دانشگاه شهید مدنی آذربایجان

Computer Networks

شبکه های کامپیوتری

دانشگاه شهید مدنی آذربایجان

دانشکده فناوری اطلاعات و مهندسی کامپیوتر

دکتر محسن حیدریان

اسلایدهای درس شبکه های کامپیوتری

معماری اینترنت

کارشناسی ارشد مهندسی فناوری اطلاعات

ترم اول ۱۴۰۳

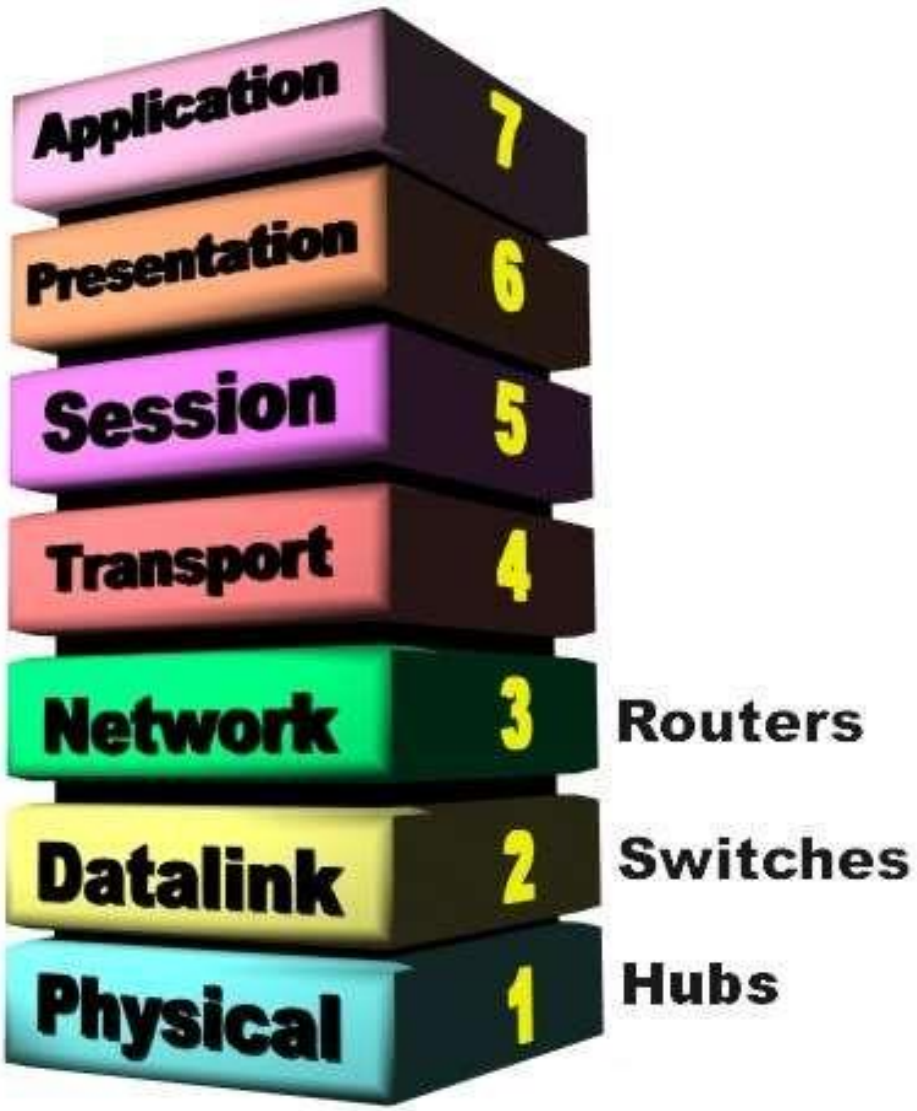
انواع معماری شبکه

به غیر از معماری OSI، معماری های دیگری هم نظیر TCP\IP وجود دارند که شامل همه لایه ها و وظایف OSI هستند، اما نحوه لایه بندی و پروتکل بندی آنها متفاوت است. تعدادی از این لایه ها بر اساس دیدگاههای عملی و پیاده سازی تدوین و تکمیل شده اند و تعدادی دیگر نیز بر اساس مفاهیم و مدلهای انتقال داده شکل گرفته اند.

در شبکه هایی که مدرن هستند و اخیرا به وجود آمده اند، مانند شبکه ATM که برای هدایت داده ها در شاه راههای داده به کار می روند، معماری شبکه، اندازه بسته، نوع خدمات و نوع لایه ها بسیار متفاوت است.

