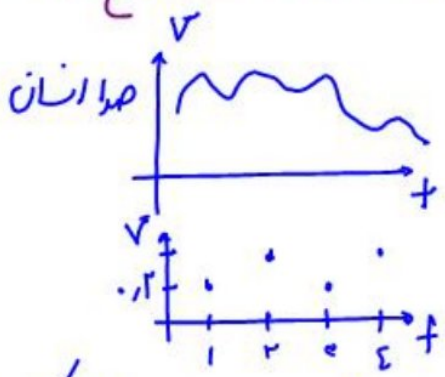
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

انتقال داده ها (Data communication) : انتقال داده ها به آنالوگ و یا دیجیتال توسط سیگنال ها انجام می شود.

- داده ها به دو شکل در شبکه های کامپیوتری می توانند رد و بدل (دیده) می شوند
  - آنالوگ (پیوسته)
  - دیجیتال (۰ و ۱)

- بیان دیگر جمله اول: داده های دیجیتال و آنالوگ به شکل موج (wave) بر روی رسانه ها منتشر می شوند
  - رسانه ها: سیم مسی، فیبر نوری، هوا

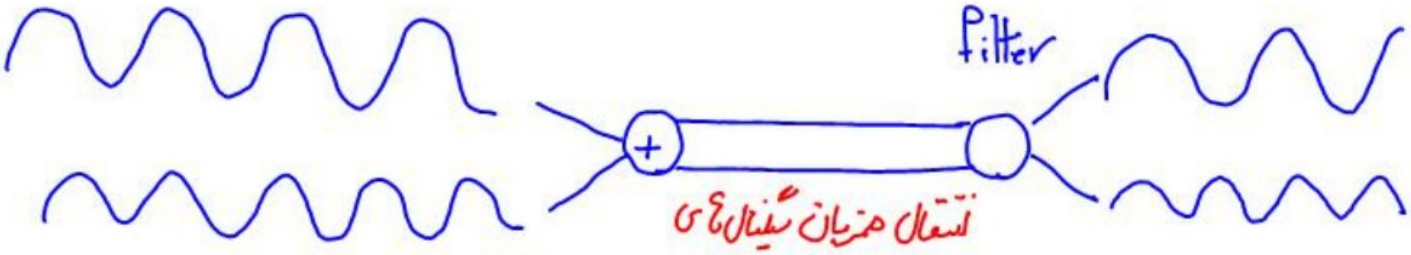


آنالوگ: یک سیگنال پیوسته در زمان

دیجیتال: ... گسسته ...

- نکته: ما واقعا line دیجیتال نداریم در دنیا خارج و هر line فیزیکی با ۲ خروجی یک موج آنالوگ روی آن جابجا می شود

آنالوگ ← در درس شبکه سیگنال ها قرار است بیت ارسال کنند ← هر سیگنالی یک مقداری بیت ارسال می کند ← سیگنال ها را می توانیم با هم ترکیب کنیم و روی یک رسانه ارسال کنیم ← در اینصورت مقدار بیتی که روی کانال قرار می گیرد برابر مجموع بیت هایی ارسالی هر یک از این سیگنال ها است



انتقال همزمان سیگنال های مختلف بر روی یک لینک فیزیکی مشترک

اشتراک منابع

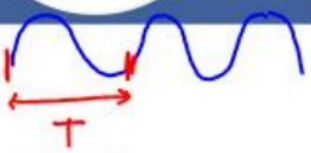
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir



$(S)\ T = \frac{1}{f}$

$(Hz)\ f = \frac{1}{T}$

نکته - سیگنال ها در حوزه زمان به ۲ دسته تقسیم می شوند: پریودیک / غیر پریودیک

- هر سیگنال غیر پریودیک را می توان با ترکیب هایی پریودیک فرض اش کنیم
- در درس شبکه های کامپیوتری به آنالیز سیگنال های پریودیک پرداخته می شود
- همه سیگنال های رونیک از جمع یک عالمه سیگنال های رونیک کسینوسی (موج های کسینوسی) تشکیل شده

* پهنا باند هم برای سیگنال تعریف می شود و هم برای کانال

۱- پهنا باند کانال : فاصله بین کمترین و بیشترین فرکانسی که از یک کانال (لینک) عبور می کند

W = Band width channel = پهنا باند کانال (Hz) $= f_{max} - f_{min}$

* پهنا باند کانال یک مفهوم آنالوگ است.

پهنا باند چشم انسان: چشم یک کانال است که تصویر از آن عبور می کند $= W_{چشم} = 10^{15} - 10^{14} = 9 \times 10^{14}$ Hz

پهنا باند گوش انسان = گوش یک کانال است که صدا از آن عبور می کند $= W_{گوش} = 20\,KHz - 20\,Hz = 19980\,Hz \simeq 20\,KHz$

نکته) در شبکه های کامپیوتری در بسیاری از کانال ها فرکانس قابل عبور از کانال به ۰ نزدیک است و بنابراین در محاسبه پهنا باند کانال می توان از آن چشم پوشی کرد. بنابراین در برخی از مسائل کانال را مثل یک پایین گذر (low pass) در نظر می گیرند.

نکته) پهنا باند یک کانال پایین گذر، برابر است با بیشترین فرکانسی که از کانال عبور می کند

$W = f_{max} = high$

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

۲ - پهنا باند سیگنال : برای تعریف پهنا باند سیگنال ها از آنالیز فوریه استفاده می‌کنیم، منظور از پهنا باند یک سیگنال پریودیک محدوده فرکانسی مولفه‌های آن است. $w = f_{high} - f_{low}$

مثال - سیگنالی داریم از فرکانس ۵ تا ۱۵ کیلوهرتز ← پهنا باند این سیگنال = ۱۰ KHZ

کانالی داریم که فرکانس ۰ تا 12KHZ از خودش عبور میدهد ← پهنا باند کانال = 12KHZ

* دقت کنید پهنا باند سیگنال من لزوما پهنا باند کانال من کمتر است ولی فقط فرکانس های ۵ تا ۱۲ کیلوهرتز سیگنال از کانال عبور می‌کند

نکته - بطور پیش فرض سیگنال ها و کانال ها را low pass در نظر میگیریم

۳ - پهنا باند دیجیتال = Bit rate = transmission rate = نرخ بیت (bps) = R

یک مفهوم دیجیتال است

تعریف: تعداد بیت هایی که در ۱ ثانیه توسط یک لینک منتقل می‌شود ← در واقع دارد سرعت خط را به ما نشان میدهد

* دیتایی که عبور می‌کند ۵ دیتا مفید + دیتا غیر مفید

۴ - بهره وری = η : $\eta = \frac{\text{بخش مفید}}{\text{کل داده}} \times 100\%$

۵ - رابطه بین پهنا باند و نرخ بیت : رابطه خطی (مستقیم) دارند باهم ↑ پهنا باند = ↑ نرخ بیت

مثال: اگر پهنا باند ۴ برابر شود، نرخ بیت نیز ۴ برابر می‌شود

فرمول شانون = $R = w \log_2^{1+\frac{S}{N}}$

فرمول نایکوئیست = $R = 2w \log_2^{M}$

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

۶- گذردهی (Throughput) : نرخ بیت مفیدی که به گیرنده تحویل داده می‌شود = γ = گذردهی

bps

گذردهی این لینکی برابر ۲Gbps است = 2×10^9 bps : این تعداد بیت مفید در ثانیه از لینک عبور می‌کند

۷- $\gamma = R \times \eta$

بهره وری یا راندمان کانال

سوال - بهره وری یک لینک ۹۰ درصد است اگر Bit rate کانال ۲Gbps باشد، گذردهی چقدر است؟

$$\gamma = 2\text{Gbps} \times \frac{9}{10} = 2 \times 10^9 \frac{b}{s} \times \frac{9}{10} = 18 \times 10^8 \frac{b}{s} = 1800 \text{Mb/s}$$

توجه) K و M و G و ... در شبکه بصورت $K = 10^3$ و $M = 10^6$ و $G = 10^9$ و در معماری کامپیوتر و OS $K = 2^{10}$ و $M = 2^{20}$ و $G = 2^{30}$

یادآوری: داده ها به شکل موج بصورت رسانه ها منتشر می‌شوند

- رسانه ها از یک منظر به ۲ دسته هدایت شونده (باسیم) و غیر هدایت شونده تقسیم می‌شوند (بی‌سیم)

هدایت شونده : ۱- coaxial cable : کابل هم محور ، شبکه آنتن تلویزیون

۲- Twisted pair : زوج سیم بهم تابیده شده ← برای کم شدن نویز بهم می‌تابانند

۳- Fiber optic

غیرهدایت شونده : ۱- هوا : WiFi

۲- آب :

۳- خلا : مرجع بررسی انتشار حتما نیاز به ماده ندارد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

- انواع موج ها: موج ها انواع گوناگونی دارند که در شبکه ۲ مورد آن را بررسی می‌کنیم

۱- موج مکانیکی، مثل صدا ← خواص امواج مکانیکی ← نیاز به ماده برای انتشار / سرعت انتشارشون کند است ← مثلاً سرعت صدا $340 \frac{m}{s}$ است.

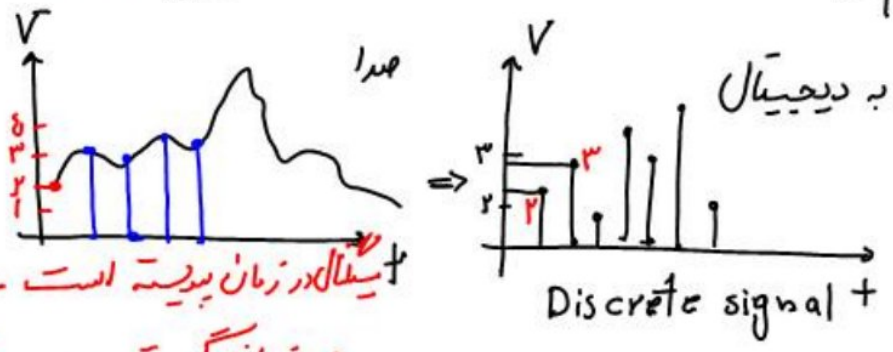
۲- امواج الکترومغناطیس ← نیاز به ماده برای انتشار ندارد / سرعت بسیار بالا: $3 \times 10^8 \frac{m}{s}$

داده ← آنالوگ / دیجیتال

A/D
D/A
D/D
A/A
← مدولاسیون

- کاری است که بتوانیم داده‌های آنالوگ را به دیجیتال و بالعکس تبدیل کنیم

تبدیل سیگنال آنالوگ به دیجیتال



سیگنال در زمان پیوسته است ← تبدیلش کنیم به در زمان گسسته ← sampling

تبدیل سیگنال آنالوگ به دیجیتال:

۱- sampling: نمونه برداری: با یک فرکانس ثابت بنام فرکانس سمپلینگ (f_s) نمونه برداری می‌کنیم

نکته) با این کار یک سیگنال پیوسته در زمان را به یک سیگنال گسسته در زمان تبدیل می‌کنیم ← بتوانیم روی خط داده را ارسال کنیم ← بی‌نهایت نقطه نمی‌شود

چرا باید نمونه برداری کنیم؟

نکته) طبق قضیه نایکوئیست اگر یک سیگنال آنالوگ را که پهنا باندش ... است با نرخ ... نمونه برداری کنیم دقیقاً می‌توانیم موج را بعداً بازسازی کنیم

نکته) اگر فرکانس sampling را کمتر از دو برابر پهنا باند بگیریم می‌گویند Aliasing distortion

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

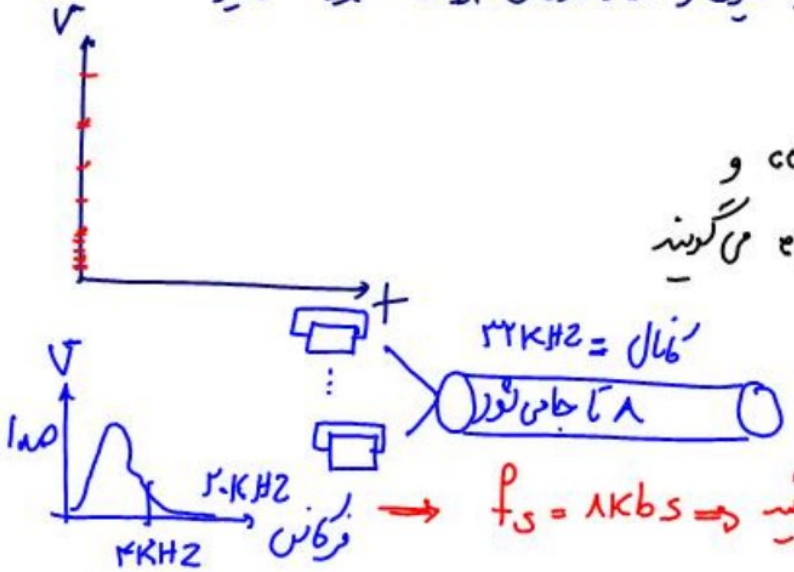
۲- کوانتیزاسیون (Quantization) : ذخیره اعداد حقیقی خیلی جا می‌گیرد و ارسال این هم خیلی پهنا باند مصرف می‌کند، بنابراین هدف کوانتیزاسیون این است که در مصرف حافظه و Bit rate صرفه جویی شود ← ۷ها را گسسته درنظر می‌گیریم ← هر sample به نزدیکترین عدد مجموعه ۷ گرد می‌کنیم

← خطا یا نویز کوانتیزاسیون ← با این کار اعوجاج به وجود می‌آید: quantization distortion

- برای خطا کوانتیزاسیون ۲ راه اصلی وجود دارد { ۱- افزایش تعداد بیت‌ها در نمونه
expanding + compression = companding ۲

* وقتی دامنه‌ها quantizer هم یکسان باشند این کوانتیزاسیون را uniform یا linear می‌گویند در ویدیو معمولاً از linear استفاده می‌شود، اما در audio چون گوش انسان به دامنه‌های کوچک حساسیت بیشتری دارد می‌آیند و دامنه کوانتیزاسیون را در دامنه‌های بزرگ، بزرگ می‌گیرند و در دامنه‌های کوچک، کوچک

- فشرده کردن دامنه‌ها را compression و
باز کردن ... یا این را expanding می‌گویند



$f_s = 8Kbs$ ⇒ ۸۰۰۰ سمپل در ثانیه ⇒ هر سمپل با ۸ بیت ⇒ 64Kbs ذخیره می‌شد

۳- کد کردن باینری (Binary encoding)

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

شبکه: هرگاه تعدادی عضو در یک مجموعه در ارتباط با یکدیگر قرار گیرند یک شبکه به وجود می آید، به هر عضو شبکه یک نود (node) و به هر خط ارتباطی یک یال (edge) گفته می شود

مثال: شبکه آب رسانی شهری، شبکه حمل و نقل شهری، شبکه های اجتماعی، شبکه های مخابراتی و شبکه های کامپیوتری

= Data Network = computer network

دو یا چند کامپیوتر مستقل (Autonomous یا خودگردان) که با یک تکنولوژی واحد به هم وصل شده اند (interconnect) به منظور اشتراک منابع و یا تبادل داده

- در خصوص اشتراک منابع، منابع می توانند
  1- دیتا باشند
  2- Hardware
  3- سرویس (service)

- تعریف Autonomous & کامپیوتری که حتما توسط مالک اش کنترل بشود ← توسط شبکه کنترل نشود

- نکته) زمانی که می گوییم چندتا کامپیوتر به هم interconnect شده اند این به این معنا نیست که حتما بین شون لینک مستقیم وجود دارد، و به این معناست که قادرند با یکدیگر تبادل اطلاعات کنند و ممکن است بین شون صدها روتر و سوئیچ و لینک باشد.

نکته - شبکه های مختلف با سایزها و استانداردها و اهداف خاص وجود دارند که با اتصال شبکه ها به یکدیگر شبکه های بزرگتری (شبکه ای از شبکه ها) ایجاد می شوند ← که اینترنت نیز که بزرگترین شبکه دنیاست نمونه ای از این مسئله است.

نکته - در گذشته وقتی صحبت از شبکه های کامپیوتری می شد، منظورشان اتصال های دستگاه های کامپیوتری به هم بود، ولی امروزه، گره ها هر چیزی می توانند باشند: اتومبیل، تلویزیون، تابلو، ساعت هوشمند و ... : IoT حدود ۲۵ میلیارد وسیله به اینترنت وصل است

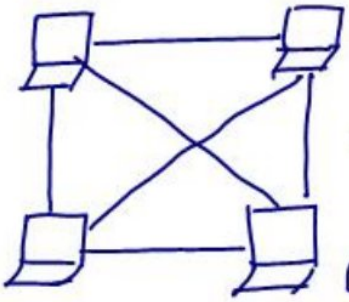
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

- شبکه‌های کامپیوتری چطور شکل گرفت

مدل ۱:



(۱) ⇒ شبکه مش کامل

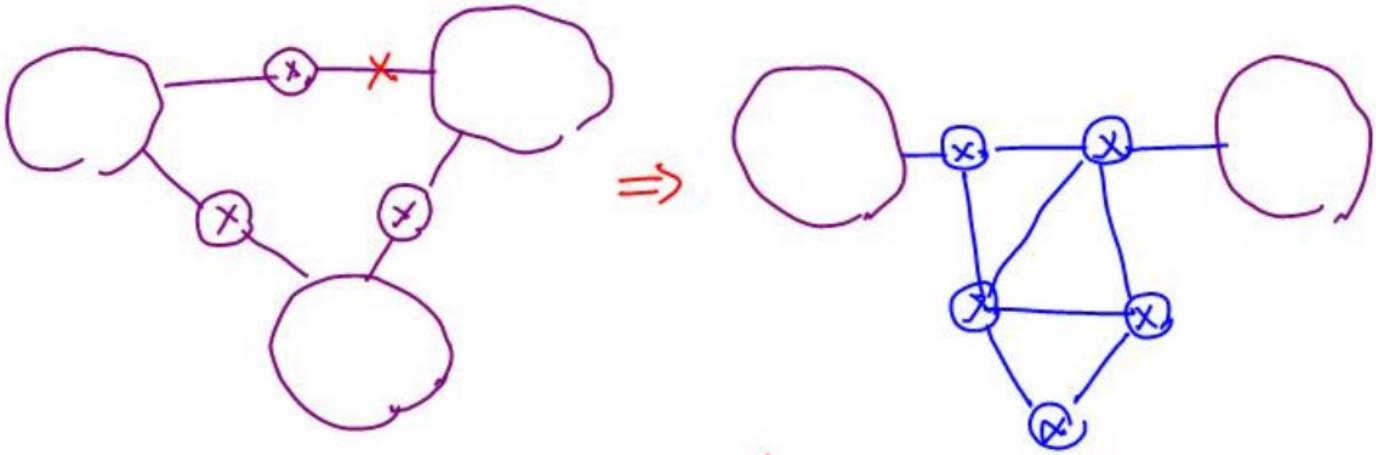
scalable نیست

تعداد لینک‌ها = $1+2+\cdots+n-1 = \frac{n(n-1)}{2} \in O(n^2)$

چندین ایراد وارد شبکه‌های مش:
۱- راه‌اندازی اش سخت بود
۲- مقدار زیادی کابل استفاده می‌شود
۳- مقیاس پذیر نیست

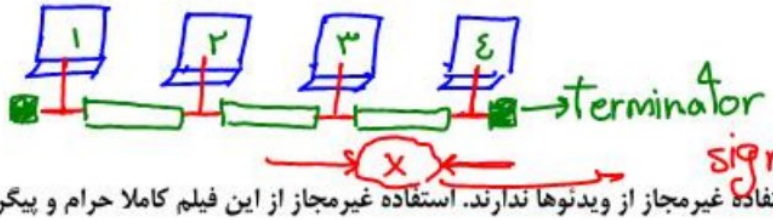
مزیت: قابلیت اطمینان بالاست
point of failure ندارد

درحد LAN یه مش تو LAN به درد نمی‌خورد
درحد شبکه زیر ساخت اینترنت: خیلی خوبه



(۲) در بحث LAN به این نتیجه رسیدند که بیایند وایک کابل به اسم Backbone را بعنوان هسته

coaxial cable



اعلی Network نان در نظر بگیرند

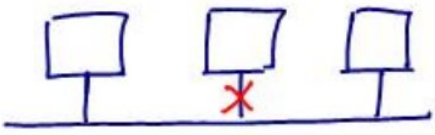
Thin Ethernet

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

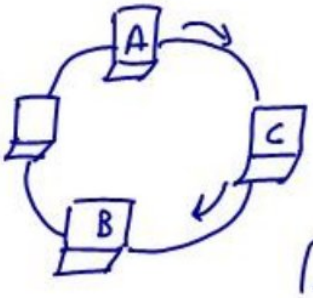
- terminator یک مقاومتی است که در انتها backbone بسته می شود که زمانی که سیگنال را دریافت می کند، سیگنال را Kill می کند
- توپولوژی این شبکه Bus است
- ایرادی که شبکه Thin Ethernet داشت این بود که اگر یک قطعی در Backbone اتفاق بیفتد شبکه به ۲ قسمت مجزا تقسیم می شد و بنابراین شبکه از کار می افتاد

(۳) راه حل: بیایم و backbone را جدا کنیم از اتصال بین کامپیوترها ← هر کامپیوتر مستقلا به backbone متصل شود ← اگر یکی از اتصالات کامپیوترها به backbone قطع شود فقط اتصال همان کامپیوتر با backbone قطع می شود



Thick Ethernet

* همزمان با این کار آمدند در توپولوژی باس بازطراحی کردند

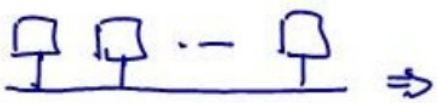


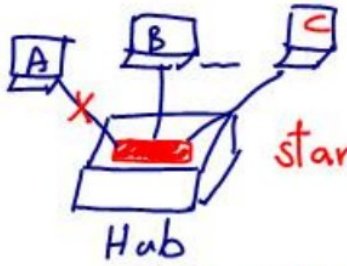
ابتدا و انتها Backbone را هم وصل کنیم ← Ring پدید آمد

← مشکل signal Bounce و استفاده از terminatore را انداریم

(۴) * خطایابی کابل در شبکه های باس سخت بود به شدت آسان تر

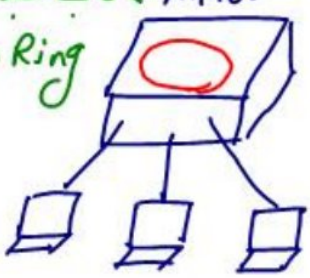
* راه اندازی آسان





هاب شبکه ← MAU

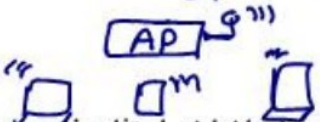
Token Ring



همین ایده در شبکه های Ring هم استفاده شد

MAU = multi station access unit

(۵) در شبکه star بیایم و ارتباط بین دستگاه مرکزی و کامپیوترها را از طریق امواج wireless برقرار کنیم



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

هاب) هاب در شبکه استار همه کامپیوترها را در لایه ۱ بهم وصل می کند

هاب تا لایه ۱ می فهمد ــ فقط ۰ و ۱ را می فهمد، (نمی تواند از این ۰ و ۱ ها فریم بسازد و MAC آدرس دیوس فریم را متوجه بشود) ← پس هاب آن اطلاعاتی را که برای تصمیم گیری برای ارسال می توانه استفاده کند، اطلاعات لایه ۱ (همان سیگنال ها) است ــ پس نمی تواند هوشمند عمل کند

هاب ۲ کار می کند:
۱ــ سیگنال دریافتی را تقویت می کند (Amplify می کند)
۲ــ آن سیگنال تقویت شده را روی همه پورت ها بیرون ارسال می کند

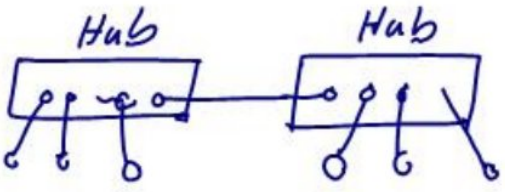
repeater = یک سیگنال را می گیرد و آن را تقویت می کند، وقتی از شبکه باس استفاده می کردیم سیگنال ها دچار افت می شد و ما repeater می ذاشتیم تا مجددا این سیگنال ها را تقویت کنیم

نکته ۱ــ در شبکه هاب نیازی به repeater نداریم

نکته ۲ــ در شبکه Token Ring هم نیازی به repeater نیست چون هر کامپیوتر سیگنال را که می گیرد خودش مجددا آن را درست می کند و برای مقصد بعدی ارسال می کند بنابراین سیگنال ها توسط کامپیوترها تقویت می شوند

نکته ۳ــ repeater دیگر استفاده نمی شود تقریبا

* شبکه های star علاوه بر اینکه خطایابی را راحت کرد، شبکه را scalable کرد



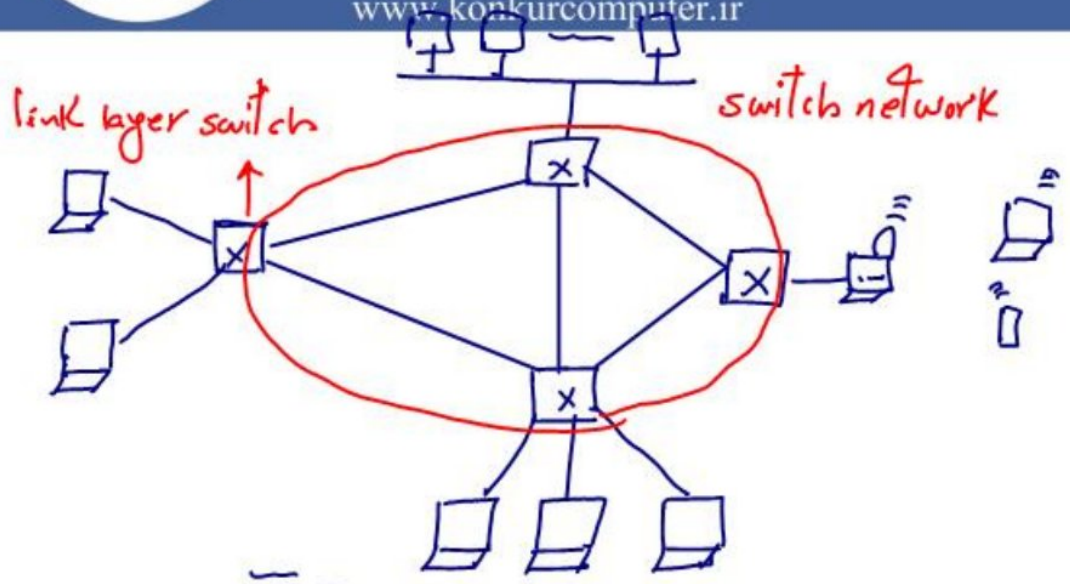
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

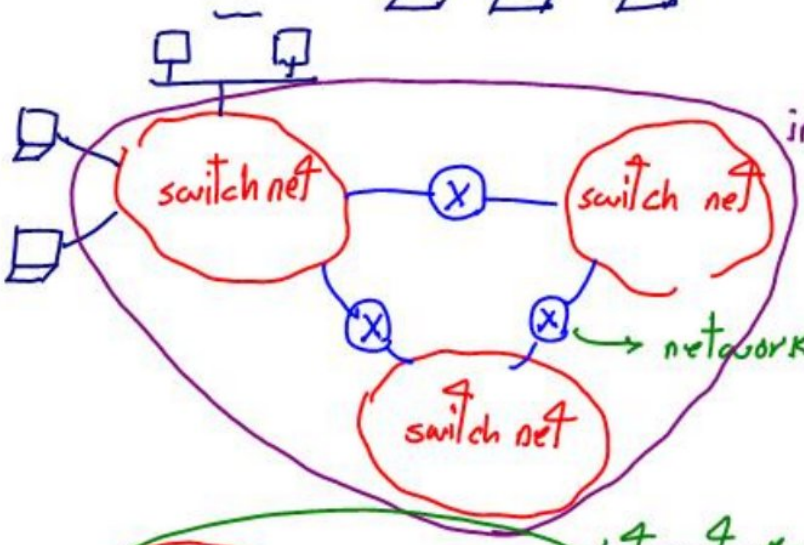
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

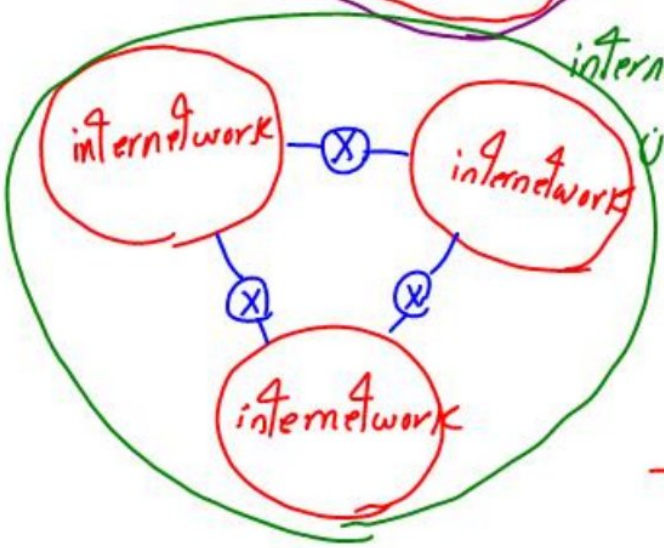
شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir







- از اتصال internetwork ها می‌توان یک internetwork بزرگتری ایجاد کرد و با ادامه دادن به این کار کل جهان را هم متصل کرد به در نتیجه Internet به وجود می آید

سوال ؟ چی شد که مخصوصا این ساختار خوب است ریشه شبکه های دیتا از کجا شکل گرفت ؟

برای پاسخ به این سوال باید برویم و ابتدا نحوه شکل گیری و پیگیری شبکه های مخابراتی را یاد بگیریم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

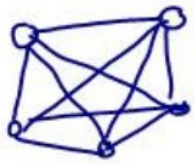
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

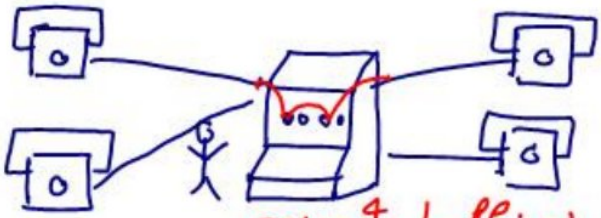
رامین رضوی

- ساختار سلسله مراتبی شبکه های مخابراتی چگونه شکل گرفت

۱- مش کامل : بهدرد نمی خورد



۲-



واقعا سیستم های سنتی بصورت

- در ابتدا مابین سیر فیزیکی از مبدا به مقصد داشتیم ← یک circuit saild : فیزیکی جمع وصل شده بودند

سوئیچ کردن : انتقال یکی از خطوط به یک خط دیگر که دائم جمع وصل نیستند

۳- بجای یک اپراتور انسانی ← دستگاه الکترو مکانیکی ← switch co

توجه) واژه switching از اینجا ابداع شد

توجه) واژه switching در ۲ جا استفاده می شود

* switching شبکه : نحوه انتقال داده ها از طریق یک شبکه از لینک ها و سوئیچ ها بین سیستم های انتهایی
* عمل سوئیچینگ در یک switch : به این عمل forwarding .

