

فصل 1	
21 2	فصل 2
40 3	فصل 3
72 4	فصل 4
97 5	فصل 5
115 6	فصل 6
125 7	فصل 7
140 8	فصل 8
152 9	فصل 9

6th شبکه های کامپیوتری: رویکردی از بالا به پایین، نسخه

راه حل هایی برای بررسی سوالات و مشکلات

تاریخ نسخه: می 2012

این سند حاوی راه حل هایی برای بررسی سوالات و مشکلات نسخه پنجم شبکه های کامپیوتری: رویکردی از بالا به پایین توسط جیم کوروز و کیت راس است. این راه حل ها فقط برای مریبان در دسترس هستند لطفاً این سند را برای دیگران (حتی سایر مریبان) کپی یا توزیع نکنید. لطفاً هیچ راه حلی را در یک وب سایت در دسترس عموم قرار ندهید. ما خوشحال خواهیم شد که یک نسخه (به روز) از این راه حل را خودمان در اختیار هر کسی که بخواهد ارائه دهیم.

تشکر و قدردانی: در طی سالیان متعددی، چندین دانشجو و همکاران ما را در تهیه این راه حل کمک کرده اند. از HongGang Zhang، Rakesh Kumar، Prithula Dhungel و Vijay Annapureddy تشکر ویژه داریم. همچنین از همه خوانندگانی که پیشنهادات و اشتباهات خود را اصلاح کرده اند، تشکر می کنم.

تمامی حقوق محفوظ است. © JF Kurose و KW Ross 1996-2012 توسط C مطالب

فصل 1 سوالات مروری

هیچ تفاوتی وجود ندارد. در سراسر این متن، کلمات "میزبان" و "سیستم پایانی" به جای یکدیگر استفاده می‌شوند. سیستم‌های پایانی شامل رایانه‌های شخصی، ایستگاه‌های کاری، سرور‌های وب، سرور‌های پست الکترونیکی، رایانه‌های شخصی، کنسول‌های بازی متصل به اینترنت و غیره هستند.

از ویکی پدیا: پروتکل دیپلماتیک معمولاً به عنوان مجموعه‌ای از قوانین بین المللی حسن نیت توصیف می‌شود. این قوانین به خوبی ثبت شده و رعایت شده در زمان، زندگی و کار مشترک را برای ملت‌ها و مردم آسان کرده است. بخشی از پروتکل همیشه تصدیق جایگاه سلسله مراتبی همه حاضران بوده است. قوانین پروتکل بر اساس اصول مدنی است.

استانداردها برای پروتکل‌ها مهم هستند تا مردم بتوانند سیستم‌های شبکه و محصولاتی را ایجاد کنند که با هم کار کنند.

HFC: از طریق خط تلفن: خانه یا دفتر کوچک. 3. کابل به DSL. مودم شماره گیری از طریق خط تلفن: خانه; 2. 1. G و 4G خانه و شرکت: 6. 3. 6. Wifi (802.11): 4. اترنت سوئیچ 100 مگابیت بر ثانیه: سازمانی; 5. پهناور.

بین کاربران به اشتراک گذاشته شده است. در کanal پایین‌دست، همه بسته‌ها از یک منبع منفرد، یعنی HFC پهناور باند 5. هد لند سرچشم می‌گیرند. بنابراین، هیچ برخوردي در کanal پایین‌دستی وجود ندارد.

کابل مودم؛ فیبر به خانه; Dial-up;DSL: در اکثر شهرهای آمریکا، امکانات فعلی عبارتند از 6.

شبکه‌های محلی اترننت دارای سرعت انتقال 10 مگابیت بر ثانیه، 100 مگابیت در ثانیه، 1 گیگابیت بر ثانیه و 10 گیگابیت بر ثانیه هستند. 7.

امروزه اترننت معمولاً روی سیم مسی جفت پیج خورده اجرا می‌شود. همچنین می‌تواند روی پیوندهای فیبر نوری اجرا شود.

9. ADSL: مودم‌های شماره گیری: حداقل 56 کیلوبیت در ثانیه، پهناور باند اختصاص داده شده است. نرخ HFC: مگابیت در ثانیه پایین دست و 2.5 مگابیت در ثانیه در بالادست، پهناور باند اختصاص داده شده است. اپلود-2: FTTH: 42.8 مگابیت در ثانیه و نرخ بالادست تا 30.7 مگابیت در ثانیه، پهناور باند مشترک است 10 مگابیت در ثانیه. دانلود 20-10 مگابیت بر ثانیه؛ پهناور باند مشترک نیست.

10. امروزه دو فناوری محبوب دسترسی به اینترنت بی سیم وجود دارد:

بی سیم، کاربران بی سیم بسته‌ها را به/از یک ایستگاه پایه (یعنی نقطه LAN در یک WiFi (802.11) در شعاع چند ده متری ارسال/دریافت می‌کنند. ایستگاه پایه معمولاً به اینترنت سیمی متصل است و بنابراین برای اتصال کاربران بی سیم به شبکه سیمی کار می‌کند.

هستند بسته‌ها سیستم‌های اینها 3 که در G و 4G شبکه‌های دسترسی بی سیم گستردگی از طریق همان زیرساخت بی سیم مورد استفاده برای تلفن همراه منتقل می‌شود، به طوری که ایستگاه پایه توسط یک ارائه دهنده ارتباطات راه دور مدیریت می‌شود. این امکان دسترسی بی سیم را برای کاربران در شعاع ده ها کیلومتری ایستگاه پایه فراهم می‌کند.

میزبان فرستنده انتقال را $t_1 = L/R$ در زمان t در زمان 11. کامل می کند و کل بسته در روتر دریافت می شود (بدون تاخیر انتشار). از آنجا که روتر کل بسته را در زمان $t_1 + L/R$ شروع به ارسال بسته به میزبان دریافت کننده کند. در زمان $t_1 + L/R$ ، روتر انتقال را کامل می کند و کل بسته در میزبان دریافت کننده دریافت می شود (دوباره، بدون تاخیر است. این $L/R_1 + L/R_2$ انتشار). بنابراین، تاخیر انتها به انتها.

یک شبکه سوئیچ مدار می تواند مقدار مشخصی از پهنای باند سرتاسر را برای مدت زمان یک تماس تضمین. 12. FDM کند. امروزه اکثر شبکه های سوئیچ بسته (از جمله اینترنت) نمی توانند هیچ تضمینی برای پهنای باند ارائه دهند. به سخت افزار آنالوگ پیچیده برای انتقال سیگнал به باندهای فرکانسی مناسب نیاز دارد.

(الف) 2 کاربر را می توان پشتیبانی کرد زیرا هر کاربر به نیمی از پهنای باند پیوند نیاز دارد. 13.

(ب) از آنجایی که هر کاربر هنگام ارسال به 1 مگابیت در ثانیه نیاز دارد، اگر دو یا کمتر کاربر همزمان ارسال کنند، حداقل 2 مگابیت در ثانیه نیاز خواهد بود. از آنجایی که پهنای باند موجود بیوند مشترک 2 مگابیت در ثانیه است، هیچ تاخیری در صفحه قبل از پیوند وجود نخواهد داشت. در حالی که اگر سه کاربر به طور همزمان ارسال کنند، پهنای باند نیاز 3 مگابیت در ثانیه خواهد بود که بیشتر از پهنای باند موجود بیوند مشترک است. در این صورت تاخیر در صفحه قبل از لینک وجود خواهد داشت.

(ج) احتمال اینکه یک کاربر معین در حال ارسال است = 0.2

$$= (d) \text{ احتمال اینکه هر سه کاربر به طور همزمان در حال ارسال هستند} \\ = (0.2)^3 = 0.008$$

از آنجایی که صفحه زمانی بزرگ می شود که همه کاربران در حال ارسال هستند، کسری از زمانی که صفحه رشد می کند (که برابر است با احتمال انتقال همزمان هر سه کاربر) 0.008 است.

با یکدیگر همتا نباشند، وقتی ترافیک را برای یکدیگر ارسال می کنند، باید ترافیک را از طریق ISP اگر دو 14. را ارائه دهند (واسطه) ارسال کنند که باید هزینه حمل ترافیک را به آن پرداخت کنند. با همکاری کردن مستقیم با ISP یک های ارائه دهنده خود کاهش دهند. یک نقطه تبادل اینترنت ISP می توانند پرداخت های خود را به ISP یکدیگر، دو می ISP نقطه ملاقاتی است که در آن چندین (معمولًا در یک ساختمان مستقل با سوئیچ های خاص خود) (IXP) IXP هایی که به ISP با گرفتن هزینه نسبتاً کمی از هر یک از ISP توانند به یکدیگر متصل و یا همتا شوند. یک IXP متصل می شوند، پول خود را به دست می اورد که ممکن است به میزان ترافیک ارسال شده یا دریافتی از بستگی داشته باشد.

شبکه خصوصی گوگل تمام مراکز داده بزرگ و گوچک خود را به هم متصل می کند. ترافیک بین مراکز داده گوگل 15. های سطح پایین ISP به جای اینترنت عمومی از طریق شبکه خصوصی آن منتقل می شود. بسیاری از این مراکز داده در های ISP تر یا نزدیک به آنها قرار دارند. بنابراین، زمانی که گوگل محتوا را به کاربر تحویل می دهد، اغلب می تواند سطح بالاتر را دور بزند. انگیزه ارائه دهنده محتوا برای ایجاد این شبکه ها چیست؟ اولاً، ارائه دهنده محتوا کنترل واسطه استفاده کند. دوم، می تواند با ارسال ترافیک کمتر به ISP بیشتری بر تجربه کاربر دارد، زیرا مجبور است از چند شبکه های ارائه دهنده در هزینه صرفهジョیی کند. سوم، اگر

ها تصمیم می‌گیرند پول بیشتری را از آرائه دهنگان محتوای بسیار سودآور دریافت کنند ISP
کشورهایی که بی‌طرفی شبکه در آنها اعمال نمی‌شود)، ارائه دهنگان محتوا می‌توانند از این پرداخت های اضافی
اجتناب کنند.

مؤلفه های تأخیر عبارتند از تأخیر های پردازش، تأخیر های انتشار و تأخیر های صفحه این.
تأخر ها ثابت هستند به جز تأخیر های صفحه که متغیر هستند.

الف) 1000 کیلومتر، 1 مگابیت در ثانیه، 100 بايت ب) 100 کیلومتر، 1 مگابیت در ثانیه، 100 بايت

نهنه;s/d؛ میلی ثانیه 10.

الف) 500 کیلوبیت در ثانیه 19.
بايت
ب) 64 ثانیه (ج) 100 کیلوبیت
در ثانیه 320؛ ثانیه

فایل بزرگ را به قطعات تقسیم می‌کند. هدر را به هر تکه اضافه می‌کند و در نتیجه چندین بسته A پایان سیستم IP است. سوئیچ بسته از آدرس (B سیستم پایانی) مقصد IP از فایل تولید می‌کند. هدر در هر بسته شامل آدرس مقصد در بسته برای تعیین پیوند خروجی استفاده می‌کند. پرسیدن اینکه کدام جاده باید طی شود، مشابه بسته ای است که با توجه به آدرس مقصد بسته، در کدام لینک خروجی باید ارسال شود.

حداکثر نرخ انتشار 500 بسته در ثانیه و حداقل سرعت انتقال 350 بسته در ثانیه است. شدت ترافیک مربوطه 21.
 $500/350 = 1.43 < 1$ است. در نهایت برای هر آزمایش ضرر رخ خواهد داد. اما زمانی که برای اولین بار از دست دادن رخ می‌دهد از یک آزمایش به آزمایش بعدی به دلیل تصادفی بودن فرآیند انتشار متفاوت خواهد بود.

پنج وظیفه عمومی عبارتند از: کنترل خط، کنترل جریان، تقسیم بندی و مونتاژ مجدد، چندگانه سازی و تنظیم اتصال. بله، این وظایف را می‌توان در لایه های مختلف کپی کرد. به عنوان مثال، کنترل خط اغلب در بیش از یک لایه ارائه می‌شود.

پنج لایه در پشت پروتکل اینترنت - از بالا به پایین - لایه برنامه، لایه انتقال، لایه شبکه، لایه پیوند و لایه فیزیکی 23.
هستند. مسئولیت های اصلی در بخش 1.5.1 بیان شده است.

پیام لایه برنامه: داده هایی که یک برنامه می‌خواهد ارسال کند و به لایه انتقال ارسال کند. بخش لایه حمل و نقل: 24.
توسط لایه انتقال تولید می‌شود و پیام لایه برنامه را با هدر لایه انتقال محصور می‌کند. دیتاگرام لایه شبکه: بخش لایه انتقال را با هدر لایه شبکه کپسوله می‌کند. قاب لایه پیوند: دیتاگرام لایه شبکه را با هدر لایه پیوند کپسوله می‌کند.

روترها شبکه، پیوند و لایه های فیزیکی را پردازش می‌کنند (لایه های 1 تا 3). (این کمی یک دروغ سفید است، زیرا 25.
روترهای مدرن گاهی اوقات به عنوان فایروال یا حافظه پنهان عمل می‌کنند

کامپونت‌ها و لایه‌ی انتقال فرآیند نیز). لایه‌های پیوند و فیزیکی را پردازش می‌کند (لایه‌های 1 تا 2). هاست‌ها هر پنج لایه را پردازش می‌کنند.

26. (الف)

برای گسترش به نوعی از تعامل انسانی نیاز دارد. مثال کلاسیک: ویروس‌های ایمیل و ویروس

(ب) کرم‌ها

و شماره پورت‌ها را اسکن می‌کند و به دنبال IP بدون نیاز به تکرار کاربرکرم در میزبان آلوه آدرس‌های فرآیندهای آسیب‌پذیر برای آلوه کردن است.

ایجاد یک بات نت مستلزم آن است که مهاجم آسیب‌پذیری را در برخی از برنامه‌ها یا سیستم‌ها پیدا کند (مثال 27). سوء استفاده از آسیب‌پذیری سرریز بافر که ممکن است در یک برنامه وجود داشته باشد (پس از یافتن آسیب‌پذیری، مهاجم باید میزبان‌هایی را که آسیب‌پذیر هستند اسکن کند. هدف اساساً به خطر انداختن یک سری از سیستم‌ها با بهره برداری از آن آسیب‌پذیری خاص است. هر سیستمی که بخشی از بات نت است می‌تواند به طور خودکار محیط خود را اسکن کند و با سوء استفاده از آسیب‌پذیری منتشر شود. یکی از ویژگی‌های مهم این بات‌نت‌ها این است که سازنده بات‌نت می‌تواند از راه دور همه گره‌های بات‌نت را کنترل کرده و دستورات را صادر کند. از این رو، این امکان به عنوان) برای مهاجم فراهم می‌شود که فرمانی را به تمام گره‌هایی که یک گره را هدف قرار می‌دهند صادر کند را به هدف بدهند، که ممکن TCP SYN مثلاً، همه گره‌های بات‌نت ممکن است توسط مهاجم دستور ارسال پیام (به هدف TCP SYN است منجر شود. در یک حمله سیل

ترودمی می‌تواند به آلیس و اندیش کند که باب است (و بالعکس) و تا حدی یا به طور کامل پیام‌های ارسال شده از باب به آلیس را تغییر دهد. به عنوان مثال، او می‌تواند به راحتی عبارت "آلیس، من به تو 1000 دلار بدهکارم" را به "آلیس، من 10000 دلار به تو بدهکارم" تغییر دهد. علاوه بر این، ترودمی حتی می‌تواند بسته‌هایی را که باب به آلیس ارسال می‌کند (و بالعکس) رها کند، حتی اگر بسته‌های باب به آلیس رمزگذاری شده باشند.

فصل 1 مسائل

مشکل 1

هیچ پاسخ درست واحدی برای این سوال وجود ندارد.
در اینجا یک پاسخ ساده در زیر آمده است:

بسیاری از پروتکل‌ها این کار را انجام می‌دهند

به نام پیام سرور ATM پیام‌ها از دستگاه

<userid>سلام

به سرور اطلاع دهید که کارتی در دستگاه خودپرداز وجود دارد

PASSWD<passwd>
تعادل
<amount>برداشت از حساب

شناسه کاربر را به سرور منتقل می‌کند ATM کارت
کاربر پین را وارد می‌کند که به سرور ارسال می‌شود
کاربر موجودی را درخواست می‌کند
کاربر درخواست برداشت پول می‌کند

خدا حافظ	کاربر تمام شد
پیام ها از سرور به دستگاه خودپرداز (نمایش) نام پیام هدف	
PASSWD خوب	از کاربر بین (رمز عبور) بخواهید آخرین عملیات درخواستی (PASSWD، WITHDRAWL) OK
ERR	آخرین عملیات درخواستی (PASSWD، WITHDRAWL) در ERROR
امیزان<amt> خدا حافظ	ارسال شد BALANCE در پاسخ به درخواست کاربر تمام شد، صفحه خوش آمدگویی را در دستگاه خودپرداز نمایش دهد

عملکرد صحیح:

مشتری	سرور
HELO (کاربر)	-> (بررسی کنید که آیا شناسه کاربری معین است) <- PASSWD
PASSWD<passwd>	-> (بررسی رمز عبور) <- خوب (رمز عبور صحیح است)
تعادل	-> <- میزان<amt>
برداشت از حساب<amt>	-> بررسی کنید که آیا دلار برای پوشش برداشت کافی است یا خیر <- خوب
ATM \$ BYE می کند	-> <- خدا حافظ

در شرایطی که پول کافی وجود ندارد:

HELO (کاربر)	->	(بررسی کنید که آیا شناسه کاربری معین است)
PASSWD<passwd>	->	(بررسی رمز عبور)
تعادل	-> <- میزان<amt>	خوب (رمز عبور صحیح است)
برداشت از حساب<amt>	->	کافی اگر بررسی \$ به پوشش و وجه کافی نیست (ERR)
پیام خطای نمایش داده نمی شود	-> <- خدا حافظ	

مشکل 2

بسته اول به مقصد رسیده است، بسته دوم در آخرین روتر، بسته سوم در روتر بعدی به آخرین و $N^*(L/R)$ در زمان بسته دوم به مقصد رسیده است، بسته سوم در آخرین روتر ذخیره، $N^*(L/R) + L/R$ غیره ذخیره می‌شود. در زمان همه بسته $(N+P-1)^*(L/R) = (N+P-1)^*(L/R) + (P-1)^*(L/R)$ می‌شود و ... در ادامه این منطق می‌بینیم که در زمانها به مقصد رسیده اند.

مشکل 3

(الف) یک شبکه سوئیچ مدار برای برنامه کاربردی مناسب است، زیرا برنامه شامل جلسات طولانی با نیازهای پهنای باند صاف قابل پیش‌بینی است. از آنجایی که نرخ انتقال مشخص است و پشت سر هم نیست، پهنای باند را می‌توان برای هر جلسه برنامه بدون اتلاف قابل توجه رزرو کرد. علاوه بر این، هزینه های سربار راه اندازی و از بین بردن اتصالات در طول مدت طولانی یک جلسه برنامه معمولی مستهلك می‌شود.

(ب) در بدترین حالت، همه برنامه‌ها به طور همزمان از طریق یک یا چند لینک شبکه ارسال می‌کنند. با این حال، از آنجایی که هر پیوند دارای پهنای باند کافی برای رسیدگی به مجموع نرخ داده‌های برنامه‌های کاربردی است، هیچ ازدحام (صف بسیار کم) رخ نخواهد داد. با توجه به چنین ظرفیت‌های پیوند سخاوتمندانه‌ای، شبکه نیازی به مکانیسم های کنترل تراکم ندارد.

مشکل 4

(الف) بین سوئیچ در سمت چپ بالا و سوئیچ در سمت راست بالا می‌توانیم 4 اتصال داشته باشیم. به طور مشابه می‌توانیم چهار اتصال بین هر یک از 3 جفت سوئیچ مجاور دیگر داشته باشیم. بنابراین، این شبکه می‌تواند تا 16 اتصال را پشتیبانی کند.

(ب) می‌توانیم 4 اتصال از سوئیچ در گوشه سمت راست بالا و 4 اتصال دیگر از سوئیچ در گوشه پایین سمت چپ عبور کنند که در مجموع 8 اتصال می‌دهد.

مسیر می‌دهیم. برای D و دو اتصال را از طریق B دو اتصال را از طریق C و A (ج) بله. برای اتصالات بین مسیر می‌دهیم. به این ترتیب حداقل 4 C و دو اتصال را از طریق A دو اتصال را از طریق D و B اتصالات بین اتصال وجود دارد. عبور از هر لینک

مشکل 5

باجه های عوارضی 75 کیلومتر از هم فاصله دارند و اتومبیل ها با سرعت 100 کیلومتر در ساعت حرکت می کنند. یک باجه عوارض به یک ماشین در هر 12 ثانیه یک ماشین سرویس می دهد.

(الف) ده ماشین وجود دارد. 120 ثانیه یا 2 دقیقه طول می کشد تا اولین باجه عوارض به 10 خودرو سرویس دهد. هر کدام از این خودروها قبل از رسیدن به باجه عوارضی دوم، 45 دقیقه تاخیر انتشار دارند (75 کیلومتر). بدین ترتیب تمامی خودروها پس از 47 دقیقه در مقابل باجه عوارضی دوم صف کشیده اند. کل فرآیند برای سفر بین باجه های عوارضی دوم و سوم تکرار می شود. همچنان 2 دقیقه طول می کشد تا باجه عوارضی سوم به 10 خودرو خدمات رسانی کند. بنابراین کل تاخیر 96 دقیقه است.

(ب) تاخیر بین باجه های عوارضی 8*12 ثانیه به اضافه 45 دقیقه یعنی 46 دقیقه و 36 ثانیه می باشد. کل تاخیر دو برابر این مقدار به اضافه 8*12 ثانیه یعنی 94 دقیقه و 48 ثانیه است.

مشکل 6

ثانیه/متر = تمیز است (ا)

ثانیه آر / L = د ترانس (ب)

ثانیه (آر / L + م/متر) - = به - پیون د (ج)

خارج می شود. (ه) بیت اول در پیوند است و A (د) بیت به تازگی از میزبان رسانیده است B نرسیده است. (و) بیت اول به میزبان B به میزبان

(ز) خواستن

$$\frac{56}{SRL} = \frac{56}{12 \times \times} \times 10^8 = 536 \text{ کیلومتر}$$

مسئله 7

اولین بیت یک بسته را در نظر بگیرید. قبل از انتقال این بیت، تمام بیت های بسته باید تولید شوند. این نیاز دارد

$$\frac{64}{56} \times \frac{8}{0} \text{ sec} = 7 \text{ msec.}$$

زمان مورد نیاز برای ارسال بسته است

$$\frac{610}{856} \times \mu \text{sec} = 224 \text{ ثانیه}$$

تاخیر انتشار = 10 میلی ثانیه

تاخیر تارمزگشایی است

$$7 \text{ ثانیه} + 10 \text{ میلی ثانیه} = 17.224 \text{ میلی ثانیه} \quad \mu\text{ثانیه}$$

تجزیه و تحلیل مشایه نشان می دهد که همه بیت ها تا خیر 17.224 میلی ثانیه را تجربه می کنند

٨ مسئله

الف) 20 کاربر قابل پشتیبانی
1.0 = p. هستند. ب)

ج) $\frac{120}{pr} \left[n - \frac{1}{r} \right] \frac{120 - nr}{pr}$

۵) ۱۲۰ ۱ μm (۱- $\frac{۱}{۴}$) $120 - n$

برای تقریب این احتمال از قضیه حد مرکزی استفاده می کنیم. اجازه دهید X^P متغیر های تصادفی به گونه ای که $P = 1$.

مستقل باش

$$(\text{پا بیشتر کاربر 21}^{\text{ا}}\text{پ}) = 1 - \frac{1}{1^{\text{ا}} d} \leq 21$$

پ ۱۲۰ کلمه پیش از ۲۱ \sum XP ۰۱۲۰ ۹.۰۱.۰۱۲۰ ۹

$$\approx \frac{286.3}{9} ZP \leq) 74.2$$

003.0 ≈ ("پا بیشتر کاربر 21") معمولی استاندارد است بنابراین rV یک Z هنگامی که

مسئله ۹

الف) 10000

$$\text{ب)} \quad \sum_{n=1}^{\infty} \frac{pn}{M} \ln \left(\frac{1}{1 - \frac{n}{M}} \right) \quad \boxed{\quad}$$

10 ملے

منشر می 1 s/d نیاز دارد تا بسته را به اولین پیوند ارسال کند. بسته بر روی پیوند اول در $R1/L$ اولین سیستم پایانی به را اضافه می کند. پس از دریافت کل بسته، سوئیچ بسته اول و دوم را به هم وصل می `dproc` شو. سوئیچ بسته تا خیر پردازش کند

منتشر می شود. به d_2 / s نیاز دارد تا بسته را به لینک دوم منتقل کند. بسته بر روی پیوند دوم در L/R_2 پیوند به طور مشابه، ما می توانیم تأخیر ناشی از سوئیچ دوم و پیوند سوم را پیدا کنیم.

اضافه کردن این پنج تأخیر می دهد

$$d = L/R_1 + L/R_2 + L/R_3 + d_1 / s 1 + d_2 / s 2 + d_3 / s 3 + d_{proc} + d_{proc}$$

برای پاسخ به سوال دوم، به سادگی مقادیر را به معادله متصل می کنیم تا $6 + 16 + 20 + 6 + 6 + 3 + 3 + 4 = 64$ میلی ثانیه به دست آوریم.

مسئله 11

از آنجایی که بیت ها فوراً ارسال می شوند، سوئیچ بسته هیچ تأخیری ایجاد نمی کند. به ویژه، تأخیر انتقال را معرفی نمی کند. بدین ترتیب

$$d = L/R + d_1 / s 1 + d_2 / s 2 + d_3 / s 3$$

برای مقادیر در مسئله 10، $6 + 16 + 20 + 6 + 4 = 46$ میلی ثانیه دریافت می کنیم.

مسئله 12

بسته دریافتی ابتدا باید منتظر باشد تا پیوند $4.5 * 1500 = 6750$ بایت یا 54000 بیت ارسال کند. از آنجایی که این بیت ها با سرعت 2 مگابیت در ثانیه ارسال می شوند، تأخیر در صفحه 27 میلی ثانیه است. به طور کلی، تأخیر در صفحه $(nL + (L - x))/R$ است.

مسئله 13

برای بسته $R/(L-1)$ ، و به طور کلی L/R (الف) تأخیر صفحه برای اولین بسته ارسالی 0، برای بسته ارسالی دوم برابر است با N است. بنابراین، میانگین تأخیر برای بسته های n ارسالی

$$\begin{aligned} & (L/R + 2L/R + \dots + (N-1)L/R)/N \\ &= L/(RN) * (1 + 2 + \dots + (N-1)) = \\ & L/(RN) * N(N-1)/2 \\ &= LN(N-1)/(2RN) \\ &= (N-1)L/(2R) \end{aligned}$$

توجه داشته باشید که در اینجا ما از واقعیت شناخته شده استفاده کردیم:

$$1 + 2 + \dots + N = N(N+1)/2$$

می رسد، با فرض N بنابراین، زمانی که هر دسته از بسته های N ثانیه برای انتقال بسته های $/ R$ کشد است. بنابراین، میانگین تأخیر یک بسته در تمام دسته های متوسط تأخیر در یک دسته است، یعنی $(N-1)L/2R$.

مسئله ۱۴

الف) تأخير انتقال است كل تأخير است. آر / ۷

آر / L = میں اجازہ دھید 1(b) + - / LP₌₁ IR

تبر
-1 K

به بی نهایت نزدیک a/b یا $1/x$ تاخیر کل افزایش می‌باید و با نزدیک شدن، x تاخیر کل = 0. با افزایش $x=0$ برای می‌شود.

15 میں

$$\text{کلی تاخیر} = \frac{1}{\text{متر}} \cdot \frac{1}{\text{مذہب}} \cdot \frac{1}{\text{امہت}} \cdot \frac{1}{\text{امہت}} \cdot \frac{1}{\text{امہت}} \cdot \frac{1}{\text{امہت}} \cdot \frac{1}{\text{امہت}}$$

16 *alma*

$N=10+1$ ، تعداد کا، بسته ها در سیستم شامل، بسته های، محدود در بافر و بسته ای، است که در حال انتقال، است نیاز این:

بجه این معنا که. تاخیر در صفت + تاخیر ارسال=a^{*}=بنابراین $(10+1)$ ، د. آ = ن
 سنته در ثانیه a=550 بنابراین $(0.01+0.01)=a^*(0.01+0.01)$

17 

و جود دارد (the میزبان منع و Q الف) گزه های

نشان می دهد $\frac{q}{prod}$ روتراها). اجازه دهید ق-1

دانشگاه آزاد اسلامی واحد تاکستان

ام و زن خ انتقال بیوند

23

دھن

۷

1

$$= \sum_{\text{گاہ}} \left[D_{\text{proc}}^q + D_{\text{trans}}^q + D_{\text{کیفیت}}^q \right]$$

تشان دهید. سیس ۹ میانگین تاخیر صفر است در گزه در ۹ ب) اجازه دهد

$$S = \left[D_q^{\text{proc}} + D_q^{\text{trans}} + \frac{\text{کیفیت}}{D} \right].$$

مسئله 18

در لینوکس می توانید از دستور استفاده کنید

`traceroute www.targethost.com`

و در خط فرمان ویندوز می توانید استفاده کنید

`tracert www.targethost.com`

در هر صورت، سه اندازه گیری تاخیر دریافت خواهد کرد. برای این سه اندازه گیری می توانید میانگین و انحراف معیار را محاسبه کنید. آزمایش را در ساعات مختلف روز تکرار کنید و در مورد هر تغییری نظر دهید.

در اینجا یک نمونه راه حل آورده شده است:

مسیرهای ردیابی بین مرکز سوپر کامپیوتر سن دیگو و www.poly.edu

الف) میانگین (میانگین) تاخیرهای رفت و برگشت در هر سه ساعت به ترتیب 71.18 میلی ثانیه، 71.38 میلی ثانیه و 0.075 هستند 71.55 ms، 0.21 ms، 0.05 ms. انحرافات استاندارد به ترتیب 0.075 میلی ثانیه است.

دارای 12 مسیریاب در هر سه ساعت در مسیر هستند. نه، مسیرها در هیچ یک از traceroutes (؛ ب) در این مثال ساعات تغییر نکردند.

از مبدأ به مقصد عبور می کنند بله، در این آزمایش بیشترین ISP از طریق چهار شبکه Traceroute (ج) بسته های های مجاور رخداد ISP تاخیر در رابطهای همتا بین

ایالات متحده) www.stella-net.net از www.poly.edu به (فرانسه).

د) میانگین تأخیرهای رفت و برگشت در هر سه ساعت به ترتیب 87.09 میلی ثانیه، 86.35 میلی ثانیه و 86.48 میلی ثانیه است. انحرافات استاندارد به ترتیب 0.53 ms، 0.23 ms، 0.18 ms هستند. در این مثال، در هر سه ساعت 11 روتور در مسیر وجود دارد. نه، مسیرها در هیچ یک از ساعت‌های Traceroute بیشترین تغییر نکردند. بسته‌های ISP را از مبدأ به مقصد منتقل کردند. بله، در این آزمایش بیشترین تأخیر در رابطهای هم‌بین ISP شبکه مجاور رخ داد.

مسئله 19 یک مثال راه

حل:

مسیرهای ریلیابی از دو شهر مختلف در فرانسه تا شهر نیویورک در ایالات متحده

الف) در این مسیرهای ریلیابی از دو شهر مختلف در فرانسه به یک میزبان مقصد در ایالات متحده، هفت پیوند مشترک هستند که از جمله آنها پیوند فرآتلانتیک است.

ب) در این مثال از مسیرهای ردیابی از یک شهر در فرانسه و از شهر دیگری در آلمان به همان میزبان در ایالات متحده، سه پیوند مشترک هستند که از جمله آنها پیوند فرآتلانتیک است.

ریابی به دو شهر مختلف در چین از پک میزبان در ایالات متحده

(ج) پنج پیوند در دو ردیاب مشترک است. این دو مسیر پیش از رسیدن به چین از هم جدا می‌شوند

20 *الإمام*

دقيقه = **{توان عملياتي** $Rs, Rc, R/M$ **}**

21 مسئله

:اگر فقط از یک مسیر استفاده کنید، حداقل توان عملیاتی، یا

اگر از همه مسیرها استفاده کنید، حداقل توان عملیاتی با $\sum K = M$ داده می‌شود.

مسائلہ 22

ps: احتمال دریافت موافقیت آمیز یک بسته عیارت است از

تعداد ارسال هایی که باید انجام شود تا زمانی که بسته با موفقیت توسط مشتری دریافت شود، یک متغیر تصادفی داده می شود. سپس، ps است. بنابر این، میانگین تعداد ارسال های مورد نیاز با: $1 - \frac{1}{ps}$ هندسی با احتمال موفقیت داده می شود. میانگین تعداد ارسال های محدد مورد نیاز با: $1 - \frac{1}{ps}$.

مسائلہ 23

می، نامیم B و سته دوم را A بسته اول را.

قرار می‌گیرد. بنابراین زمان A در اولین پیوند منتظر ارسال بسته B (الف) اگر لینک کلواگاه اولین پیوند باشد، بسته A را پسند نماید. این پسند بسته در مقصد به سادگی.

ب) اگر لینک دوم، لینک گلوبگاه باشد و هر دو بسته پشت سر هم ارسال شوند، باید درست باشد که بسته دوم قبل از اینکه لینک دوم ارسال بسته اول را تمام کند، به صفت رو و روی لینک دوم مم، رسیده این، معنا که

$$L/R_s + L/R_s + d_{prop} < L/R_s + d_{prop} + L/R_c$$

سمت چپ نابر ابری بالا نشان دهنده زمان مورد نیاز بسته دوم برای رسیدن به صفحه ورودی لینک دوم است (لینک دوم هنوز ارسال بسته دوم را شروع نکرده است). سمت راست نشان دهنده زمان مورد نیاز بسته اول برای پایان دادن به انتقال آن به لینک دوم است.

را چند ثانیه بعد ارسال کنیم، اطمینان حاصل می کنیم که هیچ تأخیری در صفحه برای بسته دوم در T اگر بسته دوم (لینک دوم وجود ندارد اگر:

$$\frac{L}{R_s} + \frac{L}{R_s} + d_{prop} + T \geq \frac{L}{R_s} + d_{prop} +$$

$$\frac{L}{R_c}$$

است $T = \frac{L}{R_c} - \frac{L}{R_s}$ بنا بر این، حداقل مقدار

مسئله 24

ترابایت = $8 * 12 * 10 * 40$ بیت. بنابراین، اگر از لینک اختصاصی استفاده کنید، $40 * 12 * 10 * 8 / 100$ می توانید تصمیم کنید که FedEx، 37 ثانیه = 3200000 روز طول می کشد. اما با تحویل یک شبه داده‌ها در یک روز می‌رسند و هزینه آن کمتر از 100 دلار است.

مسئله 25

(الف) 160000 بیت (ب) 160000 بیت (ج) حاصل ضرب تأخیر پهنه‌ای باند یک پیوند حداقل تعداد بیت هایی است که می تواند در

ارتباط. (د) عرض یک بیت = طول پیوند / محصول تأخیر پهنه‌ای باند، بنابراین 1 بیت 125 متر است

s/R (طولانی، که از زمین فوتیال بلندتر است ه

مسئله 26

$$s/R = 20000 \text{ km}, R = s/20000 \text{ km} = 2.5 * 10^8 / (2 * 10^7) = 12.5 \text{ bps}$$

مسئله 27

(الف) 80,000,000 بیت (ب) 800,000 بیت، به این دلیل است که حداقل تعداد بیت هایی که در پیوند وجود دارد

در هر زمان معین = دقیقه (محصول تأخیر پهنه‌ای باند، اندازه بسته) = 800000 بیت. (ج) 25 متر

مسئله 28

(الف) $ttrans + tprop = 400 \text{ msec} + 80 \text{ msec} = 480 \text{ msec}$.
 2 ثانیه. (ج) شکستن یک فایل برای انتقال بیشتر طول می کشد زیرا هر بسته داده و = (میلی ثانیه + 80 میلی ثانیه) 20

آن بسته تایید مربوطه تاخیرهای انتشار خود را اضافه می کند.

مسئله 29

به یاد بیاورید که ماهواره زمین ایستا 36000 کیلومتر از سطح زمین فاصله دارد. (الف) 150 میلی ثانیه
 (ب) 1,500,000 بیت (ج)
 600,000,000 بیت

مسئله 30

فرض کنید مسافر و چمدان هایش مطابق با واحد داده ای است که به بالای پشتہ بروتکل می رسد. وقتی مسافر تحويل میگیرد، چمدان های او چک می شود و یک برچسب روی چمدان ها و بلیط نصب می شود. این اطلاعات اضافی اضافه شده در لایه چمدان در شکل 1.20 که به لایه چمدان اجازه می دهد خدمات را اجرا کند یا مسافران و چمدان ها را در سمت ارسال کننده جدا کند و سپس آنها را (امیدوارم!) در سمت مقصد دوباره متحد کنند. هنگامی که یک مسافر از امنیت عبور می کند و اغلب مهر اضافی به بلیط او اضافه می شود که نشان می دهد مسافر از طریق بررسی امنیتی عبور کرده است. این اطلاعات برای اطمینان از انتقال امن افراد (مثالاً با بررسی های بعدی برای اطلاعات امنیتی) استفاده می شود.

مسئله 31

(الف) زمان ارسال پیام از میزبان مبدأ به سوئیچ بسته اول = ثانیه 4
 سوئیچینگ ذخیره و باز ارسال، کل زمان انتقال پیام از میزبان مبدأ به میزبان مقصد = ثانیه 12
 $= \times$ رازک

$\text{تعویض بسته اولین به میزبان منبع از جانب بسته خیلی ارسال به ب) زمان} = .$

$\text{زمانی که بسته دوم در اولین سوئیچ دریافت می شود} = \text{زمان. ثانیمتر } 5 \times 2 = 1$

$\text{که در آن بسته 1 در سوئیچ دوم} = \text{دریافت می شود}$
 $\text{ثانیمتر } 10 = \text{ثانیمتر } 5 \times 2$

$\text{میزبان مقصد را در اخذ شده است بسته خیلی که در ج) زمان} =$

$\text{پس از این، هر 5 میلی ثانیه یک بسته دریافت می شود. بدین ترتیب. ثانیمتر } 15 = \text{رازک} \times \text{ثانیمتر } 5$

$\text{ای. ثانیمتر } 14.4 = \text{sec} 01.4 \times 5^* 799 = \text{ثانیمتر } 15 = \text{زمانی که آخرین (800 امین) بسته دریافت می شود}$

$\text{مشاهده می شود که تاخیر در استفاده از تقسیم بندی پیام به طور قابل توجهی کمتر است (تقرباً 1/3)}$

(د)

بدون تقسیم بندی پیام، اگر خطاهای بیتی قابل تحمل نباشد، اگر یک خطای بیتی وجود داشته باشد، کل پیام باید دوباره ارسال شود (به جای یک بسته).

- ii) به شبکه ارسال می‌شوند. روتراها باید (HD مثلاً حاوی ویدیوهای) بدون تقسیم‌بندی پیام، بسته‌های بزرگ این بسته‌های عظیم را در خود جای دهند. بسته‌های کوچکتر باید پشت بسته‌های عظیم صفت بکشند و چهار تأخیرهای ناعادلانه شوند.

(e)

- بسته‌ها باید به ترتیب در مقصد قرار داده شوند. من بخش بندی پیام باعث ایجاد بسته‌های کوچکتر می‌شود. از آنجایی که اندازه سرصفحه معمولاً برای همه بسته‌ها بدون توجه به اندازه آنها یکسان است، با تقسیم بندی پیام، مقدار کل بسته‌های سرصفحه بیشتر است.

مسئله 32

بله، تأخیرهای اپلت با تأخیرهای مشکل 31 مطابقت دارد. تأخیرهای انتشار بر تأخیرهای کلی انتها به انتها هم برای سوئیچینگ بسته و هم برای تغییر پیام به طور یکسان تأثیر می‌گذارد.

مسئله 33

بیت است زمان دریافت آخرین بسته در اولین $S=80$ وجود دارد. هر بسته های F/S در دسترس هستند 2 F/S -2 ثانیه‌در این زمان، اولین بسته های $SF_+ \times 80 \text{ س}$ روتراست آر در روترا دوم است. سپس آخرین بسته باید توسط روترا اول و روترا دوم با هر انتقال ارسال شود $F/S-1$ مقصد، و بسته

ثانیه‌باین‌بار این تأخیر در ارسال کل فایل است آر، که منجر به حداقل تأخیر می‌شود S برای محاسبه مقدار $\text{delayd}S_{\leq 0} = 40 \text{ س}$

$$\text{تأخر } S = \frac{80 \times SF_+}{2}$$

مسئله 34

شبکه‌های تلفن سوئیچ مدار و اینترنت در «دروازه‌ها» به یکدیگر متصل هستند. هنگامی که یک کاربر اسکایپ (متصل به اینترنت) با یک تلفن معمولی تماس می‌گیرد، یک مدار بین یک دروازه و کاربر تلفن از طریق شبکه سوئیچ مدار برقرار می‌شود. صدای کاربر اسکایپ در بسته‌هایی از طریق اینترنت به دروازه ارسال می‌شود. در دروازه، سیگنال صوتی بازسازی می‌شود و سپس روی مدار ارسال می‌شود. در جهت دیگر، سیگنال صوتی از طریق شبکه سوئیچ مدار به دروازه ارسال می‌شود. دروازه سیگنال صوتی را بسته بندی می‌کند و بسته‌های صوتی را برای کاربر اسکایپ ارسال می‌کند.

فصل 2 سوالات مروری

اشتراك گذاري فايل; SMTP: پست الکترونيکي; HTTP: ورود از راه دور; Telnet: انتقال فايل; وب BitTorrent: پروتوكل

معماری شبکه به سازماندهی فرآيند ارتباط در لایه ها (مثلًا معماری اینترنت پنج لایه) اشاره دارد. از سوی دیگر،
معماری برنامه توسعه‌دهنده برنامه طراحی شده است و ساختار گسترده برنامه را دیگر می‌کند
مثلًا) (معماری برنامه توسعه‌دهنده برنامه طراحی شده است و ساختار گسترده برنامه را دیگر می‌کند
مشتری P2P مشتری-서버 يا

فرآيندي که ارتباط را آغاز می‌کند مشتری است. فرآيندي که منتظر تماس با آن است سرور است.