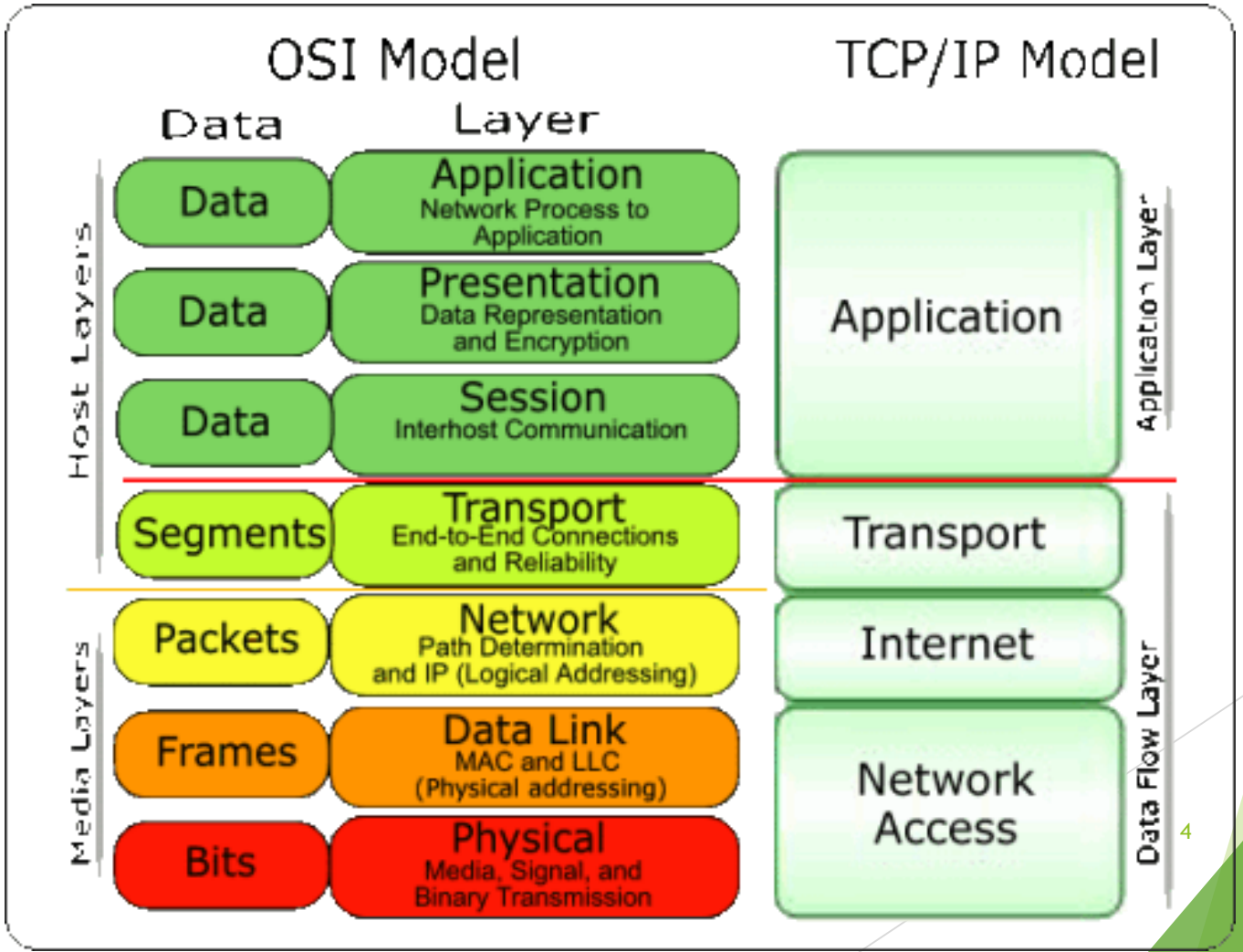
در شبکه های دیگری مانند شبکه های مالتی مدیا، نوع لایه ها برای خدمات با کیفیت بالا مدلسازی شده و کمتر سازگار با مدل مرجع OSI هستند.

یادآوری معماری OSI



مقایسه معماری اینترنت و معماری OSI

معماری اینترنت ۴ لایه است که به شرح زیر با معماری OSI معدل سازی می شود:



تشریح معماری اینترنت

لایه Application: این لایه معادل ۳ لایه کاربرد و ارایه و نشست در مدل OSI است. در واقع این لایه از اینترنت هم می تواند فرامین کاربر را دریافت کند و هم می تواند تبدیل داده انجام داده و هم می تواند نشست لازم بین مبدا و مقصد را تشکیل و مدیریت کند. پروتکل SMTP در لایه کاربرد اینترنت می تواند همه وظایف بالا برای دریافت ایمیل از کاربر و ارسال آن به مقصد را انجام دهد.

لایه Transport: همان لایه حمل در مدل OSI است که توسط دو پروتکل TCP و UDP اجرا می شود.

لایه Internet: همان لایه Network در مدل OSI است که توسط پروتکل IP پیاده سازی می شود.

لایه Access : معادل دو لایه Data Link و Physical در مدل OSI است و روشهایی را برای ارسال سیگنالهای داده بدون خطا از مبدا به مقصد ارایه می کند. این لایه رسانه انتقال را کنترل می کند. نمونه ای از این لایه، خط ADSL یا ISDN است.

مقایسه معماری اینترنت و معماری OSI

مشکلات معماری OSI در عمل: این مدل بیشتر بر روی کتاب و به صورت مفهومی ارائه شده است. این مدل بسیار کامل اما کاملا مفهومی است و البته برای تشریح مفاهیم شبکه بسیار کارامد است. اما برای ساخت تجهیزات شبکه و داشتن یک رویکرد عملی، ضعیف است و موجب گسستگی استانداردهای شبکه شده است.

دلایل پیدایش معماری TCP\IP: این مدل در عمل و کم کم شروع به ظهور کرد و در یک رویکرد عملی، برای استاندارد کردن و یکنواخت کردن شبکه ها و تجهیزات شبکه ای به کار گرفته شد. این لایه ابتدا در عمل به وجود آمد و سپس بر روی کاغذ به صورت مفهومی مستند سازی شد.

مشکل عدم رعایت استانداردها: شبکه اینترنت یک استاندارد جهانی برای به هم پیوستن شبکه های دیگر است. در واقع مدل TCP\IP را شبکه ای از شبکه ها می نامند.

مفهوم استانداردهای اینترنتی

با توجه به اینکه فناوری ها و خدمات شبکه های کامپیوتری بسیار متنوع و گوناگون هستند، در بسیاری از موارد ارایه خدمات مشترک بین این فناوری ها ممکن نیست. لذا برای حل این مشکل لازم است استانداردهایی ابداع شوند. با رعایت کردن این استانداردها، بخش مهمی از این ناهماهنگی ها از بین رفته و فناوری های مختلف شبکه ای می توانند با یکدیگر نبادل اطلاعات کنند.

در ادامه مروری بر استانداردها و موسسات استانداردگذاری اینترنت خواهیم داشت.

مفهوم استانداردهای صنعتی

یک استاندارد شامل تعاریف، قوانین و داده هایی است که یک محصول یا یک پدیده باید در آنها صدق کند تا بتوانیم در مورد ویژگی های کمی و کیفی محصولات مقایسه، ارزیابی، تایید یا رد داشته باشیم. برای اینکه تشخیص دهیم یک محصول در یک استاندارد صدق می کند یا نه، باید مجموعه تستهای مرتبط با استاندارد را بر روی محصول اجرا کنیم.

استاندارد را به نوعی زبان مشترک بین محصولات و پدیده ها هم می نامند. امروزه در همه حوزه های مهندسی، مدیریت، آموزش، ورزش، تغذیه، مصرف انرژی و غیره استانداردهای متنوع، متعدد و لازمی را به صورت شرکتی، ملی و جهانی ابداع کرده اند.