انواع switching در شبکه

circuit switching : شبکه تلفن

packet switching

Datagram : شبکه اینترنت

ATM : virtual circuit

ادامه ماجرا :

ایراد این مدل : همه کاربران یک کشور نمی توانند به یک نقطه وصل شوند ← یک سلسله مراتبی از سوئیچ ها داشتند

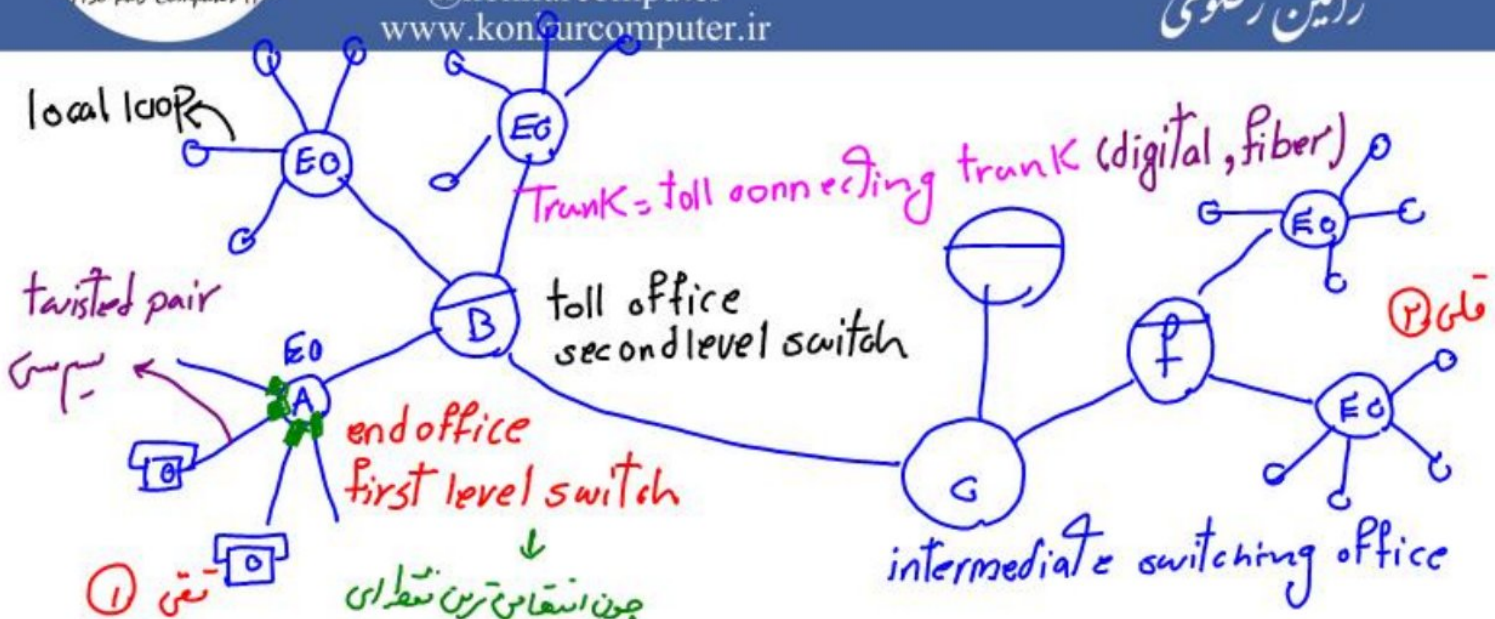
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir



یک سیستم مخابراتی شامل ۳ مولفه است

1- local loop
2- switching centers
3- Trunks

مراحل یک مکالمه تلفنی

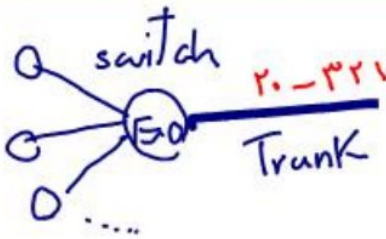
۱- connection setup OR circuit setup : ارسال درخواست ارتباط و برقراری ارتباط : سوئیچ ها برای ایجاد ارتباط باید با هم حرف بزنند
۲- رزرو منابع
۳- مکالمه
۴- خاتمه ارتباط : قطع کردن گوشی و آزاد شدن منابع رزرو شده

نکته) مرکز سوئیچ در شبکه های مخابراتی از پروتکل استک OSI تشکیل شده ۷ لایه بر مبنا

نکته) در حال حاضر اینطور نیست که واقعا یک مدار فیزیکی بین مبدا و مقصد برقرار شود

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

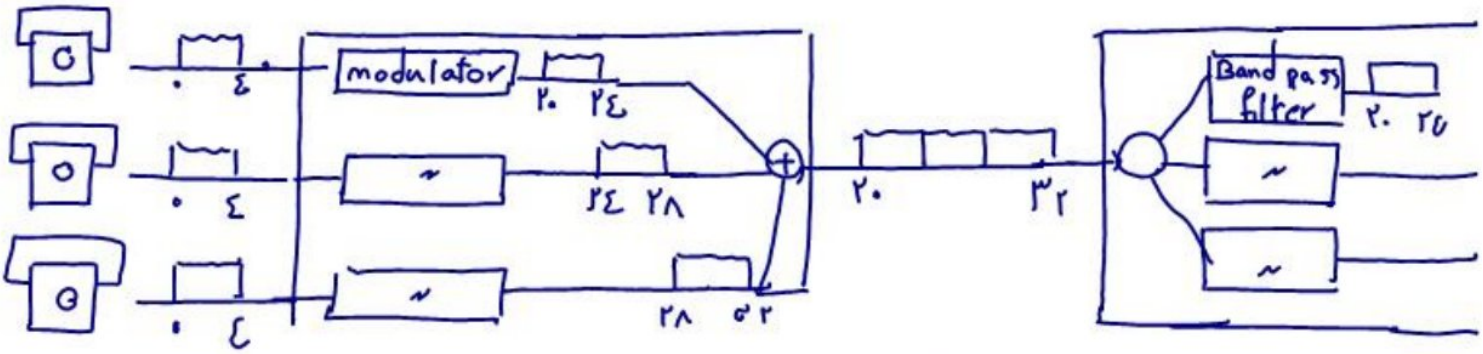
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

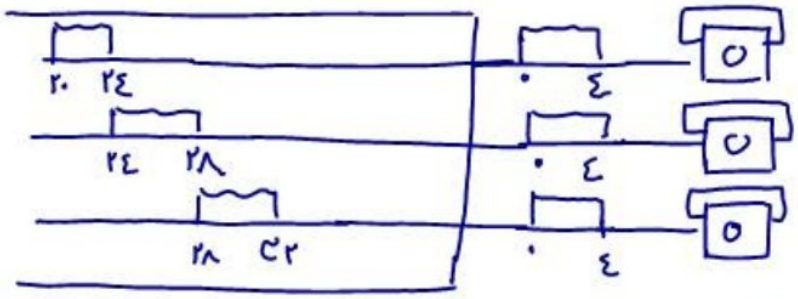


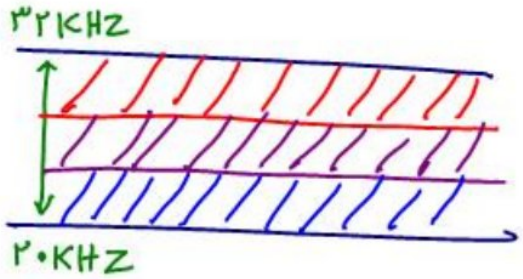
تعریف multiplexing : اشتراک منابع یک شبکه (یک لینک)
مثلاً) برای سیستم های انتقالی ... که مدل های مختلفی دارد :

FDM ، OFDM ، TDM ، WDM ، CDM

FDM







- از منظرهای متفاوتی می توانیم شبکه ها را دسته بندی کنیم

۱- از نظر توپولوژی یا همبندی

۲- " " تکنولوژی انتقال

۳- " " حوزه جغرافیایی تحت پوشش (گستردگی جغرافیایی)

۱ توپولوژی : به ۲ دسته کلی point to point (نقطه به نقطه) و Broad cast (پخشی)

- point to point : بین ماشین های مختلف مسیرهای متفاوتی وجود دارد، برخلاف شبکه های پخشی که فقط یک مسیر (یک کانال) بین همه وجود دارد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

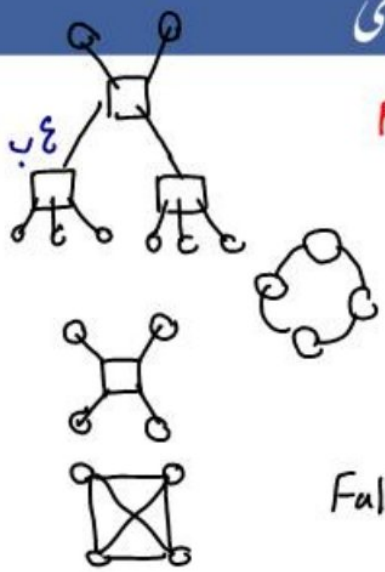
شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

۱- point to point

ب) : این توپولوژی گسترش یافته ستاره است



۱- tree

۲- Ring

۳- star

۴- Full mesh

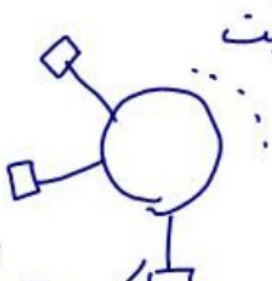
۵- گراف نامنظم

۲- Broad cast : وقتی سیگنال منتشر می‌شود هم می‌تواند آن را ببیند ولی فقط گیرنده‌ای (گیرنده‌هایی) مقصد آن را نگه می‌دارند و بقیه Drop اش می‌کنند

۱- هاوواره

۲- Bus

۳- Ring : (Token Ring)



۲- تکنولوژی انتقال : براساس اینکه آدرس مقصد یک بته چه کسی یا کسانی می‌تواند باشد

- unicast (تک پخشی) : داده به یک مقصد مشخص ارسال می‌شود
- multicast (چند پخشی) : " " " گروه از مقصدهای مشخص ارسال می‌شود
- Broadcast (هم پخشی / پخشی) : داده به تمامی افراد درون شبکه می‌رسد : مثل رادیو، مثل تلویزیون

۳- طبقه‌بندی شبکه‌ها از لحاظ گستردگی جغرافیایی

m : SAN : system area network

۱۰m : PAN : personal " "

۱۰۰m : LAN : Local " "

۱۰۰۰m : CAN : campus " " کمپی محوطه‌ای

۱۰Km : MAN = Metropolitan " " شهری

۱۰۰ - ۱۰۰۰ Km : WAN = wide " " گسترده

GAN = global " " جهانی

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

تعریف اندکی از اینترنت : اینترنت شبکه نیست و شبکه‌ای از شبکه‌ها است به این معنا که شبکه‌های مختلف با استانداردهای مختلف را بهم وصل کرده است.

* شبکه‌ها می‌توانند در لایه‌های مختلف بهم دیگر متصل شوند

repeater در لایه فیزیکی : توسط

Bridge و L_2 switches: Data link " "

Router : Network " "

transport gateway : ۵ و ۴ " "

Application gateway

سوال - یک host برای اتصال به اینترنت چه باید بکند ؟

ما چطوری به اینترنت وصل می‌شویم ؟

هر کس که می‌خواهد به اینترنت وصل شود باید از طریق یک ISP (معمولاً access ISP) به اینترنت وصل شود

ISP مخابرات تهران ← شبکه اپراتور موبایل ← BTS ← با ارتباط وایرلس ← با موبایل میل‌م را چک کنم

BTS ↓ ۵۰۰ تا ۱ کیلومتری

از طریق gateway بین‌الملل وصل می‌شود به یک (TIC) شبکه ارتباطات زیرساخت ایران ← ISP بهمنی .

ISP (Internet service provider) : (شبکه‌ای) مجموعه‌ای از سوئیچ‌ها و لینک‌های ارتباطی که بطور مستقل مدیریت می‌شوند که ارتباط میان کامپیوترها در دنیا را فعالیا می‌کنند .

- ISP‌ها لول‌ها و سطوح مختلفی دارند و در حال حاضر از پروتکل IP استفاده می‌کنند

- هر host (end systems) برای اتصال به اینترنت باید از طریق یک شبکه دسترسی (access network) به یک ISP (معمولا ISP‌های دسترسی) متصل شوند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

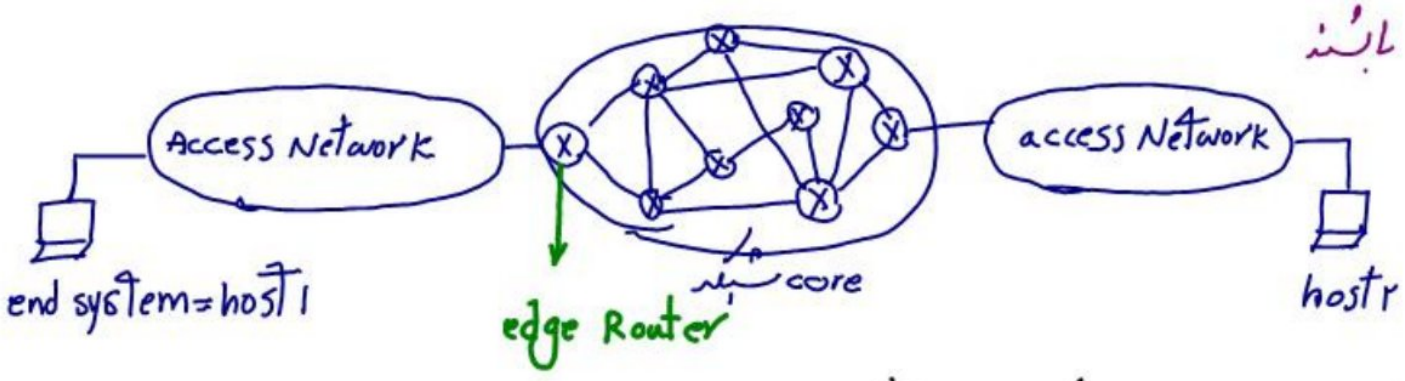
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

- نحوه وصل شدن به Isp دسترسی متفاوت است . شبکه های دسترسی می توانند تکنولوژی های مختلفی را داشته باشند



edge Router : اولین روتری که در هسته شبکه بهش وصل می شویم

شبکه دسترسی : رسانه‌ای که یک هاست را به اولین مسیریاب شبکه (edge router) متصل می کند

تکنولوژی که ارتباط بین یک Host را تا اولین نقطه شبکه (edge router) برقرار می کند

Access Network می تونند

۱- شبکه خانگی باشند

- Dial up ← شبکه تلفن (PSTN) . همزمان نمی توان هم صحبت کرد و هم دیتا فرستاد
- ADSL
- HFc : Hybrid Fiber coaxial
- FTTH
- sat

۲- شبکه سازمانی / خانگی (LAN)

- Ethernet : باسیم
- wi-Fi : بی سیم

۳- شبکه بی سیم گسترده

- 4G
- LTE
- WIMAX

چه کسانی می توانند Access Isp باشند ؟

- شرکت های مخابراتی
- تلویزیون کابلی
- دانشگاه ها
- شرکت های تجاری بزرگ

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

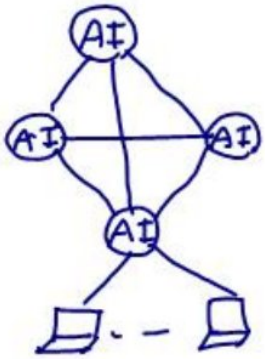
رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

- هر ISP باید به یک Access Isp وصل شود که هدف ، هم ISP ها بتوانند بهم وصل شوند
پس باید تمامی Access Isp ها بتوانند بهم وصل شوند

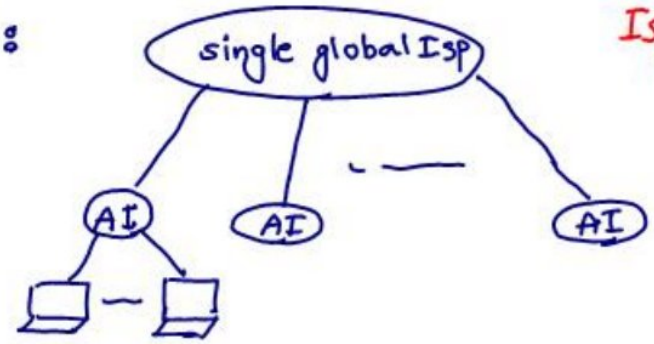
حال چطور می‌توانیم این Isp ها را بهم وصل کنیم؟

structure ۰:



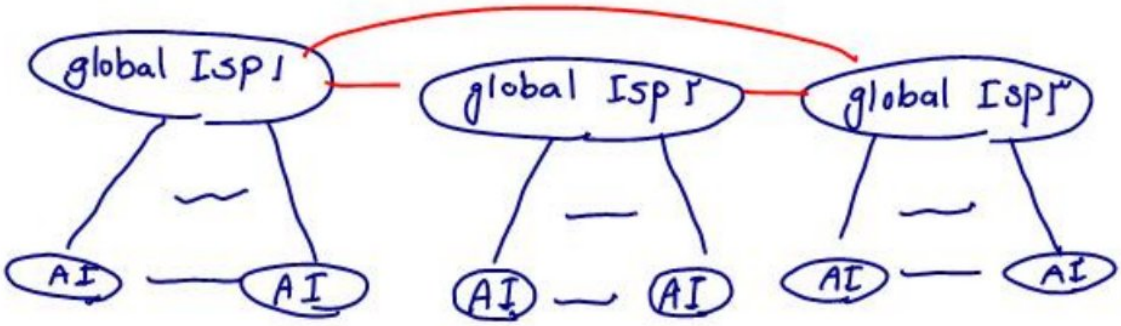
ایده مردود است

structure ۱:



- این ایده نیز مردود است ، چون این Isp
همانی باید در سترکیبی تمامی AI های دنیا
حداقل یک روتر داشته باشد
- زمان توسعه اش بسیار زیاد است .
- تغییرات زمان بر و هزینه بردار
- به وجود آمدن انحصار که باعث عدم رقابت و در نتیجه باعث عدم پیشرفت می‌شود

structure ۲:



- این مدل برای AI ها خوب است و حق انتخاب دارند ← رقابت بین global Isp ها

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

- به اسلایدها مراجعه شود

- شبکه معمولا به ۲ قسمت تقسیم می‌شود ۱ هسته شبکه ۲ لبه شبکه

هسته شبکه : از تولین روتر عمومی که داده‌ها (end systems) از طریق آن به اینترنت وصل می‌شوند شروع می‌شود و قبل از این روتر (edge router) را لبه شبکه می‌گویند.

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

اینترنت چیست؟ این پرسش را می‌توان به روش‌های گوناگونی پاسخ داد

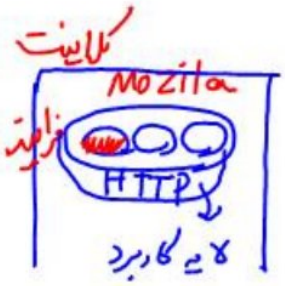
شامل چه چیزهایی است: مجموعه ای از اجزا
سخت افزاری: هاب، سوئیچ‌ها
نرم افزاری (پروتکل‌ها): IP, FTP, HTTP
TCP, UDP

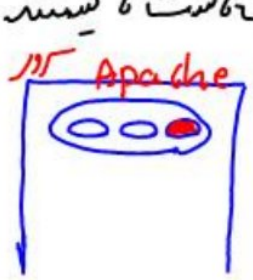
چه کاری انجام می‌دهد؟ یک زیرساخت است که به برنامه‌های کاربری سرویس میدهد ← مجموعه ای از سرویس‌ها را به App های توزیع شده ارائه میدهد

هدف از ایجاد شبکه؟ تبادل داده بین برنامه‌های کاربری بر روی هاست‌ها

نکته - برنامه‌های اینترنت فقط روی هاست‌ها (end system) اجرا می‌شوند

- در شبکه‌های کامپیوتری هم مبدا ارتباط و هم مقصد ارتباط یک فرآیند (process) (یک فرآیندی مربوط به یک App شبکه‌ای است) پس مبدا و مقصد ارتباطات هاست‌ها نیستند

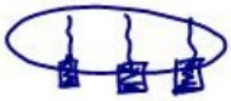




فرآیند: یک برنامه درحال اجرا روی یک end system

حال دو فرآیند که روی دو هاست مختلف چطور با هم ارتباط برقرار می‌کنند؟

هر برنامه شبکه از یک یا چند زوج فرآیند که برای اینکه با همدیگر صحبت کنند از طریق شبکه با هم پیام رد و بدل می‌کنند



- یک برنامه (فرآیند) در یک نشست یا مشتری (client) است یا سرور (server) است

فرآیند:
- server: یک فرآیند ارائه دهنده یک سرویس و درخواست را دریافت می‌کند
- client: استفاده کننده از سرویس می‌گیرد، درخواست دریافت سرویس می‌کند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

- در یک نشست ارتباطی ۲ شخص بین یک یا دو فرآیند ، فرآیندی که ارتباط را آغاز می‌کند (فرآیندی که اولین تماس را با فرآیند دیگر می‌گیرد ، فرآیندی که نشست را شروع می‌کند) فرآیند مشتری (client process) و فرآیندی که منتظر می‌ماند تا با آن تماس بگیرند فرآیند سرویس دهنده می‌گویند (server process)

معماری شبکه < (end system) Host
- Host ها یی که برنامه های کلاینت را اجرا می‌کند : لپ تاپ ها pc ها : client host
- Host ها یی که علاوه بر اینکه برنامه های کلاینت رویش اجرا می‌شود ، برنامه های سرور را اجرا می‌کند (برنامه های سرور رویش وجود دارد) : server host

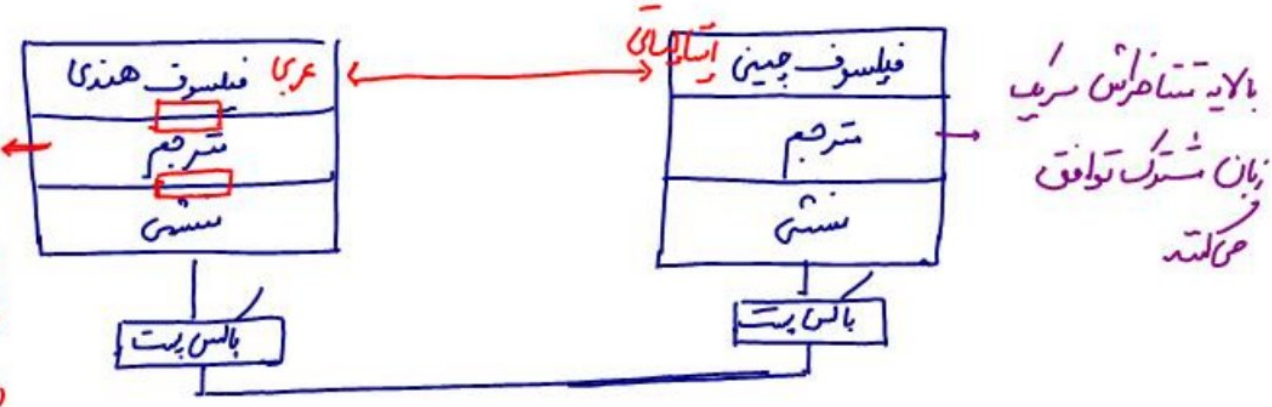
نکته - در برخی از برنامه های کاربردی مثل skype یک فرآیند همیشه نقش مشتری و فرآیند دیگر همیشه نقش سرور را بازی می‌کند ، اما در یک برنامه کاربردی مثل اشتراک گذاری فایل مثل Torent یا اشتراک گذاری فایل p2p یک فرآیند مشخص می‌تواند در یک نشست نقش مشتری و در نشستی دیگر نقش سرویس دهنده را داشته باشد ، زیرا می‌تواند هم فایل بگیرد و هم فایل به دیگران بدهد

* در شبکه های کامپیوتری تعامل نودها با هم در یک محیط بسیار پیچیده صورت می‌گیرد . در دنیا کامپیوتر نودهایی که می‌خواهند با هم ارتباط برقرار کنند نه مکان شون یکی است و نه زبان شون یکی است ، با چه بندی می‌توانیم این مشکلات را حل کنیم

- فرض دو فیلسوف هندی و چینی در دو گوشه دنیا می‌خواهند یک تعامل فلسفی با هم داشته باشند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.



مزایا معماری لایه ای

۱- ساده تر شدن پیاده سازی
۲- مدیریت راحت تر
۳- انعطاف در پیاده سازی
۴- جا بجا کردن یک لایه با لایه دیگر
۵- عوض کردن نحوه پیاده سازی سرویس های داخلی یک لایه بدون آن که هیچ تغییری در کل سیستم ایجاد شود
۶- عیب یابی راحت تر
۷- سیستم مقیاس پذیر می شود
۸- اگر هر لایه را خوب تعریف کنیم می توانیم ویژگی های خاصی را بهش اضافه کنیم
۹- افزایش قابلیت اطمینان: اگر هر لایه را متخصص های آن لایه بنویسن خطایش کمتر می شود

نکته- ما می توانیم در لایه ترجمه بجای ۱ مترجم ۱۰ تا مترجم قرار دهیم، ولی تا زمانیکه کاری که اینها انجام می دهند همان عمل ترجمه است، همه شون در لایه ترجمه قرار می گیرند

نکته- مخاطب هر لایه لایه تظیر آن در مقصد است ولی هر لایه پیام اش را به دست لایه پایین تر از خودش میدهد

نکته- هر لایه به لایه بالا ترش سرویس میدهد و از لایه پایین ترش سرویس می گیرد

نکته- اگر سرویس ۶ را خوب تعریف کنیم می توانیم یک لایه را کلا برداریم و یک لایه دیگر که همان سرویس را ارائه بدهد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

اما بطور دیگری پیاده سازی شده بالاترین کسیم بدون اینکه اطلاعاتی در سطله به وجود آید

پروتکل: مجموعه قواعد دو لایه متناظر هم برای انجام کاری است، در واقع دو لایه متناظر برای انجام وظایف شون باید بین هم اطلاعاتی رد و بدل کنند که این کار را با اضافه کردن اطلاعاتی به داده ای که از لایه بالاتر میگیرند انجام میدهند به این اطلاعات هدر و تریلر یا protocol overhead میگویند

نکته - هر لایه برای اجرا پروتکل اش لازم دارد تا overhead کاری را به بسته های لایه بالاتر اضافه کند، تولید کند، protocol overh- فرستنده ها و مصرف کننده protocol over- ها طرف گیرنده، همان لایه است.

نکته - یکی از معایب مدل لایه ای این است که به دلیل protocol overs با افزایش تعداد لایه ها سربارهای و زمانی بیشتری خواهیم داشت چون این هدرها نیاز به پردازش دارند، همین طور گاهی اوقات در میان لایه ها تغییر می کنند.

نکته - در شبکه پروتکل ها را در یک نگاه مفهومی به لایه های مختلف تقسیم بندی می کنند، برای این می گیم مفهومی چون لزومی ندارد که تناظراً در دنیا خارج شما لایه هایی را ببینید که بصورت فیزیکی از هم جدا باشند

نکته - یک لایه می تواند بصورت نرم افزاری یا سخت افزاری و یا ترکیبی از هر دو پیاده سازی شوند

توجه: پروتکل مجموعه قواعد دو لایه متناظر برای اینکه بتوانند به لایه های بالاترشون سرویس مناسب ارائه بدهند هست ولی سرویس یک چیزی بین یک لایه و لایه بالایی دو لایه پایینی اش

تست سراسری ۸۴: کدام یک از عبارات های زیر در مورد مدل لایه ای شبکه های کامپیوتری صحیح است؟

۱- هرچه تعداد لایه ها بیشتر شود پیچیدگی طراحی کاهش می یابد

۲- " " " " سربار سیستم " "

۳- " " " " اعمال تغییرات پیچیده تر می شود

۴- " " " " پیاده سازی " "

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

تست سراسری ۸۸ : دلیل استفاده از مدل لایه‌ای برای پیاده سازی شبکه‌های کامپیوتری چیست ؟

۱ - پیاده سازی ساده‌تر

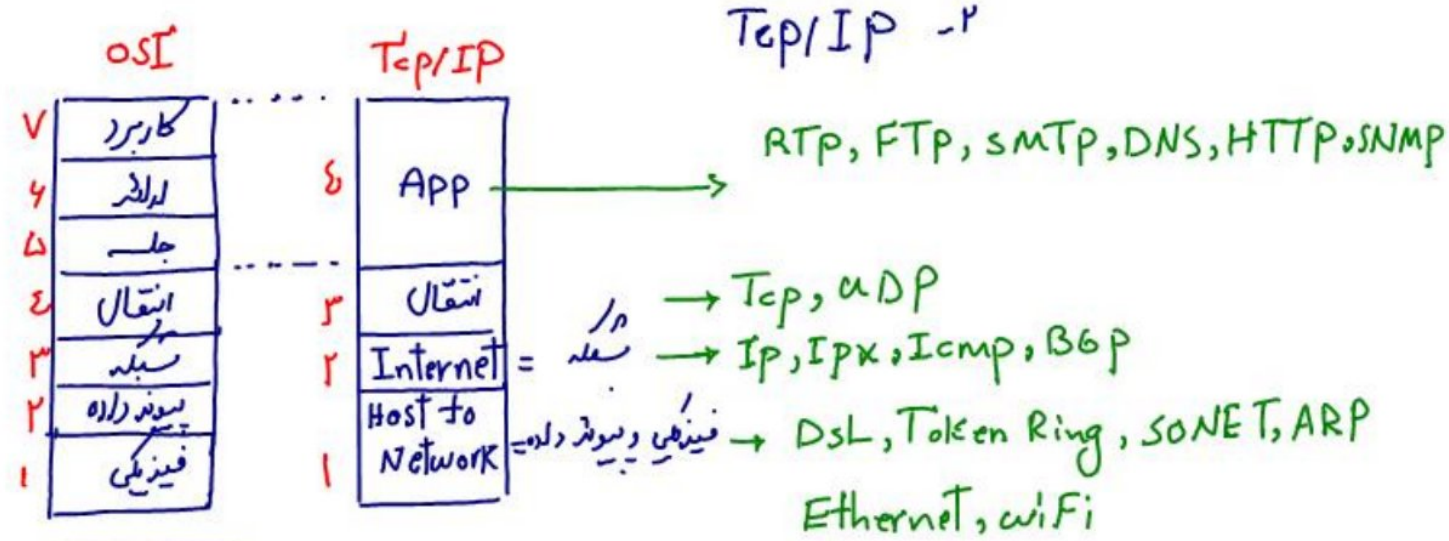
۲ - " " ، نگهداری آسانتر

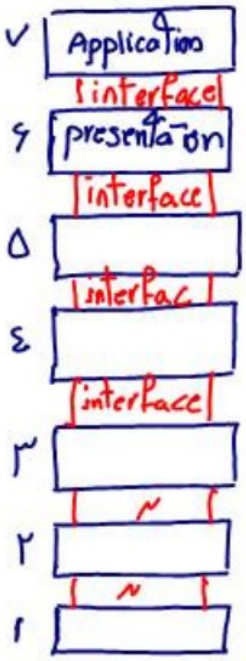
۳ - " " " ، اعمال تغییرات با هزینه کمتر

۴ - " " " " " " ، سربار کمتر

دو مدل لایه‌ای ارائه شده : ۱ - OSI (open system Interconnection)

۲ - Tcp/Ip





ارتباط بین لایه

Interface : واسط بین یک لایه و لایه بالایی و لایه پایینی اش ، که می تواند نرم افزاری یا سخت افزاری باشد

نکته - تعریف خوب interface است که باعث می شود عوض شدن یک لایه باعث نشود که لایه پایینی نتواند سرویس مناسبی از آن بگیرد و همین طور لایه جدید نتواند سرویس مناسبی را به لایه بالایی اش بدهد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

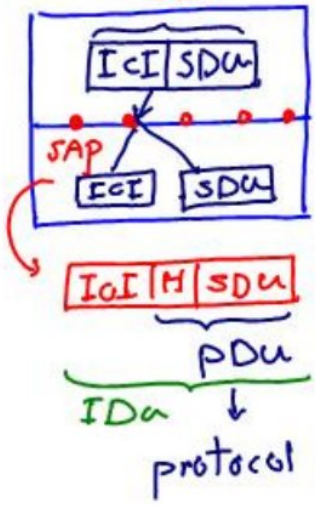
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

IDU = Interface Data unit



دیتایی که بین لایه ها رد و بدل می شود

SAP (service access point) : محل انتقال لایه بالا به لایه پایین است وقتی لایه پایین می خواهد به لایه بالا سرویس بدهد .

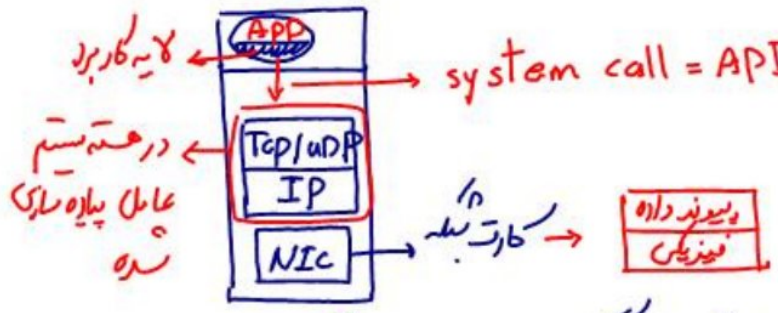
سرویس که لایه پایین به لایه بالا ارائه میدهد از طریق interface بین لایه ها

که از قدرت SAP تشکیل شده است صورت میگیرد

SDU = (service Data unit)

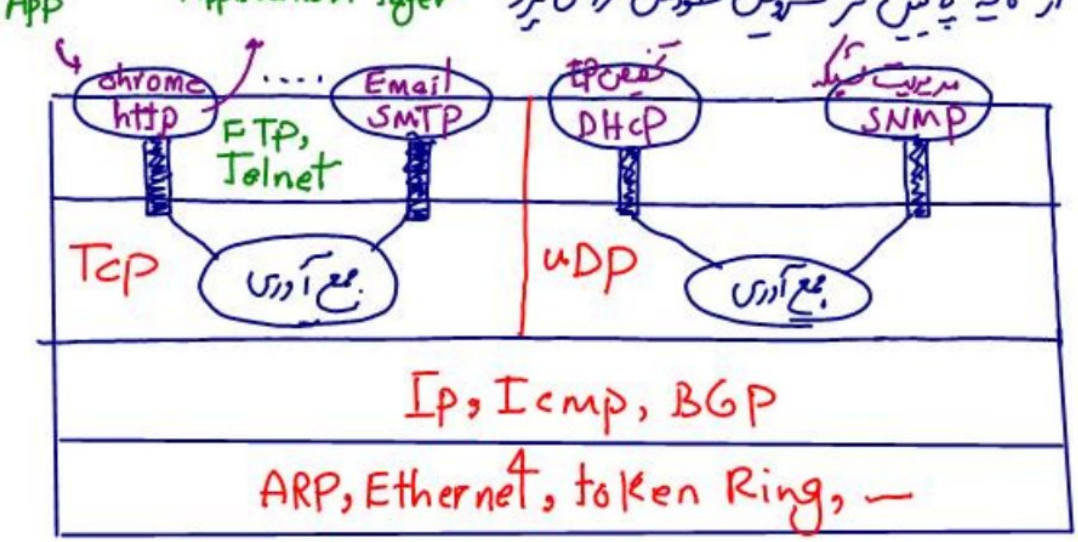
IcI = interface control information : بخشی از اطلاعاتی که لایه بالا به لایه پایین اش میدهد تا لایه پایین بتواند سرویس مناسب را به لایه بالایی اش بدهد ، مصرف IcI در همین لایه خواهد بود

توجه) همیشه IcI نداریم



* همان طور که در شکل مشخص است هرکدام سرویس خودش را از لایه پایین می گیرد ، هر لایه از طریق API یا system call از لایه پایین تر سرویس خودش را می گیرد

Application Iger



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

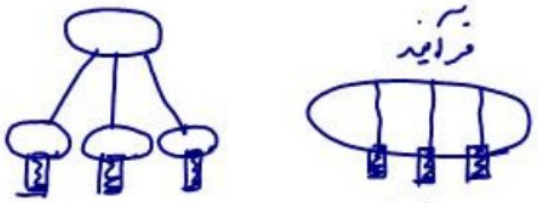
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

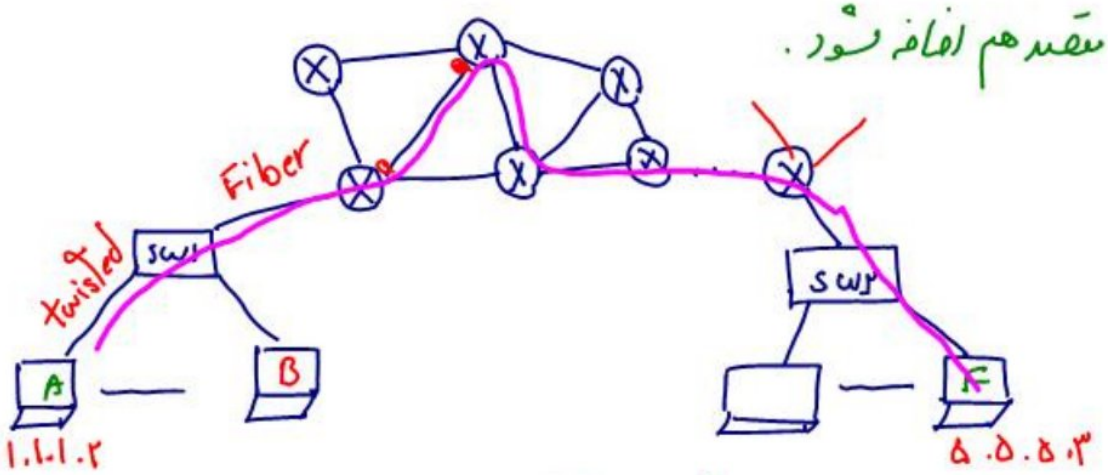
- یک App (فرآیند) وقتی می‌خواهد یک داده را به لایه انتقال بدهد یک چیزی درست می‌کند به اسم سوکت و به هر سوکت یک پورت نامبر خاص اختصاص داده می‌شود

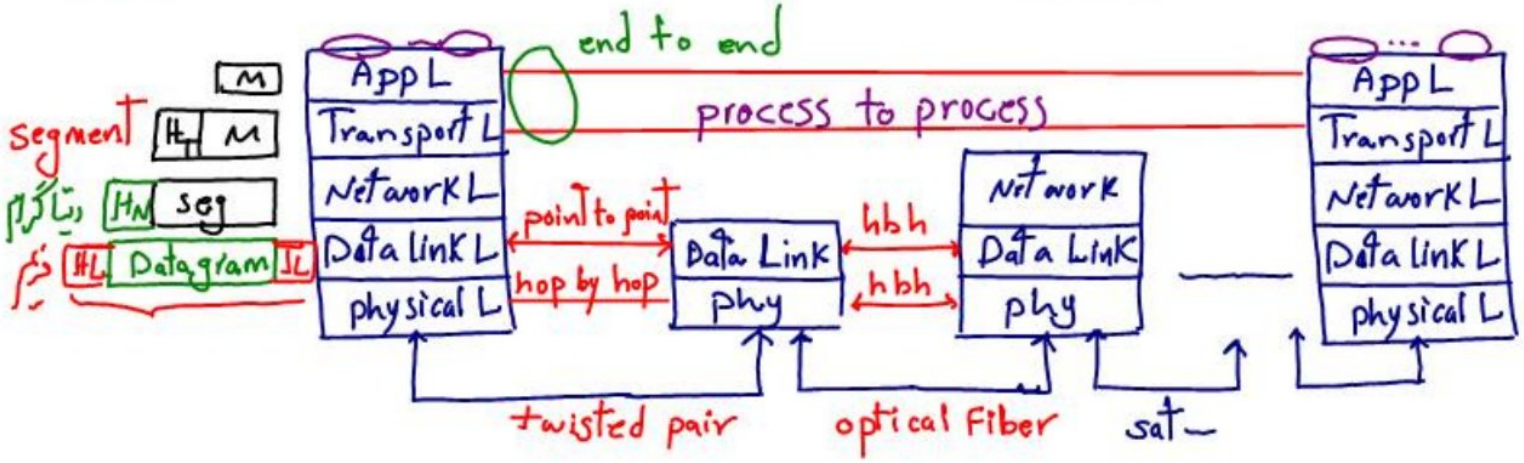


نکته - یک فرآیند می‌تواند یک یا چند سوکت داشته باشد

سوکت - دریچه‌ای است که یک فرآیند یا یک نخ، داده‌های خود را از آنجا به لایه انتقال میدهد و یا داده‌های دریافتی را در مقصد از لایه انتقال می‌گیرد

نکته - هر سوکت باید یک شناسه منحصر به فرد داشته باشد تا لایه انتقال بداند که در مقصد داده را به کدام فرآیند لایه App تحویل بدهد. ← برای ایجاد یک شناسه منحصر به فرد برای هر سوکت نیاز شد تا شماره پورت مبدا و مقصد هم اضافه شود.





سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

نکته - واحد جابجا کردن اطلاعات بین دو لایه انتقال را TPDU (Transport protocol Data unit) می‌گوییم، اگر از Tcp استفاده کنیم می‌گفت می‌نامش و بسته‌های udp را دیتاگرام می‌گویند، بسته‌های لایه شبکه را نیز دیتاگرام می‌گویند. اما برای سادگی و جلوگیری از گیج شدن زبان پس بسته‌های Tcp و udp را قطعه (سگمنت) و بسته‌های لایه شبکه را Datagram می‌نامیم

سوال - چرا سه لایه پایین، لایه‌هایی هستند که در همه نودها Run می‌شوند ؟

بین هر دو hop یک لینک باید وجود داشته باشد، بنابراین ارتباط physical layer & در هر hop باید وجود داشته باشد. همین طور اگر مبدا بخواهد برای مقصد دیتا Reliable بفرستد، هر نودی باید از نود بعدی اش confirm بگیرد. بنابراین Data link L.. هم باید در هر لینک وجود داشته باشد. برای Routing نیز هر نودی باید بتواند در آن شرکت داشته باشد و وقتی دیتا اش بهش می‌رسد بداند که به چه نودی فروارد شش کند. اما تیپ کاری که لایه transport، App انجام میدهند اصلا به نودهای میانی کاری ندارد بنابراین اینها end to end هستند

Route (مسیر) یا path: دنباله‌ای از سوئیچ‌ها و لینک‌های ارتباطی که توسط داده‌های ارسالی از host فرستنده به host گیرنده پیمایش می‌شود

نکته - همه روترهایی که روی مسیر هم نیستند باید دست به دست هم بدهند و مسیرهای خوب به مقاصد را پیدا کنند و جداول مسیریابی روترها آپدیت می‌شود

روترها باهم صحبت می‌کنند

Routing = وقتی انجام می‌شود که می‌خواهیم بهترین مسیرها را پیدا کنیم و وقتی بهترین مسیرها پیدا شد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

جدول مسیریابی روترها آپدیت می‌شود. ولی وقتی یک بسته میاد به‌ازای هر بسته روترها دوباره باهم حرف نمی‌زنند که مسیریابی کنند

Forwarding: وقتی بسته‌ای به روتر می‌رسد، IP مقصد را روتر پردازش می‌کند، چک می‌کند و درون جدول روتینگ اش نگاه می‌کند تا بفهمد باید بسته را روی کدام پورت اش بفرستد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

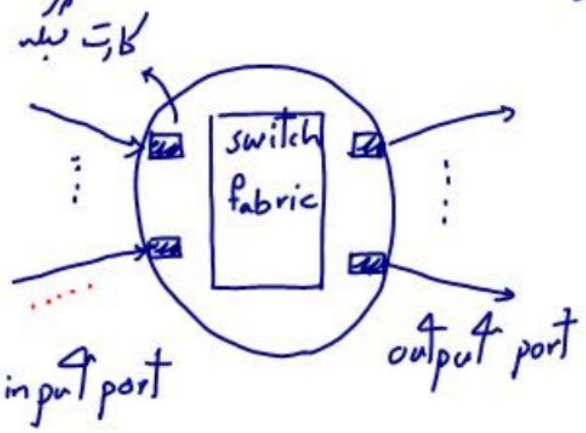
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

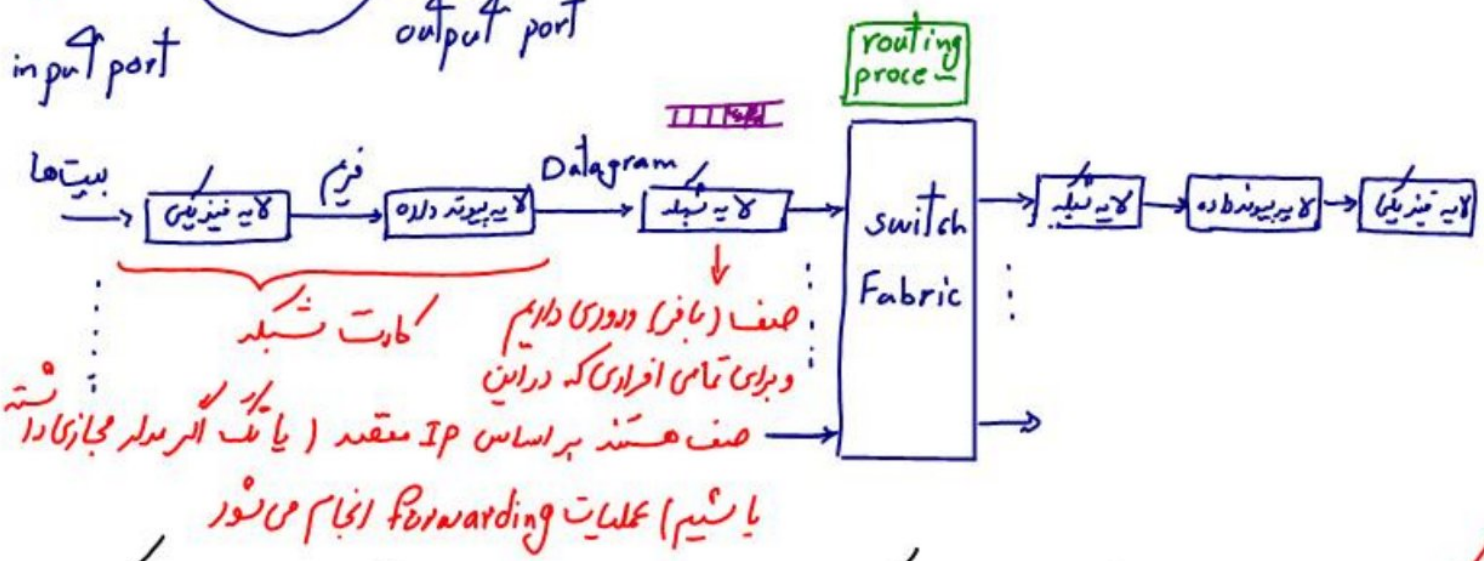
نکته ۱ - عمل routing می‌تواند بصورت Distributed یا centralized باشد. اما معمولاً Distributed است. یعنی همه نودها در این تقسیم وظایف دارند به این دلیل که نمی‌خواهیم Down شدن یک یا تعدادی از روترها باعث ایجاد اختلال در کل سیستم بشود، پس همه میرباب‌ها میان در میرپایی شرکت می‌کنند و هر میرباب بخشی از الگوریتم میرپایی توزیع شده را اجرا می‌کند

نکته ۲ - بسته‌ای که از یک سوئیچ رد می‌شود هدرهایش عوض می‌شود

نکته ۳ - در مدل TcpIP دو لایه بالا و در مدل osi چهار لایه بالا فقط در host مبدا و مقصد هستند

ساختار یک روتر : هر سوئیچ یکسری پورت ورودی و یکسری پورت خروجی دارد و پورت‌ها دو طرفه هستند. همه پورت‌ها به یک کارت شبکه وصل هستند





نکته ۱ - کار switch fabric این است که پورت‌های ورودی را به پورت‌های خروجی متصل کند

نکته ۲ - هر پورت ورودی یک cpu بنام forwarding cpu دارد و همین طور یک جدول forwarding

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

برای خودش ، البته جدول forwarding هم پورت ها شکل هم است .

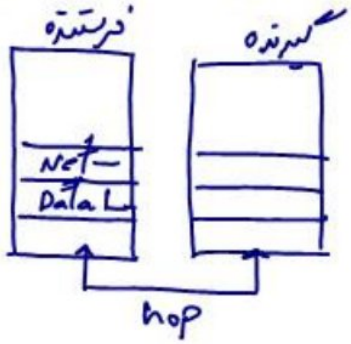
نکته ۳ - در کلیه شبکه پورت های ورودی و خروجی صف داریم و هر دو اینها می توانند پر بشوند و بنابراین هر دو جا می توانند loss به وجود بیاورد

نکته ۴ - Routing : یافتن بهترین مسیر بین فرستنده و گیرنده ها و آپدیت جداول مسیریابی روترها . هر روتر یک Routing processor دارد که توسط آن الگوریتم های (برنامه های) مسیریابی را اجرا می کند ، در اثر اجرا این برنامه یک روتر با دیگر روترها از طریق رد و بدل کردن پیام ها و بسته های سیگنالینگ صحبت می کند و forwarding table های روترهای شبکه را بصورت پریودیک آپدیت می کنند . بنابراین forwarding عملی است که در داخل یک سوئیچ برای انتقال یک بسته از پورت های ورودی به پورت های خروجی انجام می شود . اما مسیریابی فرآیندی است مربوط به کل شبکه که مسیر انتها به انتها بسته ها از مبدا به مقصد را تعیین می کند

نکته ۵ - بسته های منتظر در صف بافر ورودی با توجه به الگوریتم های مختلف انتخاب فروارد می شوند که ساده ترین اش می تواند FIFO باشد

کنترل جریان : سرعت نود ارسال کننده دیتا و دریافت کننده دیتا را تطبیق دهیم . نرخ ارسال داده از طرف یک مبدا ان به یک مقصد بیش از میزان قابل تحمل مقصد باشد فرستنده باید به نوعی نرخ ارسال اش را کاهش دهد

- ما می توانیم flow فرستنده را توسط گیرنده کنترل کنیم با دادن پیام های مناسب از گیرنده به فرستنده ، اینطوری یک فرستنده سریع نمی تواند یک گیرنده کند را overflow کند



نکته - کنترل جریان در لایه های مختلفی انجام می شود Data link layer, transport

نکته) ما برای کنترل جریان نیاز به ACK داریم

نکته) برای جلوگیری از Dead look نیاز به timer داریم در فرستنده

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

- piggy backing : گیرنده که می‌خواهد به فرستنده ack بدهد، چون خودش هم به فرستنده بسته ارسال می‌کند ack ها مربوط به بسته‌هایی فرستنده را در بسته‌هایی که خودش ارسال می‌کند می‌گذارد و بسته جدا مخصص ack ایجاد نمی‌کند

کنترل خطا : بسته‌ها ممکن است خراب شوند یا گم شوند (به ترتیب رسیدن بسته‌ها به مقصد)

نکته) از Ack برای کنترل خطا نیز استفاده می‌شود

نکته) یکی از دلایل اینکه بسته به وجود آمد این هست که به ازای هر بیت یا بایتی Ack نداشته باشیم

نکته) کنترل جریان و کنترل خطا هم از وظایف لایه پیوند داده و هم از وظایف لایه انتقال است

نکته) مخاطب Data Link layer یک نود Data link layer اولین نودی است که از طریق physical بهم وصل‌اند، بنابراین گام به گام پروتکل‌ها و استانداردهای کنترل خطا و کنترل جریان این دو کارت شبکه‌ها است (Data link layer) متفاوت است.

- کنترل جریان در Tcp لایه انتقال : اگر برنامه کاربردی متناظر با یک اتصال Tcp در گیرنده درخواست داده‌ای دریافتی کند عمل کند ممکن است بافر دریافت سمت گیرنده در اثر ارسال داده بیش از حد توسط فرستنده به سرریز شود، در اینصورت گیرنده برای جلوگیری از این اتفاق باید در هر لحظه که می‌گوید که برای فرستنده ارسال می‌کند با قرار دادن یک تعبیه بنام receive window (rwnd) فرستنده را از مقدار فضا باقیمانده در بافر خود مطلع کند و فرستنده نرخ ارسال اش را با توجه به این پارامتر کم و زیاد کند (Tcp برای انجام کارهای بیش می‌آید و برای هر اتصال یک بافر و یکسری تعبیه کنترلی در نظر می‌گیرد) فرستنده یک نسخت Tcp یک پنجره ارسال دارد که برای اطمینان از سرریز نکردن بافر دریافت کننده سعی می‌کند مقدار بایت‌های تصدیق نشده خود را همیشه کمتر از rwnd نگه دارد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

کنترل ازدحام کاهش نرخ ارسال در میدا در صورت وقوع ازدحام در شبکه و در روترها و سوئیچ های میانی به منظور حل مشکل ازدحام به وجود آمده در راستا سلامت کلی شبکه

* انواع سرویس هایی که لایه های مختلف هم می دهند را می توان از دو منظر دسته بندی کرد

۱- سرویس یا connection oriented (اتصال گرا) یا connection less (بدون اتصال)

۲- Reliable یا unReliable

۱- یک سرویس اتصال گرا سرویسی است که برای ارائه این سرویس به لایه بالاتر یک setup اولیه (طبق یک negotiate دو طرفه بین دو لایه مبدا و مقصد یکسری پارامتر ست می شود) نیاز است که بین دو لایه متناظر انجام شود. سرویسی است که قبل از ایجاد آن سرویس برای لایه بالاتر یک مذاکره دو طرفه بین مبدا و مقصد انجام می شود

- هر وقت برای ارائه یک سرویس به لایه بالاتر یک مذاکره دوطرفه برای ست کردن یکسری پارامتر ضرورت پیدا کرد می گوییم کانکشن ایجاد کردیم، پس کانکشن داشتن را به معنی یک سیم نمیزنیم رد و بدل کردن نگاه نکنید
- به علت اینکه در هر لایه یک مدلی از مذاکره را می توانیم داشته باشیم، بنابراین مفهوم کانکشن داشتن در لایه ۱ با مفهوم کانکشن داشتن در لایه ۲ و ... در پیاده سازی تفاوت است.

connection less: هر وقت که setup اولیه نمی خواهیم و تا دیتا از لایه بالا به دستمان رسید فوری ارسال انش می کنیم می گیم connection less

نکته - شما می توانید در لایه phy مثلا connection oriented باشید و در لایه دو نباشید و دوباره در لایه ۳ باشید یا نباشید و به همین ترتیب. اینکه در چه لایه ای connection oriented هستیم یا نیستیم برمی گرده

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

به نوع سرویس که این لایه می خواهد به لایه بالاترش ارائه بدهد و کاری به لایه پایینی اش ندارد

۲_ Reliable ، unReliable

سرویس Reliable سرویسی است که هیچ وقت دیتا را از دست نمی دهد و تمام دیتا را بصورت صحیح و سالم به لایه بالاتر می رساند. - برای ایجاد یک سرویس Reliable نیاز به retransmission و Ack nowledgement داریم.

نکته) یک لایه می تواند reliable باشد درصورتیکه لایه زیرین آن unreliable باشد

نکته) برخی از برنامه ها loss sensitive هستند مثل انتقال نامه، email یا تراکنش های مالی.

نکته) برخی از برنامه ها loss tolerant هستند مثل برنامه های multimedia

وظایف لایه های Tcp/Ip

۱- لایه App : در این لایه پروتکل های لایه App قرار گرفته است ، پروتکل های این لایه end to end

۲- لایه transport : سرویس جابجا کردن داده بین مبدا و مقصد را به لایه App ارائه میدهد و تمام پیچیدگی ها را از دید App پنهان می کند

end to end communication -

- وظیفه پروتکل های لایه انتقال ایجاد یک ارتباط منطقی (logical connection) بین فرآیند های درحال اجرا روی هاست مبدا و مقصد است. وقتی می گیم ارتباط منطقی یعنی از دیدگاه برنامه های کاربردی دقیقا مانند این است که میزبان هایی که این فرآیندها را اجرا می کنند مستقیما بهم وصل اند

نکته) سرویس هایی که یک پروتکل لایه انتقال می تواند به لایه بالاترش ارائه دهد اغلب وابستگی شدیدی به سرویس دارد که

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

پروتکل لایه شبکه زیرش می تونند در اختیار لایه انتقال بگذارد ، گاه لایه شبکه نتواند میزان تاخیر یا پهنا باند مشخصی را برای مبادله سگمنت های لایه انتقال بین میزبان ها ضمانت کند آن گاه لایه انتقال نیز نمی تواند هیچ تضمینی در این مورد به برنامه های کاربردی بدهد ، با این حال یک پروتکل لایه انتقال می تواند سرویس هایی را تنها مستقل از اینکه لایه شبکه چه سرویسی می تواند ارائه بدهد و از چه پروتکلی استفاده می کند ارائه بدهد ، مثلاً اگر پروتکل لایه شبکه unreliable باشد و یک سرویس غیر قابل اطمینان را تحت اختیار لایه انتقال بگذارد اما یک پروتکل لایه انتقال می تواند یک سرویس قابل اطمینان را به لایه بالاتر بدهد . یا یک پروتکل لایه انتقال می تواند با استفاده از تکنیک های رمزنگاری تضمین کند که پیام های برنامه های کاربردی توسط بوزرها نامحرم خوانده نشود حتی اگر لایه شبکه هیچ تضمینی در مورد محرمانه ماندن محتویات سگمنت ها به لایه انتقال ندهد

وظایف سرویس های (وظایف) لایه انتقال که باید در اختیار لایه App قرار بدهد

۱- تحویل داده فرآیند به فرآیند : ← این کار با Demultiplexing و multiplexing لایه انتقال عملی می گردد
(service addressing)

۲- تشخیص خطا

- ۲ پروتکل لایه انتقال داریم : ۱- Tcp ۲- Udp

(Transmission control protocol) Tcp

- Reliable
- connection oriented
- Flow control
- sequencing : ترتیب داده ها خیلی مهم است ، Tcp گارانتی می کند که ترتیب داده هایی که از App-L می گیرد به همان ترتیب به App مقصد بدهد
- Fragment byte stream into Tp message
- congestion control

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

UDP

- unreliable
- connection less
- No sequencing

- در Appهایی که ماهیت Real time دارند و برایشون تاخیر هم است و تاخیر خیلی بیشتری نسبت به اینکه گاهی اوقات بسته‌ها گم بشوند دارند از UDP استفاده می‌شود

نکته - UDP فقط همان دو سرویس پایه را ارائه میدهد و تصحیح خطایش هم در حد یک error checking ساده است، یعنی گاهی دیده که داده غلط است به فرستنده نمی‌گوید که داده را دوباره بفرست و بسته را دور می‌اندازند

نکته - Tcp برای اینکه بتواند این سرویس‌های را که گفتیم به لایه بالاتر ارائه دهد می‌آید و برای هر فرآیند یک اتصال ایجاد می‌کند و برای هر اتصال یک باقر دیگری تغییرهای کنترلی در مبدا و مقصد در نظر می‌گیرد

مالتی پلکسینگ: جمع آوری داده‌ها از سوکت‌های مختلف فرستنده و درست کردن segment‌ها و تحویل آنها به لایه شبکه

دی مالتی پلکسینگ: تحویل داده‌های داخل یک segment لایه انتقال به سوکت متناظرش

لایه شبکه

وظیفه اصلی لایه شبکه ایجاد یک ارتباط منطقی بین میزبان‌ها می‌باشد و مقصد است که این کار را با استفاده از هم پروتکل این لایه یعنی پروتکل اینترنت: IP (Internet protocol) صورت می‌گیرد

IP یک سرویس connection less - غیر قابل اطمینان را در اختیار لایه انتقال قرار میدهد، سرویسی که IP به لایه بالاتر از خودش ارائه میدهد موسوم است به سرویس best effort delivery و این به آن معناست که پروتکل IP بهترین تلاش خود را بکار می‌گیرد تا segment ها را به میزبان‌ها مقصد تحویل بدهد ولی هیچ تضمینی نمی‌دهد، همچنین پروتکل IP هیچ تضمینی در خصوص تحویل منظم بسته‌ها (براساس ترتیب ارسال) و تحویل سالم segment ها به لایه انتقال نمی‌دهد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

از وظایف دیگر لایه شبکه می‌توان به موارد زیر اشاره کرد

- Routing
- Forwarding (packet switching → possible out of order delivery)
- packetization
- Fragmentation → only IPv4
- Addressing: به هر هاست یک آدرس IP در شبکه داده می‌شود

Host to Host Network Link layer

از نظر عملکردی کارهای پروتکل‌های physical layer و Data link layer استک OSI را شامل می‌شود. لایه کنترل دسترسی چندگانه (MAC = multiple access control) هم داخل این لایه است.

LLC = logical Link control

نکته - یکی از کارهایی که MAC برای کنترل collision در شبکه‌های مختلف استفاده می‌کند خیلی به بستر شبکه بستگی دارد و با هم فرق می‌کند

- جدا از اینکه بستر شبکه چه باشد 802.2 می‌تواند کارش را بصورت مستقل انجام بدهد. LLC یک رابط است بین لایه بالایی و پایینی

وظایف Link layer

۱- ارسال دیتاگرام‌های لایه شبکه بصورت point to point

۲- کنترل دیتا point to point

۳- انتقال داده مطمئن بصورت point to point

۴- Framing

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

مدل OSI

لایه translation : presentation : آن زمانی که این استاندارد تعریف می‌شد، فرمت داده‌ها در یک کامپیوتر می‌توانست خیلی متفاوت باشد با یک کامپیوتر دیگر

- وظیفه این لایه App می‌گیرد را به فرمتی تبدیل می‌کرد که این فرمت توسط سایر لایه‌ها قابل فهم باشد

- encryption : رمزنگاری
- compression : فشرده‌سازی

لایه session : این لایه session ها را ایجاد می‌کند و نگه می‌دارد، و در نهایت end می‌کند

- check point

لایه شبکه:

congestion control

مقایسه بین TCP/IP و OSI

OSI	TCP/IP
Top down design	Bottom up (grew out of practice)
Transport: connection ori~	transport: connection ori~ OR connection less
Network: connection ori~ OR connection less	Network: connection less

Data link layer

با توجه به دو پارامتر تکه داشتن یا ندانستن و connection ori~ بودن یا connection less بودن، حالت‌های سرویس‌هایی که Data link می‌تواند در اختیار لایه شبکه قرار دهد به وجود می‌آید

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

سه مدل سرویس وجود دارد که لایه ۲ می‌تواند به لایه ۳ بدهد

۱- unacknowledged connectionless

۲- " " ack

۳- " " connec-ori

نکته۱) در یک سیستم می‌تواند ۱ یا ۲ یا هر سه اینها وجود داشته باشد

نکته۲) اینکه لایه شبکه چه زمانی از کدامیک از این مدل‌ها جابجایی اطلاعات استفاده می‌کند بستگی به تیپ کاری دارد که قرار است انجام بدهد.

مدل ۱: در دو جا استفاده می‌شود
۱- در جاهایی که ترافیک real time داریم
۳- low error channels: تصحیح خطا را در لایه‌های بالا انجام کن اگر نیاز داری

مثال: مثلاً در اینترنت Bit error rate خیلی پایین است و ما برایش نمی‌دهیم به‌ازای اینکه بیاید هر فریم ack بگیریم

مدل ۲: این سرویس معمولا جایی استفاده می‌شود که Bit error rate کانال نیز کمی بیش باشد مثل Wi-Fi (802.11)

سوال مهم: چرا ما نیامدیم و در لایه ۲ Ack و Non را نگذاشتیم؟ چرا خوب است که ما این کار را در لایه ۲ نکنیم؟

مدل ۳: وقتی لایه شبکه می‌خواهد داده‌ای که به لایه Data link میدهد اول حتما به مقصد برسد و سپس یک و فقط یک کپی و به ترتیب به لایه شبکه مقابل برسد ← connection oriented

ack ↑

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

رامین رضوی

- درواقع با این سرویس شما می‌خواهید زمانی که یک کانال فیزیکی بدون خطا را در لایه Network layer ایجاد کنید ← برای این منظور نیاز به setup اولیه دارم

نکته) یادتون باشه که در این لایه فرض ایجاد می‌کنیم این است که ما نمی‌توانیم بازاران هر بیت Ack بگیریم

Network layer

- در Routing دو بحث مهم وجود دارد
  - کنترل ازدحام
  - کیفیت سرویس

سرویس‌هایی که لایه شبکه می‌تواند به دو صورت باشد

1- connection less 2- connection orien

(1) 1- هر روتر وقتی بسته ای بهش می‌رسه، در این لحظه بهترین راهی که به ذهنش میاد که به مقصد برسه را انتخاب می‌کند ← نمی‌توانیم گارانتی کنیم که بسته همیشه از یک مسیر مشخص برود

2- یک مذاکره اولیه بین دو نود جایی انجام نمی‌شود : در conn less یک روتر اجازه دارد خودش بدون اینکه با هیچ کس دیگری هماهنگ کند هر زمانی که دلش می‌خواهد پورت خروجی یک بسته را عوض کند

- در این مدل هر وقت یک بسته دست روتر می‌رسد، روتر باید تشخیص بدهد این بسته را روی کدام پورت اش ارسال کند به آدرس IP مقصد ان که در بسته است نگاه می‌کند و سپس با توجه به forwarding table متوجه می‌شود بسته را به کدام سمت ارسال کند، هر روتر به شکل forwarding table

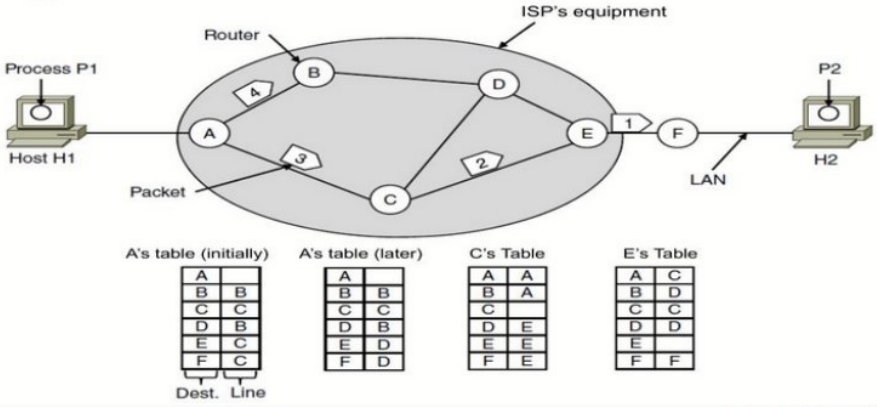
IP مقصد	پورت خروجی
⋮	⋮

است. این جداول هم می‌توانند centralize یا بشود هم Distributed.

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir
MSc-PhD Computer-IT

Implementation of Connectionless Service



connection oriented ②

در این سرویس اگر مبدا H_1 می‌خواهد به H_2 داده ارسال کند، ابتدا شبکه بر اساس تقاضایی که از H_1 وجود دارد می‌آید و طبق یکسری صحبت‌هایی که لایه‌های شبکه روترهای روی مسیر با هم انجام میدهند یک مسیر مناسب بین مبدا و مقصد ایجاد می‌شود، که می‌گوییم در ابتدا connection ها یا circuit ها در شبکه ست می‌شوند. بنابراین معنا کانکشن ست شدن این است که طبق یکسری مذاکرات اولیه در forwarding هم روترهای مسیری که بسته ها قرار است در آن مسیر حرکت کنند، سطرهای مناسبی ایجاد می‌شود. در تمام مدتی که این session برقرار است این مسیر هم در شبکه حفظ می‌شود. اگر خرابی پیش بیاید که آن رخ داد باعث قطع این ارتباط بشود در اینصورت شبکه مجددا باید یک مذاکراتی انجام دهد تا یک کانکشن دیگر ست کند

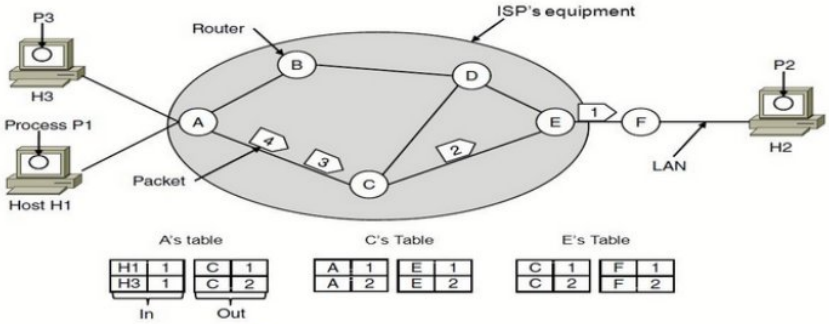
incoming		outgoing	
input port	ID	output port	ID

- در سرویس connection oriented هر forwarding table روتر به شکل: است. در نتیجه هر روتر می‌داند هر وقت از یک پورت با یک ID بسته ای دریافت کرد آن را به چه پورتی و با چه آی دی ارسال کند. در نتیجه ست شدن این مقادیر در جدول روترهای روی مسیر مربوط است که باعث می‌شود بسته ای که از مبدا ارسال می‌شود آن قدر forward شود تا به مقصد برسد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir
MSc-PhD Computer-IT

Implementation of Connection-Oriented Service

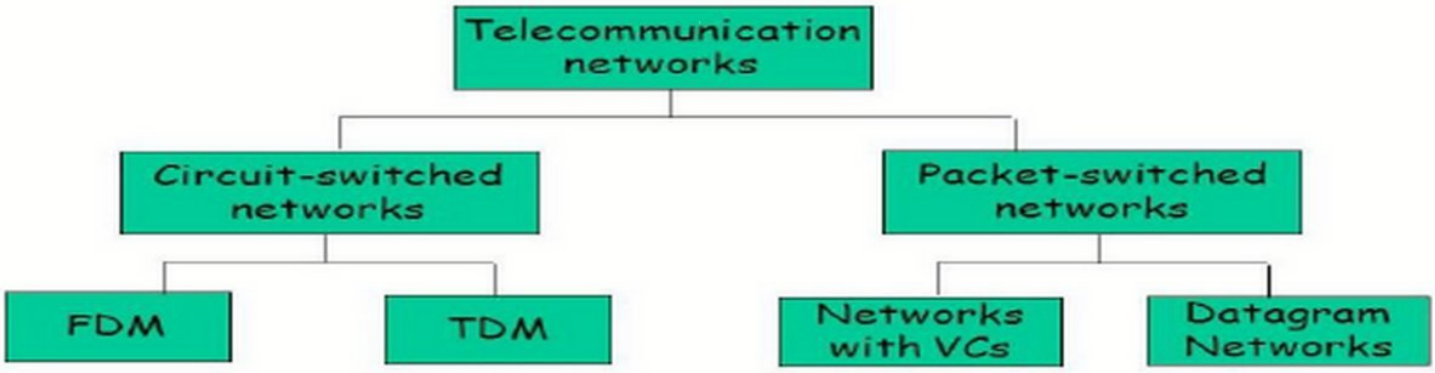


نکته) در این روش ترتیب رسیدن بسته‌ها به مقصد رعایت می‌شود و همین طور منابعی رزرو می‌شود.

- منابعی که رزرو می‌شوند:
  ۱- پهنای باند
  ۲- cpu (processing time)
  ۳- بافر

نکته- در جاهایی که کیفیت سرویس از نظر حداکثر تاخیر، پهنای باند، کنترل ازدحام و ... مهم است و می‌خواهیم یک الزاماتی را تضمین کنیم از CO استفاده می‌کنیم. در سایر کنترل ازدحام و کنترل کیفیت سرویس دشوارتر است.

دیتا به ۲ صورت در هسته شبکه انتقال می‌یابد



- در **circuit switch** داده‌ها بصورت استریم و بدون وقفه ارسال می‌شود در صورتی که در **packet switch** داده‌ها بصورت بسته بسته ارسال می‌شود و روترها از روش انتقال **store and forward** استفاده می‌کنند
- شبکه‌های کامپیوتری **packet switched** ای که در لایه شبکه فقط سرویس متصل ارائه می‌کنند را شبکه‌های مدار مجازی می‌گویند
- شبکه‌های کامپیوتری **packet switched** ای که در لایه شبکه فقط سرویس **connection less** ارائه می‌کنند را شبکه‌ی **datagram** می‌گویند
- دیتاگرام مثل اینترنت، **circuit switch** مثل (تلفن) PSTN، VCs مثل Frame Relay،ATM

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

در شبکه نیاز به شکستن بسته ها داریم

این شکستن در دو جا می تواند (ممکن است) اتفاق بیفتد ① لایه انتقال ② لایه شبکه

MTU (maximum transmission unit) : حداکثر داده ای که یک فریم لایه پیوند می تواند حمل کند

نکته: یک روتر چندین لینک مختلف با پروتکل های لایه پیوند و MTU های متفاوت را بهم وصل می کند
برای مثال فریم های اترنت می توانند تا سقف ۱۵۰۰ بایت داده را حمل کنند، درحالیکه در Token Ring
فریم ها می توانند تا سقف ۴۴۹۲ بایت داده را حمل کنند یا در FDDI (Fiber Distributed Data Interface)
MTU برابر ۴۳۵۲ است.

