامه، تعیین کنید که از کدام پروتکل استفاده می‌کند.
- سرویس‌های نام در شبکه، نظیر DNS و WINS ، این امکان را فراهم‌می‌سازند که بتوان به‌جای آدرس با اسمی‌سمبولیک به کامپیوترها اشاره نمود. البته، با از بین‌رفتن سرویس نام، می‌توان با آدرس‌های عددی به کامپیوترها متصل شد.
- سرویس‌های فهرست بیش از سرویس‌های آدرس ـ به ـ نام خدمات ارائه می‌کنند. آنها می‌توانند رد اطلاعات شبکه را نگه دارند، نظیر اسامی کاربران، رمزهای عبور و اطلاعات امنیتی.

کارگاه

پرسش و پاسخ

پرسش : آیا شبکه‌های اپل مکینتاش هم شبیه به شبکه تلفن کار می‌کنند، AppleTalk چطور؟

پاسخ : در این کتاب، در مورد کامپیوتر مک و کامپیوترهای بخصوص دیگر صحبت نمی‌کنم. تمامی مفاهیم عمومی شبکه مدنظر است.

هنوز هم رابط شبکه، رسانه اشتراکی، شماره‌های شبکه‌ای، سرویس‌های نام و غیره مطرح هستند ـ تنها مشخصات آنها متفاوت است.

AppleTalk یک پروتکل است و قواعد و قوانین خود را داراست، همانگونه که در TCP/IP یا IPX/SPX شهود می‌باشد.

پرسش : آیا لازم نیست بیشتر در مورد TCP/IP بدانم؟ آیا لازم نیست برای عیب‌یابی مسائل TCP/IP در آن خبره باشم؟

پاسخ : یادگیری هیچ موقع بیهوده نیست، اما همان طور که در فصول آتی ملاحظه خواهید نمود، برخورد واقع‌بینانه با بیشتر مسائل TCP/IP به دانش خاصی در مورد خود پروتکل نیازی ندارد ـ دانستن اطلاعاتی در مورد پیکربندی ایستگاه‌کاری و تکنیک‌های عمومی عیب‌یابی کفایت می‌کند.

پرسش : دوست شبکه‌ای‌ام می‌گوید سوئیچ‌ها و مسیریاب‌ها و پل‌ها همه یک چیز هستند. آیا این طور است؟

پاسخ : بستگی دارد از چه کسی سؤال کنید. البته، همگی آنها مکالمات (ترافیک) شبکه را از بخشی به بخش دیگر منتقل می‌کنند. همگی آنها روشهایی هستند برای متصل‌کردن بخشهای مختلف شبکه به یکدیگر. سابق، سوئیچ‌ها و پل‌ها همیشه به آدرس MAC گرایش داشتند و تنها به ترافیک در سطح DLC نگاه می‌کردند، چرا که کار با پروتکل قابل مسیریابی نظیر TCP/IP به محاسباتی نیاز داشت و کارها را کندتر می‌نمود. ابداعات جدید در مسیریابی و تکنولوژی سوئیچینگ سوئیچ‌های سطح ۳ (که به جای DLC به پروتکل وابسته است) واقع گردیده که می‌توانند نظیر مسیریاب‌ها سریع عمل نمایند. به عبارت دیگر، آنها می‌توانند هر بسته‌ای را دریافت کرده و با حداکثر سرعت ممکن انتقال دهند. از طرف دیگر، به نظر می‌رسد که تجهیزات سطح بالا و هیبرید، خط بین ابزار مورد نظر را کم‌رنگ ساخته‌اند. عملکرد سوئیچ یا مسیریاب به

مشخصات در نظر گرفته شده توسط تولیدکننده بستگی دارد؛ اگر سؤالی را در مورد سوئیچ یا مسیریاب خود دارید، بهتر است راهنمای آن را بررسی نمایید.

پرسش : مفهوم اینترانت در مقابل اینترنت چگونه در مقایسه تلفنی تشبیه می‌گردد؟
پاسخ : تصور کنید اینترانت، سیستم تلفن داخلی شما و اینترنت سیستم جهانی تلفن است.

آزمون

۱- درست یا نادرست؟ برخی از کارت‌های شبکه، به صورت توکار به سرویس‌های نام مجهز هستند.
۲- کدام مورد را همه کارت‌های شبکه دارا هستند؟

الف ـ شماره‌های تلفن
ب ـ شماره‌های حک‌شده
ج ـ آدرس‌های حک‌شده
د ـ آدرس‌های تلفن

۳- کدامیک آدرس MAC صحیحی می‌باشد؟

الف ـ 00-55-D5-AA-D5-AA-D5-AA
ب ـ ad-00-a2-00-ad-30-c0
ج ـ 00-00-c9-aa-c5-50
د ـ c9-aa-50

۴- کدام تعریف استعداد آن را دارد که مسیریاب‌ها را تشریح کند؟
الف ـ مسیریاب‌ها ابزار بررسی شبکه هستند.
ب ـ مسیریاب‌ها بسته‌ها را از نقطه A به نقطه B می‌فرستند.
ج ـ مسیریاب‌ها به بسته‌هایی از شبکه مشکل‌دار گوش فرامی‌دهند.
د ـ از مسیریاب‌ها می‌توان برای اتصال شبکه‌هایی با آدرس‌های MAC بد استفاده نمود.

۵- درست یا نادرست؟ هاب، یک سگمنت شبکه‌ای اشتراکی ایجاد می‌کند.
۶- هر آدرس TCP/IP _____ می‌تواند برنامه‌های مبتنی بر TCP/IP را از عملکرد بازدارد.
۷- اگر آدرس TCP/IP کامپیوتر شخصی شما، 200.1.5.26 است و ماسک شبکه‌تان نیز 255.255.255.0 می‌باشد، آدرس گره شما عبارت است از _____ و آدرس شبکه‌تان نیز معادل _____ می‌باشد.
۸- درست یا نادرست؟ بسته باید آدرس منابع و مقصد را در خود داشته باشد.
۹- DNS یک _____ می‌باشد.

الف ـ سوکت
ب ـ سرویس
ج ـ سرویس‌دهنده
د ـ ب یا ج

پاسخ به سؤالات آزمون

۱- نادرست
۲- ج
۳- ج
۴- ب
۵- درست
۶- تکراری
۷- 200.1.5; 26
۸- درست
۹- د

فصل ۲

نمی‌توانید بیش از اندازه مستندات، پول یا سرگرمی داشته باشید

آیا پیش آمده که مسافرت زمینی خود در کشوری غریب را بدون نقشه آغاز کنید؟ البته که این کار را نمی‌کنید، اما این همان عملی است که همه‌روزه افرادی که شبکه‌های رو به رشد خود را مستندسازی نمی‌کنند، مرتکب آن می‌شوند. زمانی که هنگام عیب‌یابی فرا می‌رسد، نقشه‌ای ندارند که از روی آن پیش بروند و شانه‌هایشان را بالا انداخته، سرشان را تکان می‌دهند. درک شبکه‌های مستندنشده بسیار مشکل است. روشهایی را برای تحمل‌کردن مشکلات نیاز دارد و مستندات شبکه می‌توانند در دریای اشتباهات، نقش قطب‌نما را بازی کنند.

راهبری یک مجموعه شبکه‌ای بد

کسانی به شما خواهند گفت که مستندسازی کامل دردسر زیادی دارد. یا خیلی زمان می‌برد و به آن اندازه به‌کار نمی‌آید. این موضوع در بین موارد دیگر اهمیت ویژه‌ای دارد. در مقام مقایسه، افرادی که بدون مستندات شبکه‌ای را عیب‌یابی می‌کنند، خود را به آب و آتش می‌زنند، این در حالی است که افراد مجهز به شبکه‌های مستندشده، مشکل را حل کرده، بعد از آن کار مؤثر دیگری انجام داده و آنگاه برای بازی‌کردن با بچه‌هایشان به منزل رفته‌اند. این مقایسه ممکن است اغراق‌آمیز به نظر برسد، اما گذشته نشان می‌دهد که شما می‌توانید کارتان را مستندسازی کنید تا مرجعی هنگام بروز مشکلات داشته و یا آنکه کاری به مستندسازی نداشته باشید تا در هر بحران چندین برابر مقدار لازم، وقت بگذارید.

مستندات ناکافی هنگام بروز مشکلات شبکه‌ای نه تنها وقت را تلف می‌کنند، بلکه باعث اشتباه و انجام امور نالازم می‌گردند.

در این راه در داشتن موقعیتی آشکار هنگام آغاز کار عیب‌یابی، به خودتان مدیون هستید.

باور کنید که هنگام تلاش برای رهیافت از مجموعه شبکه‌ای خراب به اندازه کافی شک و عدم اطمینان وجود دارد، پس دیگر این تردیدها را با کمبود یک نقشه خوب زیاد نکنید.

فواید مستندسازی

داستانهای هولناک و هشدارهای ترسناک دیگر کافی است! اجازه دهید آثار منفی منتج از فقدان و کمبود مستندات را کنار بگذاریم. در طرف مثبت، با داشتن سطح قابل قبولی از مستندات، فواید ملموسی را شاهد خواهید بود. شاید، فایده مهم شبکه

مستندسازی‌شده، آن است که می‌توانید از آن دور شوید. می‌توانید بدون نگرانی از خراب‌شدن چیزی، تعطیلات بروید. آنجا که تنها مشخصی نیستید که به اطلاعات چگونگی پیکربندی و تنظیم شبکه اشراف دارد، می‌توانید از آفتاب ساحل تعطیلات‌تان بدون خاموش‌بودن تلفن و ترس از فراخوانده‌شدن لذت ببرید. کار روزانه بیشتر از آن است که فردی را به دنبال خود این طرف و آن طرف کشانده زیر و بم شبکه را به وی نشان دهید، این کاری است که مستندات برایتان انجام می‌دهند و این امکان را فراهم می‌سازند که به کاری دیگر بپردازید. جدول ۱-۲ چهار نوع اصلی مستندات شبکه را نشان می‌دهد.

جدول ۱-۲ : انواع سند

نوع	هدف
نقشه منطقی/عملیاتی	این نوع از مستندات دیدی کلی از چگونگی جریان‌یابی داده را به صورت عمومی نشان می‌دهد. ایستگاههای کاری مد نظر نیستند، تنها بخشهای مهم شبکه (نظیر سرویس‌دهنده‌ها، مسیریاب‌ها و بخشهای شبکه) نشان داده می‌شوند.
نقشه فیزیکی/طرح	این نوع از مستندات، اطلاعات دقیق شبکه را نشان می‌دهند، شامل تمامی سیم‌ها، هاب‌ها، سوئیچ‌های محلی و ایستگاههای کاری.
برچسب‌زدن کابل‌ها و ابزارها	این نوع از مستندات، برچسب‌هایی فیزیکی را شامل می‌شود که در قالب حروف بزرگ و پررنگ، ابزارها و کابل‌ها را مورد شناسایی قرار می‌دهند.
جزئیات/شرح	این نوع از مستندات ممکن است شامل نوشتار منطقی از یک کاربرد یا سیستم و یا ثبت هر روزه آنچه که روی سیستم یا ابزار صورت می‌پذیرد، باشد و اغلب حاوی آنچه که در دید نیست و در مستندات تولیدکننده ذکرشده می‌باشد.

نقشه‌های منطقی/عملیاتی

این نقشه‌ها، احتمالاً همان مستنداتی هستند که بیشتر اوقات به آنها رجوع خواهید نمود. نقشه‌های منطقی/عملیاتی به شکل گونه‌ای از «نمودار org» شبکه مورد استفاده قرار می‌گیرند، و به گونه‌ای مناسب، نشان می‌دهند کدام ابزار یا سرویس‌دهنده، مسؤول کدام کار است، و اینکه کدام ابزار برای ادامه کار به سایر ابزارها وابسته هستند. در اینجا جزئیات اهمیت ندارند؛ آنچه به دنبال آن هستید، در واقع جریان کارهاست. می‌خواهید قادر باشید بدون به اشتباه‌افتادن با جزئیات نالازم، تشخیص دهید چرا دپارتمان A نمی‌تواند با سرویس‌دهنده صحبت کند، اما دپارتمان B می‌تواند.

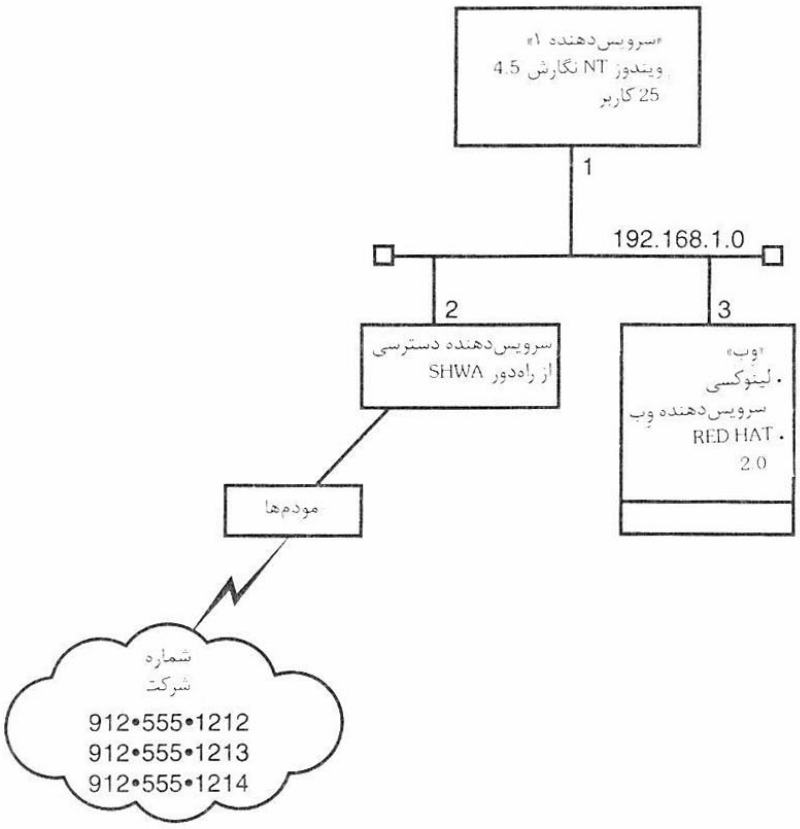
لازم نیست تک‌تک PC ها یا چاپگرها در این نمودار جای داده شوند، اما لازم است هر ابزاری که دیگران به آن وابسته هستند (نظیر سرویس‌دهنده‌ها و مسیریاب‌ها) معین و مشخص شوند. ممکن است لازم باشد در مورد واردکردن تک‌تک هاب‌ها یا سوئیچ‌ها در این نوع نمودار تصمیم‌گیری کنید، البته این موضوع به گروهی یا تکی عمل‌کردن آنان بستگی دارد. به بیان دیگر، در این نوع نمودار، هاب‌ها و سوئیچ‌ها (که در یک «همسایگی» هستند)، اغلب به شکل متکی به خود به نمایش گذارده می‌شوند، اما ممکن است حالاتی وجود داشته باشند، که در آن سوئیچی که دو «همسایگی» مختلف را به هم متصل می‌کند، به شکل مجزایی نشان داده شود. شکل ۱-۲ مثالی از یک شبکه منطقی ساده را نشان می‌دهد.

اگر شبکه‌ای دارید که پیچیده‌تر و بزرگتر از یک سایت می‌باشد، زمان آن است کاغذ دیگری بردارید (تلاش به درج همه چیز در یک نقشه بیهوده است و تنها به سخت‌تر خواندن‌شدن نقشه منجر می‌شود). در حالت کلی، سایت‌های چندگانه به

نمای سطح بالای جداگانه‌ای نیاز دارند که در آن چگونگی ارتباط‌های بین سایت‌های مختلف ترسیم می‌گردد. هر سایت با کادری نشان داده می‌شود که به نقشه جزئیات جداگانه‌ای اشاره می‌کند و نشان‌دهنده چگونگی اتصال سایت به نقشه‌های دیگر است. شکل ۲-۲ مثالی در مورد نقشه نمونه برای شبکه‌ای پیچیده‌تر را به تصویر می‌کشد.

نقشه‌های فیزیکی

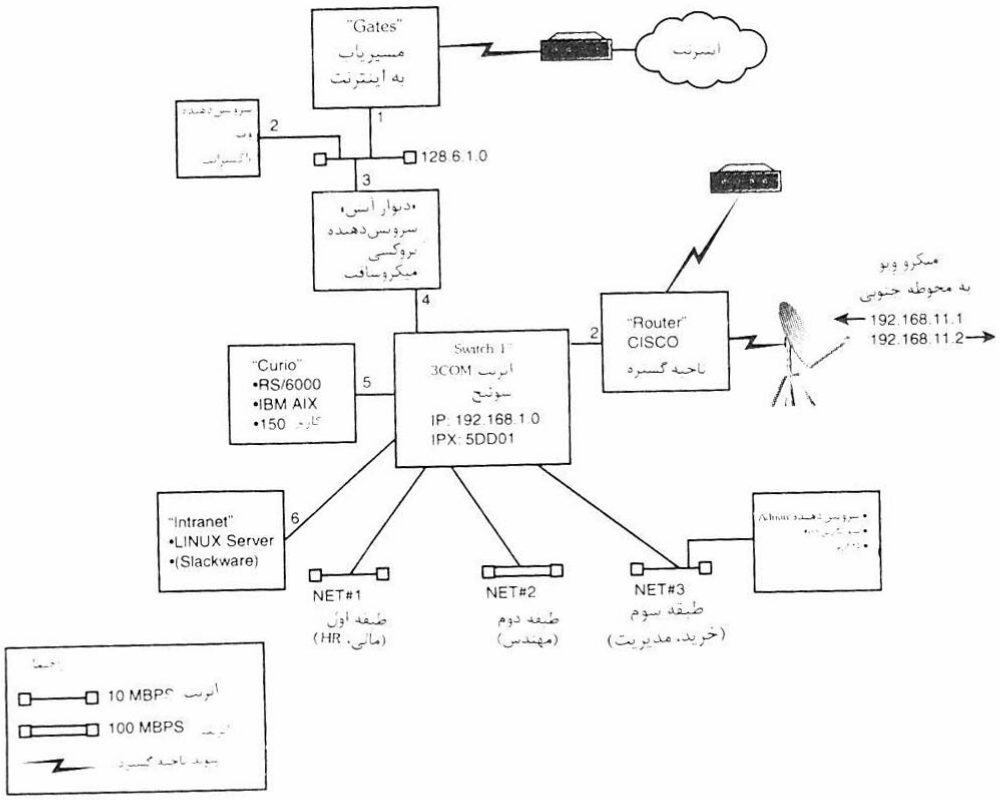
واضح است که نقشه‌های فیزیکی به دنیای فیزیکی ربط پیدا می‌کنند ـ یعنی اینکه چیزها به صورت واقعی چگونه هستند. از آنجا که نقشه‌های فیزیکی به گونه‌ای باورنکردنی جزئیات بیشتری را نسبت به نقشه‌های منطقی دربر دارند، ترجیح می‌دهید که آنها را در لقمه‌هایی متناسب بجویید. برخی سایت‌ها ممکن است با تنها یک نقشه فیزیکی نیازشان مرتفع شود (در این حالات، اغلب کمتر از ۵۰ کامپیوتر) معمولاً بیشتر در سایت‌ها به یک نقشه فیزیکی در هر سایت نیاز داریم. این روش در بیشتر سایت‌ها تقسیم‌بندی خوبی است، چرا که کلیه سیمهایی که از هر PC، چاپگر، سوئیچ و هاب خارج شده نشان می‌دهد و نیز می‌تواند بزرگ شود. به همین شکل برای سایت‌های ساده‌تر، بسیار خوب خواهد بود اگر قادر باشید دست‌تان را روی طرح معماری هر طبقه در ساختمان گذاشته و سیم‌کشی شبکه‌ای و اتاق سیم مربوط به آن را اضافه نمایید. سایت پیچیده‌تر هم ممکن است به مستندات پیچیده‌تری به شکل نقشه تقسیم‌شده فیزیکی نیاز داشته باشد.



شکل ۱-۲: یک نقشه منطقی ساده.



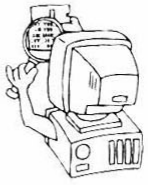
یادداشت : *منظور اشاره من به شبکه، شبکه فیزیکی یا بخش فیزیکی ـ گروهی از هاب‌ها که بدون مسیریاب یا سوئیچ متصل شده‌اند ـ می‌باشد (به عبارت دیگر «خط جمعی»). به هر هاب که از طریق یک سوئیچ یا مسیریاب متصل شده باشد، به شکل بخش فیزیکی جداگانه‌ای نگاه می‌شود. بخشهای بزرگ، نقشه‌های مجزای مربوط به خود را مطالبه می‌کنند.*



شکل ۲-۲: یک نقشه منطقی پیچیده‌تر.

برای مثال، حلقه ـ نشانه (که در فصل ۱۰، «اصول حلقه ـ نشانه» دقیق‌تر مورد بررسی قرار خواهد گرفت)، حتی در صورت اتصال تعداد زیاد هاب همواره «یک شبکه» باقی می‌ماند و می‌تواند بدون استفاده از مسیریاب‌ها به چندین دفتر کار توسعه یابد. از آنجا که در این حالت، شبکه فیزیکی پیچیده است، یک نقشه تقسیم‌شده فیزیکی مجزا مناسب خواهد بود (شکل ۲-۲ را ملاحظه کنید). می‌توان از یک صفحه کاری مستندسازی فیزیکی، بدون اهمیت داشتن نوع شبکه، به عنوان مرجع سریعی برای دسترسی به اطلاعات آن شبکه فیزیکی خاص استفاده نمود (شکل ۲-۴ را ملاحظه نمایید).

عموماً، این تمایل وجود دارد که جزییات بیشتری در اختیار قرار گیرد (تاکنون گریه کسی را به خاطر مفصل‌بودن جزییات موجود در نقشه‌ها مشاهده ننموده‌ام).



نکته : *نقشه‌هایتان را مطابق تغییراتی که می‌کنند، به‌روز درآورید. این کار را بخشی از «رعا»ی خود قرار دهید (رعا= روال عملیاتی استاندارد)[1]. در این راه از مشاور، تهیه‌کننده شبکه یا فروشنده کامپیوترها، بخصوص در صورتی که خود اقدام به افزودن ابزار می‌نمایید، کمک بگیرید.*

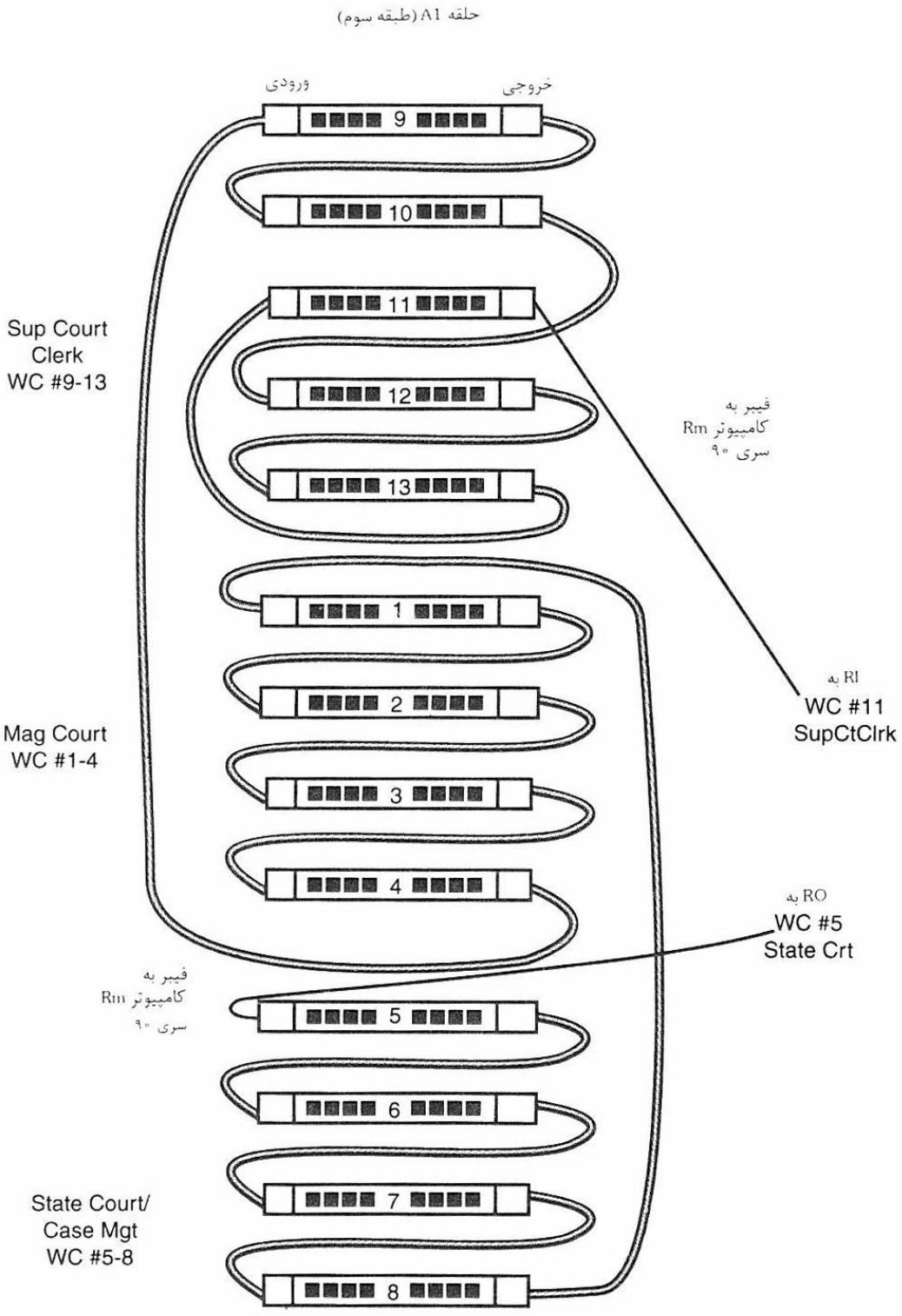


نکته : *برای نقشه‌هایتان تاریخ بگذارید! از آنجا که چیزها همواره تمایل به تغییر دارند، ممکن است در نهایت چندین نقشه از یک ناحیه عمومی داشته باشید. در صورت تاریخ‌داشتن روی هر نقشه، تعیین آخرین وضعیت موجود کاری آسان است.*

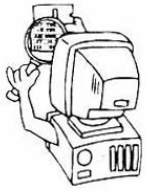
1- SOP=Standard Operating Procedure



نکته : استفاده از رنگ فکر جالبی است، اما ممکن است متوجه شوید که اشتراک نقشه‌ها با فروشندگان و عاملان دیگر که در تلاش هستند به شما کمک کنند، مشکل خواهد بود (برای مثال، تشخیص رنگها از طریق، مثلاً فکس، مشکل است). ایده بهتر آن است که از نشانهای مختلفی برای اقلامی که باید مشخص گردند، استفاده نمایید.



شکل ۳-۲ : یک نقشه فیزیکی برای حلقه ـ نشانه‌ای مثالی.



نکته : آن را ساده نگه‌دارید! افراد دیگری هم مستندات شما را مطالعه خواهند خود و هدف و مقصود شما آن است که آنان کاملاً مستندات را درک کنند. به همین خاطر، تلاش کنید که خطوط مستقیم و تمیز

به‌کار ببرید و از اسپاگتی نمودار جریان (خطوط متقاطع) بپرهیزید. اگر جزئیات بیشتری از یک د
مدنظرتان است، از صفحه دیگری کمک بگیرید.

صفحه ۰ مستندات شبکه بر شبکه فیزیکی # ـ با عنوان ـ واقع شده در ـ

محل / توضیح / شخص	آدرس MAC	آدرس IP#	تلفن #	جعبه‌دیوار #	پورت #	هاب #

شکل ۴-۲ : یک صفحه کاری مستندسازی فیزیکی.



نکته : نرم‌افزارهای نقشه‌کشی یا فلوچارت‌کشی می‌توانند خیلی زیاد به کمک بیایند، اما این اشتباه نکنید که هنگام یادگیری بسته نرم‌افزاری جدید، نقشه شبکه‌تان را ترسیم نمایید. اگر با برنامه آشنایی ندارید، نقشه شبکه را با دست ترسیم کنید ـ این باعث می‌شود که طرح سریعتر آماده شود. استفاده ا نرم‌افزار بسیار خوب است، چرا که تغییرات جزئی را به راحتی می‌توان به‌روز درآورد. البته، نیازی ب نرم‌افزاری پیچیده نیست، هر برنامه ساده ترسیمی کفایت می‌کند. به بیانی دیگر، هنگامی که عیب یابی را در پیش دارید، لازم نیست برای خود مشغله دیگری درست کنید.

برچسب‌زدن کابل‌ها و ابزارها

واضح است که نقشه به‌کار نمی‌آید، اگر نتوانید ابزاری را که روی آن نشان داده شده، پیدا کنید. نخندید. فروشگاههای زیادی را دیده‌ام که در آنها کسی نمی‌دانست مسیریاب کجاست. چگونه می‌توانید مسیریاب را راه‌اندازی مجدد کنید، اگر ندانید که کدام مسیریاب است؟ هر عیب‌یاب خوب، برچسب‌زدن واضح روی هر ابزار را قبل از بروز اشکال مدنظر قرار می‌دهد؛ کمبود و ضعف در برچسب‌ها، می‌توانند تا حدود زیادی زمان خرابی را افزایش دهند.



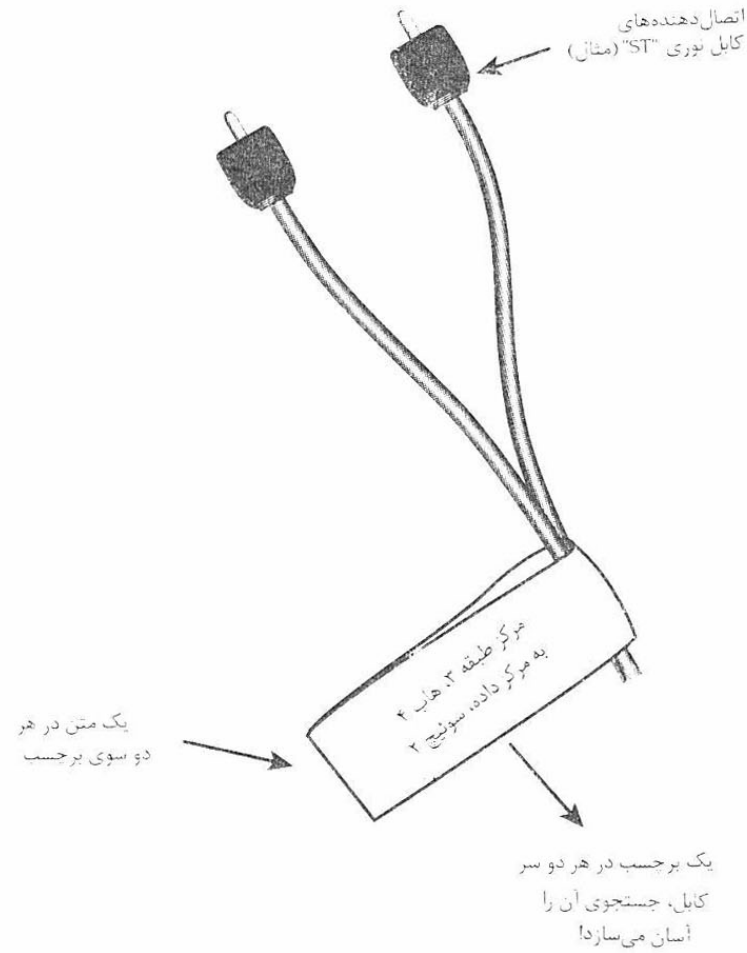
یادداشت : اگر از یکی از کشتی‌های جنگی جنگ دوم جهانی دیدن کنید، از حضور آن همه لوله و شیلنگ در سراسر کشتی و به خصوص در اتاق‌های ماشین‌آلات متعجب خواهید شد. نگاهی به روش

بسیار دقیق برچسب‌زدن روی لوله‌ها بیندازید؛ باور کنید که این کار را برای تفریح انجام نداده‌اند. لازم بود که بدانند کدام لوله محتوی هوا، بخار، آب تازه، سوخت، روغن یا آب شور است ـ تأخیر در تعمیر می‌توانست به غرق کشتی منجر گردد.

اگر آنقدر خوش‌شانس نیستید که شبکه‌تان به روش برچسبی نیروی دریایی مجهز شده باشد (و شخص نصب‌کننده نیز این کار را برایتان انجام نداده است)، لازم است از همین امروز شروع کرده و رفته‌رفته کار برچسب‌زنی را انجام دهید. هر زمان که متوجه شدید که وسیله‌ای چیست و یا کابلی به کجا می‌رود، برچسبی روی آن بزنید. فکر نکنید که به خاطرتان خواهد ماند ـ ممکن است که حافظه بسیار خوبی داشته باشید، اما درطی یک بحران، این حافظه ممکن است به تعطیلات رفته باشد. (همچنین، به خاطر داشته باشید که روزی خودتان هم به تعطیلات خواهید رفت و شخص دیگری باید بتواند کار عیب‌یابی را به انجام برساند).



نکته : *بروید بیرون و یک برچسب‌ساز بخرید. ارزش پولی آنها فقط ۵۰ دلار است، اما بسیار مفید هستند و می‌توانند برچسب‌های تمیز و خوش ظاهر را سریع ایجاد کنند. همچنین، می‌توانند برچسبی را دوبار چاپ کنید، و با یک‌بار بُرش، برچسبی دوطرفه برای کابل ایجاد نمایند، همان طورکه در شکل ۵-۲ نشان داده شده است.*



شکل ۵-۲ : استفاده از برچسب‌ساز برای ایجاد برچسب کابلی دوسویه.



هشدار : *باید خاصیت چسبندگی برچسب‌های خریداری شده را تست کنید، هیچ چیز بدتر نیست که ببینید بعد از ساخت ۲۵۰ برچسب و سپری‌شدن یک ماه، یکی‌یکی روی زمین می‌افتند هر چیز دیگری در شبکه، یک تست اولیه می‌تواند شما را از سردردهای آتی زیادی نجات همچنین، برچسب‌های کابل‌ها باید پلاستیکی باشند. در غیر این صورت، به مرور که با کابل‌ه می‌شود، ممکن است پاک شوند.*



نکته : *برچسب کابل باید با فاصله معینی از انتهای کابل قرار داده شوند (حدود ۱۲ تا ۱۸ اینچ جای کافی وجود داشته باشد). به این صورت، حتی با وجود ۵۰ کابل یا بیشتر که به یک سوئیچ تمرکزکننده‌ای دیگر متصل شده‌اند، به راحتی می‌توان برچسب‌ها را خواند.*



هشدار : *واقعاً لازم است که باتغییر اقلام یا انتقال آنها، برچسب‌ها به‌روز درآورده شوند. عیب می‌تواند وقت بسیار بیشتری از شما را به خود اختصاص دهد اگر فکر کنید کابلی درست است، حالی که چنین نبوده است.*

فرض کنید مسیریابی دارید که دفتر مرکزی زمین‌تان را به پایگاه شرکت در کره ماه متصل می‌کند. اگر اسم مسیر LOONIE باشد، یک برچسب مناسب برای آن عبارت خواهد بود از:

مسیریاب پایگاه ماه، منتقل‌کننده ماهواره Lookheed :)ONIE

کسانی را دیده‌ام که یک آدرس IP را روی چنین مسیریابی نصب می‌کنند؛ البته، این کار اختیاری است، اگر مستند کارای خوبی دارید که به طرز آشکاری مشخص می‌کند که LOONIE دارای دو آدرس IP است (مثلاً، 167.195.160.1 در طر زمین و 167.195.161.1 در سوی کره ماه). با این وجود، همان طور که مادربزرگم می‌گوید: «ضرری ندارد».

LOONIE دو اتصال در پشت خود دارد (یکی به شبکه محلی شما و دیگری به منتقل‌کننده ماهواره)؛ باید به هر اتصال نام ابزار و نقطه پایانی‌اش را برچسب بزنید. برای مثال، کابلی که به منتقل‌کننده ماهواره می‌رود را می‌توان به شکل زی مشخص نمود.

منتقل‌کننده ماهواره <- OONIE

برچسب دیگر، به صورت زیر خواهد بود:

LOONIE -> اتاق سیم #1، هاب #3

چرا باید کابلی که مستقیماً به LOONIE متصل شده است را با عبارت "LOONIE" برچسب بزنیم؟ خوب، تصور کنید باید کابل را جدا سازید. به این شکل، دانستن محل نصب هنگام بازگشت آسان خواهد بود.

من دوست دارم به هر دو سر کابل برچسب‌هایی با اسم ابزار متصل به کابل نصب کنم. به آن خاطر که دیگر برای تشخیص دو سر کابل، نیازی به فکر نخواهد بود. دیده‌ام که در سایت‌ها هر دوسوی کابل اسم منبع ذکر شده است، بنابراین تمام آنچه که می‌دانید، آن است که مسیریاب LOONIE، کابلی دارد که به LOONIE می‌رود.

بهتر است نگاهمان به برچسب‌زنی کابل، نگاهی دوطرفه باشد (هرچه باشد، یک برچسب‌ساز ۵۰ دلاری خریده‌اید و ساخت برچسب، آسان است). این کار حداقل اوضاع را بدتر نمی‌کند.

مستندسازی جزئیات/توضیحات

تفاوت بین یک سایت خوب ـ مستندشده و سایت حرفه‌ای مستندشده در جزئیات است. مستندات جزئیات ـ با وجود آنکه در رده غیرعملی‌ترین مستندات قرار دارد ـ می‌تواند ارزش سایر انواع مستندسازی‌ها را به خوبی زیاد کند. مستندات جزئیات به شکل نوشتار معمولی در مورد چگونگی انجام پیکربندی سیستم، در کنار استانداردهای ویژه سایت یا تجارب پراستفاده عیب‌یابی، می‌تواند ردیابی دوباره جای پاهای شما را برای دیگر آسانتر سازد. این نوع از مستندات، که شامل چگونگی‌ها و ترفندهاست، به طور گسترده‌ای با تواناییهای شما در ایجاد یک تعطیلات به شما یاری می‌رسانند.



نکته : *شما کاپیتان هستید، پس باید دفتر ثبت داشته باشید. پیداکردن زمان برای نشستن و یادداشت‌کردن توضیحات مربوط به تکنیک‌های عیب‌یابی قبلاً صورت گرفته، مشکل است، اما اگر نزدیک هر ابزار حساسی یک دفترچه ثبت قرار دهید، می‌توانید در عین حال به مستندسازی نیز بپردازید. عادت کنید که هر کاری که روی سرویس‌دهنده، سوئیچ یا مسیریاب انجام می‌دهید (و زمان و تاریخ این کار را) یادداشت کنید. این کار فرصت زیادی را هنگام ردیابی مجدد کارها صرفه‌جویی می‌کند. دفترچه‌های ثبت نیز در فراهم‌آوردن مستندات پشتیبانی برای فروشنده بسیار اهمیت دارند. برای مثال، واردکردن عبارت «سرویس‌دهنده جدید هر دوشنبه شب در ساعت 10:00 خراب می‌شود» ممکن است فروشنده را به این موضوع رهنمون سازد که برنامه مرتب‌سازی دیسک سخت که طبق برنامه در ساعت 9:50 دوشنبه شب‌ها اجرا می‌شود، ممکن است مشکل را ایجاد نماید.*

آیا ممکن است که بتوان یک شبکه مستندسازی‌شده را مهندسی معکوس نمود؟ البته، اما این مستلزم داشتن اطلاعات خوبی است. از آن گذشته، اتلاف وقت است اگر شبکه تحت نصب یا تغییر را همزمان مستندسازی کنیم. اگر با کابوس مستندسازی یک شبکه فصل ۲۴ روبرو هستید، «مهندسی معکوس شبکه» را مطالعه کنید.

آیا این هشداری است برای شما که هنگام عقد قرارداد نصب شبکه، از طرف قرارداد بخواهید مستندات خوبی را ارائه کند؟ بله! البته این احتمال وجود دارد که برخی از افراد حرفه‌ای این کار را برچسب‌زنی بیهوده‌ای می‌انگارند، اما در مورد شخصی که فکر می‌کند شبکه مستندنشده به معنای امنیت شغلی است، باید سختگیر باشید. اگر باید بیشتر بپردازید، یا مقداری مدلل، که باید جزیی باشد پرداخت کنید (بعلاوه زمان و پولی که در درازمدت پس‌انداز خواهید کرد)، یا آنکه فروشنده دیگری بیابید. فروشندگان زیادی هستند و نهایتاً، این شما هستید که از مزایا یا معایب مستندات شبکه و طرح کابل‌کشی بهره‌مند خواهید شد.

خلاصه

می‌توانید بهترین عیب‌یاب سراسر دنیا باشید، اما بدون مستندات، شما در دریایی قرار دارید که عاری از هر گونه قایق است. وجود مستندات به معنای ۱۰ دقیقه خرابی در مقایسه با دو ساعت و یا چیزی در حدود آن است، بنابراین، مقدار کمی کار اولیه می‌تواند در مدتی طولانی تأثیر ژرفی داشته باشد.

هر نوع مستندات به شکل و سوی خودش مهم است ـ برای مثال، برچسب‌های روی کابل‌ها، نقشه‌های مسیر کابل‌ها و دیاگرام‌های کاربردی محل سرویس‌دهنده، همچنین استفاده از یک دفترچه ثبت می‌تواند تاریخ را از تکرارشدن بازدارد. به عبارت دیگر، هنگام خرابی شبکه، نقطه‌ای مرجع در اختیار می‌گذارد.

کارگاه

پرسش و پاسخ

پرسش : من کابل‌ها را با شماره تعیین کرده‌ام، چون کاربرد هر کابل متغیر است و تعویض برچسب تمام کابل‌ها زمانبر است. آیا این حالت کفایت می‌کند؟

پاسخ : تجربه من می‌گوید خیر. کسانی هستند که همیشه رد شماره مورد استفاده را نگهداری نمی‌کنند و شـ مشخص‌کننده چیزی که در سوی دیگر قرار دارد نیست، بنابراین برای ترجمه شماره عددی کابل به ابزار فیزیکی، جدولی جداگانه نیاز است (که با تغییر ابزار باید آن را به روز درآورید). زحمت کار را به خود بقبولانید و توضیح برچـ کابل‌ها را ضمیمه سازید.

پرسش : چه چیزی را روی نقشه‌هایم باید مستند کنم؟ چه چیزی را نباید در نقشه‌ها منعکس نمایم؟

پاسخ : تکمیل‌بودن کلید پاسخ است. با کسب تجربه در انجام این کار و تمرین تکنیک‌های فصول آینده، احتمالاً به نقشه‌ه اولیه خود نگاه خواهید کرد و خواهید گفت: «نیازی نبود اینها را می‌نوشتم». البته، این موضوع را فقط بعد از کسب تجر درخواهید یافت. درحال حاضر، آن را یادداشت کنید؛ بعداً تغییرات لازم را اِعمال خواهید نمود.

پرسش : اوضاع به نظرم سردرگم‌کننده است. از کجا شروع کنم؟

پاسخ : می‌توانید کار را با نوشتن هر آنچه که در مورد شبکه می‌دانید شروع کنید ـ اسم سرویس‌دهنده، محل اتصال آ کامپیوتر شما به کام هاب متصل شده است و نظایر آنها. آنگاه می‌توانید دسته‌های مختلف مستندات را یادداشت کنید کارهای لازم انجام‌دادن برای هر دسته را فهرست کنید.

آزمون

۱- درست یا نادرست؟ مستندات منطقی، نشان‌دهنده کابل‌های متصل‌کننده جعبه‌های کابلی هستند.

۲- مستندات فیزیکی، باید شامل کدامیک از اقلام زیر باشد؟

الف ـ مجاری الکتریکی خروجی
ب ـ ناحیه‌ای کوچک از تمامی کابل‌ها و تجهیزات
ج ـ تصویری کلی از شبکه
د ـ تبادل اطلاعات سرویس‌دهنده ـ به ـ سرویس‌دهنده

۳- هنگام برچسب‌زدن انتهای مربوط به مسیریاب یک کابل چه چیزی را باید مشمول کنید؟

الف ـ اسم مسیریاب و پورت روی هاب
ب ـ اسم مسیریاب
ج ـ پورت‌های روی هاب
د ـ یا الف یا ج

۴- SOP مخفف ــــــــــ می‌باشد.

پاسخ به سؤالات آزمون

۱- نادرست

۲- روال عملیاتی استاندارد (Standard Operqtional Procodure)

۳- ج

بخش دوم

استراتژی‌های عیب‌یابی «جعبهٔ سیاه»

فصل ۳: روش دلتا: شناسایی تغییر شبکه
فصل ۴: روش ناپلئون: تفرقه‌بیانداز ـ و ـ حکومت‌کن
فصل ۵: روش خیابان سِسمی:
«یکی از چیزها شبیه بقیه نیست»
فصل ۶: روش SOAP: دادهٔ درونی، دادهٔ ظاهری،
تجزیه و تحلیل و طرح
فصل ۷: روش سادهٔ سیمون

فصل ۳

روش دلتا: شناسایی تغییر شبکه

چنین به نظر می‌رسد که در هر سرویس‌دهنده، اتاق سیم و به‌خصوص هر کامپیوتر شخصی ویندوز ۹۵، دشمنانی در کمین نشسته‌اند. اغلب، آنچه که ما دشمن می‌نامیم، نتیجهٔ آن است که کاربر چیزی را تغییر داده و آن را فراموش نموده (یا از آن اجتناب کرده) است.

همهٔ ما این‌کار را می‌کنیم؛ ما خودمان بدترین دشمنانمان هستیم. برای مثال فرض کنید که مرورگر را نصب می‌کنید و از آن خوشتان نمی‌آید، فراموش می‌کنید که آن را پاک نمایید و آنگاه روز بعد در دسترسی به اینترانت شرکت با مشکل مواجه می‌شوید. اگر خوش‌شانس باشید، فراموش نکرده‌اید که مرورگر جدیدی را نصب نموده‌اید، و این امکان وجود دارد که بعد از بازگشت نصب، همه چیز به‌خوبی کار کند. اما اگر بین این دو روز یک تعطیلات فراموش‌نشدنی را گذرانده باشید چطور؟ ممکن است مجبور شوید برای پیداکردن اشکال چندین ساعت «چرخهایتان را به‌گردش درآورید».

فاکتور انگشت شصت

این اهم هنگام تعمیر سرویس‌دهنده‌ها و مسیریاب‌ها نیز اتفاق می‌افتد. ممکن است تغییری در سرویس‌دهنده یا مسیریاب به‌منظور ارائهٔ سرویس جدید و یا حل یک مشکل، ایجاد نمایید. اگر در ابتدا چنین به‌نظر برسد که تغییر حاصله به‌خوبی کار می‌کند، آخرین چیزی که به‌عنوان منبع مشکل مورد توجه قرار می‌گیرد، همین تغییر خواهد بود. برای مثال، اگر ببینید که فایل آغازین سرویس‌دهندهٔ IntranetWare به‌طور خودکار دیسک خاصی را در دسترس نمی‌گذارد، ممکن است با ویرایش این فایل، بخواهید مشکل را برطرف کنید. روز بعد درمی‌یابید کاربران ویندوز NT ـ و نه ویندوز ۹۵ ـ از خاموش‌بودن ساعت دستگاههایشان به مدت ۵ ساعت شکایت دارند. ارتباطی وجود دارد؟ ممکن نیست! مشکل در پیکربندی NT است، ارتباطی به سرویس‌دهنده ندارد.

البته، در این سناریو که به تازگی برای من اتفاق افتاده در واقع مشکل کار در سرویس‌دهنده بوده است. این همان چیزی است که من آن را فاکتور انگشت شصت می‌نامم ـ هنگام ویرایش هر فایل پیکربندی (مهم نیست که تغییرات شما تا چه حد خوش‌خیم باشند)، ممکن است کاراکتر سرگردانی را استفاده نمایید که دستور کلیدی یا پارامتری را برای سرویس‌دهنده نامفهوم می‌سازد. در مورد حالتی که برای من پیش آمد، مشکل آن بود که من هنگام ویرایش فایل آغازین IntranetWare ، که به منظور انجام کاری کاملاً بی‌ضرر بود، کلیدی را به‌طور تصادفی در اول فایل زده بودم. اولین سطر فایل مسئول تنظیم قلمرو زمانی بود. به‌جای آنکه این سطر به شکل:

```
SET TIME ZONE=EST5EDT
```

باشد، به صورت زیر ویرایش شده بود:

```
\SET TIME ZONE=EST5EDT
```

وقتی که من فایل را با تغییرات «بی‌ضررم» ذخیره نمودم، به ناگهان سرویس‌دهنده از درک قلمرو زمانی خود عا
ماند، چرا که دستور SET\ را نمی‌شناخت. از آنجا که ویندوز NT متصل به Novell زمان را از سرویس‌دهنده می‌خوا
به‌طور گسترده‌ای به قلمروهای زمانی توجه می‌کند. شصت من به مدت پنج ساعت تمامی کامپیوترهای NT موجود
شبکه را عقب انداخت (ما در قلمرو زمانی شرقی هستیم، که پنج ساعت از زمان جهانی عقب‌تر است).

درسی که می‌گیریم این است: همیشه در ابتدا انگشت اشکال را به‌سوی خود بگیرید. همیشه فکر کنید «چه کاری را اخ
انجام داده‌ام؟». آنگاه، آماده باشید که تغییرات خود را به وضعیت اولیه بازگردانید. همان‌گونه که در فصل قبل توضیح دا
نگهداری یادداشت‌های مناسب ـ به‌خصوص به فرم یک کتابچهٔ ثبت ـ ایدهٔ بسیار خوبی است. به این شکل می‌توا
هنگامی‌که در یک تاریخ مشکلی بروز می‌کند، زمان بروز مشکل را با تاریخ‌های ثبت‌شده در کتابچه مقایسه نمایید.

البته بقیه کارکنان سازمان، ممکن است به اندازهٔ شما با مشکل سروکار نداشته باشند ـ به‌خصوص اگر شما مسئ
شبکه باشید. در این‌جا هم کتابچهٔ ثبت کمک می‌کند اما تنها نباید به موارد ثبت‌شده در آن تکیه کنید ـ گاهی لازم است
یکدیگر صحبت کرده در مورد کاری که انجام داده‌اید، بحث نمایید.



هشدار *: هنگامی‌که عیب‌یابی را آغاز می‌کنید، باید به تمامی افراد مراجعه کنید و در مورد هر تغ
انجام‌شده توسط آنها سؤال نمایید.*

به‌خصوص مهم است که هنگامی‌که شما (یا فروشنده‌تان) کاری را روی ابزاری انجام می‌دهد و بلافاصله آن را ارزیا
نمی‌نماید مورد توجه قرار دهید. در صورتی‌که ابزار مجدداً کار خود را آغاز نکند، تغییر انجام‌گرفته دیگر تغییر جدید
محسوب نمی‌شود و دیگر به‌صورت متهم نمی‌توان به آن اشاره کرد. البته، در صورت مورد توجه قراردادن این نکته چن
به‌نظر می‌رسد که کلیهٔ وسایلی که به‌تازگی کار خود را مجدداً آغاز نموده‌اند به‌عنوان ابزار منبع خطا می‌توانند در نظ
گرفته شوند.



هشدار *: به‌طور کلی، باید همیشه بعد از انجام تغییری در ابزار، مجدداً آن را راه‌اندازی کنید. گو
دیگری از این نگرش هنگامی است که کاربر دیگری، تغییری در جایی صورت می‌دهد و ابزار را مجد
به کار نمی‌اندازد. سپس شما سر می‌رسید و چیز دیگری را تغییر می‌دهید و با این‌که کاملاً در ایج
خطا بی‌گناه هستید، با آغاز مجدد کار ابزار، مشکلی را ملاحظه می‌کنید. من این مسئله را به این‌صورت
حل می‌کنم که قبل از آغاز تغییر چیزها، دستگاه را دوباره راه‌اندازی می‌نمایم. به این شکل، مطمئ
می‌شوم که تغییرات را در ابزاری صورت می‌دهم که به‌درستی کار می‌کند.*

مواظب فروشنده باشید

احتمالاً فروشندهٔ سیستم‌های شما، شکل ایده‌آل علایق شما را نمی‌شناسد. البته به‌خاطر داشته باشید، فروشنده با وجو
تمایل برای کمک به شما، دارای یک برنامهٔ زمان‌بندی است و دوست ندارد که افراد برای انجام کار بیش از حد لازم وق
صرف کنند و همچنین تمایل زیادی به فروختن اجناس بیشتر دارد. از آنجا که فروشنده پروژه‌های زمان‌بندی متعددی
دارد، این احتمال وجود دارد که شما بخواهید تغییراتی را در شبکه‌تان صورت دهید و این کار باید بر طبق زمان‌بندی مطابق

با نیازهای شما صورت پذیرد. آیا به لوله‌کش اجازه می‌دهید که گاه و بی‌گاه به خانهٔ شما بیاید و آبگرمکن منزلتان را دستکاری کند؟

برای پروژه‌های بزرگتر، لازم است روی طرح بازگشت[1] (که با عنوان طرح چتر نجات نیز شناخته می‌شود)، اصرار و پافشاری کنید. طرح بازگشت، هنگامی که کارها به صورت جدی خراب می‌شوند - یعنی وقتی که وضعیت فعلی از هنگام آغاز کار بدتر است - به جریان انداخته می‌شود. باید در مورد میزان ارزش این‌کار تصمیم‌گیری کنید: برخی اوقات بازگشت یک تغییر می‌تواند از لحاظ زمانی و هزینه‌ای ارزش زیادی داشته باشد. برای مثال، اگر یک سرویس‌دهندهٔ ویندوز NT را به سرویس‌دهندهٔ IntranetWare یا یونیکس تغییر داده باشید، ممکن است لازم شود یک تکنسین به تمامی ایستگاههای کاری سرکشی کند. بازگشت این تغییر می‌تواند زمان‌بر و در نتیجه هزینه‌زا باشد. از آنجا که فروشنده هزینهٔ طرح بازگشت را مطالبه می‌نماید، این موضوع ممکن است در مورد پروژه‌ای حیاتی به بحث گذاشته شود. هزینهٔ «به‌کار انداختن و بازگشت به وضعیت اولیه در صورت عدم کارکرد» ممکن است هزینهٔ متفاوتی با «مواجهه‌شدن با مشکل پیش‌آمده» داشته باشد. این موضوع را خود باید بررسی کنید و اگر با فروشندهٔ محترمی سروکار داشته باشید، وی در هنگام بحث در مورد پروژه و در صورتی که شما این موضوع را پیش بکشید، مشکلی را ایجاد نخواهد کرد.



***یادداشت** : داشتن ارتباطات خوب با فروشنده بسیار مهم است؛ فروشنده می‌تواند علت مشکل یا شریک عیب یابی شما باشد- بهتر است مورد دوم را هدف قرار دهید.*

عوامل خارجی

دو نوع فروشنده وجود دارند که برای ویران‌کردن شبکه‌تان به ساختمان محل کارتان مراجعه نمی‌کنند که عبارتند از ISP ها (فراهم‌آورندهٔ سرویس اینترنت)[2] که برای پیمایش وِب و ارسال پست‌های الکترونیکی به آنها اطمینان می‌کنید، و البته، شرکت‌های تلفنی، که سایت‌های شما را از طریق خطوط استیجاری به یکدیگر متصل می‌کنند. از بین این دو، شرکت تلفن، فروشندهٔ باسابقه‌تری است. شرکت‌های تلفنی مختلف مشکلات زیادی را ایجاد می‌کنند، اما از آنجا که این‌کار را چندین دهه صورت داده و سیاست‌های تغییر مدیریتی خوبی را در نظر دارند، مشکل عمده‌ای در ارتباط با آنها وجود ندارد. از طرف دیگر ISP ها کمتر از یک دهه است که کار خود را آغاز نموده‌اند و مشاهدهٔ مشکلات رو به رشد آنها و سرگردانی در ارتباط با آنها، امری قابل پیش‌بینی است.

روزهای دوشنبه ممکن است روزهایی دشوار باشند. ISP ها و شرکت‌های تلفنی در روزهای پایان هفته که بهره‌گیری از سیستم‌ها در این اوقات در سطح پایینی قرار دارند، تغییرات مورد نظر خود را اعمال می‌کنند. اگر چیزی که در جمعه درست کار می‌کرد، روز دوشنبه کار نکرد، بهتر است که تلفن را برداشته و به سرویس‌دهندهٔ مربوطه تلفن کنیم و بپرسیم که آیا چیزی تغییر نموده است؟ پاسخ ممکن است «هیچ‌چیز» باشد، اما اگر بدانید که از طرف شما هیچ تغییر و خرابی صورت نگرفته، ملاحظه خواهید نمود که مشکل به طرز اسرارآمیزی در زمان ناهار حل می‌شود.

در مورد مشکلات طولانی‌تر، ممکن است لازم باشد آنها را متقاعد کنید که در تجهیزات شرکت شما هیچ مشکلی وجود ندارد (یا این‌که دریابید خطایی وجود داشته و به‌خاطر ایجاد مشکل برای آنها عذرخواهی کنید). یک روش برای انجام این‌کار آماده‌سازی یک شبکهٔ آزمایشی است؛ اگر دو سایت قادر به ارتباط با یکدیگر نیستند ممکن است تجهیزات را به یکی

1- rollback Plan 2- Internet Service Provider

از سایت‌ها منتقل نموده و آنها را به‌صورت مستقیم به یکدیگر وصل نمایید. با انجام این‌کار و مشاهدهٔ کارکرد صحیح، خواهید شد که مشکل توسط سرویس‌دهندهٔ خارجی به‌وجود آمده و می‌توانید وی را قانع کنید که چیزی بین دو سایت یافته است.

نسبت ریسک به سود

برنامه‌های جدید جالب هستند. آنها امکاناتی ارائه می‌دهند که در نسخه‌های قبلی وجود نداشت و شاید بخواهید اولین نفر باشید که از آنها استفاده می‌نمایید. متأسفانه، تجربه نشان می‌دهد که هر ویژگی و امکان جدید، دو اشکال یا باگ را در محصول ایجاد می‌کند. سرعت گردن‌شکن عصر اینترنت بدان معنا است که تولیدکنندگان نرم‌افزار تحت فشار غیر قابل تحملی هستند که در بازار، اولین محصول را ارائه بدهند. اغلب این موضوع به تست سریع محصول، که به معنای باقیماندن برخی اشکالات در برنامه است، منجر می‌شود. به سایت‌های وِب مربوط به تولیدکنندگان نرم‌افزار مراجعه کنید ـ ملاحظه خواهید نمود که برای محصولاتی که حداقل شش ماه از ارائهٔ آنها گذشته، فهرستی از خطاهای برطرف‌شده وجود دارد که به صورت الکترونیکی قابل دریافت می‌باشد.

از آنجایی که کارهای بهتری از گزارش این اشکالات به فروشندهٔ نرم‌افزار را می‌توان در طی روز انجام داد، اجرای این فکر که اولین نفر در به کارگیری برنامهٔ کاربردی یا سیستم عامل جدید نباشید، مثمر ثمر واقع خواهد شد. مگر در صورت نیاز واقعی به امکانات جدید موجود در یک محصول، بهتر است شش ماه بعد از ارائهٔ آن و قبل از به کارگیری آن صبر نمایید. اگر لازم است این‌کار قبل از این مدت صورت پذیرد، آنچه را که جراحان نسبت ریسک به سود می‌نامند، مد نظر داشته باشید.

بعد از آنکه تصمیم گرفتید که استفاده از محصول جدیدی را آغاز نمایید، هنوز هم باید مطمئن شوید که در ابتدای کار با مشکلی مواجه نخواهید شد. برای مثال بسیاری از فروشگاههای IT قبل از ارائهٔ عملی ویندوز ۹۵، به‌طور داخلی و به‌صورت گسترده‌ای مورد استفاده قرار می‌دادند (البته استفاده از سیستم عامل جدید، دریایی از تغییرات را به‌دنبال دارد؛ مدت‌زمان یکسال زمان طولانی برای درخواست صفحه‌گسترده یا واژه‌پرداز جدید به شمار می‌رود). بخش مهمی از ارزیابی نرم‌افزار در مفهوم تولید محدود نهفته است. بعد از آنکه با محصول در ناحیه‌ای مجزا کار کردید، آن را به‌صورت محدودی ـ به‌عبارت دیگر در اختیار قراردادن محصول برای چند نفر از افراد که آن را تست نمایند ـ به‌کار ببندید. اگر خوب کار کرد، اغلب مشکل خاصی به وجود نخواهد آمد. از طرف دیگر در صورت بروز اشکال، تنها لازم خواهد بود عملیات بازگشتی برای تعداد محدودی از اشخاص صورت گیرد.

جنبهٔ دیگری که باید آن را در فکر داشته باشید، مفهوم عرضهٔ افزایشی است. این بدان معنا است که بعد از به کارگیری محدود، محصول یا سیستم را در اختیار افراد بیشتر و بیشتری قرار می‌دهید و این کار را به یکباره به انجام نمی‌رسانید. بنابراین این به کارگیری در قالب قطعات کوچکتر که رفته رفته بزرگ می‌شوند موفقیت بیشتری خواهد داشت. برای مثال ممکن است به پنج نفر برنامهٔ کاربردی جدیدی را بدهید. بعداً، این برنامه را در اختیار ده نفر دیگر، سپس پانزده، بیست و به همین ترتیب تا هنگامی‌که این میزان به سی نفر در هفته برسد ادامه دهید (در صورتی‌که اوضاع بر وفق مراد پیشرفت می‌کند). استفاده از عرضهٔ افزایشی تضمین می‌کند که در صورت بروز مشکل، حداقل تعداد افراد تحت تأثیر قرار گیرند.

حتی اگر در طی یک کاربردی این چنین مشکلی نداشته باشید، هر ابزار یا برنامهٔ کاربردی جدید ممکن است تأثیرات جانبی در بخش دیگری داشته باشد که با آنچه به تازگی مورد استفاده قرار گرفته، ارتباطی ظاهری ندارد. به همین خاطر یک قاعدهٔ خوب آن است که هنگام مشکلات ارتباطی یا شبکه‌ای، اقلام جدید را کنار بگذارید. مشکل ممکن است به ابزار یا

برنامهٔ جدید ارتباطی نداشته باشد، اما با خارج‌کردن آن از سیستم، در عمل منبع شک در مورد محل بروز مشکل را از بین خواهید برد.

اگر مشکل حل شد، می‌توانید آن را به فروشنده‌ای که محصول مشکل‌زا را از آن خریداری نموده‌اید انتقال دهید. البته مطمئن شوید که مشکل با معرفی دوبارهٔ برنامه یا ابزار به شبکه به‌صورت مجدد اتفاق می‌افتد.

باید سعی کنید به فروشنده حداکثر اطلاعات ممکن را ارائه کنید، بخصوص هنگامی‌که از پشتیبانی تلفنی بهره می‌برید تا تکنسینی بتواند موقعیت و وضعیت شما را برای خود دوباره‌سازی نماید. در این‌جا هم مستندات پشتیبان نظیر ثبت‌های دفتری و گزارشات ضمنی کلید حل مشکل خواهند بود ـ در واقع اگر که مشکل خود را در قالب نوشته ارائه کنید، بخش پشتیبانی فنی محصول توجه بسیار بیشتری به شما خواهد نمود.

خلاصه

بسیاری از مشکلات شبکه‌ای در نتیجهٔ تغییرات انجام‌شده توسط افراد می‌باشند. پیداکردن چنین تغییری مستلزم مستندسازی و ارتباط با اعمال انجام‌شده توسط خود و همچنین مصاحبه‌هایی با همکاران و فروشندگان خارج از شرکت می‌باشد. حتی تغییرات ناخواسته که در نتیجهٔ فاکتور انگشت شصت حادث می‌شوند، می‌توانند به‌صورت خیلی جدی شبکه را خراب نمایند. بنابراین توجه به این نکته که کجا بوده‌اید، بدون در نظر داشتن میزان ارتباط با مشکل، امری ضروری و مهم است. همچنین لازم است که از کار دیگران آگاه شوید و بنابراین تنها خود را به کتابچه‌های ثبت محدود ننمایید (با این‌که مستندسازی بسیار مؤثر است، اما به‌خاطر ناکامل‌بودن افراد و این‌که برخی اوقات فراموش می‌کنند آنچه انجام داده‌اند بنویسند، نمی‌توان به‌صورت کامل بر نوشته‌ها تکیه کرد).

قبل از به کارگیری محصول شبکه‌ای جدید، باید میزان ریسک را با مقدار سود احتمالی حاصله مقایسه نمود. در محصولات جدید این ریسک بسیار بالا است ـ و بنابراین لازم است حداقل چند ماهی را قبل از استفاده از محصولی جدید، صبر نمود. کاربرد محدود می‌تواند خطر احتمالی برای شبکه‌تان را کاهش دهد. همیشه باید یک طرح بازگشت را مد نظر داشته باشید، فقط به این خاطر که همیشه اوضاع در مورد محصولی جدید، مطابق انتظار پیش نمی‌رود.

کارگاه

پرسش و پاسخ

پرسش : به تازگی دو ایستگاه‌کاری ویندوز ۹۸ را نصب نموده‌ام. اما حالا، یکی از برنامه‌های ویندوز دیگر کار نمی‌کند حتی اگر تحت ویندوز ۹۵ اجرا گردد. اشکال کار در کجاست؟

پاسخ : موارد معدودی هستند که تفاوت‌هایی بین آنها در ویندوز ۹۵ و ویندوز ۹۸ وجود دارد ـ به‌عنوان مثال روشی که دیسک سخت قالب‌بندی می‌شود. بدون ملاحظهٔ ایستگاههای کاری شما تشخیص دقیق محل بروز خطا مشکل است، اما یک راه حل که در پیش دارید آن است که ویندوز ۹۵ را روی یکی از ایستگاههای کاری نصب نمایید تا این‌که ببینید که آیا ویندوز ۹۸ کل مشکل را به وجود آورده و یا این‌که اشکالی سخت‌افزاری وجود دارد (ممکن است بدون اطلاع شما برد اصلی دستگاه تعویض شده باشد).

پرسش : یکی از افرادی که در شرکت ما کار می‌کند، مرتباً چیزهایی را تغییر می‌دهد اما هرگز قبول ندارد که تغییرات دست او صورت گرفته، به خصوص هنگامی که چیزهایی خراب می‌شوند. چه‌کار می‌توانم بکنم؟

پاسخ : مگر در حالتی که رئیس این شخص باشید، کار زیادی نمی‌توانید انجام دهید البته احتمالاً رئیس این فرد عملکرد را در ایجاد اغتشاش ملاحظه خواهد نمود. متأسفانه این یک مشکل تکنیکی نیست، بلکه مشکلی اجتماعی است که باید از خود حل شود.

آزمون

۱- یک دستگاه نوار گردان تهیه‌کنندهٔ پشتیبان، از تعمیر باز گشته است. بعد از اتصال آن و راه‌اندازی دستگاه، کامپیوتر صفحهٔ BIOS متوقف می‌شود. چه کار انجام می‌دهید.

الف ـ با تعمیرگاه محلی خود تماس می‌گیرید.

ب ـ نوارگردان از دستگاه جدا می‌کنید.

ج ـ با دوستتان که به کامپیوترها وارد است، تماس می‌گیرید.

د ـ Ctrl+Alt+Del را فشار می‌دهید.

۲- نرم‌افزاری را به سرویس‌دهندهٔ NT خود اضافه نموده‌اید که به راه‌اندازی مجدد نیاز دارد. البته در این بین، آخرین دفعه‌ای که سرویس‌دهندهٔ خود را راه‌اندازی نموده‌اید به خاطر ندارید. بعد از راه‌اندازی مجدد، پیغامی را ملاحظه می‌کنید مبنی بر این‌که سرویسی برای شروع کار با مشکل مواجه شده است. نرم‌افزار را از روی سیستم برمی‌دارید و دوباره دستگاه را راه‌اندازی می‌کنید. همان پیغام ظاهر می‌شود. چه‌کار انجام می‌دهید؟

الف ـ با میکروسافت تماس می‌گیرید.

ب ـ پرس و جو می‌کنید تا ببینید آیا اخیراً کسی چیزی را تغییر داده است.

ج- نرم‌افزار را دوباره نصب می‌کنید.

د- پرس و جو می‌کنید تا ببینید آیا کس دیگری می‌تواند نرم‌افزار را نصب نماید یا خیر.

۳- درست یا نادرست؟ محصولات جدید اغلب خالی از اشکال هستند.

۴- درست یا نادرست؟ سرکشی‌های برنامه‌ریزی شده از طرف فروشنده (در مقابل ملاقات‌های درخواستی) با صرفه‌جویی در زمان می‌شود.

۵- تمامی افراد قطع اتصال شبکه را از دیروز تجربه نموده‌اند. تنها تغییراتی که به‌وجود آمده، شامل نصب نرم‌افزار ضد ویروس توسط جان روی PC خود، و دریافت یک PC جدید توسط ماری بوده‌اند. اولین قدم صحیح برای تحلیل این مشکل چیست؟

الف ـ خاموش‌کردن هر دو کامپیوتر تغییریافته.

ب ـ خاموش‌کردن PC ماری و روشن نگاه‌داشتن PC جان.

ج ـ خاموش‌کردن PC جان و روشن نگاه‌داشتن دستگاه ماری.

د ـ تنبیه جان و ماری برای به خطر انداختن محصول عمومی.

پاسخ به سؤالات آزمون

۱- ب

۲- ب

۳- نادرست

۴- درست

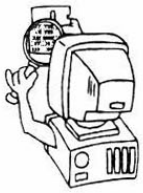
۵- الف

فصل ۴

روش ناپلئون: تفرقه‌بیانداز ـو ـحکومت‌کن

گفته شده که بعد از آنکه ناپلئون به عنوان امپراتور تاجگذاری کرد، بتهوون سمفونی Eroica خود را که قبلاً به بناپارت تقدیم کرده بود، به «خاطرهٔ قهرمانی بزرگ» تغییر داد. من تلاش می‌کنم که با مطرح‌کردن این داستان شما را مشغول نکنم اما روش‌های تفرقه‌بیانداز ـو ـحکومت‌کن که در این فصل مطرح خواهند شد، شما را به عیب‌یابی بزرگ تبدیل خواهند کرد؛ این روشها برای ناپلئون کار کردند، برای شما نیز کار خواهند کرد.

تفرقه‌بیانداز ـو ـحکومت‌کن دلالت دارد بر این مفهوم که محل مشکلی خاص را می‌توان به سادگی و از طریق تقسیم مشکل به بخشهای کوچکتر و قابل مدیریت، پیدا نمود. هنگامی‌که می‌دانید مشکل در یک ناحیهٔ معین (مثلاً بخشی از شبکهٔ فیزیکی یا جزئی از یک PC و یا پیکربندی مربوط به کاربران) قرار گرفته، می‌توانید این بخش از آن ناحیه را توسط تقسیم ناحیه به بخشهای کوچکتر پیدا کنید.



نکته : *نُه دفعه از هر ده دفعه تنها یک مشکل شبکه‌ای درکارها اختلال ایجاد می‌کند. مگر آنکه به‌تازگی دچار ساعقه‌زدگی شده باشید. احتمال بروز هم‌زمان بیش از یک مشکل بسیار نادر است. (تأثیرات جانبی را نیز باید مد نظر داشت).*

بازی اعداد

از آنجا که معمولاً یک مشکل در هر زمان وجود دارد، پیداکردن آن در شبکه‌ای هر چند بزرگ کار ساده‌ای است. برای مثال، فرض کنید که من عددی را از یک تا یک میلیون در نظر می‌گیرم و شما باید حدس بزنید که آن عدد چیست. اگر به‌طور ترتیبی بخواهید این‌کار را انجام دهید این احتمال وجود دارد که قبل از دستیابی به جواب ۹۹۹,۹۹۹ عدد را مطرح نمایید. البته اگر این حداکثر تعداد را نصف کنید و من با کلمات بیشتر یا کمتر به سؤال شما پاسخ بگویم، و تقسیم به نصف را ادامه دهید، حداکثر با ۲۳ حدس به پاسخ خواهید رسید. این پیشرفتی شگرف است. حرف مرا باور ندارید؟ به مثالی توجه کنید:

من: بسیار خوب، عددی بین یک و یک میلیون در نظر گرفتم.

شما: ۵۰۰,۰۰۰؟

من: نه، پایین‌تر.

شما: ۲۵۰,۰۰۰؟

من: نه، بالاتر.

شما: (مکثی برای محاسبهٔ ۲۵۰,۰۰۰ + ۲۵۰,۰۰۰/۲) ۳۷۵,۰۰۰؟

من: نه، پایین‌تر.

شما: (با نگاهی عاقل اندر سفیه به من برای انتخاب عددی بین ۲۵۰،۰۰۰ و ۳۵۰،۰۰۰) صبر کنید، ۱۲۵۰۰۰ عدد ۲۵۰،۰۰۰ و ۳۷۵،۰۰۰ وجود دارد و بنابراین وسط این اعداد عبارت خواهد بود از ... ۳۱۲،۵۰۰؟

من: نه، پایین‌تر.

شما: (ماشین حسابتان را درمی‌آورید) ۲۸۱،۲۵۰؟

من: نه، پایین‌تر.

شما: (سریعتر از گذشته) ۲۶۵،۶۲۵؟

من: (با تعجب) چگونه حدس زدید؟

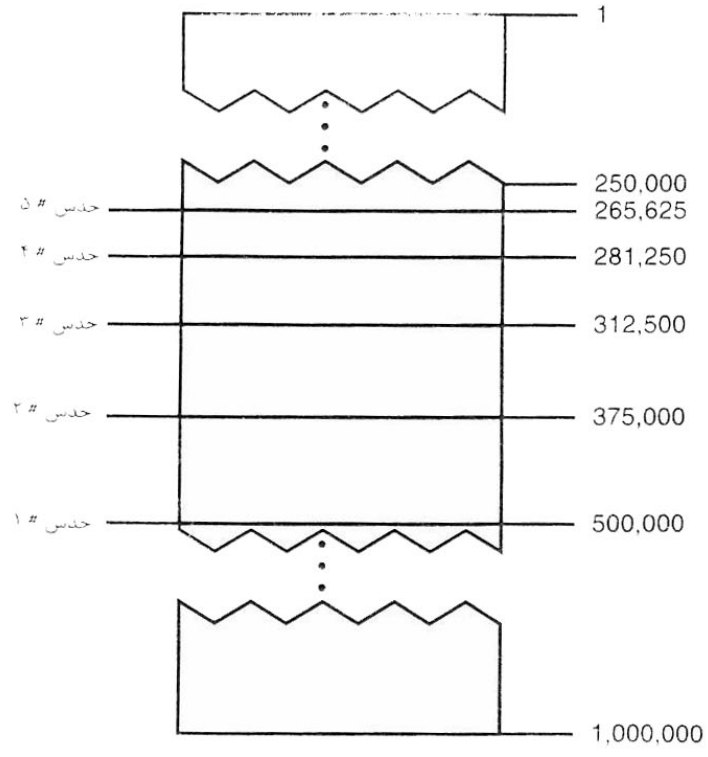
در واقع، این روال می‌توانست چند مرحلهٔ دیگر ادامه یابد، اما ایده را گرفته‌اید. گسترهٔ مورد نظر در ابتدا یک میلیون، گستره‌ای بسیار بزرگ. آنگاه به ۵۰۰،۰۰۰، سپس ۲۵۰،۰۰۰، ۱۲۵،۰۰۰، ۶۲،۵۰۰، ۳۱،۲۵۰، ۱۵،۶۲۵، ۷،۸۱۲ و به همین ترتیب تبدیل شد. ملاحظه می‌کنید که در هفت مرحله عدد به سرعت کوچک می‌شود و با ادامهٔ این روش تا هفت مرحلهٔ دیگر، تنها ۶۰ حالت ممکن باقی می‌ماند. تعجبی ندارد. همانگونه که در شکل ۱-۴ ملاحظه می‌کنید، تقسیم ناحیهٔ تحت جستجو، دامنهٔ جستجو را به نصف تقلیل می‌دهد.



یادداشت : *اگر می‌خواهید رئیس‌تان را تحت تأثیر قرار داده و یا از اسامی مرسوم استفاده نمایید، می‌توانید به این روش حدس‌زدن، جستجوی دودویی بگویید. حتی می‌توانید نمایش ریاضی این روش را روی پروژکتور اُورهِد بیندازید:*

$n = Log2\ (x)$

در این‌جا، x بزرگترین عدد در مجموعه، و n بیشترین تعداد حدس‌ها است.



شکل ۱-۴ : در جستجوی دودویی ناحیهٔ تحت جستجو با افزایش تعداد حدس‌ها، کوچک و کوچکتر می‌شود.

واترلوی عملیات شبکه متوقف است[1]

اکنون، اجازه دهید نگاهی داشته باشیم به آن چه که ممکن است هنگام پایین‌بودن شبکه انجام دهید. در وهلهٔ اول، چگونه تشخیص می‌دهید که شبکه پایین است؟ آیا مشکلی فیزیکی در شبکه اتفاق افتاده و یا مشکل مربوط به سرویس‌دهنده یا مسیریاب است؟ پاسخ: تفرقه‌بیانداز ـ و ـ حکومت‌کن. هنگامی‌که مشکلی به وقوع می‌پیوندد، باید کارتان را به‌صورت منطقی از کل شبکه (کل گسترهٔ اعداد از یک تا یک میلیون) به مشکل به‌خصوص (۲۶۵،۶۲۵) هدایت کنید. به احتمال زیاد کار خود را با روشن‌کردن این موضوع که مشکل مربوط به یک نفر (مشکلی محلی) یا گروه بزرگی از افراد (یک مشکل سیستمی) آغاز می‌کنید.

اگر تشخیص دهید که مشکل تنها به یک نفر محدود می‌شود، تکنیک سیستمی تفرقه‌بیانداز ـ و ـ حکومت‌کن شما کار خود را انجام داده و می‌توانید کار خود را با عیب‌یابی آن ایستگاه‌کاری ادامه دهید (که ممکن است به ترکیبی از تکنیک‌ها، از جمله تفرقه‌بیانداز ـ و ـ حکومت‌کن نیاز داشته باشد). در غیر این‌صورت، اگر مشکل به بیش از یک نفر محدود می‌شود لازم است که اطلاعات بیشتری را جمع‌آوری کنید. آیا همهٔ سیستم پایین است؟ اغلب خیر.



یادداشت : *من شاهد موقعیتی بوده‌ام که در آن همهٔ دستگاه پایین بوده‌اند که این در اثر خاموش‌کردن تصادفی UPS مربوط به اتاق تجهیزات اتفاق افتاده بود. این مشکلی است که «تأثیر دومینو» مربوط به دستهٔ بزرگی از مشکلات دیگر، شامل عدم سرویس‌دهی تلفنی، فقدان سرویس‌های شبکه و بی‌نظمی و اغتشاش کامل را باعث شده است.*

با یکسان‌شدن اهمیت زیرساختارهای شبکه‌ای و سیستم تلفن، مردم تمایل بسیار زیادی در استفادهٔ گسترده از این سیستم‌ها پیدا کرده‌اند. بسیاری سرویس‌دهنده‌ها مجهز به منابع تغذیهٔ مقاوم در برابر خرابی اضافی (دوگانه) می‌باشند و بنابراین اگر یکی از منابع تغذیه خراب شود، سرویس‌دهنده در کار خود باقی می‌ماند. از آنجا که اغلب سرویس‌دهنده‌ها به یک UPS (منبع تغذیهٔ بدون توقف یا واحد پشتیبان باطری‌دار) متصل هستند، این تمایل وجود دارد که هر منبع تغذیهٔ سرویس‌دهنده را به UPS متفاوتی متصل نمود؛ در غیر این‌صورت با خراب‌شدن UPSای که به تمامی منابع تغذیه متصل است، سرویس‌دهنده نیز از کار می‌افتد. این حالت ممکن است گران تمام شود، زمان بیکاری سرویس‌دهنده نیز هزینه‌زا خواهد بود. مجهزبودن شرکت شما به تغذیهٔ اضافی به این بستگی دارد که مدیریت به منظور دستیابی به قابلیت اطمینان و مقاوم‌بودن در برابر خرابی، بخواهد چقدر پول خرج کند.

وقتی که تشخیص دادید کدام گروه عملیاتی، در کار خود مشکل دارد، وقت آن فرا می‌رسد که تمام نقشه‌هایی که در فصل ۲ کشیدید به اجرا درآورید. افراد به شما می‌گویند که نمی‌توانند چیزی را در سرویس‌دهنده ثبت کنند، حروف مربوط به دیسک‌گردان‌ها محو شده‌اند، یا حتی تمامی PC های ناحیه آنها قفل کرده‌اند. باید این نکته را مشخص کنیم که این مشکل فقط در مورد این افراد وجود دارد یا تمامی کارمندان را دچار مشکل نموده است. همچنین ممکن است دانستن دپارتمان آنها مفید باشد. به همین صورت، می‌توانید نگاهی به خودتان بیندازید: اگر تمامی PC ها تا چند روز قبل می‌توانستند به شبکه متصل شوند، اما حالا نمی‌توانند برای تمامی اهداف و منظورها، بدون توجه به این‌که با یک مشکل اترنتی، یا مشکل سوئیچ یا سرویس‌دهنده مواجه هستیم، این PC ها کار نمی‌کنند.

۱- اصطلاح پایین‌بودن شبکه، هنگامی استفاده می‌شود که به دلایل مختلف شبکه یا قادر به سرویس‌دهی نیست و یا کار آن را به‌منظوری خاص متوقف نموده‌ایم.

نگاهی به نقشهٔ عملیاتی‌خود بیندازید تا بفهمید کامپیوتر افراد فوق‌الذکر در کجا قرار دارد. و بررسی کنید که چه‌چیزی مشترک هستند یا این‌که از چه طریق به سیستم متصل شده‌اند. به‌هنگام انجام این‌کار این احتمال وجود دارد مشخص گردد اشکال در کجاست. اگر دو دپارتمان می‌گویند که با مشکل مواجه شده‌اند، ممکن است سرویس‌دهنده‌ای استفاده می‌نمایند، پایین باشد ـ مستندات مربوط به جزییات کار را بررسی کنید! از سوی دیگر، اگر در نقشهٔ عملیاتی ملاحظه می‌کنید که تمامی گروه‌های مشکل‌دار، از یک مسیریاب به‌خصوص استفاده می‌کنند، زمان آن فرارسیده که بررسی آن مسیریاب بپردازید. اگر مشکل به یک بخش محدود می‌شود، احتمال زیادی وجود دارد که مسئله در فیزیکی آن بخش نهفته باشد.

بخشهای شبکه‌ای فیزیکی (یا اگر بخواهیم از زبان ساده استفاده کنیم، دسته‌ای از هاب‌ها) تناسب بسیاری عیب‌یابی با استفاده از روش تفرقه‌بیانداز ـ و ـ حکومت‌کن دارد. چرا یک بخش شبکه‌ای فیزیکی پایین می‌رود؟ اغلب به آنکه آنها شبکه‌هایی اشتراکی هستند (یا خطوط گروهی)، مشکل آن است که یک نفر بدون وقفه صحبت می‌کند و حرف زدن به کس دیگری نمی‌دهد (به فصول مربوط به اِترنِت و حلقه ـ نشانه مراجعه کنید). انواع گوناگونی تکنولوژی‌های جدید در «هاب‌های هوشمند» به‌کار گرفته شده‌اند که می‌توانند این حالت را شناسایی و متوقف نمایند. بنابراین بروز این نوع از مشکلات، امروزه دیگر معمول نیست.

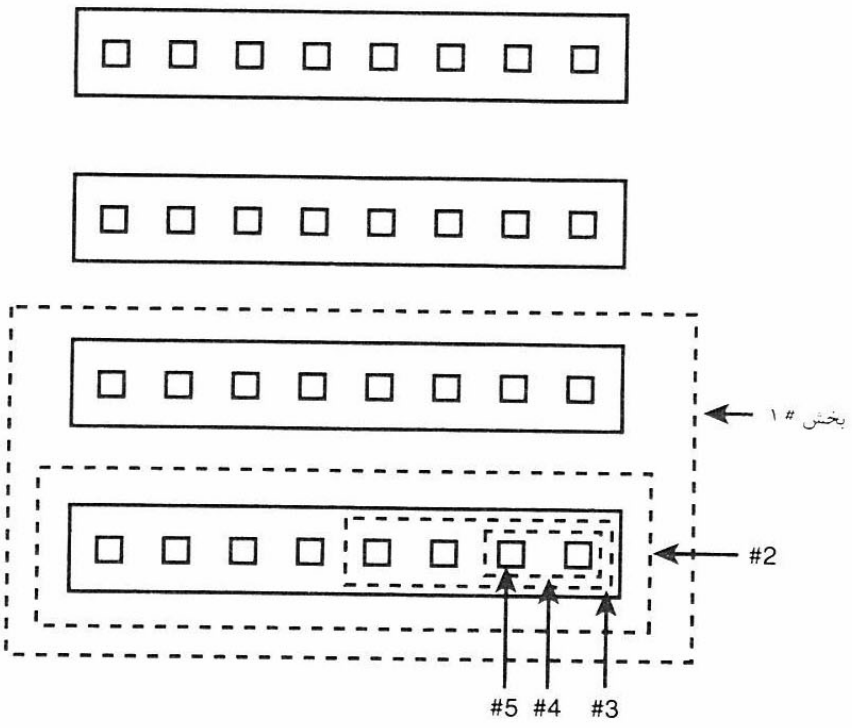


نکته : *هنوز هم گاهی ملاحظه می‌کنید که یک ایستگاه‌کاری باعث پایین‌آمدن یک بخش کامل می‌شود. این در حالتی است که در شبکه از سوئیچ‌ها استفاده نکرده باشید، چراکه حتی هاب‌های هوشمند هم با باهوشی شما نیستند (نه حتی به باهوشی تولیدکنندگانی که دوست دارند این‌گونه فکر کنند). به عبارت دیگر برای آنکه یک دستگاه بتواند بخشی را متوقف نماید، بیش از یک راه وجود دارد.*

جستجو در بخش

از آنجاکه به هر سیستم پیچیده به‌صورت مجموعه‌ای از سیستم‌های ساده‌تر نگریسته می‌شود و بدون نیاز به دانستن مشخصات هر یک از این سیستم‌ها. دلیل پایین‌بودن یک بخش خاص مهم نیست؛ تنها مسئلهٔ مهم آن است که بدانیم آن بخش از کار افتاده است. اولین کاری که بعد از تعیین پایین‌بودن یک شبکهٔ فیزیکی می‌توانید انجام دهید مراجعه به مستندات فیزیکی برای تعیین تعداد هاب‌ها یا اتاق‌های سیم درگیر در این شبکهٔ فیزیکی می‌باشد. این‌ها بلوک‌های ساختمانی مقدماتی شبکهٔ فیزیکی هستند. از آنجا که اغلب تعداد آنها در مقایسه با تعداد PC های موجود در شبکه کمتر است بهتر است از این مکان کار خود را آغاز نمایید. اگر تعداد هاب‌ها کم است بد نیست که یکی یکی آنها را مجزا نموده و ببینید که چه هنگام مشکل حل می‌شود (که در این صورت، هاب مشکل‌ساز را پیدا نموده‌اید).

اما اگر تعداد زیادی هاب دارید که به یکدیگر متصل شده‌اند ممکن است بخواهید از روش تفرقه‌بیانداز ـ و ـ حکومت‌کن که هنگام حدس عدد در نظر گرفته شده بین یک تا یک میلیون مورد استفاده قرار دادید، بهره ببرید ـ بسیار سریع‌تر است. نیمی از آنها را جدا کنید و ببینید که آیا ایستگاه‌کاری متصل به هاب‌های باقیمانده می‌تواند وارد شبکه شود. اگر نمی‌توانند بخش شبکه‌ای مشکل‌دار را پیدا کرده‌اید در غیر این‌صورت باید بخش دیگر را امتحان کنید. به تقسیم‌کردن بخش مشکل‌دار ادامه دهید. به‌زودی هابی را که، دردسر ایجاد نموده، پیدا خواهید نمود. در این نقطه، می‌توانید به خود هاب بپردازید و از طریق استفاده از همان روش تفرقه‌بیانداز ـ و ـ حکومت‌کن، پورتی که مشکل را ایجاد نموده، پیدا نمایید (شکل ۲-۴ را ملاحظه کنید).

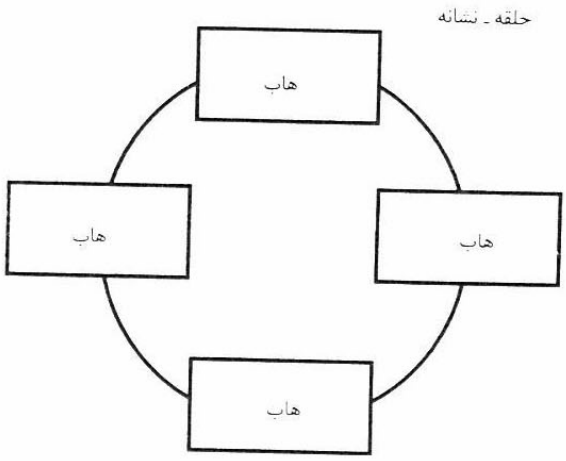


۳۲ پورت ـ ۵ حدس تقسیم‌کننده

شکل ۲-۴: پیداکردن یک هاب اِترنت با ۳۲ پورت به بیش از پنج حدس نیاز ندارد.

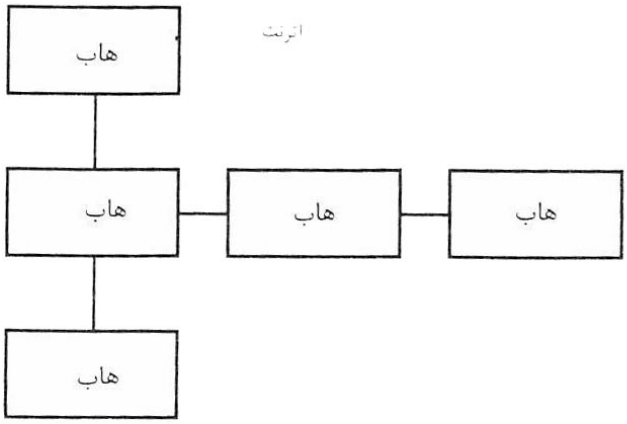


نکته : *هر هاب اِترنت برخلاف حلقه ـ نشانه اشتراکی (که تمامی هاب‌ها به شکل یک دایره که در شکل ۳-۴ نشان داده شده است، به یکدیگر متصل شده‌اند)، به بقیهٔ هاب‌ها در راستای یک خط مستقیم وصل شده است (همانگونه که در شکل ۴-۴ مشهود است). این بدان معنا است که اگر یکی از هاب‌ها را جدا کنید، هاب‌های بعد از آن را نیز جدا خواهید کرد. می‌توانید از طریق گذشتن از هابی که می‌خواهید آن را مجزا نمایید و اتصال به هاب بعدی در زنجیره، این مشکل را حل کنید. البته باید دقت کنید که قبل از قطع‌کردن چیزها، هاب آبشاری خود را کاملاً مشخص نمایید.*



شکل ۳-۴: یک شبکه حلقه ـ نشانه.

هنگامی‌که پورت ایجادکنندهٔ مشکل ـ یا حتی هاب حاوی آن پورت ـ را پیدا کردید، حتماً یک تجربهٔ آزمایشی روی آن انجام دهید (یعنی دوباره آن را به شبکهٔ اصلی بازگردانده و مطمئن شوید که هنوز هم ایجاد مشکل می‌کند).



شکل ۴-۴: یک شبکهٔ اِترنِت.

هشدار: اگر هابی که حاوی «چسب شبکه» است را جدا می‌سازید ـ این هاب، همان است که سرویس‌دهنده یا مسیریابی که شما را به سرویس‌دهنده متصل می‌کند، وصل است ـ هاب‌های دیگ قادر نخواهند بود که شبکه را ببینند و «پایین» باقی می‌مانند. اگر به این هاب مظنون هستید، بهتراس به‌جای برداشتن کل هاب، از روش تفرقه‌بیانداز ـ و ـ حکومت‌کن در سطح پورت‌ها بهره ببرید (یع بعد از تشخیص آنکه سرویس‌دهنده یا مسیریاب درست کار می‌کند). در غیر این‌صورت از ارتبا سرویس‌دهنده یا مسیریاب با بقیهٔ ایستگاههای کاری در بخش ممانعت به‌عمل می‌آورید و چنین تص می‌کنید که برداشتن این هاب مشکل را حل نمی‌کند (چرا که دستگاهها هنوز هم قادر نیستند ب سرویس‌دهنده یا مسیریاب برسند). در واقع، مشکل ممکن است یکی از ایستگاههای کاری در ها سرویس‌دهنده باشد، که می‌توانید به این مشکل با برداشتن پورت‌ها به‌جای برداشتن کل هاب برسی اگر لازم است هاب متصل به سرویس‌دهنده یا مسیریاب را بردارید، درستی یا خرابی آن را با بررس مستندات ارزیابی کنید و ببینید که آیا یکی از دستگاههای متصل به این هاب مشکل را ایجاد نموده خیر.

با پیداکردن پورت زمان آن فرامی‌رسد که به مستندات فیزیکی خود رجوع کنید تا بیابید کدام گره در شبکه از آن پورت استفاده می‌کند و آنگاه مشکل محلی را تشخیص دهید. در بیشتر حالات، این نوع از مشکلات از کابل شبکه‌ای خراب، کارت شبکه‌ای بد و یا حتی کامپیوتری که اشکال دارد ناشی می‌شوند.

در این‌جا هم، «هاب‌های هوشمند» به‌صورت خودکار انواع به‌خصوصی از مشکلات را پیدا می‌کنند و انجام این روال تا حدودی در این موضوع از «انتقال خودکار» در شبکه‌های اشتراکی، ابتدایی می‌باشد. البته خوب است بدانید که چگونه انتقالی استاندارد راهبری می‌شود؛ بعلاوه اگر بدانید که چگونه «استانداردی» را عیب‌یابی کنید، در درک بهتر چگونگی کارکرد ابزاری «خودکار»، راحت‌تر خواهید بود.

تقسیم کار

اجازه دهید به روزهای قدیمی داس بازگردیم. اگر تا کنون با داس کار کرده‌باشید برنامه‌های کوچک بسیاری را می‌شناسید که به آنها برنامه‌های TSR (برنامه‌های مقیم در حافظه) گفته می‌شود که خود را در حافظهٔ کامپیوتر نصب می‌نمودند و

برخی اوقات با سایر برنامه‌هایتان به نزاع می‌پرداختند. این مسئله در مورد کامپیوتر Apple شرکت مکینتاش نیز صادق بود، با این تفاوت که TSR ها، CDEV و INIT نامیده می‌شدند و همگی آنها نیز قادر به کار با یکدیگر نبودند. بنابراین اگر به کامپیوتر دیگری دسترسی نداشتید که به مقایسه بپردازید، لازم بود که یکی یکی از شر آنها خلاص شوید تا ببینید کدام‌یک باعث به‌وجودآمدن مشکل بوده است. البته، بیشتر اپراتورهای پشتیبانی فنی توصیه می‌نمودند که در ابتدا «راه‌اندازی وانیلی» ـ یعنی راه‌اندازی بدون هیچ‌یک از این برنامه‌های آغازین ـ را امتحان کنید. حدس بزنید آنها در واقع چه‌کاری را توصیه می‌نمودند؟ تفرقه‌بیانداز ـ و ـ حکومت‌کن! به‌جای سروکله زدن با هر برنامهٔ کوچکی، از تمامی آنها صرفنظر کرده و وجود مشکل را بررسی می‌نمودید. این‌کار نظیر کاری بود که با مشکل قبلی در هاب انجام دادید ـ هر بار نیمی از برنامه‌ها را کنار می‌گذارید تا برنامهٔ متخاصم را پیدا می‌کردید.



نکته : *در این‌جا چگونگی انجام «راه‌اندازی وانیلی» در ویندوز ۹۵ را ملاحظه می‌کنید.*

- *بعد از روشن‌کردن کامپیوتر از طریق فشردن کلید F8، کامپیوتر را در حالت safe راه‌اندازی کنید (قبل از ملاحظهٔ طرح آسمان آبی مربوط به صفحهٔ آغازین ویندوز). می‌توانید بسته به آنکه تست خود را به همراه شبکه یا بدون آن انجام می‌دهید، یکی از موارد Safe Mode یا Safe Mode with Network را انتخاب نمایید.*
- *کلید Shift را فشار داده و پایین نگه دارید (این روال برای ویندوز NT نیز کار می‌کند).*

اما برای انجام «راه‌اندازی وانیلی» از DOS:

- *بعد از روشن‌کردن کامپیوتر کلید F8 را فشار دهید. این‌کار امکان انتخاب بارگذاری TSR ها و راه‌اندازهای ابزار را در اختیار می‌گذارد.*
- *یک‌کپی پشتیبان از فایل‌های آغازین خود با کپی‌کردن AUTOEXEC.BAT در AUTOEXEC.BAK و CONFIG.SYS در CONFIG.BAK، تهیه نمایید. آنگاه به‌صورت دستی برنامه‌های TSR و راه‌اندازها را کنار بگذارید. بعد از انجام کار می‌توانید فایل‌های BAK را جایگزین فایل‌های اولیه نمایید.*

تمامی سیستم‌های شبکه‌ای منفرد از همین تکنیک استفاده می‌کنند. همانگونه در فصل قبل توضیح دادم بسیاری از مشکلات محیطی شبکه‌ای را می‌توانید تنها با بررسی تغییراتی که اخیراً صورت گرفته‌است پیدا نمایید. از طرف دیگر، بعضی اوقات تغییرات تحت نظارت شما صورت نمی‌پذیرند و از حادث‌شدن آنها غافل و بی‌خبر هستید. مثال‌های خوب از این موضوع شامل به‌روزدرآوری‌های پیمایشگر افزودنی‌ها و الگوهای حفاظت ویروسی می‌باشند. بنابراین هنگامی‌که تغییری مشهود نباشد باید به‌جای کوبیدن سر به دیوار به بررسی اصول بپردازید.

برای مثال، فرض کنید که تمامی افراد و کارکنان دفتر، با خاتمهٔ کار دستگاه خود مشکل دارند. همگی با صفحهٔ "Please Wait While Your Computer Shuts down" روبرو می‌شوند. چنین به‌نظر می‌رسد که هر کس باید خود به حل مشکل بپردازد. هیچ‌کس به‌تازگی چیزی را تغییر نداده و کسی هم قادر نیست از آنچه که پیش آمده سردرآورد.

با این‌که به‌نظر نمی‌رسد این مشکل مربوط به شبکه باشد، اما خرابی همهٔ کامپیوترهای شبکه‌ای عجیب به‌نظر می‌رسد. خوشبختانه می‌توانید از روش تفرقه‌بیانداز ـ و ـ حکومت‌کن برای پیداکردن آنچه که به‌واقع تغییر یافته، استفاده نمایید.

از آنجا که در دفتر شما، از ویندوز ۹۵ استفاده می‌شود، بسیاری از برنامه‌ها که در هنگام راه‌اندازی اجرا می‌شوند، در

منوی Startup قرار دارند. کلیه چیزهایی را که در این منو قرار دارند را برداشته و دستگاه را مجدداً راه‌اندازی کنید. ناگهان متوجه می‌شوید که می‌توانید به کار دستگاه خاتمه دهید. نیمی از برنامه‌ها را به پوشهٔ Startup بازگردانده و کار را آنقدر ادامه دهید تا منبع مشکل پیدا شود. فرض کنید اشکال در برنامهٔ آگاه‌ساز پُست الکترونیکی نهفته است. تصمیم می‌گیرید که راه‌اندازی را تنها با برنامهٔ مشکل‌دار انجام دهید و این‌بار هم موفق می‌شوید که کار دستگاه را خاتمه دهید.

در این‌حالت، دچار مشکل تداخل شده‌اید که از طریق روش محبوبمان، تفرقه‌بیانداز ـ و ـ حکومت‌کن، قابل حل است. مجدداً نیمی از برنامه‌ها را به فایل آغازین بازگردانده و به حالتی می‌رسید که در آن هم برنامهٔ حفاظت از ویروس و هم برنامهٔ آگاه‌ساز پُست الکترونیکی بارگذاری می‌شوند. همان‌گونه که حدس زده‌اید این وضعیت عیب‌یابی هم دقیقاً برای مواقع اتفاق افتاد ـ برنامهٔ حفاظت از ویروس که به‌صورت خودکار از اینترنت به‌روزدرآورده می‌شود، با برنامهٔ آگاه‌ساز پست الکترونیک تداخلی را ایجاد می‌نمود. جستجوی سریعی در سایت‌های وِب فروشندگان باعث شد که بتوانم سرویس‌گیرندهٔ پست الکترونیک خود را ترمیم کنم (مشکل از برنامهٔ حفاظت از ویروس نبود) و به مشکلی آزاردهنده پایان دهم. واضح است که روش تفرقه‌بیانداز ـ و ـ حکومت‌کن را همیشه نمی‌توان به‌عنوان روش پیداکردن مشکل مورد استفاده قرار داد، به‌خصوص، عیب‌یابی مسائل متناوبی و همچنین مشکلات کمیتی (و نه کیفیتی) که سناریویی سیاه و سفید (شکسته با نشکسته) را دنبال نمی‌کنند، سخت و طاقت‌فرسا خواهد بود.



یادداشت : *تفاوت بین مشکل کمیتی و کیفیتی را می‌توانید با به‌خاطرسپردن این‌که مشکل تجزیه و تحلیل کیفیت یک موقعیت (نظیر، «دستگاه من اصلاً قادر به چاپ نیست»). مشکل کمیتی تجزیه و تحلیل کمیت موجود در یک موقعیت می‌باشد (نظیر، «سرعت چاپ در کامپیوتر من از کامپیوتر دوستم آهسته‌تر است»).*

برای مثال روش تفرقه‌بیانداز ـ و ـ حکومت‌کن ممکن است در باور این مسئله که یک برنامهٔ کاربردی جدید باعث کاهش سرعت شبکهٔ شما شده است، مؤثر باشد (که البته ممکن است این موضوع واقعیت داشته باشد). از سوی دیگر، کنارگذاشتن برنامهٔ کاربردی جدید همیشه شدنی و عملی نیست و مشخص نیست که مشکل تنها با این برنامهٔ کاربردی خاص است و یا این‌که خود شبکه به‌صورت کلی در نقطهٔ اشباع قرار دارد. در این وضعیت ممکن است برنامهٔ کاربردی متفاوتی را امتحان کنید اما آیا واقعاً می‌توانید در زمان کوتاهی برنامهٔ کاربردی پراستفاده‌ای را کنار بگذارید؟ ممکن است ارزیابی برنامه را در مورد پیکربندی‌های نامتناسب آن کنار گذاشته و به بررسی عملکرد صحیح آن در شبکه همت گذارید.

حرف آخر این است: حتی روش تفرقه‌بیانداز ـ و ـ حکومت‌کن نمی‌تواند مستقیماً شما را به مشکل هدایت کند، اما در ارائهٔ مسیر صحیح می‌تواند مؤثر باشد.

خلاصه

مشکلی که لاینحل به‌نظر می‌رسد را می‌توان با شکستن آن به بخشهای کوچکتر، به شکل آسانتری حل نمود. مشکلات را می‌توان به دو روش تقسیم کرد: محل و جزء (سخت‌افزاری یا نرم‌افزاری). با این‌که شبکه‌ها سیستم‌هایی پیچیده و وابسته هستند و در آنها خرابی یک جزء باعث می‌شود که چنین به‌نظر برسد که همه‌چیز خراب شده است، اغلب تنها یک مشکل وجود دارد که تأثیرات جانبی را نیز به‌دنبال دارد. روش تفرقه‌بیانداز ـ و ـ حکومت‌کن به شما اجازه می‌دهد که اجزاء

مشکل‌دار را بدون دانستن دلیل خرابی پیدا کنید. هنگامی‌که با تعداد زیادی اجزاء یا مکان‌ها سروکار داشته باشید روش مذکور (که جستجوی دودویی نیز نامیده می‌شود) می‌تواند تعداد حدس‌ها را از میلیونها حالت ممکن به چند حالت معدود تقلیل دهد و بنابراین از لحاظ زمانی بسیار مقرون به صرفه است.

با این‌که روش تفرقه‌بیانداز ـ و ـ حکومت‌کن تمام و کمال روال عیب‌یابی نیست، اما در بیشتر موقعیت‌ها می‌تواند به‌عنوان ابزاری قدرتمند مورد استفاده قرار گیرد.

کارگاه

پرسش و پاسخ

پرسش : چرا باید برای عیب‌یابی در شبکهٔ شش گره‌ای خود از روش تفرقه‌بیانداز ـ و ـ حکومت‌کن استفاده کنم؟ پیداکردن هر مشکلی برای من به تنها شش حدس نیاز دارد!

پاسخ : حق با شماست استفاده از روش تفرقه‌بیانداز ـ و ـ حکومت‌کن در مورد تعداد ابزار کم، بیشتر مشکل‌زا است تا آنکه بتواند مؤثر باشد. البته استفاده از این روش باعث می‌شود که با کمتر از شش حدس به جواب مورد نظر دست بیابید.

پرسش : اگر پورت مسیریاب مشکلاتی داشته باشد، آیا چنین به‌نظر نمی‌رسد که کل شبکه پایین است؟

پاسخ : در صورتی‌که سرویس‌دهندهٔ محلی نداشته باشیم، بله. در این حالت می‌توانید از ایستگاههای کاری موجود در شبکه فیزیکی‌تان استفاده نمایید ـ این‌کار نقش بخش فیزیکی را ایفا می‌کند (برای کاربران ویندوز ۹۵ که از اشتراک فایل و چاپگر استفاده می‌کنند، تلاش کنید شخصی را بیابید که CD-ROM یا چاپگرش به اشتراک گذاشته شده است. در صورتی‌که TCP/IP نصب شده باشد، تلاش کنید ایستگاههای کاری دیگر در شبکه را Ping نمایید ـ اگر توانستید، مشخص است که شبکه پایین نیست).

پرسش: با این‌که من مشکلاتی با دستگاه خود دارم، روش تفرقه‌بیانداز ـ و ـ حکومت‌کن برایم دردسرزا است. نمی‌توانم هر آنچه را که در پوشهٔ Startup قرار دارد کنار بگذارم؛ در غیر این‌صورت قادر به کارکردن نیستم. پیشنهاد دیگری دارید؟

پاسخ: مشخصاً هر موقعیتی، منحصر به فرد است. روش تفرقه‌بیانداز ـ و ـ حکومت‌کن ممکن است در این موقعیت بهترین استراتژی نباشد. به‌جای آن ممکن است از خود سؤال کنید، «کدامیک از این چیزها نظیر بقیه نیست؟». اطلاعات بیشتر در مورد این استراتژی عیب‌یابی را در فصل آینده ملاحظه خواهید نمود.

آزمون

۱- استراتژی عیب‌یابی تفرقه‌بیانداز ـ و ـ حکومت‌کن چه‌کاری را برایتان میسر می‌سازد؟

الف ـ به‌صورت ریاضی جواب مشکل را محاسبه کنید.

ب ـ هر مشکلی در دنیا را با انجام جستجوی دودویی حل نمایید.

ج ـ محل وقوع مشکل را با تقسیم‌کردن ناحیهٔ مشکل‌زا به نصف، پیدا کنید (یا حذف نیمی از اجزاء بدون اشکال).

د ـ کار حل مشکل را بین افراد مختلف تقسیم نمایید.

۲- فرض کنید که عددی بین ۱ تا ۵۰۰ را در نظر گرفته‌اید. حدس دوم من ممکن است چه عددی باشد؟

الف ـ ۲۵ ب ـ ۲۵۰

ج ـ ۳۰۰ د ـ ۱۲۵

۳- اولین چیزی که هنگام شنیدن در مورد یک اشکال شبکه‌ای و تلاش برای حل آن باید مشخص کنید چیست؟

الف ـ تعیین آنکه مشکل برای یک کاربر یا چندین کاربر وجود دارد.

ب ـ بررسی مسیریاب.

ج ـ بررسی مستندات. د ـ بررسی خرابی در سرویس‌دهنده.

۴- یک مشکل شبکه‌ای را تا هابی که مسیریاب آن بخش روشن است دنبال نموده‌اید. بعد از آن چه می‌کنید؟

الف ـ کار را با روش تفرقه‌بیانداز ـ و ـ حکومت‌کن در سطح پورت ادامه می‌دهید.

ب ـ مسیریاب را از شبکه خارج می‌کنید.

ج ـ مستندات مسیریاب را بررسی می‌کنید. د ـ هاب را از شبکه خارج می‌کنید.

۵- مشکلی را تا یک دستگاه کامپیوتر با ویندوز ۹۵ ردیابی نموده‌اید، اما در مورد این‌که مشکل در کجاست اطلاعی ندار
چگونه یک «راه‌اندازی وانیلی» انجام می‌دهید؟

الف ـ با فشردن F8 در زمان راه‌اندازی و انتخاب Safe Mode.

ب ـ با فشردن کلید F5 در زمان راه‌اندازی و انتخاب Safe Mode.

ج ـ با فشردن کلید F8 در زمان راه‌اندازی و انتخاب Divided Mode.

د ـ با فشردن کلید F5 در زمان راه‌اندازی و انتخاب Divided Mode.

پاسخ‌های سؤالات آزمون

۱- ج ۲- د

۳- الف ۴- الف

۵- الف

فصل ۵

روش خیابان سسمی: یکی از چیزها شبیه بقیه نیست

روش «خیابان سسمی» بیشتر سرگرمی است تا کار سخت. این روش یکی از جالب‌ترین روش‌های عیب‌یابی است (حتی اگر ترانهٔ آن را هنگام کار زمزمه نکنید). اصل مورد استفاده به این صورت است: با در نظر داشتن گروهی از دو یا چند موجودیت در یک شبکه، تمام کاری که باید برای عیب‌یابی یکی از اقلامی که به درستی کار نمی‌کند انجام دهید، مقایسهٔ آن با ابزاری است که به درستی کار خود را انجام می‌دهد.

معمولاً تفاوت بین موجودیت‌ها، دلیل کارنکردن موجودیت مشکل‌زا است. برای مثال اگر فرزندانتان دوقلو باشد و یکی از آنها ـ آنکه به‌جای نان در صبحانه، شکلات می‌خورد ـ کسل می‌نماید، برای فهمیدن آنکه مشکل در کجاست نیازی به دانشمند متخصص پرتاب موشک نیست. کافی است رژیم غذایی دو کودک را مقایسه کنید تا به دلیل بروز مشکل برسید.

با فرض آنکه دوقلوها فعالیت‌های یکسانی را انجام دهند، محیط یکسانی در کلاس‌هایشان وجود دارد، از یک نوع لباس استفاده می‌کنند و همهٔ جنبه‌های مختلف‌شان به غیر از غذایی که می‌خورند یکسان است، چنین به نظر می‌رسد که رژیم غذایی باعث بروز مشکل بوده است.

همین اصل در مورد عملکرد نادرست شبکه وجود دارد: اگر موجودیتی یکسان درست کار می‌کند، تغییر پیکربندی موجودیت مشکل‌زا می‌تواند در اغلب اوقات مشکل را حل نماید.

سرویس‌دهنده‌ها و مسیریاب‌ها

می‌توانید این اصل را در مورد هر شیئی در شبکه‌تان به‌کار ببندید، اما این اصل هنگام عیب‌یابی ابزاری نظیر مسیریاب‌ها و سرویس‌دهنده‌ها کاربرد محدودی دارد. مسیریاب‌ها و سرویس‌دهنده‌ها به ندرت شکل هم هستند، گو اینکه ممکن است از لحاظ عملکرد مشابه باشند. برخی اوقات شباهت عملیاتی برای مقایسه کفایت می‌کند، اما برای مقایسهٔ سرویس‌دهنده‌هایی که «تقریباً یکی هستند»، به اطلاعات ژرف‌تری نیاز دارید. عیب‌یابی این‌گونه افزارها، در مقایسه با افزارهایی که «دوقلو» هستند، مشکل‌تر است.

به‌طور حتم سرویس‌دهنده‌ها و مسیریاب‌ها، تشابه‌های «تمامیت ابزاری» دارند ـ رای مثال، مسیریابی که با وجود کارکرد صحیح بقیهٔ افزارهای مشابه خود ایجاد خرابی می‌کنند ممکن است نگارشی دیگری از نرم‌افزار عملیاتی (یا لَخت‌افزار) را استفاده نماید. مسیریاب‌های سخت‌افزاری DOS یا ویندوز را اجرا نمی‌کنند؛ به‌جای آنها از سیستم عاملی بهره می‌برند که به واقع نرم‌افزاری کاملاً ساده است (برخلاف ویندوز با هزاران DLLاش). این موضوع باعث می‌شود که

اغلب تنها لازم است شمارهٔ نگارش بررسی شود؛ تفاوت در شماره‌های نگارش می‌تواند نشانگر تفاوت بین مسیریاب و مسیریاب مشکل‌زا باشد.

به‌طور مشابه ممکن است نگارشهای DLL و سطح قطعه‌ای سرویس‌دهندهٔ ویندوز NT مشکل‌زا را با بخش مشابه در یک سرویس‌دهندهٔ «خوب» مقایسه کنید. سرویس‌دهنده‌های نِت‌ور به Config Reader (فصل ۱۳ را ملاحظه کنید) می‌باشند که کار فوق‌العادهٔ مقایسهٔ دهها NLM (ماجول‌های قابل بارگذاری نت‌ور) را به انجام می‌رساند و آنهایی را که سرویس‌دهندهٔ تعیین شده قرار گرفته‌اند جدا می‌کند.

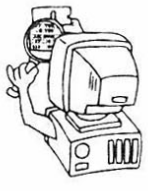
اشیاء کاربری

از آنجا که تمامی سرویس‌دهنده‌ها تا حدودی به گونه‌های متفاوتی پیکربندی می‌شوند، بهترین کار آن است که برای اشیاء کاربری موجود در شبکه از اصل خیابان سسمی استفاده نماییم. بنابر یک رسم، اشیاء کاربری (اطلاعات ورود به سیستم توسط کاربر، حقوق امنیتی وابسته به آن و خود ایستگاه‌کاری کاربر) تا حد معینی به‌صورت یکسان پیکربندی می‌شوند مگر آنکه فروشندهٔ سیستم‌ها دلیلی برای خلاف این موضوع داشته باشد.

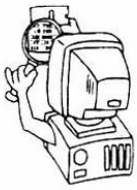
در ساده‌ترین شکل، پیداکردن آنچه که «متفاوت» است، امری ساده می‌باشد: می‌دانید که گروهی از کاربران مدتی است که به گونهٔ قابل قبولی به کار خود ادامه داده‌اند. تصور کنید که یکی از کاربران گزارش می‌دهد که نمی‌تواند برنامهٔ کاربردی خاصی را اجرا نماید؛ از آنجا که بقیه قادر هستند که این کار را با استفاده از ایستگاههای کاری خود و مجوز ورود خود با انجام برسانند، اولین گام در پیداکردن مشکل آن است که ببینیم ایستگاه‌کاری یا مجوز ورود کاربری وی صحیح می‌باشد یا خیر. می‌توانید مشکلات مربوط به ایستگاه‌کاری را با ورود آن کاربر از طریق ایستگاه‌کاری دیگری بررسی نمایید. اگر کاربر نتواند برنامهٔ کاربردی را از طریق ایستگاه‌کاری دیگری اجرا نماید، بلافاصله متوجه می‌شوید که مشکل در مجوز ورود وی به سیستم می‌باشد و نه ایستگاه‌کاری. می‌توانید این مسئله را از طریق بررسی ورود کاربری دیگر ثابت نمایید تا مطمئن شوید برنامهٔ کاربردی در این ایستگاه‌کاری به خوبی کار می‌کند. آنگاه باید از خود سؤال کنید که چطور مجوز ورود این کاربر با مجوزهای کاربران دیگر فرق دارد.



***هشدار** : باید سیبها را با سیبها مقایسه کنید ـ به بیان دیگر اگر تلاش کنید برنامهٔ کاربردی را روی یک ایستگاه‌کاری که برنامهٔ مذکور در آن نصب نشده است، اجرا نمایید، با مشکل مواجه می‌شوید. همچنین برخی از برنامه‌های کاربردی فایل‌های ویژهٔ کاربران را در ایستگاه‌کاری و نه در شبکه می‌نویسند. مواظب این‌گونه برنامه‌ها باشید. بهتر است در مورد هر یک از انواع برنامه‌ها، تجربه‌ای کنترلی را به انجام برسانید ـ قبل از آنکه با مشکلات درگیر شوید ـ تا ببینید آیا کاربری که با برنامهٔ کاربردی خاصی در یک PC کار می‌کند قادر به کارکردن با آن برنامه در PC دیگری می‌باشد. اگر چنین است می‌توانید مطمئن شوید که آن برنامهٔ کاربردی قادر است از یک ایستگاه‌کاری به ایستگاه‌کاری دیگر «شناور» شود.*



***نکته** : هنگامی‌که تنها برخی از کاربران در یک گروه کاری مشکلی را گزارش می‌کنند، ابتدا باید چیزهایی را که اخیراً تغییر کرده‌اند بررسی کنید. اگر به مورد خاصی نرسیدید (یا حتی بدتر، اگر تغییری صورت گرفته و غیر قابل بازگشت بود)، زمان آن فرا می‌رسد که بررسی کنید این کاربران به چه صورتی از بقیه کاربران متفاوت می‌باشند.*



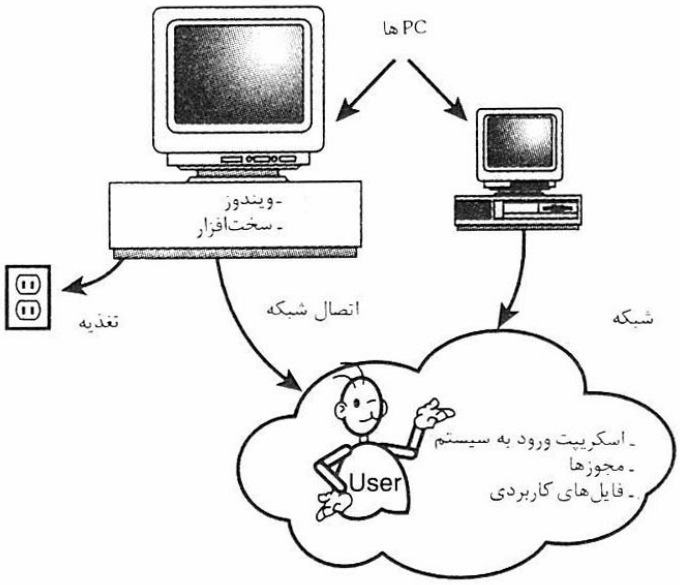
نکته : *کنارگذاشتن تکنیک عیب یابی واقعاً مؤثری است که با روش تفرقه‌بیانداز ـ و ـ حکومت‌کن مرتبط ولی متفاوت با آن است. اگر می‌توانید کار خود را با تفکر در مورد اینکه یک مشکل چه چیزهایی نیست شروع کنید، یک گام به درک آنچه که مشکل‌زا است نزدیک شده‌اید.*



نکته : *روش کنارگذاشتن به‌خصوص هنگامی‌که می‌خواهید اشیائی چندگانه را که متفاوت به نظر می‌رسند پیدا کنید، مؤثر واقع می‌شود. برای مثال اگر دو ایستگاه‌کاری کارتهای تصویری کارتهای شبکه و مقادیر RAM متفاوتی داشته باشند، ممکن است برای آنکه احتمال مشکل RAM را کنار بگذارید، به هر دو مقدار یکسانی حافظه اختصاص دهید. آنگاه می‌توانید از کارتهای شبکه‌ای یکسان برای هر دو استفاده کنید و به همین صورت، تا مشکل را بیابید.*

آن را ساده نگهدارید

حتماً ملاحظه می‌کنید که یک عنصر کلیدی در عیب‌یابی موفق آن است که همه چیزها را ساده نگهدارید. این دقیقاً همان کاری است که هنگام آغاز با سطح بالاترین شیء در موقع شروع تشخیص موارد نامتشابه با بقیه، به انجام می‌رسد (شکل ۲-۵ را ملاحظه کنید). در مثال قبل، چرا کار خود را با بررسی پیکربندی ایستگاه‌کاری قبل از کنارگذاشتن آن شروع نکنیم؟ همچنین چرا کار خود را با بررسی کارت تصویر یا کارت شبکهٔ PC شلوغ کنیم در حالی که می‌دانیم اشکالی در آنها وجود ندارد؟



شکل ۱-۵ : ابتدا به اشیاء سطح بالا نگاه کنید.

مفید خواهد بود اگر به این اقلام به‌صورت ظرفهای سطح بالایی نگاه کنیم که دارای ظرفهایی کوچکتر در درون خود هستند. تا هنگامی‌که ظرف سطح بالایی را کنار بگذارید (یا به حساب آورید)، حتی نگاه‌کردن به زیرمجموعه‌های آن کاری عبث است. می‌توانید به هر مجموعهٔ شبکه‌ای نمونه به‌صورت «جعبه‌ای از ایستگاههای کاری» (که شامل بردهای اصلی، حافظه، دیسکهای سخت و نظایر آنها می‌باشند)، «جعبه‌ای از شبکه‌ها» (که شامل کابل‌ها، هاب‌ها و نظایر آنها هستند) و «جعبه‌ای از کاربران» (که حاوی ID های کاربری، اسکریپت‌های ورود به سیستم و ویژگیهای امنیتی مختلف) فکر کنید.

تصور این اشیاء سطح بالا در جعبه‌ها، این اجازه را به شما می‌دهد که بدون آشفتگی فکری روی کار در دست اجرا متمرکز شوید و شما را به عیب‌یاب بهتری تبدیل می‌کند. اگر کشف کنید که مشکل در شبکه است، زیرعناصر ایستگاههای

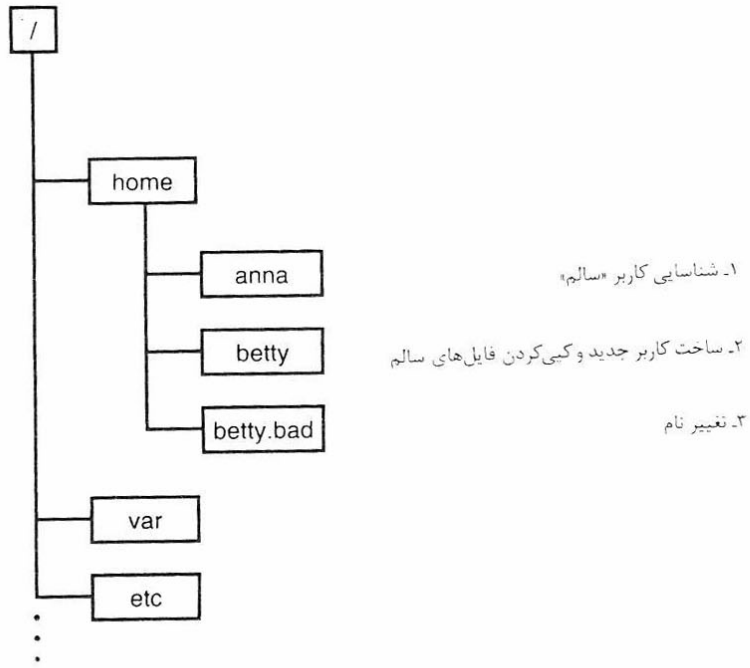
کاری فکرتان را مشغول نخواهند کرد. به عبارت دیگر، هنگامی‌که دریافتید شبکه مشکل را ایجاد نموده، باید تنها زیرمجموعه‌ها و زیرعناصر مربوط به شبکه را مورد توجه قرار دهید.

هدف‌گیری

هنگامی‌که به صورت کلی، تشخیص دادید که مشکل در کجا واقع شده است، سریع‌ترین راه آن است که از تأثیر «تفنگ شکاری» استفاده کنید ـ یعنی شیء مشکل‌زا را با شیء دیگری که کار می‌کند یکسان نمایید.

این بدان معناست که باید «تفنگ شکاری عیب‌یابی» خود را در جهت کلی به سوی هدف نشانهٔ بگیرید. آیا تا کنون نحوهٔ به‌کارگیری تفنگ شکاری را دیده‌اید؟ از دست دادن هدف هنگام تیراندازی با تفنگ شکاری کاری مشکل است، زیرا تیر رها شده به‌صورت گسترده‌ای پراکنده می‌شود. هر چیزی که در جلوی لولهٔ تفنگ قرار داشته باشد سوراخهایی را در خود خواهد دید. هدف‌گیری یک شیء به‌خصوص با تفنگ شکاری بدان معناست که هر چیزی در آن زیرمجموعه را بدون صرف وقت برای تجزیه و تحلیل عنصر مشکل‌زا، تعویض نمایید.

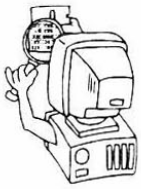
استفاده از گردونه‌های مضاعف می‌تواند کمک بسیار زیادی باشد، چرا که مقایسهٔ پیکربندی و تنظیم دیسک سخت مشکل‌دار از طریق دیسک سخت صحیح آسان است (اطلاعات بیشتر را در فصل ۱۶ ملاحظه کنید). ساخت مجدد فهرست ریشهٔ مربوط به کاربر روش خوب دیگری برای هدف‌گیری یک مشکل در مورد هدفی عمومی می‌باشد. برای مثال از آنجا که برنامه‌های یونیکس به فایل‌های پیکربندی متعددی در فهرست ریشهٔ کاربر وابسته هستند، برخی اوقات فهرست ریشهٔ کاربر را تغییر می‌دهم و فهرست ریشهٔ جدیدی را برای آن کاربر ایجاد می‌کنم و آنگاه محتویات مشابهی از کاربر بدون مشکل را در فهرست جدید کپی می‌کنم (شکل ۲-۵ را ملاحظه کنید).



شکل ۲-۵: هدف‌گیری فهرست ریشهٔ کاربر.

در مواقعی که نمی‌توانید از این تکنیک استفاده کنید (برای مثال، هنگامیکه در صورت استفاده از این روش اطلاعات حیاتی از دست می‌روند)، بهتر است عناصر زیر را که از بالاترین سطح در سمت راست تا پایین‌ترین سطح در سمت چپ ارائه شده‌اند، مورد توجه قرار دهید.

- ایستگاه کاری
- BIOS /سازنده
- گردونهٔ دیسک سخت
- پیکربندی سیستم عامل (فایل‌های آغازین، Registry)
- مؤلفه‌های سیستم عامل (DLL ها)
- برنامه‌های کاربردی محلی (که شبکه‌ای نیستند)
- ویروس
- کارت شبکه
- کابل
- کارت تصویر
- RAM
- تغذیه
- UPS
- جلوگیری از افزایش ناگهانی ولتاژ
- ورود کاربر به سرویس‌دهنده
- اسکریپت ورود به سیستم
- مجوزها
- فایل‌های پیکربندی برنامهٔ کاربردی (کاربر به فهرست دسترسی دارد؟)
- فایل‌های کاربری (فهرست ریشه)
- خود برنامهٔ کاربردی
- پورت روی سوئیچ یا هاب



نکته : بیشتر افراد از گستردگی مشکلات منبع تغذیهٔ AC خراب آگاهی ندارند - واقعاً ارزش آن را دارد که تغذیهٔ PCای را که هنگام ورود به شبکه قفل می‌کند، به پریز دیواری متفاوتی متصل کنید یا وضعیت‌سنج تغذیه را امتحان نمایید. وضعیت‌سنج تغذیه ابزاری فیلترکننده است که برای خلاصی از شوک‌ها و خروجی‌های ناگهانی که می‌توانند منبع تغذیه AC را به ستوه آورند، مورد استفاده قرار می‌گیرد.

همچنین مواظب مؤلفه‌های سطح پایین باشید. برای مثال مؤلفه‌های سیستم عامل دارای ماجراهای مربوط به خود هستند؛ ممکن است روزهای متمادی را به مقایسهٔ بین اشیاء سطح پایین‌تر در این مؤلفه‌ها سپری کنید. برخی اوقات این کار ارزشش را دارد، اما تنها در مورد بخش کوچکی از مشکلات، به خاطر داشته باشید که اطلاعاتی که نیاز ندارید را باید کنار بگذارید. به این موضوع پنهان‌سازی اطلاعات گفته می‌شود. مثال پمپ بنزین که در معرفی این کتاب آمده را به خاطر داشته باشید و هر زمان که می‌خواهید بدون نیاز واقعی به اطلاعات جزئی‌تر سرکشی کنید آن را در نظر آورید. آیا واقعاً لازم است که تمامی جزئیات مربوط به فایل‌های DLL ویندوز را فرا بگیرید اگر تنها و به سادگی می‌توانید از طریق کپی‌کردن پیکربندی سالم ویندوز، مشکل را حل نمایید؟

از سوی دیگر اگر برای مثال یک برنامهٔ پُست الکترونیک می‌گوید که نمی‌تواند MAPI32.DLL را بارگذاری کند، بد نیست

نگاهی به فایل MAPI32.DLL در گردونهٔ دیسک سخت بیندازید. برخی اوقات فایل تخریب شده است (برای مثال ممکن است بیابید که اندازهٔ آن صفر گردیده است). همچنین، ممکن است آن را با یک MAPI32.DLL «خوب» مقایسه کنید و دریابید که از آنچه که باید باشد خیلی کوچکتر است. در این حالت کپی‌کردن یک فایل از ایستگاه‌کاری «خوب» سریعتر از بارگذاری و پیکربندی دوبارهٔ کل ایستگاه‌کاری می‌باشد. این‌کار نظیر عمل متعادل‌سازی است ـ تنها کافی است به موقعیت موجود نگاه کنیم، اطلاعاتی را که دارید بررسی کنید، دریابید که چقدر طول می‌کشد چیزی را تغییر دهید، و آنچه را که سریعترین و مؤثرترین کار به نظر می‌رسد، به انجام برسانید.

این در واقع سخت‌ترین بخش این روش می‌باشد: پیداکردن آنچه که باید مقایسه کنید و اقلامی که مشکل را ایجاد می‌کنند بیابید. برای مثال، اگر بسیاری (و نه تمامی) کاربران مشکلی را گزارش می‌کنند، به‌خصوص یک مشکل متناوب و دوره‌ای، ممکن است در وحلهٔ اول وضعیتی مشکل و ترسناک به نظر برسد، چرا که محل آغاز و تعیین قطعاتی که ممکن است به مشکل منجر شده باشند، ساده به نظر نمی‌رسد. در حالاتی نظیر این بهتر است که فراخوانی‌های شبکه‌ای را ثبت کنیم و آنها را در قالبی جدول‌گونه که نشاندهندهٔ ماهیت مشکل، زمان اتفاق، شرایط وقوع، پیکربندی ایستگاههای کاری و کاربران درگیر در ماجرا می‌باشند، بنویسید. چنین نموداری ممکن است نظیر آنچه که در جدول ۱-۵ نشان داده شده است به نظر می‌رسد.

جدول ۱-۵ : صفحهٔ ثبت نمونه

تاریخ	زمان	دپارتمان	کاربر	مشکل	نوع PC
8/11	2:00	مالی	Jack	خطای عمل نامعتبر WordPrefect	Clone/486
8/11	2:20	مالی	Leona	Fata exception 06 (طی راه‌اندازی سیستم) بعد از آن مرتب به نظر می‌رسد.	Dell/P6
8/11	3:00	مالی	Tracy	خطای عمل نامعتبر ـ WordPrefect	Clone/486
8/12	9:00	مالی	Tracy	خطای عمل نامعتبر ـ WordPrefect	Clone/486
8/12	10:45	مالی	Jac	خطای عمل نامعتبر ـ WordPrefect	Clone/486
8/12	1:00	مالی	Jill	قفل شد. باید هنگام خواندن پُست الکترونیکی، راه‌اندازی مجدد نماید.	Clone/486
8/13	11:00	مالی	Jack	قفل شد. باید هنگام خواندن پُست الکترونیکی، راه‌اندازی مجدد نماید.	Clone/486
8/13	12:45	مالی	Bill	قفل شد. باید هنگام خواندن پُست الکترونیکی، راه‌اندازی مجدد نماید.	Clone/486

با نگریستن به این جدول ثبتی، روشن می‌شود که خطاهای عملیاتی نامعتبر بیشتر به وقوع می‌پیوندد (اگر نمونه‌های بیشتری را به ثبت می‌رساندید ملاحظه می‌کردید که این واقعیت آشکارتر خود را نشان می‌دهد. اقلام دیگر تکراری نیستند

و مقدار آنها بسیار کمتر است). بنابراین اکنون می‌دانید که «چه‌چیزی نظیر بقیهٔ امور نیست».

چرا بیل به اندازهٔ تریسی یا جک فراخوانی را صورت نمی‌دهد؟ یک مکالمهٔ تلفنی سریع این واقعیت را آشکار می‌سازد که وی بین روزهای یازدهم و دوازدهم در شرکت حضور نداشته و بنابراین نباید وی را در بررسیهای این دو روز به حساب آورد.

اجازه دهید به مثالی واقعی نگاهی داشته باشیم. به تازگی درگیر ارتقاء یک دپارتمان به ویندوز ۹۵ شدم، که ارتقاء به نگارش جدیدی از WordPerfect را نیز شامل می‌شد. نظر مدیریت آن بود که این عمل، تغییری استراتژیک است که امکان برگشت به حالت قبل[1] را بسیار کوچک می‌سازد؛ این به ما بستگی داشت که کارکرد آن را میسر سازیم. با این‌که ماشینهای نمونه‌ای که من روی آنها آزمایش‌های لازم را صورت داده بودم، به‌خوبی کار می‌کردند، بعد از ارتقاء مشکلاتی را ملاحظه نمودیم. برخی از کاربران (و نه تمامی آنها) خطاهای عملیاتی غیرمجاز را گزارش کردند. کاملاً مطمئن بودم که تمامی کاربران به یک شکل پیکربندی شده‌اند ـ اسکریپت‌های ورود به سیستم یکسان، مجوزهای فایلی و پیکربندی فهرست ریشه ـ اما، متأسفانه به خاطر استفاده از سخت‌افزارهای مختلف نمی‌توانستم در مورد ایستگاههای کاری مطمئن باشم.

چندین روز وقوع خطا را ثبت کردم و متوجه شدم که برخی از کاربران هرگز خطایی را گزارش نکردند. این نشان می‌داد که مشکل هدف متحرکی نبود و در برخی از جاها قرار داشت. دانستن این موضوع مهم بود؛ برخی از خطاها در تمامی مدت وقوع در یک مکان ثابت نمی‌مانند ـ یعنی از یک ایستگاه‌کاری به دیگری نقل مکان می‌کنند. این موضوع اغلب نشاندهندهٔ مشکلی سیستمی است که ربطی با ایستگاههای کاری مستقل ندارد.

در ادامه ملاحظه کردم که تنها PC هایی که از مارک خاصی نبودند مشکل را ایجاد می‌کردند هیچ‌یک از کاربرانی که از PC هایی با مارک یک تولیدکنندهٔ مشخص استفاده می‌نمود مشکل را ایجاد نمی‌کرد. بالاخره متوجه شدم که تمامی کاربران دستهٔ اول با این خطا مواجه نبودند ـ تنها برخی از انواع کامپیوترها مشکل را ایجاد می‌کردند. بدین وسیله به این نتیجه رسیدیم که در انواع خاصی از کامپیوترهایمان مشکلات مربوط به مؤلفه‌ها وجود داشت.

در ادامه برای کنارگذاشتن مشکلات کاربری PC کاربری را که با سیستم مشکلی نداشت با دستگاه دیگری که مشکل را مخابره می‌نمود عوض کردم (این‌کار ارج و قرب مرا نزد کاربر مذکور زیاد نکرد، اما به من نشان داد که مشکل دقیقاً به ایستگاه‌کاری مربوط می‌شود).

سابقه ایستگاههای کاری مشکل‌زا را بررسی نمودم تا ببینم این دستگاهها چه وجه مشترکی دارند. جدول جدیدی از مؤلفه‌های سطح پایین ایجاد کردم (جدول ۲-۵). ویندوز ۹۵ و مؤلفه‌های آن را واگذاردم، چرا که می‌دانستم تمامی ایستگاههای کاری از این جنبه یکسان هستند. بررسی خاصی نیز در مورد ویروسها به عمل نیاوردم چرا که این‌کار را هنگام نصب ویندوز به انجام رسانده بودم.

جدول ۲-۵ : نمودار ساده‌ای از مؤلفه‌های سطح پایین

ایستگاه‌کاری	Mfr/Bios	کارت تصویر	دیسک سخت	RAM	هاب/پورت
Jack	AMI	Brand-X	Quantum	16MB	8/2
Tracy	Phoenix	Brand-X	Cnnor	16MB	9/3
Bill	AMI	Brand-X	Seagate	24MB	8/1

1- rollback

بعد از مشاهدهٔ جدول جدید، برایم روشن شد با وجود آنکه PC ها از قطعات و مؤلفه‌های مختلفی استفاده می‌کردند، به گونهٔ عجیبی در یک مورد، یعنی کارت تصویر مشترک بودند.

از آنجا که تعویض کارت تصویر و استفاده از کارت تصویر متفاوت نسبتاً آسان بود، این‌کار را روی یکی از دستگاهها انجام دادم. با ادامهٔ ثبت مشکلات مشخص شد که آن ایستگاه‌کاری با کارت تصویر جدید دیگر مشکلی نداشت. کارت تصویر دستگاه دیگری را عوض کردم و مشکل آن دستگاه نیز ناپدید شد. تلاش من برای به‌روزدرآوری راه‌اندازهای تصویری در ایستگاههای کاری باقیمانده به‌جایی نرسید و مشکل به جای خود باقی ماند. راه حل نهایی را در آن یافتم که کارتهای تصویر تمامی ایستگاههای کاری مشکل‌زا را تعویض نمایم.

واضح است که داشتن تعداد زیادی ایستگاه‌کاری که تعویض قطعات آنها بر پایهٔ قاعده‌ای منظم صورت می‌گیرد، مبنای خوبی برای عیب‌یابی مشکلات شبکه‌ای نیست. از آنجا که تفاوتهای کمتر مساوی است با زمان کمتر برای پیداکردن چیزهایی که شبیه به بقیه نیستند، بهتر آن است که سعی شود تمامی مؤلفه‌ها ـ نرم‌افزار، سخت‌افزار و سایر ـ مربوط به یک دپارتمان یا گروه کاری را در قالب یک استاندارد نگاه داشت. فصل ۱۶ چگونگی همگن‌سازی شبکه‌های نامتجانس را در قالب اطلاعاتی واقعی بررسی می‌کند.



یادداشت : *شبکهٔ نامتجانس، شبکه‌ای است که در آن همگی مؤلفه‌ها متفاوتند؛ استفاده از روش عیب یابی خیابان سسمی در چنین شبکه‌ای کار مشکلی است. از سوی دیگر، مؤلفه‌های به‌کار رفته در شبکهٔ متجانس تقریباً همه از یک نوع هستند. این آرزو و رؤیای عیب یاب خیابان سسمی است. آیا تنها در شبکه‌های متجانس است که همهٔ چیزها همیشه یکسان هستند؟ شاید نه. نظیر بیشتر واقعیت‌های زندگی، واقعیت جایی در بینابین حدود قرار دارد. البته، در این حالت کلید موفقیت در یکسان نگهداشتن حداکثر مؤلفه‌ها می باشد.*

خلاصه

اگر در جایی خرابی وجود دارد، مقایسهٔ آن با مورد مشابهی که به درستی کار می‌کند، روش سریعی برای پیداکردن آنچه که خرابی در آن واقع است به دست می‌دهد. با اینکه مقایسهٔ پیکربندی سرویس‌دهنده‌ها و مسیریاب‌هایی که ذاتاً با یکدیگر متفاوتند، کاری مشکل است، مقایسهٔ سطوح نگارشی عمومی آنها و نگارشهای فایلی می‌تواند در کنارگذاشتن یک مشکل «تفاوتی» کمک نماید.

این تکنیک به خصوص هنگامی که اشیاء دیگر در شبکه، نظیر تنظیمات کاربری و پیکربندی‌های ایستگاه‌کاری مورد توجه هستند، به خوبی کار می‌کند. برخی اوقات، اگر مشکل را تا پیکربندی به خصوصی ردیابی نموده‌اید. می‌توانید کل مشکل را با یک پیکربندی «سالم شناخته‌شده» تعویض کنید (یا آن را با تفنگ شکاری مورد هدف قرار دهید). این کار درگیرشدن با موضوعات پیچیده که ممکن است کار با آنها کلاً لازم نباشد، جلوگیری می‌کند.

برای مشکلات پیچیده با شاکیان متعدد، باید اطلاعاتی را برای عیب‌یابی ثبت کنید که تفاوت پیکربندی‌ها و ایستگاههای کاری کاربران را منعکس می‌نماید. این کار به ایجاد الگویی در درک چگونگی تشابه‌های پیکربندی در کاربران «شاکی» کمک می‌کند.

کارگاه

پرسش و پاسخ

پرسش : چگونه می‌توانم بگویم که یک ایستگاه‌کاری مشکل‌زا به اندازهٔ کافی به یک ایستگاه‌کاری «خوب» شباهت دارد؟

پاسخ : لازم است که بدانید چگونه ایستگاه‌کاری نصب شده، چه کسی آن را نصب نموده و چگونه پیکربندی شده است. مستندات جزیی مربوط به سایت برای تعیین این موضوعات به کار می‌آیند. حتی مستندات مربوط به رسیدهای خرید می‌تواند تعیین کند که ایستگاه‌کاری از کجا ابتیاع شده و این‌که آیا با ایستگاههای کاری دیگر همزمانی داشته است یا خیر. اگر برای سازمانی بزرگ کار می‌کنید به احتمال زیاد دپارتمان خرید سازمانتان اطلاعات لازم در مورد PC ها را در اختیار دارد. همچنین تاریخ خرید را می‌توان جایی در پایگاه اطلاعاتی سازمان پیدا نمود.

پرسش : چگونه یک تنظیم کاربریِ «خوب» را هدف‌گیری کنم؟

پاسخ : بیشتر سیستم‌های عامل شبکه به نوعی امکان الگوسازی (برای مثال NWAdmin در InteranetWare) مجهز هستند و یا در بدترین شکل، امکان کپی‌کردن اطلاعات کاربری از جایی به جای دیگر را در اختیار می‌گذارند (User Manager در NT).

آزمون

۱- درست یا نادرست؟ لازم است در یک مسیریاب سخت‌افزاری که مشکلاتی را ایجاد می‌کند، تمامی نگارشهای DLL ها را با مسیریاب مشابهی که مشکلی را بروز نمی‌دهد، مقایسه نمود.

۲- روش خیابان سسمی برای به‌کارگیری در ــــــــــــــ بهترین کاربرد را دارد.

الف ـ تنظیمات گردونهٔ دیسک سخت کاربر　　ب ـ اسکریپت‌های ورود به سیستم کاربر

ج ـ سرویس‌دهنده‌ها و مسیریاب‌ها　　د ـ هم الف و هم ب

۳- کدامیک بخشی از «جعبهٔ» سطح بالای ایستگاه‌کاری نیست؟

الف ـ گردونهٔ دیسک سخت　　ب ـ RAM

ج ـ کارت تصویر　　د ـ اسکریپت ورود به سیستم

۴- درست یا نادرست؟ برای بررسی پیغام خطای مربوط به یک DLL «خراب» باید یک برنامه‌نویس ویندوز باشید.

۵- هنگامی‌که مشکلات یک بخش شبکه‌ای را ثبت می‌کنید و افراد متفاوتی همان مشکل را گزارش می‌کنند، به احتمال زیاد مشکل به چه قسمتی مربوط می‌شود؟

الف ـ ایستگاه‌کاری　　ب ـ شیء کاربری

ج ـ هم الف و هم ب　　د ـ شبکه

پاسخ سؤالات آزمون

۱- نادرست. مسیریاب‌های سخت‌افزاری فاقد DLL هستند؛ اغلب تنها یک شمارهٔ نگارش دارند که برای شناسایی نرم‌افزار داخلی‌شان مورد استفاده قرار می‌گیرد.

۲- الف　　۳- د

۴- نادرست　　۵- د

فصل ۶

روش SOAP: دادهٔ درونی، دادهٔ ظاهری، تجزیه و تحلیل و طرح

امیدوارم که مطالب فصل گذشته را پسندیده باشید، چرا که روش عیب‌یابی این فصل مقدار زیادی از روش مذکور کمک می‌گیرد. مداوای یک مشکل پیچیده اغلب مستلزم تهیه یادداشتهای بسیار است، چرا که باید خلأهای درک مشکل را به گونه‌ای پر کند. تا کنون، مشکلات را به گونه‌ای حل کرده‌اید که با یک تست چند جوابی برخورد می‌کنید ـ از طریق تجزیه و تحلیل تغییرات، توجه به تفاوتها و تطابق. اکنون می‌خواهیم در مورد یک آزمون پرکردن جای خالی صحبت کنیم که کمی مشکلتر است؛ در این فصل باید با اطلاعات درونی روبرو شوید، آن را با دادهٔ ظاهری تطبیق دهیم، اطلاعاتتان را تجزیه و تحلیل کنید و طرح گام بعدی خود را پی‌ریزی نمایید. به بیان دیگر در این فصل برای مواجه‌شدن با مشکلات دشوار و طاقت‌فرسا آماده خواهید شد.

دکتر شبکه

ابتدا، توضیح کوچکی در مورد روش SOAP ارائه می‌کنم. اولین بار با روش SOAP هنگامی برخورد کردم که تصمیم داشتم مثل پدرم دکتر نباشم. با این‌که اصلاً علاقه‌ای به سوزن زدن به مردم نداشتم، حضور در دفتر کار پدرم مطالب زیادی را در مورد عیب‌یابی به من یاد داد. از جهتی، طبابت بسیار مشکل‌تر از کامپیوتر می‌باشد ـ استانداردهای بسیار کمی وجود دارند، طراح هرگز صفحات اطلاعاتی را ارائه نمی‌کند (مستندات حامل بسیار کمتری وجود دارد)، و ابزاری که سعی در عیب‌یابی آن دارید، در صورت مرتکب‌شدن اشتباه می‌تواند از شما عارض شود. حرفهٔ طبابت از ترفندهای تشخیصی بسیار زیادی استفاده می‌کند ـ ما عیب‌یاب‌های شبکه چیزهای زیادی می‌توانیم از این حرفه بیاموزیم.

یکی از تکنیک‌های تشخیصی، روش SOAP در برداشتن یادداشت است. برخی دکترها در جداول مربوط به بیمارهای خود در خطوط مجزایی حروف S، O، A و P را می‌نویسند که به ترتیب بر کلمات درونی[1]، ظاهری[2]، تجزیه و تحلیل[3] و طرح[4] دلالت دارد. بنابراین اگر دکترم را به خاطر معده ویزیت کنم، او ممکن است چنین بنویسد:

S: بیمار درد معده دارد؛ شب گذشته بال جوجه میل نموده؛ اخیراً به سختی کار کرده است.

O: طپش ناحیهٔ شکم نشاندهندهٔ حساسیت بخش فوقانی سمت راست می‌باشد.

A: مضنون به گاستریک حاد.

P: پنج روز معالجه با آنتی‌اسید، رژیم ملایم و پیگیری برای بررسی شرایط پس از پنج روز.

1- Subjective 2- Objective 3- Analysis 4- Plan

اطلاعات درونی هر آن چیزی است که من به دکتر می‌گویم. اطلاعات بیرونی (ظاهری) را دکتر مشاهده می‌کند، تجزیه و تحلیل هر آن چیزی است که وی بر پایهٔ سؤالات و دلایل نتیجه‌گیری می‌کند و طرح مجموعه‌کارهایی است که برای مداوای مشکل انجام می‌دهد. دکترها عادت ندارند که پاسخ سیاه و سفیدی را دریافت کنند؛ البته اگر طرحی را داشته باشند در جهت مثبت حرکت می‌نمایند.

