



دانشگاه تربیت مدرس شهید رجایی

اصول مهندسی شبکه های کامپیوتری
(جلد دوم)

مؤلف:

فرامرز گیوه کی
مدرس دانشگاه تربیت مدرس شهید رجایی

سرشناسه	: گیوه کی ، فرامرز
عنوان و نام پدیدآور	: اصول مهندسی شبکه های کامپیوتری / مولف فرامرز گیوه کی.
مشخصات نشر	: تهران: دانشگاه تربیت دبیر شهید رجایی ، ۱۳۸۸.
مشخصات ظاهری	: ۲ج. : مصور ، جدول ، نمودار .
فروست	: سری کتابهای آموزشی به روش چند رسانه ای .
شابک	: دوره: ۲-۳۸-۲۶۵۱-۹۶۴-۹۷۸ج؛ ۹-۳۹-۲۶۵۱-۹۶۴-۹۷۸ج؛ ۲-۴۱-۲۶۵۱-۹۶۴-۹۷۸
وضعیت فهرست نویسی	: فیبا
موضوع	: شبکه های کامپیوتری.
موضوع	: آدرس دهی IP - پروتکل DNS.
موضوع	: پیکربندی دستگاه های شبکه ای.
موضوع	: پروتکل های SLIP و PPP - آزمایشگاه شبکه.
موضوع	: شبکه های بدون کابل - امنیت - چند رسانه ای .
موضوع	: سیستم تلفن - پروکسی.
شناسه افزوده	: دانشگاه تربیت دبیر شهید رجایی
رده بندی کنگره	: ۱۳۸۸ الف ۹/۵/TK۵۱۰۵
رده بندی دیویی	: ۰۰۴/۶۵
شماره کتابشناسی ملی	: ۱۷۹۵۴۱۴

عنوان کتاب : اصول مهندسی شبکه های کامپیوتری (جلد اول)

مولف : فرامرز گیوه کی

ویراستار : فرانک علی آبادی

چاپ و صحافی : دانشگاه تربیت دبیر شهید رجایی.

نوبت چاپ : اول

تاریخ انتشار : تابستان ۸۸

تیراژ : ۱۰۰۰

قیمت : ۳۹۰۰ تومان

شابک : دوره: ۲-۳۸-۲۶۵۱-۹۶۴-۹۷۸ج؛ ۹-۳۹-۲۶۵۱-۹۶۴-۹۷۸ج؛ ۲-۴۱-۲۶۵۱-۹۶۴-۹۷۸ ISDN:

آدرس : تهران: لویزان، خیابان شهید شعبانلو، دانشگاه تربیت دبیر شهید رجایی

تلفن : ۲۲۹۷۰۰۰۱ شماره پست تصویری(فاکس) : ۲۲۹۷۰۰۰۳

این کتاب طبق سر فصل های مصوب درس " اصول شبکه کامپیوتری " تدوین گردیده است.

کلیه حقوق این اثر برای مؤلف و دانشگاه تربیت دبیر شهید رجایی محفوظ است.

نشانی: تهران، لویزان - کد پستی ۱۶۷۸۸ - صندوق پستی ۱۶۳ - ۱۶۷۸۵ - تلفن: ۲۲۹۷۰۰۶۰ - ۹

نمبر: ۲۲۹۷۰۰۰۳ پست الکترونیکی: sru@srutu.edu

پیشگفتار مولف

حمد و سپاس ایزد منان را که با الطاف بیکران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی به ویژه علوم کامپیوتر و انفورماتیک گام هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم موثر واقع شویم، گستردگی علوم و توسعه روزافزون آن ، شرایطی را بوجود آورده که هر روز شاهد تحولات اساسی و چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی ترین و راحت ترین راه دستیابی به اطلاعات و اطلاع رسانی ، بیش از پیش روشن می نماید .

امید است مطالب این کتاب ، که حاصل چندین سال مطالعه و تدریس درس اصول شبکه های کامپیوتری است و به منظور استفاده ی دانش پژوهان و علاقه مندان به دانش شبکه های کامپیوتری تالیف شد است ، این کتاب مفید باشد . مولف کتاب آماده دریافت نظرات اصلاحی و پیشنهادهای ارزشمند شما ، از طریق نشانی الکترونیکی f-givkey@srtnu.edu است.