با توجه به ۲ تا چیز شکستن بسته اتفاق می افتد

۱- شبکه ای که کامپیوتر ما به آن وصل است که به این علت بسته را در لایه انتقال مبدا می شکنیم و بهش segmentation می گویند

۲- دو لینک مختلف با پروتکل های لایه پیوند و MTU های مختلف توسط یک روتر بهم وصل شده به این دلیل بسته ها را در لایه شبکه روترها می شکنیم و بهش می گن Fragmentation

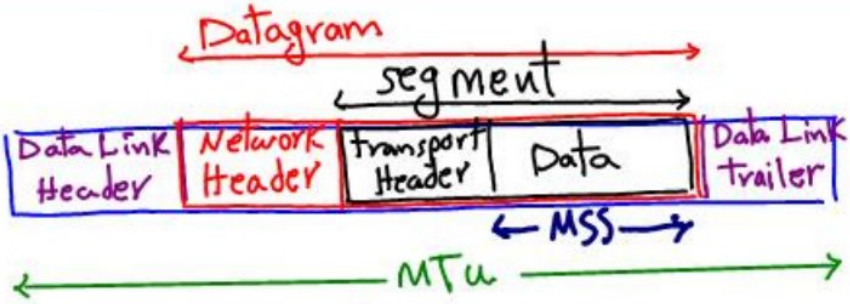
segmentation & Reassembly

یکی از مهم ترین وظایف لایه انتقال است. در لایه انتقال یک بسته بزرگ به n شکست کوچیتر شکسته می شود که طول هر شکست حداکثر می تواند به اندازه یک پارامتر به نام MSS باشد (maximum segment size) که خود این MSS بر اساس طول بزرگترین فریمی که لایه پیوند فرستنده می تواند بفرستد تعیین می شود (MTU) ← MSS بر اساس MTU تعیین می شود

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

محاسبه اندازه MSS

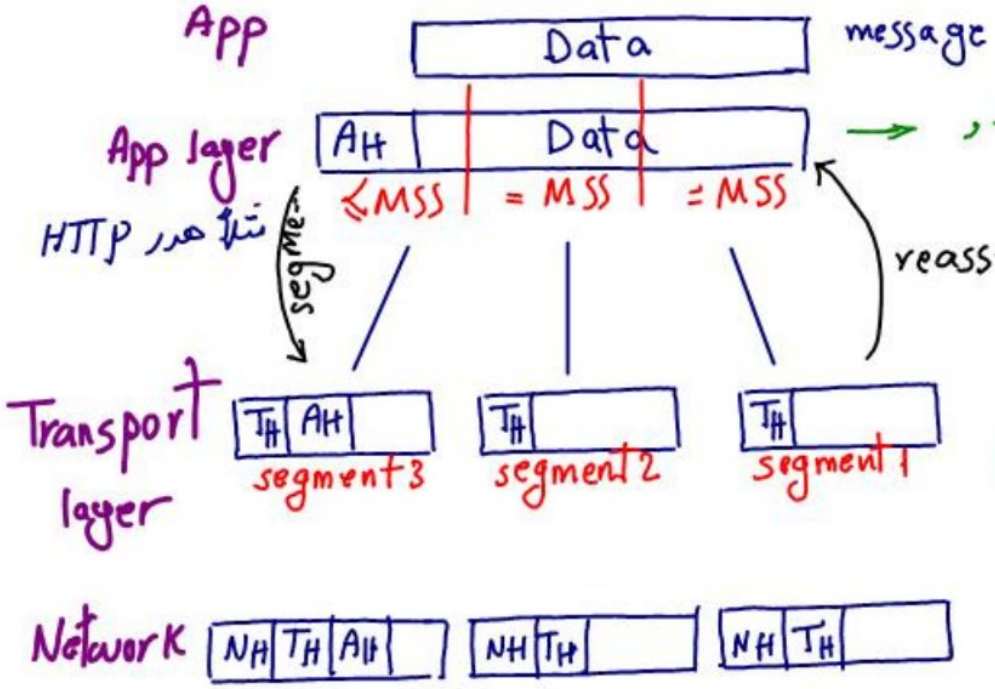


* در MTu، هدر و تریلر لایه Data link نیز در نظر گرفته شده است.

MTu = مثلاً در اترنت ۱۵۰۰ بایت

$$MSS = MTU - [DL_H + DL_T + N_H + T_H]$$

نکته) MTu از لایه Data link به لایه‌های بالاتر شبکه، انتقال گزارش می‌شود



سایز این پیام بزرگ‌تر از MSS است، بنابراین با توجه به MSS می‌شکند

T_H در اینجا هدر Tcp است.

در هدر Tcp هم شماره پورت مبدا و هم شماره پورت مقصد و هم شامل #s (شماره ترتیب) است که ترتیب قطعات را نشان می‌دهد

نکته ۱- segmentation این امکان را برای ما فراهم می‌کند که یک فایل را با هر سایز دلخواهی هر شبکه‌ای بتواند ارسال و دریافت کند، مثلاً اگر پهنای باند شبکه شما 1MB باشد و سایز فایل شما 100MB

نکته ۲- Tcp segmentation را ساپورت می‌کند ولی UDP خیر، این به این معناست که اگر یک برنامه برای ارسال داده‌هایش مراحله از Tcp استفاده کند، می‌تواند داده خودش را با سایز دلخواه خودش به

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

TCP بدهد ، اما اگر یک برنامه می‌خواهد براش ارسال داده‌اش از پروتکل UDP استفاده کند می‌تواند دیتا خودش را با سایر واقعی خودش به UDP بدهد و در این حالت برنامه خودش باید از یک مکانیزم داخلی استفاده کند تا تشخیص بدهد آیا segmentation نیاز هست یا خیر و اگر segm نیاز بود باید خودش این کار را قبل از دادن دیتاش به دست UDP انجام بدهد

سوال ۱ - برای اینکه بسته به درست گیرنده برسد نیاز است که IP مقصد را در هدر TP بگذاریم ولی چرا IP مبدا را نیز می‌گذارند؟ IP مبدا نیاز است چون گیرنده می‌خواهد هم برای فرستنده دیتا بفرستد و هم ack

سوال ۲ - لایه شبکه در مقصد از کجا می‌فهمد بسته‌ای را که گرفته به TCP بدهد یا به UDP ؟

برای این منظور فیلدی بنام upperlayer protocol در هدر لایه شبکه وجود دارد که می‌گوید پیشت استخراج شده را به چه کسی باید تحویل داد. اگر این عدد ۶ باشد به TCP و اگر ۱۷ باشد به UDP داده می‌شود

نکته - این فیلد فقط برای میزبان‌ها مبدا و مقصد در نظر گرفته شده و روترها اصلا به آن توجه نمی‌کنند

سوال ۳ - TCP یا UDP مقصد از کجا می‌فهمد که پیام را (پیام reassemble شده اگر فقط در مورد TCP صحبت کنیم) تحویل چه App ای (پروسه‌ای) بدهد؟ با استفاده از شماره پورت مبدا و شماره پورت مقصد. در واقع برای ساخت شناسه سوکت مقصد به این دو اطلاعات نیز نیاز است

* یک سوکت UDP با دو شفعه مشخص می‌شود ① آدرس IP مقصد
② شماره پورت مقصد

* یک سوکت TCP با چهار شفعه مشخص می‌شود ① و ② شماره پورت فرایندهای مبدا و مقصد
③ و ④ IP های مبدا و مقصد

نکته) نقش فیلد شماره پروتکل در دیاگرام IP مشابه نقش فیلد شماره پورت در سگمنت‌های لایه انتقال است

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

بررسی مزایا و معایب شکستن بسته ها

مزایا:

۱- تاخیر انتها به انتها با قطعه سازی کاهش پیدا می کند ← بعدا با مثال توضیح داده می شود

۲- وقتی بسته ها را به یکسری قطعه تقسیم می کنیم هر کدام از قطعات اگر خراب بشود ما همان قطعه را دوباره ارسال می کنیم و لازم نیست کل بسته بزرگ را دوباره ارسال کنیم

۳- اگر بسته ها قطعه قطعه نشوند با فرروترهای میانی باید بسیار بزرگ باشند که بتوانند برای همه پیام های همه کاربران فضا کنار بگذارند که این امکان پذیر نیست

۴- اگر بسته ها بزرگ باشند بسته های کوچکتر مجبور می شوند پشت این بسته های بزرگ صف بکشند و در این صورت از تاخیر ناعادلانه رنج می برند ← starvation

معایب:

۱- ترتیب قطعه های ارسالی در شبکه با ترتیب دریافت یکسان نیست، بنابراین شاید لازم باشد در یک لایه خودمان ترتیب قطعه ها را درست کنیم و به لایه بالاتر بدهیم

۲- در نتیجه قطعه سازی پیام ها تعداد زیادی بسته کوچک تولید می شود و چون اندازه هدر هر بسته معمولا برابر تمام بسته ها فارق از اندازه بسته، یکسان است، مقدار داده های غیرمفید درون شبکه افزایش می یابد

۳- بسته هایی که تولید می شوند روی Data path شبکه هستند و این خوب نیست

Fragmentation

از آنجاکه دیتاگرام های IP برای ارسال از یک روتر به روتر بعدی باید در داخل یک فریم لایه پیوند جاسازی شوند MTU پروتکل لایه پیوند محدودیتی سخت بر طول یک دیتاگرام لایه شبکه (IP) تحمیل می کند. همان طورکه می دانیم لینک های موجود در مسیر بین مبدا و مقصد می توانند از پروتکل های لایه پیوند مختلفی استفاده کنند که هر کدام از آنها می توانند MTU های متفاوتی داشته باشند. اگر روتری روی یکی از لینک هایش بسته ای دریافت کند و بخواهد این بسته را روی لینکی بفرستد که MTU آن لینک کمتر از طول دیتاگرام IP باشد لایه شبکه این دیتاگرام را به دو یا چند قطعه کوچکتر تقسیم می کند و هر تکه را داخل یک فریم لایه پیوند قرار می دهد.

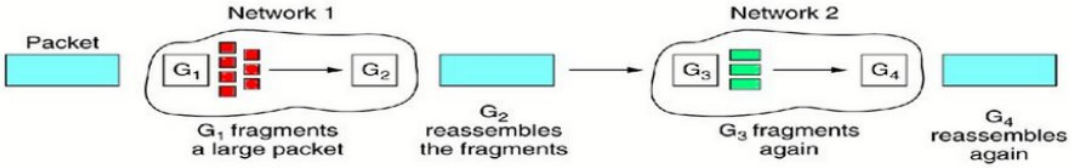
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

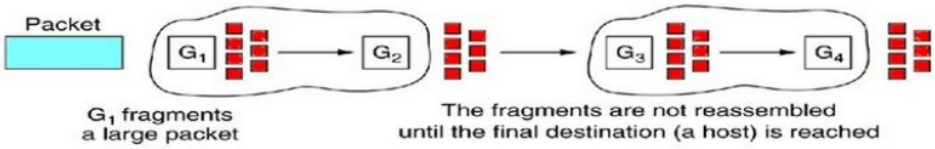
خلاصه: وقتی یک بسته بزرگ می‌خواهد وارد یک شبکه‌ای بشود که حداکثر سایز بسته ها در این شبکه کوچکتر از سایز بسته است، این بسته باید به قطعات کوچکتر شکسته بشود و دروِن آن شبکه جابجا بشود

حالا دوتا approach برای Fragmentation وجود دارد

Transparent Fragmentation_۱ Non Transparent Fragmentation_۲



(a) Transparent Fragmentation



(b) Non-Transparent Fragmentation

دیدگاه دوم می‌گوید اگر بسته ها را به قطعات کوچکتر تقسیم کردیم دیگه آنها را تا رسیدن به مقصد هرگز سرهم نکنیم

* طراحان شبکه (طراحان IPv4) براین ساده نگه داشتن هسته شبکه این وظیفه را به عهده سیستم‌های انتهایی گذاشتن ـ اگر عمل Fragmentation و reassembly (Defragmentation) را در هر روتر انجام دهیم این کار جز کارهای Data path ان شبکه می‌شود یعنی به ازای هر بسته ان این اتفاق باید رخ بدهد و هر وقت شما یک کار اضافه در Data path می‌کنید اگر دلیل خوبی براش نداشته باشید اون کار یک overhead اضافه در شبکه است

اما کوچکتر بودن بسته ها بطور یکه کوچکتر از آنی باشد که شبکه می‌تواند جابجا کند ۲ تا عیب دارد

۱ ـ یک بار اضافه برای روترها است.

۲ ـ بار شبکه ممکن است زیاد بشود: فرض کنید یک بسته را در شبکه اول به ۱۰۰ قطعه کوچکتر تقسیم کرده‌ایم و یکی از بسته ها در روتر دوم دور ریخته می‌شود و ۹۹ بسته می‌رسد به شبکه بعدی و پس این ۹۹ قطعه تمام

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه‌ی بعدی را طی می‌کند و به مقصد می‌رسد، حال ما در مقصد که می‌خواهیم Datagram را سرهم کنیم متوجه می‌شویم که یک قطعه گم شده است در این صورت لایه شبکه در سیزبان مقصد دیتاگرام ناقص را دور می‌اندازد، در اینصورت تمامی زحمت‌هایی که برای جابجا کردن ۹۹ قطعه دیگر در شبکه کشیده بودیم هدر می‌رود در صورتی که اگر بعد از اتمام هر شبکه قطعه‌ها را reassembly می‌کنیم، اگر reassemble نشد در همان جا متوجه می‌شویم و در نتیجه بقیه شبکه بعدی ارسال اش نمی‌کنیم

نکته) در حالتی که از مدل ۲ استفاده می‌کنیم وقتی مقصد نتوانست یک دیتاگرام را تشکیل دهد و آن را دور انداخت، اگر پروتکل لایه انتقال TCP باشد این پروتکل می‌تواند با استفاده از ساز و کار ارسال مجدد داده مفقود شده را دوباره بگیرد.

نکته - IpV6 عملیات Fragmentation را ساپورت نمی‌کند ← زیرا در روترهای جدید سرعت بسیار بالاست و آن قدر وقت کم داریم که فرصت تکه تکه کردن بسته‌ها را نداریم، البته دلایل دیگری هم دارد

پس چیکار می‌کند؟ در ابتدا شروع به تبادل اطلاعات MTu (min) مسیر پیدا می‌شود و از همان ابتدا این عدد به لایه انتقال گزارش می‌شود تا segmentation براساس کمترین MTu مسیر انجام شود ← RFC 1191

معایب دیگر Fragmentation

۱- تکه تکه سازی باعث پیچیده‌تر شدن روتر و عاست‌ها می‌شود، باید قابلیت قطعه قطعه کردن و چسباندن را هم در آن اضافه کنیم

۲- Fragmentation راه را برای حمله‌های DOS باز می‌کند (denial of service attack) (Jolt2)

۱- تعداد زیادی تکه کوچک که offset هیچ کدام نسبت به هم مشخص نیست به هدف ارسال می‌کند

۲- ارسال تعداد زیادی تکه که offset آنها همپوشانی داشته باشد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

تست سراسری ۸۴

- اگر مدل لایه ای دارای n لایه باشد و هر لایه h بیت سرآیند (header) به بسته دریافتی اضافه کند، برای رسیدن به بهره‌وری ۸۰٪ حداقل طول بسته داده‌ها بر حسب n و h چقدر است؟

۱) 8nh ۲) 6nh ۳) 4nh ۴) 2nh

پاسخ:

نکته ۱: وقتی در یک سوال از تریلر حرفی نمی‌زند آن را در نظر نگیرید

نکته ۲: ما می‌دانیم که لایه فیزیکال هدر ندارد ولی وقتی سوال می‌گوید n تا لایه هست که هر لایه یک هدر دارد، برای لایه فیزیکال هم هدر در نظر می‌گیریم

$$\text{بهره‌وری} = \frac{\text{مفید}}{\text{کل}} = \frac{80}{100}$$

$$\frac{k}{k+nh} = \frac{80}{100} \rightarrow 10k = 8k + 8nh \rightarrow 2k = 8nh \rightarrow k = 4nh$$

تست سراسری سال ۸۶

- برای ارسال پیام های ۱۰۰۰ بایتی لایه انتقال، ۲۴ بایت هدر در لایه انتقال و ۲۰ بایت سرآیند در لایه شبکه و ۲۲ بایت بایت سرآیند و ۴ بایت دنباله (Trailer) در لایه پیوند داده‌ها به هر واحد داده اضافه می‌شود. اگر محدودیت طول فریم در لایه پیوند داده ۲۵۰ بایت باشد، بهره انتقال چقدر خواهد بود؟

1) ٪۷۴.۱ ۲) ٪۸۵.۲ ۳) ٪۸۷.۱ ۴) ٪۸۹.۹

پاسخ: ما در لایه انتقال بشکنیم یا لایه نتورک یا لایه پیوند داده. اینکه ما در لایه پیوند داده محدودیت داریم به این معنا نیست که همین لایه محدودیت را اعمال می‌کند

گفته محدودیت طول فریم ۲۵۰ باید است و فریم شامل هدر و تریلر است، بنابراین داده فریم در این حالت می‌تواند ۲۲۴ بایت باشد، اگر میگفت محدودیت طول داده در فریم ۲۵۰ بایت است، این یعنی طول فریم ۴+۲۲+۲۵۰ یعنی ۲۷۶ بایت است.

دیتا لینک بسته را قطعه قطعه نمی‌کند و لایه شبکه هست که نمی‌تواند بسته‌های بزرگتر از ۲۲۴ بایت را به لایه پیوند داده بدهد. هدر خود لایه شبکه ۲۰ بایت است، بنابراین لایه انتقال نباید سگمنت بزرگتر از ۲۰۴ به لایه شبکه بدهد، حال هدر خود لایه انتقال۲۴ بایت است بنابراین انتقال نباید دیتای بیشتر از ۱۸۰ تا درون سگمنت‌اش بگذارد(بدون احتساب هدر).

الان ما داریم فکر می‌کنیم که قطعه قطعه شدن در لایه انتقال صورت می‌گیرد

$$\text{تعداد بسته} = \left\lceil \frac{1000}{180} \right\rceil = 6 \rightarrow \text{راندمان} = \frac{1000}{1000+6\times(24+20+22+4)} \times 100\% = 71\%$$

- اگر لایه شبکه قطعه قطعه کند
- لایه انتقال بسته با سایز ۱۰۲۴ تایی را به لایه شبکه می‌دهد

$$\text{تعداد بسته} = \left\lceil \frac{1024}{204} \right\rceil = 6 \rightarrow \text{راندمان} = \frac{1000}{1000+24+6\times(20+22+4)} \times 100\% = 77\%$$

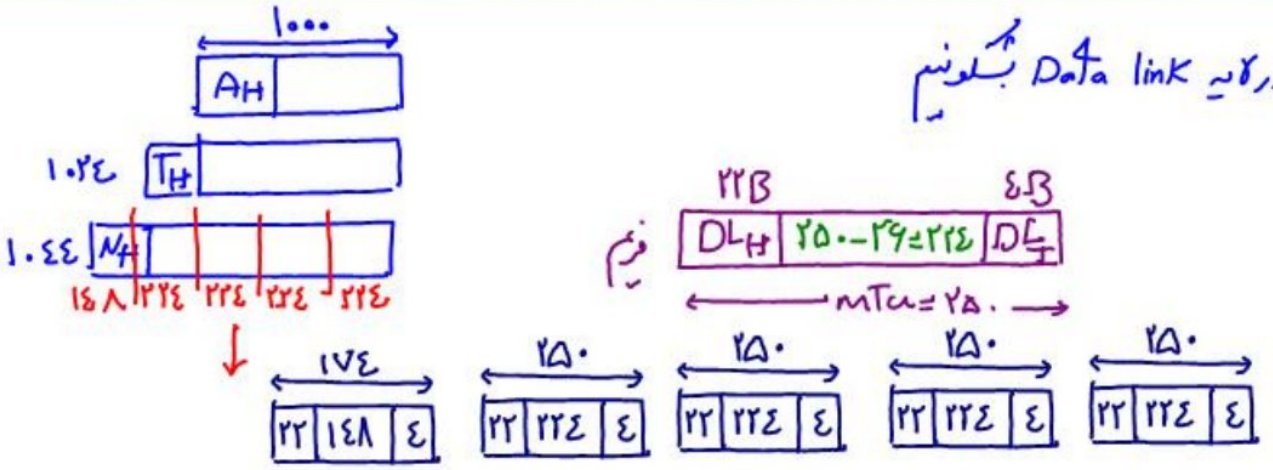
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

رامین رضوی

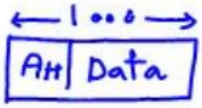
فرض ۱) در لایه Data link هستیم



$$\eta = \frac{\text{مفید}}{\text{کل داده}} = \frac{1000}{1000 + 24 + 20 + 5\times(22+4)} \times 100 \simeq 85\%$$

(T_H ، N_H)

فرض ۲) در لایه transport هستیم



$$MSS = MTU - [DL_H + DL_T + T_H + N_H]$$
$$250 - [22 + 4 + 24 + 20] = 180$$

۱۵٪) $\frac{1000}{900}\ \Big|\ \frac{180\ (MSS)}{5}$

$\frac{1000}{100}$

۲۵٪) $\left\lceil \frac{1000}{180} \right\rceil = 6$

$$\eta = \frac{\text{مفید}}{\text{کل داده}} = \frac{1000}{1000 + 6(22+4+24+20)} \times 100 = 71\%$$

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

سوالات مهم و متعددی

سوال ۱ـ ما گفتیم در لایه Data link می‌توانیم سرویس‌های Acknowledged را ارائه هیم حال چرا Ack را به لایه Data link سپردیم و به لایه Network نسپردیم اش؟

در بیشتر شبکه‌ها سایز بسته‌ای که در لایه ۳ می‌تواند جابجا شود خیلی بزرگتر از سایز بسته‌ای است که می‌تواند در لایه دو جابجا شود به علت اینکه معمولاً phy ما مجبوری است که باید بسته‌ها درون اش کوچک باشند مثلاً اندازه پکت در لایه ۳ می‌تواند ۶۴ هزار بایت باشد ولی در لایه ۲ شاید لازم است بسته‌ها شکسته به ۱۰۰۰ بایت.

سوال) فرض کنید بسته‌ای داریم 64KB که در لایه Data link به بسته‌های هزار بایتی می‌شکنند، دو سناریو را بررسی کنید ۱ـ Ack ها در لایه ۳ رد و بدل نشوند
۲ـ " " " ۲ " "

۱ـ لایه شبکه یک بسته 64KB را به لایه Data link می‌دهد، Data link این را می‌شکند به ۶۴ بسته حال اگر از این ۶۴ بسته دوتاش خراب شود یا گم بشود، چون کل قطعه‌ها نرسیده لایه ۲ طرف مقصد به لایه ۳ هیچی تحویل نمی‌دهد، ما برای این لایه شبکه ack نمی‌دهد پس ما برای این مجبور می‌شویم همه ۶۴ قطعه را دوباره ارسال کنیم اما اگر این Ack را در لایه ۲ بگذاریم فقط اون دو تکه‌ای که نرسیده دوباره به مقصد فرستاده می‌شود

۲ مزیت دارد این کار:
۱) تاخیر کمتری خواهیم داشت
۲) در منابع کانال فیزیکی صرفه جویی می‌شود

نکته) اگر سایز پکت‌های لایه ۳ و فریم‌های لایه ۲ مان مثل هم بود فرقی نمی‌کرد (که نیست)

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

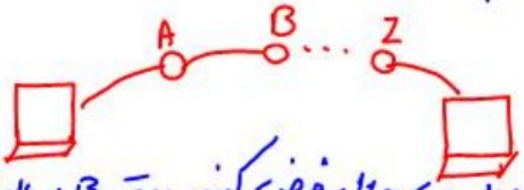
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

سوال ۲ـ اگر ما در لایه Data link ، Ack داریم و مطمئن هستیم که همیشه بین دو نود بسته هایمان می رسد چرا در لایه Transport هم Ack میگذاریم ؟



فرض کنید از A به B صد تا بسته می فرستیم و همه آنها نیز به B می رسند ، حال فرض کنید روتر B به علت پر بودن بافرهایش دو تا از این بسته ها را در لایه شبکه اش Drop می کند ، حالا روتر B به C ۹۸ بسته ارسال می کند و همه ۹۸ بسته را هم گارانتی می کند که به C تحویل بدهد که میدهد و ack هایش هم در لایه Data link دریافت می کند ، اما باز ممکن است روتر B به دلیل ازدحام بسته هایی را در لایه شبکه Drop کند بنابراین گارانتی کردن در لایه ۲ (Ack دادن) ، نمیتوان همه بسته های end to end را گارانتی می کند

سوال ۳ـ حالا که در لایه Transport ، Ack داریم در لایه دو Ack نداریم دیگر ؟ اگر در لینک AB یک بسته از A به علت نویز روی رسانه یا هر دلیل دیگری خراب شود یا گم شود بهتر نیست A دوباره همان را برای B بفرستد به جای اینکه کل یک شبکه که ۱۰۰۰ تیکه شده است را از مبدا به مقصد بفرستیم

سوال ٤ـ چرا با وجود اینکه MAC address داریم ، آدرس IP هم می خواهیم ؟

آدرس های IP ، Routable هستند ولی آدرس های MAC نیز کمی اینجوری نیستند ، مثلا هر فردی یک کد ملی یونیک دارد ، حالا آیا می شود از روی کد ملی بفهمیم براحتی که اون شخص کجاست ؟ این کار خیلی سخت تر از حالتی است که ما بخواهیم از روی آدرس پستی یکی و پیدا کنیم ، در واقع آدرس های پستی Routable هستند ولی کد ملی Routable نیست

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

سوال ۵ - چرا با وجود اینکه آدرس IP داریم به MAC address نیاز داریم؟

۱- آدرس های IP چند قطعی هستند که برای راحتی مسیریابی در اینترنت ایجاد شده و برای این ایجاد شده که ما تعداد خیلی زیادی کامپیوتر و تجهیزات داریم که می خواهیم اینها را هم وصل کنیم ولی ما در یک شبکه محلی تعداد خیلی زیادی تجهیزات نداریم و در نتیجه نیازی به مسیریابی خیلی پیچیده ای نداریم

۲- تطابق با گذشته: اگر آدرس MAC حذف بشود بسیاری از تجهیزات، پروتکلها و طراحی ها باید عوض بشود

۳- این دلیل را محیا می کند که به جای اینکه فقط شبکه های TCP/IP داشته باشیم، شبکه های نوع دیگری هم داشته باشیم و در لایه ۲ تنوع بسیار زیادی از پروتکل ها داشته باشیم که هر کدام برای شرایط و سناریوهای مختلف مناسب و بهینه است

۴- تجهیزات لایه دو معمولا ساده تر و ارزان تر است و این مورد در گسترش شبکه های محلی مهم است. برای گسترش شبکه در فواصل کوتاه نیازی نیست که ما تجهیزات گرانقیمت لایه ۳ داشته باشیم

۵- سوئیچ های لایه دو بسته ها را فقط بر اساس MAC address روی یکی از پورت هایشون Forward می کنند

۶- wireless access point ها که یکی از Device های مهم شبکه است اغلب از MAC address برای access control استفاده می کنند. AP ها فقط به Device هایی که می شناسند اجازه دسترسی می دهند، چون MAC آدرس یونیک است وقتی شما بار اول به یک AP وصل می شوید AP نگه می دارد MAC شما را

۷- برای MAC filtering در AP ها استفاده می شود

۸- DHCP server ها از آدرس MAC برای شناسایی Device ها و دادن آدرس های IP ثابت به برخی از Device ها استفاده می کند.

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

NIC (Network Internet card) : کارت شبکه می‌توانند با توجه به بستری که داریم استفاده می‌کنیم سفارش بالا . تمامی Device هایی که به اینترنت وصل می‌شوند باید کارت شبکه داشته باشند ، هر کارت شبکه یک MAC آدرس اختصاصی منحصر به فرد ۴۸ بیتی دارد MAC address : 48 Bit = 6 (Byte)

دست خود شرکت ها

01-78-3B-09-95-7c

OUI (organizationally uniq identifer) → ۳ بایت اول از سمت سازمان هایی به تولید کنندگان شبکه اختصاص داده می‌شود

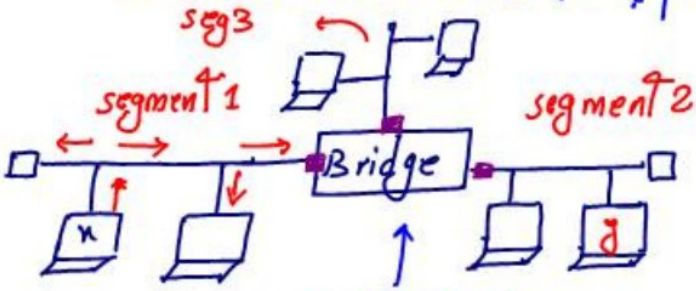
* آدرس یک توسط شرکت سازنده بر روی حافظه Rom ای که روی NIC قرار دارد برنامه ریزی می‌شود

MAC address = physical address

Hub : هاب در شبکه star تمام کامپیوترها را در لایه ۱ هم وصل میکرد . قبلا گفته شده

Repeater : قبلا توضیح داده شده

Bridge : Device ها لایه ۲ ای هستند ، یعنی اینکه توانایی این را دارند که از سگمنت ها فریم بسازند و می‌توانند داخل فریم را مشاهده کنند یعنی آدرس یک مبدا و یک مقصد را می‌توانند ببینند بنابراین می‌توانند براساس اینکه سگمنت را به کجا (کدام پورت) بفرستند هوشمندانه عمل کنند



Bridge table

MAC add	segment
mac x	۱
mac y	۲

* وقتی بسته ای به B می‌رسد B دو کار می‌کند

① learning :

② Forwarding

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

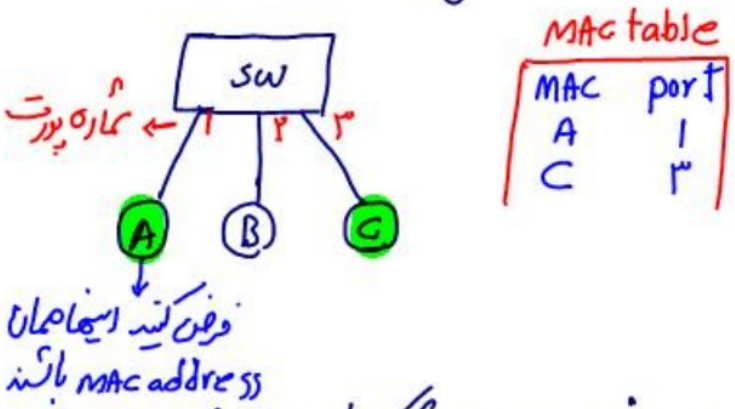
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

switch : هر سوئیچ یک MAC table که شبیه Bridge table است.

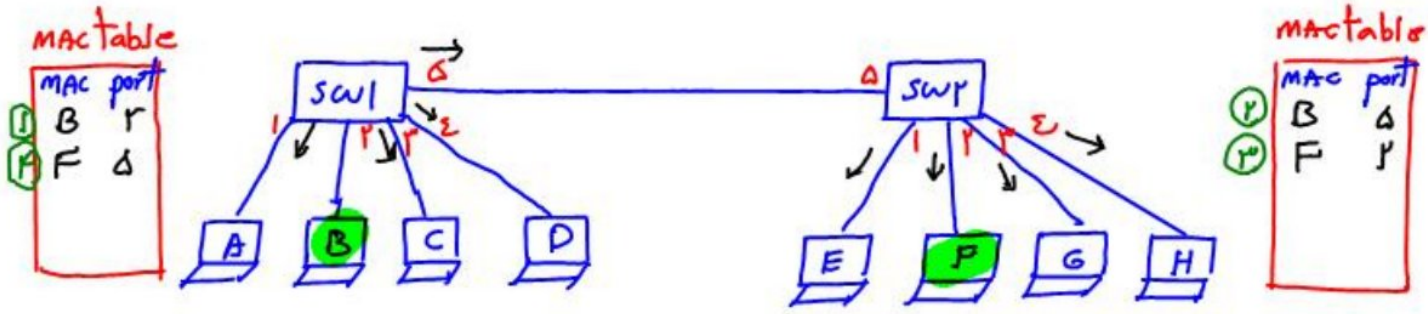


وقتی کنید اینها همان MAC address باشند

* ارتباطات همزمان را تا حدی میسر می کند

- Broadcast message : پیام هایی هستند که مقصدشون هم اعضا شبکه لوکال هستند.

(BD) Broad cast Do main : یعنی محدوده ای که اگر ما توش داد بزنیم به گوش هم می رسه، پیام های Broadcast در لایه ۲ منتشر می شوند، بنابراین تا زمانیکه شما یک شبکه دارید که توش ۱۰۰ تا هاب و سوئیچ و ... هم وصل هستند همه اینها یک BD هست، پس ما به تعداد پورت های روتر BD داریم



Router : روتر یک Device لایه ۳ (IP) است پس تا لایه ۳ می تواند بفهمد و تقسیم گیری برای ارسال را بر اساس لایه ۳ انجام دهد. در سوئیچ ما تا لایه ۲ می فهمیدیم بنابراین پورت ها لازم نیست آدرس IP داشته باشند و تقسیم گیری برای ارسال را با استفاده از MAC address انجام میدهند ولی هرکدام از پورت های روتر باید یک آدرس IP داشته باشد

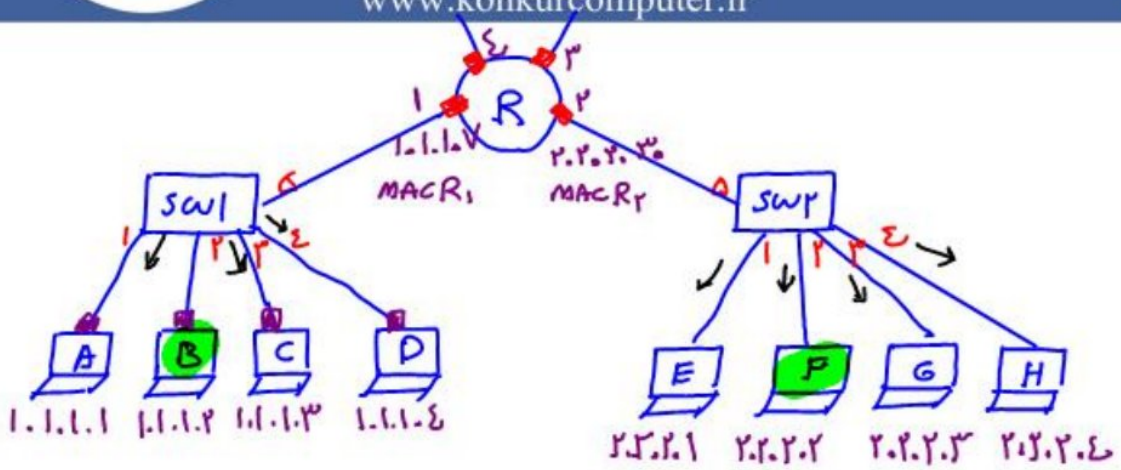
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir



نکته ـ آدرس IP مبدا و مقصد در طول مسیر تغییری نمی کند و بازی با MAC Address ها است که باعث می شود که شبکه های مختلف را رد کنیم تا در نهایت به مقصد برسیم

نکته ـ وقتی یک کامپیوتر می خواهد به یک مقصدی دیتا بفرستد، ابتدا در لایه شبکه IP مبدا و مقصد را روی Datagram لایه شبکه می گذارد، حالا وقتی می خواهد در لایه Data link فریم را ببندد، سورس مک را می گذارد ولی بر روی قرار دادن مک آدرس مقصد دو حالت وجود دارد ① یا IP مقصد و IP مبدا در یک شبکه هستند که در اینصورت کامپیوتر فرستنده آدرس مک مقصد را برابر همان مک آدرس مقصد می گذارد ② یا اینکه IP مقصد با IP مبدا در یک شبکه نیست که در اینصورت کامپیوتر فرستنده آدرس مک مقصد را برابر مک آدرس Gateway قرار می دهد

حال سوال اینجاست که دستگاه من (فرستنده) آدرس مک خودش را میدانند ولی آدرس مک یک کامپیوتر دیگر و یا یک روتر یا gateway را از کجا می داند؟

(Address resolution protocol) ARP

موقعی که داریم فریم را می بندیم اگر Destination MAC را ندانیم، در همان لحظه این لایه را متوقف می کند فرستنده و یک بسته دیگری بنام ARP Request ایجاد می کند، داخل این بسته آدرس IP و MAC مبدا و IP مقصد گذاشته می شود و Destination MAC خالی گذاشته می شود و سپس این بسته را Broadcast

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

می‌کند، این بسته به دست تمامی Device ها در این شبکه می‌رسد و آن Device ای که می‌بیند که Ip اش با Ip مقصد بسته یکی است او Ip را در جدولی بنام ARP table یادداشت می‌کند که Ip مبدا روی این بسته، چه مک آدرسی دارد و سپس این بسته را دور می‌ریزد و یک بسته دیگر بنام ARP reply درست می‌کند و هد مقادیر Ip مبدا و مقصد و مک آدرس مبدا و مقصد را در این بسته می‌گذارد و این بسته را unicast اش می‌کند و وقتی کامپیوتر مبدا این بسته را دریافت کرد دیگر می‌داند که مک آدرس مقصد چیست. در واقع موقعی که یک کامپیوتر می‌خواهد بسته‌ای ارسال کند که مک آدرس مقصد را ندارد یک بسته ایجاد می‌کند و این را Broadcast می‌کند و در واقع با این پیام می‌گوید من کامپیوتری هستم با این آدرس Ip و می‌خواهم برای کامپیوتر x که Ip اش x است یک بسته بفرستم، می‌شه هرکسی که آدرس Ip اش این هست آدرس مک اش را به من بگه

Broadcast کردن این پیام دو تا فایده دارد

1) فرستنده، آدرس مک مقصد را می‌فهمد و می‌تواند بسته را درست کند
2) چون فرستنده این پیام را Broadcast می‌کند هر کسانی که در این شبکه هستند می‌فهمند که فلان آدرس Ip، آدرس مک اش چی هست.

