به نام خدا

پروژه درس مهندسی اینترنت

(فاز اول)

رزیتا رحیمی

ارائه شده به : دکتر حسن حقیقی

پروتکل های موجود در اینترنت: 3
1.Transmission Control Protocol (TCP).....3
ارسال اطلاعات با استفاده از TCP :.....3
2.User Datagram Protocol (UDP) 5
پروتکل های موجود در لایه کاربرد:.....5
1-BGP (Border Gateway Protocol) 5
2- Dynamic Host Configuration Protocol (DHCP) 6
3- Domain Name System (DNS).....7
4-File Transfer Protocol (FTP) 8
5- Hypertext Transfer Protocol (HTTP).....9
6- Internet message application protocol (IMAP).....9
7- Internet Relay Chat (IRC).....10
8- Lightweight Directory Access Protocol (LDAP).....10
9- Network News Transfer Protocol(NNTP).....10
10- Network Time Protocol (NTP).....11
11- Post Office Protocol (POP).....12
12 - Routing Information Protocol (RIP).....12
13 - remote procedure call (RPC).....13
14 - Real-time Transport Protocol (RTP).....13
15 - Simple Network Management Protocol (SNMP).....14
16 - Secure Shell (SSH).....14
17 – Telnet.....15

پروتکل های موجود در اینترنت:

Transmission Control Protocol (TCP).1

یکی از پروتکل های استاندارد TCP/IP است که امکان توزیع و عرضه اطلاعات (سرویس ها) بین صرفا" دو کامپیوتر ، با ضریب اعتماد بالا را فراهم می نماید. چنین ارتباطی (صرفا" بین دو نقطه) ، Unicast نامیده می شود . در ارتباطات با رویکرد اتصال گرا ، می بایست قبل از ارسال داده ، ارتباط بین دو کامپیوتر برقرار گردد . پس از برقراری ارتباط ، امکان ارسال اطلاعات برای صرفا" اتصال ایجاد شده ، فراهم می گردد . ارتباطات از این نوع ، بسیار مطمئن می باشند ، علت این امر به تضمین توزیع اطلاعات برای مقصد مورد نظر برمی گردد . بر روی کامپیوتر مبداء ، TCP داده هائی که می بایست ارسال گردند را در بسته های اطلاعاتی (Packet) سازماندهی می نماید. در کامپیوتر مقصد ، TCP ، بسته های اطلاعاتی را تشخیص و داده های اولیه را مجددا" ایجاد خواهد کرد .

ارسال اطلاعات با استفاده از TCP :

بمنظور افزایش کارائی ، بسته های اطلاعاتی را بصورت گروهی ارسال می نماید . TCP ، یک عدد سریال (موقعیت یک بسته اطلاعاتی نسبت به تمام بسته اطلاعاتی ارسالی) را به هریک از بسته ها نسبت داده و از Acknowledgment بمنظور اطمینان از دریافت گروهی از بسته های اطلاعاتی ارسال شده ، استفاده می نماید. در صورتیکه کامپیوتر مقصد ، در مدت زمان مشخصی نسبت به اعلام وصول بسته های اطلاعاتی ، اقدام ننماید ، کامپیوتر مبداء ، مجددا" اقدام به ارسال اطلاعات می نماید. علاوه برافزودن یک دنباله عددی و Acknowledgment به یک بسته اطلاعاتی ، TCP اطلاعات مربوط به پورت مرتبط با برنامه ها ی مبداء و مقصد را نیز به بسته اطلاعاتی اضافه می نماید. کامپیوتر مبداء ، از پورت کامپیوتر مقصد بمنظور هدایت صحیح بسته های اطلاعاتی به برنامه مناسب بر روی کامپیوتر مقصد ، استفاده می نماید. کامپیوتر مقصد از پورت کامپیوتر مبداء بمنظور برگرداندن اطلاعات به برنامه ارسال کننده در کامپیوتر مبداء ، استفاده خواهد کرد .