حرکت در جهت مثبت تمام آن چیزی است که روش SOAP در تلاش برای رسیدن به آن می‌باشد. تمامی مشکلاتی را که با آن به عنوان یک عیب‌یاب روبرو می‌شوید ممکن است در یک روز یا هفته حل نشوند ـ به‌خصوص مشکلاتی که امکان مشاهدهٔ سریع آنها وجود ندارد. اغلب، مشکلاتی که شکل تناوبی یا دوره‌ای دارند مستلزم انجام عملیاتی عیب‌یابی پیچیده و طولانی مدت می‌باشند. برای تسلط بر یک مشکل پیچیده باید مشکل را به بخشهای مؤلفه‌ای آن تقسیم کنیم ـ یعنی گزارش درونی و حقایق ظاهری را استخراج نمایید. توانایی برای جداکردن اطلاعات درونی از اهمیت خاصی برخوردار است ـ ممکن است کسی چیزی را گزارش بکند که ارتباط غیرمستقیمی با مشکل داشته باشد اما به‌طور مستقیم در شناسایی مشکل به‌کار نیاید. تصور کنید شخصی از درد قفسهٔ سینه ناراحتی دارد ـ آیا مشکل این شخص یک حملهٔ قلبی است یا تنها مسئله به ماهیچه‌های ناحیهٔ مذکور بازمی‌گردد؟ گزارش درد در قفسهٔ سینه یک احساس درونی است ـ بررسی فعالانه که درد ماهیچه‌ای یا حملهٔ قلبی را آشکار می‌کند از یافته‌های ظاهری حادث می‌شود. اطلاعات درونی مفید هستند اما تنها با بررسی دقیق می‌توان از آنها استفاده نمود.

فقط واقعیت‌ها

هنگامی‌که واقعیت‌ها را در یک موضوع شبکه‌ای پیچیده یا تناوبی مورد توجه قرار می‌دهیم (که در این صنعت از آن با عنوان «عیب‌یابی یک مشکل خارق‌العاده» نیز یاد می‌شود)، لازم است که فهرست مقدماتی اقلام ظاهری که می‌توانند به یک راه حل رهنمون شوند را دسته‌بندی نمایید:

- فاصلهٔ زمانی مشکل (تمامی اوقات یا به‌صورت تناوبی)
- شروع مشکل (تاریخ و زمان)
- محل (مکان فیزیکی در شبکه)
- تعداد کاربران درگیر
- پیکربندی ایستگاه‌کاری (مشابه یا نامتشابه با سایر؟)
- تعداد و نوع برنامه‌های کاربردی درگیر در مشکل (اجرا به‌صورت همزمان؟)
- اسامی کاربری درگیر، گروه (ها) امنیتی وابسته
- ابعاد
- عملکرد برنامه‌های کاربردی مشابه

حتی با وجود اطلاعات ظاهری بسیار، ممکن است این اطلاعات منبع درستی برای تجزیه تحلیل به‌منظور دستیابی به نتیجهٔ صحیح نباشند. بنابراین برای ارائه «طرح» ابتدا لازم است چند تلاش اولیه برای بررسی مشکل و احیاناً جمع‌آوری اطلاعات بیشتر صورت پذیرد. خسته نشوید؛ هر چه اطلاعات بیشتری داشته باشید حدس بهتری می‌توانید بزنید.

SOAP در دنیای واقعی

اجازه دهید حالتی را مورد بررسی قرار دهیم که در آن یکی از کاربران می‌گوید نمی‌تواند اَپلت وِب خاصی را که برای کارش بدان نیاز دارد اجرا نماید. شکل ۱-۶ نقشهٔ منطقی این سایت را نشان می‌دهد؛ PC کاربر مورد نظر ما در نقطهٔ A در نقشه قرار دارد.

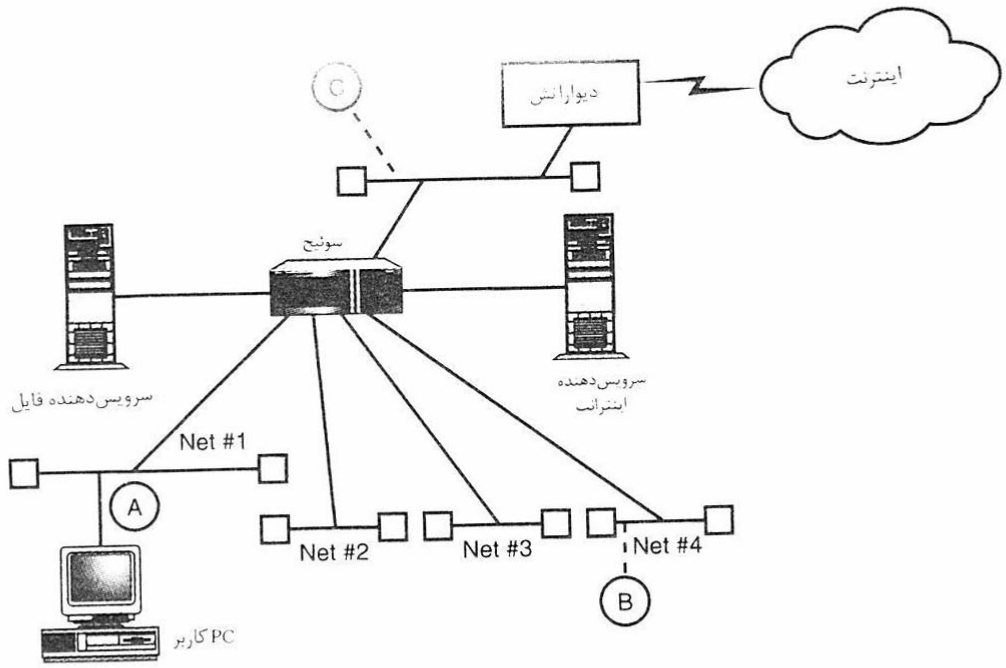
PC کاربر را بررسی کرده و می‌بینید که اَپلت به خوبی کار می‌کند. کاربر اخم می‌کند و می‌گوید، «خوب، برای من کار نکرد». او بلافاصله بعد از شما امتحان می‌کند و برنامه اجرا می‌شود، اما روز بعد دوباره همان شخص مشکل را گزارش می‌دهد. تصمیم می‌گیرید که از SOAP استفاده کنید:

S: اَپلت وِب کار نمی‌کند.

O: هنگامی‌که من آن را اجرا نمودم کار کرد.

A: شاید زمان روز در آن تأثیر می‌گذارد.

P: هنگامی‌که کاربر اغلب اوقات برنامه را مورد استفاده قرار می‌دهد، یک سری بررسی انجام گیرد.



شکل ۱-۶: عیب‌یابی یک مشکل وابسته به زمان.

تجزیه و تحلیل شما از مسئله به خوبی صورت گرفته و طرح‌تان برای جمع‌آوری اطلاعات جدید کار خواهد کرد. کاربر را هنگامی‌که وی اغلب اوقات در آن زمان‌ها تلاش می‌کند برنامهٔ اَپلت را اجرا کند ملاقات می‌کنید این‌بار برنامه کار نمی‌کند. چه اتفاقی می‌افتد؟ این‌بار، شما هستید که اطلاعات درونی را فراهم می‌کنید؛ این حدس شماست:

S: شرط می‌بندم که زمان روز با کارنکردن اَپلت در ارتباط است.

O: اَپلت وِب در ساعت هشت صبح کار نمی‌کند.

A: آیا ممکن است که این مشکل به فعالیت شبکه‌ای دیگری در آن بخش شبکه که همزمان رخ می‌دهد مرتبط باشد؟

P: بخش شبکه‌ای متفاوتی را مورد استفاده قرار می‌دهم (نقطهٔ B روی نقشه).

طرح خوبی است اما مشکل را حل نمی‌کند، همانگونه که یادداشتهایتان نشان می‌دهد:

S : فعالیت شبکه ممکن است در ساعت هشت صبح روی بخش شبکه‌ای کاربر متفاوت باشد.

O : اَپلت وِب هنوز هم در بخش شبکه‌ای متفاوت اجرا نمی‌شود.

A : سرم آسیب دیده. چه چیز دیگری می‌تواند در این ساعت از روز متفاوت باشد؟

P : بررسی کنم که در ساعت هشت صبح به طور کلی در شبکه چه اتفاقی می‌افتد.

کاربر هنوز هم در ساعت هشت صبح با وجود استفاده از بخش شبکه‌ای متفاوت مشکل دارد. اوضاع بد نیست. بخش شبکه‌ای وی را از حوزهٔ مشکلات کنار گذاشته‌اید که این خود امر بسیار مهمی است. استنتاجی کرده‌اید که اشتباه بوده است. وقت زیادی را روی آن تلف نکنید.

آیا با یک ویروس سروکار داریم؟

بعد از نوشیدن یک فنجان چای، دربارهٔ احتمال ویروسی که در ساعت هشت صبح در روز خاصی فعال می‌شود، فکر می‌کنید اما خیلی سریع این فکر را از خود دور می‌کنید ـ شما از سیستم حفاظت خوبی استفاده کرده‌اید. از آن گذشته از ایستگاه‌کاری متفاوتی استفاده کرده‌اید که مطمئن هستید که عاری از ویروس است. حدس خوبی است چرا که چیزهایی نظیر این اتفاق افتاده‌اند ـ حتی ویروسهایی که هیچ‌کاری نمی‌کنند تا این‌که روز خاصی در زمان خاصی در صبح سیستم‌های عامل را با مشکل مواجه کرده و بررسی می‌کنند که آیا روز مناسبی برای خراب‌کردن اطلاعات شما می‌باشد یا خیر.

بنابراین به صفحهٔ ترسیمی خود باز می‌گردید.

مشاوره

اوضاع حساس است، چرا که شما به نتیجه‌ای نرسیده‌اید و فکر می‌کنید شاید نتوانید مشکل را حل کنید. وسوسه می‌شوید که کار را رها کنید. حدستان چیست؟ عیب‌یاب موفق آن است که لختی درنگ کند و دوباره به حقایق نگاهی بیندازد. آنگاه درست مثل یک پزشک عیب‌یاب هم ممکن است مشاوره‌ای را صورت دهد و کار را در مسیری درست ادامه دهد.

آیا لازم است که از یک حرفه‌ای مشاوره بخواهید؟ الزاماً خیر. دریافت مشاوره به خاطر آن است که شما خیلی به مشکل نزدیک شده‌اید و نتایج مقدماتی از ماوقوع را در دست دارید. فرض کنید از شخصی ـ هر کسی ـ بپرسید که ساعت هشت صبح هر روز چه اتفاقی رخ می‌دهد. پاسخ ممکن است آن باشد که «همه PC های خود را روشن می‌کنند» و یا «همه شروع به کار می‌کنند» و یا جوابی نظیر این. این پاسخها لامپی را برای شما روشن می‌کنند ـ از آنجا که همه در ساعت هشت صبح کامپیوترهای خود را روشن نموده و وارد سیستم می‌شوند، آیا ممکن است مشکل معادل کامپیوتری ترافیک صبحگاهی در شهر باشد؟

پاسخ مثبت است. در شبکه هم ساعت پررفت و آمد مفهوم دارد. چگونه می‌توانید این امر را بررسی کنید؟ خوب، کمی مشکل است. دو روش وجود دارد:

- اندازه‌گیری دقیق (که نسبتاً مشکل است مگر آنکه فصل ۲۱ را مطالعه نموده باشید).
- تغییر موقعیت (انتقال ایستگاه‌کار به محلی که ترافیک کمتر خواهد بود.

حتی با وجود آنکه ایستگاه‌کاری را به بخش دیگری منتقل نموده‌اید این مسئله را مورد توجه قرار ندادید که بخش جدید

هم ممکن است دارای مشکل باشد. این‌کار ممکن است معادل نقل مکان از محله‌ای شلوغ به محله‌ای شلوغ‌تر باشد ـ که مسلماً تأثیر مثبتی در گریز از ترافیک صبحگاهی ندارد. اکنون، SOAP شما نظیر این خواهد بود:

S : مشکل ممکن است تراکم در شبکه باشد.

O : مشکل به‌صورت همزمان در بخشهای مختلف اصلی شبکه به وقوع می‌پیوندد.

A : تراکم ورود به سیستم در بخشهای اصلی مطرح است اما ممکن است در بخشی با کاربران کمتر، خفیف‌تر باشد.

P : نقشه‌ها بررسی و اَپلت در یک بخش شبکه‌ای «کم‌ترافیک» امتحان گردد (شاید نزدیک‌تر به بخش اینترنت و دورتر از بخشهایی که ترافیک ورود به سیستم در آنها زیاد است).

طرحتان را صف‌آرایی می‌کنید: موقتاً یک ایستگاه‌کاری در نقطهٔ C روی نقشه آماده می‌کنید هنگامی‌که اَپلت را در ساعت هشت اجرا می‌نمایید، کار می‌کند! حالا به درستی تراکم شبکه را مورد تردید قرار داده‌اید. سؤال بعدی آن است که این مشکل از آن کیست؟ به عبارت دیگر آیا فروشندهٔ اَپلت مسئول این مسئله است یا اینکه مشکل از شماست که شبکهٔ شلوغی دارید؟ پاسخ شما به این مشکل ممکن است متفاوت باشد. از یک سو ممکن است انتقال این شخص به یک بخش خلوت‌تر میسر باشد. البته این‌کار ممکن است مؤثر نیافتد چرا که شما از نقشه‌های فیزیکی‌تان درمی‌یابید که بخشهای شبکه‌ای که از PC استفاده می‌کنند در بین سرویس‌دهنده‌ها احاطه شده‌اند. به بیان دیگر، محدودیتهای فیزیکی ممکن است مانع شوند که این شخص را در بخش دیگری جای داد چرا که ممکن است هاب‌های نزدیک وی برای کاربران دیگر به کار رفته باشد. هابی با ترافیک کمتر ممکن است در مرکز شما یا در ساختمان دیگر و خارج از محدودهٔ دسترسی فیزیکی وی قرار داشته باشد (ممکن است این سؤال مطرح شود که چرا از این شخص نخواهیم که کار خود را در ساعت هشت صبح آغاز نکند، این راه حل خوبی نیست شبکه باید کار کند و شما باید آن را درست کنید).

در این نقطه اگر واقعاً لازم باشد که ایستگاه‌کاری این شخص در بخش شلوغ‌تر باقی بماند، باید عیب‌یابی برنامهٔ کاربردی را آغاز کنید. چرا این شخص مشکلی با سایر برنامه‌ها و مثلاً برنامه‌های کاربردی محلی ندارد؟ همانگونه که در فصل ۱۹ ملاحظه خواهید کرد مقایسهٔ برنامهٔ کاربردی محلی با یک برنامهٔ کاربردی اینترنتی فکر خوبی نیست؛ استفاده از برنامه‌های کاربردی اینترنتی در مقایسه با برنامه‌های کاربردی محلی نظیر مقایسهٔ یک پرواز بین‌المللی و استفاده از اتومبیل شخصی برای رفتن به خرید می‌باشد. بسیاری از اتفاقات در مسافتهای طولانی رخ دهد. مجدداً SOAP خود را می‌نویسید:

S : اَپلت کار نمی‌کند؛ بقیهٔ برنامه‌های کاربردی کار می‌کنند.

O : اَپلت تنها برنامهٔ کاربردی اینترنت مورد استفاده است.

A : برنامهٔ کاربردی اینترنت، برنامه‌های محلی محسوب نمی‌شوند.

P : در ساعات اوج ترافیک برنامهٔ کاربردی اینترنتی متفاوتی را امتحان کنید.

تا کنون پنج فهرست SOAP را به انجام رسانده‌اید طولانی و خسته‌کننده است. اما همانطور که ملاحظه می‌کنید SOAP فرایند قدرتمندی برای پالایش دانسته‌های شما و همچنین روشی برای حدس‌زدن و تبدیل آنها به وقایع و نیز روشی برای حرکت به‌سوی جلو می‌باشد.

صبح روز بعد در ساعت هشت برنامهٔ اینترنتی متفاوتی را اجرا می‌کنید و ملاحظه می‌کنید که به‌خوبی کار می‌کند با این‌که کاری که این برنامه‌ها انجام می‌دهند کاملاً یکسان نیست حداقل می‌دانید که مقایسه، مقایسهٔ بین سیبها است یعنی یک برنامهٔ کاربردی وابسته به دیوار آتش را با چنین برنامهٔ دیگری می‌سنجید. برنامهٔ دیگری را هم به منظور اطمینان اجرا

می‌کنید این برنامه نیز به خوبی کار می‌کند. جدیدترین SOAP شما به صورت زیر خواهد بود.

S : چنین به نظر می‌رسد که مشکل در برنامهٔ کاربردی است.

O : تنها دو برنامهٔ کاربردی دیگر اینترنت مورد بررسی قرار گرفته‌اند.

A : اندازه‌گیری تراکم و تأخیر ممکن است کمک کند اما با این وجود به فروشندهٔ برنامه ارتباط پیدا می‌کند.

P : با تولیدکنندهٔ برنامهٔ اَپلت تماس حاصل شود و کلیه یادداشتهایی که به این نتیجه‌گیری منجر شده است به یکدیگر پیوند داده شود.

خوشبختانه اَپلت مورد نظر «رایگان نبوده» و تولیدکننده مشتاق است که آن را برای شما به کار بیندازد. تولیدکننده یک نمونهٔ ردیابی‌شده از شبکه را درخواست می‌کند و شما از طریق پست الکترونیک برای او ارسال می‌کنید پاسخ او این است که ترافیک شبکهٔ شما بسیار بالا است اما مقدار قابل قبولی نیست. از آنجا که یادداشتهای زیادی برداشته و برای وی ارسال کرده‌اید، او درک خوبی از ماوقع داشته و می‌فهمد که مشکل احتمالاً توسط او ایجاد شده است. از آنجا که وی مایل است شما را به‌عنوان یک مشتری راضی نگه دارد، خیلی زود برنامهٔ تصحیح‌شده‌ای را روی میز کاریتان ملاحظه می‌کنید که با نصب آن در PC کاربر مشکل را حل‌شده خواهید یافت.



نکته : در موقعیتی نظیر این بهتر است که مشکل خود را به‌صورت کامل مستندسازی کنید - یا به‌صورت غیر رسمی از طریق پُست الکترونیکی با همکارانتان یا به صورت رسمی مثلاً به شکل ضمیمه‌ای در مستندات مربوط به محصول در کتابخانه). ممکن است چیزی شبیه به این را یادداشت کنید:

۹۸/۱۰/۲۰، اَپلت مشکلاتی را هنگام اجرا در شبکهٔ پرترافیک ایجاد می‌کرد. از نگارش ۲/۱، که در سرویس‌دهندهٔ شمارهٔ ۵ در محل اشتراکی `Fixes` قرار دارد استفاده نمایید.

آیا همیشه این‌طور است تولیدکنندهٔ نرم‌افزار خطای گزارش داده شده توسط شما را تصحیح می‌کند؟ در واقع خیر. مجموعهٔ ما در طی سالیان دراز اشکالات زیادی را به تولیدکنندگان منعکس نموده است هنگامی‌که از روالهای دقیق یادداشت‌برداری SOAP استفاده می‌کنید، ممکن است بتوانید همکاران پشتیبانی فنی خود را قانع کنید که با مشکلی مواجه هستید که باید با آن رسیدگی کنند. البته خیلی از اوقات پاسخ را خود باید بدهید.

خلاصه

شبکه‌های کامپیوتری کمتر از یک قرن است که وجود دارند - به‌عنوان عیب‌یابهای شبکه، تکنیکهای کار را از هر منبعی که بتوانیم، فراخواهیم گرفت. حرفهٔ طبابت از یادداشتهای SOAP استفاده می‌کند که می‌توانند در ردیابی مشکلات پیچیده بسیار مؤثر باشند. از آنجا که الزاماً تمامی وقایع هنگام ردیابی یک مشکل در دسترس نیستند استفاده از قالب SOAP برای یادداشت‌برداری این امکان را برای شما فراهم می‌کند که به گونه‌ای مؤثر اطلاعات خود را مورد تجزیه و تحلیل قرار داده، وقایع بیشتری را جمع‌آوری کرده و طرحی را ارائه نمایید.

کارگاه

پرسش و پاسخ

پرسش : کاربری ادعا می‌کند که ایستگاه‌کاری وی تغییر نکرده اما من مشکل را تا ایستگاه‌کاری وی ردیابی نموده‌ام. این مشکل چه چیزی می‌تواند باشد؟

پاسخ : به‌خاطر داشته باشید که آنچه کاربر می‌گوید همیشه درونی و ذهنی است باید خودتان بررسی را انجام دهید تا ببینید وقایع چه هستند. همچنین با افراد دیگر در دفتر وی صحبت کنید. خودتان به ایستگاه‌کاری مورد نظر نگاهی بیاندازید احتمال دارد که واقعاً چیزهایی تغییر کرده باشد. البته SOAP چنین رهنمود می‌کند که هر آنچه که کاربر گزارش می‌دهد درونی محسوب می‌شود ـ وقایع را خود باید جستجو کنید.

پرسش : قبلاً اشکالاتی را به تولیدکنندگان نرم‌افزارها گزارش کرده‌ام که موفقیتی در پی نداشته است. برخی از آنها با حالت تشکرآمیزی گوش فرامی‌دهند اما چگونه می‌توان حدس زد. کدامیک این‌گونه برخورد می‌کنند؟

پاسخ : با فرض ارائه جزییات مشکل این‌گونه فکر می‌کنم که تولیدکنندگان کوچکتر نرم‌افزاری، همانهایی هستند که با میل به مشکلات کاربران خود پاسخ می‌دهند. تولیدکنندگان بزرگتر پیغامی برای شما ارسال می‌کنند نظیر «این اشکال در نگارش آتی اصلاح خواهد شد» یا «نرم‌افزار مطابق طرح مورد نظر کار می‌کند» باور داشته باشیم یا نه حتی تولیدکنندگان برنامه‌های Shareware نیز باید به‌خصوص بعد از آنکه تعداد زیادی مجوز از آنها دریافت کردید، مسئولانه با این قضیه برخورد کنند.

آزمون

۱- درونی به معنای چیست؟

الف ـ روشی که شخص موضوعی راآنگونه ملاحظه می‌کند

ب ـ وقایع

ج ـ نتایج حاصل از بررسی

د ـ درستی موضوع

۲- درست یا نادرست؟ یادداشتهای SOAP همیشه در دفعهٔ اول به یک نتیجه منجر می‌شوند.

۳- بخشی از اطلاعات درونی باید _____ .

الف ـ حذف شود.

ب ـ در مقابل بقیهٔ بخشها قرار گیرد.

ج ـ تقسیم شود.

د ـ مورد بررسی قرار گیرد.

۴- کدامیک از موارد زیر مثالی از بخشی از اطلاعات ظاهری نیست.

الف ـ چگونگی مشاهدهٔ مشکل از طریق کاربر

ب ـ یک اندازه‌گیری

ج ـ تعداد کاربران درگیر

د ـ زمان بروز مشکل

۵- تجزیه و تحلیل اغلب عبارت است از روال فکر کردن دربارهٔ؟

الف ـ اطلاعات و دلایل روشن

ب ـ اطلاعات درونی مدلل

ج ـ فقط اطلاعات ظاهری

د ـ اطلاعات درونی و ظاهری

۶- درست یا نادرست؟ جمع‌آوری اطلاعات بیشتر طرحی عمومی است.

پاسخ سؤالات آزمون

۱- الف

۲- نادرست

۳- د

۴- الف

۵- د

۶- درست

فصل ۷

روش سیمون ساده

رابرت هِین‌لِین داستانی را در یکی از کتابهایش تعریف می‌کند که در آن دو قورباغه به درون ظرف شیری می‌پرند و نمی‌توانند از آن خارج شوند. یکی از قورباغه‌ها که وضعیت ناامیدکننده را ملاحظه می‌کند، از دست و پا زدن دست برمی‌دارد و غرق می‌شود. دیگری به تلاش ادامه می‌دهد. خیلی زود جزیره‌ای از کره در وسط سرشیر ظاهر می‌شود و او روی آن شناور باقی می‌ماند تا هنگامی که شخصی می‌آید و او را بیرون می‌اندازد.

پافشاری یکی از نشانه‌های قورباغهٔ دوم و یا یک عیب‌یاب خوب شبکه می‌باشد! حتی هنگامی‌که فکر می‌کنید شکست خورده‌اید، «یک تلاش بیشتر» می‌تواند بغرنج‌ترین مشکلات را حل کند.

همانگونه که در فصل قبل توضیح داده‌ام، هنگامی‌که اوضاع امیدبخش به‌نظر نمی‌رسد، «مشاوره» امری مهم تلقی می‌گردد. این‌کار آسان، سریع و تقریباً بدون هزینه است. از آن گذشته، با مد نظر قراردادن دیدگاه اشخاص دیگر، می‌توانید مشاهدات یا وقایعی را که تا کنون از دست داده‌اید، جمع‌آوری نمایید. از آن بهتر، هنگامی‌که مشکلی را به شخص دیگری توضیح می‌دهید، ممکن است مجبور شوید جریان بروز مشکل را به گونه‌ای نمادین توضیح داده و روی نقاط مهم مجدداً تأکید کنید ـ که این خود اغلب اوقات باعث می‌شود خودتان بتوانید دید بهتری از مسئله داشته باشید.

یک نفر قبلاً مشکل شما را حل کرده است

آیا خوب نمی‌بود اگر می‌توانستید سریع و آسان از یک متخصص مشورت می‌گرفتید؟ از آن بهتر، بسیار عالی نبود اگر می‌توانستید این کار را رایگان انجام دهید؟ این‌کار شدنی است! بیشتر سازندگان این اجازه را به شما می‌دهند که در میان هزاران و هزاران قطعه از مستندات تفصیلی از سوی پرسنل پشتیبانی فنی، جستجوهایی را به انجام برسانید. به‌ویژه می‌توانید این‌راهنمایی‌ها را از استادان پشتیبانی فنی دریافت کنید. جستجو در یک پایگاه داده‌ای اطلاعات فنی می‌تواند یکی از بهترین روشهای اجتناب از اختراع دوبارهٔ چرخ باشد، به‌خصوص در مورد مشکلات تداخلی (که در آن قطعه‌ای نرم‌افزاری یا سخت‌افزاری، قطعه‌ای دیگر را تحت تأثیر قرار می‌دهد) یا مشکلاتی که توسط مستندات ضعیف حادث می‌گردد.

این موضوع برای واقعی‌بودن بیش از حد خوب به نظر می‌رسد. چرا سازندگان این‌کار را می‌کنند؟ خوب، برای گرداندن یک مجموعهٔ پشتیبانی فنی کارا مدیران فنی به پایگاههای اطلاعاتی خوبی نیاز دارند که شامل مشکل و تحلیل هر ارجاع پشتیبانی فنی می‌گردد، بدون اهمیت‌داشتن این نکته که مقدار این تحلیل چقدر کوچک یا بزرگ خواهد بود. این‌کار به آنها اجازه می‌دهد که دیگر به اختراع دوبارهٔ چرخ نپردازندو زمان بسیار زیادی را برای خود پس‌انداز کنند (در نتیجه از لحاظ پولی نیز بسیار بهره می‌برند). از آنجا که پشتیبانی یکی از سرویس‌هایی است که باعث رجوع دوبارهٔ مشتریان می‌گردد،

برای سازندگان به صرفه است که با تلاشی جزیی این پایگاههای اطلاعاتی را در دسترس عموم قرار دهند. قابلیت دسترسی این پایگاههای اطلاعاتی به شرکتهای نرم‌افزاری این اجازه را می‌دهد که حجم پشتیبانی تلفنی رایگانی که ارائه می‌کنند، کم نمایند ـ آنها همیشه به کاربران می‌گویند که از پایگاه اطلاعاتی وِب به‌صورت مجانی استفاده نمایند.



نکته : *باید مطمئن شوید که جستجو را از صفحه‌خانهٔ[1] شرکت به‌انجام نرسانید. جستجوهایی که در صفحه‌خانه اصلی رخ می‌دهند، اغلب تمام سایت شرکت را مورد جستجو قرار داده و اطلاعات غیر فنی نظیر نگارشهای انتشاری را نیز شامل می‌شوند. اغلب شرکتها، یک صفحه‌خانه پشتیبانی فنی دارند که به جستجوی فنی مجهز است. همانگونه که صفحه‌خانهٔ شرکت را می‌توانید در آدرس www.company.com پیدا کنید، صفحات مربوط به پشتیبانی فنی اغلب در support.company.com یا www.company.com/support قرار گرفته‌اند.*



نکته : *با این‌که به نظر می‌رسد بهترین نتایج جستجو با واردکردن بیشترین کلمات ممکن به دست می‌آید، برخی اوقات این‌کار به «شلوغی جستجو» منجر می‌شود. برای مثال، اگر دنبال عبارت network card error 78E8 بگردیم، حضور کلمهٔ network باعث ایجاد تطابق در تعداد بسیار زیادی سند خواهد شد. همین وضعیت در مورد کلمات card یا error وجود دارد. در این حالت بهتر است تنها به دنبال 78E8 بگردید.*

اگر سایتی به موتور جستجوی پیچیده‌تری مجهز باشد، این روش لازم نخواهد بود. در چنین سایت‌هایی می‌توانید جستجوهایی نظیر:

network card error +78E8

یا

"network card error" AND "78E8"

را صورت دهید که هر دو به معنای آن هستند که تطابق‌ها تنها در صورت وجود عبارت 78E8 نشان داده شود.

جستجو برای پشتیبانی در تمامی محل‌های صحیح

در حقیقت، جستجو در پایگاه اطلاعاتی پشتیبانی فنی مربوط به سازنده، نظیر تماس با اپراتور پشتیبانی سطح اول در هنگام یک مکالمه برای پشتیبانی فنی می‌باشد. کلید، دانستن آنچه که باید جستجو گردد و جایی که جستجو باید صورت گیرد، می‌باشد.

برای مثال، فرض کنید که می‌خواهید از ویندوز NT در دفتر کار خود استفاده نمایید. از آنجا که شما شخص مسئول و با دقتی هستید، در ابتدا به آزمایش و استفادهٔ محدود از محصول دست می‌زنید. در نیمه راه این‌کار، یکی از کاربران گزارش می‌کند که هنگام استفاده از DOS EDIT و سایر برنامه‌های کمکی DOS با مشکل روبرو است. از او خواسته می‌شود که دیسکی را در گردونهٔ A قرار دهد، حتی اگر به دیسک کاری نداشته باشیم. این واقعاً عجیب است. از خود سؤال می‌کنید،

1- home page

«چه‌چیزی در این‌جا نظیر بقیه نیست؟» و به‌سوی ماشین کاربر دیگری می‌دوید. این‌کار را با استفاده از ماشین و اطلاعات ورود به سیستم کاربر دیگری انجام می‌دهید و همان نتایج را ملاحظه می‌کنید.

چنین به نظر می‌رسد که تمامی ماشینهایی که مورد آزمایش قرار گرفته‌اند همین مشکل را دارند. واضح است که آزمایش را متوقف می‌کنید. اما حالا مشکل عجیبی دارید ـ چرا ماشین جدیدی مثل این، چنین رفتاری را از خود بروز می‌دهد؟ در واقع هر ماشینی که مورد آزمایش قرار گرفته است، این‌گونه عمل می‌نماید. آیا این خطایی سخت‌افزاری است؟ خطایی نرم‌افزاری است؟ اگر چنین است، کدام نرم‌افزار؟ آیا این مشکل به شبکه مربوط می‌شود؟

بسیاری از افراد ممکن است در این مقطع راه را اشتباه طی کنند، بنابراین زمان خوبی برای آن است که دقایقی را به جستجو بپردازیم. خوشبختانه آنچه را که می‌خواهید مورد جستجو قرار دهیدبه‌صورت یک پیغام خطای گستاخانه، پیش رویتان قرار دارد:

```
NTVDM; No disk, Please insert a disk into drive A:
```

مشخص‌ترین محل جستجو، سایت میکروسافت، چیز مشخصی را آشکار نمی‌کند به‌جز آنکه لازم است مسیر فایل NT را برای ارجاعات به گردونهٔ A جستجو کنید، که باز هم چیزی پیدا نخواهید کرد. به‌منظور پیداکردن محل جستجوی پاسخهای خود، زمان آن فرارسیده که چیزهایی را که به ماشین جدید اضافه نموده‌اید، دسته‌بندی نمایید:

- تنظیم ویندوز NT
- محافظ ویروس Intel
- مجموعهٔ WordPerfect نگارش ۸
- نرم‌افزار پُست الکترونیکی و زمانبندی GroupWise

اما صبر کنید! در این‌جا دو قطعه از معما را جاانداخته‌اید. شما تنها به نرم‌افزارهای کاربردی فکر می‌کردید اما در واقع قطعات بیشتری هستند که باید آنها را در این فهرست جای دهید. اجازه دهید از بالا به پایین حرکت کنیم و آنچه که شما برای ایجاد این ماشین جدید انجام داده‌اید را بنویسیم. منابع احتمالی مشکل که در فهرست قبل از قلم افتاده‌اند، در فهرست ذیل به‌صورت پررنگ نشان داده شده‌اند:

- بازکردن کامپیوتر ***Dell*** از جعبه
- برنامهٔ تنظیم به‌صورت خودکار اجرا شد. NT و ***Microsoft Service Pack 3*** نصب گردید
- ***Novell IntranetWare Client32*** (که برای اتصال به سرویس‌دهندهٔ ناول لازم است) نصب شد.
- کارت شبکهٔ ***3Com Ethernet*** پیکربندی شد.
- محافظ ویروس Intel، مجموعهٔ Corel WordPerfect نگارش ۸ و GroupWise ناول، نصب شدند.

شمارش مراحل ایجاد ایستگاه‌کاری، فهرستی از تولیدکنندگان که جستجو در آنها باید صورت بگیرد را به‌دست می‌دهد. فهرست نهایی شامل موارد زیر است:

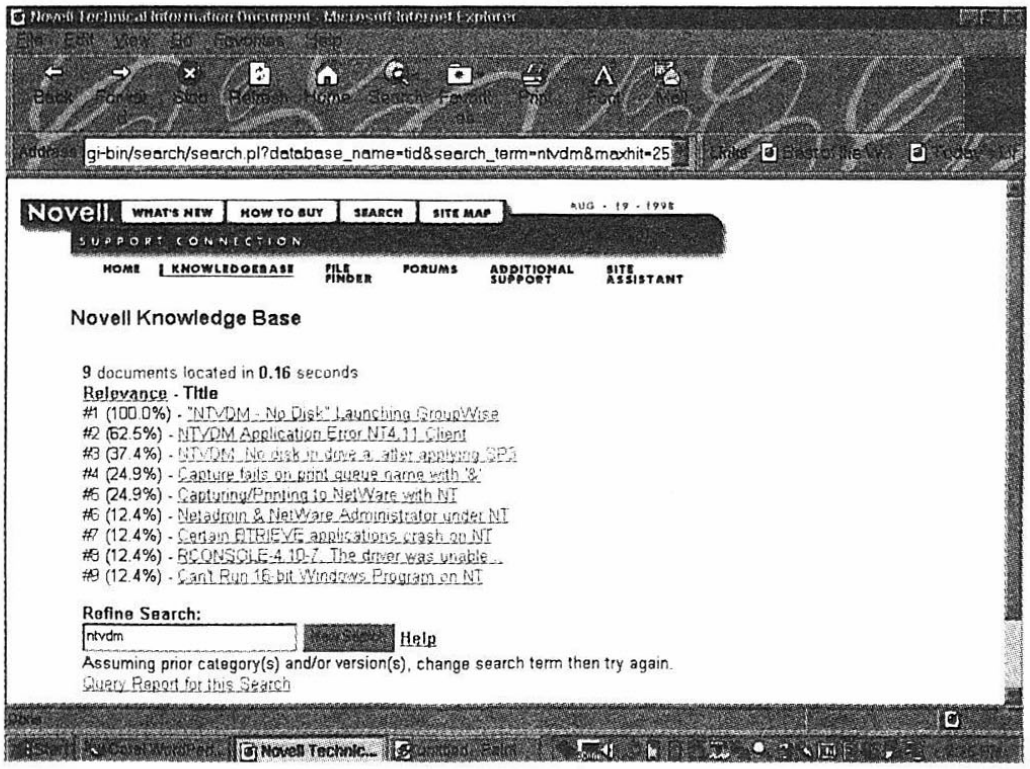
- Dell
- میکروسافت
- ناول
- 3Com
- Intel
- Corel

به‌جای ایجاد یک PC جدید از ابتدا، که ممکن است از یک ساعت تا دو ساعت به‌طول بیانجامد (اگر همه چیز مرتب باشد!)، به سایت‌های وِب زیر رفته و پیغام خطای دریافتی را در آنها مورد جستجو قرار دهید:

- http://support.dell.com
- http://support. microsoft.com
- http://support.novell.com
- http://support.3com.com
- http://support.corel.com

ممکن است کار را با واردکردن NTVDM شروع کنید، چرا که واژه‌ای منحصر به فرد است (دوباره، نمی‌خواهید که کلمات معمولی نظیر ***disk*** را در فهرست موارد پیداشده داخل کنید)، و آنگاه در صورت دریافت تطابق‌های بسیار از کل عبارت خطا استفاده نمایید. (به خاطر داشته باشید که به غیر از مواردی که می‌توانید برای کلمه «وزنی» را تعریف کنید ـ که این‌کار در تمامی سایت‌ها ممکن نیست ـ ارزش تمامی کلمات یکی است؛ بنابراین، واردکردن عبارت NTVDM insert disk تعداد زیادی سند را ارائه می‌کند که در آنها کلمات insert و disk به‌کار رفته است.)

Dell هیچ اطلاعی در مورد NTVDM ندارد. میکروسافت میلیونها سند اطلاعاتی دارد و کلمهٔ NTVDM را در نزدیک به ۱۰۰ سند پیدا خواهید نمود. تصمیم می‌گیرید که در صورتی‌که جای دیگری چیزی پیدا نکردید به این‌جا برگردید. سومین تلاش شما که در شکل ۱-۷ نشان داده شده است، ۹ سند را که عددی قابل قبول و بررسی است، ارائه می‌کند. نگاهی سریع، یک سند تکنیکی را آشکار می‌سازد که دقیقاً مشکل شما را توضیح می‌دهد. عبارت پیوندی مربوطه را انتخاب می‌کنید. در این حالت متوجه می‌شوید که Novell Client32 با Windows NT Service Pack 3 مشکلی دارد که باعث بروز مسئلهٔ شما می‌گردد. این سند جزییات رفع اشکال را یادآور می‌شود (کپی‌کردن NTDOS.SYS از دیسک ویندوز NT به فهرست C:\WINNT\SYSTEM).



شکل ۱-۷: جستجو در سایت‌های متعدد به‌جای صرف زمان زیاد می‌تواند راه‌گشای مشکلات باشد.



نکته : *هنگام عیب‌یابی مسئله‌ای که به چندین سازنده مربوط می‌شود، در ابتدای کار وقت چندانی را در هر سایت تلف نکنید ـ یکی از سازندگان ممکن است راه حل سریعی را ارائه کند، در حالی‌که در سایت دیگر ممکن است مجبور باشید صدها سند را بررسی نمایید.*

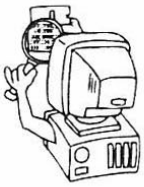
پنج دقیقه بعد از آغاز برنامهٔ مرورگر وِب، مشکل را حل نموده‌اید. ممکن است ساعتهای زیادی را صرف پیاده‌نمودن روش تفرقه‌بیانداز ـ و ـ حکومت‌کن برای پیداکردن مشکل صرف می‌نمودید، البته در صورتی‌که از قدرت باورنکردنی جستجوی پشتیبانی فنی چشم‌پوشی می‌کردید.

مشکلی تکنیکی در راه انجمن اتفاق افتاد

قدرت انجمن‌های عمومی را دست کم نگیرید ـ گروههای خبری یوزنت و فهرستهای پستی می‌توانند منبع فوق‌العاده ارزشمندی باشند. برخی از سازندگان این گروهها را در صفحه‌خانه‌های خود پشتیبانی نمی‌کنند چرا که یوزنت همیشه با آنها مهربان نیست (دیدن پیغامهای پستی با عنوان «فلان محصول بوی بد می‌دهد!»، چیز غریبی نیست). تولیدکنندگان و سازندگان دوری از یوزنت و فهرستهای پستی خارجی را ترجیح می‌دهند چرا که فاقد توانایی پاسخگویی به تبادل پیغامهای عمومی در این غرب وحشی می‌باشند. از همهٔ این موارد گذشته، این میدان‌ها و انجمن‌ها منبع اطلاعات دنیای واقعی محسوب می‌شوند ـ اطلاعاتی که نمی‌توانید آنها را از سازندگان و تولیدکنندگان به‌دست آورید (حتی با وجود غرق‌شدن در مقادیر زیادی اطلاعات، ممکن است به اطلاعات مفیدی برنخورید).



نکته : *فراموش نکنید که قبل از مراجعه به وِب، سایت‌های پشتیبانی سازندگان را جستجو کنید. برخی اوقات این‌کار باعث صرفه‌جویی در زمان می‌شود.*



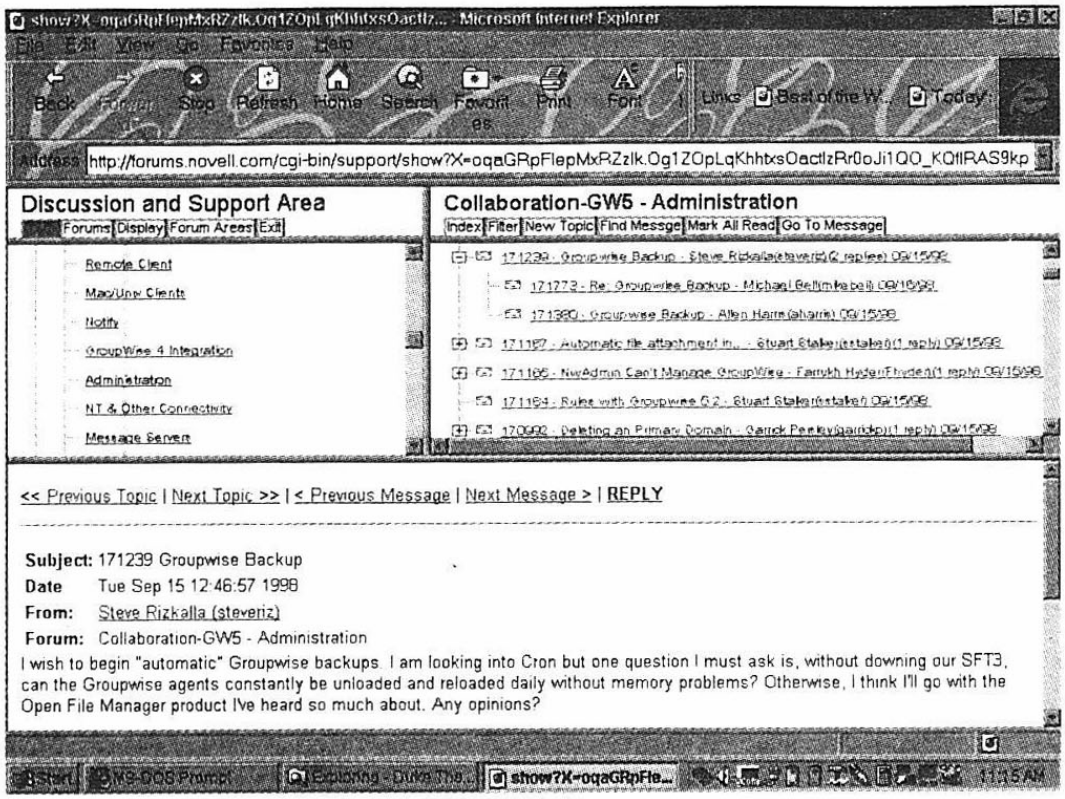
نکته : *بیشتر موتورهای جستجوی وِب (AltaVista، Lycos و نظایر آنها) این امکان را به شما می‌دهند که به‌جای جستجوی صفحات وِب، به جستجو در یوزنت بپردازید. البته استفاده از یک موتور جستجوی مخصوص گروه خبری نظیر www.dejanews.com بهتر خواهد بود؛ می‌توانید جستجوهای مخصوصی را انجام داده و همچنین جستجوی خود را به اخبار جدید محدود سازید.*

خوشبختانه می‌توانید یوزنت را نیز مورد جستجو قرار دهید. اگر فراهم‌کنندهٔ اینترنت شما گروههای خبری یوزنت را در اختیارتان نمی‌گذارد، یا اگر برنامهٔ کاربردی اخبار مورد استفاده‌تان، جستجوها را پشتیبانی نمی‌کند، می‌توانید از موتورهای جستجوی موجود در وِب برای جستجوی عنوان مورد نظر یا پیغام خطای پیش‌آمده، بهره بجویید.

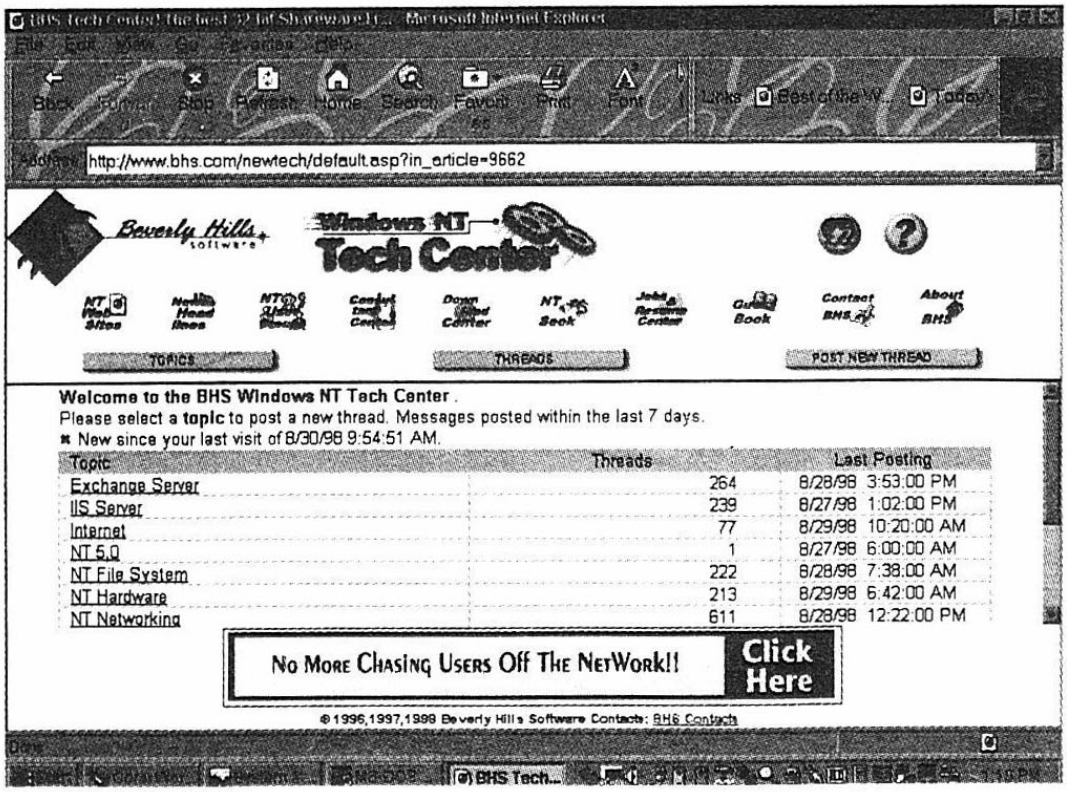
علاوه بر گروههای یوزنت و فهرستهای پستی، برخی از سازندگان و فروشندگان، انجمن‌های مبتنی بر وِب مخصوص به خودی را دارند که استفاده از آنها رایگان می‌باشد. چنین مواردی بسیار خوب هستند، چرا که توسط پرسنل پشتیبانی فنی مسلط تحت نظارت قرار می‌گیرند. با این‌که سازندگان اجباری در پاسخگویی به سؤالات ارسالی ندارند، این امکان وجود دارد که سؤالات مطرح‌شده به دست افراد مناسبی برسد و آنها قادر باشند که به شما در استفاده از محصولات بدون عیب خود کمک کنند (شکل ۲-۷ را ملاحظه کنید).

برخی اوقات انجمن‌هایی را ملاحظه می‌کنید که توسط فروشندگانی راه‌اندازی شده که از آنها برای تبلیغ ابزار تولیدی

خود استفاده می‌نمایند. جاذبهٔ این انجمن‌ها آن است که چنین تولیدکنندگانی در مورد محصول خود حساس هستند و سعی می‌کنند که آن را به شکلی کارا در اختیار سایر کاربران قرار دهند (شکل ۳-۷، صفحهٔ انجمنی نمونه را برای ویندوز NT نشان می‌دهد).



شکل ۲-۷: کاربرد انجمن وِب ناول.

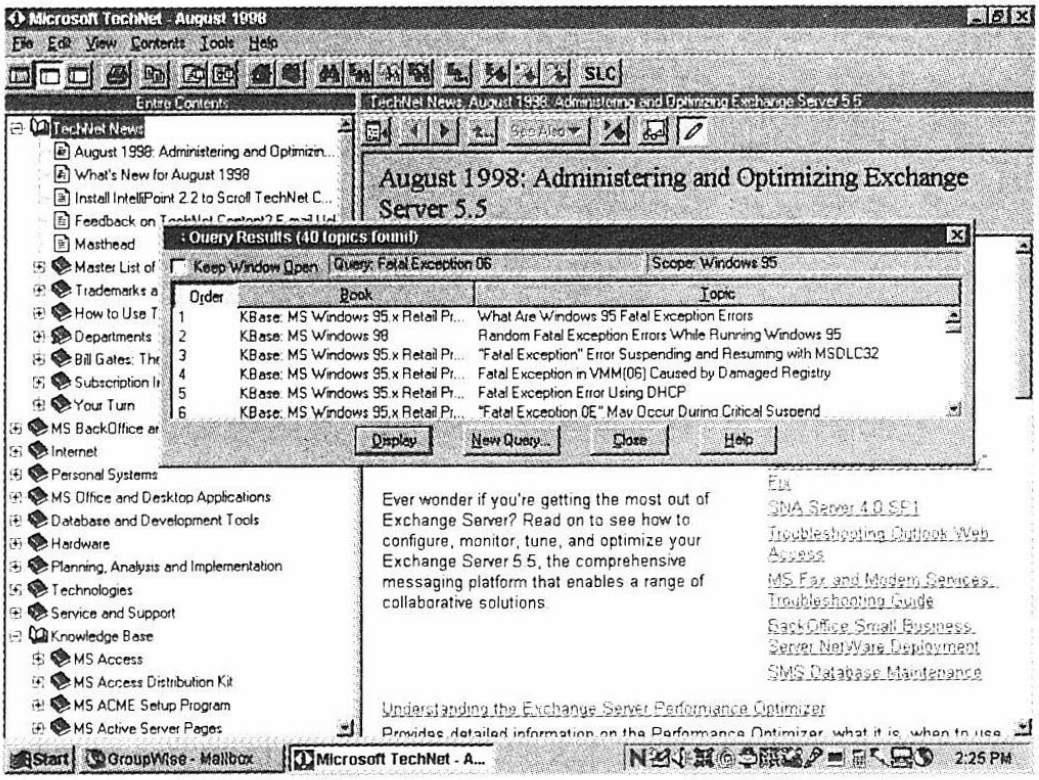


شکل ۳-۷: یک سایت پشتیبانی ویندوز NT.

بلیط بازی

پشتیبانی رایگان مسئولیت کمی را به دوش سازنده و فروشنده می‌گذارد اما می‌تواند در صورتی که از مسیر صحیح مشکل را ردیابی کنید به‌کار آید. اما هنوز برخی اوقات ممکن است به چیزی بیشتر از آن نیاز داشته باشید که بتوانید به‌صورت رایگان دریافت کنید؛ در این حالت می‌توانید از یک پایگاه اطلاعاتی پشتیبانی فنی به‌صورت CD-ROM بهره بجویید.

به‌خصوص، برخی از پایگاههای اطلاعاتی مبتنی بر وِب، نظیر میکروسافت، آنقدر شلوغ هستند که ممکن است برای انتقال هر صفحه زمان زیادی را به انتظار بگذرانید. به‌جای آن می‌توانید با پرداخت هزینهٔ‌معادل ۲۰۰ دلار در TechNet میکروسافت ثبت نام نمایید. همانند پایگاههای اطلاعاتی CD-ROM، همانقدر دریافت می‌کنید که برای آن پرداخت می‌نمایید ـ امکانات پیچیدهٔ و ویژگیهای ترکیبی بیشتر که دسترسی سریع‌تر را ممکن می‌سازد. برای مثال می‌توانید نتایج جستجوی خود را توسط نوع محصول پالایش کنید و از نشانگذاری استفاده نمایید. TechNet دارای تمامی مستندات اطلاعات فنی در سایت وِب می‌باشد و تقریباً ده برابر سریعتر اجرا می‌شود (شکل ۴-۷).



شکل ۴-۷: یک جلسهٔ TechNet میکروسافت.

صحبت با TechNet

از آنجا که من با مشکلات بسیاری در استفاده از محصولات میکروسافت مواجه هستم، از TechNet به‌صورت سنگین و گسترده‌ای استفاده می‌کنم. البته این‌کار نوعی دستپاچگی ایجاد می‌کند، چرا که TechNet باعث می‌شود شما نظیر قهرمانی به‌نظر برسید که آنچه را برای قهرمانی به انجام رسانده‌اید، با چند فشار روی دکمه‌های ماوس

روی صفحه ظاهر می‌شوند. برای مثال، روزی دو تکنسین در مورد یک خطای fatal exception از من سؤالاتی کردند. به‌جای مراجعه به ایستگاه‌کاری مورد سؤال، پیغام خطای مورد نظر را در TechNet وارد نمودم که دو مورد تطابق اعلام نمود ـ یکی از آنها به‌نظر مناسب می‌رسید. برای انجام پیشنهاد TechNet به محل مراجعه نمودیم، مشکل در ظرف مدت ۱۰ دقیقه حل شده بود.

TechNet تنها برای جستجوها به‌کار نمی‌رود. می‌توانید از طریق عناوین، صفحات سفید میکروسافت و کیتهای منبع را مرور کنید و منبعی عالی برای آموختن و مطالعه را تجربه نمایید.



***نکته** : به رئیس خود بگویید که چگونه می‌تواند به‌جای پرداخت هزینهٔ یک یا دو تلفن به بخش پشتیبانی فنی و یا یکی دو بازدید مشاور ـ ۱۵۰ ـ دلار در ساعت ـ شرکت، این گونه محصولات را خریداری کند.*



***یادداشت** : مشخص است که اگر مشکلی در یک چارچوب زمانی قابل قبول، حل نشود، باید برای دریافت کمک به بیرون از مجموعهٔ کاری خود مراجعه کنید: زمان (به‌خصوص زمان خرابی) مساوی است با پول، و چند ساعت زمان مشاوره می‌تواند در مقایسه با زمان از دست رفتهٔ کاری هنگام خرابی ابزاری حساس، مقرون به صرفه باشد. اگر در نهایت به این نتیجه رسیدید که لازم است از چنین کمکی استفاده کنید، ناراحت نشوید ـ کار شما از دست نرفته است. انجام تکالیف عیب یابی می‌تواند و خواهد توانست صدها و حتی هزاران دلار را برای شرکت‌تان صرفه جویی کند چرا که شما مشکل را تا حد زیادی برای مشاور خارجی تحلیل نموده‌اید.*

پایگاههای اطلاعاتی پشتیبانی فنی «کادیلاک» (برای مثال Support Source از شرکت MicroHouse) یکهزار دلار در سال هزینه دارند بهتر است قبل از مراجعه به این سایت‌ها و صرف چنین هزینه‌هایی به خوبی و سختی فکر کنید. با این‌که این‌گونه منابع شامل مستندات تحقیق‌شدهٔ دقیقی هستند و دارای منابع پشتیبانی فنی چند منبعی می‌باشند و از طرفی برای متخصصانی که به پاسخهایی سریع نیاز دارند، اعجاب‌انگیز به شمار می‌روند؛ باید دفعات مراجعه به آنها را مورد مطالعه قرار دهید. با این‌که این سرویس‌ها اغلب حاوی خودآموزها و مقالات مجله‌ای بسیاری هستند که قابلیت جستجو در آنها تعبیه شده است ممکن است چنین احساس کنید که می‌توانید نیازهای خود را با استفاده از موتورهای جستجوی مبتنی بر وب تأمین نمایید (شکل ۵-۷ را ملاحظه کنید). به غیر از حالتی که به مقدار زیادی با عیب‌یابی سروکار دارید (که در این حالت به ارتقاء کاری نیز نیاز خواهید داشت)، این نوع از سرویس‌ها ممکن است فاقد ارزش معادل پرداخت به کارگیری آنها باشند.

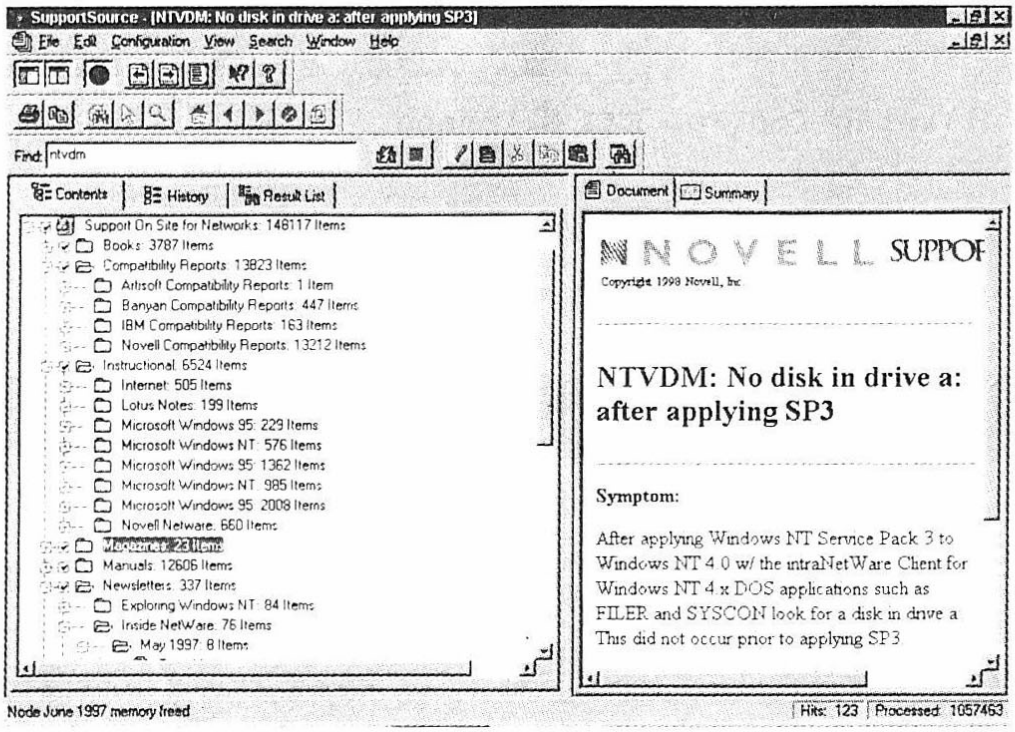
همبستگی

اگر راهنما را مطالعه کرده باشید، پایگاههای داده‌ای را بررسی نموده ولی هنوز به نتیجه نرسیده‌اید، زمان آن است که با فروشنده تماس بگیرید. بسته به این‌که با مشکلی ناامیدکننده روبرو هستید و یا این‌که قراردادی پشتیبانی دارید، دو استراتژی وجود دارند که می‌توانید با استفاده از آنها ملاقات با شخص پشتیبانی فنی حرفه‌ای را پربارتر سازید.

اولین تلاش شما، بسته به آن است که چگونه مشکل را در طی تلاشهای عیب‌یابی خود مستندسازی کرده باشید. اگر از

یادداشتهای SOAP در طی این مراحل استفاده نموده باشید، به احتمال زیاد آنچه را که چنین شخصی می‌خواهد و به آن نیاز دارد، در اختیار دارید:

- نوع سخت‌افزار درگیر
- نوع شبکه (نقشه‌ها)
- برنامه(های) کاربردی
- ارتباطهای زمانی (وقوع، زمان روز)
- وضعیت تکرار



شکل ۵-۷: یک جلسهٔ MicroHouse Support Source.



***یادداشت** : اگر نمی‌توانید مشکلی را دوباره تکرار کنید، افراد دیگر در آن سوی مکالمهٔ تلفنی برای حل مشکل نیز نمی‌توانند. البته اگر می‌توانید مشکل را در ایستگاه‌کاری متفاوت یا سرویس‌دهندهٔ دیگری تکرار کنید، به متقاعدکردن افراد پشتیبان فنی به این‌که مشکل مورد نظر معقول بوده و تنها زادهٔ محیط شبکه‌ای شما نیست، نزدیک شده‌اید.*

افرادی که قبل از جمع‌آوری این اطلاعات اساسی، با پشتیبانی فنی تماس می‌گیرند، اغلب اطلاعات بی‌ارزشی دریافت می‌کنند. (مسئله این‌جا است که بعد از انجام تحقیقات و بررسی مستندات متهم و مقصر اصلی آشکار می‌شود و بنابراین نیاز به تماس با پشتیبانی فنی در گام اول از بین می‌رود). از آنجا که شما فردی غیر حرفه‌ای محصوب می‌شویدنمی‌توانید ثابت کنید مشکل به فروشندهٔ دیگری مرتبط نیست و بنابراین نمی‌توان پشتیبانی فنی را متقاعد کرد که مشکل در محصول آنها است.

می‌توانید از طریق پافشاری بر اثبات مستند شده‌ای که آن را با کمک فروشنده و یا از طریق انجام بررسی توسط خود

به دست آورده‌اید، به مبارزه ادامه دهید. همانگونه که در فصل ۲۱ ملاحظه خواهید کرد برای ارائهٔ ردیابی‌های شبکه‌ای به پشتیبانی فنی لازم نیست در کار شبکه خبره باشید. ردیابی‌های شبکه‌ای، حسابهای لحظه به لحظه‌ای هستند از آنچه که روی خط شبکه به وقوع می‌پیوندد و می‌توانند برای تجزیه و تحلیل‌گر شبکه در آن سوی خط بسیار مفید باشند.

می‌توانید با استفاده از انجام عملیات مختلف به‌صورت دستی و بدون نفوذ قلم مورد اشاره، از هدایت نادرست اعضای پشتیبانی فنی جلوگیری کنید. به عبارت دیگر، اگر برنامه‌ای می‌گوید که نمی‌تواند در فایلی روی سرویس‌دهنده چیزی بنویسد ولی شما تصور می‌کنید که باید بتواند، سعی کنید که این کار را خودتان تحت همان اسم ورود و محیطهای جلسه‌ای (بدون راه‌اندازی مجدد یا خارج‌شدن از سیستم) به انجام برسانید. بنابراین اگر برنامهٔ تنظیم می‌گوید:

```
Can't copy "FOO.EXE" from D:\setup\foo to G:\myapp n Retry?
```

بهتر است که از محل اعلان DOS این کار را به انجام برسانید:

```
C:\> COPY D:\setup\foo\FOO.EXE G:\myapp
```

به همین صورت می‌توانید از Windows Explorer برای کپی‌کردن FOO.EXE از D:\setup\FOO به g:\myapp استفاده نمایید.

متصرداشتن دیگران

زمانی مشکل غریبی با یک سرویس‌دهنده داشتم ـ برنامه‌های کاربردی مشخصی را نمی‌توانستم در آن نصب کنم. نشانهٔ عمومی این وضعیت آن بود که برنامهٔ نصب اعلام می‌نمود که نمی‌توانست فایل‌های مشخصی را در فهرست معینی ثبت کند. تولیدکنندگان برنامه می‌گفتند «این برنامه روی هزاران سرویس‌دهندهٔ دیگر نظیر سرویس‌دهندهٔ شما به‌خوبی کار کرده است!». پاسخ فروشندهٔ سرویس‌دهنده این بود که این برنامه‌ها می‌بایست کاری غیر عادی را هنگام نصب انجام دهند. من اعتراض کردم، «نه، بیش از یک برنامه این مشکل را ایجاد می‌کند ـ مشکل باید در سرویس‌دهنده باشد!». مشکل کنار گذاشته شد تا این‌که یکی از تکنسین‌ها ایدهٔ انجام کپی دستی فایل‌های مشکل‌دار را مطرح نمود. به عبارت دیگر، یکی از برنامه‌های کاربردی که من در تلاش بودم نصب بکنم هنگام کپی‌کردن فایل KBSTUFF.SYS با شکست مواجه می‌شد، بنابراین دستور زیر را تایپ کردم:

```
f:\> copy d:\setup\dbstuff.sys f:
```

و آنطور که تقریباً مطمئن بودم، خطایی صادر شد ـ با این‌که می‌توانستم فایل‌هایی با اسامی دیگر را به آن فهرست کپی کنم (با این‌که مجوزهای فایلی برای ثبت و نوشتن در فهرست را دارا بودم) با تکنسین فروشندهٔ سرویس‌دهنده تماس گرفتم که پاسخ داد، «من باید این موضوع را از نزدیک ببینم!».

تکنسین از من خواست که ترافیک شبکه را بین ایستگاه‌کاری و سرویس‌دهنده (معادل شبکه‌ای شیرفلکه) متوقف کنم. یک روز بعد از در اختیارگذاشتن ردیابی‌های ثبت‌شده، فروشندهٔ سرویس‌دهنده اعلام نمود که، بله، سرویس‌دهنده به گونه‌ای نادرست به ایستگاه کاری پاسخ می‌داد. فروشنده پرسید، «آیا محافظ ویروس روی سرویس‌دهنده داریم؟» این چنین بود، و بعد از برداشتن بستهٔ نرم‌افزاری محافظت از ویروس، مشکلی در ارتباط با نصب برنامه‌های کاربردی مشاهده نشد. معلوم شد که تداخل بین برنامه‌های کاربردی‌ای که در سروس ,دهنده

نصب کرده بودم مشکل را ایجاد کرده بود. برنامهٔ محافظت از ویروس قدیمی بود و بنابراین با تغییرات جدید مطابقت نشده بود ـ ارتقاء نگارش این برنامه مد نظر قرار گرفت، اما حداقل آن بود که من توانسته بودم مشکل را ردیابی نمایم.

فروشنده‌هایی هستند که ممکن است اطلاعات فنی مفیدی را فراهم کنند. خوشبختانه من با برخی از این فروشنده‌ها برخورد داشته‌ام و متأسفانه به ندرت چنین افرادی را پیدا خواهید کرد در صورت مواجه‌شدن با چنین فروشنده‌ای تا می‌توانید از محصولات وی خریداری کنید. روی هم رفته تکنسینهای پشتیبانی خوب می‌توانند کمک بزرگی باشند و مسلماً نباید از تماس با آنها غافل باشید.

خلاصه

بعضی اوقات، بهترین روش حل یک مشکل پیداکردن شخص دیگری است که آن مشکل را تجربه نموده است. موتورهای جستجوی اینترنت، انجمن‌های اینترنت، فهرستهای پستی و پایگاههای داده‌ای CD_ROM روشهای بسیار خوبی برای توسعهٔ تلاشهای عیب‌یابی می‌باشند. پشتیبانی فنی به‌عنوان آخرین تیر در ترکش باید مد نظر باشد؛ اگر بهره‌گیری از پشتیبانی فنی به همراه یک مشکل قابل ایجاد و تکرار و مستندسازی شده همراه باشد به احتمال بسیار زیاد با اهمیت و توجه لازم روبرو خواهید شد اطلاعات بی‌ارزش نظیر مقصردانستن دیگران را می‌توان با استفاده از یادداشتهای خوب و تکرار مشکل بدون استفاده از محصول یا مؤلفه‌ای که فروشنده ادعای اشکال در آن را دارد، می‌تواند کنار گذاشته شود. دانسته‌های کاری از مهره‌های تجزیه و تحلیل نظیر یک فرد مسلط بر تجزیه و تحلیل شبکه، می‌توانند به حل مشکل و جمع‌آوری اطلاعات لازم به منظور اجتناب از مقصردانستن فروشندگان دیگر کمک نماید.

کارگاه

پرسش و پاسخ

پرسش : چرا فهرستی از سایت‌های پشتیبانی فنی را که می‌شناسید، معرفی نمی‌کنید؟

پاسخ : چنین اطلاعاتی هر شش ماه تغییر می‌کند؛ تکنیک‌هایی که تا به حال فراگرفته‌اید ثابت باقی می‌ماند (خبرگان کامپیوتر می‌گویند: «برو ناهار بخور، تا پاییز فرصت زیادی است»). باید فرابگیرید که چگونه سایت‌های به‌خصوصی را علاوه بر چگونگی جستجو در آنها پیدا کنید تنها کافی است راهنمایی‌های ذکر شده را برای پیداکردن سایت وِب سازندگان به کار ببندیم، نباید مشکلی وجود داشته باشد سایت‌های پشتیبانی فنی زیادی خارج از آنهایی که توسط سازندگان ارائه شده‌اند وجود ندارد اما برای تفریح هم که شده، می‌توانید با استفاده از موتورهای جستجوی استاندارد اینترنت نظیر Alta Vista جستجوهایی را صورت دهید، برای مثال، می‌توانید عبارت "**Linux free support**" را وارد کنید.

پرسش : نمی‌توانم مشکلی تناوبی را مجدداً تکرار کنم. می‌فهمم که درست نیست از پشتیبانی فروشنده تا هنگامی که مشکل قابل تولید مجدد باشد استفاده نمایم، اما چگونه می‌توانم این موضوع را برای رئیسم شرح دهم؟

پاسخ : لازم است به تکنیک تفرقه‌بیانداز ـ و ـ حکومت کن برگشته، یادداشتهای SOAP بردارید و ناحیه مشکل‌دار را با سایر نواحی کاری مقایسه کنید. اگر ایستگاههای کاری دیگر یا نصب برنامه‌های کاربردی دیگر به‌خوبی کار می‌کنند ممکن است لازم باشد کلبه را آتش زده و آن را از دوباره بسازید. به غیر از این موضوع یادداشت‌برداری منظم و کمک‌گرفتن از تجربه‌های دوستانتان که با مشکل تناوبی روبرو شده‌اند را باید مد نظر قرار دهید. من مشکل شما را درک می‌کنم. البته اگر به کار ادامه دهید، بر آن فائق خواهید شد. اگر مشکل به اندازهٔ کافی مهم است آن را با فروشنده در میان بگذارید؛ بخش فنی فروشنده ممکن است بتواند سرنخ‌هایی را به شما بدهد که شما در روال انجام کار خود جا انداخته‌اید.

آزمون

۱- با کدام‌یک از موارد زیر می‌توان بهتر در یک سایت پشتیبانی جستجو نمود؟

الف ـ حداکثر کلمات کلیدی ممکن
ب ـ یک کلمهٔ کلیدی منحصر به فرد
ج ـ عبارت یا پیغام خطای محصور در گیومه
د ـ هم ب و هم ج

۲- قیمت یک CD-ROM پشتیبانی مورد نیاز شما ۷۵۰ دلار است. رئیس‌تان از شما می‌پرسد که خریدن آن معادل چند ساعت مشاورهٔ پشتیبانی می‌باشد. با در نظر داشتن ۱۵۰ دلار در هر ساعت (که نرخ فعلی مشاوره است)، به این نتیجه می‌رسید که می‌توانید از ـــ ساعت مشاوره با خرید CD-ROM اجتناب کنید.

الف ـ ۳
ب ـ ۹
ج ـ ۵
د ـ ۱۵

۳- درست یا نادرست؟ گروههای مباحثهٔ یوزنت همیشه در مورد موضوعات تکنیکی و فنی، درست اظهار نظر می‌کنند.

۴- برای جستجو در پایگاههای اطلاعاتی پشتیبانی شرکت Frobozz Fabulous FiberSwitch از کجا شروع می‌کنید.

الف ـ http://www.frobozz.com/frotz
ب ـ http://www.support.frobozz.com
ج ـ http://support.frobozz.com
د ـ http://frobozz.com/www.support

پاسخ به سؤالات آزمون

۱- د
۲- ج
۳- نادرست
۴- ج

بخش سوم

مواظبت و تغذیهٔ اسباب شبکه

فصل ۸ : «مبانی سخت‌افزار»:
چگونه استادکار سخت‌افزار شویم؟
فصل ۹ : مبانی اِترنِت
فصل ۱۰ : مبانی حلقه ـ نشانه
فصل ۱۱ : مبانی شبکه در ویندوز
فصل ۱۲ : مبانی شبکه در یونیکس
فصل ۱۳ : مبانی شبکه در نت‌ور
فصل ۱۴ : مبانی مسیریاب و سوئیچ
فصل ۱۵ : مبانی دیوار آتش و سرویس‌دهندهٔ پروکسی

فصل ۸

«مبانی سخت‌افزار»: چگونه استادکار سخت‌افزار شویم؟

«ما تنها با از بین بردن و تخریب است که به درستی یاد می‌گیریم.»
ـ پست یوزنت، *COMP.SYS.UNIX* (سیرکا ۱۹۸۰)

خبرگان شبکه به‌صورت بسته‌بندی‌شده زندگی نمی‌کنند؛ همهٔ ما باید بدانیم که چگونه با چیزهایی که شبکهٔ ما بر پایهٔ آنها زندگی می‌کند برخورد نماییم. کارهای شبکه‌ای چه این‌که با برد سخت‌افزاری خراب یا نقطه‌ای آسیب‌دیده در گردونهٔ دیسک سخت مواجه باشیم، ضربه زننده هستند؛ آنها هنگامی‌که قطعات زیرین و بخشهای پس پرده (ساختار درونی) از کارکردن باز می‌مانند، متوقف می‌شوند. سالها است که شبکه‌کاران سخت‌افزارها را تعمیر نموده‌اند (و تصادفاً آنها را خراب کرده‌اند). بسیاری از افراد فکر می‌کنند که ما تمام مدت در مرکز دستور شبکه‌ای خود می‌نشینیم و به اعداد و شماره‌های مانیتورها زل می‌زنیم و فکر می‌کنیم. اما ما تمام چیزهایی را که در اختیار داریم رو نکرده‌ایم). هنگامی‌که مشکلی تا یکی از مؤلفه‌های سخت‌افزاری ردیابی شد، عیب‌یابی سخت‌افزاری مورد نیاز است. در این فصل، کارهایی را که باید و نباید با سخت‌افزار انجام داد توضیح داده‌ام. مبانی و اصول عناوین ذیل را مرور خواهیم کرد:

- کامپیوترهای شخصی
- بردهای الکترونیکی و سایر لوازم الکترونیکی قابل اتصال
- کابل‌ها
- منابع نظارت بر سیستم



یادداشت : *از آنجا که بسیاری از سرویس‌دهنده‌ها چیزی بیشتر از PCهای تقویت‌شده با دیسک‌گردان‌های بهتر و قوی‌تر نیستند، بسیاری از تکنیک‌های سخت‌افزاری فراهم‌آمده در این قسمت، در مورد سرویس‌دهنده‌ها نیز صدق می‌کند.*

چیزهایی که باید در مورد PC بدانید

PC کاربران اغلب اوقات متهم اصلی مشکل شبکه‌ای می‌باشد. با این‌که PC تنها مجموعه‌ای از بردهای مداری قابل اتصال و تراشه‌های روی آنها می‌باشد و می‌توان آن را از این دیدگاه مورد عیب‌یابی قرار داد، هنگام مواجه‌شدن با آن باید پیکربندی

نرم‌افزاری سطح پایین آن را نیز مورد بررسی قرار داد. سطح پایین‌ترین نرم‌افزار PC، BIOS (سیستم ورودی / خروجی پایه) آن است، که مسئول ایجاد امکان صحبت بردها و تراشه‌های به‌کار رفته در داخل کامپیوتر می‌باشد.

BIOS

می‌توان با فشردن کلیدهای Del، F1 یا F2 بلافاصله بعد از روشن‌کردن دستگاه وارد BIOS شوید (Ctrl+Alt+Esc قبلاً پرطرفدار بود، اما اخیراً به‌ندرت مورد استفاده قرار می‌گیرد). صفحهٔ تنظیم BIOS می‌تواند پیچیده یا نسبتاً ساده باشد. اغلب کامپیوترهایی با مارک مشخص دارای بایاس ساده‌تری نسبت به BIOS های عمومی می‌باشند، چرا که چنین تولیدکنندگانی استانداردسازی‌های بیشتری را در مورد مؤلفه‌هایی که به بردهای اصلی‌شان متصل می‌شوند، رعایت می‌نمایند. اغلب، صفحهٔ BIOS از نوع متنی است و فاقد کنترلهای پنجره‌ای شکل می‌باشد.

صفحهٔ تنظیم BIOS را می‌توان PC های «سالم» از همان تولیدکننده مقایسه کرد تا تنظیمات صحیح را بررسی و شناسایی نمود. اگر PC دیگری از همان نوع ندارید، می‌توانید تنظیمات را به مقادیر پیش‌گزیدهٔ اولیه بازگردانید. این‌کار در اغلب موارد مشکلی را که ایجاد شده است، حل می‌نماید.

برای مثال، تنظیمات حافظه‌ای خاصی در صفحهٔ BIOS به همراه تنظیمات نصب‌واجرا، قابل پیکربندی هستند. اگر یکی از این مقادیر به‌صورت اشتباه تغییر داده شود، سیستم شما ممکن است در عملکرد خود دچار اشکالاتی شود. این امر به‌ویژه در مورد کارتهای شبکه‌ای فاقد امکان نصب‌واجرا به چشم می‌خورد، برای مثال، اگر تعداد IRQ (درخواست وقفه) قابل استفاده توسط آنها محدود باشد، در صورتی که BIOS این IRQ ها را برای استفاده توسط ابزار نصب‌واجرا رزرو کرده باشد، کارت شبکه یا کار نخواهد کرد و یا آنکه به گونهٔ صحیحی عمل نخواهد نمود.



***هشدار** : فراموش نکنید که قبل از بازگشت‌دهی به مقادیر پیش‌گزیده، تنظیمات BIOS خود را یادداشت کنید، چرا که به برخی از این تنظیمات در آینده نیاز خواهید داشت. اغلب اوقات، بازگشت‌دهی BIOS به مقادیر پیش‌گزیده به چیزی آسیب نمی‌رساند، اما نباید احتیاط را از دست داد. برخی از PC ها گزینه‌ای برای چاپ تنظیمات BIOS روی چاپگر محلی را در اختیار می‌گذارند ـ اگر دستگاه شما چنین امکانی دارد، از آن استفاده نمایید. چاپ تنظیمات، نوشته‌شدن تمام آنها را تضمین می‌نماید.*

PC های نشاندار در مقابل PC های عمومی

مؤلفه‌ها و قطعات بیشتر PC ها تقریباً ثابت می‌باشند:

- همگی دارای یک برد اصلی هستند.
- همهٔ PC ها در یک جعبه قرار گرفته‌اند که دارای یک منبع تغذیه برای اجرای تمامی عملیات استفاده می‌شود.
- تمامی بردهای اصلی میزبان حافظه، CPU، مجموعهٔ تراشه‌ای و شکافهای توسعه برای بردهای جانبی می‌باشند.
- تمامی بردهای اصلی از یک BIOS برای ارتباط مؤلفه‌های خود با یکدیگر استفاده می‌نمایند.

عامل متفاوت بین PC ها به طرح فیزیکی مؤلفه‌ها بستگی دارد. تجربهٔ من نشان می‌دهد که کامپیوترهای عمومی ارزان‌قیمت در مقابل با ماشینهای نشاندار، از طرح ضعیف‌تری برخوردارند که می‌توانند به‌صورت عاملی در برخی از موقعیتهای عیب‌یابی مورد توجه قرار گیرد. برای مثال تصور کنید، دستگاهی را عیب‌یابی می‌کنید که بلوک اتصال‌ساز آن

در تماس با کار با یکی از کارتهای توسعه قرار می‌گیرد (اتصال ساز[1]) مکانیزمی با قابلیت نصب و برداشت می‌باشد که دو پین روی برد اصلی را به یکدیگر متصل می‌کند؛ بلوک اتصال ساز مجموعه‌ای از این پین‌ها است که معمولاً نوعی خاص از پیکربندی برد اصلی را کنترل می‌کنند). گاهی این اتفاق می‌افتد که اتصال با فلز کارت توسعه باعث تنظیم‌شدن یکی از اتصال‌سازها می‌گردد و ماجرا آغاز می‌شود.



یادداشت : *PCهای عمومی آنطور که ماشینهای نشاندار در شبکه‌ها مورد ارزیابی قرار می‌گیرند، تحت بررسی‌های سازگاری قرار داده نمی‌شوند که این خود می‌تواند ماجرا را جالب‌تر کند. سطر آخر این‌که:*

صرف چند دلار بیشتر در تهیه ماشینی نشاندار می‌تواند از بروز مشکلات زیادی جلوگیری کند. البته خرید چنین دستگاهی همیشه به معنای کارکرد صحیح در صددرصد مواقع نیست و ممکن است هنوز به اشکالات شبکه‌ای برخورد کنید البته، مهم است که در یک محیط شبکه‌ای با تعداد زیادی PC قادر باشیم که هنگامی‌که چیزها آنطور که قول داده شده کار نمی‌کنند دستاویزی برای حل مشکلات داشته باشیم ـ که این‌کار اغلب در هنگام خرید از بازارهای عمومی غیر قابل انجام است.

نصب و دعا

البته هر PC مؤلفه‌های قابل نصبی را به شکل کارتهای توسعه در اختیار خواهد گرفت (مودم‌ها، کارتهای شبکه، کارتهای تصویری و نظایر آنها). این کارتها ریزتراشه‌های قابل نصبی هستند که اغلب به دو ردیف ۸ و ۱۶ پینی مجهز می‌باشند که در سوکت هم‌اندازه‌ای جای می‌گیرد. هر یک از این انواع از مؤلفه‌ها مستعد حرکت فیزیکی بنابر انبساط و انقباض فلز که در طی گرم‌شدن و سردشدن رخ می‌دهند، می‌باشند. از آن گذشته اتصالاتی که از طلا ساخته نشده باشند استعداد اکسیده‌شدن را دارند، به همان صورت که آهن زنگ می‌زند.

هر مؤلفهٔ قابل نصبی (حتی یک کابل) مستعد دچارشدن به این مشکل می‌باشد. خوشبختانه دو راه حل ساده وجود دارد. بسیاری اوقات، فشاردادن تراشه‌ها یا بردها می‌تواند یک مشکل غیر قابل اطمینان یا تناوبی را حل کند. در غیر این‌صورت همیشه درآوردن آن قطعه و بازگرداندن آن به جای اولیه خود راه‌گشا خواهد بود. اغلب موارد این‌کار در مورد تراشه‌ها لازم نیست و فشردن آنها در جای خود کافی خواهد بود.



هشدار : *اگر می‌خواهید تراشه‌ای را از جای خود خارج کنید، هنگام بیرون کشیدن آن بسیار مواظب باشید. در غیر این‌صورت ممکن است با خم‌کردن پایه‌های کوچک، آن را خراب نمایید. همچنین مواظب باشید که پایه‌های زیر تراشه پیچ نخورند. بهتر است هنگام نصب تراشه دقت کنید که هر پین به طرز درستی در مقابل سوراخ سوکت خود قرار گرفته است.*

این مشکل در CPUهای مدرن با توجه به طرح ZIF (نیروی درج صفر) آنها به‌صورت ذکر شده وجود ندارد چرا که لازم نیست هیچ نیرویی را روی تراشه وارد آورید. بهتر است دقت کنید که اهرم سمت نزدیک CPU قبل از نصب روی تراشه بالا باشد ـ این حالت اتصال با CPU را آزاد می‌سازد.

1- Jumper

بنابراین اگر PC شما به‌طور کامل از دست رفته می‌نماید، می‌توانید به راحتی و بدون نگرانی از آسیب‌دیدن چیزی، CPU خود را بازنشانی کنید.



هشدار : *در صورت کار با قطعات الکترونیکی هنگامی‌که روشن هستند، ممکن است خسارتهای جدی به آنها وارد کنید. قبل از کار حتماً باید تغذیه چنین قطعاتی قطع شده باشد.*

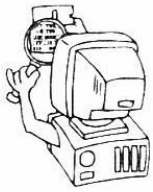
کارتهای رابطی که به برد اصلی متصل می‌شوند، تا این حد شکننده نیستند. می‌توانید آنها را بیرون آورده و دوباره جا بزنید؛ این‌کار برخی اوقات اتصال ناقصی را درست می‌کند و یا آلودگی‌ها را از پین‌ها می‌زداید.



هشدار : *قطعات الکترونیکی به کوچکترین مقادیر الکتریسیته ساکن حساسیت بسیار بالا یی دارند. باید قبل از لمس هر قطعه‌ای خود را «زمین» کنید با لمس هر فلز متصل به زمین، می‌توانید الکتریسیتهٔ ساکن جمع‌شده در بدن خود را که در اثر راه رفتن به وجود می‌آید، تخلیه نمایید. اغلب کامپیوترها دارای یک خروجی سه‌شاخه‌ای هستند که یک زمین را نیز شامل می‌شوند. اگر کامپیوتر به برق متصل باشد (اما خاموش باشد) هنگام کار با آن می‌توانید خود را با لمس شاسی فلزی درونی دستگاه زمین کنید.*

تمیزسازی

تمیزکردن قطعه یا دستگاه می‌تواند مشکلات سخت‌افزاری عجیب را حل کند. گردوغبار ممکن است به صورت کاملاً جدی در عملکرد و /یا قابل اطمینان یک مؤلفه مؤثر باشد. اگر آنقدر خوش‌شانس نیستید که در مرکز اطلاعاتی کنترل‌شده‌ای کار کنید، گردوخاک یکی از دشمنان شما محسوب می‌گردند.



نکته : *بعضی اوقات می‌توان نتایج خوبی را از طریق به‌کارگیری جاروبرقی برای تمیزکردن گردوخاک درون جعبه‌های ماشین‌ها حاصل نمود. از طرف دیگر، جاروبرقی‌های قوی ممکن است اتصال‌سازهایی را که مستحکم نصب نشده‌اند را به درون خود بکشد، بنابراین دقت کنید. همچنین خلأ حاصل توسط استفاده از جاروبرقی ممکن است الکتریسیتهٔ ساکن ایجاد کند و تمامی روز شما را خراب نماید.*

با این‌که خرید دستگاه هوای فشرده گران‌قیمت‌تر از استفاده از جاروبرقی‌های موجود می‌باشد، استفاده از چنین دستگاهی به‌خاطر قابلیت حمل آن و دقت بیشتر در هدف‌گیری محل مورد نظر، نتایج بهتری را به دست خواهد داد. البته در این حالت نمی‌توانید از دست گردوخاک راحت شوید؛ تنها آن را جابه‌جا می‌کنید.

بعضی افراد که کارهای الکترونیکی انجام می‌دهند ترجیح می‌دهند که از اسپری تمیزکنندهٔ الکترونیکی استفاده کنند. من علاقه‌ای به استفاده از چنین ابزاری روی مؤلفه‌های کامپیوتری یا شبکه‌ای ندارم ـ ممکن است نازک طبع باشم اما حقیقت آن است که استفاده از چنین ابزاری سوراخ لایهٔ ازون را بزرگتر می‌کند و برخی اوقات احساس می‌کنم که بهتر است کلاً از این نوع مواد استفاده نشود. بیشتر اوقات روشهای ذکرشده به‌خوبی کار می‌کنند.



نکته : *می‌توانید از مداد پاک‌کن نرم برای زدودن زنگ روی اتصالات کارتهای واسط خود استفاده نمایید.*

جلسهٔ تعویض

ممکن است برایتان جالب باشد که برخی اوقات یک تعویض سخت‌افزاری ساده چه مشکلاتی را می‌تواند حل نماید. به‌عنوان مثال کاملی از عیب‌یابی جعبهٔ سیاه، بیشترین کار تعمیرات سخت‌افزار از طریق تعویض بردهای مداری و سایر مؤلفه‌های مجزا و جداگانه صورت می‌گیرد مدتها است که روزهای تکنسین‌های خسته‌ناپذیر که خازن یا ریزتراشه‌ای را روی برد شکسته‌ای تعویض می‌نمودند، سپری شده است. امروزه بیشترین کار تعمیرات، به‌خاطر صرفه‌جویی در زمان، از طریق تعویض مؤلفهٔ مشکوک با معادل جدید آن صورت می‌گیرد.



یادداشت : *همیشه فکر می‌کردم چرا به‌جای تعمیر قطعات آنها را عوض می‌کنند ـ تا این‌که متوجه قیمت‌ها و هزینه‌ها شدم. قیمت‌های تعمیر از ۶۵ دلار تا ۱۵۰ دلار متفاوت است که این در مقایسه با قیمت تراشه‌های الکترونیکی (از ۱۰ تا ۵۰ دلار) این واقعیت را آشکار می‌سازد که تعویض مؤلفه از تعمیر آن ارزانتر تمام می‌شود. چرا باید یکصد دلار را صرف تعمیر کارت اِترنِت ۴۰ دلاری خود بکنید؟ می‌توانید به جای چنین تعمیری دو کارت نو ابتیاع کنید. این‌کار صلح سبز را خوشحال نمی‌کند اما مسلماً از لحاظ اقتصادی به صرفه است.*

این کاری است که حتی خودتان می‌توانید برخی اوقات انجام دهید. برای مثال تصور کنید مشکل برنامهٔ کاربردی شبکه‌ای در یک ایستگاه‌کاری به‌خصوص را ردیابی کرده‌اید و فایل‌های شبکه‌ای و اطلاعات ورود به سیستم کاربر را از مظن اتهام کنار گذارده‌اید.

سرویس‌گیرندهٔ Microsoft Exchange برای این کاربر در ایستگاه‌کاری وی کار نمی‌کند و خطای fatal exception رخ می‌دهد. وی از روی ایستگاههای کاری دیگر مشکلی ندارد.

بنابراین متوجه می‌شوید که این مشکل مربوط به سخت‌افزار است و می‌خواهید بدانید که مشکل به کدام قسمت مربوط می‌شود.

این حالت کاندیدای خوبی برای تعویض مؤلفه‌ها به‌شمار می‌رود. برخی اوقات ممکن است تعویض اولین قطعه مشخص و آشکار باشد ـ برای مثال، اگر برنامهٔ word به گونهٔ نامناسبی صفحه را ترسیم می‌کند، به احتمال زیاد در وهلهٔ اول بهتر است کارت تصویر را عوض کنید. در این مثال گفتن این‌که چه چیزی باعث بروز خطا می‌شود، امری دشوار است. این‌گونه مشکلات را ممکن است مؤلفه‌های خراب در سیستم عامل، برنامه‌های کاربردی محلی، گردونه‌های دیسک سخت خراب، راه‌اندازها یا کارتهای تصویری خراب و نظایر آنها ایجاد نمایند.

با مورد توجه قراردادن ابقاء مشکل در سیستم، اقلام زیر را تعویض کنید:

- گردونهٔ دیسک سخت با گردونهٔ دیگری که از PC مشابهی برداشته شده است.
- کارت تصویر
- DIMM های ROM
- کارت شبکه

با تعویض حافظه، خطا برطرف می‌شود. هنگامیکه این حافظه را در یک PC سالم نصب می‌کنید، مشکل مشابهی هنگام استفاده از برنامهٔ کاربردی شبکه بروز می‌کند. مهم نیست که حافظه چگونه خراب شده ـ این‌که آیا مدار خرابی در آن وجود دارد و یا آنکه با این نوع از PC/برد اصلی سازگاری ندارد، از اهمیت برخوردار نیست. مسئلهٔ مهم آن است که این حافظه از لحاظ سیستم ما خراب محسوب می‌گردد.

SIMM ها و DIMM ها

امروزه دو نوع حافظهٔ پرکاربرد وجود دارد:

- SIMM ها (ماجول‌های حافظهٔ تکی درون‌خطی)
- DIMM ها (ماجول‌های حافظهٔ دوگانهٔ درون‌خطی)

DIMM در هر دو سوی خود دارای اتصالاتی است و بنابراین از تراکم پایه‌ای بیشتر (۱۶۸ پین) و حجم اطلاعاتی بیشتر برخوردار است. با وجود آنکه SIMM در یک‌طرف دارای اتصال است، از آنجا که هر طرف به یک نقطه در برد منتهی می‌شود در واقع شصت اتصال در یک SIMM سی‌پایه‌ای و ۱۴۴ اتصال در یک SIMM ۷۲ پینی وجود دارد. اغلب اوقات SIMM ها کندتر از DIMM ها هستند.

برای برداشتن SIMM از روی برد اصلی گیره‌های فلزی نگه‌دارندهٔ آن را به طرف خارج بکشید. این کار باعث می‌شود که تراشه از حالت قرارگیری در زاویهٔ ۹۰ درجه روی برد در وضعیت ۴۵ درجه‌ای قرار گیرد. در این حال می‌توانید SIMM را بردارید. برای نصب SIMM دیگر، عکس روال را به انجام برسانید: آن را در یک وضعیت ۴۵ درجه‌ای قرار دهید و بعد از جا گرفتن در محل خود، روی تراشه فشار وارد کنید تا در حالت زاویهٔ ۹۰ درجه قرار گیرد در صورت جارفتن صحیح در سوراخهای تعبیه‌شده برای SIMM، باید جاافتادن آن را احساس کنید (اگر انجام این‌کار به سادگی ممکن نیست این امکان وجود دارد که آن را برعکس جا گذاشته باشید.

کار با DIMM آسان‌تر است: به‌صورت همزمان اهرم‌های پلاستیکی موجود در طرفین DIMM را به سمت برد اصلی فشار دهید. DIMM بیرون می‌پرد و می‌توانید آن را بردارید. به‌منظور نصب DIMM، کافی است آن را به درستی در محل خود قرار دهید ـ تعداد پین‌های به کار رفته در هر طرف آن متفاوت است ـ و آنگاه محکم تراشه را فشار دهید اهرم‌های پلاستیکی در جای خود قرار خواهند گرفت.

بسته به نوع حافظه‌ای که ماشین شما دارا است ممکن است لازم باشد حافظه‌ها را به‌صورت زوج یا چهارتایی تعویض کنید ـ این همان چیزی است که کتابچهٔ راهنمای برد اصلی با نام «ردیف حافظه» می‌شناسد. بهترین کار تعویض کل ردیف حافظه با ردیفی دیگر می‌باشد ـ که در آن لازم نیست در مورد تعداد زوج‌های لازم چیزی بدانید، حتی با این‌که برخی از کامپیوترها به هر تراشهٔ SIMM یا DIMM یک ردیف اطلاق می‌کنند.

همچنین به‌صورت مکرر درخواهید یافت که مشکلات برنامه‌های کاربردی شبکه‌ای به مشکلات قطعات ربط دارند؛ صرف نیم ساعت برای تعویض قطعات شما را از دردسر مواجه‌شدن با تکنسین‌های تعمیراتی مصون می‌دارد. به بیان دیگر مشکلات تناوبی در شبکه ممکن است هنگامی‌که تکنسینی خارج از سازمان بررسی‌های خود روی دستگاهی که شما تشخیص داده‌اید مشکل‌زا می‌باشد، صورت می‌دهد؛ ظاهر نگردند. اگر بتوانید محل مشکل را تعیین کنید، در درازمدت صرفه‌جویی زیادی در زمان خواهید نمود.

کابل همان شبکه است

دو نوع کابل شبکه به‌صورت گسترده مورد استفاده قرار می‌گیرد:

- UTP (زوج به هم تافتهٔ بدون محافظ)
- STP (زوج به‌هم تافتهٔ محافظ‌دار)

از این دو، UTP کاربرد بیشتری دارد. STP حساسیت کمتری به تداخل الکترومغناطیسی داشته اما نسبت به UDP گران‌تر و کار با آن سخت‌تر است. STP تنها در شبکه‌های حلقه نشانه مورد استفاده قرار می‌گیرد. کار با STP به این خاطر مشکل‌تر است که بسیار ضخیم می‌باشد و قابلیت انعطاف ندارد. همچنین روال خم‌کردن کابل شامل گره‌نکردن پوشش بیرونی پیدانکردن چهار سیم درونی، خم‌کردن مجزای هر سیم و آنگاه سرهم‌سازی یک اتصال DB-9 (نظیر اتصال ماوس سریال) می‌باشد. این‌کار در مقایسه با کابل‌کشی UTP که در آن سیم خارجی را برهنه کرده و تمامی سیم‌ها را در یک جک مشابه تلفن (RJ-45) قرار داده و آنگاه عمل سیم‌کشی را صورت می‌دهید، بسیار پیچیده‌تر است .

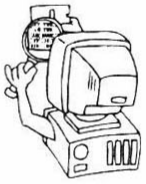


***یادداشت** : چرا از STP تنها در حلقه‌نشانه استفاده می‌شود؟ خوب، در واقع، کابل محافظ‌دار در ابتدا برای اِترنِت نیز مورد استفاده قرار می‌گرفت اما از آنجا که کار با آن مشکل است دیگر کسی آن را به‌کار نمی‌گیرد (فصل ۹ اطلاعات بیشتری در مورد اِترنِت در اختیارتان می‌گذارد).*

UTP که در دسته‌های CAT-III و CAT-V دسته‌بندی شده است، برای اِترنِت 10Mb (مگابیت) و 100Mb مورد استفاده قرار می‌گیرد. دسته‌های سیم‌کشی، روش استاندارد صنعتی اشاره به مشخصات تولیدی کابل به شمار می‌روند: ضخامت (مقیاس یا درجه) کابل، تعداد پیچش‌های سیم در هر فوت و مقاومت الکترونیکی سیم. CAT-III و CAT-V را می‌توان برای حلقه‌نشانه نیز به کار برد (فصل ۱۰ اطلاعات بیشتری در مورد کابل‌های حلقه ـ نشانه را در اختیارتان می‌گذارد). برخی اوقات، مشکلی را تا یک کابل ردیابی می‌کنیم. برای مثال، اگر کاربر نمی‌تواند به شبکه متصل شود و شما برنامهٔ تجزیه و تحلیل فراهم‌آمده توسط فروشندهٔ کارت شبکه را اجرا کنید و دریابید که کارت شبکه سالم است، متهم بعدی کابل خواهد بود. تعویض کابل کاری آسان است و اهمیتی ندارد که از کابل محافظ‌دار یا بدون محافظ استفاده کنید. بنابراین اگر کابل را با کابل سالمی عوض کنید و این‌کار باعث شود ایستگاه‌کاری به شبکه بازگردد، آنچه در دست دارید کابلی خراب است در چنین حالتی می‌توانید به سادگی کابل را دور انداخته و کابل دیگری ابتیاع کنید.



***نکته** : فقط در صورتی‌که قادر هستید کابل‌های خیلی خیلی خوب بسازید، می‌توانید از خرید کابل‌های آماده صرفنظر کنید. کابل‌های خوب هستند که شبکه خوب را می‌سازند.*



***نکته** : هنگام عیب‌یابی سیم‌های UTP، بهتر است بررسی کنید که UTP مورد نظر نزدیک موتور یا لامپ‌های فلوروسنت قرار نگرفته باشد، زیرا EMI (تداخل الکترومغناطیسی) می‌تواند مشکلاتی بسیار عجیب را باری شبکه ایجاد کند. از آنجا که کارکردن با UTP بسیار آسان است، بسیاری از افراد از کابل‌های خود استفاده می‌کنند (قطعه‌قطعه‌کردن کابل خم‌کردن و اتصال آن کاری آسان است). البته بسیاری اوقات، افراد از وجود تأثیر EMI نیز آگاه نیستند هنگام ردیابی مشکلات این‌گونه تأثیرات را مد نظر داشته باشید.*

استفاده از مولتی‌متر

از آنجا که استفاده از نیروهای خارجی برای انجام هر کاری گران تمام می‌شود، ممکن است بخواهید خود به بررسی خرابی یک کابل همت گمارید (یعنی آنکه مطمئن شوید مشکل پیش رو از کابل به وجود آمده و نه منبع دیگر نظیر EMI یا مؤلفه‌ای خراب) در چنین حالاتی، می‌توانید آزمون اتصال را با استفاده از یک مولتی‌متر ابزاری که ولتاژ الکتریکی، مقاومت و امپدانس را اندازه‌گیری می‌کنند، صورت دهید (یعنی این‌که می‌توانید چک کنید که آیا جریانی که از یک سوی کابل حرکت می‌کند به سوی دیگر می‌رسد یا خیر). خرید مولتی‌متر هزینهٔ چندانی در بر ندارد و از هر مغازهٔ لوازم الکترونیکی قابل خرید است.

مولتی‌متر می‌تواند به شما بگوید که آیا هر کابل باز (خراب) یا بسته (سالم) می‌باشد. بعد از روشن‌کردن تست اتصال مولتی‌متر می‌توانید نحوهٔ کار آن را با اتصال میله‌های ارزیابی آن ملاحظه نمایید. صدایی به گوش خواهد رسید. این صدا نشاندهندهٔ آن است که یک مسیر الکتریکی پیوسته بین دو میله وجود دارد.

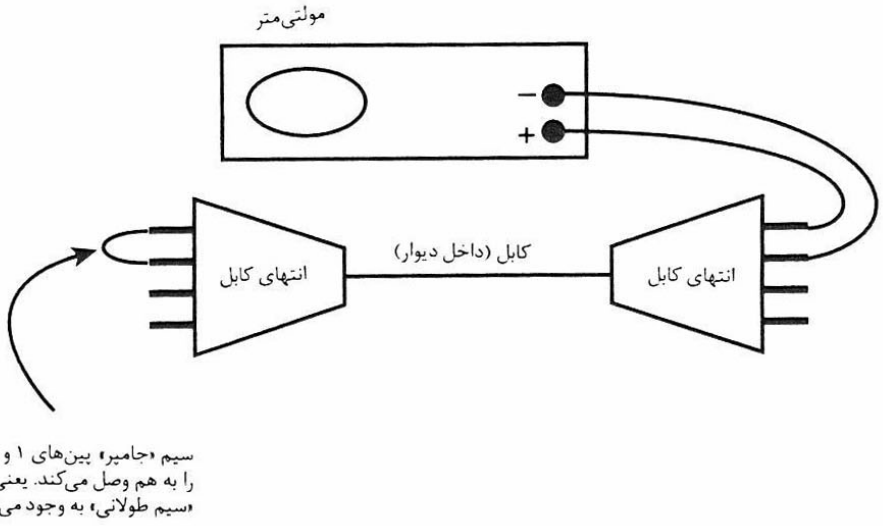
اگر دو انتهای کابل را در دستتان بگیرید می‌توانید تک تک پین‌های کابل را در دو سوی آن به یکدیگر وصل نمایید (بیشتر کابل‌های اِترنِت اتصال مستقیم دارند ـ یعنی ارتباط یک به یک بین پایه‌ها وجود دارد؛ این حالت در کابل‌های حلقه‌نشانه نیز صادق است). با انجام این‌کار باید صدایی به گوش برسد. اگر صدایی نمی‌شنوید یکی از میله‌ها را از پایه‌ای به پایهٔ دیگر حرکت دهید اگر هنوز صدایی به گوش نمی‌رسد کابل خراب است.



نکته : ***در صورتی‌که صدا از بیش از یک پایه به گوش برسد هم، اشکال وجود دارد. این نشاندهندهٔ آن است که جایی در کابل دو سیم به یکدیگر متصل شده‌اند.***

بازگشت حلقه

اگر دو انتهای کابل را نتوانید در دستانتان بگیرید، چه کار می‌توانید بکنید؟ لازم است که هر دو میله را به کابل متصل کنید. پاسخ آن است که باید دو پین را به یکدیگر متصل کرده تا یک سیم طولانی ایجاد شود (شکل ۱-۸ را ملاحظه کنید). آنگاه میله‌ها را به دو سر سیم طولانی (هردو سوی سیم طولانی در یک‌طرف کابل قرار خواهند گرفت، همان طور که در شکل مشهود است) متصل نمایید.



شکل ۱-۸ : آزمون اتصال در مورد کابلی که از میان یک دیوار می‌گذرد.

این کار بازگشت حلقه نام دارد. چرا که حلقه‌ای را در یک انتهای کابل ایجاد می‌نماییم. بازگشت حلقه تکنیک بررسی قدرتمندی است که می‌تواند در مورد سخت‌افزارهای خراب نیز اظهار نظر کند. هنگامی که در موقعیتی هستید که نمی‌توانید کارت شبکه را تعویض کنید (تصور کنید که تنها یک کارت شبکه با سرعت بالا در سرویس‌دهنده خود دارید)، به احتمال زیاد ترجیح می‌دهید برنامهٔ تجزیه و تحلیل‌گری که با کارت شبکه ارائه شده است را مورد استفاده قرار دهید. این برنامه از شما می‌خواهد که یک اتصال بازگشت حلقه ایجاد کنید ـ که باعث می‌شود کارت شبکه با خودش صحبت کند (پین‌های ارسالی مستقیماً به پین‌های دریافتی متصل می‌شوند).



***یادداشت :** اِترنِت از اتصال RJ-45 استفاده می‌کند که در آن تنها چهار پایه از هشت پایه مورد استفاده قرار گرفته‌اند. برخی از کارت‌های حلقه - نشانه از اتصال DB-9 استفاده می‌کنند که در اینجا هم چهار پایه از ۹ پایهٔ موجود استفاده می‌گردد. برخی هم از هریک از روشهای فوق می‌توانند استفاده کنند.*



***نکته :** اگر کارت شبکه بعد از بررسی حلقهٔ بازگشتی سالم به نظر می‌رسد، می‌توانید مشکلات کابلی را از طریق اتصال بازگشت حلقه از سوی خط کنار بگذارید. برای مثال می‌توانید کابل ایستگاه کاری که به صورت نرمال به دیوار متصل می‌شود را بین کارت شبکه و اتصال بازگشت حلقه قرار دهید. ممکن است لازم باشد برای انجام این کار از تغییردهندهٔ اتصال (که بسیار نظیر کوپلر تلفن برای اتصال RJ-45 می‌باشد)، استفاده نمایید. بازگشت حلقه به کوپلر متصل می‌گردد، کوپلر به کابل شبکه و کابل شبکه به کارت شبکه وصل می‌شوند و آنگاه آزمون بررسی دوباره صورت می‌گیرد.*

اگر همه چیز مرتب باشد، این امکان وجود دارد که اتصال بازگشت حلقه به انتهای کابل متصل می‌شود که این اتصال اغلب به هاب صورت می‌گیرد. در این حال می‌توان مجدداً آزمون را انجام داد. این کار باعث می‌شود که بتوانیم کل کابل را به عنوان منبعی عاری از مشکلات ارسال یا دریافت کنار بگذاریم.

اتمام سوخت در بزرگراه اطلاعات

به پایان‌رسیدن منابع سیستم معادل آن است که سیستم‌عامل با مشکل مواجه شده و شما را از عملکرد صحیح بازدارد. دانستن چگونگی کنارگذاشتن (یا به‌حساب‌آوردن) یک مشکل مربوط به منابع می‌تواند شما را به راه حل نزدیک سازد.

با اینکه تمام‌شدن فضای دیسکی امری آشکار و واضح می‌نماید، بررسی مقدار فضای آزاد باقیمانده ایدهٔ خوبی خواهد بود. به خاطر داشته باشید که ویندوز فضای لازم برای «تعویض» را به صورت پویا درنظر می‌گیرد؛ بنابراین، اگر واقعاً از لحاظ فضای دیسکی در مضیقه هستید، عمل تعویض ممکن است مشکل‌زا باشد.

می‌توانید به فضای تعویض به عنوان ناحیه سرریز RAM کامپیوتر خود نگاه کنید ـ هنگامی که تعداد برنامه‌ها زیاد باشد و در فضای RAM نتوانند جای بگیرند، ناحیهٔ سرریزی مورد استفاده قرار می‌گیرد (این ناحیه فایل مخصوصی در گردنه دیسک سخت است که ناحیهٔ تعویض نامیده می‌شود). هنگام وقوع سرریزی،

سیستم‌عامل نواحی کم‌استفادهٔ RAM را روی دیسک سخت کپی می‌کند. و اگر ناحیهٔ سرریزی وجود نداشته باشد ... خوب، خودتان حدس بزنید.

از آنجا که عمل تعویض سرعت ماشین را کم می‌کند ممکن است که ساده‌سازی ناحیهٔ رومیزی را مدنظر قرار دهید که در مقدار زیادی RAM صرفه‌جویی می‌کند. بسیاری از کاربران می‌توانند با کنارگذاشتن کاغذدیواری‌های پیچیده، محافظ‌های صفحه‌نمایش، و Active Desktop مقداری از وزن رومیز خود را کاهش دهد. اگر از روی میز خود در وضعیت فعلی آن راضی هستید، بهتر است مقداری RAM فیزیکی بیشتر خریداری نمایید و ملاحظه کنید که چقدر کارها سریعتر صورت می‌پذیرد.

ویندوز

می‌توانید منابع ویندوز 9x را با استفاده از System Resource Meter بررسی نمایید و محدودیت‌های سخت‌افزاری را با استفاده از System Monitor ارزیابی کنید. هردوی این برنامه‌ها را می‌توان از طریق Control Panel نصب نمود (شکل ۲-۸ را ملاحظه کنید). مراحل انجام این کار در زیر توضیح داده شده‌اند:

۱- گزینهٔ Start|Settings|Control Panel را انتخاب کنید.

۲- از پنجرهٔ Control Panel، Add/Remove Programs را انتخاب نمایید.

۳- برگهٔ Windows Setup را انتخاب کنید.

۴- گزینهٔ Accessories را انتخاب نمایید (در صورت استفاده از ویندوز ۹۸، روی System Tools کلیک کنید).

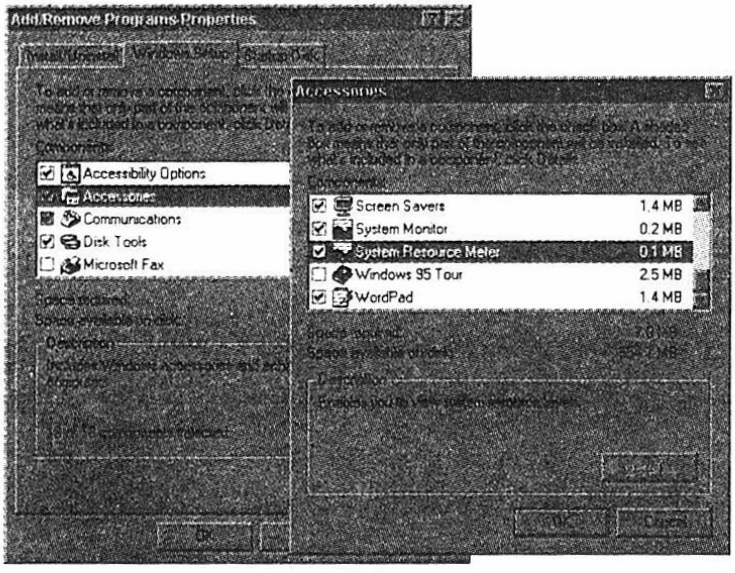
۵- روی Details کلیک کنید.

۶- روی گزینه‌های System Monitor و System Resource Meter کلیک نمایید.

۷- روی OK کلیک کنید.

۸- CD-ROM ویندوز را هنگامی که خواسته می‌شود درون دستگاه قرار دهید (بعضی از سیستم‌ها، فایل‌های تنظیم ویندوز را در دیسک‌گردان خود دارند و بنابراین ممکن است این مرحله لازم نباشد صورت پذیرد).

۹- این ابزار را با استفاده از منوی Accessories|System Tools اجرا نمایید (نیازی به راه‌اندازی مجدد نیست).



شکل ۲-۸ : اضافه‌کردن System Resource Meter و System Monitor به ویندوز 9x.

System Resource Meter

می‌توانید از این برنامه برای حصول اطمینان از تمام‌نشدن منابع یک ایستگاه کاری استفاده کنید. اجرای این برنامه و تلاش برای انجام آنچه با آن مشکل دارید و مشاهدهٔ تغییر گراف میله‌ای، کاری مؤثر و کارا خواهد بود. ممکن است ببینید که رنگ گراف به زردی یا سرخی می‌گراید که این نشان‌دهندهٔ کمبود منابع می‌باشد ـ ممکن است لازم باشد حافظه اضافه کنید، برنامهٔ کاربردی منبع‌گرای کمتری به‌کار ببرید، یا برنامه‌های کاربردی کمتری را به صورت همزمان اجرا نمایید. برای مثال، فرض کنید که هنگام چاپ از برنامهٔ WordPerfect با مشکل مواجه هستید ـ اتفاق وحشتناکی رخ نمی‌دهد، بجز اینکه خروجی چاپ‌شده به آن صورت که باید باشد نیست. چیزی که می‌خواهید چاپ کنید نامهٔ خبری پیچیده‌ای است که باعث می‌شود به تمام‌شدن سوخت ایستگاه کاری خود ظنین شوید. System Resource Monitor را اجرا می‌کنید و ملاحظه می‌کنید که یک شمایل جدید در کازیهٔ سیستم[1] ظاهر می‌شود. از آنجا که رنگ این شمایل سبز نیست، به شک می‌افتید که ممکن است منابع سیستم ویندوز رو به کاهش گذاشته باشد. برای بررسی آنکه ببینید این مشکل مربوط به شما می‌باشد، به این صورت عمل کنید:

۱- از تمامی برنامه‌های دیگر به غیر از Word Perfect خارج شوید.

۲- به نشانگر دقت کنید که به سبزی می‌گراید.

۳- کار چاپ را دوباره انجام دهید.

System Monitor

این برنامه می‌تواند تقریباً هر چیزی را تحت نظارت قرار دهد ـ در شکل ۳-۸ در کنار System Resource Meter به منظور نمایان‌کردن حافظهٔ آزاد و چگونگی سختی کار CPU در حال اجرا می‌باشد. System Monitor را می‌توان به منظور ایجاد خروجی گراف میله‌ای یا گراف خطی پیکربندی نمود و منابع مختلف و آماره متفاوتی را از طریق آن نمایش داد. در فصل ۱۱ برای بررسی توان عملیاتی شبکه از این برنامه استفاده خواهیم نمود.

فرض کنید که کامپیوتر شما به کُندی کار می‌کند می‌خواهید بررسی کنید که آیا با کمبود حافظه مواجه هستید یا خیر، بنابراین مراحل زیر را انجام می‌دهید:

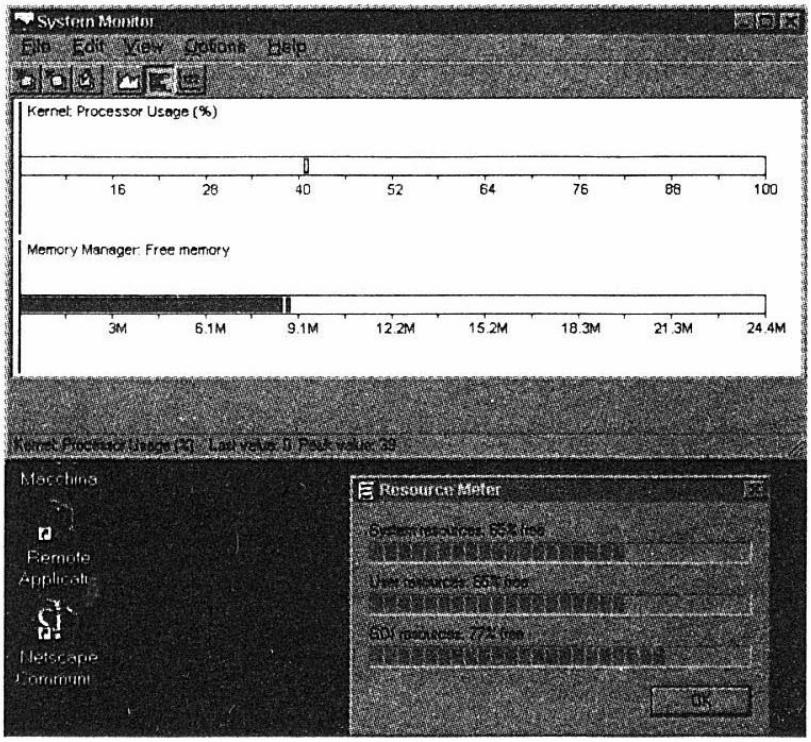
۱- برنامهٔ System Monitor را اجرا کنید.

۲- Edit|Add Item را انتخاب نموده و از دستهٔ Memory Manager، Free Memory را برگزینید (برای ردیابی حافظه فیزیکی آزاد).

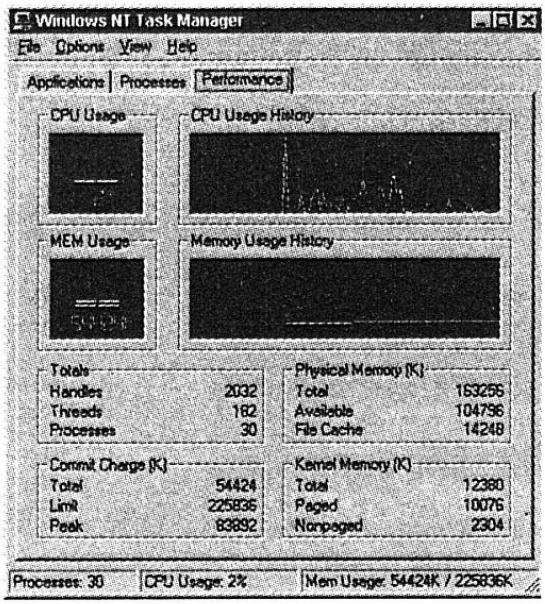
برای مثال اگر تقریباً ۹/۱ MB حافظهٔ فیزیکی آزاد داشته باشید یعنی همان طور که در شکل ۳-۸ نشان داده شده، کمبود حافظه دلیل کُندی ماشین شما نیست. این مقدار حافظه، حافظهٔ زیادی محسوب نمی‌شود ـ اما احیاناً به اندازهٔ کافی زیاد هست که عمل تعویض صورت نگیرد. اگر مقدار حداکثر (نقطهٔ موجود در سمت راست خط) بیشتر از ۰/۸ MB یا ۱ MB باشد، احیاناً با کمبود حافظه مواجه هستید که این باعث انجام تعویض‌های مکرر می‌گردد. می‌توانید این موضوع را از طریق افزودن یک میله یا گراف بررسی نمایید ـ Swapfile in Use (از دستهٔ Memory Manager) ـ و ملاحظه کنید که بزرگی آن چقدر است. اگر از دو مگابایت بیشتر باشد، صراحتاً نشان‌دهندهٔ وقوع عمل تعویض می‌باشد. در این حالت، باید ارتقاء حافظه یا کنارگذاشتن برخی از ابزارهای حافظه‌ای را مد نظر قرار دهید.

1- System Tray

یادداشت : *ویندوز NT دارای یک برنامهٔ نظارتی CPU و RAM است که در کادر تبادلی Task Manager ظاهر می‌شود (شکل ۴-۸ را ملاحظه کنید). برای بازکردن این کادر تبادلی کلید Ctrl+Alt+Delete را فشار دهید و Task Manager را انتخاب نمایید.*



شکل ۳-۸ : با استفاده از System Monitor می‌توانید میزان سختی کارکرد CPU و مقدار حافظهٔ در دسترس و همچنین سایر آمار حیاتی در مورد دستگاه را ملاحظه نمایید.



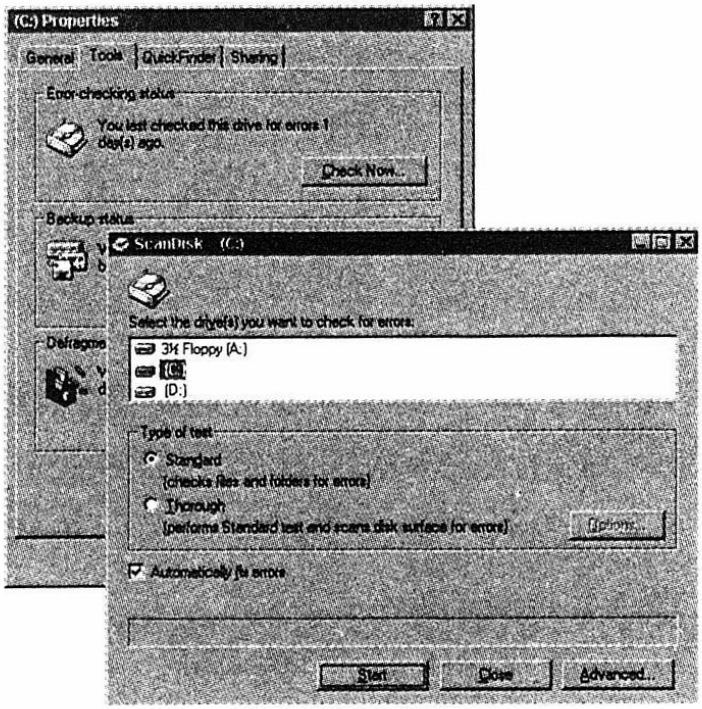
شکل ۴-۸: Performance Monitor در Task Manager ویندوز NT روش خوبی برای دریافت وضعیت ایستگاه کاری ویندوز NT می‌باشد.

ScanDisk

دیسک سخت، شکننده‌ترین منبع در سیستم می‌باشد. بد نیست که هرازچندگاهی ScanDisk را اجرا نمایید تا خطاهای

دیسک سخت را شناسایی و برطرف کنید. این موضوع به خصوص در صورت به‌کارگیری نگارش اولیه ویندوز ۹۵ صادق است ـ این نگارش، ScanDisk را به صورت خودکار بعد از خاموشی نابهنگام سیستم اجرا نمی‌کند و از این جهت با سیستم‌های جدیدتر ویندوز 9x متفاوت است! این بدان معناست که روزها و هفته‌ها ممکن است مشکلات دیسکی در اثر قطع برق و خاموشی دستگاه توسط کاربران بدون توجه باقی بمانند. این خرابیها می‌توانند جمع شده و باعث وقوع مشکلات عجیب گردند. اجرای منظم ScanDisk ـ مثلاً هر هفته ـ می‌تواند بسیار ایدهٔ خوب و مفیدی باشد. اغلب اوقات ممکن است تنها بررسی استاندارد کفایت کند اما هر ماه بهتر است که به منظور حفظ امنیت، بررسی کامل را صورت دهید.

با آنکه می‌توانید ScanDisk را از طریق منوی Programs|Accessories|System Tools اجرا نمایید، این کار از طریق راست کلیک‌کردن روی دیسک‌گردان مربوطه در Explorer و آنگاه انتخاب Properties از منوی ظاهرشده میسر خواهد بود. کادری تبادلی ظاهر می‌شود که یکی از برگه‌های آن Tools نام دارد (شکل ۵-۸). در این برگه، زمان آخرین بررسی دیسک‌گردان را ملاحظه می‌کنید. از اینجا هم می‌توانید بررسی جدیدی را صورت دهید.



شکل ۵-۸: با انجام منظم بررسی توسط ScanDisk امکان بروز مشکل کاهش می‌یابد.

کاربران غیر ویندوز

کاربر ویندوز نیستید؟ یونیکس و نِت‌ور هنگامی که ویندوز تنها برقی در چشمان بیل گیتس بود، به ابزار بررسی منابع مجهز بودند. با اینکه متدها متفاوت هستند و از ظاهری گرافیکی بهره نمی‌گیرند ـ به غیر از حالتی که از X Window یا نِت‌ور نگارش ۵ استفاده می‌کنید ـ ایدهٔ مقدماتی و اصولی یکی است: هنگام بروز مشکلات منابع را بررسی کنید و نتایج حاصله را با حالت منابع هنگامی که مشکلی ندارید مقایسه نمایید.

یونیکس

فرض کنید شما کاربر یونیکس هستید و می‌خواهید حافظهٔ موجود و ناحیهٔ تعویض خود را بررسی نمایید. کافی است تایپ کنید:

ورودی

```
moria:/$ free
```

خروجی

```
             total       used       free     shared    buffers
Mem:          7220       6948        272       2524       3356
Swap:        16416       2396      14020
```

بسیاری از کاربران یونیکس می‌توانند میزان به‌کارگیری جاری منابع را از طریق دستور VMSTAT نظیر به این مشاهده نمایید:

ورودی

```
$ vmstat 1
```

خروجی

```
procs   memory          page      faults    cpu
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
r  b    avm    fre  re   pi po fr  sr cy in   sy   cs  us sy id wa
0  0    13376  233  0    0  0  2   6  0  144  807  81  4  5  84 7
0  0    13376  233  0    0  0  0   0  0  129  757  89  2  8  89 2
0  0    13376  233  0    0  0  0   0  0  143  768  85  2  7  91 0
0  0    13376  233  0    0  0  0   0  0  140  567  1245  1  94 0
0  0    13376  233  0    0  0  0   0  0  147  387  39  1  3  96 0
```

خروجی به سنگ‌نبشته‌های یونانی می‌ماند، اگر ترجمه آن را بدانید، چندان وحشتناک نخواهد بود. در ذیل برخی از معانی علائم را ملاحظه می‌کنید.

AVM صفحات مجازی فعال (مقدار حافظهٔ فیزیکی و تعویضی)

PI میزان فعالیت صفحهٔ ورودی در هر ثانیه (مقدار سرریزی در ناحیهٔ تعویضی)

PO میزان فعالیت صفحهٔ خروجی در هر ثانیه (مقدار تحلیل سرریزی)

FRE فهرست حافظه آزاد

US میزان کاربرد CPU توسط کاربران

SY میزان کاربرد CPU توسط فرایندهای سیستمی

ID زمان بیکاری CPU

WA زمان صرف‌شده توسط CPU در حالت انتظار برای انجام فعالیت دیسک

اگر مایلید گزارشی را از این وضعیت داشته باشید، باید دستور SAR را امتحان کنید. به‌کارگیری این دستور گزارشی نظیر ذیل را به‌دست می‌دهد.

```
smp smp 4.0             2 PENTIUM 09/17/98
00:00:00  %usr          %sys       %wio          %idle
07:00:    0             0          3             97
08:00:00  0             1          4             95
08:10:00  1             2          9             87
08:20:00  2             4          11            83
08:30:00  3             5          57            35
08:40:00  2             5          23            69
08:45:00  3             6          61            30
```

توجه داشته باشید که بعد از ساعت ۸:۲۰ چگونه اوضاع به هم می‌ریزد (هنگامی که همه قهوهٔ خود را به پایان برده و می‌خواهند کار را آغاز کنند). در ساعت ۸:۳۰ تنها ۲۵ درصد منابع سیستم آزاد است که در مقایسه با ۹۷ درصد ساعت ۷ صبح مقدار بسیار اندکی است. همان طور که ملاحظه می‌کنید دستور SAR بدون نیاز به نظارت طولانی اطلاعات مفیدی را به دست می‌دهد. هم SAR و هم VMSTAT دارای صفحات راهنمایی هستند که می‌توان به صورت مستقیم از طریق تایپ دستور زیر به آنها دسترسی پیدا کرد:

man < sar یا vmstat >

نِت‌ور

در صورتی که کاربر نِت‌ور هستید، متأسفانه راه حل نظارت بر منابع برای مدت طولانی توسط ناول ارائه نشده است، البته راه حل‌های دسته سوم همیشه در دسترس هستند. می‌توانید از صفحه نظارت نِت‌ور برای بررسی منابع مختلفی استفاده کنید. کافی است تایپ کنید:

load monitor

تا صفحهٔ اولیه میزان به‌کارگیری پردازنده ظاهر شود. اطلاعات جزئی‌تر در مورد سیستم را می‌توانید با مرور زیرفهرست‌های Processor، Memory، یا Resource Utilization ملاحظه نمایید.

شاید مهمترین چیزی که بتوان آن را ردیابی نمود، تعداد بافرهای حافظه سریع است که می‌توانید آن را در منوی Resource مشاهده کنید. اگر تعداد بافرهای حافظهٔ سریع کمتر از ۴۰٪ یا در حدود آن باشد، احیاناً مشکلاتی را تجربه خواهید نمود.



یادداشت : ***حافظهٔ مجازی یا تعویضی در نت‌وِر 3.x یا 4.x وجود ندارد تا بتوان آن را بررسی نمود.***

خلاصه

آشنایی با چگونگی عیب‌یابی مشکلات مقدماتی سخت‌افزاری می‌تواند مقادیر زیادی از زمان را برای شما صرفه‌جویی نماید. PC ها هیولاهای کوچکی هستند که از مؤلفه‌های الکترونیکی قابل نصب تشکیل شده‌اند که برخی از آنها را می‌توان جابجا نمود. جعبه‌ها یا بُردهای اصلی که از طراحی ضعیفی برخوردارند می‌توانند مشکلاتی را ایجاد کنند، بنابراین با دوری از آنها از مشکلات اجتناب نمایید.

همان گونه که از کودکی فرا گرفته‌اید، پاکیزگی امر مهمی است؛ تمامی مؤلفه‌های سخت‌افزاری عکس‌العمل شدیدی نسبت به گردوخاک نشان می‌دهند. می‌توانید از جاروبرقی یا هوای فشرده برای تمیزکردن مؤلفه‌های خاک‌گرفته استفاده کنید؛ از مدادپاک‌کن برای تمیزکردن اتصالات مدارها که به نظر کثیف یا زنگ‌زده می‌آیند بهره بگیرید. تعویض مؤلفه‌ها بخش مهمی از عیب‌یابی سخت‌افزاری است. همان گونه که از طرز کار دقیق پمپ بنزین موجود در اتومبیل خود اطلاعی ندارید، تعویض یک قطعه که باعث رفع اشکال می‌شود خود می‌تواند راه‌گشای کار باشد بدون اینکه بدانیم و یا مهم باشد که بدانیم دقیقاً چه اشکالی وجود داشته است.

کابل زوج‌تافته بدون محافظ (UTP) پرکاربردترین نوع کابل شبکه می‌باشد. این نوع کابل به تداخل الکترومغناطیسی

توجه داشته باشید که بعد از ساعت ۸:۲۰ چگونه اوضاع به هم می‌ریزد (هنگامی که همه قهوهٔ خود را به پایان برده و می‌خواهند کار را آغاز کنند). در ساعت ۸:۳۰ تنها ۳۵ درصد منابع سیستم آزاد است که در مقایسه با ۹۷ درصد ساعت ۷ صبح مقدار بسیار اندکی است. همان طور که ملاحظه می‌کنید دستور SAR بدون نیاز به نظارت طولانی اطلاعات مفیدی را به دست می‌دهد. هم SAR و هم VMSTAT دارای صفحات راهنمایی هستند که می‌توان به صورت مستقیم از طریق تایپ دستور زیر به آنها دسترسی پیدا کرد:

man < sar یا vmstat >

نِت‌ور

در صورتی که کاربر نِت‌ور هستید، متأسفانه راه حل نظارت بر منابع برای مدت طولانی توسط ناول ارائه نشده است، البته راه حل‌های دسته سوم همیشه در دسترس هستند. می‌توانید از صفحه نظارت نِت‌ور برای بررسی منابع مختلفی استفاده کنید. کافی است تایپ کنید:

load monitor

تا صفحهٔ اولیه میزان به‌کارگیری پردازنده ظاهر شود. اطلاعات جزئی‌تر در مورد سیستم را می‌توانید با مرور زیرفهرست‌های Processor، Memory، یا Resource Utilization ملاحظه نمایید.

شاید مهمترین چیزی که بتوان آن را ردیابی نمود، تعداد بافرهای حافظه سریع است که می‌توانید آن را در منوی Resource مشاهده کنید. اگر تعداد بافرهای حافظهٔ سریع کمتر از ۴۰٪ یا در حدود آن باشد، احیاناً مشکلاتی را تجربه خواهید نمود.



یادداشت : ***حافظهٔ مجازی یا تعویضی در نت‌وِر 3.x یا 4.x وجود ندارد تا بتوان آن را بررسی نمود.***

خلاصه

آشنایی با چگونگی عیب‌یابی مشکلات مقدماتی سخت‌افزاری می‌تواند مقادیر زیادی از زمان را برای شما صرفه‌جویی نماید. PC ها هیولاهای کوچکی هستند که از مؤلفه‌های الکترونیکی قابل نصب تشکیل شده‌اند که برخی از آنها را می‌توان جابجا نمود. جعبه‌ها یا بُردهای اصلی که از طراحی ضعیفی برخوردارند می‌توانند مشکلاتی را ایجاد کنند، بنابراین با دوری از آنها از مشکلات اجتناب نمایید.

همان گونه که از کودکی فرا گرفته‌اید، پاکیزگی امر مهمی است؛ تمامی مؤلفه‌های سخت‌افزاری عکس‌العمل شدیدی نسبت به گردوخاک نشان می‌دهند. می‌توانید از جاروبرقی یا هوای فشرده برای تمیزکردن مؤلفه‌های خاک‌گرفته استفاده کنید؛ از مدادپاک‌کن برای تمیزکردن اتصالات مدارها که به نظر کثیف یا زنگ‌زده می‌آیند بهره بگیرید. تعویض مؤلفه‌ها بخش مهمی از عیب‌یابی سخت‌افزاری است. همان گونه که از طرز کار دقیق پمپ بنزین موجود در اتومبیل خود اطلاعی ندارید، تعویض یک قطعه که باعث رفع اشکال می‌شود خود می‌تواند راه‌گشای کار باشد بدون اینکه بدانیم و یا مهم باشد که بدانیم دقیقاً چه اشکالی وجود داشته است.

کابل زوج‌تافته بدون محافظ (UTP) پرکاربردترین نوع کابل شبکه می‌باشد. این نوع کابل به تداخل الکترومغناطیسی

خارجی (EMI) حساس است. بنابراین بهتر است به جای ساختن کابل، از کابل‌های آماده استفاده کنیم.

اگر سوخت ایستگاه کاری شما درحال تمام‌شدن است ادامهٔ کار ممکن نخواهد بود مگر آنکه به بررسی منابع سیستم خود بپردازید، که این موضوع ارتباطی با سیستم‌عامل مورد استفاده ندارد.

کارگاه

پرسش و پاسخ

پرسش : آیا لازم نیست که انجام این امور سخت‌افزاری را به یک تکنسین سخت‌افزار بسپارم؟ ممکن است چیزی را خراب کنم!

پاسخ : اگر این کارها را روی مؤلفه‌هایی که از هزاران تا میلیونها دلار ارزش دارد بخواهیم انجام دهیم، با شما موافق هستم. اگر کاملاً از این دریا دور افتاده‌اید جزئیات خوبی را می‌توانید از یکی از کتابهای عیب‌یابی سخت‌افزار برگیرید. اما اگر کار شما منجر به خرابی یک دیسک‌گردان فلاپی یا کارت تصویر شود بین ۵۰ تا ۱۰۰ دلار را از دست می‌دهید و باور کنید که دیگر آن اشتباه را تکرار نخواهید. کافی است تنها مواظب الکتریسیته ساکن باشید، قبل از آغاز کار دستگاه را خاموش کنید، قطعات را در همان جهت به جای خود بازگردانید، و مطمئن باشید که اتفاقی نخواهد افتاد.

آزمون

۱- چگونه به صفحهٔ تنظیم BIOS بیشتر کامپیوترها وارد می‌شوید؟

الف ـ کلید فاصله
ب ـ کلید بازگشت
ج ـ F5، Ctrl+Alt+Del یا Enter
د ـ F1، F2، یا Del

۲- درست یا نادرست؟ هنگامی که روی ابزاری سخت‌افزاری کار می‌کنید تغذیه باید روشن باشد.

۳- می‌توانید خودتان را با لمس‌کردن کدامیک از موارد زیر زمین کنید.

الف ـ پلاستیک جعبه PC
ب ـ پیچ پریز دیوار
ج ـ شاسی PC (در شرایطی که به برق متصل است)
د ـ گردوخاک روی دستگاه

۴- درست یا نادرست؟ حافظهٔ ناسازگار می‌تواند علت بروز برخی از مشکلات شبکه‌ای باشد.

۵- برای بررسی درستی کابل، از روش آزمون _____ استفاده می‌کنیم.

الف ـ سازگاری
ب ـ اتصال
ج ـ صنعتی
د ـ هیچ کدام

پاسخ به سؤالات آزمون

۱- د
۲- نادرست
۳- ج. شاید تعجب‌برانگیز باشد که پیچ روی پریز دیواری همیشه هم زمین نیست.
۴- درست
۵- ب

فصل ۹

مبانی اِترنِت

احتمالاً با جنگ کلاسیک بین بتاماکس و VHS آشنایی دارید که مثالی است از جنگ تکنولوژی ساده و قابل دسترس‌تر (VHS) با یک تکنولوژی گران‌قیمت‌تر و پیچیده‌تر (بتاماکس). برخی اولی را دوست دارند، برخی با دیگری انس بیشتری گرفته‌اند، اما هیچ‌کس نمی‌تواند ادعا کند که تکنولوژی ساده‌تر بر دیگری مسلط شده است.

این مقایسه اِترنِت و حلقه نشانه نیز صادق است که در این بین اِترنِت بسیار ساده‌تر و محبوب‌تر است. اما برخی حلقه نشانه را دوست دارند، برخی نیز اِترنِت را ترجیح می‌دهند. اگر شما حلقه نشانه را مورد استفاده قرار می‌دهید، بد نیست به خواندن ادامه دهید ـ دانستن در مورد تفاوت‌ها می‌تواند مفید واقع شود.

همانگونه که قبلاً ذکر کرده‌ام، حقیقت وجودی بیشتر شبکه‌ها، خطوط دسته‌جمعی است ـ یعنی خطوطی که بیش از یک کارت شبکه در آن قرار گرفته و به صحبت با بقیه می‌پردازد ـ یک تفاوت آشکار بین انواع مختلف شبکه، روشی است که آنها در خط مورد نظر با هم مشترک می‌شوند. به عبارت دیگر، این سؤال مطرح می‌شود که آیا این خط برای همه آزاد است، یا قوانینی را باید مد نظر داشت؟



نکته : *اصل خط دسته‌جمعی برای تمام شبکه‌های اِترنِت صدق نمی‌کند. شبکهٔ اِترنِت سوئیچی کامل ـ که در آن یک ایستگاه‌کاری روی هر پورت سوئیچ قرار گرفته است ـ در واقع از تعداد زیادی شبکهٔ دونفره تشکیل شده است.*

به شبکه‌ای که از دو عضو تشکیل شده باشد، شبکهٔ نقطه‌به‌نقطه گفته می‌شود، بسیار شبیه اتصال کامپیوتر شما به فراهم‌کنندهٔ سرویس اینترنت.

با این‌که بیشتر افراد از شبکهٔ نقطه‌به‌نقطه تنها هنگام صحبت در مورد خطوط تلفنی و استیجاری صحبت می‌کنند، شبکهٔ نقطه‌به‌نقطه شبکه‌ای است که دو ایستگاه در یک بخش از شبکه با همدیگر تشکیل می‌دهند. با معرفی یک سوئیچ در این دیدگاه، در واقع دو ایستگاه داریم که در یک خط مشترک (پورت سوئیچ و PC) مشترک می‌باشند، بنابراین این یک شبکهٔ نقطه‌به‌نقطه است ـ یعنی شبکه‌ای که تنها دو نقطهٔ پایانی دارد. در این حال سوئیچ درست مثل سیستم تلفن افراد را به‌هم متصل می‌کند بدون آنکه دیگران بتوانند یا بخواهند تداخلی را ایجاد نمایند.

تبعیت از قوانین: تا هنگامی‌که در شبکهٔ ما زندگی می‌کنید...

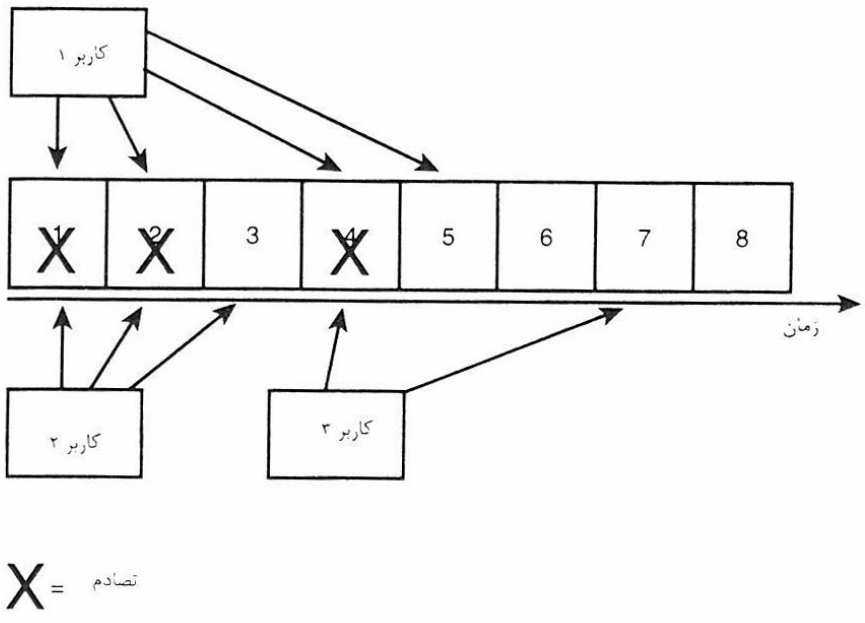
اِترنِت یک خط جمعی است با مجموعه‌ای از قوانین. این قوانین بسیار ساده و مقدماتی هستند، اما در هر حال به‌عنوان قواعدی لازم‌الاجرا مطرح می‌باشند. نام کوتاه‌شدهٔ این قوانین CSMA/CD است که مخفف تشخیص حامل با دسترسی

چندگانه/شناسایی تصادم[1] می‌باشد. همانگونه که حتی هنگام آغاز صحبت می‌توانید بشنوید که شخص دیگری صحبت‌کردن را آغاز نموده است، کارتهای شبکهٔ اِترنِت هنگام آغاز انتقال اطلاعات از طریق خط جمعی، به خط گوش فرا می‌دهند. حامل در CSMA/CD، نظیر اصوات خاصی که هنگام اتصال مودم به مودم دیگر به گوش می‌رسد، یک سیگنال از پیش تعریف شده است که می‌تواند اطلاعات را با خود حمل نماید.

تصادمها

اگر کارت شبکهٔ دیگری هنگام انتقال اطلاعات توسط کارت شبکهٔ شما شروع به کار کند، تداخل سیگنال ایجاد می‌شود ـ سیم تنها می‌تواند یک سیگنال را در هر لحظه حمل نماید این موضوع باعث وقوع خطایی می‌شود که در شبکه به آن تصادم اطلاق می‌گردد. در صورت وقوع یک تصادم، هر دو کارت شبکه مدت زمان تصادفی را صبر نموده آنگاه دوباره تلاش می‌کنند. رفته‌رفته، همانگونه که در شکل ۱-۹ نشان داده شده است کارتهای شبکهٔ فوق‌الذکر می‌توانند ـ به‌خصوص در یک بخش کم‌جمعیت کار خود را به انجام برسانند. از آنجا که هر ایستگاه‌کاری اطلاعات را در بسته‌های مجزا و کوچک انتقال می‌دهد (این موضوع در فصل یک بحث شده است)، این امکان وجود دارد که هر ایستگاه کاری بتواند در بینابین انتقالات صورت‌پذیرفته توسط ایستگاههای کاری دیگر حرف خود را بزند. این همیشه برای من به مثابهٔ جادوی سیاهی می‌ماند، اما این روش کار خود را به‌خوبی انجام می‌دهد.

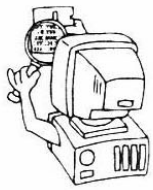
در لحظهٔ یک در شکل ۱-۹ کاربر یک و کاربر دو هر دو همزمان اقدام به انتقال اطلاعات می‌نمایند و بنابراین تصادم رخ می‌دهد. بعد از مدت‌زمانی هر دو دوباره تلاش می‌کنند، اما این‌بار هم در لحظهٔ دو با یکدیگر برخورد می‌نمایند. تلاش سوم آنها نیز صورت می‌گیرد. کاربر دو لحظهٔ سوم را به‌خود اختصاص می‌دهد. کاربر یک در لحظهٔ چهار اقدام می‌کند. اما بیچاره این‌بار با کاربر سه در لحظهٔ چهار برخورد می‌نماید وی در لحظهٔ پنج تلاشی را صورت می‌دهد و موفق می‌شود. کسی لحظهٔ شش را برای انتقال انتخاب نمی‌نماید و کاربر سه در لحظهٔ هفت انتقالی را صورت می‌دهد.



شکل ۱-۹ : تصادمها!

1- Carrier Sense Multiple Access/Collision Detect

در شبکه‌ای کوچک، تشخیص تصادم به خوبی کار می‌کند اما همانطور که قواعد غیر رسمی یک جلسه با افزایش تعداد افراد به بیش از ۱۰ یا ۱۵ نفر در اتاق کنفرانس یکی یکی شروع به شکسته‌شدن می‌کنند، اِترنِت هم هنگامی‌که تعداد ایستگاههای کاری به بیشتر از تقریباً ۲۴ دستگاه برسد، به سرعت کارایی خود را از دست می‌دهد.



نکته : *آبشاری‌کردن اِترنِت کار واقعاً ساده‌ای است؛ به این صورت که می‌توانید خط جمعی را از یک هاب توسط افزودن یک کابل و اتصال به یک هاب دیگر توسعه دهید. ارتقاء سریعی است، نه؟ سریع‌تر هابی خریده و آن را به شبکه متصل کنید!*



هشدار : *با این‌که افزودن یک یا دو هاب به منظور آبشاری‌کردن کاری ساده است، اما نباید گول بخورید. مواظب بزرگ‌شدن اِترنِت خود باشید ـ اگر تعداد هابها زیاد شوند به مشکلاتی برخورد خواهید کرد.*

بسیاری از پیاده‌سازی‌های اِترنِت در مجموعه‌های کاری کوچکتر به نوعی رشد داشته‌اند اما از ابتدای کار به منظور پشتیبانی تعداد بیشتری ایستگاه‌کاری طراحی نشده‌اند این ممکن است نتیجهٔ داشتن تعداد زیادی ایستگاه‌کاری که در یک بخش مشترک هستند باشد که به تصادم‌های زیادی می‌انجامد. نگاهی به نقشه‌های بخشهای خود بیندازید و تعداد ایستگاههای کاری در هر یک را بشمارید؛ به‌منظور کارایی بهینه و دستیابی به قابلیت اطمینان شاید بهتر باشد با استفاده از یک سوئیچ بخشهای خود را به قسمتهای کوچکتری تقسیم نمایید.

قاب‌دار و تقسیم‌شده

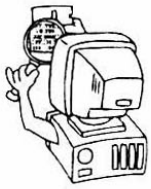
خوب است نگاهی به ساختار بسته در اِترنِت داشته باشید. از فصل اول به خاطر بیاورید که بسته کوچکترین واحد انتقال اطلاعات در شبکه می‌باشد. برخی اوقات هنگامی‌که تفاوتهایی در اندازه‌های بسته وجود دارند ممکن است بین دو بخش شبکه مشکلاتی بروز کنند، بنابراین باید حداکثر تفاوت ممکن بین اندازه‌های بسته‌های توپولوژی‌های شبکه‌ای خود را بدانیم.

بزرگترین اندازهٔ بسته در اِترنِت، یا اندازهٔ قاب، ۱۵۱۴ بایت می‌باشد. از این مقدار شش بایت برای آدرس MAC از NIC منبع، شش بایت مربوط به آدرس MAC مقصد، یک مقدار دوبایتی که نشاندهندهٔ نوع بسته است و یک بخش «دادهٔ بارگذاری» که حاوی داده است می‌باشد (مقدار این بخش حداکثر ۱۵۰۰ بایت می‌تواند باشد). بعضی از افراد (حتی آنهایی که تجزیه تحلیل‌گرهای شبکه را طراحی می‌کنند) حداکثر مقدار را ۱۵۱۸ بایت در نظر می‌گیرند. این مقدار چهار بایت را برای تشخیص خطا در پایان هر بسته شامل می‌شود. ۲۰ بایت دیگر را می‌توان در آغاز بسته پیدا نمود (که البته این مقدار تنها برای طراحان سوئیچ اِترنِت جالب توجه است).

هر بستهٔ اِترنِت که کمتر از ۶۰ بایت طول داشته باشد با عناوین کوتاه یا قطعه شناخته می‌شود و نشاندهندهٔ یک خطا در نرم‌افزار تحلیل‌گر می‌باشد. بستهٔ کوتاه ممکن است از طریق وقوع تصادم ایجاد شده باشد، بنابراین در صورت مشاهدهٔ تعداد زیادی از آنها ممکن است بهتر باشد که کاربران خود را از طریق سوئیچ‌هایی تقسیم نمایید.

سرعت اجرا

اِترنِت کلاسیک با سرعت ۱۰Mbps (مگابیت در ثانیه) کار می‌کند. یعنی ۱۰،۰۰۰،۰۰۰ بیت در هر ثانیه را می‌توان از طریق سیم منتقل نمود. تقسیم این مقدار بر ۸ بیت که در هر بایت وجود دارند، مقدار Bps ۱،۲۵۰،۰۰۰ را به دست می‌دهد.