همتای که فایل را دریافت می‌کند، معمولاً کلاینت است و همتای که P2P خیر. در برنامه به اشتراك گذاري فايل.
فايل را ارسال می‌کند، معمولاً سرور است.

میزبان مقصد و شماره پورت سوکت در فرآيند مقصد IP آدرس.

تکمیل کرد - (RTT) تراکنش را می‌توان در یک زمان رفت و برگشت، UDP استفاده می‌کنید. با UDP از مشتری ارسال می‌کند، و سرور پاسخ را به سوکت UDP مشتری درخواست تراکنش را به سوکت و دیگری برای مشتری برای ارسال، TCP مورد نیاز است - یکی برای تنظیم اتصال RTT حداقل دو، درخواست، و برای سرور برای ارسال پاسخ.

با اين حال، از آنجايي که Google Docs يك از اين نمونه ها پردازش کلمه از راه دور است، به عنوان مثال، با Google Docs اجرا می‌شود، تضمين زمان‌بندی ارائه نمی‌شود (TCP با استفاده از) از طریق اینترنت.

الف) انتقال داده قابل اعتماد.

اینطور نیست UDP يك بایت جریان قابل اعتماد بین کلاینت و سرور فراهم می‌کند اما TCP

ب) تضميني برای حفظ مقدار مشخصی برای توان عملیاتی
هیچ کدام

ج) تضمین تحويل داده ها در مدت زمان مشخص
هیچ کدام

د) محرمانه بودن (از طریق رمزگذاری)
هیچ کدام

داده های رمزگذاری نشده را از لایه برنامه می‌گیرد، آنها را SSL در لایه برنامه عمل می‌کند. سوکت تقویت SSL با TCP ارسال می‌کند. اگر توسعه‌دهنده برنامه می‌خواهد TCP رمزگذاری می‌کند و سپس به سوکت را در برنامه اضافه کند SSL شود، باید کد

اگر دو نهاد ارتباط دهنده ابتدا بسته های کنترلی را قبل از ارسال داده به یکدیگر مبادله کنند، یک پروتکل از دست 10. این کار را نمی کند **HTTP** از دست دادن در لایه برنامه استفاده می کند در حالی که **SMTP** دادن استفاده می کند.

برنامه های کاربردی مرتبط با آن پروتکل ها مستلزم این هستند که تمام داده های برنامه به ترتیب صحیح و بدون 11. این کار را نمی کند **UDP** این سرویس را ارائه می دهد در حالی که **TCP** شکاف دریافت شوند.

هنگامی که کاربر برای اولین بار از سایت بازدید می کند، سرور یک شماره شناسایی منحصر به فرد ایجاد می 12. کند، یک ورودی در پایگاه داده پشتیبان خود ایجاد می کند و این شماره شناسایی را به عنوان یک شماره کوکی بر می گرداند. این شماره کوکی در هاست کاربر ذخیره می شود و توسط مرورگر مدیریت می شود. در طول هر بازدید (و خرید) بعدی، مرورگر شماره کوکی را به سایت ارسال می کند. بنابراین سایت می داند که این کاربر (به طور دقیق تر، این مرورگر) چه زمانی از سایت بازدید می کند.

که میزبان کاربر به آن **LAN** کش وب می تواند محتوای مورد نظر را به کاربر "نرديک تر" کند، احتمالاً به همان 13. متصل است. کش وب می تواند تأخیر را برای همه اشیا، حتی اشیایی که کش نیستند، کاهش دهد، زیرا کش باعث کاهش ترافیک روی لینک ها می شود.

به طور پیش فرض در ویندوز 7 موجود نیست. برای در دسترس قرار دادن آن، به کنترل پنل، برنامه ها 14. **Telnet** را بررسی کنید. برای راه اندازی **Telnet** و ویژگی ها، روشن یا خاموش کردن ویژگی های ویندوز، مشتری **telnet webserver 80** > در خط فرمان ویندوز، دستور زیر را صادر کنید

TCP بین برنامه **telnet** که در آن "وب سرور" برخی از وب سرورها است. پس از صدور فرمان، یک اتصال را تایپ کنید. یک مثال در زیر داده شده **HTTP GET** مشتری خود و وب سرور برقرار کرده اید. پس یک پیام 15. است:

در این وب سرور از جمعه، 18 مه 2007، ساعت 09:34:23 به وقت **index.html** از آنجایی که صفحه **Not Modified** گرینویچ تغییر نکرده است، و دستورات فوق در شنبه، 19 مه 2007 صادر شده است، سرور "304" و خطوط هد را توسط کاربر وارد **GET** را برگرداند. توجه داشته باشید که 4 خط اول پیام "Modified" پاسخ سرور وب است (**HTTP/1.1 304 Not Modified**) (304 شروع از) می شوند و 4 خط بعدی

استفاده می کند، یک اتصال برای ارسال اطلاعات کنترل (مانند درخواست TCP از دو اتصال موازی FTP برای انتقال یک فایل) و اتصال دیگر برای انتقال واقعی فایل. از آنجایی که اطلاعات کنترل از طریق همان اتصالی که اطلاعات کنترل را خارج از باند ارسال می کند FTP، فایل ارسال می شود ارسال نمی شود.

ارسال می شود. سپس سرور ایمیل آليس پیام را از HTTP به سرور ایمیل او از طریق Alice پیام ابتدا از میزبان 16. به میزبان خود POP3 به سرور ایمیل باب می فرستد. سپس باب پیام را از سرور ایمیل خود از طریق SMTP ارسال می کند.

17.

از جانب:	65.54.246.203 (LOO bay0-omc3-s3.bay0.hotmail.com)
:اخذ شده	(65.54.246.203) توسط mta419.mail.mud.yahoo.com با SMTP;Sat, 19 May 2007 16:53:51 -0700
:اخذ شده	با hotmail.com ([65.55.135.106]) توسط bay0-omc3-s3.bay0.hotmail.com از Microsoft SMTPSVC(6.0.3790.2668);Sat, 19 May 2007 16:52:42 - 0700
:اخذ شده	با Microsoft SMTPSVC(Sat, 19 May 2007 16:52:41 -0700) از سرویس دریافت نامه توسط hotmail.com
:شناسه پیام	<BAY130-F26D9E35BF59E0D18A819AFB9310@phx.gbl>
:اخذ شده	:شنبه، 19 May 2007 16:55.135.123 توسط by130fd.bay130.hotmail.msn.com با HTTP19 از 23:52:36، ساعت 2007 GMT
:از جانب	"پریتولا دنگل" <prithuladhungel@hotmail.com>
:به	prithula@yahoo.com
:کپی کپی:	
:موضوع	نامه آزمایشی
:تاریخ	Sat, 19 May 2007 23:52:36 +0000
Mime-Version: 1.0	نوع محتوا:
Text/html;format=flowed	مسیر بازگشت:
prithuladhungel@hotmail.com	

شکل: نمونه سرصفحه پیام ایمیل

پیام ایمیل را شامل مهرهای SMTP این فیلد هدر دنباله ای را نشان می دهد که در آن سرورهای Received: زمانی مربوطه ارسال و دریافت می کند.

در این مثال 4 خط سرصفحه "دریافت": وجود دارد. این بدان معناست که پیام ایمیل قبل از تحویل به صندوق عبور می کند. آخرین (چهارم) عنوان "دریافت شده": جریان پیام SMTP پسی گیرنده از 5 سرور مختلف در زنجیره سرورها را نشان می دهد. سرور SMTP فرستنده به دومین سرور SMTP ایمیل از سرور در زنجیره SMTP فرستنده در آدرس 65.55.135.123 و دومین سرور SMTP by130fd.bay130.hotmail.msn.com است.

در زنجیره به سرور سوم و غیره نشان می SMTP هدر سوم "دریافت شده": جریان پیام نامه را از سرور دوم دهد.

به آخرین سرور SMTP در نهایت، اولین هدر "دریافت شده": جریان پیام های ایمیل از سرور چهارم در زنجیره را نشان می دهد (یعنی سرور ایمیل گیرنده).

شناسه پیام: F26D9E35BF59E0D18A819AFB9310@phx.gbl
 این داده شده بوده دارد عدد BAY130-
 (توسط) bay0-omc3-
 یک رشته منحصر به فرد است که در هنگام ایجاد پیام برای اولین s3.bay0.hotmail.com.Message-id بار توسط سیستم پست اختصاص داده می شود.

نشان دهنده آدرس ایمیل فرستنده نامه است. در مثال داده شده، فرستنده: "prithuladhungel@hotmail.com" است.

است "To: prithula@yahoo.com" این قسمت آدرس ایمیل گیرنده نامه را نشان می دهد. در مثال، گیرنده:

موضوع: موضوع نامه را نشان می دهد (در صورت وجود مشخص شده توسط فرستنده). در مثال، موضوع مشخص شده توسط فرستنده "ایمیل آزمایشی" است.

تاریخ: تاریخ و ساعت ارسال نامه توسط فرستنده. در مثال، فرستنده نامه را در 19 مه 2007 در ساعت 23:52:36 GMT ارسال کرد.

که برای نامه استفاده می شود. در مثال، 1.0 است MIME نسخه: Mime.

است "Content-type: text/html" نوع محتوا در متن پیام ایمیل. در مثال:

اگر گیرنده این نامه بخواهد به فرستنده پاسخ دهد، آدرس ایمیلی را مشخص می کند که نامه به: Return-Path: آن ارسال می شود. این همچنین توسط سرور ایمیل فرستنده برای بازگرداندن پیام های ایمیل تحويل ناپذیر پیام های "استفاده می شود. در مثال، مسیر بازگشت mailer-daemon@hotmail.com" است.

بازیابی کرد، پیام ها حذف می POP با دانلود و حذف، پس از اینکه کاربر پیام های خود را از سرور 18. شوند. این یک مشکل برای کاربر عشایری ایجاد می کند، زیرا ممکن است بخواهد به پیام های بسیاری از دستگاه های مختلف (کامپیوتر اداری، کامپیوتر خانگی و غیره) دسترسی پیدا کند. در پیکربندی دانلود و نگهداری، پیام ها پس از بازیابی پیام ها توسط کاربر حذف نمی شوند. این همچنین می تواند ناخوشایند باشد، زیرا هر بار که کاربر پیام های ذخیره شده را از یک دستگاه جدید بازیابی می کند، همه پیام های حذف نشده (از جمله پیام های بسیار قدیمی) به دستگاه جدید منتقل می شود.

بله سرور ایمیل و وب سرور یک سازمان می توانند نام مستعار یکسانی برای نام میزبان داشته باشند. رکورد 19. آن استفاده می شود IP برای نگاشت نام میزبان ایمیل سرور به آدرس MX.

ببینید. اما اگر کاربر از اکانت جیمیل استفاده edu. فرستنده را برای کاربری با آدرس ایمیل IP باید بتواند آدرس 20. فرستنده را ببینید IP کند، نمی تواند آدرس

لازم نیست که باب نیز تکه هایی را در اختیار آلیس فراز دهد. آلیس باید در 4 همسایه برتر باب باشد تا باب تکه هایی را برای او بفرستد. این ممکن است رخ ندهد حتی اگر آلیس در یک بازه 30 ثانیه ای تکه هایی را به باب ارائه دهد.

یک همتأیک همتأی تصادفی را انتخاب می کند و به طرز خوش بینانه ای، BitTorrent به یاد بیبورید که در 22. همتأی را برای مدت کوتاهی خفه می کند. بنابراین، آليس در نهایت توسط یکی از همسایه هایش به طرز خوش بینانه ای خفه می شود و در این مدت از آن همسایه تکه هایی دریافت می کند.

شرکت کننده 23. از گره ها تشکیل شده است شبکه همپوشانی در یک سیستم اشتراک فایل وجود داشته B و A بین TCP در سیستم اشتراک فایل و پیوندهای منطقی بین گره ها. اگر یک اتصال نیمه دائمی وجود دارد. شبکه همپوشانی B به گره A باشد، یک پیوند منطقی (یک "لبه" در شرایط تئوری گراف) از گره شامل روتزها نمی شود.

مزیت این است که برای یک پیام به همتأی (با شناسه) که نزدیکترین به کلید است، فقط یک پرش 24. Mesh DHT: دایرہ ای: مزیت DHT ردیابی کند DHT لازم است. نقطه ضعف این است که هر همتأی باید تمام همتأیان دیگر را در برای مسیریابی O(n) hops این است که هر همتأی باید فقط چند همتأی دیگر را ردیابی کند. نقطه ضعف این است که یک پیام به همتأی که نزدیکترین به کلید است مورد نیاز است.

- 25.
- (الف) توزیع فایل (ب) پیام رسانی
 - فوری (ج) جریان ویدئو (د)
 - محاسبات توزیع شده

سوکت خوشنامگویی وجود ندارد و تمام اطلاعات کلاینت های مختلف از طریق همین یک UDP با سرور 26. یک سوکت خوشنامگویی وجود دارد و هر بار که یک مشتری اتصال به TCP سوکت وارد سرور می شود. با سرور $n+1$ اتصال هم زمان، سرور به n سرور را آغاز می کند، یک سوکت جدید ایجاد می شود. بنابراین، برای پشتیبانی از سوکت نیاز دارد.

را با سرور آغاز کند. اگر سرور TCP به محض اجرای کلاینت، سعی می کند یک اتصال 27. TCP برای برنامه کلاینت بلا فاصله پس از UDP، در حال اجرا نباشد، کلاینت قادر به برقراری اتصال نخواهد بود. برای برنامه TCP (نمی کند UDP یا تلاشی برای برقراری ارتباط با سرور) اجرا اتصالات را آغاز نمی کند.

فصل 2 مسائل

مشکل 1

- (الف) F
- (ب) T
- (ج) F
- (د) F
- (ه) F

مشکل 2

دستورات کنترل سترسی: USER، PASS، ACT، CWD، CDUP، SMNT، REIN، QUIT.

دستورات پارامتر انتقال PORT، PASV، TYPE STRU، MODE.

دستورات سرویس: RETR، STOR، STOU، APPE، ALLO، REST، RNFR، RNTO، ABOR، DELE، RMD، MRD، PWD، LIST، NLST، SITE، SYST، STAT، HELP، NOOP.

مشکل 3

پروتکل های لایه برنامه: DNS و HTTP برای DNS.TCP برای HTTP

مشکل 4

نام سرور و : Host بود. فایل http://gaia.cs.umass.edu/cs453/index.html درخواست سند /cs453/index.html نام فایل را نشان می دهد.

نسخه 1.1 را اجرا می کند، همانطور که درست قبل از اولین نشان داده شد جفت HTTP (ب) مرورگر

نشان داده شده است Connection: keep-alive (ج) مرورگر درخواست اتصال دائمی دارد، همانطور که توسط

وجود ندارد. بنابراین هیچ راهی برای تشخیص HTTP (د) این یک سوال ترفند است. این اطلاعات در هیچ کجا پیام وجود ندارد. برای پاسخ به این سوال، باید اطلاعاتی از دیتابرام HTTP این موضوع از نگاه کردن به تبادل پیام های حمل می کرد (را حمل می کرد) TCP GET را که درخواست IP های

۵.۰ اطلاعات نوع مرورگر توسط سرور برای ارسال نسخه های مختلف یک شی به انواع مختلف مرورگرها مورد نیاز است.

مشکل 5

نشان می دهد که سرور توانسته است سند را با موقتی پیدا کند. پاسخ در سهشنبه، OK کد وضعیت 200 و عبارت (ا) 7 مارس 2008، ساعت 12:39:45 به وقت گرینویچ ارائه شد.

آخرین بار در شنبه 10 دسامبر 2005 ساعت 18:27:46 به وقت گرینویچ اصلاح شد index.html (ب) سند.

(ج) 3874 بایت در سند در حال بازگشت وجود دارد.

(د) پنج بایت اول سند برگشتی عبارتند از

مشکل 6

هدف واقعی این سوال این بود که شما را (ا) مورد بحث قرار گرفته است RFC 2616 (الف) اتصالات پایدار در بخش 8 بخش 8.1.2 و 8.1.2.1 از (کنید RFC و ادار به بازیابی و خواندن یک

نشان می دهد که مشتری یا سرور می تواند به دیگری نشان دهد که اتصال دائمی را می بندد. این کار را با RFC انجام می دهد درخواست/پاسخ http درخواست "close" Connection-header در قسمت "close" گذاندن نشانه اتصال.

مشتریانی که از اتصالات دائمی استفاده می» (RFC 2616 از) (هیچ خدمات رمزگذاری ارائه نمی دهد. ج) (ب) اتصالات همزمانی که آنها به یک سرور معین حفظ می کنند. یک کلاینت تک کاربره نباید بیش از 2 اتصال را با کنند باید تعداد

اتصالات همزمانی که آنها به یک سرور معین حفظ می کنند. یک کلاینت تک کاربره نباید بیش از 2 اتصال را با "هیچ سرور یا پروکسی حفظ کند".

یک مشتری ممکن است همزمان با تصمیم سرور برای بستن اتصال "بیکار" شروع به " (RFC 2616 از). د) به ارسال یک درخواست جدید کرده باشد. از نظر سرور، اتصال در حالی که بیکار بود بسته می شود، اما از نظر مشتری، یک درخواست در حال انجام است.

مسئله 7

است IP کل مدت زمان دریافت آدرس

$$RTT_1 + RTT_2 + \dots + nRTT$$

و دیگری تنظیم شود TCP می گزند تا اتصال ORTT و دیگری تنظیم شود TCP می گزند تا اتصال ORTT

برای درخواست و دریافت شی کوچک می گزند. کل زمان پاسخگویی است ORTT

$$2RTT_1 + RTT_2 + \dots + RTT_n$$

مسئله 8

(ا)

$$\begin{aligned} & RTT_1 + \dots + RTT_n + 2RTT_o + 2 \cdot RTT_o \\ & = 18 \cdot RTT_o + RTT_1 + \dots + RTT_n. \end{aligned}$$

(ب)

$$\begin{aligned} & RTT_1 + \dots + RTT_n + 2RTT_o + 2 \cdot 2RTT_o \\ & = 6RTT_o + RTT_1 + \dots + RTT_n \end{aligned}$$

(ج)

$$\begin{aligned} & RTT_1 + \dots + RTT_n + 2RTT_o + RTT_o \\ & = 3 \cdot RTT_o + RTT_1 + \dots + RTT_n. \end{aligned}$$

مسئله 9

است. میانگین زمان، اندازه متوسط جسم تقسیم L/R بر روی یک پیوند یا نرخ L (الف) زمان انتقال یک شی با اندازه R بر:

$$\Delta = \frac{0.0567}{(85000000 \text{ بیت در ثانیه}) / (\text{بیت 0.0567})}$$

داده می $= 0.0567$ (در خواست در ثانیه) $= \beta \Delta$ شدت ترافیک روی پیوند با شود. بنابراین، میانگین تأخیر دسترسی $(0.0567 \text{ ثانیه}) / (0.907 \text{ ثانیه}) \approx 0.6$ ثانیه است. بنابراین میانگین کل زمان پاسخ $0.6 \text{ ثانیه} + 3 \text{ ثانیه} = 3.6 \text{ ثانیه}$ است.

ب) شدت ترافیک در لینک دسترسی 60 درصد درخواست ها در شبکه سازمانی برآورده می شود. بنابراین میانگین تأخیر دسترسی $0.0567 = 0.089 / (0.907 \cdot (4.0 - 1))$ ثانیه است. اگر درخواست توسط حافظه پنهان (که با احتمال 0.6 اتفاق می افتد) زمان پاسخ تقریباً صفر است. میانگین زمان پاسخ $0.089 \text{ ثانیه} + 3 \text{ ثانیه} = 3.089 \text{ ثانیه}$ برای از دست دادن حافظه پنهان است (که در 40٪ موقع اتفاق می افتد). بنابراین میانگین زمان پاسخ $0.089 \text{ ثانیه} + 3.089 \text{ ثانیه} = 1.24 \text{ ثانیه}$ است. بنابراین میانگین زمان پاسخ از 3.6 ثانیه به 1.24 ثانیه کاهش می یابد.

مسئله 10

نشان دهنده T_p توجه داشته باشد که هر شیء دانلود شده را می توان به طور کامل در یک بسته داده قرار داد. بگذارید تاخیر انتشار یک طرفه بین مشتری و سرور باشد.

ابتدا دانلودهای موازی را با استفاده از اتصالات غیر دائمی در نظر بگیرید. دانلودهای موازی به 10 اتصال اجازه می دهد تا پهنهای باند 150 بیت در ثانیه را به اشتراک بگذارند و به هر کدام فقط 15 بیت در ثانیه می دهد. بنابراین، کل زمان مورد نیاز برای دریافت همه اشیا به صورت زیر داده می شود:

$$\begin{aligned} & (200/150 + T_p + 200/150 + T_p + 200/150 + T_p + 100,000/150 + T_p) + \\ & (200/(150/10) + T_p + 200/(150/10) + T_p + 200/(150/10) + T_p + 100,000/(150/10) + T_p) \\ & = 7377 + 8 * T_p \text{ (ثانیه)} \end{aligned}$$

دانمی را در نظر بگیرید. کل زمان مورد نیاز توسط HTTP اکنون یک اتصال:

$$(200/150+Tp + 200/150+Tp + 200/150+Tp + 100,000/150+Tp) \\ + 10*(200/150+Tp + 100,000/150+Tp) \\ = 7351 + 24*Tp \text{ ثانیه)$$

در Tp میکروثانیه. بنابراین $Tp=10/(300*10^6)=0.03$ با فرض سرعت نور 300 m/sec، مقایسه با تأخیر انتقال ناچیز است.

مداوم به طور قابل توجیهی سریعتر (کمتر از 1 درصد) از حالت غیر مداوم با دانلود موازی HTTP بنابراین، می بینیم که نیست.

مشکل 11 الف) بله، چون باب ارتباطات بیشتری دارد، می تواند سهم بیشتری از پیوند را به دست آورد

پهنهای باند) بله، باب هنوز نیاز به دانلود موازی دارد. در غیر این صورت او کمتر خواهد گرفت

پهنهای باند نسبت به چهار کاربر دیگر

مسئله 12

Server.py

```
az وارد کردن سوکت * serverPort=12000
serverSocket=socket(AF_INET,SOCK_STREAM)
serverSocket.bind(('',serverPort))
serverSocket.listen(1)
connectSocket, addr = serverSocket.accept()
در حالی که 1 ():
    چاپ "از connectionSocket.recv(1024) جمله،
        "سرور" \n"
serverSocket.close()
```

مسئله 13

را شناسایی می SMTP است که فرستنده پیام ایمیل به سرور SMTP پیامی از مشتری MAIL FROM: در نیست، بلکه فقط یک خط در بدن پیام ایمیل است SMTP کند. از: روی پیام ایمیل خود یک پیام

مسئله 14

از "فیلد سرصفحه HTTP" از خطی استفاده می کند که فقط حاوی نقطه است تا پایان متن پیام را مشخص کند SMTP نمی تواند از روش استفاده شده توسط HTTP، طول محتوا" برای نشان دادن طول متن پیام استفاده می کند. خبر بدنی پیام باید در SMTP می تواند داده های باینری باشد، در حالی که در HTTP استفاده کند، زیرا پیام ASCII 7 بیتی باشد قالب.

مسئله 15

می فرسنده پیام دنباله ای از MTA است. یک میزبان پیام را به یک Mail Transfer Agent (MTA) مخفف می فرماید. این پیام دنبال MTA ها را دنبال می کند تا به ایمیل خوان گیرنده برسد. می بینیم که این پیام هر زمانه زنگره ای از MTA، صادق باید گزارش دهد که از کجا پیام را دریافت می کند. توجه داشته باشید که در این پیام MTA می کند. یک از جایی که ایمیل را دریافت کرده است، گزارش نمی دهد. از آنجایی که ما "asus-4b96 ([58.88.21.177])" را دریافت کردیم فرض می کنیم که فقط مبتکر ناصادق است، بنابراین باید مبتکر باشد «asusus-4b96 ([58.88.21.177])».

مسئله 16

UIDL دستور POP3 را نشان می دهد. هنگامی که یک سرویس گیرنده "unique-ID listing" به اختصار UIDL را صادر می کند، سرور با شناسه پیام منحصر به فرد برای همه پیام های موجود در صندوق پستی کاربر پاسخ می دهد. این دستور برای "دانلود و نگه داشتن" مفید است. با نگهداری فایلی که پیام های بازیابی شده در جلسات قبلی را برای تعیین اینکه کدام پیامها در سرور قبلاً دیده شده اند استفاده کند. UIDL فهرست می کند، مشتری می تواند از دستور

مسئله 17

(الف) C: dele 1 C:
retr 2 S: (بله بلا)
(... س:بله
S: .

C: 2 خروج از: C:
خاموش شدن POP3 تأیید سرور +

(ب) ج: retr 2 س:
بلا بلا ... س:
.....بله س: ..

در حال خاموش S: +OK ج: خروج از
POP3 شدن سرور

ج) ج: فهرست S:

1 498 S: 2

912 S: رتر.

1 س: بلا س:

بله س: ج :

رتر 2 س: بلا بلا

: س :

بله س..... : .

در حال خاموش S: +OK ج: خروج از
شدن سرور POP3

مسئله 18

می تواند whois یا نام مدیر شبکه، پایگاه داده IP آدرس، (الف) برای یک ورودی معین از نام دامنه و غیره استفاده شود DNS سرور، whois برای مکان یابی ثبت کننده مربوطه، سرور

(ب) NS4.YAHOO.COM از www.register.com NS1.MSFT.NET از www.register.com

ج) دامنه محلی www.mindspring.com
سرورهای وب www.mindspring.com

207.69.189.21, 207.69.189.22,
207.69.189.23, 207.69.189.24,
207.69.189.25, 207.69.189.26,
207.69.189.26, 207.69.26, 207.69.189.23.

سرورهای پست الکترونیکی mx1.mindspring.com
(207.69.189.217) mx2.mindspring.com
(207.69.189.218) mx3.mindspring.com
(207.69.189.219) mx4.mindspring.com (20.20
سرورهای نام itchy.earthlink.net (207.69.188.196)
scratchy.earthlink.net (207.69.188.197)

www.yahoo.com: وب سرورها www.yahoo.com (216.109.112.135,
66.94.234.13: سرورهای پست الکترونیکی a.mx.mail.yahoo.com
(209.191.118.103)

b.mx.mail.yahoo.com (66.196.97.250)
c.mx.mail.yahoo.com (68.142.237.182,
216.39.53.3) d.mx.mail.yahoo.com (216.39.53.2)
e.m mail.yahoo.com (216.39.53.1)
f.mx.mail.yahoo.com (209.191.88.247, 68.142.202.247)

g.mx.mail.yahoo.com (209.191.88.239, 206.190.53.191)
 سرورهای نام: ns1.yahoo.com (66.218.71.63)
 ns2.yahoo.com (68.142.255.16)
 ns3.yahoo.com (217.12.4.104)
 ns4.yahoo.com
 (68.142.196.196.68.143.196.196.142.196.68.142.196.196.142.196.68.142.255.16)
 .116.17) ns8.yahoo.com (202.165.104.22)
 ns9.yahoo.com (202.160.176.146)

سرورهای وب www.hotmail.com: www.hotmail.com
 (64.4.33.7, 64.4.32.7)

سرورهای ایمیل mx1.hotmail.com (65.54.245.8, 65.54.244.8, 65.54.244.136)
 mx2.hotmail.com (65.54.244.40, 65.54.244.168, 65.54.245.40)
 mx3.hotmail.com (65.54.244.72, 65.54.244.200, 645.4.200,
 64.4.25 0.232, 65.54.245.104, 65.54.244.104)

سرورهای نام: ns1.msft.net (207.68.160.190)
 ns2.msft.net (65.54.240.126) ns3.msft.net
 (213.199.161.77) ns4.msft.net
 (207.46.66.5ns.5) ns4.msft.net
 (207.46.66.5ms.5) .238.126)

دارد IP د) وب سرور یاهو چندین آدرس
 www.yahoo.com (216.109.112.135, 66.94.234.13)

۵) محدوده آدرس دانشگاه پی تکنیک: 128.238.255.255 – 128.238.0.0

استفاده کند IP برای تعیین آدرس nslookup و ابزار whois و) یک مهاجم می تواند از پایگاه داده و، غیره، برای موسسه مورد نظر، DNS، محدوده، آدرس سرور

برای به دست آوردن اطلاعات در مورد whois (ز) با تجزیه و تحلیل آدرس منبع بسته های حمله، قربانی می تواند از دامنه ای که از آن حمله می شود استفاده کند و احتمالاً به مدیران دامنه مبدأ اطلاع دهد.

مسئله 19

(الف) زنجیره نمایندگی زیر برای gaia.cs.umass.edu a.root-servers.net
 استفاده می شود
 E.GTLD-SERVERS.NET
 ns1.umass.edu (معتبر)

دستور اول: dig +norecurse @a.root-servers.net any
 gaia.cs.umass.edu

اینج 172800.edu: بخش مرجع;;

edu.	اینج 172800	NS	E.GTLD-SERVERS.NET.
edu.	اینج 172800	NS	A.GTLD-SERVERS.NET.
edu.	اینج 172800	NS	G3.NSTLD.COM.
edu.	اینج 172800	NS	D.GTLD-SERVERS.NET.
edu.	اینج 172800	NS	H3.NSTLD.COM.
edu.	اینج 172800	NS	L3.NSTLD.COM.
edu.	اینج 172800	NS	M3.NSTLD.COM.
edu.	اینج 172800	NS	C.GTLD-SERVERS.NET.

بازگشتی، ما یک پرس و جو به اولین مورد ارسال می DNS در میان تمام سرورهای edu کنیم.dig +norecurse @E.GTLD-SERVERS.NET هر gaia.cs.umass.edu

umass.edu.	اینج 172800	NS	ns1.umass.edu.
umass.edu.	اینج 172800	NS	ns2.umass.edu.
umass.edu.	اینج 172800	NS	ns3.umass.edu.

معتبر بازگشتی، ما یک پرس و جو به اولین سرور ارسال می کنیم DNS در بین هر سه سرور +norecurse @ns1.umass.edu هر gaia.cs.umass.edu

gaia.cs.umass.edu. 21600 اینج آ 128.119.245.12

می تواند این باشد (ب) پاسخ google.com: a.root-servers.net

E.GTLD-SERVERS.NET
ns1.google.com (معتبر)

مسئله 20

محلى یک عکس فوري بگيريم. وب DNS در سرورهای DNS می توانیم به طور دورهای از حافظه های پنهان ظاهر می شود، محبوب ترین سرور است. این به این دلیل است که اگر کاربران DNS سروری که اغلب در کش های برای آن سرور بیشتر توسط کاربران ارسال می DNS بیشتری به یک وب سرور علاقه مند باشند، درخواست های ظاهر می شود DNS شود. بنابراین، آن وب سرور بیشتر در کش های

برای یک مطالعه اندازه گیری کامل، نگاه کنید به: کریگ ای. ویز، میخانیل میخانیلوف، هانو شانگ «استنتاج IMC'03 در، «DNS محبوبیت نسبی برنامه های کاربردی اینترنتی با پرس و جو فعالانه حافظه پنهان 27- اکتبر 2003، میامی بیچ، فلوریدا، ایالات متحده آمریکا 29

مسئله 21

محلى استفاده کنیم DNS برای پرس و جو از آن وب سایت در سرور dig بله، ما می توانیم از

را برمی گرداند. اگر چند ثانیه پیش به `cnn.com` زمان پرس و جو برای یافتن "dig `cnn.com`" ذخیره می شود، بنابراین زمان پرس و DNS در حافظه نهان محلی `cnn.com` دسترسی داشتید، ورودی `cnn.com` 0 میلی ثانیه است. در غیر این صورت، زمان پرس و جو زیاد است.

مسئله 22

برای محاسبه حداقل زمان توزیع برای توزیع مشتری-سرور، از فرمول زیر استفاده می کنیم:

$D_{cs} = \max \{NF/us, F/d_{min}\}$ به طور مشابه، برای محاسبه حداقل زمان توزیع از فرمول زیر استفاده می کنیم، P2P برای توزیع:

$$D_p = \frac{F/d_{max}}{u} = \frac{NF/(u_s + \sum u_i)}{u}$$

گیگابیت = $15 \times 1024 = 15360$ ، جایی که

مگابیت ما = 30 مگابیت بر ثانیه

$d_{min} = di = 2 \text{ Mbps}$

$Kbps = 300/1024$ توجه داشته باشید،
Mbps.

سرور مشتری

	N	10	100	1000
کیلوبیت بر 300	7680	51200	512000	
کیلوبیت بر 700 ثانیه	7680	51200	512000	
مگابیت بر 2 ثانیه	7680	51200	512000	

نظیر به نظیر

	N	10	100	1000
کیلوبیت بر 300	7680	25904	47559	
کیلوبیت بر 700 ثانیه	7680	15616	21525	
مگابیت بر 2 ثانیه	7680	7680	7680	

مسئله 23

(الف) یک طرح توزیع را در نظر بگیرید که در آن سرور فایل را به صورت موازی برای هر کلاینت با نرخ us/N ارسال می کند. توجه داشته باشید که این نرخ کمتر از هر یک از نرخ دانلود مشتری است، زیرا با فرض $us/N \leq d_{min}$ دریافت کند. از آنجایی که هر کلاینت با نرخ N / بنابراین هر مشتری همچنین می تواند با نرخ ما است. از آنجایی که همه $F/(us/N) = NF/us$ دریافت می کند، زمان دریافت کل فایل برای هر مشتری NF/us است. دریافت می کند، زمان کلی توزیع نیز NF/us مشتریان فایل را در

(ب) یک طرح توزیع را در نظر بگیرید که در آن سرور فایل را به صورت موازی برای هر کلاینت با نرخ d_{min} کمتر از نرخ پیوند سرور به ما است، زیرا با فرض N ارسال می کند. توجه داشته باشید که نرخ کل دریافت می کند، زمان دریافت کل فایل برای هر کلاینت d_{min} از آنجایی که هر کلاینت با نرخ $\geq d_{min}$ است. از آنجایی که همه کلاینت ها فایل را در این زمان دریافت می کنند، زمان کلی توزیع نیز F/d_{min} است.

(ج) از بخش 2.6 ما می دانیم که

$$D \cdot CS \geq \max \{NF/us, F/d_{min}\} \quad (معادله 1)$$

$D \cdot CS \leq NF/us$ داریم. اما از (الف) $DCS \geq NF/us$ سپس از معادله 1. $us/N \leq d_{min}$ فرض کنید که داریم. از ترکیب این دو به دست می آید:

$$D \cdot CS = NF/us \leq d_{min}. \quad (معادله 2)$$

به همین ترتیب می توانیم نشان دهیم که

$$D \cdot CS = F/d_{min} \quad us/N \geq d_{min}. \quad (معادله 3)$$

ترکیب معادله 2 و معادله 3 نتیجه مطلوب را می دهد.

مسئله 24

(الف) $u = u_1 + u_2 + \dots + u_N$ را تعریف کنید. با فرض $us \leq (u_1 + u_2 + \dots + u_N)/N$

$$us \leq (us + u)/N \quad (معادله 1)$$

$ri = ui$ را با نرخ i^{th} سرور قسمت $F/(ui/u)$ دارای اندازه $|$ قسمت تقسیم کنید که قسمت N فایل را به به طوری که نرخ کل $r_1 + r_2 + \dots + r_N = us$ ارسال می کند. توجه داشته باشید که $|$ به همتأثر us/u سرور از نرخ پیوند سرور تجاوز نکند. همچنین از هر همتأثر خواهید که بیت های دریافتی خود را با نرخ است. ما داریم $ri = (N-1)u/(N-1)$ ارسال کن. نرخ کل ارسال توسط همتأثر $N-1$ هر یک از همتأثرا

$$(N-1)ri = (N-1)(usui)/u \leq ui,$$

کمتر از نرخ پیوند آن $|$ که در آن آخرین نابرابری از معادله 1 به دست می آید. بنابراین نرخ کل ارسال همتأثر است us .

بیت های را با نرخ کل دریافت می کند $|$ در این طرح توزیع، همتأثر

$$r_1 + \sum_{i=2}^N r_i = us$$

دریافت می کند F/us بنابراین هر همتأثر فایل را در

را تعریف کنید. با فرض $u = u_1 + u_2 + \dots + u_N$ دوباره

$$us \geq (us + u)/N \quad \text{معادله 2}$$

$$\begin{aligned} ri &= ui / (N-1) \\ rN+1 &= (us - u/(N-1))/N \end{aligned}$$

$i = 1$ ، $N-1$ می رساند به هر یک از همتایان ri بیت هایی را که با نرخ r ارسال می کند. هر همتا ri با نرخ $(N+1)$ ، N به هر یک از $rN+1$ با نرخ $(N+1)$ دیگر ارسال می کند. علاوه بر این، سرور بیت هایی را از قسمت فوروارد نمی کند. همتایان ri همها ارسال می کنند.

نرخ ارسال مجموع سرور است

$$r1 + \dots + rN + N rN+1 = u/(N-1) + \dots - u/(N-1) = \text{ما}$$

است ا بنابراین، نرخ ارسال سرور از نرخ پیوند آن تجاوز نمی کند. نرخ ارسال مجموع همتا

$$(N-1)ri = ui$$

بیت ا بنابراین، نرخ ارسال هر همتا از نرخ پیوند آن تجاوز نمی کند. در این طرح توزیع، همتا ها را با نرخ کل دریافت می کند

$$n((\frac{1}{n} - \frac{1}{n-1}) + \dots + \sum_{j=n}^{n-1} (\frac{1}{n-j} - \frac{1}{n-(j+1)})) = n(\text{نیور} - \text{نیور}^*)$$

دریافت می کند. (برای سادگی، از تعیین اندازه قسمت $(us + u)/N$ فایل را به صورت peer بنابراین هر $\Delta = \Delta$ غفلت کردیم. اکنون آن را در اینجا ارائه می دهیم. اجازه دهد $N+1 = i$ فایل برای بیت است $\Delta = ri$ قسمت فایل $, N, \dots, 1 = i$. زمان توزیع باشد

$$F_1 + \dots + F_N + 1 = F$$

ج) راه حل این قسمت مشابه 17 (ج) است. ما از بخش 2.6 می دانیم که

$$D_p \geq 2, NF / (umax\{F/u\} + u)$$

ترکیب این با (الف) و (ب) نتیجه دلخواه را می دهد.

مسئله 25

وجود دارد $N(N-1)/2$ گره در شبکه همپوشانی وجود دارد. لیهه های

مسئله 26

آره. اولین ادعای او تا زمانی ممکن است که همتایان کافی برای مدت طولانی در ازدحام باقی بمانند. باب همیشه می‌تواند داده‌ها را از طریق رفع خفگی خوش بینانه توسعه سایر همتایان دریافت کند.

ادعای دوم او نیز درست است. او می‌تواند یک کلاینت را روی هر میزبان اجرا کند، به هر کلاینت اجازه دهد «رایگان» برود، و تکه‌های جمع‌آوری شده از میزبان‌های مختلف را در یک فایل واحد ترکیب کند. او حتی می‌تواند یک برنامه زمان‌بندی کوچک بنویسد تا میزبان‌های مختلف بخش‌های مختلف فایل را بخواهد. این در واقع نوعی حمله P2P در شبکه‌های Sybil است.

می‌آموزد که نظری 5 به تازگی سیستم را ترک کرده است، بنابراین 3 Peer 3 را می‌خواهد (Peer 8) شناسه جانشین بالافصل خود (Peer 4) از اولین جانشین خود را دومین جانشین خود خواهد کرد peer 8 سپس.

مسئله 28

همتای 6 ابتدا پیامی برای همتای 15 می‌فرستد که می‌گوید "سلف و جانشین همتای 6 چه خواهد بود؟" این پیام از ارسال می‌شود تا زمانی که به همتای 5 برسد، که متوجه می‌شود که سلف 6 خواهد بود و جانشین DHT طریق این اطلاعات سلف و جانشین را به 6 ارسال می‌کند peer 5، فعلی آن، نظری 8، جانشین 6 خواهد شد. در مرحله بعد که باید جانشین 5 peer جانشین خود و با اطلاع دادن به 8 peer اکنون می‌تواند با قرار دادن 6 Peer بپیوندد DHT فوری خود را به 6 تغییر دهد به.

مسئله 29

بین خودش و همه همتاها را محاسبه می‌کنیم و سپس کلید را در (k, p) با استفاده از (برای هر کلید، ابتدا فاصله ها همتای نزدیک به کلید) (یعنی با کمترین مقدار فاصله) ذخیره می‌کنیم.

مسئله 30

بله، تخصیص تصادفی کلیدها به همتایان اصلًا شبکه اصلی را در نظر نمی‌گیرد، بنابراین به احتمال زیاد باعث عدم تطابق می‌شود.

شامل تنها دو پیوند) p_1 چنین عدم تطابق ممکن است عملکرد جستجو را کاهش دهد. به عنوان مثال، یک مسیر منطقی همتاهای همسایه C و B و A و B و A که در آن، A à B à C، برای نظر بگیرید (منطقی وجود دارد (شامل 3 پیوند منطقی) C به A از p_2 هستند. فرض کنید یک مسیر منطقی دیگر

از نظر C و B از نظر فیزیکی بسیار دور باشند (و توسط روترهای زیادی از هم جدا شده اند)، و B و A ممکن است فیزیکی بسیار دور باشند (و توسط روترهای زیادی از هم جدا شده اند). ولی

همگی از نظر فیزیکی بسیار نزدیک باشند (و همه توسط روترهای کمی از هم جدا شده C، D، E، A ممکن است. اند). به عبارت دیگر، یک مسیر منطقی کوتاهتر ممکن است با یک مسیر فیزیکی بسیار طولانی‌تر مطابقت داشته باشد.

مسئله 31

TCP را اجرا کنید، کلاینت تلاش خواهد کرد تا با یک فرآیند سرور ناموجود یک اتصال TCPClient (الف) اگر ابتدا TCP را ایجاد نخواهد شد اتصال TCP ایجاد کند. اتصال

را اجرا کنید، سپس UDPClient با سرور برقرار نمی‌کند. بنابراین، اگر ابتدا TCP یک اتصال UDPClient (ب) را اجرا کنید، و سپس مقداری ورودی را در صفحه کلید تایپ کنید، همه چیز باید خوب کار کند UDPServer.