در اثر این کار هر کامپیوتر برای خودش یک جدول بنام ARP cache بصورت زیر درست می‌کند

Ip Address	MAC add	expiry Time
⋮	⋮	⋮

نکته ۱ - زمانیکه می‌خواهیم برای یک بسته مک مقصد را بدانیم اول می‌رویم سراغ ARP cache و اگر در ARP cache پیدا نشد، می‌رویم و ARP communication انجام می‌دهیم

نکته ۲ - وقتی یک کامپیوتر متصل به شبکه Boot می‌شود، یک پیام ARP بصورت Broadcast ارسال می‌کند که در آن Ip مبدا و مقصد خودش را می‌گذارد که به اینصورت هرکسانی که در آن شبکه هستند که این آدرس

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

آدرس یک لوپ بک است.

نکته ۳- این پیام بصورت پریودیک (مثلاً هر ۱۰ دقیقه یکبار) در شبکه ارسال می‌شود که entry آن در ARP cache کامپیوترهای دیگر renew بشود

نکته ۴- برای هر entry در ARP cache یک expiry time در نظر می‌گیرند که اگر در این مدت بستگان به IP آن سطر رد و بدل نشود ARP cache آن سطر را پاک می‌کند

نکته ۵- توجه کنید که ARP پروتکلی است در لایه Data link.

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

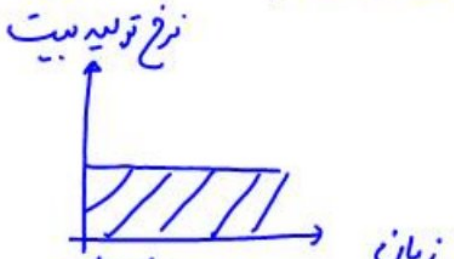
@konkurcomputer
www.konkurcomputer.ir

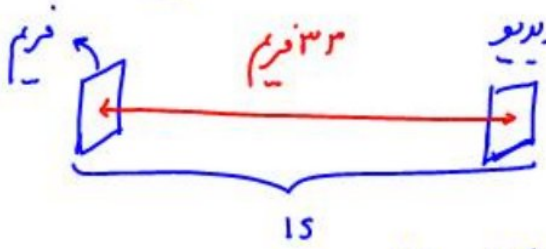
نکته ۱ - سرویس انتقال گرا به اتصال در لایه شبکه و در سیستم های انتهایی پیاده می شوند، در برقراری یک اتصال به انتقال فقط دو سیستم انتهایی طرفین آن اتصال شرکت دارند و فقط سیستم های انتهایی هستند که پارامترهای اتصال را تعیین می کنند و سیر یاب های شبکه هیچ چیز درباره آن اتصال نمی دانند.

نکته ۲ - در برقراری یک اتصال به شبکه (مفهوم connection oriented بودن به شبکه) تمام سیر یاب هایی که در مسیر مبدا و مقصد هستند از اتصال آگاه اند و اطلاعاتی از اتصال را نگه می دارند

انواع ترافیکی که ما ست ع در شبکه تولید می کنند به ۲ دسته تقسیم می شود

① CBR (constant bit rate) : نرخ بیت تولیدی در طول زمان ثابت است ← مثل

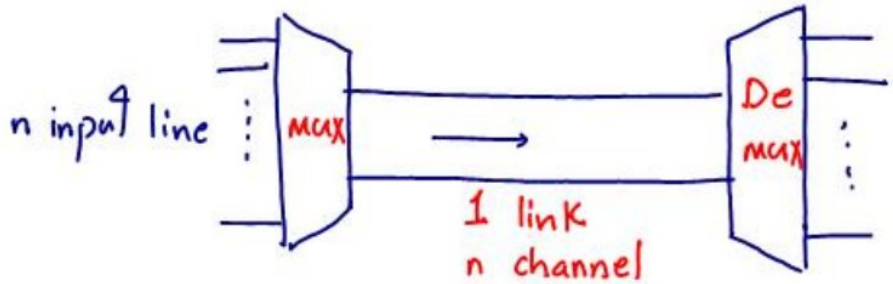




② VBR (variable bit rate)

مثال : وب گردی

انواع multiplexing



تعریف channel: بخشی از ظرفیت یک لینک یا شبکه که داده های بین یک فرستنده و گیرنده را حمل می کند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

انواع multiplexing

۱- FDM

۲- wDM (wave division ~)

۳- TDM
- TDM همگام
- TDM آسنکرون = TDM آماری (statistical TDM)

۴- cDM (code division ~)

* ما یا یکان (فضا) را می‌توانیم تقسیم کنیم یا زمان را.

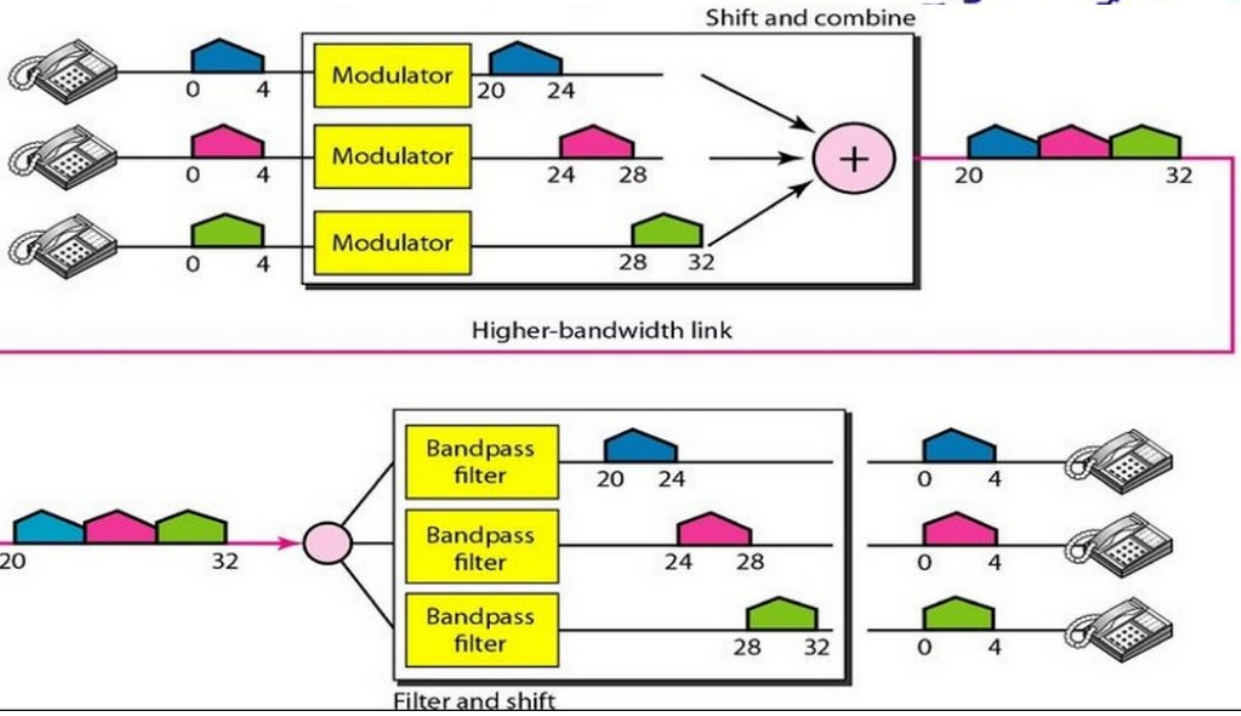
۱- FDM

فرکانس (هرتز) (f)

channel ۳
guard Band
channel ۲
guard band
channel
t →

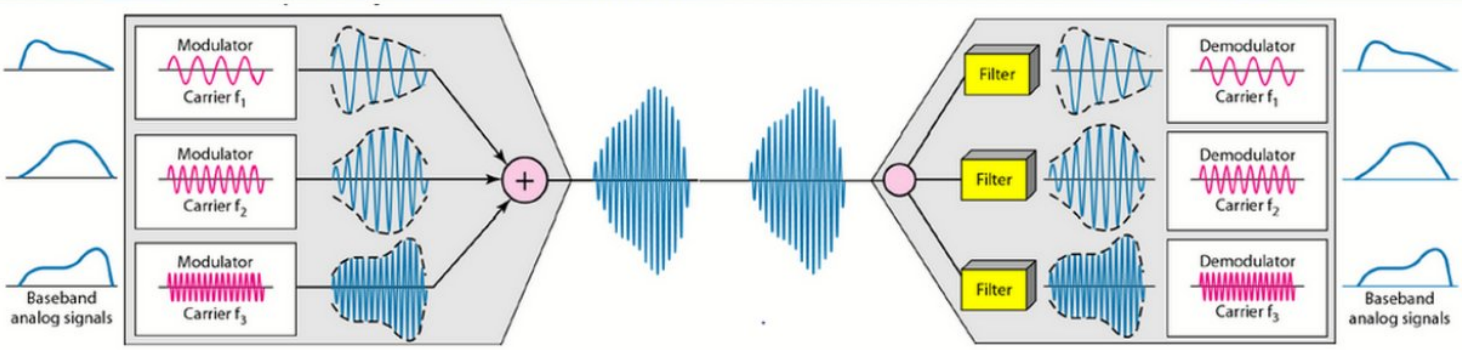
بخشی از فضا فرکانس کیک
برای همیشه به هر کانال
تخصیص داده می شود

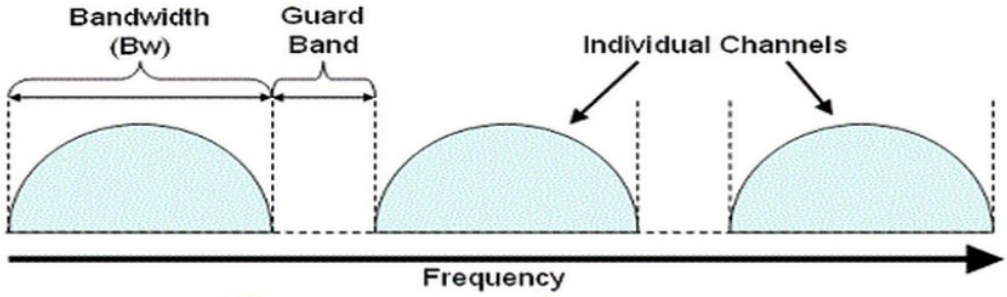
مثال - رادیو، تلویزیون، ماهواره



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

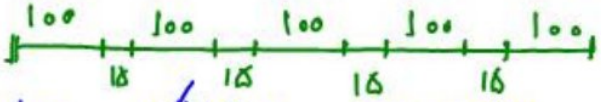
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir
MSc-PhD Computer-IT





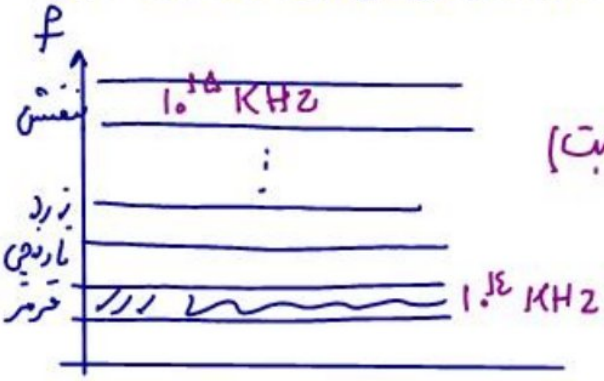
باند محافظ (Guard band) : برای جلوگیری از تداخل سیگنال های کانال های مختلف در هنگام استفاده از FDM بین کانال های فرکانسی مختلف بخشی از فرکانس را بعنوان حاشیه امنیت آزاد می گیرند

مثال - ۵ کانال داریم که هرکدام دارای پهنا باند ۱۰۰ KHZ هستند که می خواهیم این کانال ها را روی یک لینک multiplex کنیم اگر بین کانال ها مجبور باشیم (بخواهیم) یک باند محافظ 10KHZ نداریم ، حداقل پهنا باند لازم چقدر است؟



جواب = لینک Bw = ۵۶۰ KHz

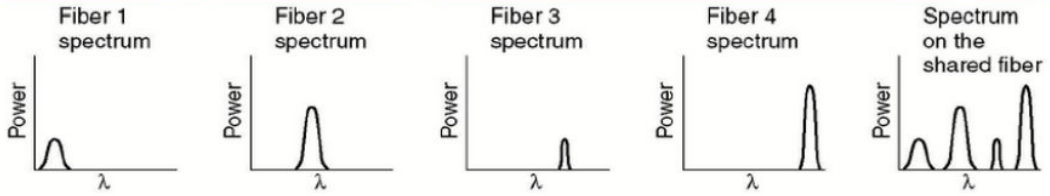
WDM (۲ : در واقع یک نوع FDM است . FDM در فرکانس های نوری های مرئی

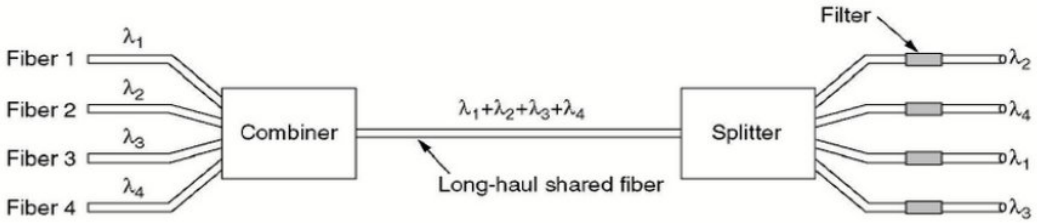


$c = f \times \lambda$ (عدد ثابت) $f \uparrow \quad \downarrow \lambda$

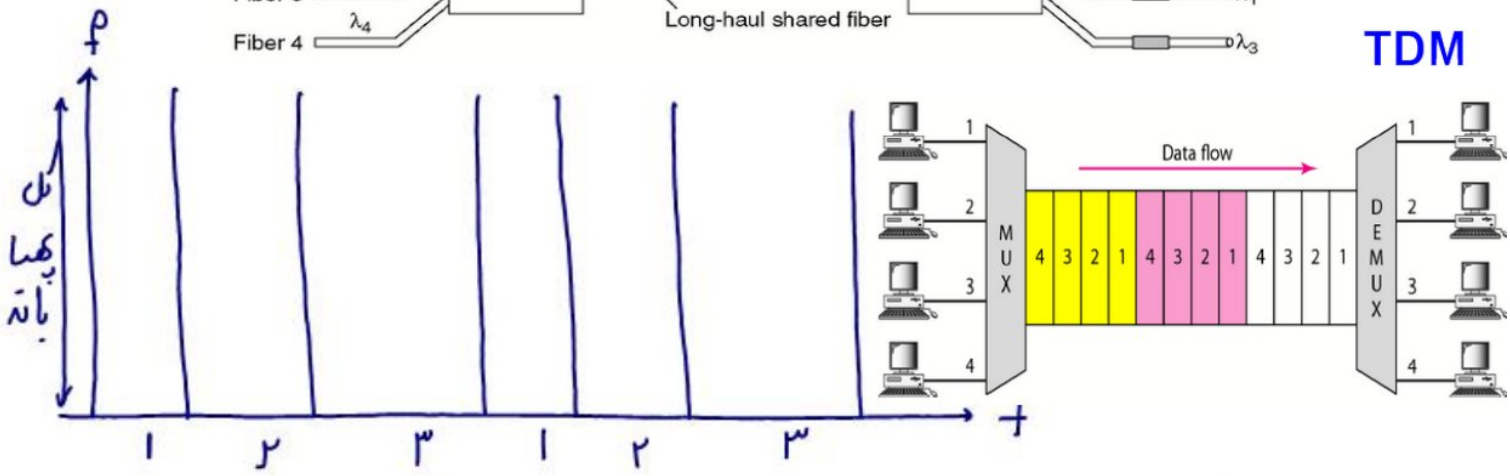
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir
شبکه های کامپیوتری
رامین رضوی

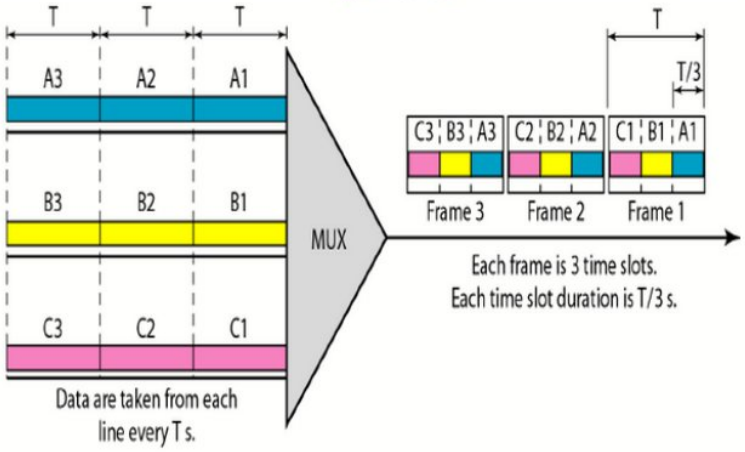


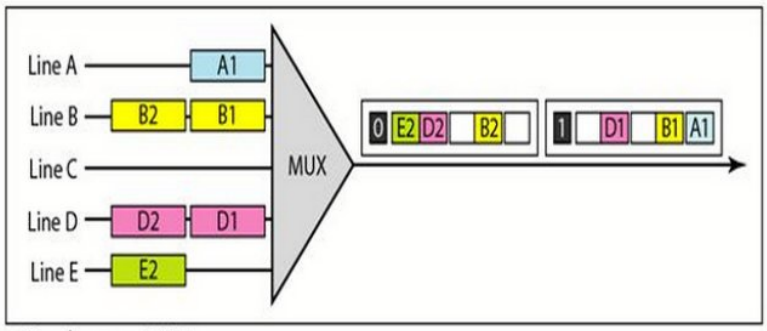


TDM

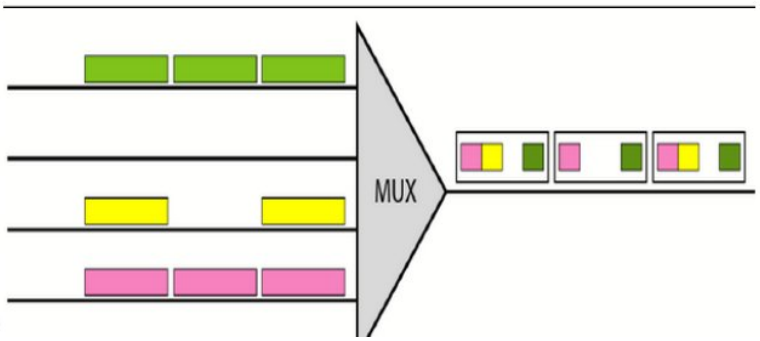


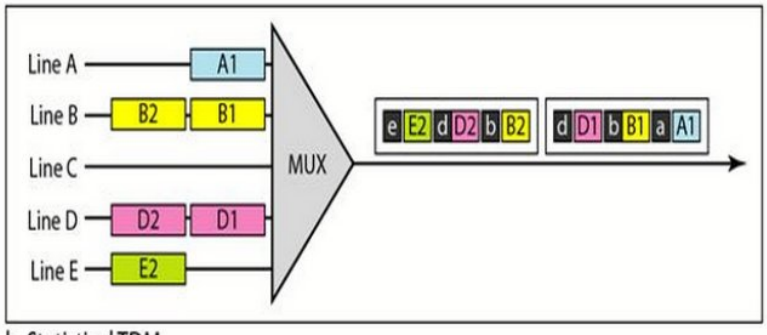
نرخ انتقال هر کانال = تعداد فریم در ثانیه × تعداد بیت هایی که در یک slot ای می توانیم انتقال بدهیم





a. Synchronous TDM





b. Statistical TDM

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

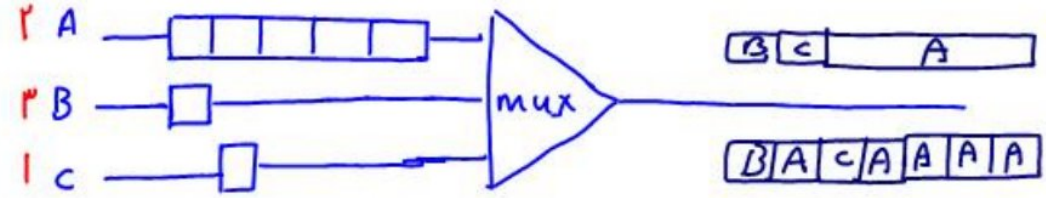
@konkurcomputer
www.konkurcomputer.ir

انواع statistical mux

نوبت گیرنده می‌شود هر : course grained manner
چقدر دیتا دارد بفرستد ← امکان ایجاد Delay و starvation

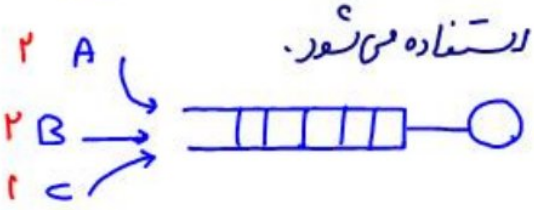
packet by packet : Fine grained manner

* گیرنده مشخص از بایت‌ها



نحوه برداشتن بسته‌ها از روی خط‌ها مختلف می‌تواند متفاوت باشد مثلاً RR یا WFQ

که بیشتر WFQ (weighted Fair queuing) استفاده می‌شود.



انواع سوئیچینگ

۱- circuit switching : سوئیچینگ مداری
۲- packet " : " بسته‌ای
۳- virtual circuit : مدار مجازی

circuit switching

۱- قبل از تبادل دیتا، جهت برقراری اتصال با یک connection setup اولیه، یک اتصال نیزیکی ثابت بین مبدا و مقصد برقرار می‌شود، بنابراین یک تاخیر اولیه داریم، یعنی به خاطر فاز اتصال اولیه شروع کندتری داریم

۲- همه بسته‌ها از یک مسیر ثابت به سمت مقصد می‌روند

۳- ترتیب دریافت بسته‌ها در مقصد به‌همان ترتیب ارسال در مبدا است

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

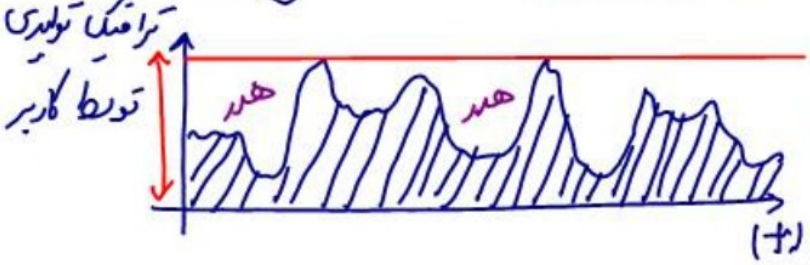
شبکه های کامپیوتری

رامین رضوی

۴ـ کلیه منابع لازم برای این ارتباط در روترها و سوئیچ ها بین راه رزرو می شوند. این منابع شامل موارد زیر هستند
۱ـ پهنای باند (Bandwidth) (FDM یا TDM)
۲ـ processing time
۳ـ (بافر) memory

* در circuit switch چون منابع Dedicate می شود کسی نیاز نیست در صف منتظر بماند (منظور صف لینک های خروجی روتر نیست)

نکته مهم: برای هر کانال (تست) به میزان حداکثری که آن تست منبع نیاز دارد رزرو می شود



⇒ به اندازه پیک رزرو می شود
⇒ تمام قسمت های بعد هدر می شود

بدی: هدر رفتن منابع
خوبی: پارامترهای کیفیت سرویس (QOS) مثل Delay، jitter، Bit rate (گفته شده) را می توانیم تضمین کنیم

۵ـ circuit sw مناسب hostهایی است که ترافیکشون CBR است، در اینصورت هیچی هدر نمی رود.

نکته بسیار مهم: در circuit sw اگر نگفتند که یک کانال چطور بین circuitها تقسیم شده خواهیم داشت
① کانال را بصورت مساوی و ثابت بین circuitها تقسیم می کنیم
② به اندازه حداکثر مورد نیاز هر circuit تقسیم می کنیم

۶ـ اگر دو host مجددا بخواهند با هم تبادل دیتا انجام بدهند، مجددا فازهای connection setup خواهیم داشت و دیتاها از مسیر ثابت جدید منتقل می شوند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

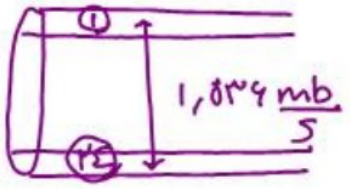
۷ - پس از پایان ارتباط connection release خواهیم داشت و سایع دزاد می‌شوند

۸ - در circuit switch هر بیتی که به روتر می‌رسد (اگر خط مشغول نباشد) ما می‌توانیم بلا فاصله به سمت مقصد ارسال اش کنیم و نیاز نیست وایستیم تا کل بسته بیاد

یعنی چی خط مشغول نباشد؟

زمانیکه بیت ها از یک بسته در حال transmit (انتقال) بر روی لینک خروجی یک روتر است لینک اشغال است

تست ۱ - فرض کنید یک شبکه circuit switching داریم که از TDM multiplexing استفاده می‌کند، در هر لینک ۲۴ برش زمانی داریم، نرخ انتقال کل link برابر $1,536 \frac{Mb}{s}$ است. اگر زمان circuit setup برابر ۵۰۰ ms باشد، کل زمان لازم برای انتقال یک فایل به اندازه ۸۰KB چقدر است؟



$$R_{channel} = \frac{R_{کل}}{24} = \frac{1,536 \times 10^6 b}{s \times 24} = 64 \times 10^3 \frac{b}{s}$$

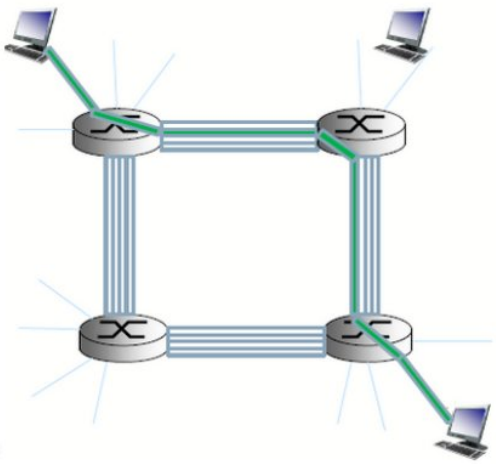
$$d_{کل\ تاخیر} = d_{circuit\ setup} + d_{trans} = 500\ ms + 10\ s = 10,5\ s$$

10^{-3}

$$d_{trans} = \frac{L}{R_{channel}} = \frac{80 \times 10^3 \times 8 \times 5}{8 \times 64 \times 10^3} = 10\ s$$

$$10 \times 10^3 \times 10^{-3}\ s = 1000\ ms$$

مثال



- فرض کنید در شبکه سوئیچ مداری صفحه قبل روی هر لینک n مدار می‌تواند بطور همزمان وجود داشته باشد (که این مدارات می‌توانند بصورت TDM یا FDM مالتی پلکس شوند) در این شبکه در هر لحظه حداکثر چند اتصال همزمان می‌تواند وجود داشته باشد؟

پاسخ : 4n

- اگر در سوال بالا همه ارتباطات بین سوئیچ بالا سمت چپ و سوئیچ پایین سمت راست باشد حداکثر تعداد اتصالات همزمانی که می‌تواند وجود داشته باشد چقدر است؟

پاسخ : می‌توانیم n اتصال از بالاترین سوئیچ گوشه راست عبور دهیم و n اتصال از پایین‌ترین سوئیچ گوشه چپ عبور دهیم، بنابراین در کل 2n اتصال خواهیم داشت

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

packet switching

۱- فاز connection setup نداریم و بنابراین تاخیر اولیه برای برقراری ارتباط وجود ندارد و بنابراین شروع اولیه سریع آن خواهیم

۲- بسته ها مسیر ثابتی بین مبدا و مقصد را نمی پیمانند مسیرها با توجه به شرایط شبکه بصورت دینامیک عوض می شوند چون هر بسته که به یک روتر می رسد، آن روتر در همان لحظه بصورت مستقل با توجه به forwarding table آن بسته را از یک پورت خارج می کند

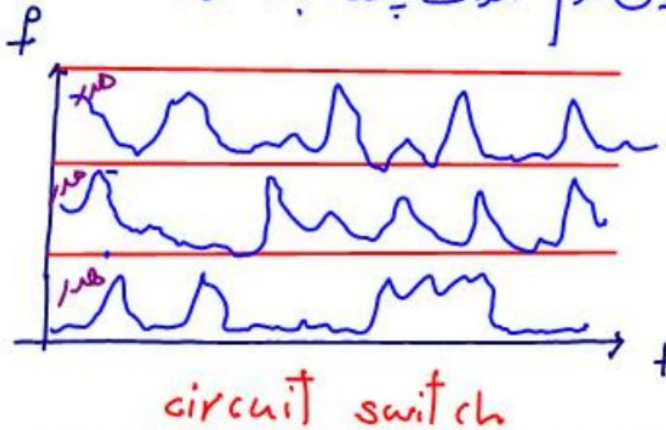
۳- ترتیب رسیدن بسته ها به مقصد با ترتیب ارسال بسته ها در مبدا لزوما یکسان نیست

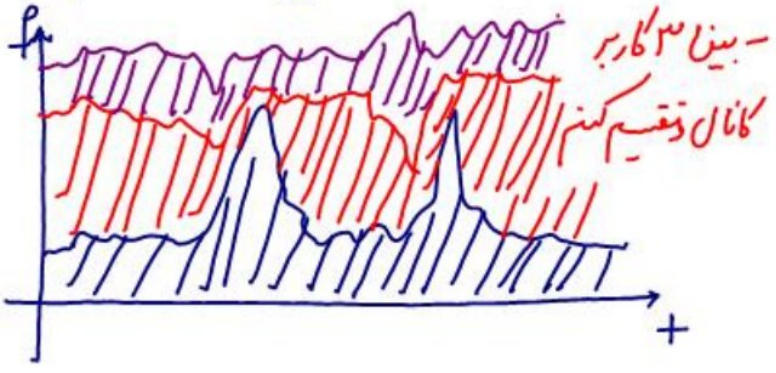
۴- در اینجا هیچ منبعی رزرو نمی شود و بنابراین نمی توان QoS را گارانتی کرد
مثلا نمی توان Delay، حداقل گذردهی، Jitter را تضمین کرد

۵* - در سوئیچ بسته ای از تکنیک store & forward استفاده می شود، یعنی اگر یک روتری بخشی از بسته را دریافت کرده باشد و مثلا هدر بسته رسیده باشد و سرچک شده باشد که IP مقصد چیست باز هم نمی توانید بسته را ارسال کنید و باید بسته بصورت کامل وارد روتر شود و ذخیره شود (store) و پس با توجه به IP مقصد forward شود

۶** - packet switch اشتراک گذاشتن خطوط انتقال بهتر عمل می کند، زیرا سوئیچ بسته ای منابع را رزرو نمی کند و یعنی باند مجازی را برحسب تقاضا کاربران به آنها تخصیص می دهد، یعنی بصورت دینامیک این کار را می کند

بنابراین یکی از مزیت ها این هم این روش عدم اتلاف پهنای باند است





سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

۷- تعداد کاربرانی که می‌توانند از منابع استفاده کنند در روش packet switch حدوداً بیش از ۳ برابر کاربران circuit switch می‌توانند

ثبت) فرض کنید n کاربر یک link با نرخ انتقال 1 Mbps را به اشتراک گذاشتند. هر کاربر به تناوب بین دوره‌های فعال و غیرفعال سوئیچ می‌کند و در دوره فعال با نرخ ثابت $100 \frac{Kb}{s}$ اقدام به ارسال داده می‌کند. همچنین فرض کنید هر کاربر فقط در ۱۰ درصد زمان‌ها فعال است

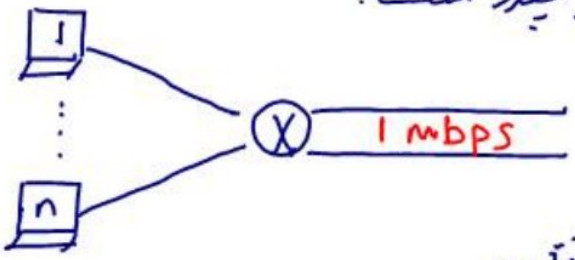
سوال ۱- در circuit switching حداکثر چند کاربر می‌توانند همزمان داده ارسال کنند

" ۲- در " packet اگر ۳۵ کاربر داشته باشیم

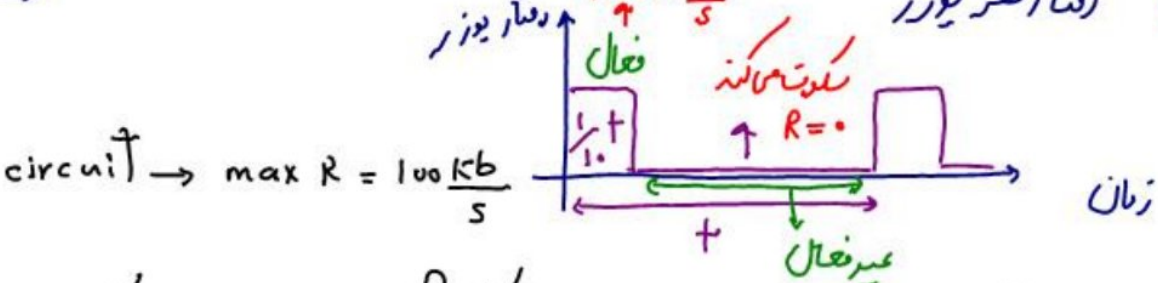
الف) احتمال آنکه در یک لحظه از زمان ۱۱ کاربر فعال باشند چقدر است؟

ب) " تشکیل صف در خروجی روتر چقدر است؟

* نکته) شکل شبه واقعیت است.