مثلا در حوزه فولاد به ASTM A6 بر خواهیم خورد که به مشخصات کلی انواع محصولات فولادی نورد شده می پردازد که اصطلاحا به آن، Basic Standard یا استاندارد پایه گفته می شود. از سوی دیگر ASTM C168 اصطلاحات و واژه های مرتبط با عایق حرارتی را بیان می کند که به اینها Terminology Standard یا استاندارد واژه شناسی می گویند. ASTM E23 را داریم که مربوط به چگونگی انجام آزمایش ضربه است و در دسته ی Testing Standard یا استاندارد آزمون جای می گیرد. ممکن است استاندارد به ویژگی های یک محصول بپردازد مانند ASTM D1785 که در مورد لوله های پلاستیکی است و Product Standard یا استانداردمحصول نامیده می شود.

سازمانهای استاندارد گذاری جهانی

استاندارد ISO

نمایندگان ۲۵ کشور در تاریخ ۱۴ اکتبر ۱۹۴۶ میلادی برابر با ۲۲ مهر ماه ۱۳۲۵ خورشیدی در لندن گرد هم آمدند و پس از مذاکرات طولانی سرانجام برای تاسیس سازمان بین المللی استاندارد ISO که کوتاه شده International Organization for Standardization است توافق نمودند. این سازمان رسما" در فوریه ۱۹۴۷ در شهر ژنو سوئیس کار خود را آغاز نمود. زمینه فعالیتهای سازمان ISO دارای هیچگونه محدودیتی نیست و در برگیرنده کلیه شاخه های تخصصی است و تنها در خصوص برق و الکترونیک که بر عهده IEC است، فعالیت نمی کند. تا سال ۲۰۲۰ میلادی ISO بیش از ۲۳۰۰۰ نسخه منتشر کرده است. همه ساله ۲۲ مهر به عنوان روز جهانی "استاندارد" گرامی داشته می شود.

مفهوم استانداردهای شبکه IEEE

در اولین روز سال ۱۹۶۳ میلادی مؤسسه Institute of Electrical and Electronics Engineers که به اختصار IEEE نامیده می شود، از به هم پیوستن دو رقیب به اسم AIEE و IRE در زمینه مهندسی های برق و کامپیوتر شروع به فعالیت کرد.

موسسه AIEE یا مؤسسه مهندسان برق و IRE مؤسسه مهندسان رادیو، دو مؤسسه آمریکایی بودند که سرانجام تبدیل به IEEE شدند. AIEE در سال ۱۸۸۴ بنیانگذاری شد. این مؤسسه توسط برخی از مخترعین بزرگ حوزه برق از جمله آنها "توماس ادیسون"، "نیکلا تسلا"، "الیهو تامسون"، "ادوارد وستون" و "ادوین هوتسون" بنیانگذاری شد. IRE نیز در سال ۱۹۱۲ بنیانگذاری شد. این مؤسسه از همکاری دو مؤسسه مهندسان تلگراف و مؤسسه بی سیم، به وجود آمد.

IEEE 488 به عنوان استاندارد یا کانکتور برای بخش I/Oدستگاه های IBM که فلش، چاپگر و ... به آن متصل میشد. به این کانکتور GPIB و HP-IB نیز می‌گفتند.

IEEE 802 به عنوان استاندارد شبکه های LAN تا MAN می باشد. همچنین بحث اصلی این استاندارد در لایه های Physical و Data Link از هفت لایه شبکه OSI می‌باشد. این استاندارد شامل زیر استانداردهای صفحه بعد می باشد:

IEEE 802 زیر استانداردهای

IEEE 802.1	Standards for LAN/MAN bridging and management and remote media access control (MAC) bridging
IEEE 802.2	Standards for Logical Link Control (MAC) standards for connectivity
IEEE 802.3	Ethernet Standards for Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
IEEE 802.4	Standards for token passing bus access
IEEE 802.5	Standards for token ring access and for communications between LANs and MANs
IEEE 802.6	Standards for information exchange between systems
IEEE 802.7	Standards for broadband LAN cabling
IEEE 802.8	Fiber-optic connection
IEEE 802.9	Standards for integrated services, like voice and data
IEEE 802.10	Standards for LAN/MAN security implementations
IEEE 802.11	Wireless Networking – "WiFi"
IEEE 802.12	Standards for demand priority access method
IEEE 802.14	Standards for cable television broadband communications
IEEE 802.15.2	Bluetooth
IEEE 802.15.4	Wireless Sensor/Control Networks – "ZigBee"
IEEE 802.15.6	Wireless Body Area Network[15] (BAN) – (e.g. Bluetooth low energy)
IEEE 802.16	Wireless Networking – "WiMAX"

شرح لایه ها و پروتکل های معماری اینترنت

TCP/IP مخفف Transmission Control Protocol / Internet Protocol می باشد. معنی لغوی آن یعنی پروتکل کنترل انتقال / پروتکل اینترنت می باشد.

TCP/IP پروتکل اولیه ارتباط به اینترنت است. مدل TCP/IP یا مدل مرجع اینترنتی که گاهی مدل مرجع ARPANET نامیده می شود، در سال ۱۹۷۰ به وسیله DARPA طراحی شده است.

لایه کاربرد: معادل سه لایه کاربرد، ارائه و نشست در مدل OSI است. این لایه شامل نرم افزارهایی است که وظیفه هر سه لایه بالا را انجام می دهند.

لایه حمل: شامل دو پروتکل مهم TCP و UDP است که سرویسهای مطمئن و تصدیق شده و برعکس غیر مطمئن و تصدیق نشده را ارئه می کنند.

لایه اینترنت: شامل پروتکل مهم IP است که آدرس دهی کامپیوترها و مسیریابی را به عهده دارد.

لایه دسترسی: که شامل دو زیرلایه پیوند داده و لایه فیزیکی است. این لایه در اینترنت تجمیع شده است و فناوری های تجمیع شده ای را شامل می شود.

