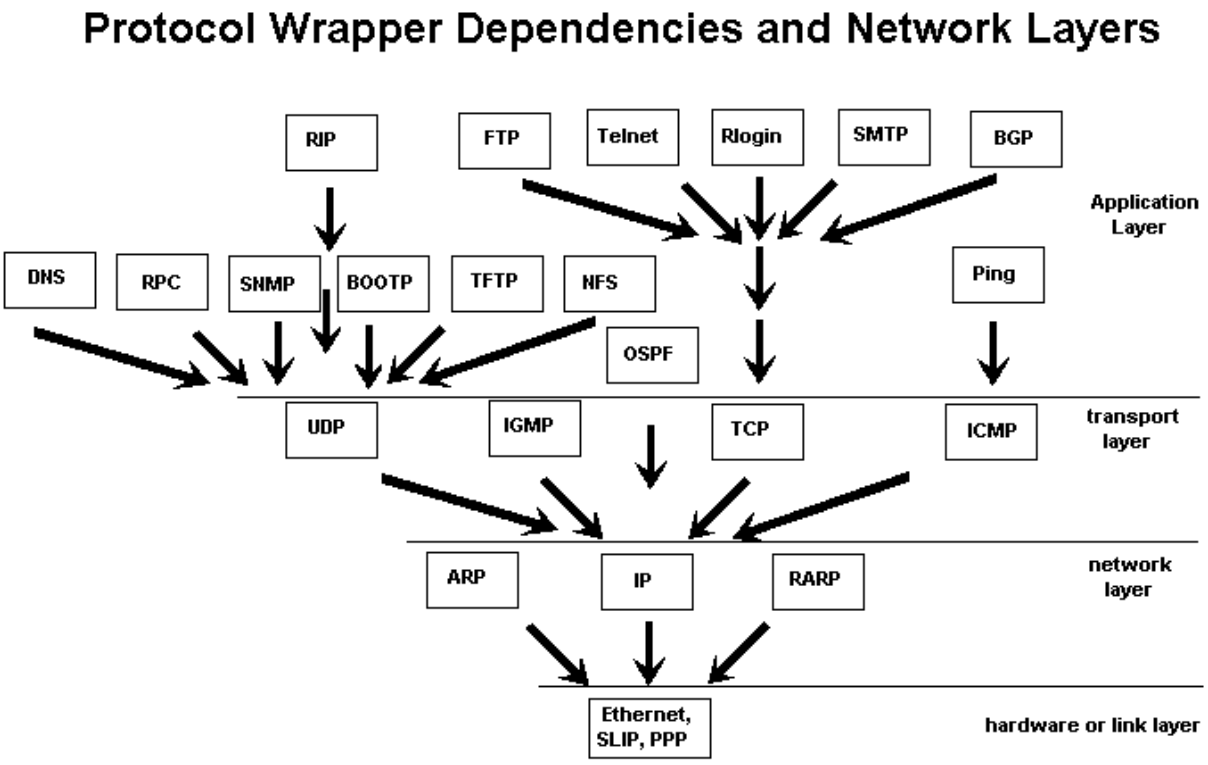
پروتکل های اینترنت

مرضیه کریمی نوری

فهرست

I. پروتکل‌ها ولایه‌های شبکه



II. پروتکلهای لایه Aplication

مجموعه ای ازقوانین یا استانداردها که برای آن طراحی شده اند تا به کامپیوترهااین امکان داده شود که با حداقل خطای ممکن با یکدیگر ارتباط برقرار نموده به تبادل اطلاعات بپردازند

- Telnet
- FTP
- NFS
- SMTP
- SNMP
- DNS
- DHCP
- POP3
- HTTP

III. برخی از پر کاربرد ترین پروتکل های اینترنت:

1. Ethernet :

2. HTTP:

دنیای شبکه های کامپیوتری دارای عمری چند ساله است و بسیاری از کاربران ، ضرورت استفاده از شبکه را همزمان با متداول شدن اینترنت در اوایل سال 1990 دریافتند . عمومیت اینترنت، رشد و گسترش شبکه های کامپیوتری را به دنبال داشته است . اینترنت نیز با سرعتی باورنکردنی رشد و امروزه شاهد ایجاد ده ها میلیون وب سایت در طی یک سال در این عرصه می باشیم .