هر یک از کامپیوترهائی که تمایل به استفاده از پروتکل TCP بمنظور ارسال اطلاعات دارند ، می بایست قبل از مبادله اطلاعات ، یک اتصال بین خود ایجاد نمایند . اتصال فوق ، از نوع مجازی بوده و Session نامیده می شود .دو کامپیوتر درگیر در ارتباط ، با استفاده از

TCP و بکمک فرآیندی با نام : Three-Way handshake ، با یکدیگر مرتبط و هر یک پایبند به رعایت اصول مشخص شده در الگوریتم مربوطه خواهند بود . فرآیند فوق ، در سه مرحله صورت می پذیرد :

مرحله اول : کامپیوتر مبداء ، اتصال مربوطه را از طریق ارسال اطلاعات مربوط به Session ، مقداردهی اولیه می نماید (عدد مربوط به موقعیت یک بسته اطلاعاتی بین تمام بسته های اطلاعاتی و اندازه مربوط به بسته اطلاعاتی)

مرحله دوم : کامپیوتر مقصد ، به اطلاعات Session ارسال شده ، پاسخ مناسب را خواهد داد .

TCP انتقال داده قابل اعتماد در یک محیط IP را فراهم می کند. **TCP** مطابق بر لایه transport از مدل OSI درمیان سرویس های **TCP** انتقال داده جریانی را فراهم می کند، قابلیت اعتماد، کنترل جریان کارا، عملیات full-duplex و .multiplexing برای استفاده قابل اطمینان، هاست های TCP باید یک جلسه مبتنی بر اتصال تاسیس کنند. برای برپایی اتصال از مکانیزم "three-way handshake" استفاده می شود. یک "three-way handshake" هر دو سوی اتصال را همزمان می کنداز طریق توافق بر سر شماره های رشته اغازین. این مکانیزم همچنین هر دو سو را برای انتقال داده اماده می سازد. این لازم است زیرا پکت ها در حال تاسیس جلسه انتقال و یا انتقال دوباره نمی شوند.

هر هاست بطور رندم یک رشته از اعداد را انتخاب می کند تا در جریان فرستادن و دریافت استفاده شود. و سپس "three-way handshake" به روش زیر ادامه می یابد:

اولین هاست(هاست آ) یک اتصال را برقرار می کند با فرستادن یک پکت با شماره رشته اغازین (X) و بیت SYN تا یک درخواست اتصال را نشان دهد. هاست دوم(هاست ب) SYN را دریافت می کند، شماره رشته X را ضبط می کند، و با تصدیق SYN (با یک ACK = X + 1) هاست ب شماره رشته خودش را شامل می کند (SEQ = Y) . یک ACK = 20 یعنی اینکه هاست بایت های 0 تا 19 را دریافت کرده و انتظار بایت 20 را دارد. این تکنیک تصدیق رو به جلو نامیده می شود. هاست آ سپس تمام بایت هایی را که هاست ب فرستاده است با یک تصدیق رو به جلو نشان می دهد که هاست آ منتظر دریافت (ACK = Y + 1) است. سپس انتقال داده شروع می شود.

چندین خصوصیت که TCP را از UDP جدا میکند:

انتقال داده مرتب – هاست مقصد بر طبق شماره رشته مرتب می کند.

هر پکت تصدیق نشده دوباره فرستاده می شود.

انتقال داده بدون خطا

کنترل جریان- انتقال داده فرستنده را محدود می کند تا تحویل قابل اعتماد را تضمین کند. گیرنده بطور مرتب به فرستنده اعلام می کند چقدر داده را می تواند دریافت کند.(کنترل شده توسط پنجره اسلاید) وقتیکه بافر هاست پر می شود، تصدیق بعدی یک سایز پنجره 0 را می فرستد تا انتقال داده را متوقف کند.

2.User Datagram Protocol (UDP)

UDP یک مدل ساده انتقال است که از دیالوگهای دارای hand-shaking برای فراهم نمودن قابلیت اعتماد، ترتیب، و جامعیت داده استفاده نمی کند، در نتیجه UDP یک پروتکل غیر قابل اعتماد محسوب می شود. بی حالت بودنUDP همچنین برای پاسخ به نیازمندیهای کوچک برای تعداد بسیار زیاد کاربران مفید است. برخلاف TCP ، UDP با انتشار پکت(فرستادن به همه شبکه محلی) و انتشار چندگانه(فرستادن به همه مشترکان) مطابقت دارد.

کاربرد های اشنای اینترنت که از UDP استفاده می کنند: Domain Name System (DNS)، رسانه های جریانی مانند IPTV, Voice over IP (VoIP), Trivial File Transfer Protocol (TFTP) و بسیاری از بازی های روی خط.