(ج) اگر از شماره‌های پورت مختلف استفاده می‌کنید، کلاینت سعی می‌کند با فرآیند اشتیاه یا فرآیندی که وجود ندارد، یک برقرار کند. خطاهای رخداد خواهد داد TCP اتصال

مسئله 32

هنگام ایجاد سوکت، شماره پورت را مشخص نمی‌کند. در این مورد، کد به سیستم UDPClient، در برنامه اصلی اجرا می‌شود، یک UDPClient عامل اصلی اجازه می‌دهد شماره پورت را انتخاب کند. با خط اضافی، هنگامی که با شماره پورت 5432 ایجاد می‌شود UDP سوکت

باید شماره پورت کلاینت را بداند تا بتواند بسته‌های را به سوکت مشتری صحیح بازگرداند. با نگاهی به UDPServer شماره UDPServer، می‌بینیم که شماره پورت مشتری به کد سرور متصل نشده است. در عوض، UDPServer با هر شماره پورت UDP پورت کلاینت را با بازگردان دیتاگرام دریافتی از مشتری تعیین می‌کند. بنابراین سرور نیازی به تغییر ندارد UDPServer مشتری از جمله 5432 کار می‌کند. بنابراین

: قبل از

انتخاب شده توسط) $x = \text{سوکت کلاینت}$
 $\text{سوکت سرور} = 9876$ (سیستم عامل

: بعد از

$5432 = \text{سوکت مشتری}$

مسئله 33

بله، می‌توانید بسیاری از مرورگرهای باز کردن چندین اتصال همزمان به یک وب سایت پیکربندی کنید. مزیت این است که به طور بالقوه فایل را سریعتر دانلود خواهید کرد. این

عیب آن است که ممکن است پهنای باند را افزایش دهید و در نتیجه سرعت دانلود سایر کاربرانی که پیوندهای فیزیکی مشابهی را به اشتراک می‌گذارند، به میزان قابل توجهی کاهش می‌پابد.

مسئله 34

یک پروتکل بایت گرا بسیار طبیعی است زیرا هیچ مفهومی از، (ssh ثابت و) برای برنامه هایی مانند ورود از راه دور مرزهای پیام در برنامه وجود ندارد. هنگامی که کاربر یک کاراکتر را تایپ می‌کند، ما به سادگی آن کاراکتر را در رها می‌کنیم TCP اتصال

در برنامه های کاربردی دیگر، ممکن است یک سری پیام ارسال کنیم که مرزهای ذاتی بین آنها وجود دارد. به دیگری چندین پیام ایمیل پشت سر هم SMTP به سرور ایمیل عووان مثال، هنگامی که یک سرور ایمیل مکانیزمی برای نشان دادن مرزها ندارد، برنامه باید خود نشانه ها را اضافه کند، از آنجایی که تا طرف دریافت کننده برنامه بتواند یک پیام را از پیام بعدی تشخیص دهد. اگر هر پیام به جای آن در یک بخش مجزا قرار داده شود، گیرنده می‌تواند پیام های مختلف را بدون هیچ نشانه ای که توسط طرف فرستنده UDP برنامه اضافه شده است، تشخیص دهد.

مسئله 35

برای ایجاد وب سرور باید نرم افزار وب سرور را روی هاست اجرا کنیم. بسیاری از فروشندهای نرم افزار وب سرور است که منبع باز و رایگان است. در Apache را می‌فروشنند. با این حال، امروزه محبوب ترین نرم افزار وب سرور طول سال‌ها، توسط جامعه متبع باز به شدت بهینه شده است.

مسئله 36

است infohash است که در حال حاضر دارای فایل تعیین شده توسط IP است، مقدار یک آدرس infohash کلید

فصل 3 سوالات مروری

می پذیرد STP، بنامید. در سمت فرستنده (STP) الف) این پروتکل را پروتکل حمل و نقل ساده 1.

STP از فرآیند ارسال، یک تکه داده بیش از 1196 بایت، یک آدرس میزبان مقصد و یک شماره پورت مقصد یک هدر چهار بایتی به هر قطعه اضافه می کند و شماره پورت فرآیند مقصد را در این هدر قرار می دهد. سپس در میزبان STP آدرس میزبان مقصد و بخش حاصل را به لایه شبکه می دهد. لایه شبکه قطعه را به STP شماره پورت را در بخش بررسی می کند، داده ها را از بخش استخراج می STP مقصد تحويل می دهد. سپس گند و داده ها را به فرآیند شناسایی شده توسط شماره پورت ارسال می کند.

STP ب) بخش اکتون دارای دو فیلد پورت مبدأ و فیلد پورت مقصد. در سمت فرستنده تکه‌ای از داده‌های بیش از 1192 بایت، آدرس میزبان مقصد، شماره پورت مبدأ و شماره پورت مقصد را یک بخش ایجاد می کند که شامل داده های برنامه، شماره پورت مبدأ و شماره پورت مقصد STP می‌پذیرد در میزبان دریافت STP است. سپس بخش و آدرس میزبان مقصد را به لایه شبکه می دهد. پس از دریافت بخش کننده، داده های برنامه و شماره پورت منبع را به فرآیند برنامه می دهد.

ج) نه، لایه انتقال نیازی به انجام کاری در هسته ندارد. لایه انتقال در سیستم های انتهایی "زنگی" می کند

2.

برای ارسال نامه، خانواده موظف است خود نامه، آدرس منزل مقصد و نام گیرنده را به نماینده بدهد. نماینده به 1. وضوح نام گیرنده را در بالای نامه می نویسد. سپس نماینده نامه را در پاکت می گذارد و آدرس خانه مقصد را روی پاکت می نویسد. سپس نماینده نامه را به سرویس پستی سیاره می دهد. در سمت دریافت کننده، نماینده نامه را از سرویس پست دریافت می کند، نامه را از پاکت خارج می کند و نام گیرنده را که در بالای نامه نوشته شده است، بداداشت می کند. سپس نماینده نامه را به یکی از اعضای خانواده با این نام می دهد

خیر، سرویس پست مجبور نیست پاکت را باز کند. فقط آدرس روی پاکت را بررسی می کند. 2.

3. X و شماره پورت مقصد ۷ شماره پورت مبدأ.

استفاده کند، که می تواند نرخ ارسال TCP یک توسعه‌دهنده برنامه ممکن است نخواهد برنامه اش از کنترل ازدحام. برنامه های خود را، IP و برنامه های ویدئو کنفرانس IP برنامه را در موقع ازدحام کاهش دهد. اغلب، طراحان تلفن جلوگیری کنند. همچنین، برخی از برنامه ها به TCP اجرا می کنند، زیرا می خواهند از کنترل تراکم UDP از طریق نیاز ندارند TCP انتقال داده قابل اعتماد ارائه شده توسط

برای ویدیو و TCP پیکربندی شده اند، از UDP از آنجایی که اکثر فایروال ها برای مسدود کردن ترافیک. 5.

ترافیک صوتی به ترافیک از طریق فایروال ها اجازه می دهد.

بله. توسعه دهنده برنامه می تواند انتقال داده قابل اعتماد را در پروتکل لایه برنامه قرار دهد. با این حال، این کار به 6. مقدار قابل توجهی کار و اشکال زدایی نیاز دارد.

بله، هر دو بخش به یک سوکت هدایت می شوند. برای هر بخش دریافتی، در رابط سوکت، سیستم عامل فرآیند را با 7. برای تعیین منشاء بخش های جداگانه ارائه می دهد IP ادرس های

برای هر اتصال دائمی، وب سرور یک "سوکت اتصال" جداگانه ایجاد می کند. هر سوکت اتصال با یک چهار 8. هنگامی که (مقصد، شماره پورت مقصد IP منبع، شماره پورت منبع، آدرس IP آدرس) تابی مشخص می شود را دریافت می کند، این چهار فیلد را در دیتاگرام بخش بررسی می کند تا مشخص کند که IP و دیتاگرام C میزبان از سوکت های مختلف B و A را به کدام سوکت منتقل کند. بنابراین، درخواست های TCP باید باز بارگذاری قطعه عبور می کند. شناسه هر دوی این سوکت ها 80 برای پورت مقصد دارد. با این حال، شناسه های این سوکت ها مقادیر را به فرآیند برنامه TCP و قتنی لایه انتقال بار یک بخش UDP منبع دارند. برخلاف IP متفاوتی برای آدرس های منبع را مشخص نمی کند، زیرا این به طور ضمنی توسط شناسه سوکت مشخص می شود IP ارسال می کند، آدرس

اعداد دنباله برای گیرنده مورد نیاز است تا بفهمد آیا بسته دریافتی حاوی داده های جدید است یا ارسال مجدد است. 9.

برای یک بسته ارسالی در مدت زمان تایم بسته دریافت ACK برای رسیدگی به ضرر و زیان در کanal. اگر 10. گم شده است. بنابراین، بسته دوباره ارسال می شود (آن ACK یا NACK یا) نشود، بسته

ضروری است. اگر زمان رفت و برگشت مشخص باشد، تنها مزیت آن rdt یک تایمر همچنان در پروتکل 11. بسته از بین رفته است، در مقایسه با (ACK یا NACK) این خواهد بود که فرستنده مطمئناً می داند که بسته یا ممکن است پس از انقضای زمان سنج همچنان در راه فرستنده باشد. با (ACK یا NACK) یا سناریوی واقعی، جایی که این حال، برای تشخیص از دست دادن، برای هر بسته، یک تایmer با مدت زمان ثابت همچنان در فرستنده لازم است.

الف) از دست دادن بسته باعث یک تایم اوست شد که پس از آن تمام پنج بسته دوباره ارسال شدند. 12.

از تأییدیه های تجمعی استفاده می کند Go-Back-N باعث ارسال مجدد نشد زیرا ACK ب) از دست دادن یک

ج) فرستنده قادر به ارسال بسته ششم نبود زیرا اندازه پنجره ارسال بر روی 5 ثابت شده است.

الف) هنگامی که بسته گم شد، چهار بسته دریافتی در گیرنده بافر قرار گرفتند. بعد از 13.

در پایان زمان، فرستنده بسته از دست رفته را مجدداً ارسال کرد و گیرنده بسته های بافر شده را به ترتیب صحیح به برنامه تحویل داد.

گم شده ارسال شده است ACK تکراری توسط گیرنده برای ACK (ب).

ج) فرستنده قادر به ارسال بسته ششم نبود زیرا اندازه پنجره ارسال بر روی 5 ثابت شده است

همه بسته ها را مجدداً ارسال می کرد در حالی که تکرار GO-Back-N، هنگامی که یک بسته گم می شد انتخابی فقط بسته از دست رفته را دوباره ارسال می کرد. در صورت از دست دادن تأیید، تکرار انتخابی یک ACK از تأیید تجمعی استفاده می کند، بنابراین GO-Back-N تکراری ارسال می کند و به عنوان ACK تکراری غیر ضروری بود.

ج) درست (د) نادرست (ه) درست (و) نادرست (ز) نادرست (الف) نادرست (ب) نادرست 14.

الف) 20 بایت (ب) عدد اک = 90

16. seq = 43، ack = 80؛ seq = 80، ack = 44؛ seq = 44، ack = 81: بخش دوم؛ بخش اول

17. R/2

18. False. به نصف مقدار فعلی پنجره ازدحام تنظیم شده است.

19. زمان جستجو. نمودار زمان بندی زیر را در نظر بگیرید $X = RTTBE$ ، $Y = RTTBE$ و $ST =$ اجازه دهید.

بین آنها (Back End) با یک پروکسی (Front End) بین مشتری و سرور TCP نمودار تبادل بسته.

زمان جستجو است + $X + Y + ST = 4 * RTT_{FE} + RTT_{BE}$ که کل زمان 4.

فصل 3 مسائل

مشکل 1

	شماره پورت منبع	شماره پورت مقصد
(الف) A → S	467	23
(ب) B → S	513	23
(ج) S → A	23	467
(د) S → B	23	513

چشم
ها.و) خیر

مشکل 2

(متایز هستند c، b، a، توجه داشته باشد که). هستند c، b، a به ترتیب C و B، A هاست های IP فرض کنید آدرس های

= مقصد IP پورت مقصد = 26145، آدرس، b = منبع IP پورت منبع = 80، آدرس: A برای میزبان

مقصد IP پورت مقصد = 7532، آدرس، b = منبع IP فرآیند سمت چپ: پورت منبع = 80، آدرس، C برای میزبانی = c

c = مقصد IP پورت مقصد = 26145، آدرس، b = منبع IP فرآیند صحیح: پورت منبع = 80، آدرس، C برای میزبانی

مشکل 3

توجه داشته باشد، در صورت سرریز آن را بپیچید.

$$\begin{array}{r}
 0 + 1 0 1 0 0 1 1 \\
 1 1 0 0 1 1 0 \\
 1 0 1 1 1 0 0 1
 \end{array}$$

$$\begin{array}{r}
 1 + 0 1 1 1 0 0 1 \\
 1 1 1 0 1 0 0 \\
 \hline
 0 0 1 0 1 1 1 0
 \end{array}$$

برای تشخیص خطاهای گیرنده چهار کلمه (سه کلمه اصلی و چک جمع) One = 1 1 0 1 0 0 0 1 مکمل را اضافه می‌کند. اگر مجموع شامل یک صفر باشد، گیرنده می‌داند که خطای وجود داشته است. همه خطاهای یک بیتی شناسایی خواهند شد، اما خطاهای دو بیتی را می‌توان شناسایی نکرد (به عنوان مثال، اگر آخرین رقم کلمه اول به 0 و آخرین رقم کلمه دوم به 1 تبدیل شود)

مسئله 4 (الف) با جمع کردن دو بایت 11000001 به دست می‌آید. با گرفتن متمم یک عدد 00111110 به دست می‌آید.

(ب) با جمع کردن دو بایت 01000000 به دست می‌آید. مکمل یک 10111111 می‌دهد.

(ج) بایت اول = 01101101؛ بایت دوم = 01010100.

مشکل 5 خیر، گیرنده نمی‌تواند کاملاً مطمئن باشد که خطای بیتی رخ نداده است. این به دلیل روشهای است که جمع چک برای بسته محاسبه می‌شود. اگر بیت‌های منتظر (که با هم جمع می‌شوند) دو کلمه 16 بیتی در بسته 0 و 1 بودند، حتی اگر این بیت‌ها به ترتیب به 1 و 0 تبدیل شوند، مجموع همچنان ثابت می‌ماند. بنابراین، 1 های تکمیل کننده محاسبه گیرنده نیز یکسان خواهند بود. این به این معنی است که چکسام حتی اگر خطای انتقال وجود داشته باشد تأیید می‌کند.

مشکل 6 فرض کنید فرستنده در حالت "منتظر تماس 1 از بالا باشید" و گیرنده (گیرنده که در مشکل تکلیف نشان داده شده است) در وضعیت "1 از پایین منتظر بماند". فرستنده بسته ای را با دنباله شماره 1 ارسال می‌کند و به این نکته اکنون ACK یا NAK منتقل می‌شود و منتظر یک "Wait for ACK or NAK 1" می‌گیرد. گیرنده بسته را با ترتیب دریافت می‌کند.

می‌فرستد، و به حالت "صفر از پایین صیر کنید" تغییر می‌کند، منتظر بسته داده ای با ACK شماره 1 به درستی، یک خراب است ACK، شماره توالی 0 است. با این حال خراب را دریافت می‌کند، بسته را با دنباله شماره 1 مجدداً ارسال می‌کند. با ACK هنگامی که فرستنده این حال، گیرنده منتظر بسته ای با شماره توالی 0 است و (همانطور که در مشکل خانه نشان داده شده است) همیشه ارسال می‌کند. بسته ای با شماره توالی 0 دریافت نمی‌کنید. بنابراین فرستنده همیشه بسته ای را با دنباله NAK یک می‌کند. هیچکدام از آن وضعیت به جلو پیشرفت نخواهند NAK شماره 1 ارسال می‌کند و گیرنده همیشه آن بسته را کرد.

مسئله 7 برای بهترین پاسخ به این سوال، در نظر بگیرید که چرا در وله اول به اعداد دنباله نیاز داشتیم. دیدیم که فرستنده به اعداد دنباله ای نیاز دارد تا گیرنده بتواند تشخیص دهد که آیا یک بسته داده تکراری از یک بسته یعنی یک شماره دنباله روی) ها، فرستنده به این اطلاعات ACK داده از قبل دریافت شده است یا خیر. در مورد واضح است، rdt3.0 تکراری برای گیرنده ACK تکراری نیاز ندارد. یک ACK برای تشخیص یک (ACK موردنیاز فرستنده ACK تکراری است. اصلی را دریافت کرد به حالت بعدی منتقل شد زیرا زمانی که نادیده گرفته می شود rdt3.0 نیست و از این رو توسط فرستنده

با سمت فرستنده پروتکل 2.2 تفاوت دارد زیرا وقههای زمانی rdt3.0 مشکل 8 سمت فرستنده پروتکل اضافه شده است. دیدهایم که معرفی وقههای را اضافه می کند

امکان تکرار بسته ها در جریان داده فرستنده به گیرنده

با این حال

اگر 2.2 rdt تکراری سمت گیرنده در) می تواند بسته های تکراری را مدیریت کند گیرنده در پروتکل rdt.2.2 گیرنده در پروتکل را ارسال کند که گم شده است و فرستنده داده های قدیمی را دوباره ارسال کند، ایجاد می ACK گیرنده یک کار خواهد کرد 3.0 rdt نیز به عنوان گیرنده در پروتکل 2.2 بنابراین گیرنده در پروتکل (شود.

مشکل 9 فرض کنید پروتکل برای مدتی فعال شده است. فرستنده در حالت "منتظر تماس از بالا" (گوشه سمت خراب در ACK چپ بالا) و گیرنده در حالت "صفر از پایین منتظر باشید". سناریوهای داده های خراب و مشکل 1 نشان داده شده است.



خراب ACK، داده های خراب: شکل 1: سناریوهای rdt 3.0.

مشکل 10 در اینجا، یک تایم ریز اضافه می کنیم که مقدار آن بیشتر از تاخیر انتشار رفت و برگشت شناخته شده "NAK1" یا ACK یا "منتظر NAK0" است. ما یک رویداد مهلت زمانی را به حالت های "منتظر اضافه می کنیم. اگر رویداد وقفه رخ دهد، آخرین بسته ارسال شده مجدد ارسال می شود. بگذارید بینیم چرا این کار می کند. rdt2.1 پروتکل همچنان با گیرنده.

- فرض کنید مهلت زمانی ناشی از یک بسته داده از دست رفته است، یعنی بسته ای در کانال فرستنده به گیرنده در این مورد، گیرنده هرگز قبلی را دریافت نکرده است. انتقال و از دیدگاه گیرنده، اگر باز ارسال مجدد دریافت شود، دقیقاً مانند انتقال اصلی به نظر می رسد.
- گم شده است گیرنده در نهایت دوباره ارسال می کند ACK حال فرض کنید یک a بسته در یک بازه زمانی ارسال مجدد دقیقاً همان عملی است که اگر ACK مخدوش است. بنابراین عکس العمل فرستنده با از دست دادن یکسان است، مانند یک ACK مخدوش رسیدگی کند ACK از قبل می تواند با یک rdt 2.1 مخدوش گیرنده.

مشکل 11 اگر ارسال این پیام حذف می شد، طرف فرستنده و گیرنده به بن بسته می رسید و منتظر رویدادی بود که هرگز رخ نمی داد. در اینجا یک سناریو وجود دارد:

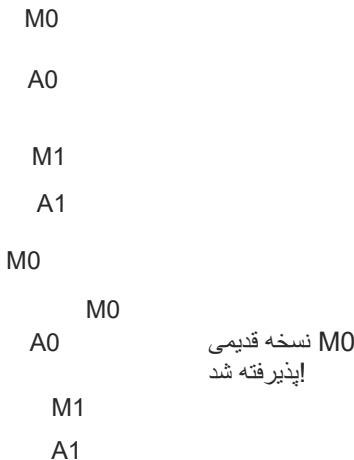
- را وارد می کند و منتظر می ماند تا بسته ای از گیرنده "ACK0" را ارسال می کند، "حالت منتظر0 فرستنده برگردان
- گیرنده در وضعیت "صفر از پایین صبر کنید" است و یک بسته خراب از فرستنده دریافت می کند. فرض کنید چیزی را پس نمی فرستد، و به سادگی دوباره وارد حالت «صفر از پایین» شوید.

از گیرنده است، و گیرنده منتظر یک بسته داده از فرستنده است - یک بن ACK منتظر یک نوع ender، اکنون بست

مشکل 12 پروتکل همچنان کار می کند، زیرا اگر بسته دریافته با خطاهای واقع‌گشته باشد، ارسال مجدد اتفاقی خواهد افتاد (و از نقطه نظر گیرنده، هرگز نمی داند که کدام یک از این رویدادها رخ می دهد)

برای رسیدن به موضوع ظریفتر پشت این سوال، باید اجازه داد که تایم اوت‌های زودرس رخ دهد. در این صورت، اگر و هر یک ACK هر کمی اضافی از بسته ارسال n اضافی باعث می‌شود که اضافی دیگری از بسته فعلی ارسال شود، تعداد دفعاتی که بسته ACK دریافت به بینهایت، بدون محدودیت افزایش می‌باید n می‌شود، با نزدیک شدن

مسئله 13



مسئله 14

دریافت $x+1$ تنها زمانی توسط گیرنده شناسایی می شود که بسته x از دست دادن بسته، NAK در یک پروتکل فقط دریافت می شود، گیرنده متوجه می $x+1$ را دریافت می کند، تنها زمانی که $x+1$ و سپس $x-1$ شود. یعنی گیرنده ها وجود داشته باشد، آنگاه زمان زیادی طول $x+1$ و ارسال x از دست رفته است. اگر تأخیر زیادی بین ارسال x شود که بازیابی شود NAK تحت یک پروتکل فقط x خواهد کشید تا.

می تواند به سرعت اتفاق NAK از سوی دیگر، اگر داده ها اغلب ارسال شوند، بازیابی تحت یک طرح فقط هرگز ACK ها فقط گاهی (در صورت نیاز) ارسال می شوند و NAK بیفتند. علاوه بر این، اگر خطاهای نادر باشد نسبت به مورد فقط NAK ارسال نمی شود - کاهش قابل توجهی در بازخورد در مورد فقط ACK.

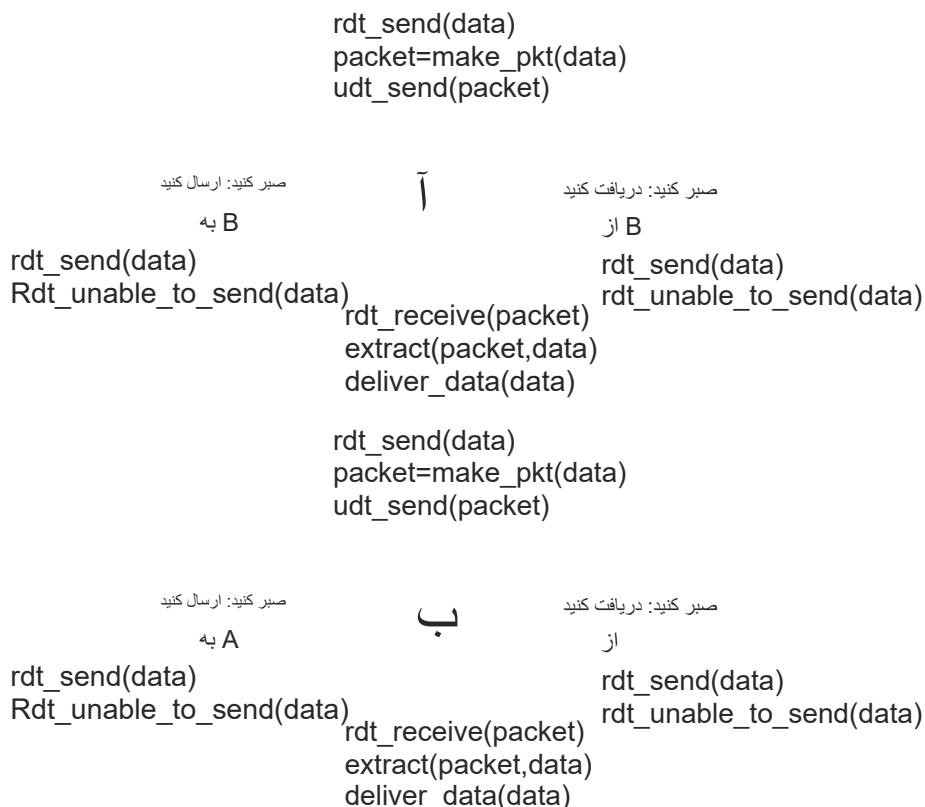
مسئله 15 برای ارسال یک بسته 12 میکروثانیه (یا 0.012 میلی ثانیه) طول می کشد، به عنوان $9.8/10^{1500} = 12$ میکروثانیه. برای اینکه فرستنده در 98 درصد موقع مشغول باشد باید داشته باشیم

$$\text{util} = \frac{9.8}{10^{1500}} = 0.012 \text{ ms}$$

نحویاً $n = 2451$ بسته.

مشکل 16 بله. این در واقع باعث می شود که فرستنده تعدادی داده خط لوله را به کانال ارسال کند. آره. در اینجا آن بخش ها را دوباره 3.0 rdt یک مشکل بالقوه وجود دارد. اگر بخش های داده در کانال گم شوند، فرستنده ارسال نمی کند، مگر اینکه مکانیزم اضافی در برنامه برای بازیابی از دست رفتن وجود داشته باشد.

مسئلہ 17



مسنون

برای یک جفت پیام دریافت کند ACK در راه حل ما، فرستنده منتظر می‌ماند تا یک

قبل از اینکه به جفت پیام بعدی بروید، بسته های داده دارای یک فیلد داده هستند و (seqnum و seqnum+1) دارای یک شماره توالی دو بیتی هستند، یعنی اعداد دنباله معتبر ۰، ۱، ۲ و ۳ هستند. (توجه: باید به این فکر کنید که دارای ACK چرا یک فضای اعداد دنباله ای ۱ بیتی ۰، ۱ تنهای در راه حل زیر کار نمی کند). پیام های هستند. شماره توالی بسته داده ای که آنها تایید می کنند ACK.

(i) برای فرستنده و گیرنده در شکل 2 نشان داده شده است. توجه داشته باشید که حالت فرستنده ثبت می کند که آیا ACK دریافت شده است یا یک (فقط) seqnum برای ACK یک (ii)، برای جفت فعلی دریافت نشده است ACK هیچ در ابتدا 0 است و فرستنده اولین seqnum دریافت شده است. در این شکل فرض می کنیم (فقط) seqnum+1 برای موردندا ارسال کرده است.

دو پیام داده (برای پیشبرد امور). یک خط زمانی برای بازیابی فرستنده و گیرنده از یک بسته گم شده در زیر نشان داده شده است:

شکل 2: فرستنده و گیرنده برای مشکل (3.18)



بسته 0 قطره ارسال بسته
1

دریافت بسته 1 بسته بافر 1
ارسال ACK 1

تایم) ACK 1 دریافت
ارسال مجدد بسته 0 (وقفه

دریافت بسته 0 جفت تحویل
ارسال (0,1) ACK 0

دریافت ACK 0

مسئله 19

است. از آنجا که ممکن است کانال پیام‌ها را از دست (rdt3.0) این مشکل یک تغییر در پروتکل توقف و انتظار ساده بدهد و از آنجا که فرستنده ممکن است پیامی را که یکی از گیرندهای قبلاً دریافت کرده است مجدداً ارسال کند (یا به دلیل مهلت زمانی پیش از موعد یا به دلیل اینکه گیرنده دیگر هنوز داده‌ها را به درستی دریافت نکرده است)، به یک شماره توالی 0 بیتی در اینجا کافی است، rdt3.0 شماره‌های ترتیبی نیاز ندارد. همانطور که در

فرستنده و گیرنده در شکل 3 نشان داده شده است. در این مشکل، حالت فرستنده نشان می‌دهد که آیا فرستنده FSM دریافت کرده است. وضعیت گیرنده نشان می‌دهد که B و C یا از هیچ یک از (فقط) C از، (فقط) B از ACK یک کدام دنباله را نشان می‌دهد. شماره ای که گیرنده منتظر آن است

شکل 3. فرستنده و گیرنده برای مشکل 3.19 (مسئله 19)

مسئله 20



شکل 4: FSM 3.18 نهاده براي سمت گير

سمت فرستنده دقیقاً همان چیزی است که در شکل 3.15 در متن آورده شده **FSM** فرستنده است

مسئله 21

باید مهلت زمانی داشته باشد و پیام های A، می تواند پیام های درخواستی را از دست بدده **A-to-B** از آنجایی که کانال درخواستی خود را مجدداً ارسال کند (تا بتواند پس از از دست دادن بازیابی شود). از آنجایی که تاخیر های کانال متغیر و B یعنی یک پیام درخواستی را که قبلاً توسط) درخواست های تکراری ارسال کند A ناشناخته هستند، ممکن است تا بتوانیم تشخیص دهیم.(دریافت شده است دوباره ارسال کند پیام های درخواست تکراری، پروتکل از شماره های دنباله ای استفاده می کند. یک شماره توالی 1 بیتی برای نوع توقف و انتظار پروتکل درخواست/پاسخ کافی است.

A دارای 4 حالت است (درخواست کننده):

- منتظر درخواست 0 از بالا باشید."در اینجا درخواست کننده منتظر تماسی از بالا برای درخواست واحد داده" ارسال می کند، تایمر را B به R0 است. هنگامی که درخواستی را از بالا دریافت می کند، یک پیام درخواست منتقل می شود. هنگامی که در حالت "صفر برای درخواست 0" راه اندازی می کند و به حالت Nadideh می گیرد A، از بالا" باشد دریافت می کند B هر چیزی که از
- است A از D0 باشید."در اینجا درخواست کننده منتظر یک پیام داده D0 منتظر" دیگری ارسال می کند، تایمر را R0 پیام A، تایمر همیشه در این حالت کار می کند. اگر تایمر منقضی شود زمان را A، دریافت شود B از D0 مجدداً راه اندازی می کند و در این حالت باقی می ماند. اگر یک پیام D1 در این حالت یک پیام داده A متوقف می کند و به حالت "منتظر درخواست 1 از بالا" می رود. اگر دریافت کند، Nadideh گرفته می شود.
- منتظر درخواست 1 از بالا باشید."در اینجا درخواست کننده دوباره منتظر تماسی از بالا برای درخواست" ارسال B را به R1 واحد داده است. هنگامی که درخواستی را از بالا دریافت می کند، یک پیام درخواست منتقل می شود. هنگامی که در حالت "Wait for D1" می کند، تایmer را راه اندازی می کند و به حالت A، "منتظر درخواست 1 از بالا" هستید دریافت می کند Nadideh می گیرد B هر چیزی را که از
- است A از D1 باشید."در اینجا درخواست کننده منتظر یک پیام داده D1 منتظر" دیگری می فرستد، تایmer را R1 پیام A، تایmer همیشه در این حالت کار می کند. اگر تایmer منقضی شود تایmer را A، دریافت شود B از D1 مجدداً راه اندازی می کند و در این حالت باقی می ماند. اگر یک پیام در این حالت یک پیام A متوقف می کند و به حالت "صفر برای درخواست 0 از بالا" منتقل می شود. اگر دریافت کند، Nadideh گرفته می شود D0 داده

بنها دو حالت دارد (B) تامین کننده داده

- دریافتی پاسخ می دهد و سپس در این حالت R0 به پیام های D0 با ارسال B، در این حالت "D0" ارسال آن به درستی دریافت شده است. بنابراین D0 دریافت کند، می داند که پیام R1 یک پیام B باقی می ماند. اگر را دور می اندازد (از آنجایی که از طرف دیگر دریافت شده است) و سپس به حالت «ارسال D0 داده های برای ارسال قطعه داده درخواستی بعدی استفاده می کند D1 منتقل می شود، جایی که از «D1

- دریافتی پاسخ می دهد و سپس در این حالت R1 به پیام های D1 با ارسال B، در این حالت "D1 ارسال" آن به درستی دریافت شده است و D1 دریافت کند، می داند که پیام R1 یک پیام B باقی می ماند. اگر منتقل می شود "D1 بنابراین به حالت "ارسال"

مسئله 22

را دریافت کرده و آن و سایر بسته های قبلی را $k-1$ داریم. فرض کنید گیرنده بسته $N=3$ (الف) در اینجا اندازه پنجره است. بعد $[k, k+N-1]$ ها توسط فرستنده دریافت شده باشند، پنجره فرستنده ACK کرده است. اگر همه این ACK و $k-1$ ها در فرستنده دریافت نشده است. در این مورد دوم، پنجره فرستنده حاوی ACK فرض کنید که هیچ یک از است. با این آرگومان ها، پنجره فرستنده $[kN, k-1]$ است. بنابراین پنجره فرستنده $k-1$ تا از جمله N بسته های شروع می شود $[kN, k]$ اندازه 3 است و از جایی در محدوده.

کرده (ACK) و) را قبل از آن دریافت کرده $N-1$ و بسته های $k-1$ باشد، بسته k (ب) اگر گیرنده منتظر بسته $[kN, k-1]$ با مقادیر ACK هنوز توسط فرستنده دریافت نشده باشد، پیام های NACK است. اگر هیچ یک از آن را ارسال کرده است، باید ارسال $[kN, k-1]$ ممکن است همچنان در حال انتشار باشند. چون فرستنده بسته های kN برای ACK دریافت کرده باشد. هنگامی که گیرنده یک $k-1$ برای ACK شود. موردنی که فرستنده قبلاً یک در حین پرواز می ACK را ارسال نخواهد کرد. بنابراین دامنه مقادیر $kN-1$ کمتر از ACK ارسال کرد، هرگز 1 $k-1$ تا $k-1$ باشد. از $kN-1$ تواند از

مسئله 23

به منظور اجتناب از سناریوی شکل 3.27، می خواهیم از قرار گرفتن لبه جلویی پنجره گیرنده (یعنی لبهای با عدد دنبالهای "بالاترین") در فضای شماره دنباله و همپوشانی با لبه انتهایی خودداری کنیم. یکی با "کمترین" شماره دنباله در پنجره فرستنده. یعنی فضای شماره دنباله باید به اندازه کافی بزرگ باشد تا با کل پنجره گیرنده و کل پنجره فرستنده بدون این شرایط همپوشانی مناسب باشد. بنابراین - ما باید تعیین کنیم که محدوده وسیعی از اعداد دنباله را می توان در هر زمان معین توسعه پنجره های گیرنده و فرستنده پوشش داد.

است. در این حالت، پنجره آن $m, m+w$ - اندازه پنجره w کرده است، جایی که کمترین شماره دنباله ای که گیرنده منتظر آن است بسته 1 با مقادیر ACK ها هنوز توسط فرستنده دریافت نشده باشد، پیام های $m-1$ و بسته های w است. اگر هیچ یک از آن توسعه فرستنده دریافت نشده ACK با این شماره های ACK ممکن است همچنان در حال انتشار باشند. اگر هیچ 1 خواهد بود $[mw, m-1]$ باشد، پنجره فرستنده.

است. برای اینکه لبه جلویی پنجره گیرنده با لبه $m+w-1$ و لبه جلویی پنجره گیرنده mw بنابراین لبه پایینی پنجره فرستنده انتهایی پنجره فرستنده همپوشانی نداشته باشد، فاصله شماره دنباله باید

را در خود جای دهد. یعنی فضای شماره دنباله باید حداقل دو W باشد و اندازه کافی بزرگ باشد تا اعداد دنباله ای 2 $\geq 2w$ ، برابر اندازه پنجره.

مسئله 24 الف) درست است. فرض کنید فرستنده دارای اندازه پنجره 3 است و بسته های 1، 2، 3 را در 0t ارسال می کند. در

زمان فرستنده تمام می شود و $t_1 > t_2$ گیرنده $t_1 < t_2$ ، گیرنده موارد تکراری را دریافت می کند و 1، 2 را دوباره تایید می کند. مجدداً 1، 2، 3 ارسال می شود. در و آن را پیش می برد ارسال کرده است. هایی را دریافت می کند که گیرنده در ACK1 فرستنده $t_2 > t_1$ ارسال می شود. هایی 1، 2 را دریافت می کند که گیرنده در ACK2 فرستنده پنجره به 4، 5، 6 در 5 ها خارج از پنجره آن هستند ACK این.

(ب) درست است. اساساً با سناریوی مشابه در (الف).

(ج) درست است.

و پروتکل بیت متناوب از نظر عملکردی معادل GBN، SR است. درست است. توجه داشته باشید که با اندازه پنجره 1 تجمعی در این ACK هستند. اندازه پنجره 1 از امکان بسته های خارج از دستور (در داخل پنجره) جلوگیری می کند. معمولی است، زیرا فقط می تواند به بسته منفرد درون پنجره اشاره کند ACK شرایط فقط یک

مسئله 25 الف) ارسال یک پیام برنامه کاربردی از طریق یک پروتکل حمل و نقل را در نظر بگیرید. با TCP،

بایت ها را بدون قرار دادن یک پیام واحد در بخش TCP برنامه داده ها را در بافر ارسال اتصال می نویسد و هر UDP، ممکن است بیشتر یا کمتر از یک پیام را در یک بخش قرار دهد. از سوی دیگر TCP می گیرد UDP چیزی را که برنامه به آن می دهد در یک بخش کسیوله می کند. به طوری که اگر برنامه یک پیغام برنامه یک برنامه کنترل بیشتری بر روی اینکه چه داده UDP خواهد بود. بنابراین، با UDP بدهد، این پیغام بار بخش هایی در یک بخش ارسال می شود، دارد.

به دلیل کنترل جریان و کنترل تراکم، ممکن است از زمانی که یک برنامه داده ها را در بافر ارسال، TCP (ب) با به دلیل UDP خود می نویسد تا زمانی که داده ها به لایه شبکه داده می شود، تأخیر قابل توجهی وجود داشته باشد. کنترل جریان و کنترل تراکم تأخیر ندارد.

مشکل 26

شماره های دنباله ای ممکن 2 32 964,967? وجود دارد

(الف) عدد دنباله با هر قطعه یک افزایش نمی یابد. بلکه با تعداد بایت های داده ارسالی افزایش می ارسال کرد به A به B بی ربط است -- حداقل اندازه فایلی که می توان از MSS یابد. بنابراین اندازه است $\approx 4.19 \text{ Gbytes}$. سادگی تعداد بایت های قابل نمایش توسط

ب) تعداد قطعات است $\frac{32}{32} = \square \square \square \square \square$ پاییت هدر به هر کدام اضافه می شود 66.

بخش مجموعاً 528857934 بایت هدر را ارائه می دهد. تعداد کل بایت های ارسال شده 32 9 باشد + $2 \times 4528,857,938 24.4 = 10$.

بنابراین 249 ثانیه طول می کشد تا فایل از طریق لینک 155 ~ مگابیت بر ثانیه ارسال شود

شماره دنباله 207 است، پورت منبع، B تا A مسئله 27 الف) در بخش دوم از میزبان

شماره 302 و شماره یورت مقصد 80 است

بخش ورودی، شماره تأیید 207، شماره پورت مبدأ 80 و شماره پورت مقصد 302 است.

ج) اگر سگمنت دوم قبل از سگمنت اول وارد شود، در تأیید قطعه ورودی اول، عدد تأیید 127 است که نشان می‌دهد هنوز منتظر بایت‌های 127 به بعد است.

2)

جذب A

میزبان B

سابت = 127، 80

فاسلہ زمانی

Seq = 307; 40 Byte

207

247 = اک

سیاست Seq = 127، 80

فاصله زمانی

247 = اک

A مشکل 28 از آنجایی که ظرفیت پیوند فقط 100 مگابیت در ثانیه است، بنابراین سرعت ارسال میزان می تواند B داده ها را سریعتر از میزان A حداکثر می تواند 100 مگابیت در ثانیه باشد. با این حال، میزان داده هارا از بافر حذف کند، به بافر دریافت می فرستد. بافر دریافت با سرعت تقریباً 40 مگابیت در ثانیه پر می سیگنال می دهد تا ارسال A به میزان RcvWindow = 0 با تنظیم B شود. هنگامی که بافر پر است، میزان TCP RcvWindow با ارسال را متوقف می کند تا زمانی که یک قطعه A داده را متوقف کند. سپس میزان TCP RcvWindow با طور مکرر متوقف می شود و ارسال را به عنوان یکتابع آغاز می A دریافت کند. بنابراین میزان 0 > آن را ارزش گذاری می کند RcvWindow کند. از

داده ها را به عنوان بخشی از این اتصال به A دریافت می کند. به طور متوسط، نرخ بلندمدتی که میزبان B از میزبان ارسال می کند، بیش از 60 مگابیت در ثانیه نیست.

مشکل 29 الف) سرور از شماره توالی اولیه خاصی استفاده می کند (که از هش به دست می آید

IP ها و پورت های مبدا و مقصد) به منظور دفاع از خود در برابر حمله SYN FLOOD.

بسته به هدف، اتصالات نیمه باز یا کاملاً باز ایجاد ACK (ب) خیر، مهاجم نمی تواند به سادگی با ارسال و استفاده می کند، متغیرهای اتصال و SYN کند. اتصالات نیمه باز امکان پذیر نیست زیرا سروی که از کوکی های بافرهای اتصال را قبل از برقراری اتصالات کامل حفظ نمی کند. برای ایجاد اتصالات کاملاً باز، مهاجم باید شماره توالی اولیه ویژه را بداند.

منبع (جعل شده) مهاجم این شماره دنباله نیاز به شماره "مخفي" دارد که هر سرور از آن IP مربوط به آدرس استفاده می کند. از آنجایی که مهاجم این شماره مخفی را نمی داند، نمی تواند شماره توالی اولیه را حس بزند.

(ج) نه، سرور می تواند به سادگی یک مهر زمانی در محاسبه آن اعداد دنباله اولیه اضافه کند و زمانی را برای ارزش زنده برای آن اعداد دنباله انتخاب کند، و اعداد دنباله اولیه منقضی شده را حتی اگر مهاجم آنها را دوباره پختش کند، کنار بگذارد.

مشکل 30 الف) اگر مقادیر مهلت زمانی ثابت باشند، ممکن است فرستندها زودتر از موعد به اتمام بررسی بنا بر این، برخی از بسته ها دوباره ارسال می شوند حتی اگر گم شوند.

افزایش اندازه بافر مطمئنا به، (انجام می دهد TCP مانند کاری که) (ب) اگر مقادیر بازه زمانی تخمين زده شوند افزایش توان عملیاتی آن روترا کمک می کند. اما ممکن است یک مشکل بالقوه وجود داشته باشد. تأخیر در صفحه ممکن است بسیار زیاد باشد، مشابه آنچه در سناریوی 1 نشان داده شده است.