تمامی وب سایت های موجود بر روی اینترنت از پروتکل HTTP استفاده می نمایند . با این که پروتکل HTTP با استفاده از پروتکل های دیگری نظیر IP و TCP ماموریت خود را انجام می دهد ، ولی این پروتکل HTTP است که به عنوان زبان مشترک ارتباطی بین سرویس گیرنده و سرویس دهنده وب به رسمیت شناخته شده و از آن استفاده می گردد . در واقع مرورگر وب صدای خود را با استفاده از پروتکل HTTP به گوش سرویس دهنده وب رسانده و از وی درخواست یک صفحه وب را می نماید.

به منظور انجام یک تراکنش موفقیت آمیز بین سرویس گیرندگان وب (نظیر IE) و سرویس دهندگان وب (نظیر IIS) ، به اطلاعات زیادی نیاز خواهد بود . پس از handshake پروتکل TCP/IP ، مرورگر اطلاعات گسترده ای را برای سرویس دهنده وب ارسال می نماید .

3. SLIP- Serial line IP (SLIP) :

نوعی انکپسوله کردن داده در خط های سریال.

4. PPP - Point to point protocol (PPP) :

نوعی انکپسوله کردن داده در خط های سریال که بهبودی در SLIP ایجاد کرده است.

5. IP - Internet Protocol (IP) :

IP یک پروتکل ارتباطی می باشد. IP یک عدد 32 بیتی است که هر 3 رقم آن با . از هم جدا می‌شوند.
شکل کلی IP را مشاهده کنید : XXX.XXX.XXX.XXX 192.168.100.100

به هر 8 بیت که با . از هم جدا می شوند یک اکتت گفته می شود. اینترنت بر اساس پروتکا TCP\IP راه اندازی شده است.

آدرس هایIP در پنج کلاس A,B,C,D,E معرفی شده اند.

6. ICMP - Internet control message protocol (ICMP) :

پروتکل ICMP در کنار پروتکل IP برای برسی انواع خطا و ارسال پیام برای مبدا بسته در هنگام بوز اشکالات ناخواسته استفاده میشود . در حقیقت ICMP یک سیستم گزارش خطا است که برروی پروتکل IP نصب میشود تا در صورت بروز هر گونه خطا به فرستنده بسته پیام مناسب را بدهد تا آن خطا تکرار نشود . در واقع ICMP وظیفه ای در قبال وقوع خطا ندارد بلکه فقط پیامی که بیانگر بروز خطا و نوع آن است به فرستنده بر میگرداند . این پروتکل اشکالات موجود را در قالب یک سری پیام گزارش میکند که این پیام خود در یک بسته IP قرار میگیرد و از جانب یک مسیر یاب یا ماشین مقصد به آدرس فرستنده باز میگردد .

7. ARP - Address resolution protocol (ARP) :

نکته ظریفی که در مورد شبکه اینترنت وجود دارد آن است که اگر چه تمامی ماشینهای میزبان و ابزارهای شبکه ای از آدرس IP که آدرس منحصر به فرد و یکتاست استفاده میکنند. ولیکن آدرسهای IP فقط در لایه شبکه قابل شناسایی و تحلیل هستند یک بسته IP قبل از ارسال روی کانال از لایه اول یعنی لایۀ فیزیکی عبور میکند و ضمن اضافه شدن اطلاعات لازم و تشکیل یک فریم ، روی کانال فیزیکی ارسال میشود . بعبارت روشنتر بسته IP قبل از ارسال درون فیلد داده از فریمی قرار میگیرد که بعداً در لایه اول تشکیل میشود؛ لایه اول وظیفه ای در قبال مسیریابی وکارهائی از این قبیل ندارد و فقط با آدرسهای فیزیکی کار میکند . بعنوان مثال اگر ماشین شما بخواهد بسته ای را برای ماشینی که روی شبکه محلی خودتان واقع است بفرستد، در لایه اول الزاماً بایستی آدرس فیزیکی ماشین شما (مبداء) و آدرس فیزیکی ماشین طرف مقابل (مقصد) معین باشد . (این آدرسها بصورت سخت افزاری در کارت شبکه درج شده است)عدم دانستن آدرسهای فیزیکی عملاً مساوی عدم توانایی برای ارتباط خواهد بود چرا که روی کانال انتقال آدرسهای IP بی معنا هستند