فرامرز گیوه کی

سایر آثار مولف

۱. با اینترنت بر فراز دهکده جهانی
۲. مبانی کامپیوتر
۳. مبانی سخت افزار کامپیوتر
۴. اصول مهندسی اینترنت
۵. تجارت الکترونیکی
۶. مبانی محیط های چندرسانه ای و گرافیک رایانه ای

صفحه	تیترا
	بخش یک: اصول مقدماتی شبکه
۲	تعریف شبکه
۴	تقسیم بندی شبکه ها
۸	انواع توپولوژی
۱۶	شبکه های LAN
۱۷	شبکه های MAN
۱۸	شبکه های WAN
۱۹	پیاده سازی های رایج LAN
۲۰	طراحی WAN
۲۴	خطوط انتقال
۲۵	کابل UTP
۲۷	کابل کواکسیال
۳۰	فیبر نوری
۴۱	بلوتوث
۴۳	مبانی شبکه
۴۶	انواع ارتباط میان دو ایستگاه
۴۶	پروتکل OSI
۴۸	لایه های پروتکل OSI
۴۸	لایه یک (Physical)
۴۹	لایه های ارتباط داده ای Data link
۵۲	لایه سه شبکه (Network)
۵۸	لایه انتقال یا Transport
۵۹	سرویس های پایه لایه انتقال
۶۲	لایه پنجم نشست یا session
۶۵	استانداردهای لایه جلسه
۶۶	لایه ششم ارائه یا presentation
۶۷	لایه هفتم کاربرد یا Application
۶۸	پروتکل های پشته ای TCP/IP
۷۱	اجزای پروتکل TCP/IP
۷۴	نحوه مبادله داده بین دو کامپیوتر

۷۹	حداکثر نرخ داده در یک کانال - پهنای باند
۷۹	مالتی پلکس یا تسهیم
۸۰	استانداردهای انتقال روی خطوط نقطه به نقطه
۸۳	اجزای یک شبکه مخابراتی - <i>DTE</i>
۸۶	استانداردها و پروتکل ها - استاندارد و شبکه های عمومی
۸۶	شبکه های <i>ATM</i>
۸۸	پروتکل <i>ATM</i>
	بخش دوم: آدرس دهی <i>IP</i>
۹۲	مدل آدرس دهی <i>IP</i>
۹۳	شبکه (<i>Net</i>) و میزبان (<i>Host</i>)
۹۳	پنج کلاس متفاوت <i>IP</i> به همراه برخی آدرس های خاص
۹۷	<i>IP6</i> نسخه شش
۱۰۰	الگوی زیر شبکه <i>Subnet Mask</i>
۱۰۲	پروتکل <i>IP</i>
۱۰۳	کاربرد دیگر <i>IP Address</i>
۱۰۴	<i>IP</i> های خاص:
۱۰۸	<i>Host Name Resolution</i>
۱۰۹	<i>Domain Name</i>
۱۱۱	تبدیل <i>Host Name</i> به <i>IP</i> با استفاده از <i>DNS Server</i>
۱۱۲	مراحل تبدیل <i>Host Name</i> به آدرس <i>IP</i>
۱۱۲	مروری بر پروتکل <i>TCP</i>
۱۱۲	چند نکته مهم در مورد این پروتکل
۱۱۴	ساختار <i>header</i> در <i>TCP</i>
۱۱۵	<i>TCP Header Length</i>
۱۱۹	روش دست تکانی سه مرحله ای
۱۲۱	روند خاتمه ارتباط <i>TCP</i>
۱۲۴	بهترین راه تنظیم زمان سنخ: روشهای وفقی و پویا
۱۲۵	پروتکل <i>UDP</i>
۱۲۷	مروری بر پروتکل <i>IPV6</i>
۱۲۷	قابلیت آدرس دهی توسعه یافته
۱۲۸	قالب هدر <i>IPV6</i>
۱۳۰	ترتیب هدرهای الحاقی
	بخش سوم: سرویس دهنده نام های حوزه- پروتکل <i>DNS</i>