مسئله 31

$$\text{TTEestimatedR} = \text{xSampleRTT} + 1(-\text{T})^{\text{EestimatedRx}}$$

$$\text{DevRTT} = \text{SampleRTT} - \text{TTEestimatedR} + 1(-\text{L})^{\text{vRTT}}$$

$$\text{ervalTimeoutInt} = \text{TTEestimatedR} * 4 + \text{DevRTT}$$

است RTT بیس از به دست آوردن اولین نمونه

$$= \text{TTEestimatedR} 106 * 125.0 + 100 * 875.0$$

$$\text{ms} 75.100 =$$

$$* = \text{DevRTT} 06 - 75.100 + 5 * 75.0$$

$$\text{ms} 06.5 =$$

$$= \text{ervalTimeoutInt} 75.100 + 06.5 * 4$$

$$\text{ms}99.120 =$$

پس از بدست آوردن نمونه دوم RTT = 120ms:

$$75.100 * 875.0 \quad 120 * 125.0 + = \text{TTEstimatedR}$$

$$\text{ms}15.103 =$$

$$= \text{DevRTT} \quad 25.0 * 120 - 15.103 + 06.5 * 75.0$$

$$\text{ms}8 =$$

$$= \text{ervalTimeoutInt} \quad 15.103 + 8 * 4$$

$$\text{ms}15.135 =$$

پس از به دست آوردن نمونه سوم RTT = 140ms:

$$15.103 * 875.0 \quad 140 * 125.0 + = \text{TTEstimatedR}$$

$$\text{ms}76.107 =$$

$$= \text{DevRTT} \quad 25.0 * 140 - 76.107 + 8 * 75.0$$

$$\text{ms}06.14 =$$

$$= \text{ervalTimeoutInt} \quad 76.107 + 06.14 * 4$$

$$\text{ms}164 =$$

پس از به دست آوردن نمونه چهارم RTT = 90ms:

$$76.107 * 875.0 \quad 90 * 125.0 + = \text{TTEstimatedR}$$

$$\text{ms}54.105 =$$

$$= \text{DevRTT} \quad 25.0 * 90 - 54.105 + 06.14 * 75.0$$

$$\text{ms}42.14 =$$

$$= \text{ervalTimeoutInt} \quad 54.105 + 42.14 * 4$$

$$\text{ms}22.163 =$$

پس از بدست آوردن پنجمین نمونه RTT = 115ms:

$$= \text{TTEstimatedR} \quad 115 * 125.0 + 54.105 * 875.0$$

$$\text{ms}71.106 =$$

$$= \text{DevRTT} \quad 25.0 * 115 - 71.106 + 42.14 * 75.0$$

$$\text{ms}88.12 =$$

$$= \text{ervalTimeoutInt} \quad 71.106 + 88.12 * 4$$

$$\text{ms}23.158 =$$

(مسئله 32 الف)

n برای تخمین بعد از نمونه (nTTEstimatedR) مشخص کن.

$$\text{TTEstimatedR}_n = x \text{SampleRTT}_1 +$$

$$1(-\text{SampleRTT}_2 +$$

$$1(-\text{SampleRTT}_3 + \text{SampleRTT}_4))$$

$$= x \text{SampleRTT}_1 + 1(-x \text{SampleRTT}_2$$

$$+ 1(-x \text{SampleRTT}_3 + 1(-x \text{SampleRTT}_4$$

(ب)

$$\text{TTEestimatedR}^j = \frac{1}{n} \cdot \sum_{j=1}^n \text{SampleRTT}_j$$

$$+ 1(-x \text{SampleRTT}_n$$

(ج)

$$\text{TTEestimatedR}^j = \frac{1}{n} \cdot \sum_{j=1}^n \text{SampleRTT}_j$$

$$= \frac{1}{n} \cdot \sum_{j=1}^n \text{SampleRTT}_j$$

وزن داده شده به نمونه های گذشته به صورت تصاعدی کاهش می یابد.

را برای یک بخش ارسال مجدد اندازه گیری کند چه TCP SampleRTT مشکل 33 بیاید بینیم که اگر منقضی می شود، و منبع سپس P1 را ارسال می کند، تایمر برای P1 مشکلی دارد. فرض کنید منبع بسته P2 را برای SampleRTT یک کپی جدید از همان بسته را ارسال می کند. بعلاوه فرض کنید منبع P2، یک P2 اندازه گیری می کند. در نهایت فرض کنید که مدت کوتاهی پس از ارسال (بسته ارسال شده مجدد) می گیرد و مقدار P2 می رسد. منبع به اشتباه این تصدیق را به عنوان یک تصدیق برای P1 تأییدیه برای نادرستی SampleRTT محاسبه می کند.

را برای یک بخش ارسال مجدد اندازه گیری کند چه چیزی ممکن است TCP SampleRTT بیاید بینیم اگر یک P2، P2 منقضی می شود، و منبع سپس P1 را ارسال می کند، تایمر برای P1 اشتباه باشد. فرض کنید منبع بسته ارسال شده (P2) را برای SampleRTT یک کپی جدید از همان بسته را ارسال می کند. بعلاوه فرض کنید منبع می P1 یک تأییدیه برای P2 اندازه گیری می کند. در نهایت فرض کنید که مدت کوتاهی پس از ارسال (مجدداً) را TCP SampleRTT می گیرد و مقدار نادرستی P2 رسد. منبع به اشتباه این تصدیق را به عنوان یک تصدیق برای محاسبه می کند.

شماره دنباله ای از آخرین بایتی است که فرستنده می 1 – t ، مشکل 34 در هر زمان معین داند به درستی و به ترتیب در گیرنده دریافت شده است. آخرین بایت دریافتی (به درستی و به ترتیب) در ممکن است بیشتر باشد اگر در لوله تایید وجود داشته باشد. بدین ترتیب t گیرنده در زمان

$$\text{SendBase-1} \leq \text{LastByteRcvd}$$

مسئله 35

دریافت می کند، فرستنده با اطمینان می داند که گیرنده همه چیز را y فرستنده تاییدیه ای با مقدار t هنگامی که در زمان $y-1$ تا y ممکن است بیشتر t دریافت کرده است. آخرین بایت واقعی دریافتی (به درستی و به ترتیب) در گیرنده در زمان $y-1$ تا y باشد اگر

با اگر تاییدیه های دیگری در لوله وجود دارد. بدین ترتیب SendBase

$$y-1 \leq \text{LastByteRvcd}$$

مسئله 36

یک اکنون $n+2$ آنگاه دریافت بسته (دریافت شوند $n+1$ ، $n+2$ ، $n+3$ یعنی به ترتیب) در امتداد مسیر انتها به انتها مرتب شوند تکراری دوم برای ارسال مجدد، باعث ارسال مجدد می شود. با ACK و تحت سیاست انتظار فقط برای n تکراری برای به درستی دریافت شوند، در n تکراری سه گانه، باید اینطور باشد که دو بسته بعد از بسته ACK انتظار برای یک تکراری سه گانه احتمالاً احساس می کرند که انتظار برای دو ACK دریافت نشده است. طراحی طرح حالی که بسته (به جای 1) معاوضه مناسبی بین راه اندازی یک ارسال مجدد سریع در صورت نیاز است، اما عدم ارسال مجدد پیش از موعد در مواجهه با سفارش مجدد بسته ها.

(مسئله 37) الف

GoBackN:

در مجموع 9 بخش ارسال می کند. آنها ابتدا بخش های 1، 2، 3، 4، 5 ارسال می شوند و بعداً بخش های 2، 3، 4، 5 دوباره ارسال می شوند.

با شماره دنباله 2، 3، 4 و 5 هستند ACKS با دنباله شماره 1 و 4 ACKS ارسال می کند. آنها 4 دارد.

در مجموع 6 بخش ارسال می کند. آنها در ابتدا بخش های 1، 2، 3، A: تکرار انتخابی 5 و بعداً بخش های 2 ارسال می شوند.

با دنباله شماره 2 وجود ACK با دنباله شماره 1، 3، 4، 5 هستند. یک ACK ارسال می کند. آنها 4 دارد.

در مجموع 6 بخش ارسال می کند. آنها در ابتدا بخش های 1، 2، 3، 4، 5 و A بعدهاً بخش های 2 ارسال می شوند.

با شماره دنباله 6 وجود دارد. توجه ACK با شماره دنباله 2 هستند. یک ACK ارسال می کند. آنها 4 B 5 ACK را با شماره دنباله مورد انتظار ارسال می کند. همیشه یک TCP ACK داشته باشد که.

از ارسال مجدد سریع بدون انتظار تا پایان زمان استفاده می کند TCP این به این دلیل است که (ب).

مسئله 38

است cwnd/RTT بله، نرخ ارسال همیشه نقریباً.

افزایش یابد، آنگاه نرخ کل ورود به صفت از $R/2$ فراتر از (b) مسئله 39 اگر نرخ ورود در شکل 3.46 ظرفیت صفت فراتر می رود و در نتیجه با افزایش نرخ ورود، ضرر افزایش می یابد. زمانی که نرخ ورود باشد، از هر سه بسته ای که از صفت خارج می شود، 1 یک ارسال مجدد است. با افزایش $R/2$ برابر با نلافات، حتی بخش بزرگتری از بسته ها

$R/2$ ، خروج از صفت خواهد بود ارسال مجدد. با توجه به اینکه حداقل نرخ خروج از صفت برای یکی از جلسات است، و با توجه به اینکه یک سوم یا بیشتر با افزایش نرخ ورود، ارسال خواهد شد، توان عملیات تحویل افزایش یابد. به دنبال استدلال مشابه، اگر نرمی از بسته هایی که از صفت λ_{out} موقوفیت آمیز داده نمی تواند بیش از λ_{out} باشد، حداقل مقدار $R/2$ خارج می شوند، ارسال مجدد باشند و حداقل نرخ بسته های خروجی در هر جلسه $(R/2)/2$ یا $R/4$ است.

در TCP در فواصل [1، 6] و [23، 26] عمل می کند (ب) اجتناب از تراکم TCP مشکل 40 (الف) شروع کند بازه های [6، 16] و [17، 22] عمل می کند. (ج) پس از انتقال شانزدهم دور، از دست دادن بسته توسط بک تکراری سه گانه شناسایی می شود ACK.

اگر یک بازه زمانی وجود داشت، اندازه پنجره از دحام به 1 کاهش می یافت.

اندازه پنجره از دحام روی 1 تنظیم شده است. (ه) آستانه در ابتدا 32 است، زیرا در این اندازه پنجره است که شروع آهسته اجتناب از تراکم آغاز می شود. (و) زمانی که از دست دادن بسته تشخیص داده شد، آستانه به نصف مقدار پنجره تراکم تنظیم می شود. هنگامی که از دست دادن در طول انتقال دور 16 تشخیص داده می شود، اندازه پنجره های از دحام 42 آستانه به نصف مقدار پنجره تراکم تنظیم می شود که (g). است. بنابراین آستانه 21 در طول هجدهمین دور انتقال است از دست دادن بسته باشد

شناسایی شده. هنگامی که از دست دادن در طول انتقال دور 22 تشخیص داده می شود، اندازه پنجره های از دحام 29 است. بنابراین آستانه 14 است (دریافت طبقه پایین 14.5) در طول دور انتقال 24

در طول اولین دور انتقال، بسته 1 ارسال می شود. بسته 2-3 در دور دوم ارسال می شود. بسته های 7-4 در دور (h) انتقال 3 ارسال می شوند. بسته های 8-15 در دور انتقال 4 ارسال می شوند. بسته های 16-31 در انتقال پنجم ارسال می شوند

گرد؛ بسته های 32-63 در دور انتقال ششم ارسال می شوند. بسته های 64 تا 96 در دور انتقال هفتم ارسال می شوند. بنابراین بسته 70 در دور انتقال هفتم ارسال می شود و قتنی از دست دادن رخ داد، آستانه به نصف مقدار فعلی پنجره تراکم (8) و پنجره تراکم روی مقدار آستانه جدید + 3 (من تنظیم می شود). بنابراین مقادیر جدید آستانه و پنجره به ترتیب 4 و 7 خواهد بود MSS.

دور 17، 1 بسته دور 18، 2 بسته دور 19، 4 بسته دور 20، 8 (آستانه 21 است، و اندازه پنجره ازدحام 1 است (j) بسته) دور 21، 16 بسته بسته دور 22، 21. بنابراین، تعداد کل 52 است.

نسبت کاهش خطی در تلفات بین اتصال 1 و اتصال 2، (a) مشکل 41 به شکل 5 مراجعه کنید. در شکل 5 خارج نمی AB یکسان است - با افزایش نسبت خطی: وحدت در این حالت، گزندگان ها هرگز از بخش خط، نسبت کاهش خطی تلفات بین اتصال 1 و اتصال 2:1 است. به این معنا که، (b) شوند. در شکل 5

هر زمان که اتفاق وجود داشته باشد، اتصال 1 پنجره خود را دو برابر مقدار اتصال 2 کاهش می دهد. می بینیم که در نهایت، پس از تلفات کافی و افزایش های بعدی، توان عملیاتی اتصال 1 به 0 می رسد و پنهانی باند کامل پیوند به آن اختصاص می یابد. اتصال 2

با افزایش خطی، کاهش خطی TCP شکل 5: عدم همگرایی

یک پروتکل توقف و انتظار بود، دو برابر کردن فاصله زمانی به عنوان یک مکانیسم TCP مشکل 42 اگر از خط لوله استفاده می کند (و بنابراین یک پروتکل توقف و انتظار TCP، کنترل تراکم کافی است. با این حال نیست)، که به فرستنده اجازه می دهد چندین بخش شناسایی نشده بر جسته داشته باشد. دو برابر شدن فاصله زمانی از ارسال تعداد زیادی از بسته های ارسالی برای اولین بار به شبکه نمی TCP مانع از ارسال یک فرستنده - شود، حتی زمانی که مسیر انتها به انتها به شدت شلوغ است. بنابراین از دحام

مکانیزم کنترلی برای جلوگیری از جریان "داده های دریافت شده از برنامه بالا" در صورت وجود نشانه هایی از تراکم شبکه موردنیاز است.

مشکل 43 در این مشکل، هیچ خطری در سرریز شدن گیرنده وجود ندارد زیرا بافر دریافت گیرنده می‌تواند کل فایل را نگه دارد. همچنین، به دلیل اینکه هیچ ضرری وجود ندارد و تأییدیه‌ها قبل از انقضای تایمیرها به طور A فرستنده را کاهش نمی‌دهد. با این حال، فرآیند در میزبان TCP برگردانده می‌شوند، کنترل ازدحام مذامن داده‌ها را به سوکت ارسال نمی‌کند زیرا بافر ارسال به سرعت پر می‌شود. هنگامی که بافر ارسال پر ارسال می‌کند $S \rightarrow R$ شد، فرآیند داده‌ها را با نزدیک متواسط یا

برای افزایش RTT افزایش یابد. CongWin طول می کشد تا RTT مشکل 44 الف) 1 به 6 MSS 7 به 3 MSS عدد RTT

برای افزایش MSS.6 RTT برای افزایش MSS.5 RTT 10 برای افزایش MSS.4 RTT 9 برای افزایش MSS.7 RTT 12 برای افزایش MSS.8 RTT 11.

ارسال شد. در سومین RTT 6 MSS ارسال شد. در دومین RTT 5 MSS ب) در اولین ارسال MSS ششم RTT 10 ارسال شد. و در MSS پنجم، 9 RTT ارسال شد. در RTT 8 MSS شد. در چهارمین ارسال شد (و تایید شد). بنابراین، می‌توان گفت که $RTT = 5+6+7+8+9+10 = 45$ MSS، RTT شد. بنابراین، تا زمان 6 بود. میانگین توان عملیاتی تا زمان 6 RTT (45 MSS)/(6 RTT) = 7.5 MSS/RTT.

نرخ تلفات مسئله 45 (الف) به تعداد بسته ها است، [] از دست رفته بسته هایی که تعداد

اً سال شد در یک حر خه، ۱ سته گم می شود تعداد بسته های ارسال شده در یک حر خه است

$$\sum_{n=0}^{\infty} n = \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \dots$$

$$= \frac{دبليو}{4} + \frac{دبليو}{2} + \frac{دبليو}{8} + \frac{دبليو}{4}$$

$$= \frac{8}{3} بليو^2 + \frac{4}{3} بليو$$

بنابراین نرخ ضرر است

$$L = \frac{1}{\frac{8}{3} + \frac{4}{2}} = \frac{1}{\frac{16}{3}} = \frac{3}{16}$$

از متن، ما. $\frac{3}{8}$ دبليو يا $\frac{4}{3}$ دبليو $\approx L$ بدين ترتيب. دبليو $\frac{3}{8}$ دبليو يا $\frac{4}{3}$ دبليو \gg بزرگ W (ب) برای بنابراین دارد.

$$\begin{aligned} \text{متوجه توان عملیاتی} &= \frac{4}{3} \cdot \frac{RTT}{MSS} \\ &= \frac{22.1}{1500} \cdot \frac{RTT}{MSS} \end{aligned}$$

نشان دهنده حداکثر اندازه پنجره اندازه گیری شده در بخش باشد. سپس W مسئله 46 (الف) اجازه دهد $W^*MSS/RTT =$

مگایت در ثانیه، زیرا اگر حداکثر سرعت ارسال از ظرفیت پیوند بیشتر شود، بسته ها حذف می شوند. بنابراین $10W/2$ حدود 125 قطعه است (ب) از آنجایی که اندازه پنجره تراکم از W داریم، سپس $1500^*8/0.15 = 10^*10^8$ متفاوت است، پس اندازه پنجره متوسط است W تا

سگمنت. میانگین توان عملیاتی $0.75W = 94$ مگایت در ثانیه است (سقف 93.75).

برای افزایش اندازه پنجره خود از TCP که این اتصالات (ج) $RTT = 0.15 * 94/2 = 0.075$ ثانیه، به عنوان تعداد یک افزایش می یابد RTT داده می شود. بدین طور پنهان، اندازه پنجره در هر $W/2$ توسعه نیاز دارد.

نشان دهنده اندازه بافر باشد. برای S نشان دهنده حداکثر اندازه پنجره باشد. اجازه دهد W مشکل 47 اجازه دهد بسته های داده را به صورت دور به دور ارسال می کند که هر دور مربوط TCP سادگی، فرض کنید فرستنده بررسد، از دست دادن رخ می دهد. سپس فرستنده اندازه پنجره از دحام W است. اگر اندازه پنجره به یک ACK بسته خود را به نصف کاهش می دهد و قبل از اینکه دوباره باخس های داده را ارسال کند منتظر می ماند. برای اطمینان از اینکه پیوند همیشه مشغول ارسال داده است، باید اجازه دهیم پیوند مشغول $W/2$ های است. بسته $W/2$ ها برای ACK این بازه زمانی است که فرستنده منتظر باشد ($C/2$) ارسال داده در دوره $S>=W/2$ باشد، یعنی $S>=W/2$ نباید کمتر از $C/2$ باشد، بنابراین (های بر جسته

رسید و $W/2$ تأخیر انتشار یک طرفه بین فرستنده و گیرنده را نشان دهد. وقتی اندازه پنجره به حداقل Tp اجازه دهد داشته باشیم، $C/2Tp \geq W/2$ بافر خالی است، باید مطمئن شویم که پیوند نیز مشغول ارسال داده است. بنابراین، باید $W/2 \geq C/2Tp$.

بنابراین $S>=C/2Tp$.

$W^*MSS/RTT = 10$ نشان دهنده حداکثر اندازه پنجره باشد. سپس W مسئله 48 (الف) اجازه دهد گیگابیت بر ثانیه، همانطور که بسته ها انجام می دهند و $10^{10} \cdot 10^9 = 10^{10}$ اگر حداکثر نرخ ارسال به ظرفیت پیوند برسد، حنف می شود. بنابراین، ما قطعه داریم $W=125000$ سپس $W=93750$ متغیر است، پس میانگین اندازه پنجره $W/2$ تا $W/2$ (ب) از آنجایی که اندازه پنجره از دحام از 7.5 است. میانگین توان عملیاتی $8=0.1 \cdot 1500 \cdot 93750$ Gbps.

(ج) $93750/2 = 46875$ دقيقه به منظور سرعت بخشیدن به روند افزایش پنجره، می توانیم اندازه پنجره را افزایش دهیم. برخی RTT با یک مقدار بسیار بزرگتر افزایش دهیم، به جای اینکه اندازه پنجره را تثبیت کنیم، یک بار در هر 2 جلسه TCP ScalableTCP یا HighSpeed TCP.

مسئله 49

$$\text{توسط } B \text{ TCP به عنوان میانگین توان عملیاتی} = \frac{22.1 \cdot T}{MSS} \text{ ب} \quad \text{بنابراین ما می دانیم که} ,$$

$L = 1.22 * MSS / (B * RTT)$ از آنجایی که بین دو از دست دادن بسته متوالی، بسته های 1 و 2 بروز می کنند. بنابراین، متوجه می شویم. $T = (1/L) * MSS/B$. وجود دارد، بنابراین TCP ارسال شده توسط فرستنده است B تابعی از T یعنی، $T = B * RTT / (1.22 * MSS)$.

مسئله 50 (الف) این است که $C2$ و $C1$ مسئله 49 (الف) تفاوت کلیدی بین.

اندازه پنجره خود را بعد از 100 میلی $C2$ اندازه پنجره خود را بعد از 50 میلی ثانیه تنظیم می کند، اما $C1$ بنابراین آن را پس از 50 میلی ثانیه و $C1$ ، ثانیه تنظیم می کند فرض کنید هر زمان که یک رویداد ضرر اتفاق می افتد یک، RTT داریم. بعد از هر TCP آن را پس از 100 میلی ثانیه دریافت می کند. ما ممچین مدل ساده زیر را از میانگین نرخ کل ارسال را در پیوند در $C1$ ، اتصال تعیین می کند که آیا باید اندازه پنجره را افزایش دهد یا خیر. برای تلفات را تشخیص 50 میلی ثانیه قبلی محاسبه می کنیم. اگر این نرخ از ظرفیت پیوند بیشتر شود، فرض می کنیم که میانگین کل نرخ ارسال را در پیوند در 100 میلی ثانیه قبلی $C2$ داده و اندازه پنجره آن را کاهش می دهد. اما برای تلفات را تشخیص داده و اندازه $C2$ محاسبه می کنیم. اگر این نرخ از ظرفیت پیوند بیشتر شود، آنگاه فرض می کنیم که پنجره آن را کاهش می دهد. بنویسید که ممکن است میانگین نرخ ارسال در 50 میلی ثانیه کنسته بیشتر از ظرفیت پیوند باشد، اما میانگین نرخ ارسال در 100 میلی ثانیه کنسته کوچکتر یا مساوی ظرفیت پیوند باشد، در این نخواهد بود $C2$ با ضرر موافق شود. رویداد اما $C1$ صورت فرض می کنیم که

جدول زیر تکامل اندازه پنجره ها و نرخ ارسال را بر اساس مفروضات فوق شرح می دهد.

	$C1$	$C2$
زمان (میلی ثانیه)	اندازه پنجره (تعداد در هر بخش)	اندازه پنجره (تعداد در هر بخش)
50	میانگین نرخ ارسال داده (بخش دوم) $= Window/0.05$	میانگین نرخ ارسال داده (بخش دوم) $= Window/0.1$
0	10	10
	[در [50-0] میلی ثانیه) 200	[در [50-0] میلی ثانیه) 100

50	پنجره را) 5 کاهش می دهد اندازه میانگین را مانند در حال ارسال جمع را به نرخ آخر که در ارتباط دان میلی 50 است $300 = 200 + 100)$	[در [100-50] میلی ثانیه) 100	[در [100-50] میلی ثانیه) 100
100	پنجره را) 2 کاهش می دهد اندازه میانگین را مانند در حال ارسال جمع را به نرخ آخر که در ارتباط دان میلی 50 است $200 = 100 + 100)$	اندازه پنجره) 5 را به عنوان میانگین کل نرخ ارسال به لینک در 100 میلی ثانیه گذشته است $250 = (200 + 100)/2 + (100 + 100)/2)$	اندازه پنجره) 50 را به عنوان میانگین کل نرخ ارسال به لینک در 100 میلی ثانیه گذشته است $(200 + 100)/2 + (100 + 100)/2)$
150	پنجره را) 1 کاهش می دهد اندازه میانگین را مانند در حال ارسال جمع را به نرخ آخر که در ارتباط دان میلی 50 است $90 = (40 + 50)$	اندازه پنجره) 20 را به عنوان میانگین نرخ کل ارسال به لینک در 100 میلی ثانیه گذشته است $80 = (40 + 20)/2 + (50 + 50)/2)$	اندازه پنجره) 50
200	1 کاهش بیشتر، به عنوان اندازه پنجره قبل 1 است	اندازه پنجره) 20 را به عنوان میانگین نرخ کل ارسال به لینک در 100 میلی ثانیه گذشته است $80 = (40 + 20)/2 + (50 + 50)/2)$	اندازه پنجره) 20
250	1 کاهش بیشتر، به عنوان اندازه پنجره	20	20

در حال حاضر 1
1 300 (نه بیشتر است) 20

اندازه پنجره) 1
را به عنوان
میانگین کل نرخ
ارسال به

مانند، نزول کردن
اندازه پنجره
(قبل از 1 است)

لینک در 100 میلی
ثانیه گذشته است

$$40 = \\ (20+20)/2 + \\ (20+20)/2$$

350	2	40	10	
400	1	20	1	10
450	2	40		10
500	1	20	1	10

پنجره را) 1
کاهش می
اندازه دهد
میانگین را مانند

در حال ارسال جمع
را به نرخ
آخر که در ارتباط داری

است 50 میلی
 $50 = (40+10)$

550	2	40	10	
600	1	20	1	10
650	2	40		10
700	1	20	1	10
750	2	40		10
800	1	20	1	10
850	2	40		10
900	1	20	1	10
950	2	40		10
1000	1	20	1	10

هر کدام 1 قطعه C2 و C1 بر اساس جدول بالا، متوجه می شویم که بعد از 1000 میلی ثانیه، اندازه پنجره های است.

کوتاهتر RTT دارای C1 است، زیرا C2 تقریباً دو برابر پهنای باند C1 ب) خیر. در درازمدت، سهم پهنای باند تنظیم کند. اگر به C2 می تواند اندازه پنجره خود را دو برابر سریعتر از C1 بنابراین، C2، C1 است، فقط نیمی از جدول بالا نگاه کنیم، می توانیم یک چرخه را در هر 200 میلی ثانیه بینیم، مثلًا از 850 تا 1000 میلی ثانیه، C2 است، که سه برابر بزرگتر از ارسال C1 $(40+20+40+20 = 120)$ شامل. در یک چرخه، نرخ ارسال است که با $(10+10+10+10 = 40)$ است.

مسئله 51

(الف) مانند مسئله آخر، در جدول زیر می توانیم اندازه پنجره های آنها را در طول زمان محاسبه کنیم. هر دو بعد از 2200 میلی ثانیه اندازه پنجره 2 پکسان دارند.

C1				C2			
زمان (میلی ثانیه)	اندازه پنجره	داده ها	سرعت در حال ارسال	اندازه پنجره	داده ها	سرعت در حال ارسال	
	از (تعداد بخش ها)	دومین مطابق بخش ها)	دومین مطابق بخش ها)	از (تعداد بخش های تبعی	ارسال شد	دومین مطابق بخش ها)	
		=0.1 بخش ها در 100 میلی ثانیه		=0.1 بخش های تبعی			
		(بعد از ارسال می شوند)		(پنجره/ه)			
0	15	150	[در [0-100] میلی ثانیه)	100	100	[در [0-100] میلی ثانیه)	
100	7	70		5	50		
200	3	30		2	20		
300	1	10		1	10		
400	2	20		2	20		
500	1	10		1	10		
600	2	20		2	20		
700	1	10		1	10		
800	2	20		2	20		
900	1	10		1	10		
1000	2	20		2	20		
1100	1	10		1	10		
1200	2	20		2	20		
1300	1	10		1	10		
1400	2	20		2	20		
1500	1	10		1	10		
1600	2	20		2	20		
1700	1	10		1	10		
1800	2	20		2	20		
1900	1	10		1	10		
2000	2	20		2	20		
2100	1	10		1	10		
2200	2	20		2	20		

پکسان دارند RTT است و اینکه هر دو اتصال AIMD TCP (ب) بله، این به دلیل الگوریتم.

(ج) بله، این را می توان به وضوح از جدول بالا مشاهده کرد. حداقل اندازه پنجره آنها 2 است. (د) نه، این همگام سازی به بهبود استفاده از پیوند کمک نمی کند، زیرا این دو

اتصالات به عنوان یک اتصال واحد در نوسان بین حداقل و حداقل اندازه پنجره عمل می کنند. بنابراین، پیوند به طور کامل مورد استفاده قرار نمی گیرد (به یاد بیاورید که فرض می کنیم این پیوند هیچ بافری ندارد). یکی از راه های ممکن برای شکستن همگام سازی، اضافه کردن یک بافر محدود به لینک و رها کردن تصادفی بسته ها در بافر قبل از سرریز شدن بافر است. این باعث می شود که اتصالات مختلف اندازه پنجره خود را در زیادی برای انجام این کار وجود دارد، (میریت صفت فعال) AQM (متناوب و یکپارچه AQQ)، (تشخیص اولیه تصادفی) RED و، (صف مجازی تطبیقی) AVQ، (متناوب و یکپارچه PI)، (REM) علامت گذاری نمایی تصادفی).

مسئله 52

نشان دهنده حداکثر اندازه پنجره است. ابتدا می‌توانیم تعداد کل بخش‌هایی را که در طول بازه W توجه داشته باشید که می‌شود، ارسال کنیم W تغییر می‌دهد و شامل W به $W/2$ اندازه پنجره خود را از TCP زمانی که

$$S = W/2 + (W/2)*(1+\alpha) + (W/2)*(1+\alpha)^2 + (W/2)*(1+\alpha)^3 + \dots + (W/2)^*(1+\alpha)^k \quad k = \log(1+\alpha) \quad S = W^*(2\alpha+1)/(2\alpha)$$

$$L = 1/S = (2\alpha) / (W^*(2\alpha+1)) \quad \text{داده می شود}$$

افزایش دهد، با W به $W/2$ طول می‌کشد تا اندازه پنجره خود را از TCP زمانی که به دست می‌آید، $(\log(1+\alpha)/2) * RTT$. مستقل است TCP که به وضوح از میانگین توان

$$B = MSS * \frac{S}{((k+1)*RTT)} = MSS / (L*(k+1)*RTT) \quad \text{داده می شود}$$

$$\frac{B}{MSS} = \frac{22.1 * T}{MSS} \quad \text{که دارای توان عملیاتی متوسط است متفاوت است TCP توجه داشته باشید که این با در مخرج ظاهر می شود } L \text{ جایی که جذر}$$

مسئله 53

TCP بباید بسته های 1500 بایتی و 100 میلی ثانیه زمان رفت و برگشت را فرض کنیم. از توان عملیاتی

$$\frac{22.1 * T}{MSS} = \frac{\text{ما داریم}}{\text{معادله}}$$

$$10 * \frac{1.22 * srqt(L)}{8 * 1500} = 1 * \text{گیگابیت در ثانیه}$$

$$srqt(L) = 14640 \quad \text{با } 9^{10} \text{ بیت}$$

$$L = 2.14 * 10^{-10}$$

مسئله 54

مجبور نیست از شروع آهسته و TCP این است که t_2 در $cwnd$ و $ssthresh$ مزیت استفاده از مقادیر قبلی برسد. یک نقطه ضعف استفاده از این t_1 اجتناب از تراکم عبور کند تا به مقدار توان عملیاتی به دست آمده در شلوغتر شده باشد، فرستنده t_2 و t_1 مقادیر این است که ممکن است دیگر دقیق نباشد. بمویزه، اگر مسیر بین بخش‌های بزرگی از پنجره را به مسیری که قبلاً (بیشتر) مترامک شده ارسال می‌کند

مسئله 55

ارسال می کند γ (الف) سرور پاسخ خود را به

به SYNACK بود γ است. اگر در آدرس دیگری جعل γ (ب) سرور می‌تواند مطمئن باشد که کلاینت واقعاً در را به عقب نمی‌فرستاد. حتی اگر مهاجم یک TCP ACK در آن میزبان، بخش ارسال می‌شد و γ آدرس با زمان مناسب ارسال کند، شماره توالی سرور صحیح را نمی‌داند (زیرا سرور از اعداد دنباله TCP ACK قطعه اولیه تصادفی استفاده می‌کند).

مسئله 56

(الف) با مراجعه به شکل زیر می‌بینیم که کل تأخیر می‌باشد

$$RTT + RTT + S/R + RTT + S/R + RTT + 12S/R = 4RTT + 14 S/R$$

(ب) به همین ترتیب تأخیر در این مورد عبارت است از:

$$RTT + RTT + S/R + RTT + S/R + RTT + S/R + RTT + 8S/R = 5RTT + 11 S/R$$

(ج) به همین ترتیب تأخیر در این مورد عبارت است از:

$$RTT + RTT + S/R + RTT + 14 S/R = 3 RTT + 15 S/R$$

را TCP اتصال
آغاز کنید

شی
درخواست

پنجره اول
 $= S/R$

RTT

پنجره دوم
 $= 2S/R$

پنجره سوم
 $= 4S/R$

پنجره چهارم
 $= 8S/R$

شی تحویل
داده شد

انتقال کامل

زمان در
مشتری

زمان در
سرور

فصل 4 سوالات مروری

بسته (لایه 3) ارسال می کند. یک سوئیچ IP بسته لایه شبکه یک دیتاگرام است. روتر یک بسته را بر اساس آدرس 1. بسته (لایه 2) ارسال می کند MAC لایه پیوند، بسته ای را بر اساس آدرس

تنظیم تماس: VC لایه شبکه مبتنی بر دیتاگرام: ارسال مسیر یابی عملکرد اضافی لایه شبکه مبتنی بر 2.

3. Forwarding مربوط به انتقال یک بسته از درگاه ورودی روتر به پورت خروجی مناسب است. مسیر یابی در مورد تعیین مسیر های انتهایی بین مبدأ و مقصد است.

بله، هر دو از جداول فوروارد استفاده می کنند. برای توضیحات جداول، بخش 4.2 را ببینید.

بسته تک: تحويل تضمینی. تحويل تضمینی با حداکثر تاخیر تضمین شده هر یک بسته ها: تحويل بسته به ترتیب؛ حداقل 5. پنهانی باند تضمین شده؛ حداکثر لرزش تضمین شده هیچ یک از این خدمات توسعه لایه شبکه اینترنت ارائه نمی هیچ یک از این خدمات را ABR. هم تحويل تضمینی و هم زمان بندی را ارائه می دهد CBR ATM شود. خدمات ارائه نمی دهد.

بهره CBR و کنفرانس ویدئویی، می توانند از خدمات IP برنامه های چند رسانه ای زنده تعاملی، مانند تلفن 6. مند شوند که زمان بندی را حفظ می کند.

با کمی سایه، جستجوی ارسال به صورت محلی، در هر پورت ورودی، بدون فراخوانی پردازنده مسیر یابی متمنکز 7. انجام می شود. چنین رویکرد غیرمتمنکری از ایجاد گلگاه پردازش جستجو در روتر جلوگیری می کند.

سوئیچینگ از طریق حافظه سوئیچینگ از طریق اتوپوس؛ سوئیچینگ از طریق یک شبکه ارتباطیک شبکه ارتباطی 8. می تواند بسته ها را به صورت موازی ارسال کند تا زمانی که همه بسته ها به پورت های خروجی مختلف ارسال شوند.

اگر سرعت رسیدن بسته ها به پارچه از نرخ سوئیچینگ فابریک بیشتر شود، بسته ها باید در درگاه های ورودی 9. صف بکشند. اگر این عدم تطابق نرخ ادامه یابد، صفات بزرگتر و بزرگتر می شوند و در نهایت از بافر های پورت برای سرعت n ورودی سرریز می شوند و باعث از دست رفتن بسته های می شوند. اگر سرعت فابریک سوئیچینگ حداقل تعداد پورت های ورودی است، از دست دادن بسته حذف می شود n خط ورودی باشد، که

با فرض یکسان بودن سرعت خط ورودی و خروجی، اگر سرعت رسیدن بسته ها به یک پورت خروجی از 10. سرعت خط بیشتر شود، باز هم می تواند از دست دادن بسته رخ دهد. اگر این عدم تطابق نرخ ادامه یابد، صفات بزرگتر و بزرگتر می شوند و در نهایت از بافر های پورت خروجی سرریز می شوند و باعث از دست رفتن بسته های می شوند. توجه داشته باشید که افزایش سرعت فابریک سوئیچ نمی تواند از بروز این مشکل جلوگیری کند

گاهی اوقات بسته‌ای که در صفحه اول در پورت خروجی قرار می‌گیرد باید منتظر: HOL مسدود کردن 11. بماند زیرا فضای بافری در پورت خروجی که می‌خواهد به آن ارسال شود وجود ندارد. وقتی این اتفاق می‌افتد، تمام بسته‌های پشت بسته اول مسدود می‌شوند، حتی اگر صفحه‌ای خروجی آنها فضایی برای جا دادن آنها داشته باشد، مسدود در درگاه ورودی رخ می‌دهد HOL کردن.

بله. آنها برای هر رابط یک آدرس دارند. 12.

13. 11011111 00000001 00000011 00011100.

دانش آموزان برای این سوال پاسخ‌های صحیح متفاوتی خواهند گرفت. 14.

رابط; 3 میز حمل و نقل 8

سربرار 50%.

حاوی اطلاعاتی است که میزبان مقصد باید قطعه را به کدام پروتکل لایه انتقال IP فیلد پروتکل 8 بینی در دیتاگرام 17 ارسال کند.

به 5 رایانه IP برای تخصیص آدرس DHCP است 18. ISP از IP نیز استفاده می‌کند زیرا فقط یک آدرس NAT شخصی و رابط روتور استفاده می‌شود. بله، روتور بی سیم از دریافت می‌کند.

می‌تواند شامل شود را IPv4 دارای یک هدر طول ثابت است که اکثر گزینه‌هایی را که یک هدر IPv6 باشد، کل هدر فقط 40 (مبدأ و مقصد IP آدرس) شامل دو آدرس 128 بینی IPv6 شامل نمی‌شود. حتی اگر هدر بایت طول ثابت دارد. بسیاری از زمینه‌ها از نظر روحی مشابه هستند. کلاس ترافیک، طول بار، هدر بعدی و به ترتیب مشابه نوع سرویس، طول دیتاگرام، پروتکل لایه بالایی و زمان زندگی در IPv6 محدودیت چهش در IPv4 است.

کپسوله شده است IPv4 در یک دیتاگرام (شامل فیلدهای هدر) IPv6 بله، زیرا کل دیتاگرام 20.

الگوریتم‌های وضعیت پیوند: مسیر کم هزینه بین منبع و مقصد را با استفاده از دانش کامل و جهانی در مورد 21. شبکه محاسبه می‌کند. مسیریابی بردار فاصله: محاسبه مسیر کم هزینه به صورت تکراری و توزیع شده انجام می‌شود. یک گره فقط همسایه‌ای را می‌شناسد که باید بسته‌ای را به آن ارسال کند تا در مسیر کم هزینه به مقصد برسد، و هزینه‌ان مسیر از خود به مقصد را می‌شناسد.

همه روتورها یک پروتکل مسیریابی، AS، سازماندهی می‌شوند. در یک (ASs) روتورها در سیستم‌های مستقل 22. فقط باید در مورد روتورهای داخل AS را اجرا می‌کنند. مشکل مقیاس حل شده است زیرا یک روتور در یک AS درون بر AS پروتکل inter-AS متصل می‌شوند بداند. برای مسیریابی در سراسر AS خود و زیرشبکه‌هایی که به آن AS اشاره می‌کنند، یک روتور از خود به مقصد را می‌شناسد.

است AS دارای استقلال اداری برای مسیریابی در یک AS خیر. هر 23.

در 7 پرش B می‌تواند از طریق D، برسد. با این حال Z به A می‌گوید که می‌تواند با 11 پرش D خیر. آگهی به 24. فقط 4 A در جدول نیست. از طرف دیگر، اگر در آگهی گفته می‌شد که Z برسد. بنابراین نیازی به تغییر ورودی Z به واقعاً جدول ارسال خود را تغییر می‌دهد D، فاصله دارد C از طریق Z پرش از.

نه فقط به AS یک روتور به طور دوره ای اطلاعات مسیریابی را برای همه روتورهای دیگر در OSPF با 25. روتورهای همسایه خود، پخش می‌کند. این اطلاعات مسیریابی ارسال شده توسط روتور دارای یک ورودی برای هر ارسال شده توسط یک RIP یک از همسایگان روتور است. ورودی فاصله روتور تا همسایه را نشان می‌دهد. یک تبلیغ است، اگرچه این اطلاعات فقط به روتورهای مجاور AS روتور حاوی اطلاعاتی در مورد تمام شبکه‌های موجود در آن ارسال می‌شود.

در مسیرها AS توالی." 26.

ها، مسائل مربوط به سیاست‌ها غالب است. ممکن است مهم باشد که ترافیکی که از یک AS خط مشی: در میان 27. معین ممکن است AS خاص دیگری عبور کند. به طور مشابه، یک AS معین سرچشمه می‌گیرد. نتواند از AS همه چیز اسماء تحت کنترل، AS‌ها حمل می‌کند، کنترل کند. در یک AS بخواهد ترافیک حمل و نقلی را که بین سایر دارد AS اداری یکسانی است و بنابراین سیاست نقش بسیار کمتری در انتخاب مسیرها با.

مقیاس: توانایی یک الگوریتم مسیریابی و ساختارهای داده‌ای آن در مقیاس‌بندی برای مدیریت مسیریابی به/در مقیاس پذیری کمتر، AS است. در یک AS میان تعداد زیادی از شبکه‌ها، موضوعی حیاتی در مسیریابی بین نگران کننده است. برای یک چیز، اگر یک دامنه مدیریتی بیش از حد بزرگ شو، همیشه می‌توان آن را به دو جدید انجام داد AS را بین دو تقسیم کرد و مسیریابی بین AS.