کمبود قابلیت اعتماد UDP سبب می شود. کاربردهای اغلب گرایش به میزانی از گمشدن، اشتباه ، و یا تکرار داشته باشند. بعضی از کاربرد ها همانند TFTP ممکن است مکانیزم های ابتدایی قابلیت اعتماد را به لایه کاربرد اضافه کنند. بیشتر مواقع، کاربرد های UDP از مکانیزم های قابلت اعتماد استفاده نمی کنند. و حتی ممکن است بوسیله انان به تعویق بیفتند. رسانه های جریانی، بازی های بلادرنگ چند بازیگری، و voice over IP (VoIP) از کاربرد هایی هستند که از UDP استفاده میکنند.

پروتکل های موجود در لایه کاربرد:

1-BGP (Border Gateway Protocol)

BGP پروتکلی برای انتقال اطلاعات مسیر یابی بین gateway host ها است (هر کدام با روتر خودشان) در شبکه ای از سیستم های خود مختار. BGP پروتکلی است که اغلب بین ها در اینترنت استفاده می شود. جدول مسیر یابی شامل لیستی از روتر های شناخته شده است ، ادرس هایی که می توان به ان ها دست یافت و یک متریک هزینه مطابق با مسیر موجود به هر روتر که بوسیله ان بهترین روتر انتخاب می شود.

هاست ها با استفاده از BGP با پروتکل TCP/IP ارتباط برقرار می کنند و جدول مسیر یابی بروز شده را تنها زمانی که تغییری در ان ایجاد شود می فرستند. و تنها قسمت تاثیر پذیرفته را می فرستند.

با دریافت جدول مسیر یابی، BGP-4 که اخرین ورژن ان است به گرداننده اجازه می دهد متریک هزینه ها را با استفاده از سیاست گذاری های بیان شده پیکر بندی نماید.

BGP با شبکه های محلی خود مختار ارتباط برقرار می کند. حال انکه با خیلی خوب کار نمی کند. روتر های داخل شبکه خود مختار دو جدول مسیر یابی را ذخیره می نمایند یکی برای پروتکل گیت وی داخلی و دیگری برای IBGP .مسیر دهی بین دامنه ای فاقد کلاس Classless Inter-Domain Routing (CIDR) را اسان می سازد که امکان داشتن ادرس های بیشتر درون شبکه نسبت به شمای ادرس ای پی فراهم می کند. نسبت به پروتکل گیت وی خارجی (EGP) جدید تر است.

Dynamic Host Configuration Protocol (DHCP) -2

DHCP نسبت دادن پارامتر های شبکه را به دستگاه های شبکه از یک یا چند سرور DHCP اتوماتیک می نماید. حتی در شبکه های کوچک DHCP مفید است زیرا اضافه کردن یک ماشین به شبکه را اسان می سازد. هنگامیکه یک کلاینت با DHCP پیکر بندی شده به شبکه متصل می شود، کلاینت DHCP یک درخواست اطلاعات لازم از یک سرور DHCP اتشار می دهد. سرور DHCP منبعی از ادرس های ای پی و اطلاعات درباره پارامتر های پیکر بندی کلاینت مانند گیت وی پیش فرض، نام دامنه، نام سرور ها، و سرور های دیگر مثل سرورهای زمانی نگهداری میکند. با دریافت یک درخواست معتبر سرور به کامپیوتر یک ادرس ای پی اختصاص می دهد، یک اجاره (مدت زمان اعتبار ادرس) و دیگر پارامتر های پیکر بندی IP، مانند subnet mask و گیت وی پیش فرض. درخواست عموما سریعا بعد از بوت شدن اغاز می شود و باید قبل از شروع ارتباط مبنی برIP هاست تکمیل شود. راه های متفاوتی برای انجام عملیات DHCP وجود دارد تا جزئیات پیکربندی را به کلاینت فراهم کند، که به سه بخش تقسیم می شود:

به طور اتوماتیک به یک کلاینت یک ادرس دائمی اختصاص دهد.به طور پویا ادرس را برای یک مقدار متناهی از زمان و یا تا وقتی که کلاینت ادرس را رها کند اختصاص دهد.اختصاص دستی که در این مورد گردانندگان سیستم پیکر بندی کلاینت را دستی انجام می دهند(استگاه های کاری واقعی)

در واقعیت کدام یک از اینها استفاده می شوند؟ عموما مورد دوم استفاده میگردد. که برای دلایل مختلفی استفاده می شود، نوعا روی بیشتر شبکه های سازمانی.