۱۳۳	آشنائی با پروتکل <i>DNS</i>
۱۳۳	پروتکل <i>DNS</i> و مدل مرجع <i>OSI</i>
۱۳۵	ساختار سرویس دهندگان نام دامنه ها در اینترنت
۱۳۶	سرویس دهنده نام های حوزه <i>DNS</i>
۱۴۰	هفت حوزه عمومی
۱۴۲	روش های پرس و جوی نام در سرویس دهنده های نام
۱۴۷	توابع مفید در برنامه نویسی شبکه
	بخش چهارم: <i>Mac Address</i> و پروتکل های دسترسی چندگانه
۱۵۲	<i>MAC Address</i>
۱۵۳	دلیل استفاده از <i>MAC Address</i>
۱۵۳	ساختار <i>MAC Address</i>
۱۵۵	اترنت
۱۵۷	تکنولوژی <i>CSMA/CD</i>
۱۵۹	پروتکل های دسترسی چندگانه
۱۶۰	کاربرد های اترنت
۱۷۳	شبکه های محلی بی سیم
۱۷۸	بلوتوث
۱۷۹	هدایت در سطح لایه پیوند داده ها
۱۸۱	انواع قالب فریم های <i>IEEE</i>
۱۸۴	یک ساختمان با سیم کشی مرکزی با بهره گیری از هاب
۱۸۴	خلاصه روش ها و سیستم های تخصیص یک کانال مشترک
	بخش پنجم: ماهیت و نحوه پیکربندی دستگاه های شبکه ای
۱۸۸	ماهیت و نحوه پیکربندی دستگاه های شبکه ای
۱۸۸	کنترل کننده ها "Repeaters"
۱۸۹	هاب ها "Hubs"
۱۹۱	چند نکته
۱۹۴	وظایف هاب
۱۹۵	مسیر یاب ها "Routers"
۱۹۶	دروازه ها "Gateways"
۱۹۷	آگاهی از تفاوت بین پروتکل های <i>routing</i> و <i>routed</i>
۱۹۷	سوئیچ <i>Switches</i>
۲۰۲	تکنولوژی سوئیچ ها
۲۰۴	انواع سوئیچ های مبتنی بر بسته های اطلاعاتی

۲۰۵	انواع سوئیچ های LAN از نقطه نظر طراحی
۲۰۶	سیستم <i>Transparent bridging</i>
۲۰۸	فراوانی و آشفته‌گی انتشار
۲۱۳	روترها و سوئیچینگ لایه سوم
۲۱۴	روترها (<i>Router</i>)
۲۱۸	انواع روترها
۲۲۰	مهمترین ویژگی های یک روتر
۲۲۱	چندمثال
۲۲۳	آشنائی با روترهای سیسکو
۲۲۳	مفاهیم مربوط به ارسال سیگنال و پهنای باند
۲۲۴	عملکرد یک شبکه <i>packet-Switching</i>
	بخش ششم: پروتکل های <i>PPP</i> و <i>SLIP</i>
۲۲۷	آشنائی با پروتکل های <i>PPP</i> و <i>SLIP</i>
۲۲۸	وجه اشتراک پروتکل های <i>PPP</i> و <i>SLIP</i>
۲۲۹	نحوه عملکرد یک اتصال <i>SLIP</i> و یا <i>PPP</i>
۲۲۹	پروتکل های لایه اینترنت <i>ICMP, ARP, RARP</i>
۲۳۲	چند نکته در ارتباط با روش آدرس دهی <i>APIPA</i>
۲۳۳	پروتکل <i>ARP</i>
۲۳۴	پروتکل <i>RARP</i>
	بخش هفتم: آزمایشگاه شبکه
۲۳۷	پورت ها
۲۳۷	اتصالات شبکه و اینترنت
۲۳۸	وظایف کارت شبکه
۲۳۸	نصب فیزیکی یک کارت شبکه
۲۴۰	تجهیزات شبکه
۲۴۰	تجهیزات غیرفعال (<i>Passive</i>)
۲۴۳	تجهیزات فعال (<i>Activ</i>)
۲۴۶	سایر تجهیزات و متعلقات
۲۴۷	کابل کشی شبکه
۲۴۷	مراحل ایجاد یک کابل <i>Straight</i>
۲۴۹	شماره پین های استاندارد <i>T568B</i>
۲۵۰	شماره پین های استاندارد <i>T568A</i>
۲۵۱	ایجاد کابل <i>X-Over</i>

۲۵۴	کابل Rollover و یا Console
۲۵۵	مستند سازی شبکه
۲۵۷	مزایای مستندسازی
۲۵۸	مراحل مستند سازی شبکه
۲۶۰	از کجا می بایست شروع کرد ؟
۲۶۱	ابزارهای لازم برای رسم نمودارها
۲۶۴	مراحل طرح یک شبکه محلی
۲۶۵	اجرای پروژه شبکه محلی (LAN) در یک ساختمان
۲۷۱	تجهیزات سخت افزاری
۲۷۲	تنظیمات مربوط به ویندوز برای ایجاد شبکه
	بخش هشتم: شبکه های بدون کابل
۲۷۵	شبکه های بدون کابل
۲۷۷	انواع شبکه های بدون کابل
۲۷۷	Bluetooth
۲۷۸	تهدیدات امنیتی مرتبط با فن آوری Bluetooth
۲۷۹	حفاظت در مقابل تهدیدات
۲۸۰	سیگنال های نوری مادون قرمز (Infrared Data Association(IrDA)
۲۸۱	SWAP و HomeRF
۲۸۳	Wi-Fi و WECA
۲۸۳	اشکالات Wi-Fi
۲۸۴	فن آوریهای نوین در شبکه های کامپیوتری بی سیم
۲۸۴	شبکه های Indoor
۲۸۵	شبکه بی سیم Ad hoc
۲۸۶	شبکه های Infra Structure
۲۸۷	مزایای شبکه های Infra Structure نسبت به ad hoc
۲۸۷	شبکه های Outdoor
۲۸۸	تجهیزات شبکه های Outdoor
۲۸۸	شبکه Broad Band ,Outdoor
۲۸۸	Wimax
۲۹۱	مزایای Wimax
۲۹۱	امنیت در شبکه های کامپیوتری بیسیم
۲۹۱	فیلتر کردن (Filtering)
۲۹۲	کد گذاری (Encryption)