بسیار خط مشی محور است، کیفیت (به عنوان مثال، عملکرد) مسیرهای AS عملکرد: از آنجا که مسیریابی بین مورد استفاده غالب یک نگرانی ثانویه است (یعنی یک مسیر طولانی تر یا پر هزینه تر که معیارهای خط مشی خاصی را برآورده می‌کند ممکن است به خوبی در یک مسیر مورد توجه قرار گیرد. مسیری که کوتاهتر است اما مرتبط با AS به غیر از تعداد پرش) ها، حتی مفهوم هزینه AS آن معیار را ندارد). در واقع، ما دیدیم که در بین واحد، چنین نگرانی‌های خطرمندی اهمیت کمتری دارند و به مسیریابی AS مسیرهای وجود ندارد. با این حال، در یک اجازه می‌دهند بیشتر بر سطح عملکرد تحقق یافته در یک مسیر تمرکز کند.

پیشنهاد کند که مسیر ISP B استفاده کند تا به ISP C می‌تواند از ISP C ساحل شرقی در BGP از طریق نقطه همتای ساحل شرقی است. برای مثال، روتور ISP D ترجیحی برای را با D می‌تواند مسیری به ISP C تبلیغ کند. روتور ساحل غربی در 5 MED را با مقدار D می‌تواند مسیری به ISP C می‌داند که ISP B ، تبلیغ کند. از آنجایی که مقدار کمتری ترجیح داده می‌شود 10 MED مقدار را نادیده بگیرد و بنابراین MED خواهد ترافیک را در ساحل شرقی دریافت کند. در عمل، یک روتور می‌تواند مقدار از طریق D ISP C که مقصد همچنان می‌تواند از مسیریابی داغ سیبزمینی برای انتقال ترافیک به ISP B است انتفاده کند.

یک زیر شبکه بخشی از یک شبکه بزرگتر است. یک زیر شبکه حاوی روتر نیست. مرازنای آن توسط رابطهای 29. **abcd/x** نوشته شده است. به شکل **CDIR** روتر و میزبان تعریف می‌شود. پیشوند بخش شبکه یک آدرس **BGP** است. یک پیشوند یک یا چند زیر شبکه را پوشش می‌دهد. هنگامی که یک روتر یک پیشوند در یک جلسه یک پیشوند همراه با **BGP** را شامل می‌شود. در اصطلاح **BGP** تبلیغ می‌کند، با پیشوند تعدادی از ویژگی‌های است. (یا به سادگی یک مسیر) **BGP** ویژگی‌های آن یک مسیر.

برای شناسایی و جلوگیری از تبلیغات حلقه‌ای استفاده می‌کنند. آنها همچنین از **AS-PATH** روترهای از ویژگی 30. اولین **IP** نشان دهنده آدرس **NEXT-HOP** آن در انتخاب بین چندین مسیر به یک پیشوند استفاده می‌کنند. ویژگی به یک پیشوند معین است. هنگام پیکربندی (دریافت کننده آگهی **AS** خارج از) روتر در امتداد یک مسیر تبلیغ شده استفاده می‌کند **NEXT-HOP** جدول ارسال، روتر از ویژگی.

با آنها **B** که **C** و **A** ردیف 1 دیگر، مثلاً **ISP** نمی‌تواند ترافیک ترانزیت را بین دو **B** ردیف 1 **ISP** پک 31. می‌گذرد تبلیغ نمی‌کند. و **C** را که از **A** مسیرهای **ISP**، قراردادهای همتا دارند، حمل کند. برای اجرای این سیاست می‌گذرد تبلیغ نمی‌کند **A** که از **C** در مسیرهای.

32. N-way unicast است، از جمله:

- کارایی: چندین نسخه از یک بسته از طریق یک پیوند برای پیوندهای بالقوه بسیاری ارسال می‌شود. منع باید چندین نسخه از همان بسته را تولید کند
- آدرس دهی: منع باید آدرس تمام گیرندهای را پیدا کند

F: درخت پوشای؛ **T**: سیل کنترل شده؛ **T**: (الف) سیل کنترل نشده. 33.

F: درخت پوشای؛ **S**: سیل کنترل شده؛ **T**: (ب) سیل کنترل نشده

34.
نادرست

به یک میزبان **IGMP** بروتکلی است که فقط بین هاست و روتور چندپوشی اولین هاپ آن اجرا می‌شود 35. اجازه می‌دهد تا گروه چندپوشی را که می‌خواهد به آن ملحق شود (به روتور چندپوشی اول) مشخص کند. سپس این به روتور چندپوشی بستگی دارد که با دیگر روترهای چندپوشی کار کند (یعنی یک پروتکل مسیریابی چندپوشی را اجرا کند) تا اطیان حاصل شود که داده‌های گروه چندپوشی متصل به میزبان به روتور آخرین هاپ مناسب و از آنجا به میزبان هدایت می‌شوند.

در یک درخت اشتراکی گروهی، همه فرستنده‌ها ترافیک چندپوشی خود را با استفاده از درخت مسیریابی 36. یکسانی ارسال می‌کنند. با درخت مبتنی بر منبع، دیناگرام‌های چندپوشی از یک منع داده شده بر روی درخت مسیریابی خاص ساخته شده برای آن منبع هدایت می‌شوند. بنابراین هر منع ممکن است یک درخت مبتنی بر منبع متفاوت داشته باشد و یک روتور ممکن است مجبور باشد چندین درخت مبتنی بر منع را برای یک گروه چندپوشی معین پیگیری کند.

فصل 4 مسائل

مشکل 1

(الف) با یک شبکه اتصال گرا، هر خرابی روتر شامل مسیریابی آن اتصال می شود. حداقل، این امر مستلزم آن است که روتر «بالادست» از روتر شکست خورده، یک بخش پایین دستی جدید از مسیر به گره مقصد، با تمام سیگنال‌های لازم در راهاندازی یک مسیر، ایجاد کند. علاوه بر این، تمام مسیریاب‌هایی که در مسیر اولیه قرار دارند و در پایین دست گره شکست خورده قرار دارند، باید اتصال ناموفق را با تمام سیگنال‌های لازم برای انجام این کار قطع کنند.

با یک شبکه دیتاگرام بدون اتصال، هیچ سیگنالی برای راهاندازی یک مسیر پایین دست جدید یا حذف مسیر پایین دست قابلیت نیست. بدین این با این حال، جداول مسیریابی باید به روز شوند (به عنوان مثال، یا از طریق یک بردار فاصله الگوریتم یا یک الگوریتم وضعیت پیوند) برای در نظر گرفتن روتر شکست خورده. بدین‌آینه با الگوریتم‌های بردار فاصله، این تغییر جدول مسیریابی گاهی اوقات می‌تواند در ناحیه نزدیک روتر شکست خورده محلى شود. بنابراین، یک شبکه دیتاگرام خواهد بود اولیه بتواند در شرایط استرس زا کار کند یکی از ARPAnet ارجح است. غالباً اینجاست که معیارهای طراحی که دلایلی بود که معماری دیتاگرام برای این جد اینترنت انتخاب شد.

(ب) برای اینکه روتر بتواند مقدار ثابتی از ظرفیت موجود را در مسیر بین گره مبدأ و مقصد برای آن جفت مبداء مقصود حفظ کند، باید ویژگی‌های ترافیک تمام جلساتی را که از آن پیوند عبور می‌کنند بداند. یعنی روتر باید حالت در روتر داشته باشد. این در یک شبکه اتصال گرا امکان پذیر است، اما با یک شبکه بدون اتصال per-session اتصال گرا ترجیح داده می‌شود VC امکان پذیر نیست. بنابراین، یک شبکه

(ج) در این سناریو، معماری دیتاگرام کنترل بیشتری از سربار ترافیک دارد. این به دلیل وجود هدر بسته‌های مختلف هنگامی که همه مدارها راه اندازی VC مورد نیاز برای مسیریابی دیتاگرام‌ها از طریق شبکه است. اما در معماری شوند، هرگز تغییر نخواهد کرد. بنابراین، سربار سیگنالینگ در دراز مدت ناجیز است.

ها روی یک پیوند = 28 = 256. ب) گره مرکز می‌تواند هر VC مسئله 2 (الف) حداقل تعداد را که آزاد از مجموعه باشد انتخاب کند عدد VC.

های کمتری از 256 در حال پیشرفت باشد، بدون اینکه VC به این ترتیب، ممکن نیست که تعداد {1-28,...,0,1} را از مجموعه 0,1,...,28-1 اختصاص دهد. بنابراین، VC (ج) هر یک از پیوندها می‌تواند به طور مستقل اعداد باید VC متفاوت برای هر پیوند در مسیر خود خواهد داشت. هر روتر در مسیر VC احتمالاً یک شماره VC یک مرتبط با پیوند خروجی جایگزین کند VC هر بسته دریافتی را با شماره VC شماره

مشکل 3

VC ورودی، رابط خروجی، شماره VC ستون ها عبارتند از: رابط ورودی، شماره، برای جدول ارسال خروجی. برای جدول ارسال دیتاگرام، ستون ها عبارتند از: آدرس مقصد، رابط خروجی.

مشکل 4

از طریق رابط 3 ارسال می شود H3 (الف) داده های مقصد برای میزبان

آدرس مقصد	رابط پیوند
H3	3

ب) خیر، زیرا قانون حمل و نقل فقط بر اساس آدرس مقصد است.

ج) یکی از تنظیمات ممکن این است:

رابط ورودی	ورودی VC شماره	رابط خروجی	خروچی شماره VC
1	12	3	22
2	63	4	18

یکسانی داشته باشند VC توجه داشته باشید که دو جریان در واقع می توانند اعداد

د) یکی از تنظیمات ممکن این است:

رابط ورودی B. روتر	ورودی VC شماره	رابط خروجی	خروچی شماره VC
1	22	2	24

رابط ورودی C. روتر	ورودی VC شماره	رابط خروجی	خروچی شماره VC
1	18	2	50

رابط ورودی D. روتر	ورودی VC شماره	رابط خروجی	خروچی شماره VC
1	24	3	70
2	50	3	76

مشکل 5

جدید را نمی توان در شبکه ایجاد کرد VC جدید اختصاص داد. بنابراین VC را نمی توان به VC (الف) هیچ شماره

موجود است. چهار لینک وجود دارد. بنابراین تعداد ترکیبات $2^4 = 16$ است. یک مثال VC ب) هر پیوند دارای دو عدد ترکیبی (10,00,00,10) است.

مشکل 6

در یک شبکه مدار مجازی، یک اتصال انتها به انتها وجود دارد به این معنا که هر روتور در طول مسیر باید حالت اتصال را حفظ کند. از این رو سرویس اتصال اصطلاحات. بر یک سرویس حمل و نقل اتصال گرا روی یک لایه شبکه بدون اتصال، سیستم های پایانی حالت اتصال را حفظ می کنند. با این حال روتورها هیچ ارتباطی ندارند. از این رو، IP سرویس اتصال محور اصطلاحات.

مسئله 7

(الف) خیر، شما می توانید هر بار فقط یک بسته را از طریق یک گذرگاه مشترک ارسال کنید.

(ب) بله، همانطور که در متن بحث شد، تا زمانی که دو بسته از گذرگاه های ورودی مختلف و گذرگاه های خروجی متفاوت استفاده می کنند، می توان آنها را به صورت موازی ارسال کرد.

(ج) خیر، در این صورت دو بسته باید همزمان از طریق یک گذرگاه خروجی ارسال شوند که امکان پذیر نیست.

مسئله 8

- (الف) (n-1)
- (ب) (n-1)D
- (ج) 0D 1

مسئله 9

X حداقل تعداد اسلات های زمانی مورد نیاز 3 است. زمان بندی به شرح زیر است. شکاف 1: ارسال در صفحه ورودی میانی ۲ در صفحه ورودی بالا، ارسال

در صفحه ورودی پایین شکاف 3: ۷ در صفحه ورودی وسط، ارسال X شکاف 2: ارسال در صفحه ورودی پایین Z ارسال

بیشترین تعداد اسلات ها هنوز 3 عدد است. در واقع، بر اساس این فرض که یک صفحه ورودی غیرخالی هرگز بیکار در صفحه ورودی میانی یا پایینی است. ۷ در صفحه ورودی بالا و X نمی ماند، می بینیم که اولین اسلات همیشه شامل ارسال صفحه، و در شکاف زمانی دوم، همیشه می توانیم دو دیتاگرام دیگر ارسال کنیم و اخیرین دیتاگرام را می توان در شکاف تایم سوم ارسال کرد.

باشد، در بدترین حالت به 4 شکاف زمانی نیاز است X توجه: در واقع، اگر اولین دیتاگرام در صفحه ورودی پایین

(مسئله 10 الف)

تطبیق پیشوند	رابط پیوند
11100000 00	0
11100000 01000000	1
11100000	2
11100001 1	3
در غیر این صورت	3

(ب) مطابقت پیشوند برای آدرس اول ورودی پنجم است: رابط پیوند 3 تطبیق پیشوند
برای آدرس دوم ورودی سوم است: رابط پیوند 2 تطبیق پیشوند برای آدرس سوم
ورودی چهارم است: رابط پیوند 3

(مسئله 11)

حدوده آدرس مقصد	رابط پیوند
00000000	0
از طریق	
00111111	
 01000000	
از طریق	1
01011111	
 01100000	
از طریق	2
01111111	
 10000000	
تا	2
10111111	
 11000000	
تا	3
11111111	
 0 = تعداد آدرس برای رابط 0	2 ⁶ 64
1 = تعداد آدرس برای رابط 1	= 2 ⁵ 32
2 = تعداد آدرس برای رابط 2	= 2 ⁶ + 2 ⁵ = 64 + 32 = 96
3 = تعداد آدرس برای رابط 3	= 2 ⁶ 64

مسئله 12

محدوده آدرس مقصد	رابط پیوند
از طریق (32 آدرس) 11000000 11011111	0
از طریق (64 آدرس) 10000000 10111111	1
از طریق (32 آدرس) 11100000 11111111	2
از طریق (128 آدرس) 00000000 01111111	3

مسئله 13

223.1.17.0/26
223.1.17.128/25
223.1.17.192/28

مسئله 14

آدرس مقصد	رابط پیوند
200.23.16/21	0
200.23.24/24	1
200.23.24/21	2
در غیر این صورت	3

مسئله 15

آدرس مقصد	رابط پیوند
00 11100000 (224.0/10)	0
11100000 01000000 (224.64/16)	1
1110000 (224/8)	2
11100001 1 (225.128/9)	3
در غیر این صورت	3

مسئله 16

در محدوده 128.119.40.191 تا 128.119.40.128 هر آدرس IP 128.119.40.128

زیر شبکه ها اندازه چهار برابر 128.119.40.64/28، 128.119.40.80/28، 128.119.40.96/28، 128.119.40.112/28

مسئله 17

هزسته	تکالیف	ممکن است	از جانب
(آ)	A: زیر شبکه 214.97.254.0/25 - B: زیر شبکه 214.97.255/24 (آدرس 256) C: زیر شبکه 214.97.254.128/2 (آدرس 120 = 128-8)	214.97.254.0/29	
(ب)	برای ساده کردن راه حل، فرض کنید که هیچ دیتاگرام رابط مسیریاب را به عنوان مقصد نهایی ندارد. همچنین برای زیر شبکه های داخلی بالا-راست، پایین و بالا-چپ به ترتیب برچسب بنویسید D، E، F.	Z: 214.97.254.0/31 E: 214.97.254.2/31 (آدرس 2) F: 214.97.254.4/30 (آدرس 4)	214.97.254/23،

روتر 1

رابط خروجی	طولانی ترین تطبیق پیشوند
A زیر شبکه	11010110 01100001 11111111
D زیر شبکه	11010110 01100001 11111110 00000000
F زیر شبکه	11010110 01100001 11111110 0000001

روتر 2

رابط خروجی	طولانی ترین تطبیق پیشوند
D زیر شبکه	11010110 01100001 11111111 00000000
B زیر شبکه	11010110 01100001 11111110 0
E زیر شبکه	11010110 01100001 11111110 0000001

روتر 3

رابط خروجی	طولانی ترین تطبیق پیشوند
------------	--------------------------

11010110 01100001 11111111 000001	زیر شبکه F
11010110 01100001 11111110 0000001	زیر شبکه E
11010110 01100001 11111110 1	زیر شبکه C

موسسه پلی تکنیک دانشگاه نیویورک عبارتند از IP مشکل 18 بلوک های آدرس:

Net Range: 128.238.0.0 -
128.238.255.255 CIDR: 128.238.0.0/16

دانشگاه استنفورد عبارتند از IP بلوک های آدرس:
NetRange: 171.64.0.0 - 171.67.255.255
CIDR: 171.64.0.0/14

دانشگاه وشنگتن عبارتند از IP بلوک های آدرس: NetRange:
140.142.0.0 - 140.142.255.255
CIDR: 140.142.0.0/16

خاص استفاده کرد IP برای تعیین دقیق موقعیت جغرافیایی یک آدرس whois خیر، نمی توان از خدمات

برای تعیین مکان سرور های وب در مؤسسه پلی تکنیک دانشگاه نیویورک، دانشگاه استنفورد و www.maxmind.com دانشگاه وشنگتن استفاده می شود.

مکان های وب سرور در مؤسسه پلی تکنیک دانشگاه نیویورک می باشد

مکان های وب سرور دانشگاه استنفورد است

مکان های وب سرور در دانشگاه ماساچوست است

مسئله 19

وجود دارد IP حداکثر اندازه فیلد داده در هر قطعه = 680 (زیرا 20 بایت

$$\text{سریتیر). بنابراین تعداد قطعات مورد نیاز است} \\ = \frac{680 \cdot 0}{2400} = 4 \quad \square \quad \square \quad \square$$

شامل هدر) هر قطعه دارای شماره شناسایی 422 خواهد بود. هر قطعه به جز آخرین قطعه دارای اندازه 700 بایت IP شامل هدر. آفست 4 قطعه، 0، 85، 170، 255 (IP شامل هدر) خواهد بود. آخرین دیتاگرام به اندازه 360 بایت (IP خواهد بود. flag=0 خواهد بود. آخرین قطعه دارای

مسئله 20

همچنین TCP حمل می شوند، با هر بخش TCP میلیون بایت. فرض کنید داده ها در بخش های 5 = MP3 حجم فایل را حمل کند MP3 دارای 20 بایت هدر است. سپس هر دیتاگرام می تواند $1460 = 40 - 1500$ بایت از فایل

$$\begin{array}{r} 1460 \quad 10 \quad 5 \quad 6 \\ \text{تعداد دیتاگرام های مورد نیاز} \\ = \frac{1460}{1500} = 3425 \end{array}$$

تمام دیتاگرام به جز آخرین دیتاگرام 1500 خواهد بود.

با این آخرین دیتاگرام 1000 = 40 + 960 بایت خواهد بود. توجه داشته باشید که در اینجا تقسیم بندی وجود ندارد - میزبان پیوندها هستند MTU منبع دیتاگرام های بزرگتر از 1500 بایت ایجاد نمی کند و این دیتاگرام ها کوچکتر از

مشکل 21 (الف) آدرس های خانه: 192.168.1.3، 192.168.1.2، 192.168.1.1 با رابط روتر

(بودن 192.168.1.4 ب)

جدول ترجمه NAT

سمت WAN	سمت LAN
24.34.112.235, 4000	192.168.1.1, 3345
24.34.112.235, 4001	192.168.1.1, 3346
24.34.112.235, 4002	192.168.1.2, 3445
24.34.112.235, 4003	192.168.1.2, 3446
24.34.112.235, 4004	192.168.1.3, 3545
24.34.112.235, 4005	192.168.1.3, 3546

به خارج ارسال می شوند، بنابراین می توانیم از یک IP مشکل 22 (الف) از آنجایی که تمام بسته های استفاده کنیم IP برای ضبط تمام sniffer بسته

با IP از آنجایی که هر میزبان دنباله ای از بسته های NAT بسته های تولید شده توسط میزبان های پشت یک اعداد متوالی و یک شماره شناسایی اولیه مجزا (بسیار به احتمال زیاد، زیرا به طور تصادفی از یک فضای را با شناسه های متوالی در یک خوشه گروه IP می توانیم بسته های ، ID) بزرگ انتخاب شده اند) تولید می کند است NAT بندی کنیم. تعداد خوشه ها تعداد میزبان های پشت

[برای الگوریتم های کاربردی بیشتر، مقالات زیر را ببینید](#)

نوفامبر 2002، 6-8 IMW'02 نوشته استیون ام. بلوین، در ، "NATted تکنیکی برای شمارش میزبان های مارسی" ، فر انسه ظاهر شد.

برای استنتاج مسیر شبکه و ویژگی های سیستم نهایی. ویفنگ چن، یونگ هوانگ، برونو IPID استفاده از فیلد اف. ریبیرو، کیونگ وون سو، هنگانگ ژانگ، ادموندو د سوزا و سیلوا، جیم کوروس، دون تاوسلی.

ایالات متحده آمریکا، MA، مارس - 01 آوریل، 2005. بوستون 31، PAM'05 کارگاه

(ب) با این حال، اگر آن شماره‌های شناسایی بهطور متوازن تخصیص داده نشوند، اما بهطور تصادفی اختصاص داده خوشه‌هایی وجود نخواهد داشت sniffed، تکنیک پیشنهادی در بخش (الف) کار نخواهد کرد، زیرا در داده‌های

مسنون

بین آرنولد و برنارد، آرنولد یا باب باید یک TCP امکان ابداع چنین تکنیکی وجود ندارد. برای برقراری ارتباط مستقیم را که از سمت SYN هایی که آرنولد و باب را پوشش می دهند، بسته های NAT اتصال را با دیگری آغاز کند. اما را به دیگری آغاز کنند اگر هر دو TCP می رساند، رها می کنند. بنابراین نه آرنولد و نه باب نمی توانند اتصال WAN باشند NAT بشت.

24 مسنله yxu، yxvu، yxwu، yxwvu، ywu، ywvu،
ywxu، ywxvu، ywvxu، yzvu، yzwvu، yzwxu،
yzwxvu، yzwvxu،

25 مسئلہ $xz : xyz$
 $xywz, xwz, xwyz,$
 $xvwz, xvwyz,$
 $xuwz, xuwyz,$
 $xuvwz, xuvwyz$

Z ㄔ u: zwu, zwvu, zwxu, zwvxu, zxvxu, zyxu, zyxvu, zyxwu, zyxwyu, zyxvwu, zywvu, zywxu, zywvxu, zywvxu, zywyxu, zywyx

$z \ddot{a} w : z w, z y w, z y x w, z y x v w, z y x u w, z y x u v w, z y x v u w$

مسئله 26

گام	N'	D(t)·p(t)	D(u),p(u)	D(v)· p(v)	D(w),p(w)	D(y)· p(y)	D(z)· p(z)
0	ایکس	∞	∞	3· x	6· x	6· x	8·
1	xv	7· v	6· v	3· x	6· x	6· x	8·
2	xvi	7· v	6· v	3· x	6· x	6· x	8·
3	xvuw	7· v	6· v	3· x	6· x	6· x	8·
4	xvuwy	7· v	6· v	3· x	6· x	6· x	8·
5	xvuwyt	7· v	6· v	3· x	6· x	6· x	8·
6	xvuwytz	7· v	6· v	3· x	6· x	6· x	8· x

مسئله 27

(الف) مرحله	N'	D(x)· p(x)	D(u),p(u)	D(v)· p(v)	D(w),p(w)	D(y)· p(y)	D(z)· p(z)
0	تی	∞	2·	4·	∞	7·	∞
1	تو	∞	2·	4·	5· u	7·	∞
2	tuv	7· v	2·	4·	5· u	7·	∞
3	tuvw	7· v	2·	4·	5· u	7·	∞
4	tuvwx	7· v	2·	4·	5· u	7·	15·
5	tuvwxy	7· v	2·	4·	5· u	7·	15·
6	tuvwxyz	7· v	2·	4· تی	5· u	7· تی	15· x

(ب) مرحله	N'	D(x)· p(x)	D(t)·p(t)	D(v)· p(v)	D(w),p(w)	D(y)· p(y)	D(z)· p(z)
	تو	∞	2· u	3· u	3· u	∞	∞
	ut	∞	2· u	3· u	3· u	9·	∞
	utv	6· v	2· u	3· u	3· u	9·	∞
	utvw	6· v	2· u	3· u	3· u	9·	∞
	utvwx	6· v	2· u	3· u	3· u	9·	14·
	utvwxy	6· v	2· u	3· u	3· u	9·	14·
	utvwxyz	6· v	2· u	3· u	3· u	9· تی	14· x

(ج) مرحله	N'	D(x)· p(x)	D(u),p(u)	D(t)·pt)	D(w),p(w)	D(y)· p(y)	D(z)· p(z)
	v	3· v	3· v	4· v	4· v	8· v	∞
	vx	3· v	3· v	4· v	4· v	8· v	11·
	vxu	3· v	3· v	4· v	4· v	8· v	11·
	vxut	3· v	3· v	4· v	4· v	8· v	11·
	vxutw	3· v	3· v	4· v	4· v	8· v	11·
	vxutwy	3· v	3· v	4· v	4· v	8· v	11·
	vxutwyz	3· v	3· v	4· v	4· v	8· v	11· x

(د) مرحله	N'	D(x)· p(x)	D(u),p(u)	D(v)· p(v)	D(t)·p(t)	D(y)· p(y)	D(z)· p(z)
	w	6· w	3· w	4· w	∞	∞	∞
	وو	6· w	3· w	4· w	5· u	∞	∞
	وای	6· w	3· w	4· w	5· u	12· v	∞
	wuvt	6· w	3· w	4· w	5· u	12· v	∞
	wuvtx	6· w	3· w	4· w	5· u	12· v	14·
	wuvtxy	6· w	3· w	4· w	5· u	12· v	14·
	wuvtxyz	6· w	3· w	4· w	5· u	12· v	14· x

(ه) مرحله	N'	D(x)· p(x)	D(u),p(u)	D(v)· p(v)	D(w),p(w)	D(t)·p(t)	D(z)· p(z)
	y	6· y	∞	8· y	∞	7· y	12· سال
	yx	6· y	∞	8· y	12· x	7· y	12· سال
	yxt	6· y	9·	8· y	12· x	7· y	12· سال
	yxtv	6· y	9·	8· y	12· x	7· y	12· سال
	yxtvu	6· y	9·	8· y	12· x	7· y	12· سال
	yxtvuw	6· y	9·	8· y	12· x	7· y	12· سال
	yxtvuwz	6· y	9· ز	8· y	12· x	7· y	12· سال

(و) قدم	N'	D(x)· p(x)	D(u),p(u)	D(v)· p(v)	D(w),p(w)	D(y)· p(y)	D(t)·p(t)
	z	8· z	∞	∞	∞	12· z	∞
	zx	8· z	∞	11·	14·	12· z	∞
	zxv	8· z	14·	11· x	14·	12· z	15·
	zxvy	8· z	14·	11·	14· x	12· z	15·
	zxvyu	8· z	14· v	11· x	14· x	12· z	15· v

$zxvyuw$	$8 \cdot z$	$14 \cdot$	$11 \cdot$	$14 \cdot x$	$12 \cdot z$	$15 \cdot$
$zxvyuwt$	$8 \cdot z$	$14 \cdot$	$11 \cdot$	$14 \cdot x$	$12 \cdot z$	$15 \cdot$

مسئله 28

هزینه		v	ایکس	y	z
برای شما					
v	∞	∞	∞	∞	∞
ایکس از جانب	∞	∞	∞	∞	∞
z	∞	6	2	∞	0

هزینه به		v	ایکس	y	z
تو					
v	1	0	3	∞	6
ایکس از جانب	∞	3	0	3	2
z	7	5	2	5	0

هزینه به		v	ایکس	y	z
تو					
v	1	0	3	3	5
ایکس از جانب	4	3	0	3	2
z	6	5	2	5	0

هزینه به UV		v	ایکس	y	z
تو					
v	1	0	3	3	5
ایکس از جانب	4	3	0	3	2
z	6	5	2	5	0

مسئله 29

جمله بندی این سوال کمی مبهم بود. منظور ما این بود که «تعداد تکرارها از زمانی که الگوریتم برای اولین بار اجرا می‌شود» (یعنی با فرض اینکه تنها اطلاعاتی که گره‌ها در ابتدا دارند هزینه نزدیکترین همسایگانشان است). فرض می‌کنیم

که الگوریتم به صورت همزمان اجرا می شود (یعنی در یک مرحله، همه گره ها جداول فاصله خود را به طور همزمان محاسبه می کنند و سپس جداول را مبادله می کنند).

هستید و همسایه A در هر تکرار، یک گره جداول فاصله را با همسایگان خود مبادله می کند. بنابراین، اگر شما گره پس از یک بار تکرار (یعنی پس از (که همگی یک یا دو پرش از شما خواهند بود) B است، همه همسایگان B شما (هزینه آن را برای شما به آنها می گوید B. آن) کوتاه ترین مسیر هزینه یک یا دو پرش را برای شما خواهند داشت.

"قطر" شبکه باشد - طول طولانی ترین مسیر بدون حلقه بین هر دو گره در شبکه با استفاده از استدلال بالا، d فرض کنید، پس از تکرارهای 1 روزه یا کمتر را برای همه گره های دیگر خواهند داشت. از آنجایی که هر مسیری با d تمام گره ها کوتاه ترین هزینه مسیر دارای حلقه خواهد بود (و بنابراین هزینه بیشتری نسبت به آن مسیر با حلقه های حذف شده دارد)، d جهش بیشتر از همگرا خواهد شد. الگوریتم حداقل در تکرارهای 1

در نتیجه تغییر در هزینه های پیوند اجرا شود، هیچ محدودیت پیشینی برای تعداد تکرارهای DV بعلوه: اگر الگوریتم مورد نیاز تا زمان همگرایی وجود ندارد، مگر اینکه یک محدودیت برای هزینه های پیوند نیز مشخص کند

$$\text{مسئله 30 الف} \quad D(x,w) = 2, D(x,y) = 4, D(x,u) = 7$$

تا زمانی) بزرگتر یا کوچکتر شود $c(x,y)$ تغییر کند چه اتفاقی می افتد. اگر $c(x,y) < c(y,z)$ باشد در نظر بگیرید که اگر $c(x,y) \geq 7$ هزینه خواهد داشت. بنابراین تغییر در u به x مسیر کمترین هزینه از $c(x,y) > 1$ که $c(x,y) > 1$ باشد نمی شود که (اگر $c(x,y) > 1$)

دارد $\delta + 6$ می گذرد و هزینه y آنگاه مسیر کمترین هزینه اکنون از $1 < \delta = c(x,y)$ اگر.

همچنان از u آنگاه مسیر کم هزینه به $1 < \epsilon = c(x,w)$ تغییر می کند. اگر $c(x,w) < \epsilon$ حال در نظر بگیرید که آیا همسایگان خود را از این هزینه جدید مطلع خواهد x . تغییر می کند $\epsilon + \text{عبور می کند}$ و هزینه آن به 5 w می گذرد و هزینه آن 11 است. دوباره y آنگاه مسیر کمترین هزینه اکنون از $6 > \delta = c(x,w)$ کرد. اگر همسایگان خود را از این هزینه جدید مطلع خواهد کرد.

به همسایگان خود از مسیر x باعث نمی شود که ($c(x,y) \geq 1$ و تا زمانی که $c(x,y) < 1$) هرگونه تغییر در هزینه پیوند اطلاع دهد u حداقل هزینه جدید به

مسئله 31

x جدول گره

هزینه به

	ایکس	y	z
ایکس	0	3	4

	y	∞	∞	∞
	z	∞	∞	∞

		هزینه به xy		
		z		
ایکس	y	0	3	4
	z	3	0	6
	y	4	6	0

		هزینه به xy		
		z		
ایکس	y	∞	∞	∞
	z	3	0	6
	y	∞	∞	∞

		هزینه به xy		
		z		
ایکس	y	0	3	4
	z	3	0	6
	y	4	6	0

		هزینه به xy		
		z		
ایکس	y	∞	∞	∞
	z	3	0	6
	y	∞	∞	∞

		هزینه به xy		
		z		
ایکس	y	0	3	4
	z	3	0	6
	y	4	6	0

ناشی از رابطه) مشکل 32 خیر، این به این دلیل است که کاهش هزینه پیوند باعث ایجاد یک حلقه نمی‌شود اتصال دو گره با یک پیوند معادل کاهش وزن پیوند از بینهایت به وزن.(بعدی بین دو گره از آن پیوند محدود است.

مسئله 33

در هر مرحله، هر به روز رسانی بردارهای فاصله گره بر اساس معادله بلمن-فورد است، یعنی فقط آن مقادیر را در بردار فاصله آن کاهش می دهد. افزایشی در ارزش ها وجود ندارد. در صورت عدم به روز رسانی، هیچ پیامی ارسال غیر افزایشی است. از آنجایی که این هزینه ها محدود هستند، در نهایت بردارهای فاصله در (x) ، $D(x)$ ، نخواهد شد. بنابراین مراحل محدود تثبیت خواهند شد.

مسئله 34 الف

z روتر	$w, Dz(x)=\infty$ به y ، $Dz(x)=6$ اطلاع می دهد
w روتر	$y, Dw(x)=\infty$ به z ، $Dw(x)=5$ اطلاع می دهد
y روتر	$w, Dy(x)=4$ به z ، $Dy(x)=4$ اطلاع می دهد

ب) بله، مشکل شمارش تا بی نهایت وجود خواهد داشت. جدول زیر فرآیند همگرای مسیریابی را نشان می دهد.فرض بردار فاصله خود را به روز می کند و به همسایگان y ، $t1$ تغییر هزینه پیوند اتفاق می افتد. در زمان $t0$ ، کنید در زمان w ، مخفف "اطلاع می دهد" است " \square "، اطلاع می دهد. در جدول زیر z و w روتر

زمان	$t0$	$t1$	$t2$	$t3$	$t4$
z	$\square w, Dz(x)=\infty$ $\square y, Dz(x)=6$		بدون تغییر	$\square w, Dz(x)=\infty$ $\square y, Dz(x)=11$	
دبليو	$\square y, Dw(x)=\infty$ $\square z, Dw$		$\square y, Dw(x)=\infty$ $\square z, Dw$		بدون تغییر
y	$\square w$ $\square z, Dy(x)=4$	$\square w, Dy(x)=9$ $\square z, Dy(x)=\infty$	$\square w, Dy(x)=10$ $\square z, Dy(x)=\infty$	بدون تغییر	$\square w$ $\square z, Dy(x)=\infty$

تشکیل می دهدند. اگر تکرارهای نشان داده شده در x یک حلقه در محاسبه هزینه های روتر z و w می بینیم که تشخیص می دهد که کمترین x از طریق پیوند مستقیم خود با z جدول بالا را ادامه دهیم، خواهیم دید که در $t30$ ، y است. در z از طریق 51 x متوجه می شود که کمترین هزینه برای w در $t29$ است. در 50 x هزینه برای به روز رسانی وجود، $t31$ به روز می کند. در نهایت، در زمان (w از طریق) به 52 x حداقل هزینه خود را به ندارد، و مسیریابی تثبیت می شود.

زمان	$t27$	$t28$	$t29$	$t30$	$t31$
z	$\square w, Dz$ $\square y, Dz$ $(x)=50$			$\square w, \infty$ از طریق	
دبليو		$\square y, Dw(x)=\infty$ $\square z, Dw$ $(x)=50$	$\square y, Dw(x)=51$ $\square z, Dw(x)=\infty$		$\square w, \infty$ از طریق
y		$\square w, Dy(x)=53$ $\square z, Dy(x)=\infty$		$\square w, Dy(x)=\infty$ $\square z, Dy(x)=52$	$\square w, 60$ از طریق

را قطع کنید z و y (ج) پیوند بین

در دسترس است، BGP به یک مقصد در AS از یک AS مشکل 35 از آنجایی که اطلاعات کامل مسیر خودش در مسیر AS مسیری را دریافت کند که شامل شماره BGP تشخیص حلقه ساده است - اگر یک همتا است، استفاده از آن مسیر منجر به یک حلقه می شود AS.

نیست به یاد بیاورید که در فرآیند انتخاب مسیر AS مشکل 36 مسیر انتخاب شده لزوماً کوتاهترین مسیر باید مسائل زیادی در نظر گرفته شود. بسیار محتمل است که یک مسیر بدون حلقه طولانی تر به یک ممکن است ترجیح AS مسیر بدون حلقه کوتاه تر به دلایل اقتصادی ترجیح داده شود. به عنوان مثال، یک کوتاهتر ارسال کند AS دهد ترافیک را به یک همسایه به جای همسایه دیگر با فاصله

(مسئله 37 الف)

eBGP

(ب) iBGP

(ج) eBGP

(د) iBGP

به سمت روتور دروازه آغاز می کند زیرا این واسط مسیر کمترین هزینه را از ۱۱ (مسئله 38 الف).

1
C.

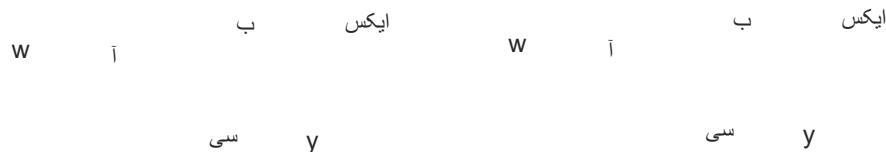
مسیری را شروع می کند که نزدیکترین مسیریاب ۲۱ برابر هستند اما AS-PATH هر دو مسیر دارای طول ۲۱.۲ را دارد.

را دارد AS-PATH مسیری را شروع می کند که کوتاه ترین ۱۱.۱۱ (ج).

مسئله 39

فقط مسیر خود C در ساحل شرقی این است که D به B به واگذاری تمام ترافیک B برای وادار کردن C یکی از راههای تبلیغ کند C از طریق نقطه همای ساحل شرقی خود با D را به

مسئله 40



از توپولوژی X دیدگاه

از توپولوژی W دیدگاه

باشد دریافت AC را که حاوی پیوند y یا w مسیر تبلیغاتی به X اطلاعی ندارد زیرا AC از پیوند X در راه حل فوق دریافت نمی‌کند. مقصد a در مسیر C و AS A هیچ تبلیغی حاوی X نمی‌کند (یعنی

مسئله 41

راشتر اک گذاری فایل BitTorrent و برنامه‌های Skype P2P به اشتراک گذاری فایل هستند. با توجه به مکانیسم Z و X، در نظر بگیرید که در آن همتای 1، 2 و 3 به ترتیب در شبکه‌های خرد اشتراک‌گذاری فایل بیت تورنت، احتمالاً همتای 2 تکه‌های داده را از همتای 1 دریافت می‌کند و سپس آن تکه‌های داده را به 3 ارسال می‌کند.

مسئله 42

C باید به A. را توصیه کند AV و AS AW دو مسیر، مسیرهای B باید به Z را دریافت می‌کند AS مسیرهای C. را توصیه کند AV، فقط یک مسیر BAW، BAV، AV.

مسئله 43

Z ارسال می‌کند. به این ترتیب، وقتی Z تبلیغات مسیر را برای Z، را انتقال دهد Z می‌خواهد ترافیک Z از آنجایی که ارسال کند. با Z می‌تواند دیتاگرام را از طریق Z، قابل دسترسی است Z است که از طریق IP دیتاگرام دارد که مقصد Z، تبلیغ کند. بنابراین، در این مورد X می‌تواند آن مسیرها را مجدداً به Z، را تبلیغ کند Z مسیرهای Z این حال، اگر شود Z به ترانزیت از طریق X نمی‌تواند مانع از ترافیک از

مسئله 44

با هزینه 11 Z متصل است y به X با هزینه 14 (=6+8) از طریق Z درخت پوشاند اقل دارای متصل می‌شود V به X (=3+8) از طریق Z با هزینه Z متصل می‌شود U به V و X با هزینه 14 (=3+3+8) از طریق Z از طریق 17 X، V و U متصل می‌شود W به U و V، (=3+3+3+8)

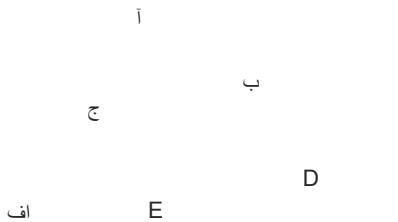
برای رشد یک درخت پوشای حداقل به دست آورد Prim این را می توان با الگوریتم

مسئله 45

دریافت متصل به فرستنده در پیکربندی درخت دودویی نشان داده شده در بالا نشان داده شده است. با پخش لایه 32 شبکه، یک کپی از پیام دقیقاً یک بار روی هر پیوند ارسال می شود. بنابراین 62 گذرگاه لینک $(32+16+8+4+2)$ فرستنده یک کپی را برای هر گیرنده در یک مسیر با 5 پرش یکپارچه می، unicast وجود دارد. با شبیه سازی کند. بنابراین 160 گذرگاه لینک $(32^2 \times 5)$ وجود دارد.

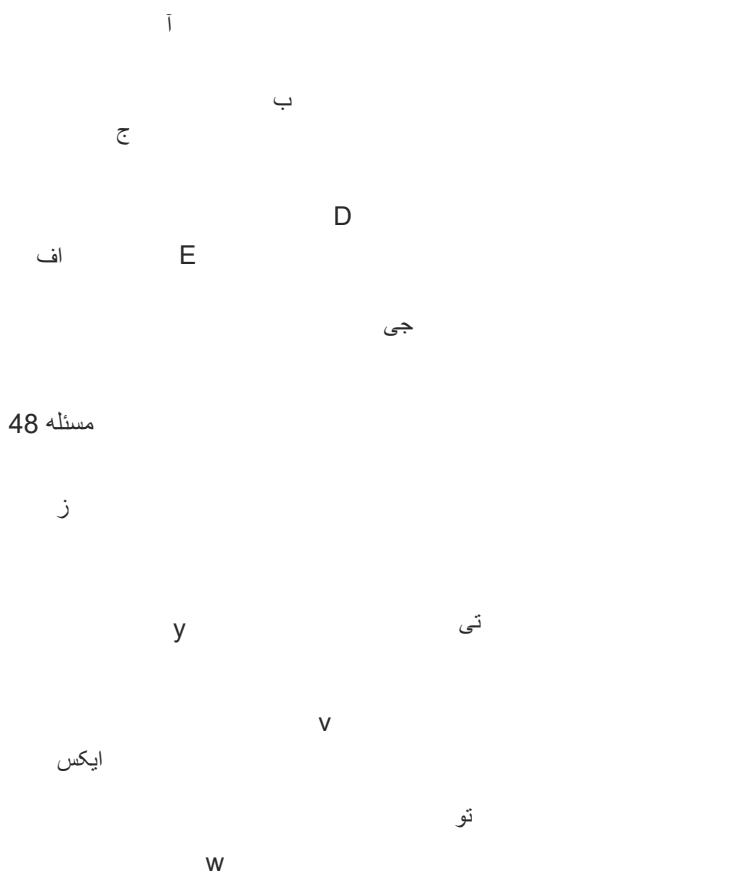
توپولوژی که در آن همه گیرنده ها در یک خط قرار دارند و فرستنده در یک انتهای خط قرار دارد، بیشترین اختلاف را خواهد داشت unicast بین هزینه پخش لایه شبکه و شبیه سازی

مسئله 46



ج
خطوط سایه دار ضخیم نشان دهنده کوتاه ترین درخت مسیر از
به تمام مقصد است. راه حل های دیگری ممکن است، اما در
مسیر دهد D یا C به A نمی تواند از B، این راه حل ها

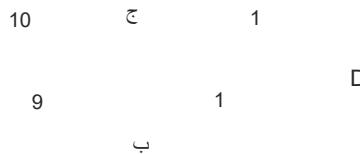
مسئله 47



متصل می C را به A، مشکل 49 درخت مبتنی بر مرکز برای توپولوژی نشان داده شده در شکل اصلی D، E و C به طریق D. همه به طور مستقیم C به F؛ و C؛ E تا B کند. متصل می شود. این درخت مبتنی بر مرکز با حداقل درخت پوشانشان داده شده در شکل متفاوت است.