Domain Name System (DNS) -**3**

یک سیستم نامگذاری سلسله مراتبی است که روی پایگاه داده های توزیع شده و برای کامپیوترها، سرویس ها و یا هر منبعی که به اینترنت یا یک شبکه محلی نصب شده است ساخته شده است. از همه مهم تر وظیفه ی معنا دار کردن تجهیزات شبکه که بصورت اعداد هستند به انسانها را دارد. برای مثال دامنه نام ***www.example.com*** به ادرس (IPv4) *192.0.32.10* و *2620:0:2d0:200::10* (IPv6) ترجمه می شود.

رکورد های منابع نرمال توسط UDP جستجو می شوند. یک انتقال هوشمندانه مورد استفاده قرار می گیرد، گرچه یکی در پروتکل مشخص نشده است، نتیجه ان مخلوطی از استراتژی های ضعیف و خوب است. خود پروتکل دارای حالت نیست، تمام اطلاعات مورد نیاز در یک پیغام گنجانده می شود. که در RFC1035 کاملا مستندسازی شده است. و دارای فرمت زیر است:

```
+---------------------+
|      Header         |
+---------------------+
|      Question       | the question for the name server
+---------------------+
|      Answer         | RRs answering the question
+---------------------+
|     Authority       | RRs pointing toward an authority
+---------------------+
|     Additional      | RRs holding additional information
+---------------------+
```

سوال ها همیشه نام، نوع، تعداد کلاس ها هستند. برای کاربردهای اینترنت، کلاس IN است، نوع یک نوع معتبر RR است، و نام یک دامنه نام کاملا دارای صلاحیت است.

جواب ها RR هستند که با نام، نوع، تعداد کلاس ها می خورند، اگر هر یک از رکورد های تطابق اشاره گر های به دیگر رکورد ها باشند، رکوردهای هدف نیز باید در جواب جاداده شوند. ممکن است چندین جواب داشته باشیم و یا چندین RR با یک برچسب داشته باشیم.

هویت RR ها از نوع رکورد های سرور نام هستند که به سرور های نامی که به انها نزدیک تر هستند اشاره می کنند. فیلد کاملا اختیاری است، اما کلاینت ها تشویق می شوند تا این اطلاعات را در صوتیکه درخواستهای بعدی محتمل باشد، در کش ذخیره کنند.

افزوده RR ها رکوردهایی هستند که سرور نام باور دارد برای کلاینت مفید است، استفاده بیشتر برای این فیلد فراهم کردن یک ادرس برای سرور های نام لیست شده در بخش هویت است.

File Transfer Protocol (FTP)-4

یک پروتکل استاندارد شبکه برای کپی نمودن یک فایل از یک هاست به دیگری از طریق یک شبکه مبنی بر TCP است. FTP بر مبنای یک معماری کلاینت سروری ساخته شده است، و ارتباط های کنترل و داده بین کلاینت و سرور را بهره برداری می کند. کاربران FTP می توانند خودشان را اعتبار ببخشند با استفاده از یک پروتکل ثبت نام کردن کاملا متنی اما می توانند بطور خود مختار متصل شوند اگر سرور اجازه ان را داده باشد. اولین کاربرد های FTP دارای ابزار های خط-دستوری تعاملی بودند، پیاده ساز استاندارد دستورات و نحو. واسط های کاربری گرافیکی بسیاری تاکنون برای بسیاری از سیستم های عامل مورد استفاده امروزی توسعه داده شده اند.

یک کلاینت یک اتصال TCP را با سرور در پورت 21 ایجاد می کند، این اتصال که اتصال کنترلی نامیده می شود، باز باقی می ماند برای مدت ان جلسه ، با یک اتصال دیگر که اتصال داده نامیده می شود، یا سرور از پورت 20 به یک پورت کلاینت باز(حالت فعال) می کند، ویا کلاینت از یک پورت دلخواه به یک پورت سرور(حالت گذشته) در صورت نیاز برای انتقال فایل داده ایجاد می کند. اتصال کنترل برای گرداندن جلسه بکار برده می شود.(مثل دستورات،شناسه ها، رمزهای عبور) انتقال یافته بین کلاینت و سرور با استفاده از یک پروتکل شبیه TelNet.