پروتکل های معماری اینترنت

مدل شبکه TCP/IP پروتکل های خود را در ۴ لایه دسته بندی کرده است که از پایین به بالا عبارتند از:

Application: پروتکل هایی مانند DHCP، DNS، FTP، HTTP، IMAP در این لایه قرار دارند. این لایه بالاترین سطح سرویس های اینترنت برای انتقال اطلاعات را فراهم می سازد (با استفاده از سرویس های لایه های پایین تر) و باعث می شوند ما براحتی با سرویس های لایه های پایینی کار کنیم.

Transport: پروتکل هایی مانند TCP و UDP در این لایه قرار دارند. این لایه سرویس انتقال پیغام ها بین برنامه هایی که برروی سیستم های remote قرار دارند را فراهم می سازد.

Internet : پروتکل هایی مانند ICMP، IPv4و IPv6 در این لایه قرار دارند. این لایه مکانیزم هایی برای ارتباطات بین سیستمی، کنترل مسیر یابی پیغام ها، چک کردن صحت validity checking و ترکیب و تجزیه header پیغام ها را فراهم می آورد.

Network Interface / Access : پروتکل هایی مانند Ethernet و PPP در این لایه قرار دارند. این لایه پایین ترین سطح انتقال اطلاعات را بر عهده دارد و امکاناتی برای تبادل اطلاعات از طریق سخت افزار شبکه را فراهم می آورد.

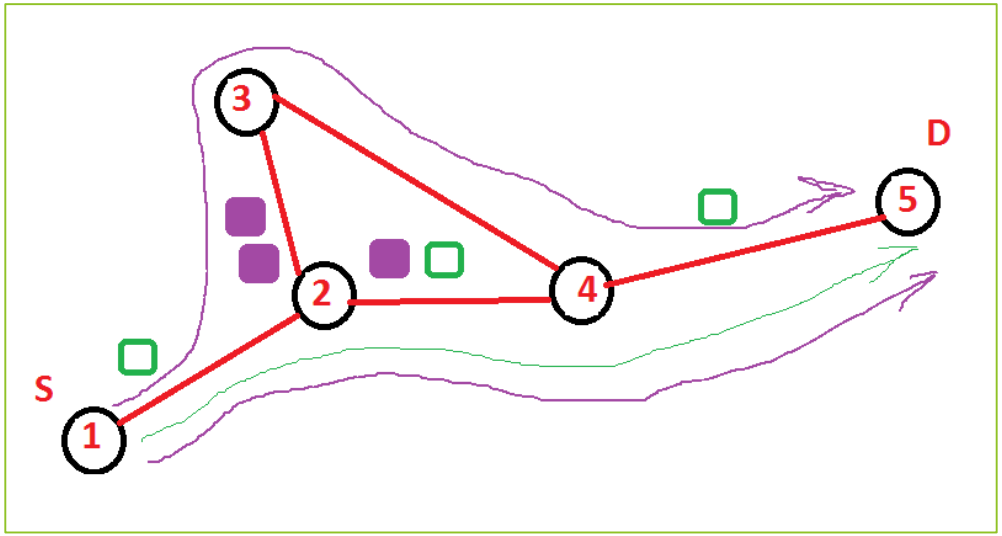
معرفی پروتکل های مهم اینترنت

پروتکل TCP یک پروتکل Connection Oriented یا اتصال گرا است و بدین معناست که تحویا دادن سالک و گامل اطلاعات ارسالی برای این پروتکل بسیار مهم است و از جهتی سرعت آن نسبتا پایین است. برعکس پروتکل UDP به ترتیب و صحت ارسال و دریافت بسته ها بی تفاوت است.

پروتکل IP یک پروتکل Connection Less یا غیر اتصال گرا است که بدین معناست صحت داده های ارسالی چندان مهم نیست و سرعت بیشتر مد نظر است. در شبکه های مبتنی بر TCP بیت به بیت داده ها بعد از انتقال در شبکه بررسی می شود و همین دلیل کندی آن است، در صورتیکه در شبکه های IP سرعت ارسال مهم است. پشته پروتکل TCP/IP نقاط ضعف هر یک از این دو پروتکل را پوشش داده است و یک پروتکل ترکیبی خوبی ایجاد کرده است.

اینترنت زیرساخت ارتباطی شبکه های جهانی است. بدین معنا که همه فناوری های مختلف شبکه باید بسته های خود را تحویل TCP\IP دهند.

تشریح لایه شبکه و حمل بر روی یک توپولوژی



تشریح بسته های سبز: فقط قرار است از طریق مسیر <1,2,4,5> به سمت مقصد بروند.

بسته های بنفش: از دو مسیر متفاوت <1,2,4,5> و <1,2,3,4,5> به سمت مقصد خواهند رفت.