U. متصل می کند V را به t مشکل 50 درخت مبتنی بر مرکز برای توپولوژی نشان داده شده در شکل اصلی متصل است. این درخت مبتنی بر V به X از طریق Z و. (همه به طور مستقیم) V به y و؛ V؛ X تا V؛ W تا V؛ W؛ X تا V؛ W؛ X؛ Y تا V؛ W؛ X؛ Y؛ Z. مرکز با درخت پوشان حداقل متفاوت است.

به عنوان منبع، منجر به یک درخت مسیر با حداقل A برای شبکه زیر، با گره Dijkstra مشکل 51 الگوریتم با هزینه رایگان کلی 20 می شود. حداقل درخت پوشان، AB، AC، BD، و، هزینه تک پخشی از پیوندهای با هزینه 11 DC، و BD، ، است AB شامل پیوندهای



مسئله 52 بعد از 1 مرحله 3 نسخه ارسال می شود و پس از 2 مرحله 6 نسخه ارسال می گام، نسخه های k شود. پس از 3 مرحله، 12 نسخه ارسال می شود و به همین ترتیب. پس از در آن مرحله ارسال می شود 2^*3^{k-1} .

3
6
12
24
48
...

مسئله 53

پروتکل باید در لایه برنامه ساخته شود. به عنوان مثال، یک برنامه ممکن است به صورت دوره ای هویت خود را در یک پیام لایه برنامه به همه اعضای گروه دیگر چندپخش کند.

مشکل 54 یک پروتکل لایه کاربردی ساده که به همه اعضا امکان می دهد هویت سایر اعضای گروه را بدانند، برای هر نمونه از برنامه کاربردی است که یک پیام چندپخشی حاوی هویت خود را برای همه اعضای دیگر ارسال کند. این پروتکل پیام را به داخل باند ارسال می کند، زیرا کانال چندپخشی برای توزیع پیام های شناسایی و همچنین داده های چندپخشی از خود برنامه استفاده می شود. استفاده از سیگنال دهی درون باند از مکانیزم توزیع چندپخشی موجود استفاده می کند که منجر به طراحی بسیار ساده می شود.

مسئله 55

بیت ها برای آدرس های چندپخشی در دسترس هستند. بنابراین، اندازه چندپخشی $32 - 4 = 28$ فضای آدرس است $28 = N$.

این احتمال وجود دارد که دو گروه یک آدرس را انتخاب کنند

$$\frac{1}{N} 2^{-8} = 1073.3^{-9}$$

این احتمال وجود دارد که 1000 گروه همه آدرس های متفاوتی داشته باشند

$$\frac{1}{1000} \cdot (999!)^2 \cdot 1121 \cdot 999! = \frac{1}{1000} \cdot (999!)^2 \cdot 1121 \cdot 999! = \dots$$

با نادیده گرفتن شرایط محصول متقابل، این تقریباً برابر است

$$1 + \frac{2 + 999}{999!} \cdot \frac{1}{1000} \cdot \frac{0.2}{999!} =$$

فصل 5 سوالات مروری

حالت حمل و نقل، به عنوان مثال، ماشین، اتوبوس، قطار، ماشین 1.

ارسال شده از طریق پیوند در انتهای دیگر پیوند بدون خط IP اگرچه هر پیوند تضمین می کند که دیتاگرام 2، IP، به ترتیب مناسب به مقصد نهایی می رسد. با IP دریافت می شود، اما تضمین نمی شود که دیتاگرام های می توانند مسیرهای مختلفی را در شبکه طی کنند و بنابراین از کار خارج می TCP دیتاگرام ها در یک اتصال همچنان مورد نیاز است تا انتهای دریافت کننده برنامه، جریان بایت را به ترتیب صحیح ارائه TCP. شوند می توانند بسته ها را به دلیل حلقه های مسیریابی یا خرابی تجهیزات از دست بدده IP کند. همچنین

نیز فریم بندی وجود دارد. دسترسی به پیوند تحويل قابل اعتماد: همچنین تحويل قابل TCP و IP کادر بندی: در 3. نیز کنترل جریان وجود دارد. تشخیص خط: همچنین تشخیص TCP وجود دارد. کنترل جریان: در TCP اعتماد در نیز فول دوبلکن است TCP full duplex: وجود دارد. تصحیح خط، TCP و IP خط در

یک برخورد وجود خواهد داشت به این معنا که در حال انتقال است، شروع به دریافت بسته ای 4.

شکافدار فقط تا حدی غیر مرکز است، زیرا نیاز به همگام سازی ساعت ها ALOHA (1، 2، 4) و 5. Slotted Aloha: حلقه نشانه: 1، 2، 3، 4. (در تمام گره ها دارد

پس از برخورد پنجم، آدپتور از بین {0، 1، 2، ...، 31} را انتخاب می کند. احتمال اینکه 4 را انتخاب کند 6.

در نظر سنجی، رهبر بحث به تنها یک شرکت کننده اجازه می دهد که در یک زمان صحبت کند، و هر شرکت کننده 7. فرصتی برای صحبت کردن به صورت دوره ای دارد. برای حلقه نشانه، رهبر بحث وجود ندارد، اما لیوان شرابی وجود دارد که شرکت کنندگان به نوبت آن را در دست می گیرند. یک شرکت کننده فقط در صورتی مجاز به صحبت است که شرکت کننده لیوان شراب را در دست گرفته باشد.

هنگامی که یک گره یک فریم را ارسال می کند، گره باید منتظر بماند تا فریم در کل حلقه منشر شود تا گره 8. کوچک باشد، پروتکل ناکارآمد خواهد بود t_{prop} در مقایسه با R/L بتواند توکن را آزاد کند. بنابراین، اگر

9. 248 آدرس IPv4 آدرس MAC; 232 آدرس IPv6.

فریم ها را پردازش می کند، اما آدپتور دیتاگرام ها را به پشته پروتکل منتقل نمی کند. اگر از آدرس پخش C آدپتور 10. هم فریم ها را پردازش می کند و هم دیتاگرام ها را به پشته پروتکل منتقل می کند C استفاده شود، آدپتور LAN

در یک فریم پخش ارسال می شود زیرا میزبان پرس و جو نمی داند کدام آدرس آدپتور با ARP یک پرس و جو 11. مورد نظر مطابقت دارد. برای پاسخ، گره فرستنده آدرس آدپتوری که پاسخ باید به آن ارسال شود را می داند، IP آدرس بنابراین

(پردازش شود LAN که باید توسط تمام گره های دیگر در) نیازی به ارسال فریم پخش نیست.

نه امکان پذیر نیست. هر شبکه محلی دارای مجموعه ای از آدپتور های متمایز خود است که به آن متصل شده است. 12. منحصر به فرد است LAN که هر آدپتور دارای یک آدرس

سه فناوری اترنت ساختار قاب پکسانی دارد. 13.

14. 2 (زیر شبکه داخلی و اینترنت خارجی)

را می توان VLAN بیتی وجود دارد. بنابراین $2^{12} = 4096$ VLAN 12 یک شناسه Q در پشتیبانی کرد.

را با هم رشته کنیم. سوئیچ اول و آخر از یک پورت برای ترانکینگ استفاده می کند. سوئیچ N می توانیم سوئیچ های پورت است $= 2N-2$. 16. (N-2) وسط از دو پورت استفاده می کنند. بنابراین تعداد کل پورت ها $= 2 + 2N-2$ های

فصل 5 مسائل

مشکل 1

1	1	1	0	1
0	1	1	0	0
1	0	0	1	0
1	1	0	1	1
1	1	0	0	0

: مسئله 2 فرض کنید با ماتریس برابری دو بعدی اولیه شروع می کنیم

0	0	0	0
1	1	1	1
0	1	0	1
1	0	1	0

: با یک خطای بیت در ردیف 2، ستون 3، برابری ردیف 2 و ستون 3 اکنون در ماتریس زیر اشتباه است

0	0	0	0
1	1	0	1
0	1	0	1
1	0	1	0

حال فرض کنید در سطر 2، ستون 2 و ستون 3 یک بیت خطای وجود دارد. برابری سطر 2 اکنون درست است! برابری ستون های 2 و 3 اشتباه است، اما ما نمی توانیم تشخیص دهیم که خطای در کدام ریفیف ها رخ داده است!

```
0 0 0 0
1 0 0 1
0 1 0 1
1 0 1 0
```

مثال بالا نشان می دهد که یک خطای دو بیتی قابل تشخیص است (اگر اصلاح نشود)

مشکل 3

```
01001100 01101001 +
01101110 01101011 ---
-----
10111010 11010100 +
001000-10 -----
-----
11011011 00100000 +
01100001 01111001 ---
-----
00111100 10011010 +
----- 01110010 01100101
00001100 10100010 ----
```

مکمل یکی از مجموع 11110011 01011101 است

مسئله 4 الف) برای محاسبه جمع کنترلی اینترنت، مقادیر را در مقادیر 16 بیتی جمع می کنیم

```
00000001 00000010
00000011 00000100
00000101 00000110
00000111 00001000
00001001 00001010 -
-----
00011110
```

مکمل یکی از مجموع 11100001 11100110 است.

(ب) برای محاسبه جمع کنترل اینترنت، مقادیر را در مقادیر 16 بیتی جمع می کنیم

```

01000010 01000011
01000100 01000101
01000110 01000111
01001000 01001001
01001010 01001011
-----1 -----1 -----1
10100100

```

مکمل یکی از مجموع 01011011 01100000 است

(ج) برای محاسبه جمع چکی اینترنت، مقادیر را در مقادیر 16 بیتی جمع می کنیم

```

01100010 01100011
01100100 01100101
01100110 01100111
01101000 01101001
01101010 01101011
-----1 -----1 -----1

```

متتم یکی از 00000000 00000101
مجموع 11111010 11111111 است.

مشکل 5

اگر $R=0100$ را به 0000 10101010 تقسیم کنیم، 1011011100 به دست می آید که باقیمانده است. $G=10011$ است. توجه داشته باشید که استاندارد CRC-4-ITU

مشکل 6

بدست می آید. (ب) $R=0101$ باقیمانده
بدست می آوریم. (ج) عدد $R=0001$ را باقیمانده
بدست می آوریم $R=0010$ را باقیمانده.

مسئله 7

است و فرض کنید $i \leq r-1$ (الف) بدون از دست دادن کلیت، فرض کنید بیت آن برگردانده شده است، جایی که 0 که کمترین بیت مهم است 0 است.

را K است. واضح است که اگر $i \leq r-1$ خطای تک بیتی به این معنی است که داده های دریافتی حداقل دو عدد 1 داشته باشد، یک خطای بیتی همیشه قابل G تقسیم کنیم، یادآور صفر نیست. به طور کلی، اگر G بر تشخیص است.

را می توان بر 11 (عدد باینری) تقسیم کرد، اما هر تعداد اعداد فرد از 1 را G ب) دیدگاه کلیدی در اینجا این است که نمی توان بر 11 تقسیم کرد. بنابراین، یک دنباله (نه لزوماً به هم پیوسته) از خطاهای بیت اعداد فرد نمی تواند بر 11 تقسیم کرد G تقسیم شود، بنابراین نمی توان آن را بر

مسئله 8

ا)

$$\begin{aligned} E(\varphi) &= Np^1(-Np^{-1}) \\ E(' \varphi) &= 1(-\varphi^0 - NNp^{-1}) - \varphi^{0-2} \\ &= (-\varphi^{0-2} 1((-\varphi) - Np^{-1}))_1 \end{aligned}$$

$$E(' \varphi) = 0 \Rightarrow \varphi^* = \frac{1}{n}$$

ب)

$$\begin{aligned} E(\varphi) &= 1 \left(\sum_{k=1}^{\infty} \frac{1}{k!} \right)_n - \frac{1}{1} = 1 \cdot 1 \left(\frac{1}{n-1} - \frac{1}{n} \right) = \frac{1}{n} \\ &\xrightarrow[n]{\text{حد}} 1 \quad \xrightarrow[n]{\text{حد}} 1 = 1 \end{aligned}$$

بدین مرتب

$$\lim_{n \rightarrow \infty} (\varphi^*) = \frac{1}{n}$$

مسئله 9

$$\begin{aligned} E(\varphi) &= Np^1(-\varphi(2^{0-1}) \\ E(' \varphi) &= n 1(-\varphi^{(2^0-2)} - Np(2n-1)) - \varphi^{(2^0-3)} \\ &= n (-\varphi^{(2^0-3)} 1((-\varphi)(2n-1)))_1 \end{aligned}$$

$$E(' \varphi) = 0 \Rightarrow \varphi^* = \frac{2}{n-1}$$

$$E(\varphi) = \frac{NN}{1_n} - \frac{(2)12}{1_n} \frac{0-1}{1}$$

$$\hat{x} = \infty \rightarrow \begin{matrix} 1 & 2 \\ 1 & 1 \end{matrix} = 2$$

مسئله 10

داده می شود. بازده $pA(1-pB)$ (الف) متوجه توان عملیاتی کل $pA(1-pB) + pB(1-pA)$ است.

است. توان عملیاتی B $pB(1-pA)=2pB(1-pB)=2pB-2(pB)$ (ب) توان عملیاتی A $pA(1-pB)=pB(1-2pB)=pB-2(pB)$ (ج) است. واضح است که توان عملیاتی B دو برابر بزرگتر از A است. نیاز داریم $pA(1-pB)=2 pB(1-pA)$ - (pA/pB) نیست. برای اینکه

است $p(1-p)N-2(1-2p)$ (الف) است و هر گره دیگری دارای توان عملیاتی A (ج) توان عملیاتی B است.

مسئله 11

در A احتمال موفقیت $= p(A)$ ، که در آن $(1 - p(A))$ 4 موفقیت $= p(A)$ (الف) یک شکاف

$$\begin{aligned} p(A) &= p(A) = p(A) \text{ نمی کند و } C \text{ نمی کند و } B \text{ ارسال می کند و} \\ &= p(A) \text{ ارسال نمی کند } D \text{ (ارسال نمی کند } C \text{ (ارسال نمی کند } B \text{ (ارسال نمی کند } A \text{ (برای اولین بار در شکاف 5 موفق می شود)} \\ &= p(1-p)(1-p)(1-p) \\ &= p(1-p)^3 \end{aligned}$$

$$\begin{aligned} &\text{(برای اولین بار در شکاف 5 موفق می شود)} \\ &= (1 - p(A))4 p(A) = (1 - p(1 - p))4 p(1 - p)3 \end{aligned}$$

$$\begin{aligned} p(A) &= p(1-p)^3 \\ p(B) &= p(1-p)^3 \\ p(C) &= p(1-p)^3 \\ p(D) &= p(1-p)^3 \end{aligned}$$

$$\begin{aligned} &p(A) = 4 p(1-p)^3 \\ &\text{(زیرا این رویدادها متقابل هستند)} \end{aligned}$$

$$\begin{aligned} &p(A) = 4 p(1-p)^3 \\ &\text{(برخی گره در یک شکاف موفق می شود)} \\ &p(A) = 4 - 1 p(1-p)^3 \end{aligned}$$

$$\begin{aligned} &p(A) = 4 - 1 p(1-p)^3 \\ &\text{(هیچ گره ای در 2 شکاف اول موفق نمی شود)} \\ &p(A) = 4 - 1 p(1-p)^3 \end{aligned}$$

$$p(A) = 4 p(1-p)^3$$

12 مسأله

مسئله 13

طول یک دور رأی گیری است
QN / نظرسنجی + آر /

است بنابراین حداقل توان عملیاتی است NQ تعداد بیت های ارسال شده در یک دور نظرسنجی

$$R_{QN} = \frac{NQ}{1 + \frac{NQ}{R_{نظرسنجی}}}$$

دکتر

مسئله 14

(الف)، (ب) شکل زیر را ببینید.

		سی	E
A	192.168.1.001 00- 00-00-00-00-00	192.168.2.001 44- 44-44-44-44-44	192.168.3.001 77- 77-77-77-77-77
LAN	روتر 1	LAN	روتر 2
			LAN
	192.168.1.002 22- 22-22-22-22-22	192.168.2.002 33- 33-33-33-33-33-33	192.168.2.003 55-55-55-55-55
B	192.168.1.003 11- 11-11-11-11-11	D	192.168.3.002 88- 88-88-88-88-88
			192.168.3.003 99- 99-99-99-99-99
			af

ج)

تعیین می کند که دیتاگرام باید به رابط 192.168.3.002 هدایت شود E جدول ارسال در 1.

ایجاد و بسته اترنت با آدرس مقصد اترنت 88-88-88-88-88-88 E آدپتور در 2.

روتر 2 بسته را دریافت کرده و دیتاگرام را استخراج می کند. جدول فوروارد در این روتر نشان می دهد که 3. بیتاگرام قرار است به 198.162.2.002 روت شود.

سپس روتر 2 بسته اترنت را با آدرس مقصد 33-33-33-33-33-33 و آدرس منبع 55-55-55-55-55-55 4. ارسال می کند IP 198.162.2.003 . از طریق رابط خود با آدرس

بررسد B این فرآیند تا زمانی ادامه می یابد که بسته به میزبان 5.

را در ARP یک بسته پرس و جو E را تعیین کند. میزبان 198.162.3.002 MAC اکنون باید آدرس E در ARP (د) را به میزبان ARP یک فریم اترنت پخش ارسال می کند. روتر 2 بسته پرس و جو را دریافت می کند و یک بسته پاسخ E توسط یک فریم اترنت با آدرس مقصد اترنت 77-77-77-77-77-77 حمل می ARP می فرستد. این بسته پاسخ E شود.

مسئله 15

LAN در همان F را بررسی کند و سپس باد بگیرد که F میزبان IP می تواند پیشوند زیر شبکه آدرس E (الف) نه ارسال نمی کند R1 بسته را به روتر پیش فرض E، است. بنابراین

$$\begin{aligned} \text{آدرس IP} &= \text{IP منبع: F} \\ \text{آدرس IP} &= \text{MAC آدرس F} \\ \text{آدرس IP} &= \text{MAC آدرس MAC F} \end{aligned}$$

به این موضوع پی ببرد B IP می تواند با بررسی آدرس E LAN ب) خیر، زیرا آنها در یک

منبع IP B مقصد = آدرس IP E's IP منبع = آدرس E تا R1: IP آدرس فریم اترنت از
که R1 رابط آدرس MAC = MAC E's Destination MAC = MAC آدرس زیر شبکه 3 متصل می شود.

دریافتنی یک ARP فریم اترنت را از طریق هر دو رابط خود پخش می کند زیرا آدرس مقصد فریم S1 (ج) سوئیچ در رابط اتصال به زیر شبکه 1 متصل S1 در زیر شبکه 1 قرار دارد که به A آدرس پخش است. و یاد می گیرد که است.

ارسال نمی کند 3 Subnet پیام را به R1 را دریافت می کند، اما ARP نیز این پیام درخواست R1 بله، روتر

ارسال نمی کند، زیرا این آدرس را می توان از پیام MAC A را برای درخواست آدرس ARP پیام پرس و جو B بدهست آورده A پرس و جو.

در جدول ارسال خود اضافه می B را دریافت کرد، یک ورودی برای میزبان B پیام پاسخ S1 هنگامی که سوئیچ در یک B و A (عنی) است B در همان رابط میزبان A کند و سپس فریم دریافتنی را رها می کند زیرا میزبان مقصد LAN شبکه هستند. بخش

R1 را فراخوانی کنیم. یعنی روتر S2 مشکل 16 اجازه دهد سوئیچ بین زیرشبکه های 2 و 3 جایگزین شده است. S2 بین زیرشبکه های 2 و 3 اکنون با سوئیچ

LAN در همان بخش F را بررسی کند و سپس یاد بگیرد که F میزبان IP می تواند پیشوند زیر شبکه آدرس E (الف) نه ارسال نمی کند S2 بسته را به E، است. بنابراین

$$\begin{aligned} \text{آدرس IP} &= \text{IP منبع: F} \\ \text{آدرس IP} &= \text{IP منبع F آدرس MAC} \\ \text{آدرس MAC} &= \text{آدرس MAC E مقصد MAC F} \end{aligned}$$

با آدرس ARP یک بسته پرس و جو E، را پیدا کند. در این مورد MAC B می خواهد آدرس E (ب) بله، زیرا مقصد که آدرس پخش است ارسال می کند.

دریافت می شود B این بسته پرس و جو توسط سوئیچ 1 مجدداً پخش می شود و درنهایت توسط میزبان

$$\begin{aligned} \text{آدرس IP} &= \text{IP منبع = آدرس E} \\ \text{آدرس IP} &= \text{آدرس MAC B مقصد MAC E} \\ \text{آدرس IP} &= \text{آدرس MAC منبع MAC FF-FF-FF-FF-FF-FF.} \end{aligned}$$

دریافتی یک ARP فریم اترنت را از طریق هر دو رابط خود پخش می کند زیرا آدرس مقصد فریم S1 (ج) سوئیچ در رابط اتصال به زیر شبکه 1 متصل S1 در زیر شبکه 1 قرار دارد که به A آدرس پخش است. و یاد می گیرد که است.

این بسته پرس و جو را به تمام رابط های خود S2 را دریافت می کند و ARP نیز این پیام درخواست S2 بله، روتر پخش می کند.

ارسال نمی کند، زیرا این آدرس را می توان از پیام A MAC را برای درخواست آدرس ARP پیام پرس و جو B بدهست آورده A پرس و جو.

در جدول ارسال خود اضافه می B را دریافت کرد، یک ورودی برای میزبان B پیام پاسخ S1 هنگامی که سوئیچ در یک B و A (یعنی) است B در همان رابط میزبان A کند و سپس فریم دریافتی را راه رها می کند زیرا میزبان مقصد هستند. بخش LAN شبکه.

مشکل 17 برای 51200 بیت زمان صیر کنید. برای 10 مگابیت در ثانیه، این انتظار است

$$\frac{10 \times 10^3 \text{ بیت}}{2.51 \text{ ثانیه}} = 12.5 \text{ msec}$$

برای 100 مگابیت در ثانیه، انتظار 512 میکرو ثانیه است.

ارسال A در 0 مسئله 18

شروع به ارسال می کند، که زمان درست قبل $t=324$ در زمان B ، ارسال را تمام می کند. در پنطین حالت $A = \bar{t} = 576$ ، می رسد. زیرا $649 < 576$ ب ه اولین بیت B از زمان B به A می کند. بنابراین $t=324+325=649$ است. در زمان B به A از رسیدن اولین بیت قاب به اشتباہ فکر می کند که فریم A ارسال کرده است، ارسال را تمام می کند. بنابراین B قبل از اینکه تشخیص دهد که آن بدون برخورد با موفقیت منتقل شده است.

مسئله 19

زمان، تی	رویداد
0	انتقال را آغاز می کنند و A
245	برخورد را تشخیص می دهند و A
293	ارسال سیگنال جم را به پایان می رسانند و A
$293+245 = 538$	یک کانال بیکار را A. می رسد A به B آخرین بیت
$538+96=634$	شروع به ارسال می کند A تشخیص می دهد که
$293+512 = 805$	باید کانال بیکار را برای B به مرحله 2 برمی گردد B 96 بیت بار قبل از ارسال حس کند
$634+245=879$	می رسد B به A انتقال

می رسد، در حالی که B به $(96+805) = 901$ قبل از زمان ارسال مجدد برنامه ریزی شده A از آنجایی که ارسال مجدد با هم برخورد نمی کنند. بنابراین فاکتور 512 و A از ارسال خودداری می کند. بنابراین B ، ارسال مجدد می کند A که در الگوریتم عقب نشینی نهایی ظاهر می شود به اندازه کافی بزرگ است.

یک متغیر تصادفی باشد که تعداد اسلات ها را تا زمان 7 مسئله 20 (الف) فرض کنید
موفقیت نشان می دهد:

$$\text{Y}_{\text{P}} = \beta^{1-\text{b}}, \quad \text{احتمال موفقیت است } \beta \text{ که در آن.}$$

این یک توزیع هندسی است که دارای میانگین است $b/1$ تعداد متوالی.
که 1- 7 یکس اسلات هدر رفته است

$$\text{بله} = \frac{1}{b-1} [1 - \text{Np}^{-1}] \quad [\text{ماشین ایکس}$$

$$\text{بله} = \text{Np}^{-1} - \text{Np}^{-1}$$

ن-1 ن-1

$$= kk : \pm ایکس - ک - p Np p Np$$

ن - ۱
ر - ۱

(ب)

β است که معادل به حداقل رساندن X به حداکثر رساندن کارایی معادل به حداقل رساندن $p = 1$ در حداکثر شده است β است. ما از متن می دانیم که ن

(ج)

$$\text{بھرہ وری} = \frac{(1 - 1)^n}{(1 - 1)^n}$$

$$\infty \rightarrow N \text{ راندمان لیم} = \frac{k}{\frac{1}{k+1}} = k - 1$$

۵) به وضوح $\lim_{k \rightarrow \infty} e^{kx} = 1$ نزدیک می شود.

21 مسئلہ

		سی	E
ا	111.111.111.001 00-00-00-00-00-00	122.222.222.001 44-44-44-44-44-44	133.333.333.001 77-77-77-77-77-77
LAN	روتر 1	LAN	روتر 2
	111.111.111.002 22- 22-22-22-22-22-22	122.222.222.002 33- 33-33-33-33-33-33	122.222.222.003 55-55-55-55-55
ب	111.111.111.003 11-11-11-11-11-11	D	122.222.222.004 66-66-66-66-66
			اف
			133.333.333.003 99-99-99-99-99-99

i) منبع: MAC 00-00-00-00-00-00 به سمت چپ: آدرس A از روتر

منبع: IP آدرس مک مقصد: 22-22-22-22-22-22

111.111.111.001

مقصد: IP 133.333.333.003

ii) منبع: MAC 33-33-33-33-33-33 از روتر چپ به روتر راست: آدرس

منبع: IP آدرس مک مقصد: 55-55-55-55-55-55

111.111.111.001

مقصد: IP 133.333.333.003

iii) منبع: MAC 88-88-88-88-88-88 آدرس F: از روتر سمت راست به

منبع: IP آدرس مک مقصد: 99-99-99-99-99-99

111.111.111.001

مقصد: IP 133.333.333.003

مسئله 22

i) منبع: MAC 00-00-00-00-00-00 به سوئیچ: آدرس A از

منبع: IP آدرس مک مقصد: 55-55-55-55-55-55

111.111.111.001

مقصد: IP 133.333.333.003

ii) منبع: MAC: 00-00-00-00-00-00 از سوئیچ به روتر راست: آدرس منبع

منبع: IP آدرس مک مقصد: 55-55-55-55-55-55

111.111.111.001

مقصد: IP 133.333.333.003

iii) منبع: MAC 88-88-88-88-88-88 آدرس F: از روتر سمت راست به

منبع: IP آدرس مک مقصد: 99-99-99-99-99-99

111.111.111.001

مقصد: IP 133.333.333.003

مسئله 23

اگر تمام گرههای $2+9=11$ داده‌ها را با حداقل سرعت ممکن 100 مگابیت در ثانیه ارسال کنند، مجموع توان عملیاتی این 1100 مگابیت در ثانیه امکان‌پذیر است.

مسئله 24

هر هاب دیارتمان یک دامنه برخورد منفرد است که می‌تواند حداقل 100 مگابیت بر ثانیه داشته باشد. پیوندهایی که سرور وب و سرور پست الکترونیکی را به هم متصل می‌کنند دارای حداقل هستند

توان عملیاتی 100 مگابیت بر ثانیه از این رو، اگر سه حوزه برخورد و وب سرور و سرور پست، داده‌ها را با حداقل سرعت ممکن 100 مگابیت در ثانیه ارسال کند، حداقل توان مجموع 500 مگابیت در ثانیه در میان 11 سیستم پایانی حاصل می‌شود.

مسئله 25

همه 11 سیستم پایانی در یک حوزه برخورد قرار خواهد گرفت. در این حالت، حداقل توان کل مجموع 100 مگابیت در ثانیه در میان 11 سیستم پایانی امکان پذیر است.

مسئله 26

عمل	وضعیت جدول را تغییر دهید	بسته پیوند(های) ارسال شده به A، C، D، E و F	توضیح است
E قاب به	رابط باد می‌گیرد تعویض آ می‌فرستد	از آنجایی که جدول سوئیچ خالی است، پس تغییر دهید رابط کاربری را نمی‌شناسد	
B با یک فریم به E	رابط باد می‌گیرد تعویض MAC B مربوط به آدرس پاسخ می‌دهد	متناظر به آدرس مک	
A می‌فرستد	رابط باد می‌گیرد تعویض MAC E مربوط به آدرس پاسخ می‌دهد	از آنجایی که سوئیچ از قبل رابط کاربری را می‌شناسد	
B قاب به	رابط باد می‌گیرد تعویض آ می‌فرستد	متناظر به آدرس MAC B	
A با یک فریم به B	آ حالت جدول مانند یکسان را باقی بگذارد	از آنجایی که سوئیچ از قبل رابط مربوط به آن را می‌داد	
	قبل از	آدرس MAC B	
		از آنجایی که سوئیچ از قبل رابط مربوط به آن را می‌داد	
		آدرس A	

مسئله 27

(الف) زمان لازم برای پر کردن بیت است لیتر 8:

$$12 \times 8 \text{ میلی لیتر} = 96 \text{ میلی لیتر}$$

تاخیر بسته بندی است L=500، 1=L ب) برای

$$\frac{16}{1500} \text{ ثانیه} = 75.93 \text{ متر}^2$$

تاخیر بسته بندی است $L = 50$ برای

$$\frac{16}{50} \text{ ثانیه} = 125.3 \text{ متر}$$

$$\text{ج) تاخیر ذخیره و ارسال} \quad \cdot = \frac{8}{+} \frac{40}{\text{آر}}$$

تاخیر است، $L = 500$ برای

$$\frac{622}{1500} \times +3 \approx \frac{4.19}{\text{ثانیه}} \text{ ثانیه}$$

$$\text{تاخیر ذخیره و ارسال} \quad L = 50 \text{ برای} \quad \text{ثانیه} \quad \text{متر}^1.$$

د) تاخیر ذخیره و ارسال برای هر دو مورد برای سرعت های معمول پیوند کوچک است. با این حال، تاخیر برای برنامه های صوتی بلادرنگ بسیار زیاد است $L =$ بسته بندی برای 1500.

مسئله 28

عبارة عن: IP آدرس های 111.111.1.1، 111.111.1.2، 111.111.1.3، 111.111.1.4 برای آن سه کامپیوتر (از چپ به راست) در بخش IP 111.111.1/24 ماسک زیر شبکه 111.111.1.3 است.

عبارة عن: IP آدرس های 111.111.2.1، 111.111.2.2، 111.111.2.3، 111.111.2.4 برای آن سه کامپیوتر (از چپ به راست) در بخش IP 111.111.2/24 ماسک زیر شبکه 111.111.2.3 است.

IP کارت رابط روتر که به پورت 1 متصل می شود را می توان به گونه ای پیکربندی کرد که حاوی دو آدرس و مورد دوم برای VLAN 11 زیرمجموعه باشد: 111.111.1.0 و 111.111.2.0. اولین مورد برای زیرشبکه بخش 11 مرتب است. فرض کنید 0.0.1.1 با MAC 111.111.1.0 در بخش IP با یک شناسه IP است. هر آدرس VLAN 11 زیرشبکه با 111.111.2.0 و 111.111.1.24 VLAN 12 باشد. این بدان معناست که هر فریمی که از زیر شبکه 111.111.2.0 و 111.111.2.1 به هر فریمی که از 111.111.2/24 باشد باید تگ 802.1 باشد. این تگ با MAC 111.111.2.1 و VLAN ID 11 و پیکربندی 802.1 باشد. اضافه می شود و به هر فریم که از 111.111.2/24 باشد تگ 802.1 باشد. این تگ با MAC 111.111.2.2 و VLAN ID 12 باشد.

B را برای میزبان IP 111.111.1.1 می خواهد یک دیتابرام IP 111.111.1.2 را در یک فریم با مقصد IP 111.111.2.1 (A) ایندا دیتابرام A ارسال کند. میزبان CS در بخش MAC 111.111.2.1 (B) کارت رابط روتر که به پورت 1 سوئیچ متصل می شود، کپسوله می MAC مقصود برابر با آدرس MAC باید از IP منتقل می کند، که تصمیم می گیرد دیتابرام IP کند. هنگامی که روتر فریم را دریافت کرد، سیس ان را به لایه را در یک فریم IP طریق زیرشاخه 111.111.2.0 به زیر شبکه 111.111.2/24 ارسال شود. سپس روتر دیتابرام با برچسب VLAN 12 کپسوله می کند و آن را به پورت 1 می فرستد. توجه داشته باشید که این فریم دارای یک برچسب تعیین شده است. هنگامی که سوئیچ پورت فریم 1 را دریافت کرد، می داند که این فریم به 802.1q می شود، بنابراین سوئیچ قابل را ارسال می کند.

را حذف می کند q این فریم را دریافت کرد، نگاهی به میزبان CS که در بخش B به میزبان

مسئله 29

30 مسئلہ

31 مسئلہ

(توضیح زیر کوتاه است، اما شامل تمام مراحل کلیدی اصلی و پرتوکل‌های کلیدی درگیر است)

ویژه به IP استفاده می کند. کامپیوتر شما ابتدایاً یک دیتاگرام IP برای بدست آوردن آدرس DHCP کامپیوتر شما ابتدایاً از ایجاد می کند و آن را در یک فریم اترنت قرار داده و در DHCP مقصد 255.255.255.255 در مرحله کشف سرور را با زمان اجاره معین IP رایانه شما می تواند یک آدرس، DHCP اترنت پخش می کند. سپس با پیروی از مراحل پروتکل در یافته کند.

روت‌های اولین هاب، زیر شبکه‌هایی که رایانه IP در اترنت همچنین لیستی از آدرس‌های DHCP یک سرور محلی (در صورت وجود) به رایانه شما می‌دهد DNS شما در آن قرار دارد و آدرس‌های سرورهای

برای دریافت آدرس های ARP رایانه شما در ابتدا خالی است، رایانه شما از پروتکل ARP از آنجایی که حافظه پنهان محلی استفاده می کند DNS روتر اولین های و سرور MAC

IP محلی آدرس DNS صفحه و ب را که می خواهد دانلود کنید دریافت می کند. اگر سرور IP کامپیوتر شما ابتداء ادرس IP برای یافتن آدرس DNS را نداشته باشد، کامپیوتر شما از پروتکل

صفحه وب را داشته باشد، در صورتی که صفحه وب در یک وب سرور محلی نباشد، IP هنگامی که رایانه شما ادرس را از طریق روتر اولین هاب ارسال می کند. این **HTTP** درخواست

محصور IP می شود و سپس بیشتر در بسته های HTTP قطعه بندی و در بسته های TCP پیام درخواست می شود و در نهایت در فریم های اترنت محصور می شود. رایانه شما فریم های اترنت را به روتر اول پرتاب ارسال می کند، جدول مسیریابی خود را بررسی IP می فرست. هنگامی که روتر فریم ها را دریافت کرد، آنها را به لایه می کند و سپس بسته ها را به واسطه مناسب از تمام رابط های خود می فرستد.

شما تا زمانی که به وب سرور برسند از طریق اینترنت هدایت می شوند IP سپس بسته های

به رایانه شما ارسال می کند. این پیامها در HTTP سرور میزبان صفحه وب، صفحه وب را از طریق پیام های پاسخ را دنبال می کنند و در IP مسیر های IP کپسوله می شوند. این بسته های IP و سپس بیشتر در بسته های TCP بسته های را با کپسوله کردن آنها در فریم های اترنت به IP نهایت به روتر اولین هاپ شما می رساند و سپس روتر آن بسته های را به لایه شما ارسال می کند.

مسئله 32

(الف) هر جریان به طور مساوی ظرفیت یک پیوند را با جریان های دیگری که از آن پیوند عبور می کنند به اشتراک می به لینک های دسترسی روتر 10 گیگابیت بر ثانیه (و همچنین مسیریاب دسترسی B گذارد، سپس 80 جریان عبوری از به پیوندهای روتر مرزی) هر کدام تنها 10 گیگابیت بر ثانیه / 80 را دریافت خواهد کرد. = 125 مگابیت بر ثانیه

(ب) در توپولوژی شکل 5.31، چهار مسیر مجزا بین سوئیچ های ردیف اول و سوم وجود دارد که با هم 40 گیگابیت در ثانیه برای ترافیک از رک های 4-1 به رک های 9-12 ارائه می کنند. به طور مشابه، چهار پیوند بین سوئیچ های ردیف دوم و چهارم وجود دارد که با هم 40 گیگابیت در ثانیه برای ترافیک از رک های 5-8 تا 13-16 فراهم می کنند. بنابراین کل پهنای باند کل 80 گیگابیت در ثانیه و مقدار هر نرخ جریان 1 گیگابیت در ثانیه است.

به اشتراک بگذارند. بنابراین TOR (ج) اکنون 20 جریان باید هر 1 گیگابیت بر ثانیه پهنای باند را بین جفت سوئیچ های نرخ بیت میزبان به میزبان 0.5 گیگابیت بر ثانیه خواهد بود.

مشکل 33 (الف) هم برنامه ایمیل و هم برنامه ویدیویی 0.1 درصد موقع از رک چهارم استفاده می کنند.

(ب) احتمال اینکه هر دو برنامه به رک چهارم نیاز دارند $0.001 * 0.001 = 0.001^2 = 6-10^{-6}$ است.

(ج) فرض کنید سه رک اول برای ویدیو، رک بعدی یک رک مشترک برای ویدیو و ایمیل و سه رک بعدی برای ایمیل است. باید فرض کنیم که رک چهارم تمام داده ها و نرم افزار های مورد نیاز برای برنامه های ایمیل و ویدئو را دارد. با توپولوژی شکل 5.31، تا زمانی که هر دو به طور همزمان از رک چهارم استفاده نکنند، هر دو برنامه هر دو از رک چهارم برای بیش از 0.000001٪ زمان، b از پهنای باند کافی برخوردار خواهند بود. از قسمت استفاده نمی کنند، که در محدوده 0.0001٪ نیاز است.

فصل 6 سوالات مروری

در حالت عملیات زیرساخت، هر میزبان بی سیم از طریق یک ایستگاه پایه (نقطه دسترسی) به شبکه بزرگتر 1. عمل می کند. در حالت ad-hoc متصل می شود. اگر در حالت زیرساخت کار نمی کند، یک شبکه در حالت هاست های بی سیم هیچ زیرساختی برای اتصال ندارد. در غایب چنین زیرساختی، خود هاست ها باید خدماتی، hoc و غیره را ارائه دهند DNS مانند مسیریابی، تخصیص آدرس، ترجمه نام شبیه به

- الف) تک هاپ، مبتنی بر زیرساخت (b) تک هاپ، بدون زیرساخت (ج) چند هاپ، مبتنی بر زیرساخت (d) چند هاپ، بدون زیرساخت

از دست دادن مسیر به دلیل تضییف سیگنال الکترومغناطیسی در هنگام عبور از ماده است. انتشار چند مسیری 3. منجر به تار شدن سیگنال دریافتی در گیرنده می شود و زمانی اتفاق می افتد که بخش هایی از موج الکترومغناطیسی از اجسام و زمین منعکس می شود و مسیر هایی با طول های مختلف بین فرستنده و گیرنده طی می کند. تداخل منابع دیگر زمانی رخ می دهد که منع دیگر نیز در همان محدوده فرکانسی شبکه بی سیم ارسال می کند.

- الف) افزایش توان انتقال (b) کاهش سرعت انتقال 4.

از طریق یکی از 11 کanal منتقل می شود. قاب‌های AP ها فریم های بیکن را انتقال می دهند. فریم های بیکن یک AP را کشف و شناسایی کنند AP چراغ به ایستگاه‌های بی سیم اطراف اجازه می دهند تا

نادرست. 6.

از طریق یکی از 11 کanal منتقل می شود. قاب‌های AP ها فریم های بیکن را انتقال می دهند. فریم های بیکن یک AP را کشف و شناسایی کنند AP چراغ به ایستگاه‌های بی سیم اطراف اجازه می دهند تا

نادرست. 8.

تنها زمانی استفاده می RTS/CTS را تنظیم کند به طوری که دنباله RTS هر ایستگاه بی سیم می تواند یک آستانه 9. RTS/CTS شود که قاب داده ای که قرار است ارسال شود طولانی تر از آستانه باشد. این تضمین می کند که مکانیسم فقط برای فریم های بزرگ استفاده می شود.