Hypertext Transfer Protocol (HTTP) -**5**

پروتکل HTTP یک پروتکل پرسش/ پاسخی است. یک کلاینت یک درخواست را به شکل یک متد درخواست، به سرور می فرستد، URI و ورژن پروتکل، در ادامه ان یک پیغام مثل MIME شامل تصحیح گران درخواست، اطلاعات کلاینت، و محتوای ممکن در یک اتصال با یک سرور.سرور با یک خط حالت پاسخ می دهد، که شامل ورژن پروتکل پیغام و کد موفقیت یا خطا، در ادامه ان یک پیغام شبیهMIME که شامل اطلاعات سرور است، اطلاعات موجودیت و محتوای ممکن درون موجودیت است. بیشتر ارتباط توسط عامل کاربر اغاز می شود که یک درخواست که باید به یک منبع که سرور سرچشمه داده شود، می شود. در ساده ترین حالت توسط یک اتصال ساده(v) بین عامل کاربر(UA) و سرور سرچشمه (O) برقرار می شود.

```
request chain ------------------------>

UA -------------------v------------------- O

<----------------------- response chain
```

جلسه HTTP یک رشته از تراکنش های درخواست-پاسخ شبکه است. یک پیغام درخواست شامل موارد زیر است:

خط درخواست، مثل `GET /images/logo.png HTTP/1.1`

سرخط مثل `Accept-Language: en`

یک خط خالی

یک بدنه پیغام دلخواه

Internet message application protocol (IMAP) -6

یکی از دو پروتکل استاندارد مهم برای ایمیل می باشد، پروتکل دیگر Post Office Protocol (POP) می باشد که بیشتر کلاینت و سرور ها هر دو را پشتیبانی می کنند.IMAP هر دو حالت در خط و خارج از خط را پشتیبانی میکند. IMAP اجازه می دهد که در یک زمان چندین کلاینت بتوانند به مدیریت یک میل باکس بپردازند. ایمیل های دریافتی به یک سرور ایمیل که پیغام ها را ذخیره می کند فرستاده می شوند، کاربر پیغام ها را دریافت می کند با یک ایمیل که از چندین پروتکل باز خوانی ایمیل پشتیبانی می کند. بعضی از کلاینت و

سرور ها ترجیحا از فروشندگان خاص، پروتکل های اولویت بندی شده، اما بیشتر از پروتکل استاندارد اینترنت یا SMTP برای فرستادن ایمیل استفاده می کنند.و از POP و IMAP برای بازخوانی و انجام عملیات متقابل با کلاینت و سرور های دیگر استفاده می کنند.

7- Internet Relay Chat (IRC)

یک فرم از چت یا پیغام متنی بلا درنگ (کنفرانس همزمان) در اینترنت است. که کلا برای ارتباطات گروهی در فروم های بحث که کانال نامیده می شود، طراحی شده است. همچنین امکان ارتباط یک به یک و پیغام خصوصی را نیز می دهد همانطور که امکان چت و به اشتراک گذاشتن داده را دارد.

IRC یک پروتکل باز است و ازTCP ویا اختیاری از TLS استفاده می کند. یک سرور IRC می تواند به دیگر سرور های **IRC** برای گسترش شبکه متصل شود. کاربران با متصل شدن کلاینت به سرور به شبکه IRC متصل می شوند. تعداد زیادی از پیاده سازی ها مانند mlRC یا Xchat برای کلاینت و IRCd اصلی برای سرور استفاده می شوند. بیشترIRC سرور ها نیازی به رجیستر شدن کاربران به یک اکانت ندارند بلکه کاربر احتیاج به انتخاب یک نیک نیم قبل از متصل شدن دارد.

8- Lightweight Directory Access Protocol (LDAP)

یک پروتکل کاربردی برای خواندن و تصحیح کردن دایرکتوری ها در یک شبکه IP است. یک دایرکتوری در این صحنه یک مجموعه سازماندهی شده از رکورد ها است مثلا یک دایرکتوری تلفن یک لیست الفبایی از افراد است با یک ادرس و شماره تلفن در هر رکورد. اخرین ورژن ان 3 است.

9- Network News Transfer Protocol(NNTP)

سرویس دسترسی به گروه های خبری(News Groups) ، به زبان ساده NNTP سرویس است برای دسترسی به اطلاعاتی که توسط افراد مختلف ارسال شده و مشترکاً مورد استفاده قرار می گیرد . این سرویس نیز از دو قسمت تشکیل شده

الف : NNTP Client (که به News Client نیز معروف است.

ب : NTTP Server (که به NTTP Server نیز مشهور است.