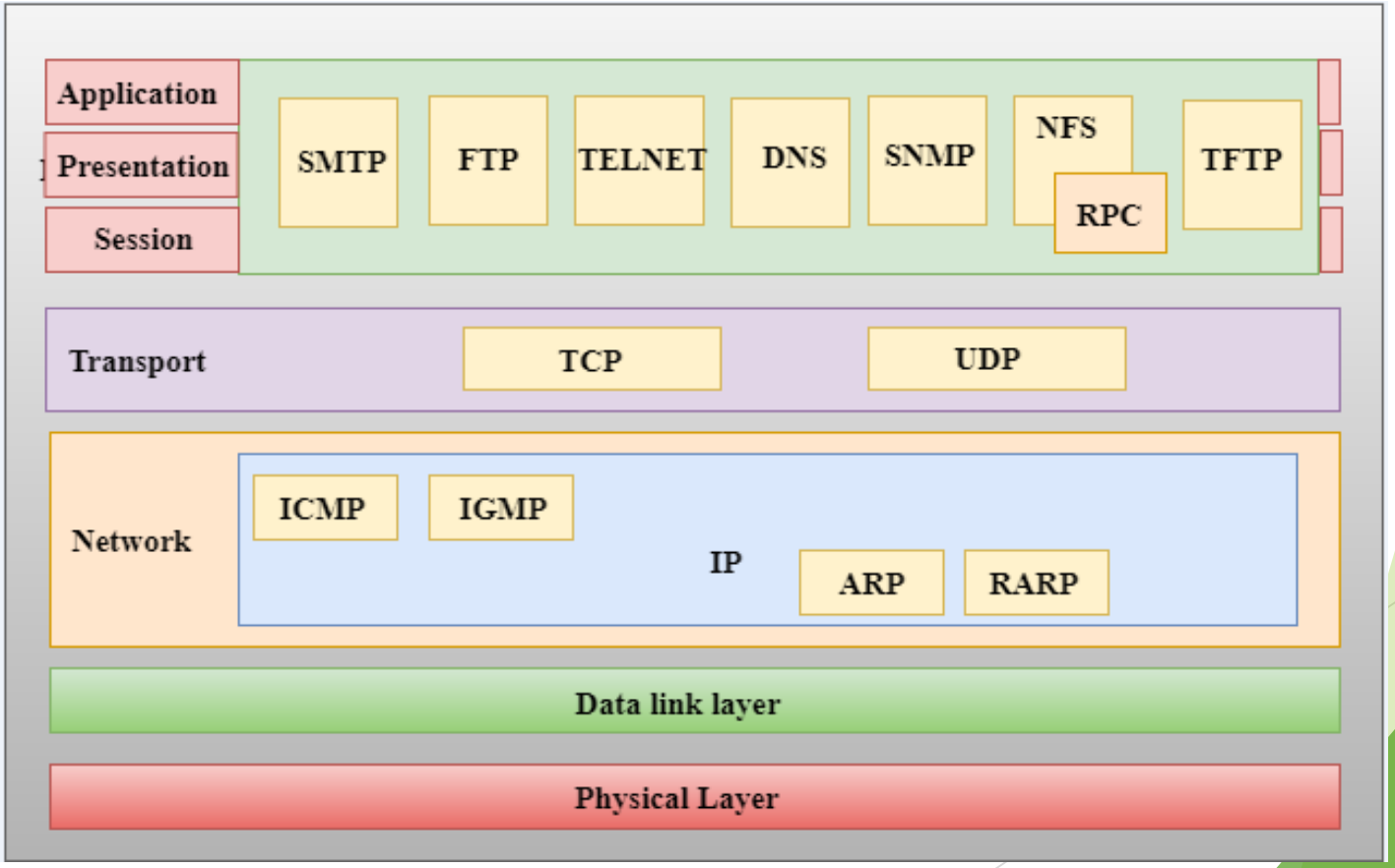
مسیرها و گره ها: یک مسیر از تعدادی گره متوالی تشکیل می شود که با اتصالات به هم متصل هستند

توپولوژی شبکه: گراف همبندی اجزای شبکه را توپولوژی می نامند

تطبیق این توپولوژی با معماری شبکه TCP\IP : پروتکل های مسیریابی، توپولوژی شبکه و مسیرها را را مشخص می کنند و پروتکل TCP هم در طول این مسیرها به بسته ها خدمات می دهند. در شکل بالا تفاوت بین خدمات لایه حمل و لایه شبکه دیده می شود.

پروتکل های اینترنت: پشته اینترنت

در شکل زیر تعدادی از مهمترین پروتکل ها و فناوری های اینترنت ارائه شده است:



عملکرد لایه ها

معماری TCP/IP پشته ای از پروتکل هاست. در هر لایه مجموعه ای از پروتکل ها را داریم. هر پروتکل عملیات خاصی انجام می دهد. مثلا صفحه ای را در مرورگر باز می کنیم. دیتا ارسال می شود و در لایه Application از پروتکل HTTP استفاده می کند و داده را به لایه پایین تر ارسال می کند و حتما در ارسال داده باید لایه ها به صورت ترتیبی طی شود. در هر لایه حتما باید یک پروتکل را انتخاب کند. مثلا در لایه Transport از پروتکل TCP استفاده می کند یا UDP و غیره.

در لایه transport مفهومی به نام پورت داریم، که از ۱تا ۶۵۵۳۵ عددگذاری شده، و به هربسته ای که از مبدا خارج می شود عددی به نام آدرس پورت اختصاص داده می شود.

بنابراین هر بسته ای که از کامپیوتر فرستنده ارسال می شود، دو آدرس پورت خواهد داشت، آدرس پورت فرستنده و آدرس پورت گیرنده. آدرس پورت سرویس دهنده باید ثابت باشد. که شماره پورت آن عددی از ۱ تا ۱۰۲۴ یا از ۱۰۲۴ تا ۴۹۱۵۱ (برای انتخاب بازه هم معیارهایی وجود دارد که در این مبحث نمی گنجد.) است. Application هایی که سرویس می گیرند دارای شماره پورتی در بازه ۴۹۱۵۱ تا ۶۵۵۳۵ است که عددی تصادفی است که توسط سیستم عامل تولید می شود.

تفاوت شماره Port با شماره IP

شماره پورت عددی بین ۰ تا ۶۵۵۳۵ است و توسط لایه حمل یا TCP و UDP به کار برده می شود. شماره پورت به یک برنامه کاربردی تخصیص می شود. اگر بین دو کامپیوتر، ۲ برنامه کاربردی مانند http و smtp در حال اجرا باشند، به بسته های هر کدام یک شماره پورت جداگانه تخصیص می شود تا مشخص شود که این بسته ها متعلق به دو پروتکل کاربردی یا دو برنامه کاربردی متفاوت هستند. شماره پورت هیچ ارتباطی با مسیرهای شبکه و کامپیوترها و آدرسهای آنها ندارد.

شماره IP یک عدد ۳۲ بیتی است و توسط لایه شبکه تولید می شود و مانند کد پستی یک ساختمان، منتحصر به فرد است و برای یافتن آن ساختمان در کشور یا کل جهان توسط اداره پست به کار می رود! توجه شود که کد پستی دقیقا آدرس یک ساختمان را در یک کشور مشخص می کند. شماره IP برای مسیریابی و پیش راندن بسته از میدا به مقصد استفاده می شود و ربطی به برنامه های کاربردی ندارد.

با تلفیق Port number و IP number شبکه اینترنت موفق می شود بسته های یک برنامه کاربردی را به یک کامپیوتر مقصد تحویل دهد و برنامه ها و کامپیوتر ها اشتباه در نظر گرفته نشوند.