نکته : *تعداد بیت در ثانیه را با حرف کوچک b و تعداد بایت در ثانیه را با حرف بزرگ B نشان می‌دهیم. بنابراین ۱۰ مگابیت در ثانیه به شکل Mbps ۱۰ و ۱۰ مگابایت در ثانیه به شکل MBps ۱۰ نشان داده می‌شود.*

این مقدار بسیار زیادی است و معنای آن این است که در حدود MB ۱ را در هر ثانیه می‌توان از طریق کابل یا شبکه انتقال داد. آیا این واقعاً اتفاق می‌افتد؟ پاسخ منفی است مگر آنکه اتصال اِترنِت، از نوع نقطه‌به‌نقطه باشد و ایستگاههای دیگر تلاشی برای اشتراک در آن به انجام نرسانند. با این‌که ۹۷ درصد اطلاعات، در واقع اصل «دادهٔ بارگذاری» می‌باشد، هر زمان که تصادمی را شاهد می‌شوید، در واقع کارایی شبکه‌تان کاهش می‌یابد و در مجموعه بسته‌های کمتری را می‌توان انتقال داد. از سوی دیگر تمام بسته‌ای که با تصادم روبرو شده است را باید دوباره انتقال داد.

تصادم‌ها تا چه حد واقعی هستند؟ هر زمان که بیش از دو ایستگاه اِترنِت را به یک بخش شبکه متصل می‌کنید، پتانسیل وقوع تصادم‌ها را بالا می‌برید. اما حتی اگر ۳۰٪ بسته‌ها با تصادم روبرو شوند هنوز MB ۰/۸ باقی می‌ماند که به اندازهٔ کافی سریع است.

البته در یک بخش اترنتی پرطرفدار ـ و در نتیجه با ترافیک بالا، نرخ وقوع تصادم‌ها ممکن است به ۸۰٪ برسد (این حالت باعث می‌شود تعجب کنید چرا برای انتقال اطلاعات از دیسکهای فلاپی استفاده نمی‌کنید). در چنین بخشهایی، مشکلات خود را به شکلهای گوناگونی نشان می‌دهند. برای مثال، از آنجا که برخی برنامه‌های کاربردی نسبت به زمان حساس هستند، اگر اطلاعات مورد نظر خود را با سرعت کافی دریافت نکنند، ممکن است هر نوع خطایی را ملاحظه کنید. بنابراین بهتر است نگاه دقیقتری به مستندات فیزیکی داشته باشید و پورت‌های هاب را شمارش کنید.



یادداشت : *مشکل تصادم، موضوعی است که توسط هواداران و طرفداران حلقه نشانه به‌عنوان دلیل آنان برای استفاده از حلقه نشانه اشاره می‌شود، این به‌خاطر توانایی حلقه نشانه در مقیاس‌پذیری و فراهم‌آوردن عرض باند ادعایی توسط آن می‌باشد. نگران نشوید. اِترنِت به اندازهٔ کافی خوب است. در مورد مشکلات و کمبودهای حلقهٔ شکسته ـ منظورم حلقه نشانه است ـ در فصل آینده صحبت خواهم کرد. در این بین، واقعیت آن است که تمامی توپولوژی‌های شبکه‌ای مشکلات خود را دارا هستند ـ کلید آن است که آنها را بشناسیم و به آنها به‌گونه‌ای برخورد کنیم که حداقل دردسر را داشته باشیم (در فصل ۱۰ کمی هم سربه‌سر اِترنِت گذاشته آن را نیز خواهم کوفت. این کار برای تفریح است، از کوره در نروید).*

اِترنِت ۱۰۰ مگابیتی

مد نظر داشتن تعداد ایستگاههای کاری که به یک بخش متصل شده‌اند در اِترنِت ۱۰۰ مگابیتی از اهمیت بیشتری برخوردار است (فعلاً کاری به اِترنِت ۱۰۰۰ مگابیتی یا اِترنت گیگ نداریم، چرا که به اتصالات فیبر نوری برای دسترسی به این

سرعتها نیاز داریم و علاوه بر آن نصب و نگهداری حرفه‌ای الزامی است).

با اینکه اِترنِت ۱۰۰ مگابیتی درست مثل اِترنِت کار می‌کند ـ حتی از لحاظ اندازهٔ قاب و تصادم‌ها ـ ده برابر سریعتر اجرا می‌شود. بنابراین به‌جای Mbps ۱، می‌توانید راجع به Mbps ۱۰ صحبت کنید. همانگونه که انتظار می‌رود دلیل استفاده از چنین شبکه‌ای دستیابی به سرعت بالاتر است. هر حوزهٔ تصادم بزرگ (عبارت رسمی برای «تعداد زیادی از کاربران که در یک بخش مشترک کار می‌کنند») می‌تواند توان عملیاتی را به گونهٔ چشم‌گیری پایین آورد و بنابراین این حس را به‌وجود می‌آورد تا بخواهید از حداکثر توان Mb ۱۰۰ خود استفاده کنید.



نکته : *برای سرویس‌دهنده‌هایتان، یک اتصال اِترنِت کامل دوطرفه سریع ممکن است مثل پادزهری در مقابل با اتصال کُند عمل نماید. اتصال دوطرفه کامل به سوئیچ به آن معناست که از هر دو سیم ارسال و دریافت به صورت همزمان استفاده شده و سرعت دوبرابر می‌گردد. این یعنی خط لوله اِترنِت Mb ۱۰۰ تان به خط لوله‌ای Mb ۲۰۰۰ تبدیل می‌شود.*

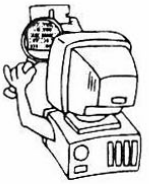
دوطرفه نیمه، اِترنِت معمولی یا اتصال حلقه ـ نشانه، مثل زمانی است که از درایو استفاده می‌کنید. ابتدا یک نفر صحبت می‌کند بعد دیگری.

دوطرفه کامل، مثل استفاده از تلفن است ـ هردوی ایستگاهها همزمان می‌توانند صحبت کنند. از آنجا که این یک خط جمعی نیست، و از آنجا که کامپیوترها (برخلاف من و شما) می‌توانند کارهای بسیاری را با هم انجام دهند، این موضوع و این شکل از کار، تصادمی را ایجاد نمی‌کند.

فقط کافی است مطمئن شوید راه‌انداز اِترنِت و همچنین سوئیچی که می‌خواهید اتصال به آن را صورت دهید، هردو عملیات دوطرفه کامل را پشتیبانی می‌کنند؛ دفترچه‌های راهنما باید بتوانند به شما بگویند چگونه این حالت را فعال سازید. بیشتر کارت‌ها و سوئیچ‌ها در صورتی که به تازگی خریداری شده باشند این حالت را پشتیبانی می‌کنند، اما وارسی مذکور مضر نخواهد بود.

کارناوال کابل‌کشی

اِترنِت به عنوان یک تکنولوژی کامپیوتری، به میزان کاملاً زیادی در صفحه باقی مانده است. این بدان معناست که چندین روش برای کابل‌بندی آن وجود دارند که ممکن است هنگامی که در هزاره بعدی قرار می‌گیرید، الزاماً برایتان تمایلی ایجاد نکنند. خبر خوب آن است که هیچ یک از ملزومات Mb ۱۰۰ به شکل هیچ یک از این روشهای قدیمی قابل پیکربندی نیستند، اما اگر از اِترنِت Mb ۱۰ استفاده می‌کنید، ممکن است مجبور باشید به پیکربندی‌های کابل‌کشی قدیمی‌تر اتکا کنید.



نکته : *جایگزینی انواع شبکه‌ای زیر در درازمدت از نقطه‌نظر هزینه و زمان به نفع شما خواهد بود. آنها منسوخ شده‌اند و با هزینه ارزان قابل جایگزینی هستند:*

نام	نوع اتصال‌دهنده	مشکلات
Thinnet 10Base-2	*BNC (کابل هم‌محور)*	*کابل‌کشی به صورت گذرگاه، به‌معنای آن است که عدم اتصال یک ایستگاه‌کاری یا یک خرابی در کابل، کل بخش را مختل می‌کند. این روش به صورت کل مشکل‌زاست و کار با آن در مقابل 10Base-T مدرن مشکلتر است.*

Thicknet	*BNC (کابل هم‌محور)*	*کابل‌کشی به صورت باس. گران، مستعد مشکلات و کمبود فروانی قطعات*
10Base-5		
AUI	*DB-15*	*گران و مشکل یافتن قطعات*

تمامی انواع این شبکه‌های بدو قدیمی قبل از ترویج تکنولوژی UTP (10Base-T و بعد از آن 100Base-T) به وجود آمده‌اند.



یادداشت : *Base در Base-T اشاره دارد به این حقیقت که اِترنِت بر مبنای تکنولوژی باند پایه ـ به جای باند کامل ـ کار می‌کند. این تنها یک واژه پیشرفته است که به روش کُدبندی سیگنال اشاره می‌نماید. T نیز برای اشاره به زوج به هم تافته (twisted pair) به‌کار می‌رود.*

این گرایش وجود دارد که روش پیشرفته اتصال اِترنِت، UTP یا 10Base-T نامیده شود. بخش مهم، امروزه، آن است که یا از CAT-V(100Mb) یا CAT-III(10Mb) استفاده می‌گردد. مجدداً، طرح CAT تنها روش استانداردی است برای اشاره‌کردن به مشخصات ساخت کابل. CAT-V سیگنال‌های خیلی بیشتری را نسبت به CAT-III می‌تواند نگه دارد؛ بنابراین اِترنِت 10Mb را می‌توان روی CAT-V به‌اجرا درآورد، اما نمی‌توان 100Mb را با سیم‌کشی CAT-III به جریان انداخت. در صورت درصدد برآمدن برای انجام این کار، با مشکلاتی برخورد خواهید نمود.



هشدار : *سعی نکنید اِترنِت 100Mb را روی کابلی که به عنوان CAT-V به تأیید نرسیده است به اجرا درآورید.*
انواع مختلف خطاهای تناوبی شبکه‌ای ممکن است به وقوع بپیوندند که باعث حادث‌شدن تأثیرات جانبی روی برنامه‌های کاربردیتان خواهند شد. از آن گذشته، به خاطر آنکه سیگنالی دریافت می‌کنید و در حال صحبت با شبکه هستید، ممکن است مشکل را در هر جای دیگری به غیر از کابل‌ها جستجو کنید.

از همه این موارد که بگذریم، اِترنِت 100Mb کاملاً نظیر اِترنِت 100Mb کار می‌کند، اما سریعتر. برای مثال، بیشترین مقدار طول کابل برای هر یک 100 متر (330 فوت) می‌باشد. هز دو از اتصال‌دهنده‌های RJ-45 استفاده می‌کنند و در هر دو از هاب یا سوئیچ استفاده می‌گردد.

چگونه تشخیص می‌دهید که کابل‌تان CAT-V می‌باشد؟ خوب، اگر بعد از سال ۱۹۹۷ نصب شده است، می‌توان حدس زد که CAT-V می‌باشد. تنها روش دانستن این موضوع، پرسیدن از نصب‌کننده یا تست‌کردن با پویشگر کابل است. در فصل ۲۱، به طور خلاصه در مورد پویشگرهای کابلی بحث خواهم نمود.



نکته : *حداقل پنج روش برای رد تأییدیه CAT-V وجود دارند، بنابراین باید از نصب‌کننده بخواهید بخش مربوط به خود در فرآیند نصب را «مورد تأیید» قرار دهد. این بدان معناست که وی پریزها، جک‌ها، کابل‌ها و تکنیک‌های سازگاری با CAT-V را به‌کار برد در آخر کار بتواند از طریق اندازه‌گیری محصول پایان ـ به ـ پایان ثابت کند که تئوری جعبه حقیقت به خود گرفته است.*

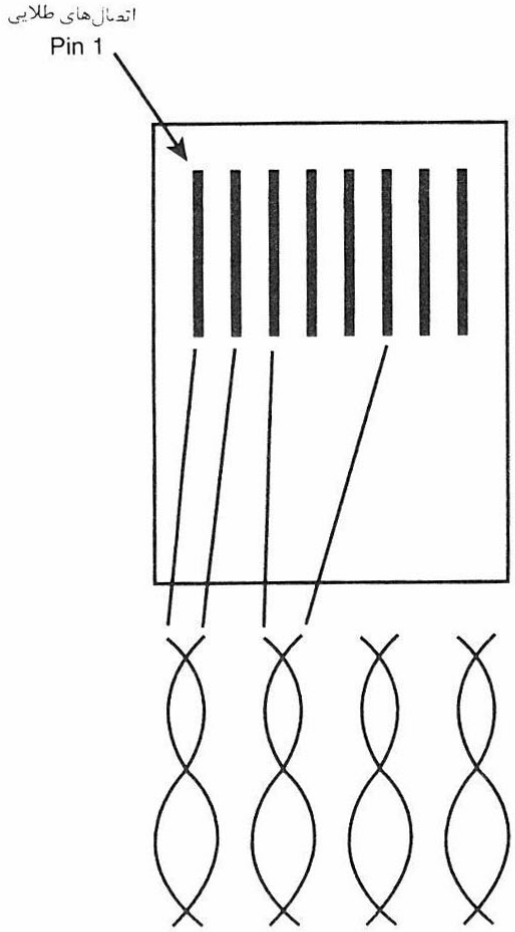
همچنین، برخی دوست دارند از نصب‌کننده‌های کابل تأییدشده کمک بگیرند ـ یعنی، نصاب کابل شبکه آشنا با صنعت شبکه.

تمامی UTP های اِترنِت از چهار سیم استفاده می‌کنند: پین‌های ۱، ۲، ۳ و ۶. آیا لازم است برای عیب‌یابی، این موضوع را بدانید؟ تنها اگر بخواهید کابل را «مرتب» کنید، همان طور که در فصل ۸ ملاحظه نمودید. به بیان دیگر، اگر پین‌های 4، 5، 7 و 8 مشکلاتی را ایجاد کرده باشند، مسأله مهمی نیست.



نکته : *فقط کابل‌های NIC ـ به ـ هاب باید مستقیم باشند ـ یعنی پین‌به‌پین. نحوه اتصال در کابل‌هایی که برای متصل‌ساختن هاب‌ها به‌کار می‌روند، ضربدری است. اگر مولتی متر دارید، بهتر است بررسی کنید هر سیم از یک طرف کابل به کدام پین در سوی دیگر متصل شده است. به خاطر داشته باشید، برای انجام این کار باید مولتی متر را در حالت پیوستگی قرار داد. یکی از میله‌های تست را روی پین 1 در یک طرف کابل می‌گذارید و آنگاه در سوی دیگر، میله تست دیگر را روی پین‌ها حرکت دهید.*

کابل‌های UTP اِترنِت چهارزوج سیم به‌هم تافته دارند. پین‌های ۱ و ۲ باید از یک زوج و نیز پین‌های ۳ و ۶ باید از یک زوج باشند (شکل ۲-۹). بااینکه ممکن است مستقیم‌ترین روش ساخت کابل اتصال پین‌های ۱ و ۲ و آنگاه ۳، ۴، ۵، ۶، ۷ و ۸ به‌نظر برسد، اما این روش درست نیست اِترنِت 10Mb با چنین کابلی به اجرا درخواهد آمد، اما تحت 100Mb به مشکلات عجیبی برخورد خواهید نمود. اگر می‌بینید که کابلی به گونه نادرستی عمل می‌کند، بهتر است آن را با کابل سالمی تعویض کنید.



شکل ۲-۹ : پیکربندی صحیح سیم‌ها و پین‌ها در اِترنِت.

آیا این بدان معناست که نحوه نصب در اِترنِت اهمیت زیادی دارد؟ حتی کابل‌های پل سیم را نیز باید در طرح کابلی کلی هر بخش محسوب نمود (طرح کابلی آن، که خطی جمعی است، به قدرتمندی ضعیفترین پیوند است ـ یک سیب پوسیده ممکن است یک جعبه سیب را خراب کند. در اینجا هم، بهتر است از کابل‌های آماده به جای ساخت کابل، از کابل‌های آماده استفاده نمایید.

پایین، پایین، پایین

این شانس وجود دارد که بخشهای مختلف اِترنِت هفته قبل، هفته قبل‌تر و هفته قبل‌تر از آن بدون هیچ مشکل نصبی کار کرده باشند، درست است؟ هر چه باشد هیچ چیز تغییر نکرده است. اجازه دهید نگاهی داشته باشیم که طریقی که هر بخش اِترنِت ممکن است تغییر کند و مشکلاتی ممکن است از پس از تغییر به وجود بیایند.

«قابلیت رشد» اِترنِت، در گذشته، نقطه ضعف آن بوده است. با اینکه امروزه می‌توان در شبکه اِترنِت با استفاده از یک سوئیچ، هاب یا هاب‌هایی را اضافه نمود، در گذشته تنها امکان آبشاری‌کردن هاب‌ها وجود داشت. افزودن هاب‌ها یا توسعه هر شبکه اِترنِت را می‌توان خارج مشخصه طراحی قرار دارد. یکی از مشخصه‌های طراحی «قاعده ۵-۴-۳» نامیده می‌شود.

قاعده ۵-۴-۳

قاعده ۵-۴-۳ اِترنِت اذعان می‌دارد:

- می‌توانید سه زیربخش پرجمعیت داشته باشید (تنها برای کابل هم‌محور، پس این مورد را فراموش کنید).
- ممکن است ۴ تکرارکننده یا متمرکزکننده‌ها داشته باشید.
- می‌توانید ۵ زیربخش به صورت سری داشته باشید ـ یعنی، یکی پس از دیگری، مثل چراغانی، قرار گرفته باشند.

از آنجا که قاعده ۳ تنها برای شبکههای کابلی هم‌محور صادق است، اجازه دهید روی قواعد ۴ و ۵ تمرکز کنیم. تکرارکننده، ابزاری است که به منظور فائق‌آمدن بر محدودیت طول سیم، سیگنال را دوباره تولید می‌کند (۱۰۰ متر با UTP). به طور خلاصه، هنگامی که سیگنالی را تا پایین خط اکو می‌کنید، زمانی صرف می‌شود؛ تعداد زیاد اکو، باعث ازدست‌رفتن مقدار زیادی زمان می‌شود.

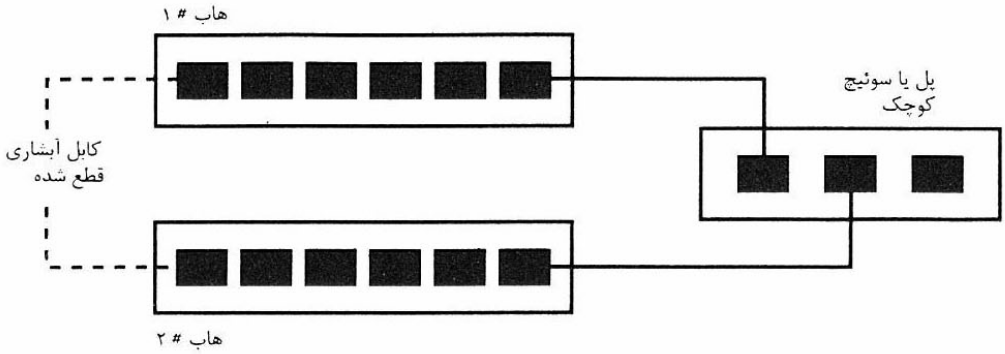
قاعده ۵ به معنای آن است که نباید بیش از ۵ هاب را در هر ردیف آبشاری کنید (هر هاب پشته‌ای با پیوند اختصاصی بین هاب‌ها، یک هاب محسوب می‌شود).

حتی اگر مطابق طرح باقیمانده و هیچ چیز تغییر نکرده باشد، امکان خرابی چیزهای مختلف وجود دارد. برای مثال، کارت‌های شبکه ممکن است خراب شوند و هنگام انتقال اطلاعات، عمل شنود را متوقف سازند که این باعث گره‌خوردن خط جمعی می‌شود. هاب‌های هوشمند دارای مدارهای «ضدحرافی» هستند که جلوی این مسأله را می‌گیرد، اما حتی هاب‌ها هم

ممکن است خراب شوند. هنگامی که هاب‌ها نتوانند با کارت شبکه خراب کنار بیایند یا خودشان خراب شوند، زمان بازی تفرقه بینداز ـ و ـ حکومت کن فرا رسیده است.



نکته : *اگر به یک مشکل فیزیکی شبکه ظنین هستید (برای مثال، یکی از بخشها، واقعاً کُند است)، لازم است هنگام عیب یابی شبکه واقعاً بالا باشد (افراد دوست ندارند در کارشان برای عیب یابی اختلالی ایجاد شود). در این حالت، باید یک سوئیچ دو پورته را در محل قرار دهید، که به شما اجازه می‌دهد با هاب بخصوصی یا گروهی از هاب‌ها، در خط جمعی مجزایی از بقیه کار کنید (شکل ۳-۹). می‌توانید از DataCommWarehouse (www.datacomwarehouse.com)، CableExpress (networksnow.com) یا دیگر فروشگاههای شبکه‌ای با امکان سفارشی پستی، مینی سوئیچی را تهیه نمایید (در زمان کتابت این نوشته، NetGear سازنده خوبی برای سوئیچ‌های دوپورته محسوب می‌شود).*
عمل نصب، خیلی سریع خواهد بود. کابل آبشاری را از هاب دوم باز کنید. آن کابل را به پورت ۱ سوئیچ وصل کنید. کابل اضافی دیگری را به پورت ۲ متصل نموده و سر دیگر آن را به هاب دوم ارتباط دهید. همین! نصب پایان گرفت.



شکل ۳-۹ : هر پل کوچک، حوزه مشکل‌زا را به دو قسمت بخش می‌کند، در عین حال کاربران می‌توانند به شکلی شفاف و عاری از هر نوع خطا دیگری، به کار خود ادامه دهند.

خلاصه

اِترنِت، یک تکنولوژی شبکه‌ای ساده از لحاظ طرح فیزیکی می‌باشد. با این وجود، نظیر هر شبکه‌ای، قواعد سخت ـ و ـ سریع مربوط به طرح و پیاده‌سازی خود را داراست. با اینکه در گذشته، اِترنِت انواع مختلفی از کابل‌کشی فیزیکی را مورد استفاده قرار می‌دهد، ساده‌ترین و قابل اطمینان‌ترین کابل‌بندی امروزی، UTP است.

بزرگ‌شدن اِترنِت به سادگی صورت می‌پذیرد و این سادگی باعث می‌شود که خیلی آسان شبکه از مشخصات طراحی خود خارج شود. این مسأله بزرگی در شبکه‌های سوئیچی نیست، چرا که هر پورت سوئیچ، به هر بخش اِترنِت (یا ایستگاه‌کاری) به جای قوانین شبکه‌های آبشاری، خط جمعی خاص خود را ارائه می‌کند.

کارگاه

پرسش و پاسخ

پرسش : آیا باید برای هر PC، یک پورت سوئیچ استفاده کنم؟
پاسخ : اگر ثروتمند هستید، این کار را بکنید. البته، بیشتر افراد روی هر پورت سوئیچ یک هاب را قرار می‌دهند و پورت‌های سوئیچ را برای سرویس‌دهنده‌ها پس‌انداز می‌نمایند.

پرسش : آیا خطاهایی به غیر از تصادم‌ها وجود دارند؟
پاسخ : تصادم‌ها خطاهای دیگر نظیر خطاهای CRC و خطاهای جزئی دیگر را به وجود می‌آورند. اما در مجموع، تمامی خطاها از تصادم منشأ می‌گیرند.

پرسش : آیا افراد از کابل‌کشی CAT-V خود استفاده نمی‌کنند؟
پاسخ : خیر. بعد از آنکه چیزی در دیوار قرار گرفت، جایگزینی آن دردآور است، پس طبیعی است که بخواهیم یک بار آن را انجام دهیم.

پرسش : قانون ۵-۴-۳ برایم اشتباه‌برانگیز است. آیا باید واقعاً آن را یاد بگیرم؟
پاسخ : اگر یک هاب کوچک روی هر پورت سوئیچ گذاشته و از تکرارکننده‌های اضافه استفاده نمی‌کنید، خیر.

آزمون

۱- طی یک انتقال عاری از خطای طبیعی، ممکن است ـــــــ سیگنال در هر بخش از اِترنِت وجود داشته باشد (باشند).

الف ـ ۵ ب ـ ۱۰
ج ـ ۲ د ـ ۱

۲- تصادم چیست؟

الف ـ هنگامی که دو کارت شبکه همزمان تلاش می‌کنند به انتقال اطلاعات بپردازند.
ب ـ هنگامی که دو کارت شبکه ریزتراشه‌های خراب ایجاد کنند.
ج ـ هنگامی که کاربر به پایگاه داده‌ای اشتباهی دسترسی پیدا می‌کند.
د ـ هنگامی که کاربر داده نادرستی را منتقل می‌کند.

۳- درست یا نادرست؟ خطاها، بخشی طبیعی از عملکرد اِترنِت می‌باشند.
۴- درست یا نادرست؟ Thinnet ، Thicknet و AUI محبوبترین انواع اِترنِت هستند که می‌توانید ابتیاع نمایید.

پاسخ به سؤالات آزمون

۱- د ۲- الف
۳- درست ۴- نادرست

فصل ۱۰

مبانی حلقه ـ نشانه[1]

«نه پرنده، نه هواپیما، و نه حتی قورباغه. این منم... قربانی بی‌عدالتی اجتماع.»

حلقه ـ نشانه، قربانی بی‌عدالتی جامعه توپولوژی‌های LAN، توسط آنان که از آن استفاده نمی‌کنند، مورد طعنه و استهزا قرار دارد و از سوی دیگر از طرف کسانی که آن را به کار می‌برند، مورد پرستش است. برای بسیاری از افراد، حلقه ـ نشانه مظهر سرعت، دقت و قابلیت اطمینان سرویس‌دهی در طول سالیان متمادی بوده است، اما پیش‌بینی آیندهٔ آن اندکی مشکل است. با این‌که فروشندگان حلقه ـ نشانه با معرفی HSTR (حلقه ـ نشانه با سرعت بالا[2]) به جرگهٔ 100Mb پیوسته و در آیندهٔ نزدیک محصولات حلقه ـ نشانه گیگ (1000Mb) را عرضه خواهند نمود، حلقه ـ نشانه نسبت به اترنتی با سرعت مشابه، گران‌تر باقی می‌ماند و پیداکردن تکنسین‌هایی که در کار با آن و عیب‌یابی آن مهارت داشته باشند مشکل‌تر شده است.



یادداشت : *بسیاری از افراد فکر می‌کنند که این کمبود تکنسین مثل تیری در تابوت حلقه ـ نشانه خواهد بود. بحث این است که حلقه ـ نشانه راه خود را همانگونه که تکنولوژی گران‌قیمت‌تر بتاماکس ادامه داده، خواهد پیمود: کاربران حلقه ـ نشانه، به کارگیری آن را برای ۳ تا ۷ سال آینده ادامه خواهند داد، اما تکنولوژی جدیدتر، تکنسین‌ها و قطعات لازم کم‌کم از آن روی خواهند گرداند و بنابراین هزینه‌های استفاده بالاتر خواهد بود. رفته‌رفته تناسب‌های هزینه‌ای، متعصب‌ترین کاربران حلقه ـ نشانه را وادار خواهد کرد که به توپولوژی‌های دیگر روی آورند.*



یادداشت : *مشاهده شده که مدیران فهیم IT به مرور در حال جایگزین‌کردن حلقه ـ نشانه خود هستند ـ به‌عبارت دیگر در صورت خرابی یک بخش، آن را تعمیر نمی‌کنند! تغییر کامل فراساختار شبکه به‌صورت همزمان ممکن است برای هر مجموعهٔ کاری، به‌خصوص در صورت عدم وجود دلایل لازم برای صرف هزینه، خطرناک و گران‌قیمت باشد. به‌طور کلی، مدیران IT‌ای که باور دارند می‌توانند نوشته‌های روی دیوار را بخوانند، در صدد خلاصی از حلقه ـ نشانه هستند و این‌کار را هنگام خرابی وسایل یا توسعه پروژه‌های شبکه‌ای جدید به انجام می‌رسانند.*

از سوی دیگر، قابلیت دسترسی به حلقه ـ نشانه با سرعت بالا این امکان را فراهم می‌سازد که آنچه را در اختیار داریم، نگه داریم، تنها با سرعتی بالاتر. تنها زمان است که ثابت می‌کند این قابلیت دسترسی باعث تولد مجدد حلقه ـ نشانه خواهد شد یا خیر. هنگامی‌که این مطالب را می‌نویسم، می‌توانم قیافهٔ سخت‌گیر و عبوس تیم تولیدکنندهٔ حلقه ـ نشانه را مجسم نمایم.

1- Token-Ring 2- High-Speed Token-Ring

آیندهٔ حلقه ـ نشانه، هر چه که باشد، این واقعیت به‌جای خود باقی است که شما در حال مطالعهٔ این فصل هستید و این نشاندهندهٔ این است که یا علاقه‌مند هستید بدانید حلقه ـ نشانه چه تفاوتی با اِترنِت دارد و یا این‌که وارث یک شبکهٔ حلقه ـ نشانه می‌باشید. حلقه ـ نشانه از طرح قوی و خوبی برخوردار است، پس بنابراین خوشحال باشید!

قواعد را دنبال کنید : به اشتراک گذارده و لذت ببرید!

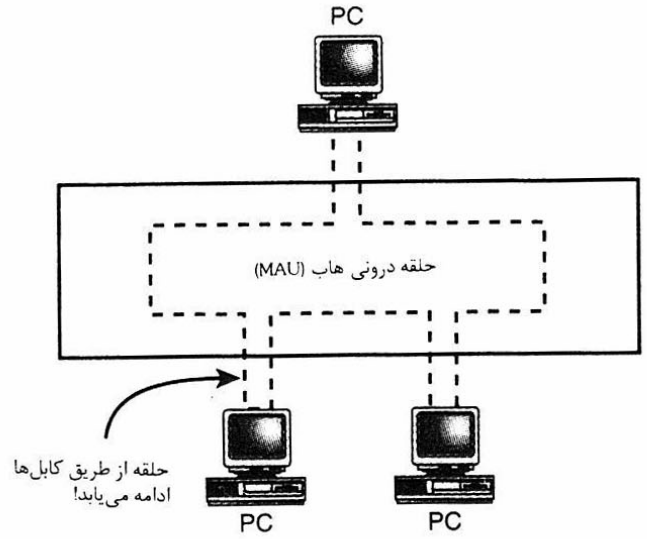
حلقه ـ نشانه، علیرغم حضور سست در بازار، دریچه‌ای است به‌سوی یک شبکهٔ اشتراکی بسیار عالی و کارآمد. برخلاف قواعد آزاد ـ برای ـ همه موجود در اِترنِت، با آن روش آزادی هر شخص و صحبت‌های تصادف‌گونه و آنگاه تکرار در صورت بروز خطا، خط جمعی حلقه ـ نشانه قواعد سختی دارد. اگر اِترنِت را مانند والدینی فرض کنیم که برایشان «در خانه‌بودن قبل از ساعت یازده» اهمیت دارد، حلقه ـ نشانه از آن نوع والدینی است که می‌خواهند بدانند با چه کسی، کجا می‌رود، چه‌کسی رانندگی می‌کند و نظایر آن. حلقه ـ نشانه قواعد بسیار بیشتری دارد و بنابراین قابلیت بازیابی و مدیریت بسیار بیشتری را در اختیار می‌گذارد.

تنها برای یک لحظه، تصور کنید که افراد موجود در شبکهٔ حلقه ـ نشانه در یک اتاق کنفرانس بزرگ حضور دارند. فرض کنید که تعداد این افراد زیاد است (مثلاً بیش از ۵۰ نفر). چگونه مکالمه امکان‌پذیر است؟ تصور کنید که خودتان در چنین موقعیتی قرار دارید. احتمالاً یک صندلی را انتخاب می‌کنید، و این صندلی است که نوبت صحبت‌کردن را در اختیار هر کس می‌گذارد. این واقعیت، بسیار شبیه کاری است که حلقه ـ نشانه انجام می‌دهد. کارآیی حلقه ـ نشانه در گروههای بزرگ بسیار بالاتر از اِترنِت است. این موضوع را می‌توان به‌صورت بحثی پارلمانی از یک سو، و بحثی خانوادگی از سوی دیگر مجسم نمود: روش به کاررفته در مورد گروههای کوچک، باعث اتلاف منابع می‌گردد، اما در مورد گروههای بزرگ صرفه‌جویی‌های بزرگی را به دنبال دارد.

ابتدا، حلقه ـ نشانه چگونه به‌صورت فیزیکی کار می‌کند؟ هر ایستگاه‌کاری که وارد حلقه می‌گردد را می‌توان به‌عنوان شخصی که جایی را گرداگرد میز کنفرانس اشغال می‌کند، تصور نمود. این دقیقاً همان شکلی است که برای کابل‌کشی حلقه ـ نشانه به‌کار می‌رود (یعنی استفاده از توپولوژی «حلقه» به‌جای توپولوژی «ستاره» مورد استفادهٔ اِترنِت). با این‌که کابل‌کشی شبیه به ستاره به‌نظر می‌رسد، مسیر کابل یک حلقه را از ایستگاه‌کاری به هاب و از هاب به ایستگاه‌کاری تشکیل می‌دهد، همانگونه که در شکل ۱-۱۰ نشان داده شده است. ممکن است تعجب کنید چرا این حالت نظیر چراغهای کریسمس کار نمی‌کند؟ پاسخ آن است از آنجا که تمامی کابل‌های به یک هاب وارد می‌شوند؛ در صورت بروز یک خرابی، هاب (که *MAU* یا واحد دسترسی چندگانه[1] نامیده می‌شود) می‌تواند سیگنال‌ها را دور از خرابی به گردش درآورد (مگر آنکه چیز دیگری خراب شده باشد).

تصور کنید هر ایستگاهی که به MAU متصل می‌شود، شخصی است که پای میز کنفرانس می‌نشیند (حلقه). به اولین ایستگاه در شبکه ناظر فعال[2] گفته می‌شود (صندلی انتخاب‌شده)، که به‌عنوان نقطهٔ تماس با بقیه به منظور گزارش خطاها، نگهداری از زمان‌بندی حلقه، تشخیص خطاهای خاص مربوط به خود حلقه و شروع عملیات خاص هنگام بروز خطاهای جدی ویژه، مورد استفاده قرار می‌گیرد. هر ایستگاهی در شبکه که متعاقباً به حلقه وارد می‌شود، ناظر آماده[3] نام می‌گیرد و می‌تواند در صورت خروج ناظر فعال از حلقه کنترل را به دست گیرد.

1- Multiple Access Unit 2- Active Monitor 3- Standby Monitor



شکل ۱-۱۰ : حتی با حضور هاب، کابل‌کشی در حلقه ـ نشانه در واقع یک حلقه را شکل می‌دهد با این‌که ممکن است شبیه ستاره به نظر برسد.

ناظر فعال همچنین مسئول صدور بستهٔ خاصی با نام نشانه[1] می‌باشد. هر بسته که روی سیم قرار می‌گیرد، از یک کارت حلقه ـ نشانه به کارت حلقه ـ نشانهٔ دیگر داده می‌شود تا کل حلقه پیموده شود. تک‌تک ایستگاههای موجود در حلقه به نوبت صحبت می‌کنند. هنگامی‌که ایستگاهی نشانه را در اختیار داشته باشد، می‌تواند اطلاعات خودش را انتقال دهد.

بلای خطا : هنگامی‌که NAUN شخص، محل یا چیز شناخته‌شده‌ای نیست

ترتیب کاری حلقه ـ نشانه بسیار جالب و فوق‌العاده است. این موضوع هنگامی‌که حلقه ـ نشانه از کار بازمی‌ایستد نیز صادق است، چرا که حلقه ـ نشانه قواعد بسیاری را برای کار با خطا در اختیار گذارده است. همانگونه که یک نمایندهٔ پارلمان می‌تواند با تخلف یک قانون بدون موکول‌کردن موضوع به جلسه‌ای دیگر برخورد کند، ناظر فعال حلقه نیز می‌تواند با موقعیت‌های مشخصی برخورد کند. البته، نظیر هر جامعهٔ آزادی، شهروندان از آزادی در تصمیم برخوردارند.

برای این‌که بسته‌ای مسیر خود را گرداگرد حلقه طی کند، هر ایستگاه باید بسته را به ایستگاه همسایهٔ خود انتقال دهد؛ در عمل هر ایستگاه محل همسایگانش را حفظ می‌کند. یعنی، آدرس نزدیک‌ترین همسایهٔ آدرسی فوقانی خود را می‌داند (NAUN خود). آیا این مهم است؟ تردید نکنید!

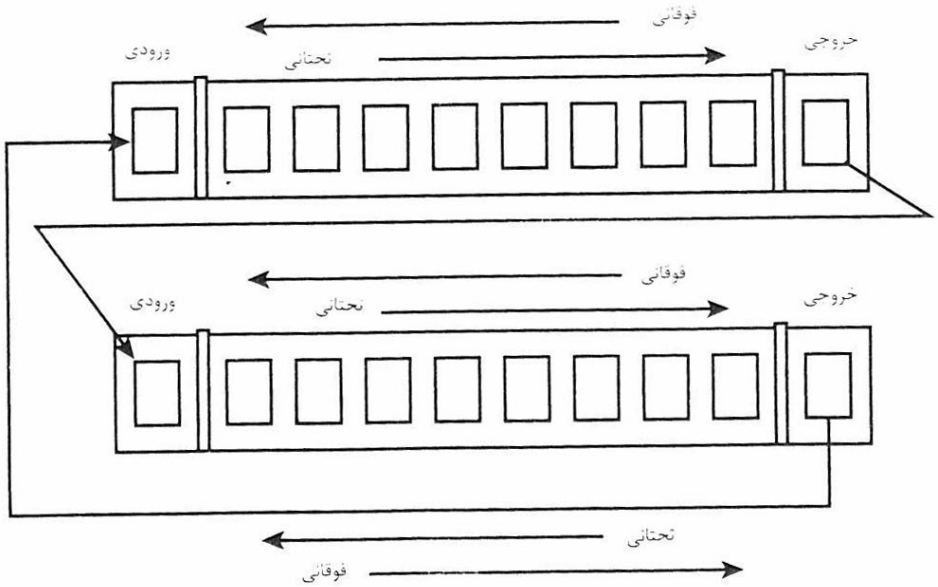
در وهلهٔ اول، منظور از کلمهٔ فوقانی چیست؟ خوب، از آنجا که حلقه ـ نشانه بسته‌ها را به ترتیب در حلقه قرار می‌دهد، فوقانی به جهتی که بسته‌ها در آن سو حرکت **نمی‌کنند**، اشاره می‌کند.

اجازه دهید کمی هم در مورد واژهٔ تحتانی صحبت کنیم. تئوری را کنار بگذارید و اجازه دهید که این موضوع را از دیدگاهی عملی بررسی نماییم. دسته‌ای از ایستگاههای کاری را به یک هاب حلقه ـ نشانه متصل می‌کنیم، سرویس‌دهنده‌ای

1- Token

را نیز اضافه کرده و آماده کار هستید، درست است؟ تحتانی در این حالت جهت اولین پورت به آخرین آن می‌باشد.

اضافه‌کردن یک هاب دیگر به آن معنا است که می‌خواهید حلقه را توسعه دهید. هر هاب حلقه ـ نشانه (MAU) دارای دو بخش با عناوین ورودی حلقه و خروجی حلقه می‌باشد که به منظور توسعهٔ حلقه در نظر گرفته شده‌اند. کار آسانی است: بسته‌ها از مسیر تحتانی به‌سوی خروجی رفته و از طریق بعدی که طبق تعریف پورت فوقانی پورتهای دیگر می‌باشد، جریان می‌یابد. این موضوع ممکن است کمی مبهم به نظر برسد، اما با نگاهی به شکل ۲-۱۰ مفهوم آن را بهتر درک خواهید کرد.



شکل ۲-۱۰ : تحتانی همواره به سوی خروجی و فوقانی به سوی ورودی MAU حلقه ـ نشانه قرار گرفته‌اند. جهت فوقانی و تحتانی با حرکت روی حلقه تعویض می‌شود.

به NAUN ها باز می‌گردیم. دلیل اهمیت آنکه هر ایستگاه NAUN خود را بشناسد، آن است که هنگامی‌که خطایی در یکی از ایستگاهها رخ می‌دهد، دو ثانیه بعد گزارش وقوع این خطا به ناظر فعال ـ رئیس حلقه ـ ارسال می‌شود. در صورت اجرای یک برنامهٔ تحلیل‌گر شبکه، گزارش خطا و آدرس NAUN را ملاحظه خواهید کرد. در صورت مشاهدهٔ NAUN در اطلاعات ثبت‌شدهٔ خطا، به ایدهٔ خوبی در مورد مبدأ خطا دست خواهید یافت.

لحظه‌ای به این موضوع فکر کنید. در یک بازی تلفنی، اگر شخصی که در سمت چپ من قرار گرفته مسئول ارائهٔ پیغام درست به من باشد و من مسئول ارسال پیغام درست به نفر سمت راستی‌ام باشم، هنگامی‌که متوجه می‌شوم پیغام دریافتی درست نیست، به‌صورت طبیعی به نفر دست چپی خود ظنین می‌شوم. اگر این پیغام‌ها بسته‌هایی باشند و من یک کارت حلقه ـ نشانه، هنگامی‌که خطایی را ملاحظه می‌کنم، به‌طور طبیعی به کارت حلقه ـ نشانهٔ فوقانی خود مشکوک می‌شوم.

انواع خطا

انواعی از خطا که تا به حال مورد بررسی قرار گرفته‌اند، خطاهای سبک مجزا نام دارند. از این جهت به چنین خطاهایی مجزا گفته می‌شود که تنها توسط یک ایستگاه حادث می‌شوند و مشکل عمومی‌ای را در حلقه ایجاد نمی‌کنند، مضاف بر این‌که ردیابی آنها تا حدودی آسان است. کلمهٔ سبک از این جهت در مورد این خطاها به‌کار می‌رود که دریافت تعداد معدودی از آنها برای حلقه امر خیلی بدی محسوب نمی‌شود. سروکار داشتن با مشخصات دقیق این خطاها به غیر از حالتی

ک، بخواهید استادکار شبکهٔ حلقه ـ نشانه باشید، ارزش دانستن ندارد؛ البته، خوب است که بدانیم کدامیک از خطاهای حلقه ـ نشانه در ردهٔ خطاهای مجزا قرار می‌گیرند. اگر که با نگاه به تحلیل‌گر بتوانید بگویید که NAUN مربوط به خطا از کدام آدرس MAC حادث شده است، تمام آن چیزی را که لازم است انجام دهید، پیداکردن آدرس MAC و خاموش‌کردن ماشین مربوطه است. به تکنیک تفرقه بینداز ـ و ـ حکومت‌کن نیازی نیست.

خطاهای مجزا عبارتند از :

- محدودکنندهٔ ناتمام
- خطای A/C
- خطای قطعی
- خطای داخلی
- خطای خط

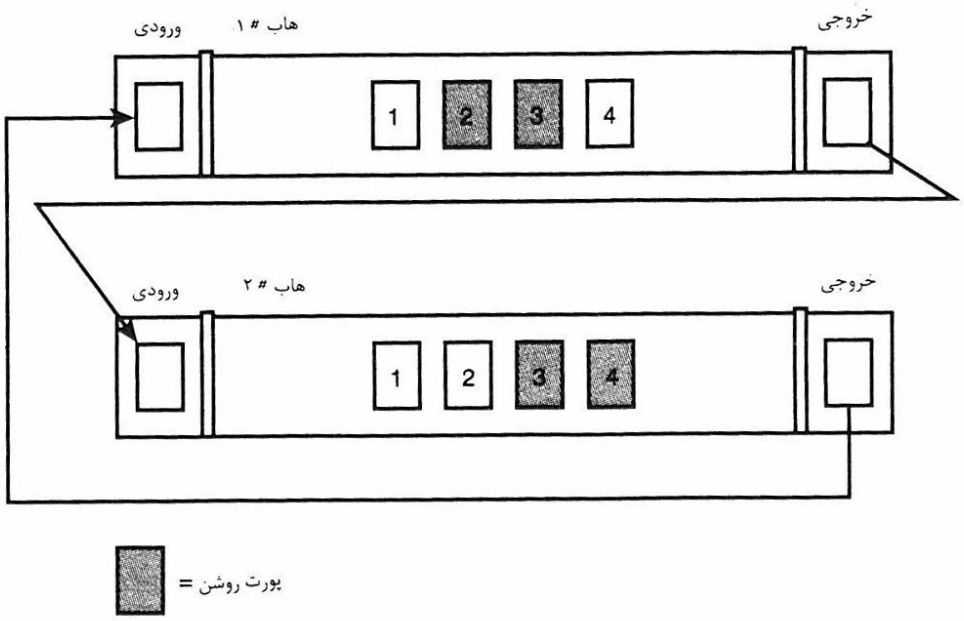
تمامی این خطاها به معنای آن است که ماشینی بیمار است و به کمک نیاز دارد. از آنجایی‌که علاقه‌ای ندارید که پزشک حلقه ـ نشانه باشید، بهترین کار آن است که NAUN را از شبکه خارج کنید و ببینید که آیا مشکلات حل می‌شوند یا خیر. از آن گذشته، ممکن است در یک بخش از شبکه، تحلیل‌گری را قرار نداده باشید تا هنگامی‌که به مشکلاتی برخورد می‌کنید ـ به بیان دیگر، بهتر است که بعد از تعیین موقعیت، دست به عمل بزنید. البته مد نظر داشته باشید که استفاده از تحلیل‌گر در حلقه ـ نشانه‌ای به ظاهر سالم، تعدادی خطا را نشان خواهد داد، بنابراین از این موضوع نهراسید.

هر ایستگاه که وارد مکالمه می‌شود یا از آن خارج می‌گردد، به‌صورت موقت حلقه را می‌شکند. این مسئله یک خطای قطعی نامیده می‌شود. ایستگاه همسایه که این موضوع را متوجه می‌شود، آن را به ناظر فعال مخابره می‌کند. این وضعیت در حلقه ـ نشانه، نظیر بروز تصادمها در اِترنت، امری معمول و عادی است. وقوع چند خطای قطعی در حلقه ـ نشانهٔ سالم امر مهمی نیست؛ این موضوع تنها نشاندهندهٔ آن است که شخصی دستگاه خود را خاموش یا روشن نموده است. اما اگر در یک فاصلهٔ زمانی کوتاه، با صدها مورد از این نوع خطا برخورد کنیم، آنگاه مشکلی وجود دارد. البته، لازم نیست در مورد تعداد کمی از این نوع خطاها نگران باشید.

خطاهای تراکم دریافت‌کننده، در صورتی‌که تعدادشان کم باشد نیز مشکلی خاص را نشان نمی‌دهد ـ تنها نشاندهندهٔ آن هستند که یکی از ایستگاههای‌کاری زمان سختی را سپری می‌کند. در صورت زیادبودن تعداد این خطاها بهتر است آنها را بررسی کنید، چرا که می‌تواند کارآیی کل شبکه را کاهش دهد. البته به‌صورت کلی تعداد کمی از این خطاها نشاندهندهٔ آن است که برخی از ایستگاههای‌کاری در همگامی با بقیه با مشکل مواجه هستند.

تحلیل‌گران نشانه

در صورت مجهزبودن به برنامهٔ تحلیل‌گر حلقه ـ نشانهٔ مناسب، پیداکردن NAUN کاری ساده است. در فصل ۲۰ با جزییات بیشتری مسئله را مطرح خواهم کرد، اما برای این‌جا، توجه داشته باشید که تحلیل‌گر مناسب می‌تواند فهرستی از NAUN ها ارائه کند که حاوی آدرس‌های MAC روی حلقه می‌باشد، آن هم به ترتیب درست! این وضعیت بسیار بهتر از اِترنِت است چرا که بلافاصله می‌توانید پیدا کنید که آدرس MAC مذکور به کدام پورت متصل شده است. در واقع، بسیاری از فروشندگان حلقه ـ نشانه برنامه‌ای را به شما نشان خواهند داد که این اطلاعات را به‌صورت رایگان برایتان جمع‌آوری می‌کند. برای ساده‌ترکردن اوضاع، اجازه بدهید فرض کنیم دو هاب را در یک بخش از شبکهٔ حلقه ـ نشانه متصل نموده‌اید (شکل ۳-۱۰).



شکل ۳-۱۰ : فهرست NAUN به این بستگی دارد که در لحظهٔ حاضر کدام ایستگاههای کاری در حلقه قرار گرفته‌اند.

دستگاه شما با برنامهٔ فهرست NAUN (که خوشبختانه علاوه بر آدرس MAC با اسم ایستگاههای‌کاری نیز کار می‌کنند) به هاب ۲، پورت شمارهٔ ۳ متصل شده است. فهرست NAUN شما در جدول ۱-۱۰ نشان داده شده است.

جدول ۱-۱۰ : فهرست NAUN

Order	Name	MAC
1	This_WORKSTATION	00-00-c9-88-54-22
2	MY-BOSS	00-00-c9-88-54-55
3	HER-BOSS	00-00-c9-88-54-d5
4	OUR-SERVER	00-00-c9-88-54-f9

۸ پورت ممکن در ۲ هاب ۴ پورته وجود دارند، اما تنها ۴ ایستگاه در فهرست ذکر شده‌اند. نگاهی سریع به هاب‌ها این موضوع را روشن می‌کند که تنها چهار چراغ از ۸ چراغ روشن شده‌اند. در وهلهٔ اول فهرست NAUN تنها مشخص می‌کند چه کسی در شبکه کار می‌کند. تولیدکنندهٔ این فهرست نمی‌تواند چیزی را که وجود ندارد، اعلام کند. در این‌جا باید سریع کار کنید و امیدوار باشید که قبل از آنکه کسی وارد شبکه شود یا از آن خارج گردد مشکل را شناسایی کنید. با نگاهی به هاب‌ها و چراغهای روی آنها که در فهرست NAUN ظاهر شده‌اند، درمی‌یابید از آنجا که ایستگاه‌کاری شما با فهرست‌کنندهٔ NAUN شمارهٔ ۱ در فهرست است و شمارهٔ ۳ مربوط به هاب است، آنگاه شمارهٔ ۴ در هاب دوم و HER-BOSS شمارهٔ دوم روی هاب اول می‌باشد و سرویس‌دهنده نیز شمارهٔ ۳ در هاب اول خواهد بود.

بیشتر اوقات من این‌کار را به‌منظور پیداکردن سریع ماشینی که می‌خواهم از شبکه خارج کنم، به انجام می‌رسانم. از آنجا که خیلی اوقات افراد در زمان نامعین و نامشخصی ممکن است به شبکه وارد یا خارج شوند نمی‌توان به این روش به‌عنوان سندی معتبر اتکا کرد. عدم توجه به این نکته ممکن است مدت طولانی شما را به اشتباه بیندازد.



نکته : *در صورت استفاده از تحلیل‌گری که طراحی آن بدون مد نظرداشتن عمل سوئیچینگ صورت گرفته است، استفاده نمایید، تعداد زیادی خطای «قاب کپی شد» دریافت می‌کنید. تحلیل‌گر با صدور این خطاها به شما می‌گوید که شخص دیگری ادعا دارد قاب را دریافت نماید اما به‌عنوان دریافت‌کننده مد نظر نبوده است.*

در واقع، از آنجا که سوئیچ دو حلقه ـ نشانهٔ مجزا را به هم متصل نموده است ایستگاه دریافت‌کننده نمی‌توانسته آن را بدون کمک سوئیچ دریافت کند. سوئیچ می‌بایست آن را به چنگ آورد. سوئیچ قاب را در شبکهٔ منبع دریافت می‌کند و آن را به شبکهٔ مقصد متفاوتی می‌فرستد که در آنجا ایستگاه‌کاری مقصد قاب را دریافت می‌کند. شبکهٔ مقصد، یک بخش حلقه ـ نشانهٔ فیزیکی مجزا می‌باشد که دارای تشکیلات مجزایی نظیر ناظر فعال است؛ مثل یک میز کنفرانس دیگر در اتاقی متفاوت. بنابراین مشکلی در ارتباط با به‌دست آوردن قاب توسط سوئیچ به منظور ارسال به مقصد وجود ندارد ـ در غیر این‌صورت هرگز به مقصد نمی‌رسید. به عبارت دیگر، تحلیل‌گر هیاهویی را به خاطر هیچ به راه می‌اندازد. سطر آخر این‌که: در چنین سناریویی نگران خطاهای «قاب کپی شد» نباشید.

دیدگاه فیزیکی

حلقه ـ نشانه نظیر اِترنِت، دارای قواعدی در مورد میزان طولانی‌بودن کابل‌هایی است که می‌توانند مورد استفاده قرار گیرند، همچنین در مورد نوع سیم و سرعت مورد استفاده محدودیتهایی وجود دارد. پرکاربردترین کابل مورد استفاده IBM نوع اول می‌باشد. کابل نوع اول زوج‌تافتهٔ محافظ دار (STP) بسیار محکم و نسبت به EMI (تداخل الکترومغناطیسی) مقاوم است اما کار با آن مشکل می‌باشد.

حلقه ـ نشانه را در دو پایهٔ سرعتی می‌توان مورد استفاده قرار داد: 4Mb و 16Mb. اگر استفاده‌کنندهٔ 4Mb هستید زمان آن فرا رسیده که آن را تغییر دهید. نمی‌توانم تصور کنم که در جایی از کارتهای حلقه ـ نشانه که با سرعت 16Mb کار می‌کنند، باشم و بدون خجالت تجهیزات مستعمل را خریداری نمایم! به‌منظور تشویق شما در حرکت به‌سوی 16Mb (و ساده نگه‌داشتن بحث) تنها در مورد قواعد به‌کار رفته در سرعت 16Mb صحبت خواهم نمود.

حلقه ـ نشانه قاعدهٔ سفت و سختی در مورد محدودیت طول کابل در هیچ‌یک از حالات اجرایی خود قائل نیست، به‌جای آن، یک محدوده برای طول کلی حلقه وجود دارد. اگر توجه کنید، از آنجا که تمامی کابل‌هایی که حلقه را می‌سازند، در محاسبهٔ طول مؤثرند، محاسبهٔ طول کلی حلقه کاری آسان خواهد بود.

هنگام استفاده از STP حداکثر طول حلقه می‌تواند ۱۸۰ متر، یا ۵۹۰ فوت باشد. این مقدار در هنگام استفاده از CAT-V UTP، ۱۰۰ متر یا ۳۳۰ فوت و درمورد CAT-III UTP ۷۰ متر یا ۲۲۰ فوت می‌باشد. این اعداد را فقط برای در دسترس قراردادن اطلاعات لازم، ذکر می‌کنم؛ تا هنگامی‌که طراحی حلقه ـ نشانه‌ها را شروع نکرده‌باشید، نیازی به این اعداد ندارید.

به‌منظور محاسبهٔ دقیق همخوانی حلقه با بودجهٔ کابلی، باید از فرمول پیچیده‌ای استفاده کنید (که باعث شد با نگاه‌کردن به آن سردرد بگیرم) که شامل طولانی‌ترین کابل مستقل، مسافت داخلی کابل مربوط به هر AMU در شبکه، کابل‌های داخلی MAU و ضرایب عجیب و غریب می‌باشد. کسانی که شبکه‌های حلقه ـ نشانه را طراحی می‌کنند باید از این فرمول سنگین استفاده کنند. خوشبختانه شما که می‌خواهید به عیب‌یابی شبکه‌های حلقه ـ نشانه

بپردازید کاری با چنین فرمولی ندارید.

در این‌جا هم نظیر اِترنِت، اگر شبکه‌تان مثل هفتهٔ قبل و هفته‌های قبل‌تر از آن کار نمی‌کند، و گردوخاک تمامی کابل‌ها را پوشانده، و کسی با کابل‌ها بازی نکرده، آخرین چیزی که باید مورد شک و ظن قرار دهید، آن است که مجموع طول کابل‌ها بیشتر از حد معتبرشان گردیده است. اگر از سوی دیگر، شخصی تعدادی MAU به شبکه اضافه کرده یا کابل طولانی‌تری را مورد استفاده قرار داده است و مشکلاتی بروز نموده‌اند، این بخشهای اضافی را باید قطع کنید و ببینید چه اتفاقی می‌افتد. برای انجام این‌کار به ریاضیات یا اندازه‌گیری نواری نیازی نیست. این‌کار تنها تغییری است که انجام آن ممکن است از اندازه‌گیری کابل‌ها، کابل‌هایی که در دیوارها و برای مدت طولانی مورد استفاده قرار گرفته‌اند، آسان‌تر است.

اندازهٔ بسته‌ها

بسته‌های حلقه ـ نشانه دارای اندازه‌های مختلفی هستند. اندازهٔ آنها ممکن است از 1KB تا 16KB متفاوت باشند که در این بین پرطرفدارترین اندازهٔ بسته که من با آن برخورد کرده‌ام 4KB می‌باشد. اندازهٔ بسته هر حلقه ـ نشانه مساوی کوچکترین اندازهٔ بسته مشخص‌شده در شبکه است ـ یعنی، شما می‌توانید به راحتی اندازهٔ بستهٔ مورد استفاده در حلقه ـ نشانه را با افزودن کارت شبکه‌ای که به‌منظور مورد استفاده قرار دادن اندازهٔ بستهٔ کوچکتری پیکربندی شده است، کاهش دهید.



نکته : *اگر شبکه‌ای گسترده یا حلقه ـ نشانه‌ای مخلوط با محیط اِترنِت دارا هستید، اندازهٔ بسته‌های بزرگ را باید مورد توجه قرار دهید. بسیاری از برنامه‌های TCP/IP (در واقع بیشتر از آنچه که فکر می‌کنید) قادر به عملکرد صحیح در مورد* قطعه‌قطعه‌سازی *نیستند. قطعه‌قطعه‌سازی چیزی است که هنگامی‌که می‌خواهید ۱۰ کیلو از یک ماده را در بسته‌های ۵ کیلویی جاسازی کنید رخ می‌دهد ـ بسته‌ها به قطعات کوچکتر و قابل مدیریت‌تری تقسیم می‌شوند. هنگام مورد استفاده قراردادن محیطی مخلوط، بسته‌ها به‌منظور تطابق با رابط‌هایی کوچکتر در مسیریاب، به قطعاتی تقسیم می‌شوند. می‌توانید با این موضوع از طریق مجبورکردن برنامه‌های کاربردی خود به استفاده از اندازه‌های کوچکتر بسته، برخورد کنید و یا این‌که می‌توانید اندازهٔ بستهٔ مورد استفاده در حلقه ـ نشانه را کاهش دهید. از سوی دیگر می‌توانید از فروشنده بخواهید این‌کار را برایتان انجام دهد؛ این موضوع به این بستگی دارد که آن روز چقدر بهینه فکر می‌کنید.*

خرابی

بیشتر حلقه ـ نشانه‌ها به‌خوبی کار خود را انجام می‌دهند. بیشترین مشکلات در ارتباط با این نوع از شبکه‌ها اغلب در انواع بزرگتر به‌وقوع می‌پیوندند، که در آنها کار بازیابی خطاها به‌خوبی صورت نمی‌پذیرد (با این‌که می‌توانید به‌صورت تئوری بیش از ۱۰۰ ایستگاه‌کاری را در یک حلقه ـ نشانهٔ منفرد قرار دهید، استفاده از بیش از ۶۰ دستگاه نوعی خودکشی محسوب می‌شود. و در این روزهای ارزانی تجهیزات سوئیچینگ، می‌توانید چندین بخش مجزا داشته باشید).

حلقهٔ خراب‌شده، معمولاً نتیجهٔ یکی از دلایل زیر است:

- علائم
- خطاهای زیاده‌روی

علامت، بیشتر اوقات، هنگامی اتفاق می‌افتد که سیگنالی در سیم از بین می‌رود. یعنی یک ایستگاه‌کاری به‌صورت صحیح و کامل از حلقه خارج نشده و هاب هنوز فکر می‌کند که ایستگاه به کار خود ادامه می‌دهد. از آنجا که ایستگاه‌کاری پاسخگو نیست (حالتی که در اثر خرابی NIC ممکن است به وجود بیاید)، همسایهٔ تحتانی آن از دست‌رفتن سیگنال را تشخیص داده و آن را مخابره می‌کند (این ایستگاه‌کاری می‌تواند هنوز با بخش تحتانی خود ارتباط داشته باشد با این‌که اطلاعات فوقانی قطع گردیده است).

ناظر فعال کار پاکسازی حلقه را شروع می‌کند (یا روکش‌کردن). اگر این‌کار مؤثر واقع نشد همسایهٔ تحتانی به خود می‌گوید «اگر اشکال به من مربوط باشد چطور؟» و به‌سرعت این موضوع را بررسی می‌کند. خودش را از حلقه خارج می‌کند، بررسی‌های خودآزما را انجام می‌دهد و مجدداً خود را وارد حلقه می‌کند. این سیکل ادامه می‌یابد تا مشکل از دست‌رفتن سیگنال تصحیح می‌شود.

خوشبختانه برنامه‌های نظارتی حلقه ـ نشانهٔ قابل اطمینانی دارید که می‌توانند وضعیت را از طریق NAUN ایستگاه مخابره نمایند. با مرور فهرست NAUN، ایستگاه‌کاری خراب را پیدا کرده، آن را از هاب منفصل نمایید تا مشکل برطرف گردد. آنگاه می‌توانید دلیل از دست‌رفتن سیگنال را به‌صورت متمرکز بررسی نمایید (اغلب کارت یا کابل خراب مقصر اینگونه مشکلات هستند). بسیاری اوقات این روالی است که باری عیب‌یابی علائم به‌کار می‌رود.

خطاهای زیاده‌روی بسیار نظیر روش فوق عیب‌یابی می‌گردد. با نگاه‌کردن به NAUN مربوط به ماشین مشکل‌زا و حذف آن از شبکه می‌توان مشکل را برطرف نمود. با این‌که مشکلات بسیاری را دیده‌ام که مسبب آنها راه‌اندازهای خراب بوده‌اند، اما می‌توانم بگویم بیشتر مشکلات از یک کارت، کابل یا هاب حادث می‌شود. اگر ناظر حلقه ـ نشانه ندارید (دوباره می‌گویم که برخی از فروشندگان، این‌گونه برنامه‌ها را به‌صورت رایگان در اختیار می‌گذارند ـ این یکی از مزایای حلقه ـ نشانه نسبت به اِترنِت است) یا به تحلیل‌گر شبکه مجهز نیستید (یا اگر تحلیل‌گرتان راهنمایی خاصی در این ارتباط نمی‌کند)، می‌توانید از روش تفرقه‌بیانداز ـ و ـ حکومت‌کن که تقریباً هر مشکلی را می‌تواند حل کند استفاده نمایید.

خلاصه

اگر کامپیوترهای مکینتاش و تکنولوژی بتاماکس را دوست دارید، شیفتهٔ حلقه ـ نشانه خواهید شد. حلقه ـ نشانه که از نقطه‌نظر فنی از اِترنِت برتر است، از لحاظ میزان کاربرد در جایگاه بعدی نسبت به اِترنِت قرار دارد. این تکنولوژی قادر است از STP و UTP استفاده نماید و با سرعت 16Mb کار نماید. شمای عبوردهی نشانه در این فن‌آوری برای اشتراک سیم بدان معنا است که تعداد افراد بیشتری می‌توانند به‌صورت کارآمد از یک سیم مشترک استفاده نمایند.

امکانات بازیابی خطا در حلقه ـ نشانه بسیار خوب کار می‌کند و در صورت عدم کارآیی آنها اطلاعات NAUN که توسط سربار حلقه ـ نشانه تولید می‌گردد عیب‌یابی پیداکردن ایستگاه‌کاری مشکل‌دار را آسان می‌کند.

کارگاه

پرسش و پاسخ

پرسش : جدی باشید و به این سؤال پاسخ دهید، کدامیک بهتر است؟ حلقه ـ نشانه یا اِترنِت؟
پاسخ : متأسفم. قادر به اقرار نیستم. آنها هر دو کار می‌کنند. افراد و اشخاص مختلف آنها را به منظورهای مختلف به کار می‌گیرند.

پرسش : آیا می‌توانم در صورتی که نخواهم حلقه‌ای را گسترش دهم، یکی از ایستگاههای کاری را به پورت ورودی حلقه یا خروجی حلقه متصل کنم؟
پاسخ : متأسفانه خیر. آنها تنها به منظور ذکرشده طراحی شده‌اند.

پرسش : چرا در MAU های حلقه ـ نشانهٔ قدیمی خود، یک صدای کلیک می‌شنوم؟
پاسخ : یک سولونئید فیزیکی به‌منظور توسعهٔ حلقه بسته می‌شود.

آزمون

۱- درست یا نادرست؟ خطاها بخشی عادی از عملکرد حلقه ـ نشانه هستند.

۲- NAUN چیست؟

الف ـ یک شخص، محل یا چیز دیگر
ب ـ شبکهٔ غیرعادی نزدیک
ج ـ نزدیک‌ترین آدرس همسایهٔ فوقانی
د ـ نزدیک‌ترین برنامهٔ کاربردی تحت مذاکره

۳- فوقانی بر کدام جهت دلالت دارد؟

الف ـ به سمت خارج هاب
د ـ به سمت داخل هاب
ج ـ به سمت پورت شمارهٔ ۳ هاب
د ـ به سمت خارج و داخل هاب

۴- هر بستهٔ حلقه ـ نشانه می‌تواند به کوچکی ـــــ کیلوبایت و به بزرگی ـــــ باشد.

الف ـ ۱، ۵
ب ـ ۴، ۱۰
ج ـ ۱، ۱۶
د ـ ۴، ۱۶

پاسخ به سؤالات آزمون

۱- درست
۲- ج
۳- ب
۴- ج

فصل ۱۱

مبانی شبکه در ویندوز

ویندوز میکروسافت، در ردهٔ سیستم‌های عامل رومیزی است که شبکه‌های نقطه‌به‌نقطه را پشتیبانی می‌کند. راه‌اندازی و گرداندن چنین شبکه‌ای آسان است. بسیاری از مفاهیم شبکه (و حتی بسیاری از دستورات) از یونیکس گرفته شده و در یک رابط کاربری گرافیکی با کاربردی آسان و زیبا بسته‌بندی شده و به شهر ارسال گردیده است.



یادداشت : *در این فصل ویندوز ۹۵، ویندوز ۹۸ و ویندوز NT مورد بحث قرار می‌گیرد. هنگامی‌که به ویندوز اشاره می‌کنم، منظورم 9x (ویندوز ۹۵ و ۹۸) و NT می‌باشد؛ جایی که بین مشخصات ویندوز 9x و NT تفاوت وجود داشته باشد، از الفاظ مربوطه استفاده خواهم نمود.*

کار را با تئوری پشت پردهٔ شبکه‌سازی مبتنی بر ویندوز شروع می‌کنم و در مورد تفاوتهای بین روشهای حوزه و گروههای کاری توضیح می‌دهم از آنجا که شبکه‌سازی TCP/IP در ویندوز اختلافات خاص خود را داراست، ابتدا به‌صورت خلاصه به شرح آن می‌پردازم و آنگاه به بررسی عناوینی نظیر پیکربندی‌های ایستگاه‌کاری و عیب‌یابی شبکهٔ توکار ویندوز و ابزار لازم برای مسلط‌شدن بر مشکلات خواهم پرداخت.

مفروض شده‌ها

NT 5.0 در راه بازار با تأخیر مواجه شده است، اما حتی در صورت رسیدن آن، پایه‌ای نظیر NT 4 خواهد داشت. از سوی دیگر با وجود کارآبودن NT 3.51 برنامه‌های کاربردی مدرن در آن اجرا نمی‌شوند و در نتیجه به‌عنوان بازیکنی جدی محسوب نمی‌شود. از سوی دیگر بهبودی‌های صورت‌پذیرفته از لحاظ قابلیت اطمینان و سرعت در ویندوز NT 4 نسبت به 3.51 استفاده از آن را به ارتقاء لازم تبدیل نموده است. اگر هنوز از ویندوز 3.x و DOS استفاده می‌کنید، خواهش می‌کنم دیگر این‌کار را نکنید!

چرا اینقدر نسبت به DOS و ویندوز 3.x متعصب هستید؟ برای من آنها نظیر خوابی وحشتناک هستند! راه‌اندازهای مقیم در حافظهٔ DOS که باید به‌صورت دستی در Config.sys و Autoexec.bat بارگذاری شوند؛ ناسازگاری‌هایی که روزانه پیش می‌آیند و مدیریت ضعیف حافظه همه مسائلی هستند که باید به‌عنوان قدیمی‌بودن این ترکیب ذکر گردند. همه چیز (و به‌خصوص شبکه‌سازی) بسیار ساده‌تر و مجتمع‌تر در ویندوزهای NT و 9.x گرد آمده‌اند. استفاده از این ابزار قدیمی تنها می‌تواند تمرینی در مازوخیسم (آزارطلبی) باشد.

بومی‌سازی

با این‌که ویندوز امکان پیوند با هر چیزی به غیر از ظرفشویی آشپزخانه را میسر ساخته است (و من شنیده‌ام که میکروسافت روی این موضوع کار می‌کند) ما در اینجا تنها روی ابزار شبکه‌سازی میکروسافت متمرکز خواهیم شد. اگر از تئوری شبکه‌سازی ویندوز آگاه باشید، بهتر خواهید توانست مشکل آن را هنگام عدم کارکرد حل کنید. هفت مؤلفه در شبکه‌سازی موفق ویندوز باید مد نظر قرار گیرند (به مرور در مورد آنها صحبت خواهم نمود):

- سرویس‌های نامگذاری (WINS، NetBIOS، DNS)
- سرویس‌های تصدیق‌گیری (حوزهٔ NT یا اشتراک در گروه کاری)
- سرویس‌های فایل و چاپ (SNB)
- سرویس‌های خاص پروتکل (WINS، DHCP)



یادداشت : *به مجموعهٔ شبکه‌ای میکروسافت برخی اوقات فایل و چاپ میکروسافت گفته می‌شود.*

همانگونه که انتظار دارید، اجرای یک شبکهٔ ویندوز ۹۵ نقطه ـ به ـ نقطه بسیار ساده‌تر از تنظیم یک شبکهٔ ویندوز NT در یک ناحیهٔ اتصالی گسترده می‌باشد؛ البته بلوک‌های ساختمانی مشابه هستند. اگر از شبکه‌سازی فایل و چاپ میکروسافت استفاده می‌کنید، کامپیوتر شما در واقع بخشی از یک گروه کاری یا حوزهٔ NT می‌باشد.

NetBEUI

ابتدا، نگاهی به NetBEUI خواهیم داشت که به‌صورت خلاصه در فصل اول مورد بحث قرار گرفت. NetBEUI یک پروتکل غیرقابل مسیریابی است که در بالای خود NetBIOS را اجرا می‌کند؛ تصور کنید که NetBEUI زبان محلی یا بومی NetBIOS می‌باشد. این روشی است که پیغام NetBIOS به سادگی بسته‌بندی شده و از طریق سیم تحویل داده می‌شود. نقطه‌ضعف NetBEUI آن است که به‌خاطر سادگی بر پایهٔ انتشارهای شبکه‌ای به‌منظور دریافت اطلاعات اتکا می‌نماید.

هر انتشار، هنگامی رخ می‌دهد که یک گره از شبکه اطلاعاتی را به تمامی گره‌های دیگر در یک بخش از شبکه ارسال می‌کند، که این به طرزی آشکار باعث ترافیک زیادی در شبکه می‌گردد. این‌کار به این دلیل صورت می‌گیرد که ردیابی تمامی گره‌های شبکه کاری مشکل است ـ اگر برای یکی از ایستگاهها تفاوتی نکند که با چه کسی صحبت می‌کند، باید روشی در شبکه وجود داشته باشد که بتوان رد افراد موجود در شبکه را پیگیری نمود و نگه‌داشت. از آنجا که NetBEUI پروتکلی ساده است، از ساده‌ترین شکل استفاده می‌کند و ما نگاهی به روش صحبت‌کردن NetBEUI خواهیم داشت.



نکته : *ایراد استفاده‌نکردن از NetBEUI آن است که پیکربندی TCP/IP مشکل است و IPX/SPX به‌صورت کامل توسط میکروسافت پشتیبانی نمی‌شود (وجود IPX/SPX در ویندوز تنها به‌خاطر ایجاد سازگاری با شبکه‌های ناول است). NetBEUI در بسیاری از شبکه‌های کوچک به‌خوبی کار می‌کند ـ در واقع اگر تعداد PCها کم باشد به‌خاطر عدم وجود سربار برای مسیریابی، سریعتر از TCP/IP کار می‌کند. از سوی دیگر برای استفاده از ۳۰ تا ۵۰ ایستگاه‌کاری بهتر است کارهای اضافی مربوط به پیکربندی TCP/IP را پذیرا شویم.*

اگر شبکهٔ بزرگتری دارید، واقعاً بهتر است که از NetBEUI استفاده نکنید. عمل انتشار در حجم نسبتاً بالا باعث ضعف در شبکه شده طوفانهای انتشاری را ایجاد می‌کنند (یعنی یک ایستگاه‌کاری انتشاری را صورت می‌دهد که باعث می‌شود دیگر ایستگاههای کاری نیز به انتشار اطلاعات بپردازند). در مقیاسی بزرگ، این موضوع باعث ایجاد ترافیک غیرلازم در شبکه می‌شود که ممکن است فعالیت شبکه را متوقف نماید. اگر برخی اوقات در شبکهٔ نسبتاً بزرگ NetBEUI خود با مشکلات توقف و قفل‌کردن دستگاهها مواجه می‌شوید، ممکن است وقوع چنین حالاتی به دلیل حادث‌شدن طوفانهای انتشاری باشند.

NetBIOS

NetBIOS (سیستم ورودی/خروجی پایهٔ شبکه) سرویس‌های نام و سرویس‌های جلسه برای برنامه‌های اشتراک فایل و چاپ بین دو کامپیوتر را فراهم می‌آورد. ویندوز می‌تواند از پروتکل غیر قابل مسیریابی NetBEUI برای حمل NetBIOS از دستگاهی به دستگاه دیگر استفاده کند؛ به طرز مشابهی می‌توان از TCP/IP یا IPX/SPX در محیطی باقابلیت مسیریابی استفاده نمود.

به‌طور مشخص‌تر، NetBIOS سرویس‌های نام برای سرویس‌های چاپ و فایل میکروسافت (و IBM) را به انجام می‌رسانند. کار دیگر آن حمل پیغامها برای گروههای کاری در شبکه و حصول اطمینان از عدم وجود اسامی تکراری ایستگاه‌کاری در گروه کاری و حوزه می‌باشد.

یک نوع خطای NetBIOS بسیار معمول است، این خطا هنگامی اتفاق می‌افتد که تکنسینی محتویات یک دیسک سخت سالم را روی دیسک سخت مشکل‌زایی کپی می‌کند و ایستگاه‌کاری مشکل‌زا را راه‌اندازی مجدد می‌نماید. بلافاصله، او با این خطای ویندوز که در واقع پیغام خطایی مربوط به NetBIOS است مواجه می‌شود.

```
Err 38: The Computer name you specified is already in use on the network, To specify a different name, double name, double-click the Network icon in Control Panel.
```

NetBIOS در مورد وجود اسم از شبکه پرس‌وجو نموده و در حقیقت این اسم وجود داشته است. البته تکنسین مذکور می‌تواند به راحتی به Control Panel مراجعه کند، برگهٔ Identification را انتخاب و اسم PC را به منظور رفع این مشکل تغییر دهد. این موضوع هنگامی‌که دو نفر در ایستگاه‌کاری خود اسم یکسانی را انتخاب کنند به‌وقوع می‌پیوندد. از آنجا که اسم انتخابی برای PC اهمیت چندانی ندارد، با مشاهدهٔ این خطا کافی است به سادگی اسم متفاوتی را انتخاب نمایید.

مرور

آیا خود پروتکل می‌تواند کار ایجاد گروههای کاری را به انجام برساند؟ خیر، این وظیفه مستلزم وجود یک برنامهٔ سرویس‌دهنده است که در سمت دیگر خط قرار دارد. باید بدانید که مکانیزمی به نام مرور، به عنوان بخشی از سیستم شبکه‌ای گروه کاری یا حوزه وجود دارد.

سیستم مرور از یک کارفرمای مرور، مرورگرهای پشتیبان و کامپیوترهای سرویس‌گیرنده تشکیل شده است. هر کامپیوتر سرویس‌گیرنده می‌تواند اطلاعاتی را در مورد منابع شبکه دریافت کند، اینکه آیا منابع سرویس‌دهنده، گروه کاری، حوزهٔ NT و نظایر آن هستند یا خیر. برای مثال، هنگامی که روی شمایل Network Neighborhood کلیک کنید، فهرست کامپیوتری که مشاهده می‌کنید از کارفرمای مرور مربوط به گروه کاری یا حوزه مربوطه دریافت می‌شود. همان گونه که مشاهده می‌کنید، مرور امر کاملاً مهمی است ـ اگر نتوانید منبعی را مشاهده کنید، نمی‌توانید آن را به‌کار ببندید.



نکته : هر کامپیوتر ویندوز ۹۵ تنها در صورت کارکرد به صورت سرویس‌دهنده در فهرست مرور ظاهر خواهد شد. برای آنکه کامپیوتر ویندوز ۹۵ شما نظیر یک سرویس‌دهنده عمل نماید، مراحل زیر را انجام دهید:

۱- *Control Panel* ویندوز را از طریق کلیک‌کردن روی *Start|Settings|Control Panel* باز کنید.
۲- روی شمایل *Network* کلیک کنید.
۳- روی *Add* کلیک کنید.
۴- *Service* را انتخاب نمایید.
۵- روی *Microsoft* کلیک کنید و آنگاه گزینهٔ *File and Printer Sharing for Microsoft Networks* را برگزینید.
۶- در صورت اعلام، *CD-ROM* ویندوز را وارد نموده و در صورت درخواست سیستم را راه‌اندازی مجدد نمایید.



یادداشت : یکبار موردی را مشاهده کردم که کاربری به هیچ وجه نمی‌توانست سایر افراد گروه کاری‌اش را مرور نماید. بعد از وارسی کارت شبکه و کابل و رسیدن به این نتیجه که هیچ چیز خراب نیست، به این نتیجه رسیدیم که بهتر است ویندوز را مجدداً نصب نماییم ـ مشکل را تا حدودی به سیستم عامل مربوط می‌دانستیم. قبل از انجام این کار، دوباره *Control Panel* را بررسی نمودیم؛ این بار، متوجه شدیم که جلوی اسم گروه کاری یک جای خالی (*Space*) قرار گرفته است. با برداشتن این جای خالی توانستیم تمامی افراد را در شبکه مرور نماییم.
موردی را به خاطر می‌آورم که در آن اسم یک گروه کاری به جای *B&O*، به صورت اشتباه *B&0* وارد شده است (صفر به جای حرف *O*). باید سعی کنید مواظب چنین اسامی گروههای کاری اشتباه باشید.



نکته : کارفرمای مرور مربوط به حوزهٔ *NT* همیشه سرویس‌دهندهٔ *NT* است که به عنوان کنترل‌کنندهٔ اولیهٔ حوزه (*PDC*) کار می‌کند.



نکته : با اینکه حوزهٔ *NT* می‌تواند در سراسر زیرشبکه‌ها (یعنی از طریق یک مسیریاب) وجود داشته باشد، گروههای کاری این امکان را در اختیار نمی‌گذارند. به جای آن، گروه کاری در دو بخش مختلف شبکه، دوبار وجود دارد، هریک دارای کارفرمای مرور و فهرست مرور خود می‌باشد. این بدان معناست که کارفرمای مرور در شبکه *A* چیزی در مورد فهرست مرور موجود در شبکهٔ *B* نمی‌داند. کامپیوترهای موجود در بخش *A*، قادر نخواهند بود در *Network Neighborhood* خود، کامپیوترهای بخش *B* را مشاهده کنند و برعکس.

کارفرمای پیمایش مربوط به گروه کاری یا حوزه، ماشینی است که مسؤولیت نگهداری از فهرست ایستگاههای کاری شرکت‌کننده را برعهده دارد. اگر کارفرمای پیمایش گروه کاری را ترک کند، مرورگر دیگری از فهرست مرورگرهای پشتیبان باید کار را برعهده گیرد. اهمیت این موضوع تنها به این دلیل است که از لحاظ منطقی کارفرماهای مرور ضعیف باعث اخلال در شبکه‌های ویندوز شده و باعث بروز مشکلاتی می‌شود. همچنین اگر یک ایستگاه‌کاری ادعا کند که کارفرمای مرور است آن هم در زمانی که چنین نیست، این موضوع نیز می‌تواند سرمنشأ مشکلاتی باشد.

بعد از آنکه اسامی ایجاد و گروههای کاری به یکدیگر متصل شدند، اشتراک فایل و چاپ در ویندوز از طریق مکانیزمی به نام بلوک پیغام سرویس دهنده[1]، یا SMB اتفاق می‌افتد. SMB یکی از امکانات موجود در NT و ویندوز 9x می‌باشد، اما با نگارش‌های متفاوت. برنامهٔ سرویس‌دهندهٔ SMB، مسؤولیت ایجاد امکان اشتراک بین کامپیوترهای PC را برعهده دارد. به همین صورت، برنامهٔ سرویس‌گیرندهٔ SMB در هر کامپیوتر سرویس‌گیرنده، این امکان را فراهم می‌کند که بتوان از فایل‌ها و چاپگرهای پیشنهادی SMB موجود در سرویس‌دهنده استفاده نمود. SMB و NetBIOS در ریشه به هم می‌پیوندند ـ برای مثال، SMB برای تحلیل نام خود از NetBIOS استفاده می‌کند. نمی‌توان SMB را بدون استفاده از NetBIOS اجرا نمود.



***یادداشت** : در حقیقت، توانایی‌های چندزبانهٔ شبکه‌ای میکروسافت، بر پایهٔ این حقیقت استوار شده‌اند که TCP/IP و IPX/SPX ویژگی حمل NetBIOS را به همراه دارند. اگر از طریق Control Panel آن را غیرفعال کنید، باید با فایل و چاپ میکروسافت خداحافظی نمایید (البته به غیر از حالتی که NetBEUI را نصب نموده باشید).*

SMB ترکیب ساده‌ای دارد و به ندرت خراب می‌شود. مشکلات مربوط به SMB اغلب در مشکلات پروتکل، سرویس نام، WINS، DHCP و مشکلات امنیتی حوزه نهفته‌اند.

حوزهٔ بزرگ

پروتکل سادهٔ SMB همیشه به عنوان پروتکلیب ناامن و ضعیف دیده شده است. این باعث شد که میکروسافت از یک مدل امنیتی جدید به نام مدل امنیتی حوزه استفاده نمود. این مدل بر پایهٔ یک یا چند سرویس‌دهنده که از یک پایگاه اطلاعاتی مشترک حاوی اسامی کاربران و رمز عبور آنها تشکیل شده است، می‌باشد.

می‌توانم تصور کنم که ابروهایتان بالا می‌رود. فکر می‌کنید، «اشتراکی؟ آیا این واقعاً ناامن نیست؟». به جز موردی که مربوط به مسائل نظامی است، امنیت حوزه، کار خود را به خوبی انجام می‌دهد. میکروسافت از تکنولوژی‌های رمزگذاری نسبتاً خوبی استفاده می‌کند که افراد معمولی نمی‌توانند از آن گذر کنند؛ خوبی قضیه در اینجا آن است که اگر یکی از سرویس‌دهنده‌ها خراب شود، بقیه می‌توانند وارد شبکه شوند. از آن گذشته از آنجا که مدل حوزه، اسامی کاربران و رمز عبور آنان را در چندین سرویس‌دهنده به اشتراک می‌گذارد، می‌توانید از دردسرهای مدیریت شبکه هنگام افزودن کاربران جدید به آن اجتناب کنید.

هر حوزهٔ NT باید به یک سرویس‌دهندهٔ NT مجهز باشد که به عنوان کنترل‌کنندهٔ اولیه حوزه عمل نماید. این سرویس‌دهنده ممکن است دارای چندین کنترل‌کنندهٔ پشتیبان حوزه باشد که سرویس‌های تصدیق‌گیری را هنگامی که PDC فعال و مرتب است به انجام می‌رسانند و در صورت خرابی PDC کل امور را به عهده می‌گیرند.



***یادداشت** : حوزهٔ NT همان گونه که در فصل ۱ تعریف کردم، یک سرویس فهرست نیست (در مورد سرویس‌های فهرست در فصل ۱۳ بیشتر صحبت خواهد شد). حوزهٔ NT به راستی قابل قیاس با فهرست نیست و از طرف دیگر چیزی بیشتر از اسامی کاربران، رمز عبور آنها، گروههای امنیتی، و*

1- Server Message Block

اطلاعات پایه در مورد ماهیت کاربر را دربر ندارد. میکروسافت قول فهرست واقعی (به نام فهرست فعال[1]) را در ویندوز NT نگارش ۵ داده است. مطمئن هستم که فهرست فعال چیزی خارق‌العاده خواهد بود، اما مطمئن باشید که قبل از نصب آن در شبکهٔ فعال خود، از شش تا ۱۲ ماه صبر خواهم نمود.

کشتی‌گرفتن با ایستگاه‌کاری

اگر از ایستگاه‌کاری NT استفاده می‌کنید، توجه داشته باشید که شبکه‌سازی با سرویس‌دهندهٔ NT، قدری با این کار در مورد کاربران ویندوز 9x متفاوت است. در مدل امنیتی حوزه، مفهومی به نام ایستگاه کاری امن وجود دارد؛ هر ایستگاه‌کاری NT باید با استفاده از مجموعه‌ای از استوارنامه‌های مدیریتی قبل از آنکه بتواند در اشتراک چاپ و فایل شرکت کند، به ثبت برسد. ماشینهای ویندوز 9x، ماشینهای امنی محسوب نمی‌شوند و بنابراین نیاز به ثبت آنها وجود ندارد.

SIDها و شما

هنگام نصب NT، فرآیند نصب یک شمارهٔ شناسایی امنیتی[2] (SID) منحصربفرد ایجاد می‌کند. این مقدار را می‌توان اعلان امنی از موجودیت ایستگاه‌کاری دانست، چرا که به صورت تصادفی ایجاد می‌شود و میلیاردها مقدار ممکن از آن وجود دارند.

در ایستگاه‌کاری NT، از این SID به عنوان نقطهٔ آغازین تولید اعداد شناسایی منحصر به فرد مربوط به کاربران، گروهها و نظایر آنها که در ایستگاه‌کاری جای می‌گیرند، استفاده می‌گردد. در سرویس‌دهندهٔ NT این SID وظیفه‌ای بیش از SID یک ماشین بر عهده می‌گیرد؛ در واقع این مقدار *SID* حوزه می‌باشد و به منظور تولید اعداد مربوط به اشیاء تمامی حوزه به‌کار می‌رود.

هنگامی که یک حساب کامپیوتری ایستگاه‌کاری NT ایجاد می‌کنید، کنترل‌کنندهٔ حوزه بر مبنای SID حوزه، یک شمارهٔ شناسایی برای ایستگاه‌کاری ایجاد می‌کند. کنترل‌کنندهٔ حوزه کانالی رمزگذاری‌شده و امن با ایستگاه‌کاری ایجاد می‌کنند که بر مبنای یک رمز عبور اشتراکی قرار دارد.

اگر اسم کامپیوتر را عوض کنیم، کامپیوتر شما دیگر همان کامپیوتری که به پایگاه اطلاعاتی حوزه اضافه شده بود نمی‌باشد و قادر به دسترسی به حوزه نخواهد بود. باید کامپیوتر را با استفاده از ابزار Server Manager از پایگاه اطلاعاتی حوزه پاک کنید و آنگاه دوباره کامپیوتر را تعریف کنید.این موضوع آسیبی به جایی نمی‌رساند اما مستلزم انجام کار بیشتر توسط شماست.

مسائل SID هنگام استفاده از گردونه‌های تکراری برای نصب ویندوز NT پیش می‌آیند ـ SID شما نباید در دو ایستگاه‌کاری NT یکی باشد. فصل ۱۶ را برای دریافت اطلاعات و جزییات بیشتر ملاحظه کنید.

بخشی از مفهوم نهفته در ایستگاه‌کاری امن NT این دیدگاه است که نمی‌توانید قبل از شناساندن خود، به یک ایستگاه‌کاری مشخص دسترسی داشته باشید. اشکال این روش در آن است که دسترسی به ایستگاه‌کاری در صورت

1- Active Directory 2- security identification number

خرابی شبکه ناممکن خواهد بود. برای مثال، فرض کنید که نمی‌توانید به خاطر خرابی مسیریابی که بین شما و سرویس‌دهندهٔ NT قرار دارد، به آن متصل شوید. به هیچ روشی قادر نخواهید بود تصدیق اعتبار خود را دریافت کنید، درنتیجه امکان ارتباط با ایستگاه‌کاری را نخواهید داشت و حتی نمی‌توانید به صورت محلی کار خود را انجام دهید (نمی‌توانید به سادگی از اعلان ورود به سیستم نظیر آن کاری که در ماشین ویندوز ۹۵ می‌کنید، رد شوید؛ لازم است که روال ورود به سیستم را صورت دهید). خوشبختانه، از آنجا که یک کپی از اطلاعات حوزه که برای آخرین بار مورد استفاده قرار گرفته روی گردونهٔ دیسک سخت ذخیره می‌شود، می‌توانید تصدیق ورود به ایستگاه‌کاری را دریافت نمایید. کاربرانی که از بیش از یک ایستگاه‌کاری استفاده می‌کنند، چنین مشکلاتی را تجربه نموده‌اند.

کاربری را به خاطر می‌آورم که رمز عبور خود در حوزه را عوض نمود و به محل دیگری رفت که مشکل شبکه‌ای در آن وجود داشت و طبیعی بود که نمی‌توانست وارد سیستم شود. مشکل چیست؟ روز قبل وی رمز عبورش را تغییر داده بود و ایستگاه‌کاری دوم مورد استفاده وی هنوز چیزی در مورد این تغییر نمی‌دانست. راه حل؟ از رمز عبور قدیمی خود استفاده نمود و به خوبی کار خود را انجام داد.



***نکته** : بسیاری از سازندگان ویندوز NT را بدون رمز عبور سرپرست ارائه می‌کنند. اگر به علت عدم توانایی در ارتباط با حوزه نمی‌توانید به ایستگاه‌کاری خود متصل شوید، می‌توانید همواره با استفاده از اسم کاربری Administrator و بدون رمز عبور وارد سیستم شوید. این کار بیش از آنچه که فکر می‌کنید مؤثر واقع می‌شود. چه ایستگاههای کاری امنی!*

موضوع اطمینان

از آنجا که حوزه‌های NT در واقع سرویس فهرست نیستند، باید راهی وجود داشته باشد که کاربر بتواند منابع مربوط به حوزهٔ NT دیگر را مورد استفاده قرار دهد. مکانیزمی که امکان استفادهٔ کاربران یک حوزه از منابع حوزهٔ دیگر را فراهم می‌آورد اطمینان نام دارد. ارتباط اطمینان ممکن است رابطه‌ای یکطرفه یا دوطرفه باشد.

فرض کنید که رئیس‌تان دسترسی به کابینت فایل‌های مربوط به حقوق کارمندان را در اختیارتان می‌گذارد. او به شما اطمینان کرده و می‌دانسته که از این طریق، فهرست دستمزدها در تمام شهر پخش نخواهد شد. به طور مشابهی شما هم به رئیس خود اطمینان دارید که وی اضافه‌کار شما را به خوبی پرداخت خواهد کرد. این یک ارتباط اطمینان دوطرفه است. از سوی دیگر فرزند کوچکتان به شما اطمینان دارد که غذای روی میز همیشه فراهم خواهد بود. اما شما اطمینان نمی‌کنید که فرزند شش‌ساله‌تان از برادر دوساله‌اش نگهداری کند. ممکن است در بازی آن روزش، وی بخواهد غذای کودک را با غذای سگ نگهبان منزل عوض کند. این موارد، مثالهایی از ارتباط اطمینان یکطرفه می‌باشد.

به طرز مشابهی در مورد اطمینان در حوزهٔ NT تصمیم‌گیری می‌کنید. اگر که می‌خواهید کارمندان حوزه A به منابع حوزه B دسترسی داشته باشند، اما نه برعکس، یک ارتباط اطمینان بین حوزهٔ A و B ایجاد می‌کنید. این حالت را با عبارات A مورد اطمینان B واقع شد و یا B به A اطمینان می‌کند، بیان می‌داریم.

اگر یکی از افراد در حوزهٔ B نتواند به منبعی (یک اشتراک یا یک چاپگر) در یکی دیگر از حوزه‌های NT مثل حوزهٔ A دسترسی پیدا کند، بهتر است ارتباط اطمینان را وارسی نماییم. باید مطمئن شوید که حوزهٔ فراهم‌آورندهٔ منبع اطمینان دارد و حوزه‌ای که به منبع نیاز دارد، مورد اطمینان است. مراحل زیر را دنبال نمایید:

۱- به سرویس‌دهندهٔ NT مربوط به حوزه‌ای که منابع را در اختیار دارد (حوزهٔ A) مراجعه کنید.

۲- از منوی Start، گزینهٔ Programs|Administrative Tools|User Manager for Domains را انتخاب نمایید.

۳- از منوی Policies در User Manager، گزینهٔ Trust Relationships را انتخاب کنید.
۴- حوزهٔ دیگر (حوزهٔ B) باید در فهرست به شکل *trusted* ظاهر شده باشد.
۵- به سرویس‌دهندهٔ NT در حوزهٔ اطمینان‌شده بروید.
۶- مجدداً لازم است ارتباطات اطمینان را با استفاده از User Manger بازرسی نمایید.
۷- حوزهٔ اول (حوزهٔ A) باید در فهرست به شکل *trusting* ظاهر شده باشد.

هنگامی، در جایی لازم داشتیم که ارتباط اطمینان دوطرفه‌ای را بین دو حوزه از طریق یک پیوند راه دور ایجاد کنیم. با وجود درستی نحوه ایجاد ارتباط اطمینان، به نظر می‌رسید که به درستی کار نمی‌کنند. سرپرست سیستم هنگامی که تلاش می‌کرد از راه دور به حوزهٔ دیگر دسترسی داشته باشد پیغام زیر را دریافت می‌نمود.

```
There are no logon servers available to service the logon request
```

نکته در اینجا بود که از آنجا که این حوزه‌ها به صورت راه دور به همدیگر متصل شده بودند، روی TCP/IP به عنوان پروتکل ارتباطی اتکا می‌نمودند. بنابراین به منظور انجام سرویس‌های نام از WINS استفاده می‌کردند. WINS به صورت مناسبی پیکربندی نشده بود؛ جستجویی سریع در TechNet کار لازم را آشکار ساخت. با به پایان‌بردن پیکربندی دوبارهٔ WINS بین دو حوزه و حصول اطمینان از کارکرد صحیح آن، مشکل اولیه نیز از بین رفت (در بخش بعدی TCP/IP و WINS را با جزییات بیشتری مورد بحث قرار خواهم داد).

سنگ‌نبشته‌های TCP/IP

دست‌نبشته‌های روی دیوارها حاکی از آن هستند که توابع ویندوز بیشتر و بیشتری بر TCP/IP مبتنی خواهند بود، بخصوص در WAN ها. بر این اساس، ممکن است که بخواهید با مفاهیم مختلف TCP/IP و دستوراتی که در آن وجود دارند، هم تحت ویندوز و هم به همراه سایر سیستم‌های عامل دیگر آشنا شوید. در این بخش، نگاهی به برنامه‌های سرویس‌دهنده که زندگی شما را به عنوان عیب‌یاب و سرپرست نیمه‌وقت شبکه را به آسانترین شکل ممکن میسر می‌سازند. نگاهی، خواهیم داشت. در این راستا نگاهی ویژه‌ای به پیکربندی خودکار شبکه خواهیم داشت. این بررسی را با DHCP شروع خواهیم نمود که به صورت خودکار آدرس‌های ایستگاههای کاری را به جای تخصیص آدرس برای هر ایستگاه توسط شما، به انجام می‌رساند. آنگاه تحلیل نام شبکه در ویندوز را بررسی خواهیم نمود.

DHCP

DHCP (پروتکل پیکربندی پویای میزبان)[1] یکی از مهمترین فن‌آوریهای به کاررفته در TCP/IP از زمان شکوفایی آن در سالهای گذشته به شمار می‌رود. DHCP این امکان را به‌وجود می‌آورد که هر ایستگاه‌کاری TCP/IP با شروع هر جلسه کاری، یکبار پیغامی را منتشر کند و به صورت خودکار آدرس و سایر اطلاعات را از سرویس‌دهندهٔ DHCP به‌دست آورد.

1- Dynamic Host Configuration Protocol

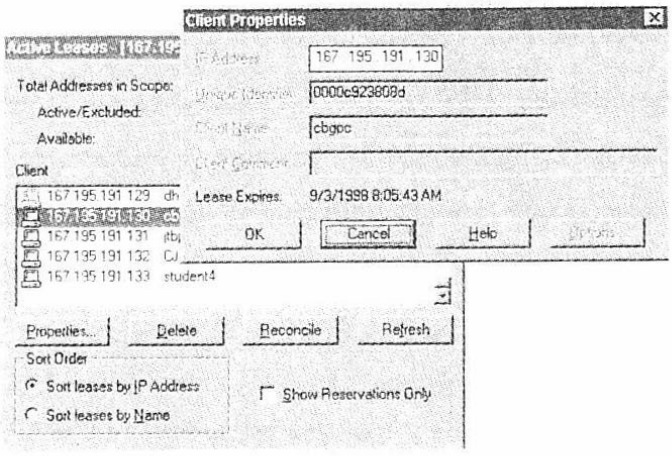
در حقیقت، روش کار به این صورت است که ایستگاه‌کاری‌ای که فاقد اطلاعات TCP/IP لازم است، باید پیغامی را در سطح کل آن بخش از شبکه منتشر کند تا از سرویس‌دهنده یک آدرس TCP/IP را اجاره نماید («سلام بر همه، من به یک آدرس IP نیاز دارم، لطفاً»). هنگامی که اجارهٔ آدرس به اتمام می‌رسد، انتشاری دوباره لازم است تا اجاره‌نامه تجدید گردد. مدت زمان اجاره در DHCP در سرویس‌دهنده قابل پیکربندی است. علاوه بر آن میدان DHCP ـ یعنی گستره‌ای از آدرس‌ها که می‌توانند به ماشینهای سرویس‌گیرنده تخصیص داده شوند ـ را نیز پیکربندی و تنظیم نمود (برای مثال، یک میدان نمونه در شبکهٔ 192.168.1 ممکن است از 192.168.1.10 تا 192.168.1.50 برای یک شبکه ۴۰ کاربره باشد). ردیابی و نگهداری از آدرس‌های IP با استفاده از DHCP بسیار آسانتر از تخصیص آدرس به هر ایستگاه می‌باشد. من در عمل مشاهده نموده‌ام که DHCP به صورت کاملاً جدی تعداد آدرس‌های IP تکراری در شبکه را کم می‌کند و در نتیجه تعداد مشکلاتی که شما با آن سروکار خواهید داشت نیز کاهش می‌یابد.



***نکته** : از آنجا که یکی از نقاط قوت DHCP آن است که امکان تعویض تعداد زیادی آدرس IP مربوط به ایستگاههای کاری را در اختیار می‌گذارد، بهتر است طول اجاره را به اندازه کافی کوتاه انتخاب کنید تا بتوانید از تغییرات پیکربندی پایان هفته استفاده نمایید ـ یعنی بهتر است طول اجاره بیشتر از یک یا دو روز نباشد.*

DHCP در کاربرد مؤثر و منطقی TCP/IP برای فایل و چاپ میکروسافت حیاتی است. در واقع، این گزینه را در اختیار دارید که ایستگاههای کاری بسازید که از TCP/IP برای تحلیل نام NetBIOS و مرور گره‌های غیر انتشاری استفاده می‌کنند.

می‌توانید ایستگاههای کاری در میدان DHCP را به صورت نقطه‌به‌نقطه و غیر انتشاری (یا گره‌های p)، گره‌های انتشاری (گره‌های b) یا گره‌های هیبرید (گره‌های h ـ یا گرهٔ نوع 0x8 که در شکل ۱-۱۱ نشان داده شده است)، پیکربندی کنید. گره‌های اخیر ابتدا سعی می‌کنند به صورت مستقیم ارتباط برقرار کنند و اگر موفق به این کار نشدند، انتشار را صورت می‌دهند. نکته در اینجا آن است که به منظور دستیابی به سرویس‌دهندهٔ DHCP باید از ویندوز NT استفاده نماییم؛ سرویس‌دهندهٔ DHCP برای گروههای کاری وجود ندارد.



شکل ۱-۱۱ : مدیر DHCP می‌تواند وضعیت اجارهٔ تمامی سرویس‌گیرنده‌ها را نشان دهد و بنابراین این امکان را فراهم می‌سازد که بتوانید به سادگی مشخص کنید کدامیک از کاربران، چه آدرس‌های IP را در اختیار دارد.

DHCP پتانسیل توزیع خودکار اقلام پیکربندی متعددی را دارا می‌باشد که یکی از آنها آدرس WINS و/یا آدرس سرویس‌دهنده DNS شبکه (بخش «تحلیل نام در TCP/IP» که در ادامهٔ این فصل آمده است را ملاحظه نمایید) می‌باشد. می‌توانید مطمئن باشید که اگر یک ایستگاه‌کاری اطلاعات DNS و WINS صحیح را در اختیار داشته باشد، این وضع در مورد همگی صدق می‌کند (که این وضعیت خیلی بهتر از درماندگی حاصل از تغییر ناخواسته اطلاعات DNS یا WINS توسط یکی از کاربران می‌باشد). این وضعیت هنگام عیب‌یابی زمان زیادی را صرفه‌جویی می‌کند.

خوب، همه چیز خارق‌العاده به نظر می‌رسد اما چه اتفاقی می‌افتد اگر سرویس‌دهنده DHCP خراب شود؟ در یک شبکه کوچک که سرویس‌دهندهٔ شبکه خود سرویس‌دهندهٔ DHCP نیز می‌باشد، این موضوع برای دوره‌های زمانی کوتاه اهمیتی ندارد. مفهوم اجاره‌های DHCP بدان معناست که در صورت خرابی سرویس‌دهندهٔ مربوطه، افرادی که از این سرویس استفاده می‌کنند حتی بدون سرویس‌دهنده آدرس‌های IP را در اختیار دارند (البته کاملاً محتمل است که این وضعیت آنها را دچار دردسر کند چرا که فایل‌هایشان روی سرویس‌دهنده قرار دارند).

افرادی که از ماسک زیرشبکه 255.255.255 استفاده می‌کنند اغلب دو سرویس‌دهندهٔ DHCP دارند، چرا که چنین شبکه‌ای به نسبت بزرگ است (کمتر از ۲۰۰ ماشین)؛ به این شکل، می‌توان میدان را به دو بخش با ۱۲۷ آدرس تقسیم نمود. به خاطر داشته باشید که، میدان DHCP گستره‌ای از آدرس‌ها است که توسط سرویس‌دهنده به کار گرفته می‌شوند. در این حالت فرض کنید که آدرس زیرشبکه عبارت است از 167.195.191.0. میدان یک سرویس‌دهنده ممکن است به صورت 167.195.191.10 تا 167.195.191.127 و میدان سرویس‌دهنده دیگر به صورت 167.195.191.128 تا 167.195.191.254 باشند.

گفتنی‌های زیادی در مورد نگهداری تعداد زیادی تخم‌مرغ در دو سبد، وجود دارد (تعداد دقیق شماره‌های قابل دسترسی برای هر میدان سرویس‌دهنده کمتر از تقسیم ۲۵۴ بر دو خواهد بود، چرا که اقلامی نظیر مسیریاب‌ها و سرویس‌دهنده آدرس‌های IP غیر پویایی دارند و این آدرس‌ها را به طرز اختصاصی مورد استفاده قرار می‌دهند).

تحلیل نام در TCP/IP

چیزی که همیشه من را هنگام آغاز کار شبکه‌سازی در ویندوز با TCP/IP به اشتباه می‌اندازد، این مطلب است: چرا دو نوع تحلیل نام وجود دارد؟ بعد از بحث مطرح‌شده در فصل اول، احتمالاً با این حقیقت کنار آمده‌اید که هر نام شبکه‌ای را باید به یک آدرس شبکه‌ای تحلیل نمود - یعنی هنگامی که از مرورگر خود می‌خواهید www.jotto.com را بیاورد، مرورگر این آدرس اسم‌گرا را از طریق DNS (سرویس نام حوزه) به آدرس شبکه‌ای 205.134.224.21 تحلیل می‌کند.

بنابراین، شما هم مثل من احتمالاً از خود می‌پرسید که چرا تنها DNS را در سیستم‌های عاملی که از TCP/IP استفاده می‌کنند، به‌کار نبرید؟ منطقی به نظر نمی‌رسد که میکروسافت تنها برای ویندوز نوع جدیدی از سرویس نام را فراهم کرده باشد. اجازه دهید در ابتدا ببینیم WINS چگونه در تصویر TCP/IP ویندوز جای می‌گیرد و آنگاه به چگونگی مجتمع‌سازی DNS در ویندوز خواهیم پرداخت.

WINS در ویندوز

سرویس نام اینترنت ویندوز، یا WINS، به منظور آسان‌کردن کار شبکه‌سازی ویندوز، حتی در ناحیه‌ای وسیع، اختراع شده است. همان طور که می‌دانید NetBEUI پروتکلی قابل مسیریابی نیست و بنابراین منطقی به نظر می‌رسد که برای اتصال ماشینهای شبکه‌ای ویندوز به پروتکل دیگری نیاز داشته باشیم. TCP/IP مناسب بود و می‌توانست NetBIOS حمل کند، اما برخی از روشهایی که در تحلیل نام توسط NetBEUI مورد استفاده قرار می‌گرفتند، لازم بود برای TCP/IP دوباره به انجام برسد. بخصوص، هنگامی که حوزهٔ شما می‌تواند در سطح چندین زیرشبکه گسترده شده باشد، استفاده از انتشار

برای تحلیل نام دیگر کار نمی‌کند ـ انتشار اغلب تنها زیرشبکهٔ محلی را تحت تأثیر قرار می‌دهد[1].

پاسخ چگونگی تحلیل نام بدون استفاده از انتشار در WINS نهفته است. سرویس‌دهندهٔ WINS قادر است ارتباط گروههای کاری ویندوز، حوزه‌ها و اسامی ماشین‌ها را در شبکه TCP/IP نگهداری کند. به جای آنکه لازم باشد ماشینی عمل انتشار در شبکه را صورت دهد، به جای آن می‌تواند با سرویس‌دهندهٔ WINS ارتباط برقرار کند و اطلاعات لازم را دریافت نماید. این کار تحلیل نام نقطه به‌نقطه نام دارد. به ماشینهایی که از این طریق اسامی را تحلیل می‌کنند، گره‌های *p* گفته می‌شود. هنگام صحبت سرویس‌گیرنده با سرویس‌دهنده WINS، این سرویس‌دهنده آدرس‌های IP و گروه کاری ماشین را به سرویس‌گیرنده اعلان می‌کند و پایگاه داده خود را به‌روز درمی‌آورد.

برنامهٔ سرویس‌دهندهٔ WINS، مثل DHCP تنها در ویندوز NT اجرا می‌شود. سرویس‌دهندهٔ WINS برای گروههای کاری وجود ندارد. کار آن نگهداری پایگاه اطلاعاتی شامل حوزه‌ها، گروههای کاری و اسامی PC ها و توزیع این اسامی و شماره‌های IP متناظر آنها به هر کسی است که آنها را مطالبه می‌نماید.

تمامی گزینه‌های لازم برای تکرار پایگاه داده‌ای مورد استفاده، در یک سرویس‌دهندهٔ WINS دیگر در اختیارتان وجود دارد. امکاناتی نظیر ایجاد تطابق‌های ایستا و نظایر آن نیز هستند، بهتر است در اینجا وارد جزئیات آنها نشویم. اگر این موضوعها برایتان جالب هستند، می‌توانید به کیت منابع NT (که به صورت برخط در دسترس قرار دارد) مراجعه کنید. و اما آخرین مطلبی که در مورد WINS می‌خواهیم بگوییم:

۱- اجرای WINS را آغاز می‌کنید.

۲- با اتصال PC ها به آن، اسامی کامپیوترها در پایگاه اطلاعاتی به ثبت می‌رسند.

۳- WINS این اطلاعات را در هنگام مقتضی و درخواست توسط ایستگاههای کاری و سرویس‌دهنده‌های دیگر توزیع می‌کند.

WINS می‌تواند بسیار اشتباه‌برانگیز باشد؛ آن را ساده نگه دارید تا مشکلی بروز نکند.



نکته : *سرویس‌دهندهٔ NT که سرویس‌دهندهٔ WINS را اجرا می‌کند باید خودش را به عنوان سرویس‌دهندهٔ WINS مورد استفاده قرار دهد. جالب است، نه؟*



نکته : *به کارگیری آخرین بسته‌های سرویس NT از اهمیت خاصی در مورد WINS برخوردار است. برخی از مشکلات دردسرساز در آنها رفع شده‌اند. بسته‌های سرویس حاوی رفع اشکال‌هایی هستند که میکروسافت آنها را از طریق سایت وِب و CD-ROM ها عرضه می‌کند. به‌کارگیری چنین بسته‌ای بسیاری از مشکلات احتمالی را حل می‌کند. بستهٔ سرویس با تصحیح حساس تفاوت دارد چرا که بسته‌های سرویس به منظور استفاده تمامی کاربران ایجاد شده‌اند در حالی که تصحیحات حساس برای کاربرانی است که مشکل بخصوصی دارند.*

استفاده از DNS

DNS را می‌توان به شکل یک سرویس نامگذاری مورد استفاده قرار داد، اما این باعث می‌شود که اتصالات اولیه‌تان تا حدودی آهسته‌تر باشند. DNS فاقد تسهیلات لازم برای تشخیص تفاوت بین گروههای کاری، حوزه‌ها، و اسامی

۱- بخشهای مختلف شبکه‌ای، از طریق ابزارهایی نظیر مسیریاب به هم متصل می‌شوند. این ابزارها انتشارها را از خود عبور نمی‌دهند. م.

کامپیوترها می‌باشد. هر ورودی DNS تنها یک اسم‌میزبان را مشخص می‌نماید.

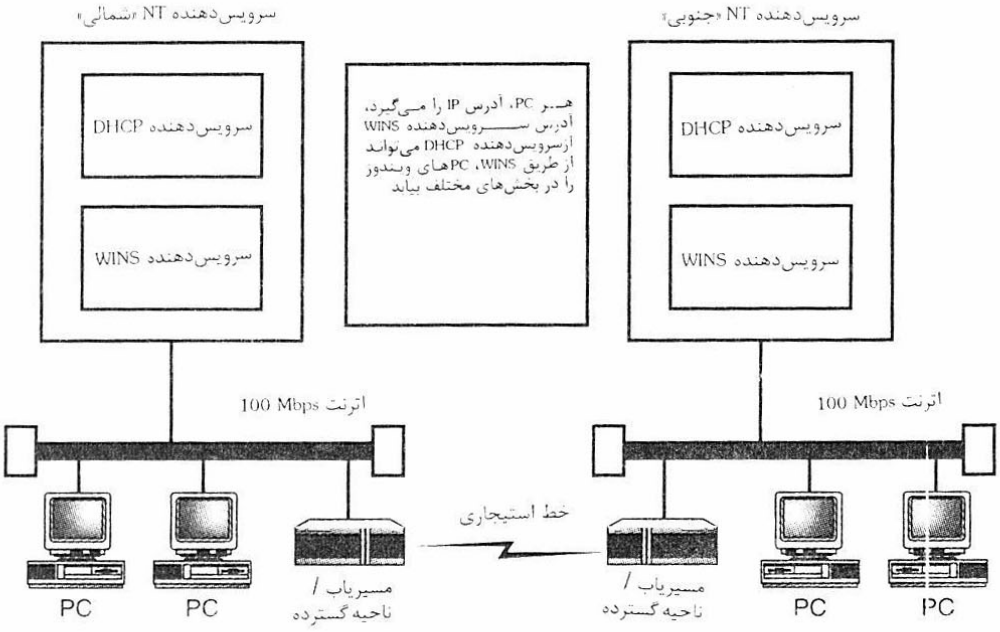
ویندوز ۹۵ به صورت خودکار هنگام خرابی بقیه امکانات، تحلیل DNS را مورد استفاده قرار می‌دهد؛ در NT لازم است این تنظیم صریحاً در پروتکل TCP/IP تعریف‌شده تحت بخش شبکهٔ Control Panel، اعلان گردد. اگر می‌خواهید DNS را مورد استفاده قرار دهید، باید چک‌باکس Use DNS for Name Resolution علامت خورده باشد.

بیشتر اوقات، استفاده از DNS مد نظر نیست؛ WINS که همراه NT عرضه می‌شود، به صورت پویا کار می‌کند و به نسبت استفاده از آن آسان است. تنظیم DNS تا حدودی به ترفندهای بیشتری احتیاج دارد و چیز زیادی را نسبت به دنیای شبکه عرضه می‌کند.

تنها زمانی که تنظیم سرویس‌دهندهٔ DNS میکروسافت لازم خواهد بود، در شرایطی است که بخواهید به عنوان یک سرویس‌دهندهٔ وِب عمل کنید. از آنجا که در شبکهٔ اینترنت شرکت کرده‌اید ـ که شبکه‌ای مبتنی بر فایل و چاپ میکروسافت نیست ـ DNS تنها گزینهٔ موجود است. بیشتر اوقات، استفاده از DNS به عنوان روشی برای تحلیل نام داخلی در شبکهٔ ویندوز کاری بیهوده می‌باشد.



یادداشت : *آیا تمام این چیزها به نظر آشفته و درهم می‌آیند؟ اشتباه نکرده‌اید: در اینجا آشفتگی وجود دارد. قطعات و بخشهای زیادی هستند که مجموعاً با TCP/IP و ویندوز به‌کار برده می‌شود. بدون شک میکروسافت برخی از این آشفتگی‌ها را، شاید در NT نگارش ۵، خواهد زدود اما برای مطمئن‌شدن باید صبر کنید. در عین حال اگر به این وضعیت آشنا شوید، درخواهید یافت که اوضاع چندان هم بد نیست. شکل ۲-۱۱ شبکهٔ ویندوز نمونه‌ای را نشان می‌دهد که از TCP/IP استفاده می‌نماید. در این شکل، مشاهده می‌کنید که PCها هنگام راه‌اندازی پیکربندی شده و از سرویس‌دهندهٔ DHCP موجود در بخش محلی خود آدرس لازم را دریافت می‌کنند. این سرویس‌دهنده دستگاهها را به آدرس‌های IP و سایر اطلاعات پیکربندی که آنها برای تحلیل اسامی دریافتی از سرویس‌دهنده WINS محلی خود لازم دارند، مجهز می‌نماید. خیلی پیچیده نیست. تنها چند مورد معدود وجود دارد که باید آنها را تنظیم نمایید.*



شکل ۲-۱۱ : یک شبکهٔ TCP/IP ویندوز نمونه.

تحلیل نام ایستا

باید بدانید که علاوه بر سرویس‌های نام پویا که توسط سرویس‌دهنده‌های نام در شبکه در دسترس قرار می‌گیرند، روش ایستایی برای هر PC وجود دارد تا بتواند یک اسم شبکه‌ای را به آدرس شبکه‌ای متناظر آن تحلیل نماید. هر PC می‌تواند به یک جدول HOSTS مجهز باشد که برای شبکه‌سازی TCP/IP عادی به‌کار می‌رود (نظیر جلسه‌های Telnet به یک سیستم میزبان و همچنین دستورات Ping). هر PC می‌تواند یک فایل LMHOSTS نیز داشته باشد که بسیار نظیر فایل HOSTS می‌باشد اما برای تحلیل نام NetBIOS مورد استفاده قرار می‌گیرد. هردوی این فایل‌ها حاوی یک سری خطوط هستند که نظیر خطوط زیر به نظر می‌رسند:

```
192.168.10.5 fido

192.168.10.6 rover
```

این بدان معناست که 192.168.10.5 آدرس عددی fido و 192.168.10.6 آدرس عددی rover می‌باشد (LMHOSTS چند گزینهٔ قالب‌بندی اضافی نیز دارد که برای نشان‌دادن توابع NetBIOS نظیر گروههای کاری به‌کار می‌روند).

هردوی این فایل‌ها در فهرست C:\WINDOWS قرار دارند. LMHOSTS.SAM یک فایل نمونه است که می‌توانید قالب چنین فایلی را از روی آن فرا بگیرید. اما نباید از این فایل‌ها استفاده کنید مگر اینکه شبکه‌تان کوچکترین شبکه دنیا باشد. کار یکنواخت به‌روز درآوری این فایل‌ها شما را وادار می‌کند آرزو می‌کردید به جای این کار با مشکلات پیچیده شبکه‌ای مواجه بودید. می‌توانید چنین فرض کنید که تطابق‌های ایستای از لحاظ کارایی از رده خارج هستند، اما خوب است که از وجود آنها آگاه باشید. ممکن است در مورد یک مشکل تحلیل نام در ارتباط با یک ایستگاه‌کاری، بدانید که کسی در فایل LMHOSTS دستکاری کرده یا خیر.

پیکربندی ایستگاه‌کاری

اجازه دهید که به بررسی راههای ارتباطی در شبکه‌های ویندوز بپردازیم و نگاهی داشته باشیم به روش پیکربندی یک ایستگاه‌کاری ویندوز و همچنین پروتکل‌ها و سرویس‌گیرنده‌هایی که می‌توان آنها را در چنین دستگاهی پیکربندی نمود.

Network در Control Panel

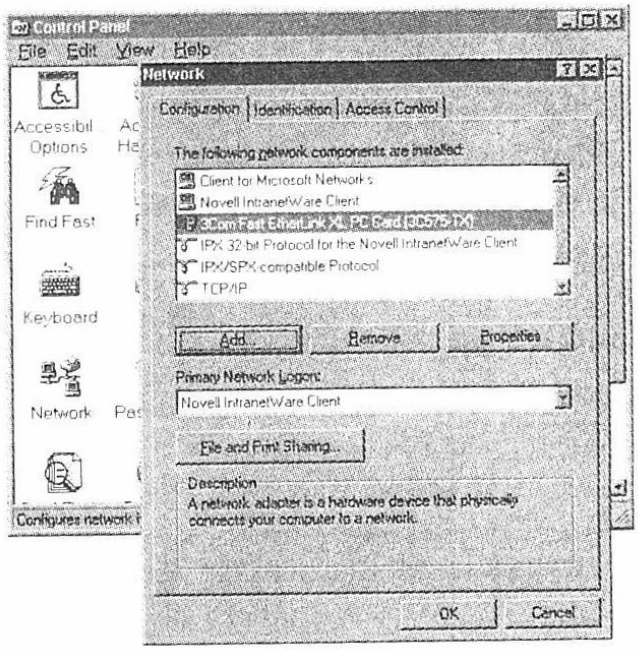
نگاهی به برنامهٔ Network ویندوز 9x که در شکل ۳-۱۱ به‌تصویر کشیده شده است، بیندازید. تصویری سطح بالا از مؤلفه‌های شبکه‌ای پیکربندی‌شده روی این دستگاه نشان داده می‌شود. برنامهٔ Network ویندوز NT از لحاظ ظاهری کمی متفاوت است، اما تمامی مؤلفه‌های شبکه‌ای شما را با همدیگر ارتباط می‌دهد و به شما اجازه می‌دهد آنها را از یک جا مدیریت کرده و وضعیت پیکربندی‌شان را وارسی نمایید. مؤلفه‌ها شامل موارد زیر هستند:

- سرویس گیرنده‌ها ـ این مؤلفه‌ها PC را قادر می‌سازند که از یک سرویس در شبکه استفاده کند.
- آداپتورهای شبکه ـ این مؤلفه‌ها و پروتکل‌ها تنظیم لازم برای ارتباط با شبکه را صورت می‌دهند.
- پروتکل‌ها
- سرویس‌ها ـ همان گونه که در فصل اول مورد بحث قرار گرفت، سرویس‌ها برنامه‌هایی هستند که اطلاعات یا منابع موجود در شبکه را ارائه می‌کنند.

در بخشهای آتی این مؤلفه‌ها را به صورت مجزا مورد بررسی قرار می‌دهم. ابتدا کار را از سرویس‌گیرنده‌ها شروع می‌کنیم و آنگاه به مسألهٔ مقیدسازی[1]، فرآیندی که به ایستگاه‌کاری شما اجازه می‌دهد که بداند کدام مؤلفه‌های شبکه‌ای به دیگری متصل شده‌اند، خواهیم پرداخت.

سرویس‌گیرنده‌ها

برای آنکه با کامپیوتر دیگری ارتباط برقرار کنید، خواه این کامپیوتر PC ویندوز دیگری باشد و یا سرویس‌دهنده‌ای در مرکز اطلاعات، همیشه به یک سرویس گیرنده نیاز دارید. بیشتر اوقات، سرویس‌گیرنده برنامه‌ای است که به ویندوز اجازه می‌دهد با منابع گروه کاری یا سرویس‌دهنده طوری رفتار کند که گویی در ایستگاه‌کاری محلی قرار گرفته‌اند. این کار اغلب توسط عمل تغییر جهت[2] فایل و چاپ صورت می‌پذیرد ـ یعنی، گردونه :G در واقع یک دیسک‌گردان در سرویس‌دهنده یا گردونهٔ CD-ROM دوست‌تان می‌باشد. و LPT3 در واقع چاپگری است که در جایی دیگر به یکی از سیستم‌ها متصل شده است و نظایر آن (در فصل ۱۸ هنگام عیب‌یابی فایل و چاپ در مورد مسائل عمومی سرویس‌گیرنده‌ها بیشتر خواهید شنید). به منظور انجام عمل تغییر جهت گردونه و چاپگر، باید نرم‌افزار گردونه را به ویندوز اضافه کنید. این کار از طریق رفتن به Control Panel و انتخاب Network که کادر تبادلی نشان داده‌شده در شکل ۳-۱۱ را ظاهر می‌سازد، صورت می‌پذیرد. از آنجایی که Control Panel نشان می‌دهد که من دارای سرویس‌گیرنده‌های لازم برای شبکه‌های میکروسافت و سرویس‌گیرندهٔ InteranetWare ناول می‌باشم، باید بتوانم هم با شبکه‌های میکروسافت و هم با شبکه‌های ناول ارتباط برقرار کنم.



شکل ۳-۱۱ : Network در Control Panel، که در آن بیشتر توابع شبکه‌ای ویندوز پیکره‌بندی می‌شوند؛ نظیر کارت‌های شبکه، پروتکل‌ها و سرویس‌گیرنده‌های مربوط به فایل و چاپ در شبکه.

البته، همان گونه که افراد مختلف دست خطهایی متفاوتی دارند، سرویس‌دهنده‌های مختلف، به انواع متفاوتی از سرویس‌گیرنده نیاز دارند. برخی از پرکاربردترین آنها عبارتند از:

- سرویس‌گیرندهٔ Banyan برای DOS/ویندوز

1- binding 2- redirection

- سرویس‌گیرنده برای شبکه‌های میکروسافت
- سرویس‌گیرنده برای IntraNetware ناول
- سرویس‌گیرنده‌های مختلف دسته سوم یونیکس (NFS، یا سیستم فایلی شبکه)



نکته : *با اینکه ویندوز سرویس‌گیرنده‌های سازندگان متعددی را عرضه می‌کنند، نگارش‌های موجود در CD-ROM نصب ویندوز اغلب قدیمی‌تر هستند و احتمالاً نسبت به نگارش‌هایی که می‌توانید آنها را از سازندگان دریافت کنید، حاوی اشکالات بیشتری می‌باشند. همیشه بهتر است نرم‌افزار را مستقیماً از تولیدکننده‌اش دریافت کنید.*

مقیدسازی

پس دانستیم که سرویس‌گیرنده، مسؤول ایجاد دسترسی به منابع فایل و چاپ توسط برنامه‌های مختلف می‌باشد. تا اینجا همه چیز مرتب است. اما، سرویس‌گیرنده چگونه با شبکه صحبت می‌کند؟ خوب، همان گونه که در فصل اول توضیح دادیم، سرویس‌گیرنده باید زبان مناسب برای صحبت‌کردن را بداند، بداند که چگونه از پروتکل استفاده کند و چگونه از کارت شبکه بخواهد یک فراخوانی را آغاز نماید. ویندوز دارای پروتکل‌ها، سرویس‌گیرنده‌ها و کارت‌های شبکه‌ای بسیاری است که تحت یک مفهوم با عنوان مقیدسازی معرفی می‌گردند. این مفهوم آنچه که را می‌تواند در مورد پروتکل‌ها، سرویس‌ها، سرویس‌گیرنده‌ها، و کارت‌های شبکه رخ دهد، ساده می‌نماید. اگر از سطح بالا شروع کنیم، هر سرویس‌گیرنده را می‌تواند به یک یا چند پروتکل مقید نمود. هر پروتکل را به نوبهٔ خود می‌تواند به یک یا چند کارت شبکه (که برخی اوقات آداپتور شبکه نامیده می‌شوند) مقید نمود.



نکته : *تنها پروتکل‌هایی را به کارت شبکهٔ مورد استفاده مقید کنید که عملاً از آن استفاده می‌نمایید. هر پروتکلی که به یک آداپتور مقید می‌شود، پردازش بیشتری توسط CPU را می‌طلبد و CPU باید هر بار که به آن آداپتور اشاره می‌شود، سربار بیشتری را تحمل نماید. فرض کنید که برای مثال آداپتور تلفنی را برای ارتباط با اینترنت از طریق TCP/IP به‌کار می‌برید. مقیدسازی IPX/SPX به این آداپتور کاری بیهوده است، چرا که اینترنت به زبان IPX/SPX صحبت نمی‌کند. از آن گذشته، اگر کارت شبکه‌ای با مقیدسازی‌های بیش از حد، به یک CPU کُند متصل شده باشد، حتی ممکن است مشکلات شبکه‌ای بروز نمایند.*

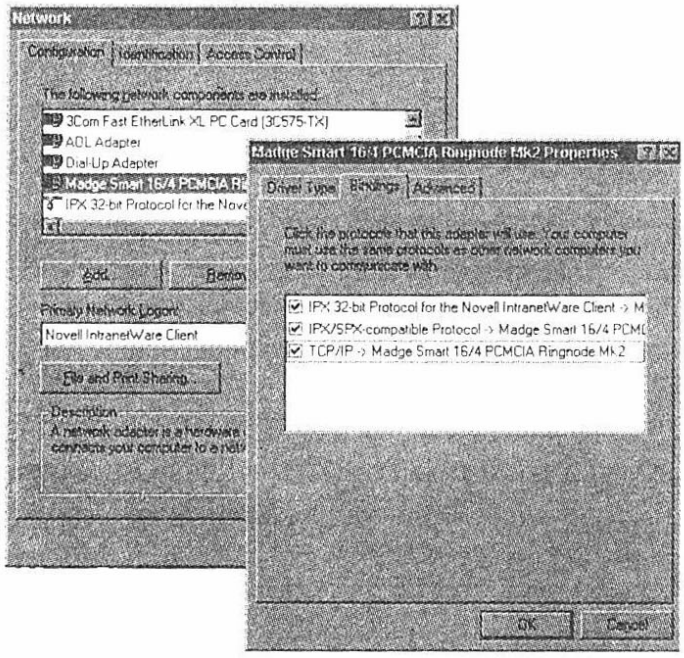


نکته : *یکی از خبرنامه‌های شبکه‌ای که در آن عضو هستم اشاره‌ای داشت به اینکه تشخیص خودکار را در محیط IPX/SPX برای تشخیص انواع قاب استفاده نکنید، چرا که این کار، ترافیک شبکه‌ای بیهوده‌ای را تولید می‌کند و می‌تواند به میزان زیادی کار شبکه را در مجموعه‌های بزرگ کُند نماید.*
انواع قاب موضوعی است که تاکنون در مورد آنها صحبت نکرده‌ام. هر نوع قاب، روشی است که کارت شبکه با آن بسته‌های شبکه‌ای را می‌سازد. می‌توانید تصور کنید که هر نوع قاب نظیر لهجهٔ پروتکل می‌باشد ـ درک لهجه‌ها کار مشکلی است حتی اگر به یک زبان تعلق داشته باشند.
می‌توانید نوع قاب مورد استفاده در شبکه نِت‌ور خود را با تایپ دستور Config در محل کنسول سرویس‌دهندهٔ نِت‌ور پیدا کنید. آنگاه می‌توانید آن را در ایستگاههای کاری ویندوز خود وارد نمایید از آنجا که تشخیص خودکار همیشه هم کار نمی‌کند، این روش می‌تواند فکر خوبی باشد. از این طریق من

توانسته‌ام مشکلات ایستگاههای کاری را حل کنم که به گونه‌ای عجیب رفتار می‌کردم.
اما اگر ایستگاههای کاری زیادی داشته باشید چطور؟ کار زیادی می برد؟ خیر. فصل ۱۶ نکاتی در مورد نحوهٔ استانداردسازی ایستگاههای کاری در اختیارتان قرار می‌دهد.

گفتنی است که مقیدسازی، خیابانی دوطرفه است؛ هر کارت شبکه نیز به یک یا چند پروتکل مقید می‌گردد. شکل ۴-۱۱ صفحه‌ای از ویندوز 9x را نشان می‌دهد که در آن می‌توانید پروتکل‌هایی که به یک کارت شبکهٔ مشخص، مقید شده‌اند، تعیین نمایید (بدون توجه به نوع کارت شبکه). برای مشاهدهٔ وضعیت در مورد کارت شبکهٔ خود، مراحل زیر را دنبال کنید:

۱- Network را از Control Panel انتخاب کنید.
۲- آداپتور شبکه خود را انتخاب نمایید.
۳- روی Properties کلیک نمایید.
۴- روی برگهٔ Bindings کلیک کنید.



شکل ۴-۱۱ : نمایش مقیدسازی‌ها روی یک کارت شبکه.

کادر تبادلی Properties امکان فعال‌کردن یا غیرفعال‌کردن یک پروتکل را برای سرویس‌گیرنده یا سرویسی مشخص، میسر می‌سازد (شکل ۵-۱۱ کادر تبادلی Properties برای TCP/IP را نشان می‌دهد). این تنها محلی است که می‌توان مقیدسازی‌ها را تنظیم نمود؛ ترجیح هم بر این است که تمامی تنظیمات لازم در یک محل صورت گیرد. در این حالت می‌توانید پروتکل TCP/IP را از Network انتخاب نموده، روی Properties کلیک کنید و آنگاه برگهٔ Bindings را برگزینید.

خوشبختانه، تحت ویندوز NT، مقیدسازی به شکل مستقیم‌تری صورت می‌گیرد (شکل ۶-۱۱ را ملاحظه کنید). هر کارت شبکه به همراه پروتکل‌های مرتبط، سرویس‌گیرنده‌ها و سرویس‌های وابسته‌اش نشان داده می‌شود و کلاً هر چیزی را می‌توان از این محل کنترل نمود. دسترسی به این کادر تبادلی از طریق Control Panel مربوط به NT و با انجام مراحل زیر صورت می‌پذیرد:

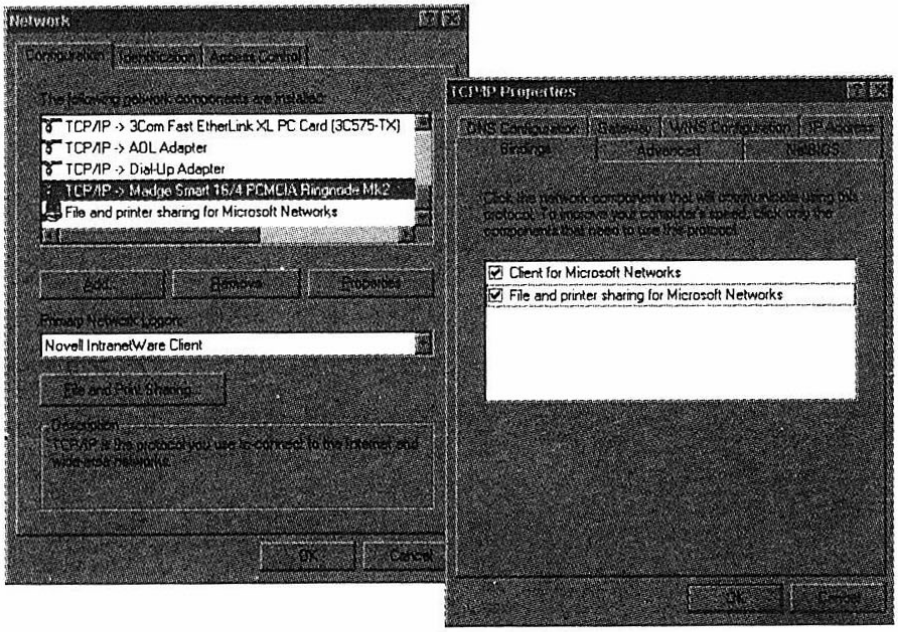
۱- روی Network دوبار کلیک کنید.

۲- روی برگهٔ Bindings کلیک نمایید.

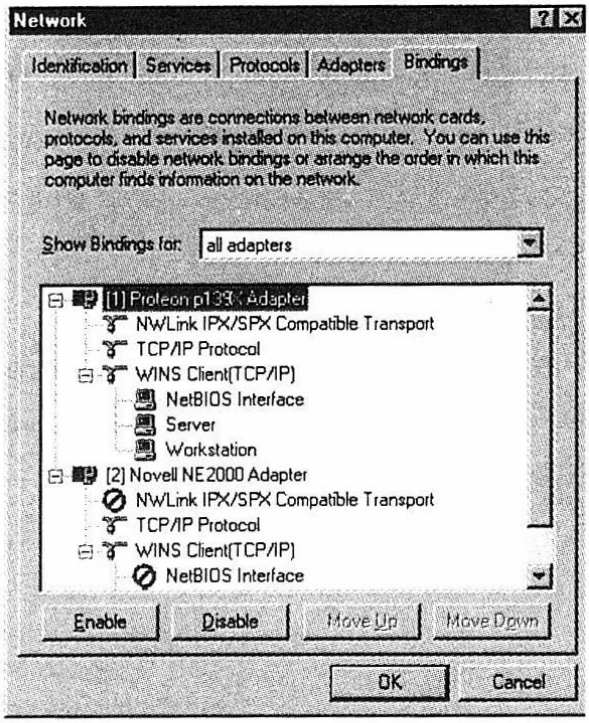
۳- گزینهٔ All Adapters را از لیست Show Bindings For انتخاب کنید.

۴- با کلیک‌کردن روی مؤلفه‌ها، زیرمؤلفه‌های مربوط به آن را نشان دهید (اگر در کنار مؤلفه‌ای علامت منفی قرار دارد، تمامی زیرمؤلفه‌های آن به نمایش درآمده‌اند).

۵- با کلیک‌کردن روی دکمهٔ Disable، قید موجود روی آن مؤلفه برداشته می‌شود؛ روشن‌کردن این مقیدسازی نیز از طریق دکمهٔ Enable صورت می‌گیرد.



شکل ۵-۱۱ : نمایش مقیدسازی‌های مربوط به یک پروتکل خاص.



شکل ۶-۱۱ : نمایش مقیدسازی‌های تمامی مؤلفه‌ها در ویندوز NT.

فرمانروایی و تسلط

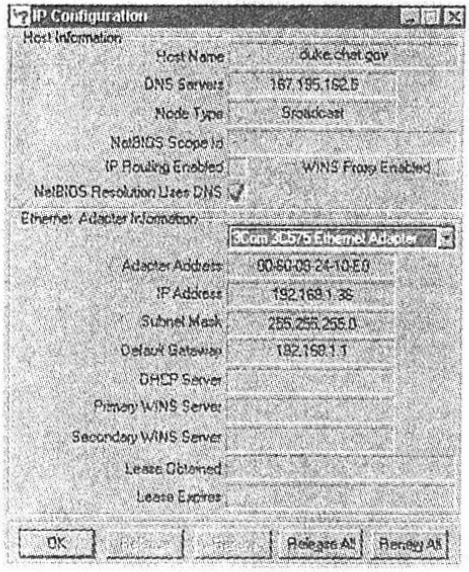
به قسمت جالب این بخش رسیدیم: عملاً کارهایی را صورت خواهید داد. بخشهای آتی برخی از دستورات TCP/IP که اطلاعات لازم برای تحلیل و بررسی هوشمندانه را در اختیار می‌گذارند، ملاحظه خواهید نمود.

winipcfg

هر زمانی که به عیب‌یابی TCP/IP می‌پردازید، می‌خواهید بدانید که ایستگاه‌کاری چگونه پیکربندی شده است. می‌توانید به Control Panel بروید اما در آنجا اطلاعات چندانی را نخواهید یافت. بخصوص اگر ایستگاه‌کاری از DHCP استفاده می‌کند. بجای آن از محل اعلان DOS در ویندوز 9x دستور زیر را اجرا کنید:

```
winipcfg
```

برای دریافت خروجی کامل نشان داده‌شده در شکل ۷-۱۱ باید روی دکمهٔ More Info کلیک کنید یا دستور را با سوئیچ /all اجرا نمایید؛ در غیر این صورت صفحهٔ کاملی ظاهر نخواهد شد. صفحهٔ نمایش داده‌شده خلاصهٔ دقیق و کاملی از تمامی گزینه‌های پیکربندی‌شدهٔ TCP/IP در این ایستگاه‌کاری را به نمایش می‌گذارد. توجه داشته باشید که حتی اگر کارت شبکه از طریق DHCP پیکربندی نشده باشد، می‌توان پیکربندی آن را از این طریق مشاهده نمود.



شکل ۷-۱۱: خروجی WinIPCfg برای سرویس‌گیرنده‌ای که از DHCP یا WINS استفاده نمی‌کند و TCP/IP را تنها برای اتصال به اینترنت مورد بهره‌برداری قرار می‌دهد.

کاربران ویندوز NT می‌توانند دستور

```
ipconfig /a
```

را تایپ کنند تا خروجی متنی مشابهی را دریافت نمایند.



نکته : *یک مقایسهٔ سریع بین اطلاعات پیکربندی IP دو ایستگاه‌کاری می‌تواند به تحلیل سریع مشکل کمک نماید. البته هر زمان که ایستگاههای کاری را مقایسه می‌کنید، باید مطمئن شوید که مقایسه بین دو ایستگاه‌کاری از یک زیرشبکه صورت پذیرد. موارد زیر را باید در مقایسه مدنظر داشته باشید:*

- **آدرس‌های IP** ـ *آدرس‌های IP ایستگاههای کاری باید نظیر هم باشند، به غیر از بخش مربوط به شمارهٔ گره (192.168.10.5 و 192.168.10.6 یکی هستند؛ اما 192.168.9.5 و 192.168.11.6 یکی نیستند).*
- **سرویس‌دهنده(های) DNS**
- **سرویس‌دهنده(های) WINS**

اگر شانس داشته باشید، در صورت وجود تفاوت بین تنظیمات، به جای مشکل سخت‌افزاری یا شبکه‌ای، تنها با یک مشکل پیکربندی روبرو هستید.

دستورات اطلاعاتی

اگر مشکل آزاردهنده‌تر از یک موضوع پیکربندی باشد، مفید خواهد بود اگر از دیدگاه ایستگاه‌کاری مشکل‌زا آگاه شوید؛ یعنی آنچه را که این ایستگاه می‌تواند ببیند و آنچه را که نمی‌تواند ببیند، و وضعیت دستورات اطلاعاتی مختلفی که می‌توان در ایستگاه‌کاری اجرا نمود. دستورات اطلاعاتی مختلفی را که در جدول ۱-۱۱ نشان داده شده‌اند، می‌توان اجرا نمود تا از دیدگاه ایستگاه‌کاری در شبکه اطلاعاتی کسب کرد (این دستورات در ویندوز 9x و NT مشترک هستند).

جدول ۱-۱۱ : دستورات اطلاعاتی

دستور	شرح
netstat -r	جدول مسیریابی TCP/IP را نشان می‌دهد
netstat -a	تمامی سوکت‌های TCP/IP تحت استفاده (سرویس‌دهنده و سرویس‌گیرنده) را نشان می‌دهد.
arp -a	جدول ترجمه آدرس MAC ـ به ـ IP را به نمایش می‌گذارد.
آدرس یا میزبان	قابلیت اتصال اولیه IP را با اسم میزبان یا آدرس به بررسی می‌گذارد.
آدرس یا اسم میزبان	مسیری که بسته از ایستگاه‌کاری جاری به اسم میزبان یا آدرس طی می‌کند، ردیابی می‌نماید. تمامی مسیریاب‌های موجود در مسیر را نشان می‌دهد.
nbtstat	جدول نام NetBIOS را وارسی می‌کند.

تمامی این دستورات (به غیر از nbtstat) کم‌وبیش از یونیکس برگرفته شده‌اند؛ فصل ۱۲ ، «مبانی شبکه در یونیکس»، مثالهایی از کاربردهای این دستورات را در عیب‌یابی مقدماتی TCP/IP نشان می‌دهد. فصل ۱۸ نیز تکنیک‌هایی را با استفاده از این دستورات به نمایش می‌گذارد.

net

خوب است با دستور net نیز آشنا شوید. تایپ کنید:

```
net | more
```

این دستور، فرمانهای عمومی شبکه‌ای که قادر به اجرای آنها هستید را نشان می‌دهد. برخی از این دستورات به فایل و چاپ و برخی به پیکربندی شبکه در حالت کلی ارتباط دارند. بعضی از این توابع فاقد معادل گرافیکی هستند. بنابراین بهتر است نیم‌ساعتی را برای آشناشدن با این دستورات کنار بگذاریم.

نظارت بر سیستم

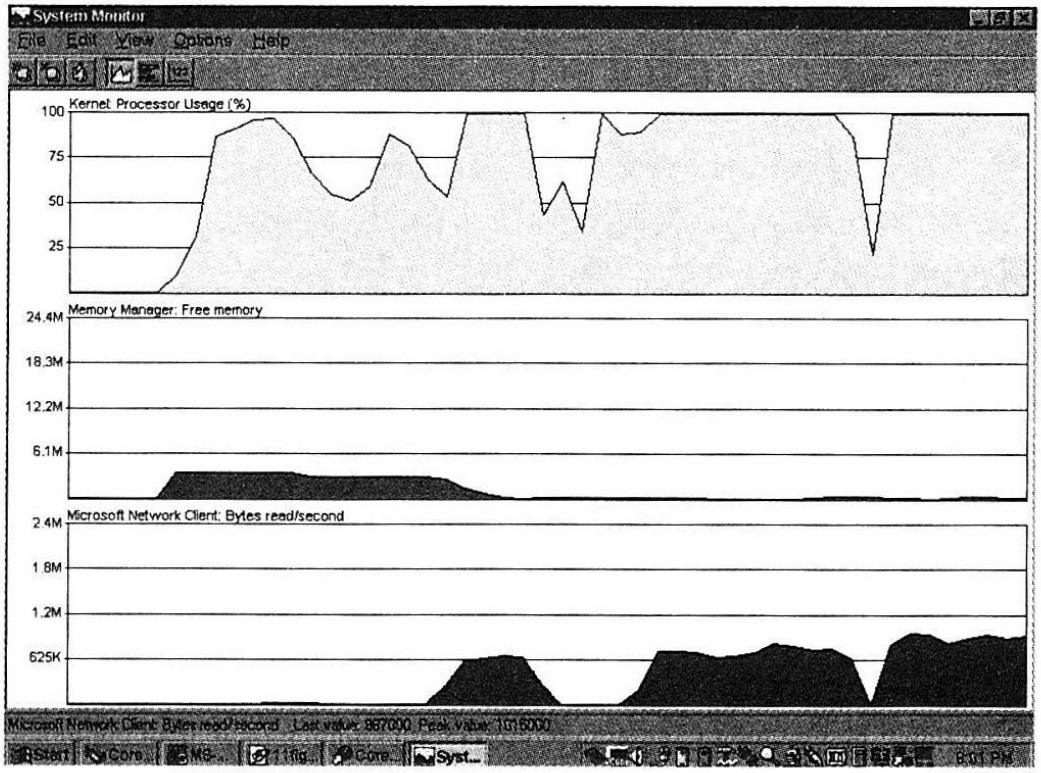
از میان بهترین ویژگیهای شبکه‌های میکروسافت، می‌توان به امکانات جمع‌آوری ایستا در برنامه‌های سرویس‌دهنده و سرویس‌گیرنده اشاره نمود. به عنوان مثال برنامهٔ SysMon که شکل کوتاه‌شدهٔ System Monitor است، شما را قادر می‌سازد که در هر زمان دلخواه، کارایی سیستم خود را بررسی نمایید. این بدان معناست که می‌توانید به سرعت و به سادگی یک بخش از شبکه یا یک سرویس‌دهنده بخصوص را مورد بررسی قرار دهید. استادکاران شبکه قبلاً برای دسترسی به چنین اطلاعاتی به تجهیزات گرانقیمتی نیاز داشتند اما اکنون میکروسافت این امکان را برای همه میسر ساخته است.

این برنامه شما را قادر می‌سازد برخی از عیب‌یابی‌ها را به صورت قدرتمندانه و ارزان‌قیمت به انجام برسانید. اجازه دهید به مثالی کوتاه نگاه کنیم: فرض کنیم برنامه‌ای داریم که به دلیلی نامشخص برای یکی از پرسنل خیل کُند کار می‌کند. برخی از افراد مشکلی با برنامه ندارند و میزان اطلاعات ما در مورد تشابه ایستگاههای کاری چندان نیست. متوجه می‌شویم که این کاربر می‌تواند با استفاده از ایستگاه‌کاری دیگر کار خود را به خوبی انجام دهد.

یک نفر پیشنهاد می‌کند که گردونه دیسک سخت کاربر را خالی کرده و دوباره تنظیم نماییم. این موضوع با سکوتی ناخوشایند از سوی کاربر مواجه می‌شود که از قضا شخص مهمی در شرکت به‌شمار می‌رود. واضح است که این روش غیرعملی خواهد بود. این کاربر مدعی است که سرعت اجرای او مثل شیرهٔ قند کُند است و ما با مشاهدهٔ وضعیت ایستگاههای کاری افراد دیگر با او هم‌عقیده می‌شویم. چه اتفاقی می‌افتد؟ مشکل در سرویس‌گیرنده یا سرویس‌دهنده است؟ چگونه می‌توان به بررسی دقیق این موضوع پرداخت؟

می‌توانستیم برای اندازه‌گیری توان عملیاتی شبکه یک تحلیل‌گر شبکه ۱۰۰۰۰ دلاری به آن بخش از شبکه متصل کنیم و تمامی بسته‌های بین سرویس‌دهنده و سرویس‌گیرنده را شکار نماییم و آنگاه با انجام محاسبات ریاضی بر اساس زمان ارسال و دریافت، مقدار اطلاعات جابجاشده در هر ثانیه را محاسبه نمایید. اما، از آنجا که محاسبهٔ توان عملیاتی شبکه با استفاده از برنامهٔ System Monitor ویندوز ۹۵ کار آسانی است، این برنامه را در ایستگاه‌کاری کاربر نصب می‌کنیم و آمار Bytes Read/Second مربوط به سرویس‌گیرندهٔ شبکه میکروسافت را به نمودار اضافه می‌کنیم. شکل ۸-۱۱ یک جلسهٔ نظارتی را نشان می‌دهد؛ این موضوع آشکار می‌شود که جلسهٔ فایل و چاپ میکروسافت در حد قابل قبولی سریع کار می‌کند: ۶۲۵KB تا ۹۹۱KB. نمی‌توانید در یک شبکهٔ اِترنِت ۱۰Mbps، سرعتی بالاتر را انتظار داشته باشید. با توجه به میزان کارکرد CPU و حافظهٔ خالی، می‌توانید بگویید که ایستگاه‌کاری به سختی در حال کارکردن است. هردوی این آمار هنگام انتقال فایل به سرعت پایین می‌آید. در این مثال می‌توانیم خروجی مشابهی را هنگام اجرای برنامه در سرویس‌دهنده‌ای متفاوت، مشاهده نماییم.

با کمینه‌کردن System Monitor و اجرای برنامهٔ کاربردی مشکل‌زا متوجه می‌شویم که سرعت اتصال LAN در نواحی راه دور با سرعت خوبی انجام می‌شود. از اینجا درمی‌یابیم که مشکل سرعت به شبکه مربوط می‌شود و ایستگاه‌کاری وی مشکلی ندارد.



شکل ۸-۱۱ : یک جلسه نظارتی با System Monitor.