نه، هیچ مزیتی وجود نخواهد داشت. فرض کنید دو ایستگاه وجود دارد که می خواهند همزمان ارسال کنند و هر 10. طولانی باشد، کanal تا زمانی که برای DATA به اندازه یک فریم RTS استفاده می کنند. اگر فریم RTS/CTS در حال برخورد تلف شده است، تلف می شود. بنابراین، تبادل DATA دو فریم RTS/CTS تنها زمانی مفید است که RTS/CTS به طور قابل توجهی کوچکتر از فریم های داده باشند

قبلی مرتبه می کند. هنگامی که AP در ابتدا سوئیچ یک ورودی در جدول ارسال دارد که ایستگاه بی سیم را با 11. ایستگاه بی سیم ایجاد می کند و MAC جدید یک فریم با آدرس AP، جدید مرتبه می شود AP ایستگاه بی سیم با فریم را پخش می کند. فریم توسط سوئیچ دریافت می شود. این سوئیچ را مجبور می کند تا جدول ارسال خود را به جدید ارسال می شوند AP روز کند، به طوری که فریم های مقصود به ایستگاه بی سیم از طریق

هر گره بلوتوث معمولی می تواند یک گره اصلی باشد در حالی که نقاط دسترسی در شبکه های 12. 802.11 دستگاه های خاصی هستند (دستگاه های بی سیم معمولی مانند لپ تاپ های نمی توانند به عنوان نقاط دسترسی استفاده شوند)

13.
نادرست

زمان بندی فرصت طلب" به تطبیق پروتکل لایه فیزیکی با شرایط کانال بین فرستنده و گیرنده و انتخاب گیرنده" 14. هایی که بسته ها برای آنها ارسال می شود بر اساس شرایط کانال اشاره دارد. این به ایستگاه پایه اجازه می دهد تا بهترین استفاده را از رسانه بی سیم داشته باشد.

15. UMTS و CDMA-2000 و IS-95.

خیر. یک گره می تواند در طول اتصال خود به اینترنت به همان نقطه دسترسی متصل باقی بماند (بنابراین، سیار 16. نباشد). گره سیار گری است که در طول زمان نقطه اتصال خود را به شبکه تغییر می دهد. از آنجایی که کاربر همیشه از طریق یک نقطه دسترسی به اینترنت دسترسی دارد، موبایل نیست

آن است که در شبکه خانگی خود باشد. یک آدرس دائمی برای یک گره موبایل آدرس 17. توسط عامل خارجی (که می تواند COA) همان آدرسی است که هنگام بازدید از یک شبکه خارجی دریافت می کند مسیریاب لبه در شبکه خارجی یا خود گره موبایل باشد) تعیین می شود.

18.
نادرست

را نگهداری می کند که شامل (HLR) یک پایگاه داده به نام ثبت موقعیت مکانی GSM شبکه خانگی در 19. همچنین HLR. شماره تلفن همراه دائمی و اطلاعات مشخصات مشترکین در مورد هر یک از مشترکین خود است حاوی اطلاعاتی در مورد مکان فعلی این مشترکین است. شبکه بازدید شده یک پایگاه داده به نام ثبت مکان دارد که حاوی ورودی برای هر کاربر تلفن همراه است که در حال حاضر در بخشی از شبکه (VLR) بازدیدکننده با ورود و خروج کاربران موبایل به شبکه می آیند VLR ارائه می شود. بنابراین ورودی های VLR است که توسط و می روند.

در VLR و روتر لبه در شبکه خارجی مشابه GSM در HLR موبایل مشابه IP روتر لبه در شبکه خانگی در GSM است.

ی است که تلفن همراه هنگام شروع تماس برای اولین بار از آن بازدید می کند. بنابراین 20. Anchor MSC در طول تماس بدون تغییر باقی می ماند. در طول مدت تماس و صرف نظر از تعداد انتقال های بین MSC لنگر به MSC خانگی به MSC که توسط موبایل انجام می شود، تماس از بازدید شده که در آن تلفن همراه در حال حاضر قرار دارد هدایت می شود.

از TCP (الف) (بازیابی محلی (ب) آگاهی فرستنده 21. پیوندهای بی سیم (ج) رویکردهای اتصال تقسیم

فصل 6 مسائل

مشکل 1

$$\text{خروجی} = d_1 = [-1, 1, -1, 1, -1, 1, -1, 1] \\ \text{مربوط به بیت } 0 = [1, -1, 1, -1, 1, -1, 1, -1]$$

مشکل 2

$$[1, 1, 1, -1, 1, 1, 1, 1, -1] ; [1, 1, 1, -1, 1, 1, 1, 1, -1] = 2$$

مشکل 3

$$1 \times \underset{8}{= 2 + (-1 \times 1)} + 1 \times 1 + 1 \times 1 + 1 \times 1 + (-1 \times 1) + 1 \times 1 + 1 \times 1 = 1 \\ 1 \times \underset{8}{= 2 + (-1 \times 1)} + 1 \times 1 + 1 \times 1 + 1 \times 1 + (-1 \times 1) + 1 \times 1 + 1 \times 1 = 1$$

مشکل 4

$$\begin{array}{l} \text{کانال 1:} (1, -1, 1, 1, 1, 1, 1, 1) \\ \text{کانال 2:} (1, 1, 1, 1, 1, 1, 1, -1) \end{array}$$

مشکل 5

متفاوتی خواهد بود. ایستگاه بی سیمی که به کافه می رسد با یکی MAC و آدرس SSID معمولاً دارای AP (الف) دو وجود AP مرتبط می شود. پس از ارتباط، یک پیوند مجازی بین ایستگاه جدید و (ها AP یعنی یکی از) ها SSID از مرتبط است. هنگامی که ایستگاه AP1 برچسب گذاری کنید. فرض کنید ایستگاه جدید با AP2 و AP1 ها را AP دارد. نیز فریم را دریافت می کند، اما آدرس AP2 داده می شود. اگرچه AP1 جدید یک فریم می فرستد، به می تواند به صورت موازی در یک کانال ISP پردازش نمی کند زیرا فریم به آن آدرس داده نمی شود. بنابراین، دو از پنهانی باند بی سیم یکسانی استفاده خواهد کرد. اگر ایستگاه های بی سیم در متفات AP کار کنند. با این حال، دو است

حداکثر نرخ انتقال کل برای دو b ها همزمان ارسال می کنند، یک برخورد وجود خواهد داشت. برای ISP 802.11 مگابیت در ثانیه است.

های مختلف (و در نتیجه کانال های مختلف) به طور همزمان ارسال کنند، حال اگر دو ایستگاه بی سیم در ISP 22 Mbps 802.11 برخوردی وجود نخواهد داشت. بنابراین، حداکثر نرخ انتقال کل برای دو است.

مشکل 6

را MP3 باشد که AP ممکن است یک H1). دارای 1000 فریم بلند برای ارسال است H1 فرض کنید ایستگاه بی سیم تنها ایستگاهی است که می خواهد ارسال کند، اما در H1 فرض کنید در ابتدا (به یک ایستگاه بی سیم دیگر ارسال می کند می خواهد یک فریم را ارسال کند. برای سادگی، همچنین فرض H2، حالی که در نیمه راه ارسال اولین فریم خود است H2، کنید هر ایستگاه می تواند سیگنال هر ایستگاه دیگر را بشنود (یعنی هیچ پایانه پنهانی وجود ندارد). قبل از ارسال تصادفی انتخاب می کند که کانال مشغول است، و بنابراین یک مقدار backoff احساس می کند که کانال مشغول است، و بنابراین یک مقدار

و (DIFS) به مرحله 1 برگرد. یعنی مدت کوتاهی منتظر می ماند H1، حال فرض کنید پس از ارسال اولین فریم در عقب نشینی گیر کرده و منتظر یک H2 سپس در حالی که H1 سپس شروع به ارسال فریم دوم می کند. فریم دوم فرستنی برای H2 باید تمام 1000 فریم خود را قبل از اینکه H1، کانال بیکار است، منتقل می شود. بنابراین پس از ارسال یک فریم به مرحله 2 برود، آنگاه H1 دسترسی به کانال داشته باشد، ارسال کند. از سوی دیگر، اگر می دهد. بنابراین، انصاف دلیل H2 نیز یک مقدار پسانداز تصادفی انتخاب می کند و در نتیجه شناس منصفانه ای به اصلی این انتخاب طراحی بود.

مسئله 7

مانند) یک فریم بدون داده 32 بایت طول دارد. با فرض نرخ انتقال 11 مگابیت بر ثانیه، زمان ارسال یک فریم کنترل است. زمان $23 \text{ usc} = 23 \text{ مگابیت در ثانیه} / (256 \text{ بیت})$ یک فریم CTS یا یک فریم RTS یک فریم 8256 بیت) / (11 مگابیت در ثانیه) = 751 است. مورد نیاز برای انتقال فریم داده (8256 بیت) / (11 مگابیت در ثانیه) = 751 است.

DIFS + RTS + SIFS + CTS + SIFS + FRAME + SIFS + ACK

$$= DIFS + 3SIFS + (3*23 + 751) \text{ usec} = DIFS + 3SIFS + 820 \text{ usec}$$

مسئله 8

الف) 1 پیام / 2 اسلات ب)
پیام / شکاف ج) 1 پیام /
شکاف

پیام / 2 (ii) پیام/شاخه 1 (i) د
پیام/اسلات 2 (iii) شاخه

ه) i) پیام 1: شکاف 1 Aà B، پیام 4 اسلات b) شکاف 2 Dà C
 2: شکاف Ack Bà A
 Slot 3: Ack Cà D
 = پیام / 3 اسلات 2

III)
 شکاف 1: اسلات Cà D 2: پیام Ack
 شکاف 3: Ack Aà C، پیام B 3: Ack
 تکرار
 Bà A
 = پیام / 3 اسلات 2

مسطه 10

در حال سرویس دهی A ارسال شود. این راه حل منصفانه نیست زیرا فقط A (الف) 10 مگابیت در ثانیه اگر فقط به گره است. منظور از "عادلانه" این است که به هر یک از چهار گره باید تعداد مساوی اسلات اختصاص داده شود.

(ب) برای شرط انصاف به طوری که هر گره در طول هر فریم پایین دستی مقدار مساوی داده را دریافت کند، اجازه دهد دریافت می کنند، نشان دهند D و C، B، A به ترتیب تعداد اسلات هایی را که n1، n2، n3، n4 و،

در 1 اسلات = A 10
 با فرض اینکه مدت) تر مگابیت ارسال می شوند
 بنابراین (باشد t زمان هر شکاف

= (اسلات n1 در) A مقدار کل داده ارسال شده به

است t n4 و n3 به ترتیب برابر با 5 و، C، به طور مشابه، کل داده های ارسال شده به

حال برای برآوردن شرط انصاف داده شده، شرط زیر را داریم:

$$10t n1 = 5t n2 = 2.5t n3 = t n4$$

از این رو،

$$\begin{aligned} n2 &= 2 n1 \\ n3 &= 4 n1 \\ n4 &= 10 n1 \end{aligned}$$

است. بنابراین N اکتون، تعداد کل اسلات ها

$$\begin{aligned} n_1 + n_2 + n_3 + n_4 &= N \text{ یعنی } n_1 + 2 \\ n_1 + 4n_1 + 10n_1 &= N \text{ یعنی } n_1 = \\ N/17 & \end{aligned}$$

از این رو

$$\begin{aligned} n_2 &= 2N/17 \\ n_3 &= 4N/17 \\ n_4 &= 10N/17 \end{aligned}$$

میانگین نرخ انتقال توسط:

$$\begin{aligned} (10t n_1 + 5t n_2 + 2.5t n_3 + t n_4) / tN &= (10N/17 + 5 * \\ 2N/17 + 2.5 * 4N/17 + 1 * 10N/17) / N &= 40/17 = 2.35 \\ \text{مگابیت بر ثانیه} & \end{aligned}$$

در طول فریم فرعی، داده دریافت کند. از این رو D و C ، B دو برابر گره های A (ج) اجازه دهد گره

$$\begin{aligned} 10tn_1 &= 2 * 5tn_2 = 2 * 2.5tn_3 = 2 * tn_4 \\ \text{یعنی } n_2 &= n_1 \\ n_3 &= 2n_1 \\ n_4 &= 5n_1 \end{aligned}$$

از نو

$$\begin{aligned} n_1 + n_2 + n_3 + n_4 &= N \\ n_1 + n_1 + 2n_1 + 5n_1 &= N \\ \text{یعنی } n_1 &= N/9 \end{aligned}$$

در حال حاضر، میانگین نرخ انتقال داده شده توسط

$$\begin{aligned} (10t n_1 + 5t n_2 + 2.5t n_3 + t n_4) / tN & \\ = 25/9 &= 2.78 \text{ مگابیت بر ثانیه} \end{aligned}$$

دو برابر بیشتر از هر گره دیگر داده دریافت می کنند، مقادیر D یا C ، B به طور مشابه، با در نظر گرفتن گره های متفاوتی برای میانگین نرخ انتقال می توان محاسبه کرد.

مسنثه 11

الف) خیر. همه روترها ممکن است نتوانند فوراً دیناگرام را مسیریابی کنند. این به این دلیل است که الگوریتم غیر مرکز است و مدتی طول می کشد تا پایان (BGP مانند AS و همچنین پروتکل های مسیریابی بین) یابد. بنابراین، در طول زمانی که الگوریتم همچنان در نتیجه تبلیغات شکه خارجی جدید اجرا می شود، برخی از روترها ممکن است نتوانند دیناگرام های مقصود به گره موبایل را مسیریابی کنند.

ب) بله. این ممکن است زمانی اتفاق بیفتد که یکی از گره ها به تازگی یک شبکه خارجی را ترک کرده و به یک شبکه خارجی جدید ملحق شده باشد. در این شرایط، ورودی های مسیریابی از شبکه خارجی قدیمی ممکن است به طور کامل حذف نشده باشند، زمانی که ورودی های شبکه جدید منتشر می شوند.

ج) مدت زمانی که طول می کشد تا یک مسیریاب مسیری به گره موبایل را بیاموزد به تعداد پرسش های بین روتر و روتر لبه شبکه خارجی برای گره بستگی دارد.

مسئله 12

اگر خبرنگار متحرک باشد، آنگاه هر دیتابرام مقصد برای خبرنگار باید از طریق عامل خانه خبرنگار عبور کند. عامل شبکه‌ای که بازدید می‌شود نیز باید درگیر شود، زیرا این عامل خارجی است که به عامل اصلی خبرنگار از مکان خبرنگار اطلاع می‌دهد. دیتابرام‌های دریافت شده توسط عامل اصلی خبرنگار باید بین نماینده داخلی و عامل خارجی کپسوله/تونل شوند (مانند مورد نمودار مخصوص شده در بالای شکل 6.23).

مسئله 13

از آنجایی که دیتابرام‌ها ابتدا باید به نماینده خانگی و از آنجا به موبایل ارسال شوند، تاخیرها معمولاً بیشتر از مسیریابی مستقیم خواهند بود. توجه داشته باشید که ممکن است با این حال، تاخیر مستقیم از خبرنگار به تلفن همراه (به عنوان مثال، اگر دیتابرام از طریق عامل اصلی مسیریابی نشود) در واقع می‌تواند کوچکتر از مجموع تاخیر باشد.

از خبرنگار به عامل خانه و از آنجا به موبایل. این بستگی به تأخیر در این بخش های مختلف مسیر دارد. توجه داشته باشید که مسیریابی غیرمستقیم همچنین یک تأخیر در پردازش عامل خانگی (به عنوان مثال، کپسولاسیون) اضافه می کند.

مسئله 14

ابتدا منذکر می شویم که زنجیره سازی در پایان بخش 6.5 مورد بحث قرار گرفت. در مورد زنجیره زدن با استفاده از مسیریابی غیرمستقیم از طریق یک عامل خانگی، رویدادهای زیر رخ می دهد

- است و A به عامل خانه اطلاع می دهد که تلفن همراه اکنون در حال بازدید از A، می رسد A گرہ موبایل به ارسال شوند A در (COA) دیتاگرام های تلفن همراه باید اکنون به آدرس مراقبتی مشخص شده.

- اطلاع دهد که تلفن همراه A باید به نماینده خارجی در B منتقل می شود. عامل خارجی در B گرہ متحرک به را دارد. از آن زمان به B مشخص شده در COA ساکن است و B ساکن نیست اما در واقع در A دیگر در بعد، نماینده خارجی در وصیت نامه نشان داده می شود B موبایل در COA به A موبایل در COA دیتاگرام های ارسالی دریافت می کند که آدرس

- اطلاع دهد که B باید به نماینده خارجی در C حرکت می کند. عامل خارجی در C گرہ متحرک به سمت را دارد. از C مشخص شده در COA ساکن است و C ساکن نیست اما در واقع در B تلفن همراه دیگر در که به (A از عامل خارجی در) دیتاگرام های را که دریافت می کند آن زمان به بعد، عامل خارجی در ارسال می کند C تلفن همراه در COA آدرس داده شده است به B موبایل در COA.

توجه داشته باشید که وقتی تلفن همراه آفلاین می شود (بعنی آدرسی ندارد) یا به شبکه اصلی خود باز می گردد، حفظ می شود باید حذف شود. این تحریب نیز باید از C و B، وضعیت ارسال دیتاگرام که توسط عوامل خارجی در مطلع نیست و A طریق پیام های سیگنالینگ انجام شود. توجه داشته باشید که نماینده خانه از تحرک موبایل فراتر از خبرنگار اصلاً از تحرک موبایل مطلع نیست.

بر صورت عدم استفاده از زنجیر، اتفاقات زیر رخ می دهد

- است و A به عامل خانه اطلاع می دهد که تلفن همراه اکنون در حال بازدید از A، می رسد A گرہ موبایل به ارسال شوند A در (COA) دیتاگرام های تلفن همراه باید اکنون به آدرس مراقبتی مشخص شده.

- و نماینده داخلی اطلاع A باید به نماینده خارجی در B منتقل می شود. عامل خارجی در B گرہ متحرک به را B مشخص شده در COA ساکن است و B ساکن نیست اما در واقع در A دهد که تلفن همراه دیگر در A می تواند وضعیت آن را در مورد تلفن همراه حذف کند، زیرا دیگر در A دارد. عامل خارجی در B تلفن همراه در COA نیست. از آن زمان به بعد، عامل اصلی دیتاگرام های را که دریافت می کند به ارسال می کند.

- و نماینده داخلی اطلاع B باید به نماینده خارجی در C منتقل می شود. عامل خارجی در C گرہ متحرک به را C مشخص شده در COA ساکن است و C ساکن نیست اما در واقع در B دهد که تلفن همراه دیگر در نیست. B می تواند وضعیت آن را در مورد تلفن همراه حذف کند، زیرا دیگر در B دارد. نماینده خارجی در ارسال می کند C تلفن همراه در COA از آن به بعد، عامل اصلی دیتاگرام های را که دریافت می کند به

هنگامی که تلفن همراه آفلاین می شود یا به شبکه اصلی خود باز می گردد، وضعیت ارسال دیتاگرام که توسط عامل حفظ می شود باید حذف شود. این تحریب نیز باید باشد C خارجی در

از طریق پیام های سیگنالینگ انجام می شود. توجه داشته باشید که نماینده خانگی همیشه از شبکه خارجی فعلی موبایل مطلع است. با این حال، خبرنگار هنوز به طرز سعادتمندی از تحرک تلفن همراه بی خبر است.

مسئله 15

دو تلفن همراه مطمئناً می توانند در یک شبکه بازدید شده یکسان آدرس مراقبتی داشته باشند. در واقع، اگر مراقبت از آدرس، نشانی عامل خارجی باشد، این نشانی همان خواهد بود. هنگامی که عامل خارجی دیتاگرام تونل شده را کپسوله می کند و آدرس موبایل را تعیین می کند، باید از آدرس های جدایگانه برای ارسال دیتاگرامها به طور جدایگانه به مقصد های مختلف (موبایل) در شبکه بازدید شده استفاده شود.

مسئله 16

(۴) به روز شود HLR باید در MSRN تغییر کرد، مقدار MSRN ارائه شود، هر زمان که HLR به MSRN اگر این است که HLR در MSRN مزیت داشتن. (دارد MSRN عنوان مثل، زمانی که انتقالی وجود دارد که نیاز به تغییر نیازی به MSRN به جای VLR ارائه کرد. با ارائه آدرس VLR مقدار را می توان به سرعت و بدون پرس و جو در نیست HLR در MSRN تازه کردن.

فصل 7 سوالات مروری

1.

نرخ بیت	بایت ها در 67 دقیقه منتقل شدند
فیس بوک فرانک	کلوبیت بر ثانیه 40
مارتا موزیک	کلوبیت بر ثانیه 200
ویکتور ویدئو	مگابایت بر ثانیه 4

مگابایت 20

مگابایت 100

گیگ 2

افزونگی فضایی: افزونگی در یک تصویر داده شده است. به طور شهودی، تصویری که عمدتاً از فضای سفید تشکیل شده است، دارای درجه بالایی از افزونگی است و می‌تواند به طور موثر فشرده شود، بدون اینکه کیفیت تصویر به میزان قابل توجهی کاهش یابد.

افزونگی زمانی نشان دهنده تکرار از تصویر به تصویر بعدی است. برای مثال، اگر یک تصویر و تصویر بعدی دقیقاً یکسان باشند، دلیلی برای رمزگذاری مجدد تصویر بعدی وجود ندارد. در عوض نشان دادن این که تصویر بعدی دقیقاً یکسان است، در هنگام رمزگذاری کارآمدتر است. اگر دو تصویر بسیار شبیه به هم باشند، ممکن است نشان دادن تفاوت تصویر اول به جای رمزگذاری مجدد تصویر دوم کارآمد نباشد.

کمی کردن یک نمونه به معنای 1024 سطح به معنای 10 بیت در هر نمونه است. نرخ حاصل از سیکال صوتی دیجیتال. کلوبیت بر ثانیه است 160 PCM.

پخش جریانی صوتی/تصویری ذخیره شده: در این دسته از برنامه ها، رسانه زیربنایی ویدئویی از پیش ضبط شده است، مانند یک فیلم، یک نمایش تلویزیونی، یا یک رویداد ورزشی از پیش ضبط شده. این ویدیوهای از پیش ضبط شده روی سرورها پخش می‌شوند و کاربران در خواست هایی را برای مشاهده ویدیوها در صورت تقاضا به سرورها ارسال می‌کنند. امروزه بسیاری از شرکت های اینترنتی ویدئوهای پخش جریانی را ارائه می‌کنند، از جمله YouTube، Netflix و Hulu.

صدای مکالمه بی‌درنگ از طریق اینترنت اغلب به عنوان تلفن اینترنتی: IP مکالمه صوتی و تصویری از طریق Voice-over-IP (VoIP) شناخته می‌شود، زیرا از بی‌دیگاه کاربر، شبیه به سرویس تلفن سنتی سوئیچ مدار است. معمولاً به آن نیز گفته می‌شود. ویدیوی مکالمه مشابه است با این تفاوت که شامل ویدیوی شرکت کننگان (VOIP) و همچنین صدای آنها می‌شود. صدا و تصویر مکالمه امروزه به طور گسترده در اینترنت استفاده می‌شود، روزانه صدها میلیون کاربر دارند Skype و Google Talk و Google Hangouts شرکت های اینترنتی مانند

پخش زنده صدا و تصویر: این برنامه ها به کاربران اجازه می‌دهند که از طریق اینترنت یک انتقال زنده رادیویی یا تلویزیونی دریافت کنند. امروزه هزاران ایستگاه رادیویی و تلویزیونی در سراسر جهان در حال پخش محتوا از طریق اینترنت هستند.

سرور ویدئو را با نرخی که با نرخ مصرف ویدئو مشتری مطابقت، UDP با پخش جریانی: UDP 5 با یک نرخ ثابت، انتقال می‌دهد UDP دارد، با کلاک کردن تکه های ویدئو بر روی

به عنوان فایل معمولی با یک HTTP ویدیو به سادگی در سرور، HTTP در جریان: HTTP خاص ذخیره می‌شود. وقتی کاربر می‌خواهد ویدیو را ببیند، مشتری URL

صادر می کند. سپس URL برای آن HTTP GET با سرور برقرار می کند و یک درخواست TCP یک اتصال در سریع ترین زمان ممکن ارسال می کند، یعنی به همان HTTP سرور فایل ویدئویی را در یک پیام پاسخ و کنترل جریان اجازه می دهد TCP سرعتی که کنترل تراکم.

ویدیو چندین نسخه مختلف، HTTP در جریان تطبیقی پویا از طریق (DASH) تطبیقی HTTP جریان کنگذاری می شود که هر نسخه دارای نرخ بیت متفاوت و به تبع آن سطح کیفیت متفاوتی است. کلاینت به صورت پویا تکه هایی از بخش های ویدیویی چند ثانیه ای را از نسخه های مختلف درخواست می کند. هنگامی که مقدار پنهانی باند موجود زیاد باشد، کلاینت به طور طبیعی تکه هایی را از یک نسخه با نرخ بالا انتخاب می کند و زمانی که پنهانی باند موجود کم است، طبیعتاً از یک نسخه با نرخ پایین انتخاب می کند.

6. عبارتند از UDP Streaming سه اشکال مهم:

با نرخ ثابت UDP با توجه به مقدار غیر قابل پیش بینی و متغیر پنهانی باند موجود بین سرور و کلاینت، جریان 1. برای پردازش کلاینت به RTSP، می تواند پخش مدام را ارائه ندهد. 2. به یک سرور کنترل رسانه، مانند سرور نیاز دارد.

درخواست های تعاملی سرور و رديابي وضعیت مشتری برای هر جلسه مشتری در حال انجام.

را مسدود کنند و از دریافت UDP بسیاری از فایروال ها به گونه ای پیکربندی شده اند که ترافیک 3. توسط کاربران پشت این فایروال ها جلوگیری می کنند UDP ویدیویی.

می خواند و بایت ها در بافر TCP خیر. در سمت کلاینت، برنامه سرویس گیرنده بایت ها را از بافر دریافت 7. برنامه مشتری قرار می دهد.

ثانیه است $t_{\text{p}} = Q/x = 4$ تا خیر اولیه بافر.

9. Enter Deep: این فلسفه ورود عمیق به شبکه های دسترسی ارائه دهنده خدمات اینترنت، با استقرار خوش های های دسترسی در سراسر جهان است ISP سرور در.

به خانه بیاورید: دومین فلسفه طراحی این است که با ساختن خوش های بزرگ در تعداد کمتری از مکان های کلیدی را به خانه بیاوریم ISP و اتصال این خوش ها با استفاده از یک شبکه پرسرعت خصوصی، خانه

انتخاب نزدیکترین خوش از نظر جغرافیایی و انتخاب اندازه گیری زمان واقعی می تواند خوش خوبی با توجه به 10. خوش خوبی را با توجه به خود مشتری انتخاب می کند IP anycast. پیدا کند LDNS.

بار روی خوش - مشتریان نباید به سمت بارگذاری بیش از حد خوش ها هدایت شوند. 11.

های خاصی برای حمل ترافیک ISP خوش ها ممکن است به گونه ای انتخاب شوند که - ISP ها و ISP به مشتری استفاده شوند، با در نظر گرفتن ساختار های مختلف هزینه در روابط قراردادی بین CDN اپراتور های خوش.

تأخیر انتها به انتهای مدت زمانی است که طول می کشد تا یک بسته در سراسر شبکه از مبدأ به مقصد سفر 12. نوسان تأخیر انتها به انتهای از بسته به بسته بعدی است Delay jitter کند.

بسته ای که پس از زمان پخش برنامه ریزی شده خود می رسد قابل پخش نیست. بنابراین، از دیدگاه برنامه، بسته گم 13. شده است.

تکه n انحصاری OR قطعه، یک قطعه رمزگذاری شده اضافی ارسال کنید. تکه زائد با n طرح اول: پس از هر 14. اصلی به دست می آید. طرح دوم: یک طرح نرخ بیت کم با وضوح پایین را به همراه جریان اصلی ارسال نیاز به پهنای باند یک جریان را افزایش نمی دهد. Interleaving کنید.

در همان جلسه جریان می یابد: فیلد RTP در جلسات مختلف: آدرس های چندپوشی مختلف جریان های 15. متمایز می شوند. RTCP با استفاده از شماره پورت های متمایز از بسته های RTP بسته های SSRC.

مربوطه آنها را که در حال حاضر استفاده می IP این است که کاربران و آدرس های SIP نقش یک ثبت کننده 16. INVITE کاربران متعلق به دامنه خود را ردیابی می کند. همچنین پیام های SIP کنند، پیگیری کند. هر ثبت کننده که کاربر در حال حاضر استفاده می کند، ارسال می کند. از این نظر، نقش IP را به آدرس (برای کاربران دامنه خود) است DNS آن شبیه به یک سرور نام معنبر در.

در صف، اولویت های غیر پیشگیرانه، انتقال یک بسته پس از شروع آن قطع نمی شود. در صف اولویت 17. پیشگیرانه، اگر بسته با اولویت بالاتر قبل از اتمام ارسال بررسد، ارسال بسته قطع می شود. این بدان معناست که بخش هایی از بسته به عنوان تکه های جداگانه به شبکه ارسال می شود. این تکه ها دیگر همه فیلدهای هدر مناسب را ندارند. به همین دلیل از صف اولویت پیشگیرانه استفاده نمی شود.

یک رشته زمان بندی که صرفه جویی در کار نیست، مالتی پلکسی تقسیم زمان است که به موجب آن یک قاب 18. چرخان به شکاف ها تقسیم می شود و هر شکاف منحصرآ برای یک کلاس خاص در دسترس است.

ادغام ترافیک (برداشتن 1 وسیله نقلیه از لاین اول و سپس 1 وسیله نقلیه از: RR. خط در استارباکس: 19. FIFO: باجه بلیط در فروندگاه به 2 نفر از فرست کلاس و 1 نفر: WFQ: خط دوم و سپس 1 وسیله نقلیه از خط اول و غیره) از اکنومی و دوباره 2 نفر از فرست کلاس و غیره خدمات ارائه می دهد.

فصل 7 مسائل

مشکل 1

کلاینت پخش را شروع می کند و بلوک های ویدئویی باید در مدت زمان ثابت t_1 (الف) به محض رسیدن بلوک اول به وارد شود تا در زمان مناسب $d + t_1$ بنابراین نتیجه می شود که بلوک ویدیویی دوم باید قبل از زمان d ، پخش شوند. پخش شود، بلوک سوم در ساعت

و غیره. از شکل می توانیم ببینیم که فقط بلوک های شماره $6, 5, 4, 3, 2$ قبل از زمان پخش خود به گیرنده $t_1 + 2d$ می رسند.

پخش d ، شروع می کند و بلوک های ویدیویی باید در مدت زمان ثابت $d + t_1$ (ب) کلاینت پخش را در زمان وارد شود تا در زمان مناسب پخش شود، $d + 2t_1$ شوند. بنابراین نتیجه می شود که بلوک ویدیویی دوم باید قبل از زمان و غیره. از شکل می توانیم ببینیم که بلوک های ویدیویی که از 1 تا 6 شماره گذاری شده اند، به $d + 3t_1$ بلوک سوم در جز 7، قبل از زمان پخش خود به گیرنده می رسند.

و $d + 3t_1$ (ج) حداقل دو بلوک ویدیویی در بافر مشتری ذخیره می شود. بلوک های ویدیویی با شماره 3 و 4 قبل از می رسند، بنابراین این دو بلوک در بافر مشتری ذخیره می شوند. بلوک ویدیویی با شماره 5 قبل از $d + t_1 + 2t_1$ و بعد از وارد می شود که در بافر مشتری به همراه بلوک ویدیویی از قبل ذخیره شده با $d + 3t_1 + 4t_1$ و بعد از $t_1 + 4d$ زمان شماره 4 ذخیره می شود.

باشد تا اطمینان حاصل شود که هر بلوک به موقع رسیده است $d + 3t_1$ (د) کوچکترین پخش در مشتری باید.

مشکل 2

کاهش می یابد. بنابراین، پس از $x - r$ شروع می شود و با نرخ Q (الف) در طول یک دوره پخش، بافر با بیت های ثانیه است. هنگامی که $(x - r)/Q$ ثانیه پس از شروع پخش، بافر خالی می شود. بنابراین، دوره پخش مداوم $(x - r)/Q$ دارد و پخش شروع می Q ثانیه پر می شود، در این زمان بیت x/Q به مدت x بافر خالی می شود، با سرعت ثانیه است x/Q شود. بنابراین دوره انجامad

$B - Q$ ثانیه است. زمان اضافه کردن بیت های x/Q داشته باشد Q (ب) زمان تا زمانی که بافر بیت r ثانیه است $B - Q$ ثانیه است. بنابراین زمان پر شدن بافر برنامه r

ثانیه

مشکل 3

است $H/2$ (الف) میانگین نرخ ارسال سرور.

فریم بعدی بعد از زمان پخش برنامه ریزی شده فریم بعدی می رسد. بنابراین پخش پس از نمایش اولین فریم متوقف می شود.

باید در $Q = q(t)$ نشان دهد. پخش زمانی شروع می شود که t تعداد بیت های بافر را در زمان $q(t)$ (ج) اجازه دهد ما داریم. x در پایان اولین چرخه برای Q به طوری که $Q \geq HT/2$ سراسر این مسئله فرض کنیم که

$$q(t) = \frac{\int_0^t r(s)ds}{T} = \frac{HT2/2T}{T} = \frac{HT2}{2T}$$

است زمانی که $q(t) = Q$ ، بنابراین $2QT/H =$ شهر.

به طوری که پخش شروع می شود. اگر متعاقباً انجماد وجود نداشته باشد، به $q(t) = T$ در زمان $t = T$ ، $q(t) = HT/2 = Q$ نیاز داریم، ما باید $T \geq t \geq 0$ برای همه

$$\begin{aligned} q(t+T) &= HT2 - rt + \int_t^{t+T} x(s)ds \\ &> HT2(T-t) + \int_t^{t+T} x(s)ds \end{aligned}$$

از بالا داریم، $0 < \Delta < T$ با

$$\begin{aligned} q(t+T) &> HT2(T-t) - nT - \Delta + nHT2 + \frac{H\Delta2T}{H\Delta2T} \\ &= \frac{T-\Delta}{H2} + \frac{nHT2}{H2\Delta2T} \end{aligned}$$

امکان پذیر است $T < \Delta$ که به راحتی دیده می شود که برای همه 0

را در نظر بگیرید. ما داریم $[0, T]$ ابتدا

$$q(t) = HT2(t-tp) - r(t-tp) \quad \text{برای } tp \leq t \leq T$$

اگر و فقط اگر $tp \geq 0$ $q(t) = rT/H$ به حداقل می رسد. سپس می توان نشان داد که $t = rT/H$ را برای همه $0 < t < T$ اثبات را می توان گسترش داد تا، $tp = rT/2H$ باشد. علاوه بر این، اگر $T < rT/2H$ و $Q = r2T/8H$.

رسیده T قبل از زمان B این یک مشکل بسیار چالش برانگیز است. با فرض اینکه $(x - r)^*$ را برای هستند و نلف می شوند E بیت های $(x - r)^*$ رشد می کند. در زمان r (الف) بافر با نرخ

مشکل 4

در بافر هستند و نلف می شوند E بیت های $(x - r)^*$ رشد می کند. در زمان r (الف) بافر با نرخ

E تا زمان $r - x$ بافر با سرعت S زمانی باشد که سرور کل ویدیو را ارسال کرده است. اگر S (ب) اجازه دهد ثانیه های ویدیو هنوز در E باشد، در زمان $E - T$ ، E است. اگر $S = (r - x)^*E$ رشد می کند، بنابراین ضایعات دوباره $(T - E)^*$ بافر پخش می شود. بنابراین ضایعات E).

مشکل 5

$$\text{الف) } N^*N = N^2.$$

$$\text{ب) } N+N = 2N$$

مشکل 6

$$\text{بايت ها هر 20 ميلى ثانие ارسال می شوند. بنابراین نرخ انتقال است} \\ \text{بايت ها هر 20 ميلى ثانie ارسال می شوند. بنابراین نرخ انتقال است} \\ \text{بايت ها هر 20 ميلى ثانie ارسال می شوند. بنابراین نرخ انتقال است} \\ \text{بايت ها هر 20 ميلى ثانie ارسال می شوند. بنابراین نرخ انتقال است}$$

ب)

$$\text{بايت 20 هدر IP:}$$

$$\text{بايت هدر UDP: 8 هدر}$$

$$\text{بايت RTP: 12}$$

$$\text{بايت (افزایش 25 درصدی در نرخ انتقال!) (ج) } h=40$$

مسئله 7

برای تخمین بعد از نمونه nd (الف) نشان دهد.

$$d_1 = r_4 - r_1$$

$$d_2 = r_2 - r_3 + 1(r_2 - r_3)(r_3 - r_4)$$

$$d_3 = r_2 - r_1 + 1(r_2 - r_1)(r_3 - r_4) + 1(r_2 - r_1)(r_3 - r_4)$$

$$= r_2 - r_3 + 1(r_2 - r_3) + 1(r_2 - r_3)^2 r_4 - r_1 \quad \text{صورت حساب}$$

$$d_4 = r_1 - r_2 + 1(r_1 - r_2)$$

$$= r_1 - r_2 + 1(r_1 - r_2) + 1(r_1 - r_2)^2 r_3 - r_2 + 1(r_1 - r_2)^3 r_4 - r_1 \quad \text{صورت حساب}$$

ب)

$$d^{(n)} = \sum_{j=1}^n 1(r_1 - r_j) r_j - r_1 + 1(r_1 - r_n) r_n - r_1$$

ج)

$$U^d = \sum_{j=1}^{\infty} (r_j - t_j)$$

$$= \sum_{j=1}^{\infty} D^j (r_j - t_j)$$

وزن داده شده به نمونه های گذشته به صورت تصاعدی کاهش می یابد.

مسئله 8

اجازه دهدید. n برای تخمین بعد از نمونه (الف) نشان دهد

$$D^j t_j = \dots$$

$$v^{(1)} = D(t_1 - r_1) = 0$$

$$v^{(2)} = D(t_2 - r_2) + 1(-t_1) D(t_1 - r_1)$$

$$v^{(3)} = D(t_3 - r_3) + 1(-v^{(2)}) D(t_2 - r_2) + 1(-v^{(1)}) D(t_1 - r_1)$$

$$= D(t_3 - r_3) + 1(-t_2) D(t_2 - r_2) + 1(-t_1)^2 D(t_1 - r_1)$$

$$v^{(4)} = D(t_4 - r_4) + 1(-v^{(3)}) D(t_3 - r_3) + 1(-v^{(2)}) D(t_2 - r_2)$$

$$= D(t_4 - r_4) + 1(-t_3) D(t_3 - r_3) + 1(-t_2)^2 D(t_2 - r_2) + 1(-t_1)^3 D(t_1 - r_1)$$

$$= [D(t_n - r_n) + 1(-t_{n-1}) D(t_{n-1} - r_{n-1}) + 1(-t_{n-2})^2 D(t_{n-2} - r_{n-2}) + \dots + 1(-t_1)^{n-1} D(t_1 - r_1)]$$

$$+ 1(-t_0) D(t_0 - r_0)$$

)

$$v^{(n)} = \sum_{j=1}^{n-1} 1(-t_0)^{j-1} D(t_j - r_j) + 1(-t_0)^n D_n - r_0$$

مسئله 9

$$i) r_1 - t_1 + r_2 - t_2 + \dots + r_{n-1} - t_{n-1} = (n-1)d_n - 1$$

می دهد d_n جایگزین کردن این به عبارت

$$\sum_{n=1}^{\infty} d_n = \sum_{n=1}^{\infty} r_d^{n-1} + t_n$$

ب) برآورد تأخیر در قسمت (الف) میانگین تأخیرها است. به تأخیرهای اخیر و تأخیرهای «قديمی» وزن يکسانی می دهد. برآورد تأخیر در بخش 6.3 به تأخیرهای اخیر اهمیت بيشتری می دهد. تأخیر در گذشته دور تاثیر نسبتاً کمی بر برآورد دارد.

مسئله 10

اين دو روش بسيار مشابه هستند. هر دو آنها از فرمول يکسانی استفاده می کنند و در نتيجه وزن نمونه های گذشته را به طور تصاعدي کاهش می دهند.

زمان ارسال داده ها و دريافت تاييدие در همان ماشين ثبت می RTT، يك تفاوت اين است که برای تخمین ميانگين شود. برای برآورد تأخير، اين دو مقدار در ماشين های مختلف ثبت می شوند. بنابر اين تأخير نمونه در واقع می تواند منفی باشد.

مسئله 11

تاخير بسته 2 اسلات است. تاخير بسته 3 9 اسلات است. تاخير بسته 4 8 اسلات است. تاخير بسته 5 7 اسلات است. تاخير بسته 6 9 اسلات است. تاخير بسته 7 8 اسلات است. تاخير بسته 8 > 8 اسلات است.

به موقع برای پخش خود دريافت نمی شوند $t=8$ ب) بسته های 3، 4، 6، 7 و 8 در صورت شروع پخش از.

به موقع برای پخش خود دريافت نمی شوند $t=9$ ج) بسته های 3 و 6 در صورت شروع پخش از.

شروع شود، هیچ بسته ای پس از زمان پخش خود نمی رسد $t=10$ د) اگر زمان پخش از.

مسئله 12

پاسخ قسمت های الف و ب در جدول زير آمده است:

شماره بسته	مي بينيم كه	د	v_i
1	7	7	0
2	8	7.10	0.09
3	8	7.19	0.162
4	7	7.17	0.163
5	9	7.35	0.311
6	9	7.52	0.428
7	8	7.57	0.429
8	8	7.61	0.425

مسئله 13

(الف) هر دو طرح به 25 درصد پهنانی باند بیشتر نیاز دارند. اولین طرح دارای تاخیر پخش 5 بسته است. طرح دوم دارای 2 بسته تاخیر است.

(ب) طرح اول می تواند رمزگذاری صوتی با کیفیت بالا را بازسازی کند. طرح دوم از رمزگذاری صوتی با کیفیت پایین برای بسته های گم شده استفاده می کند و بنابراین کیفیت کلی پایین تری خواهد داشت.

(ج) برای طرح اول، بسیاری از بسته های اصلی گم می شوند و کیفیت صدا بسیار ضعیف خواهد بود. برای طرح دوم، هر قطعه صوتی در گیرنده در دسترس خواهد بود، اگرچه فقط نسخه با کیفیت پایین برای هر قطعه دیگر در دسترس خواهد بود. کیفیت صدا قابل قبول خواهد بود.

مسئله 14

را برای آغازگر ارسال می $r \text{ bps}$ دیگر یک جریان صوتی با نرخ 1 - N (الف) هر یک از شرکت کنندگان ایجاد کند. سپس یک کپی از 2 کند. آغازگر این جریان را با جریان خروجی خود ترکیب می کند تا جریانی از نرخ (N-1) ارسال می کند. بنابراین آغازگر تماس با نرخ کل 1 - N جریان ترکیبی را برای هر یک از شرکت کنندگان دیگر 1 (N-1) r bps (N-1) ارسال می کند، و نرخ کل جمع آوری شده روی همه شرکت کنندگان 2 $r = N(N-1) r \text{ bps}$.