۲۹۳	صدور مجوز (<i>Authentication</i>)
۲۹۳	اجزای مختلف یک شبکه <i>wireless</i> با ایمنی <i>802.1x</i>
۲۹۴	پروتکل های تصدیق
۲۹۵	کاربردهای عینی شبکه های <i>Wireless</i>
۲۹۸	دستگاه های دیجیتالی شخصی
۲۹۹	استانداردهای بی سیم
۳۰۰	تعدیل و کاهش خطرات امنیتی بی سیم
۳۰۳	دید کلی نسبت به شبکه های محلی بی سیم
۳۰۴	فرکانس و نرخ انتقال داده
۳۰۴	ساختار ۸۰۲/۱۱
۳۰۶	اجزای تشکیل دهنده <i>lan</i> بی سیم
۳۰۸	فواید
۳۰۸	امنیت <i>lan</i> های بی سیم ۸۰۲/۱۱
۳۱۱	حریم
۳۱۲	مشکلات امنیتی استاندارد <i>IEEE 802/11</i>
۳۱۳	مشکلات امنیتی <i>wep</i>
۳۱۴	شرایط لازم برای امنیت
۳۱۵	حملات عمومی
	بخش نهم: امنیت
۳۱۸	مقدمه
۳۱۸	اهداف افراد نفوذگر
۳۱۹	سرویس های امنیتی در شبکه ها
۳۱۹	مفاهیم اصطلاحات سرویس های امنیتی
۳۲۰	تعریف حمله
۳۲۱	دو راه کلی برای حراست و حفظ امنیت اطلاعات
۳۲۲	مثال هایی از حملات فعال
۳۲۲	انواع حملات غیر فعال
۳۲۳	دیوار آتش <i>Firewall</i>
۳۲۴	پس از پردازش و تحلیل بسته
۳۲۵	مبانی طراحی دیوار آتش
۳۲۷	لایه اول دیوار آتش
۳۲۸	لایه دوم دیوار آتش
۳۲۸	لایه سوم دیوار آتش