تعدادی شماره پورت مهم قابل استفاده در پروتکل های اینترنت

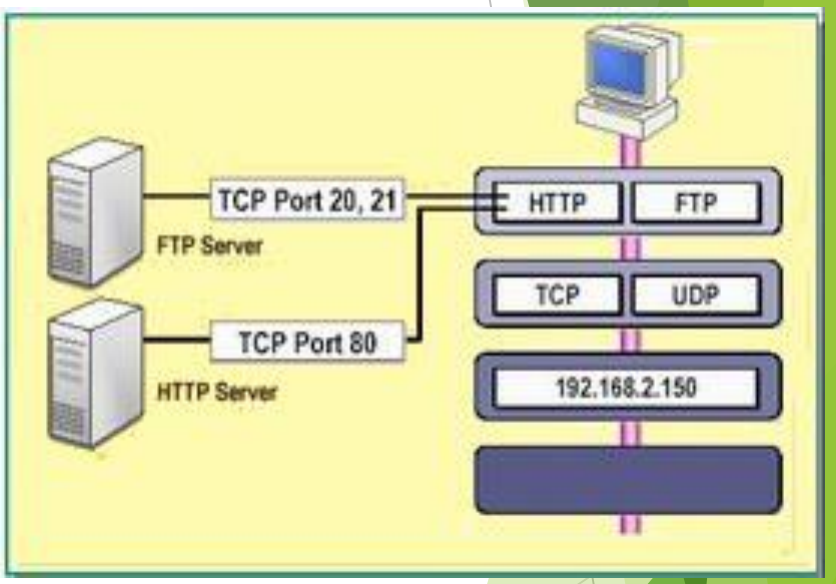
در جدول زیر دیده کی شود که که کدام پروتکل های لایه کاربرد توسط کدام پروتکل های لایه حمل و با کدانم شماره پورت در اینترنت سرویس دهی می شوند.

Label on Column	Service Name	UDP and TCP Port Numbers Included
DNS	Domain Name Service – UDP	UDP 53
DNS TCP	Domain Name Service – TCP	TCP 53
HTTP	Web	TCP 80
HTTPS	Secure Web (SSL)	TCP 443
SMTP	Simple Mail Transport	TCP 25
POP	Post Office Protocol	TCP 109, 110
SNMP	Simple Network Management	TCP 161,162 UDP 161,162
TELNET	Telnet Terminal	TCP 23
FTP	File Transfer Protocol	TCP 20,21
SSH	Secure Shell (terminal)	TCP 22
AFP IP	Apple File Protocol/IP	TCP 447, 548

تفاوت خدمات در لایه حمل اینترنت

تفاوت های دو لایه TCP و UDP در شکل زیر ارائه شده است. هر کدام از این پروتکل ها در خدمات خاص خودشان کاربرد دارند. از UDP برای انتقال آنلاین و از TCP برای دانلود فیلم می توان استفاده کرد. شکل سمت چپ ویژگی های دو پروتکل TCP و UDP را نشان می دهد و شکل سمت چپ هم نشان می دهد که لایه حمل چگون به کاربردهای مختلف خدمات می دهد. همچنین نحوه تعامل یک آدرس IP را هم نشان می دهد.

TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement



تشریح ویژگی های TCP و UDP

ویژگی Reliable: یعنی همه بسته ها به طور صحیح و حتما به مقصد تحویل داده خواهند شد

ویژگی Connection Oriented: یعنی بین مبدا و مقصد یک مسیر قطعی و کامل تشکیل خواهد شد و همه بسته ها از طریق آن به مقصد ارسال خواهند شد.

ویژگی Retransmission: یعنی بسته ای که به مقصد نمی رسد، دوباره ارسال خواهد شد و آنقدر ارسال خواهد شد تا حتما به مقصد برسد.

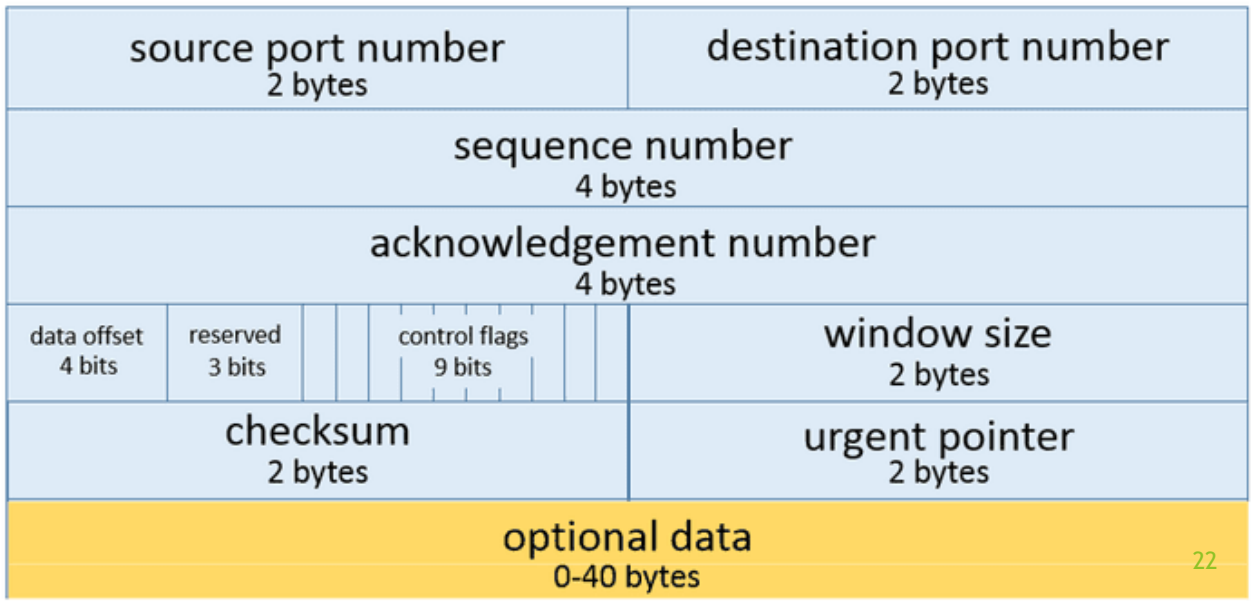
ویژگی Sequencing: یعنی هر بسته به طور جداگانه شماره گذاری می شود تا از ارسال و دریافت آن و در سایر امور استفاده شود.