حال فرض کنید ماشین شما میخواهد بسته ای را برای ماشین دیگر ارسال کند که روی شبکه فعلی شما نیست. در این حالت هم لایه اول یک فریم برای ارسال روی کانال فیزیکی تشکیل میدهد

8. TCP :

TCP/IP

این عنوان شامل مجموعه ای بیش از 100 قرارداد می باشد که برای متصل ساختن کامپیوترها و شبکه ها استفاده می شوند. نام TCP/IP از دو قرارداد بزرگ به نامهای Transmission Control protocol و Internet protocolاخذ شده است .

در داخل اینترنت اطلاعات به صورت جریان ثابتی بین کامپیوترها منتقل نمی شوند، بلکه داده ها به صورت بسته های کوچک اطلاعات به نام پکت pecket ، شکسته شده و انتقال می یابند .

TCP/IPیک پروتکل با قابلیت مسیریابی است ، بدین معنی که در اینترنت هر کدام از packet های مذکور که دارای آدرس اختصاصی هستند، مسیر یابی شده و هدایت می شوند. مسیریابها (Routers) آدرس هر packet را بررسی کرده و آنرا به سمت نزدیکترین مسیر به سوی کامپیوتر هدف سوق می دهند .

به عنوان مثال، بین دو کامپیوتر در اینترنت، یک پیام در حال تبادل می باشد:
کامپیوتر اول، پیام را به سمت کامپیوتر دوم ارسال می کند. ابتدا TCP پیام را به تعدادی Packet تقسیم میکند. همانگونه که گفته شد هر packet از طریق شبکه فرستاده می شوند . در اینجا IP باید آنها را به کامپیوتر دوم منتقل کند. کار انتقال Packet ها شروع می شود و در شبکه جهانی به سمت کامپیوتر دوم حرکت می کنند. در بین راه مسیریابهای موجود در پایگاههای اینترنتی آدرس Packet ها را بررسی کرده و آنها را به نزدیکترین و منطقی ترین مسیر راهنمایی می کنند تا اینکه packet ها به کامپیوتر دوم برسند. حال در کامپیوتر دومTCP ، packetها را به دریافت کرده و آدرسها و وجود خطاها را بررسی می نماید. بعد از اینکه تمام packet ها به درستی دریافت شدند، TCPاز شماره های موجود در آدرسهای هر Packet برای ساختن مجدد پیام اصلی استفاده کرد و پیام را بازسازی می نماید. بدین ترتیب با استفاده از پروتکل TCP/IP ، داده ها انتقال می یابند .

به طور خلاصه می توان گفت ، کار IP گرفتن و انتقال Packet ها از یک مکان به مکان دیگر است و کار TCP اداره جریان و تضمین صحت اطلاعات می باشد.

9. UDP :

این پروتکل برای کاهش overflow طراحی شده و در خیلی از موارد وابسته به TCP هستش.

نکته مهم اینه که وقتی با یه پورت خاص روی یک کامپیوتر دیگه ارتباط برقرار می کنیم ، این ارتباط می تونه از نوع TCP یا UDP باشه . بنابراین وقتی می خوایم یه کامپیوتر خاصی رو از نظر پورت ها بررسی کنیم ، هر دو باید بررسی بشه.