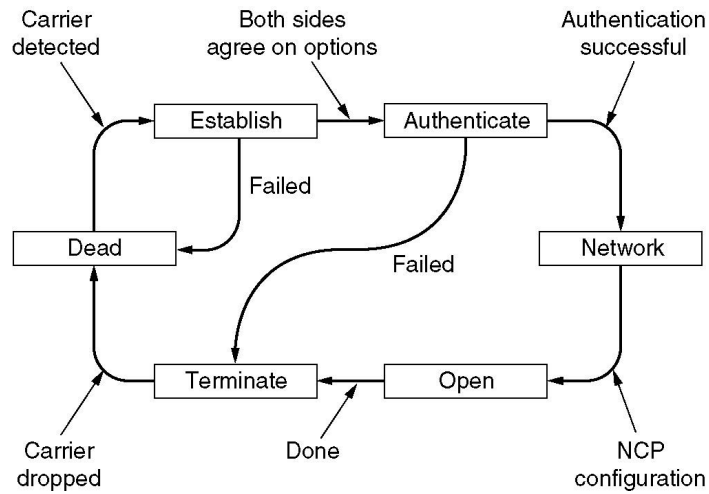
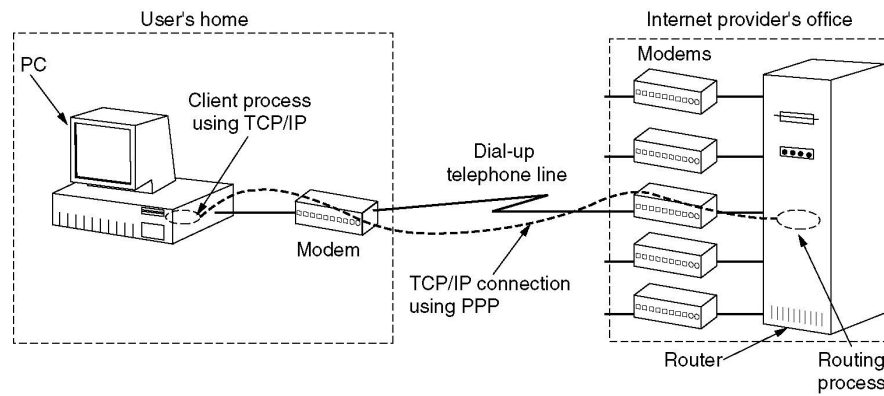
	اجزای جانبی یک دیوار آتش
	۳۲۹
۳۳۱	راه حل نهائی
۳۳۱	انواع فایروال ها
۳۳۲	نحوه پیکربندی بهینه یک فایروال
۳۳۳	NAT
۳۳۴	فیلترینگ پورت ها
۳۳۶	ناحیه غیرنظامی (DMZ (Demilitarized Zone
۳۳۶	فورواردینگ پورت ها
۳۳۸	استراتژی حفاظت از اطلاعات
۳۴۱	امنیت اطلاعات در شبکه های کامپیوتری
۳۴۲	دشمنان، انگیزه ها ، انواع حملات اطلاعاتی
۳۴۳	انواع حملات اطلاعاتی
۳۴۴	ایمن سازی اطلاعات
۳۴۵	انسان
۳۴۶	تکنولوژی
۳۴۸	عملیات
۳۴۹	رمزنگاری DES & RSA Cryptography
۳۵۰	روشهای جانشینی (Substitution)
۳۵۱	رمزنگاری جایگشتی Permutation
۳۵۳	استاندارد DES
۳۵۷	رمزگذاری کلید عمومی (Public Key Cryptography)
	بخش دهم: چند رسانه ای در شبکه
۳۶۳	مقدمه
۳۶۳	صوت
۳۶۷	تصویر
۳۶۸	سیستم های آنالوگ
۳۷۱	سیستم های دیجیتال
۳۷۳	فشرده سازی داده ها
۳۷۴	رمز گذاری آنتروپی
۳۷۵	رمز گذاری منبع
۳۷۸	استاندارد جی پی ئی جی
۳۸۳	استاندارد ام پی ئی جی

۳۸۶	خروجی ام پی ئی جی متشکل از چهار نوع قاب است
۳۸۹	ام پی ئی جی - ۲
۳۹۱	فیلم های ویدیویی در خواستی
۳۹۴	کارگزارهای فیلم ویدیویی
	بخش یازدهم: سیستم تلفن
۳۹۷	سیستم تلفن
۳۹۸	ساختار سیستم تلفن
۴۰۳	مولفه های اصلی تلفن
۴۰۳	سیاست های تلفن ها
۴۰۶	حلقه محلی
۴۰۷	مشکلات انتقال
۴۰۸	مودم ها
۴۱۳	فیبر در حلقه محلی
۴۱۴	شاه سیم ها و تسهیم سازی
۴۱۶	تسهیم سازی تقسیم فرکانس
۴۱۷	تسهیم سازی تقسیم طول موج
۴۱۸	تسهیم سازی تقسیم زمانی
	بخش دوازدهم: پروکسی
۴۲۱	پراکسی سرور
۴۲۱	پراکسی چیست؟
۴۲۲	تفاوت پراکسی با <i>Packet filter</i>
۴۲۳	تفاوت پراکسی با <i>Stateful packet filter</i>
۴۲۴	پراکسی ها یا <i>Application Gateways</i>
۴۲۵	عملکردهایی پراکسی سرور
۴۲۷	ویژگی های <i>Proxy Server</i>
۴۲۸	خدمات <i>Proxy Server</i>
۴۳۰	برخی انواع پراکسی
۴۳۱	پراکسی <i>SMTP</i>
۴۳۲	<i>HTTP Proxy</i>
۴۳۴	<i>FTP Proxy</i>
۴۳۵	<i>DNS Proxy</i>
۴۳۷	معیارهای موثر در انتخاب <i>Proxy Server</i>
۴۳۸	پیوست

بخش ششم:

پروتکل های

ICMP و RARP ، ARP ، PPP ، SLIP



آشنائی با پروتکل های SLIP و PPP

(Serial Line Internet Protocol) SLIP

(Point-To-Point) PPP

مبادله اطلاعات بر روی اینترنت با استفاده از پروتکل TCP/IP انجام می شود . با این که پروتکل فوق یک راه حل مناسب در شبکه های محلی و جهانی را ارائه می نماید ، ولی به منظور ارتباطات از نوع Dial-up طراحی نشده است .