روال کار بدین صورت است که ابتدا توسط News Client به یک News Server متصل شده سپس گروه خبری را انتخاب و در آن عضو می شویم (Subscribe) پس از عضویت در گروه خبری ، اطلاعات و اخبار متنوع در زمینه ی مورد نظر از سرور به گیرنده انتقال پیدا می کند.

با توسعه مشترکان شبکه های محلی و اینترنت، این امر برای خوانندگان روزنامه برای اجرا شدن روی شبکه های محلی مورد استقبال قرار گرفت. از انجائیکه سیستم های توزیع شده هنوز به خوبی رشد نکرده بودند، یک پروتکل جدید بر پایه مدل کلاینت – سرور توسعه یافت. که شباهت به SMTP دارد، اما برای مقاله های روزنامه سازمان داده شده است.

پورت TCP 119 برای NNTP رزرو شده است، هنگامیکه کلاینت به سرور خبری با پروتکل Transport Layer Security (TLS) متصل می شوند. پورت TCP 563 مورد استفاده قرار می گیرد. که گاهی اوقات به NNTP اشاره می کند.

10- Network Time Protocol (NTP)

پروتکلی برای همزمان سازی کلاک های سیستم های کامپیوتری بر روی شبکه های پکت-سوئیچ و تاخیر-متغیر می باشد. بطور خاص برای مقاومت در برابر اثرات تاخیر متغیر با استفاده از بافر جیتر طراحی شده است. NTP از پروتکل UDP روی پورت 123 استفاده می کند.

NTP از الگوریتم مارزولا استفاده می کند، و شامل ویژگی های پشتیبانی مانند ثانیه های پرشی دارد. NTP ورژن 4 می تواند زمان را در اینترنت عمومی تا 10 میلی ثانیه نگهداری کند. و می تواند دقت 200 میکروثانیه یا بهتر در شبکه های محلی و در شرایط ایده ال داشته باشد.

NTP زمان جهانی را هماهنگ می کند. هیچ اطلاعاتی در مورد نواحی زمانی و ذخیره سازی زمان روز ندارد. این اطلاعات خارج از محدوده ان است و باید بطور جدا جمع اوری شود. در شبکه های محلی منفرد می تواند با قاعده کلی برای یک مقیای زمانی دیگر توزیع شود اما این غیر معمول است.

پیاده سازی NTP در نرم افزار:

Unix: برای سیستم های مدرن Unix کلاینت NTP بعنوان یک فرایند اهریمنی که بطور پیوسته در فضای کاربر اجرا می شود پیاده سازی شده است. به دلیل حساسیت به زمانبندی پیاده سازی استاندارد کلاک حلقه فاز –قفل شده NTP در هسته مرکزی اهمیت دارد. تمامی ورژن های Linux, BSD, Mac OS X, Solaris وAIX در این روش پیاده سازی شده اند.

Microsoft Windows: تمامی ورژن هایMicrosoft Windows 2000 قابلیت همزمانی کلاک کامپیوتر با سرور را دارند.

Post Office Protocol (POP) –11

یک پروتکل استاندارد لایه پروتکل است که توسط کلاینت های ایمیل برای بازخوانی ایمیل از یک سرور راه دور استفاده می شود. POPوIMAP دو پروتکل استاندارد رایج اینترنت هستند که برای بازخوانی ایمیل استفاده می شوند. بیشتر سرویس های وب ایمیل مانند Hotmail, Gmail and Yahoo! Mail از POP3 استفاده می کنند.

POP از نیازمندیهای ساده بارگذاری و حذف حمایت می کند. با وجود اینکه بیشتر کلاینت های POP اختیار رها کردن ایمیل روی سرور بعد از بارگذاری را دارند، کلاینت های POP معمولا متصل شده ، تمام پیغام ها را بازیابی می کنند، ان را روی کامپیوتر کاربر ذخیره می کنند، و از سرور پاک می کنند و سپس اتصال را قطع می کنند. بقیه پروتکل ها، بطور برجسته IMAP عملیات از راه دور کامل و پیچیده تری را ارائه می دهد. با این حال کمتر Internet Service Providers (ISPs) هایی از IMAP حمایت می کنند.

Routing Information Protocol (RIP) - 12

RIP یک پروتکل مسیر یابی دینامیک می باشد که در شبکه های محلی و نواحی بزرگ استفاده می شود. که به عنوان interior gateway protocol (IGP) کلاس بندی می شود. و از الگوریتم مسیریابی distance-vector استفاده می کند. با اینکه این توسط تکنیک های پیشرفته همچون Open Shortest Path First (OSPF) و OSI protocol IS-IS منسوخ شده است هنوز هم مورد استفاده قرار می گیرد. همچنین با شبکه های IPv6 منطبق شده است.