10. DNS - Domain Name Service :

DNSمخفف عبارت Domain Name Service می باشد. وقتی میخواهید وارد سایتی شوید، باید آدرس وب سرور آنرا بدانید.آدرس وب سرور با IP مشخص میشود. اما به خاطر سپردن آدرس IP دشوار است. می توان به جای IP از domin name ها استفاده کرد. برای هر IP یک domin name در نظر گرفته شده است. مثلا IP آدرس گوگل 66.249.91.103 است. که شما برای دسترسی به گوگل میتوانید از ip یا آدرس www.google.comاستفاده کنید.

11. RARP - Reverse address resolution protocol (RARP) :

یک پروتکل برای تعیین نشانیIP یک گره در یک شبکه محلی که به اینترنت متصل است این کار زمانی که تنها نشانی سخت افزاری معلوم است انجام می شود

12. BOOTP :

13. DHCP - Dynamic host configuration protocol (DHCP) :

پروتکل پیکربندی پویای میزبان (DHCP) به شما اجازه می دهد ادرسهای IP را بصورت پویا به کامپیوترها و وسایل جانبی روی شبکه اختصاص دهید. آدرس های IP از مخزنی از آدرس های تهیه شده و به کامپیوترها اختصاص داده می شوند. اختصاص آدرس IP بصورت دائم و مو قت خواهد بود. وقتی این مسئله را در نظر بگیرید که باید به هر کامپیوتر مشتری ، آدرس IP ماسک زیر شبکه و آدرس دروازه اختصاص دهید در می یابید که احتمال خطا در اختصاص آدرس ها بسیار بالاست .

DHCPیک محیط پویا ایجاد می کند که آدرس های IP را به کامپیوترها و وسایل جانبی روی شبکه اختصاص می دهد. با این روش با دردسرهای اختصاص آدرس IP بصورت دستی روبه رو نمی شوید و اختصاص آدرس های IP به کامپیوترها با دقت بالایی انجام می گیرد .

سرور DHCP وظیفه دارد آدرس IP ، ماسک زیر شبکه، دروازه پیش ساخته، آدرس سرور DNS و آدرس سرور WINS را به مشتری DHCP ارائه دهد. مشتری DHCP هر کامپیوتر یا وسیله ای روی شبکه است که برای کسب پویای آدرس IP پیکربندی شده است.

14. IGMP - Internet Group Management Protocol :

پروتکلی است که مدیریت لیست اعضاء برای IP Multicasting ، در یک شبکه TCP/IP را بر عهده دارد . IP Multicasting، فرآیندی است که بر اساس آن یک پیام برای گروهی انتخاب شده از گیرندگان که گروه multicat نامیده می شوند ؛ ارسال می گردد . IGMP لیست اعضاء را نگهداری می نماید .

15. SNMP - Simple Network Management Protocol (SNMP) :

پروتکل SNMP پروتکلیست جهت کنترل و دریافت اطلاعات از کلیه تجهیزات تحت شبکه که این پروتکل را پشتیبانی میکنند.

این پروتکل در مجموع دارای دو متد بسیار مهم می باشدمتد SET و متد GET .متد SET جهت اعمال تنظیمات و متد GET جهت دریافت اطلاعات از قطعات IP Based مورد استفاده قرار می گیرد.معمولا در بحث SNMP مباحثی چون MIB و OID نیز مطرحست.هر Device تحت شبکه که پروتکل SNMP رو ساپورت می کنه OID های مربوط به خود رو داره.بطور مثال شما قصد دارید با کمک این پروتکل یک روتر سیسکو را از راه دور ریستار کنید برای این منظور شما بایستی با متد SET مقدا ر(OID (.3.6.1.4.1.9.9.48.1.1.1.6.1 را ست نمود تا بتوانید از راه دور روتر را ریستار نمایید.البته بحث درمورد پروتکل SNMP بسیار وسیع تر از آنچیزیست که من اینجا مطرح نمود.مباحثی چون Trap و MIB Browser از جمله مطالبیست که در بحث پروتکل SNMP مطرح می باشد.