ارتباط Dial-up ، یک لینک نقطه به نقطه (Point-To-Point) با استفاده از تلفن است . در چنین مواردی یک روتر و یا سرویس دهنده، نقطه ارتباطی شما به شبکه با استفاده از یک مودم خواهد بود. سرویس دهنده دستیابی راه دور موجود در مراکز ISP ، مسئولیت ایجاد یک ارتباط نقطه به نقطه با سریس گیرندگان Dial-up را برعهده دارد . در ارتباطات فوق ، می بایست از امکانات خاصی به منظور ارسال IP و سایر پروتکل ها استفاده گردد . با توجه به این که لینک ایجاد شده بین دو نقطه برقرار می گردد ، آدرس دهی مشکل خاصی را نخواهد داشت.

SLIP و PPP پروتکل هایی می باشند که امکان استفاده از TCP/IP بر روی کابل های سریال نظیر خطوط تلفن را فراهم می نمایند (SLIP و PPP : دو روش متفاوت به منظور اتصال به اینترنت) . با استفاده از پروتکل های فوق ، کاربران می توانند توسط یک کامپیوتر و مودم به اینترنت متصل شوند . از پروتکل SLIP در ابتدا در سیستم عامل یونیکس استفاده می گردید ولی امروزه تعداد بیشتری از سیستم های عامل نظیر لینوکس و ویندوز نیز از آن حمایت می نمایند . در حال حاضر استفاده از پروتکل SLIP نسبت به PPP بمراتب کمتر است .

PPP نسبت به SLIP دارای مزایای متعددی است :

PPP امکان مبادله اطلاعات به صورت همزمان و غیر همزمان . در پروتکل SLIP صرفاً امکان مبادله اطلاعات به صورت همزمان وجود دارد .
ارائه امکانات لازم به منظور تصحیح خطاء .

تصحیح خطاء در پروتکل *SLIP* عموماً "مبتنی بر سخت افزار استفاده شده به منظور برقراری ارتباط (نظیر مودم) و یا استفاده از قابلیت های پروتکل *TCP/IP* است .
PPP ارائه امکانات لازم برای فشرده سازی . پروتکل *SLIP* در اغلب بخش های آن چنین ویژگی را دارا نمی باشد . در این رابطه نسخه هائی از *SLIP* به منظور فشرده سازی نظیر *Compressed SLIP* و یا *CSLIP* طراحی شده است ولی متداول نمی باشند .
ارائه امکانات لازم به منظور نسبت دهی آدرس ها به صورت پویا و اتوماتیک . پروتکل *SLIP* می بایست به صورت دستی پیکربندی گردد (در زمان *Dial-up* و یا تنظیم اولیه *Session*) .
امکان استفاده از چندین پروتکل بر روی لینک های *PPP* وجود دارد (نظیر *IP* و یا *IPX*) .
در پروتکل *SLIP* صرفاً " امکان استفاده از پروتکل *IP* وجود خواهد داشت .

وجه اشتراک پروتکل های *PPP* و *SLIP*

هر دو پروتکل قابل روتینگ نمی باشند . با توجه به نوع ارتباط ایجاد شده که به صورت نقطه به نقطه است و صرفاً " دو نقطه در ارتباط درگیر می شوند ، ضرورتی به استفاده از روتینگ وجود نخواهد داشت .

هر دو پروتکل قادر به کپسوله نمودن سایر پروتکل هائی می باشند که در ادامه برای روتر و سایر دستگاه ها ارسال می گردند . در مقصد، اطلاعات مربوط به پروتکل های *SLIP* و یا *PPP* برداشته شده و پروتکل های ارسالی توسط لینک سریال نظیر *IP* ، در طول شبکه فرستاده می گردد .

یک کامپیوتر با استفاده از یک ارتباط *SLIP* و یا *PPP* قادر به شبیه سازی یک اتصال مستقیم به اینترنت است . در این رابطه به امکانات زیر نیاز می باشد :

- ✓ یک کامپیوتر و مودم
- ✓ یک *account* از نوع *SLIP* و یا *PPP* از *ISP* مربوطه
- ✓ نصب نرم افزارهای *TCP/IP* و *SLIP/PPP* بر روی کامپیوتر کاربر (نرم افزارهای فوق معمولاً در زمان استقرار سیستم عامل بر روی کامپیوتر نصب خواهند شد) .
- ✓ یک آدرس *IP* . آدرس فوق ممکن است به صورت دائم و یا پویا (استفاده از سرویس دهنده *DHCP*) به کامپیوتر کاربر نسبت داده شود.