شاید هم این حرف درست نیست؟ سرویس‌دهندهٔ متفاوتی داریم که در دستگاه دپارتمانی دیگر به درستی کار می‌کند، پس بنابراین تصمیم می‌گیریم که چنین اندازه‌گیری را روی آن سرویس‌دهنده با استفاده از همان برنامهٔ کاربردی صورت دهیم. در این حالت اندازه‌گیری‌ها با آنچه که در ایستگاههای کاری دیگر که در LAN مشاهده می‌کنید، بیشتر در یک خط قرار می‌گیرند. چنین به نظر می‌رسد که این سرویس‌دهنده و ایستگاه‌کاری شخص مورد نظر زیاد از یکدیگر خوششان نمی‌آید. پنج دقیقه‌ای که به بررسی با System Monitor صرف کردیم، دو نکته مهم را روشن ساخت:

- کُندی برنامه از تصورات شخص نیست؛ اطلاعات مستندی برای اثبات آن در دست داریم.
- مشاهده نمودیم که ایستگاه‌کاری می‌تواند بدون مشکل کاهش سرعت به سرویس‌دهندهٔ دیگری متصل شود؛ پس می‌دانیم که باید بررسیهای بیشتری را پیرامون سرویس‌دهنده یا ایستگاه‌کاری مشکل‌زا صورت دهیم.

در این حالت بخصوص، به نظر می‌رسد که سرویس‌دهنده مشکل‌زا باشد. این سرویس‌دهنده از میکروسافت نیست؛ بلکه سرویس‌دهنده یونیکسی است که نسخهٔ قدیمی‌تری از سرویس‌دهندهٔ SMB را به‌کار می‌برد. با اینکه سرویس‌دهنده به خوبی با سایر سرویس‌ها کار می‌کند، نکته‌ای در مورد سن سرویس‌دهنده و نرم‌افزار سرویس‌گیرنده در PC کاربر متناسب به نظر نمی‌رسد.

با دقتی خاص، سرویس‌گیرندهٔ فایل و چاپ میکروسافت را در ایستگاه‌کاری مجدداً نصب می‌کنیم که با سایر ایستگاههای کاری موجود در دپارتمان سازگاری داشته باشند؛ آنگاه Service Pack شمارهٔ یک ویندوز ۹۵ را دوباره به‌کار می‌اندازیم. در این حالت از آنجا که با یک شخص مهم طرف هستیم، یک کپی پشتیبان از دیسک‌گردان وی تهیه می‌کنیم ـ چرا که ممکن است مشکلات جدیدی را طی این فرآیند ایجاد کنیم. بعد از به‌کارگیری سرویس‌گیرنده و بستهٔ سرویس جدید، دوباره System Monitor را اجرا می‌نماییم. مشکل رفع و کاربر مهم عزیز، خوشحال شده است.



یادداشت : *در مورد توان عملیاتی شبکه در فصل ۲۲ بیشتر خواهید شنید.*

خلاصه

شبکه‌سازی ویندوز 9x و NT بهتر از ویندوز 3.x و DOS می‌باشد. کار عیب‌یابی نیز ساده‌تر است.

شبکه‌سازی گروه کاری در ویندوز با شبکه‌سازی حوزهٔ ویندوز NT متفاوت است، اما این دو روش تشابه‌های بسیاری دارند بخصوص در مورد پروتکل‌هایی که این سرویس‌ها را ارائه می‌کنند. NetBEUI و NetBIOS زبانهای بومی ویندوز هستند؛ از آنجا که NetBEUI قابل مسیریابی نیست، خوشحال هستیم که NetBIOS می‌تواند توسط TCP/IP و IPX/SPX حمل گردد. تنظیم TCP/IP با ترفندهایی همراه است بسیار بهتر است که اگر از ابزارهای تنظیم خودکار TCP/IP نظیر WINS و DHCP استفاده نمایید. البته به منظور استفاده از این ابزار خودکارسازی، باید از ویندوز NT استفاده نمایید.

ویندوز برنامه‌ها و دستورات توکار بسیاری دارد که برای بررسی و پیکربندی شبکه به‌کار می‌آیند؛ خوب است که مدت زمانی را صرف بررسی آنها بنماییم تا هنگام مواجه‌شدن با مشکلات بتوانید آنها را مورد استفاده قرار دهید.

کارگاه

پرسش و پاسخ

پرسش : من از TCP/IP بدون استفاده از WINS یا DHCP به خوبی بهره می‌جویم. چرا باید از این ابزار استفاده کنم؟

پاسخ : احتمالاً شما از محیطی که مسیریابی در آن صورت نمی‌گیرد استفاده می‌کنید و/یا پیکره‌بندی شما در فایل‌های متنی LMHOSTS در گردونهٔ دیسک سخت صورت گرفته است. اگر این وضعیت برای شما کار می‌کند، عالی است! هنگامی که پیکربندی را تغییر دهید و بخواهید کارها را کمی خودکار نمایید ممکن است نظرتان عوض شود.

پرسش : چرا اینقدر باید از انتشار اجتناب نمود؟

پاسخ : در یک محیط سوئیچی، تمامی ایستگاههای کاری انتشارها را دریافت می‌کنند. اگر ۳۰۰ ایستگاه‌کاری داشته باشید که هریک هر زمان برای متصل‌شدن به یک گردونه، استفاده از چاپگر و کارهای نظیر آن انتشاری را صورت دهند، خیلی سریع مشاهده می‌کنید که تعداد زیادی ترافیک انتشاری دارید که عرض باند زیادی را در شبکه به خود اختصاص می‌دهند و بنابراین شبکه شما را کند می‌کنند. یکبار انتشار طی پیکربندی DHCP بسیار مقرون به صرفه‌تر است.

آزمون

۱- درست یا نادرست؟ بهتر است تمامی پروتکل‌ها را به یک کارت شبکه مقید سازید تا در صورت لزوم مورد استفاده قرار گیرند.

۲- SMB مخفف کدامیک از موارد زیر است؟

الف ـ Server My Baguette　　ب ـ Server Mini Broadcast

ج ـ Service Messaging Broadcast　　د ـ Server Message Block

۳- درست یا نادرست؟ WINS تنها سرویس نامگذاری قابل استفاده برای کاربران ویندوز است.

۴- DHCP می‌تواند اطلاعات ـــــــــــ را برای ایستگاههای کاری که اطلاعات پیکربندی را درخواست می‌کنند، توزیع کند.

الف ـ آدرس‌های IP، آدرس‌های سرویس‌دهندهٔ WINS و آدرس‌های DNS

ب ـ آدرس‌های IP، مکانهای سرویس‌دهندهٔ وِب و آدرس‌های سرویس‌دهندهٔ WINS

ج ـ آدرس‌های IP، آدرس‌های DNS و دریافت ماهواره‌ای

د ـ آدرس‌های IP، آدرس‌های WINS و مکانهای مربوط به FTP

پاسخ به سؤالات آزمون

۱- نادرست　　۲- «د»

۳- نادرست　　۴- «الف»

فصل ۱۲

مبانی شبکه در یونیکس

یکی از ویژگیهای یونیکس آن است که بیش از یک میلیون شکل مختلف از آن وجود دارد. از سوی دیگر، ویژگی خوب این موضوع آن است که ابداعات شبکه‌ای بسیاری از این اشکال مختلف حادث می‌شود. شاید اینترنت وجودش را به ابداعات شبکه‌ای مبتنی بر یونیکس مدیون باشد. البته، خود TCP/IP نیز باعث شکوفایی کامپیوترهای یونیکس شده است؛ بنابراین بسیاری مفاهیم TCP/IP و دستورات یونیکس کاملاً برای سیستم‌های عامل دیگر به‌خصوص ویندوز NT فراهم آمده‌اند. حتی اگر در محیط کاری خود، به یونیکس دسترسی نداشته باشید بهتر است مطالب این فصل را مطالعه کنید، چرا که به احتمال زیاد مطالب مربوط به TCP/IP به کارتان خواهد آمد. هدف این فصل آموزش یونیکس برای افراد ناآشنا با آن نیست؛ البته، اگر تنها با چگونگی ورود به سیستم آشنا باشید، می‌توانید مؤلفه‌های شبکه‌ای یونیکس را تجربه نمایید.



***یادداشت** : شناختن فروشندگان مهم در یونیکس مهم نیست؛ چیزی که از اهمیت برخوردار است دانستن این نکته می‌باشد که انواع مختلفی از یونیکس وجود دارد. با این‌که روش کارکرد آنها با دیسک‌های سخت و ترمینال‌ها بسیار متفاوت است، اما بسیاری از دستورات TCP/IP از تشابه بسیاری برخوردارند.*

دیدگاه کلی

اجازه دهید نگاهی به چگونگی پیکربندی سرویس‌دهنده‌های یونیکس داشته باشیم. بله، این سرویس‌دهنده‌ها قابلیت انجام «فایل و چاپ» به شکلی که شبکه‌های ویندوز به انجام می‌رسانند را دارند و می‌توانید حروف گردونه‌ای ویندوز ۹۵ یا پورت‌های LPT را به یونیکس متصل کنید (اگر در دستگاه ویندوز ۹۵ شما، سرویس‌گیرندهٔ شبکه‌ای مناسب بارگذاری شده باشد). البته گذشته از این، سرویس‌دهنده‌های یونیکس در بیشتر اوقات به شکل سرویس‌دهنده/سرویس‌گیرنده برخورد می‌کنند.



***یادداشت** : باید این مطلب را ذکر کنم که تفاوت بسیار کوچکی بین ایستگاه‌کاری یونیکس و سرویس‌دهندهٔ یونیکس وجود دارد که این تفاوت جدای از افزونگی سخت‌افزار و سرعت می‌باشد.*

سرویس‌گیرنده/سرویس‌دهنده

در فصل ۱۸ کمی در مورد سرویس‌گیرنده/سرویس‌دهنده صحبت خواهم نمود. در این‌جا، دانستن این نکته کافی است که

سرویس‌گیرنده/سرویس‌دهنده در اصل روشی است برای گفتن، «اگر از کسی قیمت یک ویجت را بپرسم، پاسخی به من داده خواهد شد».این حالت خلاف شکل فایل و چاپ است که در آن، کاتالوگ کامل ارائه می‌شود. می‌توانید تصور کنید که سرویس‌گیرنده/سرویس‌دهنده شبیه حالت پرسش/پاسخ است. برای مثال، سرویس‌های نام DNS، نمونه خوبی از سرویس‌گیرنده/سرویس‌دهنده می‌باشند. هنگام برقراری ارتباط با www.jotto.com، پرسش شما از سرویس‌دهنده و درخواست شما، فهرست کامل ناحیهٔ com. نیست؛ به‌جای آن، آدرس IP مربوط به www.jotto.com مورد نظر است. سرویس‌دهنده آدرس 205.134.224.21 را باز می‌گرداند. تراکنش ساده‌ای است. سرویس‌گیرنده سؤالاتی را می‌پرسد و سرویس‌دهنده پاسخها را فراهم می‌کند. در صورت پیکربندی برای انجام چنین کاری، هر ماشین می‌تواند به شکل سرویس‌دهنده یا سرویس‌گیرنده عمل نماید.



***یادداشت** : با نحوهٔ بیان کلمات مشغلهٔ الکترونیکی، VPN و اکسترانت توسط فروشنده‌ای که هراز گاهی به شما سر می‌زند آشنا هستید؟ سابق این حالت در مورد سرویس‌گیرنده/سرویس‌دهنده وجود داشت. از این واژه یکی دو سال پیش به گونهٔ وسیعی استفاده می‌شد. البته با این‌که تب سرویس‌گیرنده/سرویس‌دهنده از انواع بازاری آن فروکش کرده، اما به‌خوبی می‌تواند چگونگی رخداد سرویس‌های یونیکس را توضیح دهد.*

هنگام آموزش در یک کلاس، اغلب به هر سرویس شبکه که نظیر فایل و چاپ نیست، شبکهٔ سرویس‌گرا می‌گویم، اما از آنجا که شاید هیچ‌کس دیگری در دنیا این لغت را استفاده نکند، من نیز به استفاده از واژهٔ سرویس‌گیرنده/سرویس‌دهنده اکتفا می‌کنم.

پیکربندی یونیکس

پیکربندی یونیکس نظیر هر کامپیوتر دیگری با اتصال یک کارت شبکه روی برد اصلی، اتصال این کارت به هاب، روشن‌کردن کامپیوتر، و پیکربندی آن صورت می‌گیرد. چندان سخت به نظر نمی‌رسد. مطلبی که در مورد یونیکس باید به خاطر داشته باشید آن است که تنها استانداردهای موجود، استانداردهای مبتنی بر TCP/IP می‌باشند. استانداردی برای NetBEUI و IPX/SPX وجود دارند اما توسط فروشندگان دستهٔ سوم عرضه می‌شوند (و خارج از میدان کاری این کتاب می‌باشند).

سرویس‌دهنده‌های یونیکس از طریق برنامه‌های کاربردی سرویس‌گیرنده/سرویس‌دهنده، سرویس‌ها و پایگاههای اطلاعاتی خود را در اختیار کاربران قرار می‌دهند. در گذشته این کار اکثراً توسط *Telnet* صورت می‌پذیرد که روشی بود برای اجرای یک جلسهٔ ترمینالی مبتنی بر کاراکتر روی یک کامپیوتر یونیکس در شبکه. اخیراً، این شکل تبدیل شده به استفاده از پایانه‌های گرافیکی ویندوز که تقریباً همان کار را انجام می‌دهند (گو این‌که ممکن است ارتباط با میزبان یونیکس از طریق شمارهٔ سوکت متفاوتی صورت گیرد). بیشتر این ارتباط، از طریق TCP/IP انجام می‌شود.

از آنجا که TCP/IP به صورت گسترده‌ای مورد استفاده است، مانعی در استفاده از یونیکس ایجاد نمی‌کند. مشکل اصلی یونیکس برای بیشتر افراد آن است که دستورات رمزگونهٔ بسیاری وجود دارند که باید برای پیکربندی کامپیوتر تایپ شوند. با این‌که یونیکس قبل از آنکه ویندوز 3.1 برقی در چشمان بیل گیتس باشد، به سیستم پنجره‌ای (به نام X Window مجهز بود، همیشه کمی «با کاربر متخاصم» به نظر رسیده است ـ استفاده از آن مستلزم ویرایش فایل‌های پیکربندی بسیار است و نابخشنده در مورد اشتباهات صورت‌گرفته توسط کاربر می‌نماید. خلاصه، باید گفت که با وجود رشد و بلوغ سیستم پنجره‌ای در سالهای اخیر، استفاده از آن همیشه یک مشکل واقعی بوده است. روشهای استانداردی برای پیکربندی

شبکه از طریق سیستم پنجره‌ای وجود ندارد؛ بنابراین در مورد پیکربندی شبکه از سطر فرمان و عیب‌یابی آن به این صورت صحبت خواهم کرد. اجازه ندهید که این موضوع مانع کار شما شود ـ فکر کنید که برای تقویت تایپ این کار را انجام می‌دهید. از آن گذشته، با یادگیری این موضوعات، بیشتر آن تحت ویندوز 9x و NT به‌کار خواهد آمد ـ چیزی که بیشتر آن در پس پرده مخفی مانده بود) کار میکروسافت در تبدیل پیکربندی اولیه شبکه به تجربه‌ای زیبا و بدون درد سر عالی بوده است).



***یادداشت** : افراد زیادی را می‌شناسم که از کار با سیستم‌های یونیکس در هراس هستند و به سیستم عامل لینوکس روی آورده‌اند که می‌توان گفت تنها شبیه به یونیکس کار می‌کنند. بسیاری از افراد در کامپیوترهای شخصی خود این سیستم را نصب می‌کنند و با آن آموزش می‌بینند. این موضوع را بسیار توصیه می‌کنم ـ از تخریب حاصل از آموزش و یادگیری نترسید که این یکی از بهترین روشهای آموختن است. همچنین نصب سیستمی را انجام می‌دهید که به نظر سیستم عامل پیچیده‌ای می‌آید و خواهید دید که کاملاً آسان می‌باشد.*

بسیاری از فروشندگان یونیکس تجاری نیز تنها به همین منظور گونه‌هایی از یونیکس تک‌کاربرهٔ خود را ارائه می‌کنند. اگر به فراگیری یونیکس نیاز دارید بهتر است این شکل را امتحان کنید. برای مثال شرکت‌های SCO (www.sco.com) و Sun (www.sun.com) از این سیاست پیروی می‌کنند.

با وجود تلاش میکروسافت، NT هنوز موفق نشده تمامی ناهار یونیکس را میل کند. توانایی یونیکس در پیکربندی دوباره بدون نیاز راه‌اندازی مجدد و مسیری که در بهترشدن می‌پیماید، باعث شده که همواره توسط افرادی که مراکز اطلاعاتی بدون توقف را اداره می‌کنند، مورد توجه باشد. سرویس‌دهنده‌های یونیکسی را دیده‌ام که بدون راه‌اندازی مجدد دو سال کار کرده‌اند (سرپرست آن سیستم یونیکس، کمی مجنون به‌نظر می‌رسید، چرا که رهاکردن هر سرویس‌دهنده‌ای به این مدت طولانی، بازی‌کردن با آتش است؛ اما با این وجود نکتهٔ جالب و احساس‌برانگیز است).

دیمون‌های دوست‌داشتنی

اجازه دهید در مورد روش ردیابی برنامه‌های اجرایی روی سرویس‌دهندهٔ یونیکس صحبت کوتاهی داشته باشیم. همان‌طور که می‌دانید، ویندوز ۹۵ برنامه‌هایی را که در حال اجرا هستند، در کازیهٔ سیستم (میلهٔ خاکستری رنگ در گوشهٔ پایینی صفحه) نشان می‌دهد. در مورد سرویس‌دهندهٔ یونیکس اغلب اوقات صدها برنامه با هم به اجرا درمی‌آیند ـ شاید به این خاطر که هر سرویس‌گیرنده‌ای که به سرویس‌دهنده متصل می‌شود، اغلب باعث شروع یک برنامهٔ جدید برای سرویس‌دهی به سرویس‌گیرنده می‌گردد. در ویندوز ۹۵، اگر می‌خواستیم این تعداد را در کازیه نشان دهیم، کمی شلوغ می‌شد! به‌جای آن، یونیکس از یک جدول داخلی فرایند استفاده می‌کند که شماره‌ها، اسامی و سایر اطلاعات فرایندها را نگهداری می‌نماید.



***یادداشت** : هر سرویس‌دهندهٔ یونیکس نظیر دستگاه ویندوز ۹۵ شما می‌تواند تعداد زیادی برنامه را به صورت همزمان اجرا کند. تمامی این برنامه‌ها ممکن است به‌صورت مستقیم با کاربر تراکنشی نداشته باشند. بسیاری از آنها در پس‌زمینه اجرا می‌گردد. به این برنامه‌های پس‌زمینه، دیمون گفته*

می‌شود. تمامی سرویس‌های یونیکس نظیر Telnet، HTTP و FTP به‌صورت دیمون اجرا می‌شود. هنگامی‌که به فهرست فرایندها نگاه می‌کنید، درمی‌یابید که هر فرایند یک دیمون است: حرف d در پایان اسم آن ظاهر می‌شود. هنگامی‌که در مورد دیمون صحبت می‌کنیم، اغلب حرف d را در پایان تلفظ می‌کنیم، مثلاً برای named می‌گوییم name-dee.

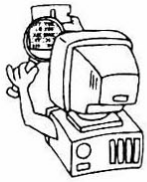
فرض کنید که سرویس خاصی در سرویس‌دهندهٔ یونیکس مورد نظر در حال اجرا نباشد؛ برای مثال، به نظر می‌رسد که سرویس‌دهندهٔ وِب فعال نیست. به‌جای راه‌اندازی مجدد سرویس‌دهنده (ممکن است در کار بقیهٔ سرویس‌ها با انجام این عمل وقفه ایجاد شود)، بهتر است ابتدا بررسی کنید که فرایند سرویس‌دهندهٔ وِب در حال اجرا است یا خیر و آنگاه تصمیم بگیرید که آن را متوقف نموده و یا مجدداً آغاز کنید. اغلب اوقات برای توقف یا شروع فرایندها باید به‌صورت کاربر ویژه (root) وارد شده باشید.



***هشدار** : می‌توانید هنگام اجرا با عنوان کاربر ریشه، تخریب زیادی را ایجاد کنید؛ باید از دستور su (کاربر ویژه) برای دستیابی موقت به حقوق خاص کاربر ویژه استفاده کنید، دستورات خود را به اجرا درآورید، و آنگاه خارج شوید. می‌توانید به میزان زیادی با نصب یک سیستم آموزشی روی یک دستگاه PC به میزان زیادی اعتماد به نفس خود را بالا ببرید.*
از آنجا که اعلان ریشه (#) اغلب از اعلان معمولی ($) متفاوت است، من در این متن از اعلان ویژهٔ ریشه استفاده می‌کنم تا نشان دهم دستورات را در حالت استفاده از کاربر ویژه اجرا می‌نمایم.

بسته به نوع یونیکس مورد استفاده، یکی از دستورات زیر را برای نگریستن به جدول فهرست مورد استفاده قرار دهید:

```
ps -ef
ps -ax
```



***نکته** : منظور از ef- و ax- چیست؟ خوب، اینها نشانهایی هستند که به برنامهٔ ps (وضعیت فرایند) می‌گویند که شما می‌خواهید تمامی اقلام موجود در جدول فرایندها را مشاهده کنید. در سیستم‌های مختلف، این نشانها با یکدیگر متفاوت هستند. بنابراین خیلی سریع باید بدانید که کدامیک از نشانها را مورد استفاده قرار دهید. بیشتر سیستم‌های یونیکس دارای صفحات راهنمایی هستند که در سیستم قابل دسترسی و استفاده است. دستور man (مخصوص وارسی صفحات راهنما) جزئیات هر دستوری که بخواهید را در اختیارتان می‌گذارد. برای مثال، به‌منظور دریافت جزئیات مربوط به نشانهای ef- و ax- و معانی آنها در دستور ps، و همچنین پیداکردن سایر نشانه‌های موجود، دستور زیر را اجرا کنید:*

```
man ps
```

یکی از بهترین روش‌های فراگیری یونیکس، استفاده از صفحات man می‌باشد؛ برای یادگیری در مورد چگونگی استفاده از دستور man، می‌توانید فرمان زیر را به اجرا درآورید:

```
man man
```

دستور ps مخفف کلمات process status (وضعیت فرایند) می‌باشد. در یک سیستم شلوغ، صدها فرایند صفحه‌نمایش را اشغال می‌کنند. خوشبختانه می‌توانید صفحه‌نمایش را متوقف کنید یا حتی بهتر در جدول فرایندها دنبال آنچه که می‌خواهید بگردید. برای مثال فرض کنید در جستجوی سرویس‌دهندهٔ وِب، دیمون http، یا httpd می‌گردید (http از http:// آمده که هنگام پیداکردن یک صفحهٔ وِب آن را مورد استفاده قرار می‌دهیم و مخفف پروتکل انتقالی فوق متن[1] می‌باشد. بنابراین این برنامهٔ httpd هم دیمون پروتکل انتقالی فوق متن است). می‌توانستید دستور زیر را اجرا کنید.

```
ps -ax | grep httpd
```

ممکن است پاسخی بازگردانده نشود ـ که این احتمالاً به معنای ختم httpd می‌باشد و لازم است دوباره آن را اجرا کنید. البته در صورت عدم خاتمهٔ اجرا، ممکن است پاسخی نظیر این را دریافت کنید:

```
52 ?   s      0:01   /usr/sbin/httpd
```

شمارهٔ اول، عبارت است از شناسهٔ فرایند (یا *PID*) این شماره‌ای است که هنگامی‌که کاری با فرایند دارید به آن مراجعه می‌کنید. برای مثال، دستورات خاتمه و اجرای دوبارهٔ فرایند به شکل زیر خواهند بود:

```
$ ps -ax | grep httpd
   52  ? S    0:01 /usr/sbin/httpd
$ su
Pasword:
#kill 52
# ps -ax | grep httpd
# /usr/bin/httpd
# ps -df | grep httpd
   871 ? S    0:01 /usr/sbin/httpd
```

توجه کنید که از su تا هنگامی‌که دقیقاً نخواهم فرایند را خاتمه دهم و دوباره آن را به اجرا آورم استفاده ننموده‌ام. بعد از آن هم بلافاصله از جلسهٔ su خارج شده‌ام تا خطر استفاده از کاربر ویژه را به حداقل برسانم. همچنین مایلم که جدول فرایندها را قبل و بعد از شروع دوبارهٔ دیمون وارسی نمایم تا مطمئن شوم قبل و بعد از اجرای دستورات، فرایند در چه وضعیتی قرار دارد.

آیا لازم است هنگام بررسی دیمون‌ها همگی حضور داشته باشند؟ در واقع، خیر. به روزهای کمبود حافظه بازگردیم، که در آن مفهوم دیمون پذیرا ابداع گشته بود تا دیمون‌هایی که استفاده نمی‌شدند، در حافظه بارگذاری نمی‌گردیدند. این برنامهٔ پذیرا، inetd (دیمون اینترنت) نامیده می‌شود و مسئول ارائهٔ فهرست ارتباطات بوده و به فراخواننده می‌گوید که صبر کند و آنگاه دیمون مورد نظر را بیدار کرده و فراخوانی را به انجام می‌رساند. برخی دیمون‌هایی که به این شکل فراخوانی می‌شوند عبارتند از telnetd (دیمون Telnet) و ftpd (دیمون FTP). با مشاهدهٔ محتویات inetd.conf که چیزی نظیر این به نظر خواهد آمد، می‌توانید دیمون‌هایی را که توسط inetd فراخوانی می‌شوند، مشاهده نمایید:

```
# If you make changes to this file, either reboot your machine or send
# the inetd a HUP  signal:
# Do a "ps x" as root and look up the pid of inetd. Then do a
# "kill -HUP <pid of inetd>".
# The inetd will re-read this file whenever it gets that signal.
# Echo, discard, daytime, and chargen are used primarily for testing.
# Format is:
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
echo      stream   tcp   wait   root    internal
```

1- Hypertext Transfer Protocol

```
echo      dgram    udp   wait   root    internal
discard   stream   tcp   nowait root    internal
discard   dgram    udp   wait   root    internal
daytime   stream   tcp   nowait root    internal
daytime   dgram    udp   wait   root    internal
chargen   stream   tcp   nowait root    internal
chargen   dgram    udp   wait   root    internal
ftp       stream   tcp   nowait root    /usr/sbin/tcpd    /usr/sbin/wu.ftpd-a
telnet    stream   tcp   nowait root    /usr/sbin/tcpd    /usr/sbin/in.telnetd
```

می‌توانید با استفاده از دستور kill اجرای inetd را متوقف‌کرده و یا آغاز بخشید. این‌کار تأثیر بیشتری از خاتمهٔ اجرای یک دیمون دارد، چرا که inetd نظیر میزبان بسیاری از سرویس‌ها عمل می‌کند؛ بهتر است از دستور kill -HUP PID استفاده کنیم تا inetd مجبور شود در ابتدا پیکربندی خود را مجدداً بخواند.

البته دیمون‌های با اهمیت، با اتکاء به خود اجرا می‌شوند که از آن جمله می‌توان دیمون نام DNS (named) را نام برد که برخی اوقات به آن in.named نیز اطلاق می‌شود. آغاز دوبارهٔ این دیمون‌ها نیز نظیر httpd، می‌تواند بدون نگرانی از تحت تأثیر قرار گرفتن سایر سرویس‌ها صورت پذیرد.

در مورد named، اگر در حال اجرا بوده اما اطلاعات درستی را حتی پس از آغاز دوباره ارائه نمی‌کند، ممکن است بخواهید صحت برخی از فایل‌های پیکربندی مربوط به آن را وارسی کنید (همواره می‌توانیم از یک کپی پشتیبان «سالم» بازنشانی نمایید). فایل اولیه named، عبارت است از /etc/named.boot که فایل‌های متعدد دیگری را برای عملکرد دیمون شامل می‌شود. برای دریافت اطلاعات بیشتر در مورد named می‌توانید به صفحات راهنمای موجود در man مراجعه کنید.



نکته : *خوب است ذکر کنیم که سرویس‌گیرندهٔ named در سرویس‌دهندهٔ یونیکس همیشه جستجوی اسامی را از سرویس‌دهندهٔ نام خود صورت نمی‌دهد؛ و تمامی سرویس‌دهنده‌های یونیکس نیز سرویس‌دهندهٔ نام را اجرا نمی‌کنند. پیکربندی جاری مربوط به سیستم خود را می‌توانید از طریق بررسی فایل /etc/resolv.conf ملاحظه نمایید.*

هر سرویسی ممکن است بیش از یک دیمون را اجرا کند. برای مثال، NFS (سیستم فایلی شبکه، سرویس فایل و چاپ برای یونیکس) این‌گونه است. این سرویس دیمون‌های مختلفی را برای وظایف مختلف اجرا می‌کند ـ biod، nfsd، mountd ـ و به دیمون دیگری به نام portmapper اتکا می‌کند. NFS می‌تواند یک هیولا باشد؛ اگر خوش‌شانس باشید ممکن است در سیستم‌تان برای هر سرویس یک اسکریپت آغازین وجود داشته باشد.که مثلاً برای آغاز دوبارهٔ NFS دستورات زیر را تایپ و اجرا نمایید:

```
# cd /etc/init.d
# ./S80nfs stop
# ./S80nfs start
```

اغلب، سیستم‌هایی که از استانداردهای SVR4 (که به‌صورت اس وی آر فور تلفظ می‌شود و مخفف سیستم V، نگارش ۴ می‌باشد) استفاده می‌کنند، نظیر UNIXWare و Red Hat Linux، این نوع اسکریپت‌های شروع و پایان را دارا هستند. اگر سیستم شما بیشتر به نگارش دانشگاهی یونیکس (BSD، یا توزیع استاندارد برکلی[1]، نظیر AIX و

1- Berkley Standard Distribution

Slackware Linux)، می‌ماند به یک دستور start مجهز است که جایی در فایلی به نام /etc/rc.something قرار دارد. می‌توانید بررسی کنید چه کسی برای استفاده از یک فایل سیستمی به‌خصوص مجاز است (معادل اشتراک تحت ویندوز NT). فایل /etc/exports این اطلاعات را در اختیارتان می‌گذارد. اگر در این فایل تغییری بدهید، لازم خواهد بود دستور exportfs -a را اجرا نمایید. اسم میزبانی که اضافه کرده‌اید باید در ناحیهٔ DNS شما در فایل /etc/hosts ظاهر شود (برای مثال company.com).

برقراری سوکت

برخی اوقات صرفاً آغاز و پایان‌بخشیدن به یک دیمون مشکل را حل نمی‌کند. در مورد inetd ممکن است در موقعیتی باشید که این معالجه از خود بیماری بدتر باشد. در چنین حالاتی، به معالجهٔ ملایم‌تری نیاز داریم.

دستور netstat -a را اجرا کنید. این دستور برای سوکت‌های شبکه، نظیر ps برای فرایندها می‌ماند (از فصل ۱ به‌خاطر بیاورید که سوکت نظیر یک انشعاب تلفنی است که با آن یک سرویس منتظر دریافت تماسها می‌ماند). netstat فهرست تمامی سوکت‌هایی را که در اتصال جاری مورد استفاده قرار گرفته‌اند و یا در وضعیت شنود برای آغاز اتصال به سر می‌برند، نشان می‌دهد. این برنامه وضعیت ثبت، محل ثبت و سوکت‌هایی که در هر دو انتهای تماس مورد استفاده قرار گرفته‌اند را ارائه می‌کند. دستور netsata -an تنها امکان مشاهدهٔ مقادیر عددی را میسر می‌سازد که هنگامی‌که می‌خواهید سرویس‌های نام را از تصویر خروجی کنار بگذارید، به‌کار می‌آید. اجازه دهید به مثال خاصی توجه کنیم.

فرض کنید شخصی با شما تماس می‌گیرد و می‌گوید که نمی‌تواند وارد FROTZ شود. وی عصبانی‌تر از آن است که به سؤالات شما پاسخ دهد.

می‌دانید که این شخص در دپارتمان مالی کار می‌کند. پاسخ سؤال «آیا افراد دیگر هم این مشکل را دارند؟» نیز داده نمی‌شود. بنابراین تصمیم می‌گیرید که خودتان این موضوع را روشن کنید. با بررسی سریع نقشهٔ یک شبکه و آشکارشدن آدرس بخش مالی در زیرشبکهٔ 200.1.1.0، به میزبان یونیکس FROTZ وارد می‌شوید و دستور زیر را تایپ می‌کنید:

ورودی

```
netstat -a | grep 200.1.1
```

پاسخ زیر داده می‌شود:

خروجی

```
Proto send-q  recv-q  Local Address           Foreign Address   (State)
tcp    0      0      frotz.frob.com.telnet   200.1.1.10.1673   ESTABLISHED
tcp    0      0      frotz.frob.com.telnet   200.1.1.25.1975   ESTABLISHED
tcp    0      0      frotz.frob.com.telnet   200.1.1.27.1772   ESTABLISHED
tcp    0      0      frotz.frob.com.telnet   200.1.1.29.1968   ESTABLISHED
tcp    0      0      frotz.frob.com.telnet   200.1.1.33.1492   ESTABLISHED
tcp    0      0      frotz.frob.com.telnet   200.1.1.34.1444   ESTABLISHED
tcp    0      0      frotz.frob.com.telnet   200.1.1.35.2855   ESTABLISHED
```

تحلیل ستون عناوین را برای وضوح بیشتر وارد کرده‌ام؛ هنگام جستجوی یک آدرس این ستون ارائه نمی‌شود. خیلی سریع مشخص می‌شود که افرادی از شبکهٔ 200.1.1 در حال کار بوده و به درستی و بدون مشکل به فعالیت خود ادامه می‌دهند. (در واقع، می‌توانستید از دستور who استفاده کنید که در بیشتر ماشینهای یونیکس نشاندهندهٔ کسانی است که

وارد سیستم شده و محلی که از آن این کار را انجام داده‌اند. البته، netstat تمامی سرویس‌ها را نشان می‌دهد و نه تنها Telnet را). اکنون می‌دانید که افراد بخش 200.1.1.0 وارد سیستم شده‌اند و به این موضوع شک می‌کنید که مشکل کاربر، مربوط به ایستگاه‌کاری وی می‌باشد.

proto پروتکل مورد استفاده است. در بیشتر حالات، tcp یا udp می‌باشد. TCP معادل یک تماس تلفنی (با گرایش مداری) و UDP معادل پرتاب کاغذهای یادداشت به سوی یکدیگر (بدون اتصال) می‌باشد. اطلاعات بیشتر در مورد UDP را در فصل ۱۵ و فصل ۱۸ پیدا خواهید نمود. send-q و recv-q نمایندهٔ محل‌های نگهداری اطلاعات ارسالی و دریافتی در حافظهٔ میزبان می‌باشد. می‌توانید تصور مشابهی از صف چاپ نسبت به آنها داشته باشید. آنها حاوی اطلاعاتی هستند که منتظر پردازش مانده‌اند. برخلاف صف چاپ، در عملکردی عادی وضعیت این مکانهای حافظه‌ای، خالی می‌باشد. یعنی این مقادیر برای شبکه‌های محلی اغلب صفر هستند، چرا که این‌گونه شبکه‌ها با سرعت زیادی اجرا می‌شوند.

اگر این مقادیر صفر نباشند چه؟ خوب تغییری در «صف ارسال» به آن معنا است که پایانهٔ دیگر در آن سو اطلاعات را پردازش می‌کند، اما به‌خاطر دلیلی متوقف یا کند شده است. این اغلب، یک وضعیت معمولی برای سرویس‌دهندهٔ چاپ در LAN می‌باشد؛ این صف، به‌واقع یک صف چاپ است، بنابراین اطلاعاتی را پردازش می‌کند آنگاه متوقف می‌شود و اطلاعات بیشتری را دریافت می‌کند و به همین صورت به کار خود ادامه می‌دهد. اگر صف ارسال غیر صفر باشد و مقدار آن برای یک سوکت تغییر نکند، این اغلب به معنای آن است که چیزی در آن سوی خط پذیرش اطلاعات را متوقف نموده است.

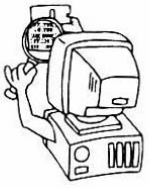
صف دریافت غیر صفر می‌تواند بدان معنا باشد که چیزی در خود میزبان یونیکس با کمبود منابع مواجه شده و موقتاً قادر به پردازش اطلاعات ورودی نیست. این وضعیت در عمل بسیار نادر می‌باشد.

آدرس محلی، سرویس‌دهنده‌ای است که دستور netstat روی آن اجرا شده و در این حالت که در مورد سرویس Telnet صحبت می‌کنیم، آدرس کامل wefrotz.frobozz.com.telnet می‌باشد. اگر از دستور netstat با سوئیچ an- استفاده کرده بودیم، این آدرس به‌صورت 192.168.55.10.23 (Telnet در سوکت 23 واقع شده است) ظاهر می‌شد. آدرس خارجی، آدرس ماشین سرویس‌گیرنده می‌باشد. در این‌جا سوکت اهمیت چندانی ندارد ـ هر شمارهٔ بزرگی که از قبل مورد استفاده قرار نگرفته را می‌توان در طرف سرویس‌گیرنده استفاده کرد.



نکته : *می‌توانید تعداد سوکت‌های سرویس‌گیرنده/سرویس‌دهنده جاری را در هر زمان دلخواه، مثلاً در سرویس‌دهندهٔ پستی imap شمارش کنید:*

```
netstat -a | grep imap | wc -1
```



نکته : *می‌توانید سرویس‌های منتظر ارتباط را با استفاده از دستور زیر پیدا کنید:*

```
netstat -a | grep LISTEN
```

این دستور سرویس‌هایی را که به منظور ایجاد اتصالهای جدید در حال شنود هستند را نشان می‌دهد. از آنجایی که اسامی سرویس اغلب اسمی مشابه یا مطابق با اسامی برنامه‌ها دارند (سرویس http /برنامهٔ httpd)، به‌راحتی می‌توانید بیابید که چه برنامه‌ای مسئول ارائه چه سرویسی می‌باشد.

بازی اسامی

بدون سرویس‌های نام، کار خیلی کمتری خواهیم داشت. با این‌که می‌توانید مشکل مربوط به سرویس نام را بدون استفاده از نام و تنها با آدرس IP صورت دهید، مشکلاتی که برای سرویس‌های نام پیش می‌آیند اغلب پیچیده بوده و با ترفندهای خاص قابل حل می‌باشند.



یادداشت : *درک این موضوع مهم است که اتصالات موجود به کار خود ادامه خواهند داد؛ تنها اتصالات جدید ممکن است با شکست مواجه شوند.*

هر میزبان یونیکس بعد از ایجاد اتصال در میزبان تحلیل نامش به جستجوی نام می‌پردازد تا موجودیت سمبولیک فراخواننده را دریافت کند. بنابراین، اگر سرویس‌های اسامی با مشکلی مواجه باشند، این موضوع می‌تواند یک تأثیر جانبی را ایجاد کند که باعث بروز مشکلاتی برای سایر سرویس‌ها می‌گردد.

من در عمل مشکلات بسیاری را مشاهده می‌کنم که به DNS وابسته هستند، حتی با این وجود که برخی از آنها در وهلهٔ اول چنین حقیقتی را آشکار نمی‌سازند. برای مثال، بعد از ختم یک سرویس‌دهندهٔ نام در میزبان یونیکس، جلسه‌های Telnet به آن میزبان برای نمایش اعلان ورود به سیستم، کاربر را با وقفه‌ای طولانی مواجه می‌سازند. یعنی، با این‌که اتصال مورد پذیرش واقع شده و خروجی دستور netstat -an نشاندهندهٔ برقراری اتصال است، چیزی از دریافت اعلان ورود به سیستم جلوگیری می‌کند.

این چیز سرویس‌دهندهٔ DNS است. سرویس‌دهندهٔ Telnet طوری پیکربندی شده که تمامی آدرس‌های Telnet متصل‌شونده را بعد از اتصال آنان جستجو کند؛ با وجود ختم سرویس‌دهندهٔ نام، سرویس Telnet تلاش خود را قبل از انتشار اعلان ورود به سیستم صورت می‌دهد. بسته به سیستم عامل و پیاده‌سازی Telnet، این موضوع می‌تواند وقفه‌های طولانی را ایجاد نماید.

nslookup

ابزار بررسی سرویس‌های نام، nslookup نامیده می‌شود. همانگونه که از اسم آن پیداست، این ابزار با یک سرویس‌دهندهٔ نام تماس می‌گیرد (حروف ns در نام ابزار از name server آمده است) و به جستجوی اطلاعات در آن می‌پردازد. اگر بدانید که میزبان یونیکس‌تان در حال اجرای named می‌باشد و باید بتواند به پرس‌وجوهای نام مربوط به خود و دیگران پاسخ دهد، می‌توانید دستور زیر را اجرا کنید:

```
nslookup اسم‌میزبان اسم‌میزبان
```

باید پاسخی دریافت کنید. در صورت دریافت پیغام خطا، named‌ای که روی اسم‌میزبان اجرا می‌شود، احتمالاً فعال نیست.



یادداشت : *توجه داشته باشید که می‌توانید nslookup را روی هر میزبانی به اجرا درآورید، اجرای این برنامه از هر جایی که وارد سیستم شده‌اید، میسر است.*

یک حالت محاوره‌ای نیز وجود دارد که برای تحلیل موضوعات پیچیدهٔ DNS مفید واقع می‌شود. این ویژگی را در فصل ۱۹ بررسی خواهیم کرد.

مکان قطبی

بعضی اوقات یک مشکل شبکه‌ای در یونیکس، در سرویس‌های سطح بالا و برنامه‌ها وجود ندارد ـ به‌عبارت دیگر، ممکن است مشکل در «افراد پشت خط تلفن» نباشد بلکه خود تلفن یا سیستم ارتباطی مشکل داشته باشد. برای تشخیص این موضوع می‌توانید تکنیک‌ها و دستوراتی را به کار بگیرید.



نکته : *هنگامی‌که هیچ‌چیز کار نمی‌کند، ممکن است مجبور باشیم از ترمینالی که به‌صورت فیزیکی به سرویس‌دهنده متصل شده است استفاده نموده وارد سیستم شوید. اگر کنسول مذکور هم پاسخ نمی‌دهد، سرویس‌دهندهٔ یونیکس قفل کرده است. این موضوع ربطی به شبکه ندارد ـ بسیار به ندرت این اتفاق می‌افتد، اما باید متوجه وقوع آن باشید. تنها گزینهٔ شما در این‌جا آن است که خود را عقب بکشید، سرویس‌دهنده را خاموش کنید و امیدوار باشید که بدون مشکل دوباره به‌کار بیفتد.*

با فرض کارکردن کنسول، زمان آن می‌رسد که این موضوع را روشن کنید که چرا سرویس‌دهندهٔ یونیکس از طریق شبکه دیده نمی‌شود. اجازه دهید از درون به بیرون نگاه کنیم و فرض کنیم که، نظیر دکتر فروید، تمامی تحلیل‌ها از خود شروع می‌شود. اولین چیزی که باید به آن توجه کنید آن است که برای دسترسی به هر چیزی به یک کارت شبکه نیاز دارید. اجازه دهید اول آن را بررسی نماییم:

```
# ifconfig -a
lo      Link encap:Loopback
        inet addr:127.0.01 Bcast:127.255.255 Mask:255.0.0.0
        UP BROADCAST LOOPBACK RUNNING MTU:2000 Metric:1
        RX packets:0 errors:0 dropped:0 overnus:0
        TX packets:37231 errors:0 dropped:0 overruns:0

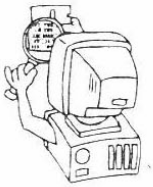
eth0    Link encap:10Mbps Ethernet HWaddr 00:00:c0:82:26:94
        inet addr:167.195.160.6 Bcast:167.195.160.255 Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:816928 errors:0 dropped:0 overruns:0
        TX packets:654019 errors:0 dropped:0 overruns:0
        Interrupt:10 Base address:0X350 Memory:c8000-cc000
```

موارد کلیدی که باید به آنها توجه کنیم کلمات up و running می‌باشند. اگر آنها را نمی‌بینید، چیزی باعث شده که کارت شبکه‌تان فعالیت نکند. این حالت در مورد برخی از کارتهای شبکه هنگامی پیش می‌آید که پورتی روی یک هاب اشکال داشته باشد، پس باید صبر کنید پورت را عوض نمایید. راه‌اندازی مجدد ممکن است اوضاع را به وضع عادی برگرداند یا این‌که ممکن است عملاً کارت شبکه خراب باشد. همچنین می‌توانید از netstat -a برای بررسی تعداد خطاها و /یا از ethstat برای مشاهدهٔ انواع خطاهایی که وجود دارند استفاده نمایید. این‌کار ممکن است مشکلی شبکه‌ای را و نه مشکلی یونیکسی را آشکار سازد.

کار بعدی که انجام می‌دهید استفاده از دستور ping برای بررسی توانایی ماشین در صحبت با خودش می‌باشد:

```
$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=255 time=8.5 ms
64 bytes from 127.0.0.1: icmp_seq=0 ttl=255 time=8.5 ms
<CONTROL-C>
-127.0.0.1 ping statistics-
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 6.8/7.6/8.5 ms
```

به این آدرس توجه خاصی داشته باشید: 127.0.0.1 آدرس مخصوصی است که از آن به‌عنوان آدرس بازگشت حلقه یاد می‌شود. اگر نتوانید آن را ping کنید، با وضع واقعاً عجیبی روبرو هستید. در این‌جا هم راه‌اندازی مجدد ممکن است کارها را مرتب نماید. این یک بازگشت حلقهٔ نرم‌افزاری است، بنابراین مشکل در این‌جا ارتباطی به سخت‌افزار ندارد.



***نکته** : آدرس بازگشت حلقه روشی است که با آن می‌توانید سیستم یونیکس خود را وادار کنید با برنامه‌های TCP/IP خودش ارتباط برقرار کند، بدون آنکه از کارت شبکه برای این ارتباط بهره ببرد. هنگامی‌که به‌صورت موفق با استفاده از حلقهٔ بازگشت ارتباط برقرار می‌کنید، پشتهٔ برنامه‌ای TCP/IP را از مجموعهٔ مشکلات احتمالی کنار می‌گذارید.*

گام بعدی آن است که کارت شبکهٔ خود را ping کنید. اگر برای مثال، شمارهٔ TCP/IP سرویس‌دهنده‌تان 192.168.99.5 می‌باشد دستور زیر را اجرا نمایید:

```
$ 192.168.99.5
```

خروجی این دستور باید مثل خروجی ping حلقهٔ بازگشت باشد.

اگر این حالت کار کرد، باید مسیریاب را ping کنید. در صورت عدم کارکرد، باید مطمئن شوید که می‌توانید بقیه ایستگاههای کاری در بخش مربوط به خود را می‌بینید. آیا آنها می‌توانند مسیریاب را ببینند؟ مسیریاب ممکن است غیر فعال شده باشد، و به این ترتیب افراد سایر بخشها ممکن است تصور کنند میزبان یونیکس غیر فعال گردیده است.

در فصل ۱۴، netstat -r و همچنین traceroute را توضیح خواهم داد. دستور اول مسیری را که میزبان یونیکس فکر می‌کند بسته‌ها باید از طریق شبکه بپیمایند را نشان می‌دهد. دستور traceroute روشی عالی برای پیداکردن مسیریاب‌هایی است که هر بسته برای رفتن از نقطهٔ a به نقطهٔ b از آن عبور می‌کنند. نکته‌ای که در مورد این فرمان و یونیکس وجود دارد آن است که برخی از پیاده‌سازی‌های یونیکس آن را پشتیبانی نمی‌کنند. البته می‌توانید آن را از طریق ftp://ftp.ee.lbl.gov/traceroute.tar.Z دریافت نماید. برای استفاده از چنین منبعی باید با سطر فرمان یونیکس راحت بتوانید کار کنید، چرا که این برنامه در قالب خود منبع عرضه می‌شود ـ لازم است از دستور tar برای استخراج کُد منبع و دستور make برای ترجمه‌کردن و ساخت برنامه استفاده نمایید.

خلاصه

میزبانهای یونیکس، سرویس‌دهنده‌های قابل اطمینانی هستند که برای سکونت پایگاههای داده‌ای، برنامه‌های کاربردی سرویس‌گیرنده/سرویس‌دهنده و جلسه‌های Telnet به کار می‌رود. همچنین سرویس‌دهنده‌های وِب و ftp را می‌توان روی

آنها به اجرا درآورد.

بیشتر سرویس‌های یونیکس از طریق برنامه‌های پس‌زمینه‌ای که دیمون نامیده می‌شود به اجرا درمی‌آیند. برخی از مشکلات سرویسی را می‌توان با متوقف نمودن و شروع دوبارهٔ یک فرایند دیمون حل نمود.

بسیاری اوقات، لازم است دستوراتی را به‌عنوان کاربر ریشه (کاربر ویژه) اجرا نماییم. برای راحتی و افزایش قابلیت اعتماد به خود بهتر است یک سیستم آزمایشی راه‌اندازی کنید تا با آموزش در آن اشتباهات‌تان یک سیستم حساس را متأثر نکنند.

می‌توان سرویس‌ها و سرویس‌گیرنده‌هایی را که در سیستم به اجرا درآمده‌اند، با استفاده از دستور netstat -a ردیابی نمود. هر سیستم پرکار یونیکس می‌تواند از صدها تا هزاران سوکت باز داشته باشد؛ می‌توان با استفاده از دستور grep به همراه دستور netstat، دنبال اطلاعات سوکت مورد نظر خود بگردید.

در تشخیص محل مشکل و این‌که در سرویس‌دهندهٔ یونیکس، شبکه یا مسیریاب قرار گرفته است، ping بهترین دوست‌تان می‌باشد (و همچنین در عیب‌یابی TCP/IP).

کارگاه

پرسش و پاسخ

پرسش : من نمی‌توانم به فایلی در گردونهٔ G: (که روی سیستم فایلی home/ سرویس‌دهندهٔ یونیکس‌ام گذاشته شده) دسترسی داشته باشم، اما همکار بغل دستی‌ام می‌تواند. هنگامی‌که با مشخصات او وارد سیستم می‌شوم، می‌توانم فایل را دریافت کنم. مشکل در کجاست؟

پاسخ : موضوع امنیت در یونیکس و مجوزهای فایلی، موضوع وسیعی است و من در فصل ۱۸ به آن خواهم پرداخت، البته برای پاسخ به سؤال شما این امکان وجود دارد که فایل یا فهرست به گروهی تعلق داشته باشد که شما جزء آن نیستید. با استفاده از دستور ls -la نگاهی به فایل گروهها بیندازید و خودتان را به گروه مورد نظر اضافه کنید.

پرسش : به تازگی از امکانات یک فراهم‌کنندهٔ سرویس اینترنت جدید استفاده می‌کنیم و تمامی شماره‌های IP مان تغییر یافته‌اند. اکنون، هر زمان که سیستم یونیکس‌ام را راه‌اندازی می‌کنم، پیغام «NFS Server Belboz not responding» را دریافت می‌کنم. چرا؟

پاسخ : چنین به نظر می‌رسد که سیستم Belboz تنها در فایل /etc/hosts مربوط به سیستم یونیکس ذکر شده است. فایل را بررسی کنید، احتمالاً درمی‌یابید که شمارهٔ TCP/IP اشتباه است؛ آن را به مقدار جدید تغییر دهید.

پرسش : شنیده‌ام که امنیت یونیکس از سایر سیستم‌های عامل کمتر است. آیا این موضوع صحت دارد؟

پاسخ : خیر مشکل یونیکس آن است که از سیستم‌های عامل دیگر قابلیت پیکربندی بیشتری دارد، که این بدان معناست که برخی اوقات به صورت اشتباه پیکربندی شده و در نتیجه ناامن‌تر می‌نماید. با این‌که سطح دانش به‌کار گرفته شده در ساختار داخلی یونیکس بالاست، در برخی از پیاده‌سازی‌های کُد منبع وجود دارد که به ماجراجویان این امکان را می‌دهد که سوراخهای امنیتی در برنامه‌های ایجاد کنند. در واقع با این‌که کُد منبع ویندوز NT در دسترس نیست، مشکلاتی در برنامه‌های آن مشاهده شده است. یونیکس هم نظیر هر سیستم عامل دیگری مشکلات متعددی دارد، برنامه‌های

سرویس‌دهندهٔ گسترده ـ نظیر sendmail ـ باعث شده‌اند که نگرانی‌های امنیتی در مورد سیستم عامل بروز کنند اما این‌گونه اختراعات خیلی سریع رفو شده‌اند.

آزمون

۱- درست یا نادرست؟ برای دسترسی به تمامی دستورات شبکه‌ای در یونیکس لازم است به ریشه دسترسی داشته باشیم.

۲- NFS مخفف چه کلماتی است؟

الف ـ Network File Server
ب ـ Nothing Falls Slowly
ج ـ Network Failure System
د ـ Network File System

۳- درست یا نادرست؟ named از inetd به‌عنوان سرویس‌دهندهٔ پذیرا استفاده نمی‌کند؛ named با اتکا به خود در تمامی زمانها اجرا می‌شود و هر زمان که کاربر درخواست نمود، فراخوانی نمی‌گردد.

۴- درست یا نادرست؟ linux تنها به‌صورت رایگان یا سیستم ارزان‌قیمت یونیکس در دسترس است.

۵- تفاوت بین یک سرویس‌دهندهٔ یونیکس و ایستگاه‌کاری یونیکس اغلب در چیست؟

الف ـ نرم‌افزار متفاوت
ب ـ عرض باند متفاوت
ج ـ سرعت متفاوت
د ـ سخت‌افزار متفاوت

۶- بهتر است هنگام مواجه‌شدن با مشکلی در مورد یک سرویس یونیکس چه کاری را انجام دهید؟

الف ـ فرایند را متوقف و دوباره آغاز کنیم.
ب ـ راه‌اندازی مجدد نماییم.
ج ـ پلیس را صدا بزنیم.
د ـ ping کنیم.

پاسخ به سؤالات آزمون

۱- نادرست
۲- د
۳- درست
۴- نادرست
۵- د
۶- الف

فصل ۱۳

مبانی شبکه در نت‌ور

مسافری از سرزمینی باستانی را ملاقات کرد که گفت: «دو پایه بزرگ و بی‌تنه از سنگ در صحرا ایستاده بود. نزدیک آنها، روی شن، صورتی خردشده در دل خاک فرورفته بود، با اخمی و چروکی روی لب و استهزایی که دستور سرد و خشن برجای گذارده بود. اینها گویای تعصب و اشتیاق مجسمه‌ساز بودند که هنوز بر آن اشیا بی‌جان روح می‌دادند. دستی که آنها را تغذیه کرده بود و قلبی که آن دست را استهزاء کرده بود. در پایه ستون این کلمات مشهود بودند ـ اسم من ازیانديا‌س، شاه شاهان است. به کارهای من بنگرید و ناامید شوید! چیزی باقی نمی‌ماند. شن‌های کوچک صحرا آن را تراشیده و می‌برند».

ناول را می‌توان با امپراتوری روم مقایسه نمود؛ زمانی تمامی نقشهٔ شبکه متعلق به آن بود. تنها ارائه‌کنندهٔ شبکهٔ فایل و چاپ محسوب می‌شد. البته در سالهای اخیر، ناول بخش بزرگی از بازار را از دست داده و در فکر شراکت با NT شرکت میکروسافت می‌باشد. آیا زمان سقوط روم فرارسیده است؟ شاید خیر. محصولات ناول از پنج سال پیش رو به زوال گذاشتند و تنها یک فهرست سرویس بزرگ را به همراه خود یدک می‌کشد ـ که البته خود برای استادکاران شبکه امر مهمی محسوب می‌شود. سرعت و قابلیت اطمینان سرویس‌دهنده‌های ناول هنوز هم آنها را به‌عنوان انتخابی مطرح باقی می‌گذارد. با این وجود از آنجا که سرویس‌دهنده‌های ناول در محیطی غیر پنجره‌ای اجرا می‌شوند، منابع بسیار کمتری را نسبت به ویندوز NT مطالبه می‌کنند، چرا که تمرکز آنها بر سرویس‌های فایل و چاپ می‌باشد و نه پنجره‌سازی.

با این وجود بسیاری از مجموعه‌های کاری، سرویس‌دهنده‌های ناول 3.x خود را از رده خارج می‌کنند و سرویس‌دهنده‌های NT به‌جای آنها کار می‌گذارند. این موضوع کم و بیش به‌صورت جنگی مقدس بین استادکاران جریان دارد: نظیر جنگ اِترنِت/حلقه ـ نشانه، هواخواهان NT و فدائیان نت‌ور با هم در ستیزند.

نظر من آن است که نت‌ور برای برخی از کارها و NT برای برخی دیگر مناسب می‌باشد. برخی از برنامه‌های کاربردی سرویس‌گیرنده/سرویس‌دهنده به‌صورت جدی و بدون تعصب، روی سرویس‌دهندهٔ ناول اجرا نمی‌شود. البته، ناول سرویس فایل و چاپ فوق‌العاده سریعی را عرضه می‌کند و چیزی را داراست که سایر سیستم‌های عامل شبکه‌ای فاقد آن هستند: سرویس فهرست واقعاً خوب.

شبکهٔ NDS

اگر در مجموعهٔ کاری خود نت‌ور دارید و آن را به تازگی خریداری کرده‌اید، در صورتی که بخواهید از سرویس فهرست ناول *(NDS)* استفاده کنید این شانس را خواهید داشت که بتوانید کلیه اطلاعات سرویس‌دهنده، کاربر، ورود به سیستم،

امنیت و پیکربندی خود را در یک پایگاه داده‌ای سلسله مراتبی، قسمت‌بندی‌شده و توزیع‌شده در اختیار بگیرید. این حالت باعث می‌شود که بتوانید به یکباره شبکهٔ خود را پیکربندی نمایید.

اما منظور از این توزیع‌شده، قسمت‌بندی‌شده و سلسله مراتبی چیست؟ این عبارت بازاری به‌نظر می‌آید. در حقیقت این موضوع در کنار کیفیت بالای مطلب، صادق است. به‌طور خلاصه که بگوییم. NDS این امکان را فراهم می‌آورد که بتوانید کاربران و سرویس‌دهنده‌های بیشتری را با افراد کمتر مدیریت نمایید. که این موضوع برای مدیریت هر مجموعه‌ای جذاب است. NDS سلسله مراتبی است. چرا که سطوح چندگانه‌ای دارد که اطلاعات را می‌توان در آنها ذخیره نمود. این باعث منظم‌ماندن هر سطح و ساده‌شدن امور برای شما می‌شود. طبیعتاً سادگی باعث آسان‌ترشدن عیب‌یابی می‌گردد.



یادداشت : *نگارشهای قدیمی DOS امکان ایجاد شاخه‌ها (پوشه‌ها) را فراهم نمی‌آوردند. تمامی فایل‌ها باید در یک مکان روی دیسک جای داده می‌شدند. آیا می‌توانید تصور کنید که تمامی فایل‌های Office خود را در یک محل ذخیره نمایید؟ به‌نظر بچگانه نمی‌آید؟ این نشان می‌دهد که حالت سلسله‌مراتبی تا چه میزان در فهرست شبکه از اهمیت برخوردار است.*

نقطه‌ضعف فهرست سلسله مراتبی این است که اسامی کاربران چندین بخش اضافه به همراه خود دارند. هنوز هم یک نام (که به آن نام عمومی گفته می‌شود) وجود دارد، ولیکن شناسه‌ای هم موجود است که این کاربر را در درخت سلسله مراتبی جای می‌دهد.

برای مثال Quizro.finance.ny.frob بر کاربر Quizro که در دپارتمان Finance دفتر شهر نیویورک از شرکت Frobozz Magical Gadgets کار می‌کند، دلالت دارد. ممکن است تصور کنید این آدرسی اینترنتی است. به‌خاطر داشته باشید که بخش اول، اسم کاربر را شامل می‌شود.

NDS توزیع‌شده است، چرا که چندین کپی از پایگاه داده‌ای در چندین سرویس‌دهنده نگهداری می‌شود و از دست‌رفتن کل اطلاعات در صورت خراب‌شدن یکی از سرویس‌دهنده‌ها منتفی خواهد بود.

در نهایت، NDS قسمت‌بندی‌شده است، چرا که سطوح مختلف سلسله‌مراتبی را می‌توان به‌صورت جداگانه‌ای مورد استفاده قرار داد. این بدان معناست که پایگاه داده‌ای می‌تواند بخشهای مختلف و متعددی داشته باشد که تمامی آنها در هر زمان نیازی به به‌روز درآوری ندارند. قسمت‌بندی‌کردن پایگاه اطلاعاتی NDS باعث کاهش ترافیک شبکه می‌گردد؛ اگر ده هزار کاربر داشته باشید که هر هزار نفر آنها به‌صورت جغرافیایی نزدیک یکدیگر باشند، چرا باید هنگام به‌روزدرآوری یکی از نواحی کاری، کل اطلاعات ده‌هزار نفر را تغییر دهید؟

از همهٔ این موارد مهم‌تر، امکان قسمت‌بندی شما را قادر می‌سازد یک پایگاه داده‌ای بزرگ و متصل داشته باشید بدون آنکه به ترافیک راه دور خود اضافه نمایید. فرض کنید شرکتی وارداتی با دفاتری در نیویورک و ساوانا هستید. فرض کنید که یک خط استیجاری بین این دفاتر وجود دارد که شبکه‌های دفاتر را به یکدیگر پیوند می‌دهد. از آنجا که بابت زمان ارسال اطلاعات، هزینه پرداخت می‌کنید، مایل هستید که زمان استفاده از خط به کمترین مقدار ممکن کاهش یابد. همچنین مایلید که خط را آزاد نگه دارید تا افرادی که می‌خواهند بین دفاتر با یکدیگر ارتباط برقرار کنند بتوانند با بیشترین سرعت ممکن کارشان را به انجام برسانند. بهتر است یک قسمت بین سایت ساوانا و سایت نیویورک ایجاد کنید، این‌کار به NDS می‌گوید که پایگاههای اطلاعاتی ساوانا و نیویورک باید به‌صورت موجودیت‌های «توزیعی» مجزا مورد استفاده قرار گیرد. از آنجا که آنها ارتباط مستقیمی با هم ندارند، ترافیک تکراری متناوبی که بین سرویس‌دهنده‌های NDS توزیع‌شده به وقوع می‌پیوندد، خط بین ساوانا و نیویورک را مسدود نخواهد کرد.

البته، این ویژگیها باعث جذابیت NDS می‌شود، اما این قدرت در سایهٔ پرداخت یک بها به‌دست می‌آید. سرویس‌دهنده‌های ناول از شکل رومیزی ویندوز استفاده نمی‌کنند. آنها از یک کنسول متنی بهره می‌برند که نظیر آن چیزی است که تحت DOS ملاحظه می‌نمودید.

عدم استفادهٔ سرویس‌دهنده‌های ناول از جاذبه‌های گرافیکی و پنجره‌ای باعث می‌شود که ضمن اجرای سریعتر و نیاز به سخت‌افزار کمتر، عیب‌یابی سرویس‌دهنده‌ها آسان‌تر باشد.

با این‌که سرویس‌دهنده در حالت کاراکتری اجرا می‌شود، می‌توانید از برنامه‌های کمکی ناول برای مدیریت NDS در محیط ویندوز استفاده کنید؛ برای مثال، ابزار MWADMN32 که توسط سرپرست شبکه به‌منظور افزودن، حذف و تغییر کاربران، گروهها ویژگیهای امنیتی و غیره استفاده می‌گردد، تحت ویندوز NT و ویندوز ۹۵ به اجرا در می‌آید. این ابزار از نوع پنجره‌ای است، اما از آنجا که حالت پنجره‌ای در ایستگاه‌کاری به اجرا در می‌آید، ارتباطی با سرور پیدا نمی‌کند.



***نکته :** اگر از سرویس‌دهنده‌های قدیمی‌تر نت‌ور 3.x استفاده می‌کنید، می‌توانید از برنامهٔ مدیر سیستم SYSCON استفاده نمایید که از نسخهٔ 3.2 در دسترس قرار گرفته است. سایر نگارش‌های 3.x دیگر توسط ناول پشتیبانی نمی‌شوند. البته برای استفاده از NDS باید سیستم خود را به نگارشهای 4.x و یا بالاتر ارتقاء دهید.*



***یادداشت :** سرویس‌دهنده‌های نت‌ور 3که NDS را پشتیبانی نمی‌کنند، چه‌چیزی را جایگزین این نوع سرویس‌ها می‌نمایند؟ هر سرویس‌دهنده باید فهرست کاربران و گروههای خود را نگهداری کنند که به آن بایندری[1] گفته می‌شود. بایندری سرویس‌دهنده، موجودیتی مستقل است که به هیچ‌وجه با سایر سرویس‌دهنده‌ها ارتباط ندارد. اگر گروههای مشترک و اسامی کاربران بین سرویس‌دهنده‌ها مد نظر باشند سرپرستان شبکه باید به‌صورت دستی آنها را هماهنگ سازند.*

بایندری از نت‌ور 4.x به بعد منسوخ شده است، اما هنوز یک حالت شبیه‌سازی بایندری وجود دارد که باعث می‌شود سرویس‌دهندهٔ نت‌ور 4.x بتواند به درخواستهای بایندری گونهٔ نت‌ور 3.x پاسخ دهد.

مبانی Das

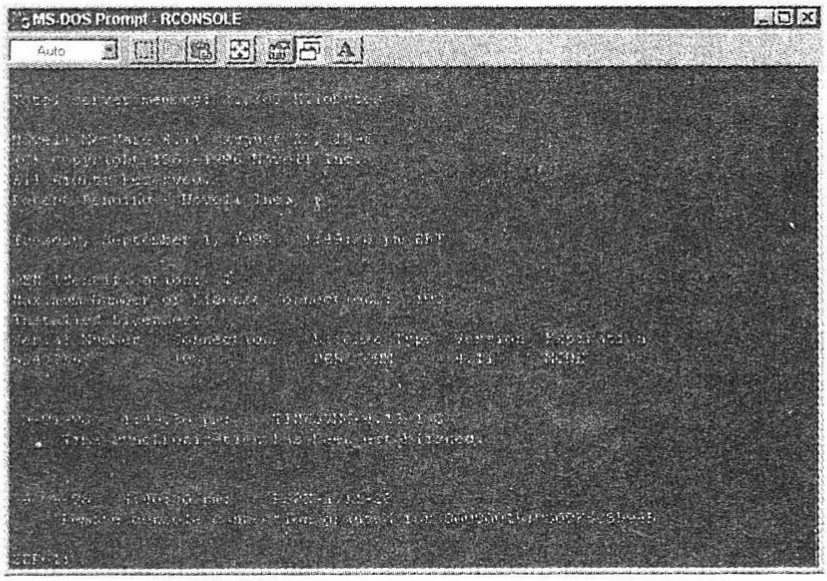
هر سرویس‌دهندهٔ ناقل اصولاً برنامه‌ای ۳۲ بیتی است به‌نام SERVER.EXE که از اعلان DOS اجرا می‌شود (همانطور که ویندوز 3.x از اعلان DOS اجرا می‌شد) این بدان معناست که فایل AUTOEXEC.BAT در گردونهٔ C وجود دارد که اغلب حاوی سطری شامل SERVER.EXE می‌باشد. این برنامهٔ سرویس‌دهنده در واقع کار زیادی را انجام نمی‌دهد؛ برای مثال نمی‌تواند شبکه را با اتکا بر خود ایجاد کند و یا به دیسک‌های سخت دسترسی داشته باشد. هنگامی‌که برنامهٔ SERVER.EXE بارگذاری می‌کنید صفحهٔ کنسول سرویس‌دهنده باز می‌شود. این صفحه، که در شکل ۱-۱۳ نشان داده شده است، یک مفسر متنی است که دستورات مختلفی را قبول می‌کند.

NLM ها

برنامهٔ سرویس‌دهنده، علاوه بر پذیرش دستورات، نظیر یک مأمور راهنمایی و رانندگی برای منابع سرویس‌دهنده عمل

1- bindery = صحافی

می‌کند و به‌منظور فراهم‌آوردن سرویس‌های خاص به ماجول‌های قابل بارگذاری تکیه می‌نماید. به‌طور کلی به این ماجول‌ها *NLM* گفته می‌شود که شکل کوتاه‌شدهٔ ماجول قابل بارگذاری نت‌ور می‌باشد. NLM ها هر چیزی را می‌توانند، از برنامهٔ گزارش آماری (MONITOR.NLM) گرفته تا برنامه‌های پیکربندی (INSTAL.NLM)، فراهم سازند؛ بعلاوه، NLM ها سرویس‌دهنده را قادر می‌سازند که با پروتکل‌های خاصی صحبت کنند (TCPIP.NLM).



شکل ۱-۱۳ : RCONSOLE (یا کنسول راه دور) این امکان را فراهم می‌سازد که از راه دور سرویس‌دهنده را از دستگاه خود کنترل کنید.

اشکال خاصی از NLM ها شامل گرداننده‌های قدیمی دیسک (برای مثال، IDE.DSK)، گرداننده‌های دیسکی جدیدتر (برای مثال، IDE.HAM)، و گرداننده‌های کارت شبکه (برای مثال، NE2000.LAN) هم وجود دارند. تمامی این ماجول‌ها به همراه SERVER.EXE برای ایجاد قابلیت صحبت سرویس‌دهنده با شبکه و پاسخگویی مناسب با درخواستها به کار می‌روند. قطعات و اجزاء بسیار زیادی وجود دارند. هر سرویس‌دهندهٔ نت‌ور، در هر لحظه دهها NLM بارگذاری‌شده دارد. اگر همه چیز مرتب باشد این مجموعه تحسین‌برانگیز است.

طبقه‌بندی مشکلات

یکی از وظایف مهم عیب‌یاب نت‌ور، نگهداری رد تمامی NLM ها و شناسایی مشکل به‌وجود آمده توسط NLM خراب می‌باشد. در گذشته این کار وحشتناکی بود؛ باید بسیاری فایل‌های متفاوت را بارگذاری می‌کردیم تا سرویس‌دهنده را «تعمیر» می‌نمودید. امروزه، به سادگی می‌توانید آخرین مجموعهٔ سرویس‌ها را از ناول دریافت کنید (صفت خوبی که از میکروسافت گرفته شده است. میکروسافت همیشه بر دریافت یک مرحله‌ای تمامی تصحیح‌ها و بهینه‌سازی‌ها اصرار ورزیده است). فراهم‌آوردن مجموعه‌های سرویس کاری آسان است.

اصلاح

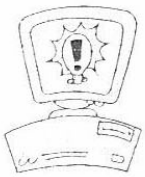
همانگونه که میکروسافت برای ویندوز NT اصلاحیه‌های فوری منتشر می‌کند، ناول نیز مشکلات نسبتاً جدی را در قالب چنین اصلاحیه‌هایی ارائه می‌نماید (اصلاحیه‌ها قبل از انتشار مجموعهٔ سرویس بعدی، در دسترس جمعیت کاربران قرار

می‌گیرد). با این‌که تمامی اصلاحیه‌ها برای همهٔ محیط‌های کاری مفید واقع نمی‌شوند ممکن است برای هر یک مشکل خاصی در سرویس‌دهنده به چنین اصلاحیه‌هایی نیاز داشته باشید.



نکته : *هر زمان که به مشکلاتی در سرویس‌دهندهٔ ناول برخورد می‌کنید، پایگاه اطلاعاتی ناول را در http://support.novell.com را بازرسی نمایید. علاوه بر آنکه می‌توانید این پایگاه را برای مشکل جاری خود مورد جستجو قرار دهید، این امکان وجود دارد که فهرست اصلاحات را وارسی نمایید. این‌کار می‌تواند گام اولیهٔ مهمی در عیب‌یابی باشد، چرا که می‌توانید به راحتی بررسی کنید که تمامی اقلام موجود در فهرست اصلاحات را در سرویس‌دهنده‌تان بارگذاری نموده‌اید.*

در واقع، حتی در صورت برخورداری از پشتیبانی حق بیمهٔ ناول، اولین کاری که باید در مواجه‌شدن با اشکالات انجام دهید، آن است که مطمئن شوید آخرین و مهمترین اصلاحات را در اختیار دارید. بسیاری از مشکلات در این ارتباط هستند که به راحتی می‌توان آنها را حل نمود.



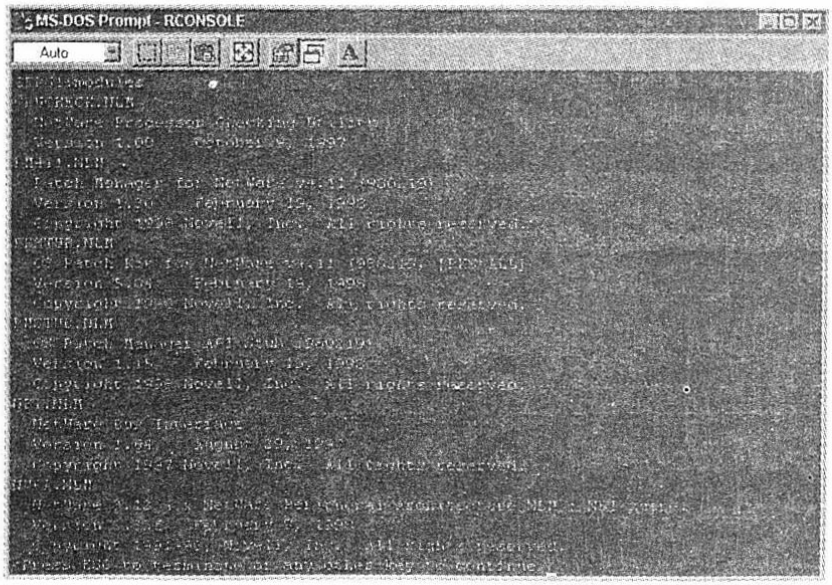
هشدار : *اصلاحات می‌توانند مشکلات را برطرف کنند، اما از طرفی ممکن است خرابی‌هایی به وجود بیاوردند. اما لازم نیست نگران باشید، چرا که این صنعت راه بسیار بسیار طولانی را برای هر چه امن‌ترکردن فرایند اصلاح پیموده است. برای مثال، فرایند اصلاح اکنون کپی‌های پشتیبانی را از فایل‌های قبلی‌تان، نگهداری می‌کند. اما به هر حال برای اطمینان خود، مطمئن شوید که قبل از به‌کارگیری هر اصلاحیه‌ای، کپی‌های پشتیبان خوب و سالمی از سرویس‌دهنده‌هایتان در اختیار دارید (این شامل تمام اصلاحیه‌ها و نه تنها اصلاحیه‌های ناول می‌گردد).*

در این‌جا باید امتیاز مثبتی را برای ناول قائل شوم: ناول از دیرباز به‌خوبی مشکلاتش را حل نموده است و با تشخیص آنها و بر عهده‌گرفتن مشکل و حل‌نمودن آنها پیش‌قدم بوده است. از جهتی همراهی با میکروسافت از آن جهت که دیگر غولی در صنعت شبکه نیست، برای ناول سودمند بوده است. اکنون ناول یکی از خطوط کشتی‌رانی این صنعت می‌باشد که نظیر یک مؤسسهٔ کرایه اتومبیل «بیش از پیش تلاش می‌کند».

مجموعهٔ NLM

در مورد NLM هایی که ناول آنها را فراهم ننموده است چه‌کار باید بکنیم؟ به بیان دیگر، NLM هایی که سایر تولیدکنندگان در اختیار می‌گذارند چه؟ مثالهایی از این دسته عبارتند از نرم‌افزار کپی پشتیبان، راه‌اندازهای کارت شبکه، برنامه‌های اندازه‌گیری نرم‌افزاری و برنامه‌های متعدد حفاظت از ویروس در سرویس‌دهنده. اگر شما از آن دسته کسانی هستید که علاقه‌ای به پیگری دقیق امور ندارید، نگهداری رد سطوح بازبینی این‌گونه ابزار، برایتان مشکل خواهد بود. این موضوع به‌خصوص در صورتی که سرویس‌دهنده‌های ترکیبی داشته باشید و افراد مختلفی با این سرویس‌دهنده‌ها کار کنند، واقعیت خواهد داشت؛ دانستن این‌که شخصی یکی از سرویس‌دهنده‌ها را به‌روز درآورده است، مشکل خواهد بود.

به همین صورت، هنگامی‌که با یکی از سرویس‌دهنده‌ها مشکلی دارید، باید بازی خیابان سسمی را انجام دهید و سطوح NLM را مقایسه نمایید. این‌کار را با اجرای فرمان modules در پای اعلان کنسول سرویس‌دهنده به انجام می‌رسانید (شکل ۲-۱۳).



شکل ۲-۱۳ : دریافت فهرستی از ماجول‌ها از سرویس‌دهندهٔ InteranetWare 4.11.



نکته : *اگر چنین به نظر می‌رسد که این‌کار مستلزم انجام مقدار زیادی فعالیت است، حق با شماست! می‌توانید از سایت ناول ابزار CONFIG.NLM را منتقل کنید (به همراه Config Reader):*

http://support.novell.com

CONFIG.NLM پیکربندی سرویس‌دهنده‌تان را خوانده، در شاخه SYS:SYSTEM گزارش CONFIG.TXT را می‌نویسد (شکل ۳-۱۳) برنامهٔ Config Reader که در ویندوز اجرا می‌شود خروجی تولیدشده توسط CONFIG.NLM که در شاخهٔ سیستم قرار داده شده را خوانده و آن را به گونهٔ قابل خواندنی پردازش می‌کند.

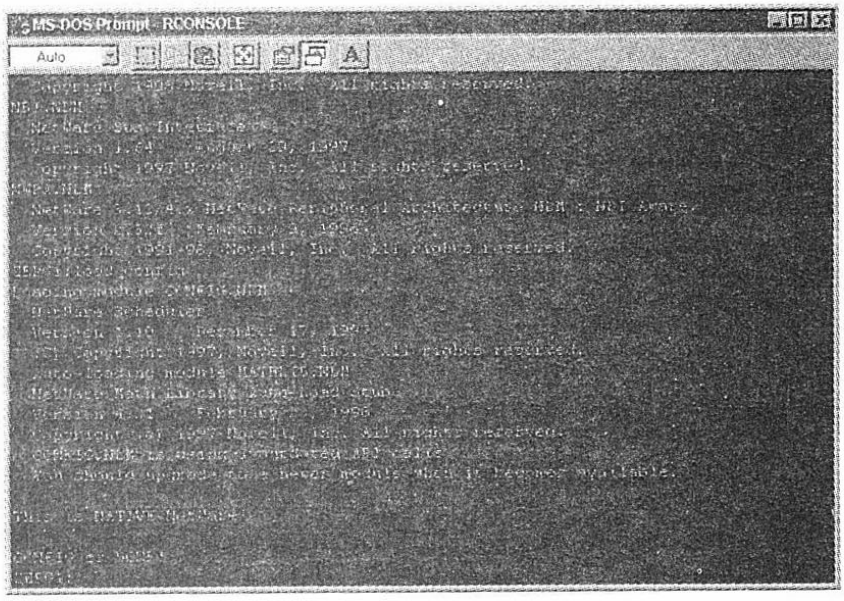
این برنامه، که در شکل ۴-۱۳ نشان داده شده است، به‌صورت خودکار اطلاعات جاری را از سایت وب ناول منتقل می‌کند و آنگاه نمایی کلی از سیستم ارائه می‌دهد که NLMهایی که از رده خارج شده‌اند مشخص گردیده و دو سرویس‌دهندهٔ موجود را با یکدیگر مقایسه می‌کنند. این حالت باعث می‌شود تفاوتهای بین سرویس‌دهنده‌های مختلف را آسانتر با یکدیگر مقایسه نمایید.

سکوت فهرست

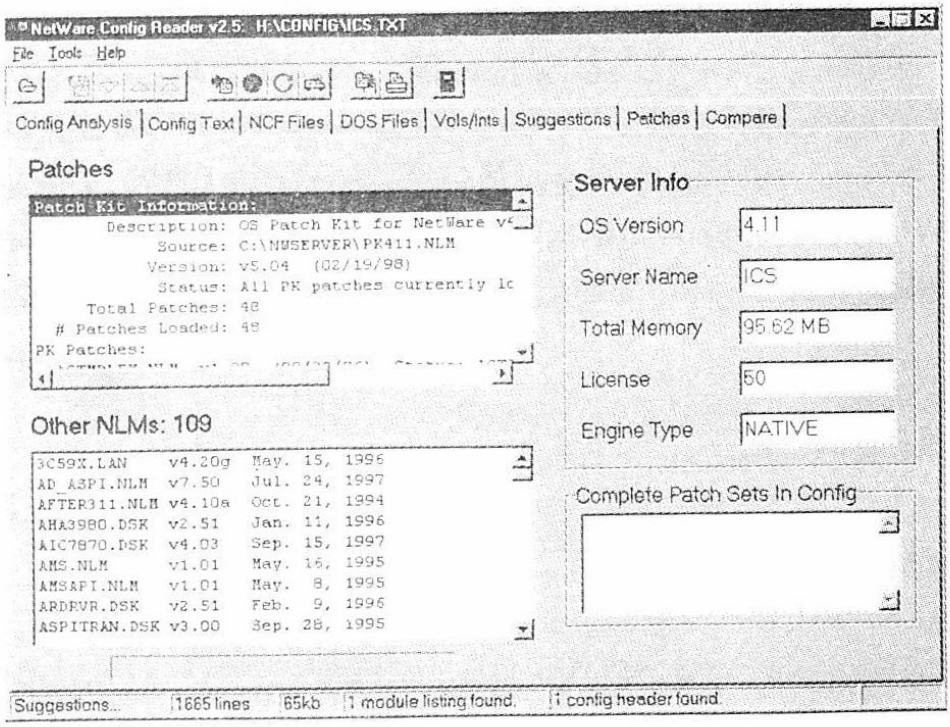
با این‌که NDS ابزار خارق‌العاده‌ای است، برخی اوقات مشکلات ارتباطی و یا سخت‌افزاری که به هیچ وجه با خود NDS در ارتباط نیستند، باعث بروز خرابی‌هایی در آن می‌شوند. این خرابیها ممکن است به طرق مختلفی آشکار شود ـ که بیشتر به شکل مشکلات ورود به سیستم و سطوح امنیتی بعد از ورود به سیستم ظاهر می‌گردند.



یادداشت : *در واقع، هر مشکل وابسته به NDS می‌تواند از خرابی یا نقص در NDS تأثیر پذیرد. این شامل ـ و نه محدود به ـ مواردی نظیر مشکلات سرویس‌دهندهٔ چاپ، برنامه‌های حفاظت از ویروس، ابزار جمع‌آوری خودکار، ابزار مدیریت ایستگاه‌کاری و نظایر آن، می‌گردند.*



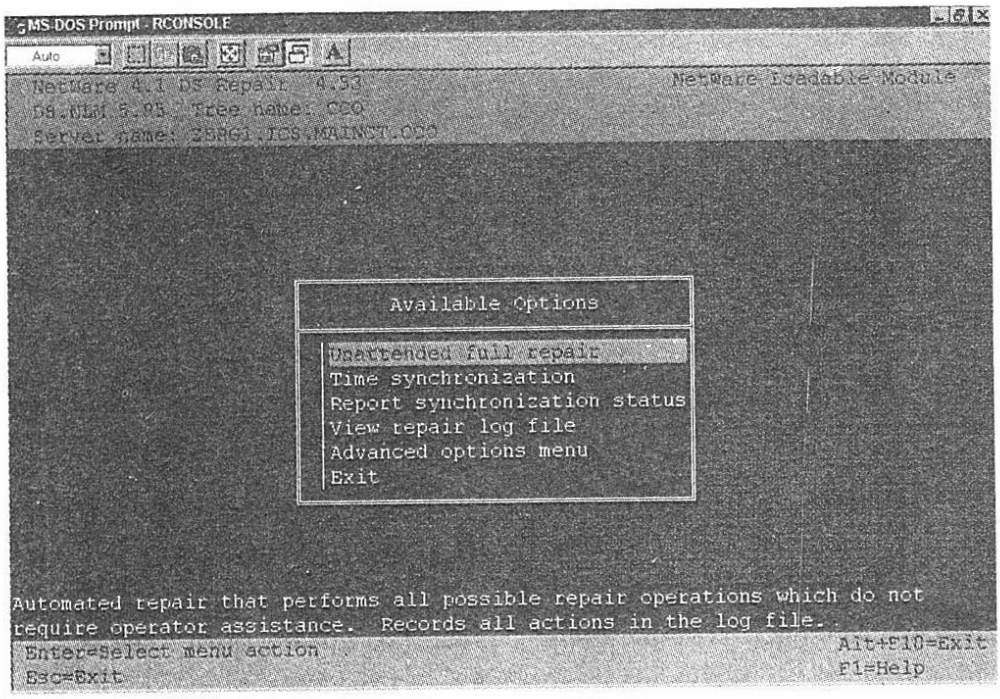
شکل ۳-۱۳ : *CONFIG.NLM باید قبل از استفاده از Config Reader در سرویس‌دهنده‌های مورد نظر بارگذاری شده باشد.*



شکل ۴-۱۳ : *برنامهٔ Config Reader در پیداکردن «چیزی که با بقیه متفاوت است» مفید واقع می‌شود.*

می‌توانیم بسیاری از مشکلات NDS را با استفاده از تایپ‌کردن فرمان زیر در محل اعلان کنسول و آنگاه انتخاب گزینهٔ Unattended Full Repair از منوی ظاهرشده برطرف نمایید (شکل ۵-۱۲ را ملاحظه کنید):

```
LOAD DSREPAIR
```



شکل ۵-۱۳ : همانگونه که ScanDisk مشکلات دیسک سخت را برطرف می‌کند، DSRepair.NLM نیز می‌تواند در برطرف ساختن مشکلات NDS مثمر ثمر واقع شود.



نکته : *اجرای DSREPAIR در بسیاری از موقعیت‌ها آسیبی ایجاد نمی‌کند و علاوه بر آن می‌توانید احتمال خرابی NDS را هنگام تحلیل یک مشکل پیچیده کنار بگذارید.*



نکته : *مطمئن شوید که آخرین اصلاحیه‌های ناول را به‌کار بسته‌اید ـ بسیاری مشکلات غریب در NDS برطرف شده‌اند.*

«دوستتان»، ABEND

اگر مدت زمانی طولانی از محصولات ناول استفاده کرده باشید، می‌دانید که چقدر دریافت ABEND غم‌انگیز است. ABEND که شکل کوتاه‌شدهٔ کلمات *abnormal end* می‌باشد، هنگامی بروز می‌کند که سرویس‌دهنده نمی‌تواند با وضعیت پیش‌آمده کاری صورت دهد و باید عملکرد خود را به منظور جلوگیری از احتمال خرابی اطلاعات متوقف نماید. تصمیم مشکلی است ـ ترجیح می‌دهید کار را ادامه دهید و خطر خرابی اطلاعات را بپذیرید، یا این‌که ترجیح می‌دهید کار متوقف شود؟

چه چیزی باعث وقوع ABEND می‌شود؟ به بیان ساده، مشکلات سخت‌افزاری و نرم‌افزاری باعث وقوع ABEND ها می‌گردد. قابل درک است که CPU یا حافظهٔ خراب می‌توانند کار کل سرویس‌دهنده را متوقف سازند ـ چرا که بدون حافظه یا CPU سالم، اجرای برنامه‌های غیر ممکن است. اما چرا برنامه‌ای (مثل برنامهٔ سرویس‌دهندهٔ وب) باعث می‌شود که سرویس‌دهنده متوقف شود؟ خوشبختانه جدیدترین نرم‌افزار سرویس‌دهندهٔ ناول قادر است ماهیت مشکل مهم و مشکلی کم‌اهمیت را از یکدیگر تمیز دهد.

این یکی از بهترین دلایل ارتقاء از نگارش قدیمی نتور به نگارش‌های جاری IntraNetWare 4.11 یا NetWare 5 می‌باشد.



یادداشت : *ناول نگارش 4.11 خود را سیستم عامل IntraNetWare نامید تا بر سرویس‌های اینترانت گنجانده شده در این محصول تأکید کرده باشد. نگارش ۵ پیشوند Intra را از دست داده و دوباره NetWare شده است. از من سؤال نکنید، من مسبب این قضیه نبوده‌ام!*

ناول برنامه‌های کاربردی را در دو دستهٔ متفاوت رده‌بندی نموده است:

- برنامه‌های کاربردی که از حافظه یا منبع مشترک دیگری با برنامهٔ سرویس‌دهنده، استفاده می‌کنند (خطرناک، اما سریع).
- برنامه‌های کاربردی که از یک حالت حفاظت‌شدهٔ مخصوص استفاده می‌کند که مقدار تخریبی که می‌توانند در سرویس‌دهنده ایجاد کند به حداقل رسیده است (آهسته‌تر، اما امن‌تر). (می‌توانید این‌حالت را با صخره‌نوردی که با دست خالی صعود می‌کند ـ سریع ـ با حالتی که از ابزار استفاده می‌نماید ـ آهسته‌تر اما امن‌تر ـ مقایسه نمایید.)

روش اخیر در ناول، «اجرای برنامه در حوزه‌ای متفاوت» نامیده می‌شود. هر نامی که به آن بدهیم، قابلیت اطمینان بیشتری دارد و در نگارشهای جدید به‌صورت خودکار به اجرا درمی‌آید. کسی را سراغ ندارم که از ۲ درصد آهسته‌تر کارکردن سرویس‌دهنده در ازای دستیابی به قابلیت اطمینان بیشتر شکایتی داشته باشد.



نکته : *اگر هنوز از سطح پایین‌تری از نت‌ور استفاده می‌کنید و یا حتی در صورت ارتقاء به IntraNetWare، ممکن است ABENDهای وابسته به سخت‌افزار یا نرم‌افزاری که در حوزهٔ حفاظت‌شده‌ای اجرا نمی‌شود، دریافت کنید. خوب است به TID (سند اطلاعاتی فنی[1]) شمارهٔ ۲۹۱۷۵۳۸ مراجعه کنید و یا تنها در پایگاه اطلاعاتی ناول به دنبال عبارت* **ABEND Troubleshoot** *بگردید. بسیاری اوقات مفید واقع می‌شود.*

ناظر بزرگ شاهد است

همانقدر که به Microsoft System Monitor علاقه دارم، جایی را در قلبم برای Novell Monitor محفوظ نگاه داشته‌ام. Novell Monitor با وجود متنی‌بودن (این برنامه به هیچ‌وجه گرافیکی نیست)، بسیار کامل است و می‌تواند بهترین دوست عیب‌یاب باشد. در محل اعلان به سادگی تایپ کنید:

```
LOAD MONITOR
```

و با استفاده از منوها تمامی دنیا را تحت کنترل خواهید داشت.

هر منبعی در سرویس‌دهندهٔ ناول توسط Monitor ردیابی می‌شود و این موضوع جالبی است. برخی از موارد خوبی که توسط Monitor نظارت می‌شوند، عبارتند از:

- اتصالات سرویس‌دهنده و آمار مربوط به جلسه
- قفل‌های فایل (چه‌کسی از فایل استفاده می‌کند؟)

1- Technical Information Document

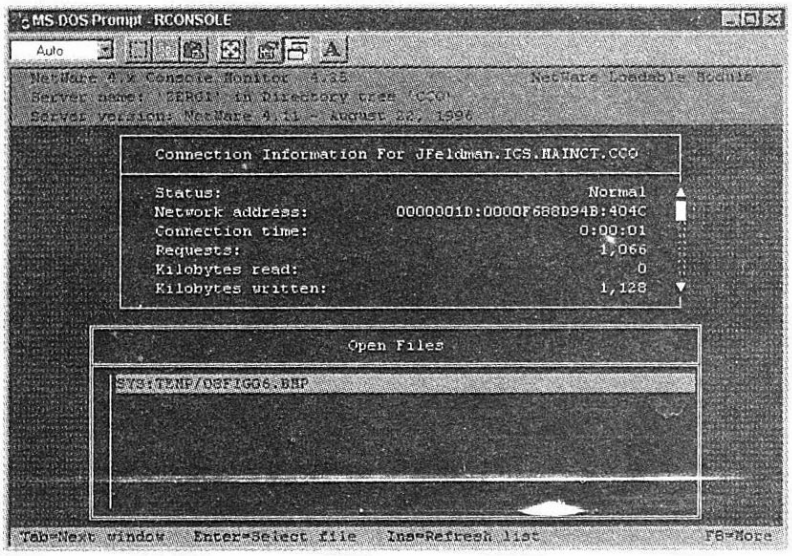
- منابع سیستم (زمان CPU، حافظه)
- فرایندها (زیربرنامه‌ها)



نکته : تصور کنید کاربری گزارش می‌دهد که نمی‌تواند به سرویس‌دهنده متصل شود. بعد از بررسی آنکه بقیه می‌توانند با سرویس‌دهنده کار کنند، سعی می‌کنید که خودتان وارد سیستم شوید و نمی‌توانید. یک وارسی سریع صفحهٔ *Monitor* تعداد اتصالات مورد استفاده را آشکار می‌سازد ـ ممکن است کشف کنید که اتصالی برای سرویس‌دهنده باقی نمانده است تا در اختیار بگذارد.
هر کاربر که به سرویس‌دهنده متصل شده است، از یک مجوز سرویس‌دهنده استفاده می‌کند. اگر با کمبود اتصال مواجه شوید، احتمالاً باید مجوزهای بیشتری را از ناول دریافت نمایید.



نکته : هنگامی‌که فضای دیسکی سرویس‌دهنده رو به اتمام بگذارد، می‌توانید از طریق فهرست اتصالی کاربر در *Monitor*، ببینید که چه کسی فضای دیسکی زیادی را اخیراً مورد استفاده قرار داده است؛ نتیجهٔ این‌کار چیزی شبیه به حالت نشان داده شده در شکل ۶-۱۳ می‌باشد.
در این‌حالت، ملاحظه می‌کنید که کاربر *JFeldman* در طی حضور یک دقیقه‌ای خود در سیستم، ۱/۱۲۸*Kb* (یا ۱/۱۲*Mb*) اطلاعات را به ثبت رسانده است. او ممکن است متهم و مقصر قضیه نباشد ـ ۱ مگابایت اطلاعات اغلب باعث سرریزی یک دیسک روی سرویس‌دهنده نمی‌شود. باید به سایر اتصالات دنبال چیزی شبیه به ۵ تا ۱۰ مگابایت یا حتی بیشتر بگردید. همچنین آدرس شبکه را مورد توجه قرار دهید: *JFeldman* از شبکهٔ *1D* و آدرس *MAC* معادل *00-00-f6-88-d9-4b* و سوکت *404C* وارد سیستم شده است. با پیداکردن کاربر مورد نظر، مشکل سریعاً حل می‌شود. سایر روشهای پیداکردن اتلاف فضای دیسکی را در فصل ۱۸ مورد بررسی قرار خواهیم داد.



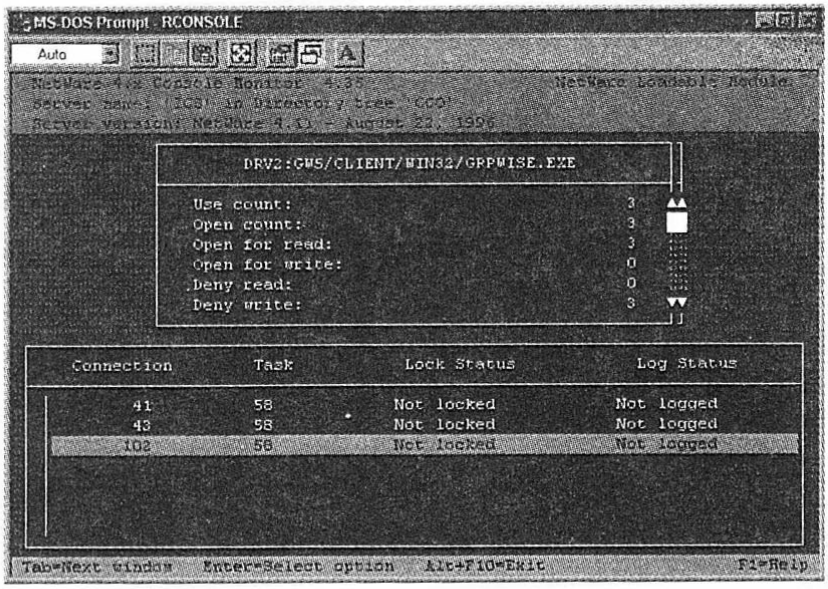
شکل ۶-۱۳ : می‌توانید از *Monitor* برای مشاهدهٔ اطلاعات اتصال بهره جویید.



نکته : ممکن است در اثر مورد استفاده قرارداشتن یک فایل اشتراکی، نتوانید نرم‌افزاری را نصب کنید. دریافت چنین پیغامی واقعاً ناامیدکننده است، چرا که آنچه که ویندوز می‌گوید آن است که نمی‌توانید

روی فایل چیزی بنویسید و اطلاعاتی در مورد شخصی که از این نوشتن ممانعت به عمل می‌آورد را اعلام نمی‌دارد.

با استفاده از Monitor می‌توانید شخصی را که فایل را مورد استفاده قرار داده، پیدا نمایید. کافی است به منوی File Open|Lock Activity بروید و آنگاه فایل مورد نظر خود را بیابید. Monitor شماره‌های اتصالی افرادی را که از فایل استفاده می‌کنند را نشان می‌دهد (شکل ۷-۱۳). آنگاه می‌توانید با استفاده از لیست اتصالها، اسامی ورود به سیستم این افراد را استخراج کنید؛ بعد از آنکه این افراد را شناسایی کردید می‌توانید از آنها خواهش کنید برای چند لحظه از برنامه خارج شوند.



شکل ۷-۱۳ : Monitor می‌تواند نشان دهد چه کسی فایلی را «قفل نموده است».

ترس به خود راه ندهید؛ Monitor اینجا است!

Monitor بیش از یک دفعه از پوست‌کندن من جلوگیری کرده است. یکبار، به همراه سرپرست شبکه، کاملاً از مشکلی که به نظر می‌رسید به برنامهٔ کپی پشتیبان مربوط باشد، درمانده و عاجز شده بودیم. این برنامه، که به صورت یک NLM به اجرا درمی‌آمد، به‌منظور انجام کار خود لازم داشت که به NDS متصل شود. هر هفته یا چیزی در حدود آن، برنامهٔ کپی پشتیبان اعلام می‌نمود که قادر نیست وارد سیستم شود و ما می‌بایست سرویس‌دهنده را مجدداً راه‌اندازی کنیم تا آن برنامه بتواند دوباره وارد سیستم گردد.

مسؤولین تولیدکنندهٔ نرم‌افزار کپی پشتیبان، اشکال را متوجه ناول می‌دانستند: «این مشکل مربوط به NDS است.» آنها می‌گفتند «قاعدتاً باید مشکلی در NDS شما وجود داشته باشد؛ نرم‌افزار ما اشکالی ندارد». جستجو در سایت فروشندهٔ کپی پشتیبان و ناول نیز چیزی را آشکار نکرد؛ خوشبختانه، هنگامی‌که با ناول تماس گرفتیم آنها در این‌که این مشکل به‌نظر به NDS مربوط می‌شد هم‌رأی بودند. این وضع برای مدتی ادامه داشت.

تا این‌که ناگهان، در طی یکی از جلسه‌های تلاش بیهوده برای راه‌اندازی نرم‌افزار کپی پشتیبان قبل از راه‌اندازی مجدد، یکی از کاربران بنا به مشکلاتی مربوط به ایستگاه‌کاری، از سیستم خارج شد؛ هنگامی‌که تلاش کرد که دوباره به سیستم وارد شود، نتوانست. Monitor را وارسی نمودیم و متوجه شدیم که اتصالات موجود به اتمام رسیده است. تصادفی بود؟ شاید. دفعهٔ بعد که مشکل کپی پشتیبان رخ داد، تعداد اتصالات روی سرویس‌دهنده را بررسی نمودیم و متوجه شدیم که هر

بار با اتمام اتصالات مواجه هستیم.

چرا قبلاً به این موضوع توجه نکرده بودیم؟ اغلب، کاربران قبل از آغاز کار کپی پشتیبان وارد سیستم شده و در حال انجام کار خویش بودند. هنگامی برنامه موفق به کارکردن می‌شد که ساعت، حدود ۷ صبح بود و افراد هنوز به شبکه وارد نشده بودند. این بدان معنا بود که قبل از آنکه دیگران متوجه فقدان اتصالات شوند، دستگاه را مجدداً راه‌اندازی می‌کردیم.

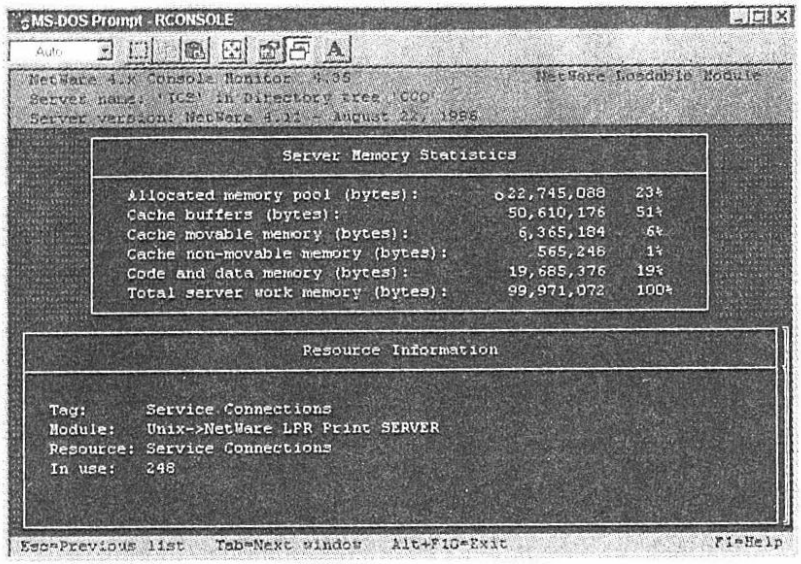
مجوز اتصالات بیشتری را خریداری نمودیم، اما باز هم با کمبود اتصالات مواجه می‌شدیم. چه اتفاقی رخ می‌داد؟

با نگاه‌کردن به فهرست اتصالات در Monitor، متوجه شدیم که تمامی اتصالات اضافه از طرف خود سرویس‌دهنده پر می‌شد. از شکل ۶-۱۳ به‌خاطر بیاورید که نمایش مربوط به اتصال، آدرس IPX ایستگاه اتصالی را نشان می‌دهد. در این حالت، اتصالات اضافی از سوی شمارهٔ IPX داخلی منحصر به سرویس‌دهنده می‌آمد (بخش «IPX/SPX» که در ادامه می‌آید را ملاحظه نمایید). این موضوع به‌طور واضحی به یک NLM مربوط بود.



یادداشت : *عیب‌یابی این مسئله بدون Monitor کاری بس مشکل است. برای مثال استفاده از روش تفرقه‌بیانداز-و-حکومت‌کن برای این مسئله بسیار مشکل است، چراکه این یک مشکل تناوبی است و ما می‌خواستیم در طی روز کاری تمامی NLMهایمان بارگذاری شده باشد. نمی‌توانستیم کاری را بدون NMLهای مذکور صورت دهیم.*

از آنجا که Monitor قادر است از نزدیک چنین مواردی را ردیابی کند، قادر بودیم که منبعی به نام اتصالات سرویس را پیدا کرده و تعداد اتصالات هر NLM را وارسی نماییم (شکل ۸-۱۳) موردی که دارای مقدار بیش از حد بزرگی بود مقصر قضیه شناخته شد. با بارگذاری‌نکردن این ماجول (که از قضا توسط ناول تهیه شده بود)، تمامی اتصالات اضافی از بین رفتند و مشکل حل شد.



شکل ۸-۱۳ : ماجولی که تمامی اتصالات جواز ما را به چنگ می‌انداخت، نتوانست از چشم Monitor پنهان بماند.

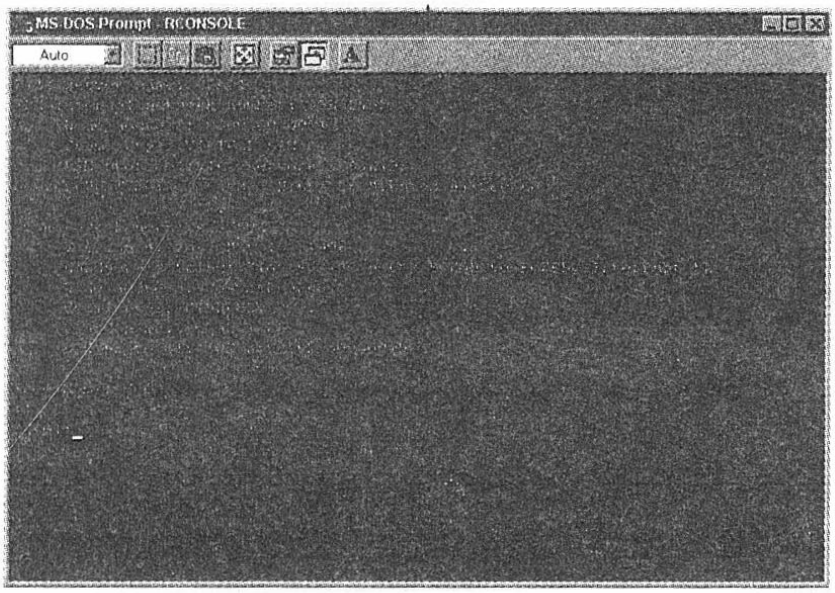
ما این مشکل را به ناول گزارش نمودیم. با این‌که ناول از قبل مشکل را می‌دانست، هنوز اصلاحیه‌ای را در اختیار عموم قرار نداده بود. هنگامی‌که جستجویی را بر اساس اسم NLM به انجام رساندیم، متوجه شدیم که یک TID در مورد این

مشکل وجود دارد. متأسفانه، از آنجا که هنگام جستجوی اولیه نمی‌دانستیم که دقیقاً با چه مشکلی مواجه هستیم، به این موضوع دقت نکرده بودیم. بلافاصله بعد از به کارگیری اصلاحیه، مشکل برطرف شد. سه هورا برای Monitor!

مشکلات پروتکلی

اگر سرویس‌دهنده را خودتان نصب کرده باشید، احتمالاً با INETCFG NLM آشنایی دارید. من آن را چاقوی ارتشی شبکهٔ ناول می‌نامم. این NLM، که شبیه به Network در Control Panel ویندوز می‌باشد، راه‌اندازهای شبکه را بارگذاری می‌کند و پروتکل‌ها را به آنها مقید ساخته و پیکربندی می‌نماید. می‌توانید برای مشاهدهٔ سریع نحوهٔ پیکربندی ابزار، آن را مورد استفاده قرار دهید.

در روش متناظر، می‌توانید به سادگی در محل اعلان کنسول، فرمان CONFIG را اجرا کنید (منظور LOAD CONFIG نیست؛ این ماجول تولیدکنندهٔ فایل پیکربندی است) INETCFG می‌گوید عناصر و مؤلفه‌ها چگونه باید باشند، اما CONFIG وضعیت فعلی آنها را نشان می‌دهد (شکل ۹-۱۲).



شکل ۹-۱۳ : خروجی CONFIG مربوط به سرویس‌دهنده‌ای که دارای یک کارت شبکه و یک پروتکل شبکه (IPX/SPX) می‌باشد.

اگر CONFIG با INETCFG مطابقت نداشته باشد، احتمالاً مشکلی وجود دارد. برخی اوقات می‌توانید با انجام یک خانه تکانی شبکه‌ای در سرویس‌دهنده، این مشکل را حل نمایید. کافی است فرمان زیر را تایپ کنید:

```
REINITIALIZE SYSTEM
```

بر خلاف هیبت دستور فوق، تمامی کاری که صورت می‌پذیرد، بارگذاری دوبارهٔ راه‌اندازهای کارت شبکه در صورت نیاز، و مقیدسازی پروتکل‌ها به این کارتها می‌باشد. سرعت آن به‌خوبی بالا است، آنقدر سریع که اجرای آن در سرویس‌دهندهٔ آزمایشی باعث توقف جلسه نمی‌گردد. البته این‌کار را در سرویس‌دهندهٔ فعال امتحان نکرده‌ام.

IPX/SPX

تاکنون اندکی در مورد خودکاربودن پیکربندی IPX/SPX صحبت کرده‌ام. نگارش‌های قدیمی‌تر نت‌ور فاقد پیکربندی خودکار سرویس‌دهنده بوده‌اند؛ این‌کار به سرپرست شبکه واگذار می‌شد. نگارشهای جدیدتر شبکه را پویش می‌کنند و تلاش می‌نمایند عناصر و مؤلفه‌ها را تنظیم کنند. در هر حال، اجازه دهید نگاهی به ترتیب پیکربندی IPX/SPX در سرویس‌دهنده داشته باشیم، چرا که در صورت درست نبودن آنها، به دردسر می‌افتید.

هر بخش در IPX/SPX به یک شمارهٔ شبکه نیازمند است. مشکل خاصی در این ارتباط وجود ندارد؛ می‌توانید هر عددی در مبنی ۱۶ را انتخاب کنید. تنها محدودیت موجود آن است که هر بخش IPX باید منحصربه فرد باشد. قاعدهٔ خشکی که وجود دارد این است: اگر این بخشها از طریق یک سوئیچ به هم متصل شده باشند، باید دارای شمارهٔ شبکه‌ای یکسان باشند، چرا که بخشها اصولاً یک شبکه محسوب می‌شوند. اما اگر از سوی دیگر بخشهای شبکه‌ای از طریق یک مسیریاب به هم وصل شده باشند، آنها باید شماره‌های منحصربه خود را دارا باشند. اگر شمارهٔ شبکهٔ IPX برای هر یک از بخشهای شبکه واحد نباشد مشکلاتی از قبیل ناتوانی سرویس‌دهنده‌ها و ایستگاههای کاری در بخشهای مختلف در «دیدن یکدیگر»، بروز می‌کند.

در نت‌ور شمارهٔ دیگری وجود دارد که شمارهٔ شبکه‌ای داخلی *IPX* نامیده می‌شود. این شماره هم باید منحصر به فرد باشد و می‌تواند در ردیابی مشکلات مؤثر واقع گردد (همانگونه که در بخش «ترس به خود راه ندهید؛ Monitor اینجا است!» اتصالات اضافی به خود سرویس‌دهنده را ردیابی نمودم). این شماره در مبنی ۱۶ می‌باشد؛ و اگر با شمارهٔ سرویس‌دهندهٔ دیگری یکی باشد، مشکلات بزرگی بروز می‌کنند (به خصوص اگر سرویس‌دهنده‌ای به‌عنوان مسیریاب عمل نماید). در چنین حالتی شماره‌های داخلی IPX یکسان، می‌تواند مسیریابی را متوقف نماید.

اگر نمی‌دانید که شمارهٔ شبکه‌ای داخلی IPX سرویس‌دهندهٔ بخصوصی چیست، یا نمی‌دانید که شمارهٔ شبکه‌ای مربوط به شبکه‌های متصل‌شده به آن کدامند، کافی است دستور CONFIG را اجرا نمایید.

سرویس‌دهنده یا مسیریاب

هر سرویس‌دهندهٔ IntraNetWare یا NetWare که بیش از یک کارت شبکه داشته باشد به‌صورت خودکار نظیر یک مسیریاب عمل می‌کند. هر مسیریاب، طبق تعریف بیش از یک کارت شبکه دارا است چرا که از این طریق می‌تواند شبکه‌ای را به شبکه‌ای دیگر متصل نماید.

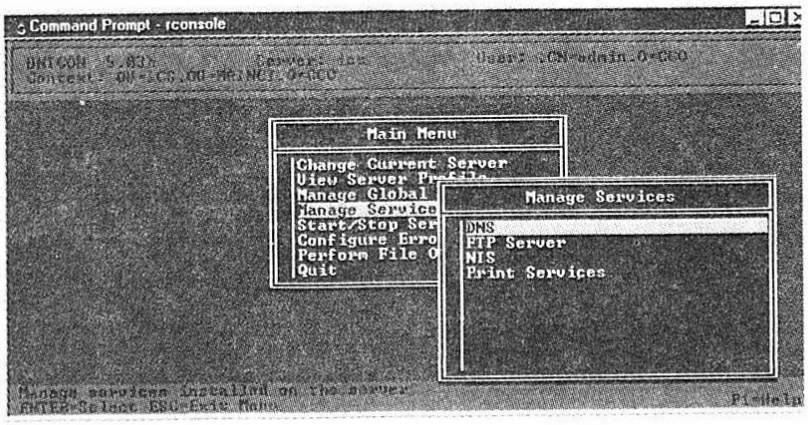
تنها چیزی که باید در مورد مسیریابی IPX/SPX، از نقطه‌نظر یک عیب‌یاب بدانید آن است که دو نوع مسیریابی IPX/SPX وجود دارد: NLSP (پروتکل سرویس‌های اتصالی نت‌ور)[1] و RIP (پروتکل اطلاعاتی مسیریابی)[2]. سرویس‌دهندهٔ نت‌وری که با RIP پیکربندی شده باشد، نمی‌تواند با مسیریاب NLSP صحبت کند مگر آنکه مسیریاب NLSP در وضعیت سازگاری با RIP اجرا شده باشد (در فصل ۱۴ به مقایسهٔ سریع RIP و NLSP خواهیم پرداخت). مشکلات زیادی را در ارتباط با این موضوع مشاهده کرده‌ام، خوب است که بدانید تفاوتهایی بین RIP (قدیمی‌تر) و NLSP (جدیدتر) وجود دارند.

1- NetWare Link Services Protocol

2- Routing Information Protocol

پیکربندی TCP/IP نظیر هر پروتکل دیگر صورت می‌گیرد: از طریق INETCFG.NLM. پیکربندی مقدماتی روشی است که با آن یک ایستگاه‌کاری را پیکربندی می‌نماییم. البته چند مورد کار بیشتر را روی سرویس‌دهنده به انجام خواهیدرساند، که بیشتر عبارتند از سرویس‌هایی که سرویس‌دهنده ارائه می‌کند. برای انجام این‌کار، از برنامهٔ کمکی UNICON استفاده کنید. می‌توانید از این برنامه برای وارسی پیکربندی‌های سرویس و همچنین برای متوقف‌کردن و شروع دوبارهٔ سرویس‌ها در صورتی که به خرابی کارکرد آنها ظنین هستید، استفاده نمایید. همانگونه که در شکل ۱۰-۱۳ مشهود است، UNICON اقلام زیر را پیکربندی می‌کند:

- DNS
- NIS (به این بخش نیازی ندارید مگر آنکه در مجموعهٔ کاری خود یونیکس داشته باشید).
- سرویس‌های چاپ یونیکس
- FTP



شکل ۱۰-۱۳ : UNICON سرویس‌های شبیه یونیکس را در سرویس‌دهندهٔ نت‌ور پیکربندی می‌کنند.



یادداشت : *UNI را در UNICON ملاحظه می‌کنید؟ فکر می‌کنید که اشاره به UNIX است؟ حق با شماست! تمامی این سرویس‌ها برخلاف عمومیت سرویس‌های TCP/IP، منشأ یونیکسی دارند.*



نکته : *همچنین می‌توانید فایل‌های پیکربندی TCP/IP در شاخهٔ SYS:ETC را بازرسی نمایید و یا احیاناً پیکربندی‌هایی را از نوار مغناطیسی کپی پشتیبان بازنشانی کنید.*



نکته : *فایل SYS:ETC/RESOLV.CFG، از اهمیت زیادی در پیکربندی برخوردار است ـ جستجوهای اسامی سمبولیک (DNS) در صورت عدم پیکربندی صحیح این فایل کار نخواهند کرد.*

بازی TCPCON

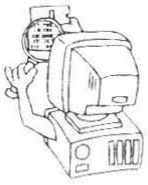
هنگام بارگذاری TCPCON، می‌توانید بیش از آنچه که می‌خواهید، آمار و کارکرد مربوط به TCP/IP را وارسی نمایید. TCPCON می‌تواند کارهای زیادی را انجام دهد که در جدول ۱-۱۳ نشان داده شده‌اند.

جدول ۱-۱۳ : توابع TCP/IP که از طریق TCPCON در دسترس قرار می‌گیرند

تابع	راهبری TCPCON
وارسی آمار TCP/IP و تعداد خطاها	منوی Statistics
وارسی جدول مسیریابی	جدول مسیریابی IP
وارسی جدول سوکت جاری TCP یا UDP (درست نظیر netstat -a در یونیکس یا ویندوز)	Protocol Information|TCP یا UDP|Connections
وارسی جدول آدرس MAC ـ به ـ TCP/IP (مثل arp -a در یونیکس یا ویندوز)	Protocol Information|IP|IP Address Translations

سایر ابزار TCP/IP عبارتند از:

- **LOAD PING** : برای ping استاندارد(با این تفاوت که می‌توانید همزمان چندین ایستگاه‌کاری را کنترل کنید)
- **LOAD IPTRACE** : پاسخ ناول به traceroute



نکته : *نمی‌توانید IPTRACE یا PING را بارگذاری کنید؟ این ماجولها در توزیع استاندارد TCP/IP ناول قرار نداشته‌اند. آخرین اصلاحیه‌ها را بارگذاری کنید و خواهید دید که می‌توانید از این ابزار استفاده کنید.*

خلاصه

NDS ناول یکی از دلایلی است که سیستم عامل شبکه‌ای ناول هنوز رها نشده است. سرویس‌دهندهٔ ناول چیزی بیشتر از یک برنامهٔ ۳۲ بیتی DOS نیست. اما اطلاعات لازم را برای بیشترین استفاده از سخت‌افزار فراهم می‌آورد و با استفاده از NLM های مختلف که کار سیستم را انجام می‌دهند، شبکه را ایجاد می‌کنند. پیمانه‌ای‌بودن سیستم به آن معناست که NLMای که خوب کار نمی‌کند ممکن است تمامی روزتان را خراب کند، اما ابزاری وجود دارند که می‌توان با کمک آنها مدیریت چنین خرابیهایی را به دست گرفت و کار ردیابی و ارتقاء را به انجام رساند.

Monitor می‌تواند در کارهای عیب‌یابی بسیار کارآ باشد، چرا که قادر است تمامی منابع متصل به سرویس‌دهنده را ردیابی و نگهداری نماید. علاوه بر این می‌تواند منابع حافظه و CPU و آنچه را که هر فرایند NLM در اختیار می‌گیرد کنترل نماید.

پیکربندی پروتکل IPX/SPX نسبتاً ساده است، اما در خیلی از جاها به TCP/IP نیازمند هستیم. هر دوی این پروتکل‌ها از طریق INETCFG.NLM قابل پیکربندی هستند. برنامه‌های کاربردی TCP/IP را می‌توان از طریق UNICON پیکربندی و بسیاری آمارها و جداول داخلی را می‌توان از طریق TCPCON ملاحظه و بررسی نمود. از آن گذشته اکنون ناول ابزار استانداردی نظیر PING و IPTRACE را در محصول TCP/IP خود ارائه می‌کند.

کارگاه

پرسش و پاسخ

پرسش : چرا ناول خود را از مفهوم ABEND ها خلاص نمی‌کند؟

پاسخ : هر سیستم عامل، چه یونیکس و چه NT، خطاهای غیر قابل تصحیحی دارد. این طبیعت ماجرا است. ایده این است: خیلی بهتر است که راه‌اندازی مجدد کنیم به‌جای آنکه مجبور شویم تمامی اطلاعات از دست رفته را در اثر توقف‌نکردن سرویس‌دهنده بازنشانی نماییم.

می‌توانید در سرویس‌دهندهٔ ناول خود دستور زیر را اجرا کنید تا بعد از وقوع ABEND های نرم‌افزاری به‌صورت خودکار راه‌اندازی مجدد شود، این‌کار در بیشتر اوقات روال بازیابی را خودکار می‌سازد (اگر می‌خواهید بعد از ABEND های سخت‌افزاری راه‌اندازی مجدد شود، باید از عدد ۲ هم استفاده کنید):

```
SET AUTO RESTART AFTER ABEND=1
```

پرسش : یکی از دوستان من که سرویس‌دهندهٔ ناولی را به اجرا درمی‌آورد، اذعان داشته که برخی اوقات وقتی که تلاش می‌کند NLM ای را پایین بیاورد، اعلان کنسول هرگز باز نمی‌گردد. آیا راهی برای خلاصی از این وضع وجود دارد؟

پاسخ : IntraNetWare 4.11 و نگارش‌های بالاتر ناول، این امکان را فراهم می‌آورند که در محل کنسول از کلید ترکیبی Ctrl+Alt+Esc استفاده نمایید. این باعث نمایش اعلان زیر می‌گردد:

```
Down Server and exit to DOS?
```

پاسخ به این سؤال بلی می‌باشد. گو این‌که دوست دارم به اعلان کنسول دیگری دسترسی داشته باشم و یا آنکه حداقل اعلان کنسول را هنگام وقوع چنین حالتی آزاد نمایم، اما تا کنون ناول چنین امکانی را در اختیار نگذارده است.

اگر هنوز از نتور 3.x استفاده می‌کنید می‌توانید از برنامهٔ FCONSOLE برای پایین‌آوردن سرویس‌دهنده‌ای که پاسخ نمی‌دهد استفاده نمایید؛ در این‌جا کلید ترکیبی Ctrl+Alt+Esc کار نمی‌کند.

آزمون

۱- منظور از سلسله‌مراتبی چیست؟

الف ـ ترجمهٔ هیروگلیف از اسناد باستانی کامپیوتری
ب ـ داشتن سطوح چندگانه
ج ـ توانایی بازیابی خطاها
د ـ داشتن بخشهای چندگانه در یک پایگاه اطلاعاتی

۲- هر پایگاه اطلاعاتی توزیع‌شده می‌تواند _____.

الف ـ در چندین سرویس‌دهنده قرار داشته باشد
ب ـ مجموعه‌ای از اطلاعات را بهتر در دسترس قرار دهد
ج ـ نه الف و نه ب
د ـ هم الف و هم ب

۳- درست یا نادرست؟ قسمت‌بندی یک پایگاه داده‌ای شبکه‌ای بزرگ آن را قابل مدیریت‌تر می‌سازد.

۴- اسم برنامهٔ سرویس‌دهندهٔ اصلی در ناول چیست؟

الف ـ SERVER.COM
ب ـ SERVER.EXE
ج ـ SERVER.NLM
د ـ SERVER.LAN

۵- هنگامی‌که مشکلی در سرویس‌دهندهٔ ناول دارید وارسی کدامیک از موارد زیر ایدهٔ خوبی به نظر می‌رسد؟

الف ـ دیسک سخت
ب ـ کارت LAN
ج ـ سطوح اصلاحیه
د ـ NLM BIOS حساس

۶- سرویس‌دهنده‌های IPX/SPX هر یک به ـــــــــــــ منحصربفرد نیاز دارند.

الف ـ شمارهٔ شبکه‌ای داخلی
ب ـ شمارهٔ شبکه‌ای اینترنت
ج ـ شمارهٔ هسته‌ای اینترنت
د ـ شمارهٔ هسته‌ای داخلی

۷- پروتکل TCP/IP سرویس‌های مقدماتی و اصلی را می‌توان از طریق ـــــــــــــ پیکربندی نمود.

الف ـ TCPCON
ب ـ INETCFG
ج ـ TCPCON و UNICON
د ـ INETCFG و UNICON

پاسخ به سؤالات آزمون

۱- ب
۲- د
۳- درست
۴- ب
۵- ج
۶- الف
۷- د

فصل ۱۴

مبانی مسیریاب و سوئیچ

با وجود تفاوت بسیار بین یک سمفونی بتهوون و یکی از کارهای باخ، هر دو از ترکیب و تئوری پایه‌ای یکسانی بهره می‌برند. با این‌که فضای زیادی برای خلاقیت و ابداع در میدان قوانین تئوری و ترکیبی وجود دارد، در صورتی‌که این قوانین دنبال نگردند، سازنده‌ها ممکن است به چیزی برسند که نظیر صدای قوطی حلبی در کوچه‌ای باریک به نظر برسد.

با وجود دهها مسیریاب و سوئیچ مبتنی بر سخت‌افزار که در بازار وجود دارند، اگر غیر ممکن نباشد، مشکل خواهد بود که روشهای مشخصی را در مورد نحوهٔ عملکرد آنها ارائه داد. خوشبختانه آنها نیز از اصول ساختاری و تئوری مبنایی مربوط به مسیریاب‌ها و سوئیچ‌ها استفاده می‌کنند؛ در این فصل تئوری موجود در ورای مسیریابی و سوئیچینگ را توضیح می‌دهم و چند پیشنهاد عملی ارائه می‌کنم. این مطالب در ترکیب با مستندات مسیریاب یا سوئیچ می‌تواند ضربه شصت مؤثری در حل بسیاری از مشکلات مربوط به مسیریاب یا سوئیچ باشند.

تئوری و عملی

چرا در مورد مسیریابی و سوئیچینگ با هم گفتگو می‌شود؟ خوب، مسیریاب و سوئیچ از لحاظ اصول بسیار شبیه به یکدیگر کار می‌کنند: هر یک بسته‌ای را از طریق یکی از رابطهای خود دریافت نموده و به رابط دیگری می‌دهد. تنها لایهٔ شبکهٔ مسیریاب با لایهٔ مربوط به سوئیچ متفاوت است؛ مسیریاب‌ها در لایهٔ پروتکلی (برای مثال، TCP/IP) کار می‌کنند، در حالی‌که عملکرد سوئیچ‌ها در لایهٔ پیوند داده صورت می‌پذیرد (یعنی آنها مستقیماً با کارتهای شبکه صحبت می‌کنند).



یادداشت : *هنگامی‌که استادکاران شبکه در مکالمهٔ خود به لایه‌ها اشاره می‌کنند، منظورشان مدل OSI (مؤسسهٔ استانداردهای باز) می‌باشد که از یکی خیالی با هفت طبقه یا لایه تشکیل گردیده است:*

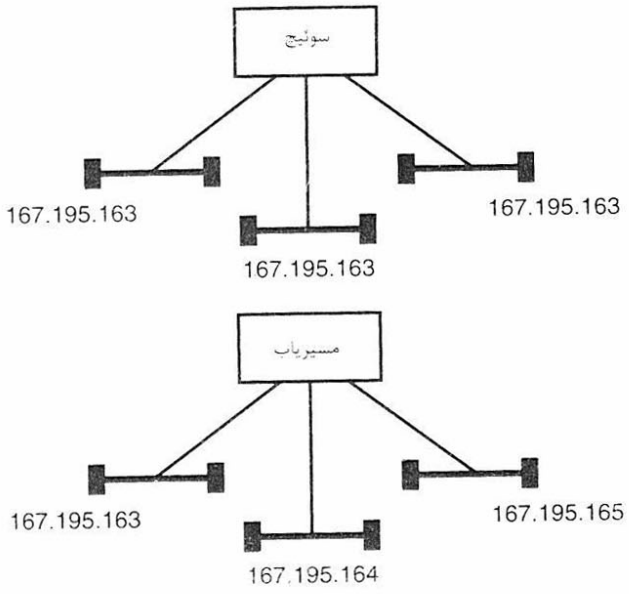
- *فیزیکی*
- *پیوند داده*
- *شبکه*
- *حمل*
- *جلسه*
- *نمایش*
- *کاربرد*

توجه داشته باشید که در شبکه‌های واقعی نماینده‌ای برای تک تک این لایه‌ها وجود ندارد. برخی از این لایه‌ها هنگام تفکر در مورد شبکهٔ واقعی مفید واقع می‌شود. برای مثال لایهٔ فیزیکی بر قواعد الکترونیکی و سیگنالی که در سیم اِترنِت به اجرا در می‌آید، دلالت دارد؛ در حالی‌که لایهٔ پیوند داده در مورد مکالمات کارت به کارت (MAC) کارتهای شبکه می‌باشد. لایهٔ شبکه به پروتکل شبکه (TCP/IP یا IPX/SPX) اشاره می‌کند. منظور از لایهٔ کاربرد نیز سرویس‌هایی مثل سرویس وِب یا FTP می‌باشد.



نکته : *بنا به تعریف، هم به مسیریاب‌ها و هم به سوئیچ‌ها میزبانهای چند خانه‌ای گفته می‌شود - یعنی آنها بیش از یک رابط شبکه دارند که به بیش از یک بخش از شبکه متصل شده است. می‌توانید چنین تصور کنید مسیریاب‌ها و سوئیچ‌ها دارای تعداد بیشتر از یک شبکه هستند که به آنها خانه اطلاق می‌کنند.*

در جهان واقعی با وجود این‌که بین مسیریاب‌ها و سوئیچ‌ها تفاوت گذاشته می‌شود، بیشتر سوئیچ‌های بزرگ توانایی‌های مسیریابی را دارا هستند و مسیریاب‌های پیشرفته نیز قادرند عملیات سوئیچینگ را به انجام برسانند (یا آنچه که پل سازی نامیده می‌شود). بنابراین، از جنبهٔ مسائل قابل توجه عملی، بهتر است بدانید که ممکن است سوئیچ طوری پیکربندی شده باشد که عملیات مسیریابی را نیز به انجام برساند و همچنین مسیریاب هم ممکن است برای انجام توابع سودیچینگ پیکربندی شده باشد. شکل ۱-۱۴ تفاوت عملی بین مسیریاب و سوئیچ را نشان می‌دهد (توجه داشته باشید که آدرس‌های IP متفاوتی به مسیریاب متصل شده‌اند، در حالی که شبکه‌های مختلفی به سوئیچ متصل گردیده‌اند).

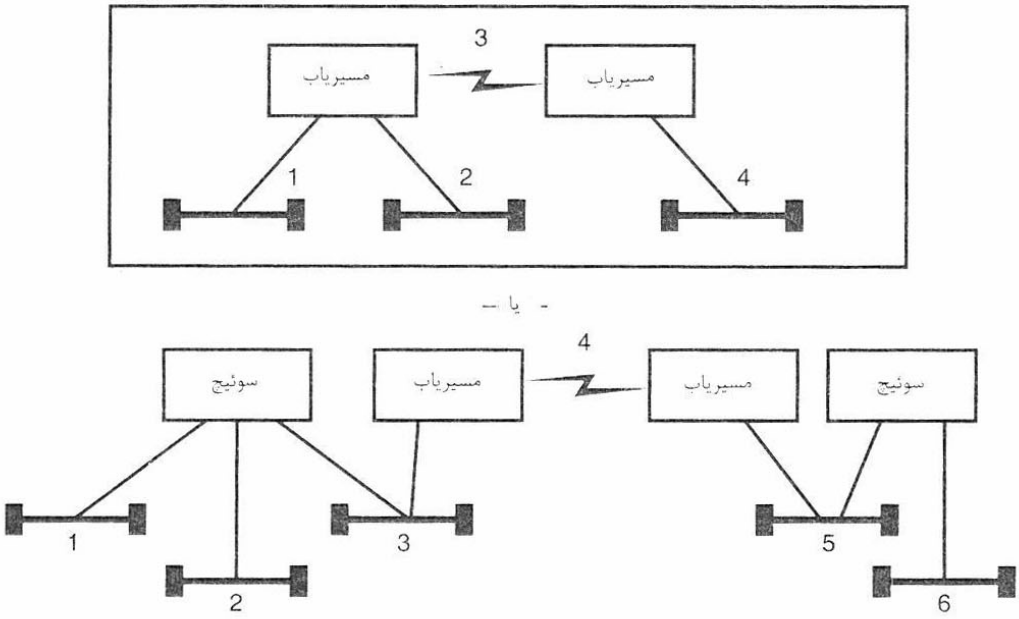


شکل ۱-۱۴ : تفاوت اصلی بین مسیریاب و سوئیچ: تمامی شبکه‌های متصل به سوئیچ دارای یک شمارهٔ شبکه‌ای هستند.



یادداشت : *سوئیچ ابزاری است که می‌تواند بسته‌ها را با سرعت دریافت آنها به خارج ارسال کند. این بدان معناست که اغلب در پیوند کند و آهسته از سوئیچ استفاده نمی‌شود (یعنی، پیوندی از نوع گسترده). دلیل این مطلب آن است که ارتباط پیوند داده اغلب بسیار بسیار وابسته به زمان است - که*

این موضوع قابل لمس است، چرا که اطلاعات پیوند داده اغلب در یک خط جمعی بدون فاصله‌ای به دنبال یکدیگر قرار دارد. بنابراین نباید پتانسیل آشفتگی ارتباطات را از طریق به هم ریختن زمانبندی بیشتر کرد. این یک نمونه از عدم به‌کارگیری سوئیچ و مسیریاب به جای یکدیگر می‌باشد. اغلب از مسیریاب به شکلی ترکیبی استفاده می‌شود (شکل ۲-۱۴ را ملاحظه کنید).



شکل ۲-۱۴ : برنامه‌های کاربردی مخصوص نواحی گسترده، اغلب از مسیریاب‌ها در ارتباط‌دهی بخشهای مختلف استفاده می‌کنند.

به وضوح مشخص است که باید به خوبی با مستندات سوئیچ یا مسیریاب خود آشنا باشید. با وجود یکسان‌بودن تئوری به‌کار گرفته شده در مسیریاب‌ها و سوئیچ‌ها، نحوهٔ پیکربندی هر سوئیچ یا مسیریاب با بقیه متفاوت است. این موضوع در عمل هنگامی‌که فرصت محدودی برای نواختن ادوات موسیقی خود داشته باشید صادق خواهد بود ـ برای مثال هنگامی‌که موقع ورود به صحنه، همه چیز آماده و مورد بهره‌برداری قرار گرفته شده است (مردم به این گونه موارد حساسیت ویژه‌ای دارند. هنگامی‌که ابزاری در خط تولید قرار گرفت، بنا به دلایلی، تغییر چیزها به منظور مشاهدهٔ تأثیر تغییرات کاری ناشایست به نظر می‌رسد).



یادداشت : *اگر بتوانید ابزاری را قبل از مورد استفاده قرارگرفتن متوقف کنید بسیار بهتر خواهد بود. آشنایی با دستورات، تسهیلات مخابرهٔ خطا و روال پیکربندی ابزار، شما را قادر می‌سازد هنگام بروز مشکلات بعد از قرارگرفتن در خط تولید و مورد استفاده واقع‌شدن، بهتر عمل نمایید.*

یک مورد وجود دارد که بین مسیریاب‌ها و سوئیچ‌ها پایدار و ثابت می‌ماند ـ آنها اغلب از طریق اقلام زیر قابل پیکربندی هستند:

- Telnet
- Web
- پایانهٔ نمایشی

گزینهٔ پایانهٔ نمایشی، شکل عمومی‌تری دارد ـ این امکان را فراهم می‌سازد که حتی در صورت پایین‌بودن شبکه، با ابزار ارتباط برقرار کنید.



نکته : *اگر سوئیچ یا مسیریابتان دارای حالت پایانهٔ نمایشی باشد، می‌توانید پورت سریال PC خود را با استفاده از یک کابل مودم پوچ به آن متصل نمایید. اتصال از طرف دستگاه یکی از دو شکل DB-9 (نر) یا DB-25 (نر) می‌باشد؛ اگر اتصال شکل دیگری دارد، احیاناً ممکن است به پورت پایانهٔ نمایشی تعلق نداشته باشد.*

بعد از اتصال کابل می‌توانید از هر برنامهٔ مودمی (ProComm,HyperTerminal,NetTerm و نظایر آنها) برای اتصال به ابزار استفاده نمایید. عمومی‌ترین تنظیمات مربوط به حالت پایانه‌ای نمایشی عبارتند از: ۸ بیت داده‌ای، حالت قیاسی غیرفعال، ۱ بیت توقف و ۹۶۰۰bps. برخی اوقات این اطلاعات را به صورت 9600-8-N-1 نشان می‌دهند.



هشدار : *برخی از مسیریاب‌ها و سوئیچ‌ها امکان برداشت کپی پشتیبان از اطلاعات پیکربندی خود را در اختیار نمی‌گذارند. اغلب نمی‌توان نوارگردان لازم برای انجام چنین کاری را در مسیریاب یا سوئیچ نصب نمود و بیشتر آنها این امکان را فراهم نمی‌آورند که پیکربندیشان را به سرویس‌دهنده‌ای که به نوارگردان مجهز گردیده است، منتقل کنند.*

دست آخر این‌که: مطمئن شوید که کلیهٔ اطلاعات پیکربندی را مستندسازی نموده‌اید. هنگامی‌که با مسیریاب کار می‌کنید، اغلب یک دستور برای نمایش پیکربندی (SHOW CONFIGURATION) وجود دارد؛ اگر این دستور و خروجی آن را با استفاده از برنامهٔ پایانه‌ای خود ضبط نمایید، می‌توانید آن را چاپ کنید تا به عنوان کپی پشتیبان مورد استفاده قرار گیرد علاوه بر همهٔ این موارد مسیریاب‌ها و سوئیچ‌ها، مکانهای حساسی هستند که بهتر است تغییرات در آنها به گونهٔ مفید و کاملی به ثبت برسد.

تئوری مسیریاب

هر مسیریاب به هر یک از رابطهای چندگانهٔ خود گوش فرامی‌دهد تا درخواستهای مسیریابی را دریافت نماید از فصل ۱ به خاطر دارید که بسته کوچکترین واحد ارتباطی بین دو کارت شبکه است. هنگامی‌که یک کارت شبکه بسته‌ای را که به مقصد بخش شبکه‌ای متفاوت ارسال‌شده، به مسیریاب می‌دهد، مسیریاب باید تصمیم‌گیری کند که بسته را به کدامیک از رابطهای شبکه‌ای خود تحویل نماید. اگر مسیریاب مستقیماً به بخش شبکه‌ای مقصد متصل باشد، تنها کاری که صورت می‌گیرد بازکردن رابط متصل‌شده به آن بخش است. در غیر اینصورت، بسته را باید به مسیریاب دیگری بدهد که به بخش مورد نظر متصل گردیده است (یا نزدیک‌تر به مسیریابی که مستقیماً به آن بخش وصل شده است).

تصور کنید که بسته مثل فردی است بدون اتومبیل. این فرد می‌تواند هر جایی که می‌خواهد در محدودهٔ محلی قدم بگذارد، اما برای رفتن به منزل دوستش در آن سوی شهر باید سوار اتوبوس گردد. می‌تواند از خط اتوبوس محلی خود استفاده کند، اما ممکن است از خطوط اتوبوسرانی مختلفی برای رسیدن به مقصد نهایی خود بهره ببرد.

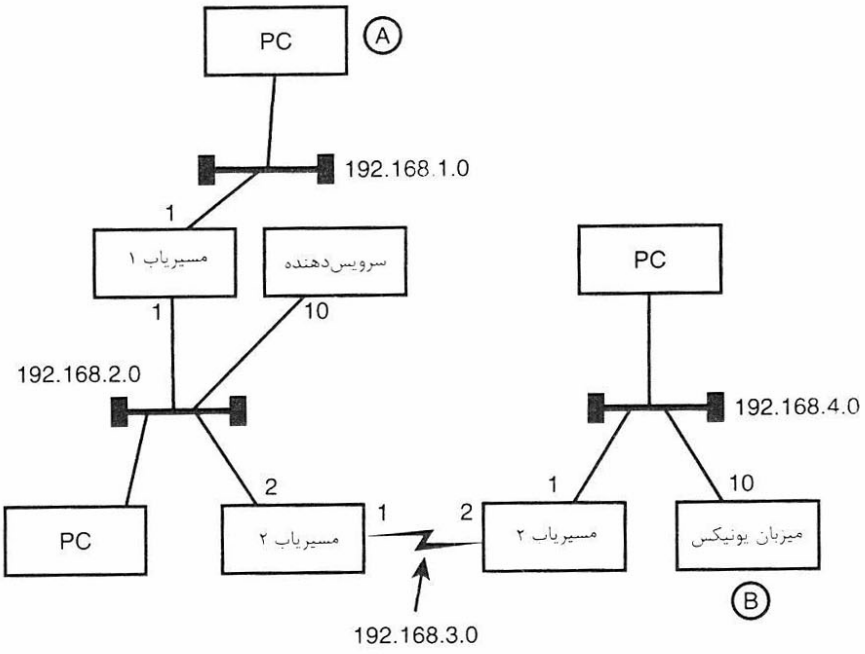


یادداشت : *هر ایستگاه‌کاری چگونه آدرس پروتکلی مسیریاب خود را می‌شناسد؟ بیشتر اوقات، سرپرست شبکه آدرس مربوطه را در پیکربندی ایستگاه‌کاری وارد می‌کند. اما بهتر است بدانیم چیزی به نام کاوشگر مسیریاب[1] وجود دارد که عمل جستجو به دنبال مسیریاب را در زیرشبکه برای ایستگاه‌کاری به انجام می‌رساند.*

جداول مسیریابی

واضح است که اگر مسیریاب اتصال مستقیمی به یک بخش ویژه داشته باشد، می‌داند که چگونه بسته را به آن تحویل دهد. اما اگر بستهٔ دریافتی، متعلق به بخشی نباشد که مسیریاب مستقیماً به آن متصل شده باشد چطور؟ چگونه مسیریاب «خط اتوبوسرانی» که باید بسته به آن سوار شود، تشخیص می‌دهد؟

هر مسیریاب یک جدول داخلی دارد که حاوی تمامی شبکه‌هایی است که در مورد آنها اطلاع کسب نموده است. به چنین جدولی جدول مسیریابی گفته می‌شود. جدول مسیریابی شامل فهرستی از شماره‌های شبکه‌ای است که نشاندهندهٔ نحوهٔ دسترسی به این شمارهٔ شبکه‌ای از طریق مسیریاب یا رابط دیگر می‌باشد. همچنین مسافت یا زمان مسیر در جدول منعکس می‌گردد. جدول مسیریابی مسیریاب ۱ در شکل ۳-۱۴، به‌صورت جدول ۱-۱۴ منعکس گردیده است.



شکل ۳-۱۴ : شبکه‌ای ساده با امکان مسیریابی.

جدول ۱-۱۴ : جدول مسیریابی برای مسیریاب ۱

شبکه	جهش بعدی	اندازه
192.168.1.0	192.168.1.1	0 (مستقیم)
192.168.2.0	192.168.2.1	0 (مستقیم)
192.168.3.0	192.168.2.2	1
192.168.4.0	192.168.2.2	2

1- router discovery



یادداشت : *بسته به مسیریابتان، کلمات جهش بعدی در جدول مسیریابی ممکن است با کلماتی نظیر مقصد یا آدرس دروازه تعویض گردد. کلمهٔ اندازه نیز ممکن است جایگزینی نظیر هزینه داشته باشد. در چنین حالتی، اندازه به تعداد جهش‌هایی که شبکه از مسیریاب فاصله دارد، اشاره می‌کند.*

برای مثال نگاهی به شکل ۳-۱۴ بیندازید و تعداد مسیریاب‌هایی را که باید از مسیریاب 1 به 192.168.1.0 طی شوند، بشمارید. لازم نیست از طریق هیچ مسیریابی عمل کنید، بنابراین تعداد جهشها صفر است. چند مسیریاب از مسیریاب 1 به 192.168.3.0؟ درست است، یک جهش ـ از طریق مسیریاب 2.

قالب این جدول، بسته به نوع مسیریاب 1 متفاوت است، اما محتویات آن یکی خواهد بود. توجه داشته باشید که جدول مسیریابی می‌تواند تنها «جهش بعدی» مقصدهایی را ارائه کند که به صورت مستقیم توسط آن مسیریاب قابل دسترسی هستند. به بیان دیگر، اطلاعات مسیریاب تنها در مورد شبکه‌هایی است که به صورت فیزیکی به آن متصل شده‌اند، درست نظیر اتوبوس شهری که تنها نقاط نقل و انتقال موجود در خیابانهای مسیر خود را می‌شناسد. تمامی شبکه‌های دیگر از طریق مسیریاب‌هایی که به زیرشبکهٔ مشترک متصل شده‌اند، قابل دسترسی می‌باشند.

دو میلی ثانیه از زندگی یک بسته

اجازه دهید مثال دیگری را با ردیابی بسته‌ای در میان شبکهٔ نشان داده شده در شکل ۳-۱۴ ، دنبال نماییم. PC موجود در نقطهٔ A، می‌خواهد سرویس‌دهندهٔ یونیکس موجود در نقطهٔ B را Telnet نماید. از آنجا که در مورد مسیریابی صحبت می‌کنیم، توجهی به مشخصات مکالمهٔ شبکه نخواهیم داشت؛ تنها می‌خواهیم ببینیم چگونه فراخوانی نقطهٔ A به نقطهٔ B می‌رسد. مراحل کار به شکل زیر است:

۱- «واسطه»‌ای که اجازه می‌دهد برنامهٔ کاربردی با راه‌انداز کارت شبکه صحبت کند، پشته نامیده می‌شود. پشتهٔ پروتکلی TCP/IP در PC شما باید اتصالی را با سرویس‌دهندهٔ یونیکس در آدرس 192.168.4.10 ایجاد نماید. پشتهٔ TCP/IP، می‌داند که آدرس IP خودش چیست (192.168.1.20) و متوجه می‌شود که 192.168.4 در همان شبکه وجود ندارد. بنابراین، به‌جای ایجاد مکالمه‌ای با مقصد، پشتهٔ IP مکالمه‌ای را با مسیریاب آغاز می‌کند.

۲- پشتهٔ IP بستهٔ اول مکالمهٔ Telnet را به مسیریاب موجود در 192.168.1.1 می‌دهد (مسیریاب 1).

۳- مسیریاب، ابتدا شبکهٔ مقصد را در جدول مسیریابی خود پویش می‌کند. در این حالت، مقصد در جدول مسیریابی مسیریاب 1 وجود دارد و از طریق مسیریاب 192.168.2.1 (مسیریاب 2) قابل دسترسی است.



یادداشت : *در صورتی‌که شبکهٔ مقصد در جدول مسیریابی وجود نداشته باشد، مسیریاب بسته را دور می‌اندازد و یک بستهٔ IP مخصوص بازگشت می‌دهد که نشاندهندهٔ غیرقابل دسترسی‌بودن این مقصد می‌باشد.*

۴- مسیریاب 1 مکالمه‌ای را با مسیریاب 2 آغاز می‌کند. جدول مسیریابی این مسیریاب در جدول ۲-۱۴ نشان داده شده است.

جدول ۲-۱۴ : جدول مسیریابی برای مسیریاب 2

شبکه	جهش بعدی	اندازه
192.168.2.0	192.168.2.2	(مستقیم)0
192.168.3.0	192.168.3.1	(مستقیم)0
192.168.1.0	192.168.2.1	1
192.168.4.0	192.168.3.2	1

۵- بسته می‌خواهد به نقطهٔ B از مسیریاب 2 برود. مسیریاب 2 شبکهٔ مقصد (192.168.4) را در جدول مسیریابی خود مورد جستجو قرار می‌دهد و درمی‌یابد که اتصال مستقیمی به آن شبکه ندارد. به‌جای آن، جهش بعدی در 192.168.3.2 (مسیریاب 3) می‌باشد که در سوی دیگر اتصال ناحیهٔ گسترده قرار دارد. جدول مسیریابی مسیریاب 3 در جدول ۳-۱۴ نشان داده شده است.

جدول ۳-۱۴ : جدول مسیریابی برای مسیریاب 3

شبکه	جهش بعدی	اندازه
192.168.3.0	192.168.3.2	(مستقیم)0
192.168.4.0	192.168.4.1	(مستقیم)0
192.168.1.0	192.168.3.1	2
192.168.2.0	192.168.3.1	1

۶- و بالاخره مقصد 192.168.4.10 به‌صورت مستقیم به شبکه متصل شده است! تمام کاری که مسیریاب 3 انجام می‌دهد، ایجاد یک اتصال در سطح اِترنِت با میزبان یونیکس و در اختیار قرار دادن بسته‌های دریافتی از مسیریاب 2 می‌باشد. به این‌صورت بسته‌ها به جریان می‌افتد.

البته، پاسخهای میزبان یونیکس به مقصد PC در نقطهٔ A از طریق میزبان یونیکس به مسیریاب 3، به مسیریاب 2، به سمیریاب 1 و آنگاه به PC می‌روند. ممکن است اشتباه‌برانگیز به نظر برسد اما اگر نگاهی به نقشه و تک تک جداول مسیریابی بیندازید، با در نظرداشتن این‌که این‌بار مقصد عبارت است از 192.168.1، ملاحظه خواهید نمود که هر جستجو در جدول، مسیریاب صحیح بعدی را نشان می‌دهد.