ویژگی Acknowledgment: یعنی بسته ای که با شماره مشخصی به مقصد می رسد، تاییدیه آن به مبدا ارسال می شود تا مبدا مطمئن شود که آن بسته به مقصد رسیده است.

پروتکل TCP همه موارد بالا را ارائه می کند ولی UDP ارائه نمی کند.

فرمت بسته TCP

فرمت بسته در پروتکل TCP شماره پورت Port مبدا و مقصد را نمایش می دهد. همچنین بسته های ارسالی را شماری گزاری می کند sequence، تا مرتبا ارسال و دریافت شوند. همچنین برای هر بسته دریافت شده یک تصدیق بر می گرداند acknowledgment. برای کنترل خطا و کنترل جریان نیز اقدامات لازم را انجام می دهد flow control. قسمت window size هم برای کنترل ترافیک استفاده می شود.



فرمت بسته TCP

پورت مبدأ Source Port به طول ۱۶ بیت: این بخش پورت مبدأ پردازش درخواست را در دستگاه فرستنده تعیین می‌کند.

پورت مقصد Destination Port به طول ۱۶ بیت: این بخش پورت مقصد پردازش اپلیکیشن را در دستگاه گیرنده تعیین می‌کند.

شماره تأیید وصول Acknowledgement Number به طول ۳۲ بیت: زمانی که فلگ ACK تعیین شده باشد، این شماره شامل شماره توالی بعدی داده‌ها است که انتظار می‌رود دریافت شود و به عنوان تأیید وصول داده‌های دریافتی قبلی عمل می‌کند.

آفست داده‌ها Data Offset به طول ۴ بیت: این فیلد هم به معنی اندازه هدر TCP (کلمه‌های ۳۲ بیتی) و هم آفست داده‌ها در بسته کنونی در کل قطعه TCP است.

ذخیره شده Reserved به طول ۳ بیت: این بخش برای استفاده‌های آتی ذخیره شده و همه آن‌ها به صورت پیش‌فرض روی صفر تنظیم می‌شوند.

فلگ‌ها Flags: هر کدام، به طول ۱ بیت:

NS – بیت Nonce Sum برای پردازش سیگنال رسانی «اعلان تراکم صریح» Explicit Congestion Notification استفاده می‌شود.

CWR – زمانی که یک میزبان بسته‌ای با بیت ECE دریافت می‌کند، اقدام به کاهش پنجره‌های تراکم می‌کند تا تصدیق کند که ECEدریافت شده است.

ECE – دو معنا دارد:

فرمت بسته TCP

اگر بیت Syn به مقدار صفر تنظیم شده باشد، در این صورت ECE به این معنی است که بسته IP دارای CE تجربه تراکم یا (congestion experience) خاص خود است.

اگر Syn روی ۱ تنظیم شده باشد، ECE به این معنی است که دستگاه قابلیت ECT دارد.

URG - این مقدار نشان می‌دهد که فیلد «اشاره‌گر ضروری» Urgent Pointer داده‌های مهمی دارد و باید مورد پردازش قرار گیرد.

ACK - این بخش اعلام می‌کند که فیلد تأیید وصول اهمیت دارد. اگر ACK به مقدار صفر تنظیم شده باشد، نشان می‌دهد که بسته شامل هیچ تأییدی نیست.

PSH - زمانی که تنظیم شده باشد، یک درخواست به دستگاه دریافت‌کننده می‌فرستد تا داده‌ها را (به محض رسیدن) بدون بافر کردن به اپلیکیشن دریافت‌کننده PIUSH کند.

RST - فلگ ریست است و قابلیت‌های زیر را دارد:

برای نپذیرفتن اتصال ورودی استفاده می‌شود.

برای رد کردن اتصال ورودی استفاده می‌شود.

برای ری‌استارت کردن اتصال ورودی استفاده می‌شود.

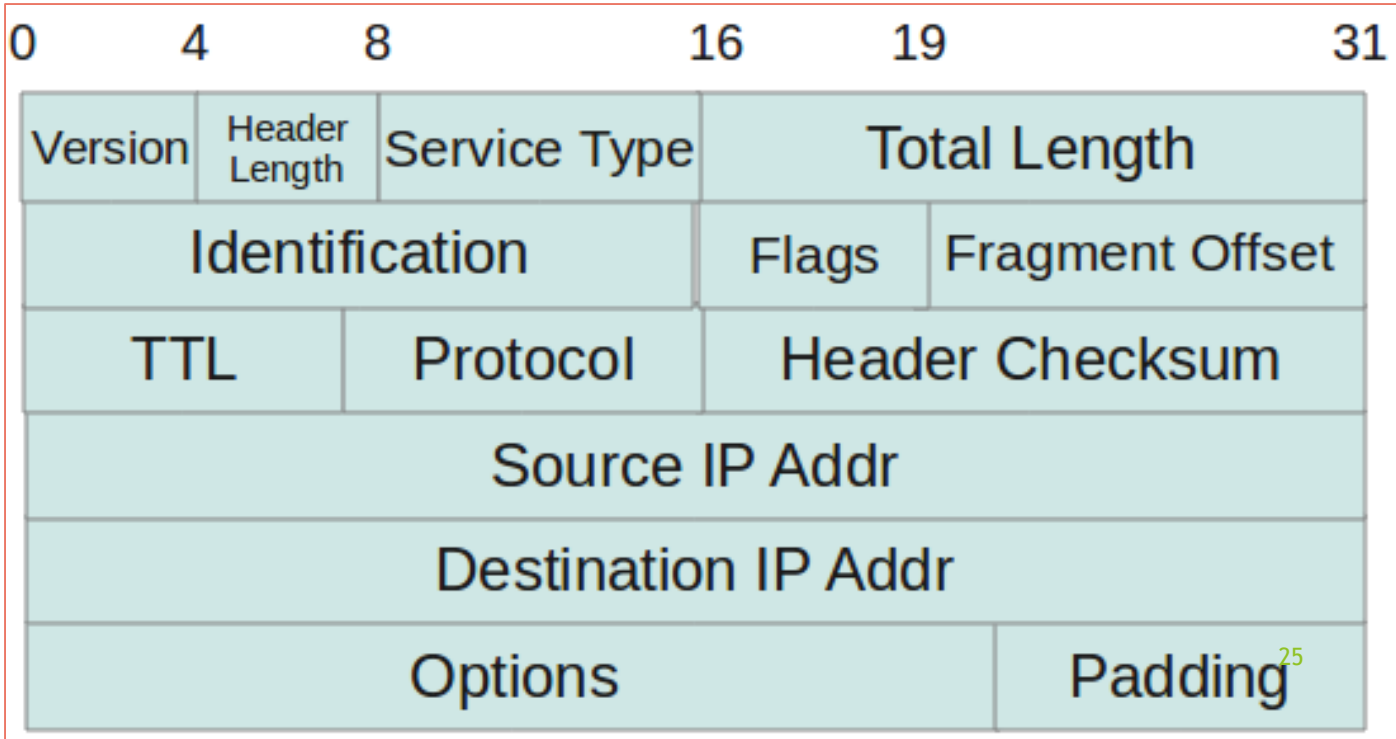
SYN - این فلگ برای راه‌اندازی یک اتصال بین میزبان‌ها استفاده می‌شود.