حل سوال ۱) رفتار هر یوزر



تعداد افرادی که می‌توانند همزمان داده ارسال کنند $= \frac{R_{کل}}{R_{channel}} = \frac{1 Mbps}{100 Kbps} = \frac{10^6 bps}{100 \times 10^3 bps} = \boxed{10}$

* باید بطور دائم بران هر یوزر $100 \frac{Kb}{s}$ کنار بذاریم که در اینصورت ۱۰ یوزر می‌توانیم داشته باشیم

* ۹۰ درصد ظرفیت انتقال کانال دارد هدر می‌شود چون هم اون ۱۰ تا کاربر فقط در ۱۰ درصد زمان ۱۰۰ kb را پر می‌کنند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

رامین رضوی

نکته) درحالتی که ۳۵ یوزر داریم، اگر تعداد یوزرهایی که همزمان با هم فعال می‌شوند کمتر مساوی ۱۰ باشد بسته‌ها بدون تاخیر انتظار سیگنال عبور می‌کنند و صف تشکیل نمی‌شود و مثل حالت circuit switching عمل می‌شود

اگر ۱۱ کاربر بخواهند بطور همزمان عمل ارسال را انجام بدهند پهنای باند مورد نیاز $\frac{mb}{s}$ ۱/۱ خواهد بود که از پهنای باند در دسترس لینک به اشتراک گذاشته شده بیشتر است و درنتیجه صف تشکیل می‌شود و تاخیر صف خواهیم داشت

نتیجه: اگر بیشتر از ۱۰ کاربر بصورت همزمان بخواهند دیتا ارسال کنند صف خروجی روتر شروع به زیاد شدن می‌کند

الف) باید ۱۱ تا فعال باشند و ۲۴ تا دیگر حتما غیرفعال باشند

احتمال فعال بودن ۱ کاربر = احتمال ارسال کردن ۱ کاربر = ۰/۱

احتمال آنکه کاربر ۱ و کاربر ۲ باهم ارسال کنند = ۰/۱ × ۰/۱ = ۰/۱۲

$$\binom{35}{11} (0/1)^{11} \times (0/9)^{24}$$

نکته) بطور کلی اگر در این سوال m کاربر در یک لینک مشترک می‌بودند، بطوریکه احتمال فعالیت هر کاربر برابر p باشد، احتمال آن که در یک لحظه از زمان n کاربر فعال باشند برابر است با

$$\binom{m}{n} p^n \times (1-p)^{m-n}$$

ب)

احتمال تشکیل صف = احتمال ارسال ۱۱ تا همزمان + احتمال ارسال ۱۲ تا + ـــ + احتمال ارسال ۳۵ تا همزمان

$$\sum_{i=11}^{35} \binom{35}{i} (0/1)^i (0/9)^{35-i} = 0/0004$$

* در ۹۹/۹۶٪ لحظات صف تشکیل نمی‌شود و کیفیت مانند circuit switching است و در ۰/۰۴٪ لحظات صف داریم و کمی تاخیر داریم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

تست) فرض کنید ۱۰ کاربر داریم و یک کاربر بطور ناگهانی فایلی به حجم 1 Mbit ارسال می‌کند (۱۰۰۰ بسته ۱۰۰۰ بیتی ارسال می‌کند)، همچنین فرض کنید در این زمان (لحظه) فقط این کاربر ارسال می‌کند، اگر نرخ انتقال link برابر 1Mbps باشد مطلوبست محاسبه زمان انتقال این فایل

الف) در circuit switch

ب) در packet switch

الف) $R_{channel} = \frac{R_{Link}}{n} = \frac{1Mbps}{10} = 100 \frac{Kb}{s}$ per channel

$$d_{trans} = \frac{1 \times 10^6 b}{100 \times 10^3 b} = \boxed{10\ s}$$

ب) تقسیم بر حسب تقاضا و داینامیک است ← فقط ۱ تعرفعال است

$$R_{channel} = R_{Link} \qquad d_{trans} = \frac{1Mb \times s}{1Mb} = \boxed{1\ s}$$

اگر ۲ کاربر بصورت همزمان فعال باشند ← به هرکدام نصف پهنا باند می‌رسد ← ۲ ثانیه طول می‌کشد

" ۳ " ← " " " " " ۱/۳ " " ← " " " " " ۳ "

⋮

" ۱۰ " ← " " " " " ۱/۱۰ " " ← " " " " " ۱۰ "

* حتی اگر تعداد کاربران در CS و PS یکسان باشند باز هم PS بهتر است، چون PS می‌تواند نرخ بیشتری را در اختیار کاربرین فعال قرار بدهند

- PS از پهنا باند کانال بصورت بهینه استفاده می‌کند

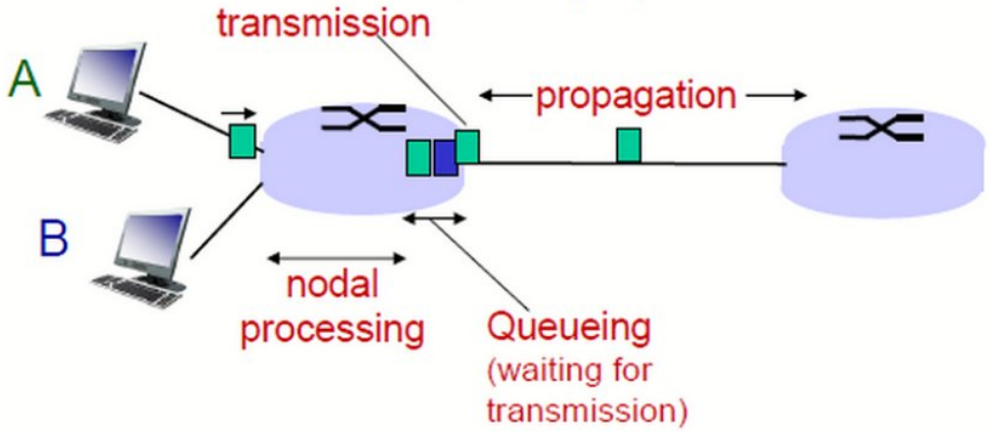
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Packet switching versus circuit switching

- روش packet switch در اشتراک گذاشتن ظرفیت خطوط انتقال بهتر است
  - سوئیچینگ بسته‌ای منابع را رزرو نمی‌کند و پهنای باند لینک مخابراتی را بر حسب تقاضای کاربران به آنها تخصیص می‌دهد(دینامیک) بنابراین یکی از مزیت‌های سوئیچینگ بسته‌ای عدم اتلاف پهنای باند خواهد بود
- پیاده‌سازی روش packet switch ساده‌تر و کم هزینه‌تر است
- packet switch تاخیر اولیه setup کردن را ندارد
- تعداد کاربران مجاز با استفاده از سوئیچینگ بسته بیش از سه برابر سوئیچینگ مدار هست
- Packet switch بدلیل تاخیر انتها به انتها متغیر و غیرقابل پیش بینی برای سرویس‌های real time ای نظیر تماس‌های تلفنی و ویدیو کنفرانس مفید نیست
  - Packet switch دارای Jitter است.
- شبکه سوئیچینگ مداری می‌تواند مقدار مشخصی از پهنای باند انتها به انتها را برای مدت زمان برقراری اتصال گارانتی کند ولی packet switch برخی از پارامترهای کیفیت سرویس نظیر حداکثر تاخیر، حداکثر تلفات بسته، و گذردهی را تضمین تمی‌کند.
- یکی دیگر از مزیت‌های شبکه سوئیچ بسته‌ای عدم نگهداری اطلاعات وضعیت در سوئیچ‌های میانی است

انواع تاخیر در شبکه ها

- تاخیر پردازش در گره (nodal processing delay) d_{proc} = ثابت
- تاخیر صف بندی (queuing delay) d_{queue} = متغیر
- تاخیر انتقال (transmission delay) d_{trans} = ثابت
- تاخیر انتشار (propagation delay) d_{prop} = ثابت



$$d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$$

Scanned with CamScanner

انواع تاخیر در شبکه ها

dproc: nodal processing

- بررسی سرآیند بسته
- مشخص کردن لینک خروجی
- بررسی خطاهای بیت
- typically < msec

d_{queue}: queueing delay

- زمان انتظار در صف خروجی برای ارسال
- متغیر است و به تعداد بسته‌هایی بستگی دارد که جلوتر از بسته مورد نظر در صف هستند

dtrans: transmission delay(۱)

- *زمان لازم برای ارسال(بیرون دادن) تمام بیت‌های بسته روی لینک خروجی*
- *هیچ ارتباطی با فاصله بین دو نود ندارد*
- *L*: packet length (bits)
- *R*: link *bandwidth (bps)*
- $d_{trans} = L/R$

d_{prop}: propagation delay

- *زمان لازم برای منتشر شدن یک بیت از ابتدا تا انهای یک لینک*
- *سرعت حرکت بیت‌ها روی هر لینک برابر سرعت انتشار امواج الکترومغناطیس روی آن لینک است*
- *d*: length of physical link
- *s*: propagation speed in medium (2×10^8 m/sec to 3×10^8 m/sec)
- $d_{prop} = d/s = D/V$

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

چرا virtual circuit ایجاد شد؟

در circuit switch یک کانال ارتباطی ثابت بین فرستنده و گیرنده برقرار می‌شود و منابع بطور کامل و به اندازه حداکثر از ابتدا تا انتها ارتباط رزرو می‌شوند، بنابراین پس از اینکه ارتباط برقرار شد ما نیاز نداریم در هر بسته آدرس مبدا و مقصد بگذاریم، چون مشخص است که بسته‌ها چه مسیری را باید طی کنند، اما این کانال اختصاص داده شده بصورت کارا استفاده نمی‌شود، بنابراین میان و سنگین بیایم کانال و share اش کنیم که packet switch به وجود آمد، حال وقتی shared داریم هر بسته‌ای باید یک آدرس مبدا و یک آدرس مقصد روی اش بزنیم تا هر روتری که یک بسته بهش می‌رسد بفهمد که بسته را به کجا باید ارسال کند، اینطوری از منابع کانال خوب استفاده می‌شود اما چند تا بدی دارد یکی اینکه در packet switch ممکن است دیتا useful ای که می‌فرستیم کم باشد و بنابراین بهره وری (η) و گذردهی (Throughput) می‌آید پایین (فرض کنید ما هر 2ms میخواهیم یک صدایی که ۱۶ بایت هست را بفرستیم، حال مبدا مثلاً ۴۰ بایت به این دیتا اضافه می‌کند در این حالت بهره وری خیلی میاد پایین درحالی که در cs ما این سربارها را نداریم)، بدی دیگری که ps دارد این است که بسته‌ها out of order به مقصد می‌رسند. این مورد در مورد دیتا مشکلی به وجود نمی‌آورد، چون در مقصد صبر می‌کنیم و بعد reorder می‌کنیم و تحویل برنامه می‌دهیم ولی در ویدیو این انتظار برای reorder کردن تا بتوان ویدیو را پخش مناسب نیست همچنان در cs این مزیت را داریم که بسته‌ها ارسال تاخیرشون مشخص است و کسی در صف نمی‌ایستد

حال برای حل کردن این مشکلات ps و cs را با هم مخلوط کردن و vcs را به وجود آوردند در vcs برعکس اینکه بصورت بلندمدت از کانال استفاده کنند آمدند و کانال را بصورت مجازی تعریف کردند تا هر وقت لازم کردیم بتوانیم کانال را از یک نفر بگیریم و به یک نفر دیگر بدهیم یعنی در یک لحظه از زمان یک آیتم circuit مال یک ارتباط است و لحظه بعد مال ارتباط دیگری است

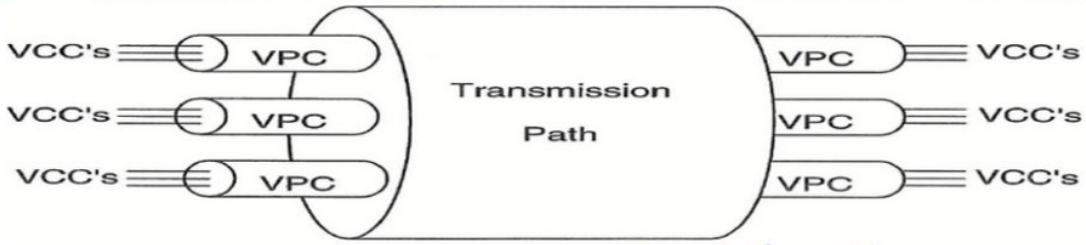
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir



* VpI , VcI در حقیقت جایگزین آدرس های سورس و مقصدهستند . داستان از این قرار است که کل پهنا باند یک لینک را path می گیرند و بعد channel هایی درون هر لینک است. پس وقتی یک cell می رسد به یک سوئیچ و می خواهد از یک مسیر دیگر برود ، فقط کافی است بگوییم روی چه path ای باید برود و روی کدام کانال آن path قرار می گیرد ، از این لحاظ انگلیسی ها به VCs می گویند lable swaping یا lable switching

- کانال هایی که در شکل بالا می بینید هم virtual هستند ، یعنی وقتی بسته می خواهد از این path رد بشود اون کانال مال شماست ولی وقتی بسته رد می شود ، این کانال disconnect می شود برای آن ارتباط و می تواند به فرد دیگری اختصاص یابد

نکته) ما می خواستیم که بهره وری را بالا ببریم برای همین دوست داریم هدر پکت کوچک بشود ، اگر می خواهیم هدر را کوچک کنیم باید آدرس مبدا و مقصد را بطور کامل در هدر بسته ها نداریم ، برای همین آمدند از VcI VpI استفاده کردند که اینها آدرس دهی local است ، بنابراین برای اینکه بسته ها بتوانند از مبدا به مقصد برسند ، باید قبل از شروع ارتباط یک مسیر بین فرستنده و گیرنده ایجاد بشود (نازک) (connection setup) به اینصورت که فرستنده به گیرنده یک بسته ارسال می کند (در payload دیتا نیست و آدرس است) و بعد اگر گیرنده آزاد بود یک Ack برای فرستنده می آید و بعد از آن ارتباط شروع می شود ، با این کار برای این VC در forwarding table روترهای موجود در آن ارتباط یک entry اضافه می شود ، همچنین تمامی روترها می توانند منابعی را رزرو کنند ، با این کار پکت های دیگر فقط همین مسیر را طی می کنند بنابراین دیگه لزومی نداره که آدرس های مبدا و مقصد را بصورت کامل داشته باشند ← هم اینها ۲ خوبی برای ما دارند ۱- هدر کوچک می شوند

۲- بسته ها in order به مقصد می رسند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

- نکته) ما در packet switch دو نوع کانکشن می توانیم داشته باشیم یکی oriented و یکی غیر oriented در oriented اگر در مسیری که انتخاب کردیم ازحام به وجود بیاید بسته ها دیر به گیرنده می رسند چون باید از همان مسیر بروند ولی وقتی oriented نیستیم بسته ها out of order می رسند ولی بسته ها زودتر می رسند.

نکته) محیط بیان Data از connectionless استفاده می شود ولی برای audio , video از co

جمع بندی

- virtual circ... سعی کرده است که خوبی های circuit switch و packet switch را با هم داشته باشد

خواص virtual circuit را می توان به ۲ دسته تقسیم کرد. ۱ خواصی مشابه circuit switch

۲ " " packet switch

① خواص شبیه circuit switch

۱- در VC فاز برقراری اتصال (connection setup) و همچنین قطع اتصال (connection rel...)

۲- در فاز برقراری اتصال و قبل از شروع تبادل داده ها مسیر ثابت بین فرستنده و گیرنده مشخص می شود بنابراین

۱- منابع آن رزرو می شوند

۲- ترتیب رسیدن بسته ها در گیرنده به ترتیب ارسال آنها توسط فرستنده است

منابع مانند CS به اندازه حداکثر رزرو می شوند و به اندازه ظرفیت معادل (equivalent capacity) شبه میانگین آماری

بنابراین کیفیت سرویس (QOS) را می توانیم بصورت ۱۰۰ درصد تضمین کنیم

ولی با احتمال بالایی تضمین می کنند و گر از SLA شان تخطی کردند جریمه پرداخت می کنند

اینکه چه تضمین هایی به مشتری ها داده می شود بستگی به خواسته مشتریان دارد و برای اعلام QOS چهار کلاس قرار دادند در ATM

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Network Performance Parameters

- ITU Recommendation I.356 defines the following cell-level network performance parameters:
  - Cell Transfer Delay (CTD),
  - Cell Delay Variation (CDV),
  - Cell Loss Ratio (CLR),
  - Cell Error Ratio,
  - Cell Misinsertion Rate,
  - Severely Errored Cell Block Ratio.

Quality of Service Parameters

- Three of the QoS parameters:
  - Cell error ratio
  - Cell misinsertion rate
  - Severely errored cell block ratio

are primarily caused by impairments in the physical transmission media and are thus not readily controlled, or selectable, on a connection by connection basis (modulo selecting or avoiding routes with particular transmission media).

- Thus, these parameters are given default values that apply across all classes (except the "U" class for which no performance objectives are stated).
- The default values are as follows.
  - The upper bound on the cell error ratio is 4×10^{-6}.
  - The upper bound on the mean cell misinsertion ratio is 1/day.
  - The upper bound on the severely errored cell block ratio is 10^{-4}.

Scanned with CamScanner

Quality of Service Parameters

- The remaining three QoS parameters:
  - Cell transfer delay,
  - Cell delay variation,
  - Cell loss ratio,

are influenced by the choice of route and by buffering and scheduling capabilities and policies in network nodes, as well as influenced by physical transmission media.

- Thus, it is reasonable for a user to be able to select on a per-connection basis objectives for these QoS parameters, from amongst the objectives supported by the network service provider.
- In particular, the user can select on a per-connection basis the QoS class, where each class is associated with a unique set of objective values.

	Provisional performance objectives[a]			
QoS class	Upper bound on the mean cell transfer delay	Upper bound on the difference between the upper and lower 10^{-8} quanitles of cell transfer delay	Upper bound on the cell loss probability (regardless of the value of the CLP bit in the cell header)	Upper bound on the cell loss probability for cells with CLP bit = 0
Stringent class	400 ms	3 ms	3×10^{-7}	None
Tolerant class	U	U	10^{-5}	None
Bilevel class	U	U	U	10^{-5}
"U" class	U	U	U	U

[a] U, unspecified, or unbounded.

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

③ خواص شبیه packet switch

تقریبا بصورت بهینه از منابع استفاده می‌شود . زیرا اگر یک connection از منابع خودش استفاده نکند ، آن منابع را بصورت پویا به سایرین تخصیص می دهد

نکته) end point در ATM connection دو مدل می‌تواند باشد

۱. user interface : یعنی در آم خط می‌تواند یک یوزر به ATM وصل باشد که امروزه خیلی این حالت را نداریم ، چون صحبت کردن با شبکه و چاند زدن براش پیچیده باشد و ... کار ساده‌ای برای user نیست

۲. Network inter- : یعنی اتصال Network به Network

ما باید در ATM یک traffic contract با شبکه داشته باشیم و همین باعث می‌شود که خیلی سخت باشد که user بتواند از ATM استفاده نکند و براش همین ATM پیشرفت نکرد چون مهمترین عامل در پیشرفت تکنولوژی user friendly بودن است که ATM ، user نیست . ترافیک user ها بصورت bursty است و زور و کردن پیدا باشد برای اینها سخت است و دقیقا مشخص نیست که یوزر چقدر پهنا باشد را می‌خواهد رزرو بکند .

← وقتی در rate بالا و در یک کانال بزرگ که هزاران یوزر وارد می‌شوند ، طبق تئوری expected value وقتی تعداد کاربران زیاد باشد ، EP می‌شود همان عدد min و ترافیک معلوم است که چقدر است و در اینجا براحتی می‌توان پهنا باشد را رزرو کرد

بنابراین ATM تو Desktop نیامد و در back bone شبکه استفاده می‌شود

QOS: Quality of service

در QOS باید گارانتی شود (تضمین بشود) که معیارهای قابل اندازه‌گیری (کمی) مورد نظر مشتری از توافق سطح سرویس (SLA) که انجام شده است تجاوز نکند ، اگر هم تجاوز کرد ISP باید جریمه بپردازند

QOS به شدت به کنترل از حجم وابسته است.

برخی از معیارهای کیفیت سرویس (QOS metrics)

۱- Delay ۲- jitter ۳- loss ۴- گذردهی

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

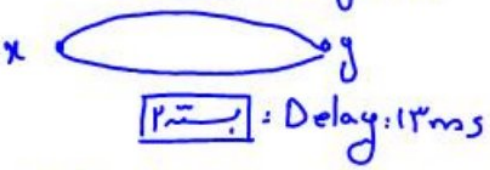
رامین رضوی

① تاخیر (Delay)

در مورد Delay بعداً مفصل صحبت خواهیم کرد. اما تعریف کلی آن بصورت زیر است:
چقدر طول می‌کشد تا یک بسته (یا تعداد زیادی بسته) به طول L از نقطه x به نقطه x برسد
این تاخیر می‌تواند شامل تاخیر پردازش روتر، تاخیر گذاشتن بسته‌ها روی لینک، تاخیر صف، تاخیر انتشار روی کانال‌ها باشد

② jitter (لرزش تاخیر، نوسانات تاخیر) (jitter تغییرات Delay است)

jitter برابر است با حداکثر مقداری که تاخیر بازی می‌کند



نوسان تاخیر $= 13\,ms - 0ms = 8\,ms$

علاوه بر اینکه بسته‌ها می‌توانند از مسیرهای مختلفی به سمت مقصد بروند و درنتیجه تاخیرهای متفاوتی را تجربه می‌کنند، بسته‌هایی که در یک مسیر نیز می‌روند ممکن است تاخیرهای مختلفی داشته باشند زیرا در همان مسیر هم در زمان‌هایی می‌توانند ازدحام وجود داشته باشد و در زمان‌هایی خلوت باشد

$$jitter = delay_{max} - delay_{min}$$ = حداکثر مقداری که تاخیر بازی می‌کند

بنابراین jitter تغییرات Delay است، یعنی ممکن است که با Delay بسیار زیادی داشته باشیم اما jitter کمی داشته باشیم و بالعکس

مثال: فرض کنید ۲ ارتباط داریم:

ارتباط ۱: $delay_{max} = 250\,ms$, $delay_{min} = 245\,ms$ $\Rightarrow jitter = 250 - 245 = 5\,ms$

ارتباط ۲: $delay_{max} = 25\,ms$, $delay_{min} = 5\,ms$ $\Rightarrow jitter = 25 - 5 = 20\,ms$

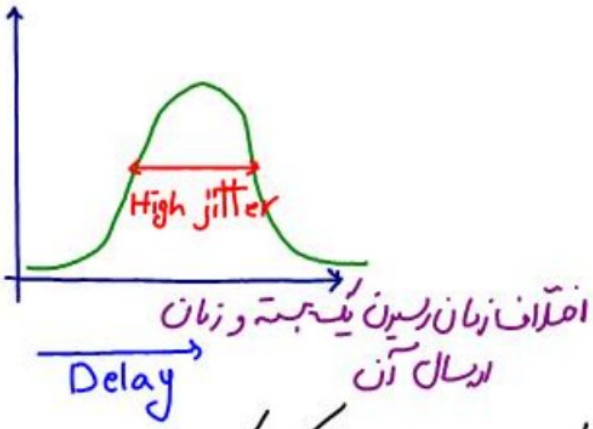
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

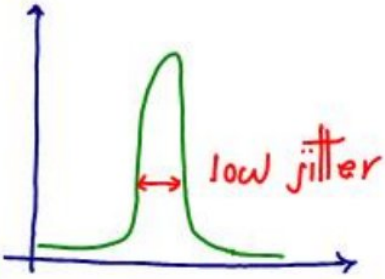
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

نکته) در کاربردهای Real time ما اصلا jitter را دوست نداریم، چون درصورت داشتن جیتر بعضی وقت ها بسته ها زود می رسند و بعضی وقت ها بسته ها دیر می رسند؛ و ما در کاربردهای Real time یکنواختی رسیدن بسته ها برایمان مهم است.

- نمودارهای توزیع میزان زمانی که طول می کشد تا بسته ها به مقصد برسند

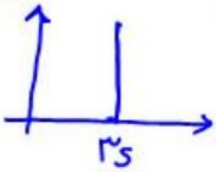
packet





گاهی بسته ها از زمان ارسال تا دریافت شان ۳s طول می کشند

هیستوگرام شان بصورت زیری میشه



نکته) jitter در شبکه اجتناب ناپذیر است زیرا شبکه نمی تواند گارانتی کند که Delay برای همه بسته ها یکسان است و بنابراین کاری که ما می توانیم بکنیم و دوست داریم بکنیم کنترل کردن jitter است حال یکی از کارهای خیلی رایج برای مدیریت jitter این است که می آیند و با هزینه کردن Delay زمینه جبران jitter را می کنند (trade off بین Delay و jitter)، و این کار را به اینصورت انجام می دهند که می آیند و در گیرنده بسته های دریافتی را برای مدتی بافر می کنند و سپس شروع می کنند و با یک نرخ ثابتی اینها را Display می کنند

نکته) در یک کنفرانس ویدیویی دوطرفه (۲ نفرک با ویدیو با هم صحبت می کنند) هم Delay مهم است و هم jitter (یا مثلاً VOIP : ۲ نفر می خواهند با وین با هم در بستر اینترنت صحبت کنند) بنابراین سخت ترین شاخه های برنامه های Real time از نظر QOS برنامه های تعاملی است

تست کنکور: برای رفع مشکل jitter اندازه بافری که در گیرنده استفاده می شود باید چقدر باشد؟

۱- به اندازه jitter ۲- حداکثر تاخیر ۳- حداقل تاخیر ۴- هیچکدام

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

برای محاسبه طول بافر باید بدترین حالت رسیدن بسته ها از نظر تاخیر را در نظر بگیریم، بدترین حالت این است که فریم اول با کمترین تاخیر برسد و دقیقاً فریم بعدی آن با بیشترین تاخیر برسد و ما بخواهیم بسته ها را پشت سرهم نمایش بدهیم.

مثال: فرض کنید که $delay_{min}$ = 5ms و $delay_{max}$ = 23ms باشد. اگر شرایط بالا رخ بدهد بسته اول در لحظه 5ms به مقصد می‌رسد، حالا این بسته را 18 ms در بافر نگه می‌داریم و بعد شروع می‌کنیم به پخش کردن، چون بسته دوم در بدترین شرایط در 23ms به مقصد می‌رسد پس زمانیکه ما پخش بسته اول را تمام کنیم بسته دوم رسیده است و آماده پخش کردن است.

پس اگر ما 18 ms بافر کنیم بدترین شرایط هم هندل می‌شود

تست) فرض کنید فردی سایت کنکور کامپیوتر را باز کرده است و می‌خواهد فیلم جلسه اول شبکه را مشاهده کند، فرض کنید برای نمایش روان این فیلم 30 فریم در ثانیه باید برای کاربر پخش شود که اندازه هر فریم 10 KB است. اگر تاخیر انتها به انتها بین 3 تا 9 ثانیه نوسان کند حجم بافر مورد نیاز در مقصد برای رفع jitter باید چقدر باشد؟

۱- 1 MB ۲- 1,2 MB ۳- 1,6MB ۴- 1,8 MB

ابتدا باید محاسبه کنیم که به چه مدت آن باید بافر کنیم؟ که این برابر jitter بود

$jitter = delay_{max} - delay_{min} = 9s - 3s = 6s$

= نرخ ورود داده به بافر × مدت زمان بافر کردن = بنابراین حجم بافر مورد نیاز

$= 6s \times 30 \frac{frame}{s} \times 10 \times 10^3 B = 1,8 MB$

تست) کاربرد نگاه کردن فیلم از طریق آپارات (streaming) به چند مورد از موارد زیر حساس است؟

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

- حساس به loss
- حساس به delay
- " " error
- " " jitter

۱_۱ ۲_۲ ۳_۳ ٤_٤

نکته) error بیشتر به کانال انتقال ربط دارد، مثلا در فیبر نوری error خیلی کمتر از وایرلس است ولی loss بیشتر به ازدحام شبکه مربوط می‌شود و یا اینکه error ان در هدر بسته به وجود بیاید که بسته اشتباها به سمت مقصد نرود و به دست فرد دیگری برسد در این حالت برای کسی که بسته اشتباه به آن رسیده این یک misinsertion (مثلاً در ATM یکی از پارامتر ها کیفیت سرویس cell misinsertion rate است) است و برای مقصد اصلی یک loss محسوب می‌شود.

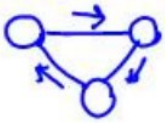
③ loss (از دست رفتن بسته)

در چه شرایطی ممکن است بسته ها گم شوند؟

۱- در هدر بسته error رخ بدهد و به جای اشتباهی برود

۲- در بافر خروجی روترها دور ریخته شوند (به هر دلیلی)

۳- بسته در loop بیفتد



loss یک شبکه را چگونه بیان می‌کنند؟ با پارامتر packet loss ratio (PLR)

سوال: PLR=10^{-8} است، این به چه معناست؟ یعنی از هر 10^{8} بسته، یک بسته گم می‌شود بصورت میانگین.

Ratio یک کسر است و اصلا واحد ندارد مثلاً $\frac{1}{10^{8}} = 10^{-8}$ ولی Rate یعنی تعداد در واحد زمان، پس Rate واحد دارد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

احتمال loss شدن (یا نشدن) یک بسته در مسیر

در یک مسیر شامل n لینک متوالی، اگر احتمال مفقود شدن بسته در هر لینک برابر p باشد و این احتمال بردن هر لینک مستقل از دیگر لینک ها باشد، آن گاه داریم:

احتمال دریافت موفقیت آمیز بسته توسط گیرنده: $(1-p)^n$

احتمال مفقود شدن بسته در طول مسیر = سالم رسیدن بسته - کل = $1-(1-p)^n$

* حال اگر یک بسته در مسیر رسیدن به دست مشتری مفقود شود فرستنده دوباره آن را ارسال می کند، حال بردن آنکه یک بسته با موفقیت به مشتری برسد

① هر بسته بطور میانگین $\frac{1}{(1-p)^n}$ بار توسط فرستنده ارسال می شود

② " " " " " " " " " " " مجدد می شود $\frac{1}{(1-p)^n} - 1$

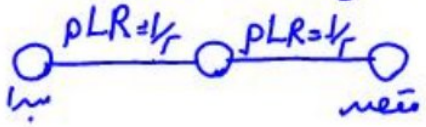
یا دلوری از آمار: در یک آزمایش برنولی داریم: میانگین تعداد ارسال = $\frac{1}{\text{احتمال موفقیت}}$

آزمایش برنولی: اگر هر بار انجام آزمایش مستقل از نتایج بدست آمده از دفعات قبلی فقط و فقط به یکی از دو پیشامد موفقیت یا شکست با احتمال ثابت p و $p-1$ منجر شود

* در این حالت پدیده ای که احتمال موفقیت اش p است را باید $\frac{1}{p}$ بار تکرار کنیم تا به اولین موفقیت برسیم

مثال) چند بار یک سکه را پرتاب کنیم تا به اولین شیر برسد؟ ممکن است خوش شانس باشیم و بار اول شیر بیاید یا ممکن است بد شانس باشیم و هزار بار بیندازیم و خط بیاید حاکا سوال این است که بطور میانگین چند بار باید بیندازیم تا اولین شیر بیاید

سوال- با توجه به شکل زیر PLR کل را بدست آورید؟



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

④ گذردهی (توان عملیاتی)

ما گفتیم که گذردهی برابر است با نرخ بیت مفید و موثری که به گیرنده تحویل داده می‌شود که واحدش bps است و گفتیم:

Bit rate ← داده مفید و غیرمفید

$$\gamma = R \times u$$

γ: Throughput — u: utilization $= \frac{\text{بخش مفید}}{\text{کل داده}} \times 100$ (بهره وری، راندمان)

این گذردهی میانگین است

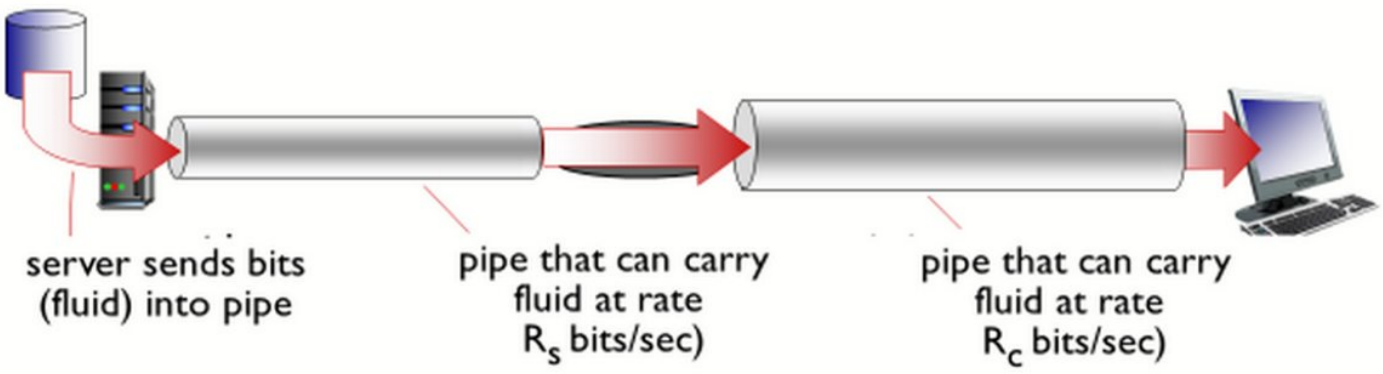
بنابراین به طریقی دیگر می‌توان گفت که گذردهی میانگین برابر است با: $\frac{F}{T}$

F : مقدار داده منتقل شده بین دو حد ست

T : مدت زمانی که انتقال این فایل F سپی طول کشیده

Throughput

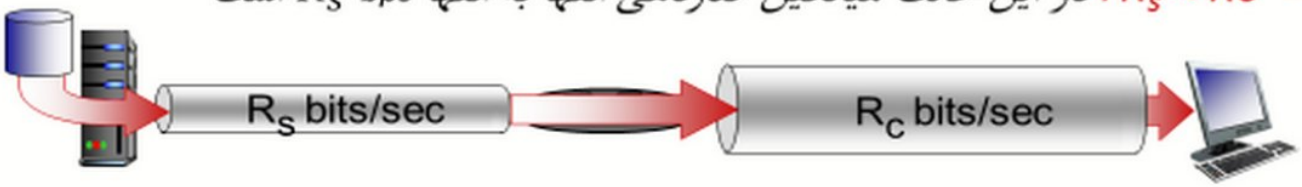
- یکی دیگر از معیارهای ارزیابی کارایی در شبکه‌های کامپیوتری گذردهی انتها به انتها است
- *Throughput (گذردهی)* : نرخ انتقال بیت ها بین فرستنده و گیرنده برحسب بیت/ثانیه
  - *Instantaneous Throughput (گذردهی لحظه‌ای)* : نرخ دریافت داده توسط گیرنده در یک لحظه از زمان
  - *Average Throughput (گذردهی میانگین)* : نرخ دریافت داده در یک مدت زمان طولانی
    - اگر انتقال F بیت داده T ثانیه طول بکشد، آنگاه گذردهی میانگین برابر است با : $\frac{F}{T}$
- گذردهی را با دو فرض تقریب می‌زنند
  - به جز ترافیک ارسالی از سرور به مشتری ترافیک دیگری در شبکه وجود نداشته باشد
  - به جز ترافیک ارسالی از سرور به مشتری ترافیک‌های تداخل کننده دیگری نیز در شبکه وجود داشته باشد



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Throughput

- $R_s < Rc$: در این حالت میانگین گذردهی انتها به انتها R_S bps است



- $Rs > Rc$: در این حالت میانگین گذردهی انتها به انتها R_c bps است

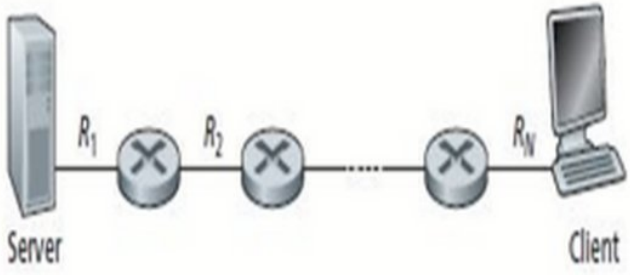
bottleneck link

for this simple two-link network the throughput is min{*Rc*, *Rs*}, that is, it is the transmission rate of the **bottleneck link**.