در دنیای واقعی، این‌کار با پیچیدگی بیشتری صورت می‌گیرد. هر جدول مسیریابی ممکن است صدها ـ یا حتی هزاران ـ ورودی داشته باشد. البته، مبانی اصولی بدون تغییر باقی می‌ماند؛ بیشتر آن چیزی که لازم است از نقطه‌نظر عیب‌یابی درک شود، آن است که بدانید چگونه به مسیریابتان دستور دهید که جدول مسیریابی خویش را نمایان سازد. به این صورت، می‌توانید آن را وارسی کنید. برای مثال، اگر جدول مسیریاب 1 نشان می‌داد که جهش بعدی به 192.168.4.0 عبارت بود از 192.168.2.10 (سرویس‌دهندهٔ فایل و چاپ)، باید تحقیق می‌کردید که چرا مسیریاب 1 فکر می‌کند بهترین مسیر به سوی 192.168.4 از طریق این سرویس‌دهنده می‌باشد (عبور از سرویس‌دهنده به خودی خود موضوع دهشتباری نیست ـ به‌خصوص اگر سرویس‌دهنده، یک سرویس‌دهندهٔ چندخانه‌ای باشد که مثل مسیریاب عمل نماید. اما در این حالت، نقطه‌ای کشنده محسوب می‌گردد).

مسیریاب‌های پویا

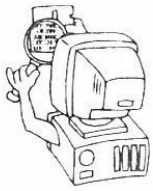
حدود چهار پاراگراف قبل شنیدم که سؤال کردید، «جدول مسیریابی چگونه ساخته می‌شود؟» .نمی‌خواستم از این سؤالتان

چشم‌پوشی کنم؛ سؤال خوبی است. برای شروع پاسخ به آن، اجازه دهید انواع اصلی ورودیهای مسیریابی را مورد بحث قرار دهید.

دو نوع مسیریاب وجود دارند که ممکن است در جدول مسیریابی تشکیل شوند:

- **مسیرهای ایستا** : مسیر ایستا، مسیری است که توسط خود شما از طریق کنسول مسیریاب، وارد می‌شود. این‌کار کسل‌کننده است و روش قابل انعطاف و آسانی در پیکربندی دوبارهٔ شبکه محسوب نمی‌شود.

- **مسیرهای پویا** : مسیرهای پویا از طریق پروتکل‌های مسیریابی ساخته می‌شوند.



***نکته** : یک مسیر ایستای ویژه که بهتر است آن را بشناسید، **مسیر پیش‌گزیده** نامیده می‌شود. این مسیر با شبکهٔ مقصد 0.0.0.0 شناخته شده و مسیری است که هنگام نامشخص بودن مقصد بسته و عدم تطابق آن با اطلاعات جدول مسیریابی، مورد استفاده قرار می‌گیرد.*

پروتکل‌های مسیریابی بر اساس این مفهوم کار می‌کنند که هر مسیریاب شبکهٔ محل زندگی خود را «می‌شناسد»، و می‌تواند با شبکه‌های دیگر از طریق مسیریاب‌های دیگر ارتباط برقرار کند. نگاهی دوباره به شکل ۳-۱۴، مشخص می‌کند که مسیریاب 1 می‌تواند در مورد شبکهٔ 192.168.1 برای مسیریاب 2 تعریف کند و مسیریاب 2 نیز می‌تواند از شبکهٔ 192.168.3 برای مسیریاب 1 بگوید ـ همچنین اطلاعاتی در مورد شبکهٔ 192.164.4 ، بعد از آنکه مسیریاب 3 اطلاعات مربوطه را در اختیار مسیریاب 2 قرار داده است.

خوب است که این‌کار کم و بیش به‌صورت خودکار صورت می‌پذیرد، چرا که در شبکه‌ای بزرگ، بسیار وقت‌گیر و حتی غیر ممکن خواهد بود. در این‌جا دوباره مسیرهای پویا در کارکرد این شبکهٔ نمونه را ملاحظه می‌کنید:

مسیریاب 1	به مسیریاب 2 از 192.168.1 می‌گوید
مسیریاب 2	به مسیریاب 1 از شبکهٔ 192.168.3 می‌گوید
	به مسیریاب 3 در مورد 192.168.1 می‌گوید
	به مسیریاب 1 اطلاعات 192.168.4 را می‌دهد
مسیریاب 3	به مسیریاب 2 از شبکهٔ 192.168.4 خبر می‌دهد

مسیریابی در صلح و صفا: پروتکل‌های مسیریابی

چهار نوع عمومی و پرکاربرد از پروتکل‌های مسیریابی وجود دارند که باید در مورد آنها بیشتر بدانید ـ بیش از هر چیز دیگری برای وارسی پیکربندی (با حصول اطمینان از این‌که مسیریاب‌ها برای پروتکل‌های مسیریابی یکسانی پیکربندی شده‌اند). هر یک از مجموعه‌های TCP/IP و IPX/SPX دو پروتکل عمومی دارند. پروتکل مسیریابی قدیمی‌تر برای هر دوی این مجموعه‌ها، پروتکل اطلاعات مسیریابی (*RIP*)[1] نامیده می‌شود.



***یادداشت** : درک این موضوع مهم است که پروتکل‌های شبکه‌ای متفاوت (TCP/IP در مقابل IPX/SPX)، پروتکل‌های مسیریابی متفاوتی دارند. با این‌که RIP مربوط به TCP/IP شبیه RIP مربوط به IPX/SPX کار می‌کند، در واقع، تفاوتهایی وجود دارد.*

1- Routing Information Protocol

RIP

هم TCP/IP RIP و هم IPX/SPX RIP پروتکل‌هایی انتشاری هستند ـ یعنی هر مسیریاب RIP، جدول مسیریابی خود را به تمامی افراد شبکه هر چند وقت یکبار اعلام می‌کند. همچنین هر دوی RIP ها هزینهٔ مسیر را بر پایهٔ تعداد جهش‌ها و نه بر اساس سرعت مسیر اعلام می‌کنند (این موضوع برای حالاتی که مسیرهای چندگانه برای رسیدن به یک شبکه وجود دارد مهم است). RIP می‌تواند در شبکه‌های پیچیده، ترافیک شبکه‌ای زیادی را ایجاد نماید، چرا که خیلی صحبت می‌کند (TCP/IP RIP هر ۳۰ ثانیه یک بار، انتشاری را صورت می‌دهد).



یادداشت : *IPX/SPX پروتکل متناظر با RIP دارد که* **SAP** *(پروتکل آگهی سرویس[1]) نامیده می‌شود. این پروتکل از جهت انتشار اطلاعات به شبکه برای هر کسی که ممکن است گوش فراداده باشد، شبیه به RIP است. تفاوت آن با RIP آن است که به منظور آگاه‌سازی سرویس‌دهنده‌ها و نه مسیریاب‌ها به کار می‌رود.*

دلیل وجودی SAP نظیر RIP می‌باشد ـ این امکان را به وجود می‌آورد که تمامی مسیریاب‌ها از طریق انتشار اطلاعات مشترکی را داشته باشند.

OSPF و NLSP

اگر شبکه‌تان پیچیده و انبوه است، ممکن است بهتر باشد استفاده از IPX RIP را کنار گذاشته و سراغ NLSP بروید (NLSP جایگزین SAP و RIP شده است). به گونهٔ مشابهی اگر شبکهٔ TCP/IP تان بزرگ و پیچیده شده، ممکن است بخواهید OSPF را جایگزین RIP نمایید. OSPF (انتخاب مقدم کوتاهترین مسیر[2]) برای TCP/IP و NLSP (پروتکل وضعیت پیوند نت‌ور[3]) برای IPX/SPX پروتکل‌های مسیریابی پیشرفته‌تری هستند. آنها سرعت پیوند را نیز به حساب می‌آورند و بر اساس آن هزینه را تعیین می‌کنند. هر مسیریاب NLSP یا OSPF خود را به سایر مسیریاب‌های آن شبکه می‌شناساند و مسیرهای شناسایی‌شده توسط سایر مسیریاب‌ها را یاد می‌گیرد. در صورت تغییر، مسیریاب‌ها به‌صورت مستقیم با آن ارتباط برقرار می‌کنند؛ چرا که آنها متناوباً وارسی‌های سریعی را انجام می‌دهند (اغلب هر ۱۰ ثانیه)، مسیریاب خراب مورد شناسایی واقع شده و جداول مسیریابی به سرعت به‌روزدرآورده می‌شوند.

مشکل چندانی در ارتباط با پروتکل‌های مسیریابی وجود ندارد، به غیر از مشکلاتی که بیشتر حالت تأثیر جانبی دارد ـ یعنی مشکلاتی که در اصل توسط پورت هاب، کابل، کارت شبکه، یا تأخیر پیکربندی نامتناسب ایجاد می‌شوند. با این وجود خوب است که با مبانی و اصول کار آشنا باشید و بتوانید پیکربندی را از مسیریاب خود خوانده و تصوری اولیه از آنچه که می‌گذرد ایجاد نمایید.



نکته : *تمامی سرویس‌دهنده‌های مدرن ـ NT، یونیکس یا نت‌ور ـ را می‌توان طوری پیکربندی نمود که مسیریاب‌های ساده و ارزانقیمتی باشند. البته برای آنکه بتوان آنها را به چند شبکه وصل نمود، باید از نوع چندخانه‌ای باشند.*

برخی اوقات از این روش برای کنارگذاشتن مسیریاب‌ها استفاده می‌کنند. اگر به وابستگی مشکلی شبکه‌ای به یکی از مسیریاب‌ها مظنون باشم، بسیار بهتر و ارزانتر خواهد بود اگر به صورت موقت یک

1- Service Advertisement Protocol
2- Open Shortest Path First
3- NetWare Link State Protocol

ماشین یونیکس را که نظیر مسیریاب عمل می‌کند به‌جای خرید مسیریابی ده هزار دلاری تنها برای کنارگذاشتن احتمال خرابی مسیریاب، مورد استفاده قرار دهم.

غرش مسیریاب!

هنگام آغاز تجربه با مسیریاب‌ها، مواظب باشید. مسیریاب‌ها برخلاف سرویس‌دهنده‌ها که موجودیت‌هایی متکی بر خود هستند، در صورت شرکت در پروتکل‌های مسیریابی در شبکه، هنگام پیکربندی نامناسب می‌توانند به‌صورت جدی وضعیت اتصالی شما به شبکه را تخریب نمایند.

موقعیتی را دیده‌ام که در آن شخصی مسیریابی را به شبکهٔ A متصل نمود که طوری پیکربندی شده بود که شبکهٔ A را به شبکهٔ B وصل نماید. این‌کار به خاطر آن بود که مسیریاب جدید قرار بود جایگزین مسیریابی شود که به شبکهٔ B سرویس می‌داد.

متأسفانه، رابط ثانویه مسیریاب جدید برای اتصال به شبکهٔ B پیکربندی شده بود و با آنکه هنوز به شبکهٔ B اتصال درستی نداشت، شروع کرد به پخش آگهی از طریق پروتکل‌های مسیریابی که آن را بهترین مسیر به شبکهٔ B فرض می‌نمود. این‌کار باعث بروز اشتباهاتی در جداول مسیریابی شد ؛ برخی از بسته‌ها به‌سوی این مسیریاب حرکت کردند، تنها به این منظور که از آن عبور کنند، اما خروجی‌ای وجود نداشت! مسیریاب درنظرگرفته شده برای شبکهٔ B آنچه را که از آن خواسته شده بود به انجام می‌رساند اما کار آن توسط مسیریاب جدید مختل شده بود.

در اینجا درسی را می‌گیریم: مسیریاب جدید را نباید به شبکه‌ای فعال متصل نمود تا زمانی که وقتش فرا رسد؛ به‌جای آن، باید از یک شبکهٔ مجزا استفاده کرد. هابهای آزمایشی به اندازهٔ کافی ارزانقیمت هستند ـ ایجاد دو بخش آزمایشی نباید بیشتر از ۱۰۰ دلار هزینه داشته باشد.

همچنین موقعیتی را شاهد بوده‌ام که در آن یک مسیریاب RIP برای شبکهٔ C اشتباهاً به شبکهٔ A متصل شده بود. از آنجا که مسیرهای RIP به‌جای حرکت آدرس به آدرس، انتشاری هستند، مسیریاب می‌توانست به تمامی مسیریاب‌های آن بخش بگوید که بهترین راه منتهی به شبکهٔ C را می‌داند. دوباره ناگهان افراد آن بخش از شبکه نمی‌توانستند کار خود را انجام دهند تا این‌که اشتباه کشف شد.

خطاهای انسانی را می‌توان با انجام تجزیه تحلیل تغییرات مشخص نمود هر دوی این خطاها از طریق آزمایش جدول مسیریابی پیدا شد. خوشبختانه از آنجا که شبکه‌ها به خوبی مستندسازی شده بودند تعیین مسیر اشتباه آسان بود و شخص می‌توانست با نگاه‌کردن به جدول مسیریابی تعیین کند که جهش بعدی به سوی شبکه‌ای خاص در جدول درست یا نادرست می‌باشد.

وارسی مسیرها

مشکلات مسیریابی را می‌توان از طریق خود مسیریاب پیگیری نمود اما می‌توان علاوه بر آن این‌کار را از طریق شبکهٔ متصل به مسیریاب انجام داد. می‌توانید فعال‌بودن مسیریاب را از طریق Ping کردن آن بررسی کنید (این کار باید از طریق بخش شبکه‌ای مربوط به مسیریاب صورت پذیرد، چرا که Ping کردن مسیریاب از بخشهای شبکه‌ای دیگر مسیریاب‌های دیگری را درگیر می‌کند). به همین شکل می‌توانید از traceroute، tracert و rptrace به منظور مشاهدهٔ چگونگی حرکت بسته از یک ایستگاه‌کاری به محلی دیگر از میان شبکه، استفاده کنید. از فرمان netstat -r برای بررسی سرویس‌دهنده‌های

چندخانه‌ای و جدول مسیریابی آنها استفاده کنید تا ببینید آنها چه تصوری از مسیرها دارند. با انجام این‌کارها، می‌توانید نتایج را با آنچه باید طبق مستندات سایت رخ دهد، مقایسه نمایید و یک مرحله به تحلیل مشکل نزدیک‌تر شوید.

تئوری سوئیچ

هنگامی‌که پسربچه‌ای بیش نبودم، تا این حد سوئیچینگ پیچیده نبود. از پل برای اتصال شبکه‌هایمان استفاده می‌کردیم و از آن وضعیت راضی بودیم!

روزی روزگاری، سوئیچ‌های کوچکتر، پل اطلاق می‌شدند. کاری که آنها انجام می‌دادند، نظیر پل، اتصال دو شبکه به یکدیگر بود. امروزه سوئیچ‌ها دهها بخش شبکه‌ای را به یکدیگر متصل می‌کنند، اما قواعدی که از آنها تبعیت می‌شود، همان هستند که برای پیشینیان کوچکترشان ابداع شده بود.

امروزه، بسیاری از سوئیچ‌ها را جایگزین هابها نموده‌اند ـ رسانهٔ اشتراکی در صورت بروز خطاهای مکرر در آن آزاردهنده می‌شود (نظیر تصادم‌ها)، و ظرفیت کامل آن غیرقابل دسترسی خواهد بود. به همین خاطر، پروتکل‌های شبکه‌ای مورد استفاده در آنها از پروتکل‌های مورد استفاده در مسیریاب‌ها متفاوت است.

سوئیچ از طریق یادگیری آدرس‌های MAC تمامی ایستگاههای متصل به آن کار می‌کند. اگر یک آدرس MAC در یکی از بخشها بخواهد با آدرس MAC دیگری صحبت کند، سوئیچ از طریق یک مدار شخصی آنها را به یکدیگر متصل می‌کند، بسیار شبیه اپراتور تختهٔ سوئیچی که امکان مکالمهٔ افراد را از طریق اتصال سیمهای تلفن میسر می‌ساخت. البته، بر خلاف این اپراتور، سوئیچ‌ها علاقهٔ چندانی به محتویات مکالمات ندارند؛ این ابزار به سادگی افرادی را که می‌خواهند با یکدیگر صحبت کنند به یکدیگر متصل می‌کند و مکالمات دیگر را از آن دور نگه می‌دارد. این مجزاسازی از سایر مکالمات، یکی از دلایلی است که از سوئیچینگ برای سریعترکردن شبکه‌ها استفاده می‌گردد.

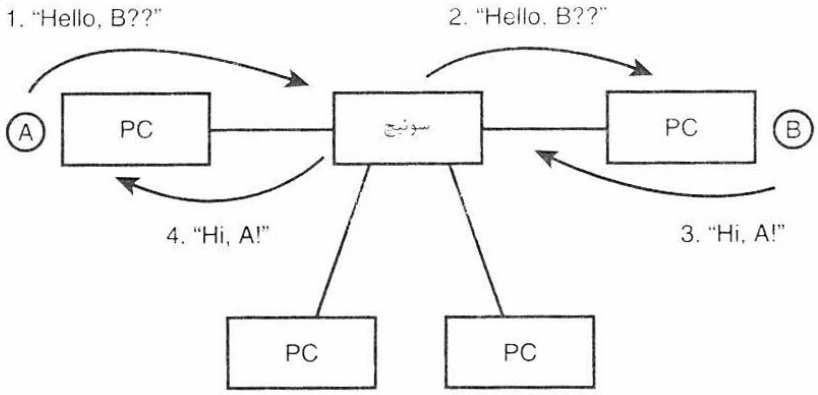


نکته : *آیا تاکنون با مشکلات عجیب و غریب در شبکه‌های سوئیچی‌شدهٔ بزرگ خود برخورد کرده‌اید؟ تعداد آدرس‌های MAC همزمانی که سوئیچ‌هایتان پشتیبانی می‌کنند را بررسی کنید ـ سوئیچ‌های قدیمی‌تر تعداد زیادی را پشتیبانی نمی‌کنند و نمی‌توانند در مقابل تعداد زیاد ایستگاهها تاب بیاورند، که این حالت ممکن است به قفل‌شدن PCها و قطع ارتباطها منجر شود.*

آیا لازم است که هر ایستگاه بداند که یک سوئیچ در مجموعه قرار گرفته است؟ خیر. این به آن خاطر است که سوئیچ هنگامی‌که یکی از ایستگاهها دیگری را فراخوانی کند پاسخ می‌دهد. به عبارت دیگر، فرض کنید ایستگاه A در شکل ۴-۱۴ می‌خواهد با ایستگاه B که در سمت دیگر سوئیچ قرار دارد صحبت کند. ایستگاه B هرگز سوئیچ را نمی‌بیند؛ به‌جای آن، قاب دست نخورده ارسالی از ایستگاه A را می‌بیند که سوئیچ از یک بخش به بخش دیگر منتقل نموده است. قاب دارای منبع A و مقصد B است؛ آدرس‌های MAC مربوط به سوئیچ هیچگاه داخل ماجرا نمی‌شود.



نکته : *همیشه به خاطر داشته باشید که روی هر پورت سوئیچ یک بخش شبکه وجود دارد (خواه نشان داده شده باشد یا اینطور نباشد). به عبارت دیگر، هنگامی‌که نموداری را مشاهده می‌کنید که پیوندی نقطه‌به‌نقطه‌بین یک PC و یک سوئیچ، و یا بین یک سرویس‌دهنده و سوئیچ نشان داده شده، احتمالاً منظور یک بخش از شبکه بین گره و سوئیچ است و این ارتباط تنها با یک PC نشان داده شده است.*



شکل ۴-۱۴ : چگونگی ارتباط دو ایستگاه از طریق سوئیچ.

توقف و سوئیچ

دو نوع روش سوئیچینگ وجود دارد:

- **میانبر** : همانگونه که از نام آن پیداست در این روش، انتقال بسته با دریافت آن شروع می‌شود و بسیار سریع است. البته اگر بسته خراب باشد، و خطایی در انتهای آن وجود داشته باشد، سوئیچ در واقع خطایی را منتقل نموده است.

- **ثبت و ارسال** : با سوئیچینگ ثبت و ارسال، سوئیچ تمامی بسته را دریافت می‌کند و آنگاه آن را به بخش مقصد ارسال می‌نماید. در صورت بروز خطا در این حالت، این امکان وجود دارد که سوئیچ بتواند به‌جای انتشار خطا، از بسته چشم‌پوشی کند. البته از آنجا که سوئیچ تا دریافت تمامی بسته صبر می‌کند، وقفه‌ای ایجاد می‌شود.

تقابل میان دو روش فوق، رویارویی سرعت در مقابل قابلیت اطمینان است؛ اگر مشکلاتی را با شبکهٔ سوئیچی‌شدهٔ خود دارید، بهتر است این موضوع را مد نظر داشته باشید. بهای سرعت برخی اوقات بیشتر از مقداری است که مایلید برای آن بپردازید.

اخبار انتشاری

اگر تعداد زیادی از برنامه‌ها، سرویس‌دهنده‌ها یا سرویس‌دهنده‌های چاپ دارید که بر اساس و پایهٔ انتشارهایی در سطح پیوند داده (یعنی ترافیک پیوند داده‌ای که به تمامی ایستگاههای شبکه منتقل می‌شود) کار می‌کنند، به خاطر داشته باشید که انتشار در تمامی بخشها سرایت می‌کند. اگر بخشهای سوئیچی‌شده را به هم متصل کرده باشید، انتشار از یک بخش به تمامی بخشها نشت می‌کند. این موضوع باعث به وجود آمدن ترافیک بسیار زیادی شده و می‌تواند مشکلات ناخواسته‌ای را ایجاد کند.



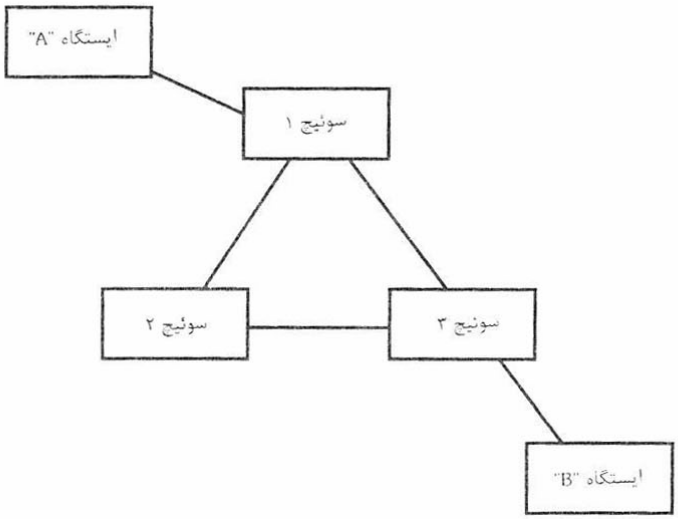
یادداشت : *خوب است در مورد استفاده از سوئیچ یا مسیریاب اندکی فکر کنید. دو شبکه با آدرس‌های پروتکلی متفاوت در انتشارهای سطح پیوند داده مشترک* نخواهند بود.

سوئیچ به‌صورت کاملاً گنگی عمل می‌کند. این ابزار چیزی در مورد مکالمهٔ تلفنی نمی‌داند ـ آنچه که می‌داند تنها آن است که چه کسی در حال صحبت‌کردن است. آیا سوئیچ می‌تواند طوری پیکربندی شود که دو بخش مجزا را بر پایهٔ پروتکل‌ها تقسیم نماید؟ البته، اما آنگاه سوئیچ به‌صورت مسیریاب عمل خواهد نمود.

درخت‌های نجات‌بخش

یک جنبهٔ مهم از عمل سوئیچ آن چیزی است که هنگامی‌که سوئیچ‌ها به یکدیگر متصل می‌شوند، رخ می‌دهد. از آنجا که هیچ پروتکل مسیریابی هنگامی‌که سوئیچ مثل سوئیچ عمل می‌کند، وجود ندارد؛ چه اتفاقی می‌افتد اگر سوئیچ 1 به سوئیچ 2 و سوئیچ 3 هم به سوئیچ 2 و هم به سوئیچ 1 متصل شده باشد؟ به نظر می‌رسد چیز شومی در حال رخ‌دادن است؟

خوب، حق با شماست. اتفاق شومی در شرف وقوع است. همانگونه که از شکل ۵-۱۴ مشهود است، دو مسیر از ایستگاه A به ایستگاه B وجود دارد. از آنجا که سوئیچ A هاب را از ایستگاه A به شبکهٔ بعدی می‌فرستد، چنین به نظر می‌رسد که سوئیچ 2 و سوئیچ 3 مکالمهٔ ارسالی از A را برداشته و تلاش می‌کنند آن را به B بفرستند. اگر چنین شکلی بدون انجام بازرسیها ادامه یابد، به زودی مشکلی بروز می‌کند: انتقال بسته‌ها آنقدر ادامه می‌یابد تا حدی که بار شبکه بالا رفته و ارتباطها شکننده شده و ممکن است از بین بروند.



شکل ۵-۱۴ : بدون بسط دادن پروتکل درختی، پلها باعث بروز حلقه‌ای می‌شوند که می‌توانند به بد کارکردن شبکه منجر شوند.

از این موقعیت می‌توان توسط یک پروتکل پل به نام درخت توسعه اجتناب نمود. با این پروتکل، یک بستهٔ مخصوص توسط هر پل یا سوئیچ در شبکه ارسال می‌شود؛ هر سوئیچ در مورد بقیهٔ سوئیچ‌ها اطلاعاتی را فرا می‌گیرد و این‌گونه کارهای بیهوده قبل از آغاز آنها با بلوکه‌شدن یکی از رابطها، نظیر آنکه بین سوئیچ‌های 1 و 3 قرار دارد، منتفی خواهد شد. در صورت تغییر شبکه در اثر خارج از سرویس‌شدن یکی از سوئیچ‌ها، یا از دست‌رفتن حافظهٔ یکی از آنها، تلاش می‌شود که درخت توسعه به‌صورت خودکار تنظیم شود. تمامی سوئیچ‌هایی که امروزه خریداری می‌کنید، امکان این‌کار را در اختیارتان می‌گذارند (یا آن را به‌صورت خودکار به انجام می‌رسانند) اما برخی از سوئیچ‌های قدیمی این‌کار را به انجام نمی‌رسانند و این ممکن است مشکلاتی را تولید کنند. در این حالت، دو گزینه پیش رو داریم: یا این‌که سوئیچ‌ها را به شکل حلقه به یکدیگر متصل نکنید و یا استفاده از ابزار قدیمی را رها نمایید.

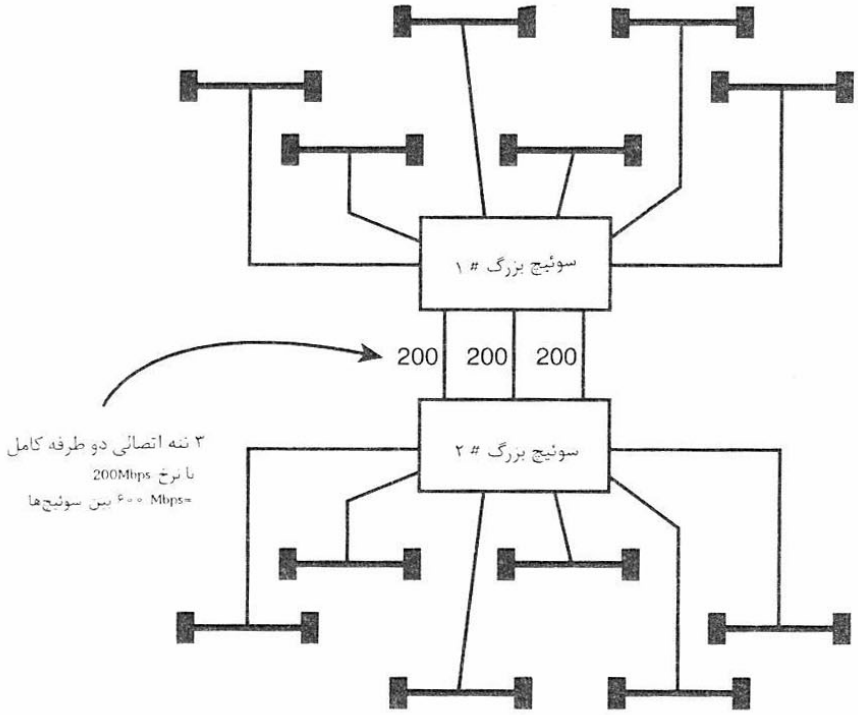
تنهٔ درختان

همانگونه که در فصل ۹، «مبانی اِترنِت» ذکر کرده‌ام، امکان ارتباط دوطرفهٔ کامل بین سوئیچ و گره‌ای نظیر سرویس‌دهنده

امری میسر است. این موضوع هم برای سوئیچ‌های اِترنِت و هم برای سوئیچ‌های حلقه‌نشانه صدق می‌کند. در این حال عرض باند مؤثر دوبرابر می‌شود: 32Mbps برای حلقه‌نشانه و 200Mbps برای اِترنِت سریع.

ارتباط دوطرفه کامل برای اتصال سرویس‌دهنده‌ها و یا کاربران پرکار به سوئیچ‌ها بسیار کارآمد به نظر می‌رسد، اما ارتباطات سوئیچ ـ به ـ سوئیچ ممکن است به عرض باند بیشتر از این هم نیاز داشته باشند. دلیل این مطلب آن است که سوئیچ مسؤول است که به کاربران بسیار بیشتر از یک کاربر پاسخ دهد. مطابق این موضوع، توانایی استفاده از خطوط چندگانه برای ارتباط بین دو سوئیچ در نظر گرفته شده است. به این کار تنومندسازی[1] گفته می‌شود. این عمل عرض باندی بسیار بیشتر از آنچه که ممکن است برای اتصال بین دو سوئیچ مورد نیاز باشد، ایجاد می‌کند. می‌توانید تصور کنید که خیابانهای کوچکی به هم پیوسته اتوبانی را پدید می‌آورند.

از آنجا که سوئیچ‌های نشان داده شده در شکل ۶-۱۴ دارای شش بخش 100Mbps می‌باشند، توان عملیاتی متمرکز[2] (یا مقدار ترکیبی آنچه که بین سوئیچ‌ها جریان می‌یابد می‌تواند 600Mbps باشد. برای حصول اطمینان از این‌که نقطهٔ مسدودی بین دو سوئیچ وجود نداشته باشد، ممکن است سه تنهٔ دوطرفهٔ کامل را بین سوئیچ‌ها متصل کنید تا به بزرگراه 600Mbps لازم بین سوئیچ‌ها دست یابید.



شکل ۶-۱۴ : در صورت نیاز به اتصال سوئیچ‌هایی با ظرفیت بالا می‌توانید از اتصال دوطرفه کامل و تنومندسازی بهره بگیرید.

از آنجا که تنومندسازی جدیداً وارد صحنه شده است ـ و اتصال دو طرفهٔ کامل نیز دندانی قدیمی به حساب نمی‌آید ـ بهتر است قبل از استفاده از این امکانات در کنار یکدیگر، موضوعات سازگاری را مورد بررسی قرار دهید.

1- Trunking 2- aggregate throughput

خلاصه

می‌توانید تصور کنید مسیریاب‌ها و سوئیچ‌ها پسرعمو هستند. مسیریاب‌ها بسته‌ها را در سطح پروتکل شبکه (TCP/IP یا IPX/SPX) سوئیچ می‌کنند، در حالی که سوئیچ‌ها بسته‌ها را در سطح پیوند داده (اِترنِت یا حلقه‌نشانه) مسیریابی می‌نماید. سوئیچ‌ها اغلب ابزاری سریع هستند، اما مسیریاب‌ها می‌توانند با تأخیر کار کنند (نظیر یک اتصال از نوع ناحیهٔ گسترده). اغلب از سوئیچ‌ها برای اتصال نواحی جغرافیایی مجزا استفاده می‌شود؛ این در حالی است که از مسیریاب‌ها برای اتصال نواحی جغرافیایی پراکنده استفاده می‌گردد. می‌تواند سوئیچ به‌عنوان جایگزینی برای هاب استفاده کرد تا کاربران بتوانند از خط غیر اشتراکی برای ارتباط با سایر ابزار شبکه لذت ببرند.

به مستنداتی که همراه سوئیچ یا مسیریاب ارائه می‌شوند، باید بسیار اهمیت داده شوند. این‌کار در حل مشکلات بسیار مؤثر خواهد بود. با این‌که دانستن تئوری‌ها بسیار مهم است، اما تئوری عملکرد مسیریاب‌ها و سوئیچ‌ها سود مستقیم زیادی به همراه نخواهد داشت؛ لازم است اطلاعات ویژه و دستورات پیکربندی ابزار خود را بشناسید.

مسیریاب‌ها بسیار پیچیده‌تر از سوئیچ‌ها هستند و از طریق پروتکل‌های مسیریابی کار خود را انجام می‌دهند. از سوی دیگر سوئیچ‌ها، بسیار گنگ عمل می‌کنند و تنها می‌توانند با یکدیگر به منظور اجتناب از مسیری تکراری به یک ایستگاه‌کاری صحبت کنند. هم سوئیچ‌ها و هم مسیریاب‌ها اغلب ابزاری هیبرید هستند که می‌توانند بسته‌ها را در سطح پروتکلی مسیریابی نموده و یا در سطح پیوند داده سوئیچ کنند، تمام عملکرد آنها بستگی به این دارد که چگونه آنان را پیکربندی نماییم.

کارگاه

پرسش و پاسخ

پرسش : رئیسم معتقد است که ما باید تمامی ابزار سوئیچینگ و مسیریابی خود را رها کرده و سوئیچ‌های سطح سه تهیه نماییم. منظور وی چیست؟

پاسخ : اجازه دهید ابتدا سوئیچ سطح سه را تعریف کنیم. برای انجام این‌کار، باید مدل هفت‌لایه‌ای OSI که قبلاً در مورد آن صحبت نمودم را مرور نماییم. لایه‌های OSI به ترتیب زیرند.

- فیزکی
- پیوند داده
- شبکه
- حمل
- جلسه
- نمایش
- کاربرد

بدون آنکه بخواهیم توضیح زیادی داده باشیم، سوئیچینگ لایهٔ سه به لایهٔ شبکه اشاره دارد، یعنی پروتکل شبکه (برای مثال TCP/IP یا IPX/SPX). و منظور از وسیله‌ای که بتواند اطلاعات این لایه را دریافت کند و تصمیم گیرد که با آن

چه‌کار نماید چیست؟ بله، مسیریاب. سوئیچ لایهٔ سه واژهٔ بازاری جدیدی است برای مسیریاب فوق‌العاده سریع. بنابراین پاسخ سؤال شما چنین است: آیا به مسیریاب جدیدی نیاز دارید؟

پرسش: من تلاش نمودم که به مسیریاب/سوئیچ خود، از طریق کابل سریال متصل شوم. کاملاً مطمئنم که کابل مودمی پوچ استفاده نموده‌ام، اما هر زمان که از برنامهٔ ارتباطی خود استفاده می‌کنم یک دسته کاراکتر نامفهوم ظاهر می‌شود. چرا؟

پاسخ: نگران نشوید هر زمان کاراکترهای نامفهومی نظیر آنچه که مشاهده می‌کنید در یک ارتباط سریال مشاهده نمودید احتمال بدان معناست که از پارامترهای ارتباطی نادرستی استفاده کرده‌اید. اگر مطابق با مستندات خود از پارامترهای پیش‌گزیده و صحیح بهره می‌برید، ممکن است سرعت اتصال را شخص دیگری تغییر داده باشد و شما از آن آگاه نباشید. سرعت‌های ۱۹۲۰۰ bps، ۳۸۴۰۰ bps و یا ۵۷۶۰۰ bps را امتحان کنید. اگر کار نکرد سعی کنید بیتهای توقف و یا قیاسی را تغییر دهید ـ اما بدانید که اغلب این مقادیر تغییر داده نمی‌شوند و بیشتر اوقات مشکل به وجود آمده مربوط به سرعت نامتناسب می‌باشد.

آزمون

۱- تفاوت اصلی بین مسیریاب و سوئیچ چیست؟

الف ـ کار با پیوند داده به‌جای پروتکل شبکه
ب ـ کار با برنامهٔ شبکه به‌جای پروتکل
ج ـ کار با لایهٔ MAC به‌جای پیوند داده
د ـ کار با شبکهٔ داده‌ای به‌جای پروتکل

۲- درست یا نادرست؟ اتصال سوئیچ از طریق پیوند ناحیهٔ گسترده کار خوبی است.

۳- درست یا نادرست؟ اغلب می‌توانید به منظور تهیه کپی پشتیبان از اطلاعات مسیریاب، یک نوارگردان را به آن متصل کنید.

۴- جدول مسیریابی را به کدام‌یک از روشهای زیر می‌توان ایجاد نمود؟

الف ـ مسیرهای ایستا
ب ـ مسیرهای پویا
ج ـ هیچ‌یک از موارد بالا
د ـ هم الف و هم ب

۵- پروتکل مسیریابی روشی است که مسیریاب‌ها برای کدامیک از موارد زیر استفاده می‌کنند؟

الف ـ کار با عرض باندهای مختلف روی شبکه
ب ـ تبادل شبکه‌ها و مسیرهای شناخته‌شده
ج ـ فرض اطلاعات مسیریابی به‌صورت داخلی
د ـ تبادل اطلاعات خطا در شبکه

۶- مسیریاب ۸۸ دارای جدولی مسیریابی نظیر این می‌باشد:

شبکه	ماسک شبکه	آدرس دروازه	هزینه
200.1.1.0	255.255.255.0	200.1.1.1	(محلی)0
200.1.2.0	255.255.255.0	200.1.2.1	(محلی)0
200.1.3.0	255.255.255.0	200.1.2.2	1
200.1.4.0	255.255.255.0	200.1.2.2	2

برپایهٔ این جدول مسیریابی مسیریاب ۸۸ چگونه بسته‌ای را به مقصد 200.1.3.10 ارسال می‌کند؟

الف ـ مستقیماً با گرهٔ 200.3.1.10 صحبت می‌کند.
ب ـ مستقیماً با مسیریاب 200.1.2.2 صحبت می‌کند.
ج ـ مستقیماً با مسیریاب 200.1.1.2 صحبت می‌کند.
د ـ بسته را دور انداخته پیغام خطایی صادر می‌کند.

۷- چگونه ممکن است مسیریاب ۸۸، بسته‌هایی را که به هیچ‌یک از ورودیهای مسیریابی خود شباهت ندارند به مسیریاب ۹۹ ارسال نماید؟

الف ـ مسیریاب ۹۹ را به اطلاعات اشتراکی پروتکل مسیریابی مربوط به مسیریاب ۸۸ اضافه نماییم.
ب ـ مسیر یاب ۹۹ را به عنوان مسیر پیش‌گزیده برای مسیریاب ۸۸ انتخاب کنیم.
ج ـ مسیریاب ۸۸ را به مجموعهٔ اشتراکی پروتکل مسیریابی مربوط به مسیریاب ۹۹ اضافه کنیم.
د ـ مسیریاب ۸۸ را به‌عنوان مسیر پیش‌گزیده برای مسیریاب ۹۹ انتخاب کنیم.

۸- درست یا نادرست؟ هر پروتکل شبکه پروتکل‌های مسیریابی مخصوص به خود را داراست.

۹- درست یا نادرست؟ هر ایستگاه کاری باید در پیکربندی شبکه‌ای خود آدرس MAC سوئیچ پیش‌گزیده‌اش را داشته باشد.

۱۰- با استفاده از روش سوئیچینگ ثبت و ارسال به‌جای روش میانبر می‌توان کدامیک از اقلام زیر را کاهش داد؟

الف ـ سرعت لازم برای ارسال یک بسته
ب ـ نفوذ خطا به بخشهای دیگر
ج ـ سرعت لازم برای قالب‌بندی بسته
د ـ خطاهایی که در پروتکل اطلاعاتی مسیریابی رخ می‌دهد.

پاسخ به سؤالات آزمون

۱- الف
۲- نادرست
۳- نادرست
۴- د
۵- ب
۶- ب
۷- ب
۸- درست
۹- نادرست
۱۰- ب

فصل ۱۵

مبانی دیوار آتش و سرویس‌دهندهٔ پروکسی

سه نفر در صورتی می‌توانند رازی را نگه دارند که دو نفرشان فوت کنند.
- بنیامین فرانکلین

در این فصل با ماجراهای زیادی روبرو خواهیم شد. قرار است مانند جیمز باند اسلحه برداشته با ابزارآلات عجیب و غریب، انفجارها و آدم‌های خوب و بد سروکار داشته باشیم. (نه، واقعاً نه؛ این یک کتاب آموزندهٔ خانوادگی است!)
بنا به دلایلی، چنین به نظر می‌رسد که احساس عمومی بر آن است که سرویس‌دهندهٔ پروکسی یا دیوار آتش اصلی‌ترین موضوع امنیتی در هر شبکه‌ای می‌باشد. البته در دنیای واقعی، با وجود آنکه سرویس‌دهندهٔ پروکسی یا دیوار آتش خوب پیکربندی‌شده از اهمیت بسیار زیادی برخوردار است، اما در مدل امنیتی بزرگتر تنها یک جزء محسوب می‌گردد. با این‌که قصد ندارم در این‌جا با جزییات زیاد شما را مواجه کنم، اما گفتنی است که امنیت در شبکه به سیاست‌های رمزگذاری خوب، پیکربندی سرویس‌دهنده، کاربرد مناسب از امکانات امنیتی سیستم عامل و اصلاحیه‌های برنامه‌های کاربردی، بازبینی شبکه و سیاستهای ورود کاربر به سیستم (تنها اسمی از چند مورد در کنار دیوارهای آتش) بستگی دارد. درست همانطور که هر شرکتی روی درهایش قفل نصب می‌نماید (دیوارهای آتش) همچنین می‌توان برچسب‌های شناسایی کمکی و نظایر آن برای کنترل‌های بیشتر استفاده نمود. تمامی شرکتها هم نگهبانان امنیتی ندارند - به‌خصوص نگهبانان امنیتی مسلح - اما درها را با قفل می‌بندند که خود تا حدودی امنیت اولیه را ایجاد نمایند.



یادداشت : *تئوری شخصی من در مورد امنیت شبکه این است: بهترین سیستم امنیتی در شبکه، قطع هاب، جداکردن تمامی پورت‌های تلفنی، سوزاندن مسیریاب اینترنت، منفک‌ساختن گردونه دیسک سخت سیستم و استفاده از کاغذ می‌باشد (بنا به دلایلی، این سیاست امنیتی محبوبی نیست!).*
با شکست این سیاست، تمام کاری که می‌توانید انجام دهید، آن است که بیشترین تمهیدات امنیتی را به‌کار ببندید و کپی‌های پشتیبانی خوبی تهیه نمایید. ایجاد دیوارهای آتش، شروع خوبی محسوب می‌شوند. آنها بیشتر نقاط ورودی به سیستم را مسدود می‌کنند و مانند دروازه‌ای از درون شبکه‌تان به دنیای خارج عمل می‌نمایند.

رموز فوق سری

اجازه دهید تعاریفی را در اینجا ارائه نماییم. هنگامی که بیشتر افراد از دیوارهای آتش سختی می‌رانند، اغلب منظورشان مسیریاب فیلترکننده بسته (Packet-filtering router) است. همان گونه که در فصل قبل مورد بررسی قرار دادیم، مسیریاب

چسب بین دو یا بیشتر بخش شبکه‌ای می‌باشد. بنابراین، منظور از مسیریاب فیلترکننده بسته، مسیریابی است که قوانینی دارد دال بر آنکه چه کسی و چه چیزی مجاز است بین رابط‌های آن مسیر کند.

سرویس‌دهنده پروکسی چیست؟ اول از همه، باید گفت که این مفهوم، به هیچ وجه مسیریاب نیست. پس سرویس‌دهنده پروکسی چیست؟ مانند هر سرویس‌دهنده‌ای، سرویس‌دهنده پروکسی، سرویس‌هایی را در اختیار می‌گذارد و در حقیقت سرویس‌دهنده چند خانه‌ای است که در خواست‌هایی را از یک سوکت دریافت می‌کند و آنها را به سرویس‌دهنده دیگری در سوی دیگر روانه می‌کند.

می‌توانید این گونه تصور کنید که سرویس‌دهنده پروکسی، نگهبان امنیتی بزرگ و بدی است که برایتان به همسایگی شبکه‌ای بد می‌رود، آنچه را که می‌خواهید استخراج می‌کند و آن را برای شما باز می‌آورد ـ تمامی این کارها بدون دخالت شما صورت می‌پذیرد. مثل حالت رای‌گیری، سرویس‌دهنده پروکسی، نماینده شما می‌شود ـ یعنی، مثل وکیلتان برای صورت‌پذیرفتن کاری عمل می‌کند و آنگاه نتایج حاصل را به شما گزارش می‌دهد. اگر بخواهیم از دوست قدیمیمان، قیاس تلفنی کمک بگیریم، به خاطر داشته باشید که سرویس‌دهنده پروکسی، «تجهیزات تلفنی» نیست؛ تنها نماینده‌ای است که دو تلفن مختلف متصل به دو سیستم تلفنی متفاوت دارد.

ساختار این سرویس‌دهنده، با جنس تشکیل‌کننده جاسوسان داستانی متفاوت است. از آن گذشته، اغلب اوقات شما خود سرویس‌دهنده پروکسی یا دیوار آتش فیلترکننده بسته‌تان را پیکربندی نمی‌کنید. این کار، ایده خوبی است؛ دیوار آتشی که به شکل نامناسبی پیکربندی شده باشد، تقریباً به بدی نداشتن آن است و برخی اوقات حتی بدتر از نداشتن است، چرا که احساس اشتباه امنیت را القا می‌کند.

در اینجا هم، ما پیکربندی دیوار آتش مدنظرمان نیست، اما نگاه به تئوری آن خواهیم داشت که به کمک آن می‌توانید موقعیت موجود را مورد بازرسی قرار داده و آنچه را که ممکن اشتباه باشد، بیابید.

TCP در مقابل UDP

ایده اصلی نهفته در دیوارهای آتش، آن است که اتصالات را می‌توان بر مبنای سرویس پیشنهادی یا مورد جستجو، محدود نمود. از آنجا که هر سرویس TCP/IP، شماره سوکت منحصر به فردی دارد که بدان گوش فرامی‌دهد (از مقایسه تلفنی، به خاطر بیاورید که سوکت، شماره انشعابی است که مشخص سرویس‌دهنده برای شرکت پاسخگوست)، مشخصاً محدودکردن اتصالات به این سوکت‌ها برای مسیریاب یا سرویس‌دهنده پروکسی کار آسانی خواهد بود. از آنجا که محدودیت‌ها بر شماره سوکت‌ها اِعمال می‌شوند، خود سرویس نیز محدود می‌گردد. این بدان معناست که می‌توانید سرویس‌هایی که ممکن است به دیوار آتش وارد یا از آن خارج می‌شوند، انتخاب نمایید.



یادداشت : *در واقع، لازم نیست سرویس‌ها روی شماره سوکت پیش‌گزیده‌شان اجراشوند؛ همان‌طور که رئیس‌تان می‌تواند شماره تلفن جدیدی به‌شما بدهد، سرپرست شبکه نیز می‌تواند شماره سوکت یک سرویس را عوض کند. این حالت کمی نامعمول است، اما به هر حال برخی اوقات روی می‌دهد. برای مثال، برخی اوقات دانشجویان سرویس‌دهنده‌های وِب خود را روی سوکت‌های دیگری به اجرا درمی‌آورند، چرا که دانشگاه سوکت وِب پیش‌گزیده را برای سرویس‌دهنده رسمی وِب اشغال نموده است. نکته منفی این قضیه در مورد دیوار آتش آن است که اگر سرویس را در سوکتی غیراستاندارد اجرا کنید، افراد ممکن است قادر نباشید از دیوار آتش برای اتصال استفاده کنند.*

این کار در مورد سوکت‌های TCP (پروتکل کنترلی انتقال) آسان است. هر پیوند TCP، فراخوانی اتصال‌گر است ـ مثل یک مکالمه تلفنی واقعی، که در آن شخصی شماره دیگری را می‌گیرد و پیوندی دوطرفه شکل می‌گیرد.

از سوی دیگر، در مکالمه‌ای از نوع UDP (پروتکل داده‌گرام کاربر). مثل آن است که من کاغذ مچاله‌شده‌ای حاوی پیغام را برایتان پرت کنم و شما نیز پاسخ را این‌چنین بازگردانید. به این حالت، جلسه بدون اتصال گفته می‌شود. تفاوت بین TCP و UDP، مثل استفاده از دو قوطی حلبی و ریسمان برای صحبت (TCP) و استفاده از یادداشت‌های سر کلاس (UDP) می‌باشد. به خاطر داشته باشید که یادداشت‌ها ممکن است به سادگی تغییر جهت داده شوند.

محدودکردن اتصالات TCP آسان است، چرا که پاسخ به اتصال در خودش قرار دارد. انجام این کار، در مورد سوکت‌های UDP بسیار مشکل‌تر است. در اتصال UDP، بسته‌ای پرتاب می‌شود و منتظر پاسخ می‌ماند. از آنجا که اتصالی وجود ندارد، دیوار آتش باید برای پذیرش بسته‌های UDP نامنظم پیکربندی شود که هرکدام‌ها ممکن است حاوی پاسخ باشند.

برخی سرپرستان (بسته به سیاست‌های امنیتی سایت‌شان) UDP را از طریق دیوار آتش مجاز نمی‌دارند. بقیه به دیوارهای آتش SMIT (بازرسی حالات چندسطحی) اتکا می‌کنند، که بسته‌هایی که از آن گذر کرده‌اند «به خاطر می‌سپارند» و بنابر آن، پاسخ‌هایی را مورد پذیرش قرار می‌دهند.

مسیریاب‌های فیلترکننده بسته

هر مسیریاب فیلترکننده بسته، اغلب به قوانین دسترسی ـ یعنی قوانینی که در داخل نرم‌افزار مسیریاب تنظیم می‌شوند ـ بستگی دارد. هر فیلتر بسته‌ای، معمولاً مجموعه قوانینی دارد که از نامعمولترین شروع شده و تا معمولترین ادامه می‌یابد. مجموعه قوانین چیست؟ هر مجموعه قوانین، برخی اوقات شبیه به جدول مسیریابی است که علاوه بر آدرس‌ها، سوکت‌ها را نیز شامل می‌شود. هر بسته‌ای که وارد می‌شود، با کانون 1، آنگاه قاون 2 و به همین ترتیب الی آخر سنجیده می‌شود. اگر هر زمان با یکی از قوانین سنخیت داشت، فرآیند متوقف می‌شود. برای مثال برای شبکه 122.168.1.0، قوانین ممکن است به صورت زیر باشند:

- پذیرش 192.168.1.0:any اگر از 0 برای اتصال به all:any
- اجتناب all:any برای اتصال به all:any

این بدان معناست که هر کسی از طریق شبکه 192.168.1.6 (در صورت ورود از رابط 0 مسیریاب) می‌تواند به هر چیزی که می‌خواهد متصل شود. اگر شرط یک درست نباشد، آنگاه شرط دوم به‌کار بسته می‌شود که از هر گونه اتصالی اجتناب می‌کند. این شاید معمولترین شکل پیکربندی دیوار آتش باشد: پذیرش سوکت‌های خاص (یا تمامی سوکت‌ها) از داخل به خارج و عدم پذیرش تمامی اتصالات دیگر (برای مثال، اتصالاتی از خارج).



نکته : *بیشتر مسیریاب‌های فیلترکننده بسته کارآمد، علاوه بر آدرس IP بسته ورودی، کار فیلترسازی را روی «کدام رابط» نیز انجام می‌دهند. این کار از حقه‌بازی بسته جلوگیری می‌کند، که طی آن بسته ادعا می‌کند از شبکه خاصی آمده است، در حالی که این چنین نیست.*



هشدار : *مجموعه قوانین پیچیده، باعث اشتباه و پیکربندی نادرست می‌شود. در صورتی که قصد دارید مجموعه قوانینی را پیکربندی کنید، آن را ساده نگه‌دارید.*



نکته : *باید بدانید که برنامه‌های کاربردی خاص (نظیر FTP فعال) آدرس ایستگاه مقصد را برای ایجاد اتصال به ایستگاه درخواست‌کننده، مطالبه می‌کنند، حتی اگر برنامه‌ای کاربردی از نوع TCP باشند. این کار شبیه به درخواست «سلام، وقتی فیلم شروع شد، منو صدا کن» می‌باشد.*
از این کار در بسیاری از دیوارهای آتش اجتناب می‌شود، چراکه به معنای آن است که دیوار آتش باید طوری پیکربندی شود که یک ایستگاه‌کاری از خارج بتواند اتصالی را به ایستگاه‌کاری داخلی دلخواهی راه‌اندازی کند.
معمولاً این امکان وجود دارد که این مشکل را از طریق به‌کارگیری حالت متفاوتی از برنامه برای مثال، FTP غیرفعال، که در آن تنها ایستگاه‌کاری درخواست‌کننده اتصال را ایجاد می‌کند ـ حل نمایید. پیش‌گزیده بیشتر مرورگرها، FTP غیرفعال است، اما تمامی سرویس‌گیرنده FTP مستقل اینچنین نیستند.

با وجود ثبت خطاها، اغلب دیوارهای آتش فاقد امکان ثبت وقایع و حسابگری می‌باشند. در اینجا، عیب‌یابی بسیار نظیر عیب‌یابی مسیریاب با کمک ping، traceroute و **فهرست جداول مسیریابی و مجموعه قوانین** صورت می‌پذیرد. شرح حال مشکلات مواردی نظیر دیوار آتش فیلترکننده بسته، مثل مشکلات مسیریابی، مسیریاب، یک شرح حال برای مشکلات در اینجا ممکن عدم دسترسی به یک سرویس در آن سوی انضباط باشد.

تقویت فیلتر بسته

دیوارهای آتش جدیدتر، که توجهی به خوب‌بودن مسیریاب‌ها ندارند، تمامی ترفندهای جدید را به‌کار می‌بندند. برخی ترجمه‌های آدرس شبکه[1] (NAT) را انجام می‌دهند، که شما را قادر می‌سازد به دنیای خارج بگویید آدرس متفاوتی با آنچه که واقعاً هست، دارید. این بدان معناست که در صورت تغییردادن فراهم‌کننده سرویس اینترنت، نیازی نیست که شماره‌های IP خود را تغییر دهید (قبلاً فقط سرویس‌دهنده‌های پروکسی برای این کار مناسب بودند، چرا که آنان در هر حال از دو حوزه مسیریابی مختلف بهره می‌برند. اما امروزه فروشندگان دیوارهای آتش این موضوع را نیز پشتیبانی می‌کنند.

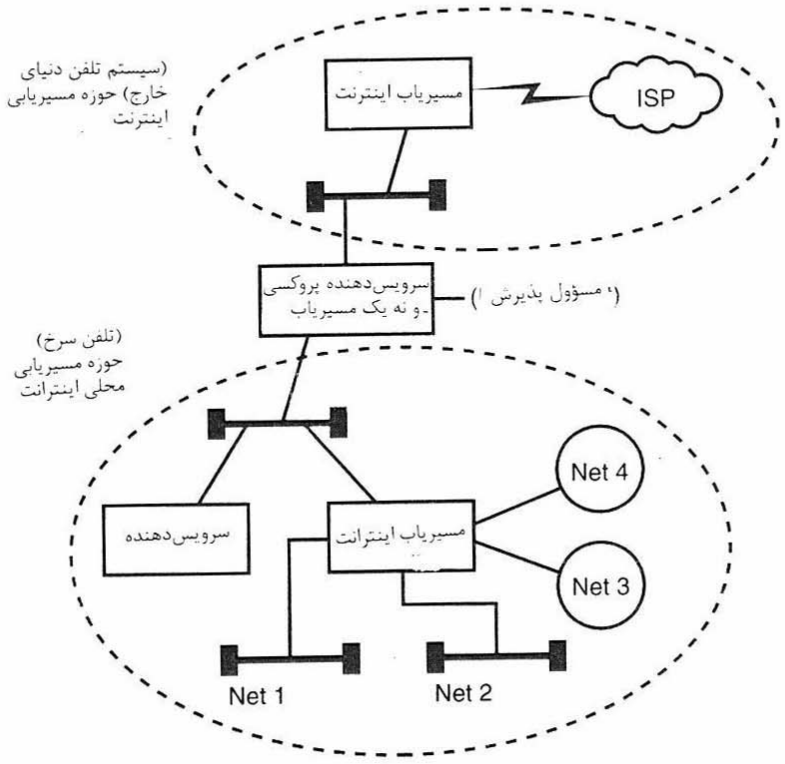
بازرسی وضعیت چندسطحی نیز، فن‌آوری بسیار غنی‌ای می‌باشد که این امکان را فراهم می‌آورد سوکت‌های UDP در مبنایی مفهومی وارد شوند ـ یعنی، یادداشت شما به دوستتان را خوانده و آنگاه فقط یادادشتی از وی را می‌پذیرد که به نظر می‌رسد با محتویات یادداشت شما در یک ارتباط باشند. این کار، به دیوار آتش بسیار ویژه‌ای نیاز و تا حدود زیادی به کاربرد بستگی دارد. اگر دیوار آتش دوستتان را «نشناسد»، نمیتواند تشخیص دهد که یادداشت ارسالی وی واقعی است یا خیر. چنین دیوارهای آتشی با قوانینی مخصوص برای برنامه‌های پرکاربرد نظیر Telnet، email، FTP و نظایر آنها، از قبل پیکربندی می‌شوند. اگر مشکلی در به‌کارگیری دیوار آتش SMLI در رابطه با برنامه کاربردی نامعمولی دارید، بهتر است با فروشنده آن تماس بگیرید تا ببینید چه کمکی می‌تواند ارائه کند.

اجازه دهید کمی عمیقتر تئوری سرویس‌دهنده پروکسی را بشکافیم. فرض کنید که سرویس‌دهنده پروکسی، مسؤول

1- Network Address Tanslations.

پذیرش یک سازمان جاسوسی است که دو مجموعه تلفنی دارد: تلفن داخلی سازمان («تلفن قرمز») و سیستم تلفنی دنیای خارج. سیستم اخیر به صورت مستقیم توسط هیچ یک از کارکنان سازمان قابل استفاده نیست؛ آنها باید پیغامی برای مسؤول پذیرش بفرستند و اوست که سفارشات خارجی را انجام می‌دهد. سازمان جاسوسی با انجام این کار روشی را پیش گرفته که در آن هیچ یک از مدارات داخلی‌اش با شبکه عمومی تلفن ارتباط مستقیم ندارد ـ که این چیز خوبی است! البته این بدان معناست که مسؤول پذیرش بدون اشتباه کار می‌کند، اما حداقل او در داخل سازمان است، قابل اطمینان بوده و حساب کارهایش را پس می‌دهد و البته، به سادگی قابل نظارت است، چرا که تنها نقطه ارتباطی بین سازمان و دنیای خارج محسوب می‌شود.

نکته مهم آن است که به خاطر داشته باشید که دو نوع مختلف مکالمه تلفنی وجود دارد، چرا که مسؤول پذیرش یک خط (خط قرمز) را متوقف و تلفن خارجی را برمی‌دارد تا طی مکالمه مجازایی، اطلاعات را رله کند. به این مشکل، دو حوزه مسیریابی ممختلف وجود دارد (دو سیستم تلفنی) که درگیر این کار می‌شوند. با اینکه کمی عجیب به نظر می‌رسد، اما آنچه که تمامی اینها معنی می‌دهند، آن است که دو مجموعه شبکه (سیستم تلفنی قرمز و عمومی) از صحبت‌کردن با یکدیگر منع شده‌اند، چرا که مسیریاب فقط شبکه مشترکی بین آن دو شبکه می‌باشد (شکل ۱-۱۵ را ملاحظه کنید).



شکل ۱-۱۵ : چگونگی به‌کارگیری سرویس‌دهنده پروکسی.

آیا قوانینی هستند که معین کنند که با چه کسی در داخل و خارج می‌توان تماس گرفت؟ البته. نظیر دیوار آتش فیلترسازی بسته، سرویس‌دهنده‌های پروکسی یک سیاست «اجتناب از هر چیز به غیر از آنچه که از پس می‌آید» دارند، و شما هستید که آنچه مجاز است را تعیین می‌کنید. برای مثال، فرض کنید، عاملان اجرایی شرکت همگی در شبکه ۴ در شکل ۱-۱۵ قرار داشته باشند. تنها آنان می‌توانند به اینترنت دسترسی داشته باشند و بنابراین قانون مجزای زیر را باید تعریف نمایید:

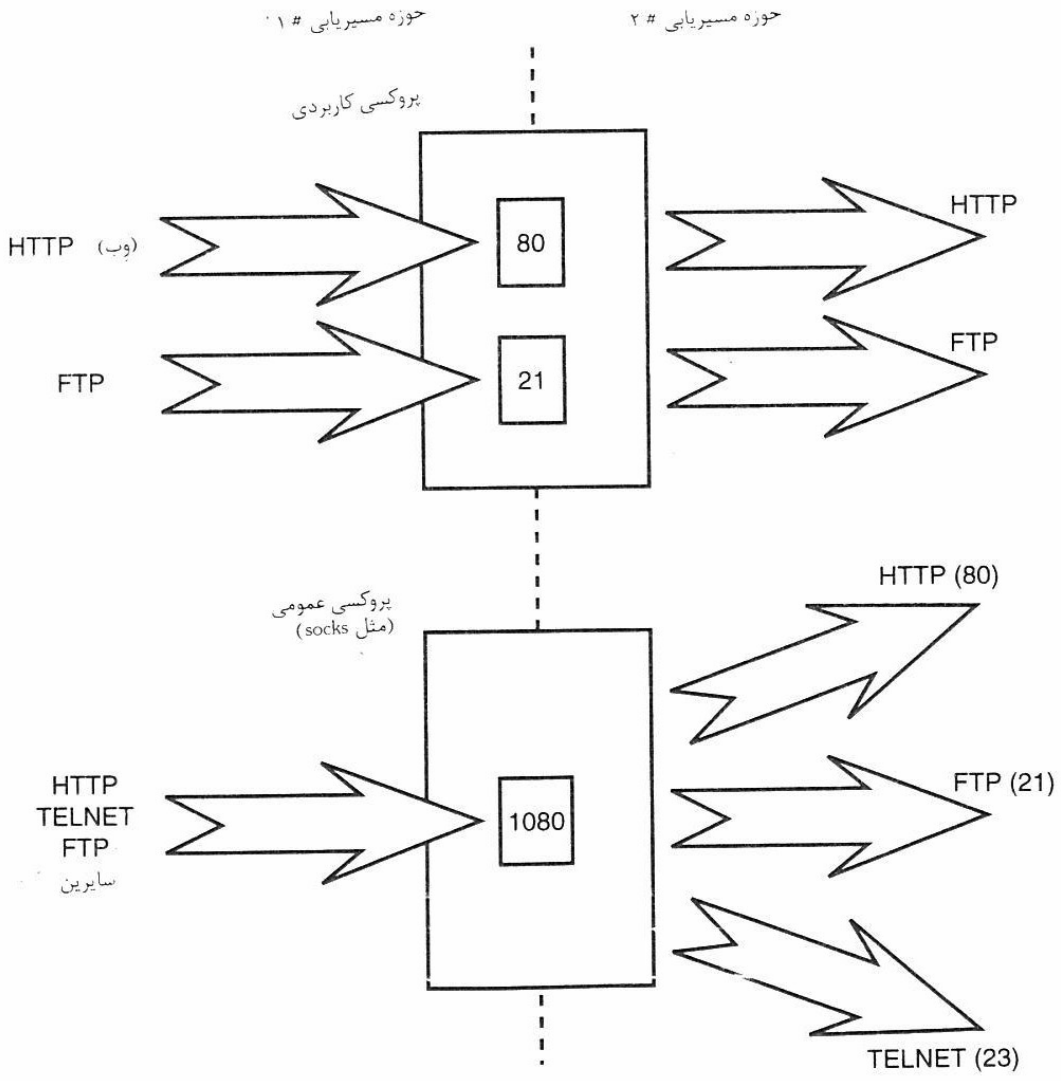
پذیرش تمامی ترافیک از شبکه ۴ از رابط «داخلی» سرویس‌دهنده پروکسی.
از بقیه ترافیک، مثلاً از شبکه ۴ جلوگیری می‌شود.

نوع پروکسی

دو نوع سرویس‌دهنده پروکسی وجود دارد:

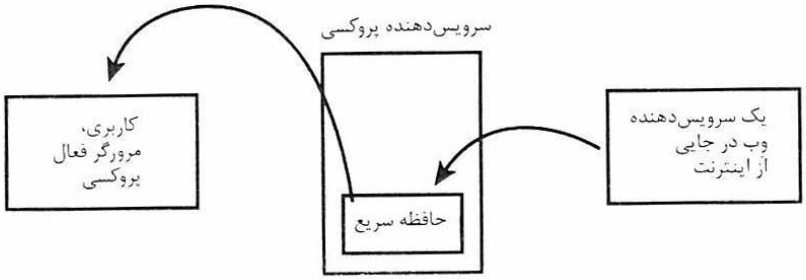
- **پروکسی کاربردی** : هر پروکسی کاربردی، پروکسی بسیار خاصی است که تنها نمایندگی یک نوع برنامه کاربردی، نظیر FTP، HTTP و نظایر آنها را برعهده می‌گیرد ـ یعنی پروکسی FTP، اتصال HTTP را قبول نمی‌کند. اگر می‌خواهید برنامه‌های کاربردی بیشتری از طریق سرویس‌دهنده پروکسی‌تان قابل دسترسی باشند، باید مطمئن شوید که سرویس‌دهنده پروکسی، سرویس‌های پروکسی آن برنامه‌های کاربردی را به خوبی اجرا نموده است.

- **پروکسی مداری** : پروکسی مداری، پروکسی‌ای است که تنها در سطح شبکه کار می‌کند. محبوبترین پروکسی مداری Socks نامیده می‌شود (که در ابتدا به صورت مجموعه‌ای رایگان تولید شد، اما امروزه به صورت تجاری از سوی تعدادی از فروشندگان عرضه می‌شود). این نوع از پروکسی، پروتکل و شماره سوکت را درک می‌کند. معمولاً، پروکسی‌های مداری، عمومی هستند ـ آنها می‌توانند برای کار با هر نوع سوکتی به‌کار روند ـ که در شکل ۲-۱۵ ملاحظه می‌کنید.



شکل ۲-۱۵ : پروکسی مداری، و پروکسی کاربردی.

تفاوت در کجاست؟ خوب، یک تفاوت، آن است که پروکسی مداری قابل انعطاف بیشتری دارد ـ تمامی سرویس‌های TCP/IP را پشتیبانی می‌کند. البته، پروکسی کاربردی نیز لیاقت‌ها و شایستگی‌های خاص خود را داراست. برای مثال، پروکسی وِب (که نام دیگر آن پروکسی HTTP می‌باشد) صفحات وِبی را که منتقل نموده است، در حافظه سریع خود ثبت می‌کند و در نتیجه بسیار سریع آنها را به کاربران عرضه می‌کند. این بدان خاطر است که پروکسی کاربردی، دانش عمیقی از آنچه به وقوع می‌پیوندد، داراست، در حالی که پروکسی مداری چیزی در مورد برنامه کاربردی نمی‌داند ـ آنچه می‌داند، تنها در مورد اتصال است. به عبارت دیگر، هر پروکسی HTTP «می‌داند» که صفحات وِبی از یک سرویس‌دهنده دریافت می‌کند، چیستند و آنها را به صورت محلی ذخیره می‌کند، همان گونه که در شکل ۳-۱۵ نشان داده شده است. دفعه بعدی که کاربر آن صفحات وِب را می‌خواهد، پروکسی آنها را از ناحیه حافظه سریع برمی‌دارد و بنابراین در زمان صرفه‌جویی می‌شود (نگران نباشید ـ در صورت پست صفحات جدید، حافظه سریع آنها را در اختیار می‌گذارد).



شکل ۳-۱۵ : سرویس‌دهنده پروکسی اطلاعات را تا هنگام به‌روزبودن آنها ذخیره می‌کند: کاربران می‌توانند بدو اضافه‌کردن ترافیک شبکه و یا معطل‌ماندن صفحات مورد نظر را تجدید و مشاهده نمایند.

تنها نرم‌افزار اضافه کنید

هر سرویس‌گیرنده پروکسی، نرم‌افزار سرویس‌گیرنده‌ای دارد که باید در ایستگاه‌کاری به‌کاربرنده پروکسی نصب گردد. این کار ممکن است ساده باشد ـ هر کپی از Internet Explorer و Netscape Navigator یا Communicator، امکان پشتیبانی از پروکسی مداری Socks را داراست و همچنین به صورت توکار، بیشتر سرویس‌دهنده‌های پروکسی پرطرفدار را پشتیبانی می‌کند (شکل ۴-۱۵، تنظیمات پروکسی را در Internet Explorer نشان می‌دهد).

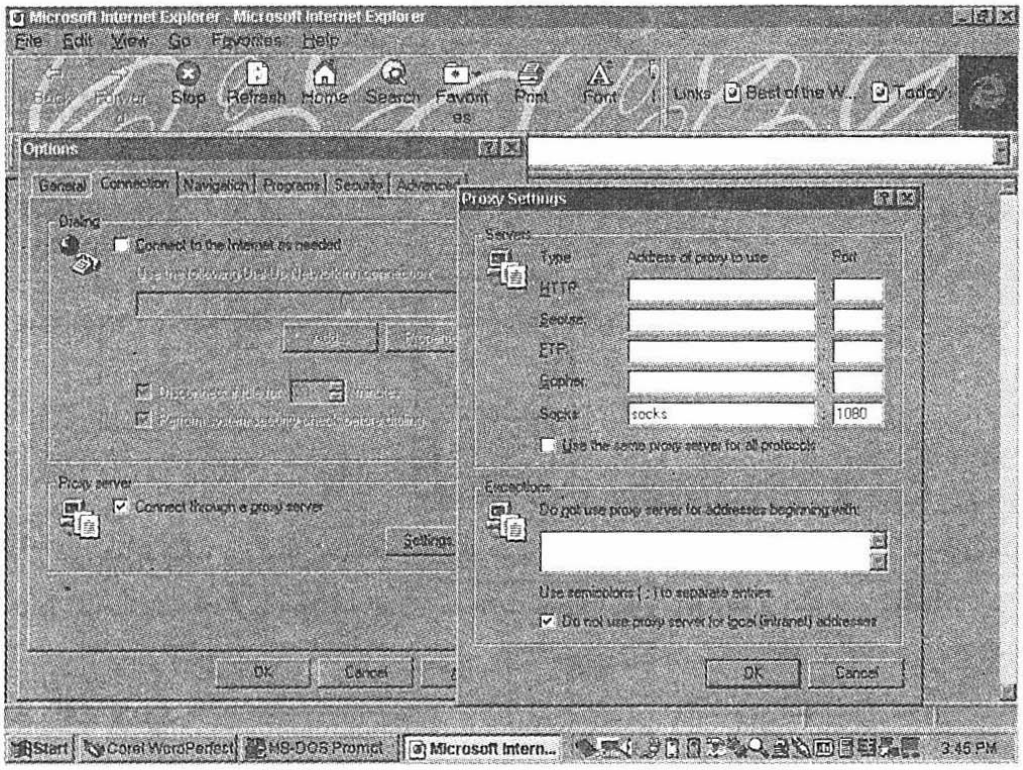
پیکربندی پروکسی

کار مهمی که در هنگام تنظیم نرم‌افزار سرویس‌گیرنده باید انجام دهید آن است که مطمئن شوید سرویس‌دهنده پروکسی برای ترافیک محلی مورد استفاده قرار نگرفته باشد. بیشتر سرویس‌دهنده‌های پروکسی می‌توانند کار خود را با مقدار گرافیکی که در خطی که در بیشتر سایت‌های متصل به اینترنت کار با ترافیک T یا 1/5Mpbs برای بیشتر سرویس‌دهنده‌ها آسان است ـ استفاده می‌شود، به خوبی به انجام برسانند. البته، اگر قرار باشد که سرویس‌دهنده پروکسی به درخواست‌های ترافیک ۱۰Mpbs یا ۱۰۰Mpbs محلی نیز پاسخ دهد، کارها.... رفته رفته.... آهسته و کند..... می‌شوند. به زودی با افراد خشمگینی روبه‌رو می‌شوید که می‌خواهند بدانند چرا دسترسی‌شان به اینترنت کُند شده است!

برای پیکربندی Internet Explorer به منظور اجتناب از درگیری سرویس‌دهنده پروکسی برا ترافیک محلی، دقت کنید که چک‌باکس (Do Not Use Proxy Server for Local (Interanet Address (به شکل ۴-۱۵ توجه کنید)، علامت خورده باشد. فرض میکروسافت بر آن است که هر آدرس در حوزه‌تان (http://server.mycompany.com) یا نام سرویس‌دهنده بدون حوزه (http://server) یک آدرس محلی است. پیکربندی Netscape کمی پیچیده‌تر است؛ اگر می‌خواهید این کار را انجام دهید،

باید سرویس‌دهنده پیکربندی Netscape را اجرا نمایید.

البته، حتی اگر نرم‌افزار را به درستی پیکربندی کنید، ممکن است کسی آن را بعداً «به هم بزند»؛ بهتر است این نوع رفتار غیراجتماعی (!) را در سرویس‌دهنده ممنوع کنید. البته، کسی که پیکربندی ایستگاه‌کاری خود را به هم می‌زند، کارکرد صحیحی را مشاهده نخواهد نمود، اما بهتر است یکی دو نفر مشکل داشته باشند تا اینکه مرتب صدای «اینترنت کُند است» به گوش برسد. در این موضوع به من اطمینان داشته باشید.



شکل ۴-۱۵ : صفحه *Proxy Settings* از *Internet Explorer*.



نکته : *در صورت ادامه یافتن وضعیت کُندی، اگر ترافیک زیادی از طریق سرویس‌دهنده پروکسی عمومی‌تان صورت می‌گیرد، ممکن است بهتر باشد به سراغ پروکسی‌های کاربردی خاص بروید. این حقیقت که پروکسی کاربردی، صفحات پرکاربرد را در حافظه سریع قرار می‌دهد، واقعاً می‌تواند حجم ترافیک را کاهش دهد و با افزایش سرعت در این صفحات، سرعت عمومی نیز بالاتر می‌رود، چرا که آن صفحات مرتباً بارگذاری نمی‌شوند.*

مشکل پروکسی

باید با سرویس‌دهنده پروکسی خود مثل سرویس‌دهنده‌ای رفتار کنید که به دو شبکه مختلف متصل شده است. به این صورت، معمولاً لازم خواهد بود که بتوانید هنگام عیب‌یابی، وارد آن سیستم شوید.



هشدار : *محتمل است که دیوار آتش شما نوعی ورود به سیستم امنیتی داشته باشد. به خاطر بسپارید که فرضیات شما باعث چه اتفاقی خواهد شد! مطمئن شوید که جلسه ورود به سیستم‌تان رمزگذاری شده باشد؛ اگر نمی‌دانید، از سازنده سؤال کنید. در صورت عدم رمزگذاری ورود به سیستم، چیزی از*

شرایط ورود به اینترنت را تغییر ندهید. در غیر این صورت، دیوار آتش امن شما دیگر امن نخواهد بود، چرا که اشخاص خارجی هم می‌توانند وارد سیستم شوند.

بعد از ورود به سیستم، می‌توانید با سرویس‌دهنده پروکسی مثل هر ایستگاه کاری معمولی کار کنید. البته، به خاطر داشته باشید که این دستگاه، ایستگاهی کاری معمولی است با دو «جان»: یک «جان» در شبکه شما و دیگری در اینترنت. روال‌های عادی عیب‌یابی را صورت می‌دهید: traceroute ، ping و غیره. از آن گذشته، می‌توانید کسانی که در حال حاضر از سرویس‌دهنده استفاده می‌کنند را با **netstat -a** یا **netstat -an** (بسته به آنکه بخواهد خروجی عددی داشته باشید) مشاهده نمایید.

به خطوط LISTENING توجه کنید؛ این خطوط نشان‌دهنده خود سرویس‌دهنده‌های پروکسی هستند. اگر یکی از آنها کنار برود احتمالاً برنامه پروکسی مرتبط با آن خاتمه یافته است. برای مثال، سرویس‌دهنده پروکسی Socks ، روی سوکت 1080 به گوش می‌ایستد. اگر چیزی شبیه به عبارات زیر را ملاحظه نمی‌کنید، باید بررسی کنید که آیا برنامه Socks در حال راست یا نه (از netstat -a استفاده کنید):

```
Active  Connections
Proto   Local Address          Foreign Address  State
TCP     proxy.myhost.com:1080  0.0.0:*          LISTENING
```

در این حالت، برنامه Socks در حال اجراست. اینکه درست عمل می‌کند، داستان دیگری است (برای مثال، ممکن است قانون دسترسی برای شبکه‌تان به صورت تصادفی حذف شده باشد: یا اینکه می‌توانید به سوکت متصل شوید، حق استفاده از پروکسی به شما داده نمی‌شود. این موضوع را می‌توانید تنها با استفاده از اجرای آن از شبکه‌تان بررسی نمایید). این ترفند را می‌توانید در صورت دانستن شماره سوکت پروکسی‌های دیگر، برای آنها نیز به‌کار برید. HTTP در سوکت 80 واقع شده، FTP در سوکت ۲۱ و گوفر در سوکت ۷۰ قرار دارند.

همان بازی نام : DNS و دیوارهای آتش

سرویس‌های نام چطور؟ آیا لازم نیست این سرویس‌دهنده‌ها را روی اینترنت با سرعت بیشتری به اجرا درآورید؟ این همه شمه‌ای در مورد DNS و دیوارهای آتش.

دیوارهای آتش فیلترکننده بسته را می‌توان طوری پیکربندی نمود که سرویس‌دهنده‌های NDS داخلی بتوانند جستجوهایی را از خارج انجام دهند. در این حالت، قواعد عیب‌یابی استاندارد در DNS به‌کار می‌آیند. شکل جستجوی DNS چیزی نظیر این است:

۱- ایستگاه‌کاری سرویس‌گیرنده، از سرویس‌دهنده NDS محلی می‌خواهد که ww.jotto-com را تحلیل کند.
۲- DNS موجود در سرویس‌دهنده محلی، نمی‌تواند jotto.com را پیدا کنید؛ به سرویس‌دهنده DNS خارجی رجوع می‌کند.
۳- سرویس‌دهنده DNS خارجی، آدرس IP را به ایستگاه‌کاری سرویس‌دهنده DNS محلی بازمی‌گرداند.
۴- سرویس‌دهنده DNS محلی، آدرس IP را به ایستگاه‌کاری سرویس‌گیرنده بازگشت می‌دهد.
۵- ایستگاه‌کاری سرویس‌گیرنده، تلاش می‌کند اتصال را برقرار کند؛ دیوار آتش فیلترکننده بسته اتصال را بررسی می‌کند و عبور آن را ممکن می‌سازد.

کارکردن سرویس‌های DNS را می‌توانید با اجرای ping وارسی نمایید. این امکان وجود دارد که اجرای خود ping با شکست مواجه شود ـ برخی از سرویس‌دهنده‌های اینترنت، اجازه نمی‌دهند که از خارج ping شوند و از طرف دیگر ممکن است دیوار آتش فیلترکننده بسته شما برای مجازدانستن انجام ping پیکربندی نشده باشد. البته، باید بتوانید آدرس را تحلیل کنید. برای مثال، در صورتی که DNS فعال باشد، ping ای به یک میزبان خارجی به این حالت شبیه خواهد بود:

```
C:\WINDOWS> ping www.jotto.com
Pinging www.jotto.com [205.134.224.21]with 32 bytes of data:
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
```

پیغام Destination host unreachable ممکن است قابل قبول نباشد، اما حداقل، می‌دانید که تحلیل نام کار می‌کند، چرا که آدرس IP [205.134.224.21] به دنبال www.jotto.com ظاهر شده است. اگر تحلیل نام کار نمی‌کرد. جلسه ping شبیه این بود:

```
C:\WINDOWS > ping www.jotto.com
Bad IP address www.jotto.com
```

در این مثال، آدرس IP از اسم DNS به دست نیامده است. پیغام Bad IP address www.jotto.com از ویندوز به معنای شکست در تحلیل نام است.

برخی از سرویس‌دهنده‌های پروکسی، این امکان را در اختیار می‌گذارند که سرویس‌دهنده‌های DNS خود را از DNS جهانی مجزا کنید. به این حالت *DNS* پروکسی گفته می‌شود و به صورت زیر کار می‌کند:

۱- نرم‌افزار سرویس‌گیرنده پروکسی تلاش می‌کند جستجویی محلی را به دنبال اسم (www.jotto.com) به انجام برساند.
۲- نرم‌افزار سرویس‌گیرنده پروکسی که در جستجوی محلی با شکست روبه‌رو می‌شود، فرض می‌کند که اسم مربوط به یک سایت راه دور است و از سرویس‌دهنده پروکسی می‌خواهد که اسم را تحلیل و وکالت درخواست را به عهده گیرد.
۳- سرویس‌دهنده پروکسی اسم را با کمک سرویس‌دهنده DNS خارجی تحلیل می‌کند.
۴- سرویس‌دهنده پروکسی درخواست را پردازش می‌کند و صفحه وِب نتیجه را به سرویس‌گیرنده تحویل می‌دهد.

توجه داشته باشید که آدرس IP به سرویس‌گیرنده بازگردانده نمی‌شود. این بدان معناست که نمی‌توانید ترفند ping را در صورت استفاده از DNS پروکسی سرویس‌گیرنده به جای ارتباط سرویس‌دهنده‌های DNS داخلی با DNS خارجی، به‌کار ببندید. همیشه پیغام Bad IP address host.outside company.com را دریافت می‌کنید.



یادداشت : ***برخی پروکسی‌ها، امکان DNS پروکسی را فراهم نمی‌آورد. برای مثال Socks نگارش 5، در صورت پیکربندی این کار را انجام می‌دهد، اما نگارش 4 این برنامه فاقد امکان مذکور است.***

خلاصه

به هر مسیریاب فیلترکننده بسته اغلب با عنوان دیوار آتش یاد می‌شود. این مسیریاب‌ها، قوانینی دارند که تعیین می‌کنند در مبنایی سرویس ـ به ـ سرویس چه چیزی در شبکه مجاز است و چه چیز مجاز نیست. دیوارهای آتش تخصصی شده‌تر و جدیدتر بازار، امکاناتی نظیر NAT، SMLI، ورود به سیستم و گزارشگرهای ویژه‌ای را ارائه می‌کنند که مسیریاب‌های عادی فاقد آنها هستند.

سرویس‌دهنده‌های پروکسی از جهت مسیریاب‌نبودن با دیوارهای آتش فیلترکننده بسته تفاوت دارند؛ آنها مثل یک

ایستگاه‌کاری در اینترنت کار می‌کنند و نتایج را به ایستگاههای کار درون شبکه‌تان بازمی‌گردانند. این حالت باعث می‌شود که در پایانه سرویس‌گیرنده به تنظیمات بیشتری نیاز داشته باشند و از مشخصات عیب‌یابی متفاوتی نسبت به مسیریاب ساده برخوردار باشند (باید بررسی کنید که مسیریاب برای هر دو شبکه صحیح است و همچنین سرویس پروکسی در سرویس‌دهنده پروکسی فعال و به خوبی پیکربندی شده است). از آنجا که هر سرویس‌دهنده پروکسی، مثل مسؤول پذیرش تلفن سازمان جاسوسی دو «سیستم تلفن» مجزا دارد، برخی اوقات لازم است برای عیب‌یابی، وارد سیستم سرویس‌دهنده پروکسی شوید.

DNS می‌تواند موضوعی آزاردهنده و خاردار باشد، بهتر است قبل از مواجه‌شدن با مشکلات، نوع تحلیل نام DNS را بررسی نمایید). برخی از سرویس‌دهنده‌های پروکسی خاص، تحلیل DNS پروکسی را انجام می‌دهند که باعث می‌شود ابزار عیب‌یابی DNS برای حل مشکلات تحلیل نام اینترنت کارایی خود را از دست بدهند.

کارگاه

پرسش و پاسخ

پرسش : رئیس‌مان خواست که دیوار آتشی داشته باشیم، اکنون یکی داریم که به نظر می‌رسد کار خود را خوب انجام می‌دهد. با این وجود، من نگران شبکه داخلی خودمان هستم، چرا که ما تعداد زیادی DC با PC Anyware هستند که می‌توانند آزادانه به پورت‌ها متصل شوند. پول چندانی برای قفل‌کردن شبکه‌مان ندارم و بنابراین نمی‌توانم از برنامه‌های نظارت بر شبکه گرانقیمت و سیستم‌های ممیزی استفاده کنم. چکار می‌توانم انجام دهم؟

پاسخ : اگر می‌خواهید امنیت خود را بدون صرف زمان زیاد بهبود بخشید، سری به http://www.ceroty بزنید. هشدارهای امنیتی بسیاری از فروشندگان (و چگونگی پرهیز از خطرات) در آنجا ارائه شده‌اند. همچنین باید تلاش فراوانی در آموختن سیاست‌های امنیتی شبکه داشته باشد. کتابهای خوبی نظیر دیوارهای آتش و امنیت در اینترنت نوشته Cheswick و Bellovin و نیز امنیت در یونیکس از دیدگاهی عملی کار Garfinkel و Spafford نیز مفید واقع خواهند شد.

پرسش : فروشنده دیوار آتش، می‌گوید که محصول وی سرویس‌دهنده پروکسی یا مسیریاب فیلترکننده بسته نیست. پس چه چیزی در آن گنجانده شده است؟

پاسخ : من علاقه زیادی به فروشندگان دارم. آنها برخی اوقات خیلی خنده‌دار هستند. موضوع از این قرار است: یکی دوسال قبل وقتی که شخصی نشان داد که چگونه می‌توان مسیریاب‌های فیلترکننده بسته را از سر راه برداشت، این ابزارها به شدت تحقیر شدند. بنابراین، امروزه دیوارهای آتش پیشرفته را دیگر مسیریاب‌های فیلترکننده بسته نمی‌دانند ـ گو اینکه آنها هنوز بسته‌ها را مسیریابی می‌کنند. هنوز هم در سطح شبکه با بسته‌ها کار می‌کنند و هنوز فیلتر می‌کنند. همچنین این ابزار با آنهایی که SMLI دارند (که در سطح کاربرد تصمیم‌گیری می‌کند) متفاوت هستند. پس، اگر مثل اردک راه می‌رود...

پرسش : آیا ممکن است اشکالاتی در سرویس‌دهنده پروکسی‌ام وجود داشته باشند؟

پاسخ : هر چیزی ممکن است چه سرویس‌دهنده پروکسی داشته باشید و چه دیوارهای آتش، با فروشنده ارتباط داشته باشید و اصلاحیه‌های امنیتی را از آنان دریافت کنید. در هر حال، سرویس‌دهنده پروکسی نباید بجز برنامه‌های پروکسی، چیز دیگری را به‌اجرا درآورد ـ مگر آنکه در امور امنیتی خبره و مطمئن باشید که سایر برنامه‌ها سرویس‌دهنده را به خطر نمی‌اندازند.

آزمون

۱- تفاوت بین سرویس‌دهنده پروکسی و مسیریاب فیلترکننده بسته در چیست؟

الف ـ سرویس‌دهنده‌های پروکسی در سطح شبکه فیلتر می‌کنند، در حالی که مسیریاب‌ها این کار را در سطح کاربرد به انجام می‌رسانند.

ب ـ سرویس‌دهنده‌های پروکسی در سطح کاربرد و مسیریاب‌ها در سطح شبکه فیلترسازی می‌کنند.

ج ـ پیکربندی نامناسب مسیریاب‌ها، خطرات امنیتی درپی دارد.

د ـ پیکربندی نامناسب سرویس‌دهنده‌های پروکسی، خطرات امنیتی درپی دارد.

۲- درست یا نادرست؟ سرویس‌دهنده پروکسی «چسب شبکه» محسوب نمی‌شود، بلکه «تنها سرویس‌دهنده دیگری» است (ولو یک سرویس‌دهنده چندخانگی).

۳- مسیریاب فیلترکننده بسته و سرویس‌دهنده پروکسی هردو _____ هستند.

الف ـ کاربران بازرسی وضعیت چندسطحی ب ـ چندخانه‌ای

ج ـ کاستی‌های امنیتی د ـ راکت‌های سوکتی

۴- TCP _____ و UDP _____ هستند.

الف ـ مشکلی برای پیکربندی؛ خارق‌العاده ب ـ مشکل‌زا؛ عالی

ج ـ آسان؛ سخت د ـ اتصال‌گرا؛ بدون اتصال

۵- هر سرویس‌دهنده پروکسی را برای کدامیک از اقلام زیر گنجایش زیادی ندارد؟

الف ـ کاربرانی که درخواست اتصالات محلی LAN دارند.

ب ـ کاربرانی که از آن می‌خواهند اتصالات اینترنتی بیشتری ایجاد کند.

ج ـ ترافیک T1 بالا د ـ جستجوی بسیار در یک سایت وِب

۶- استفاده از ابزار عیب‌یابی DNS در صورت درست‌بودن کدامیک از اقلام زیر میسر است؟

الف ـ DNS از طریق سرویس‌دهنده DNS محلی مسیریابی شود.

ب ـ DNS از طریق سرویس‌دهنده پروکسی مسیریابی شود.

ج ـ مسیریاب به درخواست‌های داخلی DNS را رتق و فتق نماید.

د ـ سرویس‌دهنده پروکسی تمامی درخواست‌های DNS را رسیدگی کند.

پاسخ به سؤالات آزمون

۱- ب ۲- درست

۳- ب ۴- الف

۵- الف ۶- الف

بخش چهارم

در خندق‌ها

فصل ۱۶ : ثبات عمیق، زیباست : نجات از مشکل
فصل ۱۷ : از کجا شروع کنم؟
درس ۱۸ : «افراد مختلف بسیار در همسایگی شما» : عیب‌یابی عمقی کاربردی
درس ۱۹ : عیب‌یابی اینترنت/اینترانت
درس ۲۰ : عیب‌یاب‌های شبکه تنها می‌خواهند سرگرمی داشته باشند
درس ۲۱ : برایم از شبکه‌ات بگو: تحلیل‌گران شبکه
درس ۲۲ : ابزار مدیریت شبکه
درس ۲۳ : شبکه کُند است! دریافت پاسخی صریح به سؤالی مبنایی
درس ۲۴ : مهندسی معکوس شبکه

فصل ۱۶

ثبات عمیق، زیباست : نجات از مشکل

مؤلفه‌هایی که به شکل ثابت پیکربندی نشده‌اند، برای عیب‌یاب پرکار شبکه مشکل‌زا خواهد بود. در این فصل، سه تکنیک را آموزش خواهم داد که با کمک آن خواهید توانست شبکه‌ای با ثبات (همگون، از دیدگاه استادکاران شبکه) ایجاد و نگهداری کنید:

- روش‌های ثبات دستی (که بیشتر بر مهارت‌های سازمانی در ترکیب با امکانات و بهره‌برداری از ویژگیهای سیستم عامل اتکا دارند)
- مضاعف‌سازی گردونه دیسک سخت (انبوه‌سازی)
- استفاده از ابزار گسترش خودکار جدید

این تکنیک‌های ثبات، جدای از منافع واضح حاصل از یکبار طراحی و گسترش و به‌کارگیری چندباره، می‌توانند کار عیب‌یابی را بسیار ساده‌تر نمایند.

مضاف بر آن، اگر این چهار مؤلفه شبکه‌ای استاندارد نگه داشته شوند، کار عیب‌یاب ساده خواهد ماند:

- پیکربندی گردونه دیسک سخت
- اسکریپت‌های ورود به سیستم در شبکه
- ویژگیها و صفات کاربر شبکه
- پیکربندی کاربردی شبکه

داشتن مؤلفه‌های یکسان پیکربندی‌شده، بدان معناست که اگر یکی از مؤلفه‌ها در محلی درست کار می‌کند، باید در بقیه جاها هم همین طور باشد، مگر آنکه مشکلی سخت‌افزاری وجود داشته باشد (مشکلات سخت‌افزار در صورت مقایسه وضعیت یکسان در سیستم‌های عامل، خود را به سادگی، به وضوح نشان می‌دهند).

این حالت، همچنین بدان معناست که برای عیب‌یابی، لازم نیست مسائل زیادی را درک کنید. به جای درک زیروبم نهفته در یک پیکربندی شبکه‌ای پیچیده، اقلام ساده‌ای را با اقلام «سالم» مشابه مقایسه می‌کنید (برای مثال، اسکریپت‌های ورود به سیستم یا صفات کاربر) یا سریعاً اقلام پیچیده‌تر را دوباره به انجام می‌رسانید.

برای مثال، بعد از کشف آن که یکی از ایستگاههای کاری که مشکلی در سیستم‌عامل یا برنامه‌ای کاربردی دارد، شاید با سایر ایستگاهها یکسان باشد (شیء کاربر، صفات کاربر و پیکربندی کاربردی شبکه را از مجموعه ممکن مشکلات کنار گذاشته‌اید)، خیلی ساده می‌توانید گردونه دیسک سخت را مرد توجه قرار دهید. این کار ۱۵ دقیقه طول می‌کشد (در مقابل چندین ساعتی که در غیر این صورت می‌بایست صرف کنید). از آن گذشته، اگر گردونه هر دیسک سخت، به یک شکل

پیکربندی شده باشند، تکثیر ایستگاه کاری مضر نخواهد بود ـ یعنی، حداقل به پیکربندی‌ای که تصور می‌شود در گردونه تنظیم شده باشد، آسیب نمی‌رساند.



هشدار : *برای آنکه کاربران ناراحت نشوند، باید قبل از «پریدن»، ارتباط برقرار کنید. یعنی، کاربرانتان باید بدانند که نگهداشتن فایل‌های داده‌های روی گردونه دیسک سخت‌شان ایده بسیار بسیار بدی است. سوای این واقعیت که اطلاعاتشان در صورت خرابی دیسک از بین می‌رود، انجام تکثیر دیسک سخت هرگونه اطلاعات ثبت‌شده به شکل محلی را پاک می‌کند.*

کلام آخر اینکه : کار عیب‌یابی با تشخیص محلی یا سیستماتیک‌بودن مشکل شروع می‌شود. اگر مشکل محلی باشد، اغلب می‌توانید از طریق همگن‌سازی ایستگاه‌کاری یا شیء کاربر آن را برطرف سازید. این بدان معناست که اغلب، تمام توان مغزی خود را روی مشکلات سیستماتیک صرف خواهید نمود. اگر تکنیک‌های این فصل را به‌کار ببندید، حل مشکلات محلی نیازی به سوزاندن فسفر مغز ندارند.

استانداردسازی دستی

استفاده از ابزار گسترش خودکار به منظور سازماندهی، الزامی نیست (از سوی دیگر، باید گفت که با به‌کارگیری آنها، کارها بسیار سریعتر و آسانتر خواهند شد). چه از ابزار قدرتمند استفاده کنید و چه با متد دستی به جنگ کارها بروید، لازم است یک طرح کاری خوب تعریف شده، داشته باشد (چگونه می‌توان کاری را به صورت خودکار به انجام رساند، در حالی که لازم است به صورت دستی صورت پذیرد؟)

اجازه دهید نگاهی به بخشهای مختلف طرح مذکور داشته باشیم، که در هر صورت، چه انجام خودکار و چه دستی، یکسان خواهند بود:

- تقسیم وظایف به وظایف مربوط به ایستگاه‌کاری و تنظیم کاربر
- ایجاد چک لیست از وظایفی که باید به پایان برد
- نگهداری و ثبت کامل اوضاع
- نوشتن طرح با جزییات، مطرح‌کردن مشکلات در آن و پالایش دوباره طرح
- مقاومت در مقابل وسوسه انحراف از طرح

به طور خلاصه، مشخصات طرح خوب شبکه ـ بزرگ یا کوچک ـ نشان‌دهنده حالات خوب شما هست که به شبکه منتقل شده‌اند. سعی کنید که اینگونه در نظر داشته باشید که طرح شبکه، مثل کاری در کارخانه یا مثل برش مشکلات است. هر چیزی که روی یک شیء شبکه انجام می‌شود را باید روی شیء بعدی نیز به انجام رساند.



یادداشت : *با اینکه می‌توان اشیاء را به صورت یکسانی پیکربندی نمود، به خاطر وجود خطای انسانی، تضمینی در این ارتباط وجود ندارد.*

عصر ابزار قدرتمند

سیستم‌عامل شبکه، ابزار اولیه را برای کمک به شما در جستجوی ثبات، در اختیار می‌گذارد.

- **الگوهای کاربردی** شما را قادر می‌سازند که کاربر موجودی را کپی کنید.

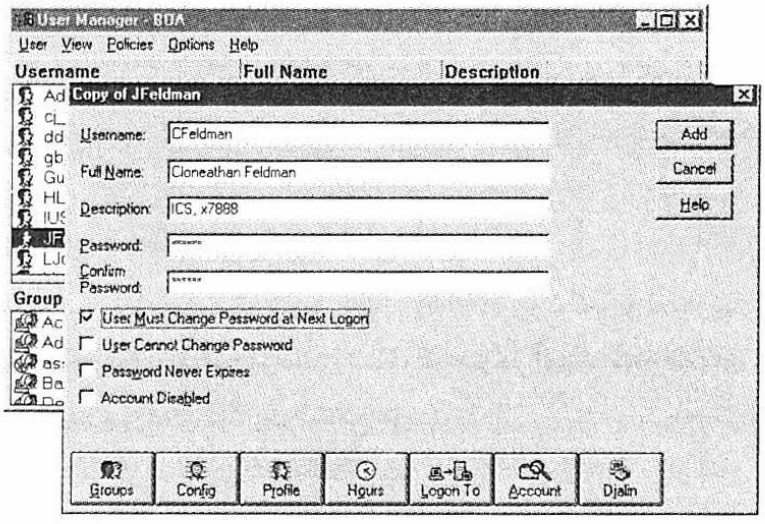
- **اسکریپت‌های ورود به سیستم در سطح کاربر** این اسکریپت‌ها برای انجام پیکربندی‌های آغازی مختلف، مثل افزودن PATH به محیط کاربر، نمایش پیغام روز و نظایر آن به‌کار می‌روند. اسکریپت‌های ورود به سیستم در سطح کاربر، هنگامی که کاربران مستقل وارد سیستم می‌شوند، به اجرا درمی‌آیند.

- **اسکریپت‌های ورود به سیستم سازمانی یا در سطح گروه** اسکریپت‌های گروهی یا سازمانی هنگامی که شخصی از گروه یا سازمان بخواهد وارد سیستم شود، اجرا می‌شوند.

- **پروفایل‌های شبکه‌ای کاربر** پروفایل‌های شبکه‌ای، اطلاعات شبکه‌ای پیکربندی نظیر رومیزی ویندوز، منوی Start، ترجیح‌ها و نظایر آن می‌باشند (این اقلام را در ادامه این فصل با ذکر جزییات مورد بررسی قرار خواهیم داد).

الگوهای کاربری

تنظیم الگوهای کاربری مشکل است، اما سالیان سال است که کمک بزرگی به سرپرستان شبکه محسوب می‌شوند. ایجاد یک کاربر نمونه، بررسی و آزمودن آن و آنگاه کپی‌کردن کلیه صفات وی خصوصیات برای بقیه کاربران. در واقع، تنها سیستم‌عامل شبکه که می‌دانم امکانات ویژه و فرمول‌بندی‌شده‌ای برای الگوهای کاربری دارد، نتور می‌باشد (از طریق NDS ناول). سایر سیستم‌ها، برنامه‌های کمکی مختلفی برای کپی‌کردن کاربر دارند ـ و صادقانه باید گفت که همگی به خوبی کار می‌کنند، البته اگر یادتان باشد که از آنها استفاده نمایید. شکل ۱-۱۶ امکان کپی‌کاربر در ویندوز NT را نشان می‌دهد.



شکل ۱-۱۶: می‌توانید برای کپی‌کردن هر کاربر حوزه، از User Form Domains استفاده نمایید.

کاربر نمونه

اگر سیستم‌عامل مورد استفاده‌تان، الگوهای کاربری را فراهم نمی‌آورد، واقعاً لازم است کاربر نمونه‌ای ایجاد کنید (در واقع ممکن است چندین کاربر برای دپارتمان‌های مختلف ایجاد کنید). برای این کار باید ورود به سیستم، وابستگی‌های گروهی، و شاخه خانه و فایل‌های پیکربندی مختلف در شاخه خانه کاربر را به وجود آورید. برای مثال، گروههای مختلف کاربران یونیکس ممکن است به فایل‌های آغازینی مثل .xdefaults، .xinitrc، .pinerc و نظایر آنها نیاز داشته باشند. به همین شکل، برخی برنامه‌های کاربردی ویندوز هم ممکن است به فایل‌های ویژه کاربر، برای تنظیمات شبیه‌سازی ترمینال، تنظیمات لوتوس 1-2-3 و نظایر آنها نیاز داشته باشند.

هر زمان که به کاربر جدیدی نیاز دارید، می‌توانید کاربر نمونه را کپی کنید. محتویات شاخه خانه وی را به شاخه خانه کاربر جدید کپی کنید و مطمئن باشید که تمامی اقلام برای انجام کارهایشان را در اختیار دارد. می‌توانید این گونه تصور کنید که این کار مثل استفاده از یک فایل الگوست که هر هفته برای ارسال یک نامه مورد استفاده قرار می‌گیرد ـ تمام کاری که لازم است انجام دهید، کپی‌کردن سند، چند تغییر مشخص و صرف جویی در زمان و انرژی می‌باشد.

اسکریپت‌های ورود به سیستم در سطح کاربر

هر سرویس‌دهنده قادر است اسکریپت‌های ورود به سیستم برای تمامی کاربران را اجرا کند. این اسکریپت‌ها، وظایف عمومی برای تمامی کاربران را به انجام می‌رسانند.

برخی مثالها عبارتند از:

- نمایش پیغام روز
- تنظیم متغیرهای محیطی که برای برنامه‌های کاربردی لازم هستند
- به‌روزدرآوری نرم‌افزار ایستگاه‌کاری
- همسان‌سازی زمان (ساعت) ایستگاه‌کاری با شبکه
- تنظیم محیطی ترمینالهای نمایشی (در مورد یونیکس)

باید حتی‌المقدور از استفاده از اسکریپت‌های ویژه کاربر اجتناب کنید، چرا که پیکربندی تک‌تک ایستگاههای کاری، بسیار زمانبر است. به جای آن تا آنجا که می‌توانید روی اسکریپت ورود به سیستم و اسکریپت‌های گروهی کار کنید.

اسکریپت‌های ورود به سیستم گروهی/سازمانی

اسکریپت‌های ورود به سیستم در سطح سیستم شامل /etc/profile در یونیکس و اسکریپت ورود به سیستم در نت‌ور 3.x می‌شوند. این اسکریپت‌ها این امکان را برای سرپرستان شبکه فراهم می‌آورند که اتفاقهای خاصی برای همه افراد سیستم رخ دهد. البته، ممکن است بخواهید چیزهای دیگر در سطح هر دپارتمان ـ و نه در سطح کل سیستم ـ به وقوع بپیوندند.

تا هنگام ظهور DNS، سرپرستان توانایی ارائه اسکریپت برای کاربران یک دپارتمان را در اختیار نداشتند. این کار، تعداد اسکریپت‌هایی که باید ردیابی شوند را افزایش می‌دهد، اما به خوبی امکان طبقه‌بندی و مدیریت اسکریپت‌ها را در اختیار می‌گذارد.

بنابراین، اسکریپت‌های دپارتمانی یا گروهی خوب هستند یا نه؟ خوب، پاسخ به آن بستگی دارد که به آنان نیاز داشته باشید یا نه. اگر در شرکت شما همه از یک سری برنامه کاربردی استفاده می‌کنند که به یک سری تنظیمات ثابت نیاز دارد، اسکریپت‌های سیستمی برایتان بس خواهند بود. از سوی دیگر اگر دپارتمان‌های مختلف در سازمان شما، به تنظیمات متفاوتی از بقیه نیاز داشته باشند، اسکریپت‌های گروهی تقریباً یک نیاز خواهند بود.

اسکریپت‌های کمکی

اوضاع برای کاربران DNS مرتب به نظر می‌رسد، اما برای بقیه چطور؟ کج‌خلقی نکنید ـ ترفندهایی هستند که به شما اجازه می‌دهند عملیات مربوط به گروه را از طریق اسکریپت ورود به سیستم اصلی، اعمال نمایید.



یادداشت : *اسکریپت‌های ورود به سیستم NT، اغلب فایل‌های BAT، یا CMD هستند که البته، همان فایل‌های دستوری قدیمی‌اند.*

برای مثال، تحت ویندوز NT برای هر کاربر در بخش مالی، یک راه کار برای ایجاد امکان اسکریپت‌های ورود به سیستم در سطح گروه، آن است که اسکریپتی به نام FINANCE.BAT برای کاربران آن گروه تعریف کنید که دستورات لازم برای گروه را به اجرا درمی‌آورد.

اما در مورد کاربرانی که نیازهای مخصوص به خود را دارند چطور؟ اگر کاربران خاصی، به اسکریپت‌های ورود به سیستم مخصوص به خود نیاز دارند (و شما باید به خوبی در این مورد فکر کنید، چرا که کار نگهداری بسیار مشکلتر خواهد شد)، می‌توانید در انتهای FINANCE.BAT سطر ذیل را بگنجانید:

```
if exist %USERBAME%.bat %USERNAME%.bat
```

این کار باعث می‌شود اسکریپت کاربر در صورت موجودبودن در شاخه login به اجرا درآید.

در یونیکس، در صورت استفاده از پوسته استاندارد ksh یا sh، می‌توانید تست گروه را در اسکریپت /ect/profile انجام داده و اگر شخص مورد نظر در گروه بود، مجموعه خاصی از دستورات را به انجام برسانید:

```
groups | grep -q -w finance && {
  echo "Your're in the Finance group, no party for You!
  cat /finance/message-of-the-day
  PARTY="false"
}
     groups | grep -q -w network && {
       eccho "Hello network person, party on!"
       cat /network/message -of-the-day
     }
```

پتانسیل اشتباهی که در پشت اسکریپت‌های گروهی نهفته است، آن است که برخی از کاربران ممکن است در چندین گروه عضویت داشته باشند. برای مثال، کاربر مثال قبل را مورد توجه قرار دهید که هم عضو گروه مالی و هم عضو گروه شبکه است. کار او با "TRUE" باقی‌گذاردن متغیر PARTY به اتمام می‌رسد. آیا این چیزی است که می‌خواهید؟ اگر نه، باید آن را تغییر دهید تا اول گروه شبکه تست شود.

اگر کماکان به استفاده از نت‌ور ۳/۲ اصرار می‌ورزید، می‌توانید از SYSCON برای ویرایش اسکریپت ورود به سیستم استفاده کنید تا وظایف گروهی را هم بتوانید به انجام برسانید. کافی است به اسکریپت ورود به سیستم Supervisor Options|System بروید و نظیر زیر عمل کنید:

```
if member of "Finance" then begin
   write "Hi, Finance Person! Parties prohibited!"
   display f:\public\finance\message.txt
   dos set PARTY="false"
end
```



هشدار : *زیاد هم در مورد امکان تأثیرگذاری روی تعداد زیادی از کاربران به هیجان نیایید. هنگامی که با تعداد زیادی سروکار داشته باشید، لغزش در چاقوی الکترونیکی‌تان می‌تواند پتانسیل ناراضی‌شدن تعداد زیادی افراد را فراهم کند.*
تا آنجا که ممکن است، باید آزمایش‌هایی را دور از چشم تماشاچیان به انجام برسانید. اگر سرویس‌دهنده آزمایشی داشته باشد، بهتر است آن را به‌کار اندازید؛ در هر شکل، باید از گروه آزمایشی و کاربر آزمایشی هنگام آزمودن اسکریپتی جدید یا آزمایش هر چیز جدید استفاده نمایید.

پروفایل‌های میکروسافت

ویندوز ۹۵ و NT توانایی این را دارند که اطلاعات ویژه هر کاربر را در شبکه ثبت کنند (البته یک نسخه از اطلاعات در گردونه دیسک سخت محلی نیز قرار داده می‌شود). این اطلاعات، اقلام زیر را شامل می‌شوند:

- منوی Start (میانبُر)
- رومیزی (میانبُر)
- فایل‌هایی که اخیراً استفاده شده‌اند (میانبُرها)
- User Registry (نسخه‌ای از Registry حاوی تنظیمات خاص کاربر)

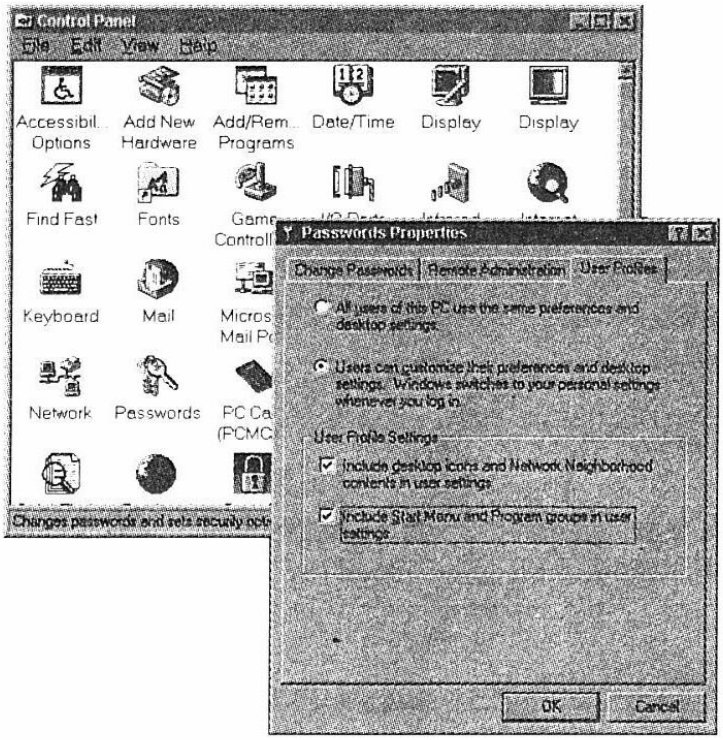
پروفایل‌ها، ابزار استانداردسازی خارق‌العاده‌ای هستند و همچنین وسیله مناسبی برای عیب‌یابی شبکه محسوب می‌شوند. از آنجا که تنظیمات کاربر به راحتی از ایستگاههای کاری وی جدا شده‌اند، انتقال کاربر و کارکرد وی در جایی دیگر بدون مشکل خواهد بود ـ برخی اوقات حتی نیازی به نصب دوباره برنامه‌های کاربردی برای انتقال تنظیمات کاربردی نیست.



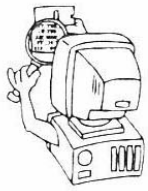
نکته : *از آنجا که در ویندوز 9x، پروفایل‌ها به صورت پیش‌گزیده غیرفعال هستند (بنابراین هر کاربر از همان سری تنظیمات استفاده می‌کند)، باید مطمئن شوید این امکان را فعال ساخته‌اید. این کار از طریق Control Panel، انتخاب Passwords و انتخاب برگه User Profiles از کادر تبادلی Password Properties و انجام تغییرات مناسب، میسر می‌باشد (شکل ۲-۱۶ را ملاحظه کنید.)*



یادداشت : *پروفایل‌های کاربران در کجا قرار دارند؟ در شبکه ویندوز NT و همچنین ناول 4.2 به بالا، پروفایل‌ها در شاخه‌های خانه کاربران قرار داده می‌شوند. در ناول 3.x، آنها را در شاخه SYS:MAIL تحت شاخه‌هایی با نام IDهای عددی منحصر به فرد کاربران قرار می‌دهند (می‌توانید ID عددی منحصر به‌فرد هرکاربر را با استفاده از SYSCON|User Information|User Name|Other Information مشاهده کنید).*



شکل ۲-۱۶ : Control Panel در ویندو 9x این امکان را فراهم می‌سازد که پروفایل‌ها را برای هر ماشین خاموش و روشن کنید. بسیاری از شبکه‌ها از تنظیمات نشان داده شده در این صفحه استفاده می‌کنند.



***نکته** : اگر می‌خواهید چیزی را در فایل‌های پروفایل شبکه کاربران اضافه کنید یا تغییر دهید، باید مطمئن شوید کاربر در سیستم نیست، چرا که ویندوز هنگام خروج کاربر از سیستم اطلاعات را بازنویسی می‌کند. بنابراین، ممکن است اطلاعات تغییریافته شما را از بین ببرد.*

ارسال انبوه

مضاعف‌سازی دیسک، یکی از آن نوآوری‌هاست که استفاده از سیستم‌های عامل رومیزی پیچیده مثل ویندوز را به تجربه شیرینی برای سرپرستان شبکه تبدیل کرده است. این امکان، به سرپرستان شبکه اجازه می‌دهد به کل ویندوز، به چشم یک کتری پر از DLLها، VXD ها و فایل‌های پیکربندی در یک قالب قابل مدیریت نگاه کنند. مضاعف‌سازی درمان همه درد و غمهای استانداردسازی نیست، اما مسلماً کمک می‌کند که راحت‌تر کارها صورت پذیرد. ایده نهفته در آن، این است که وقتی یکبار برای هر گروه کاری تنظیم شود، بارها قابل بهره‌برداری است.

به جای نصب جداگانه ویندوز 9x یا NT از CD-ROM روی ۴۰ ایستگاه‌کاری که حدود ۴۰ ساعت طول می‌کشد - می‌توانید مضاعف‌سازی ۱۰ دقیقه‌ای را انجام دهید که اندکی بیش از ۶ ساعت به درازا می‌کشید.



***یادداشت** : بله، میکروسافت اسکریپت‌های خودکار را برای ویندوز ۹۵ و NT پشتیبانی می‌کند، که شما را قادر می‌سازند، جلسه کاری تنظیمی غیرحضوری را برای تعداد زیادی از کامپیوترها از طریق شبکه صورت دهید. البته، نوشتن چنین اسکریپت‌هایی به مقدار زیاد «اطلاعات عمیق» و سفارش‌سازی سایت نیاز دارد. اگر با برنامه‌نویسی راحت هستید، می‌توانید از نقطه کار را شروع کنید - اما بدانید زمان زیادی طول می‌کشد. کلام آخر اینکه: به آسانی و سرعت مضاعف‌سازی دیسک نیست.*

از آن گذشته، علاوه بر تفاوت زمانی، می‌دانید که ایستگاههای کاری یکی هستند. نیازی نیست هیچ چیزی را بنویسید ـ معنی آن نیشگون‌های کوچکی که برای بهینه‌سازی سیستم صورت می‌دهید ـ مطمئن شوید تمامی تنظیمات درست برای تمام نصب‌ها صورت گرفته است.



هشدار : *بهتر است قبل از انجام مضاعف‌سازی از یکسان‌بودن سخت‌افزار ایستگاههای کاری مطمئن شوید؛ در غیر این صورت، خطرات تناوبی یا مشکلات صعب‌العبور را پیش‌رو خواهید داشت. این وضع هنگامی که ۱۰ تا ۲۰ PC خریداری می‌کنید، کمتر پیش می‌آید، چراکه احتمال کمی وجود دارد که آنان را از منابع مختلف خریداری کنید. اما هنگام ارتقاء دستگاه، این بررسی بیش از پیش رنگ می‌گیرد.*

بله، ویندوز 9x برای تشخیص تغییرات سخت‌افزار بسیار مناسب است ـ اما چرا ریسک هر مشکلی را بپذیریم؟ مضاعف‌سازی را به منظور اجتناب از مشکل مورد توجه قرار داده‌ایم، نه برای ایجاد آن.



نکته : *بسیاری اوقات، مهم نیست که چقدر مطمئن هستید که مضاعف‌سازی، «خوب» است باید بررسی کنید که تصویر مضاعف‌سازی همان چیزی است که باید مدنظر قرار گیرد. برای مثال، نرم‌افزار چاپ و فایل ممکن است تغییر یافته باشند و مضاعف‌سازی‌تان نیازمند به‌روزدرآوری باشد.*

هر مضاعف‌سازی در ساده‌ترین شکل خود، یک جلسه DOS با دیسک راه‌انداز شبکه است. از دیسک DOS راه‌اندازی می‌کنید، سرویس‌گیرنده شبکه را بارگذاری می‌کنید، وارد سیستم شده و آنگاه نرم‌افزار مضاعف‌سازی خود را به اجرا درمی‌آورید. این شکل از کار به شما اجازه می‌دهد محتویات کامل دیسک سخت جاری را به فایلی در شبکه کپی کنید و یا محتویات فایل شبکه را روی دیسک سخت محلی منتقل کنید. انتخابهای دیگری نیز وجود دارند. می‌توانید مضاعف‌سازی را دیسک به دیسک، روی نوارگردان یا روی CD-ROM انجام دهید، همه اینها به نرم‌افزار مضاعف‌سازی‌ای که انتخاب می‌کنید بستگی دارد.



یادداشت : *می‌گویید، حالات زیادی وجود دارند! بله، درست است. البته تکنولوژی مضاعف‌سازی فعلی، امکان فشرده‌سازی را نیز در اختیار می‌گذارد و دیسک سخت ۲ با GB فضای خالی، تنها 250MB فضا را در شبکه اشغال می‌کند.*

این کار مثل ساختن یک فایل ZIP روی دیسک سخت است ـ اما با تمامی فایل‌های مخفی، سیستم و محتویات خاص دیسک‌گردان، مثل قطاع راه‌انداز.

البته آگاه باشید که تمامی نرم‌افزارها مضاعف‌سازی هم امکان بازیابی فایل‌ها از یک فایل مضاعف‌شده را در اختیار نمی‌گذارند ـ در برخی تنها امکان بازنشانی کل دیسک سخت را فراهم ساخته‌اند.

بعد از انجام مضاعف‌سازی، باید پارامترهای مستقل هر ایستگاه‌کاری را تنظیم کنید ـ برای مثال، اسم ماشین و آدرس TCP/IP (اگر از DHCP استفاده نمی‌کنید). نرم‌افزارهای پیشرفته مضاعف‌سازی، امکان انجام این کار را به صورت خودکار فراهم ساخته‌اند. عالی است!

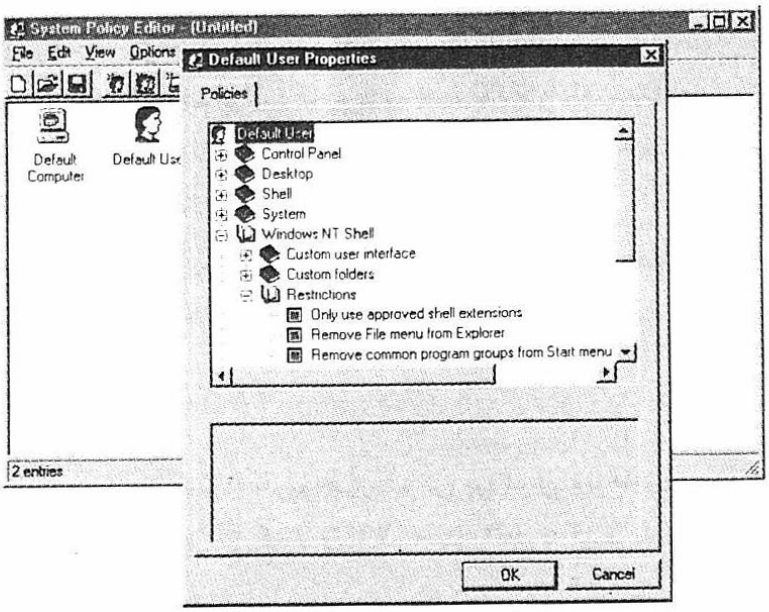
سیاست محافظت : ابزار سرپرستی خودکار

«کاربران را از دست خودشان نجات دهید!» فریادی است که از بسیاری از سرپرستان شبکه به گوش می‌رسد. مطمئنم شما نیز به این موضوع فکر کرده‌اید. بانویی را تصور کنید که چگونگی تغییر رنگهای صفحه نمایش را یاد گرفته است. او تمامی رنگها را به رنگ زرد ـ رنگ مورد علاقه‌اش تغییر می‌دهد ـ خواندن از چنین صفحه‌ای کمی مشکل است!

سیاست‌ها

به منظور جلوگیری از چنین وضعیتی، میکروسافت یک ابزار مدیریتی مخصوص به اسم فایل سیاست معرفی نموده است. هر فایل سیاست، هنگام قرارگرفتن در شاخه SYS:PUBLIC سرویس‌دهنده ناول یا شاخه NETLOGON سرویس‌دهنده NT، تنظیمات Registry خاصی را برای کاربران پیش‌گزیده یا کاربران ویژه اِعمال می‌کند. این حالت، شلیک کاربران به سوی خودشان را سخت کرده و کار شما را نیز آسان می‌سازد.

میزان محدودکنندگی یا مجازداشتن اعمال‌شده توسط فایل سیاست توسط شما تعیین می‌شود. می‌توان تمام یا بخشی از Control Panel را قفل کنید، نصب برنامه‌ها را محدود ساخته و نظایر آنها، مطابق شکل ۳-۱۶ محدودیت‌ها را ایجاد کنید. به طور خلاصه، می‌توانید از محبوبیت خودبین کاربران خیلی خیلی بکاهید. سؤال این است ـ چه مقدار محدودیت، محافظت مناسبی را ایجاد می‌کند و چه مقدار آن ناخوشایند خواهد بود؟ این موضوع، کاملاً به فرهنگ شرکتی بازمی‌گردد.



شکل ۳-۱۶ : با System Policy Editor در ویندوز NT می‌توانید تقریباً روی هر موضوعی برای کاربران محدودیت قائل شوید.

سیاست‌های ویندوز، این امکان را فراهم می‌سازند که بتوانید یکسان‌بودن برخی صفحات ویندوز را بین PC های شبکه تضمین کنید.

این سیاست‌ها، با وجود شسته و رفته‌بودن، از دیرباز به صعب‌الاستفاده‌بودن معروف شده‌اند (فایل اجرایی Poledit را از CD-ROM ویندوز اجرا کنید و ببینید با این نظر موافق هستید یا خیر). البته، این امکانات بعد از معرفی Zero Administration Kit(ZAK) رفته‌رفته بیشتر قابل استفاده شده‌اند.



یادداشت : *این بخش از سایت میکروسافت را وارسی کنید:*

http://www.microsoft.com/NTworkstation/Deployment/Deployment/default.asp

ناول نیز به تازگی Z.E.N. Works(Zero Effort Networking) را ارائه نموده است. این محصول، علاوه بر موارد دیگر اجازه می‌دهد سیاست‌های ویندوز را با استفاده از واحدهای سازمانی، گروهی و کاربردی DNS مدیریت نمایید. Z.E.N همچنین ابزار گسترش نرم‌افزار و کنترل از راه دور را فراهم می‌کند). بدنیست برای اطلاعات بیشتر، نگاهی به http://www.novell.com/products/nds/zenworks بیندازید.

برنامه‌های کاربردی در یک نگاه

سابق، وقتی که می‌خواستید استفاده از یک برنامه کاربردی شبکه‌ای را گسترش دهید، کافی بود گزینه‌ای از یک منو یا میانبُری را در اختیار کاربری بگذارید. برنامه‌های ویندوز از پیچیدگی خیلی بیشتری برخوردار هستند؛ برخی بسیاری فایل روی ایستگاههای کاری نصب می‌کنند، تغییراتی را در Registry کاربر اِعمال می‌کنند و می‌توانند، صادقانه بگویم، کار سرپرستان شبکه را مختل نمایند.



***یادداشت :** برخی (اما نه همه) برنامه‌های کاربردی ویندوز را می‌توان به سادگی استاندارد نمود. تمامی آنچه که لازم است انجام هدی، نصب برنامه در شاخه اشتراکی شبکه است که افراد بسیاری بر آن دسترسی دارند. با این روش، می‌توانید برنامه کاربردی را از این محل مرکزی پیکربندی کنید.*

برای مثال در NetTerm، یک برنامه کاربردی Telnet، کاربران بسیاری می‌توانند بدون اجرای برنامهٔ تنظیم‌کننده روی هر ایستگاه‌کاری، آن را به اجرا درآورند. روش کار به این صورت است:

۱- برنامه تنظیمی NetTerm را اجرا کنید.

۲- محلی را در شبکه برای برنامه مشخص نمایید (برای مثال، G:\NetTerm).

۳- شمایلی برای NetTerm روی Desktop هر کاربر ایجاد کنید که به فایل G:\netterm\netterm.exe اشاره می‌کند.

این کار را می‌توانید با ملاقات با کاربر یا از طریق پروفایل شبکه‌ای وی انجام دهید.

باید مستندات سازنده را بررسی کنید و یا در محل تجربه کنید تا ببینید آیا چنین ویژگی‌ای را برنامه پشتیبانی می‌کند.

ابزار گسترش برنامه، در مورد برنامه‌های کاربردی پیچیده، تقریباً به جالبی مضاعف‌سازی دیسک هستند. آنها عکسی از PC قبل از نصب برنامه و عکسی بعد از نصب آن تهیه می‌کنند. تفاوتها ـ چه در Registry، در فایل‌های دیسک سخت و یا هر چیز دیگری ـ محاسبه شده روی شبکه به ثبت می‌رسند. این تفاوتها را می‌توان برای هر دستگاهی به‌کار برد. برنامه‌ای کاربردی فوری دارید که حداقل تراکنش را با کاربر دارد، چرا تمامی اطلاعات را شبکه فراهم می‌سازد. این روش در کنار مضاعف‌سازی دیسک مجموعه بسیار خوبی برای استانداردسازی ایستگاههای کاری کاربران تشکیل می‌دهد.

تنها نکته‌ای که باید به خاطر بسپارید، آن است که هنگام استفاده از یکی از ابزار گسترش برنامه ـ برای مثال، SYSDIFF میکروسافت، SnAPPshot ناول یا Picture Taker از شرکت Ghostsoft ـ و در لحظه تهیه عکس «قبل»، ایستگاه‌کاری باید

کاملاً تمیز باشد. یعنی، نباید به هیچ وجه برنامه قبلاً روی آن ایستگاه نصب شده باشد (هدف و منظور، مؤلفه‌های مشترکی است که برنامه نیاز دارد). من ترجیح می‌دهم یک کپی نصب‌شده و تروتازه ویندوز (در کنار سرویس‌گیرنده فایل و چاپ انتخابیم) را به صورت یک فایل مضاعف‌سازی دیسک نگهداری کنم؛ درست قبل از تهیه عکس، این فایل را روی دیسک سخت بارگذاری می‌کنم. این کار، تضمین می‌کند که برنامه شانس اجراشدن روی سیستم کاملاً تازه‌ای را داشته باشد.

آیا مشکلی در این ارتباط وجود دارد؟ ممکن است ـ مشکلات تداخلی در نصب خودکار، درست نظیر نصب معمولی ممکن است رخ دهند. تنها راه حل، تست و بررسی هرچه پیشتر یا پیش از مورد استفاده قراردادن و گسترش برنامه است. انجام این کار، ساعت‌ها، روزها و هفته‌ها زمان عملیات عیب‌یابی را می‌کاهد.

خلاصه

استفاده از مؤلفه‌های شبکه‌ای مشابه، بدان معناست که برای حل بسیاری از مشکلات محلی و نه سیستماتیک) نیازی به انجام روال‌های عمقی عیب‌یابی نخواهید داشت. علاوه بر آن، رفتار یکسان مؤلفه‌های همگون ـ در صورت استفاده از یک پیکربندی «سالم» ـ کمک بسیار خواهد بود.

جدا از استفاده از عادات کاری احساسی، هنگام ایجاد کاربران و ایستگاههای کاری بهتر است که امکانات توکار انبوه‌سازی سیستم‌عامل شبکه خود را بررسی کنید، چیزهایی مثل الگوهای کاربری و کپی‌هایی از کاربر «نمونه». با اینکه کمی اطلاعات در زمینه اسکریپت‌سازی می‌توانید چیز خطرناکی باشد، (منظورم خطر ایجاد خرابی در اثر ناکافی‌بودن دانسته‌هاست) می‌تواند در یکسره‌کردن تنظیم‌های ورود به سیستم کاربران، کمک بزرگی باشد.

پروفایل‌های کاربری و مضاعف‌سازی دیسک روشهای ساده و آسانی هستند که وحدت شکل کاربران را تضمین می‌کنند و همچنین می‌توانند راهنمای تنظیم ایستگاه‌کاری یا بازگرداندن تنظیم ایستگاهی نامتعادل باشند. از سوی دیگر دیگر، بسته‌های مدیریت سیاست، مثل ZAK و ZEN Works هم می‌توانند واقعاً کمک مؤثری باشند. با افزودن ابزار گسترش برنامه به صورت حساب، مخلوطی از ابزار قدرتمند جهت ثبات هر چه بیشتر پیش‌رو خواهید داشت.

کارگاه

پرسش و پاسخ

پرسش : چیزهای وحشتناکی در مورد آنچه که بعد از مضاعف‌سازی ویندوز NT اتفاق می‌افتد، خوانده‌ام. شنیده‌ام در صورت استفاده از مضاعف‌سازی دیسک، میکروسافت دیگر از شما پشتیبانی نمی‌کند.

پاسخ : خوب، درست است که میکروسافت مضاعف‌سازی دیسک را در ایستگاه‌کاری‌ای بعد از نصب حالت متنی ویندوز NT به پایان رسیده، پشتیبانی نمی‌کند. البته، این به معنای غیرعملی‌بودن این کار نیست. میکروسافت، بیشتر دو چیز را مدنظر قرار می‌دهد:

- یک ID امنیتی منحصربه‌فرد (SID) برای هر ایستگاه‌کاری تشکیل می‌شود. مضاعف‌سازی مستقیم، باعث می‌شود همه ایستگاههای کاری شما یک SID داشته باشند که بالطبع ممکن است مشکلاتی در شبکه را باعث شوند.

- در صورت عدم اجرای Setup، NT شانسی برای بررسی سخت‌افزار پیدا نمی‌کند که این خود می‌تواند به مشکلاتی منجر شود.

مشخص است که موضوع SID را باید جدی بگیرید؛ خوشبختانه، بیشتر فروشندگان نرم‌افزارهای مضاعف‌سازی، یک تغییردهنده SID فراهم ساخته‌اند که بعد یا قبل از فرآیند مضاعف‌سازی. به اجرا درمی‌آید و بنابراین موضوع اول منتفی است. مسأله عدم شناسایی سخت‌افزار توسط NT در صورت اجرانکردن Setup نیز درست است. آیا اگر تجارب مضاعف‌سازی را به خوبی دنبال کرده باشید و تنها این کار را در مورد سخت‌افزارهای مشابه به انجام برسانید، نباید به مشکلی برخورد کنید.

بنابراین، باید بین آنچه که کار می‌کند و آنچه که از آن اجتناب شده‌اید، یکی را انتخاب کنید. انتخاب با شماست و شما هستید که باید تحقیقات را انجام داده و در صورت تمایل، بررسی‌های بیشتری را صورت دهید.

خبر خوب آن است که میکروسافت اخیراً اعلام نموده که نگارش‌های آتی ویندوز با پشتیبانی وسیعتر کپی تصویری دیسک طراحی خواهند شد.

پرسش : یک سری تنظیم Registry مبتنی بر ایستگاه‌کاری مخصوص برای یک کارت شبکه دارم که باید به زودی روی دسته از ایستگاه‌کاری نصب نمایم. چگونه می‌توانم از یک ویرایشگر سیاست، برای انجام این کار استفاده نمایم؟

پاسخ : بجز حالتی که بخواهید به صورت عمیق از Microsoft Windows Resource Kit استفاده کنید و دریابید که چگونه می‌توان الگوهای ویرایشگر سیاست و تنظیمات سفارش Registry اضافه نمود، پیشنهاد من آن است که چنین کاری را با استفاده از REGEDIT درست قبل از مضاعف‌سازی دیسک صورت دهید. این کار، دریافت تنظیمات توسط کاربران را تضمین می‌کند. البته، همیشه بیشتر از یک راه برای انجام کارها وجود دارد.

پرسش : کدام نرم‌افزار مضاعف‌سازی برای من مفید است؟

پاسخ : نرم‌افزارهای مضاعف‌سازی به شکل شگرفی رشد کرده‌اند. دهها فروشنده چنین نرم‌افزارهایی ارائه می‌کنند. راه حل د را در وِب خواهید یافت. برخی انتخاب‌ها عبارتند از:

- Symantec (Ghost) www.ghost.com
- Key Labs (ImageBlaster, Lab Expert, and RepiDeploy) www.keylabs.com
- PowerQuest (DriveImage) www.powerquest.com
- Microhouse (ImageCast) www.imagecast.com

آزمون

۱- در نیمه راه عرضه ایستگاههای کاری یک دپارتمان، متوجه می‌شوید، با وجود آنکه سرویس‌گیرنده چاپ و فایل به درستی کار می‌کند، اما آخرین و جالبترین نگارش از آن سیستم نیست. یک روش محتاطانه حفظ ثبات، آن است که چه کار کنید؟

الف ـ استفاده از آخرین و جالبترین سرویس‌گیرنده را برای بقیه ماشینها تجویز می‌کنید.

ب ـ استفاده از آخرین و جالبترین سرویس‌گیرنده را برای ماشینهای قوی‌تر درنظر می‌گیرید.

ج ـ از همان سرویس‌گیرنده روی ماشین‌های قوی‌تر استفاده می‌کنید و روی بقیه از آخرین سرویس‌گیرنده استفاده می‌نمایید.

د ـ همان سرویس‌گیرنده را برای بقیه ماشین‌ها به‌کار می‌برید.

۲- درست یا نادرست؟ چه در صورت استفاده از مضاعف‌سازی دیسک و چه در صورت عدم استفاده از آن، فکر خوبی است که به کاربران توصیه کنیم از گردونه دیسک سخت خود به عنوان رسانه ذخیره‌سازی دائمی استفاده نکنند.

۳- کدامیک از جملات زیر در رابطه با الگوهای کاربردی درست هستند؟

الف ـ در تمامی سیستم‌های عامل در دسترس هستند، به طوری که کپی‌برداری از کاربران مطلوب نیست.

ب ـ در هیچ سیستم‌عاملی وجود ندارد، به طوری که کپی‌برداری از کاربران اجباری است.

ج ـ در برخی سیستم‌های عامل در دسترس نیستند، اما امکان کپی کاربران میسر است.

د ـ هیچ یک از موارد فوق

۴- به منظور حفظ ثبات، بهتر است که:

الف ـ تا آنجا که ممکن است، از اسکریپت‌های ورود به سیستم متفاوتی استفاده نماییم.

ب ـ از اسکریپت‌های ورود به سیستم گروهی یا سیستمی استفاده کنیم

ج ـ هم الف و هم ب

د ـ نه الف و نه ب

۵- هنگام کپی‌برداری از کاربر «نمونه»، باید انجام چه کاری را به خاطر بسپارید؟

الف ـ کپی‌کردن شیء کاربر، اسکریپت ورود به سیستم کلی و فایل‌های شاخه‌خانه

ب ـ کپی‌کردن شیء کاربر، فایل‌های شاخه‌خانه و اسکریپت ورود به سیستم در صورت لزوم

ج ـ کپی‌کردن الگوی خانه

د ـ کپی‌کردن الگوی ورود به سیستم

۶- درست یا نادرست؟ ترفندهایی هستند که با آنها می‌توانید حتی در صورت عدم پشتیبانی مستقیم سیستم‌عامل از اسکریپت‌های ورود به سیستم گروهی، چنین اسکریپت‌هایی را انجام دهید.

۷- درست یا نادرست؟ مضاعف‌سازی برای هر گونه نصب ایستگاه‌کاری مناسب می‌باشد.

۸- یکی از کاربران، مرتباً تنظیمات راه‌انداز نمایشی خود را عوض می‌کند و شما مجبورید مرتباً مشکل مربوط به شبیه‌سازی ترمینال را برطرف کنید. برای برطرف‌کردن این مشکل، چه کار باید بکنید؟

الف ـ Registry وی را ویرایش کنید.

ب ـ یک فایل سیاست ایجاد نمایید.

ج ـ نه الف و نه ب

د ـ هم الف و هم ب

۹- هنگام ایجاد هر نوع عکس برای گسترش برنامه‌ای کاربردی، باید مطمئن باشید چه کاری را انجام دهید؟

الف ـ از ایستگاه‌کاری استفاده کنید که آن برنامه قبلاً روی آن نصب شده است

ب ـ از ایستگاه‌کاری یکی از کاربران استفاده کنید.

ج ـ از ایستگاه‌کاری تمیزی استفاده نمایید، که هیچ مؤلفه‌ای روی آن نصب نشده است.

د ـ هیچ یک از موارد فوق

پاسخ به سؤالات آزمون

۱- د ۲- درست

۳- ج ۴- ب

۵- ب ۶- درست

۷- نادرست. تنها برای نصب گروههایی که سخت‌افزار مشابه دارند، مناسب است.

۸- ب ۹- ج

فصل ۱۷

از کجا شروع کنم؟

مجبور نیستید وظیفه‌ای را به اتمام برسانید؛ اما این آزادی را هم ندارید که آن را به دست غفلت بسپارید.
-*R.Tarfon, Pirkey Avot* (Chapter2, Mishna21)

ممکن است پاسخ به سؤال «از کجا شروع کنم؟» چنین باشد: هر روز کمی امور را بهبود ببخشید. در کلام استادان این شکل از کار عیب‌یابی فعالانه نامیده می‌شود و در فصل ۲ در مورد مستندسازی و فصل ۱۶ در مورد همگون‌سازی آن مطالبی دیدید (در فصل ۲۲، نگاه بیشتری به عیب‌یابی فعالانه خواهیم داشت).

بهترین نوع عیب‌یابی، آن نوع از عیب‌یابی است که طی آن، قبل از آغاز مشکلات از وقوع آنان جلوگیری می‌کنید ـ البته عیب‌یابی فعالانه قابل درک‌تر است. عالی است و مناسب برای یافتن مشکلات؛ البته، بدون توجه به اینکه چقدر می‌توانید کارها را بهتر سازید، هنوز هم باید با عیب‌یابی عکس‌العملی هنگام وقوع چیزهایی که مطابق برنامه پیش نمی‌روند، استفاده کنید. همزمان که مرتباً روی عیب‌یابی فعالانه خود از طریق مستندسازی، بررسی شبکه و طرح‌ریزی ادامه می‌دهید، مرتباً به صورت عکس‌العمل عیب‌یابی می‌کنید. این اجتناب‌ناپذیر است.

حتی با اینکه ترجیح می‌دهیم قبل از آغاز مشکلات با آموختن علل وقوع آنان و ایجاد سیاست‌ها و روال‌هایی از اجتناب از آنان در آینده جلوگیری کنیم، حتی با اینکه این چنین می‌کنیم، باز هم مشکلات جدید راهی برای خودنمایی پیدا می‌کنند. عیب‌یابی‌های فعالانه و عکس‌العملی، تنها ابزار این بازی هستند. استفاده از هیچ یک از آنان به پایان نمی‌رسد؛ تنها کاری که می‌توان انجام داد، آسانترکردن آنان است.

بر همین اساس، در این فصل، مبانی چگونگی شروع عیب‌یابی مشکلات شبکه‌ای به روش عکس‌العملی را دوباره بررسی می‌کنیم. این مشکلات ممکن است به برنامه کاربردی پروتکل شبکه یا شبکه فیزیکی مربوط باشند. این حالت به شما اجازه می‌دهد بدون توجه به ترکیبات شکل و تئوری نهفته در آن، بتوانید آن را بیابید.

هیچ کتابی نمی‌تواند در چنین نبرد شبکه‌ای، آسوده خاطر مطلقی را ایجاد کند. با روشن‌ترشدن این موضوعات برای شما و آغاز مشکل‌دهی مجموعه عادات عکس‌العملی عیب‌یابی، کم‌کم درمی‌یابید که هر چند که مشکل مرموز باشد، با ادامه کار شما، کمک صورت زشتش را بیرون می‌آورد. با عادی‌شدن این گونه مسائل، سطح اضطرابتان طی تشخیص مسأله به میزان محسوسی کاهش می‌یابد.

تعیین حوزه ناقص : «در آغاز ...»

بجز وقتی گوی کریستالی یا نوعی نرم‌افزار مدیریت شبکه داشته باشید، اولین منبع خبریتان، خبر خرابی شبکه، هیچ ارتباطی به شبکه ندارد و کاملاً از طریق تلفن اعلام می‌شود. بخصوص اگر سازمان‌تان چندین سایت یا چندین بخش

شبکه‌ای داشته باشد، تنها شما نیستید که از خرابی شبکه رنج خواهید برد؛ بنابراین، تا هنگامی که کسی (یا چیزی) شما را در جریان نگذارد، نخواهید دانست چه اتفاقی در شرف وقوع است.



یادداشت : *نرم‌افزار مدیریت شبکه را در فصل ۲۲ توضیح خواهم داد. فعلاً، فرض می‌کنیم از چنین نرم‌افزاری استفاده نمی‌کنید و برای در جریان گرفتن بروز هر مشکل در شبکه به تلفن اتکا نموده‌اید.*

ابتدا، باید از تلفن‌کننده بپرسید که آیا سایر افراد و کاربران هم همین مشکل را دارند. ممکن است برای دریافت جواب این سؤال، مجبور باشید وی را «غلغلک» بدهید؛ او به خاطر مشکل پیش آمده ناراحت است، ممکن است بخشی از کارش را ازدست داده باشد و یا ممکن است با محدودیت زمانی انجام روبه‌رو باشد و غیره. باید مؤدب اما محکم باشید ـ نمی‌توانید در صورت عدم شناخت از میدان مشکل، کمکی فراهم کنید. اگر سایر کاربران نیز همان مشکل را دارند، مشکل، از نوع سیستماتیک است ـ یعنی، می‌توان مطمئن بود که تمامی PC ها در یک شکل و یک زمان، با هم خراب نشده‌اند. بنابراین، پاسخ را می‌توان در چیزی یافت که همه PC ها در آن مشترک هستند ـ «چسب» شبکه‌ای مشترکشان. در اینجا فهرستی را می‌بینید، که از اقلامی تشکیل شده که به صورت معمول و گسترده، برای اتصال PC ها به‌کار می‌روند (از «محلی‌تر» به «گسترده‌تر»).

- هاب‌ها
- سوئیچ‌ها
- مسیریاب‌ها
- سرویس‌دهنده‌ها

اگر خوش‌شانس باشید، ۹۰ ثانیه اول مکالمه، نهانگاه مشکل را به شما می‌نمایاند، که خوب، کاملاً آرام‌بخش است. بعد از دانستن نوع مشکل، عیب‌یابی «مواظبت» از خود را به عهده می‌گیرد. اگر بدانید مشکل سیستماتیک است، برخی اوقات می‌توانید تکنیک‌های مورد بحث در فصل ۴، روش ناپلئون. تفرقه بینداز ـ و ـ حکومت کن»، را تمرین کنید. اگر تشخیص دادید که مشکل محلی است (مربوط به یک PC)، می‌توانید آسوده باشید ـ حداقل با افراد زیادی مشکل ندارید. از آن گذشته، اگر از تکنیک‌های ثبات شبکه که در فصل ۱۶ توضیح دادیم، بهره کافی برده باشید، شانس برگرداندن و حل سریع مشکل، بسیار بالا خواهد بود.

شیرجه به درون جزییات

برخلاف تمایل همگی‌مان به ایده‌آل‌بودن، همیشه هم به موقعیت‌های آسانی برخورد نخواهیم کرد. برخی اوقات، شبکه برای تمام افراد خراب نیست. اگر فراساختار شبکه به صورت کامل، نادرست رفتار نکند، برخی ازتماسهای کاربران، حاکی از دریافت خطاهای عملیاتی مختلف خواهد داشت. شاید کاربری گزارش دهد که چاپی را انجام داده، اما خروجی‌ای بیرون نیامده است.



یادداشت : *برخی مشکلات شبکه‌ای، به صورت مستقیم، ارتباطی با پروتکل شبکه یا صفات فیزیکی شبکه ندارند. این مشکلات بیشتر در زمره مشکلات کاربردی جای می‌گیرند، چه برنامه‌های سرویس‌گیرنده/سرویس‌دهنده باشند و چه برنامه‌های چاپ و فایل. در فصل ۱۸، مقادیر زیادی عیب یابی کاربردی انجام خواهیم داد.*

جمع‌بندی یک راه حل : تکنیک‌های اولیه مدیریت تماس تلفنی

اجازه دهید در مورد تکنیک‌های اولیه مدیریت تماس تلفنی را که هنگامی که تصویر واضحی از رویدادها عرضه نمی‌شود، می‌توان به‌کار بست، صحبت کنیم. با فرض اینکه کاربر مخاطب، مشکلات کاربردی نامعینی دارد، چگونه می‌توانید اطلاعات بیشتری را به‌دست آورید؟ استفاده از تئوری SOAP را فراموش نکنید ـ در نظرگرفتن بیشترین تعداد واقعیت، در مورد هر مشکلی می‌تواند چاره‌ساز باشد. تا آنجا که می‌توانید، از کاربر سؤالات بامفهوم و واقعی برسید. مثالهایی از این دست سؤالات عبارتند از:

- چه اتفاقی افتاد؟
- چه هنگام؟
- در حین چه کاری؟ در شرایطی که برنامه‌ها بارگذاری شده بودند؟
- درست قبل از بروز مشکل، چه‌کار می‌کردید؟
- آیا زمان تلف‌شده‌ای وجود داشته؟
- آیا قبلاً اتفاق افتاده بود؟ چگونه مشکل برطرف شد؟



نکته : *پرسیدن در مورد نمونه‌های قبلی مشکل فعلی، بسیار مهم است. برخی اوقات، تاریخچه مشکل، آن را در مرکز توجه شما قرار می‌دهد. برای مثال، ممکن است شخصی به شما بگوید که مشکل هر هفته در یک زمان پیدا می‌شود ـ که این خود راهنمای خوبی است. برخی اوقات، حتی ممکن است کاربر بتواند بگوید چگونه دفعه قبل مشکل مرتفع شد. یکی از دوستان پزشکم می‌گوید تاریخچه نُه‌دهم معاینه است؛ خیلی بی‌راه نمی‌گوید.*

کل این فرآیند ـ بخصوص اگر در محل ایستگاه کاری مخاطب نباشید ـ ممکن است مثل گشتن در تاریکی به نظر برسد. اگر مبنایی برای سؤالات خود نداشته باشید، مشکل خواهد بود سؤالات مناسبی را انتخاب کنید. برخی اوقات، ساده‌تر آن است که آن را برای خود مطرح کنید (بخصوص، هنگامی که مشکل، از نوع محلی آن باشد). البته قبل از انجام این کار، بهتر است تلاش کنید مشکل را روی دستگاه خودتان مجدداً ایجاد نمایید.

برای مثال، برای کنارگذاشتن احتمال خطای اپراتوری، می‌توانید از کاربر آن سوی خط، بخواهید که ایستگاه‌کاری مشکل‌زا را مجدداً راه‌اندازی کند. بعد از خاموش‌کردن دستگاه، از وی بخواهید که در هر مرحله از فرایند راه‌اندازی به شما بگوید که چه اتفاقی رخ می‌دهد. هنگامی که زمان اجرای برنامه کاربردی فرامی‌رسد، همان برنامه کاربردی را روی ایستگاه‌کاری خود به اجرا درآورید و از کاربر بخواهید کارهایی را که به وقوع خطا منجر می‌شوند را توضیح دهد؛ در عین حال، همان کارها را برای خود انجام هید. این فرایند، کمی حساس است و به تمرین نیاز دارد، بخصوص اگر یکی از طرفین با برنامه کاربردی آشنا نباشند.

گزینه بهتر، بخصوص اگر برای دستیابی به ایستگاه‌کاری کاربر، لازم است کل شهر را بپیمایید، بررسی کاربرد یکی از بسته‌های کنترل از راه دور شبکه، نظیر موارد زیر می‌باشند:

- PCAnywhere
- ReachOut
- RemotelyPossible
- Novell Z.E.N. Works Remote Control
- Microsoft SMS Remote Control

این بسته‌های نرم‌افزاری، به شما اجازه می‌دهند، آنچه را که کاربر در آن سو در حال انجام است دقیقاً مشاهده کنید که می‌تواند بسیار بسیار مثمر ثمر باشد. برخی اوقات، کافی است آنچه را که کاربر انجام می‌دهد تصحیح کنید. در غیر این صورت، حداقل می‌توانید متوجه شوید، مشکلی که وی مخابره می‌کند، واقعی است.



***یادداشت :** البته، برنامه کنترل از راه دور شبکه اگر ایستگاه‌کاری با شبکه صحبت نکند، به‌کار نمی‌آید، پس ممکن است بهتر باشد بخواهید مهارتهای عیب یابی تلفنی خود را تقویت نمایید.*

مشکلات پروتکلی

اگر فکر می‌کنید که برنامه کاربردی به درستی نصب شده، ولی ایستگاه‌کاری، قربانی ضعف چسب شبکه‌ای گردیده است، لازم گامهای عیب‌یابی اولیه پروتکلی را طی کنید تا اطلاعات بیشتری را جمع‌آوری نمایید. من اصولاً این اندازه‌گیری را به صورت طبیعی انجام می‌دهم، بنابراین قبل از دریافتن این اطلاعات، تصور نمی‌کنم که تصویر کاملی را پیش‌رو دارم.