نحوه عملکرد یک اتصال SLIP و یا PPP

- ✓ مودم موجود بر روی کامپیوتر اقدام به شماره گیری یک کامپیوتر از راه دور در یک ISP می نماید .
- ✓ نرم افزار SLIP/PPP درخواست یک اتصال SLIP/PPP را می نماید .
- ✓ پس از برقراری ارتباط ، ISP مربوطه به کامپیوتر کاربر یک آدرس IP را اختصاص خواهد داد (در مواردی که از یک سرویس دهنده DHCP استفاده می گردد) .
- ✓ نرم افزار TCP/IP بر روی کامپیوتر کاربر ، کنترل و مدیریت مبادله اطلاعات بین کامپیوتر کاربر و اینترنت را برعهده خواهد گرفت .

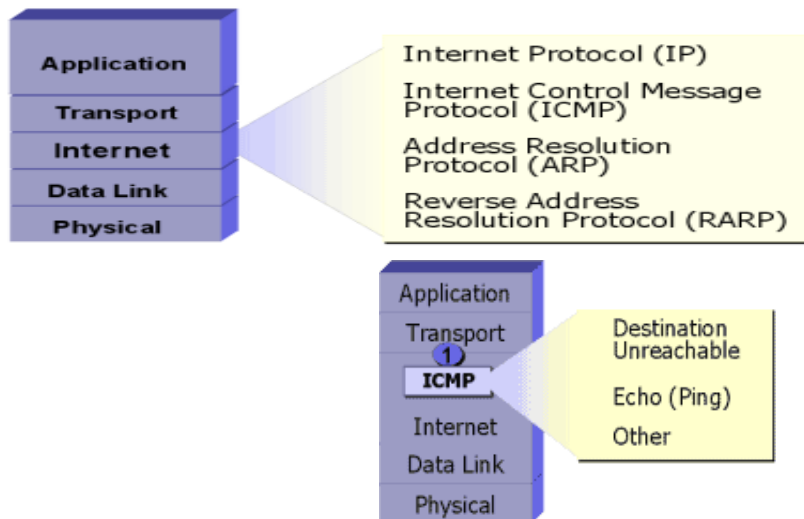
دیگر پروتکل های لایه اینترنت

در پیاده سازی لایه اینترنت سه پروتکل دیگر نیز وجود دارد که شامل ICMP, ARP, RARP هستند.

ICMP (Internet Control Message Protocol)

پروتکل کنترل پیام اینترنت (ICMP) بوسیله میزبان های TCP/IP پیاده سازی می شوند . پیام های ICMP در داده گرام های IP حمل می شوند و برای فرستادن خطا ها و پیام های کنترل استفاده می شوند .

ICMP: از انواع پیام های تعریف شده زیر استفاده می کند.



Destination Unreachable
Time Exceeded
Parameter Problem
Subnet Mask Request
Redirect
Echo
Echo Reply
Timestamp
Timestamp Reply
Information Request
Information Reply
Address Request

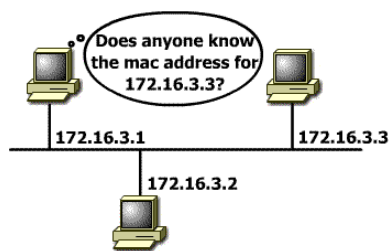
پروتکل تعیین آدرس

پروتکل تعیین آدرس برای رفع کردن یا نشان دادن یک آدرس IP شناخته شده به یک زیر لایه آدرس MAC برای اجازه دادن جهت انتقال به یک واسط چند منظوره مثل اترنت استفاده می شود. برای تعریف آدرس مقصد برای یک داده گرام حافظه Cache روی ARP چک شده اگر آدرس درون حافظه نبود ARP آدرس را جهت جستجو برای یافتن ایستگاه مقصد به همه ایستگاه های درون شبکه پخش می کند و همه ایستگاه ها پیام را دریافت می کنند.

واژه ARP محلی برای شرح و رفع یک آدرس استفاده شده زمانیکه هر میزبان تقاضا کننده و میزبان مقصد دارای رسانه مشترک باشند.

معکوس ARP

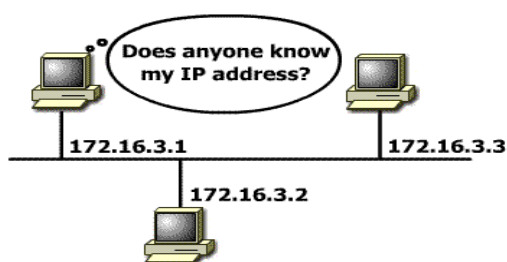
RARP برحضور یک سرویس دهنده RARP با یک جدول ورودی تکیه دارد.