RIP از الگوریتم مسیریابی distance-vector استفاده می کند که تعداد هاپ را بعنوان متریک مسیریابی بکار میگیرد. زمان نگهداری 180 ثانیه است. RIP ماکسیسم تعداد هاپ ها را 15 در نظر می گیرد. این محدودیت همچنین سایز شبکه هایی که RIP می توان پشتیبانی کند را محدود می کند. یک شماره هاپ 16 یک فاصله بینهایت در نظر گرفته می شود.

اصولا هر روتر تمامی بروزرسانی ها را هر 30 ثانیه انتقال می دهد. در هر استقرار اولیه، جدول های مسیر یابی به اندازه کافی کوچک هستند تا ترافیک مهم نباشد. با رشد شبکه ها در سایز اشکار است با سیلاب هر 30 ثانیه ای ترافیک شدیدی ایجاد می شود. حتی اگر روتر ها در زمان های تصادفی آغاز شوند. تصور می شد در نتیجه آغاز تصادفی بروز رسانی ها ممکن بود در زمان پخش شود، اما در عمل اینگونه نبود.

remote procedure call (RPC) – 13

یک ارتباط بین فرایندی است که به یک برنامه کامپیوتر اجازه می دهد تا سبب شود تا یک زیرروتین یا رویه بدون برنامه ریزی صریح جزئیات کد برای این تعامل از راه دور در یک فضای ادرسی دیگر کارکند(معمولا روی یک کامپیوتر در شبکه به اشتراک گذاشته شده). یعنی، برنامه نویس اصولا همان کدی را که زیر روتین محلی، و یا از راه دور ، اجرا می کند، می نویسد. هنگامیکه برنامه مورد سوال از مفاهیم شی گرا استفاده می کند به RPC ، remote invocation یا remote method invocation ، می گویند.

یک RPC با یک کلاینت اغاز می شود، که یک پیغام درخواست را به یک سرور از راه دور شناخته شده برای اجرای یک رویه خاص بدون پارامتر های فراهم شده می فرستد. سرور از راه دور یک پاسخ به کلاینت می فرستد و کاربرد به فرایندش ادامه می دهد. تعداد بسیاری از متغیر ها و زیر نویس ها در پیاده سازی های متفاوت وجود دارند، که نتیجه ان وجود انواع مختلفی از پروتکل های RPC است. هنگامیکه سرور در حال پردازش فراخوانی است، کلاینت بلاک می شود (صبر می کند تازمانیکه سرور پردازش اش را قبل از بازگشت به اجرا تمام کند.)

یک تفاوت مهم بین فراخوانی رویه های از راه دور و فراخوانی های محلی انستکه فراخوانی های از راه دور ممکن است بخاطر مشکلات غیر قابل پیش بینی شبکه رد شوند. همچنین فراخواننده باید با چنین شکست هایی بدون دانستن اینکه رویه از راه دور به درستی احضار شده است یا نه کنار بیاید.

Real-time Transport Protocol (RTP) – 14

یک فرمت استاندارد از پکت را ارائه می دهد که برای بردن تصویر و صدا روی شبکه های IP تعریف می کند. RTP بطور گسترده در ارتباطات و تفریحات که شامل رسانه های جریانی مانند تلفنی و کنفرانس ویدئویی و ویژگی های بزن- تا- حرف بزنی تحت وب، می شود مورد استفاده قرار می گیرد.

RTP در پیوند با RTP Control Protocol (RTCP) استفاده می شود. در حالیکه RTP جریان های رسانه را حمل می کند. RTCP برای به تصویر کشیدن امار و کیفیت سرویس استفاده می شود و کمک به همزمان سازی جریان های چندتایی می کند. زمانیکه هر دو پروتکل در پیوند استفاده می شوند، RTP از شماره های پورت زوج سرچشمه می گیرد و دریافت می شود وRTCP با شماره پورت های فرد بعدی بکار می رود.

یکی از پایه های تکنیکی Voice over IP می باشد و در این محتوا معمولا در پیوند با یک پروتکل سیگنال کننده که تلاش برای برقراری ارتباطات در شبکه می کند استفاده می شود.