❖ زمان تقریبی انتقال فایلی با اندازه‌ی F بیت از سرویس دهنده به مشتری معادل $\frac{F}{\min\{Rc, Rs\}}$ است

Throughput

- transmission rates of the N links being $R_1, R_2, \ldots, R_N$
- throughput for a file transfer from server to client is $\min\{R_1, R_2, \ldots, R_N\}$
- which is once again the transmission rate of the bottleneck link along the path between server and client



example motivated by today's Internet.

- The server is connected to the network with an access link of rate Rs
- client is connected to the network with an access link of rate *Rc*
- suppose that all the links in the core of the communication network have very high transmission rates
- Also suppose that the only bits being sent in the entire network are those from the server to the client.
- throughput = $\min\{R_s, R_c\}$
- Therefore the constraining factor for throughput in today's Internet is typically the access network.

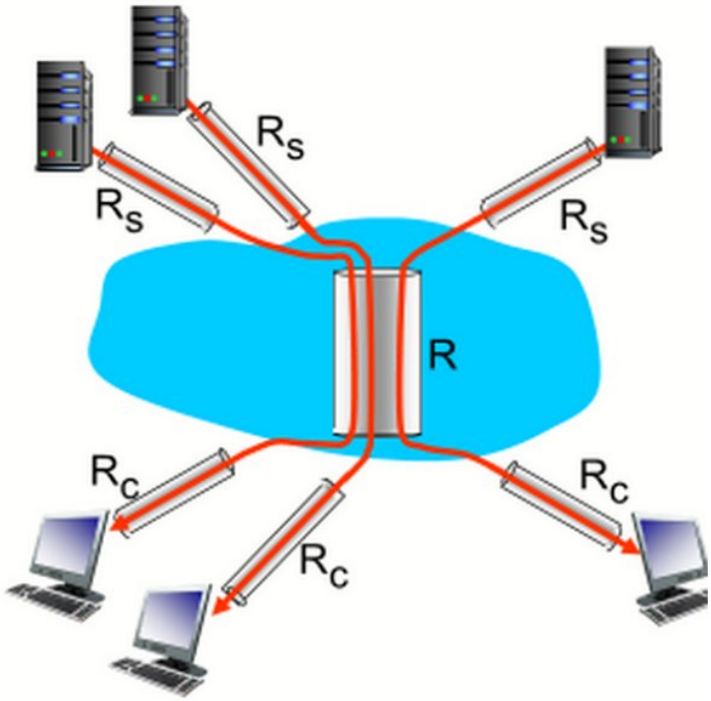
Scanned with CamScanner

Throughput

- generally the throughput depends not only on the transmission rates of the links along the path, but also on the intervening traffic
- 10 simultaneous downloads taking place, involving 10 client-server pairs
- Suppose that these 10 downloads are the only traffic in the network at the current time.
- If R, is larger than both R_s and R_c:
- throughput for each download:

$$\min\{R_s, R_c\}$$

- Otherwise:
- per-connection end-to-end throughput: $\min(R_c, R_s, R/10)$
- in practice: R_c or R_s is often bottleneck



10 connections (fairly) share backbone bottleneck link R bits/sec

- در یک شبکه سوئیچ بسته میزبان A می‌خواهد یک فایل 8 MB را برای میزبان B ارسال کند، اگر مسیر A به B از سه لینک با آهنگ‌های ارسال R_1= 3 Mbps و R_2= 2 Mbps و R_3= 5 Mbps تشکیل شده باشد، با فرض اینکه هیچ ترافیک دیگری روی این شبکه وجود نداشته باشد زمان انتقال فایل به میزبان B چقدر است؟

1) بیشتر از ۴ ثانیه
2) کمتر از ۴ ثانیه
3) بیشتر از ۳۲ ثانیه
4) کمتر از ۳۲ ثانیه

پاسخ : وقتی در مورد بقیه تاخیرها صحبتی نکرده آنها را صفر در نظر میگیریم .

$$T_{total} = \frac{L}{R} \sim \frac{\mathbf{L}}{\min\{R_1, R_2, R_3\}} = \frac{8\times10^6\times8}{2\times10^6} = 32s$$

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

مثال

- با توجه به شکل زیر، فرض کنید M مسیر بین مشتری و سرویس دهنده وجود دارد و هیچ لینکی بین آنها مشترک نیست، حال فرض کنید مسیر Kام از N لینک با آهنگ‌های ارسال R_1^k تا R_N^k تشکیل شده است. اگر یک سرویس دهنده برای ارسال داده به مشتری خود فقط از یک مسیر بتواند استفاده بکند

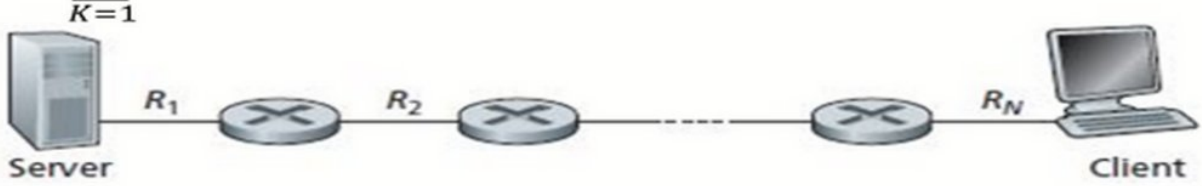
الف) حداکثر گذردهی که این سرویس دهنده می‌تواند به آن دست یابد چیست؟

ب) اگر یک سرویس برای ارسال داده به مشتری خود بتواند از تمامی M مسیر استفاده کند، حداکثر گذردهی که این سرویس دهنده می‌تواند به آن دست یابد چقدر است؟

پاسخ الف) باید ببینیم کدام یک از این M مسیر بیشترین گذردهی را به سرویس دهنده ارائه می‌کند

$$\max\left\{min\{R_1^1, R_2^1, \dots, R_N^1\}, min\{R_1^2, R_2^2, \dots, R_N^2\}, \dots, min\{R_1^M, R_2^M, \dots, R_N^M\}\right\}$$

پاسخ ب) گذردهی تمامی مسیرها را باید با هم جمع کنیم $\sum_{K=1}^{M} min\{R_1^K, R_2^K, \dots, R_N^K\}$

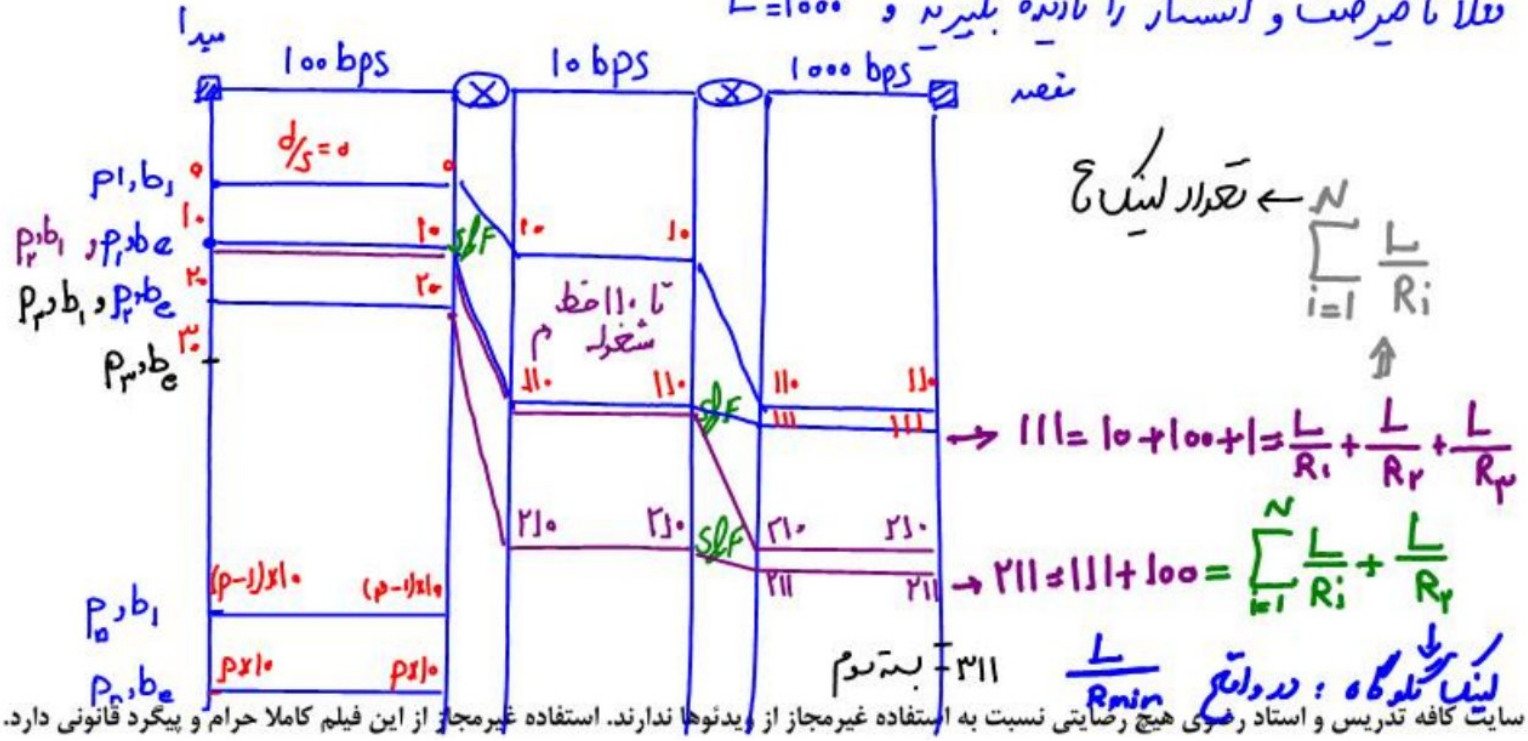


Delay ⑥

محاسبه تاخیر در شبکه‌های circuit switch, packet switch

۱_ محاسبه تاخیر ارسال p بسته در شبکه ps:

فعلا تاخیر صف و انتشار را نادیده بگیرید و L=1000



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

نتیجه گیری :

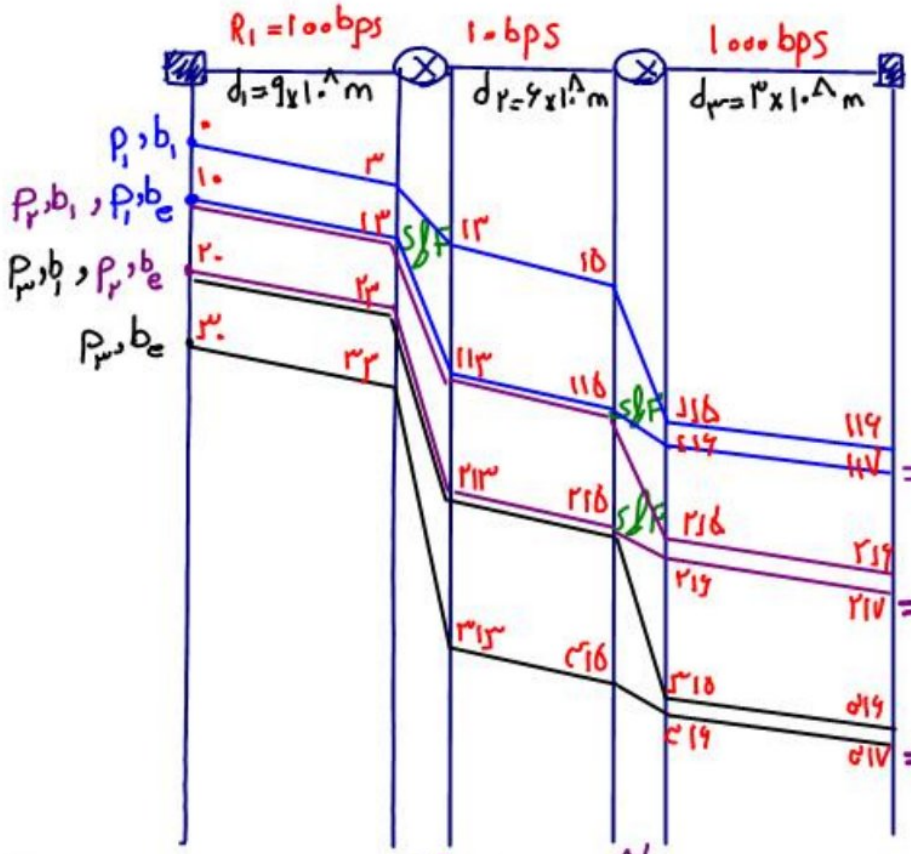
$$delay_{total} = \sum_{i=1}^{N} \frac{L}{R_i} + (p-1)\frac{L}{R_{min}}$$

توجه) دقت کنید که در اینجا سایز بسته L را ثابت گرفتیم ولی می‌توانید لزوما به این شکل نباشد

انکته $(p-1)\frac{L}{R_{min}} = (p-1) \times \max\{d_{trans_i}\} = (p-1) \times \max_{\forall i}\{\frac{L}{R_i}\}$

در مثال قبل تاخیر انتشار را نیز در نظر بگیرید و فرض کنید که $d_{prop(1)}=3s$ و $d_{prop(2)}=2s$ و $d_{prop(3)}=1s$

$(s = 3\times 10^8 \frac{m}{s})$



$$3+2+1 \quad \sum_{i=1}^{N}\frac{d_i}{s}$$

$$\Rightarrow 111+6 = \sum\frac{L}{R_i} + \frac{d_1}{s}+\frac{d_2}{s}+\frac{d_3}{s}$$

$$\Rightarrow 111+6+100 = \sum\frac{L}{R_i} + \sum\frac{d_i}{s} + \frac{L}{R_{min}}$$

$$\Rightarrow \sum\frac{L}{R_i} + \sum\frac{d_i}{s} + 2\times\frac{L}{R_{min}}$$

نتیجه گیری

$$delay_{end\ to\ end} = \sum_{i=1}^{N}\frac{L}{R_i} + \sum_{i=1}^{N}\frac{d_i}{s} + (p-1)\frac{L}{R_{min}}$$

تاخیر انتقال و تاخیر انتشار به ازای هر لینک یکبار جمع می‌شود و اگر تعداد بسته L بیشتر از یکی بود به اندازه یکی کمتر از تعداد بسته L هم به تاخیر اضافه می‌شود $\frac{L}{R_{min}}$

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

نکته) ارسال بسته ها در شبکه packet switch به این صورت است و می توانیم اینطور فکر کنیم که بسته اول تمام تاخیرها را متحمل می شود (مادر) و از بسته دوم به بعد هر بسته به اندازه تاخیر لینک گلوگاه به تاخیر کلی اضافه می کند

توجه) وقتی تعداد لینک ها N تاست، تعداد سوئیچ ها N-1 است

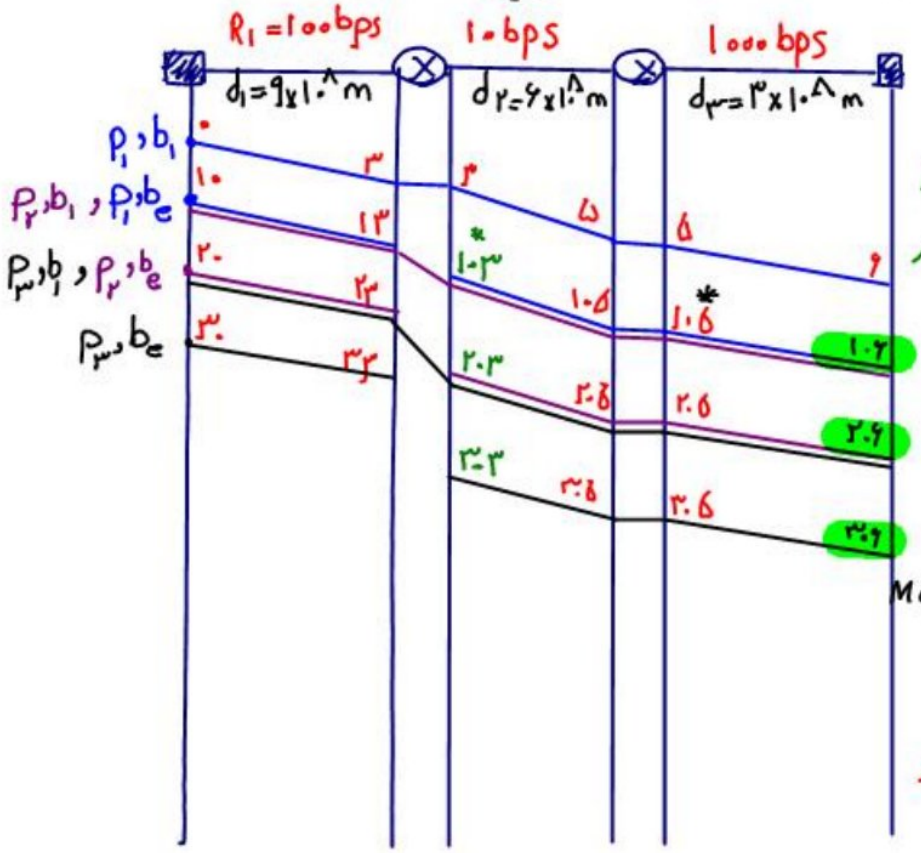
نکته) در صورتی که تاخیر پردازش، صف را داده باشند خواهیم داشت:

$$\text{تاخیر انتها به انتها} = \sum_{i=1}^{N} \frac{L}{R_i} + \sum_{i=1}^{N} \frac{d_i}{s} + \sum_{i=1}^{N-1} d_{proc}(i) + \sum_{i=1}^{N-1} d_{queue}(i)$$

- اگر ترافیک دیگری روی شبکه نباشد تا تاخیر صف که علت آن حضور سایر کاربران در شبکه باشد نداریم و فقط تاخیر صفی که دلیل آن خود مان هستیم را در نظر می گیریم (همان تایم هایی که خط اشغال است)

۲ـ محاسبه تاخیر ارسال P بسته در شبکه circuit switch

نکته مهمی که در اینجا داریم این است که دیگر Forward & store نداریم



* در بسته که بیت آخر بسته اول در ثانیه ۱۳ می رسد به سوئیچ دوم و می سوئیچ دوم از لحظه ۳ که بیت اول بسته بعدش می رسد بیکار نمی نشیند و شروع می کند به ارسال کردن بسته: $3 + \frac{L}{R_2} = 3 + 100 = 103$

* در واقع داریم:

max (زمان رسیدن بیت آخر و $\frac{L}{R}$ + زمان شروع به ارسال بیت اول)

↓

چون ممکن است خط مشغول باشد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

$$1.6 = 100 + 6 = \frac{L}{R_{min}} + \sum \frac{d_i}{s}$$
$$2.6 = 2\times100 + 6 = 2\times\frac{L}{R_{min}} + \sum \frac{d_i}{s}$$
$$3.6 = 3\times100 + 6 = 3\times \quad " \quad " \quad "$$

نتیجه گیری :

$$d_{end\ to\ end} = \sum_{i=1}^{N} \frac{d_i}{s} + P\times\frac{L}{R_{min}}$$

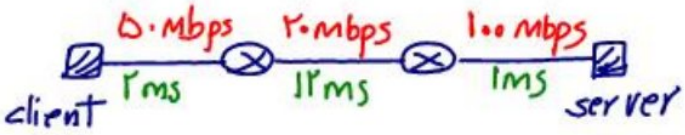
IT 94 _ شبکه‌ای بصورت زیر بین مبدا و مقصد وجود دارد، حداقل زمان لازم برای انتقال ۵۰۰ بسته ۱۰۰۰ بایتی برحسب میلی ثانیه کدام است؟

۱_ ۲۱۵

۲_ ۲۱۵,۱۲

۳_ ۲۱۸,۱۶

۴_ ۲۱۸,۶۴



$$\text{تاخیر کل} = \frac{L}{R_1} + \frac{L}{R_2} + \frac{L}{R_3} + (500-1)\times\frac{L}{R_2} + 15\ ms$$

نکته عالی ۲: به جای اینکه ۴۹۹ را در $\frac{L}{R_2}$ ضرب کنیم، ۵۰۰ را ضرب می‌کنیم، چون همیشه $\frac{L}{R_{min}}$ در بین $\sum \frac{L}{R}$ ۶ وجود دارد. و به جایش $\frac{L}{R_{min}}$ دون $\sum \frac{L}{R_i}$ را در نظر نمی‌گیریم

نکته عالی ۲: اگر عدد ترم ۶ اینقدر هم تریک نبود این تست را خیلی سریع می‌شد زد. $\frac{L}{R_{min}}$ در بین تمامی $\frac{L}{R_i}$ ۶ بزرگترین عدد است، بنابراین می‌توان متوجه شد که مقدار اصلی تاخیر را $P\times\frac{L}{R_{min}} + \sum \frac{d_i}{s}$ تشکیل می‌دهد، اگر این مقدار را محاسبه کنیم عدد 215 ms به دست می‌آید

نکته عالی ۳_ اگر در سوالی مقدار تقریبی تاخیر را بخواهند، این مقدار برابر است با:

$$P\times\frac{L}{R_{min}} + \sum \frac{d_i}{s} = \frac{F}{R_{min}} + \sum \frac{d_i}{s} = \frac{F}{8} + \sum \frac{d_i}{s}$$

اگر بهره وری کانال را به ما داده باشند به جای 8 می‌زنیم $R_{min}\times 8$

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

نکته عالی ۴ - با توجه به اینکه اختلاف گزینه ۴ در مقدار اعشار آنهاست، می‌توانیم فقط مقدار اعشار را محاسبه کنیم

محاسبه: $\frac{L}{R_1}+\frac{L}{R_3}=\frac{1000\times 8b\times 5}{50\times 10^6\times b}+\frac{1000\times 8b\times 5}{100\times 10^6\times b}=\frac{2\times 1000\times 8+8000}{100\times 10^6}s=$

$\frac{24\cancel{00}}{100\times 10^{\cancel{3}}}\times 10^{-3}s=0,24\ ms \Rightarrow$ گزینه ۳

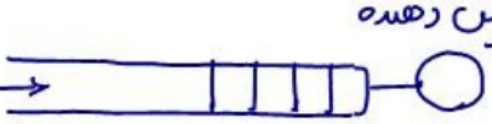
محاسبه دقیق بقیه فرمول تاخیر

$50\times\frac{1000\times 8\times b\times 5}{2\times 10^6\times b}+15\ ms=200\ ms+15\ ms=215\ ms$

یکا 10^3 را می‌برم تا ms شود $\rightarrow \times 10^3$

تاخیر صف

گفتیم که هر لینک خروجی روتر یک بافر یا همان صف خروجی دارد، حال اگر فابریک سوئیچ بخواهد بسته‌ای را به یک لینک خروجی ارسال کند ولی آن لینک مشغول فرستادن بسته دیگری باشد (یا افراد دیگری در صف باشند) بسته تازه وارد شده باید برود و در صف خروجی آن لینک بنشیند



سرویس دهنده با نرخ میانگین μ بسته در ثانیه به بسته ها سرویس می‌دهد

بسته ها با نرخ میانگین λ بسته در ثانیه وارد صف می‌شوند

- ترافیکی که وارد صف می‌شود، ترافیکی است که در آن، نرخ ورود داده‌ها دارای توزیع تصادفی و بدون حافظه پواسن با میانگین λ فریم در ثانیه است، بنابراین زمان بین وارد شدن فریم‌های مختلف دارای توزیع نمایی با میانگین $\frac{1}{\lambda}$ ثانیه است، و این یعنی هر $\frac{1}{\lambda}$ ثانیه یک فریم وارد صف خواهد شد
- زمان سرویس دادن سرور به فریم‌ها متناسب است با طول فریم و طول فریم‌ها هم تصادفی است و بصورت رندم عوض می‌شود، بنابراین نرخ سرویس دادن سرور هم نیز دارای توزیع تصادفی و بدون حافظه

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

پواسن با میانگین M فریم در ثانیه است .

نکته) زمان سرویس دادن سرور به یک بسته بصورت میانگین برابر است با : $T_{\text{سرویس دادن}} = \frac{L_{avg\ packet}}{R\ \text{لینک خروجی}}$

M : میانگین نرخ سرویس دادن $= \frac{1}{\text{میانگین زمان سرویس دادن}} = \frac{R}{L_{avg\ packet}}$

Queueing delay

- هرجایی که ما یک سرویس دهنده و یکسری سرویس گیرنده‌هایی داریم که باید در انتظار باشند تا از سرویس دهنده سرویس بگیرند یک صف خواهیم داشت
- یک صف تنها با ۳ مشخصه بصورت $A/S/C$ معرفی می‌شود (Kendall's notation)
  1. A : نوع (نرخ و زمان) ورود فریم‌ها به صف
  2. S : نوع (نرخ و زمان) سرویس دادن سرور به فریم‌ها
  3. C : تعداد سرورهای موازی
- در تحلیل صف یکی از مدلهای ساده و رایج مدلی است با فرضهای زیر

1. ترافیکی که دارد وارد صف می‌شود ترافیکی است که در آن نرخ ورود داده‌ها دارای توضیع تصادفی و بدون حافظه پواسن با میانگین λ فریم در ثانیه (زمان بین وارد شدن فریم‌های مختلف دارای توزیع نمایی با میانگین $\frac{1}{\lambda}$ ثانیه است،یعنی هر $\frac{1}{\lambda}$ ثانیه یک فریم وارد صف خواهد شد)
2. فرض می‌کنیم زمان سرویس دادن سرور به فریم‌ها متناسب باشد با طول فریم و فرض می‌کنیم طول فریم‌ها بصورت رندم عوض می‌شود و طول فریم‌ها هم دارای توزیع نمایی هستند در این صورت نرخ سرویس دادن سرورمان به فریم‌ها دارای توزیع پواسن با میانگین μ فریم در ثانیه باشد
3. یک سرور داشته باشیم

- چنین صفی را $M/M/1$ می‌گویند
  - M stands for Markov or memoryless and means arrivals occur according to a Poisson process
- در چنین صفی میانگین زمان انتظار در صف برابر : $\frac{1}{\mu-\lambda}$
- μ همیشه باید بزرگتر از λ باشد : اگر اینگونه نباشد طول صف کم‌کم زیاد می‌شود و به مرور زمان به سمت بی‌نهایت میل می‌کند
- بعضی می‌گویند اگر μ همیشه بزرگتر از λ است صف تشکیل نمی‌شود
  - اما اشتباه است : چون زمان ورود فریم‌ها به صف و همینطور زمان سرویس دادن به فریم‌ها تصادفی است
  - فرض کنید قرار است بطور میانگین ۱۰ فریم در ساعت وارد صف شود و نرخ سرویس دادن هم ۱۵ فریم در ساعت باشد اما ۱۰ فریم همه می‌توانند در دقیقه اول وارد شوند و مثلا ۵۹ دقیقه بعدی چیزی وارد نشود در اینصورت صف تشکیل می‌شود

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir
شبکه های کامپیوتری
رامین رضوی

- *اگر فرض کنیم که طول صف خیلی بزرگ است*
- $\frac{\lambda}{\mu} \sim 0$: *میانگین تاخیر صف تقریبا صفر است،بسته‌ها با یک صف خالی مواجه می‌شوند*
- $\frac{\lambda}{\mu} > 1$: صف بزرگ و بزرگتر می‌شود تاخیر صف به سمت بی‌نهایت میل می‌کند،loss زیاد می‌شود
- $\frac{\lambda}{\mu} < 1$: در اینصورت μ بزرگتر از λ است

❑ ما فرض کردیم که ظرفیت صف نامحدود است ولی در دنیای واقعی صف‌ها ظرفیت محدودی دارند . وقتی تاخیر زیاد می‌شود بافرها شروع می‌کنند به پر شدن و در اینصورت loss زیاد می‌شود وقتی بسته‌ای loss می‌شود ما آن بسته را مجددا ارسال می‌کنیم،بنابراین علاوه بر بسته‌هایی که در حالت عادی باید ارسال کنیم یکسری بسته هم باید مجددا و اضافه بر سازمان بفرستیم بنابراین صف‌ها پرتر و تاخیرها بیشتر می‌شود بنابراین loss باز هم زیادتر می‌شود و این ماجرا ادامه دارد تا شبکه به حالت انفجار می‌رسد

- **سوال:** فرض کنید یک سوئیچ بسته، یک بسته را دریافت می‌کند و سپس تعیین می‌کند که از کدام پورت خروجی به سمت مقصد خارج شود، وقتی این بسته به این پورت خروجی می‌رسد، می‌بینند که ۴ بسته جلوتر از آن در صف ارسال وجود دارد، و همین طور این پورت خروجی در وسط ارسال یک بسته دیگر است، اگر همه بسته‌ها ۱۵۰۰ بایتی باشند و نرخ ارسال لینک خروجی $2\ Mbps$ باشد تاخیر صف برای این بسته چقدر خواهد بود؟

پاسخ : بسته‌ای که می‌رسد ابتدا باید صبر کند تا ۶۷۵۰ بایت توسط لینک با نرخ ۲ مگابیت در ثانیه انتقال پیدا کند

$$\frac{6750\times 8\ bit}{2\times 10^6\ \frac{bit}{s}} = 27\ ms$$

نکته: بطور کلی اگر همه بسته‌ها L بیتی باشند و نرخ ارسال لینک خروجی سووئیچ R باشید و X بیت از بسته در حال ارسال فعلی مخابره شده باشد و n بسته دیگر در صف باشد تاخیر صف برای آخرین بسته وارد شده به صف برابر است با: $\frac{NL + L - X}{R}$

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سوال مهم

- فرض کنید N بسته بطور همزمان وارد لینکی می‌شوند که در آن هیچ بسته‌ای را ارسال نمی‌کند و هیچ بسته‌ای هم در صف ارسال ندارد. طول هر بسته L بیت و آهنگ ارسال لینک خروجی سوئیچ R بیت در ثانیه است، میانگین تاخیر صف هر یک از این N بسته چقدر است؟

پاسخ : تاخیر برای ارسال اولین بسته ارسالی ۰ و برای دومین بسته ارسالی $\frac{L}{R}$ و برای Nامین بسته ارسالی $(N-1)\frac{L}{R}$ بنابراین میانگین تاخیر برابر است با :

$$Average\ deley = \frac{\frac{L}{R}+\frac{2L}{R}+\cdots+(N-1)\frac{L}{R}}{N} = \frac{N-1}{2}\times\frac{L}{R}$$

سوال : اگر فرض کنیم در هر $L\frac{N}{R}$ ثانیه N بسته وارد این لینک می‌شود میانگین تاخیر صف یک بسته چقدر است؟

پاسخ : هر N بسته $N\frac{L}{R}$ طول می‌کشد تا ارسال شود، بنابراین وقتیکه یک دسته Nتایی جدیدی از راه می‌رسد بافر خالی است، بنابراین میانگین برابر با عدد بالا یی خواهد بود

شدت ترافیک

- به $\frac{\lambda}{\mu}$ شدت ترافیک گویند و آن را با I نشان می‌دهند : $I=\frac{\lambda}{\mu}$
- اگر زمان سرویس دادن به یک بسته یا همان زمان ارسال یک بسته در واحد ثانیه را معکوس کنیم تعداد بسته‌ای که می‌توانیم در واحد ثانیه ارسال کنیم بدست می‌آید، بنابراین

$$\mu = \frac{1}{T_f} = \frac{1}{\frac{L}{R}} = \frac{R}{L}$$

- در کتاب راس a همان λ است، بنابراین شدت ترافیک می‌شود

$$I = \frac{a}{\mu} = \frac{a}{\frac{R}{L}} = \frac{aL}{R}$$

- حال اگر بخواهیم میانگین تاخیر صف را بر اساس شدت ترافیک بدست آوریم خواهیم داشت:

$$T_{queue} = \frac{1}{\mu-\lambda} = \frac{1}{\frac{R}{L}-a} \xrightarrow{\times\frac{L}{R}} \frac{\frac{L}{R}}{1-\frac{L}{R}a} = \frac{L}{R}\times\frac{1}{1-I}$$

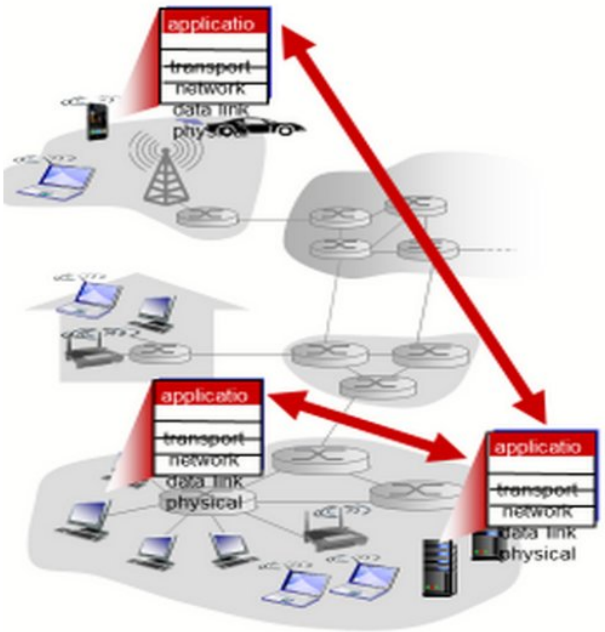
- با نزدیک شدن شدت ترافیک به ۱ میانگین تاخیر صف به سرعت افزایش می‌یابد بعبارت دیگر فقط چند درصد افزایش در شدت ترافیک باعث چند برابر شدن تاخیر می‌شود.