در قسمت های محلی RARP می تواند استفاده شود برای شروع بار گذاری سیستم عامل از راه دور RARP, ARP مستقیما بر روی لایه پیوند داده ها پیاده سازی می شوند.

APIPA چیست ؟ Automatic Private IP Addressing

در یک شبکه کامپیوتری سرویس ها و خدمات متعددی از طریق سرویس دهندگان مختلف در اختیار سرویس گیرندگان قرار می گیرد . اختصاص پویای اطلاعات مربوط به آدرس دهی IP توسط سرویس دهنده DHCP (برگرفته از Dynamic Host Configuration Protocol) ، نمونه ای در این زمینه است .



DHCP ، پس از پروتکل BOOTP مطرح و مهمترین هدف آن تامین اطلاعات مورد نیاز یک ایستگاه و یا سایر دستگاه های شبکه ای در ارتباط با پروتکل TCP/IP است . بدین منظور از سه روش متفاوت استفاده می گردد :

اختصاص اتوماتیک : در این روش سرویس دهنده DHCP یک آدرس دائم را به یک سرویس گیرنده نسبت می دهد .

اختصاص پویا : متداولترین روش استفاده از سرویس دهنده DHCP در یک شبکه می باشد که بر اساس آن سرویس دهنده یک آدرس را به صورت پویا در اختیار سرویس گیرنده قرار می دهد . آدرس نسبت داده شده به سرویس گیرنده بر اساس مدت زمان مشخص شده توسط سرویس دهنده DHCP تعیین می گردد (محدود و یا نامحدود)

اختصاص دستی : در این روش که معمولاً توسط مدیران شبکه استفاده می گردد ، یکی از آدرس های موجود در بانک اطلاعاتی سرویس دهنده DHCP به صورت دستی به یک سرویس گیرنده و یا سرویس دهنده خاص نسبت داده می شود (Reservations) .

در صورتی که پیکربندی پروتکل TCP/IP بر روی یک کامپیوتر بگونه ای انجام شده است که کامپیوتر و یا دستگاه شبکه ای مورد نظر را ملزم به استفاده از خدمات سرویس دهنده DHCP می نماید (تنظیمات انجام شده در صفحه Properties پروتکل TCP/IP) ولی در عمل سرویس دهنده وجود نداشته باشد و یا سرویس گیرندگان قادر به برقراری ارتباط با

آن نباشند و یا برای سرویس دهنده DHCP مشکل خاصی ایجاد شده باشد ، تکلیف سرویس گیرندگان و متقاضیان استفاده از خدمات سرویس دهنده DHCP چیست ؟ در چنین مواردی سرویس گیرندگانی که بر روی آنان یکی از نسخه های ویندوز (به جزء ویندوز NT) نصب شده است ، می توانند از APIPA (برگرفته از Automatic Private IP Addressing) استفاده نمایند . با استفاده از سرویس فوق که صرفاً در شبکه های کوچک قابل استفاده خواهد بود (حداکثر ۲۵ دستگاه موجود در شبکه) ، هر یک از سرویس گیرندگان می توانند به صورت تصادفی یک آدرس IP خصوصی را بر اساس مشخصات جدول زیر به خود نسبت دهند.

آدرس رزو شده توسط APIPA
169.254.0.1 TO 169.254.255.254
Subnet Mask
255 . 255 . 0 . 0

چند نکته در ارتباط با روش آدرس دهی APIPA :

زمانی که یک سرویس گیرنده پاسخ مناسبی را از سرویس دهنده DHCP دریافت ننماید ، پس از مدت زمان کوتاهی یک آدرس تصادفی را از شبکه دریافت می نماید . با توجه به این که سرویس گیرنده به صورت کاملاً تصادفی یک آدرس IP را انتخاب می نماید ، همواره این احتمال وجود خواهد داشت که یک کامپیوتر آدرسی را انتخاب نماید که قبلاً توسط کامپیوتر دیگری استفاده شده باشد . برای حل این مشکل ، پس از انتخاب یک آدرس IP توسط سرویس گیرنده ، یک بسته اطلاعاتی broadcast شامل آدرس IP توسط سرویس گیرنده در شبکه ارسال و بر اساس پاسخ دریافتی ، در خصوص نگهداری و یا آزادسازی آدرس IP تصمیم گیری می گردد . اطلاعات ارائه شده توسط APIPA ، یک آدرس IP و یک Subnet mask می باشد و سایر اطلاعاتی که عموماً توسط سرویس دهنده DHCP ارائه می گردد را شامل نمی شود . مثلاً با استفاده از APIPA نمی توان آدرس gateway پیش فرض را در اختیار سرویس