***یادداشت :** این بحث در قالب یک PC ویندوزی صورت می‌گیرد، اما مراحل یادشده را می‌توان در هر نوع ایستگاه‌کاری به‌کار برد ـ تنها کافی است دستورات اندکی متفاوت را به‌کار برید.*

TCP/IP

اگر از TCP/IP استفاده می‌کنید، مراحل یادشده در فصل ۱۲ ، «مبانی شبکه در یونیکس» به‌کار خواهند آمد.

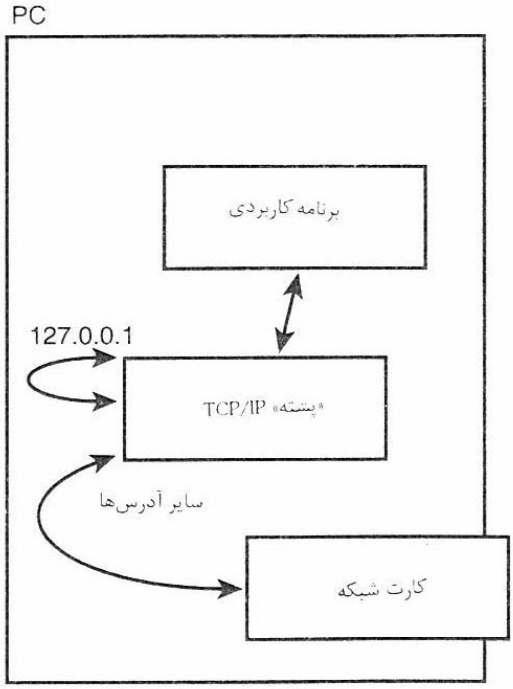
گام ۱ : آدرس بازگشت حلقه را ping کنید

ابتدا باید PC کاربر و منبع مورد نظر وی در شبکه را روی نقشه شبکه معین کنید. بهتر است به آن ایستگاه‌کاری مراجعه کنید و ببینید که آیا می‌توانید آدرس بازگشت حلقه (127.0.0.1) را ping نمایید.



***یادداشت :** همان‌گونه که تاکنون دریافته‌اید، آدرس بازگشت حلقه، از امکانات خاص یونیکس نیست. هر ایستگاه مجهز به TCP/IP، یک آدرس بازگشت حلقه معادل 127.0.0.1 دارد. این آدرس نقشی نظیر اتصال بازگشت حلقه که در فصل ۸ از آن سخن راندم داراست و این امکان را فراهم سازد که برنامه*

پروتکل IP، بدون هیچ نفوذ خارجی مثل کارت شبکه، با خودش صحبت کند.
هوم؟ بدون کارت شبکه؟ چگونه می‌توان بدون کارت شبکه با چیزی صحبت کرد؟ به من اطمینان کنید.
می‌شود، به خاطر اینکه پروتکل TCP/IP (پشته)، برنامه خودش است و همان طور که می‌تواند با کارت شبکه صحبت کند، می‌تواند با خودش هم حرف بزند، همان طور که در شکل ۱-۱۷ ملاحظه می‌کنید.
این کار، کنارگذاشتن احتمال خرابی پشته یا محیط PC را به عنوان منبع مشکل، میسر می‌سازد.



شکل ۱-۱۷ : پشته TCP/IP دستگاه شما می‌تواند با خودش صحبت کند و به شما اجازه دهد ظن خود رااز محیط PC به عنوان یکی از منابع مشکل برطرف سازید.

گام ۲ : آدرس IP ایستگاه‌کاری را ping کنید

در گام بعد، آدرس IP ایستگاه‌کاری را ping نمایید. اگر نمی‌دانید که این آدرس چیست، نگاهی به خروجی دستور Winipcfg بیندازید (این دستور ممکن است چیز دیگری را نیز روشن کند: آیا با کمبود اجاره‌نامه‌های میدان DHCP مواجه شده‌اید؟ آیا سرویس‌دهنده DHCP پایین است؟).

ممکن است یک خطای سخت‌افزاری در انجام هریک از این دو ping محلی رخ دهد، که به معنای آن است که با مشکلی سخت‌افزاری روبه‌رو هستید. در این حال، لازم است برنامه تحلیل‌گر کارت شبکه که با کارت شبکه عرضه می‌شود را به اجرا درآورید.

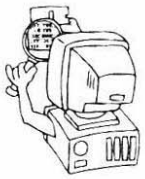


نکته : *اگر نتوانید آدرس IP ایستگاه‌کاری را pingکنید، شاید کاربر از پیغام خطای اولیه ویندوز که نشان‌دهنده وجود تداخل آدرس IP و غیرفعال‌کردن پروتکل توسط ویندوز بوده است، چشم‌پوشی نموده است ـ بدان معنا که TCP/IPای وجود ندارد! در صورت مشاهده چنین وضعی، بهتر است یکبار دستگاه را مجدداً راه‌اندازی کنید (در فصل ۲۱، نکاتی را در مورد چگونگی شکار یک آدرس IP تکراری با کمک تحلیل‌گر شبکه را نشان خواهم داد).*

گام ۳: آدرس IP ایستگاه‌کاری دیگری را در همان بخش شبکه‌ای ping کنید

اگر توانستید خود ایستگاه‌کاری را ping کنید، ببینید آیا می‌توانید به ایستگاه دیگری در همان بخش از شبکه دسترسی داشته باشد یا خیر. اگر می‌توانید، پس این ایستگاه‌کاری در سطح پیوند داده به خوبی کار می‌کنند؛ یعنی می‌توانند تماسهای محلی را انجام دهند. اگر نه، ممکن است با یک مشکل پیوند داده‌ای مواجه باشید.

آدرس یکی از ایستگاههای آن بخش را نمی‌دانید؟ سعی کنید آدرس انتشاری (آدرس مخصوصی که به تمامی ایستگاههای کاری بخش می‌گوید که جواب بدهند) را امتحان کنید.



نکته : *معمولاً آدرس انتشاری، IP شبکه به همراه 255 به جای شماره گره می‌باشد. بنابراین، اگر آدرس IP شما 192.168.10.5 ماسک زیر شبکه 255.255.255.0 باشد، آدرس گره شما 5 است که در صورت تعویض با 255، به آدرس 192.255.255.10.255 که آدرس انتشاری است می‌رسیم.*

بعد از ping کردن آدرس انتشاری، جدول پروتکل تحلیل آدرس (ARP) را باز کنید (این کار اطلاعاتی در مورد تحلیل آدرس IP ـ به ـ MAC در اختیار می‌گذارد). به این صورت:

```
arp -a
```

اگر پیغام زیر را مشاهده می‌کنید، احتمالاً مشکلی وجود دارد:

```
No ARP Entries Found
```

اگر بقیه افراد این بخش، مشکلی ندارند، کابل و کارت ایستگاه‌کاری را بررسی کنید. در غیر این صورت، چنین خواهید دید:

ورودی

```
C:\>ping 167.195.163.255
```

خروجی

```
Pinging 167.195.163.255 with 32 bytes of dat A
Reply from 167.195.163.255: bytes=32 time<10ms TTL=128
Reply from 167.195.163.255: bytes=32 time<10ms TTL=128
Reply from 167.195.163.255: bytes=32 time<10ms TTL=128
Reply from 167.195.163.255: bytes=32 time<10ms TTL=128
```

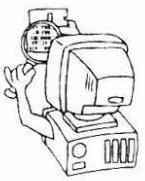
ورودی

```
C:\>arp -a
```

خروجی

```
Interface: 167.195.163.7 on Interface 1
Internet         Address Physical Address Type
167.195.163.3    00.00-c9-ec-7f      dynamic
167.195.163.9    00.00-c9-ec-7f      dynamic
167.195.163.15   00.00-c9-ec-7f      dynamic
167.195.163.17   00.00-c9-ec-7f      dynamic
```

این تکنیک دو کار را برایتان انجام می‌دهد: یکی آنکه فهرستی از آدرس‌های MAP ـ به ـ IP کارآمد را در اختیارتان می‌گذارد، دیگر آنکه می‌گوید این کارت شبکه، در رابطه با پشته TCP/IP درست کار می‌کند.



نکته : *یادداشت‌هایی از چیزهایی که کار می‌کنند و آنها که کار نمی‌کنند و آنها که کار نمی‌کنند بردارید. کم‌کم می‌بینید که تصویر کامل می‌شود.*

گام ۴: مسیریاب بخش را ping کنید

سعی کنید مسیریاب بخش را ping نمایید. به احتمال زیاد، اگر توانسته باشید ایستگاههای بخش را ping کنید، در اینجا هم به مشکلی برنخواهید خورد.

گام ۵: سرویس‌دهنده را هم با نام و هم با آدرس ping کنید

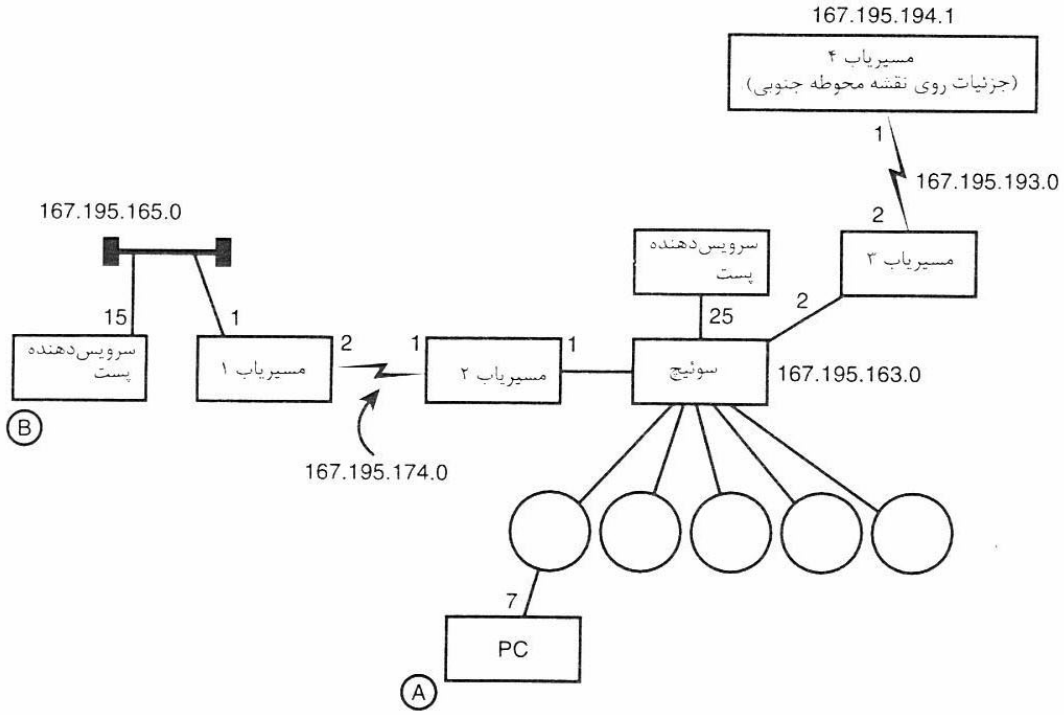
سرویس‌دهنده را با آدرس IP و آنگاه با اسمش ping نمایید. چیز مهمی که باید به خاطر داشته باشید آن است که قبل از بررسی سرویس‌های نام ابتدا باید شماره‌های IP را وارسی کنید؛ در غیر این صورت، ممکن است در موضوعی که به خودی خود پیچیده است، به اشتباه بیفتید.

اگر ping آدرس کار می‌کند، ولی ping نام جواب نمی‌دهد، بهتر است پیکربندی DNS ایستگاه‌کاری یا خود سرویس‌دهنده DNS را بازرسی نمایید.

یادداشت : *در یونیکس و NT، چک‌کردن پیکربندی DNS از طریق ابزار nslookup میسر است (در فصل ۱۹ بیشتر در مورد DNS خواهیم گفت).*

اگر ping آدرس IP کار نمی‌کند، بهتر است "traceroute"کردن آدرس را امتحان کنید. لیست ۱-۱۷ ، tracerouteای صحیح از یک ایستگاه‌کاری سالم به سرویس‌دهنده را نشان می‌دهد (شکل ۲-۱۷).

یادداشت : *دستور traceroute روی بیشتر مسیریاب‌ها و سیستم‌های یونیکس به صورت ذکر شده استفاده می‌شود، اما در ویندوز 95/NT به صورت tracert به‌کار می‌رود.*



شکل ۲-۱۷ : استفاده از دستور traceroute هنگام عیب یابی مشکلات مسیریابی مفید واقع خواهد شد.

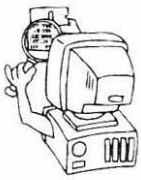
لیست ۱-۱۷ : یک TRACERUTE صحیح

ورودی

```
C:\>tracert 167.195.105.15
```

خروجی

```
Tracing route to mail2.blibdoolpoolp.com [167.195.165.15]
over a maximum of 30 hops:
1 10 ms 10 ms 10 ms 167.195.163.1
2 10 ms 70 ms 61 ms 167.195.174.2
3 10 ms 71 ms 60 ms mail2.blibdoolpoolp.com [167.195.165.15]
```



***نکته** : اگر تنها مسیریابی که به زیر شبکه سرویس می‌دهد، پایین باشد، بسته به تنظیم آن، ممکن است یک پیغام destination unreachable دریافت کنید. در برخی از پیاده‌سازی‌های traceroute، این وضعیت را با N! نشان می‌دهند.*
وقوع این موضوع به خاطر فعال‌نبودن مسیریاب است؛ بنابراین مسیریاب نمی‌تواند پروتکل‌های مسیریابی که شبکه را به سایر مسیریاب‌ها می‌شناسانند، تولید کند. اگر هیچ مسیریابی چیزی در مورد آن نداند و هیچ مسیر پیش‌گزیده‌ای آن را به مسیریاب «مطلع‌تری» عبور ندهد، آنگاه محتمل است که مقصد وجود نداشته باشد.

تمامی مسیریاب‌ها مسیر در خروجی traceroute نشان داده می‌شوند. بدیهی است که در صورت توقف کار traceroute، به احتمال زیاد نقطه شکست را پیدا کرده‌اید. برای مثال، اگر tracereute در لیست ۱-۱۷ در 167.195.163.1 متوقف شود و هرگز جهش بعدی خود (167.195.174.2) را انجام ندهد، احتمالاً در پیوند ناحیه گسترده (شاید شرکت تلفن) مشکلی وجود دارد یا آنکه مسیریاب ۱ خراب شده است. ping موفق 167.195.174.1 و ping ناموفق 167.195.174.2 این موضوع را تأیید می‌کند (همچنین نشان می‌دهد که مسیریاب ۲ کارش را انجام می‌دهد، اما نمی‌تواند با آن سوی پیوند ناحیه-گسترده ارتباط برقرار کند).



***یادداشت** : به خاطر بسپارید که در هر traceroute تنها یک رابط از مسیریاب نشان داده می‌شود. توجه داشته باشید که گزارشی از گذر بسته از 167.195.165.1 یا 167.195.174 وجود ندارد.*

همچنین می‌توانید پیکربندی‌های اشتباه را با دستور traceroute مشخص کنید. برای مثال، اگر سعی کنید سرویس‌دهنده پشتی را traceroute کنید و خروجی زیر را دریافت نمایید، آنگاه مسیریاب ۳ به صورت جدی اشتباه است، اطلاعات پیکربندی خرابی دارد و یا اطلاعات نادرستی را از یکی از پروتکل‌های مسیریابی دریافت می‌کند:

```
c:\>tracert 167.195.165.15
Tracing route to mail2.traceroute.com [167.195.165.15]
over a maximum of 30 hops

1 <10 ms <10 ms <10 ms 167.194.163.2
2 <10 ms 10 ms 10 ms 167.195.195.1
3 <10 ms 10 ms 10 ms 167.195.163.2
4 10 ms 10 ms 10 ms 167.195.194.1
5 10 ms 10 ms 20 ms 167.195.163.2
6 10 ms 20 ms 20 ms 167.195.194.1
7 10 ms 20 ms 20 ms 167.195.163.2
^C
```

در اینجا، مسیریاب ۴ می‌گوید، «هی، این بسته برای من نیست، پسش بگیر!» آنگاه مسیریاب ۳ می‌گوید: «نه عزیزجان، این بسته برای توست!» در این حالت، باید به جداول مسیریابی مسیریاب‌های زیادی نگاه کنید تا بفهمید مشکل چه بوده

است (این حالت را حلقه مسیریابی می‌نامند که اغلب هنگامی رخ می‌دهد که پیکربندی ایستای مسیریاب به صورت اشتباه صورت گرفته است).

IPX/SPX

IPX/SPX پروتکل جمع و جورتر و قابل اطمینان‌تری است. بیشتر عیب‌یابی‌های IPX/SPX به سؤالات «آیا می‌توانید آن را ببینید؟ و «آیا فضای جدول در سخت‌افزار مسیریاب‌ها تمام نشده‌اند» منجر خواهند شد.

اگر در مجموعه کاری خود از ناول استفاده می‌کنید ـ یا حتی اگر از IPX/SPX برای صحبت با سرویس‌دهنده‌های NT استفاده می‌کنید ـ می‌توانید از IPXPING.NIM برای بررسی پاسخ ارسالی از ایستگاههای IPX استفاده کنید. اگر می‌خواهید IPX/SPX را از DOS یا پنجره ویندوز اجرا کنید، بهتر است به سایت ناول:

(http://support.novell.com/cgi-bin/show-file? FileName=ipxpng.exe)

رفته و فایل IPXPING.EXE را دریافت کنید. با این کار، می‌توانید سرویس‌دهنده‌ها یا ایستگاههای کاری را ping نمایید. pin کردن ایستگاه‌کاری برپایه شماره شبکه‌ای IPX آن به همراه آدرس MAC صورت می‌گیرد، مثل این:

```
F:\PUBLIC>ipxping 1d 0000c9108c78
0000001D:0000C9188C76 is alive
```

ping کردن سرویس‌دهنده هم به شکل فوق و هم با استفاده از شماره IPX داخلی منحصر به فردش و استفاده از 1 به ی آدرس MAC میسر است، مثل این:

```
F:\PUBLIC>ipxping ddeeff 1
00DDEEFF:000000000001 is alive
```

اگر از مسیریاب‌های غیرناولی در کار خود استفاده کرده‌اید، باید بدانید که برخی از مسیریاب‌ها محدوده‌های قابل تنظیم دارند. با فرارفتن از این محدوده‌ها، مشکلاتی را تجربه خواهید کرد. اگر بین دو سایت که با مسیریابی سخت‌افزاری به هم متصل‌شده‌اند مشکلی دارید، باید علاوه بر پروتکل‌های آگهی سرویس IPX (SAP) آن را نیز بررسی نمایید. بیشتر مسیریاب‌ها به شما می‌گویند که x ورودی از تعداد y ممکن را استفاده کرده‌اید. اگر x مساوی y باشد، محتمل است در جداول خود سرریزی داشته باشید و لازم باشد که ورودی‌های بیشتری را در برنامه پیکربندی مسیریاب خود اضافه کنید.



***نکته** : بزرگترین مشکلی که در سرریزی‌های جدول SAP مشاهده نموده‌ام، افزودن تعداد زیادی سرویس‌دهنده چاپ مستقل، مثل کارت‌های HP JetDirect می‌باشد. آنها، حضورشان را از طریق انتشار به شبکه اعلام می‌کنند و هر مسیریاب نیز این انتشار را برای مسیریاب‌های دیگر تکثیر می‌کند. بیشتر افرادی که من می‌شناسم، تعداد زیادی چاپگر دارند ـ اگر هر چاپگر یک ورودی SAP داشته باشد، جدول خیلی زود پر خواهد شد.*

علاوه بر پرشدن جدول SAP، ورودی‌های عدیده SAP هم چنین می‌توانند باعث کندشدن WAN شوند. بهتر است مستندات مسیریاب‌تان را برای یافتن راههایی برای فیلترکردن SAPهای ناخواسته انتشار آنان در کل شبکه وارسی نمایید.

می‌توانید اسامی و شماره‌های سرویس‌های IPX/SPX شبکه ناول خود را از طریق اجرای دستور زیر به نمایش بگذارید:

```
display servers
```

به همین صورت، اگر می‌خواهید که آدرس‌ها و کمیت‌های مربوط به شبکه‌های IPX/SPX را مشاهده کنید، می‌توانید دستور زیر را به اجرا درآورید:

```
display networks
```

دستورات خوبی هم هستند که می‌توانند به شما اطمینان دهند که سرویس‌دهنده نت‌ورتان شبکه را به صورت کلی «می‌بیند».

خلاصه

فکر خوبی است که هر روز بتوانید وقت خود را در تقویت مجموعه شبکه‌ای خود صرف نمایید. متأسفانه، واقعیت چیز دیگری را دیکته می‌کند و شما علاوه بر فعالیت‌های عیب‌یابی، باید بدانید چگونه در مقابل مشکلات عکس‌العمل نشان دهید.

بهبودسازی عادات عکس‌العملی، روش خوبی درکاستن سطح استرس و کارامدترشدن شما به عنوان یک عیب‌یاب می‌باشد.

«مکالمه» و استفاده از مهارت در طی تماس کاربری که با شکل مواجه شده است، سهم بزرگی را در تشخیص محلی یا سیستماتیک‌بودن مشکل ایفا می‌کند. برخی اوقات هم لازم است خودتان دست به کار شده، از برنامه کنترلی از راه دور استفاده کنید و یا اجازه دهید که کاربر در ایجاد دوباره مشکل روی ایستگاه‌کاری خودتان، شما را راهنمایی کند.

بعد از آنکه توانستید مشکلات محلی را کنار بگذارید، بهتر است در مورد عادات ارزیابی اتصالات تمرین کنید. ابزاری نظیر ping، traceroute، arp و nslookup در کنار مکانیزم بازگشت حلقه TCP/IP، می‌توانند محل پنهانی مشکل در شبکه را به شما بنمایانند. در طی این مسیر از ابزار بازگشت حلقه به مقصد مورد نظر، اطلاعات مفیدی را در مورد ماهیت مسأله کسب خواهید نمود. همیشه، قبل از دخیل‌کردن سرویس‌های نام در تصویر، به صورت عددی عیب‌یابی کنید تا از پیچیده‌ترشدن موضوع بیش از آنچه که هست جلوگیری کرده باشید.

عیب‌یابی IPX/SPX تا حدود زیادی ساده است و چند وسیله برای بررسی مشکلات اتصالی در دسترس هستند که خیلی سریع مشکل را رو می‌نمایند. برخی از این مشکلات به سرریزی جدول مسیریابی مرتبط هستند و می‌توانید از دستورات مسیریاب یا دستورات سرویس‌دهنده نت‌ور برای نمایش تعداد ورودی‌های مسیر و SAP در شبکه IPX/SPX خود استفاده نمایید.

کارگاه

پرسش و پاسخ

پرسش : اگر من آدرس بازگشت حلقه را ping کنم که موفق‌آمیز نباشد، چه اتفاقی می‌افتد؟

پاسخ : ممکن است لازم باشد پروتکل TCP/IP را از Network در Control Panel حذف نموده و دوباره نصب نمایید. این کار می‌تواند به اصلاح فایل‌های خراب پشته TCP/IP منجر شود. البته، این کار چندان معمول نیست و نشان مشکلات بزرگتری در ایستگاه‌کاری باشد.

پرسش : می‌توانید بیشتر در مورد nslookup توضیح دهید؟

پاسخ : ابزار قدرتمندی است، اما تجربه من نشان می‌دهد که nslookup در محیطهای DNS پیچیده مثل اینترنت مفیدتر است؛ بنابراین در فصل ۱۹ بیشتر از هر جای دیگری در مورد آن صحبت خواهد شد. بیشتر شبکه‌ها کمتر از ۲۰۰ گره دارند و از محیط DNS بسیار ساده‌ای استفاده می‌کنند ـ وارسی پیکربندی ایستگاه‌کاری بعد از انجام یک ping اسمی سمبولیک برای نشان‌دادن مشکلات DNS کافی خواهد بود. دلیل ذکر آن در اینجا تنها به این خاطر بود که ممکن است برخورد با DNS پیچیده‌تر، بخشی از کار عیب‌یابی‌تان باشد.

پرسش : آیا دستورات جمع‌آوری اطلاعات دیگری IPX/SPX وجود دارند؟

پاسخ : بله می‌توانید دستور track on را در کنسول سرویس‌دهنده خود اجرا کنید و مسیرهای IPX/RIP بین مسیریاب‌های IPX را ملاحظه نمایند. این کار بیشتر شبیه به نمایش فرعی می‌ماند (بجز آنکه شما عملاً در جریان کار مسیریابی IPX قرار دارید). بیشتر اوقات، سایر روشهای عیب‌یابی برای حل مشکلات IPX/SPX مناسب‌ترند.

آزمون

۱- درست یا نادرست؟ عیب‌یابی فعالانه کاری است که هنگام تماس تلفنی که مشکلی در شبکه را گزارش می‌دهد، انجام می‌دهید.

۲- عادات عیب‌یابی عکس‌العملی، شامل کدامیک از موارد ذیل هستند؟

الف ـ مصاحبه با کاربران
ب ـ وارسی اتصالات
ج ـ نه الف و هم ب
د ـ هم الف و هم ب

۳- درست یا نادرست؟ دانستن اینکه مشکل قبلاً اتفاق افتاده است، می‌تواند در حل سریعتر مشکل کمک نماید.

۴- کاربری تماس گرفته است و می‌گوید که به هیچ وجه نمی‌تواند وارد شبکه شود. چیز بیشتری را هم نتوانستید از وی کسب کنید. می‌توان ایستگاه‌کاری او را به راحتی از محل خود ping نمایید و ورود به سیستم وی را در فهرست اتصالات سرویس‌دهنده فایل مشاهده می‌کنید. چکار لازم است انجام دهید؟

الف ـ اتصال وی را به سرویس‌دهنده فایل محکم کنید
ب ـ دوباره او را ping کنید
ج ـ گوشی را با عصبانیت قطع می‌کنید
د ـ به ملاقاتش بروید و خودتان ملاحظه نمایید

۵- درست یا نادرست؟ نمی‌توانید ایستگاه‌کاری یکی از کاربران را ping کند، اما می‌توانید با استفاده از برنامه کنترل از راه دور پیکربندی‌اش را مشاهده و تصحیح نمایید.

۶- آدرس بازگشت حلقه در TCP/IP کدام است؟

الف ـ 127.0.0.1
ب ـ 1.0.0.127
ج ـ 128.0.01
د ـ هیچ یک از موارد فوق

۷- یکی از کاربران نمی‌تواند به سرویس‌دهنده SpaceMonkey وصل شود؛ ping به SpaceMonkey از ایستگاه‌کاری وی با شکست روبه‌رو می‌شود. گام بعدی شما چیست؟

الف ـ سرویس‌دهنده دیگری را ping می‌کنید تا مطمئن شود SpaceMonkey غیرفعال نیست.

ب ـ آدرس بازگشت حلقه SpaceMonkey را ping می‌کنید.

ج ـ آدرس IP عددی SpaceMonkey را یافته و سعی کنید. یا آن ping را انجام دهید.

د ـ آدرس بازگشت حلقه SpaceMonkey را پیدا می‌کنید و سعی می‌کنید با آن ping را صورت دهید.

۸- آدرس TCP/IP من 200.1.1.55 می‌باشد و ماسک شبکه‌ام نیز عبارت است از 255.255.255.0. آدرس انتشاری‌ام چیست؟

الف ـ 200.1.255.255 ب ـ 200.1.1.255

ج ـ 200.1.1.0 د ـ 200.1.0.0

۹- بعد از ping کردن آدرس انتشاری، از چه دستوری برای مشاهده جدول متناظر آدرس MAC به IP استفاده می‌کنید؟

الف ـ netstat -a ب ـ traceroute -a

ج ـ arp -a د ـ ping -a

۱۰- traceroute مشخص نموده که ایستگاه‌کاری نمی‌تواند از جهش سوم فراتر رود. مشکل ممکن است در کجا باشد؟

الف ـ مسیریاب موجود در جهش سوم ب ـ مسیریاب موجود در جهش چهارم

ج ـ مسیریاب موجود در جهش پنجم د ـ مسیریاب موجود در جهش دوم

پاسخ به سؤالات آزمون

۱- نادرست ۲- د

۳- درست ۴- د

۵- نادرست ۶- الف

۷- ج ۸- ب

۹- ج ۱۰- ب

فصل ۱۸

«افراد مختلف بسیار در همسایگی شما»: عیب‌یابی عمقی کاربردی

متأسفانه، بیشتر مشکلات با عباراتی نظیر «نمی‌توانم پایگاه اطلاعاتی مشتریان را به خاطر مجوزهای فایلی ناکافی به‌روز درآورم یا «یک خطای جمع بررسی‌کننده شبکه‌ای به خاطر کُد مسیریاب نامناسب چاپ فایل مرا تحریف می‌کند» گزارش داده نمی‌شوند (کاش این طور بود!). بیشتر اوقات، علاوه بر مکانیزهای عمومی عیب‌یابی در بخش دوم و تکنیک‌های بررسی اولیه کاربردی ،که در فصل ۱۷، «از کجا شروع کنم؟»، مورد بحث قرار گرفتند، لازم است بررسی‌های مخصوصی در سطح کاربرد انجام دهید.

در این فصل، همسایگی شبکه را مورد بررسی قرار می‌دهیم تا از آن برای تشخیص محل نهفتن مشکل شبکه‌ای یک برنامه کاربردی استفاده نماییم. در مورد شبکه‌سازی چاپ و فایل، تفاوت آن با/از شبکه‌سازی سرویس‌گیرنده/سرویس‌دهنده صحبت خواهیم کرد و در مورد مشکلات عمومی بحث نموده و تکنیک‌هایی را برای هر دو بررسی خواهیم کرد.

تعاریف سرویس‌ها

دو نوع سرویس وجود دارند که سرویس‌دهنده می‌تواند در اختیار ایستگاههای کاری بگذارد:

- فایل و چاپ
- سرویس‌گیرنده/سرویس‌دهنده

این موضوعات، عناوین بخشهای بعدی را تشکیل خواهند داد.

سرویس‌های فایل و چاپ

هنگامی که بیشتر افراد در مورد روشهای عمومی شبکه‌سازی و اشتراک فایل‌ها فکر می‌کنند، سرویس‌های فایل و چاپ مدنظرشان است. این همان روشی است که کاربران ویندوز دیسک سختی را با سایر کاربران به اشتراک می‌گذارند و اجازه می‌دهند که آنان از یک طرف گردونه‌ای را در PC خود برای دسترسی به دیسک‌گردان شبکه‌ای، بهره ببرند.

سرویس‌های فایل و چاپ امکان انتقال کل فایل‌ها را در شبکه میسر می‌سازند ـ همین. هیچ نوع «هوشمندی» در آن سوی ارتباط و در سرویس‌دهنده وجود ندارد؛ نمی‌تواند فایل یا فایل‌ها را به آن صورت که Yahoo و یا AltaVista انجام می‌دهند، جستجو نماید. شبکه‌سازی از نوع فایل و چاپ، سرویس ساده‌ای را برای انتقال فایل فراهم می‌سازد.

برای مثال، تمامی برنامه‌های کاربردی که می‌توانند با استفاده از سرویس فایل و چاپ از شبکه به اجرا درآیند، لازم دارند که فایل‌های کاربردی در حافظه کامپیوتر شما کپی شده باشند.

به همین شکل، اگر می‌خواهید محتویات فایلی را هنگام استفاده از شبکه‌سازی فایل و چاپ جستجو کنید، باید ابتدا کل فایل را از طریق شبکه منتقل نموده و آنگاه از برنامه‌ای برای انجام جستجو بهره برید. نارسا به نظر می‌رسد، نه؟



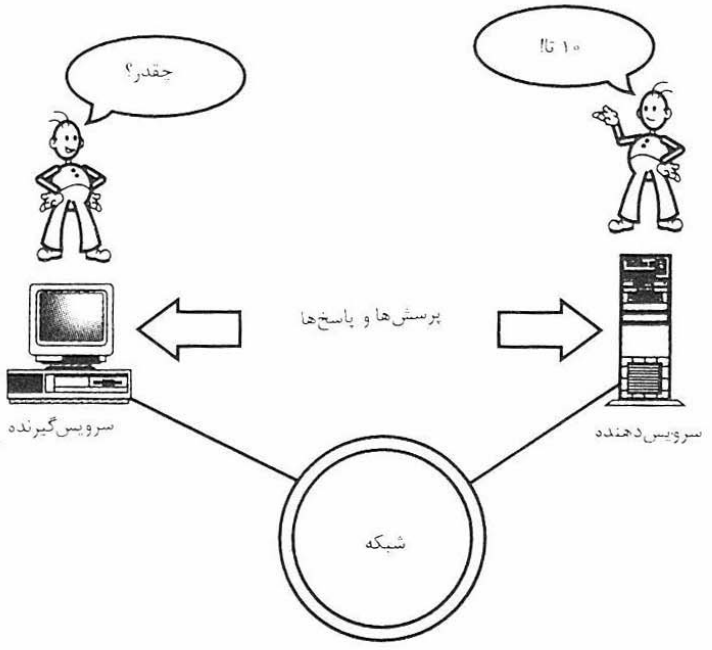
یادداشت : *تنها به عنوان کنجکاوی ـ و اعتراف ـ یکبار سربار ترافیک شبکه‌ای انتقال فایل‌های مربوط به نگارشی از WordPerfect را اندازه گرفتم: در حدود 14MB.*



یادداشت : *در واقع، برخی برنامه‌های پایگاه اطلاعاتی فایل و چاپ می‌توانند قطعاتی از فایل (یا رکوردها) را تشخیص داده و مطالبه کنند، اما آن را برای انجام این کار، بدون درنظرگرفتن اینکه برنامه چقدر ایندکس دارد، باید به منظور پیداکردن اطلاعاتی درخواستی شما، این قطعات و برشهای فایلی را پیمایش کنید.*

محاسبات سرویس‌گیرنده/سرویس‌دهنده

برعکس، محاسبات سرویس‌گیرنده/سرویس‌دهنده به هوشمندی بیشتری در سرویس‌دهنده نیاز دارد. در اینجا دیگر توانایی گره‌زدن فایل به نقاله شبکه و هل‌دادن آن به سوی شما کافی نیست. همان طور که در فصل ۱۲، «مبانی شبکه در یونیکس» مورد بحث قرار دادیم، سیستم‌های سرویس‌گیرنده/سرویس‌دهنده می‌توانند به سؤالاتی پیرامون قیمت، از کاتالوگی از اقلام پاسخ گویند. برای مثال، سیستم سرویس‌گیرنده/سرویس‌دهنده به جای آنکه مثل سرویس‌دهنده فایل و چاپ، کل کاتالوگ را پیش رویتان قرار دهد، مؤدبانه به پرسش‌تان در مورد هزینه یکی از ابزار گوش می‌دهد، در پایگاه داده‌ای محلی خود جستجویی را صورت می‌بخشد و آنگاه مطابق شکل ۱-۱۸ پاسخ را اعلام می‌کند.



شکل ۱-۱۸ : می‌توانید در مورد روش سرویس‌گیرنده/سرویس‌دهنده این گونه تصور کنید که دو انسان هوشمند در دو سوی خط مکالمه نشسته‌اند. سرویس‌گیرنده سؤالات سرویس‌دهنده پاسخها را فراهم می‌سازند.

سیستم سرویس‌گیرنده/سرویس‌دهنده دیگر چه‌کار می‌تواند بکند؟ خوب، اول مرورگر وِب خود را در نظر بگیرید. این برنامه، سرویس‌گیرنده یک ارتباط سرویس‌گیرنده/سرویس‌دهنده است. سرویس‌گیرنده می‌گوید: «سلام، صفحه وِب پیش‌گزیده‌ات را به من بده» و سرویس‌دهنده آن را به سرویس‌گیرنده می‌دهد (در ادامه این فصل بیشتر در این رابطه خواهیم گفت).

به علاوه، روش سرویس‌گیرنده/سرویس‌دهنده را هنگام ارائه اطلاعات لازم به جستجوی Yahoo مورد استفاده قرار می‌دهید. اگر از XWindow یا برنامه‌های کاربردی جاوا استفاده می‌کنید، در واقع نهایتاً از سرویس‌دهنده/سرویس‌گیرنده استفاده نموده‌اید. البته، برنامه‌نویس روی سرویس‌دهنده می‌تواند پیچیده باشد (با اینکه نمی‌خواهم وارد جزئیات شوم، اما دانستن آن مفید است که - بدون درنظرگرفتن هر واژه‌ای - هر گونه ارتباط سوکتی بین سرویس‌گیرنده و سرویس‌دهنده را می‌توان در مورد رابطه‌ای از نوع سرویس‌گیرنده/سرویس‌دهنده طبقه‌بندی نمود).



یادداشت : *ارتباطات سطح بالاتر و پیچیده‌تری هم هستند که در سرویس‌گیرنده/سرویس‌دهنده ریشه دارند. برای مثال، آیا سرویس‌گیرنده‌های فایل و چاپی که روی ایستگاه‌کاری‌تان بارگذاری می‌کنید، می‌شناسید؟ Client for Microsoft Networks و Novell InteranetWare Client32؟ واضح است که آنها با سرویس‌دهنده ارتباط برقرار نموده، از آن سو سؤالاتی می‌کنند و پاسخ‌ها را می‌گیرند. این به معنای سرویس‌گیرنده/سرویس‌دهنده‌بودن آنهاست، درست است؟ حقیقتاً این طور است، اما آنها روش پشرفته و به اندازه کافی پیچیده خود را دارا هستند.*

مشکلات فایل و چاپ

سرویس‌گیرنده فایل و چاپ را فروشنده آن فراهم می‌کند که می‌توانید روی ایستگاه‌کاری خود بارگذاری نمایید (اغلب، سرویس‌دهنده، برنامه تنظیمی‌ای دارد که به صورت خودکار سرویس‌گیرنده را روی ماشین‌تان پیکربندی و بارگذاری می‌کند. جداً آسان است). اولین گام در عیب‌یابی فایل و چاپ، احراز صحت نگارش سرویس‌گیرنده است. باید برای این کار از فروشنده سؤال کنید، اما منظور من از صحت، آخرین نیست. کافی است بدانید که نگارش‌های یکسانی از سرویس‌گیرنده روی دو ماشین کاری قرار دارند (که یکی از آنها خراب است).

سرویس‌گیرنده‌ها چگونه کار می‌کنند؟ حتی با وجود اینکه سرویس‌گیرنده‌ها ممکن است ساده به نظر برسند، واضح است که درونی پیچیده دارند. اجازه دهید به عنوان یک مثال، به سرویس‌گیرنده نت‌ور نگاهی بیندازیم. سرویس‌گیرنده برای آنکه اشتراک فایل و چاپ را برای شما بدون زحمت سازد، باید مواردی نظیر این را انجام دهد:

- ایجاد ورود به سیستم برای شما، یا مجوزگیری، در شبکه
- تعیین محل سرویس‌دهنده در شبکه از طریق پروتکل مرکزی ناول (NCP)[1]
- اتصال به دیسک‌گردان سرویس‌دهنده و آنگاه خواندن و نوشتن فایل‌ها و شاخه‌ها
- اتصال به سرویس‌دهنده و آنگاه انتقال فایل‌ها به صف چاپ سرویس‌دهنده
- ظاهرساختن حرف گردونه یا چاپگر در ایستگاه‌کاری و ایجاد این حالت که فایل در ایستگاه‌کاری قرار دارند، در حالی که روی سرویس‌دهنده قرار گرفته‌اند (تغییر جهت‌دهنده)[2].

1- Novell Core Protocol 2- redirector



یادداشت : *نکته جالب توجه آن است که نگارش DOS سرویس‌گیرنده نت‌ور قبلاً تمامی این امکانات را به صورت مجزا بارگذاری می‌کرد، که به شما این امکان را می‌داد که آنهایی را که می‌خواهید، انتخاب نمایید (و به این ترتیب در حافظه صرفه‌جویی می‌شد). این ماجول، VLMSها یا ماجول‌های قابل بارگذاری مجازی[1] نامیده می‌شوند.*



یادداشت : *نرم‌افزار سرویس‌گیرنده فایل و چاپ به اندازه کافی پیچیده است که به سادگی در اثر مشکلات جانبی حاصل از سایر نرم‌افزارهای ایستگاه‌کاری آسیب می‌بیند. بررسی پیکربندی‌های صحیح ایستگاه‌کاری نیز در عیب‌یابی فایل و چاپ اهمیت ویژه‌ای دارد.*

این بخش عمده مشکلاتی را که ممکن است با آنها در هر سیستم فایل و چاپی برخورد کنید، پوشش می‌دهد:

- مشکلات چاپ
- مشکلاتی با فایل‌ها
- مشکلاتی با برنامه‌های کاربردی

نمی‌توانم چاپ کنم!

اگر سراسر کشور را بگردید و از مدیران یا سرپرستان بپرسید با کدام مشکل شبکه بیش از بقیه برخورد کرده‌اند، شرط می‌بندم که یکی از بیشترین پاسخ‌ها، مشکلات چاپ در شبکه خواهد بود. بنابراین، ما عیب‌یاب‌ها باید بتوانیم برای حل آنها آماده باشیم.



یادداشت : *متأسفانه، منشاء بسیاری از مشکلات چاپی، به خاطر کمبود مستندات چاپگرهاست. هنگامی که به «چاپگر کاربر» اشاره می‌شود، برای افراد همکار معنا دارد، اما برای شما از دیدگاه یک عیب‌یاب، بی‌معناست (مگر آنکه با عبارتی مثل «چاپگر شماره ۱۰ مالی در سرویس‌دهنده PENELOPE" دنبال شود).*

در اختیار داشتن جدولی از دپارتمان‌ها و چاپگرها برخی اوقات مؤثر است، اما برای من راحت‌تر است که برچسبی شامل اطلاعات سرویس‌دهنده/فهرست/صف روی آن نصب کنم. به این شکل، اگر از کاربر بپرسید: «برچسب چاپگر چیست؟» می‌توانید بلافاصله محل آن را به دست آورید.

اجازه دهید نگاهی داشته باشیم به آنچه که چاپ در شبکه اغلب درپی دارد. از طریق مرور سرویس‌دهنده‌ها یا درخت سرویس‌های فهرست به صف چاپگر شبکه متصل می‌شوید و راه‌اندازهای مناسب با آن چاپگر را نصب می‌کنید. تا اینجا شبیه نصب چاپگری می‌ماند که به پورت LPT1 کامپیوتر وصل شده، این طور نیست؟ تنها تفاوت آن است که محلی اسرارآمیز در شبکه را به جای پورتی محلی تعیین می‌نمایید.

هنگام چاپ چه اتفاقی می‌افتد؟ برای پاسخ، اجازه دهید مراحل زیر را ازنظر بگذرانیم.

۱- برنامه کاربردی شما، یک متافایل چاپ را ایجاد می‌کند و آن را به راه‌انداز چاپ می‌فرستند. متافایل، واژه‌ای

1- Virtual Loadable Modules

میکروسافتی است که برای فایل گرافیکی مبنایی عمومی که هم برنامه‌های کاربردی و هم راه‌اندازهای چاپگر می‌دانند چگونه بخوانند، به‌کار می‌رود، آنگاه راه‌انداز چاپگر، فایل را پردازش می‌کند.

۲- راه‌انداز چاپ، متافایل را پردازش می‌کند و نتیجه را در یک فایل آماده چاپ ویژه چاپگر. فایل آماده چاپ[1] جایی است که کار چاپی تا زمان چاپ در چاپگر نگه داشته می‌شود. کلمه به‌کاررفته (Spool) به معنای قرقره است. تصور کنید، قرقره‌ای نخی که به مرور استفاده می‌شود و نخی که در بالای قرقره گرفته، ابتدا چاپ می‌گردد.

۳- چاپچی[2] (برنامه‌ای در کامپیوتر که با فایل‌های آماده چاپ کار می‌کند) با کمک سرویس‌گیرنده فایل و چاپ، فایل آماده چاپ را به صف چاپگر مناسب در سرویس‌دهنده منتقل می‌کند.

۴- سرویس‌دهنده، در صورت مشغول‌بودن چاپگر، فایل آماده چاپ را در شاخه مناسب انتظار، قرار می‌دهد. با فایل‌های آماده چاپ، برمبنای «ورود مقدم، سرویس مقدم» کار می‌شود.

۵- فایل آماده چاپ به چاپگر فیزیکی منتقل می‌شود (یا یک سرویس‌دهنده چاپ شبکه‌ای). این کار در صورت آزادبودن چاپگر (بعد از چاپ سایر کارها) صورت می‌گیرد.

با وجود پنج قطعه پتانسیلی شکست (در برخی حالات، حتی بیشتر)، تعجبی ندارد که مشکلات چاپی زیادی وجود داشته باشند. خوشبختانه، بیشتر این مشکلات را می‌توان با استفاده از روشهای تفرقه بینداز ـ و ـ حکومت کن و خیابان سسمی حل نمود. یعنی، بهتر است ببینید که آیا سایر کاربران می‌توانند روی آن چاپگر چاپ کنند، همچنین آیا کاربری که مشکل را گزارش نموده است، می‌تواند روی چاپگر دیگری چاپ نماید. قصد دارم کل این روال را با شکستن آن به پنج گام عیب‌یابی برایتان ساده کنم.

گام اول : برنامه کاربردی را بررسی کنید

قدم اول هنگام رویارویی با مشکلی چاپی، بررسی برنامه کاربردی است. با اینکه ممکن است ابلهانه به نظر برسد، اما بسیاری از مشکلات چاپی‌ای که ملاحظه نموده‌ام، به خاطر آن بوده که مثلاً، در یک پایگاه داده‌ای اصولاً خروجی‌ای برای چاپگر ایجاد ننموده است. ممکن است تصور شود که سازنده پایگاه داده‌ای، باید اعلام کند که پارامترهای گزارشگیری کاربر، خروجی‌ای را تولید نمی‌کند، بله، اما این همیشگی نیست (می‌توانید صف را غیرفعال کنید و دوباره چاپ را انجام دهید تا ببینید که آیا اصولاً کاری برای چاپگر تولید می‌شود یا خیر).



نکته : *بهتر است ابتدا در مورد کاربر ویندوز ۹۵ چک شود که کاربر ویندوز ۹۵ وارد سیستم شبکه شده باشد.*
ویندوز ۹۵ کاربر را مجاز می‌دارد که با فشردن Esc از پنجره login صرف نظر کند؛ بنابراین، ممکن است کاربر بدون ورود به شبکه بخواهد روی چاپگری شبکه‌ای چاپ کند.

مشکلات پیچیده‌تری هم می‌توانند حادث شوند، مثل وقتی که برنامه کاربردی به شکل نامناسبی پیکربندی شده باشد و یا مشکلات DLL ای داشته باشد که خودشان را به اشکال دیگری نشان نمی‌دهند. برای مثال، برنامه‌ای کاربردی دیده‌ام که به DLL های ویژه‌ای برای چاپ نیاز داشته؛ هنگامی که این DLL ها توسط برنامه دیگری در نگارشهای خاص خود از این

1- spool file 2- spooler

DLL ها را نصب می‌نمود، یا با مشکلات ساده دیسک سخت، خراب می‌شدند، برنامه چاپ را متوقف می‌نمود، حال با وجود آنکه سایر کارهای خود را بی‌عیب و نقص انجام می‌داد.

صحت اینکه مشکل چاپی از برنامه‌ای کاربردی نشأت گرفته را می‌توانید از طریق چاپ از برنامه‌ای دیگر، امتحان نمایید ـ مثلاً Notepad یا WordPad . در یونیکس، دستور ذیل را برای بررسی چاپ خارج از برنامه کاربردی مورد نظر اجرا کنید:

```
lp -dprintername etc/services
```

گام ۲ : بررسی راه‌انداز

اگر دو برنامه در یک ایستگاه‌کاری نتوانند چاپ کنند، ترجیح می‌دهم چاپگر دیگری را وارد صحنه کنم. بخصوص، دوست دارم چاپگری محلی با مقصد LPT1 را تنظیم نمایم. اگر چاپگری به LPT1 چاپگر متصل نشده باشد، ناامید نشوید ـ تنها کافی است مقصد را FILE تعیین کنید، که خیلی ساده باعث هدایت خروجی به دیسک سخت می‌گردد. آنگاه می‌توانید فایل مذکور را بازبینی کنید تا مطمئن شوید اوضاع مرتب است.



نکته : *برای حصول اطمینان از مرتب‌بودن فایل چاپی، می‌توانید آن را به ایستگاه‌کاری دیگری که چاپگری متصل بدان وجود دارد، منتقل کنید و دستوری نظیر ذیل را به اجرا درآورید:*

```
Copy /b PRINTFILE LPT1:
```

برای کنارگذاشتن مشکلات مربوط به راه‌انداز، سعی کنید از راه‌انداز متفاوتی برای چاپگر مورد آزمایش خود استفاده نمایید. ترجیح می‌دهم از حالت «عمومی/تنها متن» برای چنین وضعیتی استفاده نمایم، اما در صورتی که برنامه کاربردی‌تان گرافیکی باشد، این کار غیرممکن است. با کنارگذاشتن احتمال مربوط به راه‌انداز، دیگر مهم نیست که از کدام راه‌انداز چاپی استفاده می‌کنید، چرا که از سالم‌بودن آن مطمئن هستید.



نکته : *برخی اوقات، حتی با وجود سالم‌بودن راه‌انداز، ایستگاه‌کاری شما ممکن است با کمبود «سوخت» مواجه شود، آن هم هنگامی که راه‌انداز، متافایل را پردازش می‌کند. منابع را همان طور که در فصل ۸ مورد بحث قرار گرفت، بررسی نمایید.*

گام ۳: بررسی چاپی

آیا کس دیگری می‌تواند با صف سرویس‌دهنده کار کند؟ در این صورت، اولین حدس شما آن است که مشکل در ایستگاه‌کاری نهفته باشد. در این حالت، بهتر است مطمئن شوم که چاپگر و نحوه تنظیم ایستگاه‌کاری، طوری است که اطلاعات به صف درستی می‌رود و حافظه خود را از دست نداده است.

برای انجام این کار، چاپگر دیگری را روی این ایستگاه‌کاری آماده می‌کنم ـ که به صف سرویس‌دهنده درستی اشاره می‌کند ـ تنها برای اینکه مطمئن شوم. اگر کار نکرد، این ایستگاه‌کاری به هم ریخته است. اگر مؤثر افتاد، یعنی مشکل ممکن است در ایستگاه‌کاری نهفته نباشد؛ احتمالاً بین ایستگاه‌کاری و صف سرویس‌دهنده اولیه مشکلی در رابطه با ارتباطات یا امنیت وجود دارد.

بررسی کنید که آیا می‌توانید به هر شکل دیگری سرویس‌دهنده را ببینید: آیا می‌توانید به آن وصل شوید؟ آن را ping

کنید؟ حقوق امنیتی خود در این صف را بررسی کنید، یا حتی بهتر، سعی کنید با عنوان شخص دیگری، یک کار چاپی برای آن مهیا سازید.

گام ۴: سرویس‌دهنده را بررسی کنید

ممکن است سرویس‌دهنده نشان دهد که فایل آماده چاپ را به خوبی دریافت می‌کند ـ ولی با این وجود، خروجی درستی ایجاد نمی‌گردد. چند چیز ممکن است باعث وقوع این حالت شده باشند که تنها یکی از آنها، اشکالات ارتباطی بین ایستگاه‌کاری و سرویس‌دهنده است. در چنین موقعیتی ممکن است بخواهید مشکل ارتباطی را از مظان اتهام کنار بگذارید.

یکی از روشهایی که می‌توانید با آن صحت سالم‌بودن فایل آماده چاپ که سرویس‌دهنده دریافت می‌کند، بررسی کنید، آن است که درست هنگام دریافت توسط سرویس‌دهنده نگاهی به آن بیندازید. برای انجام این کار باید چاپگر مورد نظر را در حالت غیرفعال قرار دهید، چرا که سرویس‌دهنده بعد از آنکه فکر می‌کند چاپگر پردازش فایل آماده چاپ را به پایان برده است، آن را پاک می‌کند. به خاطر بلوکه‌کردن چاپگر، فایل‌های آماده چاپ به حال خود رها می‌شوند. آنگاه می‌توانید نگاهی به فایل آماده چاپ تحویل داده‌شده به سرویس‌دهنده بیندازید. اما فایل‌های آماده چاپ در کجا قرار دارند؟ ایده اولیه را می‌توانید از جدول ۱-۱۸ بگیرید.

جدول ۱-۱۸ : مقرهای فایل آماده چاپ

سیستم‌عامل	محل نگهداری فایل‌های آماده چاپ
Windows 9x	%WINSYSIR%\spool\printers\jobnum.spl
Windows NT	%SYSTEMROOT%\system32\spool\printers\jobnum.spl
(Intra)NetWare	QueueVol:SYSTEM\QUEUENUM.QDR
UNIX	/usr/spool/lp/requests (فایل‌های صف)
	/usr/spool/lp/requests (فایل‌های کنترلی)

ویندوز

اغلب، متغیر WINSYSDIR% (که می‌توانید با اجرای فرمان set از محل سطر فرمان آن را ملاحظه کنید)، C:\WINDOWS می‌باشد، اما ممکن است چیز دیگری مثل C:\Win95 باشد. به گونه مشابهی در ویندوز NT، SYSTEMROOT% اغلب WINNT است اما چیز دیگری مثلاً ویندوز سرویس‌دهنده پایانه نگارش 4.0، WTSRV باشد. *jobnum* یک عدد تخصیص داده‌شده توسط سیستم است و هر چیزی ممکن است باشد ـ بهتر است در سیستم خلوتی عیب‌یابی را انجام دهید تا مجبور نشوید از بین هزار فایل آماده چاپ، از آن خود را بیابید.

نت‌ور

هر صف به جایی برای ذخیره‌سازی فایل‌های خود نیاز دارد؛ NWAdmin امکان انتخاب یک محل، مثل SPACEMONKEY_SYS را فراهم می‌سازد. *QueueVal* معمولاً یکی از دیسک‌های SYS: روی سرویس‌دهنده است، اما باید جزئیات NWAdmin را برای تعیین محل دقیق صف به‌کار ببندید.

هر صف در نت‌ور هم یک شماره شانزدهی ۸ رقمی منحصر به فرد دارد که در بخش خصوصیات NWAdmin ذکر شده است. کافی است در محل *QUEUENUM* شماره شانزدهی را وارد کنید. برای مثال، ممکن است صف من در SPACEMONKEY_SYS:\system\f00d160d.qdr قرار داشته باشد.

یونیکس

بیشتر انواع یونیکس SVR4 فایل‌های آماده چاپ خود را در اینجا نگه می‌دارند، اما برخی محل دیگری را مورد استفاده قرار می‌دهند، بهتر است مستندات فراهم‌آمده توسط فروشنده را بررسی کنید.

بعد از پیداکردن فایل، با آن چه می‌کنید؟ همیشه با یک ویرایشگر فایل‌های متنی به آن نگاه کنید. اگر با چاپگر لیزری یا جوهرافشان سروکار دارید، به نظر درهم‌وبرهم خواهد آمد. در این حالت بهتر است موقتاً راه‌انداز مربوط به ایستگاه‌کاری را در حالت «عمومی/فقط متن» قرار دهید، مگر آنکه با زبان چاپگر لیزری آشنا باشید. به این صورت، هنگامی که فایل را می‌یابید، می‌توانید آن را بخوانید.

علاوه بر خواندن فایل آماده چاپ روی سرویس‌دهنده و بررسی عدم تکرار الگویی خاص در آن ـ یا چیزی زائد که ممکن است به خاطر مشکلات ارتباطی شبکه به وجود آمده باشد ـ بهتر است اندازه فایل را با منبع آن مقایسه کنید. تنها کافی است دستور DIR را روی اسم مربوطه اجرا کنید و اندازه فایل را با فایل روی ایستگاه‌کاری مقایسه نمایید (برای تعیین مورد اخیر در ایستگاه‌کاری، قبل از چاپ، چاپگر را روی حالت غیرفعال قرار دهید).



***نکته** : در برخی حالات، وجود تفاوت اندکی در اندازه بین دو فایل روی ایستگاه‌کاری و فایل روی سرویس‌دهنده اشکالی ندارد. برای مثال، فیلتر چاپ دروازه یونیکس ـ به ـ نت‌ور ناول یک کاراکتر بازگشت حامل را بعد از هر خط جدید اضافه می‌کند (چیزی که چاپگرهای DOSگونه به آن نیاز داشته و چاپگری یونیکس از آن بی‌نیاز هستند). این بدان معناست که فایل روی سرویس‌دهنده به خاطر وجود این کاراکترها اندکی بزرگتر خواهد بود. البته، در بیشتر مواقع، اندازه متفاوت فایلی، چیز بدی است.*

گام ۵: چاپگر را بررسی کنید

آخرین گام بین خروجی شما و سرویس‌دهنده، پیوند بین سرویس‌دهنده و چاپگر می‌باشد. در بیشتر حالات، اگر پیوند مشکل داشته باشد، همه مشکلات چاپی خواهند داشت. به ندرت ممکن است مشکل به کاربر یا ایستگاه‌کاری مربوط باشد (در واقع باید می‌گفتم هرگز، بخصوص هنگامی مشکلات چاپی عجیبی رخ می‌دهند.).

بنابراین، فرض کنید که کاربری چاپگر PC خود را در تمام دفتر Space Monky به اشتراک گذارده است. Space Monkey و سایر کاربران هردو قادر به چاپ نیستند. ابتدا باید دید خود کاربر می‌تواند چاپ کند. پاسخ آن است که او هم نمی‌تواند.

او از طریق پورت موازی دستگاه خود و یک کابل موازی مستقیماً به چاپگر متصل شده است. کابل مورد استفاده سالم است (این را از تعویض کابل و استفاده از آن در چاپگر شخص دیگر متوجه می‌شوید).

سپس، سعی کنید مستقیماً روی چاپگر چاپ کنید، کلاً از ویندوز دوری کنید. از محل اعلان فرمان، دستور زیر را به‌اجرا درآورید:

```
dir > lpt1;
```

این کار هم، حتی بعد از ری‌سِت‌کردن دستگاه کاربر مؤثر نمی‌افتد. کاملاً مطمئن می‌شوید که پورت LPT1 وی سوخته است. کاربر ناراحت است. خوشبختانه، کارت موازی یدکی به همراه دارید. با تعویض آن، مشکل حل می‌شود. کاربر خوشحال است.



***یادداشت** : یک پیوند ویژه سرویس‌دهنده ـ به ـ چاپگر وجود دارد که مختص سرویس‌دهنده چاپ در شبکه می‌باشد. برخی از آنها طوری پیکربندی شده‌اند که سرویس‌دهنده باشند (سرویس‌دهنده‌های چاپ یونیکس معمولاً این گونه هستند) و بنابراین مستقیماً مورد تماس ایستگاههای کاری سرویس‌گیرنده واقع می‌شوند. بقیه به شکل غیرمستقیم به سرویس‌دهنده متصل می‌شوند و بنابراین بعد از انجام انتقال‌های ایستگاه‌کاری روی فایل صف با سرویس‌دهنده تماس می‌گیرند. (سرویس‌دهنده‌های چاپ شبکه ناول این گونه هستند). برای آنکه بدانید که از چه نوعی استفاده می‌کنید، بهتر است مستندات سرویس‌دهنده چاپ مورد استفاده خود را وارسی نمایید.*



***نکته** : حتی با وجود آنکه نتوانید فرمان :dir > lpt1 را روی سرویس‌دهنده چاپ به نجام برسانید، برخی از چاپگرها یک دکمه دارند (که ممکن است پیداکردن آن مشکل باشد) که باعث می‌شود یک صفحه آزمایشی چاپ شود. آگاه باشید که چاپ این صفحه به معنای توانایی چاپ محلی در این حالت نیست.*

انبوه فایل

مشکلات فایلی را می‌توان در قالب چندین دسته کلاس‌بندی نمود:

- ناتوانی در استفاده از یک فایل (خواندن، نوشتن، حذف)
- مشکلات منابع (فقدان فضای دیسکی)
- مشکلات برنامه کاربردی (آشفتگی و اغتشاش در سلسه مراتب فایل یا خرابی در فایل‌ها).

تکنیک‌های بسیاری را می‌توان برای حل چنین مشکلاتی به‌کار برد؛ تعدد مشکلات نشان‌دهنده تعدد راه‌حل‌هاست.

ممنوع است!

هر مشکل دسترسی فایلی، اغلب خودش را در قالب عدم توانایی خواندن یا نوشتن یکی از کاربران، ظاهر می‌سازد. کاربر ممکن است پیغام ذیل را ملاحظه کند:

This file already open , and can only be opened read-only

این حالت می‌تواند سرمنشأهای مختلفی داشته باشد:

- شخصی فایل را به صورت فقط خواندنی تنظیم نموده است تا از بازنویسی اتفاقی جلوگیری کند.
- کاربر فاقد مجوزهای امنیتی لازم برای دسترسی به فایل است.
- اتصال سرویس‌دهنده کاربر به خاطر خطایی شبکه‌ای (یا هر چیز دیگری) قطع شده است و اتصال مجدد خودکار به خاطر آنکه شخص دیگری ابتدا اتصال را به دست‌آورده با شکست روبه‌رو گردیده است (این حالت نادر است).

فقط خواندنی

وارسی فایل فقط خواندنی آسان است. اگر ایستگاه‌کاری‌تان ویندوز است روی فایل راست کلیک کنید، به Properties رفته و ببینید که آن چک‌باکس Read-Only علامت دارد یا نه. اگر دارد، ممکن است شخصی آن را فقط خواندنی کرده باشد. باید دلیل را بیابید (در همین کادر تبادلی، می‌توانید نام صاحب فایل را ملاحظه کنید).

امنیت

بهتر است که فایل‌ها و شاخه‌های مربوطه را بررسی کنید تا ببینید که آیا کاربر اصولاً می‌تواند به فایل‌های مورد نظر دسترسی داشته باشد یا خیر.

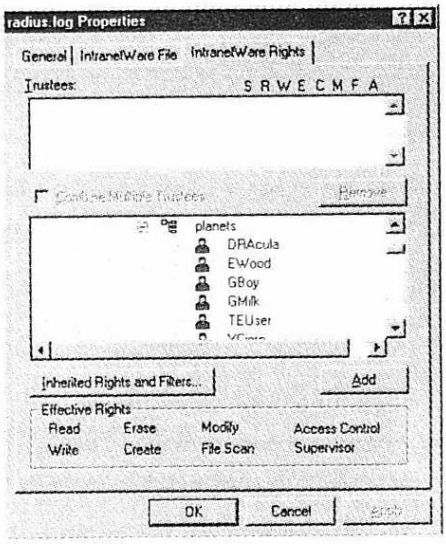
در یونیکس بهتر آن است که خصوصیات کامل فایل را بررسی کنید و مطمئن شود که فایل توسط کاربر مورد نظر قابل خواندن یا نوشتن می‌باشد. مثالی از خواص کامل فایل به شکل زیر است:

```
Is -1a mysecretfile
-rwxrwx- - - 1 monkey root 140 Nov 14 1997 mysecretfile
```

خصوصیات فایل‌های یونیکس حتی در نگارش‌های مختلف آن یکی هستند. سه دسته rwx در سمت چپ قرار دارند که هریک نشان‌دهنده «مجوز خواندن، نوشتن و اجرا» برای هر دسته می‌باشند. اولین دسته، «مجوز کاربر» دومی «مجوز گروه» و سومی مجوز «عمومی» است.

در این مثال، فایل mysecretfile تحت تملک کاربر monkey و متعلق به گروه root می‌باشد. ۱۴۰ بایت طول دارد و آخرین بار در ۱۴ نوامبر ۱۹۹۷ تغییر داده شده است. گروه و کاربر مجوز کامل خواندن، نوشتن و اجرا را دارا هستند، اما از دنیای خارج هیچ‌گونه دسترسی به فایل وجود ندارد.

با استفاده از رومیزی ویندوز، می‌توانید خصوصیات فایل را وارسی کنید. برخی از سرویس‌گیرنده‌های شبکه، نظیر سرویس‌گیرنده ناول، مثل شکل ۲-۱۸ برگه‌ای را به خصوصیات فایل اضافه می‌کنند که در آن مجوزهای فایلی قابل بررسی است. کافی است روی هر فایلی راست کلیک کنید و از منوی ظاهرشده Properties را انتخاب نمایید.



شکل ۲-۱۸ : خصوصیات فایلی، آن گونه که سرویس‌گیرنده اینترانت در ناول در ایستگاه‌کاری ویندوز ۹۵ ارائه می‌کند.

اگر می‌بینید که کاربری به فایل دسترسی دارد، اما کاربر دیگری نمی‌تواند به آن دست یابد، باید گروههایی که کاربران به آنها تعلق دارند را مقایسه کنید. در عمل صلاح نیست مجوزهایی در سطح کاربر را به فایل‌هایی که گروهی از افراد نیاز دسترسی به آن را دارند، اعطا نمود.

وقتی که همه ترفندها با شکست روبه‌رو می‌شوند (و می‌خواهید موهایتان را بکنید)، بهتر است به کاربر ارزش کاربر ویژه اعطا نموده و یکبار دیگر تلاش کنید (انجام این کار در ناول از طریق تخصیص Admin به برگه Security Equivalences در NWAdmin صورت می‌گیرد؛ کاربران NT می‌توانند علاوه بر گروه Domain Administrators به Administrators هم تعلق داشته باشند). اگر توانستید بعد از این کار، موفق شوید، درخواهید یافت که با موضوعی امنیتی روبه‌رو هستید که می‌توانید بعداً آن را دنبال کنید.



اخطار : *هر مسؤول امنیتی در هر کجای کره زمین به خاطر گفتن این موضوع به من حمله‌ور خواهد شد. در این کار خطر وجود دارد. من از تجربه کار کاربران معمولی با عنوان سوپروایزر یا سرپرست سیستم دفاع نمی‌کنم ـ این کار مشکلات جدیدتری را به وجود خواهد آورد (خوشتان می‌آید کاربری دیسک سخت سرویس‌دهنده را پاک کند؟ من که فکر نمی‌کنم).*

حرف من این است که می‌توان به این شکل، مشکلات مربوط به مسائل امنیتی را کنار گذارد. اگر موقتاً به کاربری این حقوق را بدهید ـ و آنگاه بعد از انجام کار و نتیجه‌گیری، آنها را پس بگیرید ـ روشی قدرتمند در محسوب‌کردن (یا نکردن ۹ مشکل روزمره مسائل امنیتی در دست خواهید داشت.

حرف آخر اینکه: تا وقتی که فراموش نکنید که این کار را به صورت موقتی و در زمان کوتاه و حساب‌شده‌ای به انجام برسانید، مشکل پیش نخواهد آمد.

قفل‌ها

قفل‌های فایلی می‌توانند هر نوع مشکل عجیب و غریبی را به وجود آورند. برای مثال، برخی از برنامه‌های تهیه کپی پشتیبان، نمی‌توانند با کاربری که فایلی را باز نگهداشته کار کنند ـ که این مشکلاتی را در کار آنها ایجاد می‌کند. برخی از برنامه‌های پُست الکترونیکی یا موتورهای پایگاه اطلاعاتی حتی هنگام عدم کاربرد، فایل‌های خود را باز نگه می‌دارند ـ که این باعث می‌شود برنامه‌های کپی پشتیبانی هنگام تهیه کپی از آنان چشم‌پوشی کنند. راه‌حل در تهیه یک برنامه پشتیبان است که به مدیر فایل باز مجهز باشد و بتواند از چنین مشکلاتی اجتناب کند (مشکلی که در ناول و ویندوز وجود دارد، اما یونیکس عاری از آن است).

البته، بسیاری از مشکلات که توسط کاربر ایجاد می‌شوند، به فایل‌ها مربوط هستند. مثلاً، تصور کنید که می‌خواهم صبح زود، یک برنامه شبیه‌ساز ترمینال را به‌روز درآورم، مثلاً ساعت 5:30 یا 6:00. سعی می‌کنم که برنامه جدید را نصب کنم اما پیغام خطای Can't Write to file دریافت می‌کنم. برنامه نصب، این گونه اذعان می‌دارد که فکر می‌کند شخص دیگری در حال استفاده از فایل است. به طرز مشابهی، ممکن است یکی از کاربران به من بگوید که می‌خواهد فایلی را به‌روز درآورد، اما WordPrefect به او می‌گوید که وی تنها می‌تواند فایل در حالت فقط خواندنی باز کند. در هر دو این حالت، اگر اسم فایل را بدانم، می‌توانم با استفاده از برنامه‌های کمکی سرویس‌دهنده تعیین کنم چه کسی در حال استفاده از فایل است.

تحت نت‌ور، به منوی File Open|LockActiviy در Monitor رفته و فایل را از میان دیسک‌ها و شاخه‌ها پیدا کند، اتصالات سرویس‌دهنده که قفل‌های فایلی را نشان می‌دهد، به نمایش گذارده می‌شوند. آنگاه به Connection Information رفته و شماره اتصال را بیابید. اسم کاربر را در آنجا خواهید یافت.

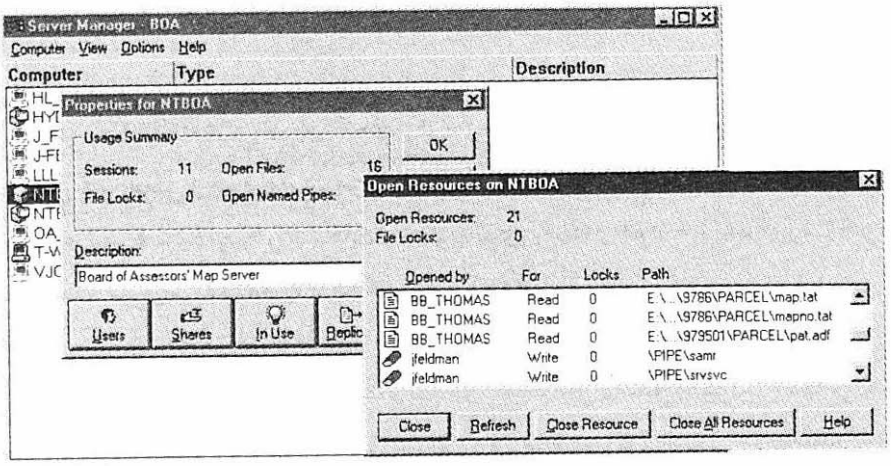
در مورد NT، از Server Manager برای نمایش فایل‌های تحت استفاده بهره جسته، همان طور که در شکل ملاحظه می‌کنید، و آنگاه مراحل زیر را دنبال نمایید:

۱- روی منوی Start کلیک کنید و آنگاه Programs|Administration Tools|Server Manager را انتخاب نمایید.

۲- روی سرویس‌دهنده مورد نظر راست کلیک کنید.

۳- Properties را انتخاب نمایید.

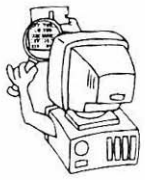
۴- دکمه InUse را فشار دهید.



شکل ۳-۱۸ : Server Manager قادر است فایل‌هایی که (و سایر منابع) روی سرویس‌دهنده NT تحت استفاده قرار دارند، نشان دهد.



یادداشت : *یونیکس فاقد یابنده قفل فایل استاندارد است. می‌توانید با استفاده از دستور fuser (صفحه man مربوطه را ببینید)، تعیین کنید که فایل سیستم توسط چه کسی مورد استفاده قرار گرفته است اما این کار در سطح فایل‌های مستقل عملی نیست.*



نکته : *یکی از کارهای مورد علاقه‌ام هنگام به‌روز درآوری هر برنامه، آن است که آن را به‌روز درنیاورم. فرض کنید که من می‌خواهم برنامه NETTERM را که در شاخه G:\NETTERM قرار دارد به‌روز درآورم. لازم است نگارش جدید را برای استفاده کاربران در آنجا بگذارم. یکی از روشهای مورد علاقه‌ام (که در تمامی موارد به‌کار نمی‌آید، اما در این حالت ساده‌ترین کار است)، تغییر نام شاخه قدیمی است، بدین معنا که برنامه قدیمی را دست نمی‌زنم. به جای آن، برنامه جدیدی را در همان محل نصب می‌نمایم. برای نگهداری از نسخه قدیمی‌تر، از محل اعلان فرمان، دستورات زیر را اجرا می‌نمایم:*

```
G:|> move netterm netterm.old
G:|>mkdir netterm
```

اگر خطایی به وجود آمد و لازم باشد برنامه قدیمی را سریعاً جایگزین کنم، می‌توانم کارهای زیر را صورت دهم:

```
G:|> deltree netterm
G:|> move netterm.old netterm
```

همچنین می‌توانستید این کار را از طریق Explorer به انجام برسانید. فایدهٔ این حالت آن است که قفل‌های فایلی مؤثر واقع نمی‌شود ـ برنامهٔ کاربردی قدیمی به‌روزدرآورده نمی‌شود؛ بلکه برنامهٔ جدیدی در یک شاخهٔ خالی نصب می‌گردد.
نکته‌ای که در این‌جا وجود دارد آن است که باید صفات امنیتی یکسان با شاخهٔ قدیمی را برای شاخهٔ جدید نیز تخصیص دهید؛ در غیر این صورت، هیچ‌یک از کاربرانتان قادر به دیدن آن نبوده و در نتیجه نمی‌توانند آن را مورد استفاده قرار دهند.

پرونده فضای گم‌شده

مهم نیست که چقدر فضای دیسکی دارید، هیچ گاه کافی نیست. حتی با وجود رشد چشمگیر اندازه گردونه‌های دیسک سخت در سالهای اخیر، مقدار اطلاعات چندرسانه‌ای که به صورت برخط ذخیره می‌شوند و اندازه برنامه‌های کاربردی نیز بسیار بیشتر شده است و بنابراین فایل‌های اطلاعاتی آنها فضای بسیار بیشتری را مطالبه می‌کنند. به ویژه اگر سیستمی آموزشی بدون سهیمه فایل داشته باشید (باید گفت که NT فاقد این امکان است)، کاربران هر مقدار فضایی که در اختیارشان قرار دهید به مصرف می‌رسانند.

در حالت کلی، هنگامی که با مشکلات دیسکی روبه‌رو می‌شود، کارها به شکل خردکننده‌ای متوقف می‌شود. توانایی تشخیص بلوک‌سازی فضای دیسکی بسیار مهم است تا بتوان به سرعت جلوی آن را گرفت (کاربران ناول: در فصل ۱۳، چگونگی نظارت برای پیداکردن کاربرانی که فضای دیسکی زیادی را استفاده کرده‌اند نشان داده شده است).



نکته : *سرپرستان سیستم زیادی را می‌شناسم که همیشه از روکردن دست خود طفره می‌روند ـ آنها یک فایل مخفی با اندازه چندین صد مگابایت نگهداری می‌کنند (که هنگام پرشدن دیسک می‌توانند به سرعت آن را پاک کنند)، یا خیلی ساده بلافاصله تمامی فضای دیسکی را تقسیم نمی‌کنند.*
دفترچه‌های راهنمای سیستم‌عامل خود را بررسی کنید؛ روشهایی هستند که نمودی سریع ندارند ولی می‌توان برای افزودن فضای دیسکی آنها را مورد استفاده قرار داد. به طور خلاصه، می‌توان فضای دیسکی را را تخصیص داد و قسمتی از آن را برای استفاده آتی نگه داشت (تحت AIX، Logical VolumeManager و تحت ناول، INSTALL.NLM را ببینید.

در روزی که بدون اشکال فضای دیسکی آغاز می‌شود، این احتمال وجود دارد که باقیمانده فضای دیسکی شما توسط هریک از اقلام زیر مصرف شود:

- فایل‌های بزرگی که آن روز ایجاد می‌شوند.
- تعداد زیادی فایل‌های کوچکتر که در عرض چند روز جمع می‌شوند.
- فایل‌های بزرگی که طی روزهای گذشته ایجاد شده و با انجام فعالیتهای عادی کاربر صحنه را پر می‌کنند.

چگونه چنین اقلامی را می‌یابید؟ اگر مثل بیشتر شرکت‌ها باشید، هزاران فایل و صدها شاخه و زیرشاخه دارید ـ که کار را مشکل می‌سازند. خوشبختانه، ابزار خودکاری در اختیار دارند که می‌توانید به شما کمک کنند.

Find

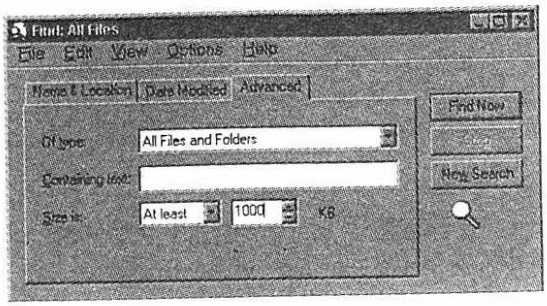
بهترین دوست من در یونیکس، دستور find است. هنگامی که با مشکل کمبود فضا روبه‌رو می‌شوم، می‌توانم دستورات زیر را به انجام برسانم:

```
/full filesystem
nd . -mtime -1 -print | xargs ls - lad | more
```

این یعنی «همه فایل‌ها که در یک تاریخ تغییر کرده‌اند، پیداکن و اندازه و نام آنها را نشان بده، آن هم صفحه به صفحه.
به طور مشابهی، ممکن است دستور ذیل را انجام دهم:

```
find . -size + 2048 -print | xargs ls - lad | more
```

این دستور فایل‌هایی با اندازه بزرگتر از 2048 بلوک (1,048,576 بایت یا 1MB) را پیدا می‌کند.
اگر نتیجه‌ای حاصل نشد، دستور اول را با mtime معادل 3 به جای 1 به‌کار برید. اغلب نتیجه می‌دهد.
ابزار Find در ویندوز ابزار بسیار خوبی است (شکل ۴-۱۸) به شما اجازه جستجو از طریق تاریخ و اندازه داده می‌شود
آیا زمان زیادی طول می‌کشد؟ بله. شاید این دلیل خوبی برای نگهداری مقداری فضای آزاد دیسکی باشد.



شکل ۴-۱۸ : تنظیمات پیشرفته در ابزار Find ویندوز می‌تواند در رهیابی فایل‌های بزرگ (و بنابراین انباره‌های بزرگ فضای دیسکی) کمک خوبی باشد.

آهای! جلوی برنامه نوکرده را بگیرید!

برخی اوقات، پیداکردن فایل‌های مستقل از یکدیگر فایده‌ای ندارد. برای مثال، مسؤول سیستم یونیکس‌مان و من یک صبح دوشنبه می‌خواستیم فایل علت پربودن فایل usr/ را پیدا کنیم. متوجه شدیم که بیشتر فایل‌هایی که در پایان هفته تولید شده بودند، فایل‌های آماده چاپ بودند، پس با متوقف‌کردن چاپچی، حذف وظایف موجود در صف و شروع دوباره چاپ منتظر نشستیم. فایل سیستم در مدت ۱۵ دقیقه دوباره پر شد.

نگاهی به فایل‌های کنترلی چاپچی انداختیم و دیدیم که به یک کاربر خاص تعلق داشتند. لیست پردازش وی را به دست آوردیم:

```
ps -fu mory
```

فرآیند lp که او آغاز کرده بود را از بین بردیم، چاپچی را متوقف و فایل‌ها را پاک کردیم و چاپچی را از دوباره به‌راه انداختیم. بعد از خاتمه پردازشهای آن کاربر همه چیز خوب بود، اما حداکثر نیم ساعت بعد مشکل بروز پیدا می‌کرد.

نتیجه می‌گیریم که: فقط پیداکردن فایل‌ها مهم نیست؛ برخی اوقات باید دلیل به‌وجودآمدن آنها را بررسی نمایید.

جشن برنامه کاربردی

بعضی از برنامه‌های کاربردی، کاملاً پیچیده هستند. برای مثال، برنامه‌های زمان‌بندی و پُست الکترونیکی ممکن است بسیار پیچیده بوده و از فایل‌های پیکربندی، شاخه‌های ورودی، خروجی، مدیریتی و صفوف اضافی و نظایر آنها استفاده نمایند. شناسایی فایلی خراب ـ یا هر علت دیگری در نادرست‌بودن کارکرد ـ ممکن است مشکل و سخت باشد.

برخی از استراتژیهایی که در مواجه‌شدن با مشکلات کاربردی فایل و چاپ به‌کار می‌آیند، عبارتند از:

- بررسی اطلاعات ثبتی در سرویس‌دهنده و برنامه کاربردی
- تعویض و تغییر قواعد (آیا می‌توانید آنها را ساده کنید؟ آیا می‌توان برنامه را جابجا کرد؟)
- بازنشانی از یک نقطه «شناخته‌شده» خوب در زمان مناسب

اطلاعات ثبتی

هر فایل ثبتی اغلب می‌تواند به خوبی داستان را بازگو کند. بهتر است برنامه کاربردی‌تان را در صورت مواجه‌شدن با مشکلات در حالت ثبت وقایع قرار دهید. برای آنکه بتوانید کار لازم بعد از نگاه‌کردن به فایل‌های ثبتی را انجام دهید، لازم نیست در این کار حرفه‌ای باشید ـ همیشه می‌توان پیغام خطای روی وِب را جستجو کنید وقتی در برخی حالات فایل ثبتی عملی را پیشنهاد می‌کند، مثل این:

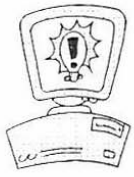
```
file.idx is corrupt -run rebuild process
```

محیط

تغییر محیط کاملاً به حالت جاری بستگی دارد. برای مثال، ممکن است برای کنارگذاشتن مشکلات سرویس‌دهنده، برنامه کاربردی را از سرویس‌دهنده‌ای به دیگری منتقل کنید ـــ اما این کار باید با دردست‌داشتن دلیل کافی مبنی بر اشکال سرویس‌دهنده باشد. اگر مشکلی دارید که به نظر به ظرفیت مربوط می‌شود، می‌توانید برخی از کاربران را به سرویس‌دهنده کاربردی دیگری منتقل کنید.

بازنشانی از یک نقطه شناخته‌شده خوب

اگر روی برنامه کاربردی خبره نباشید، هیچ یک از دو استراتژی اول به‌کار نخواهد آمد، نکته جالب در مورد برنامه‌های کاربردی در سطح فایل آن است که تعمیر آنها از طریق بازنشانی به‌آسانی صورت می‌پذیرد. به نظر می‌رسد که باید محل فایل‌ها را برای بازنشانی بدانید. اگر خودتان برنامه را نصب کرده باشید یا اگر دفترچه راهنما را در اختیار داشته باشید، پیداکردن این اطلاعات چندان مشکل نیست.



***هشدار** : برنامه‌های کاربردی پیچیده برخی اوقات در بیش از یک محل قرار می‌گیرند ـ برنامه کاربردی‌ای که اطلاعات وضعیتی را با محل دیگری تبادل می‌کند، نباید به خودی خود بازنشانی شود. برنامه کاربردی ممکن است به مقدار زیادی به مشکل بیفتد اگر تنها نیمی از مغزش بازنشانی شود.*

مبارتهای عملی

در جایی بودم که هیچ کس برای سیستم پُست الکترونیکی آموزش ندیده بود؛ یعنی، با اینکه هم از آن استفاده می‌کردند، اما هیچ کس برای مدیریت و سرپرستی سیستم آموزش ندیده بود. بنابراین وقتی که یک روز سیستم از

کار افتاد، هیچ کس واقعاً نمی‌دانست که چگونه آن را حل کند.

فایل‌های ثبتی چیز بخصوصی را آشکار نساختند. جستجوی روی وِب هم چیز به‌دست نداد. بخش فنی اعلام نمود که به زودی ـ شاید بعد از ظهر ـ بتواند راه حلی را ارائه کند.

تمامی پرسنل IT در این شرکت، حرفه‌ای‌های آموزش دیده بودند اما برای مدیریت این برنامه کاربردی راه‌کار را نمی‌دانستند، اطلاعات آنها هم برای بررسی این مشکل بی‌فایده بود. اما صبرکردن تمام مدت روز برای بخش فنی، گزینه محبوبی تلقی نمی‌شد.

بعد از بازنشانی از پشتیبان، همه چیز بخوبی کار می‌کرد ـ هیچ کس حتی یک نامه را از دست نداد بود، چراکه مشکل شب هنگام و بعد از اجرای تهیه پشتیبان رخ داده بود. تا به امروز، کسی نمی‌داند مشکل دقیقاً چه بود ـ و کسی اهمیت نمی‌دهد. نتیجه منطقی داستان: کپی‌های پشتیبان خوب، برنده می‌شوند.

سرویس‌گیرنده / سرویس‌دهنده

اساس عیب‌یابی سرویس‌گیرنده/سرویس‌دهنده بر آن است که بررسی شود ارتباطات TCP/IP به صورت صحیح کار می‌کنند و آنگاه اینکه برنامه سرویس‌دهنده در آن سوی خط، پاسخگوی تماس است ـ یعنی سوکت مناسب در پایانه سرویس‌دهنده در حال شنود باشد.

اجازه دهید خیلی سریع تکنیک‌های اتصال در TCP/IP را مرور کنیم:

۱- ping از طریق اسم: آیا اسم قابل تحلیل است؟

۲- ping از طریق آدرس: آیا امروز سرویس‌دهنده قابل دسترسی است؟

۳- استفاده از traceroute: چرا نمی‌توانید به آنجا برید؟ بسته ارسالی در کجا متوقف می‌شود؟

وضعیت آدرس سوکت

عادت کنید که از دستور netstat -a استفاده کنید ـ ابزاری است که در عیب‌یابی برنامه‌های کاربردی سرویس‌دهنده/سرویس‌گیرنده مفید واقع می‌شود. بیایید سریعاً خروجی netstat -a را بررسی کنیم تا ببینیم چه چیزهایی نشانمان می‌دهد:

```
Proto Local Address Foreign Address state
```

- Proto به پروتکل (یا TCP یا UDP) اشاره می‌کند.
- Local Address آدرس و سوکتی است که ایستگاه‌کاری برای صحبت‌کردن مورد استفاده قرار می‌دهد.
- Foreign Address نشان‌دهنده آدرس راه دور و شماره سوکتی است که با آن صحبت می‌کنید.
- State وضعیت سوکت را توصیف می‌کند (به یادداشت ذیل توجه کنید).



یادداشت : *آیا آدرس سوکت محلی مهم است؟ خیر. مثل هر مکالمه تلفنی، هر انشعاب خالی‌ای را می‌توانید برای شماره‌گیری به‌کار ببندید ـ کامپیوتر این کار را به صورت خودکار انجام می‌دهد. آدرس سوکت محلی تنها در صورتی که کامپیوتری که پای آن نشسته‌اید، یک سرویس‌دهنده باشد، اهمیت دارد. در چنین حالتی، باید در شماره سوکت صحیح در حال شنود باشد، در غیر این صورت، هیچ کس نخواهد توانست با آن صحبت کند.*

بسته به سیستم‌عامل، یکی از وضعیت‌های ذیل را در ستون State ملاحظه خواهید نمود:

وضعیت	شرح
LISTENING	«من سرویس‌دهنده‌ام و آماده صحبت می‌باشم»
ESTABLISHED	«من در حال انجام یک مکالمه‌ام»
SYN_SENT	«در تلاشم مکالمه با شخص را همزمان سازم، اما تابحال شانس انجام این کار را نداشته‌ام»
SYN_RECN	«در حال انجام همزمان‌سازی هستم»
CLOSE_WAIT	«از آن طرف ارتباط به پایان رسیده است؛ منتظر آزادشدن خط هستم»
TIME_WAIT	«من قطع می‌کنم؛ موقتاً این ورودی را رها می‌کنم»
LAST_ACK	«از آن طرف خط خداحافظی می‌کنند و به زودی ارتباط قطع می‌شود»
FIN_WAIT1	«سوکت بسته شده است. اندکی این مکالمه را رها می‌کنم»
FIN_WAIT2	«سوکت از سوی طرف مقابل بسته شده است. کمی این مکالمه را به حال خود رها می‌کنم»

سرویس‌های متبسم

در مورد هر سرویس سرویس‌دهنده/سرویس‌گیرنده‌ای، بهتر است که بتوانید به صورت مبنایی وضعیت شنود سرویس‌دهنده را وارسی کنید. این اغلب به معنای تلاش برای ارتباط با آن از طریق یک ماشین سرویس‌گیرنده است. به منظور ایجاد اتصال ـ یا بررسی یک سرویس در طرف سرویس‌دهنده ـ بهتر است علاوه بر نام سرویس‌های شناخته‌شده، شماره آنها را نیز بشناسید.



***نکته** : فهرستی از سرویس‌های در دسترس تحت ویندوز در C:\Windows\Services قرار دارد. محل این فهرست در یونیکس /etc/services و تحت نت‌ور در SYS:ETC\Services می‌باشد. همچنین می‌توانید اطلاعات مختلف مربوط به شماره‌های سرویس‌های استاندارد، شماره‌های شبکه‌ای و نظایر آنها را در http://www.kashpureff.org/nic/rfes/1300/rfc1340.txt.html بیابید.*

جدول ۲-۱۸ مقادیر عددی برخی از سرویس‌هایی که من بسیار با آنها کار می‌کنم نشان می‌دهد (سرویس‌های زیاد دیگری هم هستند).

جدول ۲-۱۸ : مقادیرعددی سرویس‌های پرکاربرد

اسم سرویس	شماره	شرح
FTP	۲۱	پروتکل انتقال فایل (اینترنت)
Telnet	۲۳	سرویس ورود به سیستم برای یونیکس (برخی اوقات NT یا ناول)
SMTP	۲۵	پُست الکترونیکی سرویس‌دهنده ـ به ـ سرویس‌دهنده اینترنت ـ گونه
Domain	۵۳	سرویس‌های DNS (UDP و TCP)
Gopher	۷۰	گوفر اینترنت
HTTP	۸۰	پروتکل انتقال فوق متن (وِب)
POP2	۱۰۹	پروتکل دفتر پستی ـ نگارش ۲ (پُست الکترونیکی کاربر)

ادامهٔ جدول ۲-۱۸ : مقادیرعددی سرویس‌های پرکاربرد

اسم سرویس	شماره	شرح
POP3	۱۱۰	پروتکل دفتر پستی ـ نگارش ۳ (پُست الکترونیکی کاربر)
NNTP	۱۱۹	اخبار USENET
netbios-ns	۱۳۷	سرویس نام NetBIOS
netbios-dgm	۱۳۸	سرویس داده‌گرام NetBIOS (خود داده)
netbios-ssn	۱۳۹	سرویس جلسه NetBIOS (سلام، چطوری؟)
shell	۵۱۴	سوکت Rlogin (یونیکس یا NT)
printer	۵۱۵	دیمون چاپگر خطی (چاپ شبکه برای یونیکس)
socks	۱۰۸۰	سرویس‌دهنده پروکسی Socks (Socks نگارش ۴ و ۵)



نکته : *اگر شماره سوکت برنامه سرویس‌گیرنده/سرویس‌دهنده مورد استفاده خود را ندانید، چه‌کار می‌شود انجام داد؟ ساده است ـ برنامه سرویس‌دهنده را متوقف کنید و دستور* ***netstat -an*** *را به اجرا درآورید. خروجی آن را چاپ کنید یا در فایلی ذخیره کنید:*

```
netstat -an > socklist.txt
```

آنگاه برنامه سرویس‌دهنده را دوباره اجرا کنید و مجدداً ***netstat -an*** *را امتحان کنید. دو لیست را مقایسه کنید. شماره سوکت جدید در لیست دوم، شماره (یا ستاره‌های) سوکت برنامه سرویس‌گیرنده/سرویس‌دهنده‌تان است.*

سوکت‌های اتصال‌گرا و بدون اتصال

همان گونه که در فصل ۱۵ بحث کردیم، برای اهداف مورد نظر ما، دو نوع سوکت وجود دارد: UDP و TCP. هنگامی که برنامه‌ای یک بسته UDP ارسال می‌کند، راهی برای بررسی دریافت بسته در اختیار ندارد، چرا که روش کار بدون اتصال است، مثل پیغامی در یک بطری. از نظر اهداف عیب‌یابی‌ها، از UDP بیزاریم. بچه مسؤولیت‌ناپذیری است. TCP را دوست داریم، چرا که خیلی سریع می‌توانیم بگوییم که آیا یک سوکت TCP در حال شنود است. از آنجا که سوکت TCP، سوکتی اتصال‌گر است، می‌توانیم خودمان مکالمه‌ای را شروع کنیم و ببینیم که سیگنال مشغول‌بودن یا برای برقراری ارتباط را دریافت می‌نمایم.

یک روش برای بررسی ایجاد سوکت، استفاده از خود برنامه سرویس‌گیرنده و آنگاه وارسی لیست سوکت در ایستگاه‌کاری می‌باشد. برای مثال چگونگی اتصال با یک سرویس FTP در یک پنجره و اجرای netstat -an در پنجره‌ای دیگر به شکل زیر است:

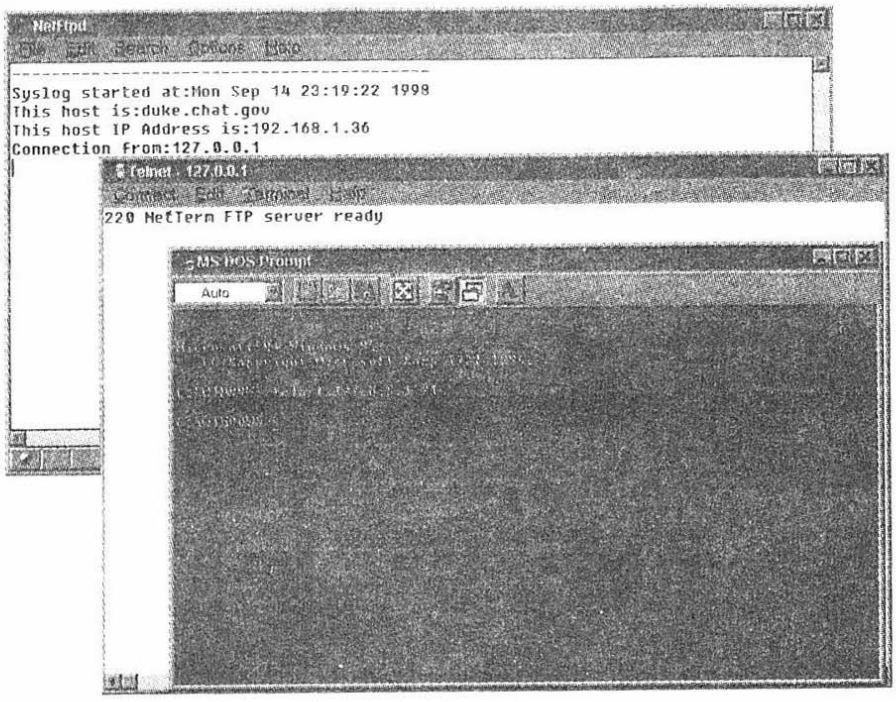
```
C:\WINDOWS > netstat -an | find ":21"
TCP 192.168.10.5:1025 192.168.5.1:21 ESTABLISHED
```

در اینجا یک اتصال برقرارشده (ESTABLISHED) موجود است، بنابراین سوکت سالمی در دست دارید. در این حالت، ممکن است در صورت مواجه‌شدن با مشکلات، بخواهید نگاهی به پیکربندی سرویس‌گیرنده بیندازید.

یک روش دیگر، برای بررسی آنکه سوکت راه دوری در حال شنود است، Telnet کردن به آن سوکت است. برای مثال،

اجازه دهید تجربه‌ای کنترلی انجام دهیم. می‌توانید یک سرویس‌دهنده FTP را روی یک PC اجرا کنید و از Telnet برای بررسی حالت شنود آن استفاده نماید. به این ترتیب، حتی به شبکه خارجی هم نخواهید رفت. از آدرس بازگشت حلقه استفاده کنید (آدرس بازگشت حلقه در TCP/IP همیشه 127.0.0.1 می‌باشد). می‌توانید با تایپ فرمان زیر نتایج را مشاهده کنید (شکل ۵-۱۸ را ببینید):

```
telnet 187.0.01 21
```



شکل ۵-۱۸ : می‌توانید یک سرویس‌دهنده FTP محلی را روی PC خود به اجرا درآورده و از طریق مشخص‌کردن آدرس حلقه بازگشتی و سوکت 21 با Telnet به آن متصل شوید.

همان گونه که در شکل ۵-۱۸ نشان داده شده است، صفحه نمایش نشان‌دهنده آن است که سرویس‌دهنده FTP در حال اجراست. این ترفند خوبی است که می‌توانید برای هر سرویس TCP به‌کار ببندید. آیا همواره پاسخی دریافت می‌کنید؟ خیر، برخی اوقات اعلانی در کار نخواهد بود. اگرچه، اصل ترفند آن است که بلافاصله CONNECT FAILED را از برنامه Telnet دریافت کنید یا نکنید.



نکته : *از آنجاکه نگارش Telnet ارائه‌شده با ویندوز، خیلی در مورد اینکه چرا اتصالی با شکست مواجه می‌شود، گویا نیست، برخی اوقات از طریق اعلان سطر فرمان، یک دستور ftp کاراکتری را اجرا می‌کنم. می‌توانید سوکتی برای آن هم ایجاد کنید و هنگامی که سرویس‌دهنده‌ای از سوی دیگر به آن سوکت گوش نمی‌دهد، پیغام مناسبی بازگشت داده می‌شود. برای مثال، من می‌دانم سرویس‌دهنده Telnet روی PCام به اجرا درنیامده است؛ برای اثبات آن، از ftp استفاده خواهم کرد:*

```
c:\WINDOWS > ftp
ftp> open 127.0.0.1 23
-> ftp:connect:connectionreused
```

می‌توانم این کار را برای بررسی وضعیت شنود هر سوکت TCP به انجام برسانم.

در هر سیستم‌عاملی که مورد استفاده قرار دهید، شماره سرویس یکی خواهد بود. برای مثال هر سرویس‌دهنده ناول یا NT که کاری چاپی را از سرویس‌دهنده یونیکس می‌گیرد، اغلب به سوکت چاپگر (#515) گوش فرامی‌دهد. اگر بر سرویس‌دهنده 515، Telnet کنید و پیغام Connection refused را دریافت نمایید، زمان آن فرا رسیده که برنامه سرویس‌دهنده را وارسی کنید.



نکته : *آگاه باشید که تمام کارهای چاپی یونیکس از طریق سوکت صورت نمی‌گیرد. یک روش چاپ، به نام چاپ عبوری وجود دارد که به کُدهای نامرئی خاصی که با متنی ارسال می‌شوند، عکس‌العمل مناسبی نشان دهد. برای مثال، اگر برنامه کاربردی‌تان روی یک میزبان یونیکس کُد Control-T را به ترمینال Wyse-60 شما می‌فرستد، ترمینال شما ـ یا شبیه‌ساز ترمینال ـ چاپ متنی که بلافاصله بعد از کُد ارسال شده است را آغاز می‌کند و دیگر آن را به شما نشان نمی‌دهد. کُدی دیگر ـ برای مثال، Control-R ـ وضعیت را به حالت معمولی بازمی‌گردانند. مواظب این مسأله باشد؛ ممکن است از درماندگی و سرگردانی نجات پیدا کنید.*

نمی‌توانم کاری برای چاپ انجام دهم

در شرکتی بودم که میزبان یونیکس جدیدی خریداری کرد، برخی از صف‌های چاپ را جابجا نمود و متوجه شد که برخی از کارهای چاپی، قبل از چاپ مدت زمان زیادی در صف باقی می‌مانند. بررسی نشان داد که این امر تنها در مورد چاپگر متصل به ناحیه گسترده و چاپگرهایی که مختص سرویس‌دهنده‌های چاپ نصب شده بودند رخ می‌داد.

آنگاه متوجه شدیم در هر سرویس‌دهنده چاپ مستقل، تنها یک چاپگر در هر لحظه می‌توانست چاپ کند. فروشنده میزبان جدید، ادعا می‌کرد که مشکل از شبکه است، اما فروشنده سرویس‌دهنده چاپ تقصیر را متوجه میزبان می‌دانست.

بعد از ارسال کارهای چاپی به صف‌های چندگانه از میزبان به یکی از سرویس‌دهنده‌های چاپ مستقل‌مان، روی میزبان دستور ذیل را اجرا نمودم:

```
netstat -an | grep 515
```

تنها یک سوکت باز برای سرویس‌دهنده چاپ مشاهده کرد. دلایل برای من کافی بود ـ از قرار معلوم، سرویس‌های چاپ این نگارش از یونیکس، بیش از یک چاپگر را روی هر میزبان شبکه‌ای پشتیبانی نمی‌کرد و در هر لحظه یک کار ارسال می‌شود. به همین دلیل، کارهای ناحیه گسترده هم با اشکال کار می‌کرد ـ بیش از یک چاپگر در سوی دیگر پیوند WAN وجود داشت و به جای ارسال کارهای چاپی به صورت چندتایی، یک کار چاپی بزرگ می‌توانست جلوی بقیه، یعنی کارهای چاپی کوچکتر را سد کند. ردیابی‌های شبکه این موضوع را تأیید می‌کرد.

فروشنده ادعا داشت که این رفتار اشتباه «مطابق طرح» صورت می‌گیرد و از رفع آن امتناع می‌ورزید. بنابراین ما رفتیم و چیزی خریدیم که به درستی کار می‌کرد.

ارزیاب محتویات

برای سرویس‌های خاصی، مثل HTTP، می‌توانید محتویات را بررسی کنید. برای مثال، لیست ۱-۱۸ یک جلسه عیب‌یابی با سرویس‌دهنده وِب را نشان می‌دهد.

لیست ۱-۱۸ : جلسه عیب یابی با سرویس‌دهنده وِب

```
mori A ~$ telnet 167.195.160.6 80
Trying 167.195.160.6...
Connected to 167.195.160.6.
Escape character is '^]'.
GET /
<title>Neato Geeky Stuff(tm)</title>
<B>Neato Geeky Stuff(tm)</B><P>
<img src="jonny/smguru.gif">
<B>Leo sez:</B>
<p> Check it out. <I> Losta</I> neato geeky stuff.
...
```

مثل یک صفحه کامل HTML می‌ماند. خیلی بیشتر از یک ping گفته می‌شود ـ وضعیت بالابودن سرویس‌دهنده وِب و سرویس HTML بازگو می‌شود. به عبارت دیگر، کسی اهمیت می‌دهد که یک سرویس‌دهنده وِب به ping ها پاسخ می‌دهد؟ برای پاسخ‌دادن به ping ها لازم نیست که این سرویس‌دهنده را تهیه کرده‌اید. اما اگر به ping ها پاسخ می‌دهد اما سرویسی برای صفحات وِب ارائه نمی‌کند، به تمام و کمال معنا «پایین» است. از طریق بررسی محتویاتی این چنین، می‌توانید پی ببرید که به طرز مناسبی کار می‌کند.

خرابی پست الکترونیکی

اگر می‌توانید به سوکت telnet کنید اما هنوز مشکلات برنامه کاربردی به جای خود باقی هستند، زمان آن فرارسیده که برنامه کاربردی را مورد هدف قرار دهید. من یک سیستم پُست الکترونیکی خصوصی دیدم که در مورد یک سایت راه دور با مشکل روبه‌رو بود ـ کاربران می‌توانستند متصل شوند، اما مدت مدیدی طول می‌کشد تا نامه‌های خود را دریافت کنند. ما یک سرویس‌دهنده پُست الکترونیکی محلی برای سرویس‌دهی به آنان درنظر گرفتیم (برای از صحنه خارج‌کردن ناحیه گسترده)، و نتیجه آن بود که مشکل کاربران برطرف شد. البته، هنگامی که سرویس‌دهنده پُست الکترونیکی جدید سعی می‌کرد با سرویس‌دهنده اصلی ارتباط برقرار کند، تعداد زیادی سوکت قطع شده ـ تعداد زیادی سوکت در وضعیت TIME_WAIT نصیبمان می‌شد. منظورم از تعداد زیاد 30 تا 50 مورد است. این نشان‌دهنده آن بود که اتصالات موفق بسیار و بعد از آنها قطعی‌هایی رخ می‌دهد.

معمولاً هنگامی که اتصالی به وجود می‌آید، بدون مشکل کارش را ادامه می‌دهد. قطع اتصالات اغلب به علت مشکلات شبکه‌ای به وقوع می‌پیوندد. البته، من می‌توانستم با Telnet هرچقدر که بخواهم به سوکت متصل باقی بمانم. این نتیجه، کاملاً برنامه کاربردی را در مظان اتهام قرار داد.

جستجویی روی سایت وِب فروشنده بر اساس وضعیت سوکت، آشکار ساخت که با پیکربندی‌های خاصی از مسیریاب، این مشکل به وقوع می‌پیوست. فروشنده تغییر در مسیریاب را توصیه می‌نمود، اما در کنار آن اصلاحیه‌ای برای نرم‌افزار سرویس‌دهنده و سرویس‌گیرنده ارائه نموده بود که به حل مشکل انجامید.

خلاصه

شبکه‌سازی فایل و چاپ و سرویس‌گیرنده/سرویس‌دهنده، نان و کره بیشتر مجموعه‌های شبکه‌شده می‌باشند. با وجود شبکه‌سازی فایل و چاپ و پروتکل‌های متنوع سرویس‌گیرنده/سرویس‌دهنده، کار مشکل‌تر از آن است که به اشکال گوناگون با آن کنار آمد. سرویس‌های فایل و چاپ به طرز سنگینی به سرویس‌گیرنده‌هاشاان تکیه می‌کنند، بنابراین بهتر است یک صفحه تحت موسیقی را در اختیار همه قرار دهید.

چاپ یکی از مهمترین و کاربردی‌ترین کارهای شبکه است. درک فرآیند چاپ می‌تواند در یافتن نهانگاه مشکل یاری‌رسان باشد. مستندات مربوط به چاپگر به ویژه هنگامی که به صورت یک برچسب روی خود چاپگر آدرس‌دهی شده باشد، به طرز خارق‌العاده‌ای کمک می‌کنند. دانستن چگونگی ردیابی یک مشکل چاپی برای مشکلات پیچیده واقعاً مفید است.

خطاهای فایلی الزاماً همیشه دقیق نیستند ـ کسی که فایلی فقط ـ خواندنی را باز می‌کند، ممکن است تنها به خاطر دلایل امنیتی امکان تغییر فایل را نداشته باشد. دانستن چگونگی راهبری امنیت در سرویس‌دهنده، در اینجا بسیار اهمیت دارد. می‌توان ارتباط مشکلات مسائل مربوط به امنیت از طریق تخصیص حقوق کاربر ویژه به آن کاربر و آنگاه بازگشت سریع آنها، روشن نمایید.

مشکلات فضای دیسکی ممکن است تمامی عملیات را متوقف سازند. جدای یافتن مقصر، می‌توانید مشکل را با کنارگذاشتن مقدار فضای دیسکی تسکین بخشید.

عیب‌یابی در سطح سوکت، بعد از کنارگذاشتن مشکلات در سطح شبکه‌ای، کلید اصلی عیب‌یابی برنامه کاربردی سرویس‌گیرنده/سرویس‌دهنده می‌باشد. یکی از بهترین دوستان شما در اینجا، دستور netstat -a می‌باشد. دانستن شماره سرویس‌ها و وضعیت‌های سوکتی می‌تواند در معاینه مشکل کمک بزرگی باشد. به ویژه، انجام ترفند Telnet می‌تواند خیلی سریع آشکار سازد که آیا سرویسی در میزبان مورد نظر به‌اجرا درآمده است و آیا می‌تواند کار خود را به صورت مناسب به انجام برساند.

کارگاه

پرسش و پاسخ

پرسش : منظور از صف چیست؟

پاسخ : صف یعنی ترتیبی از چیزها یا اشخاص، مثل صف بانک. استفاده از آن برای علوم کامپیوتری، اشاره به هر موقعیتی است که با چیزی بر مبنای «ورود اول، خروج اول» برخورد می‌شود. در مفهوم فایل و چاپ، صف یک ردیف تصوری است که کارهای چاپی برای دریافت سرویس در آن منتظر می‌مانند.

پرسش : نمی‌توانم از یک ایستگاه به خصوص چاپ کنم، و اشکال را تا سرویس‌دهنده ردیابی نموده‌ام که به نظر می‌رسد که به آن مرتبط می‌باشد. به این دلیل که فایل صف روی سرویس‌دهنده با فایل روی ایستگاه‌کاری فرق دارد. گام بعدی چیست؟

پاسخ : اگر بقیه می‌توانند به صورت موفق از طریق این صف سرویس‌دهنده چاپ را انجام دهند ممکن است مشکل در

ایستگاه‌کاری روی یک بخش شبکه‌ای دیگر متفاوت با سایرینی که چاپ را بدون مشکل انجام می‌دهند، قرار گرفته باشد. آیا می‌توانید ایستگاه‌کاری را جابجا کنید؟ این کار می‌تواند نشان‌دهنده مسیریاب یا پورت سوئیچ خراب باشد.

پرسش : آیا راهی وجود دارد که قفل‌های اشخاص دیگر روی یک فایل را بدون قطع اتصال آنها از سرویس‌دهنده پاک نمود؟

پاسخ : NT می‌تواند قفل سایرین را از روی فایل بردارد؛ ناول نمی‌تواند برای پاک‌کردن قفل روی فایل سایران در یک سرویس‌دهنده ناول، یا باید کاربر را صدا زده و از وی بخواهید دیگر استفاده نکند و یا باید اتصال شبکه‌ای از سرویس‌دهنده را پاک نمایید.

پرسش : آیا ابزاری Telnet مانند برای UDP وجود دارد که بتوان با آن حالت شنود سوکت UDP را بررسی نمود؟

پاسخ : برای بررسی حالت شنود یک سوکت بدون اتصال، باید پاسخی دریافت کنید. برای گرفتن پاسخ، باید «یادداشت» صحیحی ارسال کنید. بنابراین پاسخ منفی است. تنها ابزاری که می‌توان از راه دور بالابودن سرویس‌دهنده UDP را بررسی کرد، سرویس‌گیرنده است.

آزمون

۱- تفاوت اصلی بین شبکه‌سازی فایل و چاپ و سرویس‌گیرنده/سرویس‌دهنده چیست؟

الف ـ در چاپ شبکه‌سازی سرویس‌گیرنده/سرویس‌دهنده، تنها بعد از انتقال فایل دریافت اطلاعات میسر است.

ب ـ سرویس‌گیرنده اغلب پیچیده‌تر از سرویس‌گیرنده فایل و چاپ است.

ج ـ نه الف و نه ب

د ـ هم الف و هم ب

۲- پرس‌وجویی را منتقل می‌سازم؛ سپس سرویس‌دهنده پایگاه اطلاعاتی بزرگی را روی گردونه دیسک محلی‌اش جستجو می‌کند و پاسخی را برایم پس می‌فرستد. این مثالی از چیست؟

الف ـ شبکه‌سازی فایل و چاپ

ب ـ سرویس‌گیرنده اغلب پیچیده‌تر از سرویس‌گیرنده فایل و چاپ است.

ج ـ نه الف و نه ب

د ـ هم الف و هم ب

۳- در طی یک جلسه عیب‌یابی چاپ، متوجه شده‌اید که برنامه کاربردی، خروجی را تولید نموده است و راه‌انداز چاپ به درستی کار می‌کند. کار بعدی که در انجام عیب‌یابی باید مورد توجه قرار دهید چیست؟

الف ـ انتقال فایل آماده چاپ به سرویس‌دهنده

ب ـ انتقال فایل آماده چاپ به ایستگاه‌کاری

ج ـ انتقال فایل آماده چاپ به چاپگر فیزیکی

د ـ انتقال فایل آماده چاپ به دپارتمانی دیگر

۴- ویندوز NT فایل‌های آماده چاپ خود را در کجا ذخیره می‌کند؟

الف ـ WINDOWS\Printers ب ـ %SYSTEMROOT%\System32\Printers

ج ـ %SYSTEMROOT%\Printers د ـ WINDOWS\System32

۱- درست یا نادرست: می‌توانید از برنامه کمکی Find در ویندوز برای پیداکردن فایل‌هایی اندازه معینی دارند، استفاده کنید.

۸- درست یا نادرست؟ بازنشانی کلیه فایل‌های برنامه کاربردی از یک نقطه «شناخته‌شده خوب»، باید آخرین روش رفع اشکال آنها باشد.

۹- در تلاشید مرورگر وِب یکی از کاربران را به‌کار اندازید. دریک پنجره اعلان DOS دستور **netstat** را بلافاصله بعد از آزمون مرورگر انجام می‌دهید. اتصالی در وضعیت TIME_WAIT ملاحظه می‌کنید، اما به سرویس‌دهنده‌ای اشتباه که شماره سوکت اشتباهی هم داراست. به احتمال زیاد، چه چیزی باعث بروز این حالت شده است؟

الف ـ مروگر به خاطر خطاهای شبکه‌ای به دردسر افتاده است.

ب ـ پیکربندی مرورگر اشتباه است.

ج ـ پشته TCP/IP اشکال دارد. د ـ کاربر باید مرورگر را به‌روز درآورد.

پاسخ به سؤالات آزمون

۱- د ۲- ب

۳- الف ۴- ب

۵- نادرست ۶- ب

۷- درست ۸- درست

۹- ب

فصل ۱۹

عیب‌یابی اینترنت/اینترانت

به خوبی به خاطر دارم که زمانی یکی از همکارانم با صدای بلند می‌گفت که اینترنت و کار روی آن اتلاف زمان است و همهٔ ما که مجذوب آن شده‌ایم بهتر است خط کاری دیگری را انتخاب نمائیم. خوب، با وجود اینکه وی آدم خوبی است، اما به هیچ عنوان پیشگوی موفقی نبوده است. موفقیت اینترنت بیش از آن بوده که در مخیلهٔ هر یک از ما می‌گنجیده است.

ایدهٔ اصلی این فصل آن است که نقاط ضعف برای تعمیر «شاهراه اطلاعاتی» که برای عیب‌یابی خیابانهای محلی و کوچه‌ها نیز به کار می‌آیند را روشن سازیم. کار خود را با تعریف اینترنت و اینترانت‌ها و آنگاه گردشی سریع در تکنیک‌های عیب‌یابی آغاز می‌کنیم.

تعاریف

لازم نیست کسی اینترنت را برای شما تعریف کند. منبع زندگی، مرکز تمدن کامپیوتر، آبشاری از جریانهای اطلاعاتی و کوهی از بسته‌های خوب و بد را می‌توان به اینترنت تشبیه نمود. اینترنت از منبعی خوب برای دانشجویان، به منبعی واجب و حتمی برای استادان کامپیوتر و به همین صورت برای تمامی افراد تبدیل شده است. بسیاری از افراد اینترنت را «منبعی غیربحرانی» می‌نامیدند. اما امروزه به‌خصوص اگر شغلتان برای برقراری ارتباط با مشتریان از پُست الکترونیکی یا یک صفحهٔ وِب صورت پذیرد، دیگر گفتهٔ مذکور صادق نخواهد بود. امروزه، اینترنت منبعی حیاتی است؛ اگر اشکالی در آن وجود داشته باشد، بیشتر اوقات افراد قادر به انجام کار خود نخواهند بود. برای مثال این کتاب تا حدود زیادی از طریق اینترنت ویرایش شده است. اگر اینترنت خراب شده بود ـ حتی نمی‌خواهم به آن فکر کنم!

میلیونها و میلیونها کامپیوتر و شبکهٔ TCP/IP در سراسر دنیا شبکه‌ای را تشکیل داده‌اند که در فصل اول در مورد آنها صحبت نمودیم، اما در اینجا مقیاس متفاوت است. هنگامی که ایستگاه کاری شما درخواستی را مربوط به یک صفحهٔ وِب به سرویس‌دهندهٔ موجود در www.microsoft.com می‌فرستد، یک جستجوی DNS اسم ـ به ـ آدرس IP انجام می‌شود؛ آنگاه یک فراخوانی TCP/IP برای سرویس‌دهنده تنظیم می‌شود که توسط یاری ۳ تا ۱۲ مسیریاب در میانهٔ مسیر به مقصد می‌رسند.

آیا عیب‌یابی اتصال اینترنت با عیب‌یابی TCP/IP که تاکنون فراگرفته‌اید، متفاوت است؟ اصولاً خیر. البته همیشه سطح پیچیدگی بالاتر به تکنیک‌های عیب‌یابی متفاوتی نیاز دارد. به طور خلاصه، هر اشکال در اتصال اینترنت به ISP تان مربوط می‌شود اما همیشه هم نباید تقصیر را بر عهدهٔ آنان دانست. ما در مورد انواع دیوار آتشی که ممکن است مورد استفاده قرار دهید صحبت خواهیم کرد و آنگاه روشهای پیداکردن مشکلات مسیریابی، تحلیل نام و اینکه آیا باید در مورد مشکل پیش آمده با ISP تان تماس بگیرید، بحث خواهیم نمود.

اینترانت = داخلی

واژهٔ اینترانت و پیشینهٔ آن اِکسترانت (شبکه‌ای که شما و همکار شغلی‌تان را به هم متصل می‌کند)، واژه‌هایی بازاری هستند

که همیشه مرا به اشتباه می‌اندازند. پیشوند اینترا به معنای همراه و در حین می‌باشد و اِکسترا معنای بدونِ می‌دهد. در مرکز اطلاعاتی خود، ما اغلب به برنامه‌های کاربردی که به صورت خارجی اجرا می‌شوند «دسترسی عمومی» می‌گوییم. می‌توانید این‌گونه تصور کنید که پیشوند اینتر برای هر آنچه که خارج از مجموعهٔ شما قرار دارد، اینترا هر آنچه که در داخل قرار دارد و اِکسترا برای مرز بین این دو به کار می‌روند.

واژه اینترانت کاربرد اصلی خود را ندارد ـ اما عبارت «شبکهٔ من» معنای لازم را می‌رساند. منظور از این واژه، برنامه‌های کاربردی شبه ـ اینترنتی است که در مرزهای شبکهٔ داخلی به اجرا درمی‌آید ـ از تکنولوژی‌هایی استفاده می‌شود که بر مبنای وِب به بلوغ و تکامل رسیده‌اند. هر اینترانت می‌تواند نظیر یک فهرست تلفنی فعال در وِب از تمامی کارمندان با تمامی امکانات جستجو و یا یک صفحهٔ وِب ثابت که ورود شما به اینترانت شرکت خاصی را خوش‌آمد می‌گوید، تشکیل شده باشد.

بسیاری از ابزار که برای وارسی اتصال اینترنت به کار می‌روند، در عیب‌یابی اینترانت‌ها نیز کاربرد دارند، بنابراین بخش مربوط به اینترنت را به دقت مطالعه کنید (تکنیک‌های مطرح شده در فصل ۱۸ نیز برای عیب‌یابی اینترانت‌ها، بسیار مفید واقع می‌شوند).

با ذکر مطلب فوق، در ادامهٔ این فصل، مطالب عیب‌یابی خاصی را برای شبکهٔ محلی‌تان مطرح خواهیم نمود: سرویس‌های داخلی و خارجی وِب، پُست الکترونیکی و مشکلاتی که کاربران تلفنی شبکه ممکن است با آنها روبرو شوند.

آشفتگی مجازی

به خاطر واژه‌های اغواءکنندهٔ زیادی که اینترانت را دربرگرفته‌اند، به آسانی ممکن است این واقعیت که اینترانت تنها یک شبکهٔ TCP/IP بزرگ است، از دیده پنهان بماند. اجازه دهید نگاهی داشته باشیم به تکنیک‌های عیب‌یابی مخصوص TCP/IP که می‌تواند مشکلات اینترنتی مجموعهٔ کاری شما را نمایان سازند.

برای شروع، لازم است که مشخص کنیم شما چه نوع اتصال اینترنتی دارید. بعد از دانستن نوع اتصال، بهتر است که تعیین کنیم کدامیک از تکنیک‌های ذیل برای شما مناسب هستند.

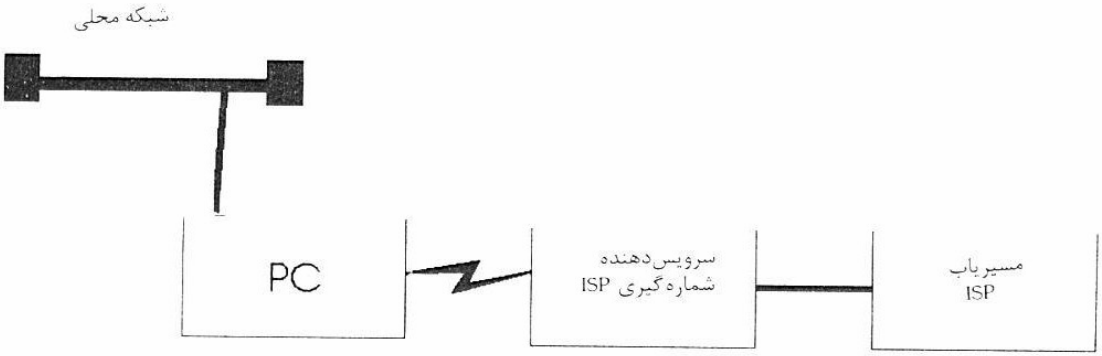
به غیر از حالتی که کار شما نظیر یک شرکت چندملیتی با اتصالات اینترنتی با توانایی تحمل بروز مشکل گسترده باشد، احتمالاً تنها یک دیوار آتش با یک حوزهٔ اسمی (company.com) می‌باشید.

در واقع اگر برای یک شرکت بزرگ که هزاران عضو ویژهٔ تکنولوژی اطلاعاتی داراست، کار کنید؛ به احتمال زیاد شانس رسمی تمرین آنچه که در این کتاب آموخته‌اید را خارج از شبکهٔ محلی خود نخواهید یافت. اغلب چنین شانسی برای دسترسی به شبکه خارج از دیوار آتش در چنین محیطی بسیار نادر یا هیچ است. به خاطر داشته باشید: اگر گیر افتادید یا کشته شدید، منشی از افشای فعالیت‌های شما سر باز خواهد زد. این کتاب نیز به طور خودکار در عرض ۵ ثانیه نابود خواهد شد!

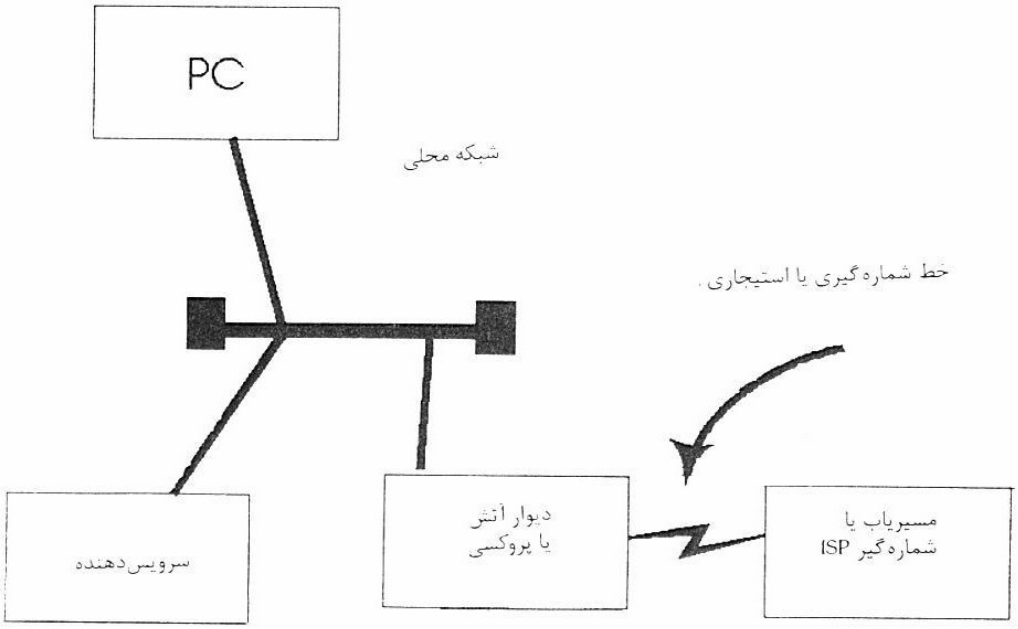
شناسایی اینترنت

به احتمال زیاد یکی از انواع دسترسی اینترنتی زیر را در اختیار دارید:

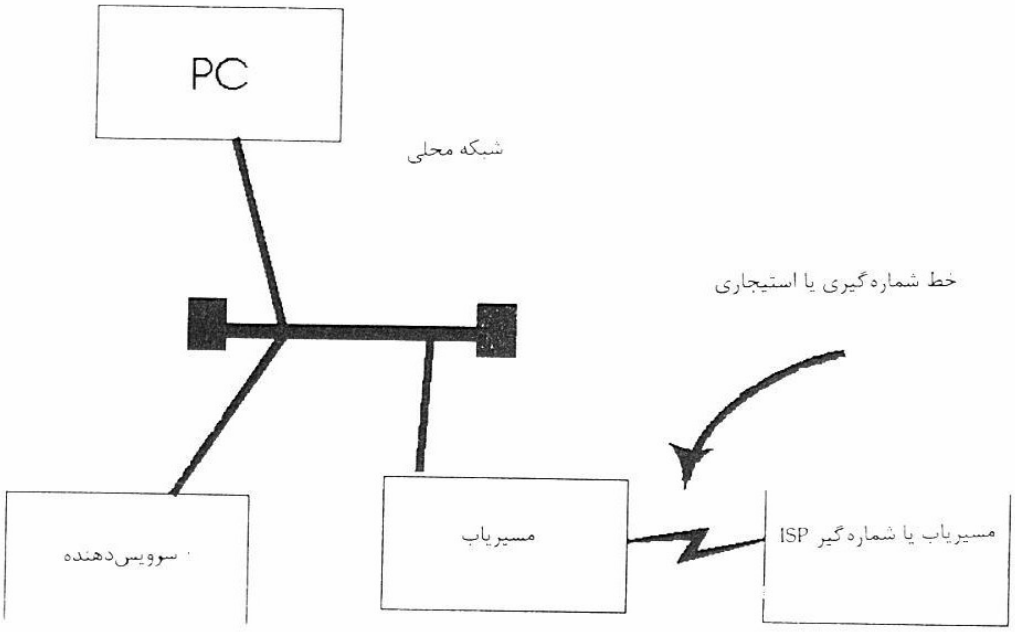
- روش ۱ : تنها اتصالات تلفنی از طریق ایستگاه کاری (شکل ۱-۱۹).
- روش ۲ : اتصال مستقیم دیوار آتش یا پروکسی به ISP (شکل ۲-۱۹).
- روش ۳ : تنها مسیریاب ISP بدون دیوار آتش (شکل ۳-۱۹).
- روش ۴ : دیوار آتش یا پروکسی، شبکهٔ DMZ (ناحیهٔ غیرنظامی) به مسیریاب ISP (شکل ۴-۱۹).



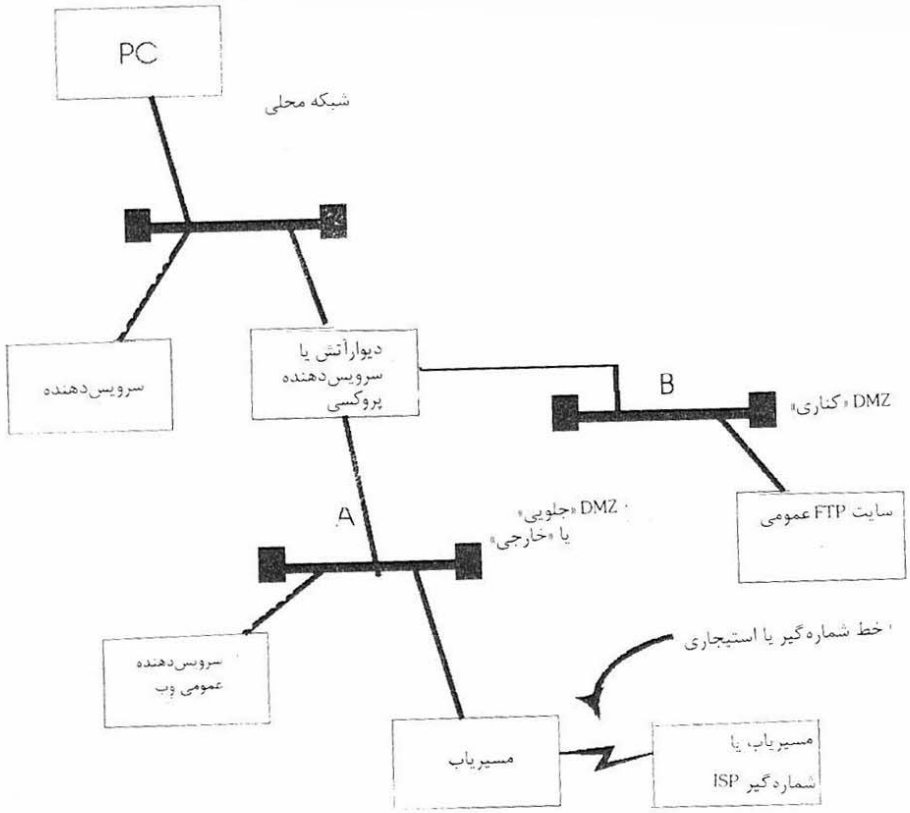
شکل ۱-۱۹ : شماره‌گیری ایستگاه کاری برای اتصال به فراهم‌آورندهٔ سرویس اینترنت.



شکل ۲-۱۹ : سرویس‌دهندهٔ پروکسی یا دیوار آتش در شبکهٔ شما که به ISP متصل می‌شود.

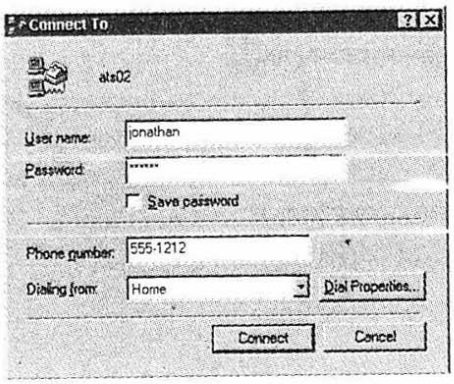


شکل ۳-۱۹ : مسیریابی که به صورت مستقیم شبکه را به ISP متصل می‌کند و اتصال مستقیمی به اینترنت ایجاد می‌کند. (این روش بنا به دلایل امنیتی کمتر مورد استفاده قرار می‌گیرد).



شکل ۴-۱۹ : یک الگوی ناحیهٔ غیرنظامی که دسترسی «مجاز» به سرویس‌دهنده‌های دسترسی عمومی را میسر می‌سازد.

شناسایی نوع اتصال، از اهمیت زیادی برخوردار است. چگونه این کار را انجام می‌دهید؟ خوب، روش اول کاملاً آسان است ـ اگر از شبکه تلفنی ویندوز برای اتصال به اینترنت استفاده می‌کنید، اغلب صدای تماس و شماره‌گیری مودم را می‌شنوید و کادر تبادلی شبکه‌ای تلفنی را قبل از برقراری ارتباط ملاحظه می‌کنید. (شکل ۵-۱۹ را ببینید). هر اتصال تلفنی، پیوندی «وابسته به خود» را ایجاد می‌کند و در واقع در قالب روش ۳ (اتصالی مستقیم به ISP بدون دیوار آتش) رده‌بندی می‌شوید. به عبارت دیگر به غیر از حالتی که ایستگاه کاری شما نظیر یک مسیریاب (ویندوز ۹۵ فاقد این امکان است و ویندوز NT برای انجام این کار باید پیکربندی شده باشد) عمل نماید، کس دیگری در شبکهٔ شما نمی‌تواند از اتصال اینترنتی‌تان استفاده کند. (اگر تصمیم بگیرید که از NT به‌عنوان مسیریاب ارزان‌قیمتی برای اتصال به ISP استفاده کنید، به‌خاطر داشته باشید که اتصال شما در ردهٔ روش ۳ قرار می‌گیرد ـ دیوار آتشی برای محافظت از شبکهٔ شما وجود نخواهد داشت. مواظب باشید!).



شکل ۵-۱۹ : کادر تبادلی شبکهٔ تلفنی.

در حالت عمومی، اولین گامهای عیب‌یابی این روش از اتصال به اینترنت کاملاً آسان می‌باشد ـ یا اتصال برقرار می‌شود یا نمی‌شود! در بیشتر حالات، مشکل در غیرفعال‌بودن تجهیزات موجود در ISP یا شرکت تلفن می‌باشد. بعد از برقراری اتصال مشکل دارید؟ بخش «در اینجا دوباره ping می‌کنم» در ادامهٔ این فصل را ملاحظه نمایید.

به‌خصوص، در صورت استفاده از روش‌های ۲ تا ۴ اغلب کاری بیشتر از راه‌اندازی ایستگاه کاری صورت نخواهید داد. شبکهٔ محلی به‌عنوان پایه مورد استفاده قرار می‌گیرد.

روش ۲ یکی از معمول‌ترین پیکربندی‌هاست، به‌خصوص اگر ISP میزبانی صفحات وِب شما را به عهده داشته باشد (یعنی سرویس‌دهنده‌ای را به اجرا درمی‌آورد که صفحات وِب شما در آن قرار دارند و نیازی به اجرا درآوردن سرویس‌دهنده وِب خصوصی نخواهید داشت). این روش آسانی برای انجام کارها در مورد مجموعه‌های کاری کوچک تا متوسط می‌باشد؛ تنها لازم است اتصالی از نوع گسترده (تلفنی یا استیجاری) از دیوار آتش یا پروکسی به ISP خود داشته باشید.

روش ۳ نامعمول است. در این روش کاربر اهمیتی به مسئلهٔ امنیتی نمی‌دهد و یا آنکه فرض بر این است که مسائل امنیتی در ISP به انجام می‌رسد. با اینکه هنوز در ایالات متحده افرادی وجود دارند که درهایشان را قفل نمی‌کنند، اما تعداد آنها رو به کاهش است و همچنین تعداد کسانی که از دیوارهای آتش خصوصی بهره نمی‌برند نیز کم و کمتر می‌گردد.

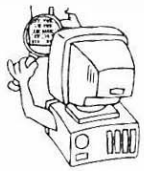
برای شرکتهای نسبتاً بزرگتر روش ۴ بیشتر مورد استفاده قرار می‌گیرد. حضور یک شبکهٔ میانی یا «ناحیهٔ غیرنظامی» (DMZ) به چه معناست؟ ماشین‌هایی که ماشین‌های کاملاً سری محسوب می‌شوند باید خارج از شبکه قرار داده شده باشند و دور از دسترسی کاربران خارجی اینترنت قرار بگیرند. این واقعیت که آنها «جلوی» دیوار آتش یا «کنار» دیوار آتش قرار داده می‌شوند بدان معناست که آنها به صورت مجزایی از شبکهٔ تولید قرار گرفته‌اند.



یادداشت : *اگر یک ماشین خارجی «کنار» دیوارهٔ آتش قرارگرفته باشد، این بدان معناست که کاربران خارجی باید بتوانند به سرویس‌دهنده دسترسی داشته باشند، اما از طرفی شما می‌خواهید این کاربران از جهاتی محدودیت‌هایی داشته باشند. به جای پیکربندی چندین سرویس‌دهنده تنها کافی است که دیوار آتش برای مجاز داشتن ترافیک خاصی پیکربندی گردد. برای مثال، ممکن است امکان تشکیل جلسه‌های FTP از دنیای خارج برای دسترسی به سرویس‌دهندهٔ FTP موجود در نقطه B در شکل ۴-۱۹ را مجاز کنیم اما امکان انجام هر کار دیگری را مسدود سازیم.*

هنگامی که سرویس‌دهنده‌ای «جلوی» دیوار آتش قرار می‌گیرد، بدان معناست که دیوار آتش به هیچ‌وجه سرویس‌دهنده را محافظت نمی‌کند. برخی اوقات این کار به این خاطر انجام می‌شود که دیوارآتش کارایی سرویس‌دهنده را از آن می‌گیرد. برای مثال از آنجا که هر سرویس‌دهندهٔ پروکسی به سرویس‌گیرندهٔ پروکسی نیاز دارد، در این حالت غیرعملی خواهد بود که از یک DMZ «کناری» برای ماشین‌هایی که به منظور دسترسی عمومی درنظر گرفته شده‌اند، استفاده نماییم. در این حالت یک DMZ جلویی بدان معناست که ترافیک اینترنت می‌تواند به ماشین‌های دسترسی عمومی بدون محدودیت ایجاد شده توسط سرویس‌دهندهٔ پروکسی دسترسی پیدا نماید.

DMZ خارجی از آن جهت که می‌توان به سادگی وضعیت روشن‌بودن هاب را بررسی نمود و علاوه بر نظارت در ترافیک شبکه از نرم‌افزارهای تشخیص داخلی برای بررسی دسترسی افراد ناخواسته استفاده کرد، بسیار جالب است. مهمتر از همه آنکه می‌توانید از یک تحلیل‌گر شبکه یا کامپیوتر همراه ویندوز ۹۵ برای عیب‌یابی محدودیت‌های ناخواستهٔ دیوار آتش استفاده نمایید (به نقطهٔ A در شکل ۴-۱۹ دقت کنید).



نکته : *حتی اگر سرویس‌دهنده پروکسی‌ای داشته باشید که اجازهٔ عبور بسته‌های Ping، traceroute، جستجوهای DNS را ندهد، می‌توانید به ناحیهٔ BMZ متصل شده و به خاطر صرفه‌نظرکردن از دیوارآتش، کار عیب یابی را انجام دهید.*

هفت سال آزگار...

بعد از تشخیص نوع دیوار آتش، بسیار مهم است که قبل از حملهٔ مشکلات، سعی کنید که تکنیک‌های عیب‌یابی به کار را در این فصل را تمرین کنید تا بدانید که در طی یک پریود «عادی» چه چیزهایی کار می‌کنند و چه چیزهایی کار نمی‌کنند.

اگر که ندانید حالت معمولی اوضاع در مجموعهٔ کاریتان چگونه است، چطور می‌خواهید تشخیص دهید که خرابی‌ای وجود آمده است؟ به عبارت دیگر، اگر سرویس‌دهنده پروکسی اجازهٔ انجام Ping را در اختیار نمی‌گذارد، تلاش برای انجا Ping هنگام بروز خرابی هیچ نتیجه‌ای نخواهد داشت. البته، اگر بدانید که Ping از طریق دیوارآتش کار می‌کند، آنگاه در طر بروز خرابی اگر نتوانید Ping را از میان دیوار آتش به انجام برسانید، ممکن است بتوان این‌گونه تصور کرد که یا دیوار آتش پایین است و یا اینکه پیوند (اترنت یا خط استیجاری) به مسیریاب فراهم‌کنندهٔ سرویس اینترنت اشکال دارد. در چنین حالتی است که می‌توانید به طور مناسب بازرسی‌های لازم را انجام دهید.

در اینجا دوباره Ping می‌کنم

ماجرای اتصال اینترنت با انجام همان کارهایی که به صورت داخلی اغلب صورت می‌دهید، آغاز می‌شود. بخش آسان عیب‌یابی اینترنت آن است که از آنجا که به احتمال زیاد یک مسیریاب یا دیوار آتش را برای اتصال مورد استفاده قرار می‌دهید، بررسی علت عدم دستیابی کامل به اینترنت کاری آسان است چرا که کافی است وضعیت فعال یا خراب‌بودن ابزار مذکور را بررسی نمایید.



یادداشت : *به این مسیریاب یا دیوارآتش نقطهٔ انسداد گفته می‌شود چرا که در صورت خرابی، مکانی است که تمامی ترافیک را مسدود می‌نماید.*

اگر نتوانید آدرسی را خارج از دیوار آتش، مسیریاب، یا سرویس‌دهنده پروکسی خود Ping نمایید می‌توانید مطمئن باشید که نقطهٔ انسداد، مشکل دارد. به خاطر داشته باشید که به‌جای اسم DNS برای Ping کردن از آدرس IP استفاده کنید ـ به این ترتیب مطمئن خواهید شد که مشکلات تحلیل نام را وارد صحنه نکرده‌اید. (در صورت عدم کارکرد اتصالات IP، می‌توان مطمئن بود که تحلیل DNS نیز کار نخواهد کرد).

چگونه تشخیص می‌دهید که کدام آدرس را باید Ping کنم؟ سؤال خوبی است! می‌توانید از فراهم‌کنندهٔ سرویس اینترنت در مورد آدرس «راه‌دور» این مسیریاب سؤال کنید. (منظور رابط مسیریابی است که دور از شما ـ در انتهایی از ارتباط که به سیستم شما متصل نیست ـ قرار گرفته است). همچنین می‌توانید تعدادی آدرس IP از میزبانهای مطمئنی در اینترنت را در دسترس داشته باشید. اغلب یک Ping می‌تواند نام DNS را به آدرس IP تحلیل نماید، بنابراین Ping کردن چند آدرس www و یادداشت‌برداشتن از آنها می‌تواند مفید واقع شود.



نکته : *می‌توانید از traceroute برای ردیابی مسیر تا آدرس WWW مورد علاقهٔ خود استفاده کنید و جهش دومی که traceroute گزارش می‌دهد را یادداشت نمایید. این آدرس احتمالاً آدرس «راه دور» مسیریاب ISP تان می‌باشد.*

من ترجیح می‌دهم که ابتدا ISP خود و آنگاه آدرسی خارجی را Ping می‌کند. اگر ارتباط ISP فعال است اما نمی‌توانید به چیز دیگری دسترسی پیدا کنید ممکن است ارتباط بین ISP و دنیای خارجی مشکلاتی داشته باشد. با اینکه به احتمال زیاد ISP از وجود این مشکل مطلع است، انجام یک تماس و گزارش یک موضوع مضر نخواهد بود.

مشکلات DNS

فرض کنید که اتصال IP تان اشکالی ندارد. با وجود آنکه می‌توانید آدرس‌های IP را Ping نمایید، با واردکردن اسامی حوزه‌ای در صحنه، مرورگر دچار مشکل می‌شود. اشکالی ندارد! اجازه دهید نگاهی داشته باشیم به انواع مشکلات DNS که ممکن است با آنها برخورد کنیم:

- مشکلات داخل-به-خارج ـ نمی‌توانید اسامی DNS مربوط به بقیه را ببینید.
- مشکلات خارج-به-داخل ـ سایرین نمی‌توانند اسامی DNS شما را ببینند.

برای هر دو این دو نوع مشکل، nslookup ابزار مناسبی است. nslookup اجازه می‌دهد که به سرویس‌دهنده DNS مشخص متصل شوید و تعیین نمایید که آن سرویس‌دهنده DNS چگونه در مورد چیزها فکر می‌کند. به بیان دیگر، هنگامی که Ping می‌کنید، مجبور هستید که از سرویس‌دهنده DNS پیکره‌بندی شده برای پشتهٔ TCP/IP خود استفاده کنید، اما nslookup به شما اجازه می‌دهد که از این سرویس‌دهنده گذر کرده و سرویس‌دهنده‌ای را که می‌خواهید با آن صحبت کنید، انتخاب نمایید. می‌توانید سرویس‌دهنده‌ها را از طریق آدرس IP (هنگامی که تغییرنام اصلاً کار نمی‌کند) یا اسم (هنگامی که مشکل عجیبی را ردیابی می‌نمایید) مشخص کنید و به nslookup بگویید که چه نوع اطلاعاتی را برای شما بازگرداند.

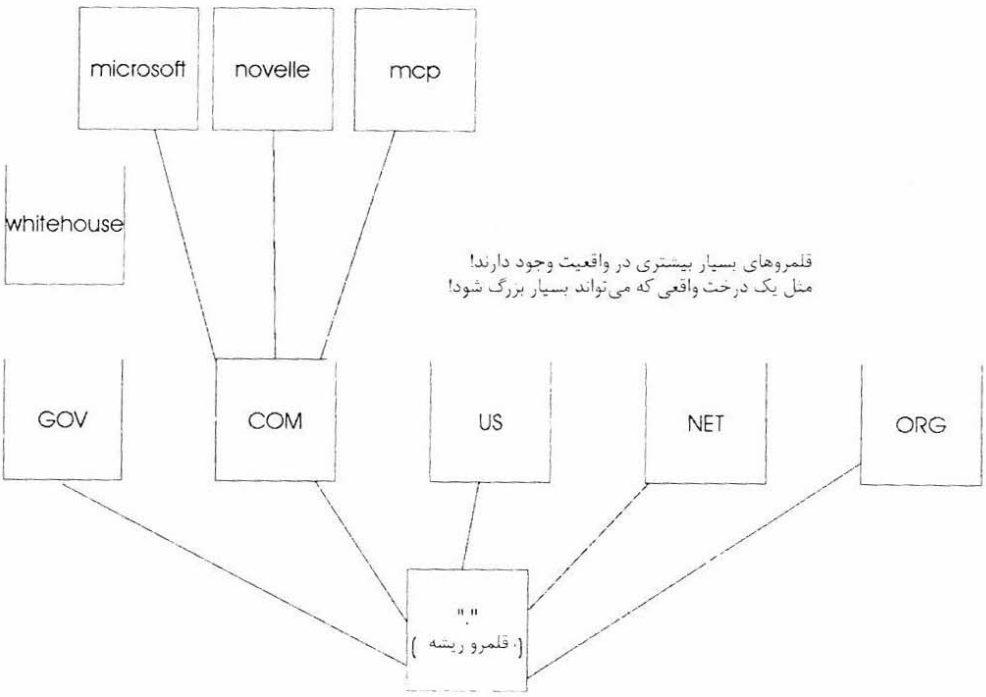


***یادداشت** : از ویندوز ۹۵ یا ۹۸ استفاده می‌کنید؟ با اینکه میکروسافت نسخهٔ کاملاً مشابهی از nslookup در یونیکس برای NT فراهم آورده است، بنا به دلایلی، این برنامه در ویندوز ۹۸/۹۵ مهیا نیست. ناامید نشوید. می‌توانید با جستجو در سایت محلی نرم‌افزارهای اشتراکی (www.shareware.com، www.tuocows.com و نظایر آنها) معادل‌های نسبتاً خوبی را برای nslookup بیابید. من نتوانستم معادل کاملاً دقیقی را پیدا کنم اما بسیاری از برنامه‌ها، کارایی‌هایی نظیر nslookup را ارائه می‌کنند. مثالهایی از این برنامه‌ها عبارتند از:*

- *dns11.zip*
- *nsb32-5 zip*
- *lookup.zip*
- *setuptk.exe*

سلسله‌مراتب DNS

برای آنکه بتوانید به گونه‌ای کارا ابزار nslookup را مورد استفاده قرار دهید، باید اصول سلسله‌مراتب DNS را بشناسید. DNS، نظیر دیسک سخت، رکوردهای مستقل بسیاری دارد که به سطوح مختلف بسیاری تقسیم شده و از یکدیگر مجزا گردیده‌اند (پوشه‌ها در دیسک سخت؛ قلمروها در دنیای DNS). نگاهی به شکل ۶-۱۹ بیندازید. درختی ترسیم شده است که باید از بالا به پایین خوانده شود (قلمروها توسط نقطه از یکدیگر جدا می‌شوند) چندان سخت نیست. این روشی است که کل DNS با آن سازماندهی شده است.



شکل ۶-۱۹ : قلمروهای DNS، نظیر پوشه‌های دیسک سخت در قالب یک ساختار درختی مرتب شده‌اند.

اکنون اجازه دهید چگونگی پیاده‌سازی این موضوع را در دنیای واقعی مورد بررسی قرار دهیم. هر قلمرو اغلب توسط یک سرویس‌دهندهٔ اولیه و چندین سرویس‌دهندهٔ ثانویه مدیریت می‌شود. چگونه مشخص می‌شود که کدام سرویس‌دهنده مسئول کدام قلمرو است؟ هر قلمرو رکورد ویژه‌ای دارد به نام SOA که مخفف عبارت آغاز جواز[1] می‌باشد. جزییات مربوط به اینکه کدام سرویس‌دهنده‌ها مسئول آن قلمرو هستند به همراه سایر رکوردهای مدیریتی و اطلاعات تماس برای دسته‌ای از سرویس‌دهنده‌ها که مسئول آن قلمرو هستند، در رکورد SOA هر قلمرو وجود دارد.