مولفه های پروتکل :

خصوصیات RTP دو زیر پروتکل را تعریف میکند:

پروتکل انتقال داده RTP که با انتقال داده بلادرنگ سر و کار دارد. اطلاعات فراهم شده با این پروتکل شامل استمپ های زمان (برای همزمان سازی) شماره های رشته (برای گمشدن پکت و مرتب سازی دریافت) و فرمت سربار که فرمت داده کد گذاری شده را نشان می دهد.

یک پروتکل که برای تشخیص کیفیت سرویس و همزمان سازی بین جریان های رسانه بکار می رود. ترافیک پهنای باند در مقایسه با RTP کوچک است نوعا 5٪ .

یک سیگنال اختیاری مانند H.323, MGCP, Megaco, SCCP, or Session Initiation Protocol (SIP) signaling protocols

یک توصیف رسانه اختیاری مانند session description protocol

15 – Simple Network Management Protocol (SNMP)

یک پروتکل استاندارد اینترنت برای مدیریت دستگاه ها روی شبکه های IP است. دستگاه های رایجی که SNMP پشتیبانی می کند روتر ها، سوئیچ ها، سرور ها، ایستگاه های کاری، پرینتر ها، و راک های مدرن و ... هستند. معمولا در سیستم های مدریریتی شبکه برای به تصویر کشاندن دستگاه های متصل به شبکه جهت وضعیت های مورد نیاز به توجه سرپرست بکار می رود. شامل استاندارد هایی از مدیریت شبکه است از جمله پروتکلی از لایه شبکه، یک شمای پایگاه داده ای ، و یک مجموعه از اشیا داده ای .

16 – Secure Shell (SSH)

یک پروتکل شبکه است که به داده اجازه می دهد تا در یک کانال امن بین دو دستگاه شبکه شده جابجا شود. بطور اولیه در Linux و Unix استفاده می شد تا به اکانت های شل دستیابی کند. جایگزینی برای Telnet و دیگر شل های از راه دور بدون ایمنی، که

اطلاعات را می فرستند بطور برجسته رمز های عبور، در متن خالی، تحویل اماده انها برای انالیز پکت، طراحی شده است. رمز نگاری در SSH قصد دارد اطمینان و جامعیت داده روی یک شبکه غیر ایمن مانند اینترنت را فراهم کند.

SSH از رمز نگاری با کلید عمومی استفاده می کند تا کامپیوتر از راه دور را هویت شناسی کند و به کامپیوتر از راه دور اجازه می دهد تا کاربر را در صورت لزوم، هویت شناسی کند.

Telnet – 17

Telnet یک پروتکل شبکه است که روی اینترنت یا شبکه های محلی برای فراهم نمودن امکانات ارتباطات مبتنی بر وب تعامل دوسویه با استفاده از اتصال پایانه مجازی بکار می رود. داده کاربر در – باند با کنترل اطلاعات در یک اتصال داده ای 8- بیتی مبتنی بر بایت روی یک Transmission Control Protocol (TCP) پراکنده می شود.

به طور تاریخی Telnet دستیابی به واسط کاربری دستور – خط را روی یک هاست از راه دور فراهم می کند(معمولا روی یک سیستم عامل). بیشتر تجهیزات شبکه و سیستم های عامل با یک استک TCP/IP از سرویس Telnet برای پیکر بندی از راه دور استفاده می کنند. (شامل سیستم های مبتنی بر Windows NT)

اصطلاح Telnet ممکن است همچنین به نرم افزاری که مخش کلاینت را از پروتکل را پیاده سازی می کند اشاره کند.کاربرد های کلاینت Telnet بطور مجازی برای تمامی سکو ها کامپیوتری قابل دسترس هستند.Telnet همچنین به عنوان یک فعل استفاده می شود. Telnet کردن یعنی یک اتصال را تاسیس کردن با پروتکل Telnet یا با دستور- خط و یا با یک واسط کاربری برنامه ریزی شده. برای مثال یک رهنمود ممکن است " تغییر رمز عبور، Telnet به سرور، لاگین و اجرای دستور رمز عبور" باشد. اغلب اوقات یک کاربر با یک سیسیتم سرور شبیه یا یک دستگاه شبکه (مانند یک روتر) Telnet می کند. و به یک اعلان لاگین به یک واسط کاربری مبتنی دستور خط و یا مدیر صفحه – کامل مبتنی بر کامپیوتر دستیابی پیدا می کند.