16. RIP - Routing Information Protocol (RIP) :

RIP (برگرفته شده از Routing Information Protocol) به معنی واقعی یک پروتکل distance-vector است . پروتکل فوق در هر 30 ثانیه تمام اطلاعات موجود در جدول روتینگ را برای تمامی اینترفیس های فعال ارسال می نماید . RIP صرفا" از تعداد hop برای تعیین بهترین مسیر به شبکه راه دور استفاده می

نماید .حداکثر تعداد hop می تواند عدد 15 را داشته باشد و نسبت دهی عددی بالاتر از 15 به منزله غیرقابل دسترس بودن شبکه است.
RIP در شبکه های کوچک به خوبی کار می کند ولی برای شبکه های بزرگ که دارای لینک های ارتباطی WAN (برگرفته شده از wide area network) کند و تعداد بسیار زیادی روتر هستند مناسب نمی باشد .
در نسخه شماره یک RIP صرفا" از روتینگ classful استفاده می گردد . این بدان معنی است که تمامی دستگاه های موجود در شبکه می بایست از mask subnet مشابهی استفاده نمایند . محدودیت فوق به دلیل ماهیت ارسال اطلاعات بهنگام می باشد. در نسخه شماره یک RIP ، اطلاعات بهنگام ارسالی شامل اطلاعات subnet mask نمی باشند .
در RIP نسخه دو ، ویژگی جدیدی به نام روتینگ Prefix ارائه شده است که به کمک آن امکان ارسال اطلاعات subnet mask به همراه مسیرهای بهنگام شده فراهم می گردد . به این نوع روتینگ ، اصطلاحا" روتینگ classless گفته می شود .

17. OSPF - Open Shortest Path First (OSPF) :

پروتکل OSPF (Open Shortest Path First) بر اساس حالتی است که شبکه دارای مسیریاب‌های متعددی است و این مسیریاب‌ها به صورت مسیریابی سلسله مراتبی به یکدیگر پیوند داده شده‌اند.

ریشه یا رأس هرم سلله مراتب یک مسیریبا مستقل دیگری متصل می‌شود. مرحله بعدی در بالاترین منطقه OSPF مسیریاب های ستون مهره‌ای هستند. مسیریاب های مرزی به مناطق متعددی متصل شده‌اند و می‌توانند کپی های متعددی از الگوریتم مسیریابی را اجرا کنند. در انتها مسیریاب‌های داخلی هستند که بک پایگاه اطلاعاتی برای یک منطقه را اجرا می کنند.

با تقسیم شبکه به یک سلسله مراتب مسیریابی، مشکلات گذشته حل خواهد گردید. هر سطح برای خود یک جدول مسیر انتقال کوچک دارد و زمان طولانی و ترافیک برای بهنگام‌سازی این جدول را نخواهیم دشت.
باوجود اینکه OSPF به عنوان یکی از بهترین و پر قدرت ترین پروتکل routing محسوب می شود ، اما همواره استفاده از پروتکل های Distance Vector و یا static routing بر پروتکل Link state نظیر OSPF حتی در شبکه های بزرگ نیز ترجیح داده می شود. مهم ترین دلایل این امر می توابه 2 دسته تقسیم کرد .دسته اول را می توان بار حاصل از اجرای پروتکل OSPF بر روی اجزای device مثل CPU و RAM فرض کرد و عمدتا دلیل دوم نیاز به دانش بالای اجرا ، نگهداری و عیب یابی شبکه های مبتنی بر OSPF می باشد.

18. BGP - Border Gateway Protocol (BGP) :

پروتکلی است که در هسته Routing اینترنت از آن استفاده می شود.
وظیفه این پروتکل اتصال و Routing بین Autonomous System ها و شبکه های بزرگ IP است. بطور مثال ارتش برای اتصال شبکه های نیروهای زمینی،هوائی و دریایی خود – که هر کدام شبکه ای بزرگ IP دارند – از BGP بعنوان Exterior Routing Protocol استفاده میکند.