با اینکه سرویس‌دهنده‌های ثانویه اطلاعات خود در مورد قلمرو را از سرویس‌دهندهٔ اولیه دریافت می‌کنند، به غیر از این موضوع کاملاً نظیر سرویس‌دهندهٔ اولیهٔ قلمرو عمل می‌نماید. از آن گذشته سرویس‌دهنده‌های ثانویه ممکن است هر آدرس IP دلخواهی داشته باشند ـ لازم نیست که از لحاظ جغرافیایی یا فیزیکی نزدیک به سرویس‌دهندهٔ اولیه قرار گرفته باشند. قلمرو یک مفهوم «منطقی» است و هیچ محدودیت فیزیکی در مورد آن وجود ندارد.

در نهایت، از آنجا که DNS سلسله‌مراتبی است، اگر سرویس‌دهندهٔ DNS مورد استفادهٔ شما پاسخ یک پرس‌وجوی DNS را نداند، باید پرس‌وجو را به سمت «بالای درخت» و به سرویس‌دهنده قلمرویی فوقانی خود بفرستد تا ببیند که آیا می‌تواند پاسخی دریافت نماید. اگر پاسخی دریافت کند، آن را در حافظهٔ سریع خود ذخیره می‌کند. به این ترتیب اگر همان اسم میزبان دوباره از وی سؤال شود، می‌توانند پاسخ را بدون پرس‌وجو از قلمروی فوقانی خود به سرویس‌گیرنده DNS بازگرداند.

با درنظرداشتن این اطلاعات اجازه دهید نگاهی داشته باشیم به یک مشکل واقعی از نوع داخل-به-خارج در DNS.

نمی‌توانم تو را ببینم!

در سایتی بودم که در جستجوهای DNS خود دچار مشکلات تناوبی بود. برخی اوقات جستجوی DNS به خوبی کار

1- start of authority

می‌کرد؛ بقیه اوقات اینطور نبود ـ کاربران ایستگاههای کاری ویندوز شکایت می‌کردند که پیغام خطایی دریافت می‌کنند حاکی از آنکه ورودی DNSای برای www.company.com وجود ندارد. (در این مثال از اسامی ساختگی استفاده می‌کنیم). با فرض آنکه سرویس‌دهنده DNS سایت در آدرس 200.1.1.6 مسئول قلمرو ci.monkey.ny.us باشد، کارهایی که بلافاصله باید انجام داد به شرح زیر است:

- باید مطمئن شویم که اینترنت آدرس 200.1.1.6 را برای ci.monkey.ny.us به رسمیت می‌شناسد. من به این نکته شک نداشتم اما به‌عنوان اولین هدف خوب است که آن را بررسی نماییم.
- باید «کسی» که سرویس‌دهندهٔ قلمرویی فوقانی ما محسوب می‌شود را پیدا کنیم (ci.ny.us) شک من بر آن بود که این نقطه‌ای است که مشکل از آنجا ناشی می‌شود. هر پرس‌وجویی که در سرویس‌دهندهٔ DNS محلی وجود نداشته باشد، توسط قلمرو فوقانی آن پردازش می‌شود).

برای انجام اولین کار، با استفاده از nslookup به صورت زیر عمل نمودیم:

```
> server a.root-servers.net
Default Server: a.root-servers.net
Address: 198.41.0.4
> set type=soa
> ci.monkey.ny.us
Server: a.root-servers.net
Address: 198.41.0.4

Authoritative answers can be found from:
    US nameserver = NS.ISI.EDU
    US nameserver = RS0.INTERNIC.NET
    US nameserver = NS.UU.NET
    US nameserver = ADMII.ARL.MIL
    US nameserver = VENERA.ISI.EDU
    US nameserver = EXCALIBUR.USC.EDU
    NS.ISI.EDU internet address = 128.9.128.127
    RS0.INTERNIC.NET internet address = 198.41.0.5
    NS.UU.NET internet address = 128.9.176.32
    VENERA.ISI.EDU internet address = 128.9.0.32
        EXCALIBUR.USC.EDU internet address = 128.125.51.11
> server ns.isi.edu
Default Server: ns.isi.edu
Address: 128.9.128.127

> ci.monkey.ny.us
Server: ns.ci.monkey.ny.us
mail addr = hostmaster.ci.monkey.ny.us
        serial = 29981
    refresh = 3600 (1 hour)
    retry = 600 (10 mins)
    expire = 86400 (1 day)
minimum ttl = 3600 (1 hour)
```

به این ترتیب مستقیماً به یک سرویس‌دهنده ریشه رفتیم ـ یعنی سرویس‌دهنده‌ای که مجوز لازم برای تمامی قلمروهای ریشه (com,.us,.gov. و نظایر آن) را داراست ـ و از آن پرسیدیم که آیا در مورد قلمرو موردنظر ما چیزی می‌داند یا خیر. پاسخ حاکی از آن بود که باید به سرویس‌دهندهٔ دیگری برویم یعنی آنکه همه چیز را در مورد حوزهٔ us. می‌دانست. ما از آن سرویس‌دهنده همان سؤال را پرسیدیم و پاسخ مناسبی داده شد، بنابراین مشکلی در ارتباط با شکل و شمایل قلمرو وجود نداشت.



نکته : *تمامی سرویس‌دهنده‌های ریشه علاوه بر بودن در قلمرو «نقطه» یا «ریشه»، همچنین در قلمرو root-servers.net قرار دارند. هر سرویس‌دهنده به همراه یک حرف قرار می‌گیرد. بنابراین می‌توانیم به سرویس‌دهنده‌های b.root-servers.net، c.root-servers.net و نظایر آنها برویم.*

کار بعدی ما آن بود که ببینیم چه قلمرویی بالای ما قرار گرفته است:

```
> monkey.ny.us
Server: ns.isi.edu
Address: 128.9.128.127

Non-authoritative answer:
monkey.ny.us
   origin = Buggy.net
   mail addr = postmaster@Buffy.net.savanah.ga.us
   serial = 1998080901
   refresh = 3600 (1 hour)
   retry = 1200 (20 mins)
   expire = 12096000 (140 days)
   minimum ttl = 14400 (4 hours)

Authoritative answers can be found from:
monkey.ny.us nameserver = dns2.Buggy.net
monkey.ny.us nameserver = dns1.Buggy.net
   dns2.Buggy.net internet address = 128.6.1.9
   dns1.Buggy.net internet address = 128.6.1.10
```

از قرار معلوم سرویس‌دهندهٔ مسئول برای monkey.ny.us، dns.buggy.net نامیده می‌شود که دارای آدرس‌های IP معادل 128.6.1.9 و 128.6.1.10 می‌باشد. از آنجا که این سرویس‌دهنده‌ها در یک زیرشبکه قرار گرفته‌اند، نگاهی به فاصلهٔ آنها و مدت‌زمانی که بسته از اینجا تا نزد آنها می‌رود را مورد بررسی قرار دادیم.

با انجام یک جلسهٔ Ping، مشخص شد که این مدت زمان از ۸۰۰ ms (یک هشتم ثانیه) تا ۱۵۰۰ ms (یک و نیم ثانیه) متغیر است. یک و نیم ثانیه در شبکه، ابدی و جاودانگی است! آیا ممکن است که اتصالی کُند به سرویس‌دهندهٔ قلمرو در بالای درخت مشکلی ایجاد کند؟ البته که اینطور است! DNS مدت زمان کمتری را قبل از تصمیم‌گیری به اینکه پاسخی مهیا نیست، صبر می‌کند و در صورت عدم دریافت پاسخ، پیغام خطایی را به سرویس‌گیرنده می‌فرستد. پس بنابراین ما چگونه این مشکل را حل کردیم؟

در اینجا دو پاسخ وجود دارد. لازم بود که خط اینترنت را ارتقاء دهند چرا که با ترافیکی مواجه بودند که برایشان کُشنده بود (یکی از افراد که در حال انتقال اطلاعات بود آنقدر خط را اشغال کرده بود که ترافیک DNS با سرعت کافی قادر به پاسخگویی نبود). از آن گذشته یک traceroute مشخص کرد که ns.ultra-monkey.net، به اندازهٔ ۱۶ جهش فاصله داشت. ۱۶ جهش مقدار زیادی است. درخواست از ISP به منظور قبول مسؤلیت قلمرو monkey.ny.us نیز کمک زیادی در حل مشکل بود چرا که این بدان معناست که آنها تنها یک جهش بین کاربران و قلمرو والدشان فاصله داشتند.

بعضی اوقات ممکن است سرویس‌دهندهٔ DNS سایرین خاموش باشد. این اغلب به آن معناست که قادر نخواهید بود اسامی DNS مربوط به یک حوزه را مشاهده کنید. بیشتر سایت‌ها دارای چندین سرویس‌دهندهٔ DNS هستند. و بنابراین چنین اتفاقی نباید حادث شود، گواینکه چنین اتفاقی می‌افتد. این بدان معناست که تنها باید صبر کنیم تا مشکل به وجود آمده در آن قلمرو برطرف شود.

به طور خلاصه، مواردی که باعث می‌شوند آدرس‌های خارجی را نتوانیم جستجو کنیم عبارتند از (مشکل پرس‌وجوی داخل-به-خارج):

- فاصلهٔ زیاد بین شما و قلمرو فوقانی
- قابل دستیابی نبودن سرویس‌دهنده‌های DNS فوقانی
- خاموش بودن یا قابل دستیابی نبودن سرویس‌دهندهٔ DNS برای یک قلمرو خاص

نمی‌توانید مرا ببینید!

فرض کنید که نمی‌توانید هیچ‌گونه پُست الکترونیکی را دریافت کنید. گوشی تلفن را برمی‌دارید و با دوستتان تماس می‌گیرید. او به شما می‌گوید که پُست الکترونیکی وی برای خودش بازگشت داده شده است. همچنین به شما می‌گوید که مشغول انجام کاری ضروری است و قبل از آنکه بتوانید جزییاتی را از او بپرسید قطع می‌کند. البته با وجود اینکه او چنین چیزی را ذکر نکرده شما حدس می‌زنید که امکان دسترسی به صفحات وِب شما نیز وجود نداشته باشد. به این موضوع ظنین می‌شوید که با مشکل DNS «خارج-به-داخل» مواجه هستید. چرا که می‌توانید هر جایی که بخواهید Ping نموده و آدرس‌های DNS آنها را تحلیل نمایید.

چگونه می‌توانید بررسی کنید که دنیای خارج شما را چگونه می‌بیند؟ اولین کاری که باید انجام دهید استفاده از nslookup است. اجازه دهید که این کار را با وارسی سرویس‌دهندهٔ DNS که متهم اصلی می‌باشد آغاز کنیم:

```
$ nslookup - dns.frob.com
Default Server: dns.frob.com
Address: 167.195.160.6

> www
Server: dns.frob.com
Address: www.frob.com

Name: wizard.frob.com
Server: 167.195.160.10
Address: www.frob.com

> mail
Server: dns.frob.com
Address: 127.0.0.1

Name: dragon.frob.com
Server: 167.195.160.8
Address: mail.frob.com
```

هوم. از دیدگاهی محلی همه چیز مرتب به نظر می‌رسد.



یادداشت : بسیاری (اما نه همه) سرویس‌دهنده‌های DNS در اینترنت، «dns» یا «ns» نامیده می‌شوند تا مشخص شوند که سرویس‌دهندهٔ اسم حوزه و یا تنها سرویس‌دهنده‌های عمومی اسم می‌باشند.

خوب، سرویس‌دهندهٔ DNS شما در واقع با دنیا ارتباط دارد ـ هنگامی که پرس‌وجوهایی در مورد حوزهٔ شما را دریافت می‌کند، به خوبی پاسخ می‌دهد. اما در غیراین‌صورت باید کار عیب‌یابی را عمقی‌تر صورت دهید: آیا غیرفعال است؟ آیا فایل‌های داده‌ای آن خراب شده‌اند؟ (در این صورت باید کار بازنشانی از یک کپی پشتیبان را انجام دهیم).

سرویس‌دهندهٔ DNS سالم است، بنابراین مشکلات ممکن دیگر را مدنظر قرار می‌دهیم. استفادهٔ دوباره از nslookup می‌تواند در پیداکردن اینکه سرویس‌دهنده‌های ریشه چگونه به دیگران می‌گویند که سرویس‌دهندهٔ شما را جستجو کند، مؤثر واقع شود. به عبارت دیگر، لازم است که به رکورد SOA از حوزهٔ شما نگاهی داشته باشیم:

```
$ nslookup - moria.co.chatham.ga.us
Default Server: Moria.co.chatham.ga.us
Address: 167.195.160.6

> set type=soa
>server a.root-servers.net
Default Server: a.root-server.net
Address: 198.41.0.4

>frob.com.
Server: a.root-servers.net
Address: 198.41.0.4

Authoritative answers can be found from:
frob.com nameserver = NS4.frob.com
frob.com namesarver = NS2.com
NS4.frob.com internet address = 167.195.160.15
NS4.frob.com internet address = 167.195.160.6
```

چه اتفاقی افتاده است؟ یک آدرس IP برای سرویس‌دهنده در اینجا ذخیره شده که شما چیزی در مورد آن نمی‌دانید. در واقع چنین نیست، این آدرس سرویس‌دهنده‌ای است که قرار است ماه آینده و نه این ماه به جریان بیافتد. از قرار معلوم یکی از همکارانتان به اینترنت سرویس‌دهندهٔ اسم شما به این آدرس جدید تغییر یافته است. متأسفانه سرویس‌دهندهٔ نام فعلی بنا بر یک اشتباه در فهرست جاری ذکر نگردیده است. مراجعه‌ای سریع به صفحهٔ www.internic.net و بحثی با همکارتان مسئله را حل می‌کند.

این سناریو کمی بعید به نظر می‌رسد (گو اینکه من با آن مواجه شده‌ام). البته مثال خوب و ایدهٔ جالبی در مورد انواع مشکلاتی است که می‌تواند در دنیای DNS به وقوع بپیوندد. شرکتهایی را دیده‌ام که سرپرست ناراضی سیستم بعد از ترک شرکت اسم حوزه را ربوده است. بنابراین شرکت قادر به دریافت پُست الکترونیکی یا برقراری تماسهای وِب از خارج از مجموعهٔ خود نخواهد بود.

آیا وقوع این امر ممکن است؟ متأسفانه بله. در هر ورودی DNS دو تماس ظاهر می‌گردد. یکی از آنها مربوط به سرپرستی و دیگری مربوط به تماس فنی است. اگر سرپرست سیستم خود را به عنوان هر دو معرفی کند می‌تواند آدرس را به آدرس خانهٔ خویش تغییر دهد و آنگاه بعد از ترک شرکت، رکورد SOA را با چیز دیگری عوض کند. از نقطه‌نظر فنی کار چندانی در این‌باره نمی‌توان انجام داد. بهتر آن است که از نقطه‌نظر شغلی وارد عمل شد: InterNIC (www.internic.net) را از آنچه که اتفاق افتاده مطلع کرده و وارد یک «جدال اسم حوزه» شوید. به این صورت ممکن است بتوانید بدون نیاز به پیگیری قانونی اسم حوزهٔ خود را پس بگیرید.

مشکلات مسیریابی

فرض کنید که می‌توانید به سایت‌های وِب خاصی بروید اما به برخی از سایت‌ها دسترسی ندارید ـ یا اینکه پُست الکترونیکی‌تان در بعضی از سایت‌ها با مشکل مواجه می‌شود. بهترین کاری که در چنین مواردی می‌توانید انجام دهید، بعد از حصول اطمینان از توانایی در تحلیل نام، انجام traceroute به آدرس IP سایت می‌باشد.

برای مثال سیستم کتابخانهٔ ما در دستیابی به آدرس وِب خاصی مشکل داشت. من با استفاده از traceroute روی آدرس IP، متوجه شدم که بستهٔ traceroute‌ام مرتباً بین دو مسیریاب به گردش درمی‌آید. این حلقهٔ مسیریابی مشخص‌کنندهٔ یک مشکل مسیریابی بود، اما تشخیص اینکه چه کسی مسئول قضیه است اندکی مشکل می‌نماید.

من مشکل را به ISP کتابخانه گزارش دادم و همچنین پرسنل مسئول مسیریاب‌ها را در جریان گذاشتم. چگونه شخص

مسئول مسیریاب را پیدا می‌کنید؟ در اینجا هم nslookup کارساز است!

هر آدرس IP در اینترنت باید (اما همیشه اینطور نیست) یک اسم DNS متناظر در قلمرو مخصوصی به نام in.addr.arpa داشته باشد. این به آن خاطر است که بتوانید سریعاً یک آدرس IP را با استفاده از نوع خاصی از رکورد به نام اشاره گر یا *PTR* به اسم DNS تحلیل نمایید. اگر در SOA اسم DNS ـ یا شمارهٔ شبکه ـ را پیدا کنید می‌توانید به صورت مکرر گروه مسئول برای آدرس را بیابید. تنها نکتهٔ مهم آن است که باید آدرس را به صورت برعکس وارد نمایید. این کار، برای سهولت‌بخشیدن به کار قلمروهای DNS است. البته لازم نیست که خیلی نگران آن باشید ـ تنها نکتهٔ مهم آن است که آدرس‌ها سر و ته وارد شوند. برای مثال، فرض کنید دو مسیریابی که حلقه را ایجاد کرده بودند، در 192.168.1.10 و 192.168.2.5 قرار داشتند. در طی جلسهٔ عیب‌یابی از nslookup به شکل زیر استفاده نمودم:

```
$ nslookup
> set type=PTR
> 10.1.168.192.in-addr-arpa
Server: dns.frob.com
Address: 209.52.182.122

10.1.168.192.in-addr.arpa name = router10.foo.net

> 5.2.168.192.in-addr.arpa
Server: dns.frob.com
Address: 209.52.182.122

5.2.168.192.in-addr.arpa name = router5.foo.net

> (Ctrl-D)
$ whois foo.net
[rs.internic.net]

   Registrant:
John E. Monster (FOONET-DOM)
P.O. Box 4242
Indianapolis, IN 46219

Domain Name: FOO.NET

Administrative Contact:
Monster, Jhon E. (JEM12) monster@FOO.NET
317-555-1400 ext. 5066 (FAX) 317-555-1800
Technical Contact, Zone Contact:
Monster, Joey (JM48) joey@FOO.NET
317-555-1400 ext.5067
Billing Contact:
Monster, John E. (JEM12) monster@FOO.NET
317-555-1400 ext. 5066 (FAX) 317-555-1800

Record last updated on 07-Aug-98.
Record created on 25-Sep-97.
Database last updated on 29-Sep-98 08:19:55 EDT.
```



نکته *: می‌توانید اطلاعات مربوط به مسئولیت را در مورد هر قلمرو با استفاده از برنامهٔ کمکی whois پیدا کنید. در صورتی که از یونیکس استفاده نمی‌نمایید، برخی از برنامه‌های کمکی ویندوز چنین کاری را برایتان انجام می‌دهد ـ برای مثال Internet Anywhere Toolkit (www.tnsoft.com).*

خوب، حالا اطلاعات کافی برای گزارش این شیطنت‌ها را در اختیار دارم. صاحب هر دوی مسیریاب‌ها foo.net می‌باشد. اجرای whois روی foo.net آدرس پُست الکترونیکی فرد مسئول برای این قلمرو را به دست می‌دهد. من برای ISP و

joey@foo.net نامه‌ای الکترونیکی فرستادم که حاوی خروجی traceroute بود و به آنها گفتم که با کدام آدرس traceroute را انجام داده‌ام، مشکل در عرض چند ساعت حل شد. برخی اوقات نامهٔ دوستانه‌ای دریافت می‌کنید که علت بروز مشکل را توضیح می‌دهد ـ برخی اوقات هم با سکوت سنگینی مواجه می‌شوید. به شخصه با هر دوی این موارد مواجه شده‌ام، اما حداقل توانسته‌ام به کارکنان کتابخانه بگویم که مشکل چیست و من آن را گزارش نموده‌ام.

عیب‌یابی در اینترانت

اگر شما اینترانت پیچیده‌ای با قلمروهای چندگانه DNS دارا هستید، عیب‌یابی آن را می‌توانید به صورت رفع اشکال در اینترنت ـ با nslookup، traceroute و ping ـ به انجام برسانید. به طرز مشابهی، برنامه‌هایی که اینترانت را به‌اجرا درمی‌آورند، طبیعت مشابهی با برنامه‌های اجرایی در اینترنت دارند و بنابراین می‌توانید از تکنیک‌های بحث‌شده در بخشهای آتی در سرویس‌دهنده‌های اینترنت خود نیز استفاده نمایید.

سرویس‌دهندهٔ وِب

تکنیک عیب‌یابی سرویس‌دهنده وِب مورد علاقه من (که به صورت خلاصه در فصل ۱۸ ذکر نمودم)، عبارت است از Telnet کردن به سوکت ۸۰ مربوط به سرویس‌دهندهٔ وِب و بررسی امکان استفاده از دستور GET HTTP. بیشتر اوقات این کار باعث می‌شود سرویس‌دهنده صفحهٔ شاخص اصلی را برایم ارسال کند. اگر موفق شوم، این بدان معناست که سرویس‌دهنده به درخواستهای HTTP پاسخ می‌دهد و کاربران نباید مشکلی در دسترسی به سرویس‌دهنده به منظور دریافت صفحات HTML داشته باشم. این موضوع نشانگر آن است که شبکهٔ موجود بین شما و سرویس‌دهندهٔ وِب عاری از خرابی است.

بیشتر مشکلات سرویس‌دهندهٔ وِب در سه رده قرار می‌گیرند:

- مشکلات قابلیت اطمینان
- مشکلات سرویس‌دهندهٔ سوم
- مشکلات شبکه

در اینجا مشکلات شبکه را به بحث نخواهیم گذاشت ـ می‌توان با استفاده از تکنیک‌هایی که در بخش «آشفتگی مجازی» و فصل ۱۷ و ۱۸ ذکر گردیده‌اند، با آنها کنار آمد.

مشکلات قابلیت اطمینان

این مشکلات در دو زیررده جای می‌گیرند:

- مشکلات ظرفیتی (سربار در سرویس‌دهنده)
- مشکلات خرابی (سرویس‌دهنده با نمایش صفحهٔ آبی، آشفتگی درون هسته و نظایر آنها از کار می‌افتد)

اگر سرویس‌دهنده‌تان به صورت واقعی آنقدر محبوب باشد که با سربار کاری (احتمالاً در صورتی که سرویس بسیار پرطرفداری را از طریق اینترنت ارائه کنید) مواجه شود، بهتر است که اول فایل‌های ثبتی سرویس‌دهنده را بررسی کنید. آیا

موارد موجود «رسمی» هستند؟ یا اینکه یکی از کاربرانتان صفحهٔ وِب غیرکاری (اما خیلی پرطرفدار) را پُست نموده است؟ مواجه‌شدن با سربار روی سرویس‌دهنده‌ای که به اینترنت متصل نیست، از احتمال کمی برخوردار است. بیشتر سرویس‌دهنده‌های وِب می‌توانند صدها و حتی هزاران کاربر را بدون بروز هیچ مشکلی مدیریت نمایند. اما در صورتی که صدها درخواست در هر ثانیه داشته باشید، واقعاً با یک مشکل مواجه هستید.

اگر واقعاً می‌خواهید تا این اندازه محبوب باشید، باید فایل‌های ثبتی خود را جمع‌آوری کنید و ISP و فروشندهٔ سرویس‌دهنده را نیز دخیل نمایید، حتی بهتر است دو چیز را ارتقا دهید: سرویس‌دهندهٔ وِب و اتصال اینترنت. بسته به مقدار اطلاعات وِب که فایل‌های ثبتی انتقال آن را نشان می‌دهند، دو فروشندهٔ مذکور می‌توانند در مورد نحوهٔ ارتقا توصیه‌هایی را ارائه دهند.

این احتمال، بخصوص در مورد یک سرویس‌دهندهٔ اینترانت مجزا از اینترنت وجود دارد که مشکلات شما از نوع مشکلات خرابی می‌باشند. نهراسید ـ بیشتر مشکلات قابلیت اطمینان به نگارش نرم‌افزارها یا وجود نرم‌افزارهای دیگر در سرویس‌دهنده مربوط می‌شوند. حتماً آخرین نگارش‌ها و/یا اصلاحیه‌های سرویس‌دهندهٔ وِب مورد استفاده خود را به‌کار ببندید همچنین می‌توانید در مورد سرویس‌هایی که روی سرویس‌دهنده به اجرا درمی‌آیند از روش‌های تفرقه‌بیانداز ـ و ـ حکومت کن و کنارگذاشتن، استفاده نمایید.

برای مثال، من یک سرویس‌دهندهٔ NFS را روی یک سرویس‌دهندهٔ NT در ارتباط با سرویس‌دهندهٔ وِب اجرا نمودم. سرویس‌دهنده برپایه منظمی از کار می‌افتاد ـ یعنی تا زمانی که سرویس‌دهندهٔ NFS را برداشتم و سرویس‌دهندهٔ NFS ای متعلق به فروشندهٔ دیگری را جایگزین نمودم.

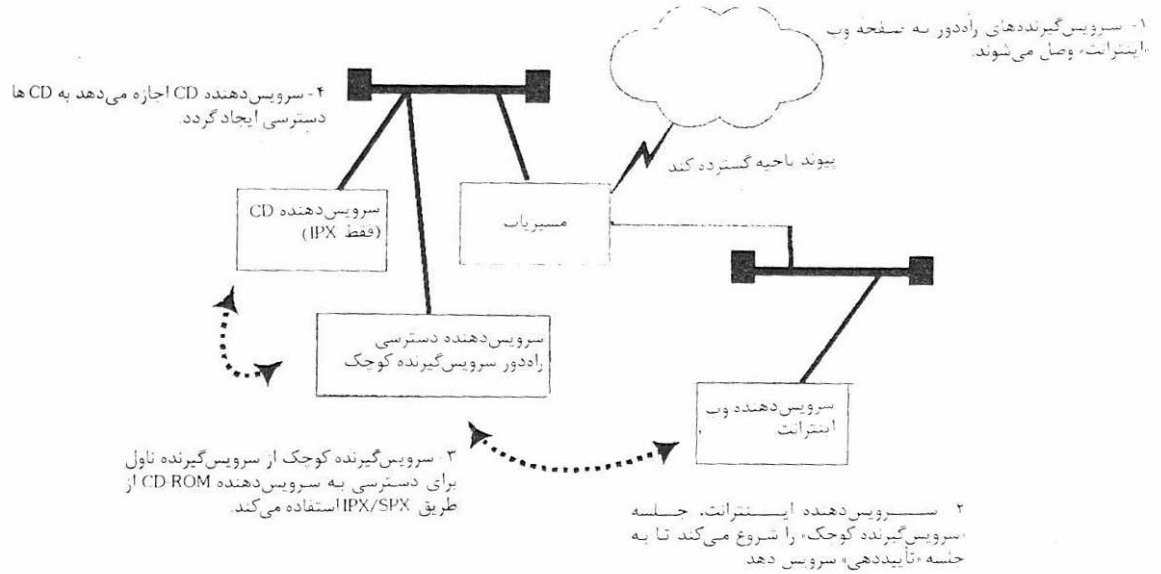
بهتر است سعی کنیم در مورد بسته‌های سرویس مربوط به سیستم‌عامل خود به‌روز باشید. برای مثال، در این هنگام که این نوشته به تحریر درمی‌آید، سرویس‌دهندهٔ NT نگارش ۴ باید Service Pack 3 را نصب نموده باشد و به زودی Service Pack 4 نیز در دسترس خواهد بود.

به طور خلاصه می‌توانید بر مشکلات قابلیت اطمینان در سرویس‌دهندهٔ وِب، با تمرین روش تفرقه‌بیانداز ـ و ـ حکومت‌کن از فصل ۴ و جستجوی پیغامهای خطای ویژه با استفاده از تکنیک‌های فصل ۷ فایق شوید.

مشکلات سرویس‌دهندهٔ سوم

با وجود اینکه سرویس‌دهندهٔ وِب به نرمی کار می‌کند و پاسخگوی درخواستهای HTML می‌باشد، ممکن است هنوز مشکلاتی را در برنامه‌های کاربردی اینترانت خود تجربه نمایید. برنامه‌های اینترانت به بیش از یک سرویس‌دهنده اتکاء دارند، بنابراین بهتر است نموداری از چگونگی تراکنش این برنامه‌ها با یکدیگر تهیه نمایید. برای مثال، در شکل ۷-۱۹، نموداری از یک برنامهٔ کاربردی اینترانت به نام Knowledgenet را نشان می‌دهد. ملاحظه کنید که چگونه سرویس‌دهندهٔ وِب خود به تنهایی یک بخش و یک قطعه از کل است. برای آنکه برنامهٔ کاربردی عمل نماید، سرویس‌دهندهٔ کنترل از راه دور «سرویس‌گیرندهٔ کوچک» باید بتواند عمل نماید و سرویس‌دهندهٔ CD-ROM نیز باید بتواند کار خود را به انجام برساند. توجه کنید که سرویس‌دهندهٔ CD-ROM تنها قادر است به IPX/SPX صحبت نماید و اصولاً یک سرویس‌دهندهٔ ناول است ـ یعنی براساس TCP/IP کار نمی‌کند.

کلام آخر آنکه: حتی با وجود عملکرد سرویس‌دهندهٔ وِب، هر بخش و هر مؤلفه که به درستی کار نکند باعث توقف کارکرد برنامهٔ کاربردی اینترانت می‌گردد. دوباره در اینجا باید گفت که مستندات کلید حل مشکل می‌باشند؛ اگر کسی به شما بگوید که برنامهٔ کاربردی Knowledgenet کار نمی‌کند و شما این نمودار را در اختیار داشته باشید، طبیعتاً می‌دانید که کدام سرویس‌دهنده را وارسی نمایید.



شکل ۷-۱۹ : یک مثال از اینترانت چندسرویس‌دهنده‌ای، چندپروتکلی «سرویس‌گیرندهٔ کوچک».

مشکل در پُست الکترونیکی؟

پُست الکترونیکی شخصی در اصل یک برنامهٔ سرویس‌گیرنده/سرویس‌دهنده یا در برخی از حالات یک برنامهٔ اشتراک فایلی ویژه می‌باشد. هنگامی که مشکلی در سیستم پُست الکترونیکی شخصی شما به وجود می‌آید (سیستم‌هایی مثل GroupWise ، Lotus Notes یا Exchange) بهتر است که مستندات محصول را بررسی کرده و از تکنیک‌های عیب‌یابی سرویس‌گیرنده/سرویس‌دهنده یا فایل ـ و ـ چاپ که در فصل ۱۸ مورد بحث قرار دادیم، استفاده نماییم.

هریک از این سیستم‌ها استانداردهای اینترنت/اینترانت را نیز پشتیبانی می‌کنند و دروازه‌هایی را برای کارکردن با اینترنت در اختیار می‌گذارد. پُست الکترونیکی اینترنت (و در نتیجه اینترانت) دارای سه مؤلفه است:

- SMTP ـ پروتکل سادهٔ انتقال پست (ارتباط سرویس‌دهنده به سرویس‌دهنده)
- POP ـ پروتکل دفتر پستی (ارتباط سرویس‌گیرنده به سرویس‌دهنده)
- IMAP ـ پروتکل کاربردی پست اینترنت (ارتباط سرویس‌گیرنده به سرویس‌دهنده)

می‌توانید از طریق Telnet کردن به سوکت ۲۵، فعال‌بودن دروازه‌های SMTP و قابلیت پذیرش اتصالات را وارسی نمایید. در اینجا مثالی ارائه شده است:

```
$ telnet wpo 25

Trying 167.195.160.7...
Connected to wpo.co.chatham.ga.us.
Escape character is '^]'.
220 wpo.co.chatham.ga.us GroupWise SMTP/MIME Daemon 4.11 Ready
1993, 1996 Novell, Inc.
```

همچنین می‌توانید به سوکت POP (سوکت ۱۰۹ و ۱۱۰، بسته به نگارش POP مورد استفاده) Telnet کنید. و همچنین سوکت IMAP (سوکت ۱۴۳) تا مطمئن شوید که سرویس‌دهنده‌هایی که تصور می‌شود این گونه اتصالات را مورد پذیرش قرار می‌دهند، فعال می‌باشند. یک مثال عبارت است از:

```
$ telnet moria 143
Trying 167.195.160.6...
Connected to moria.co.chatham.ga.us.
Escape character is '^']

* OK moria.co.chatham.ga.us IMAP4rev1 v10.170 server ready
```

اگر در دریافت پستی از دنیای خارج از طریق اینترنت به اینترانت خود مشکل دارید، بهتر است با استفاده از nslookup رکورد MX قلمرو خود را بررسی نمایید. رکورد *MX*، رکورد ویژه‌ای است که «تبادلگر پستی» مربوط به قلمرو شما را نشان می‌دهد. به مثال زیر توجه کنید:

```
$ nslookup
> set tupe=mx
> co.chatham.ga.us
co.chatham.ga.us    preference = 10, mail exchanger = moria.co.chatham.ga.us
moria.co.chatham.ga.us internet address =167.195.160.
```

اگر سرویس‌دهندهٔ درستی انتخاب نشود و یا اصولاً سرویس‌دهنده‌ای موجود نباشد، بهتر است روی سرویس‌دهندهٔ DNS خود تغییر را اِعمال نمایید و یا از ISP خود این کار را درخواست کنید.

مشکلات شماره‌گیری

آیا هنگام انجام شماره‌گیری از انواع زیر با مشکلاتی مواجه می‌شوید؟

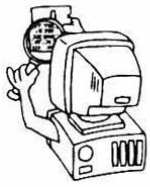
- شماره‌گیری از اینترانت به اینترنت
- شماره‌گیری از اینترانت به اینترانت سایرین

شماره‌گیری از اینترانت به اینترنت؟ حتی هنگامی که اتصال اینترنت وجود دارد؟ نخندید ـ بیش از آنچه که فکر می‌کنید این امر به وقوع می‌پیوندد. این یک سیاست بازدارنده است که باعث می‌شود اینترنت مورد استفاده شخصی قرار نگرفته و توسط افراد به منظور مشاغل غیرکاری به‌کار نرود.

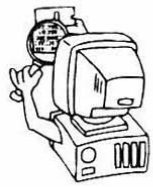
شماره‌گیری IP شبکه به منظور برقراری تماس با اینترانت سایرین هم بسیار معمول است. بنابراین نگاهی خواهیم داشت به نکات فنی شماره‌گیری IP شبکه به IP شبکه دیگر (چه اینترنت و چه اینترانت)، در کنار برخی از مشکلات عمومی که ممکن است با آنها برخورد نماییم.

شماره‌گیری DNS

هنگامی که شبکهٔ IP شخص دیگری را شماره‌گیری می‌کنید، از شماره‌های IP آن شخص در یکی از رابط‌های خود استفاده می‌کنید و همچنین بر سرویس‌دهنده‌های DNS آن شخص برای جستجوی آن اسامی اتکا می‌نمایید. از آنجا که این سرویس‌دهنده‌های DNS، اسامی سمبولیک سرویس‌دهنده‌های شما را نگهداری نمی‌کنند، این امکان وجود دارد که تحلیل نام در مورد میزبانهای محلی با شکست مواجه شود. از آنجا که سرویس‌دهنده DNS به جای شکست در جستجو و عدم ارائهٔ پاسخ، پیغام «چنین میزبانی وجود ندارد» را بازمی‌گرداند، کامپیوتر شما برای تلاش مجدد به سرویس‌دهنده DNS بعدی نخواهد رفت ـ درخواست شما به سادگی به شکست می‌انجامد.



نکته : *بهتر است کاربران را از این موضوع که ممکن است آنان قادر نباشند هنگام شماره‌گیری شبکهٔ دیگر به برنامه‌های TCP/IP «محلی» دسترسی پیدا کنند، مطلع سازید.*



نکته : *شبکه‌سازی شماره‌گیری میکروسافت امکان «clear the existing DNS servers» را فراهم می‌آورد که اجازه می‌دهد کاربران بدانند که نباید این کار را انجام دهند؛ در غیر این صورت قادر نخواهند بود به سرویس‌های شبکه‌ای محلی شما دسترسی داشته باشند.*

می‌توانید تا سه ورودی DNS را در Control Panel ویندوز وارد نمایید. اگر کاربری دارید که از خارج از اینترانت شما شماره‌گیری می‌نماید، نباید بیشتر از دو مورد را در محل مذکور تعیین نمایید. دلیل این کار آن است که در صورت وجود سه مورد از قبل، هنگامی که آداپتور شماره‌گیر تلاش می‌کند که یک مورد را اضافه نماید (برای شبکه راه دور)، با شکست مواجه می‌شود و کاربر قادر نخواهد بود اسامی راه دور را تحلیل نماید.

خلاصه

اینترانت شما بسیار نظیر اینترنت عمل می‌کند ـ تنها در مقیاسی کوچکتر. بر این اساس، استراتژیهای عیب‌یابی بین این دو مشترک است.

یکی از بخشهای آماده‌شدن برای عیب‌یابی اتصال اینترنت تشخیص نوع اتصال است. بعد از انجام این کار، بهتر است با استفاده از nslookup، ping و traceroute نحوهٔ کارکرد این ابزار را در دیوار آتش خود بررسی نمایید. برای آنکه بتوانید موضوعات اتصالی IP را در مقابل مشکلات DNS کنار بگذارید، بهتر است چند شمارهٔ IP مربوط به میزبانهای قابل اطمینان در شبکه را تهیه کرده، در دسترس قرار دهید.

اگر دارای یک بخش DMZ (ناحیهٔ غیرنظامی) «در جلوی» دیوار آتش خود هستید، می‌توانید حتی با وجود عدم فراهم‌آوردن امکان کارکرد ابزار تحلیلی توسط دیوار آتش، کامپیوتری همراه یا ایستگاه کاری دیگری را به منظور اهداف عیب‌یابی مورد استفاده قرار دهید.

کمی دانش DNS هنگام مواجه‌شدن با مشکلات اینترنتی، بسیار مثمر ثمر خواهد بود ـ چه اینکه مشکل مربوط به تحلیل اسم میزبان از جانب شما باشد و یا آنکه سایرین نتوانند میزبانهای شما را مشاهده نمایند. ابزار nslookup کمک زیادی هنگام عیب‌یابی موضوعات DNS ارائه می‌نماید.

مشکلات مسیریابی را می‌توان نظیر مشکلات مسیریابی شبکه شخصی حل نمود؛ کلید معما در یافتن مسؤولان مسیریاب‌های مشکل‌زا و آگاه‌کردن آنان است. در اینجا هم nslookup رهگشا خواهد بود!

مشکلات سرویس‌دهنده وِب و برنامه‌های کاربردی اینترانت اغلب به مسائل ظرفیت، قابلیت اطمینان یا اصولاً به سرویس‌دهندهٔ کامل متفاوتی مربوط می‌شود (مثل سرویس‌دهنده CD-ROM در مثال قبل). با اینکه ممکن است سوخت سرویس‌دهنده‌ای به اتمام برسد، این موضوع در مورد بیشتر سرویس‌دهنده‌های اینترانت صادق نیست. مستندات خوب و به‌روزنگهداشتن سیستم‌عامل و استفاده از سطوح اصلاحیهٔ به‌روز برای سرویس‌دهنده وِب، می‌تواند مشکلات بسیار زیادی را به صورت خودکار برایتان حل نماید.

کارگاه

پرسش و پاسخ

پرسش : خوانده‌ام که اینترنت از پروتکل‌های مسیریابی متفاوتی نسبت به شبکهٔ محلی استفاده می‌کند، بنابراین چگونه می‌توان تکنیک‌های عیب‌یابی در اینترانت را در اینترنت نیز مورد استفاده قرار داد؟

پاسخ : درست است، مسیریاب‌های اینترنت از تنوع زیادی برخوردار هستند. اما با وجود این تنوع، همگی آنها باید از قوانین اصلی مسیریابی پیروی کنند: هر بسته که از یک رابط وارد می‌شود باید به رابط دیگر فرستاده شود و (جهش بعدی) شکل گیرد یا اینکه در صورت در دسترس‌نبودن مقصد دور انداخته شوند. در حقیقت، پروتکل‌های مسیریابی تنها روشهایی برای به‌روزدرآوری جداول مسیریابی هستند ـ به همین خاطر اهمیتی برای ما ندارد، چرا که ما ISP نیستیم. ما فقط مشکل را مشخص نموده و آن را گزارش می‌کنیم. اگر بسته‌ای آن طور که مورد انتظار است عمل نمی‌نماید، مشکل قابل گزارشی داریم و مسؤولیت ما در اینجا به اتمام می‌رسد. کلام آخر اینکه: تا آنجا که بسته‌های ما به خوبی در مسیر خود به گردش درمی‌آیند، نگرانی در ارتباط با پروتکل‌های مسیریابی متوجه ما نیست. و ISP باید در این باره عمل نماید.

پرسش : سرویس‌دهندهٔ پروکسی من به صورت مستقیم از طریق یک خط استیجاری به ISP متصل شده است و من نمی‌توانم از ping، traceroute و nslookup از میان آن استفاده کنم. می‌خواهم بتوانم مشکلات خود را عیب‌یابی کنم، اما DMZ ندارم و دیوار آتش در سر راه قرار دارد! پیشنهادی دارید؟

پاسخ : از ISP خود یک حساب شماره‌گیری دریافت کنید (ممکن است بتوانید برای این کار هزینه‌ای را پرداخت نکنید البته در صورتی که خط استیجاریی که برای بخش اصلی کارتان به‌کار می‌رود بزرگ و گرانقیمت باشد) و عیب‌یابی را با استفاده از آن انجام دهید. حساب شماره‌گیری به شما اجازه می‌دهد که در DMZ مربوط به ISP قرار گیرید و باید بتوانید از روال‌های استاندارد عیب‌یابی از طریق آن نقطه استفاده نمایید.

آزمون

۱- منظور از ISP چیست؟

الف ـ شریک فراهم‌آورندهٔ اینترنت
ب ـ فراهم‌آورندهٔ سرویس اینترنت
ج ـ فراهم‌آورندهٔ سرویس داخلی
د ـ هیچ یک از موارد فوق

۲- کدامیک از موار زیر روشی معمول در اتصال به ISP است؟

الف ـ اتصالات تلفنی ایستگاه‌کاری
ب ـ اتصال مستقیم دیوار آتش یا پروکسی به ISP
ج ـ نه الف و نه ب
د ـ هم الف و هم ب

۳- DMZ به چه معناست؟

الف ـ قلمرو اصلی DNS
ب ـ قلمرو غیرنظامی
ج ـ ناحیهٔ ممنوع
د ـ قلمرو ناشناختهٔ DNS

۴- ابزار اصلی برای تحلیل مشکلات DNS چیست؟

الف ـ dnslookup
ب ـ nslookup
ج ـ ping
د ـ traceroute

۵- اگر سرویس‌دهندهٔ DNS ای که از آن سؤالی پرسیده‌شده، پاسخ سؤال را نداند، چه کار باید انجام دهد؟

الف ـ فریاد بزند و گریه سردهد
ب ـ از یکی از سرویس‌دهنده‌های فایل داخلی شما سؤال کند
ج ـ از سرویس‌دهنده قلمرویی «والد» خود سؤال کند
د ـ از ISP سؤال کند

۶- درست یا نادرست؟ هر SOA حاوی اطلاعاتی در مورد سرویس‌دهنده‌های اسم قلمرو و نقطهٔ تماس می‌باشد.

۷- برای جستجو اسم میزبان مربوط به میزبان 167.195.160.6، بعد از اجرای nslookup و تایپ‌کردن دستور set type=ptr، چه چیزی را وارد می‌کنید.

الف ـ 167.195.160.6.in-addr.arpa
ب ـ 6.160.195.167.in-addr.arpa
ج ـ 6.160.195.167.in-reverse..arpa
د ـ 167.195.160.6.in-address.arpa

پاسخ به سؤالات آزمون

۱- الف
۲- د
۳- ب
۴- ب
۵- ج
۶- درست
۷- ب

فصل ۲۰

عیب‌یاب‌های شبکه تنها می‌خواهند سرگرمی داشته باشند

لعنت برتو! تو می‌دانی که هدف ما آن است که عکس آنچه را که می‌خواهی به تو بدهیم! از آنجا که تو چیزی نمی‌خواهی، ما باید همه چیز به تو بدهیم!

Dilbert از Scott Adams، ۱۹۹۸

فرض کنید که رئیس‌تان از شما خواسته است با عیب‌یابی شبکه آشنا شوید. تا اینجای کار او خیلی خوب عمل کرده و این کتاب را به شما داده است، شما را به کلاسهایی فرستاده و همه چیز عالی به نظر می‌رسد. یک مشکل آن است که تقریباً هیچ وقت چیزی خراب نمی‌شود. گویی که شبکه می‌داند شما آماده شده‌اید و منتظر است که نگهبان شما به خواب برود - مشکلات شبکه‌ای هنگامی به وقوع می‌پیوندند که شما آموخته‌های خود را فراموش کرده‌اید.

خوب، شما می‌توانید نقشه‌های مکارانهٔ آنها را با تکیه بر روشهای عیب‌یابی خود نقش برآب کنید. این فصل مطالبی را در اختیار شما می‌گذارد که به منظور انجام بازیهای مختلف و استفاده از اسباب‌بازیهای غیرکاری دیوار آتش یا سرویس‌دهندهٔ پروکسی نیاز دارید. چرا که نه؟ شما به سختی کار کرده‌اید و شایستگی آن را دارید. این فصل برای شما که مستقیماً به آن مراجعه کرده‌اید، چیزی ندارد! فرض بر آن است که ۱۹ فصل قبل را به خوبی مطالعه کرده‌اید و با عیب‌یابی TCP/IP بخصوص مفاهیم فصل ۱۸ و ۱۹ آشنا هستید.

یادگیری چگونگی استفاده از بازیها (البته در زمان مربوط به خود) و اسباب‌بازیهای اینترنت روش تمرینی بسیار خوبی برای عیب‌یابی اینترنت و سرویس‌گیرنده/سرویس‌دهنده می‌باشند. این کار به شما یاد می‌دهد که چگونه انواع تکنیک‌های عیب‌یابی را بر پایه‌ای غیربحرانی به انجام برسانید - به بیان دیگر، لازم نیست که تحت فشار عصبی در کمک به شخص دیگر مطالب لازم را فراگیر کنید. از آن گذشته، تجربهٔ بیشتری در مورد تکنیک‌های عیب‌یابی خواهید داشت که در زمان وقوع مشکلات واقعی به‌کار خواهد آمد. کمک به افراد در انجام سرگرمی‌ها فواید زیر را داراست:

- سرگرم‌کننده است
- تمرین آموزشی خوبی است
- روش مفیدی در ایجاد آمادگی در کاربران است
- روشی است برای اجتناب از به‌وجودآمدن محیط کاری نظیر Dilbert

همان گونه که خواهید دید، پیکربندی اسباب‌بازیها برای استفاده در شبکه، دانسته‌های شبکه‌ای شما را با توانایی استفاده از سوکت‌های شبکه مورد استفاده و نیز استفاده از کادرهای تبادلی، ترکیب می‌کند. با این گفته، اجازه دهید

مستقیماً به برخی از برنامه‌های کاربردی که افراد مختلف لازم است برای کمک به کار عیب‌یابی در شبکه، آنها را تنظیم نمایند نگاهی بیندازیم.

پیداکردن دیوار آتش

ابتدا باید دریابید که از سرویس‌دهندهٔ پروکسی یا دیوار آتش فیلترکنندهٔ بسته استفاده می‌کنید. اگر فرض کنید که مرورگرتان کار می‌کند، مشکلی وجود ندارد. مرورگر را آغاز کنید و صفحهٔ پیچیده‌ای را از اینترنت بارگذاری کنید (صفحه‌ای که بیش از یک یا دو ثانیه زمان برای بارگذاری آن لازم است). آنگاه در محل اعلان DOS دستور زیر را تایپ کنید:

```
netstat -a> before.txt
```

آنگاه تایپ کنید:

```
netstat -a> after.txt
```

البته در مورد دستور دوم کلید Enter را هنوز فشار ندهید. به مرورگر بازگردید و صفحه را تجدید کنید. آنگاه خیلی سریع به اعلان DOS بازگشته و کلید Enter را فشار دهید. بعد از انجام این کار، دو فایل خواهید داشت: before.txt و after.txt. تفاوت بین این فایل‌ها، سوکت‌های اضافی که هنگام تجدید صفحهٔ مرورگر باز شده‌اند را منعکس می‌سازد ـ این نشان‌دهندهٔ آن است که آیا شما از سرویس‌دهندهٔ پروکسی استفاده می‌کنید یا دیوار آتش فیلترکنندهٔ بسته. فرض کنید که این کار را برای یک صفحهٔ وِب موجود در www.quizro.com به انجام می‌رسانید:

```
C:\windows> fc before.txt after.txt
Comparing files before.txt and after.txt
****** before.txt
TCP duke:1071    frotz.frob.com:23 ESTABLEISHED
****** after.txt
TCP duke:1572    socks.frob.com:1080 ESTABLISHED
TCP duke:1071    frotz.frob.com:23 ESTABLISHED
```

قانون به شکل زیر است: اگر اسم میزبانی متفاوت با اسم میزبانی که در شبکه به آن مراجعه کرده‌اید مشاهده می‌نمایید، از سرویس‌دهنده پروکسی استفاده می‌کنید (در مثال قبل سوکتی برای سوکت ۸۰ مربوط به www.quizro.com ایجاد نشده است و به جای آن سوکتی به socks.frob.com ملاحظه می‌کنید؛ بنابراین در اینجا از یک سرویس‌دهندهٔ پروکسی استفاده شده است). اسم میزبانی که مشاهده می‌نمایید، نام سرویس‌دهندهٔ پروکسی است؛ شمارهٔ سوکت هم عبارت است از شمارهٔ سوکت پروکسی. می‌توانید از این اطلاعات بعداً برای پیکربندی اسباب‌بازیهایتان استفاده کنید.

اگر اتصالی را مستقیماً به سایت وِب خارجی ملاحظه می‌کنید، احتمالاً از یک دیوار آتش فیلترکنندهٔ بسته استفاده می‌نمایید. چنین دیوار آتشی مثل یک مسیریاب عمل می‌کند؛ به صورت خودکار درخواست شما را برای یک اتصال به خارج مسیرگردانی می‌کند و بنابراین نیازی به دانستن اسم یا محل ندارد. همین!

البته به منظور پیکربندی مرورگر یا هر اسباب‌بازی دیگر لازم است که اسم سرویس‌دهندهٔ پروکسی را بدانید. اسامی مرسوم برای سرویس‌دهنده‌های پروکسی عبارتند از «proxy»، «socks»، «http»، «firewall». البته می‌توانید با انجام یک nslookup، اسامی DNS را مرور کنید تا اسامی احتمالی سرویس‌دهنده‌های پروکسی را مشاهده نمایید:

```
$ nslookup
Default server: 192.168.1.6
```

```
> ls -d mycompany.com
[ns.mycompany.com]
mycompany.com.   SOA    ns.mycompany.com postmaster.mycompany.com.
(1017 10800 3600 604800 86400)
mycompan.com     NS     ns.mycompany.com
ns               A      192.168.1.6
ns               A      192.168.3.6
ntserver         A      192.168.1.10
mailserver       CNAME  ntserver.mycompany.com
cotton           A      192.168.3.7
socks            CNAME  cotton.mycompany.com
```

در این خروجی ملاحظه می‌کنید که «cotton» اسم واقعی سرویس‌دهنده «socks» که در آدرس 192.168.3.7 واقع شده است، می‌باشد. البته روش آسانتر آن است که تلفن را برداشته و از IT مربوطه سؤال نماییم.

اگر شما مسؤول تمامی امور شبکه در مجموعهٔ کاری خود هستید و شبکه‌ای مستندنشده را در دست دارید، فصل ۲۴ نکات و مطالبی در مورد چگونگی کشف سرویس‌ها در شبکه دراختیار می‌گذارد.

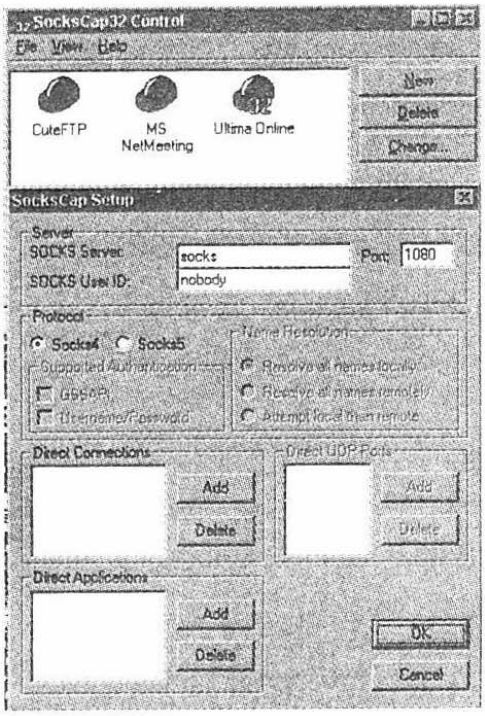
مطالبی در مورد Socks

Socks یک سرویس‌دهنده پروکسی عمومی و پرکاربرد است. نکته‌ای که در ارتباط با تمامی سرویس‌دهنده‌های پروکسی عمومی وجود دارد آن است که به غیر از حالتی که پشتیبانی توکار برای برنامهٔ کاربردی موردنظر فراهم شده باشند، باید از سرویس‌گیرندهٔ Socks مجزایی استفاده نمایید. دو شرکت که نرم‌افزار سرویس‌گیرندهٔ رایگان که برای بازیها و سایر ابزار سرگرم‌کننده در اختیار می‌گذارند عبارتند از:

- NEC (http://www.socks.nec.com) این سرویس‌گیرنده تا حدودی خودسرانه عمل می‌کند؛ یعنی خودش را به عنوان یک «آغازکننده» بدون نیاز به تغییر فایل‌های سیستم به اجرا درمی‌آورد. کادرهای تبادلی برای پیکربندی آن با اسم سرویس‌دهندهٔ Socks، پورت Socks (به صورت پیش‌گزیده)، پورت 1080 و اسامی و مکانهای فایل‌های برنامه‌ای که می‌خواهید از سرویس‌دهندهٔ Socks استفاده می‌کنند، به‌کار برده می‌شوند. شکل ۱-۲۰ یک پیکربندی نمونه را نشان می‌دهد. همان طور که ملاحظه می‌کنید کار بسیار ساده‌ای است.
- Hummingbird Communications (http://www.hummingbird.com) این سرویس‌گیرنده فایل‌های DLL شبکه‌ای پس‌زمینه‌ای را می‌گیرد و برای تمامی اتصالات TCP/IP حایلی ایجاد می‌کند. عملکرد این سرویس‌گیرنده بسیار خودسرانه‌تر است، چرا که فایل‌های سیستم ویندوز را با فایل‌های خود جایگزین می‌کند. نکتهٔ ناخوشایند دیگر در مورد سرویس‌گیرندهٔ Hummingbird آن است که مشخص نیست که ایستگاه کاری آن را به‌کار برده است یا خیر؛ چرا که هیچ شمایلی را در صفحه ظاهر نمی‌کند. بنابراین کار عیب‌یابی عمومی مشکلتر می‌شود، چرا که ممکن است تشخیص ندهید که این سرویس‌گیرنده در ایستگاه‌کاری در حال اجراست.

آیا این سرویس‌گیرنده‌ها همهٔ اوقات برای همهٔ برنامه‌ها کار می‌کنند؟ خیر، اما حداقل یکی از آنها با اغلب نرم‌افزارها قادر به کارکردن است. اگر با هریک از آنها به موفقیت رسیدید کار با آنها بسیار ساده‌تر (و امن‌تر) از پیکربندی دیوار آتش می‌باشد.

نکته : *برای آنکه متوجه شوید که روی یک PC سرویس‌گیرنده Hummingbird نصب شده است، در شاخهٔ C:\Windows\System به دنبال فایلی به اسم WSOCK320.DLL بگردید ـ اگر این فایل را پیدا کردید. این احتمال وجود دارد که سرویس‌گیرنده مذکور در این دستگاه نصب شده باشد.*



شکل ۱-۲۰: پیکربندی و استفاده از SocksCap32 بسیار آسان است.

همچنین تنظیم گرافیکی‌ای وجود ندارد. باید سرویس‌گیرنده را از طریق ویرایش فایل SOCKS.SNF در شاخهٔ سیستم ویندوز پیکربندی نمایید. در ذیل مثالی را مشاهده می‌کنید از چگونگی پیکربندی سرویس‌گیرنده Hummingbird برای یک شبکه دوبخشی ساده:

```
Direct 192.168.1.0 255.255.255.0
Direct 192.168.2.0 255.255.255.0
@SockD4 =192.168.2.10 0.0.0.0.0.0.0.0
```

به طور خلاصه این فایل به معنای آن است که شما به صورت مستقیم به 192.168.1.0 و 192.168.2.0 متصل شده‌اید. ترافیک این بخشها از سرویس‌دهندهٔ Socks استفاده نخواهد کرد. بقیهٔ ترافیک به سرویس‌دهنده Socks 4 موجود در 192.168.2.10 فرستاده می‌شود.

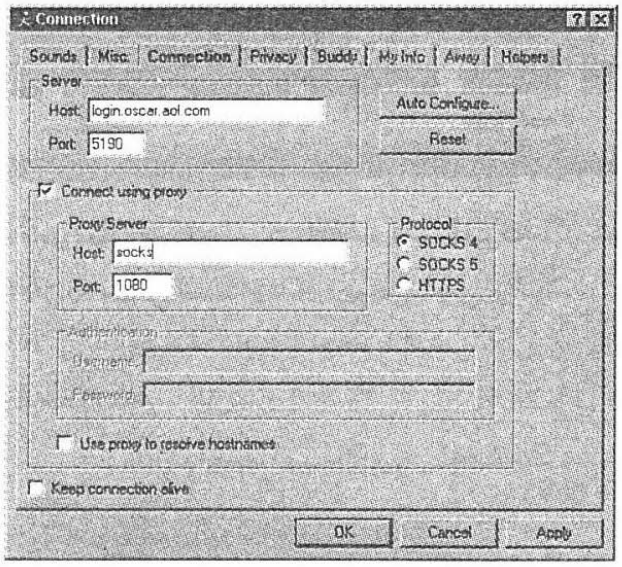
در مجموع باوجود سختی پیکربندی، سرویس‌گیرندهٔ Hummingbird قابلیت پیکربندی بالایی دارد و از سیاست «هر چیزی را که در شبکه در جریان است را بگیر و مطابق با فایل پیکربندی من با آن برخورد کن» رفتار می‌کند. با وجود آنکه این سرویس‌گیرنده با برنامه‌های کاربردی، بیشتری نسبت به سرویس‌گیرندهٔ NEC کار می‌کند، اما تمامی برنامه‌های کاربردی مورد اجرا را تحت تأثیر قرار می‌دهد. از سوی دیگر، سرویس‌گیرندهٔ NEC کمتر خودسرانه عمل می‌کند و پیکربندی آن آسانتر است. همچنین برای هر برنامهٔ کاربردی به پیکربندی مجزایی احتیاج دارد و برخی اوقات به خاطر کمتر خودسرانه رفتارکردن با برخی از برنامه‌ها اصلاً کار نمی‌کند.

اجازه دهید که نگاهی به بعضی از اسباب‌بازیها داشته باشیم؛ می‌توانید تکنیک‌های به‌کاررفته در آنها را برای سایر برنامه‌های کاربردی سرگرم‌کننده استفاده کنید. ما کار خود را با مثالهای ساده‌ای آغاز خواهیم کرد و به مرور حالات پیچیده‌تری را بررسی خواهیم نمود.

AOL Instant Messenger

موضوع از چه قرار است؟ AIM چیست؟ AIM روشی سرگرم‌کننده برای صحبت‌کردن از طریق اینترنت به شکل همزمان است. البته از شما خواسته می‌شود که اتصالی از نوع TCP با یکی از سرویس‌دهنده AOL ایجاد کنید و ممکن است دیوار آتش شما از این کار ممانعت به عمل آورد.

باید مطمئن شوید که دیوار آتش‌تان، Socks 5190 مربوط به TCP را برمبنای خارج‌شونده آزاد گذاشته است (اگر سیاست دیوار آتش شما آن باشد که بتوان هر اتصالی را از داخل به خارج برقرار نمود این کار میسر است). اگر دارای سرویس‌دهنده پروکسی Socks یا HTTPS (HTTP امن) داشته باشید، مشکلی وجود ندارد. همان گونه که در شکل ۲-۲۰ ملاحظه می‌کنید صفحه تنظیم AIM امکان پیکربندی انواع سرویس‌دهنده‌های پروکسی را در اختیار می‌گذارد. این صفحه بسیار کارها را آسان می‌کند.

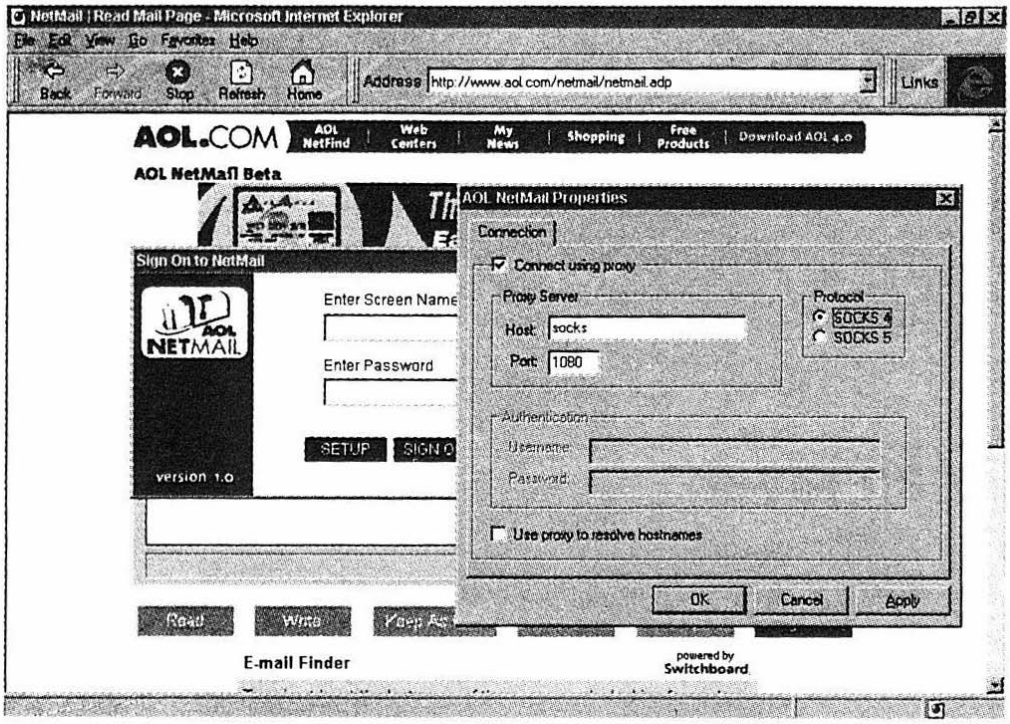


شکل ۲-۲۰: AOL Instal Messenger قادر است Socks 4، Socks 5 یا یک پروکسی HTTPS را مورد استفاده قرار دهد.

AOL NetMail

America Online به کاربرانش اجازه می‌دهد که با استفاده از یک رابط مبتنی بر وِب خارج از نرم‌افزار معمولی خود، پُست الکترونیکی‌شان را وارسی نمایند. یک Plug-in محسوس به مرورگر منتقل می‌شود و شما می‌توانید در یک لحظه و دردم پیغامهای خود را ملاحظه نمایید. مؤلفهٔ وِب کاری به تنظیمات پروکسی مرورگر شما ندارد؛ تنها کافی است مطابق شکل ۳-۲۰ نظیر مرورگر آن را پیکربندی نمایید (می‌توانید از این اطلاعات برای پیداکردن محل سرویس‌دهنده پروکسی خود استفاده کنید.

NetMail شبیه Instant Messenger می‌باشد؛ تنها از اتصال TCP خارج‌شونده به پورت 5190 در سمت سرویس‌دهنده استفاده می‌کند.



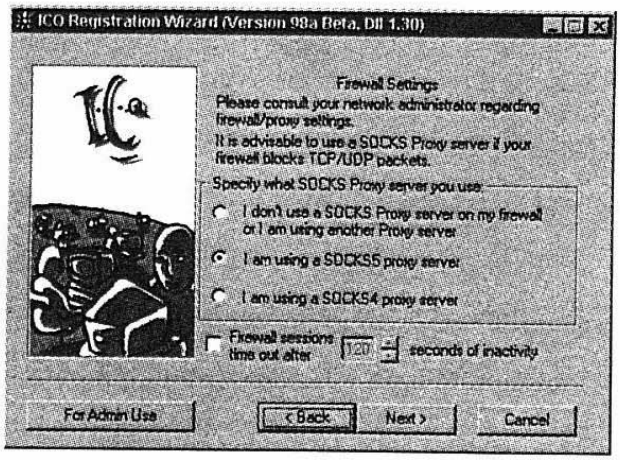
شکل ۳-۲۰: AOL NetMail قادر است Socks 4 و Socks 5 را پشتیبانی کند اگر تنها پروکسی‌های ویژهٔ برنامه کاربردی نظیر FTP و HTTP دارید، ممکن است چندان خوش‌شانس نباشید.

ICQ

ICQ از شرکت Mirabilis بدون تردید پرطرفدارترین برنامهٔ Chat می‌باشد. همان گونه که در شکل ۴-۲۰ ملاحظه می‌کنید سرویس‌دهنده‌های Socks در آن به خوبی پشتیبانی می‌شوند. البته این برنامه، از آن دست برنامه‌هایی است که استفاده از آن به‌همراه دیوار آتش فیلترکننده مشکل است؛ گواینکه فقط به یک پورت TCP (4000) برای برقراری ارتباط با سرویس‌دهنده ICQ در اینترنت نیاز دارد و آنگاه ایستگاه‌کاری باید قادر باشد که اتصالات فرستاده‌شده از خارج را روی پورت‌های متعدد TCP ـ یعنی اتصالات واردشونده به شبکه دریافت نماید (ICQ در صورت پیکربندی برای Socks نیازی به اتصالات واردشونده ندارد؛ تنها اتصال ایجادشده از طریق پروکسی مورد استفاده قرار می‌گیرد).

درصورت عدم استفاده از Socks، نرم‌افزار سرویس‌گیرنده ICQ ترجیح می‌دهد که حداقل ۱۲ پورت ورودی را مورد استفاده قرار دهد؛ و حتی بدتر از آن دوست دارد تخصیص آنها به صورت نامنظم و تصادفی باشد. برای آنکه زندگی برای شما یا سرپرست دیوار آتش‌تان آسانتر شود، ICQ امکان مشخص‌کردن گسترهٔ پورتی «ثابتی» را فراهم می‌آورد که بدان معناست که باید به صورت دستی هر سرویس‌گیرنده ICQ را پیکربندی کنید. با این وجود، بسیاری از سازمانها در اتصالات دیوار آتش خود از سیاست فقط خارج‌شونده استفاده می‌کنند و آزادکردن این تعداد پورت ورودی برای آنکه افراد بتوانند یک بازی شبکه‌ای را انجام دهند، کمی مشکل است.

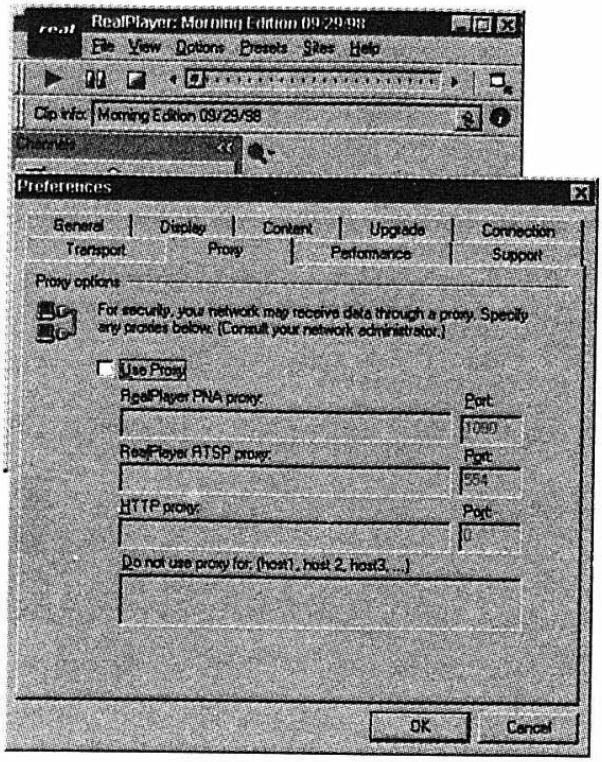
دست‌آخر اینکه: می‌توانید از ICQ با دیوار آتش فیلترکننده استفاده کنید اما استفاده از آن به همراه سرویس‌دهنده پروکسی بسیار ساده‌تر و امن‌تر است.



شکل ۴-۲۰: برای ICQ، Socks 4 و Socks 5 سرویس‌دهنده‌های پروکسی مناسبتری هستند؛ پیکربندی دیوار آتش فیلترکننده بسیار مشکلتر است.

RealPlayer

RealPlayer به شما اجازه می‌دهد اطلاعات صوتی و تصویری را بدون انتقال آنها از اینترنت ببینید و بشنوید. استفاده و پیکربندی RealPlayer در صورت به‌کارگیری یکی از پروکسی‌های ازپیش پیکربندی‌شدهٔ آن آسان است (شکل ۵-۲۰). متأسفانه، بسیاری از شبکه‌ها فاقد «پروکسی RealPlayer PNA» یا «پروکسی RealPlayer RTSP» می‌باشند. بغیر از حالتی که کار شغلی‌تان مستقیماً با امکانات صوتی تصویری مرتبط باشد، احتمال بسیار کمی وجود دارد که مدیریت تصمیم گرفته باشد که چنین سرویس‌گیرنده‌های پروکسی را نصب نماید.

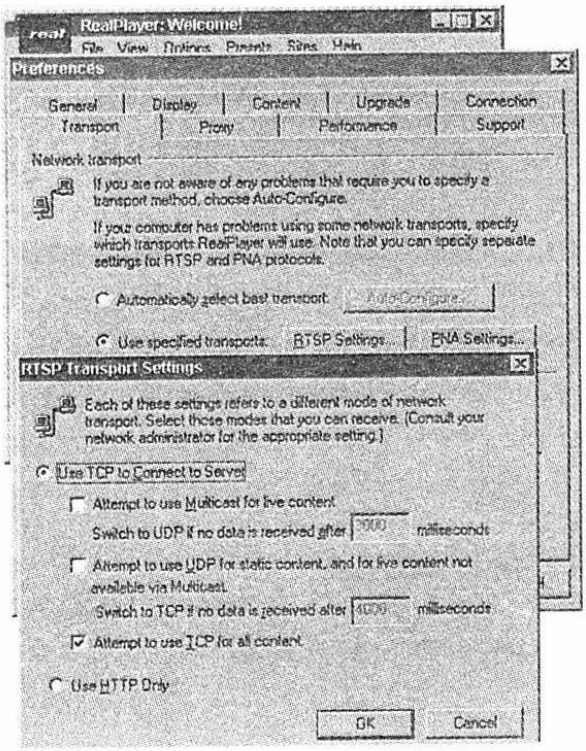


شکل ۵-۲۰: RealPlayer با پروکسی‌های خودش بسیار خوب کار می‌کند، اما علاوه بر آن قادر است پروکسی برنامه کاربردی HTTP را پشتیبانی نماید.

پروکسی HTTP پشتیبانی شده است و در صورتی که دارای پروکسی HTTP باشید می‌توانید از آن استفاده کنید. البته بسیاری اوقات از من سؤال می‌شود که چگونه می‌توان RealPlayer را برای استفاده از یک سرویس‌دهنده پروکسی «فقط خارج‌شونده» Socks 4 یا Socks 5 پیکربندی نمود. پاسخ این است: بنا به دلایلی، RealPlayer با SocksCap32 از NEC کار نخواهد کرد؛ یا به خاطر آنکه RealPlayer از کارایی شبکه ۱۶ بیتی استفاده می‌کند و یا آنکه از قدرت جادویی غیراستانداردی در TCP/IP بهره می‌گیرد.

من چگونه می‌دانم که RealPlayer با سرویس‌دهنده NEC کار نخواهد کرد؟ RealPlayer را از طریق نرم‌افزار سرویس‌گیرنده NEC اجرا نموده‌ام و هنگامی که تلاش می‌کرد تا اتصال را برقرار کند، در یک پنجرهٔ DOS دستور Netstat -a را اجرا نمودم. متوجه شدم که RealPlayer تلاش می‌کند که به صورت مستقیم با میزبان خود روی اینترنت تماس بگیرد، چرا که آدرس IP غریبه و وضعیت سوکت SYN_SENT را مشاهده نمودم (فصل ۱۸ جزییات وضعیت سوکت را به صورت مشروح در اختیار قرار می‌دهد). در صورتی که RealPlayer می‌توانست به طور مناسب با سرویس‌گیرنده NEC ارتباط برقرار کند، می‌بایست سوکتی به سرویس‌دهنده Socks خود در وضعیت Stablish یا در وضعیتی بدتر، CIOSE_WAIT یا TIME_WAIT را ملاحظه می‌نمودم. این به من می‌گفت که مشکل من در نرم‌افزار سرویس‌گیرنده نیست.

به هر صورت، RealPlayer با سرویس‌گیرنده Socks شرکت Hummingbird کار می‌کند. گواینکه، لازم است برخی پیکربندی‌های RealPlayer را خود انجام دهید. Socks 4 قادر به پشتیبانی از UDP نیست و برخی از سرویس‌دهنده‌های Socks 5 به هیچ عنوان برای کار با اتصالات واردشونده پیکربندی نشده‌اند. برای راه‌اندازی RealPlayer بدون دست‌زدن به سرویس‌دهنده پروکسی، باید RealPlayer را طوری پیکربندی کنید که تنها از اتصالات TCP استفاده نماید. به این ترتیب مقداری از سرعت خواهید کاست ـ اتصالات TCP کندتر از اتصالات UDP هستند ـ اما چه کسی اهمیت می‌دهد؟ شکل ۶-۲۰ تنظیم مناسب برای وادارساختن RealPlayer به منظور ایجاد اتصالات TCP را نشان می‌دهد.



شکل ۶-۲۰: برخی اوقات لازم است که فقط اتصالات TCP را برای کارکردن RealPlayer از میان دیوار آتش انتخاب نمایید.

استراتژی بازی

برخی از بازیها رفتار بسیار خوبی دارند. برای مثال، Origin's Ultima Online پروکسی بسیار دوست‌داشتنی‌ای می‌باشد. تنها از اتصالات PC استفاده می‌کند و اتصال را از ایستگاه‌کاری شروع می‌کند ـ یعنی از داخل شبکه شروع می‌شوند. بنابراین می‌تواند بدون هیچ مشکلی از طریق سرویس‌گیرنده‌های Socks مورد بررسی قرار گرفته در این فصل و حتی دیوار آتش فیلترکننده بسته به اجرا درآورد. من چنین اسباب‌بازی‌های شبکه‌ای را بسیار گرامی می‌دارم!

بازیهای دیگر، نظیر StarCraft and Diablo از شرکت Bilizard از شما می‌خواهد که سوکت‌های TCP و UDP را روی دیوار آتش خود باز نگه دارید (تمامی بازیهای شبکه‌ای این شرکت از پورت TCP و 6112 UDP استفاده می‌کنند). آنها در دیوار آتش «فقط خارج‌شونده» یا سرویس‌دهنده پروکسی کار نخواهند کرد و به دسترسی واردشونده شبکه شما نیاز دارند. باید در مورد بازکردن پورت‌های ورودی تصمیم‌گیری کنید.

البته چیزهای دیگری هم هستند که اسباب‌بازیهای شبکه‌ای شما را از کارکردن بازمی‌دارند؛ استراتژیهای عیب‌یابی اولیهٔ جعبهٔ سیاه را فراموش نکنید. بخصوص، بهتر است منابع سیستم را تحت نظارت قرار دهید. (برخی از این اسباب‌بازیها مقادیر زیادی از منابع را مصرف می‌کنند). همان طور که در فصل ۱۸ انجام دادید، بررسی کنید که آیا سرویس‌دهنده موجود در اینترنت آمادهٔ «شنود» اتصالات است یا خیر. اگر قادر هستید که پورت TCP خاصی که برنامهٔ بازی مورد استفاده قرار می‌دهد را Telnet کنید، (و TCP تنها چیزی است که این برنامه سعی در استفاده از آن دارد)، احتمال آنکه دیوار آتش در این عملیات دخالت کند بسیار ضعیف است.

خلاصه

می‌توانیم به صورت همزمان مهارتهای عیب‌یابی شبکه خود را تقویت بخشیده و همچنین کاربران شبکه را راضی نگه دارید. اسباب‌بازی‌های شبکه‌ای نظیر برنامه‌های Chat، نمایش صوتی تصویری و بازیها را می‌توان به منظور سرگرمی از شبکه بارگذاری نمود. اما باید بدانید که آنها برای استفاده در منزل و یا به منظور مشتریان خاص طراحی شده‌اند. برای کاربرد موفق این گونه اسباب، یا لازم است که امکان پشتیبانی پروکسی توکار آنها را فعال کنید و برای پشتیبانی پروکسی، سرویس‌گیرنده‌ای خارجی اضافه نمایید؛ یا اینکه در دیوار آتش‌تان تغییری دهید که شماره‌های سوکت لازم برای آنها را بدون محدودیت عبور دهد.

اگر سیاست شرکت شما امکان ایجاد اتصالات ورودی را مهیا می‌سازد، افزودن پورت‌های اضافی به پیکربندی دیوار آتش کار آسانی است. اما به هرحال شخصاً از افزودن پورت‌های ورودی تنها به خاطر بازی شبکه‌ای بیزار هستم چرا که با این کار ممکن است مهمترین تجهیزات امنیتی شبکه نتوانند کار خود را به نحو احسن انجام دهند.

کارگاه

پرسش و پاسخ

پرسش : چگونه باید دریابم که یک بازی یا ابزار بخصوص از چه پورتی استفاده می‌کند؟

پاسخ : اینکه فروشنده به شما نگوید برایم عجیب است. با این وجود، برخی از فروشندگان این کار را نمی‌کنند. بهتر

است با استفاده از ترفند «تفاوت» پورت موردنظر را پیدا کند. به حساب شخصی اینترنتی خود رفته و دستور زیررا تایپ نمایید:

```
netstat -a> before.txt
```

آنگاه برنامه را اجرا کنید، اتصال را باقی نگه داشته و به اعلان DOS برگردید و دستورات زیر را اجرا نمایید:

```
netstat -a> after.txt
fc before.txt after.txt
```

با انجام این کارها شماره(های) سوکت مورد استفاده بازی اعلام می‌شود. این روش دو کاستی دارد: پورت‌های UDP به این طریق نشان داده نمی‌شوند، چرا که در واقع «اتصالی» وجود ندارد. همچنین نمی‌توان دریافت که آیا اتصال TCP متفاوتی در طی انجام بازی هنگام ورود به آن مورد استفاده قرار می‌گیرد.

اگر باید دقیقاً بدانید که کدام پورت توسط بازی مورد استفاده قرار می‌گیرد. بهتر است فصل ۲۱ را مطالعه نموده و از یک تحلیل‌گر شبکه برای تسخیر بسته‌هایی از یک جلسه بازی استفاده نمایید. این کار بجز موقعی که تحلیل‌گر شماره‌ای (سریال) داشته باشید باید از DMZ صورت گیرد. اینجا زمانی فرا می‌رسد که باید از خودتان سؤال کنید که آیا واقعاً می‌خواهید بازی به این بدی را انجام دهید؟

آزمون

۱- می‌توانید با استفاده از وارسی ـــــــــ هنگام استفاده از یک مرورگر که قادر به کارکرد می‌باشد، آدرس سرویس‌دهنده پروکسی را بیابید.

الف ـ بستهٔ سوکت
ب ـ لیست سوکت
ج ـ لیست مسیریابی
د ـ راکت مسیریابی

۲- درست یا نادرست؟ سرویس‌گیرنده Socks شرکت Hummingbird (در مقابل سرویس‌گیرنده Socks شرکت NEC) روی تمامی برنامه‌های کاربردی که در ایستگاه‌کاری محل نصب آن به اجرا درمی‌آید، تأثیر می‌گذارد.

۳- دستور nslookup را برای فهرست‌گیری از تمامی ورودیهای موجود در قلمرو DNS شرکت مورد استفاده قرار دادیم. آن دستور چه بود؟

الف ـ netstat -rn company.com
ب ـ ls -la company.com
ج ـ ls -d company.com
د ـ netstat -d company.com

۴- هر برنامه کاربردی را می‌توان طوری پیکربندی نمود که از اتصالات TCP یا UDP استفاده نماید. به منظور استفاده از این برنامه به همراه یک دیوار آتش تنها خارج‌شونده، باید برنامه را طوری پیکربندی نمایید که چه کار کند؟

الف ـ فقط از اتصالات TCP استفاده کند
ب ـ فقط از اتصالات UDP استفاده کند
ج ـ هم از اتصالات TCP و هم UDP استفاده کند
د ـ از هیچ یک از اتصالات TCP و UDP استفاده نکند.

پاسخ به سؤالات آزمون

۱- ب
۲- درست
۳- ج
۴- الف

فصل ۲۱

برایم از شبکه‌ات بگو : تحلیل‌گران شبکه

بیشتر حالات عیب‌یابی شبکه را می‌توان در ردهٔ مواردی قرار داد که می‌توان از طریق استنتاج منطقی حل نمود. البته، برای حل بیشتر مشکلات شبکه‌ای سخت، به تحلیل‌گران شبکه نیاز داریم که به شما اجازه می‌دهند اطلاعات لازم برای حل مشکل را جمع‌آوری نمایید.

استفاده از تحلیل‌گران شبکه نباید بدون تشخیص صورت مسئله پذیرد؛ مشخصاً باید هدف خود را قبل از به کارگیری تحلیل‌گر بدانیم. همیشه باید قبل از استفاده از این ابزار یک تئوری برای خود ساخته باشیم ـ در غیر این‌صورت، دنبال چه چیزی خواهید گشت؟

با این وجود هنگامی که به مشکلی برمی‌خورید که به تحلیل‌گر نیاز دارد، بعد از ایجاد تئوری، تحلیل‌گرها می‌توانند تئوری شما را از طریق ملموس‌کردن وقایع به اثبات برسانند.

تحلیل‌گر شبکه چیست؟

هر زمان که در مورد تحلیل‌گرهای شبکه فکر می‌کنم، لبخند می‌زنم: همیشه فکر می‌کنم که شبکه روی تختی دراز کشیده است و چند روانشناس ریش‌سفید مثل فروید از آن سؤالاتی دربارهٔ منشاء و مبداء وی سؤال می‌نمایند. با اینکه ممکن است این شماء کمی غیرعادی به نظر برسد، اما خیلی دور از واقع نیست ـ وظیفهٔ اولیه هر تحلیل‌گر شبکه شنیدن صحبت‌های شبکه است.

دو نوع اصلی از ابزار تجزیه و تحلیل شبکه عبارتند از:

- پویشگرهای کابلی (تحلیل‌گرهای سخت‌افزاری)
- ردیاب‌های بسته‌ای (تحلیل‌گرهای نرم‌افزاری)

کار اولیهٔ پویشگر کابلی، بررسی مشخصات الکتریکی سیم شبکه است. همانطور که در فصل ۹ در مورد آن صحبت شد، کابل CAT-V باید مشخصات الکتریکی ویژه‌ای داشته باشد که بدون آنها خطاهای پیوند داده صادر می‌شود. هر پویشگر کابلی قادر است تمامی سیم‌ها را یک به یک از یک سر تا سوی دیگر بررسی نموده و وجود هرگونه قطعی را مخابره نماید.

بعضی از پویشگرهای پیچیده‌تر قادر هستند به سیگنال موجود روی سیم گوش فرادهند تا ببینند که آیا مشکلات پیونددادە یا فیزیکی در شبکه وجود دارد. برای مثال تنها راه واقعی تشخیص تصادم‌ها در هر شبکه اِترنِت، استفاده از پویشگر کابلی است. استفاده از پویشگر کابلی نسبتاً آسان است (کافی است آن را روشن نموده به هاب وصل کنیم و

خطاهای به نمایش درآمده را بررسی نماییم).

البته نحوهٔ عملکرد آن با روش سایر پویشگرها متفاوت است و از طرفی گرانقیمت نیز می‌باشد (بیش از ۳۰۰۰ دلار برای یک پویشگر مدرن)

در مقابل، تحلیل‌گرهای نرم‌افزاری شبکه تنها به ترافیک پیونددادهٔ گوش فرامی‌دهند و کابل فیزیکی که ترافیک روی آن به گردش درآمده را بررسی نمی‌کنند. هر تحلیل‌گر نرم‌افزاری اغلب یک PC با نوع خاصی از کارت شبکه در آن می‌باشد. تحلیل‌گرهای نرم‌افزاری از کارت‌های شبکه‌ای خاصی استفاده می‌کنند که قادر هستند در حالت «همگانی» به اجرا درآیند. یعنی آنها به صورت فیزیکی قادرند به تمامی بسته‌هایی که حتی برای آنها ارسال نشده است گوش فرا دهند.



نکته : *تحلیل‌گرهای نرم‌افزاری شبکه اغلب خیلی گران نیستند. قیمت برخی از آنها به ۱۰۰۰۰ دلار هم می‌رسد اما بسیاری کمتر از ۱۰۰۰ دلار هم قیمت دارند. فهرستی از تحلیل‌گرهای نرم‌افزاری ارزانقیمت‌تر را می‌توانید در http://feldman.org/analyzers.html ملاحظه نمایید.*

همچنین می‌توانید Network Monitor که همراه سرویس‌دهندهٔ ویندوز NT نگارش ۴ ارائه می‌شود را بازرسی نمایید. این ابزار در C:\WINNT\SYSTEM32\NETMON قرار گرفته است و هم در سرویس‌دهندهٔ NT و هم در ایستگاه کاری NT کار می‌کند. این ابزار تنها قادر است بسته‌هایی که از یا به ایستگاه کاری‌ای که از روی آن به اجرا درآمده تسخیر نماید و از طرفی محدودیت‌های دیگری نیز دارد. نگارش کامل Network Monitor میکروسافت را تنها در صورت خرید SMS (Systems Management Server) می‌توانید در اختیار داشته باشید. البته نگارش رایگان ابزار مذکور، روش خوبی برای آشنا شدن با نحوهٔ کارکرد این‌گونه برنامه‌هاست.

و بالاخره، از آنجا که تحلیل‌گرها نرم‌افزاری، تمامی بسته‌های پیوند داده روی سیم را تسخیر می‌کنند، آنها قادرند از نرم‌افزاری پیچیده برای رمزگشایی این بسته‌ها استفاده نموده و به شما اجازه دهند مشکلات پروتکلی و کاربردی را بررسی نمایید. (شکل ۱-۲۱ نمونه‌ای از پنجرهٔ رمزگشایی است). این واقعیت که تحلیل‌گرهای نرم‌افزاری در قالب تراشه‌های الکترونیکی قالب‌بندی نشده‌اند، باعث می‌شود که از قابلیت انعطاف بسیاری برخوردار باشد؛ در صورت لزوم می‌توانید نمونه‌های مختلفی را ارزیابی و خریداری نمایید، آنها را روی یک دستگاه همراه نصب نموده و از هر کدام که برای حل مشکل موجود مناسبتر است استفاده نمایید! گزینه‌ها و برنامه‌های کاربردی بسیار بیشتری در مورد تحلیل‌گرهای شبکه نسبت به پویشگر کابلی وجود دارد؛ ما در بقیهٔ این فصل تحلیل‌گرهای نرم‌افزاری را از لحاظ تئوریکی و عملی مورد بررسی قرار خواهیم داد.

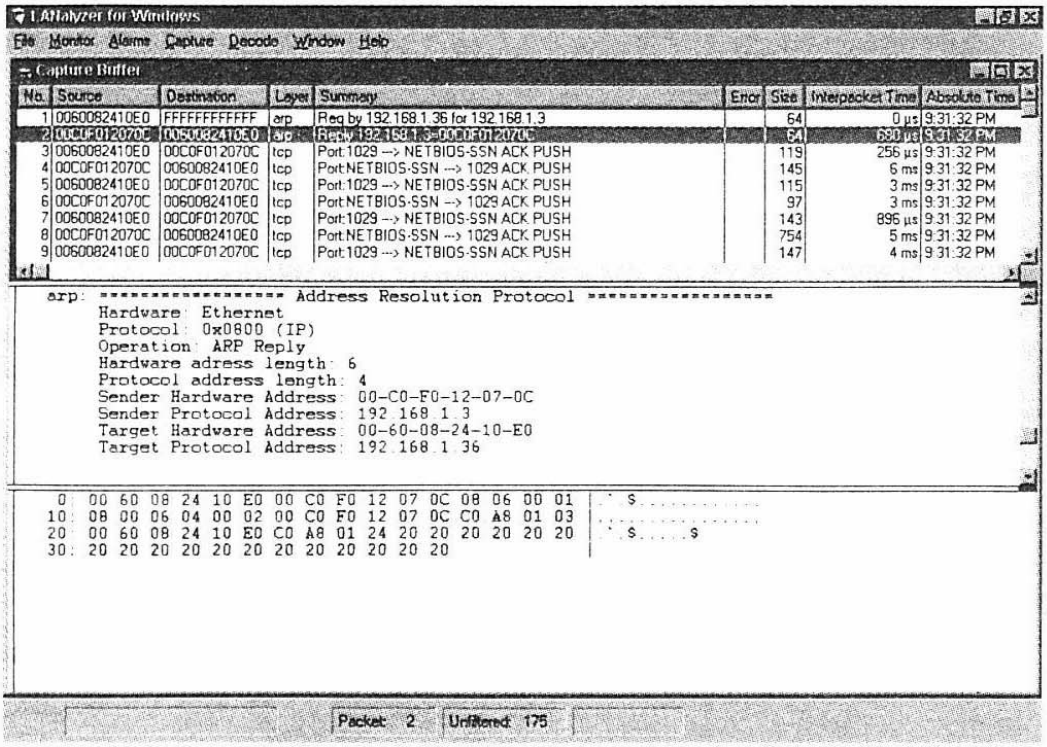
عملکرد عمومی

بیشتر تحلیل‌گرهای شبکه دو حالت عملیاتی دارند:

- تسخیر
- رمزگشایی

در طی فاز تسخیر، تحلیل‌گر می‌تواند عمل جمع‌آوری آماری، شامل تعداد خطاهای هر ایستگاه، تعداد بسته‌های ارسال‌شده / دریافت‌شده توسط هر ایستگاه، میزان کاربرد شبکه (تراکم در شبکه) و غیره به انجام برساند.

تحلیل‌گرهای جالب، قادر هستند گراف‌هایی را نشان دهند و بنابراین می‌توانید هنگام فاز تسخیر نحوهٔ نمایش را به طرق مختلف و مثلاً «پرحرف‌ترین ایستگاه» تنظیم نمایید. فاز رمزگشایی این امکان را فراهم می‌آورد که اطلاعات خاصی که تحلیل‌گر تسخیر نموده است را وارسی نماییم.



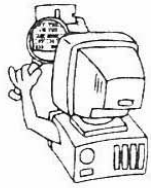
شکل ۱-۲۱: رمزگشایی بستهٔ پاسخ مربوط به یک تبادل ARP (پروتکل تحلیل آدرس).

بستهٔ به اسارت درآمده

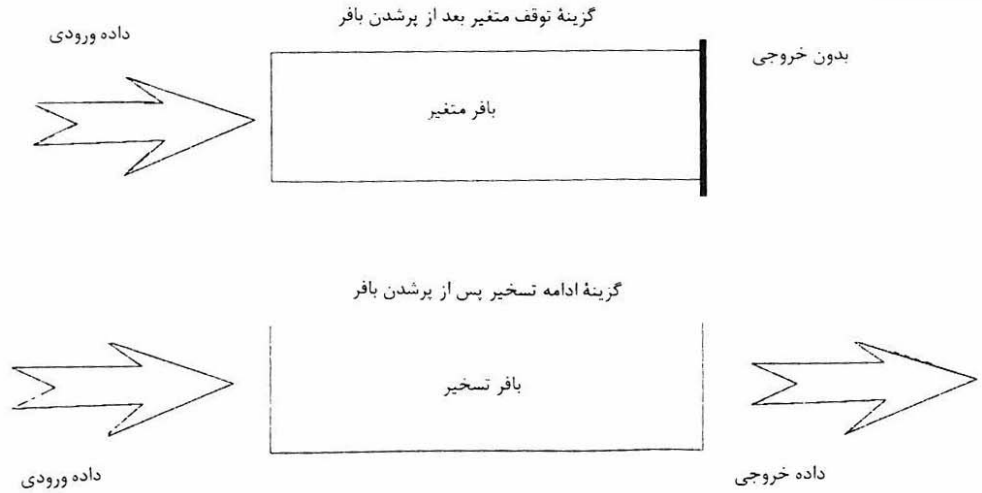
تسخیر هر چیزی در هر شبکهٔ اشتراکی میسر است ـ با اینکه این امر ممکن است منابع هنگفتی از تحلیل‌گر را به خود اختصاص دهد! یک شبکه 100Mbps شلوغ را درنظر بگیرید: یک تخمین خوش‌بینانه و محافظه‌کارانهٔ 6MBps، بدان معناست که به ۳۶۰ مگابایت حافظهٔ فیزیکی و برای تسخیر یک دقیقه از اطلاعات نیاز است (حافظهٔ مجازی برای اینکه عقب نماند کمی تند است).

وضعیت حلقه-نشانه و اِترنِت 10Mbps چندان بد نیست، به این صورت که برای نگهداری اطلاعات یک دقیقه به ترتیب به 90MB و 36MB نیازمند می‌باشیم. البته با این وجود، مقدار زیادی از اطلاعات باید مرور و ذخیره شود. تحلیل‌گرها چگونه با این مسئله روبرو می‌شوند؟

بیشتر تحلیل‌گرها دارای یک «فضای بافری» هستند که برای تسخیر اطلاعات تخصیص داده‌اند. هنگامی که بافر پُر می‌شود، این گزینه در اختیار وجود دارد که تسخیر متوقف شده و یا اینکه به سادگی از داده‌ای که در پایان بافر قرار دارد به منظور فراهم‌آوردن جا برای اطلاعات جدید استفاده گردد. (شکل ۲-۲۱ را ملاحظه کنید).



نکته **:** *به منظور آگاهی از سخت‌افزار مورد نیاز برای استفاده از تحلیل‌گر نرم‌افزاری به منظور پیش نیامدن مشکلات با سازندهٔ آن تماس بگیرید. برای مثال برخی از سخت‌افزارها قادر نیستند که با سرعتی کافی برای تسخیر اِترنِت 100Mbps کار کنند و در نتیجه بخشی از ترافیک از دست می‌رود.*



شکل ۲-۲۱: هر تحلیل‌گر می‌تواند هنگام پرشدن بافر یا از اطلاعات قدیمی‌تر صرف‌نظر کند و یا آنکه به کلی عمل تسخیر اطلاعات را متوقف نماید.

شما چگونه با این موضوع برخورد می‌کنید؟ به بیان دیگر، آیا این انتظار از عیب‌یاب‌های شبکه وجود دارد که صدها مگابایت اطلاعات را به منظور یافتن مشکل جستجو کنند؟ خیر! همانطور که پلیس در یک زمان قادر به شنود ۵۰ خط مختلف نیست، این انتظار وجود دارد که عیب‌یاب کارآمد شبکه تنها تعداد محدودی از مکالمات شبکه‌ای را در هر زمان بررسی و پویش نماید.

همان‌گونه که در ادامه بحث خواهد شد، اغلب تمامی اطلاعات موجود در سیم را تسخیر نمی‌کنیم ـ اگر این کار صورت پذیرد، هدف اصلی جمع‌آوری آمار است و علاقه‌ای به مصاحبه و بررسی مشخصات محتویات هر بسته وجود ندارد، بنابراین بسیاری اوقات، بسته به سناریوی درنظر گرفته‌شده، به تحلیل‌گر خود می‌گویید که برخی از اقلام زیر برایتان جالب هستند:

- پروتکل‌هایی به‌خصوص
- ایستگاههای کاری خاص
- برخی از سرویس‌ها

به این ترتیب مقدار اطلاعاتی که لازم خواهد بود آن را وارسی نماییم به طرز فاحشی کاهش می‌یابد. همان‌گونه که در ادامه مطرح خواهد شد، این یکی از کارهای مهم هر تحلیل‌گری می‌باشد.

رمزگشا

بعد از عمل تسخیر تحلیل‌گر این امکان را برای شما فراهم می‌آورد که به اطلاعات تسخیرشده دسترسی داشته باشید. تحلیل‌گر بیت و بایت‌های دریافتی مربوط به هر بسته را به شکلی که برای انسان قابل خواندن باشد، «رمزگشایی» می‌کند. آیا تمامی بیت‌ها و بایت‌ها ترجمه می‌شوند؟ خیر، شاید نه. چرا نه؟ خوب، سه نوع ترجمه وجود دارد که تحلیل‌گر شما باید قبل از آنکه بتوانید اطلاعات را مرور کنید به انجام برساند:

- MAC
- پروتکل
- سرویس

لایهٔ MAC به نوعی آسان است. روش‌های متعددی برای قراردادن اطلاعات روی سیم وجود ندارد و مشخصات این موضوع نیز به خوبی تعیین شده است. لایهٔ پروتکل کمی پیچیده‌تر است، چرا که تحلیل‌گر لازم است زبان بیت و بایت‌ها را به منظور نمایش آنچه که در وقوع است «بفهمد». اوضاع در مورد سرویس‌ها بسیار پیچیده‌تر می‌شود. صدها و صدها سرویس وجود دارند و این امکان برای هر تحلیل‌گر وجود ندارد که بتواند به خوبی تمامی آنها را رمزگشایی کند. (تصور کنید که این کار مانند آن است که از مترجم خود در کشوری دیگر انتظار داشته باشید که فوتبالیست، برق‌کار، دکتر، تکنسین، هنرمند، و آرشیتکت خوبی هم باشد. البته ممکن است چنین مترجمی پیدا کنید اما احتمالاً بهتر است چندین مترجم با چنین مهارتهایی بیابید.

کلام آخر آنکه هر تحلیل‌گری نمی‌تواند هر سرویسی را مدیریت نماید. البته سرویس‌های عمومی نظیر Telnet ، DNS ، فایل و چاپ میکروسافت و ناول به خوبی در تمامی آنها پشتیبانی شده‌اند برخی تنها در بعضی از تحلیل‌گرها تحت پوشش قرار گرفته‌اند و برای برخی نیز کلاً تحلیل‌گری وجود ندارد! (برای مثال من کسی را نمی‌شناسم که رمزگشایی برای بستهٔ پرطرفدار گفتگوی اینترنتی ICQ ساخته باشد. ICQ نسبتاً سرویسی خصوصی است).

آیا این یک نابسامانی محسوب می‌شود؟ در واقع خیر. با اینکه تحلیل‌گر نمی‌تواند سرویس را طوری رمزگشایی کند که شما بتوانید آن را بخوانید، اما هنوز هم می‌تواند آنچه را که روی می‌دهد تسخیر نماید. اگر با پشتیبانی فنی یک سرویس خصوصی کار می‌کنید، می‌توانید مطمئن باشید که آنها قادر هستند اطلاعات ردیابی‌شدهٔ شما را با استفاده از رمزگشاهای خانگی خود بخوانند. از همهٔ اینها گذشته، یکی از اهداف ما در استفاده از یک تحلیل‌گر شبکه تسخیرکردن رویدادها به منظور در جریان قراردادن فروشنده است و اگر فروشنده نتواند سرویس خودش را رمزگشایی کند، همهٔ ما به دردسر افتاده‌ایم.

متأسفم، نمی‌توانم آن را تحلیل کنم

برخی از تحلیل‌گرهای شبکه یک حالت «ماهر» دارند که در حین تسخیر بسته‌ها، در مورد خرابی شبکه حدس‌هایی می‌زنند. این موضوع از لحاظ تئوریکی بسیار جالب است. من و شما نمی‌توانیم صدها مکالمه را بلافاصله مرتب کنیم؛ این کار در ردهٔ کارهایی قرار می‌گیرد که به خوبی توسط کامپیوتر قابل انجام است.

در عمل؟ خوب، تجربهٔ من با تحلیل‌گرهای «ماهر» برایم روشن ساخته است که آنها از مهارت چندانی برخوردار نیستند. البته آنها قادرند ایستگاههای کاری که به کُندی کار می‌کنند تشخیص دهند ـ بینش آنها در تشخیص ایستگاه کاری که تأخیر قابل‌ملاحظه‌ای در پاسخ‌دادن به یک درخواست دارد، بسیار خوب است. آنها همچنین قادر هستند که آدرس‌های IP تکراری و مشکلات سادهٔ دیگر را به خوبی تشخیص دهند. اما نمی‌توان گفت که در کارشان مهارت زیادی وجود دارد. می‌توان آنها را به دانشمندانی دیوانه تشبیه کرد. بر این باور هستم که هر مشکل پیچیده‌ای را باید یک انسان برطرف کند؛ ناشناخته‌ها و احتمالات زیادی وجود دارد، به طوری که ممکن است کامپیوتر از عهدهٔ آنها برنیاید. آموزش کامپیوتر به منظور چگونگی حل مشکلات پیچیده احتمالاً به سختی آموزش آن به منظور چگونه فکرکردن است.

کاملاً واضح است که من نمی‌خواهم از ارزش تحلیل‌گرهایی با امکان «ماهر» بکاهم ـ آنها برای حل مشکلات سادهٔ عمومی واقعاً مفید هستند. تنها کافی است این تصور را از ذهن خود بیرون کنید که چنین تحلیل‌گری می‌تواند تمامی مشکلات پیچیدهٔ شبکه را برایتان حل کند. البته تحلیل‌گرهای ماهر می‌توانند همراهانی بسیار قدرتمند در عیب‌یابی شما باشند؛ آنها مشکلات حاشیه‌ای را نشان می‌دهند که می‌توانند به حل مسئلهٔ اصلی کمک نمایند.

شبکه‌درمانی : تکنیک‌هایی برای استفاده از تحلیل‌گر

تحلیل‌گرها با هم تفاوت دارند؛ انتخاب اسلحهٔ مناسب یکی از اولین گامهای موفقیت در کار با تحلیل‌گر شبکه است. برای مثال، هنگامی که مشکلی عمومی در یک بخش از شبکهٔ حلقه-نشانه وجود دارد (آن بخش از شبکه «پایین» است)، هیچ‌کس از Sniffer Token-Ring Analyzer شرکت Networe Associate استفاده نمی‌کند، چرا که این برنامه در طی عمل تسخیر فهرست NAUN حلقه-نشانه را نگهداری نمی‌کند (بخش مهمی از خطاهای هر بخش حلقه-نشانه هنگام عیب‌یابی). ابزار دیگری به نام Sniffer Token-Ring Monitor ساخته‌اند که مناسب‌تر است، چرا که فهرست نام را پشتیبانی می‌کند. هنگام عیب‌یابی یک شبکهٔ حلقه-نشانهٔ نِت‌وِر، ترجیح می‌دهم که از LANalyzer ناوِل استفاده کنم این برنامه هم از فهرست NAUN (که ناوِل آن را ناظر حلقه می‌خواند) و برای پروتکل‌ها و سرویس‌های ویژه نِت‌وِر بسیار خوب است.

به‌عنوان مثال، در مورد مشکلی که به ایستگاههای کاری NT، حلقه‌نشانه و ناوِل مربوط می‌شد، تصمیم گرفتم که از LANalyzer ناوِل استفاده کنم چرا که به نظر می‌رسید مشکل از جانب ناوِل باشد. در آن وضعیت، مشکلی هنگام صحبت با میزبانهای یونیکس یا میکروسافت نداشتم. همچنین می‌دانستم که مشکل فقط به حلقه-نشانه مربوط می‌شود (ایستگاههای اِترنِت مشکلی نداشتند)، بنابراین تصمیم گرفتم در صورت عدم ملاحظهٔ چیز واضحی با LANalyzer از LANDecoder شرکت Triticol استفاده کنم. برنامهٔ اخیر را در انجام کار رمزگذاری بسیار کامل یافته‌ام (در مورد این مشکل در ادامهٔ این فصل بیشتر صحبت خواهد شد) ـ مسئلهٔ بسیار شیرینی است!

کلام آخر آنکه: سناریوی شما همیشه ابزار مورد نیاز را دیکته می‌کند. همیشه یک ابزار بیشتر به کار نمی‌آید چرا که یک مشکل روی داده است! از آنجا که نمی‌توانید تمامی ابزارهای در دسترس را خریداری نمایید، بهتر است که قبل از بررسی به صورت کامل محیط شبکهٔ خود را بشناسید. به این صورت قادر خواهید بود مناسب‌ترین ابزارها را ابتیاع کنید

بسته‌های فیلترشده

همانگونه که قبلاً ذکر کردم دانستن اینکه اطلاعات ثبت‌شده و تسخیرشدهٔ خود را چگونه و چه زمانی فیلتر کنید، یکی از مهمترین مهارتهایی است که می‌توانید هنگام استفاده از تحلیل‌گر شبکه به منظور تسخیر ترافیک شبکه به کار بگیرید. در غیراین‌صورت، کارتان نظیر آن است که در انبار کاهی به‌دنبال سوزنی بگردید! حتی ماهرترین استادان کامپیوتر هم در صورت عدم فیلترسازی مناسب اطلاعات، کاری را از پیش نخواهند برد.

انواع مختلفی فیلتر وجود دارد:

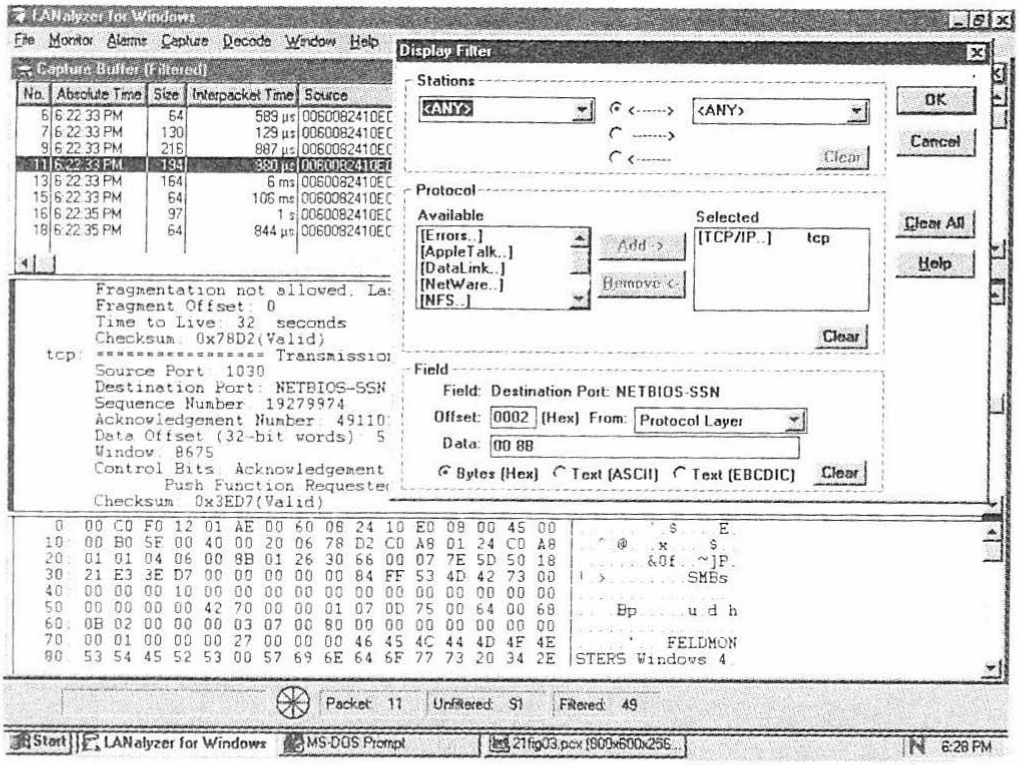
- فیلترهای ایستگاهی ـ نشان‌دهندهٔ آنکه اطلاعات کدام ایستگاه کاری و/یا سرویس‌دهنده باید تسخیر شود.
- فیلترهای پروتکلی ـ TCP/IP، IPX/SPX و NetBEUI
- فیلترهای سرویسی ـ سرویس‌های موردنظر که نمایش داده خواهند شد.
- فیلترهای عمومی ـ مقادیر شانزدهی در داخل بسته

کلیهٔ انواع فیلترها در هر تحلیل‌گر در دسترس نیستند؛ برای مثال، برخی از تحلیل‌گرها نمی‌توانند هر نوع سرویسی را فیلتر کنند، اما می‌توانیم با استفاده از یک فیلتر عمومی بر این مشکل فائق شویم.



نکته : *اجازه دهید نگاهی داشته باشیم به اینکه چگونه می‌توان تحلیل‌گری را بر مبنای سرویس فیلتر نمود. برای مثال LANalyzer ناوِل به شما اجازه نمی‌دهد که جلسه‌های Telnet (Display) را مشخص کنید. اما می‌تواند بگوید چه هنگام بسته در جلسهٔ Telnet (یا نوع دیگری از جلسه) قرار دارد. تمام کاری*

که لازم است انجام دهید آن است که روی آن بخش از اطلاعات نمایشی رمزگشایی که برایتان جالب است کلیک کنید. در حالتی که در مورد آن صحبت می‌کنیم، جلسهٔ NetBIOS، سوکت ۱۳۹ مربوط به TCP که معادل شانزدهی 8B می‌باشد، برایمان جالب است (شکل ۳-۲۱ را ملاحظه کنید).
توجه کنید که چگونه بایت‌های متعددی پررنگ شده‌اند؛ این بایت‌ها در بسته‌هایی هستند که کُدهای شانزدهی آنها نشان‌دهندهٔ آن است که این بسته به جلسهٔ NetBIOS مربوط است. آنگاه می‌توانید روی این بایت‌ها دو بار کلیک کنید تا LANalyzer پنجرهٔ فیلتر عمومی را که از قبل با این مقادیر پر شده‌اند را ظاهر سازند. می‌توانید از این اطلاعات برای سرویس‌های دیگر نیز استفاده کنید.



شکل ۳-۲۱ : LANalyzer ناوِل این امکان را فراهم می‌آورد که تنها با دو بار کلیک‌کردن روی هر فیلدی در ناحیهٔ رمزگشایی روی آن فیلتر ببندید.

تحلیل‌گر برای فیلترکردن دو روش در اختیار دارد:

- قبل از تسخیر[1] ـ هنگامی مفید است که نمی‌خواهید بافرتان با اطلاعات و داده‌های غیرلازم سرریز شود.
- بعد از تسخیر[2] ـ هنگامی مفید واقع می‌شود که اطلاعات عمومی را از قبل تسخیر کرده و می‌خواهید در جستجویتان پالایش‌هایی را صورت دهید.

بسته‌های قاتل

در اینجا موقعیتی را تعریف می‌کنیم که چگونگی فیلترسازی در مورد یک سرویس‌دهندهٔ پرکار را در هنگام عیب‌یابی نشان می‌دهد. متوجه شدم که هنگام ارسال کارهای چاپی از سرویس‌دهندهٔ یونیکس به سرویس‌دهندهٔ ناوِل مشکلی رخ می‌دهد. سرویس‌دهندهٔ ناول به صورت ناگهانی و به صورت نامنظم، خطاهایی را در صفحه‌های یونیکس خود (PLPD) تولید

1- Precapture 2- Postcapture

می‌کند و روند پردازش را متوقف می‌نماید. تنها بارگذاری مجدد فایل PLPD.MLM پردازش کارهای چاپی یونیکس را دوباره راه می‌انداخت. سؤال اول ما آن بود که، «چه کسی چیزی را در سرویس‌دهندهٔ ناوِل تغییر داده است؟» پاسخ... هیچ‌کس بود. هیچ چیزی در سرویس‌دهندهٔ ناوِل تغییر نیافته بود. از هیچ بازرسی و پرسشی برای تأیید این موضوع دریغ نشد؛ کاملاً مطمئن شدیم که هیچ‌کسی در محدوده زمانی موردنظر هیچ چیزی را در سرویس‌دهنده تغییر نداده بود.

عیب‌یابی این مسئله بسیار سخت می‌نمود. جستجوی سایت پشتیبانی ناوِل در مورد پیغام خطای PLPD چیزی را آشکار نساخت و مشکل کماکان به‌صورت متناوب ظاهر می‌شد. ما به پاسخ نسبتاً سریعی نیاز داشتیم چرا که این دروازهٔ چاپ، مسئول پردازش کار چاپ برای کاری حساس به زمان بود. از آنجا که می‌دانستیم که چیزی در سرویس‌دهندهٔ ناوِل یا سرویس‌دهندهٔ یونیکس تغییر نکرده بود (در واقع سرویس‌دهندهٔ یونیکس به خوبی کار چاپ را روی سرویس‌دهنده‌های ناوِل دیگر انجام می‌داد) تصمیم گرفتیم که ببینیم چه اتفاقی روی شبکه رخ می‌دهد. ممکن است بستهٔ شریر و سرگردانی باعث شده باشد که سرویس‌دهندهٔ PLDP سلامتی فکری خود را از دست بدهد.

ما یک ردیاب را به بخش شبکه‌ای مربوط به سرویس‌دهنده متصل نمودیم (زیرا به این موضوع مشکوک بودیم که اتفاق بدی برای Server رخ می‌دهد) و مواردی که می‌خواستیم فیلتر کنیم را به صورت زیر مورد توجه قرار دادیم:

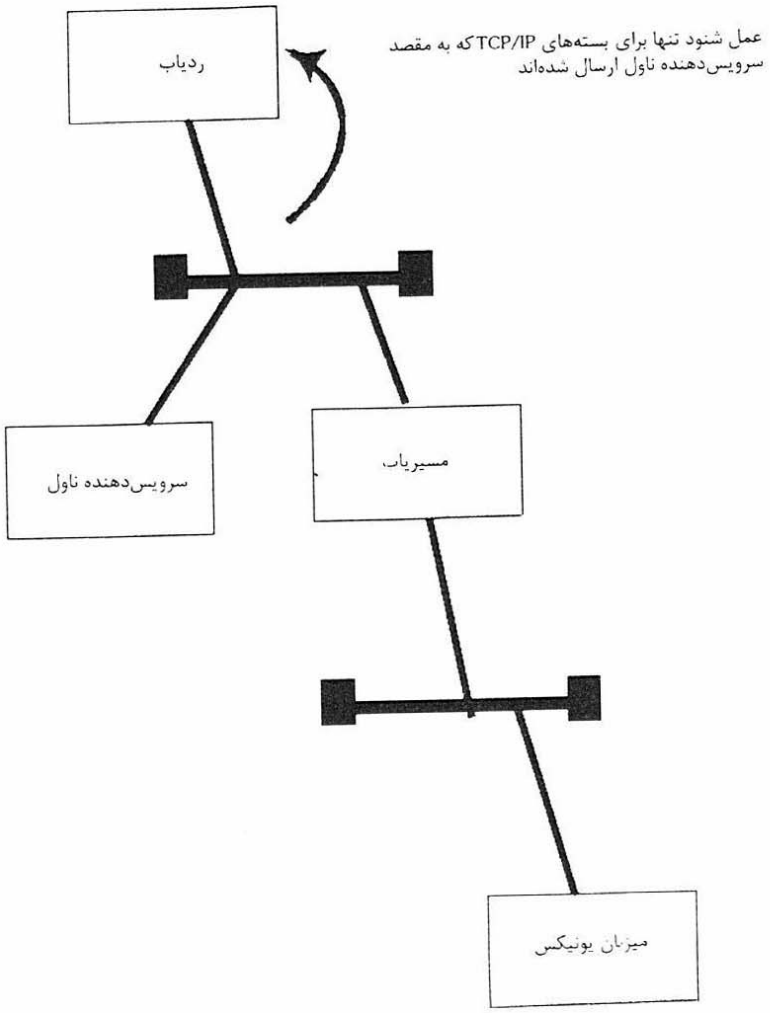
- از آنجا که ما می‌دانستیم اتفاقی برای سرویس‌دهندهٔ ناوِل رخ می‌دهد، تصمیم گرفتیم تنها بسته‌هایی را که به مقصد آدرس MAC سرویس‌دهنده ناوِل ارسال می‌شود، تسخیر کنیم.
- از آنجا که می‌دانستیم این سرویس‌دهنده، سرویس‌دهندهٔ فایل و چاپ پرکاری است، منطقی به نظر نمی‌رسید اگر تمامی بسته‌های ارسالی به آن را تسخیر نماییم.
- از آنجا که می‌دانستیم مشکل با PLDP مربوط است و نیز می‌دانستیم که PLDP سرویس‌های چاپی یونیکس را از طریق TCP/IP دریافت می‌کند، تنها بسته‌های TCP/IP را مورد پذیرش قرار دادیم. این کار باعث شد بیشتر بسته‌های ارسالی به این سرویس‌دهنده، که بسته‌های فایل و چاپ IPX/SPX ناوِل بودند، حذف گردند. با این کار تنظیم آزمایشی که نظیر شکل ۴-۲۱ بود، به دست آمد.

با وقوع دوبارهٔ مشکل، نگاهی به بسته‌های تسخیرشده انداختیم دو مفهوم مهم در اینجا وجود دارند. اول تحلیل‌گر را بعد از مخابرهٔ خطا اجرا کرده و متوقف ساختیم. دوم ساعت تحلیل‌گر شبکه را قبل از آغاز تسخیر با ساعت شبکه همسان کردیم و از کاربری که مشکل را گزارش نمود خواستیم که زمان وقوع مشکل را نیز اعلام کند. از آنجا که این سرویس سرویس کار خودکاری بود مطمئن بودیم که گزارش مشکل در عرض ۲ یا ۳ دقیقه بعد و قبل از زمان مطرح شده می‌باشد، بنابراین اکنون تنها کافی بود بسته‌های موجود در محدودهٔ زمانی مذکور را بررسی کنیم که این کار حجم اطلاعات مورد بررسی‌مان را کاهش می‌دهد.

با رسیدن به انتهای اطلاعات ردیابی‌شده ابتدا فیلتری را روی سوکت TCP مربوط به LPD، شمارهٔ ۵۱۵ ایجاد می‌کنیم. مشکلی را ملاحظه نمودیم: سرویس‌دهنده پاسخ به درخواستهای LPD از سوی میزبان یونیکس را متوقف می‌سازد، ما این را بدون انجام ردیابی نیز می‌دانستیم. البته، این اطلاعات مفید بود: به ما نشان داد که مشکل در کجای فهرست بسته رخ می‌دهد. بنابراین، از شر فیلتر LPD راحت شدیم و به بسته‌ای که مشکل در آن رخ می‌داد رفتیم و بسته‌های موجود قبل از هنگام وقوع مشکل را بررسی نمودیم. از قرار معلوم، درست قبل از وقوع مشکل، یک درخواست ARP صورت می‌گرفت (پروتکل تحلیل آدرس در TCP/IP).

به خاطر دارید که هر آدرس TCP/IP باید آدرس MAC متناظری داشته باشد تا دو کارت شبکه بتوانند با یکدیگر صحبت کنند. درخواست ARP، که ملاحظه کردم با آدرس MAC اشتباهی پاسخ داده می‌شد. هر بسته ARP با آدرس MAC

اشتباه، اغلب به معنای آن است که شخص دیگری آدرس TCP/IP یکسانی را با شما مورد استفاده قرار داده است، بنابراین در ارتباطات وقفه ایجاد می‌شود ـ اما چنین امری در اینجا اتفاق نمی‌افتاد.



شکل ۴-۲۱: تنظیم آزمایشی برای مشکل چاپی نِت‌وِر به یونیکس.

ما سعی کردیم آدرس MAC گزارش داده شده توسط درخواست ARP را پیدا کنیم، اما چنین کارت شبکه‌ای در شبکهٔ ما وجود نداشت علاوه بر آن نتوانستیم OUI آدرس MAC را در جدول OUI که به آن نیز ظنین بودیم پیدا کنیم. از آن گذشته، در تمامی این شبکه از یک یا دو کارت مربوط به فروشندگان شناخته‌شده استفاده شده بود.

از آنجا که چنین ابزاری در شبکه وجود نداشت، پیکربندی سوئیچ را بررسی نمودیم (از فصل ۱۴ به خاطر بیاورید که ابزارهایی که در طرفهای مختلف سوئیچ قرار گرفته‌اند به صورت مستقیم با یکدیگر صحبت نمی‌کنند). از آنجا که مشکل در سطح MAC بود، طبیعتاً به سوئیچ مظنون شدیم. از کسی که مسئول پیکربندی سوئیچ بود پرسیدیم که آیا چیزی در طی دو روز گذشته تغییر کرده بود ـ و، در حقیقت، چنین بود. در نتیجه او پیکربندی را به وضعیت سابقش بازگرداند و مشکل برطرف شد.

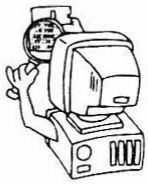
البته هنوز دو چیز مرا آزار می‌داد. چرا می‌توانستم سرویس‌دهنده ناوِل را با وجود نادرست‌بودن ARP، Ping نمایم؟ خوب، از آنجا که ARP هر دو دقیقه یکبار «مجدداً انجام می‌شود» زمانی که به عیب‌یابی می‌پرداختم، ARP دوباره درست شده بود؛ بنابراین، می‌توانستم سرویس‌دهنده را بدون مشکل Ping نمایم. سوئیچ تنها بعضی اوقات در ازاء درخواست

ARP اشتباه می‌کرد و اغلب کار خود را درست انجام می‌داد. مسئلهٔ دوم آن بود که چرا یک ARP بد سرویس LPD را با
می‌ریخت. این سؤال مشکل‌تری بود و من نمی‌خواستم که پاسخی برای آن بیابم، چرا که برایم مهم نبود. فایل LPD.NLM
(در همان مناسبت فایل TCPIP.NLM) در سرویس‌دهندهٔ ناوِل تا حدودی قدیمی بود و وقفه‌ای در جریان داده‌ای آن مشکل
می‌شد. بعد از رفع اشکال پیکربندی سوئیچ و برطرف‌شدن مشکل ARP یکبار دیگر همه چیز مرتب بود. (و این تنها
موضوعی است که از اهمیت برخوردار است).

مرور اطلاعات

در نهایت، هنگام مشاهدهٔ تک بسته‌های ردیابی‌شدهٔ خاص، بهتر است که گزینه‌های مرور و بازبینی موردنظر خود را
بشناسیم. بیشتر تحلیل‌گرها تعداد زیادی گزینه دارند که قابلیت انعطاف زیادی را در مورد ردیابی صورت گرفته و نحوهٔ
نمایش آن ارائه می‌کنند. برخی از این صفات شامل موارد زیرند:

- نمایش شانزدهی بسته.
- زمان تسخیر
- رمزگشایی‌های مربوط به MAC و/یا پروتکل و/یا سرویس
- آدرس MAC یا پروتکل
- اسم شبکه‌ای (DNS NetBIOS)

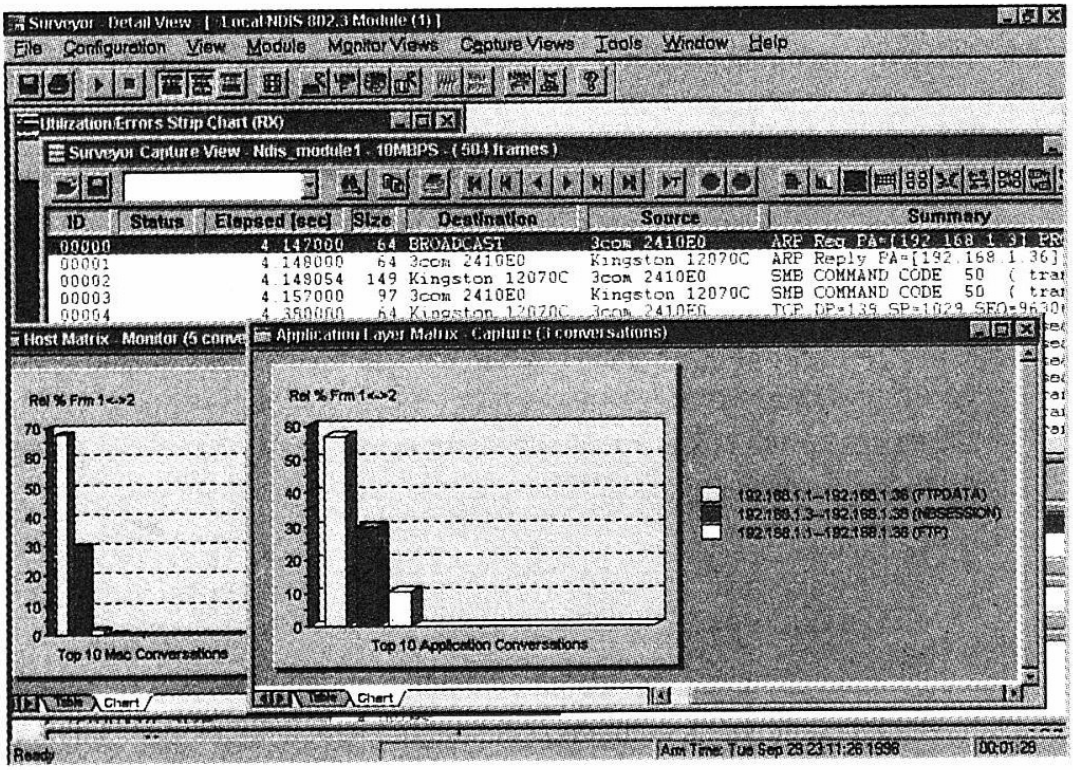


***نکته** : بسیاری از تحلیل‌گرهای شبکه‌ای دارای امکان جمع‌آوری نام هستند؛ یعنی بسته‌ها را هنگام عبور «می‌خوانند» و می‌بینند که آیا شناسهٔ نامی در آنها وجود دارد یا خیر. اگر وجود داشته باشد، تحلیل‌گر آن را در جدول نام خود قرار می‌دهد که این به شما اجازه می‌دهد یک فیلتر تسخیر یا نمایش بر اساس اسم شبکه‌ای، ایجاد نمایید. این شکل، روش «کاربرپسندانه‌تری» برای مشخص‌کردن فیلتر یا نمایش اطلاعات می‌باشد.*

آگاه باشید که بعضی از تحلیل‌گرها اسامی را به صورت خودکار تسخیر نمی‌کنند؛ باید این کار را به صورت دستی روی اطلاعاتی که از قبل تسخیر شده‌اند و در پی تجزیه و تحلیل خود هنگام مشاهدهٔ اطلاعات به انجام برسانند.

حتی با وجود یک ابزار مبتنی بر ویندوز مغز شما نمی‌تواند اطلاعات زیادی را در هر لحظه پردازش کند؛ امکان انتخاب گزینه‌های نمایشی به شما اجازه می‌دهد که در حجم زیادی از اطلاعات غوطه‌ور نشوید. بر این اساس، می‌توانید نمودارهای نواری مختلفی را که جنبه‌های خاص از اطلاعات را خلاصه می‌نمایند، همانطور که در شکل ۵-۲۱ نشان داده شده است، خلاصه نمایید. شکل مذکور ترافیک شبکه را بر اساس کاربرد تقسیم می‌کند.

شما هم می‌توانید گزینه‌های نمایشی رمزگشایی بسته‌ها را تغییر دهید ـ به‌خصوص چگونگی نمایش زمان و اسامی شبکه‌ای. از آنجا که هر شبکه، موجودی حساس به زمان است، گزینه‌های وابسته به زمان از اهمیت خاصی برخوردارند. زمان نسبی یا درون بسته‌ای از آن جهت مهم است که تأخیر بین دو بسته را نشان می‌دهد. مقداری خارج از مقادیر معمول نشان‌دهندهٔ وجود یک تأخیر در کسب شبکه نظیر مسیریاب‌ها یا سوئیچ‌ها می‌باشد. یا به احتمال بیشتر تأخیری که به واسطهٔ پردازش در سوی دیگر مکالمه رخ داده است (برای مثال توسط یک سرویس‌دهندهٔ پرکار).



شکل ۵-۲۱ : Shomiti Surveyor و سایر تحلیل‌گرها می‌توانند گراف‌هایی از آمار مختلف ارائه دهند و بنابراین به شما در تفسیر اطلاعات مختلف کمک کنند.

تسخیر عمومی

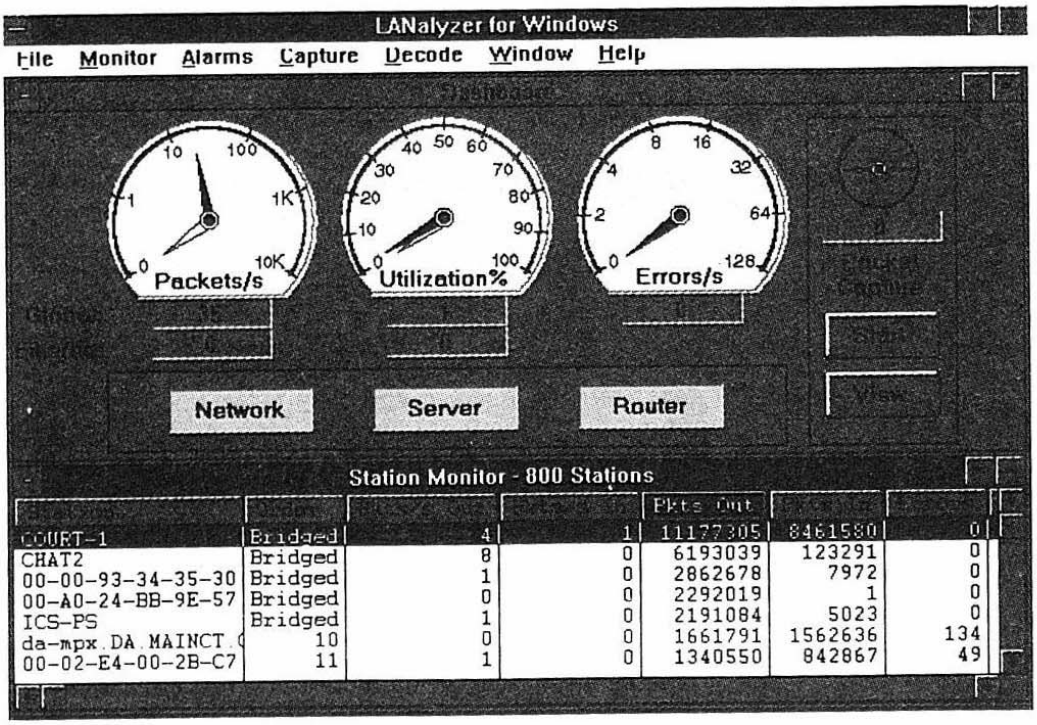
همانطور که تسخیر بسته‌های ویژه می‌تواند در پیداکردن مشکلی خاص مفید باشد، برخی اوقات حالتی پیش می‌آید که تحلیل‌گر خود را در شکلی گسترده به منظور دریافت دیدگاهی عمومی از یک بخش از شبکهٔ خود مورد استفاده قرار می‌دهیم.

برای مثال هنگامی که همهٔ کارکنان موجود در یک شبکه از کُندی عمومی شبکه شکایت می‌کنند، ممکن است بخواهیم تحلیل‌گر را طوری به کار بیندازیم که به صورت کلی آمار مربوط به شبکه را جمع‌آوری کند. تحلیل‌گر به احتمال زیاد قادر است مجموع اقلام مختلفی نظیر اقلام زیر را نگهداری کند.

- تعداد خطاهای هر ایستگاه
- قاب‌های دریافت‌شده توسط هر ایستگاه
- قاب‌های ارسال‌شده توسط هر ایستگاه
- میزان کاربرد کلی شبکه
- تعداد خطاهای شبکه

در یک بخش که به آهستگی کار می‌کند، ممکن است ببینید که میزان کاربرد کلی شبکه بالا و در حدود ۶۵٪ می‌باشد (راندمان کار اِترنت بعد از ۳۵٪ کاهش می‌یابد بنابراین، این مقدار بسیار بالا است). احتمالاً می‌خواهید بدانید که چرا نرخ کاربرد اینقدر بالا رفته است: آیا به تعداد کاربران که همگی از بخش خاصی از شبکه استفاده می‌کنند مربوط است یا اینکه دو تن از آنان منابع شبکه را به خود اختصاص داده‌اند؟ یک روش خوب برای پیدا کردن پاسخ مرتب‌سازی فهرست آمار است. برای مثال، اگر از LANalyzer ناوِل برای مرتب‌سازی آمار خود بر اساس «Packets Outs» با استفاده از کلیک‌کردن در

سرستون مربوطه استفاده کنیم، بلافاصله متوجه خواهید شد که یکی از ایستگاهها مقدار زیادی از منابع را به تخصیص می‌دهد (شکل ۶-۲۱).



شکل ۶-۲۱: تحلیل‌گرها می‌توانند ایستگاههای فعال را بر اساس هر نوع آماری مرتب کنند.

ممکن است بخواهید اطلاعات ویژه‌ای از این ایستگاه کاری را تسخیر کنید تا متوجه شوید چه نوع ترافیکی ایجاد می‌شود ـ یا حتی سریعتر، مستندات MAC خود را بررسی نموده و با یک تماس تلفنی از کاربر بپرسید که در حال انجام چه کاری است. در این حالت، فرض کنید که مکالمهٔ تلفنی آشکار می‌سازد که کاربر در حال تهیه یک کپی پشتیبان از دیسک سخت خود روی شبکه بوده است. بهتر است مؤدبانه از وی بخواهید در طی ساعات پرکار شبکه از این کار اجتناب کند و روش‌های دیگری را برای تهیهٔ کپی پشتیبان از دیسک سخت، مثل استفاده از نوارگردان، پیشنهاد نمایید.

برای آنکه مطمئن شوید که شبکه از سلامت برخوردار است می‌توانید فهرست ایستگاهها را بر اساس خطاها مرتب نمایید. وجود تعداد معدودی خطا در اینجا و آنجا امری طبیعی است فقط کافی است مطمئن شوید که یکی از ایستگاهها با رفتار ناشایست، آزادراه را بند نیاورده باشد.

تجزیه و تحلیل مناسب

اجازه دهید نگاهی داشته باشیم به چند سناریو که استفادهٔ مناسبی برای تحلیل‌گر را پیشنهاد می‌کند. توجه داشته باشید که در تمامی آنها، به یک تئوری دست می‌یابیم که از طریق استفاده از تحلیل‌گر سعی در اثبات آن خواهیم نمود. نگاهی خواهیم داشت به یک برنامهٔ وابسته به فروشنده و مشکلی مربوط به سرویس، آدرس MAC که از درستی محل آن اطمینان ندارید را بررسی خواهیم نمود و آنگاه مشکلی را وارسی می‌نماییم که به کاربرد دو تحلیل‌گر شبکه به صورت همزمان نیاز دارد.

عتیقه‌جات کاربردی

اجازه دهید به فصل ۱۸ و به مشکل مطرح‌شده در بخش «نمی‌توانم کاری را برای چاپ آماده کنم» بازگردیم. به خاطر بیاورید که میزبان یونیکسی داشتیم که در هر لحظه نمی‌توانست بیش از یک کار چاپی به یکی از سرویس‌دهنده‌های چاپ شبکه ارسال کند، با اینکه چندین چاپگر به سرویس‌دهندهٔ چاپ متصل شده بودند. به عبارت دیگر، میزبان تصور می‌کرد که هر سرویس‌دهندهٔ چاپ تنها یک چاپگر دارد ـ که فرضی کاملاً اشتباه بود! در این سناریو، حتی با وجود آنکه از طریق روش عیب‌یابی جعبهٔ سیاه، برای خودم ثابت کرده بودم که میزبان موردنظر منبع به‌وجودآوردن مشکل است، می‌خواستم که مدرک و دلیلی قاطع برای ارائه به فروشنده به دست بیاورم تا به وی ثابت کنم که محصولش متفاوت با سایر پیاده‌سازی‌های فروشندگان دیگر کار می‌کند تا بتوانم وی را برای رفع مشکل تحت‌فشار قرار دهم.

ایجاد یک سری اطلاعات ردیابی از موضوع توسط مشخص نمودن فیلتر تسخیرکنندهٔ آدرس MAC یا آدرس TCP/IP مربوط به سرویس‌دهندهٔ چاپ نسبتاً آسان است. چرا این کار را در مورد میزبان یونیکس انجام ندهم؟ زیرا میزبان یونیکس صدها و صدها کاربر داشت که همگی از طریق TCP/IP به آن دسترسی داشتند ـ در صورت هدف قراردادن میزبان یونیکس، بیش از آنچه که می‌توانستم راهبری نمایم اطلاعات در اختیارم قرار می‌گرفت.

من دو صف آزمون روی میزبان مورد ظن ایجاد نمودم. صف ۱ و صف ۲ ـ یک صف برای هر یک از چاپگرهای متصل به سرویس‌دهندهٔ چاپ. به عنوان یک «تجربهٔ کنترلی» همان دو صف را روی میزبان دیگری آماده ساختم. تسخیر را در تحلیل‌گر آغاز نمودم. و خیلی سریع دو کار چاپی را برای دو صف آزمایشی ارسال کردم. به تحلیل‌گر بازگشتم، تسخیر را متوقف نموده و آن را روی دیسک ذخیره کردم، اسم فایل را Problem گذاشتم.

آنگاه همان روال را با استفاده از میزبان دیگر به انجام رساندم. اسم این فایل را Good گذاشتم، چرا که تسخیر صورت‌پذیرفته در مورد میزبان یونیکسی اتفاق می‌افتاد که مغزش از کار نیافتاده بود. (با اینکه عملکرد فروشندهٔ مزبور سریع و بلافاصله نبود، مسئول فروش‌مان نحوهٔ کارکرد ما روی اطلاعات به دست آمده را پسندید و برای میزبان مذکور جایگزینی خریداری نمود که تأثیر مثبت زیادی در ارتباطمان با این فروشنده داشت ـ بنابراین کار ما ارزش انجام خود را نشان داد. در حقیقت، هنگامی که با شروع مشکلات در آن ماشین و پیاده‌سازی یونیکس درگیری پیدا کردیم، ماشین جدیدی تا هنگام تعمیر در اختیارمان قرار گرفت).

برخی از نکات مهم که هنگام ارائهٔ اطلاعات ردیابی شدهٔ تحلیل‌گر به فروشنده باید درنظر گرفته شوند، عبارتند از:

- ردیابی‌ها باید کوچک باشند. تا آنجا که می‌توانید فیلتر کنید.
- ردیابی‌ها باید گسسته باشند. همانطور که قبلاً نشان داده شد باید چندین ردیابی مختلف داشته باشید که نشان‌دهندهٔ عملکرد سالم در مقابل عملکرد خراب باشند.
- به همراه ردیابی‌ها باید توضیحاتی مختصر و مفید در مورد مشکل و نحوهٔ انجام عملیات عیب‌یابی را به همراه داشته باشید.

تشخیص ایستگاه

سایت‌هایی را دیده‌ام که در آنها آدرس‌های MAC به خوبی مستندسازی نشده بودند و بنابراین از بین بردن خطاهای مربوط به MAC امری مشکل بود. برای مثال، تصور کنید که ویندوز اعلام می‌کند که آدرس TCP/IP تکراری روی آدرس MAC 00:00:C9:05:89:62 وجود دارد. اگر آدرس‌های MAC مستندسازی نشده باشند و اگر تحلیل‌گر شما به صورت خودکار اسامی شبکه‌ای را برایتان مشخص نکند، ممکن است فکر کنید که بدشانسی آورده‌اید. همین امر در صورتی که تحلیل‌گر ماهرتان به شما بگوید که 00:08:02:55:29:2A احتمالاً کارت شبکه‌ای خرابی است و خطاهای شبکه‌ای بسیاری را

باعث می‌شود صادق است.

اما این مشکلی نیست! می‌توانید به تمامی ترافیک MAC تولیدشده توسط این ایستگاه کاری گوش فرا دهید و این احتمال وجود دارد که چیزی را دریافت کنید که کاربر را شناسایی کند. با نگاهی به اطلاعات شانزدهی یا پنجرهٔ رمزگشایی کاراکتری، اطلاعات گوناگونی را ملاحظه می‌کنید که ممکن است به شناسایی ایستگاه کاری کاربر (یا دپارتمان وی) کمک کند. این چیزی است که به کمی تمرین نیاز دارد، اما با به‌کار انداختن فکر به‌زودی بر چنین کاری مسلط خواهید شد، برای مثال فیلترکردن جلسه‌های Telnet دیدگاهی کلی روی Telnet کاربر به شما ارائه می‌کند. به آغاز بروید و اسم ورودی را دریافت کنید. با حذف اطلاعات اضافی، ممکن است گزارش یا صفحه منویی را ببینید که تنها کاربری خاص یا دپارتمانی به‌خصوص مورد استفاده قرار می‌دهد. به این ترتیب بد نیست که در مطالعهٔ رمزگشایی‌های پروتکلی خود ماهر شوید. اگر در مورد یک مشکل غیربحرانی فرصت کافی داشته باشید، بهتر است این کار را انجام دهید!



نکته : اگر فیلتری را برای جلسه‌های TCP ساخته‌اید، جستجویی به دنبال یک بستهٔ SYN صورت دهید. این بسته آغازکنندهٔ هر جلسهٔ TCP است. معادل «الو؟» هنگام برداشتن تلفن می‌باشد ـ و احتمالاً اسم کاربر را در یکی از بسته‌های نزدیک آن پیدا خواهید کرد.

حلقه شکسته

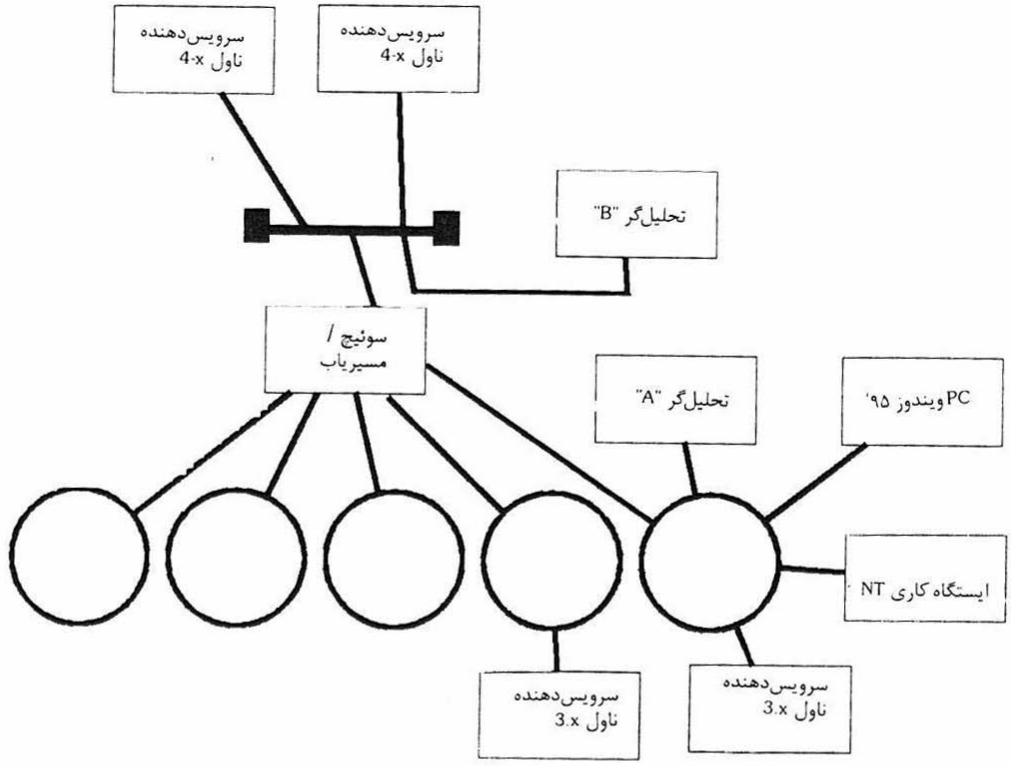
موقعیتی را مورد توجه قرار دهید که در ابتدای این فصل در مورد آن سخن راندیم: ویندوز NT که در شبکهٔ حلقه-نشانده در استفاده از سرویس‌دهنده‌های ناوِل دچار مشکل می‌شد. با وجود اینکه صدها PC ویندوز ۹۵ به خوبی کار می‌کردند اولین آزمایش ارزیابی ایستگاه کاری ویندوز NT مشکلات اتصالی متعددی را با سرویس‌دهنده‌ها آشکار ساخت ـ یعنی، هیچ‌یک از ایستگاههای کاری جدید نمی‌توانستند هیچ یک از سرویس‌دهنده‌های جدید ناول را ببینند. اما می‌توانستند برخی از سرویس‌دهنده‌های قدیمی‌تر را مشاهده کنند. البته تمامی آنها می‌توانستند با تمامی سرویس‌دهنده‌های NT و یونیکس با استفاده از TCP/IP تماس برقرار کنند. نگاهی به شکل ۷-۲۱، نموداری از سناریو را نشان می‌دهد: تمامی ایستگاههای کاری در حلقه-نشانه قرار داشتند. سرویس‌دهنده‌های جدید در اِترنِت سریع و سرویس‌دهنده‌های قدیمی‌تر به حلقه-نشانه متصل بودند. سرویس‌دهنده‌های جدیدتر از نِتوِر نگارش ۴/۱۱ استفاده می‌نمودند؛ قدیمی‌ترها از نگارش 3.x استفاده می‌کردند.

از آنجا که ارزیابی آزمایشی ما در یک بخش صورت می‌پذیرفت برای امتحان یکی از ایستگاههای کاری را به بخش دیگری منتقل نمودیم. با توجه، اکنون می‌توانستیم با سرویس‌دهنده‌های ناوِل 3.x رابطه برقرار کنیم. از قرار معلوم تنها سرویس‌دهنده‌های ناوِلی را می‌توانستیم ببینیم که مستقیماً به حلقه‌ای که در آن بودیم متصل شده بودند. این باعث شد که باور کنیم مشکل به سوئیچ مربوط است.

برای آنکه ببینیم سوئیچ داده‌ها را به شکل مناسبی عبور می‌دهد، دو تحلیل‌گر به شبکه متصل نمودیم: یکی به بخشی که ایستگاه‌کاری در آن قرار داشت (نقطه A) و دیگری به بخشی که «سرویس‌دهنده مشکل‌زا» در آن واقع شده بود (نقطه B). هر بسته‌ای که از سوئیچ عبور نمود، می‌بایست بسته متناظری در سوی دیگر داشته باشد.

به خاطر کوچک نگاه‌داشتن فایل‌های ردیابی، تحلیل‌گر نقطه A را طوری تنظیم نمودیم که تنها بسته‌های دریافتی از ایستگاه‌کاری آزمایشی را تسخیر نماید. از آنجا که بسته‌های نقطه B به نظر نمی‌رسیدند که از آدرس MAC ایستگاه‌کاری آزمایش ارسال شده باشند (به جای آن، از سوئیچ ارسال شده بودند)، ما از قصد ایستگاه‌کاری را به یک سرویس‌دهنده آزمایش کم‌استفاده متصل نموده و تمامی اطلاعاتی که به آن سرویس‌دهنده می‌رفت را تسخیر نمودیم. ایستگاه‌کاری NT

رامجدداً راه‌اندازی کردیم و سعی کردیم به سرویس‌دهنده آزمایشی متصل شویم. همین که در انجام عمل ورود به سیستم با شکست مواجه شدیم، هر دو تحلیل‌گر را متوقف نمودیم.



شکل ۷-۲۱: مشکلی که به تسخیر در دو بخش به صورت همزمان نیاز داشت.

تحلیل‌گرها روشن ساختند که در واقع، سوئیچ است که برخی از بسته‌ها را ازبین می‌برد (اشکال در بسته‌های «خراب»ای که به سرویس‌دهنده رسیده اما قابل درک نبودند، ناشی نمی‌شد). عالی است، پس چه اتفاقی می‌افتاد!

ما همین تست را با یک ماشین ویندوز ۹۵ انجام دادیم و نتایج را مقایسه کردیم. ماشین‌های ویندوز NT از «مسیریابی منبع»، یک پروتکل لایه پیوند حلقه ـ نشانه استفاده می‌کردند که البته در مورد ویندوز ۹۵ این طور نبود (برای عیب‌یابی این مسأله، نیازی نیست که بدانیم مسیریابی منبع چیست؛ کافی است بدانیم که تفاوت بین دو ردیابی می‌باشد). از آنجا که پیکربندی سوئیچ، امکان مسیریابی منبع را فراهم نمی‌کرد، بسته‌ها از دست می‌رفتند. دو راه حل پیش رویمان قرار داشتند: پیکربندی سوئیچ به منظور مجازساختن مسیریابی منبع یا پیکربندی ایستگاه‌کاری NT بدون مسیریابی منبع. هر دو گزینه آسان و سریع هستند. پرونده مختومه اعلام شد!