FIN - این فلگ برای آزادسازی یک اتصال استفاده می‌شود و هیچ داده اضافی پس از آن مبادله نخواهد شد. از آنجا که بسته‌ها با فلگ SYN و FIN شماره توالی دارند، با ترتیب صحیح پردازش می‌شوند.

فرمت بسته IP

فرمت بسته در IP نوع سرویس، مدت زمان حضور بسته در شبکه، آدرس مبدا و مقصد، کنترل خطای بسته و اطلاعاتی برای نسخه پروتکل را فراهم می کند.

بستهIP در مسیریابها و سوییچ ها اطلاعات لازم برای ارسال صحیح بسته رو به جلو را فراهم می کند.



فرمت بسته IP

Version : نسخه شماره پروتکل اینترنت استفاده شده را نشان می دهد به عنوان مثال IPv4

IHL : طول Header بسته؛ طول کل هدر IP

DSCP : یا Differentiated Services Code Point، این نوع خدمات Type of Service هم نامیده می شود.

ECN : Explicit Congestion Notification؛ اطلاعات مربوط به ازدحام دیده شده در مسیر را به همراه دارد.

Total Length : طول کل بسته های IP از جمله هدر IP و IP Payload است.

شناسایی Identification: اگر بسته IP در حین انتقال قطعه قطعه شود، تمام قطعات دارای شماره شناسایی یکسان هستند. برای شناسایی بسته IP اصلی که به آن ها تعلق دارد.

پرچم ها Flags : طبق منابع شبکه مورد نیاز ، اگر IP Packet برای رسیدگی بیش از حد بزرگ باشد ، این "پرچم ها" می گوید که آیا آن ها می توانند تکه تکه شوند یا خیر. در این پرچم ۳ بیتی ، MSB همیشه روی "۰" تنظیم شده است.

Fragment Offset : این افست موقعیت دقیق قطعه در بسته اصلی IP را بیان می کند.

زمان زنده ماندن Time to Live: برای جلوگیری از لوپ در شبکه ، هر بسته با برخی از مقادیر TTL ارسال می شود ، که به شبکه می گوید یک پکت اجازه دارد از چند هاپ یا دستگاه دیگر عبور کند و با هر بار عبور پکت از یک هاپ، یک عدد از مقدار TTL فعلی آن کم می شود و وقتی مقدار به صفر رسید ، بسته حذف می شود.

فرمت بسته IP

پروتکل Protocol: به لایه Network در میزبان مقصد می گوید که این بسته به آن پروتکل متعلق است، یعنی پروتکل سطح بعدی. به عنوان مثال تعداد پروتکل ICMP 1، TCP 6 و UDP 17 است.

Header Checksum: این فیلد برای نگه داشتن مقدار checksum کل هدر استفاده می شود که برای بررسی این که آیا بسته بدون خطا دریافت می شود استفاده می شود.

آدرس منبع Source Address: آدرس ۳۲ بیتی فرستنده (یا منبع) بسته است.

آدرس مقصد Destination Address: آدرس ۳۲ بیتی گیرنده (یا مقصد) بسته است.

Options: این قسمت اختیاری است ، که اگر مقدار IHL بیش تر از ۵ باشد استفاده می شود. این Options ممکن است دارای مقادیر گزینه هایی مانند Security، Record Route، Time Stamp و غیره باشد.

مثالی برای درک مدل معماری انیترنت

فرض کنید یک دانشجو در منزل شخصی خودش قصد انجام انتخاب واحد از طریق سایت دانشگاه را دارد. لذا ایشان ضمن اجرای یک مرورگر، آدرس دامنه ای azaruniv.ac.ir را در تایپ و Enter را می فشارد.

اکنون پروتکل ClientHTTP (به عنوان یک کاربرد) در کامپیوتر دانشجو سعی می کند با استفاده از آدرس azaruniv.ac.ir به پروتکل HTTP در سرور دانشگاه متصل شود اما نمی تواند زیرا HTTP با آدرس IP کار می کند نه با آدرس دامنه. در این مرحله پروتکل ClientDNS (کاربرد بعدی با پورت ۵۳) کامپیوتر وارد عمل می شود و با دریافت azaruniv.ac.ir از ClientHTTP، آدرس IP دانشگاه را استخراج و تعیین می کند. سپس ClientHTTP مجددا با استفاده از IP به دست آمده اقدام به برقراری ارتباط با سرور دانشگاه خواهد کرد.

توجه شود در این مثال هر دو برنامه ClientHTTP و ClientDNS در لایه کاربرد کامپیوتر دانشجو کار می کنند و سرور دو پروتکل HTTP و DNS نیز بر روی کامپیوتر دانشگاه فعال هستند.

سپس پروتکل HTTP محتوی وب سایت دانشگاه را به صورت بسته های کوچک با پورت شماره 80 به کاکپیوتر دانشجو منتقل می کند و مرورگر هم صفحات وب را مجددا در کامپیوتر دانشجو بازنمایی باز چیدمان می کند. بدین ترتیب دانشجو می توان انتخاب واحد را انجام دهد.