در واقع BGP حامل اطلاعات Autonomous هاست تا از این طریق شبکه های IP (در درون Autonomous) را پیدا کند. از مشخصات کلی این پروتکل میتوان به موارد زیر اشاره کرد:

یک پروتکل Path Vector است تا Distance Vector.
VLSM و CIDR را پشتیبانی میکند.
ارتباط با همسایگان را روی پورت 179 TCP برقرار میکند و با Keep-alive آن را نگه میدارد.
Routing Table مستقل خود را دارد.
Metric در BGP، Attribute نامیده می شود.
نسبت به پروتکل های Interior کاملا متفاوت بوده و برای ارتباط بین AS هاست. بعبارتی Inter-autonomous Systems Routing Protocol است.
انعطاف پذیر (Flexibility) بوده و با Policy-based Routing حرفه ای همراه است. به هرحال Routing در اینترنت بصورت Hop-by-hop است و سیاست های شما در طول مسیر بوسیله روترهای میان راه – که کنترلی رویشان ندارید – ممکن است بکار گرفته نشود.

19. CIDR - Classless Interdomain Routing (CIDR) :

پروتکل مخصوص [Only Registered Users Can See Links. Click Here To Register...] های تعریف شده برای هر IP است

20. FTP - File Transfer Protocol (FTP) :

یک پروتکل سریع در سطح برنامه کاربردی که بطور گسترده ای برای کپی کردن فایلها از کامپیوتر راه دور یک شبکهTCP/IP مورد استفاده قرار میگرد این پروتکل همچنین به کاربر امکان میدهد تا از فرامین FTPبرای کار با فایلها مثلا فهرست فایلها و داریکتوری ها در سیستم راه دور استفاده کنند

21. TFTP - Trivial File Transfer Protocol (TFTP) :

FTPنگارش ساده شده ای از که امکان انتقال فایل را بدون اعتبار سنجی فراهم نموده است و اغلب برای کردن فایلهای مورد نیاز برای نصب Downloadمورد استفاده قرار می گیرد

22. SMTP - Simple Mail Transfer Protocol (SMTP) :

SMTP مخفف SIMPLE MAIL TRANSFER PROTOCOL است که پروتکل ساده و در عین حال مهم و اساسی برای انتقال ایمیل است. این اصطلاح از آن رو به کار میرود که نسبت به سایر پروتکل های ایمیل قبلی بسیار ساده عمل میکند SMTP . فقط به نام کاربری و دامنه نیاز دارد تا مستقیم پیغام را به سمت گیرنده مسیریابی کند SMTP یک پروتکل ارسال است و برای دریافت مناسب نیست به همین دلیل برای دریافت مناسب نیست به همین دلیل برای دریافت ایمیل به جای SMTP از پروتکل های دریافت ایمیل مثلIMAP و POP3 استفاده می‌شود.

23. NFS - Network File System (NFS) :

NFS پروتکلی است که از طریق آن می‌توان به فایل‌ها، چاپگرها و سایر منابع پایدار شبکه که به اشتراک گذاشته شده‌اند، دسترسی پیدا کرد. این پروتکل که برای اولین بار در سال 1983 توسط شرکت Sun ارائه شد، تا به حال تغییرات زیادی پیدا کرده است و آخرین نسخه آن نسخه شماره 4 می‌باشد. این پروتکل بیشتر در سیستم‌های عامل خانواده Unix کاربرد داشته و گسترش یافته است. در NFS عملیات دسترسی به فایل و ابزار مشترک با رد و بدل یک سری پیغام در هر دو سوی سرویس‌دهنده و سرویس‌گیرنده NFS صورت می‌گیرد.

24. Telnet :

پروتکلی که امکان برقراری ارتباط و وارد کردن فرامین در یک کامپیوتر متصل به اینترنت را به گونه ای فراهم میکند که گویی با پایانه متنی کار می کند که مستقیما به آن کامپیوتر متصل است

25. Pop3- Post Office Protocol:

پروتکلی برای سرویس دهند هایی در اینترنت که پست الکترونیکی را دریافت و ذخیره نموده و به سرویس گیرنده های کامپیوترهایی که به سرویس دهنده ها متصل می شوند انتقال می دهند تا بتوانند آنها را Download, Uploadنمایند