محدودیت‌ها و راه‌حل‌ها

همان طور که ملاحظه می‌کنید، استفاده از تحلیل‌گر، مطابق میل‌تان، در زمان صرفه‌جویی می‌کند. اگر دانش‌آموز مدرسه ابتدایی بودید که فرصت کافی در خواندن دیکشنری و لغت‌نامه را در اختیار دارد، می‌توانستید وقت زیادی را روی رمزگشایی‌های پروتکلی صرف کنید. البته، اگر کارهایتان زیاد است، ممکن است تنها بتوانید آه بکشید و رمزگشایی‌های پروتکلی را برای زمان کم‌مشغله‌تری ذخیره کنید ـ و از مهارتهای عیب‌یابی جعبه سیاه خود برای مجزاسازی در جایی که به استفاده از تحلیل‌گر نیاز است، استفاده نمایید.

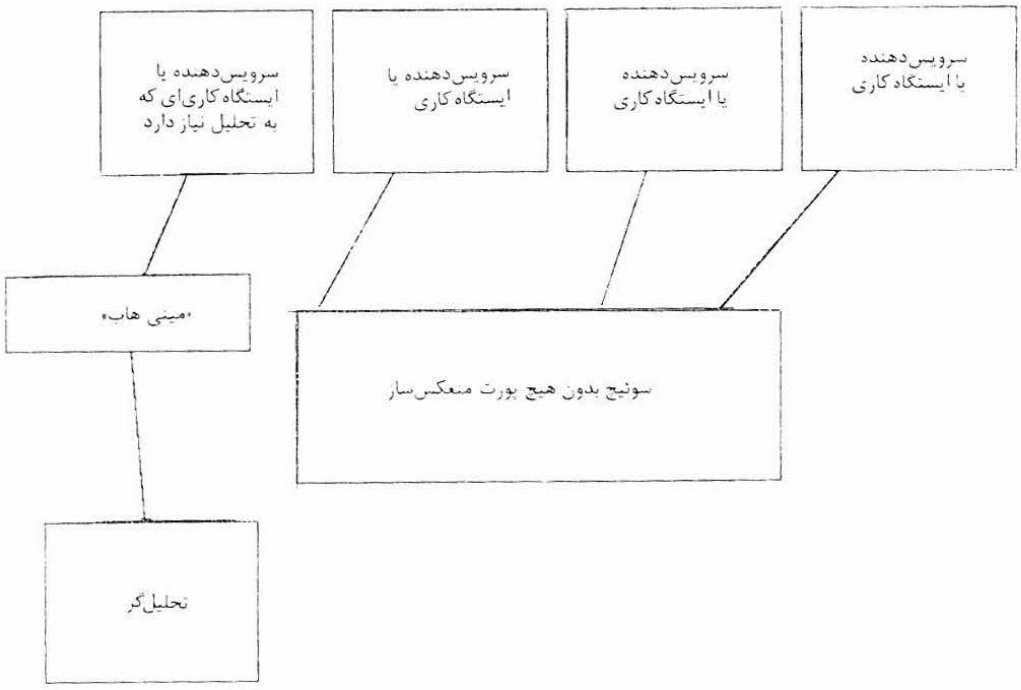
تا آنجا که به محدودیت‌های فیزیکی مربوط می‌شود، به خاطر داشته باشید که هر تحلیل‌گر تنها می‌تواند عمل شنود را روی یک خط جمعی به انجام برساند. نمی‌توانید عمل شنیدن را در مورد ایستگاهی که اتصالی نقطه ـ به ـ نقطه به یک سوئیچ دارد انجام دهید، زیرا هابی برای اتصال و شنود وجود دارد. پس چه باید کرد؟



نکته : *در مستندات سوئیچ خود، دنبال امکانی به نام* همانندسازی پورت[1] *بگردید. این امکان، به‌شما اجازه‌می‌دهد مشخص‌کنید کدام پورت سوئیچ برای شنود به‌کار رود. کافی‌است تحلیل‌گرتان را به‌پورت دیگری از سوئیچ وصل کنید تا سوئیچ نقش خود را ایفا کند و در مورد آن به تحلیل‌گر اطلاع دهد. در صورت عدم پشتیبانی از همانندسازی پورت در سوئیچ، مطابق شکل ۸-۲۱، می‌توانید دست به‌کار شوید. کافی است مراحل زیر را انجام دهید:*

۱- یک مینی‌هاب (اِترنِت) یا یک «مضاعف‌ساز گره» (حلقه ـ نشانه) فراهم کنید.
۲- کابل شبکه را از ایستگاه مورد نظر خود جدا سازید.
۳- کابل ایستگاه را به پورت آبشاری مینی‌هاب یا «لُب (بخش)» مضاعف‌ساز گره متصل کنید.
۴- کابل شبکه‌ای را از مینی‌هاب یا مضاعف‌ساز گره به تحلیل‌گر متصل نمایید.
۵- کابل شبکه‌ای را از مینی‌هاب یا مضاعف‌ساز گره به ایستگاه مقصد متصل کنید.

این‌کار، معلول ایجاد بخشی اشتراکی در پورت سوئیچ است، حالا می‌توانید عمل شنود را انجام دهید.



شکل ۸-۲۱: می‌توانید با استفاده از یک «مینی‌هاب» و ایجاد یک بخش بین سوئیچ و ایستگاه نهایی، نقش همانندسازی پورت را خود بازی کنید.

بسیاری از تحلیل‌گرهای امروزی، عامل‌های نظارتی راه دور[2] یا پراب‌ها را عرضه می‌کنند که امکان نظارت چندین بخش از شبکه را با استفاده از تنها یک تحلیل‌گر میسر می‌سازد. این «عامل‌ها» یا «نماینده‌ها» تنها برنامه‌های کوچکی

1- port mirroring 2- Remote monitoring agents

هستند که روی ایستگاه‌کاری یا سرویس‌دهنده به اجرا درمی‌آیند و مجموعه‌ای از توابع تحلیل‌گری بدون رمزگشایی یا توابع تحلیل آماری را دارا هستند. این عامل‌ها، داده‌های جمع‌آوری‌شده را به تحلیل‌گر اصلی می‌فرستند که در جایی از شبکه که شما می‌خواهید، قرار گرفته است. البته، این حالت در صورتی امکان دارد که شبکه و ایستگاههای پراب‌دار، بالا باشند، اما در مجموع روش بسیار خوبی برای مشکلات چندبخشی و نظارت در عین اجرا می‌باشند، به این دلیل که می‌توانید کلیه این کارها را از پشت میز خود به انجام برسانید.

خلاصه

تحلیل‌گر شبکه، ابزاری است که به بسته‌های شبکه در بخشی اشتراکی گوش فرامی‌دهد و آنها را در قالب قابل خواندن توسط انسان، رمزگشایی می‌نماید. برخی از آنها بسیار گرانقیمت و برخی ارزانقیمت هستند. نکته بااهمیت در مورد آنها این است که اگر کارت شبکه‌ای از نوع مناسب ـ یعنی کارت شبکه‌ای «همگانی»، که قادر است تمامی بسته‌های شبکه را دریافت کند ـ داشته باشید، استفاده از آنها در هر نوع PC ای میسر است.

بسته به تحلیل‌گر، می‌توانید تواناییها و امکانات مختلفی را از آن انتظار داشته باشید که به شما کمک می‌کنند اطلاعات خام تسخیرشده توسط تحلیل‌گر را تجزیه و تحلیل نمایید. برخی از این توابع، فیلترسازی روی تسخیر، نمایش‌های آماری قابل مرتب‌سازی، تحلیل «هوشمندانه» داده و نماهای سفارشی را شامل می‌گردند.

همیشه بیش از یک تحلیل‌گر در بازار وجود دارد، چرا که مشکلات متعددی هم ممکن است بروز کنند. تحلیل‌گرهای مختلف برای بررسی مشکلات متفاوتی مناسب هستند. به ویژه، حلقه ـ نشانه به امکانات خاصی نیاز دارد که در تحلیل‌گرهای عمومی وجود ندارند.

دانستن اینکه چه زمان و چه چیزی را فیلتر نماییم، بخش مهمی از آموختن در به‌کارگیری تحلیل‌گر می‌باشد. بعد از آنکه یاد گرفتید چگونه فایل‌های ردیابی کوچک قابل مدیریتی ایجاد نمایید، خواهید توانست با بازبینی آنها، آنچه که برای حل مشکلات لازم دارید، به دست آورید و یا از فروشنده‌ای خاص برای حل مشکل یاری بطلبید.

تحلیل‌گرها، مثل هر ابزار دیگری، محدودیت‌هایی دارند؛ اما اگر با آنها کنار بیایید، در کنار تواناییهای خود شما، ابزاری قدرتمند در عیب‌یابی خواهند بود.

کارگاه

پرسش و پاسخ

پرسش : تحلیل‌گران شبکه، سالها روی بررسی داده پروتکلی وقت صرف می‌کنند. چگونه از من انتظار دارید که ظرف یک ساعت آن را فراگیرم؟

پاسخ : کلید معما، میدان محدودی است از آنچه که شما انتظار دارید که انجام شود. صحیح است. با وجود آنکه احتمالاً قادر هستید پروتکل‌ها و سرویس‌های نهان در هر برنامه و سرویس را بشناسید و دوست داشته باشید، چرا باید بخواهید چنین کاری انجام دهید؟ تحلیل‌گرها، به سادگی روش کارآمد برای به‌کارگیری مهارتهای عیب‌یابی جعبه‌سیاه می‌باشند. اگر هر آنچه راکه روی صفحه رمزگشایی ظاهر می‌شود، درک نمی‌کنید، ناامید نشوید ـ فقط به‌خاطر داشته باشید که مرتب از خود

سؤالاتی نظیر «کدامیک ازآنها مثل بقیه نیست؟» را بپرسید و مطمئن باشید که راه درست را می‌پیمایید. اگر احساس می‌کنید که باید عمیقتر حفر کنید، یک کتاب پروتکل بردارید و مشغول شوید. البته، در بسیاری حالات، این‌کار غیرضروری است.

پرسش : مینی‌هاب اِترنِت یا مضاعف‌ساز گره حلقه ـ نشانه را از کجا می‌توانم تهیه کنم؟

پاسخ : از همانجا که می‌توانید مینی سوئیچ را تهیه کنید: کافی است یکی از فروشگاههای شبکه که صفحه خانه‌هایی روی شبکه دارند ملاقات کنید. من www.networksnow.com و www.datawarehouse.com را پیشنهاد می‌کنم که هریک می‌توانند اقلام مورد نظر را دراختیار بگذارند.

آزمون

۱- درست یا نادرست؟ تفاوت بین پویشگر کابلی و تحلیل‌گر شبکه آن است که اولی می‌تواند تمامی مشکلات سطح شبکه را حل کند.

۲- بیشتر تحلیل‌گرها دارای عدم دو حالت عملیاتی هستند؟

الف ـ تسخیر نشان و یک حلقه رمزگشایی سری
ب ـ تسخیر بسته و رمزگشایی بسته
ج ـ تسخیر داده و رمزگشایی اِترنِت
د ـ نمایش و مرتب‌سازی

۳- تحلیل‌گر شبکه به یک کامپیوتر و کارت شبکه _____ نیاز دارد.

الف ـ همگانی
ب ـ تک پورته
ج ـ دوپورته
د- بسته‌ای

۴- درست یا نادرست؟ تشخیص زمان و ماهیت فیلترسازی بخش مهمی از آموزش چگونگی استفاده از تحلیل‌گر را تشکیل می‌دهد.

۵- فیلتر می‌تواند _____ باشد.

الف ـ وابسته به ایستگاه‌کاری
ب ـ وابسته به پروتکل
ج ـ هم الف و هم ب
د ـ نه الف و نه ب

۶- درست یا نادرست؟ اگر تحلیل‌گر شما، اسامی شبکه‌ای (نظیر DNS یا NetBIOS) را جمع‌آوری نکند، تعیین آنکه کدام کامپیتر با یک آدرس MAC متناظر است، غیرممکن خواهد بود.

۷- قصد دارید تحلیل‌گری را به یک بخش از یک شبکه متصل کنید. برای حصول بهترین نتایج، ابتدا باید چه کاری را به انجام برسانید؟

الف ـ بسته‌هایی را ردیابی کرده باشید
ب ـ گزینه دیگری را شکل داده باشید
ج ـ یک تئوری مدنظر داشته باشید
د ـ تصمیم گرفته باشید که از فیلتر استفاده نکنید

پاسخ به سؤالات آزمون

۱- نادرست
۲- ب
۳- الف
۴- درست
۵- ب
۶- نادرست
۷- ج

فصل ۲۲

ابزار مدیریت شبکه

هیچ چیزی به اندازهٔ مسؤولیت مستقل، قضاوت را قدرت نمی‌بخشد و وجدان را تحت تأثیر نمی‌گذارد.
الیزابت کدی استانتون

«مدیریت شبکه» شاید یکی از پرکاربردترین عبارات در شبکه باشد. سابق معنای آن هر چیزی از مدیریت تغییر تا نظارت بر شبکه و پیکربندی مجدد از راه دور بود و به عنوان عبارتی که رابطهٔ نزدیکی با پول داشت در بازار مطرح شده بود. بدان معنا که می‌توانستید دهها هزار دلار سخت‌افزار و نرم‌افزار خریداری کنید که به رهیافتی خصوصی که کار چندانی را انجام نمی‌داد، منتهی گردد که نتایج بسیار ضعیفتری را نسبت به هزینهٔ صرف‌شده به دنبال داشت.

اما این موضوع دیگر تمام شده است! بسته‌های مدیریت شبکه امروزی ابزار قدرتمندی را برای کمک به شما به منظور هماهنگ‌سازی وظیفهٔ نگهداری ردیابی از صدها ابزار شبکه و هزاران ایستگاه‌کاری شبکه، فراهم می‌آورند. با اینکه ایستگاههای مدیریتی سطح بالا و پراب‌های شبکه‌ای مرتبط با آنها گرانقیمت می‌باشند، انتخاب بین استفاده از ابزار ساده و بی‌هزینه یا ابزار پیچیده و جامع با شماست.

بسته‌های مدیریت هرچیزی را شامل می‌شوند. آنها بخصوص ابزاری دارند که ما به طور خلاصه مورد بحث قرار داده‌ایم:

- ابزار به‌کارگیری عمومی برنامه‌های کاربردی شبکه (فصل ۱۶)
- کنترل از راه دور و پشتیبانی (فصل ۱۷)

در این فصل، ابزار مدیریت شبکه را به عنوان هر وسیله‌ای که به شما در نظارت بر ساختار شبکه، برنامه‌های کاربردی و سرویس‌دهنده‌ها از راه دور کمک می‌کنند، تعریف خواهیم نمود. خواهید دید که مدیریت شبکه می‌تواند کنترل اوضاع را در اختیار شما قرار دهد و شبکه قابل اطمینان‌تری ایجاد نماید.

ناظر بزرگ مشغول نظارت است

کار اصلی مدیریت شبکه، در واقع نظارت بر سرویس‌ها و فراساختارهای کلیدی می‌باشد. ما به عنوان عیب‌یاب‌های شبکه، مشاهده در شرایطی که چیزها با خرابی روبه‌رو می‌شوند و بعد از وقوع خرابی، برایمان جالب است. با انجام نظارت، اقلام زیر برایمان قابل توجه است:

- کارایی ـ آیا منبع مورد نظر به پایان رسیده است؟ چه چیزی باعث به پایان‌رسیدن آن شده است؟

- زمان کارکرد ـ چه مدت‌زمان به طور صحیح فعال بوده است؟ آیا باید با آن به‌شکل پیمانه‌ای اجتناب‌پذیر برخورد کنیم؟
- قابلیت دسترسی ـ آیا منبع در دسترس قرار دارد، یا اینکه پایین است؟

از آنجا که می‌توانید صدها منبع مستقل را از طریق شبکه نظارت کنید ـ برای مثال، منابع تغذیه در سرویس‌دهنده، تک‌تک گردونه‌های دیسک سخت، نمای داخلی CPU، بافرهای کارت شبکه و غیره ـ بسته‌های مدیریت شبکه مفاهیم آستانه‌ها و هشدارها معرفی نمودند.

هنگامی که منبعی از آستانه‌های تأمین‌شده توسط شما یا سازنده، خارج می‌شود، یک هشدار برای شبکه تولید می‌گردد و شما از آن آگاه می‌شوید. این مفهوم اولیه در ورای نظارت بر شبکه می‌باشد.

بسته به ابزار مدیریت شبکه انتخابی، روال کار ممکن است کم‌وبیش به صورت خودکار باشد. برخی از بسته‌های مدیریتی از روشهای خاص خود برای نظارت استفاده می‌کنند (که در صورت کارکرد، استفاده از آن مشکل نخواهد بود) و برخی از نظارت استاندارد استفاده می‌نمایند. کدامیک برای شما مناسب است؟ این موضوع واقعاً به این بستگی دارد که مجموعهٔ کاری شما چقدر بزرگ باشد، چه ابزاری را فروشنده برایتان هنگام خرید ابزار شبکه فراهم آورده باشد، و چقدر خوب آنها در یک راه حل مدیریتی گنجانده شوند. ما این موضوع را در ادامهٔ بحث روشن خواهیم ساخت، اما ابتدا اجازه دهید نگاهی به استانداردهای نظارتی موجود داشته باشیم.

MIB

مدیریت شبکه، مثل شکل کلی و حالت موجود در تمامی امور شبکه، پر است از واژه‌ها و کلمات کوتاه‌شده. سه کلمه مخفف مهم (که استانداردهای مهم TCP/IP بااهمیت‌تر می‌سازند) عبارتند از: SNMP، MIB و RMON.

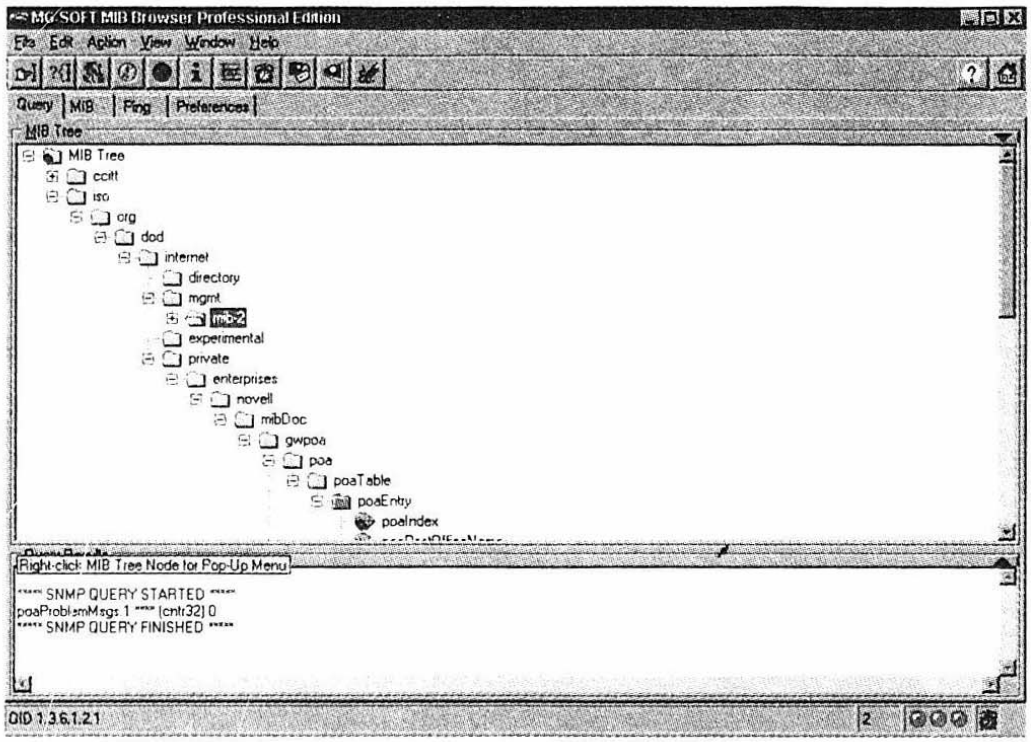


نکته : *پاسخ به سؤالات عمومی در مورد SNMP، RMON و MIBها را در بخش دوم کتاب، «استراتژی‌های عیب یابی جعبه سیاه» و نیز ftp://rtfm.mit.edu/pub.usenet/news.answers/snmp-faq/part1 خواهید یافت.*

SNMP مخفف پروتکل سادهٔ مدیریت شبکه[1] می‌باشد. و روش استانداردی است برای فراهم‌آوردن اطلاعات شبکه برای گره‌هایی که این اطلاعات را درخواست می‌کنند، در حالی که گره‌های مجاز می‌توانند آنها را تغییر نیز بدهند. این کار چگونه انجام می‌شود؟

SNMP یکی دیگر از سرویس‌های TCP/IP می‌باشد، سرویسی که در سوکت ۱۶۱ مربوط به UDP اقامت دارد. هر ایستگاه‌کاری، سرویس‌دهنده، مسیریاب، سوئیچ و به طور کلی هر ابزار شبکه‌ای که سرویس SNMP روی آن به اجرا درآمده باشد، عامل *SNMP* نامیده می‌شود. هر عامل SNMP متغیرهای خاصی را برای ایستگاههای مدیریتی درخواست‌کننده فراهم می‌آورد. به هر مجموعهٔ عمومی از متغیرهای مشخص، یک MIB گفته می‌شود. MIB ها اطلاعاتی را که از طریق SNMP در دسترس قرار می‌گیرند، تشکیل می‌دهد. شکل ۱-۲۲ یک مرورگر MIB را از شرکت MG-Soft (www.mg-soft.com) نشان می‌دهد.

1- Simple Network Management Protocol



شکل ۱-۲۲: مرورگر MIB از شرکت MG-Soft روش خوبی برای شروع آشنایی با SNMP و MIB ها می‌باشد.

MIB چیست؟ MIB مخفف پایگاه اطلاعاتی مدیریت‌شده[1] می‌باشد و روش مختصری برای اشاره‌کردن به تمامی متغیرهای منبع که در یک گروه وجود دارند، است. برای مثال، تمامی عامل‌های SNMP به متغیرهای MIB-I و MIB-II، نظیر SysContact، SysName، SysLocation برای ثبت رکورد و ifOutOctets و ifInOctets که به تعداد بایت‌های دریافتی یا ارسالی توسط یک رابط (if) اشاره می‌کنند، پاسخگو هستند. البته برای قادربودن به خواندن متغیرهای هر عامل، به یک ایستگاه مدیریت شبکه نیاز دارید.

بسیاری از سازندگان MIB های خاص خود را فراهم ساخته‌اند، چرا که آنها اطلاعات ویژه‌ای دارند که در MIB های عمومی گنجانده نشده است. برای مثال، سیستم GroupWise من، دو متغیر ویژه در MIB های خود دارد که برای هیچ سیستم دیگری قابل استفاده نیست (برای مثال، poaUndeliverableMsgs که مخفف پیغامهای غیرقابل تحویل عامل دفتر پستی می‌باشد). فرض بر آن است که عاملی که روی یک ابزار یا نرم‌افزار اقامت دارد، از قبل MIB خود را می‌شناسد؛ گواینکه یک فایل MIB وجود دارد که به شما اجازه می‌دهد MIB را به مدیر شبکه‌ای که چیزی در مورد آن نمی‌داند «صادر» کنید و در آن بگنجانید.



نکته : *مرورگر MIB که در شکل ۱-۲۲ نشان داده شده است، ابزار خوبی در دنیای MIB و SNMP به شمار می‌رود. این ابزار شامل یک کامپایلر MIB است و بنابراین شما می‌توانید MIB های فراهم‌آمده توسط فروشنده را در آن درج کنید و اطلاعاتی را عامل مربوطه فراهم می‌آورد وارسی نمایید.*

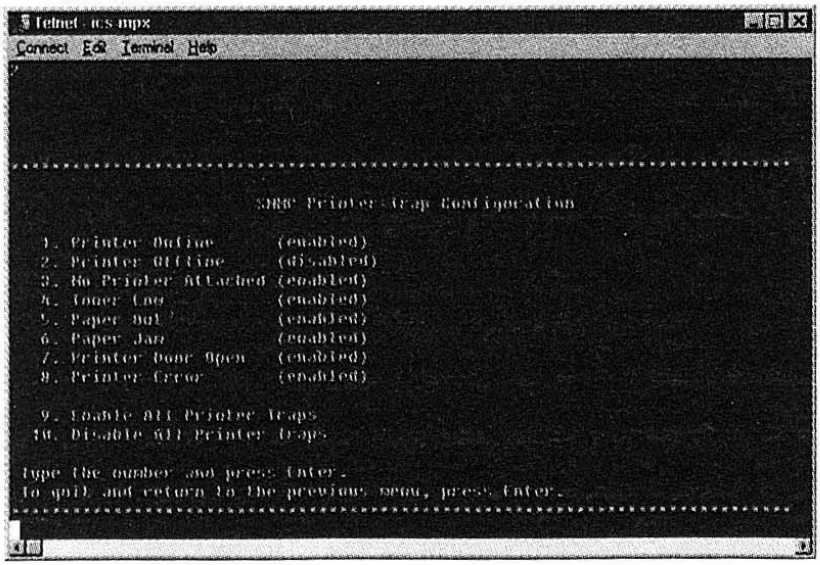
بنابراین داشتن یک عامل SNMP روی یک وسیله، به شما اجازه می‌دهد اطلاعات ردیابی میلیونها منبع را در یک زمان نگهداری کنید. اما تکلیف هشدارها چیست؟ یعنی، هنگامی که چیزی از آستانه‌های خود فراتر می‌رود، SNMP چگونه در

1- Managed Information Base

مورد آن به شما خبر می‌دهد؟

هر عامل SNMP را می‌توان طوری پیکربندی نمود که تله‌ای را برای شبکه منتشر کند (تله کلمه دیگری است برای هشدار). اگر ایستگاه مدیریت شبکه شما در حال شنود تله‌ها باشد، شما را از طریق یک نشان اضطراری آگاه می‌سازد. برای مثال می‌تواند شما را صدا بزند و یا اینکه هر کار دیگری که بخواهید انجام دهد. تله‌ها روش بسیار خوبی برای آگاه‌سازی از وقوع خرابی در شبکه می‌باشد.

البته در دنیای واقعی تله ممکن است هشداری بی‌اهمیت باشد. برای مثال سرویس‌دهنده‌های چاپی که ما مورد استفاده قرار می‌دهیم، همگی یک تلهٔ SNMP را هنگام برخط‌نبودن چاپگرهایشان ارسال می‌کنند. ما صدها چاپگر در شبکه داریم که بسیاری از آنها از قصد خاموش می‌شوند (برای تغییر کاغذ، افزودن فُرم‌ها و غیره). راهی برای ممانعت از آنها در ارسال تله‌ها به ایستگاه مدیریت شبکه وجود ندارد. خوشبختانه هنگام پیکربندی سرویس‌دهندهٔ چاپ، امکان خاموش‌کردن این تله در اختیار گذاشته می‌شود. (شکل ۲-۲۲ را ملاحظه کنید).



شکل ۲-۲۲: نمایی از سرویس‌دهنده چاپ با پیکربندی SNMP از طریق جلسهٔ Telnet.

برخی از عاملان SNMP را می‌توان طوری پیکربندی نمود که چندین «سطح» مختلف از تله‌ها را به مدیر شبکه ارسال کند. به این شکل، دیگر برای امور جزئی و بی‌اهمیت صدا زده نمی‌شوید. برای مثال GroupWise MIB مورد استفاده من برخی از تله‌ها را به عنوان تله‌های «اطلاعاتی» (برای مثال هنگام شروع کار دفتر پستی) و برخی دیگر را «بحرانی» (برای مثال هنگامی که دفتر پستی باید پایین برود یا غیرفعال شود) تعریف کرده است. مسلماً، تمایل دارم که تنها برای موضوعات بحرانی و نه برای مواقع حادث‌شدن موارد اطلاعاتی صدا زده شوم.

RMON

MIB های اینترنتی (MIB-I و MIB-II) مجموعه‌ای از متغیرها هستند که اجازه می‌دهند وسایل و ابزار مستقل اطلاعات *وضعیتی* وضعیت *دروئی* خود را نگهداری کند. اما وضعیت بخشی از شبکه که این ابزار در آن قرار گرفته‌اند چطور می‌شود؟ اینجا جایی است که RMON وارد ماجرا می‌شود. RMON (Remote Moitoring) یک MIB مخصوص می‌باشد که برای وسیله‌ای خاص تعریف شده است ـ یعنی وسیله‌ای که تنها هدفش نگهداری اطلاعات ردیابی آمار ترافیک شبکه است. شباهت زیادی با تحلیل‌گر شبکه دارد؟ خوب، بله و نه. هر پراب RMON رد آمار شبکه را بسیار شبیه به تحلیل‌گر هنگام

تسخیر بسته‌ها نگهداری می‌کند. البته این انتظار از پراب‌های RMON وجود ندارد که بسته‌ها را متناوباً تسخیر کند؛ به جای آن، وظیفهٔ آنها جمع‌آوری پیوسته اطلاعات آماری در مورد شبکه و سایر ایستگاههای شبکه‌ای می‌باشد (بله، برخی از پراب‌های RMON بسته‌های خاصی را از شبکه، نظیر تحلیل‌گر شبکه، به تسخیر درمی‌آورند).

از آنجا که پراب‌های RMON همیشه فعال هستند، هنگام بروز یک مشکل این شانس وجود دارد که پراب آنچه که به وقوع پیوسته را دریافت کرده باشد. برای مثال، به جای اتصال ردیاب یا سایر تحلیل‌گرهای شبکه‌ای به بخش مورد نظر و جستجو به دنبال مشکل، به سادگی می‌توانید از عامل RMON در مورد چگونگی وضعیت سؤال کنید. از آنجا که RMON رد کاربردی هر ایستگاه را نگهداری می‌کند، در صورت کند بودن شبکه، می‌توانید اطلاعات آماری را وارسی نموده و به سادگی کسانی را که بیش از همه صحبت می‌کنند را شناسایی نمایید.

بسته نرم‌افزاریی که RMON را در ترکیب با پراب‌های RMON پشتیبانی می‌کند، همچنین قادر می‌سازد که تجزیه و تحلیل آماری طولانی مدتی روی بخشهای چندگانه شبکه انجام داده و خط پایه‌ای از چگونگی کارکرد شبکه هنگام سالم‌بودن آن ایجاد نمایید. این مفهوم هنگام تلاش برای پیداکردن دلیل کُندی امروز شبکه در شرایطی که دیروز چنین نبوده، بسیار مهم است؛ در فصل ۲۳ بیشتر در مورد خط پایه صحبت خواهیم نمود. برخی از بسته‌های نرم‌افزاری مدیریت سازگار با SNMP عبارتند از:

- Kaspia Network Audit Techology (www.kaspia.com)
- Technically Elite MeterWare(www.tecelite.com)
- HP OpenView (www.hp.com)
- IBM NetView (www.ibm.com
- NetScout (www.netscout.com)

مدیریت شبکه غیراستاندارد

من استانداردها را دوست دارم. چرا که آنها تضمین می‌کنند که همه اعضای ارکستر از یک صفحه موسیقی کار خود را به انجام می‌رسانند. البته ایستگاههای مدیریت SNMP و RMON بزرگ و راه حل‌هایی گرانقیمت محسوب می‌شوند و برخی اوقات برای کاری که می‌خواهید انجام دهید، مناسب نیستند به همین خاطر بسیاری از فروشندگان ابزار نظارتی خصوصی خود را استفاده می‌کنند یا حتی ترکیبی از SNMP و نرم‌افزار نظارتی خصوصی خویش را به شما عرضه می‌دارند. اشکالی در این کار وجود ندارد. اگر برایتان کار کند، بسیار هم عالی خواهد بود!

برای مثال شرکت Dell نگارشی مخصوص از مدیر سرویس‌دهنده مربوط به HP OpenView را فراهم می‌آورد ـ که تمام کاری که انجام می‌دهد نظارت بر سرویس‌دهنده‌های Dell می‌باشد که در صورتی که تنها سرویس‌دهنده‌های Dell داشته باشید، بسیار رهگشاست. ALR، Compaq و HP نیز چنین ابزاری را فراهم ساخته‌اند.

برخی اوقات فروشندگان سوئیچ و هاب نیز بسته‌های نظارتی مخصوص به خود را ارائه می‌کنند. برای مثال، Olicom یک برنامهٔ کاربردی مدیر سوئیچ مبتنی بر ویندوز جمع‌وجور فراهم می‌آورد که آمار سوئیچ را جمع‌آوری می‌کند، مشکل را مخابره می‌کند و کارهای نظیر آن. چنین بسته‌هایی هنگامی که تنها ابزار موجود سوئیچ‌های مربوط به یک فروشنده باشند، کارآمد هستند اما اگر برای نظارت ۱۸ قطعه تجهیزات لازم باشد ۱۲ برنامه مختلف را اجرا نمایید، کاستی‌های این روش نمودار می‌شوند.

علاوه بر ابزار نظارتی فراهم‌آمده توسط فروشنده، ابزارهای نظارتی دسته سومی هستند که می‌توانند هر سرویس سرویس‌دهنده‌ای را که انتخاب می‌نمایید، تحت نظارت خود درآورد. این ابزارها به صورت زیر کار می‌کنند:

۱- فهرستی از شماره‌های IP و سرویس‌ها (شماره‌های سوکت) را که کاربر قصد نظارت آنها را دارد، دریافت می‌کند.

۲- هر از چندگاه، سعی می‌کند سرویس را بررسی کند (وارسی آن با استفاده از پروتکل مناسب).

۳- اگر چیزی درست کار نکند و پاسخ ندهد، هشداری را صادر می‌کند (از طریق پیجِر، پست الکترونیک و غیره).

این روش بسیار خوبی برای نظارت سرویس‌ها می‌باشد؛ ممکن است SNMP بتواند کار خود را انجام دهد اما در تحلیل نهایی، آنچه می‌خواهید بدانید آن است که سرویس‌تان کار می‌کند. چه اهمیتی دارد اگر SNMP فکر کند که سرویس‌دهنده وِب بالاست؟ در صورت عدم پاسخگویی آن به هنگام دسترسی از طریق یک ایستگاه شبکه‌ای آیا می‌توان صحت کارکرد سرویس‌دهنده وِب را تأیید نمود؟ بسته‌های نرم‌افزاری دسته سوم بسیاری در دسترس قرار دارند؛ برخی از آنها سوکت‌های TCP عمومی را بررسی می‌کنند و از «زنده و در حال شنودبودن» آنها خبر می‌دهند، در حالی که برخی برنامه‌های پیچیده هستند که برای نظارت بر برنامه‌های کاربردی ویژه نظیر پُست الکترونیکی یا پایگاههای اطلاعاتی شبکه‌ای مفید واقع می‌گردند.

مثالهایی از بسته‌های نرم‌افزاری نظارت بر سرویس در اینجا ذکر می‌شوند:

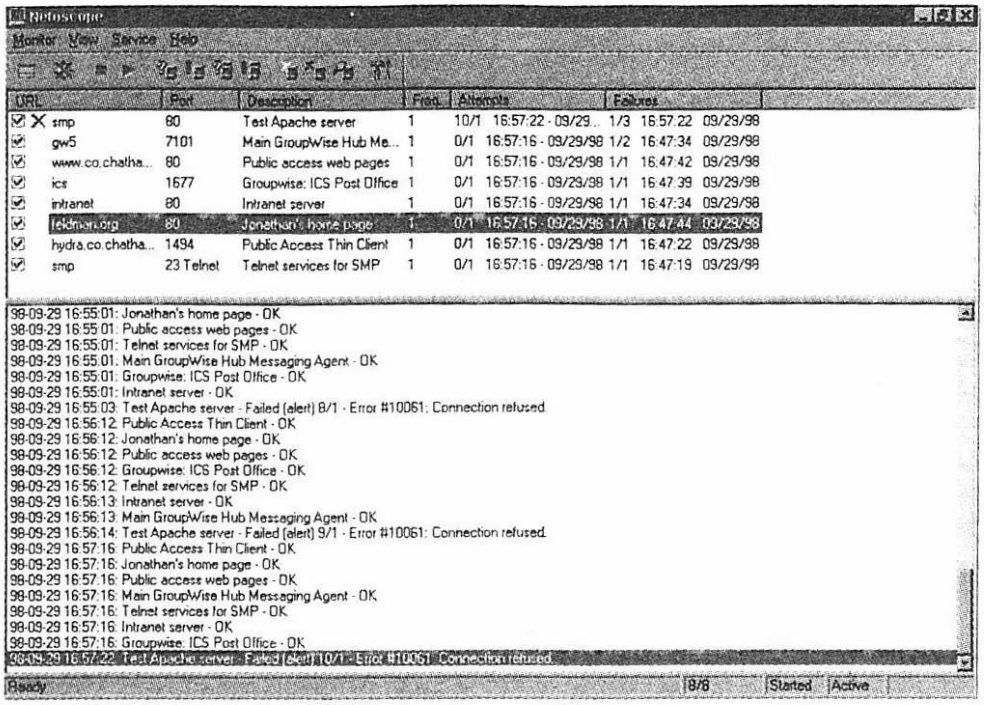
- Sitter (ftp://feldman.org/pub/sitter) یک اسکریپت Bash در لینوکس که پورت‌ها را با استفاده از تلهٔ Telnet وارسی می‌کند و هنگام پیداکردن مشکلات، آنها را به کنسول اعلام می‌کند. این ابزار باید برای سایت مورد نظر به صورت دستی مجدداً پیکربندی شود.
- Netoscope (http://www.basta.com) یک برنامه کمکی ویندوز برای وارسی قابلیت دسترسی سوکت‌ها از سرویس‌دهنده‌های مشخص‌شده. هنگام وقوع مشکلات هشدارهای سمعی صادر می‌کند یا برنامه‌ای را (نظیر پُست الکترونیکی) به اجرا درمی‌آورد.
- IPSentry (http://www.ipsentry.com) یک بسته نرم‌افزاری مدیریت سوکت که تحت ویندوز اجرا می‌شود. این برنامه آدرس‌های IP و سوکت‌های مورد نظر شما را مورد بررسی قرا می‌دهد. آن هم با تواتر مورد نظر شما. در صورت بروز مشکل نیز می‌تواند شما را آگاه کند.
- Whats Up و Whats Up Gold (http://www.ipswitch.com) این برنامه، ابزاری است گرافیکی با امکانات Paging. Whats Up Gold علاوه بر موارد مذکور دارای دسترسی وِب، امکانات SNMP و نظارت بر IPX نیز می‌باشد. نکته دیگر در مورد آن اینکه قیمت گرانی نسبت به ماهیت کاری خود داراست (حدود ۱۰۰۰ دلار در زمان نوشتن این جملات).

چه موقع از چنین ابزارهایی به جای مدیران SNMP استفاده می‌کنید؟ این بستگی به آن دارد که شما به چه چیزی نیاز داشته باشید. در تجربهٔ من، تنها مجموعه‌های بزرگتر از حد متوسط به استفاده از مدیران SNMP نیاز دارند؛ چرا که آنها گرانقیمت بوده، منابع زیادی مصرف می‌کنند و نصب و نگهداری آنها نیز پیچیده است.

البته مدیران SNMP اطلاعات زیادی را فراهم می‌آورند. به ویژه، آنها می‌توانند اطلاعات سرویسی فراهم آورند ـ یعنی نه تنها اعلام می‌کند که منبع «بالا» است بلکه سرعت پاسخگویی، تعداد بایت‌های باقیمانده از منابع و غیره را نیز اعلام می‌دارند. این اطلاعات، مدیران SNMP را هنگام بهینه‌سازی شبکه بسیار گرانقدر می‌سازند. مدیران SNMP برای نگهداری اطلاعات ردیابی طولانی مدت (خط پایه) از چگونگی وضعیت شبکه و منابع در یک روز عادی بسیار کارآمد می‌باشد. همان طور که در فصل ۲۳ ملاحظه خواهید نمود، خط پایه و ایجاد آن بخش مهمی از تشخیص مسأله است. بخصوص هنگامی که

صحبتی نظیر «شبکه کند است!» شنیده می‌شود. از همه اینها گذشته اگر ندانید که اوضاع هنگام مواقع عادی چگونه است، چطور می‌خواهید بگویید چیزی از گسترهٔ خود خارج شده است؟ نگهداری اطلاعات ثبت‌شده طولانی مدت مربوط به سرویس‌ها، روشی برای شناخت ـ و روشی برای نشان‌دادن به مافوق ـ این مسأله است که همه چیز به طرز کارا و مناسبی عمل خود را به انجام می‌رساند.

با این وجود، بسته‌های نرم‌افزاری سرکشی به شبکه می‌تواند به شکل خارق‌العاده‌ای مؤثر واقع شود. هزینهٔ صرف‌شده برای آنها نسبت به میانگین هزینهٔ صرف‌شده در نصب SNMP بسیار کمتر است و استفاده و پیکربندی آنها نیز بسیار آسان است. با اینکه موضوعات سرویسی در آنها پیاده‌سازی نشده است، این احتمال وجود دارد که در آیندهٔ نزدیک آنها بتوانند چنین اطلاعاتی را فراهم آورند. البته هیچگاه به سطح غنی اطلاعات فراهم‌آمده توسط SNMP دست نخواهید یافت، که البته ممکن است به آن نیازی نیز نداشته باشید. به طور خلاصه، هر بستهٔ سرکشی به شبکه برنامهٔ کاربردی تکایستگاهی است که می‌توانید با آن به راحتی سرویس‌های بسیاری را تحت نظارت درآورید. شکل ۳-۲۲ یکی دیگر از آنها را نشان می‌دهد.



شکل ۳-۲۲ : Netoscope از شرکت Basta همواره به سرکشی به شبکه می‌پردازد!

مراجع واقعی

مدیریت شبکه می‌تواند هزینهٔ بالایی داشته باشد. البته هنگامی که یک ایستگاه مدیریت شبکه نصب می‌کنید و شبکهٔ خود را برای انجام کار مدیریت پیکربندی می‌نمایید، این کار شما تلاشی است برای صرفه‌جویی در زمان و اجتناب از اتلاف آن ـ که هر دو در افزایش کارایی‌تان مؤثر می‌باشد.

با این وجود قبل از آنکه بیرون رفته و پول به سختی به‌دست‌آمده خود را خرج کنید، حتماً قبل از آن مراجع مختلفی را در مورد بسته‌های نرم‌افزاری مدیریت شبکه بررسی نمایید. علاوه بر آن سعی کنید مشاغلی را پیدا کنید که نظیر مجموعهٔ

کاری شما عمل می‌کند. می‌توانید از تجربهٔ آنها در مدیریت شبکه استفاده کنید. با این کار امکان دارد بتوانید از اشتباهاد گرانقیمتی اجتناب کنید. به این شکل، خواهید دانست که چه چیزی را باید از مدیریت شبکه خود انتظار داشته باشید.

خلاصه

«مدیریت شبکه» می‌تواند عبارتی اشتباه‌برانگیز باشد. این موضوع در سودمندترین شکل خود نظارت بر شبکه را دربر می‌گیرد که به شما اجازه می‌دهد. سلامت شبکه خود را ارزیابی نمایید.

SNMP (پروتکل سادهٔ مدیریت شبکه) در قلب خود راه حلهای پیچیده قرار دارد؛ بسیاری از فروشندگان، عـامل‌ها و MIB های نسبتاً کاملی را برای تجهیزات و نرم‌افزارهای خود ارائه می‌کنند که می‌توانند توسط ایستگاههای مدیریت SNMP خوانده شوند. ایستگاههای مدیریت SNMP به منظور نظارت طولانی مدت منابع واقعاً عالی هستند و می‌توانند در ایجاد خط پایه «شبکه» به شما کمک کنند.

عامل‌های SNMP قادر هستند تله‌هایی را در شبکه منتشر کنند که توسط ایستگاههای مدیریتی برداشته شده و روی آنها کار می‌شود. اغلب، آگاه‌سازی (نظیر فعال‌ساختن یک پیجِر) بهترین چیزی است که ایستگاههای مدیریتی می‌توانند «مدیریت» کنند. تله‌های SNMP ممکن است آزاردهنده و یا با اهمیت باشند. این موضوع به این بستگی دارد که نیمهٔ شب به خاطر جمع‌شدن کاغذ در چاپگر از خواب بیدار شوید و یا آنکه بدان وسیله از خرابی یک سیستم امنیتی عمومی آگاه گردید.

بسته‌های نظارت بر سوکت عمومی برای سرویس‌های TCP نیز در دسترس هستند و همچنین بسته‌های نظارتی ویژهٔ سرویس‌ها. بسته‌های عمومی از این جهت که اغلب تنها به شما می‌گویند که سرویسی فعال یا غـیرفعال است، مـحدود شده‌اند. اغلب آنها قادر نیستند اعلام کنند که یک سرویس تا چه حد منابع را مورد استفاده قرار داده و زمانهای پاسخگویی آن چه اندازه است.

برخی از برنامه‌های کمکی نظارتی ویژهٔ سرویس‌ها و یا ارائه‌شده توسط فروشندگان، نظیر برنامه‌های نظارتی که همراه سرویس‌دهنده‌ها، سوئیچ‌ها و مسیریاب‌های بخصوصی ارائه می‌شوند، اطلاعاتی نظیر SNMP، بدون سربار لازمه در SNMP ارائه می‌کنند. بسته به مقدار هزینه‌ای که روی رهیافت نـظارتی شـبکه، صـرف مـی‌کنید، بـهتر است قـبل از دست‌به‌کارشدن، مراجع مختلفی را بررسی نمایید. البته، با وجود آنکه رهیافت‌های نرم‌افزاری نظارتی سرکشی به شبکه اغلب آنقدر ارزان هستند که در صورت عدم انجام نیازهای شما به راحتی می‌توان آنها را کنار گذاشت، بهای راه حل کامل SNMP در حدی است که باید قبل از به‌کارگیری آن تحقیقات لازم را در مورد نحوهٔ به‌کارگیری و حتی بهتر، نتیجهٔ استفاده در مجموعهٔ مشابه مجموعهٔ شما، به عمل آورد.

کارگاه

پرسش و پاسخ

پرسش : چگونه باید عامل‌های SNMP خود را به منظور ارسال تله‌ها به ایستگاه مدیریت SNMP خود پیکربندی نماییم؟
پاسخ : شما نباید کاری انجام دهید. SNMP تله‌های خود را منتشر می‌کند که به ایستگاه مدیریتی شما می‌رسند.

پرسش : سه سرویس‌دهنده فایل و چاپ، یک سرویس‌دهنده اینترانت، ۴۰ ایستگاه‌کاری، یک دیوار آتش اینترنت، یک DMZ و یک سرویس‌دهنده وِب در خارج از مجموعه دارم. چه نوع نظارت شبکه‌ای برای من مناسب است؟

پاسخ : واژهٔ «نظارت» را بدون کلمه «پیش‌بینی» یا «منبع» به‌کار بردید بنابراین حدس می‌زنم تنها این موضوع برایتان اهمیت دارد که آیا تجهیزات فعال هستند یا نه و ایجاد خط پایه یا مدیریت منابع مد نظرات نیست. نظارت وِب به خوبی از طریق عمل سرکشی شبکه انجام می‌شود. پیشنهاد من آن است که هزینهٔ کوچکی را در به‌کارگیری راه حل نظارتی از نوع سرکشی صرف کنید و آنگاه در صورت عدم برآورده‌شدن نیازها راه حل SNMP را مورد بررسی قرار دهید. البته با توجه به اندازهٔ شبکه شما، حدس می‌زنم که همان راه حل اولیه برایتان کفایت کند.

آزمون

۱- هنگامی که شبکه‌ای را تحت نظارت قرار می‌دهید، معمولاً چه چیزی برایتان اهمیت دارد؟

الف ـ سطح کاربرد منابع　　ب ـ قابلیت دسترسی

ج ـ نه الف و ب　　د ـ هم الف و هم ب

۲- درست یا نادرست؟ بسته‌های نرم‌افزاری نظارتی سرکشی به شبکه، برخلاف رهیافت‌های SNMP، تصویری با جزئیات سطح کاربرد منبع و آمار تجهیزات را در اختیار می‌گذارد.

۳- تلهٔ SNMP چیست؟

الف ـ هنگامی که فروشنده‌ای پول زیادی بابت ارائه رهیافت SNMP از شما مطالبه می‌کند.

ب ـ یک پیغام انتشاری در شبکه به سوکتی مشخص، که توسط مشکلی روی عامل SNMP ایجاد می‌گردد.

ج ـ ارتباطی نقطه‌به‌نقطه بین دو ایستگاه مدیریتی

د ـ رویدادی که بعد از قطع برق سرویس‌دهنده به وقوع می‌پیوندد.

۴- RMON چیست؟

الف ـ SNMP MIB

ب ـ استانداردی برای انواع اطلاعاتی که هر پراب می‌تواند برای یک ایستگاه مدیریتی فراهم آورد.

ج ـ هم الف و هم ب　　د ـ نه الف و نه ب

۵- ایستگاه مدیریت SNMP خوب، برخلاف نرم‌افزارهای سرکشی سرویس، شما را قادر می‌سازند که چه کاری انجام دهید.

الف ـ انتشار　　ب ـ خط پایه

ج ـ تکبر و فخرفروشی　　د ـ هیچ یک از موارد فوق

۶- مزایای استفاده از نرم‌افزار سرکشی چیست؟

الف ـ ارزانی، نصب سریع، اجازه می‌دهد که بدانید چه موقع تجهیزات خراب یا غیرفعال شده‌اند.

ب ـ ارزانی، نصب آسان، اجازه می‌دهد که ایستگاههای پایانی را پیکربندی کنید.

ج ـ سازگار با SNMP، نصب سریع، شما را از خرابی یا غیرفعال‌شدن تجهیزات مطلع می‌سازد.

د ـ سازگار با SNMP، امکان ایجاد خط پایه و پیکربندی ایستگاههای پایانی

۷- درست یا نادرست؟ نرم‌افزار سرکشی، برخلاف رهیافت SNMP به تحقیقات و بررسیهای مرجعی گسترده قبل از خرید و به‌کارگیری نیاز ندارد.

پاسخ به سؤالات آزمون

۱- د
۲- نادرست (کاملاً برعکس است)
۳- ب (سوکت ۱۶۲ مربوط به UDP)
۴- ج
۵- ب
۶- الف
۷- درست

فصل ۲۳

شبکه کُند است! دریافت پاسخی صریح به سؤالی مبنایی

یکی از ناهنجارترین مشکلاتی که ممکن است با آن مواجه شوید «کُندی شبکه» است. بخصوص هنگامی که پشت میز خود نشسته‌اید و به راحتی از شبکه استفاده می‌کنید، باورکردن چنین گزارشهایی مشکل است و دست‌به‌کار شدن برای رفع آن کاری مشکلتر خواهد بود ـ نمی‌توانید چیزی را که به نظر نمی‌رسد خرابی دارد، تعمیر نمایید! با این وجود کاربری دارید که چنین شکواییه‌ای دارد، بنابراین وظیفهٔ شماست که این مشکل نامرئی را ردیابی نمایید.

ردیابی و محوسازی کُندی شبکه کاری مشکل اما جالب است. کلید یافتن علت کُندی کار شبکه، تقسیم مشکل به قطعات کوچکتر و قابل مدیریت‌تر می‌باشد؛ یعنی بعد از آنکه تمام چیزهایی را که با اتصال کاربر در تداخل است، تشخیص دادید، امکان بررسی هر قطعه به صورت مستقل و تعیین قطعهٔ مسبب کندی کاری آسانتر خواهد بود. دلیل اینکه کاربری در همان «شبکه» که کاربران دیگر بدون مشکل با شبکه کار می‌کنند، مشکل دارد؛ آن است که جلسه‌های شبکه‌ای ممکن است بسیار پیچیده باشند. ساده‌سازی امور شما را قادر می‌سازند که به شکلی سریع و کارآمد عیب‌یابی انجام دهید.

در ذیل دو نوع گزارش کُندی را ملاحظه می‌کنید:

- بلافاصله بعد از استفاده از برنامهٔ کاربردی یا سرویس‌دهنده‌ای جدید
- بعد از تغییر چیزی ناشناخته در شبکه، خرابیها یا اتمام منابع

در این فصل، تمرکز ما روی مورد دوم خواهد بود، به این دلیل که نوع اول اغلب بسیار آسان است. اگر چیزی جدید را در شبکه‌ای که نقصی ندارد به‌کار بندید و مشکل ایجاد شود، کاملاً مشخص است که منبع مشکل در کجاست. از آن گذشته، اگر در عیب‌یابی نوع دوم گزارشهای کُندی ماهر شوید، قادر خواهید بود با نوع اول نیز به خوبی دست‌وپنجه نرم کنید.

عوامل محدودکننده

وقتی افراد «کُندی شبکه» را گزارش می‌کنند، اغلب منظورشان «کُندی برنامهٔ کاربردی» است. از آنجا که هر برنامهٔ کاربردی، میوهٔ درخت شبکه محسوب می‌شود، اجازه دهید نگاهی سیستماتیک داشته باشیم به عوامل محدودکننده در هر شبکه:

- مقدار عرض‌باند در دسترس
- «تأخیر» مسیریابی و سوئیچینگ

- کارایی برنامه کاربردی
- عوامل مربوط به سرویس‌دهنده

اولین و مشخص‌ترین عامل در هر شبکه‌ای، سرعت شبکهٔ اشتراکی است که برنامهٔ کاربردی در آن زندگی می‌کند. واژهٔ به‌کاررفته برای این سرعت، «عرض‌باند در دسترس» می‌باشد که نوعی محدودهٔ سرعت در آزادراه به حساب می‌آید.

عرض‌باند و توان عملیاتی

عرض‌باند خام به تنهایی هیچ معنایی ندارد. همان طور که همیشه در محدوده سرعت مشخص‌شده در اتوبان رانندگی نمی‌کنید، برنامه‌های کاربردی شبکه نیز همیشه از عرض‌باند در دسترس استفاده نمی‌کنند. سرعت شما در اتوبان به مهارتهای رانندگی، عادات رانندگی و غیره بستگی دارد. به سرعتی که در عمل برنامه کاربردی شبکه‌ای با آن به رانندگی می‌پردازد، توان عملیاتی گفته می‌شود. توان عملیاتی هر جلسه از برنامه کاربردی را می‌توان از طریق اندازه‌گیری تعداد بایت‌هایی که در آن جلسهٔ شبکه‌ای در هر بسته گذاشته می‌شود و تقسیم این عدد بر تعداد ثانیه‌هایی که در آن جلسه تکمیل می‌گردد، به دست آورد. فرمول آن به شکل زیر است:

$$\text{توان عملیاتی برنامهٔ کاربردی در هر ثانیه} = \frac{\text{کل اطلاعات برنامهٔ کاربردی}}{\text{تعداد ثانیه‌های سپری‌شده}}$$

به خاطر داشته باشید که سرعت کلی شما در یک سفر شامل تمام مسیری است که در آن رانندگی کرده‌اید. برای مثال اگر نیمی از سفرتان را در یک اتوبان و نیمی دیگر را در جادهٔ خاکی که سوراخهای بزرگی در هر چند قدم به چند قدم آن وجود دارد رانندگی کرده باشید، زمان کلی رانندگی در آن جاده ممکن است دو یا سه برابر سفر در یک اتوبان به درازا انجامیده باشد. بر این اساس هنگام محاسبهٔ توان عملیاتی برنامهٔ کاربردی باید تمامی جهشهای طی‌شده توسط بسته‌های آن برنامه مد نظر قرار گیرند.

اجازه دهید پیوندهای شبکه‌ای پرکاربرد موجود و سرعتهایشان را مرور نماییم:

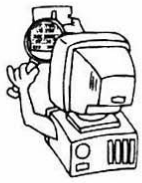
- اِترنِت ۱۰ یا ۱۰۰Mbps
- حلقه ـ نشانه ۱۶ یا ۱۰۰Mbps
- ISDN مخصوص مشتری با سرعت ۶۴ یا ۱۲۸Kbps
- ۹/۶Kbps (۹۶۰۰bps)، ۵۶Kbps یا ۱/۵Mbps (T1) برای خطوط استیجاری مرسوم

همان گونه که می‌توانید تصور کنید، هر بستهٔ برنامه کاربردی شما ممکن است نیمی از راه خود را با سرعت ۱۰۰ مایل در ساعت روی اتصال اِترنِت سریع طی کند اما آنگاه مجبور شود برای گذر از خط استیجاری T1 سرعت خود را تقریباً یک کیلومتر در هر ساعت کاهش دهد. اگر این بسته از طریق خط ۹/۶Kbps حرکت کند، سرعت معادل آن نظیر سفر با سرعت ۰/۰۱ کیلومتر در هر ساعت خواهد بود. وضعیت خط ۵۶Kbps اندکی بیشتر و در حدود $\frac{۱}{۱۲}$ کیلومتر در هر ساعت است.

تأخیر

اکنون فرض کنید که هر «جاده» که توسط بسته برنامه کاربردی مورد استفاده قرار می‌گیرد؛ در هر سر خود، یک باجهٔ عوارض داشته باشد. واضح است که در مورد مسیریاب یا سوئیچی صحبت می‌کنم که دو بخش شبکه را به هم پیوند می‌دهند. وقفهٔ حاصله، تأخیر آن ابزار نامیده می‌شود. اغلب اوقات می‌توان از تأخیر چشم‌پوشی کرد. اما نباید فراموش کنید

که هر ابزاری که در سر راه بسته قرار می‌گیرد وقفه‌ای در کار بسته است. برخی از مسیریاب‌ها و سوئیچ‌های سریع وقفهٔ قابل توجهی را ایجاد نمی‌نمایند (نظیر بعضی از باجه‌های عوارضی الکترونیکی جدید) اما این وضع در مورد سایرین صدق نمی‌کند. باید با آزمایش این موضوع را بیابید.



***نکته** : دو سال پیش در کلاسی خسته‌کننده حضور داشتم که استاد آن روشی سریع و آسان برای اندازه‌گیری تأخیر هر «باجهٔ عوارضی شبکه‌ای» آموزش داد. دو تحلیل‌گر شبکه را در هر طرف ابزاری که می‌خواهید ترافیک بین ایستگاه A و ایستگاه B تسخیر نمایید، آماده سازید. آنگاه از ایستگاه A، ایستگاه B را Ping کنید.*

زمان دقیقی که تحلیل‌گر برای خروج اولین ایستگاه (A1) مخابره می‌کند و آنگاه زمان رسیدن به دومین ایستگاه (B1) را ثبت نمایید. سپس، زمان دقیق پاسخ بستهٔ بازگشتی از ایستگاه دوم (B2) و آنگاه زمان بازگشت به ایستگاه اول (A2) را یادداشت کنید.

آنگاه می‌توانید محاسبه زیر را به انجام برسانید:

تأخیر = (A2-A1) - (B2-B1)/2

ایدهٔ نهفته در این تحلیل تأخیر، اندازه‌گیری تأخیر قبل از بارگذاری و آنگاه مشاهدهٔ تأخیر آن بعد از ایجاد ترافیک در آن است. بنابراین اگر ۵۰ تا ۱۰۰ میکروثانیه (۰/۰۰۰۵ تا ۰/۰۰۰۱ ثانیه) تأخیر در یک عصر اندازه‌گیری کنم، اما در طی روز ۳۰۰ میکروثانیه یا حتی ۸۰۰ میکروثانیه تأخیر داشته باشم، مشخصاً در ابزار خود با یک سربار مواجه هستم و باید آن را به عنوان مانع سرعتی مورد توجه قرار دهم.

سطر آخر آنکه: مسیری که توسط برنامه کاربردی مورد استفاده قرار می‌گیرد هنگام تعیین سرعت اجرای برنامهٔ کاربردی از اهمیت فوق‌العاده‌ای برخوردار است.

کارایی پروتکل و برنامه کاربردی

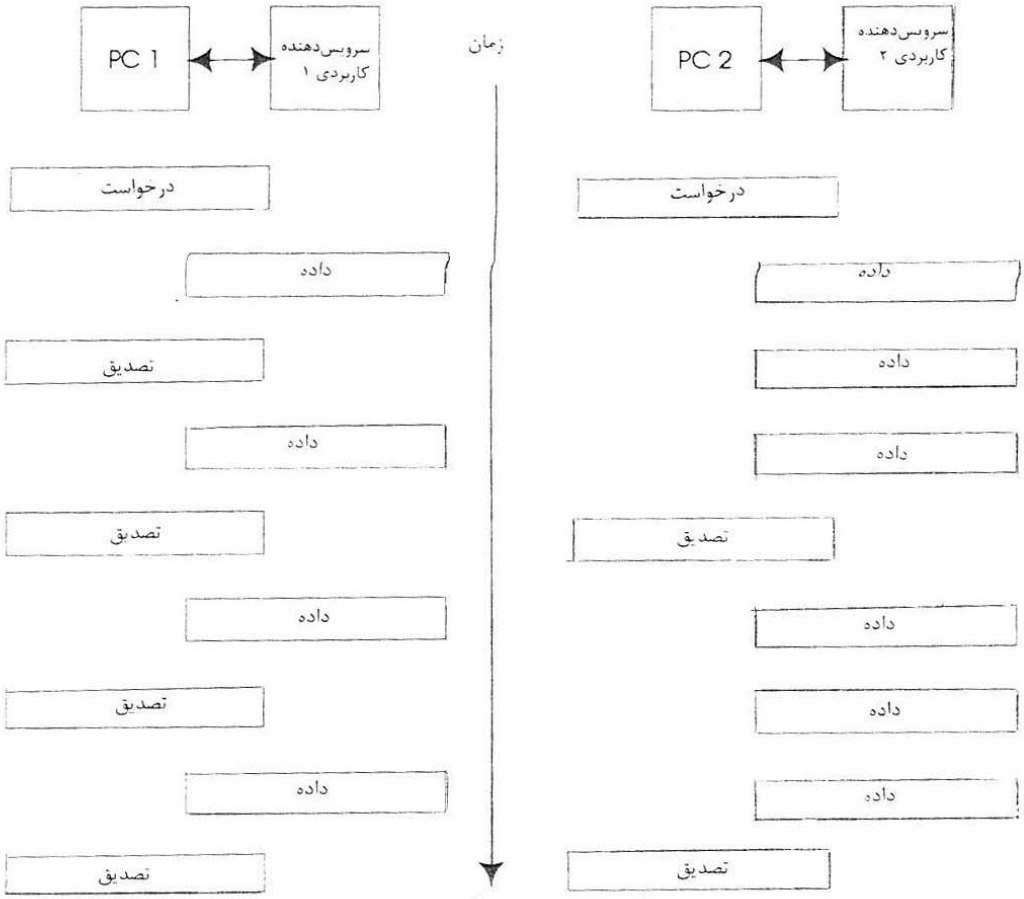
اجازه دهید مثال راننده‌ای را که هر چند دقیقه برای مشاهدهٔ منازل توقف می‌کند، مورد توجه قرار دهیم. این روش کارایی برای رانندگی نیست. اما بعضی افراد عملاً چنین کاری انجام می‌دهند. به گونهٔ مشابهی، برخی از برنامه‌های کاربردی از بعضی از امکانات کارآمد پروتکلی استفاده نمی‌کنند. پروتکل چه کاراییهایی می‌تواند در این زمینه ارائه نماید.

اجازه دهید نگاهی به مثالی یکپارچه داشته باشیم. «حالت انفجاری بسته» در ناوِل برای IPX/SPX، روشی است که با آن هر برنامهٔ کاربردی در یک سو می‌توانند از ایجاد تأثیر «پینگ‌پنگ» با ایستگاه پایانی جلوگیری کند. در شبکه‌های غیرقابل اطمینان، برخی اوقات لازم است برای هر بستهٔ منتقل‌شده، یک تصدیق برای عمل انتقال دریافت کنید.

اما در شبکه‌ای قابل اطمینان، این کار تنها باعث به وجود آمدن ترافیک غیرضروری می‌گردد. به شکل ۱-۲۳ نگاه کنید. ایستگاه‌کاری سمت راست تمام بسته‌های مورد نیاز خود را در طی ۶ انتقال دریافت می‌کند؛ ایستگاه کاری سمت چپ برای دریافت همان اطلاعات به تعداد بسیار بیشتری بسته نیاز دارد چرا که برنامه کاربردی موجود در آن بر دریافت تصدیق در مورد هر بسته پافشاری می‌کند. در حجم زیاد، این شکل از کار کاملاً نامناسب و غیرکاراست؛ حالت انفجاری ناوِل روشی برای اجتناب از این موضوع است. البته شبکه‌های قدیمی‌تر ناوِل که از سرویس‌گیرنده‌های قدیمی استفاده می‌نمایند قادر به بهره‌برداری از این مزیت نمی‌باشند.



نکته : *یک روش جدی برای ارتقاء سرعت شبکه‌های قدیمی ناوِل ـ بدون تغییر در سخت‌افزار. به‌کاربستن جدیدترین Client32 برای ایستگاههای کاری DOS یا ویندوز می‌باشد. باید مطمئن شوید که PBURST.NLM در سرویس‌دهنده 3.x تان بارگذاری شده باشد (چنین عملی در سرویس‌دهنده 4.x لازم نیست). از سرعت بسیار بیشتر شبکه خود به هیجان خواهید آمد.*



شکل ۱-۲۳ : ترافیک غیرضروری شبکه.

TCP/IP هم یک «حالت انفجاری» به نام پنجره‌های لغزشی دارد. چرا؟ به این دلیل که هنگام مرتب‌بودن شرایط، «پنجرهٔ» TCP (مقداری از اطلاعات که می‌توان با تصدیق‌گیری ارسال نمود) بزرگ است، اما با بدشدن شرایط این مقدار به منظور جبران خسارت به پایین می‌لغزد. با خوب‌شدن دوبارهٔ اوضاع، مجدداً به سمت بالا حرکت می‌کنم.

هنگام ارزیابی کارایی شبکه‌ای دو برنامه کاربردی مشابه، می‌توانید به سادگی یک عمل را دوبار انجام دهید، مقدار اطلاعات منتقل‌شده را اندازه‌گیری کنید و به توان عملیاتی هریک در هر ثانیه دست یابید. زمانی این کار را برای دو برنامه کاربردی سرویس‌گیرنده به انجام رساندم و به این نتیجه رسیدم که کارایی یکی چهاربرابر دیگری است!

کارایی برنامه کاربردی اغلب تغییر نمی‌کند مگر آنکه نحوهٔ طراحی برنامه باعث شود که رویدادهای خاصی سبب گردند که برنامه در آستانه‌های بخصوصی به گونه‌ای متفاوت کار کنند. (بیشتر از X شاخص؟ بیشتر از X کاربر؟)، که این می‌تواند باعث تغییر در کارایی گردد. متأسفانه، فرمولی در ارتباط با نحوهٔ مواجه‌شدن با این حالت وجود ندارد؛ باید از روی غریزه با آن برخورد کنید و آنگاه تئوری خود را بیازمایید.

محدودیت‌های سرویس‌دهنده

هر سرویس‌دهنده ممکن است با کمبود منابع روبه‌رو شود. بعد از تعیین آنکه در سرویس‌دهنده برنامه‌ای کاربردی به آهستگی به اجرا در می‌آید، بهتر است اقلام زیر را وارسی نمایید:

- سطح کاربرد CPU
- آمار انتظار CPU برای انجام I/O
- آمار معکوس‌سازی/ RAM در دسترس

مسلماً، هر پردازنده‌ای ممکن است با «فقدان سوخت» روبه‌رو شود. اما بیشتر اوقات، سطح کاربردی کمتر از ۱۰۰٪ را در مورد CPU را شاهد خواهید بود. حتی با وجود سیکل‌های CPU در دسترس فراوان، هنوز احساس کُندی و آهستگی می‌کنید. چرا؟ خلاصهٔ پاسخ این است: سرعت گردونه‌های دیسک سخت نسبت به حافظهٔ فیزیکی بسیار پایین است و آنها فاصلهٔ زیادی را برای رسیدن به سرعت حافظهٔ سریع باید بپیمایند. این مقایسه‌ها را مورد توجه قرار دهید:

- استفاده از حافظهٔ سریع مثل رسیدن به کابینت برای برداشتن یک قوطی کنسرو است.
- به‌کارگیری حافظهٔ معمولی نظیر قدم‌زدن به سوی آشپزخانه به منظور برداشتن یک قوطی کنسرو می‌باشد.
- استفاده از حافظهٔ مجازی (معکوس) نظیر آن است که سوار اتومبیل خود شده و برای خرید قوطی کنسرو به فروشگاه برویم.

آیا اوضاع تا این حد بد است؟ واقعیت بسیار نزدیک به مثال ذکر شده می‌باشد. حتی هنگام مشغول نبودن CPU، اگر برنامهٔ شما لازم باشد از حافظهٔ فیزیکی به حافظهٔ مجازی (دیسک سخت) رجوع کند، زمان زیادی طول می‌کشد که در نحوهٔ عملکرد و کارایی تأثیر خواهد داشت. چه مقدار معکوس‌سازی قابل قبول است؟ برای رسیدن به پاسخ این سؤال بهتر است به بخش «خط پایه» در ادامهٔ این فصل مراجعه نمایید.

نکتهٔ آخر آنکه، برنامهٔ کاربردی شما ممکن است بدون توجه به حافظهٔ فیزیکی موجود، دیسک‌گرا باشد ـ یعنی اصولاً پردازش زیادی با دیسک صورت دهد. برنامه‌های کارگاه اطلاعاتی در صورت اقامت در دیسک‌های بهینه‌سازی‌نشده از مشکلات کارایی رنج می‌برند و در این بین چگونگی شاخص‌بندی آنها مطرح نیست. این مشکل معمولاً مشکل «جدیدی» محسوب نمی‌شود ـ از اولین هنگام نصب برنامهٔ کاربردی با آن مواجه خواهید بود. البته اگر فایل‌های شاخص یا پایگاه داده تا نقطهٔ معینی رشد کنند، دربرگرفتن فضای دیسک بیشتر (و بنابراین افزایش زمان لازم برای بارگذاری) باعث پایین‌آمدن سطح کارایی خواهد شد. می‌توانیم دیسک‌گرابودن برنامهٔ خود را با بررسی آمار انتظار CPU برای I/O وارسی نماییم. اگر درصد زیادی در سطح کاربرد CPU مشاهده می‌کنید ممکن است مشکلاتی وجود داشته باشد.

دو بار اندازه‌گیری، یک بار برش

تنها روشی که می‌توان با آن از کمبود یا فقدان هر چیزی ـ عرض‌باند، منابع سرویس‌دهنده و نظایر آنها ـ اطلاع حاصل کرد، اندازه‌گیری می‌باشد. هر حالت دیگری به غیر از این کار، حدسی بیش نخواهد بود. ابتدا چه چیزی را اندازه‌گیری می‌کنید؟ این بستگی به تئوری‌تان دارد. به خاطر داشته باشید که هنگامی که شخصی به شما می‌گوید «شبکه کُند است»، اندازه‌گیری‌هایی را با استفاده از روشهای عیب‌یابی جعبهٔ سیاه به انجام خواهید رساند. کافی است تمامی قطعاتی که کل

اتصال را تشکیل می‌دهند مشخص نموده و آنگاه یکی یکی اقلام را کنار بگذارید تا به دلیل کُندی و آهستگی نزدیک شوید. اگر یک بخش محلی را برای لحظهٔ کنونی (سایر افراد این بخش مشکلی ندارند) و مسیر (سایر افرادی که از آن مسیر برای برنامه‌های کاربردی مختلف استفاده می‌کنند برای انجام کار مشکلی ندارند) ممکن است به سرویس‌دهنده ظنین شویم. اما اگر سرویس‌دهنده برای برنامه‌های کاربردی دیگر به خوبی کار کند، نمی‌دانید که چه اتفاقی در آن بخش شبکه رخ می‌دهد که باعث آزردگی کاربر می‌شود و اینجا زمانی است که باید اندازه‌گیری‌هایی را روی بخش مورد سؤال به عمل آورید.

چگونه اندازه‌گیری می‌کنید؟ بستگی دارد. در مورد کارهای نظارتی طولانی‌مدت، تحلیل‌گرهای شبکه‌ای توزیع‌شده یا پراب‌های مدیریتی بهترین انتخاب هستند؛ در تعیین و تشخیص یک مشکل کوتاه‌مدت، می‌توانید به تحلیل‌گر شبکه‌ای مستقل خود اطمینان کنید. مشکلات تناوبی تناسب بیشتری با پراب‌ها دارند و مشکلات پیشرونده را بهتر است با تحلیل‌گرهای منفرد اندازه‌گیری نمود.

سربار اشتراک

پس شما هم نجوای «اینترنت کُند است!» را شنیده‌اید. در واقع کاربران معتقدند اغلب اوقات این کُندی وجود دارد. با وجود آنکه کاربران موردنظر از اتصال T1 به ISP خود استفاده می‌کنند، می‌گویند مرورگرشان هنگام تماس با AOL یا CompuServe کُندتر عمل می‌نماید.

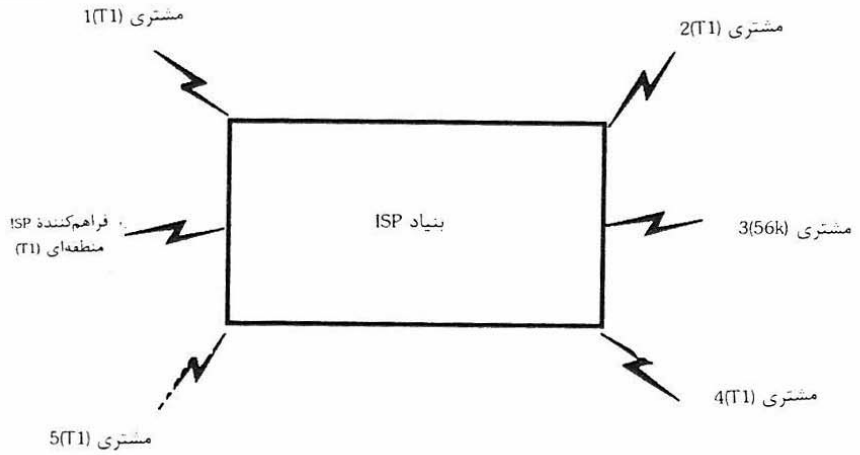
دو احتمال وجود دارد: یا کاربران و یا فراهم‌کنندهٔ سرویس مسئول کُندی هستند. می‌توانید با استفاده از اندازه‌گیری سطح کاربرد شبکه از DMZ احتمال مسئول‌بودن فراهم کننده را کنار بگذارید. همچنین، تحلیل‌گری را انتخاب می‌کنید که قادر است میزان سطح کاربرد عمومی شبکه در هر بخش آن و به‌خصوص توان عملیاتی مسیریاب ISP را ارائه نماید.

حدس بزنید چه اتفاقی می‌افتد؟ بیشترین توان عملیاتی که مشاهده می‌کنید که به مسیریاب ISP می‌رود از ۶۴ Kbps تا ۸۰ Kbps می‌باشد ـ که تناسبی با تعداد کاربران شبکه ندارد. از آنجا که تلاش کرده‌اید از طریق ایستگاه دیگر بسته‌های بیشتری را روی خط ارسال کنید (که تأثیری نداشته است)، از نتیجهٔ کار خود مطمئن هستید و می‌دانید که دلیل این مشکل مسیریاب یا فراهم‌کننده می‌باشد. خطایی در مسیریاب وجود ندارد؛ منابع آن به‌خوبی کار می‌کنند. از آن گذشته مسیریاب قادر است توان عملیاتی کامل T1 را به طور کامل در هر لحظه مدیریت کند. پس چه اتفاقی می‌افتد؟

پاسخ: جواب مسئله در سربار اشتراکی است، یک مشکل عمومی که متأسفانه بسیار در مورد ISP ها رخ می‌دهد. این مشکل هنگامی رخ می‌دهد که ISP بیش از ظرفیت خط انتقالی خود فروش کند، مثل وقتی که خطوط هوایی بلیط‌های بیشتری نسبت به ظرفیت موجود در پروازهای خود به فروش برساند. با فراتر رفتن میزان استفاده از ظرفیت، انباشتگی کاربران باعث تأخیر در کارها می‌شود. شکل ۲-۲۳، یک ISP را نشان می‌دهد که در آن خطوط واردشونده به آن از خطوط خارج‌شونده بیشتر هستند. طبیعی است که با تجمع ترافیکی روبه‌رو خواهد شد.

اتمام سوخت سرویس‌دهنده

فرض کنید که به این موضوع مظنون می‌شوید که سرویس‌دهنده به قدرتمندی آنچه که باید باشد، نیست. چگونه این موضوع را بررسی می‌کنید؟ اجازه دهید مثالی را مورد بررسی قرار دهیم که در آن کاربری به شما می‌گوید برنامهٔ کاربردی او ۱۰ مرتبه تُندتر از قبل به اجرا درمی‌آید. این موضوع زندگی وی را تحت‌تأثیر قرار داده است؛ او باید شب‌هنگام به محل کارش بیاید و قبل از آغاز روز جدید اجرا را به اتمام برساند. همچنین می‌گوید، «این شبکه روز به روز کُندتر و کُندتر می‌شود».



شکل ۲-۲۳: کاربران یک ISP که با سربار اشتراک روبه‌رو است، راه‌بندان‌های «ترافیکی» را تجربه خواهد کرد.

شما می‌دانید که برنامهٔ کاربردی موردنظر وی روی یکی از میزبانهای یونیکس اجرا می‌شود. این دانستن از آنجا ناشی شده که شما از وی خواسته‌اید کُندی کار را به شما نشان دهد. در غیر این صورت یک اختلاف یا اشتباه ارتباطی (بین شما و او) می‌تواند مسیر اشتباهی را پیش‌روی شما قرار دهد. همین که مشاهده نمودید که او یک جلسهٔ Telnet به میزبان یونیکس را باز کرد و وارد سیستم شد، حدس زدید که این برنامه باید روی یکی از میزبانهای یونیکس قرار داشته باشد. سایر کاربران میزبان یونیکس را بررسی کنید. آیا آنها هم مشکلاتی دارند؟ برخی از آنها موضوع را تأیید می‌کنند: «بله، کارها به مراتب کُند انجام می‌شوند». برخی دیگر چنین نیستند. با انجام این بررسی مشخص می‌شود که بیشتر افراد که مشکل دارند، آنهایی هستند که گزارش‌هایی را از سیستم دریافت می‌کنند. از آنجا که می‌دانید که پردازش گزارش‌ها در خود میزبان یونیکس به وقوع می‌پیوندد، طبیعی است که به میزبان یونیکس به‌عنوان متهم مظنون شویم. اگر در این مرحله به این موضوع شک داشته باشید که مشکل ممکن است شبکه‌ای باشد، ممکن است فایل بزرگی را از طریق انتقال FTP به این میزبان یونیکس منتقل نموده و زمان انجام کار را اندازه‌گیری کنید تا مشخص شود مشکل به شبکه ارتباطی ندارد. البته در اینجا این ظن وجود ندارد؛ چرا که، مشکل تنها در مورد کاربرانی است که گزارش‌هایی را از میزبان یونیکس دریافت می‌کنند و اصل پردازش‌ها در میزبان یونیکس صورت می‌پذیرد. تصمیم می‌گیرید که منابع میزبان یونیکس را تحت‌نظارت قرار دهید. انجام یک vmstat به نتیجه زیر می‌انجامد.

```
procs memory         page       faults   cpu
- - - - - - - - - - - - - - - - - - - - - -
r  b   avm    fre   re  pi  po  fr   sr   cy   in     sy    cs  us  sy  id  wa
0  0   16894  120   1   0   78  208  312  0    279    1208  94  5   19  54  22
0  0   17091  173   1   8   95  288  872  0    271    2730  180 13  34  33  20
4  1   17112  123   0   48  0   168  635  0    293    3751  386 20  51  0   29
6  1   17050  267   0   48  0   152  652  0    267    4124  359 24  44  0   32
```

ترسناک به نظر می‌رسد. این خروجی رمزگذاری‌شده چه معنایی دارد؟ (یادآوری): فصل هشتم توضیحات مربوط به عناوین این ستونها را ارائه داده است).

برای اهداف این بحث، نقاط مهم در ستون‌های fre، po و pi قرار دارند. آنچه که این خروجی در مرحلهٔ اول بیانگر آن است وجود حافظهٔ بسیار کم در فهرست آزاد و انجام عملیات ورود و خروج صفحه بسیار بالا می‌باشد.

به خاطر داشته باشید که عمل تعویض صفحه در مقایسه با حافظهٔ فیزیکی زمان بسیار بسیار طولانی‌تری را به خود اختصاص می‌دهد. انجام این مقدار فعالیت تغییر صفحه، کارها را کُند می‌نماید. برای این که کاملاً مطمئن شویم که مشکل را

یافته‌ایم، فعالیت تغییر صفحه را در پی اوقاتی که کاربران با کُندی مواجه می‌شوند، تحت‌نظارت قرار می‌دهید. به طور مشخصی همبستگی وجود دارد. توصیه می‌کنیم که حافظهٔ بیشتری به کار گرفته شود و بلافاصله بعد از نصب حافظهٔ بیشتر مشکل از بین می‌رود.



نکته : *فروشندگان دسته سوم مختلفی هستند که ابزارهای گزارش‌گیری از منابع سرویس‌دهنده با امکانات گرافیکی و گزارش‌گیری طولانی‌مدت ارائه می‌کنند؛ اگر با مشکلات طولانی‌مدت مواجه هستید ممکن است به‌کارگیری آن مفید واقع شود. نمایش‌گرافیکی منبع می‌تواند در ثبت اطلاعات مختلف به ویژه قبل از بروز مشکل کمک بزرگی باشد (برنامهٔ System Monitor میکروسافت نقطهٔ آغازین خوبی است اما از ابزار پیچیده‌تر و بهتر غفلت نکنید).*

خط پایه

همانطور که قبلاً در جاهای مختلف به این موضوع اشاره شده است، اگر ندانید که هنگام مرتب‌بودن اوضاع اقلام مختلف موجود در سیستم چه وضعیتی دارند، هنگام بروز مشکلات نخواهید توانست دنبال منبع بروز مشکل بگردید. بر این اساس، بسیار مفید است اگر با انجام تلاشی کم، تصویری از فراساختار شبکه‌ای خود ایجاد کنید که تعیین‌کنندهٔ وضعیت عادی چیزها در سیستم می‌باشد.

کلامی در مورد طول خط پایه: هر تصویر آماری خوب باید به همراه مثال کاملی ارائه شود تا بتوان با آن از صحت اطلاعات مطمئن شد. به بیان دیگر، مؤسسهٔ پزشکی آمریکا، مقادیر آزمایشگاهی «نرمال» از نمونهٔ جمعیتی بزرگی استفاده می‌کند تا بتواند مقادیر واقعی کلسترول، آهن، گلبولهای سفید خونی و غیره را به بهترین نحو اندازه‌گیری و تعیین نماید. اگر دکتر تشخیص دهد که خون شما در گستره‌های غیرطبیعی قرار دارد، با توجه به شرح‌حالی که از خود به وی ارائه نموده‌اید خواهد توانست علت غیرطبیعی بودن مقادیر مختلف در مورد شما را تحقیق و بررسی نماید.

همین موضوع نیز در مورد خط پایه صادق است. نمی‌توان انتظار داشت که نمونه‌ها را از شلوغ‌ترین اوقات سال برداشت نمود و به مقادیر طبیعی دست یافت. همچنین نمی‌توانید این کار را در مدت یک روز انجام دهید و انتظار داشته باشید که قابل تعمیم باشد. به جای این کار، باید حداقل یک هفته از سال را که در آن میزان کارها در حد معمولی قرار دارد به جمع‌آوری اطلاعات اختصاص دهید. می‌توانید اطلاعات جمع‌آوری شده را به شکل نمودارهایی برای هنگام مواجه‌شدن با مشکلات نگهداری نمایید. با انجام این کار و صورت‌دادن اندازه‌گیری‌های یکسان می‌توانید به راحتی آماری که با شماره‌ها و وضعیت خط پایه متفاوت هستند به راحتی تشخیص دهید. برای مثال، فرض کنید که سطح کاربرد شبکه در بخش شمارهٔ ۳ هیچ‌گاه از ۱۵٪ تجاوز نمی‌کند و نرخ خطا در آن در اوقات معمولی از ۲٪ بیشتر نیست. اگر متوجه شوید که سطح کاربرد به ۶۵٪ و نرخ خطا به ۱۲٪ رسیده است، بهتر است بخش مذکور را مورد بازبینی دقیق‌تر قرار دهید. این است جادوی خط پایه.

ایجاد خط پایه به صورت خودکار

اگر زیر ساختار RMON و SMNP داشته باشید، می‌توانید از آنها برای ایجاد خط پایه شبکهٔ خود استفاده نمایید. شرکتهایی نظیر NetScout و Kaspa می‌توانند در انجام این کار به شما کمک کنند. با اینکه تحقیقات و بررسی‌های اولیه

ممکن است کمی تند به نظر برسند ـ باید مطمئن شوید که هر یک از سرویس‌دهنده‌ها، مسیریاب‌ها، سوئیچ‌ها و برنامه‌های کاربردی دارای یک عامل SMNP می‌باشند، مضاف بر آن که باید ایستگاه مدیریتی موردنظر خود را نیز بررسی نمایید ـ این یک سرمایه‌گذاری اولیه است که خطوط پایه‌ای را برای مدت‌های مدید برایتان فراهم می‌سازد.

اگر نمی‌دانید که آیا به ایجاد خط پایه به صورت خودکار نیاز دارید، سعی کنید آمار مربوطه را به صورت دستی ایجاد کنید. تلاش زیادی را می‌برد که باید دو بار در هر سال صورت پذیرد. می‌توانید فرض کنید که مثل آن است که «مغازه را ببندید تا انبارگردانی صورت دهید» ـ کار زیادی است که انجام آن الزامی می‌باشد.

تلاش انجام کار به صورت دستی

دو نوع نظارت کارایی که به منظور تهیهٔ دستی خط پایه شبکه لازم است به اجرا برسند، عبارتند از: خطوط‌پایهٔ I/O و CPU و سطح کاربرد شبکه

چرا نامی از خطوط پایهٔ مسیریاب یا سوئیچ ذکر نشده است؟ متأسفانه این موضوع در مورد هر مسیریاب یا سوئیچی متفاوت است. از آن گذشته مکانیزم‌های جمع‌آوری اطلاعات یا به صورت شخصی و اختصاصی هستند و یا ـ همانطور که حدس زدید ـ بر اساس SNMP می‌باشد.

آمار سرویس‌دهنده

فرض کنید بگوییم شما یک سیستم یونیکس دارید که می‌خواهید از آن یک خط پایه تعرف کنید. روز دوشنبه sar (گزارشگر فعالیت سیستم)[1] را برای جمع‌آوری اطلاعات مربوط به کارایی هر روز آماده می‌سازید. در برخی از سیستم‌ها از قبل جمع‌آوری اطلاعات به صورت پیش‌گزیده فعال شده است. برای آنکه ببینید که می‌توانید گزارشی دریافت کنید، دستور زیر را تایپ کنید:

```
sar -A | more
```

اگر نمی‌توانید، این احتمال وجود دارد که جمع‌آوری داده فعال نشده باشد.



نکته : *می‌توانید در سیستم‌های یونیکس از طریق اجرای فرمان زیر جمع‌آوری اطلاعات sar را فعال کنید:*

sarenable

اگر این دستور کار نکرد، دستور زیر:

man sar

را اجرا کنید تا در جریان نحوه فعال‌سازی جمع‌آوری اطلاعات قرار بگیرید.

در پایان هر روز، ورودی دستور sar را در یک فایل متنی ذخیره کنید. آنگاه می‌توانید فایل متنی را به lotus 123، کواترو یا هر صفحهٔ گسترده‌ای که دوست دارید منتقل کنید. این کار را چند روز انجام دهید.

دو ایده در مورد کاری که می‌توان با این اطلاعات هر روزه انجام داد، وجود دارد. من شخصاً دوست دارم که کل هفته را به صورت مرتب و پشت‌سر هم بررسی کنم ـ به این دلیل که آنچه که روز جمعه اتفاق افتاده الزاماً روز سه‌شنبه تکرار

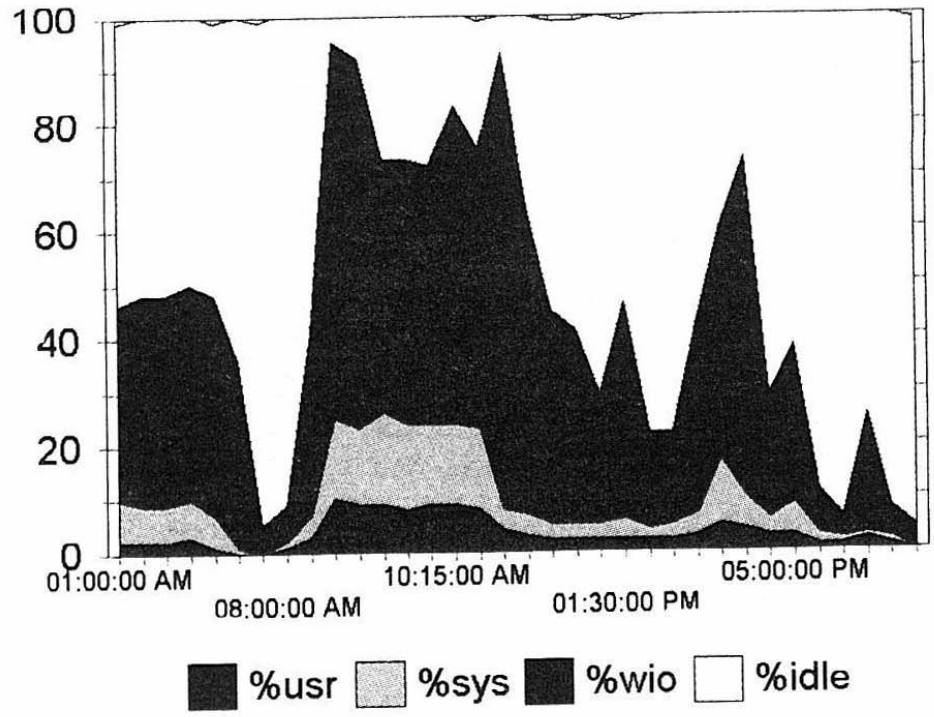
1- System Activity Reporter

نمی‌شود. البته برخی هم دوست دارند از اطلاعات هفته میانگین‌هایی تهیه کنند.

بهتر است گراف‌های زیر را به‌منظور تهیه مرجعی بصری تهیه نمایید:

- یک گراف میزان کاربرد CPU بر اساس درصد کاربری، درصد سیستمی و درصد انتظار برای I/O
- یک گراف تعویض صفحه
- گراف میزان کاربرد حافظه

از آنجا که برخی از پیاده‌سازی‌های sar متفاوت هستند. باید صفحهٔ راهنمای sar را برای درک عبارات مخفف به کار رفته در آمار مختلف، مطالعه نمایید. در تمامی گراف‌ها باید زمان در محور xها در نظر گرفته شود، بنابراین می‌توانید به راحتی نتیجهٔ گراف‌ها را با یکدیگر مقایسه کنید (به گراف نمونه نشان داده شده در شکل ۳-۲۳ توجه کنید).



شکل ۳-۲۳ : یک گزارش sar که به گراف کواتروپرو تبدیل شده است.

همانطور که در شکل ۳-۲۳ ملاحظه می‌کنید فعالیت کاربر (USR%)، فعالیت سیستم (SYS%)، فعالیت انتظار برای I/O (WIO%) و زمان بیکاری (IDLE%) همگی مجموع ۱۰۰٪ را به دست می‌دهند. با وجود آنکه قدرت پردازنده در این گراف رو به اتمام نگذاشته است، مشاهده می‌کنید که مشکلی در مورد WIO% وجود دارد: این حالت هنگام ترسیم نمودار مربوط به فعالیت تغییر صفحه بدیهی است؛ این فعالیت بسیار شبیه به منحنی WIO% می‌باشد. نظیر مثال قبلی vmstat احتمالاً مشکلی در حافظه یا معکوس‌سازی وجود دارد.



یادداشت : *هنگام جمع‌آوری آمار دستی از سایر سیستم‌های عامل، باید با نکته‌های زیر آشنا باشید:*

- *NetWare برای کار با منابعش به یک ایستگاه مدیریتی SNMP نیاز دارد؛ راهی برای استخراج منابع سرویس‌دهنده به صورت دستی وجود ندارد.*
- *قبلاً با قدرت System Monitor ویندوز آشنا شده‌اید. همچنین می‌توانید از Performance Monitor*

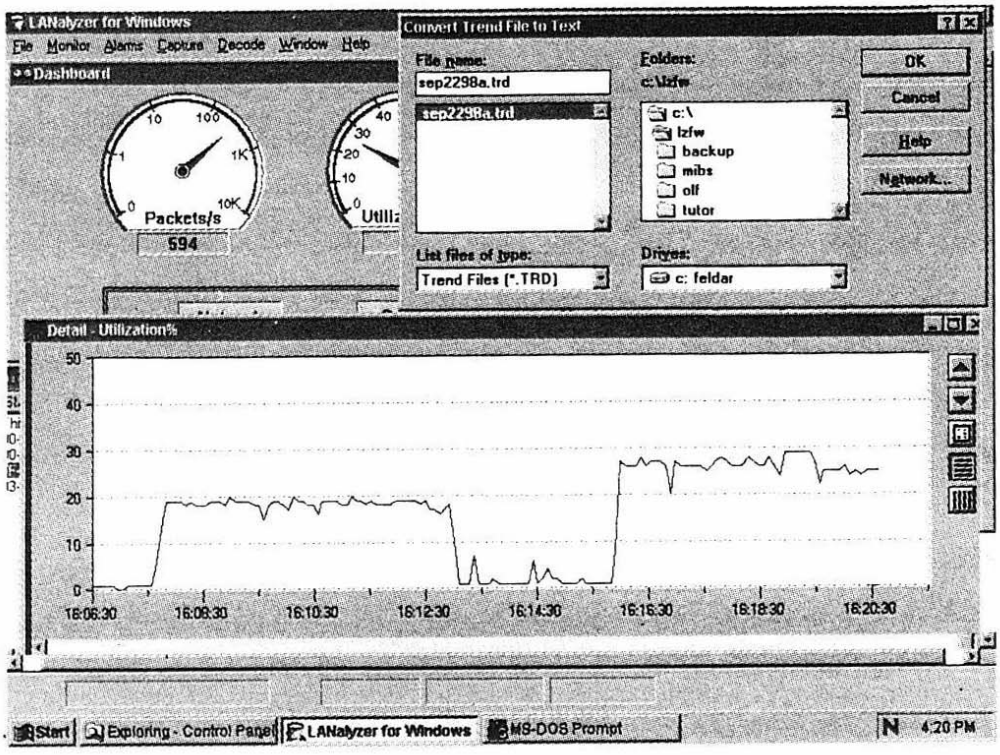
در NT (PERFMON.EXE) استفاده نمایید و گزارش‌ها را در قالب جداشده توسط کاما ذخیره کنید و آنگاه به راحتی گزارش‌ها را به یک صفحه گسترده منتقل نمایید.

بسته‌های تجاری مختلفی نیز به منظور ردیابی منابع سرویس‌دهنده‌ها در دسترس هستند؛ این برنامه‌ها نسبتاً ارزان‌قیمت بوده و می‌توانند به میزان زیادی کار شما را کم کنند. برای مثال، کاربران یونیکس می‌توانند از SarCheck محصولی از شرکت AURORA Softwell (www.sarcheck.com) استفاده نمایند. رهیافتی نظیر این می‌تواند سازشی بین ایجاد خط پایه منابع به صورت دستی و خرید راه‌حل SNMP کامل ایجاد نماید.

آمار شبکه‌ای

بهترین روش دستی برای جمع‌آوری آمار شبکه‌ای طولانی‌مدت، استفاده از تحلیل‌گر می‌باشد. اگر تعداد بخش‌های شبکه زیاد باشد، باید تحلیل‌گری با یک سیستم پراب مثل Obserever ، LANalyzer Agent یا Distributed Sniffer تهیه نمایید. برای اهداف موردنظر ما، وانمود می‌کنیم که تنها یک بخش داریم که مایلیم آمار آن را جمع‌آوری نماییم.

فرض کنید که در مجموعهٔ کاری من تنها تحلیل‌گر موجود، LANalyzer باشد. هر LANalyzer این امکان را فراهم می‌سازد که جزئیات اطلاعات را به یک فایل دیسکی منتقل کنیم و آنگاه آن را به درون هر صفحه گسترده‌ای که دوست دارید برده مورد استفاده قرار دهید. تمام کاری که من انجام می‌دهم، شروع استفاده از آن در دوشنبه و پایان‌دادن به آن در دوشنبه شب و ثبت اطلاعات ردیابی‌شده روی دیسک می‌باشد (شکل ۴-۲۳) آنگاه همین کارها را در روزهای سه‌شنبه، چهارشنبه، پنجشنبه و جمعه به انجام می‌رسانم.



شکل ۴-۲۳ : LANalyzer می‌تواند جزئیات اطلاعات موردنظر را نشان دهد.

با کمک LANalyzer، آمار اصلی و حیاتی مهمی نظیر موارد زیر را هر ۱۵ ثانیه یک بار نمونه‌برداری می‌کنند:

- تعداد بسته‌ها در هر ثانیه
- تعداد خطاها در هر ثانیه
- درصد سطح کاربرد شبکه
- تعداد کیلوبایت‌ها در هر ثانیه

مشخص است که مایلم نمودار تعداد کیلوبایت‌های به جریان درآمده در هر ثانیه را تقسیم نمایم ـ این به من اجازه می‌دهد که بتوانم نحوهٔ جریان اطلاعات در بزرگراه کوچکم تا چه اندازه سریع است. نمودار سطح کاربرد را نیز ترسیم می‌کنم با اینکه نتیجه حاصله بسیار شبیه منحنی مربوط به آمار کیلوبایت در ثانیه می‌باشد، اما داشتن آن ضرری ندارد و نشان‌دهندهٔ میزان باقی‌مانده از خط مورد استفاده می‌باشد. با ترسیم نمودار مربوط به خطاها، به خطی مسطح در پایین نمودار با تعداد محدودی لبه برخورد خواهید کرد.

کلام آخر در مورد خط پایه

بعد از انجام تکلیف ایجاد خط پایه، هنگامی که یکی از کاربران کُندی شبکه را گزارش می‌کند، مقایسه مقادیری که اکنون دریافت می‌کنید با آنچه که باید مطابق با گراف‌های پایه داشته باشند، کاری آسان است. این به شما اجازه می‌دهد که تعیین کنید کدامیک از آمارها خارج از محدودهٔ قبلی خود در شبکه قرار گرفته‌اند آنگاه می‌توانید به گونه‌ای مناسب عمل نمایید:

- آیا سطح کاربرد شبکه بسیار بالاست؟ ـ با استفاده از تحلیل‌گر دنبال «حراف‌ترین»ها بگردید و مسئله را حل کنید.
- آیا تعداد خطاهای شبکه بالاست؟ ـ با استفاده از تحلیل‌گر منبع تولیدکنندهٔ خطا را پیدا نموده و آن را از بین ببرید. همچنین بهتر است کابل‌ها را وارسی نمایید.
- عمل تعویض صفحه در سرویس‌دهنده زیاد صورت می‌گیرد؟ ـ تعداد کاربران یا برنامه‌های کاربردی روی سرویس‌دهنده را کاهش داده و یا حافظهٔ بیشتری را اضافه نمایید.
- سرویس‌دهنده برای انجام I/O مدت‌زمان زیادی منتظر می‌ماند؟ ـ حافظهٔ سریع دیسک را ارتقاء داده و یا دیسک سریعتر و با کارایی بالاتری تهیه نمایید.
- سطح کاربرد CPU در سرویس‌دهنده از حد معمول بسیار بیشتر است؟ ـ تعداد کاربران یا برنامه‌های کاربردی سرویس‌دهنده را کاهش دهید، CPU اضافه کنید یا اینکه سرویس‌دهنده را تعویض کنید.

خلاصه

با وجود آنکه عیب‌یابی مشکلات مربوط به کُندی و آهستگی، ممکن است هنری سیاه به نظر برسد، هنگامی که هر جلسهٔ شبکه‌ای را به بخش‌های مؤلفه‌ای‌اش در شمایی از نوع تفرقه بینداز و حکومت کن تجزیه می‌کنید، خیلی سریع مشخص می‌شود که کدام بخش گلوگاه بزرگراه اطلاعاتی می‌باشد.

سفر خانوادگی شما ممکن است بنا بر ترافیک بزرگراه یا ترافیک جاده زمان بیشتری از آنچه احتیاج دارید به طول بیانجامد. به طرز مشابهی، برنامهٔ کاربردیتان نیز ممکن است بنا به دلایل متعددی آهسته‌تر حرکت کند ـ که مهمترین این دلایل سطح کاربرد شبکه می‌باشد. دلایل دیگر عبارتند از کُندی کار سرویس‌دهنده، تأخیر سوئیچ یا مسیریاب، و مشکلات

کارایی در پروتکل یا برنامهٔ کاربردی.

ایجاد خط پایه برای شبکه، گام مهمی در ایجاد توانایی در تشخیص سریع آنکه کدامیک از این دلایل باعث بروز کُندی شده است می‌باشد؛ اگر ندانید که هنگامی که زندگی شیرین است پارامترهای سیستم چگونه هستند، مرجعی برای عیب‌یابی ندارید. با در دست داشتن خط پایه می‌توانید آمار فعلی را با آمار «نرمال» مقایسه کنید. همانطور که یک پزشک هنگام تجزیه و تحلیل نتیجهٔ آزمایش خون شما، آنها را با مقادیر معمول مقایسه می‌کند ـ و خیلی سریع عملیات لازم برای تعمیر را در پیش بگیرید. می‌توانید تهیهٔ خطوط پایه را به صورت دستی انجام داده و یا از اینکه از بسته‌های مدیریت SNMP که خط پایه را ایجاد خواهد نمود استفاده کنید. مسلم است که SNMP گزینهٔ بهتری است؛ گو اینکه به‌کارگیری آن مستلزم صرف هزینه‌های بالاتری می‌باشد.

کارگاه

پرسش و پاسخ

پرسش : از کدام تحلیل‌گرهای شبکه می‌توان برای ایجاد خط پایه یک بخش از شبکه به صورت دستی استفاده نمود؟
پاسخ : تقریباً تمامی تحلیل‌گرهای جدید. تکنیک دقیق مورد استفاده ممکن است متفاوت باشد، اما عملکرد اولیه جمع‌آوری آمار در مورد هر بخشی که تحلیل در آن انجام می‌گیرد یکی است. تحلیل‌گرهای مبتنی بر داس قدیمی ممکن است نتوانند آمار را در یک چارچوب زمانی ذخیره کنند. قبل از اقدام به خرید باید در مورد توانایی‌های تحلیل‌گر تحقیق به عمل آورید.

پرسش : در مورد آن روش تجزیه و تحلیل تأخیر: آیا لازم است که تحلیل‌گرها ساعت‌های همزمان شده داشته باشند؟
پاسخ : خیر. شما تفاوتهای زمانی موجود در هر دو sar را اندازه‌گیری می‌کنید. از آنجا که تفاوت بین این اختلاف‌های زمانی باید مساوی کل مقدار زمان صرف‌شده توسط بسته در سوئیچ یا مسیریاب در هر دو سو باشند، برای دستیابی به تأخیر در مورد سفر یکطرفه، عدد به دست آمده را بر ۲ تقسیم کنید.

آزمون

۱- یک برنامهٔ کاربردی حفاظت از ویروس را روی یکی از سرویس‌دهنده‌های خود نصب کنید. بلافاصله بمبارانی از شکوائیه‌ها مبنی بر اینکه شبکهٔ موردنظر کُند شده است دریافت می‌کنید. قدم بعدی‌تان چیست؟
الف ـ روی آن بخش از شبکه یک تحلیل‌گر شبکه را به اجرا درمی‌آورید.
ب ـ همه چیز را انکار می‌کنید.
ج ـ برنامهٔ کاربردی جدید را پاک می‌کنید. د ـ سرویس‌دهنده را خاموش می‌کنید.

۲- توان عملیاتی برنامهٔ کاربردی را می‌توان از طریق تقسیم‌کردن ------- بر ------- به دست آورید.
الف ـ تعداد ایستگاههای کاری، تعداد مسیریاب‌ها.
ب ـ تعداد بایت‌های انتقال‌شده، زمان سپری شده.
ج ـ تعداد بایت‌های منتقل‌شده، ایستگاههای کاری درگیر در ماجرا.
د ـ تعداد ایستگاههای کاری، زمان سپری شده.

۳- اِترنِت MDPS ۱۰ تقریباً ------- مرتبه سریعتر از خط استیجاری T1 می‌باشد.

الف ـ ۵ ب ـ ۲

ج - ۱ د ـ ۱۰۰

۴- بیشتر کُندی‌ها هنگامی رخ می‌دهند که -------- یا -------- توسط برنامهٔ کاربردی شبکه مورد استفاده قرار نگرفته باشند.

الف ـ انفجار بسته، پنجره‌های لغزشی ب ـ پنجره‌های بسته‌ای، انفجار لغزشی

ج - جداسازی‌پنجره‌ای، ضمیمه‌سازی انفجار د ـ انفجار پنجره‌ها، بسته‌های لغزشی

۵- کُندترین نوع حافظه در هر سرویس‌دهنده کدام است.

الف ـ حافظهٔ فراموش‌شده ب ـ حافظهٔ سریع

ج - حافظهٔ پویا د ـ حافظهٔ مجازی

۶- چه هنگام می‌گوییم برنامه‌ای «دیسک‌گرا» است؟

الف ـ هنگامی که فاکتور محدودکننده سرعت اجرایی دیسک است.

ب - هنگامی که برنامه با تسمه‌ای به دیسک سخت متصل شده است.

ج - هنگامی که دیسک با حداکثر سرعت خود در حال اجرا است.

د - هیچ یک از موارد فوق.

۷- چه هنگامی «سربار اشتراک» به وقوع می‌پیوندد.

الف ـ هنگامی که عرض‌باند ورودی به سرویس‌دهنده اینترنت از عرض‌باند خروجی بیشتر است.

ب - هنگامی که فراهم‌کننده بلیط‌های زیادی را می‌فروشد.

ج - هنگامی که شبکه به اشباع می‌رسد.

د - هنگامی که سایت‌های وِب متعددی توسط کاربران مورد استفاده قرار بگیرند.

۸- درست یا نادرست؟ می‌توانید حتی بدون داشتن خط پایه به راحتی بگویید آمار جاری از محدودهٔ خود خارج شده‌اند.

پاسخ به سؤالات آزمون

۱- ج ۲- ب

۳- ج ۴- الف

۵- د ۶- الف

۷- الف ۸- نادرست

فصل ۲۴

مهندسی معکوس شبکه

تبریکات مرا بپذیرید. اکنون آنقدر می‌دانید که بتوانید شبکهٔ مستندسازی نشدهٔ شخص دیگری را مهندسی معکوس کنید. بسیار مفتخر هستم!

حتماً توجه کرده‌اید که مستندسازی یکی از مقوله‌های اصلی این کتاب بوده است. و چرا نه؟ اگر در ناامیدی به این فصل رو آورده باشید، ممکن است قربانی شبکهٔ مستندنشدهٔ شخص دیگری باشید و می‌دانید که چقدر این کار می‌تواند بی‌نتیجه باشد. ناامید نباشید. اینجا جایی است که ما پیچیدگی‌های شبکهٔ مستندسازی نشده را روشن خواهیم ساخت و آن را به موجودی قابل اطمینان و قابل مدیریت تبدیل خواهیم نمود. این موضوع را با ادامهٔ مطالعهٔ فصل درخواهید یافت. مداد نوک‌تیزی بردارید و نفس عمیقی بکشید، می‌خواهیم قلمرویی مرزبندی‌نشده را روی کاغذ بیاوریم. ما کار خود را با ردیابی کابل‌های فیزیکی و آنگاه حرکت به سوی شبکه‌های TCP/IP و IPX/SPX آغاز خواهیم کرد. (چرا با NetEBUI کاری نداریم؟) به خاطر داشته باشید، NetBEUI یک پروتکل بسیار سادهٔ غیرقابل مسیریابی است ـ نمی‌تواند خیلی پیچیده باشد و ترسیم یک دیاگرام کابل‌کشی فیزیکی احیاناً کفایت خواهد نمود) فرض ما آن است که شما مالک یک شبکهٔ در حال کارکرد هستید؛ مهندسی معکوس شبکه‌ای که خراب شده است، بسیار سخت می‌باشد. بنابراین، بیایید عجله کنیم و قبل از خراب‌شدن آن را مستندسازی نماییم. شبکه بالا است و امروز روز مناسبی است.

ردیابی کابل

کابل بدون برچسب کابوس عیب‌یاب محسوب می‌شود. کابل درون دیوار جای می‌گیرد و بنابراین دانستن محلی که بدان می‌رود، مشکل است. خوشبختانه بیشتر سایت‌ها، تعداد مشخصی اتاقک الکتریکی دارند که تعداد محل‌هایی که لازم است جستجو نمایید را کاهش می‌دهد. یکی از ابزارهای لازم برای ردیابی (و برچسب‌زدن) کابل‌های بدون برچسب، که با بهایی کمتر از ۱۰۰ دلار قابل خریداری است، مولد صدای قیاسی و ردیاب صدای قیاسی می‌باشد (یکی از جاهایی که می‌توانید این ابزار را از آن تهیه نمایید Jensen Tools، www.jensentools.com، می‌باشد). تئوری موجود در استفاده از صدای قیاسی آن است که می‌توان از سیگنال قدرتمندی روی سیم ایجاد کند به طوری که ردیاب آن را «بشنود» ـ حتی بدون لمس‌کردن سیم. این به شما اجازه می‌دهد که خیلی سریع و به راحتی سیمی را از یک طرف تا سوی دیگر ردیابی نمایید.

نحوهٔ عملکرد زوج مولد/ردیاب بسیار آسان است. مراحل زیر را دنبال نمایید:

۱- پریز دیواری یا انتهای کابلی که می‌خواهید کار خود را از آن شروع کنید تعیین نمایید (به دلایلی که به زودی خواهید دید، من کار خود را با انتهای دورتر شروع می‌کنم).

۲- مولد صدا را به کابل قلاب کنید (مطمئن شوید که جهت سیم‌ها که به همراه آن ارائه می‌شود را رعایت کرده باشید).

آن را روشن نمایید.

۳- ردیاب صدا را برداشته و با انجام آزمونی سریع مطمئن شوید که همه چیز به درستی کار می‌کند: چند فوت در راستای سیم از مولد فاصله بگیرید و مطمئن شوید که می‌توانید صدا را بشنوید ـ به خاطر داشته باشید که برای شنیدن صدا نیازی به لمس کابل نیست. توجه کنید که صدا با حرکت شما به سوی کابل قوی‌تر می‌شود.

۴- ردیاب صدا را به سایتی که به نظر می‌رسد بیشتر کابل‌ها به آن «ختم می‌شوند» ببرید و ردیاب را نزدیک تمامی کابل‌ها تکان دهید. اگر صدایی می‌شنوید، در ناحیهٔ درستی قرار دارید. با بیشترشدن صدا، به کابل موردنظر نزدیکتر می‌شوید؛ با کمترشدن آن از کابل فاصله می‌گیرید.

۵- این کار را با اتاقک‌های مختلف، کابل‌ها و سایر مراکز دیگر انجام دهید تا کابل را پیدا کنید.

۶- روی آن برچسب بزنید.

اکنون می‌دانید که چرا مولد را در پایانه ایستگاه کاری قرار داده‌اید. به‌این ترتیب تعداد محل‌هایی که با ردیاب به آنها سرکشی خواهید نمود کاهش می‌یابد.

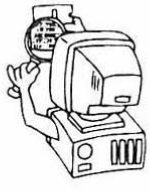
البته اگر سایت بسیار کوچکی دارید که تنها یک یا دو هاب در آن مورد استفاده قرار گرفته‌اند، همیشه می‌توانید از دوست خود بخواهید هنگامی که شما به هاب نگاه می‌کنید، کامپیوتر را خاموش کند. چراغ روی پورت هاب که بلافاصله خاموش می‌شود متعلق به آن PC است که خاموش گردیده است. اکنون می‌توانید به طرز مناسبی روی سیم برچسب بزنید. با این وجود صدایاب‌های قیاسی کاربردی جالب دارند که می‌توان مورد استفاده قرار داد.

کشف TCP/IP

اولین کار شما در کشف چگونگی طرح هر شبکهٔ TCP/IP آن است که «چسب» شبکه را مشخص کنید ـ مسیریاب‌ها! آسانترین راه برای کشف مسیریاب‌های شبکه آن است که به یکی از ایستگاههای کاری فعال رفته و پیکربندی TCP/IP را وارسی کنید. اگر در مورد داشتن بخش‌های چندگانه مطمئن نیستید باید به محل‌های مختلفی سرکشی کنید.

پیکربندی مسیریاب

آیا می‌توانید به مسیریاب Telnet کنید؟ عالی است. اوه نه! یک رمز عبور از شما می‌خواهد. خوشبختانه، چون شما صاحب این مسیریاب هستید رمز عبور آن را دارید (روی جلد یا پشت جلد راهنمای مربوطه را وارسی کنید؛ بعضی عادت دارند رمزعبور را در چنین محلهایی بنویسند) در غیراین صورت با پشتیبانی فنی سازنده تماس بگیرید. اگر سازنده کمکتان نکرد، ناامید نشوید. با وجود آنکه باید به منظور عیب‌یابی یا تغییر پیکربندی این مسیریاب، رمزعبور را داشته باشید، هنوز هم می‌توانید بدون آن به اکتشاف شبکهٔ خود بپردازید ـ فقط کافی است که کنجکاوی بیشتری نشان دهید.



نکته : *رمزهای عبور زیر را انتخاب کنید:*

- *manager*
- *security*
- *supervisor*

- *admin*
- *administrator*
- *root*
- *[ENTER]*
- *12345 (و گوناگونی‌هایی نظیر آن)*
- *اسم شرکت یا یکی از کلمات موجود در آن*

برایتان جالب خواهد بود بسیاری از افراد (به خصوص افرادی که شبکه‌هایی را که می‌سازند مستند نمی‌کنند) رمزهای عبور «پیش‌گزیده» را روی ابزار باقی می‌گذارند و یا از رمزهای عبور «نامناسب» استفاده می‌نمایند.

توانایی در Telnet کردن مسیریاب بدان معناست که می‌توانید گزارش وضعیت مربوط به تناظر رابطها و شماره‌های شبکه‌ای را ایجاد نمایید. آنها را یادداشت کنید! نمی‌دانید که چگونه آدرس‌های مسیریاب را نشان‌دهید؟ دفترچهٔ راهنمای آن را بررسی کنید.



نکته : *بسیاری مسیریاب‌ها از طریق تایپ‌کردن*

?

یا

help

دستورات موجود و قابل دسترس در خود را نمایان می‌سازند. اگر نمی‌توانید راهنمای مربوط به مسیریاب را پیدا کنید، قبل از خرید یک کپی دیگر سایت وِب سازنده را بررسی نمایید. برخی از سازندگان به عنوان سرویسی برای مشتریان دفترچه‌های راهنما را از طریق وِب عرضه می‌کنند.

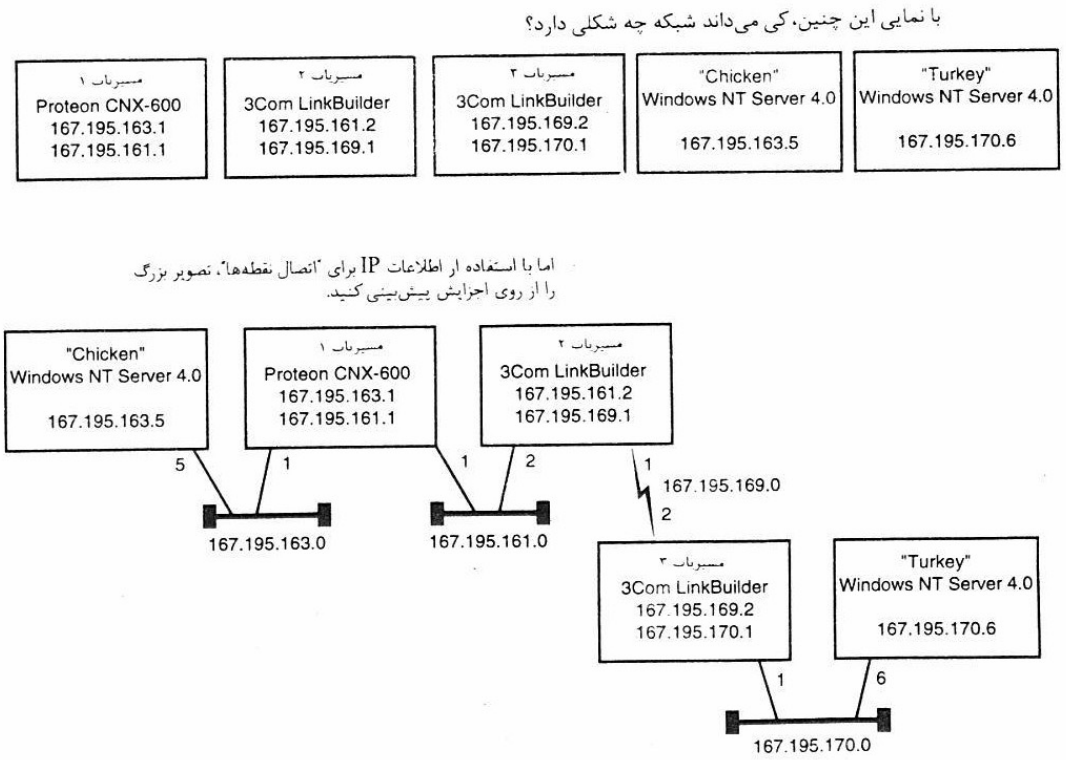
یک کار جالب و مهم دیگر که می‌توانید با مسیریاب انجام دهید، ملاحظهٔ جدول مسیریابی است. این بدان معناست که فهرست تمامی مسیرهای شناخته‌شده برای آن مسیریاب را ملاحظه خواهید نمود. تمامی مسیریاب‌هایی که به سازمان شما تعلق دارند در جدول مسیریابی ظاهر خواهند شد ـ حتماً فهرست شماره‌های شبکه‌ای (حتی اگر مسیریاب به آنها متصل نشده باشد) و جهش‌های بعدی آنها را یادداشت نمایید. جهش بعدی، مسیریابی است که چیز بیشتری در مورد آن شبکه می‌داند و این احتمال وجود دارد که تنها به فاصلهٔ یک یا دو جهش از شبکه قرار داشته باشد. این فرآیند را آنقدر تکرار کنید تا تمامی شناسه‌های مسیریاب‌های موجود در شبکه را یادداشت کرده باشید.



نکته : ***بنا به یک رسم بیشتر مسیریاب‌های یک بخش شبکه، شماره‌های گرهی پایینی دارند، که از یک شروع شده و به تعداد مسیریاب‌های موجود در آن بخش بالا می‌رود.***

بعد از شناسایی مسیریاب‌ها و شماره‌های IP آنان، باید بتوانید ترسیم یک نقشه را آغاز کنید. این کار را با مسیریاب شروع کنید. و بخشهای شبکه‌ای مربوط به هریک را ترسیم نمایید. و آنگاه «نقطه‌ها را به یکدیگر وصل نمایید». به این

صورت مشخص می‌شود که کدام مسیریاب‌ها شماره‌های شبکه‌ای عمومی را در اختیار دارند. بعد از ایجاد این همبستگی می‌توان آنها را به یکدیگر متصل نمود (شکل ۱-۲۴).



شکل ۱-۲۴: بعد از تعیین قطعات شبکه مثل بازی‌های جورچین، می‌توانید با استفاده از شماره‌های شبکه‌ای عمومی آنها را به یکدیگر متصل نمایید تا تصویری کلی ظاهر شود.

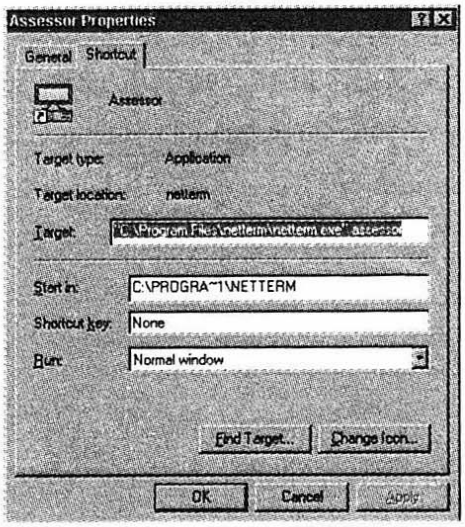
سرویس‌دهنده‌ها

اگر که می‌دانید اسامی سرویس‌دهنده‌ها چیستند، یک گام در جهت درست جلوتر هستید. در غیر این صورت، باید عملیات کشف اسامی را انجام دهید. از محل یک ایستگاه فعال، نگاهی به پیکربندی DNS بیندازید. پیکربندی DNS وجود ندارد؟ این ممکن است ـ برخی از سایت‌ها از DNS استفاده نمی‌کنند، اما احتمال آن در صورت استفاده از اینترنت بسیار کم می‌باشد. اگر مطمئن هستید که DNS ی وجود ندارد، دو گزینه برای جمع‌آوری اطلاعات مربوط به اسامی میزبان و آدرس‌های IP مربوط به سرویس‌دهنده‌ها پیش‌رو دارید:

- فایل C:\Windows\Hosts روی چندین ایستگاه کاری فعال را بررسی کنید.
- پیکربندی سرویس‌گیرنده مربوط به چندین ایستگاه کاری فعال را بررسی نمایید.

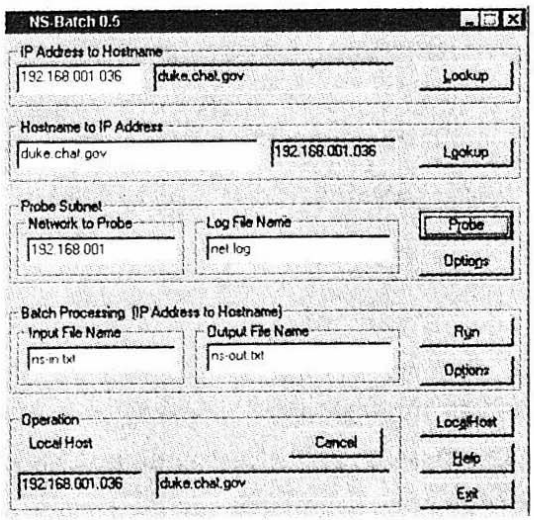
در مورد گزینهٔ دوم باید با سرویس‌گیرنده آشنا باشید. (برای مثال، سرویس‌گیرندهٔ Telnet). بسیاری از سرویس‌گیرنده‌های Telnet از شما می‌خواهند یک اسم میزبان یا آدرس IP در سطر فرمانی که برنامه را فراخوانی می‌کند قرار دهید، بنابراین باید خصوصیت‌های یک شمایل کاری برای انتخاب و برداشتن اسامی میزبان یا آدرس‌های IP وارسی نمایید. (شکل ۲-۲۴ را ملاحظه نمایید).

کاملاً محتمل است که کل مجموعه تنها با آدرس‌های IP کار کند. من خود این مطلب را آزموده‌ام.



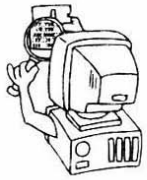
شکل ۲-۲۴ : شمایل "assessor" به برنامهٔ NetTerm اشاره می‌کند. اما به عنوان پارامتر سطر فرمان کلمهٔ assessor را فراهم می‌سازد.

اگر DNS در صحنه حاضر باشد همانطور که در فصل ۲۰ مشاهده کردید، معمولاً می‌توانید جدول اسامی را با استفاده از nslookup ملاحظه نمایید. به‌خاطر داشته باشید، nslookup برای ویندوز 9x کار نمی‌کند؛ بهتر است بـه دنـبال یکـی از معادل‌های آن باشیم. برخی از ابزار «اکتشاف شبکه» که در بخش بعدی فهرست شده‌اند نیز می‌توانند هر جدول اسمی را به نمایش بگذارند (شکل ۲-۲۴ را ببینید).



شکل ۳-۲۴ : از آنجا که nslookup برای کاربران ویندوز 9x فراهم نشده است، باید از یک برنامهٔ کمکی دسته سوم استفاده نمایید. NS-Batch یک روش برای مشاهدهٔ جدول DNS می‌باشد.

بعد از در دست‌داشتن اسامی سرویس‌دهنده یا آدرس‌های IP برای سرویس‌دهندهای مهم، آنها را به بخش‌های مناسب روی طرح ترسیم‌شده هنگام اکتشاف مسیریاب‌ها مـتصل کـنید. اگـر سـرویس‌دهنده‌ها در بـخشی هسـتند کـه آن را نمی‌شناسید، با انجام دستور "traceroute" به سرویس‌دهنده مسیر منتهی به آن بخش از شبکه را تعیین کنید. می‌توانید به هر جهش صورت پذیرفته Telnet کنید (به این دلیل که مشخصاً یک موجودیت مسیریاب در آن قرار گرفته است)، اطلاعات پیکربندی مسیر را جمع‌آوری نموده و در نقشهٔ خود منعکس سازید.



نکته : *بعضی افراد سرویس‌دهنده‌های نام خود را طوری پیکربندی می‌کنند که انجام نمایش اسامی از هر ایستگاه کاری دلخواه میسر نباشد. این کار از لحاظ امنیتی خوب است. اما در کار اکتشاف شبکه مشکل ایجاد می‌کند. بهتر است به سرویس‌دهندهٔ اولیه یا ثانویه وارد شده و فایل پیکربندی DNS را چاپ کنیم. در یونیکس، اغلب می‌توانید نگاهی به فایل /etc/namd/boot بیندازید:*

```
directory/usr/local/named
primary mycompany.com named.company
chache root.cache
forwarders 192.168.1.10
```

این فایل شما را به فایل‌های اطلاعاتی رهنمون می‌کند (در این حالت، این یک سرویس‌دهندهٔ اسم اولیه است؛ پایگاه داده‌ای قلمرو آن در فایل named.company قرار دارد. از آنجا که کلمهٔ کلیدی "directory" در فایل راه‌اندازی درج شده است، می‌توانید فایل اطلاعاتی را به جای فهرست etc/که پیش‌گزیده است، در /usr/local/named.company بیابید).

انجام خودکار برای افراد

چند ابزار اکتشاف شبکه در دسترس هستند که می‌توان آنها را مورد استفاده قرار داد. این ابزار بسیار مفیدند و قیمتی کمتر از ۱۰۰ دلار دارند. نحوهٔ کار آنها به همان شکلی است که من و شما انجام می‌دهیم: اجرای traceroute ها، انجام جستجوهای اسمی، بازکردن سوکت‌هایی در مقصد به منظور مشاهدهٔ وضعیت شنود آنها و نظایر آن. البته از آنجا که کامپیوتر قادر است با صبری بی‌همتا خسته‌کننده‌ترین و تکراری‌ترین کارها را به انجام برساند، ابزار کشف شبکه بسیار کاملتر از من و شما عمل می‌کند!

به ویژه، این ابزار خودکار اکتشاف شبکه، قادرند گستره‌ای از آدرس‌های IP را در نظر گرفته و پشت‌سرهم Ping کنند و همچنین بسیاری از پورت‌های سرویسی عمومی در هر مقصد را وارسی نمایند. در مورد یک شبکهٔ بزرگ این کار ممکن است دهها هزار بررسی را شامل شود (با فرض آنکه حدود ۲۰ سرویس در هر مقصد بررسی می‌شوند و ۲۵۴ شمارهٔ میزبان ممکن در هر شبکه و اینکه تلفیقی از چند شبکه داشته باشیم). از آن گذشته، اگر ابزار اکتشاف خودکار خود را شب‌هنگام ترک نمایید، صبح روز بعد بسیاری از پاسخ‌ها را بدون از دست‌دادن ذره‌ای خواب در اختیار خواهید داشت!

در مورد شماره‌های سوکتی اختصاصی برای سرویس‌هایی نظیر Lotus Notes یا Group Wise چطور؟ نگران آنها نباشید. بعد از تشخیص آنکه سرویس‌دهنده‌ای در آدرس IP معینی در حال اجراست، می‌توانید یک پویش پورتی کامل صورت دهید (شکل ۴-۲۴ را ملاحظه کنید).

قاعدهٔ کار چنین است: با وجود اینکه امکان دارد بتوان هر پورتی را در دنیا با استفاده از این ابزار پویش نمود، پویش یک پورت «سرویس‌دهنده» عمومی نظیر Telnet (۲۳)، SMTP (۲۵) یا NetBIOS (۱۳۹) روی تمامی آدرس‌ها و آنگاه انجام پویشی کامل‌تر روی ماشین بعد از پیداکردن سرویس‌های عمومی آن بهتر به‌نظر می‌رسد.

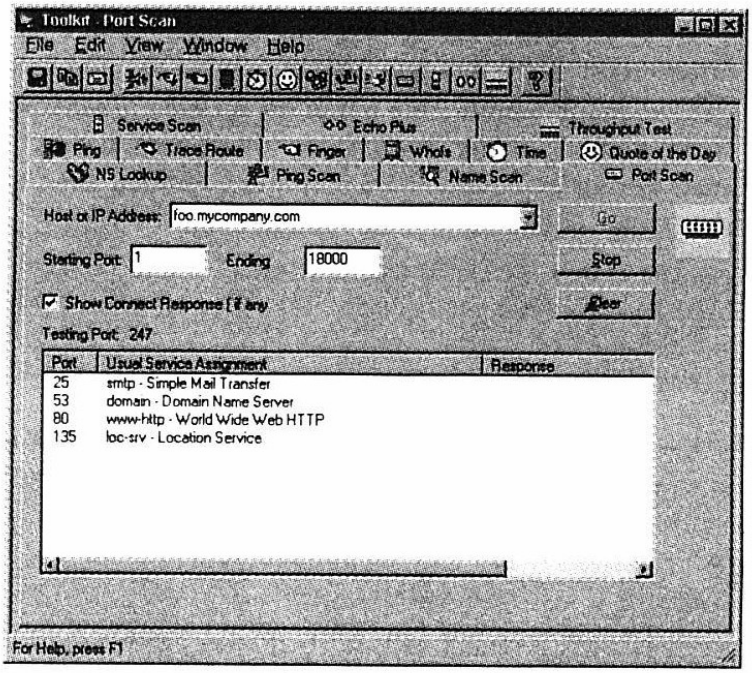
پویشگرهای SNMP برای اکتشاف شبکه بسیار خوب هستند. با وجود آنکه SNMP یکی از سرویس‌های UDP است و بنابراین نمی‌تواند «اتصالی» داشته باشد، برنامه‌ای که SNMP را «درک می‌کند»، می‌تواند داده‌گرام‌های SNMP را به گستره‌ای از آدرس‌های TCP/IP ارسال کند و طی گزارشی به شما بگوید کدامیک پاسخ می‌دهند. این موارد احتمالاً سرویس‌دهنده‌ها، مسیریاب‌ها، سوئیچ‌ها، یا هاب‌های «هوشمند» می‌باشند.

این قبیل ابزار را می‌توانید در سایت‌های زیر پیدا کنید:

- www.tnsoft.com
- www.solarwind.net

- www.tucows.com
- www.shareware.com

در مورد دو سایت آخر، دنبال "Network Tools" بگردید.



شکل ۴-۲۴: پویشگرهای پورت نظیر Internet Anywhere Toolkit می‌توانند پورت‌های «در حال شنود» را روی سرویس‌دهنده کشف کنند (از هزاران حالت ممکن).

مرور TCP/IP

اجازه دهید نقاط مهم و حساس مربوط به اکتشاف شبکهٔ TCP/IP را مرور نماییم. همیشه «فاکتورهای شناخته شده»ای در «شبکهٔ ناشناخته»تان دارید، مثل ایستگاههای کاری فعال و/یا سرویس‌دهنده‌هایی که می‌توانید به صورت فیزیکی به آنها مراجعه کنید. اطلاعات مربوط به این فاکتورهای شناخته‌شده را می‌توانید جمع‌آوری نموده و اسکلت شبکهٔ خود را قبل از ترسیم کلی آن به دست آورید. (اطلاعاتی نظیر آدرس‌های TCP/IP، آدرس‌های سرویس‌دهندهٔ نام، آدرس‌های مسیریاب و سرویس‌دهنده).

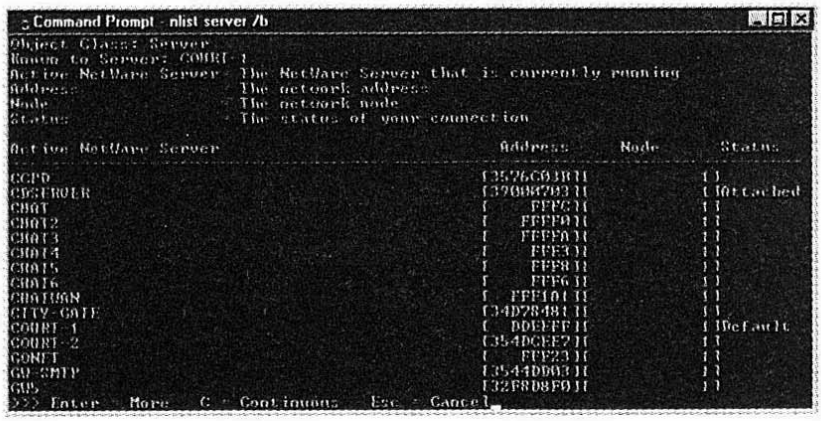
بعد از تعیین آدرس‌های مسیریاب‌های شبکه، می‌توانید از طریق Telnet کردن به آن مسیریاب‌ها و بررسی جداول مسیریابی، اطلاعات بیشتری را در مورد بخش‌های شبکه به دست آورید. می‌توانید با استفاده از جهش بعدی به‌عنوان سرنخی برای دستیابی به مسیریاب بعدی استفاده کنید و این فرآیند را تا هر زمانی که لازم باشد ادامه دهید.

اکتشاف شبکهٔ TCP/IP می‌تواند فرآیندی طولانی و خسته‌کننده باشد، به ویژه هنگامی که با تعداد زیادی از میزبانها سر و کار داشته باشیم؛ در این حالت، ابزارهای اکتشاف خودکار می‌تواند کمک بسیار بزرگی باشد.

اکتشاف IPX/SPX

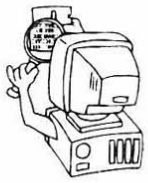
سرویس‌دهنده ناول خودشان را به شبکه اعلان و معرفی می‌کنند، بنابراین شناسایی آنان بسیار ساده است. برای نمایش اسامی تمامی سرویس‌دهنده‌های NetWare می‌توان از برنامهٔ کمکی NLIST استفاده نمایید. (شکل ۵-۲۴). اگر کاربر

NetWare3.x هستید می‌توانید به‌جای آن از برنامهٔ کمکی SLIST استفاده نمایید. این دو برنامهٔ کمکی آدرس‌های IPX داخلی سرویس‌دهنده‌ها را برای شما به نمایش درمی‌آورند ـ حتماً آنها را یادداشت کنید.



شکل ۵-۲۴ : می‌توانید با استفاده از فرمان nlist روی شبکهٔ NetWare دنبال سرویس‌دهنده‌ها بگردید. برای آنکه فقط سرویس‌دهنده‌های سازگار با بایندری ارائه شوند، می‌توانید از گزینهٔ /B استفاده نمایید.

بعد از آنکه به اسامی سرویس‌دهنده‌های IPX دسترسی پیدا کردید، می‌توانید با استفاده از برنامهٔ کمکی RCONSOLE (با فرض آنکه سرویس‌دهنده‌ها در مکانهای ناشناخته هستند) برای اتصال به سرویس‌دهنده‌ها استفاده نمایید. در اینجا هم مثل مسیریاب‌های TCP/IP باید رمز عبور را بدانید.



***نکته :** اگر رمز عبور RCONSOLE مربوط به سرویس‌دهنده‌های ناوِل خود را نمی‌دانید، هنوز می‌توانید در صورت داشتن مجوز خواندن فایل SYS:SYSTEM\AUTOEXEC.CNF می‌توانید وارد سیستم شوید. دنبال سطری بگردید که شبیه به این می‌باشد:*

load remote foobar

کلمهٔ آخر عبارت است از رمز عبور راه دور (در این حالت، "foobar") این احتمال وجود دارد که رمز عبور راه دور برای تمامی سرویس‌دهنده‌ها یکی باشد.
اگر نتوانید فایل مذکور را بخوانید اما به کنسول یکی از سرویس‌دهنده‌ها دسترسی داشته باشید می‌توانید دستور زیر را تایپ کنید:

LOAD EDIT AUTOEXEC.NCF

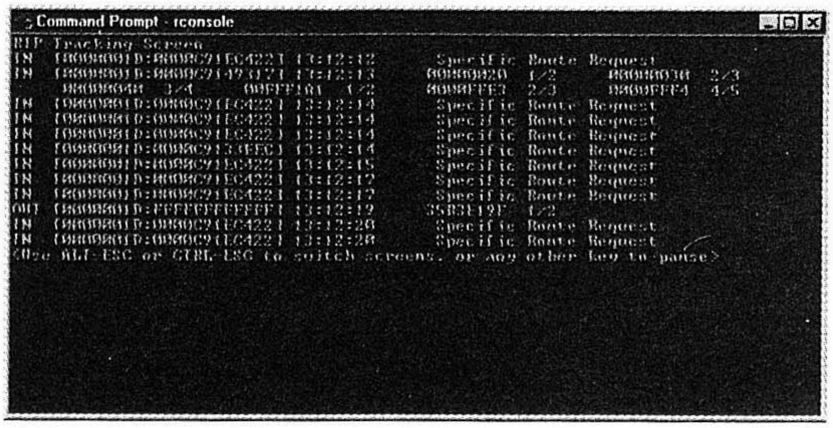
آنگاه قادر خواهید بود از آنجا فایل مذکور را بخوانید. (هنگام استفاده از کنسول، به عنوان سوپروایزر شبکه به فایل‌ها دسترسی دارید). محتمل است که این رمز عبور را بتوانید برای بقیهٔ سرویس‌دهنده‌ها نیز استفاده کنید.

بعد از دستیابی به کنسولی از راه‌دور می‌توانید در محل اعلان کنسول دستور CONFIG را اجرا کنید که آدرس‌های شبکه‌ای IPX که این سرویس‌دهنده به‌آنها متصل است را نشان می‌دهد. از آنها یادداشت بردارید. به خاطر داشته باشید که هر سرویس‌دهندهٔ NetWare چند خانه‌ای به عنوان مسیریاب نیز عمل می‌کند.

با یادداشت‌کردن آدرس شبکه‌ای و اسم سرویس‌دهنده، تصور خوبی از چگونگی شبکه به دست خواهید آورد. به خاطر داشته باشید سرویس‌دهنده‌هایی که دارای شمارهٔ شبکه‌ای مشترک هستند در یک شبکه اقامت دارند: سرویس‌دهنده‌ای که بین دو شبکه جای دارد به عنوان چسب آن دو شبکه عمل می‌کند. در نهایت دستور زیر را اجرا کنید تا مطمئن شوید برای هر شبکه مسیریابی را تعیین و ترسیم نموده‌اید:

```
display networks
```

اگر در دیاگرامتان جاهای خالی به چشم می‌خورد. برای مثال اگر می‌بینید که شماره‌های شبکه‌ای خاصی وجود دارند که سرویس‌دهنده‌ای به آنها متصل نیست ممکن است «فیلترهایی» برای مسیریابی وجود داشته باشند که جلوی دیدن سرویس‌دهنده‌ها یا مسیریاب‌های خاصی را گرفته‌اند. در این حالت بهتر است در محل اعلان کنسول نتیجهٔ دستور track on را وارسی نمایید. این کار باعث بازشدن پنجرهٔ ردیابی «مسیر» می‌شود. ظاهر آن کمی مبهم است اما بعد از آنکه به استفاده از آن عادت کردید، خواندن اطلاعات داده شده آسان خواهد بود (شکل ۶-۲۴).



شکل ۶-۲۴ : ردیابی درخواستهای مسیریابی از طریق صفحهٔ نمایشی مربوطه در NetWare.

اصولاً، دو نوع ورودی در این صفحه نشان داده می‌شود. ورودی IN و ورودی OUT. ورودی IN جایی است که سایر سرویس‌دهنده‌ها و مسیریاب‌ها به سرویس‌دهندهٔ جاری اعلام اطلاعات می‌کند. ورودی OUT جایی است که سرویس‌دهندهٔ شما به سایر سرویس‌دهنده‌های شبکه که به آنها متصل شده است اعلام موجودیت می‌کند. منظور نظر ما و تمرکز کار ما روی ورودی IN خواهد بود. ورودی IN شامل عددی است که در داخل براکت قرار گرفته است، برای مثال [0000001D:0000C91D5488] این شماره آدرس یک مسیریاب خارجی است. می‌توانید استفاده از این آدرس را در RCONSOL از طریق فشردن کلید Insert به جای انتخاب اسم سرویس‌دهنده، انتخاب نمایید. آنگاه می‌توانید آدرس شماره‌ای مذکور را وارد کرده و سعی کنید که اتصال برقرار شود. به این روش می‌توانید به سرویس‌دهنده‌ای که حتی در فهرست سرویس‌دهنده‌ها ظاهر نمی‌شود متصل شوید.

البته لازم نیست هیچیک از این کارها را در صورتی که می‌دانید سرویس‌دهنده‌ها کجا قرار گرفته‌اند انجام دهید. می‌توانید به راحتی با صرف چند ساعت وقت اطلاعات لازم را از محل کنسول هر یک از سرویس‌دهنده‌ها جمع‌آوری کرده و با در کنار یکدیگر قرار دادن این اطلاعات، نقشهٔ شبکه را تکمیل کنید. از آنجا که سرویس‌دهنده‌های ناوِل هم از TCP/IP استفاده می‌کنند، تکنیک‌های به کار گرفته شده در بخش قبل در اینجا نیز ممکن است به کار بیایند.

خلاصه

بعد از آنکه تکنولوژی به کار رفته در شبکه‌ای را شناسایی کردید، انجام مهندسی معکوس در مورد آن کار دشواری نیست. البته اگر تعداد زیادی کابل بدون برچسب دارید، استفاده از مجموعهٔ مولد صدای قیاسی امری ضروری به نظر می‌رسد.

از دیدگاه پروتکلی و شبکه‌ای، اگر سرویس‌دهنده‌ها بتوانند با یکدیگر و با ایستگاههای کاری صحبت کنند، همیشه ردپایی وجود دارد که می‌توانیم به تعقیب آن بپردازیم. اغلب اوقات بعد از تشخیص «چسب» شبکه که باعث همبستگی شبکه می‌شود، شناسایی بقیهٔ شبکه به تحقیقات کمتری نیاز دارد. اگر شبکه‌تان از نوع TCP/IP است، خوش‌شانس هستید. چرا که می‌توانید از ابزار اکتشاف خودکار استفاده نمایید.

مهندسی معکوس شبکه‌های ناوِل نسبتاً آسان است؛ تنها کافی است به کنسول‌های سرویس‌دهنده‌ها دسترسی داشته باشید. چه از راه دور و چه به صورت محلی. اگر در محیط شبکه‌ای خود از تلفیقی از TCP/IP و IPX/SPX استفاده می‌کنید، باید تکنیک‌های اکتشافی هر دو را مورد استفاده قرار دهید.

کارگاه

پرسش و پاسخ

پرسش : برخی از کارهای اکتشاف شبکه نظیر عملیات جاسوسی می‌ماند. آیا مطمئن هستید که باید چنین کارهایی صورت پذیرد؟

پاسخ : اگر شبکه‌ای که کار اکتشافی روی آن صورت می‌دهید شبکه‌ای است که مصونیت آن بر عهدهٔ شما نیست، پاسخ مشخصاً منفی می‌باشد. جمع‌آوری این‌گونه اطلاعات بدون داشتن مجوز کاری غیراجتماعی و حتی غیرقانونی محسوب می‌شود. البته اگر شما مسئول شبکه هستید باید این اطلاعات را بدانید. اگر ردپای کاغذی برای شما به جا نمانده باشد باید خود آن را ایجاد کنید. نظیر سینما، افراد خوب هم از همان ابزاری که افراد بد مورد استفاده قرار می‌دهند بهره می‌جویند - این تنها به این بستگی دارد که انگیزه‌ها و مسئولیت‌های شما چیستند.

پرسش : رهنمود دیگری برای اکتشاف در TCP/IP بدون استفاده از ابزار خودکار نداریم؟

پاسخ : البته، اما صرف ۱۵ دلار به تلف‌نشدن چندین ساعت از وقت شما نمی‌ارزد؟ استفاده از ابزار اکتشاف خودکار را قویاً توصیه می‌کنم. من خود ساعات متمادی از زندگی‌ام را صرف اکتشاف دستی شبکه‌ها نموده‌ام که در غیرآن صورت می‌توانستم صرف تفریح یا کاری خلاق بنمایم.

یکی دیگر از کارهایی که می‌توانید در صورتی که مسیریاب‌هایتان غیرقابل دسترسی هستند انجام دهید، بارگذاری مسیریابی میکروسافت برای تست‌کردن سرویس‌دهندهٔ NT می‌باشد که با توجه به اشتراکی که با پروتکل‌های مسیرهایی که با TCP/IP در شبکهٔ شما دارند می‌توان جدول مسیریابی را با استفاده از اجرای دستور زیر ملاحظه نمود:

```
NetStat -RN
```

می‌توانید کار مشابهی را روی جعبهٔ لینوکس انجام دهید؛ تنها کافی است بستهٔ «GATED» را به آن اضافه کنید، و با آن به RIP گوش فرادهید و ببینید که آیا چیزی آشکار می‌شود. انجام این کار در مقایسه با انتقال و خرید یک برنامهٔ ارزان‌قیمت ویندوز بسیار زیاد به نظر می‌رسد، اینطور نیست؟

آزمون

۱- بخش «مولد» زوج مولد/ردیاب صدای قیاسی باید کجا قرار داده شود؟

الف ـ در گوشه‌ای دور از جایی که بیشتر کابل‌ها به آنجا وصل می‌شوند.

ب ـ در انتهای متمرکزکننده که بیشتر کابل‌ها به آنها ختم می‌شوند.

ج ـ در وسط کابل.

د ـ هیچ‌یک از موارد فوق.

۲- اولین چیزی که هنگام انجام اکتشاف شبکه صورت می‌دهیم پیداکردن آدرس چه چیزی است؟

الف ـ سرویس‌دهنده

ب ـ سرویس فایل و چاپ ناوِل

ج ـ سرویس‌دهنده وِب

د ـ مسیریاب

۳- درست یا نادرست؟ بعد از کشف تمامی مسیریاب‌ها در شبکه، تطابق تمامی سرویس‌دهنده‌ها به جایی که به آن تعلق دارند کار ساده‌ای است.

۴- درست یا نادرست؟ تمامی شبکه‌های TCP/IP از DNS استفاده می‌کنند.

۵- نمی‌توانید سرویس‌دهندهٔ DNS مربوط به شبکه‌ای که می‌خواهید مهندسی معکوس را روی آن انجام دهید را بیابید. یک روش منطقی برای پیداکردن آدرس‌های میزبان آن است که ------- مربوط به یک PC فعال را وارسی نمایید.

الف ـ کارت شبکه

ب ـ ورودی مسیریاب

ج ـ پیکربندی برنامهٔ کاربردی سرویس‌گیرنده

د ـ جهش مقصد

۶- درست یا نادرست؟ تمامی پورت‌ها در هر آدرس IP شبکه باید مورد بررسی و جستجو قرار گیرند.

۷- رمز عبور RCONSOL برای سرویس‌دهندهٔ ناوِل در کجا قرار گرفته است؟

الف ـ SYS: SYSTEM\AUTOEXEC.NCF

ب ـ SYS: PUBLIC\AUTOEXEC.NCF

ج ـ SYS: SYSTEM\AUTOEXEC.BAT

د ـ SYS: SYSTEM\AUTOEXEC.BAT

پاسخ به سؤالات آزمون

۱- الف

۲- د

۳- درست

۴- نادرست

۵- ج

۶- نادرست. ابتدا باید تمامی آدرس‌های IP ممکن برای پورت‌های عمومی را پویش کنید و آنگاه دنبال سایر احتمالات بگردید.

۷- الف