را برای آغازگر ارسال می $r \text{ bps}$ دیگر یک جریان ویدئویی با نرخ 1 - N (ب) مانند قبل، هر یک از شرکت کنندگان کند. اما چون جریان ها اکنون ویدئویی هستند، آغازگر دیگر نمی تواند آنها را در یک جریان واحد ترکیب کند. در عوض، شرکت کننده ارسال کند. بنابراین آغازگر تماس با نرخ کل 2 - N آغازگر باید هر جریانی را که دریافت می کند برای (N-1)*(N-1)r bps (N-1) ارسال می کند، و نرخ کل جمع آوری شده روی همه شرکت کنندگان $r = N(N-1) r \text{ bps}$.

(ج) $N * (N-1) r \text{ bps}$

مسئله 15

مقصد و IP با دو تایی متشكل از آدرس UDP (الف) همانطور که در فصل 2 مورد بحث قرار گرفت، سوکت های شماره پورت مقصد شناسایی می شوند. بنابراین این دو بسته در واقع از یک سوکت عبور می کنند.

های مختلفی را انتخاب می کنند، بنابراین آليس می SSRC (ب) بله، آليس فقط به یک سوکت نیاز دارد. باب و کلر چگونه می Alice تواند بین این دو جریان تمايز قائل شود. سوال دیگری که می توانستیم پرسیم این است: نرم افزار است؟ در واقع، نرم افزار آليس Alice و کدام جریان متعلق به Bob متعلق به (SSRC یعنی) دارد که کدام جریان را SSRC ممکن است بخواهد نام فرستنده را زمانی که فرستنده در حال صحبت است نمایش دهد. نرم افزار آليس دریافت می کند RTCP برای نگاشت نام از گزارش های شرح منبع

مسئله 16

را می توان به از هر شماره پورتی RTP الف) درست ب) درست ج) خیر، جریان های در مراجعه کنید SIP ارسال کرد. به مثال

متفاوتی به SSRC بخش 6.4.3 د) خیر، معمولاً مقادیر آنها اختصاص داده می شود. ه) درست است

نادرست، نشان می دهد (g) را دریافت کند GSM نادرست، نشان می دهد که می خواهد صدای f درست، 5060 برای هر دو شماره (h) که می خواهد صدا را در پورت 48753 دریافت کند پورت منبع و مقصد

درست است، واقعی (من)
است و نه H.323 SIP. این مورد نیاز (ی

مسئله 17

الف) یکی از زیرالهای ممکن 1 2 1 3 1 2 1 3 1 2 ... است

توالی ممکن دیگر 1 1 3 1 1 3 1 1 3 1 1 2 1 1 3 1 1 2 1 ... ب) 3 1 1 3 ...

مسئله 18

ا)

بسته	زمان خروج از صفحه	تلخیر انداختن
1	0	0
2	1	1
3	2	1
4	3	2
5	5	2
6	4	2
7	6	3
8	7	2
9	8	3
10	9	2
11	10	2
12	11	3
تلخیر متوسط		1.91

ب)

بسته	زمان خروج از صفحه	تلخیر انداختن
1	0	0
2	2	2
3	1	0

4	6	5
5	4	1
6	7	5
7	3	0
8	9	4
9	5	0
10	10	3
11	8	0
12	11	3
تأخير متوسط		1.91

(ج)

بسته	زمان خروج از صف	تأخير انداختن
1	0	0
2	2	2
3	4	3
4	1	0
5	3	0
6	6	4
7	5	2
8	7	2
9	9	4
10	11	4
11	8	0
12	10	2
تأخير متوسط		1.91

(د)

بسته	زمان خروج از صف	تأخير انداختن	نحوه بندی پیش
1	0	0	WFQ
2	2	2	WFQ
3	1	0	WFQ
4	5	4	WFQ
5	3	0	WFQ
6	7	5	زمان بندی ایده آل WFQ
7	4	1	WFQ
8	9	4	WFQ
9	6	1	زمان بندی ایده آل WFQ
10	10	3	WFQ
11	8	0	WFQ
12	11	3	WFQ
تأخير متوسط		1.91	

(ه) می توان توجه داشت که میانگین تاخیر برای هر چهار مورد یکسان است (1.91 ثانیه).

مسئله 19

یک پاکت

	زمان خروج از صف	تاخیر اندختن
1	0	0
2	4	4
3	5	4
4	1	0
5	3	0
6	2	0
7	6	3
8	9	4
9	7	2
10	10	3
11	8	0
12	11	3
تاخیر متوسط		1.91

(ب)

پسته	زمان خروج از صف	تاخیر اندختن
1	0	0
2	1	1
3	3	2
4	2	1
5	6	3
6	4	2
7	5	2
8	9	4
9	7	2
10	10	3
11	8	0
12	11	3
تاخیر متوسط		1.91

(ج)

پسته	زمان خروج از صف	تاخیر اندختن
1	0	0
2	1	1
3	2	1
4	3	2

5	9	6
6	6	4
7	4	1
8	7	2
9	5	0
10	8	1
11	11	3
12	10	2
تاخیر متوسط		1.91

مسئله 20

اسلات زمان	بسته ها در صفحه	تعداد توکن ها در سطل
0	1، 2، 3	2
1	3، 4	1
2	4، 5	1
3	5، 6	1
4	6	1
5	-	1
6	7، 8	2
7	9، 10	1
8	10	1

اسلات زمان	بسته ها در بافر خروجی
0	1، 2
1	3
2	4
3	5
4	6
5	-
6	7، 8
7	9
8	10

مسئله 21

اسلات زمان	بسته ها در صفحه	تعداد توکن ها در سطل
0	1، 2، 3	2
1	3، 4	2
2	5	2
3	6	2
4	-	2
5	-	2
6	7، 8	2
7	9، 10	2

8

-

2

اسلات زمان	بیسته ها در بافر خروجی
0	1، 2
1	3، 4
2	5
3	6
4	-
5	-
6	7، 8
7	9، 10
8	-

مسئله 22

نه. پاسخ همچنان مانند مسئله 21 باقی می ماند.

مسئله 23

شکل زیر را بینید. برای سطح نشتی دوم

$$r = bp = .1$$

شکل: راه حل مسئله 26

مسئله 24

خبر

مسئله 25

را به عنوان آغاز یک T اجازه دهد زمانی باشد که در آن جریان 1 ترافیک شروع به جمع شدن در صفحه می کند. ما زمان دیگری در همان جریان-1 باشد $T > t$ دوره شلوغ جریان-1 می نامیم. بگذارید مقادیر جریان-1 ترافیک منتقل شده در بازه زمانی باشد تن t_1 تا t_2 دوره شلوغ اجازه دهد به وضوح

[۲۲]

$$\sum_j W_{tR} \geq t_i - t_i(t_i)$$

باشد. به وضوح t ترافیک در صف در زمان-1 مقدار W_{tR} س اجازه دهد
 $t_i(t_i) = t_i - r_i$

$$\begin{aligned} & \leq r_i + t_i + \sum_j W_{tR} \\ & = r_i + \sum_j W_{tR} \end{aligned}$$

بنابراین حداقل مقدار جریان-1 ترافیک در صف. $b \leq t_i$ است

حداقل نرخی که این ترافیک با آن ارائه می شود $\sum_j W_{tR}$ است.

بنابراین، حداقل تاخیر برای یک بیت جریان 1 است

$$b = \sum_j W_{tR}$$

فصل هشتم سوالات مروری

محرمانه بودن ویژگی است که پیام متن ساده اصلی را نمی توان توسط مهاجمی که رمزگذاری متن رمزی پیام 1. متن اصلی را هگیری می کند، تعیین کرد. یکپارچگی پیام خصوصیتی است که گیرنده می تواند تشخیص دهد که آیا پیام ارسال شده (خواه رمزگذاری شده باشد یا نه) در حین انتقال تغییر کرده است. بنابراین این دو مفاهیم متفاوتی هستند و یکی می تواند یکی را بدون دیگری داشته باشد. پیام رمزگذاری شدهای که در انتقال تغییر می کند ممکن است همچنان محرمانه باشد (مهاجم نمی تواند متن اصلی اصلی را تعیین کند) اما اگر خطای شناسایی نشود، یکپارچگی پیام را نخواهد داشت. به طور مشابه، پیامی که در حین انتقال تغییر می کند (و شناسایی می شود) می تواند به صورت متن ساده ارسال شود و بنابراین محرمانه نخواهد بود.

2. DNS دو سرور نام (iii) دو روتر؛ (ii). لپ تاپ کاربر و یک وب سرور.

یک تفاوت مهم بین سیستم های متقارن و کلید عمومی این است که در سیستم های کلید متقارن هم فرستنده و هم گیرنده 3. باید کلید (مخفي) یکسانی را بدانند. در سیستم های کلید عمومی، کلیدهای رمزگذاری و رمزگشایی متمایز هستند. بنابراین

کل جهان (از جمله فرستنده) کلید رمزگذاری را می شناسد، اما کلید رمزگشایی را فقط گیرنده می شناسد.

4. در این مورد، یک حمله متن ساده شناخته شده انجام می شود.
اگر به نحوی پیام رمزگذاری شده توسط فرستنده توسط مهاجم انتخاب شده است، سپس این یک حمله متن ساده انتخابی خواهد بود.

5. یک رمز 8 بلوکی دارای 2 بلوک ورودی ممکن است. هر نگاشت جایگشتی از 28 بلوک ورودی است. بنابراین 2 وجود دارد! نقشه برداری های ممکن بنابراین 2 وجود دارد! کلیدهای ممکن

6. کاربر دیگر ارتباط برقرار کند، هر جفت کاربر باید یک کلید متقارن مشترک داشته N اگر هر کاربر بخواهد با چنین جفتی وجود دارد و بنابراین وجود دارد $\frac{N(N-1)}{2}$. باشد کلید با یک سیستم کلید عمومی، هر کاربر یک کلید عمومی دارد که برای همه شناخته شده است و در سیستم کلید N یک کلید خصوصی (که مخفی است و فقط توسط کاربر شناخته می شود). بنابراین کلیدهای 2 عمومی وجود دارد.

7. $a \bmod n = 23$, $b \bmod n = 4$. $(a^*b) \bmod n = 23^*4=92$

8. 175

9. دیگری که همان خلاصه پیام را M' یافتن پیام، یکی از الزامات خلاصه پیام این است که با توجه به یک پیام که دارای "M" داشته باشد بسیار دشوار است و به عنوان نتیجه، با توجه به مقدار خلاصه پیام، یافتن پیام دشوار است مقدار خلاصه پیام داده شده است. ما "یکپارچگی پیام" به معنایی که داریم داریم و پیام امضا شده آن، این را هضم می کند M اطمینان معقولی که با توجه به یک پیام پیام تغییر نکرد زیرا خلاصه پیام محاسبه و امضا شد. این هست

در مورد چکسوم اینترنت درست نیست، جایی که در شکل 7.18 دیدیم که یافتن دو پیام با چکجمع اینترنت یکسان آسان است.

خیر. این به این دلیل است که یک تابع یک طرفه است. یعنی با توجه به هر مقدار هش، پیام اصلی 10. بازیابی کرد h را از m نمی‌توان، $h = H(m)$ به گونه‌ای که h قابل بازیابی نیست (با توجه به

این طرح به وضوح ناقص است. ترودی، یک مهاجم، ابتدا می‌تواند ارتباط را بشنود و با استخراج آخرین بخش 11. به عنوان $H(t+s)$ و ارسال t را از مشترک را بدست آورد. ترودی می‌تواند با ایجاد پیام، $H(m+s)$ ارقام از فرستنده خود را بپوشاند.

فرض کنید باب یک سند رمزگذاری شده برای آلیس می‌فرستد. برای اینکه قابل تأیید باشد، آلیس باید بتواند خود را 12. مقاععد کند که باب سند رمزگذاری شده را ارسال کرده است. برای غیرقابل جعل بودن، آلیس باید بتواند خود را مقاععد کند که فقط باب می‌تواند سند رمزگذاری شده را ارسال کرده باشد (به عنوان مثال، هیچ کس دیگری نمی‌توانست یک کلید را حدس بزند و سند را رمزگذاری یا ارسال کند) برای غیرقابل اعتماد بودن، آلیس باید می‌تواند شخص دیگری را مقاععد کند که فقط باب می‌تواند سند را ارسال کند. برای نشان دادن تمایز اخیر، فرض کنید باب و آلیس یک کلید مخفی مشترک دارند و آنها تنها کسانی در جهان هستند که کلید را می‌دانند. اگر آلیس سندی را دریافت کند که با کلید رمزگذاری شده است، و بداند که خودش سند را رمزگذاری نکرده است، انگاه سند قابل تأیید و غیرقابل جعل است (با فرض اینکه از یک سیستم رمزگذاری قوی استفاده شده باشد). با این حال، آلیس نمی‌تواند شخص دیگری را مقاععد کند که باب باید سند را ارسال کرده باشد، زیرا در واقع آلیس خودش کلید را می‌دانست و می‌توانست سند را رمزگذاری/ارسال کند.

خلاصه پیام امضا شده با کلید عمومی "بهتر" است، زیرا تنها به رمزگذاری (با استفاده از کلید خصوصی) 13. گران است، RSA خلاصه پیام کوتاه، به جای کل پیام نیاز است. از آنجایی که رمزگذاری کلید عمومی با تکنیکی مانند مطلوب است که مجبور به امضا کردن (رمزگذاری) مقدار کمتری از داده نسبت به مقدار بیشتری از داده باشد.

شامل یک امضای دیجیتال است که هش اطلاعات certifier.com، این نادرست است. برای ایجاد گواهی 14. امضا شده است certifier.com است و با کلید خصوصی (شامل کلید عمومی آن) foo.com.

آلیس باید یک کلید مشترک با هر گیرنده بالقوه ایجاد کند. با امضای دیجیتال، او، MAC برای یک طرح مبتنی بر 15. از همان امضای دیجیتال برای هر گیرنده استفاده می‌کند. امضای دیجیتال با امضای هش پیام با کلید خصوصی او ایجاد می‌شود. امضای دیجیتال در اینجا به وضوح انتخاب بهتری است.

دفاع در برابر حمله مجدد است nonce هدف. 16.

بیگر هرگز از آن مقدار برای بررسی اینکه nonce یک بار در طول عمر به این معنی است که نهاد ارسال کننده 17. آیا موجودیت دیگری "زنده" است یا خیر استفاده نخواهد کرد.

18. مهاجم خود را بین آلیس و باب قرار می دهد و داده های ارسال شده بین، Man-in-the-Middle، آنها را تغییر می دهد. اگر باب و آلیس یک کلید احراز هویت مخفی را به اشتراک بگذارند، هر گونه تغییر شناسایی خواهد شد.

19. آلیس یک امضای دیجیتالی ارائه می دهد که باب می تواند از طریق آن تأیید کند که پیام از آلیس آمده است. MAC برای یکپارچگی پیام از امضای دیجیتال استفاده می کند نه

20. از اعداد دنباله ای ضمنی استفاده می کند SSL نادرست.

21. هدف از نونهای تصادفی در دست دادن، دفاع در برابر حمله پخش مجدد اتصال است.

22. ارسال می شود SSL هنگام دست دادن، SSL همیشه به صورت واضح ارسال می شود. در IV درست است.

23. را ایجاد کرد، آن را با کلید عمومی آلیس رمزگذاری می کند و (PMS) پس از اینکه کلاینت یک راز اصلی را رمزگشایی کند، زیرا کلید PMS ارسال می کند. ترویجی نمی تواند Trudy رمزگذاری شده را برای PMS سپس قادر به تعیین کلید احراز هویت مشترک خواهد بود. او ممکن است در Trudy خصوصی آلیس را ندارد. بنابراین عوض با انتخاب یک کلید تصادفی یکی را حدس بزند. در آخرین مرحله از دست دادن، او با استفاده از کلید احراز را Bob MAC از تمام پیام های دست دادن را برای باب ارسال می کند. هنگامی که MAC هویت حدس زده، یک را پایان خواهد داد TCP ناموفق خواهد بود و باب اتصال MAC دریافت کرد، تست

24. ایجاد می شود. سپس تمام بسته های موجود در B و میزبان A ابتدا بین میزبان IPsec SA نادرست. معمولاً یک استفاده می کند SA جریان از

25. برای هر بسته ای که ارسال می کند، شماره دنباله را افزایش می دهد IPsec.

26. استفاده می شود IPsec SA برای ایجاد یک یا چند IKE SA نادرست.

27. 01011100

28. درست. است

29. میز فیلتر و جدول اتصال. جدول اتصال، اتصالات را ردیابی می کند و امکان فیلتر کردن بسته ها را به میزان کمتری می دهد.

30. درست. است

31. درست. است

32. اگر فیلتر بسته وجود نداشته باشد، کاربران در داخل شبکه موسسه همچنان می توانند به میزبان های خارج از شبکه موسسه ارتباط مستقیم برقرار کنند. فیلتر کاربران را مجبور می کند ابتدا به دروازه برنامه متصل شوند.

درست. 33.
است

فصل 8 مسائل

"مشکل 1 رمزگذاری "این یک مشکل آسان است "uasi si my cmiw lokngch" خیلی جالب نبود" "rmij'u uamu xyj" است. رمزگشایی

در متن ظاهر می شوند، پس متن رمزی "bob" و "alice" مشکل 2 اگر ترویدی می دانست که کلمات b,o,a,l,i,c,e تنها رنگ برجسته در متن است. پیام، و "الیس" تنها کلمه 5 حرفی "bob" را می دانست (زیرا است که اگر ترویدی 7 حرف را می داند، فقط باید 19 حرف را امتحان کند، نه 26؛ تفاوت بین 19 را! و 26 9 میشه 26...24*25*26 که میشه 3315312000 یا تقریباً 10.

مشکل 3 هر حرف در الفیا در عبارت "روباه سریع از روی سگ تنبل قوه ای می پرد" ظاهر می شود. با توجه به این عبارت در یک حمله متن ساده انتخاب شده (جایی که مهاجم هم متن ساده و هم متن رمز را دارد)، رمز ساز Vigenere، شکسته می شود - مزاح نویسه متن رمز را برای هر کاراکتر متن ساده می شناسد. با این حال

Vigenere رمز همیشه هر بار یک کاراکتر متن ساده را به همان نویسه متن رمزی ترجمه نمی کند، و از این رو رمز بلاfacسله با این حمله متن ساده شکسته نمی شود.

مسئله 4 (الف) خروجی برابر است با 00000101 که هشت بار تکرار شده است. (ب) خروجی برابر داریم که در ARBRCR)R = CBA (است با 00000101 تکرار هفت بار + 10000101. ج به معنای معکوس است R رشته ها هستند و A، B، C

: عمل بین ترتیب

برای (الف)، خروجی 10100000 است که هشت بار تکرار شده است.

برای (ب)، خروجی 10100000 + 10100001 هفت بار تکرار شده است.

مسئله 5 (الف) 8 جدول وجود دارد. هر جدول دارای 28 ورودی است. هر ورودی 8 بیت دارد.

تعداد جداول * اندازه هر جدول * اندازه هر ورودی = 8 * 28 * 8 = 214 بیت

(ب) 264 ورودی وجود دارد. هر ورودی 64 بیت دارد. 271 بیت

مسئله 6 (الف) 011011011 <= 100100100 (ب)

(ترویدی می داند که سه متن ساده بلوک یکسان هستند. ج

= KS(m(i)) XOR c(i-1))

$$c(1) = KS(100 \text{ XOR } 111) = KS(011) = 100$$

$$c(2) = KS(100 \text{ XOR } 100) = KS(000) = 110$$

$$c(3) = KS(100 \text{ XOR } 110) = KS(010) = 101$$

مسئله 7

ممکن است ایده خوبی باشد که به دانشآموزان اشاره کنیم که 9 مقدار مناسبی برای انتخاب است، زیرا محاسبات احتمال کمتری دارد که با مشکلات ثبات عددی مواجه e . حاصل از 3 و $1(20)(1)(1)$ نسبت به سایر گزینه‌های هیچ فاکتور مشترکی ندارند $= qp$ = شوند.

دقیقاً بر تقسیم پذیر است $80 = 1 \cdot d + 9$ و بنابراین $d = 80 - 9 = 71$ همچنین به طوری که $9=d$ انتخاب کنید را با استفاده از آن انجام دهیم RSA اکنون می‌توانیم رمزگاری و رمزگشایی 20. $9=e$ و $33=n$ ، $9=d$

حرف	متر	m^{**e}	متن رمزی = $m^{**e} \bmod 33$
d	4	262144	25
o	15	38443359375	3
g	7	40353607	19

متن رمزی	ج	$m = c^{**d} \bmod n$	حرف
25	38146972265625	4	d
3	19683	15	o
19	322687697779	7	g

ابتدا هر حرف را به عنوان یک عدد 5 بیتی در نظر می‌گیریم: 00111, 01111, 00100. اکنون هر حرف $m=4583$ را به هم متصل می‌کنیم تا 001000111100111. را بدست آوریم و عدد اعشاری حاصل را نیاز $< n$ فلی ($= 33$) است. ما به n بزرگتر از ($= 4583$) m رمزگذاری می‌کنیم. عدد اعشاری الحاقی استفاده می‌کنیم 4452 = $p = 43$, $q = 107$, $n = p \cdot q = 4601$, $z = (p-1) \cdot (q-1) = 4452 - 1 = 4451$. بنابراین ما از $e = 61$, $d = 73$

$$\text{ciphertext} = m^{**e} \bmod 4601$$

$$\begin{aligned} m^{**e} = & 21386577601828057804089602156530567188611499869029788733808438 \\ & 80430286459562061395672594748584747416 246785033236197 \\ & 777129730258961756918400292048632806197527785447791567255101894492820 \\ & 9725081828 \end{aligned}$$

$$\text{m}^{**e} \bmod 4601 = 402$$

$$\begin{aligned} c^{**d} = & 1283813313619771634195712132539793287643533147482536209328405262793 \\ & 0271588610123920532875 15012934241370540204 \\ & 5814598714979387232141014703227794586499817945633390592 \end{aligned}$$

$$\text{m}^{**e} \bmod 4601 = 4583$$

مسئله 8

$p = 5, q = 11$ a) $n = p^*q = 55, z = (p-1)(q-1) = 40$ b) $e = 3$ کمتر از n که هیچ عاملی از n ندارد. ج) $d = 27$

د) $m = 8, me = 512$ من رمز $c = m \mod n = 17$

مسئله 9

آلیس	باب
کلید مخفی:	SA
کلید عمومی:	$TA = (g^A \cdot SA) \mod p$
کلید مشترک:	$S = (TB \cdot TA)^{-1} \mod p$

$$\begin{aligned} a) S &= (TB \cdot SA)^{-1} \mod p = ((g^A \cdot SB)^{-1} \mod p)^{-1} \mod p = (g^{-(A+B)} \mod p)^{-1} \mod p \\ &= ((g^A \mod p)^{-1} \cdot SB)^{-1} \mod p = (TA^{-1} \cdot SB)^{-1} \mod p = S' \end{aligned}$$

(ب و ج) $p = 11, g = 2$

آلیس	باب
کلید مخفی:	$SA = 5$
کلید عمومی:	$TA = (g^A \cdot SA) \mod p = 10$
کلید مشترک:	$S = (TB \cdot TA)^{-1} \mod p = 1$

د)

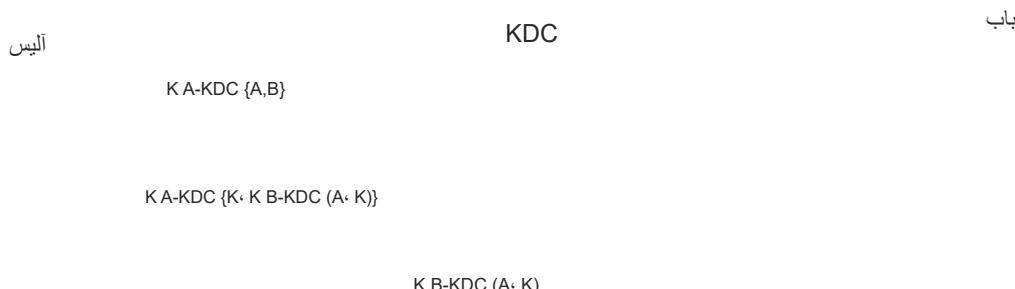


ممکن است توسط انسان در وسط مورد حمله قرار گیرد Diffie-Hellman الگوریتم رمزگذاری کلید عمومی.

1. را برای باب (TT) را دریافت می کند و ارزش عمومی خود (TA) در این حمله، ترودی ارزش عمومی آلیس می فرستد.
2. می فرستد (TT) را ارسال می کند، ترودی کلید عمومی او را برای آلیس (TB) هنگامی که باب ارزش عمومی خود.
3. و ترودی و باب بر روی کلید مشترک دیگر (S AT) بنابراین ترودی و آلیس در مورد یک کلید مشترک BT توافق دارند.

4. S پس از این تبادل، ترودی به سادگی هر پیامی را که توسط آلیس یا باب ارسال می شود توسط کلیدهای عمومی AT و $S BT$ رمزگشایی می کند.

مسئله 10



ارتباط K باب و آلیس اکنون با استفاده از کلید جلسه متقاضی برقرار می کند

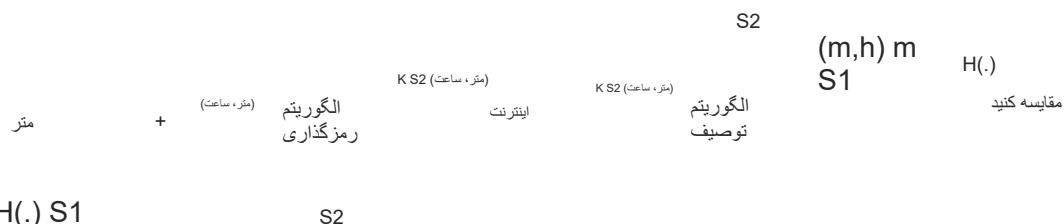
مسئله 11

پیام

من	O	U	1
9	0	.	9
0	ب	O	ب

همان چک سام را دارد

مسئله 12



$H(\cdot) S1$

$S2$

مسئله 13

SHA-**MD5** یا (با) فایل به بلوک هایی با اندازه مساوی تقسیم می شود. برای هر بلوک، هش را محاسبه کنید. هش های همه بلوک ها در فایل تورنت ذخیره می شوند. هر زمان که یک همتا یک بلوک را دانلود می کند، هش این (1) بلوک را محاسبه می کند و آن را با هش موجود در فایل تورنت مقایسه می کند. اگر دو هش برابر باشند، بلوک معتبر است. در غیر این صورت، بلوک جعلی است و باید دور اندخته شود.

مسئله 14

همه روت‌ها در OSPF با مقامات صدور گواهی نیاز دارند. برای (PKI) امضای دیجیتال به زیرساخت کلید عمومی روی هر روتر مستقر کند PKI یک دامنه قرار دارند، بنابراین مدیر می تواند به راحتی کلید متقاضی را بدون نیاز به

مسئله 15

دارند که برای ترویج KA-B باب نمی داند که در ابتدا با ترویج صحبت می کند یا آليس. باب و آليس یک کلید مخفی ناشناخته است. ترویج از باب می خواهد که او (ترویج) را به عنوان آليس تأیید کند. ترویج قرار است باب خود را احراز هویت کند و منتظر می ماند تا باب شروع کند: 1. باب به ترویج: تفسیر "من باب هستم": باب شروع به احراز هویت می کند. باب

احراز هویت خود به طرف دیگر سپس برای چند مرحله متوقف می شود.

ترویج به باب: "من آليس هستم" تفسیر: ترویج شروع به احراز هویت خود به عنوان آليس می کند. 2.

K باب به مرحله 2 با ارسال یک نанс در پاسخ پاسخ می دهد. ترویج هنوز "R" تفسیر: را نمی داند، بنابراین هنوز نمی تواند پاسخ دهد (R AB).

ترویج به مرحله 1 پاسخ می دهد و اکنون احراز هویت باب را ادامه می دهد، و به: "R" تفسیر: عنوان نقطه ای برای رمزگذاری باب انتخاب می کند، دقیقاً همان مقداری که باب برای رمزگذاری در مرحله 3 برای او فرستاده بود.

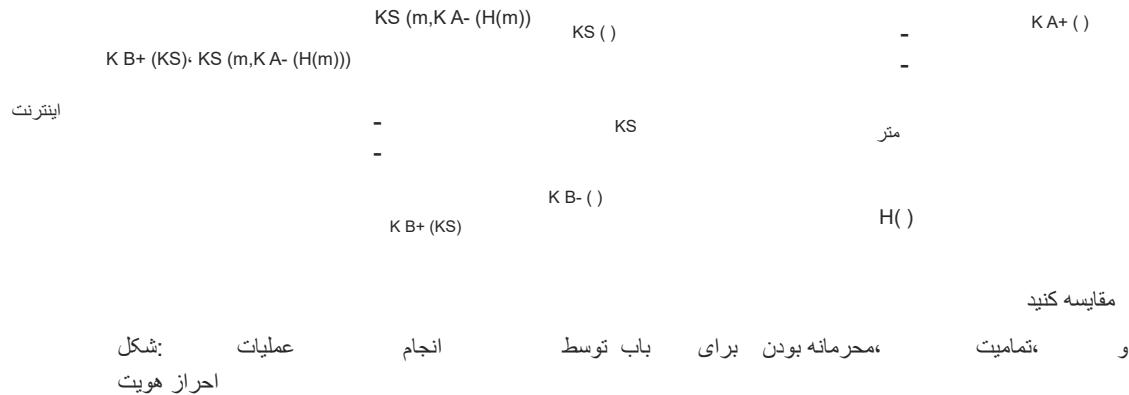
5. Bob-to-Trudy: "K AB nonce" باب احراز هویت خودش را به طرف دیگر با رمزگذاری (R) دارد. (توجه: او K AB مرحله 4 فرستاده بود تکمیل می کند. ترویج اکنون ندارد و نیازی ندارد KAB را دارد.)

که باب در مرحله 3 در بالا R ترویج احراز هویت خود را تکمیل می کند و به "R" (R) پاسخ می دهد. از آنجایی که ترویج نونس رمزگذاری شده ای را که باب در مرحله 3 (R) ارسال کرده بود با ارسال می کند، برگردانده است، باب فکر می کند ترویج آليس است!

مسئله 16

این واقعاً مشکل را حل نمی کند. همانطور که باب فکر می کند (به اشتباہ) در نیمه اول شکل 7.14 در حال احراز هویت آليس است، ترویج نیز می تواند آليس را فریب دهد که فکر کند (به اشتباہ) او در حال احراز هویت باب است. ریشه مشکلی که نه باب و نه آليس نمی توانند بگویند کلید عمومی است که آنها دریافت می کنند، در واقع کلید عمومی آليس باب است.

مسئله 17



مسئله 18

- (الف) خیر، بدون یک جفت کلید عمومی-خصوصی یا یک راز از پیش به اشتراک گذاشته شده، باب نمی تواند تأیید کند که آلیس پیام را ایجاد کرده است.
- (ب) نه، آلیس به سادگی پیام را با کلید عمومی باب رمزگذاری می کند و پیام رمزگذاری شده را برای باب می فرستد.

مسئله 19

- (الف) مشتری ب IP: 216.75.194.220 پورت: 443 (ج) 283
- (د) 3 رکورد
- (ز) 6
- آخرین بایت: bc;29: f. شده است

مسئله 20

TCP اعداد دنباله ای را ارائه نمی دهد. فرض کنید ترددی، یک زن در وسط، یک بخش SSL مجددًا فرض می کنیم که را حذف کند. برای اینکه باب کاری انجام ندهد، ترددی باید اعداد دنباله ای را در بسته هایی را در بسته های بعدی ارسال شده از آلیس به باب و اعداد تأیید ارسال شده از باب به آلیس را نیز تنظیم کند. نتیجه این خواهد بود که باب، ناگاهانه، مقدار یک بسته بایت را در جریان بایت از دست خواهد داد.

مسئله 21

ناموفق خواهد بود (مشترک استفاده می کند MAC که از یک کلید) خیر، بسته جعلی در بررسی یکپارچگی.

مسئله 22

- الف) ج ب) ت
ج) ت د) ف

مسئلہ 23

تکراری را، **ESP**، هنگام بررسی شماره ترتیب در هدر R2، اگر تردی زحمت تغییر شماره ترتیب را به خود ندهد ناموفق خواهد بود R2 تشخیص می‌دهد. اگر تردی عدد توالی را افزایش دهد، بسته در بررسی یکارچگی در

24 مسئلہ

..... جریان کلید 111110100000 = 11، (الف) از آنجایی که

$m = 10100000$ با توجه به
 $1010 \text{ XOR } 0000 = 1010$ این سه فیلد
 عبارتند از:

IV: 11 10100000 پیام رمزگذاری شده: XOR 11111010 =
 01011010 ICV 1010 رمزگذاری شده: XOR 0000 = 1010

.....را استخراج کرده و جریان کلید 111110100000 (11) VII ب) گیرنده

XOR 11111010 = پیام رمزگذاری شده را با جریان کلید برای بازبایی پیام اصلی: XOR 01011010 = 10100000

ICV را بازیابی کند تا XOR رمزگذاری شده را با چریان کلید

1010 XOR 0000 = 1010

XOR 0000 = XOR 1010 می کند: 4 بیت اول پیام بازیابی شده را با 4 بیت آخر آن (بازیابی شده است) ICV که برایر (با) 1010

بیت اول پیام با 4 بیت آخر پیام محاسبه می شود، بیت اول یا بیت 5 پیام باشد XOR به عنوان ICV (ج) از آنجایی که را انجام دهد ICV برگردانده شود تا سنته دریافتی برسی.

د) برای قسمت (الف)، پیام رمزگذاری شده 01011010 بود که بیت اول 11011010، باینری گردانید.

XOR این پیام را با جریان کلید: 11011010
1111010 = 00100000

دربافتی توسط گیرنده 0010 است ICV رمزگذاری شده را برگرداند، مقدار ICV اگر ترودی اولین بیت از

XOR را دریافت کند: ICV 0010 می کند تا XOR گیرنده این مقدار را با جریان کلید 0000 = 0010

که برابر با) XOR 0000 = 0010 ICV را از پیام بازیابی شده محاسبه می کند: ICV 0010 گیرنده اکنون عبور می کند ICV بازیابی شده است و بنابراین بسته دریافتی از بررسی

مسئله 25

جدول فیلتر:

عمل	آدرس منبع	آدرس مقصد	پروتکل	پورت منبع	پورت مقصد	بیت پرچم	اتصال را بررسی کنید
اجازه	222.22/16	خارج از 222.22/16	TCP	> 1023	23	هر	
اجازه		خارج از 222.22/16	TCP	23	> 1023	ACK	ایکس
اجازه		خارج از 222.22/16	222.22.0.12 TCP	> 1023	80	هر	
اجازه 222.22.0.12 خارج از 222.22/16			TCP	80	> 1023	هر	
انکار	همه	همه	همه	همه	همه	همه	

جدول اتصال:

آدرس منبع	آدرس مقصد	پورت منبع	پورت مقصد
222.22.1.7	37.96.87.123	12699	23
222.22.93.2	199.1.205.23	37654	23
222.22.65.143	203.77.240.43	48712	23

مسئلہ 26

ا)

الیس

K 1+ (S 1
))

پروکسی

1

(ب)

الیس

S 1 (K 2+ (S 2
))

پروکسی

1

پروکسی

2

K 2+ (S 2)

ج)

الیس

S 1 (S 2
(قیمت))

پروکسی

1

پروکسی

2

S 2
(قیمت)

Activist.com

قیاس

S1 (S 2
((صفحہ))

S 2
(صفحہ)

صفحہ

فصل 9 سوالات مروری

یک مدیر شبکه می‌خواهد قابلیت‌های مدیریت شبکه را داشته باشد که (الف) یکی از اجزای شبکه از کار بیفتد، ۱. (ب) یکی از اجزای شبکه در شرف از کار افتادن است، و در حال عملکرد "پوست" (ج) یک جزء از شبکه است. از با پر DOS نقطه نظر امنیتی به خطر افتاده است و به شبکه حمله می‌کند، به عنوان مثال، با راه اندازی یک حمله کردن شبکه با بسته ها، (د) سطح ترافیک از یک آستانه معین در یک پیوند فراتر می‌رود، و باعث می‌شود بسته ها حذف شوند، (ه) همه چیز بدون مشکل اجرا می‌شود (برای اینکه بدانید همه چیز به خوبی پیش می‌رود و هیچ مشکلی وجود ندارد). بسیاری وجود دارد.

دلایل اضافی نیز

۲. مدیریت عملکرد، مدیریت خطأ، مدیریت پیکربندی، مدیریت حسابداری، مدیریت امنیت.

مدیریت شبکه تعریف محدودتری دارد، زیرا بر منابع موجود در شبکه متمرکز است - ناظارت بر عملکرد آنها و ۳. کنترل عملکرد آنها. این منابع به روش‌های مختلف برای پیاده سازی خدمات ترکیب می‌شوند (استفاده می‌شوند). توجه داشته باشید که در حالی که منابع شبکه ممکن است همه آنطور که باید کار کنند، ممکن است برای اجرای یک سرویس با سطح عملکرد معین کافی نباشند. این نگرانی اخیر جنبه‌ای از مدیریت خدمات است.

۴.

نهاد مدیریت: جمع آوری، پردازش، تجزیه و تحلیل، نمایش اطلاعات مدیریت شبکه را کنترل می‌کند و توسط مدیر شبکه برای کنترل دستگاه‌های موجود در شبکه استفاده می‌شود.

دستگاه مدیریت شده: قطعه‌ای از تجهیزات شبکه که تحت کنترل نهاد مدیریت است.

عامل مدیریت: یک فرآیند نرم افزاری که بر روی یک دستگاه مدیریت شده اجرا می‌شود که با نهاد مدیریت ارتباط برقرار می‌کند و در دستگاه مدیریت شده تحت کنترل نهاد مدیریت اقدام می‌کند.

قطعاتی از اطلاعات مرتبط با تمام اشیاء مدیریت شده در یک دستگاه: MIB.

پروتکل مدیریت شبکه: بین نهاد مدیریتی عوامل مدیریت در دستگاه‌های مدیریت شده اجرا می‌شود و به عوامل اجازه می‌دهد تا نهاد مدیریت را در مورد مشکلات احتمالی آگاه کنند و به نهاد مدیریت اجازه می‌دهد تا دستورات را برای عوامل مدیریت ارسال کند.

۵. SMI استفاده می‌شود SNMP یک زبان تعریف داده است که برای تعریف قطعات اطلاعات در یک

پیام تله توسط عامل مدیریت برای نهاد مدیریت ارسال می‌شود (و نیازی به پاسخگویی از طرف نهاد مدیریت ندارد). یک پیام درخواست-پاسخ توسط نهاد مدیریت ارسال می‌شود که پاسخ آن از طرف عامل مدیریت ارسال می‌شود.

7. GetRequest، GetNextRequest، GetBulkRequest، SetRequest، InformRequest، پاسخ، دام

است که ارسال، پردازش، احراز هویت، کنترل دسترسی و به موقع SNMP بخشی از پیاده سازی SNMP موتور 8. را مدیریت می کند. شکل 8.5 SNMP بودن پیام های

یک راه استاندارد برای نامگذاری اشیا ارائه می دهد ASN.1 درخت شناسه شی.

نقش لایه ارائه اجازه ارسال و دریافت داده ها در قالبی مستقل از ماشین (یعنی بدون توجه به ذخیره سازی و 10. قراردادهای معماری خاص فرستنده و گیرنده) است

اینترنت لایه ارائه ندارد.

بر عهده مجریان است

پروتکل هایی برای اطمینان از ارسال و دریافت داده ها در فرمت دلخواه.

هر قطعه داده با نوع، طول و مقدار خود برچسب گذاری می شود، TLV در رمزگذاری.

فصل 9 مسائل

مشکل 1

حالت پاسخ به درخواست عموماً به دلایل مختلفی سربار بیشتری دارد (بر حسب تعداد پیام های رد و بدل شده انداز مگیری می شود). اول، هر بخش از اطلاعات دریافت شده توسط مدیر نیاز به دو پیام دارد: نظرسنجی و پاسخ. تله گذاری تنها یک پیام را برای فرستنده ایجاد می کند. اگر مدیر واقعاً نخواهد زمانی که شرایطی رخ می دهد به او اطلاع داده شود، نظرسنجی هزینه بیشتری دارد، زیرا بسیاری از پیام های نظرسنجی ممکن است نشان دهند که شرایط انتظار هنوز رخ نداده است. به دام انداختن تنها زمانی پیامی ایجاد می کند که شرایط رخ دهد.

همچنین در صورت وقوع یک رویداد بالافاصله به مدیر اطلاع می دهد. با نظرسنجی، مدیر باید نیمی از Trapping چرخه نظرسنجی (به طور متوسط) بین زمان وقوع رویداد تا زمانی که مدیر متوجه شود (از طریق پیام نظرسنجی خود) که رویداد رخ داده است، صبر کند.

اگر پیام تله گم شود، دستگاه مدیریت شده کپی دیگری ارسال نخواهد کرد. اگر پیام نظرسنجی یا پاسخ آن گم شود، مدیر می داند که پیامی گم شده است (زیرا پاسخ هرگز نمی رسد). از این رو مدیر می تواند در صورت نیاز دوباره نظرسنجی کند.

مشکل 2

اگل، زمانی که مدیریت شبکه بیشترین نیاز را دارد، در موقع استرس است، زمانی که شبکه ممکن است به شدت شلوغ باشد می شود که TCP کنترل ازدحام، روی SNMP شود و بسته ها در حال از دست رفتن هستند. با اجرای SNMP عقب نشینی کند و ارسال پیام را دقیقا در زمانی که مدیر شبکه نیاز به ارسال پیام دارد متوقف کند.

مسئله 3

1.3.6.1.2.1.5

مشکل 4

فرمت های فایل مایکروسافت تحت 1.2.840.113556.4 هستند (به بخش 8.3.2 مراجعه کنید)

مشکل 6

اگر مقدار قبل از طول باشد، این احتمال وجود دارد که طول را به اشتباه تفسیر کنیم تا بخشی از مقدار باشد.

مسئله 7

47Michael21 '10100101'

مسئله 8

47Sridhar 21 '10010001'