Scanned with CamScanner

فصل دوم : لایه کاربرد

Principles of Network Applications

هدف از ایجاد شبکه تبادل داده بین برنامه‌های کاربردی است که روی هاست های مختلف در شبکه قرار دارند، این برنامه های از طریق API ها (system call) از پروتکل‌های استاندارد لایه کاربرد سرویس می‌گیرند



برنامه‌های شبکه باید : که به هر زبانی می‌توانید بنویسیدشان

- باید بتوانند روی سیستم‌های انتهایی مختلف اجرا شوند
- باید بتوانند با برنامه‌های دیگر شبکه ارتباط برقرار کنند
- مثال : برنامه مرورگر که در هاست میزبان اجرا می‌شود ارتباط برقرار می‌کند با برنامه سرویس دهنده وب که روی هاست سرور اجرا می‌شود
- نیازی نیست طوری بنویسید که روی دستگاه‌های هسته شبکه اجرا بشود (سوئیچ‌ها و روترها)
- دستگاه‌های هسته شبکه نمی‌توانند برنامه‌های کاربرها را اجرا کنند
- محدود کردن برنامه‌های کاربردی به سیستم‌های انتهایی
  - سرعت در ایجاد برنامه‌ها
  - سهولت در توسعه
  - سرعت در انتشار

Network Application Architectures

- معماری برنامه‌های کاربردی (توزیع شده) توسط برنامه نویس طراحی می‌شود و این معماری مشخص می‌کند (در اینجا معماری نرم افزاری مد نظرمون هست)
  - برنامه شامل چه مولفه‌ها و اجزا نرم افزاری باشد
  - ارتباط بین برنامه‌ها و اجزا به چه شکل باشد
    - اینکه مکانیزم ارتباطی مون چی باشه و از چه پروتکل هایی در لایه های پایین تر استفاده کنم؟
  - ساختار برنامه روی سیستم‌های انتهایی به چه شکل باشد
    - مثلا آیا یک فرایند همیشه کلاینت و یک فرایند همیشه سرور است یا یک فرایند در یک نشست می‌تواند کلاینت و در نشستی دیگر سرور باشد
- برنامه‌های شبکه اغلب بر اساس دو نوع معماری طراحی می‌شوند (معماری برنامه‌ی کاربردی)
  - client-server
  - peer-to-peer (P2P)
- برخی از برنامه‌ها از معماری ترکیبی بهره می‌برند و قسمت‌هایی از هر دو معماری مشتری_سرویس دهنده و نظیر به نظیر را ترکیب می‌کنند
  - در اغلب برنامه‌های پیام رسان فوری چند سرویس دهنده وجود دارد که آدرس‌های IP کاربران را ثبت و نگهداری می‌کند ولی پیام‌های بین کاربران بدون دخالت سرویس دهنده‌ها بین هم رد و بدل می‌شود

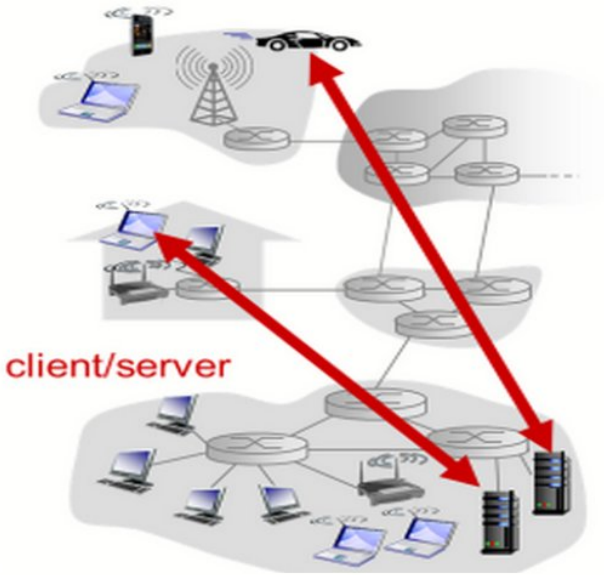
Scanned with CamScanner

معماری شبکه در مقابل معماری برنامه لایه کاربرد

- معماری شبکه به ساختار و سازمان فرآیندهای ارتباطی درون لایه‌ها اشاره می‌کند
  - مثلا معماری شبکه می‌گوید معماری اینترنت از ۵ لایه تشکیل شده
- معماری برنامه کاربردی ساختار برنامه را روی سیستم‌هایی انتهایی مختلف مشخص می‌کند
- از دید برنامه نویس(تولید کننده برنامه) : معماری شبکه ثابت است که مجموعه‌ای از سرویس‌های مشخص را در اختیار برنامه می‌گذارد

client-server architecture

در یک ارتباط مشخص (یک نشست) یکی کلاینت است و یکی سرور
- تعدادی از برنامه‌هایی با معماری کلاینت_سرور : وب، FTP، Telnet، email



Server

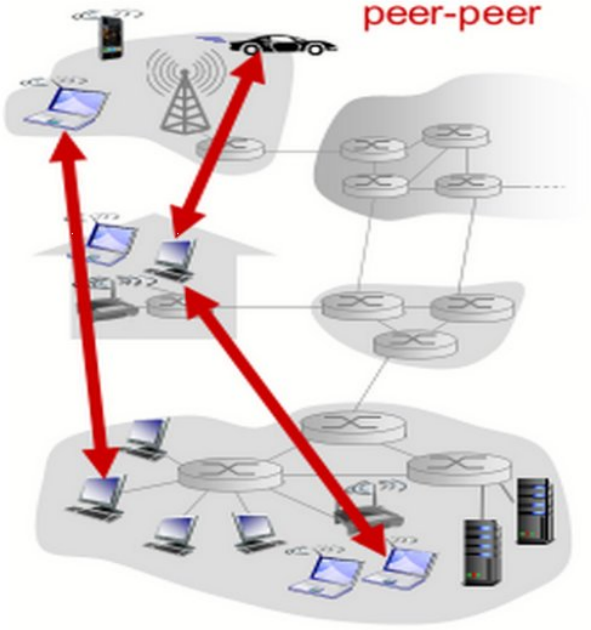
- همیشه روشن است
- دارای آدرس IP ثابت و شناخته شده هستند
- استفاده از دیتا سنتر در درخواست‌های بالا
- شروع کننده نیستند
- پاسخ دهنده به یک درخواست (سرویس) هستند

Clients

- لزومی ندارد همیشه روشن باشند
- یک مشتری با سرور ارتباط برقرار می‌کند
- کلاینت‌ها هرگز بطور مستقیم با همدیگر ارتباط برقرار نمی‌کنند
- آدرسهای IP می‌تواند عوض شود
- آغازگر ارتباط هستند
- درخواست کننده یک سرویس هستند

P2P architecture

- برنامه‌های کاربردی بدون واسطه یک سرویس دهنده مرکزی و از ارتباط مستقیم بین میزبانهای متصل به یکدیگر استفاده می‌کنند. به این میزبانها peer می‌گویند، که این نظیرها مختص به افراد است
- در معماری نظیر به نظیر هیچ گونه سرویس دهنده مرکزی وجود ندارد یا تعداد آن در کمترین میزان ممکن است
  - کمترین تکیه بر روی سرورهای تخصیص یافته شده داخل دیتا سنترها
- نودها بطور متناوب متصل می‌شوند و امکان دارد آدرس IP شان را عوض کنند
- میزبان‌ها بطور خودسرانه با یکدیگر ارتباط برقرار می‌کنند
- مدیریت پیچیده
- نودها می‌توانند on یا off باشند
- مثال: تورنت، اسکایپ، تلویزیون اینترنتی (IPTV)



مزیت

- Self scalability :درسته اضافه شدن peer جدید درخواست جدیدی را اضافه می‌کند اما ظرفیت پاسخ را نیز بالا می‌برد
- cost effective : مثل client server نیازی به زیرساخت و پهنای باند قابل توجهی برای سرورها ندارد

Scanned with CamScanner

چالش‌های پیش روی برنامه‌های P2P

- ISP Friendly : ISP های محلی پهنای باند خود را بصورت نامتقارن در اختیار کاربران خود قرار می‌دهند (downstream بیشتر از upstream)
  - در سمت کلاینت پهنا باند دانلود کاربران بیشتر از پهنا باند آپلود آنها است و در سمت سرور پهنا بلند آپلود بیشتر از دانلود است
  - برنامه‌های P2P بار ترافیک را از سرویس دهنده‌ها به ISP های محلی منتقل می‌کنند که باعث فشار بر روی ISP ها می‌شود
  - برنامه های p2p هم سرویس می‌دهند و هم سرویس می‌گیرند که این مسئله نیازمند این است که ISP ها یک سرویس متقارن به کاربران ارائه بدهند (سرویسی که پهنا باند دانلود و آپلود یکسانی به کاربران بدهد که این در واقعیت وجود ندارد در حال حاضر)
- *Security : ماهیت برنامه‌های p2p باز و توزیع شده است که این امر باعث می‌شود که راه نفوذ هکرها باز تر باشد*
- *Incentives (انگیزش‌ها) : متقاعد کردن داوطلبان برای در اختیار گذاشتن داوطلبانه رسوس‌هایشان*
  - *با تشویق*
  - *با تنبیه*

Processes communicating

Process : برنامه در حال اجرا درون یک میزبان (end system)

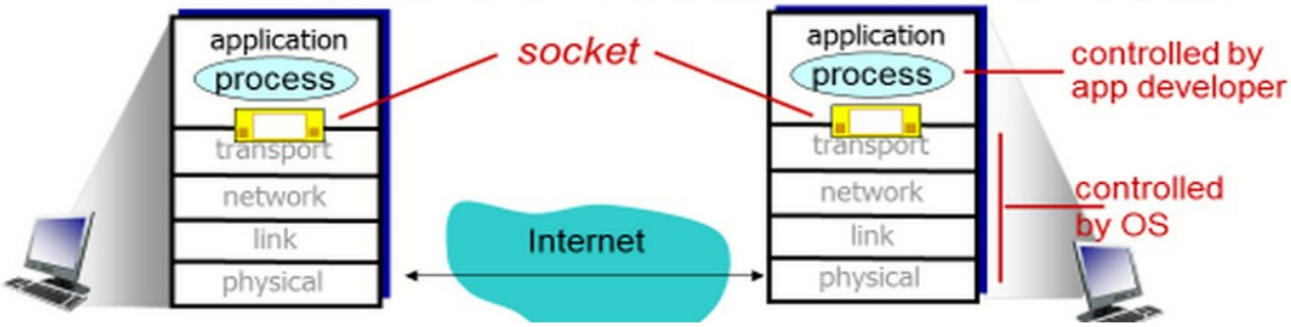
- *اغلب برنامه‌های کاربردی از یک یا چند زوج فرآیند تشکیل می‌شوند که از طریق شبکه با یکدیگر پیام مبادله می‌کنند*
- *در یک هاست دو فرآیند با استفاده از inter-process communication تحت کنترل os با همدیگر ارتباط برقرار می‌کنند*
- *در os برای ارتباط بین دو فرآیند مکانیزم‌هایی متعددی مثل file sharing و shared memory و call و ... داریم که چون در شبکه فرآیندهای روی هاست‌های مختلف می‌خواهند با هم ارتباط برقرار کنند هیچ کدام از این روش‌ها قابل استفاده نیست*
- *پروسس‌های روی هاست‌های مختلف از طریق تبادل message با هم ارتباط برقرار می‌کنند*
- در یک نشست ارتباطی مشخص بین یک زوج فرآیند
  - *client process: فرآیندی که ارتباط را آغاز می‌کند(initiates می کند) (فرآیند ارسال کننده)*
  - *server process: فرآیندی که منتظر می‌ماند تا با آن تماس بگیرند (فرآیند دریافت کننده)*
- *مثال: در برنامه‌های وب*
  - *مرورگر مشتری : فرآیند مرورگر مشتری*
  - *سرویس دهنده وب، فرآیند سرویس دهنده وب*
- *نه تنها معماری مشتری_سرویس دهنده بلکه برنامه‌هایی با معماری P2P هم client processes و هم server processes دارند*

Scanned with CamScanner

Sockets

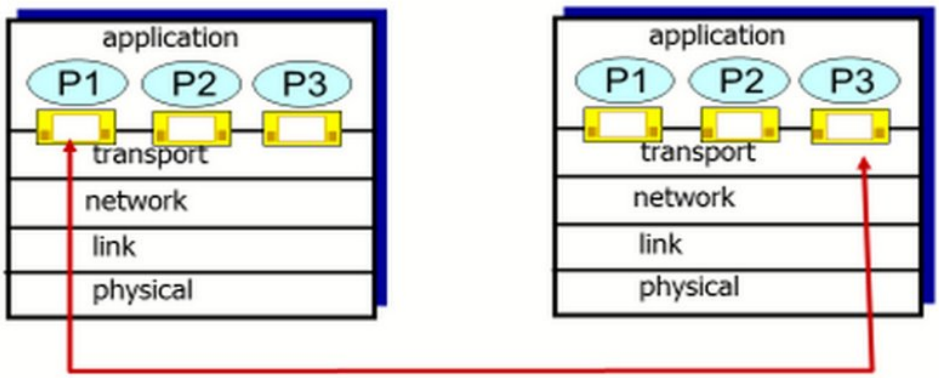
- فرآیندها، پیام‌ها را از طریق سوکت‌شان (یک واسط نرم افزاری، یک در) به شبکه ارسال یا از شبکه دریافت می‌کنند
- فرآیندهای شبکه از طریق ارسال پیام به سوکتهای خود با یکدیگر ارتباط برقرار می‌کنند
- سوکت واسط بین لایه کاربرد و لایه انتقال است
- سوکت یک واسط برنامه‌نویسی است که برنامه‌های کاربردی طبق آن نوشته می‌شوند بنابراین به آن واسط برنامه‌نویسی برنامه API (Application Programming Interface) می‌گویند
- سوکت شبیه در خانه است
  - فرآیند ارسال کننده پیام‌ها را از درب‌اش به بیرون پرتاب می‌کند
  - فرآیند ارسال فرض می‌کند که زیر ساخت ارتباطی وجود دارد که پیام‌اش را تا درب فرآیند مقصد منتقل خواهد کرد
- تولید کننده برنامه کنترل ناچیزی در سمت لایه کاربرد سوکت شامل موارد زیر دارد:

۱) انتخاب پروتکل لایه انتقال ۲) تعیین تعداد کمی از پارامترهای لایه انتقال مثل ماکزیمم سایز سگمنت‌ها



Addressing processes

- فرآیند مبدا برای ارسال پیام به فرآیند مقصد، باید آدرس (شناسه) فرآیند مقصد را داشته باشد
- هاست‌ها دارای آدرس IP منحصر به فرد ۳۲ بیتی هستند
- آیا آدرس IP مقصد برای شناسایی و ارسال پیام به فرآیند مورد بحث مقصد کافی است؟
- خیر- چون فرآیندهای بسیاری مربوط برنامه‌های شبکه مختلف می‌توانند روی میزبان مقصد اجرا بشوند
- اینکه شناسه یک سوکت چگونه در TCP و UDP مشخص می‌شود را قبلا اشاره کرده‌ایم و بعدا دقیق تر بررسی می‌کنیم
- شماره‌های پورت زیر ۱۰۲۴ معمولا پورت‌های شناخته شده برای برنامه‌های مشخص شده‌ای هستند
- مثلا : FTP : 20 and 21 ، mail server: 25 ، HTTP server: 80



مثلا برای ارسال یک پیام HTTP به سایت konkurcomputer.ir

IP address: 128.139.223.8
port number: 80

Scanned with CamScanner

سرویس‌هایی که متصور است که لایه انتقال ب‌تواند در اختیار لایه کاربرد قرار دهد

- شبکه‌ها بیش از یک پروتکل لایه انتقال دارند، بنابراین برنامه شبکه ما باید با توجه به سرویس‌هایی که میخواهد یکی از پروتکل‌ها را انتخاب کند
- سرویس‌هایی که لایه انتقال در اختیار لایه کاربرد قرار می‌دهد را در ۴ بعد می‌توان بررسی کرد

Reliable Data Transfer

- برخی از برنامه‌ها (مثل انتقال فایل و انتقال سندهای وب و ...) نیاز این دارند که ۱۰۰ درصد دیتا را reliable منتقل کنند و loss sensitive هستند
  - همه بسته‌ها حتما به مقصد برسند (no loss)
  - همه بسته‌ها درست به مقصد برسند (no error)
  - بسته‌ها به ترتیب به مقصد برسند (in order)
  - بسته‌ها تکراری به مقصد نرسند (no replicate)
  - میل، انتقال فایل، تراکنش‌های مالی، انتقال سندهای وب، Telnet نیاز به انتقال دیتا قابل اطمینان دارند
- برخی از برنامه‌ها (مثل کنفرانس ویدیویی و ...) loss را تحمل کنند و loss tolerant هستند

Throughput

- یک نوع سرویس دیگر که لایه انتقال می‌تواند ارائه کند گذردهی تضمینی با یک آهنگ مشخص است با این سرویس برنامه کاربردی می‌تواند از پروتکل لایه انتقال بخواهد تا یک گذردهی مشخص در اختیار آن قرار دهد
- چون ممکن است چند نشست بطور مشترک از پهنای باند یک مسیر شبکه استفاده کنند، و چون این نشست‌ها به دلخواه ارسال و دریافت می‌کنند گذردهی در طول زمان ممکن است تغییر کند
- برخی از برنامه‌ها (مثل مالتی مدیا) برای اینکه موثر باشند به مینیمم مقداری از گذردهی نیاز دارند.
- برنامه‌هایی که به گذردهی تضمینی نیاز دارند را برنامه‌های bandwidth sensitive می‌گویند
- برخی دیگر از برنامه‌ها که به آنها elastic apps می‌گویند از هر گذردهی ای که در اختیارشان قرار بگیرد استفاده می‌کنند و خود را به گذردهی موجود تطبیق می‌دهند (مثل Electronic mail,
- file transfer, and Web transfers)

What transport service does an app need?

Timing

- برخی از برنامه‌ها (مثل تلفن اینترنتی یا بازی‌های تعاملی، کنفرانس اینترنتی) برای اینکه موثر باشند نیاز به تاخیر پایین دارند
  - بنابراین نیاز به تضمینی برای حداکثر تاخیر دارند
- بعضی از برنامه‌ها هستند که با تاخیر نسبی مشکلی ندارند ولی نوسانات تاخیر را نمی‌پسندند (مثل پخش ویدیو)
  - بنابراین نیاز به تضمینی برای حداکثر jitter دارند

Security

- یک پروتکل انتقال می‌تواند سرویس‌های امنیتی نظیر رمزگذاری و رمزگشایی و احراز هویت نقطه انتهایی(end-point authentication) و ... در اختیار برنامه‌های کاربردی بگذارد
- محرمانگی (confidentiality) : فقط ارسال کننده و گیرنده مد نظر وی باید بتوانند محتوای پیام ارسالی را بفهمند. پروتکل لایه انتقال فرستنده می‌تواند داده‌هایی که قرار است به سمت مقصد ارسال شود را قبل از ارسال روی شبکه رمزنگاری کند
- end-point authentication: فرآیندی که در آن یک موجودیت در یک شبکه کامپیوتری هویت خود را به موجودیتی دیگر اثبات می‌کند. آیا اون کسی که من دارم باهاش ارتباط برقرار می‌کنم، واقعا همونی هست که انتظار دارم
- صحت داده (پیام) (data integrity): فرستنده و گیرنده باید مطمئن شوند که محتوای پیام‌های ارسالی و دریافتی آنها چه تصادفی و چه عمدا دچار تغییر نخواهد شد

Scanned with CamScanner

ویژگی‌های برخی از برنامه‌های شبکه

Application	Data Loss	Throughput	Time-Sensitive
File transfer/download	No loss	Elastic	No
E-mail	No loss	Elastic	No
Web documents	No loss	Elastic (few kbps)	No
Internet telephony/ Video conferencing	Loss-tolerant	Audio: few kbps–1Mbps Video: 10 kbps–5 Mbps	Yes: 100s of msec
Streaming stored audio/video	Loss-tolerant	Same as above	Yes: few seconds
Interactive games	Loss-tolerant	Few kbps–10 kbps	Yes: 100s of msec
Instant messaging	No loss	Elastic	Yes and no

Scanned with CamScanner

نیازهای Application ها

- شبکه‌ها بیش از یک پروتکل لایه انتقال دارند، بنابراین برنامه شبکه ما باید با توجه به سرویس‌هایی که میخواهد یکی از پروتکل‌ها را انتخاب کند
- سرویس‌هایی که لایه انتقال در اختیار لایه کاربرد قرار می‌دهد را در ۴ بعد می‌توان بررسی کرد

Reliable Data Transfer

- برخی از برنامه‌ها (مثل انتقال فایل و انتقال سندهای وب و ...) نیاز این دارند که ۱۰۰ درصد دیتا را reliable منتقل کنند و loss sensitive هستند
  - همه بسته‌ها حتما به مقصد برسند (no loss)
  - همه بسته‌ها درست به مقصد برسند (no error)
  - بسته‌ها به ترتیب به مقصد برسند (in order)
  - بسته‌ها تکراری به مقصد نرسند (no replicate)
  - میل، انتقال فایل، تراکنش‌های مالی، انتقال سندهای وب، Telnet نیاز به انتقال دیتا قابل اطمینان دارند
- برخی از برنامه‌ها (مثل کنفرانس ویدیویی و ...) loss را تحمل کنند و loss tolerant هستند

Throughput

- یک نوع سرویس دیگر که لایه انتقال می‌تواند ارائه کند گذردهی تضمینی با یک آهنگ مشخص است با این سرویس برنامه کاربردی می‌تواند از پروتکل لایه انتقال بخواهد تا یک گذردهی مشخص در اختیار آن قرار دهد
- چون ممکن است چند نشست بطور مشترک از پهنای باند یک مسیر شبکه استفاده کنند، و چون این نشست‌ها به دلخواه ارسال و دریافت می‌کنند گذردهی در طول زمان ممکن است تغییر کند
- برخی از برنامه‌ها (مثل مالتی مدیا) برای اینکه موثر باشند به مینیمم مقداری از گذردهی نیاز دارند.
- برنامه‌هایی که به گذردهی تضمینی نیاز دارند را برنامه‌های bandwidth sensitive می‌گویند
- برخی دیگر از برنامه‌ها که به آنها elastic apps می‌گویند از هر گذردهی ای که در اختیارشان قرار بگیرد استفاده می‌کنند و خود را به گذردهی موجود تطبیق می‌دهند (مثل Electronic mail,
- file transfer, and Web transfers)

نیازهای Application ها (ادامه)

Timing

- برخی از برنامه‌ها (مثل تلفن اینترنتی یا بازی‌های تعاملی، کنفرانس اینترنتی) برای اینکه موثر باشند نیاز به تاخیر پایین دارند
  - بنابراین نیاز به تضمینی برای حداکثر تاخیر دارند
- بعضی از برنامه‌ها هستند که با تاخیر نسبی مشکلی ندارند ولی نوسانات تاخیر را نمی‌پسندند (مثل پخش ویدیو)
  - بنابراین نیاز به تضمینی برای حداکثر jitter دارند

Security

- یک پروتکل انتقال می‌تواند سرویس‌های امنیتی نظیر رمزگذاری و رمزگشایی و احراز هویت نقطه انتهایی(end-point authentication) و ... در اختیار برنامه‌های کاربردی بگذارد
- محرمانگی (confidentiality) : فقط ارسال کننده و گیرنده مد نظر وی باید بتوانند محتوای پیام ارسالی را بفهمند. پروتکل لایه انتقال فرستنده می‌تواند داده‌هایی که قرار است به سمت مقصد ارسال شود را قبل از ارسال روی شبکه رمزنگاری کند
- end-point authentication: فرآیندی که در آن یک موجودیت در یک شبکه کامپیوتری هویت خود را به موجودیتی دیگر اثبات می‌کند. آیا اون کسی که من دارم باهاش ارتباط برقرار می‌کنم، واقعا همونی هست که انتظار دارم
- صحت داده (پیام) (data integrity): فرستنده و گیرنده باید مطمئن شوند که محتوای پیام‌های ارسالی و دریافتی آنها چه تصادفی و چه عمدا دچار تغییر نخواهد شد

Scanned with CamScanner

سرویس‌های لایه انتقال اینترنت (شبکه‌های TCP/IP): TCP service

Tcp سرویسی که به لایه بالایی اش می‌دهد Byte Stream oriented است. Tcp استریمی از بایت ها را از سوکت‌اش می‌گیرد و دقیقا همان استریم را به سوکت سمت مقصد تحویل می‌دهد. برای TCP پیام‌های لایه App سر و ته ندارد. باندری App لایری اگر در استریمی که لایه App به لایه انتقال میدهد وجود داشته باشد، TCP این باندری را نه می‌بیند و نه براش مهم است، در نتیجه آن کسی که باید سر و ته پیام ها را بدست بیاورد لایه App هست. TCP در ۲ طرف ارتباط اش بایت‌هایی که می‌خواهد بفرستد و بگیرد را بفر می‌کند و بافر کردن در TCP یک امر اجتناب ناپذیر است، با استفاده از مدیریت مناسب این بافرها در مبدا و مقصد است که TCP می‌تواند قول دهد که هر دنباله‌ای از بایت‌ها را که از مبدا می‌گیرد بدون از دست دادن هیچ بایتی و به همان ترتیبی که در مبدا گرفته است در مقصد تحویل دهد، البته همین بافرهاست که باعث می‌شود که ما وقتی از TCP استفاده می‌کنیم خیلی کنترلی در مورد اینکه تاخیر رساندن داده ها از لایه کاربرد مبدا به لایه کاربرد مقصد نداریم. مجموعه بایت‌هایی که از طرف فرستنده می‌خواهد به طرف گیرنده ارسال شود دسته بندی می‌شود در unit هایی به نام سگمنت، سایز سگمنت می‌تواند کوچک و بزرگ شود، کوچک و بزرگ شدن سگمنت ها این امکان را به TCP می دهد که با کنترل سایز سگمنت‌ها نرخ فرستادن داده هایش داخل کانال را تنظیم کند. هر سگمنت TCP یک هدر ۲۰ بایتی دارد. سایز سگمنت TCP را کمتر مساوری MSS می‌گیرند که در لایه دیتا لینک segmentation و reassembly نداشته باشیم.

ویژگی های TCP

سرویس انتقال داده‌ی قابل اطمینان (reliable transport) : تمام داده فرآیندها را بدون خطا و با ترتیب درست و بدون تکرار به سوکت سمت مقابل تحویل می‌دهد

ارسال مجدد دارد (retransmission)

TCP کنترل خطا دارد

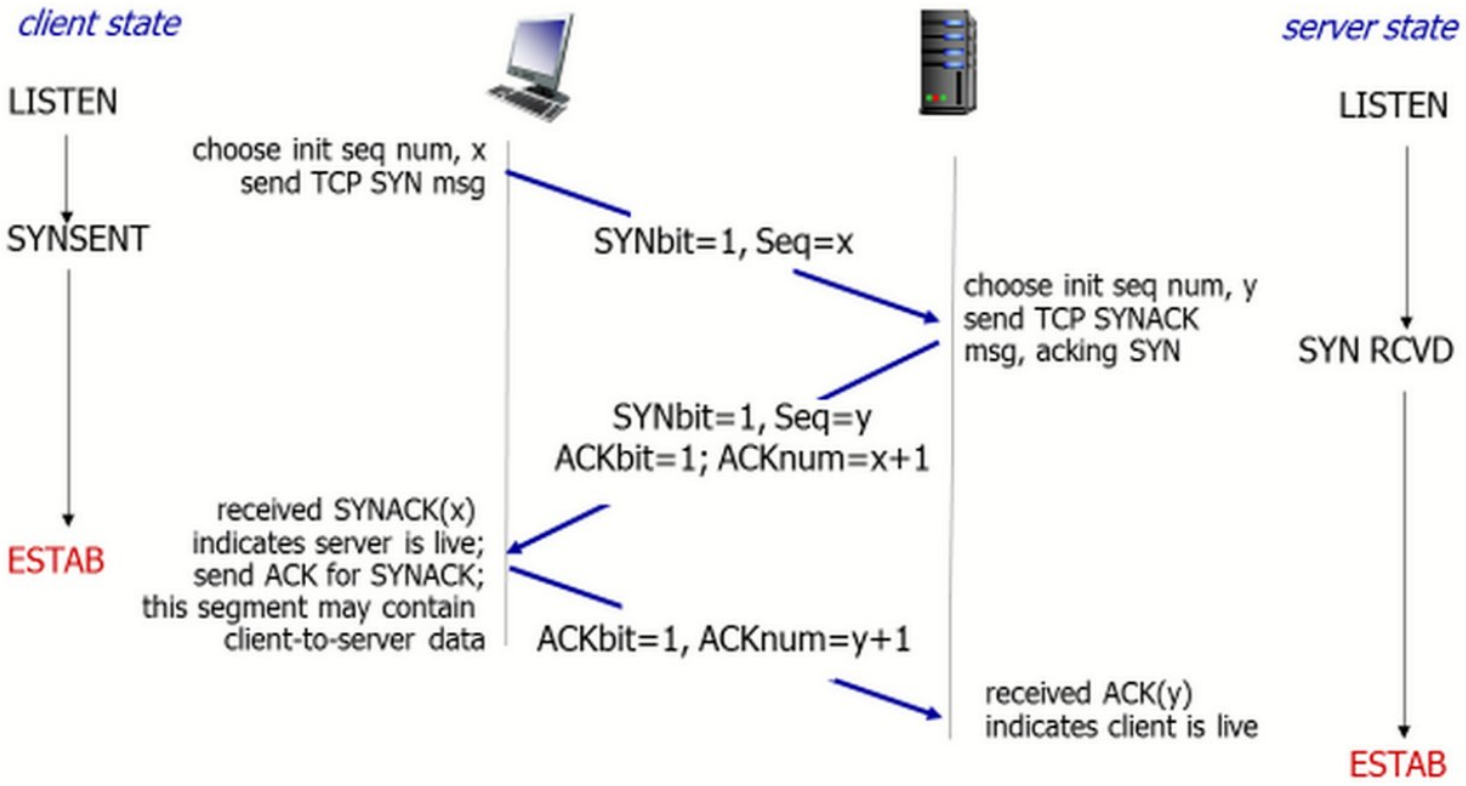
سرویس اتصال گرا (connection-oriented) :

این اتصال یک اتصال منطقی بین دو فرایند است و یک اتصال فیزیکی بین دو ماشین نیست، حال اتصال منطقی به چه معناست و چطور ایجاد می‌شود؟

قبل از شروع ارسال پیام‌های application-level ، طبق فرآیندی به نام 3 way handshaking مشتری و سرویس دهنده باید اطلاعات کنترلی لایه انتقال را مبادله و پارامترهای انتقال داده را تعیین کنند، 3 way handshaking، مشتری و سرویس دهنده را به حالت آماده باش در می‌آورد و به آنها اجازه می‌دهد تا خود را برای حجوم بسته‌های داده آماده کند. در اثر 3 way handshaking یک کانکشن TCP دو طرفه بین دو فرآیند شکل می‌گیرد، ارتباط دوطرفه (full-duplex) هست یعنی هر دو طرف می‌توانند همزمان به یکدیگر دیتا بفرستند. پس از پایان تبادل داده کانکشن باید release شود.

Scanned with CamScanner

TCP 3-way handshake



سرویس‌های لایه انتقال اینترنت (شبکه‌های TCP/IP): TCP service

کنترل ازدحام (congestion control) : کنترل ازدحام در این لایه در راستای منافع کل شبکه است نه برای فرایندهای دو طرف کانال ارتباطی، در صورت تشخیص شلوغ بودن شبکه

- فرستنده با نرخ پایین‌تری داده ارسال می‌کند
- سعی می‌کند هر اتصال TCP در مصرف پهنای باند شبکه از سهم منصفانه‌اش تجاوز نکند

کنترل جریان (flow control) : سرعت فرستنده و گیرنده را به هم تنظیم می‌کند

نکته: TCP فقط در سیستم‌های انتهایی اجرا می‌شود نه در روترها و سوئیچ‌های میانی، بنابراین این دستگاه‌ها اطلاعات حالت اتصال‌های TCP را نگه نمی‌دارند و بنابراین مسیریابهای بین راه هیچ درکی از اتصال‌های TCP ندارند

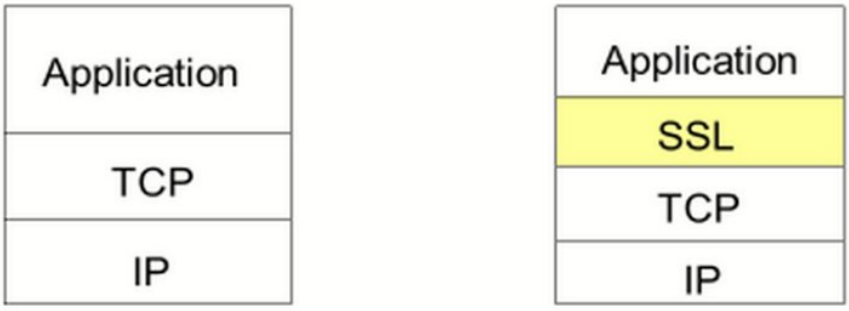
نکته: اتصال‌های TCP همیشه نقطه به نقطه(point to point) هستند و ارتباط بین یک فرستنده و یک گیرنده وجود دارد و انتقال داده از یک فرستنده به چندین گیرنده(چند پخشی) با TCP ممکن نیست و اگر می‌خواهید چنین کاری بکنید باید n کانکشن جداگانه از نقطه مبدا به n نقطه مقصد ایجاد کنید

نکته: TCP همزمانی، مینیمم گذردهی و امنیت را پشتیبانی(ارائه) نمی‌کند

Scanned with CamScanner

SSL and TCP/IP

- TCP خودش به تنهایی امنیت ندارد، اما به کمک SSL (secure socket layer) که در لایه کاربرد پیاده سازی می‌شود امنیت برقرار می‌شود
- TCPتقویت شده با SSL سرویس های زیر را در اختیار فرآیندها می‌گذارد
  1. رمز نگاری
  2. صحت داده
  3. احراز هویت نقطه انتهایی



normal application *application with SSL*

- SSL provides application programming interface (API) to applications
- C and Java SSL libraries/classes readily available

UDP service

این پروتکل وظایف یک پروتکل انتقال را در کمترین سطح ممکن انجام می‌دهد و غیر از عملکرد multiplexing و demultiplexing و کمی بررسی خطا UDP چیز خاص دیگری به پروتکلIP اضافه نمی‌کند، UDP به پیام‌های لایه کاربرد شماره پورت مبدا و مقصد، طول قطعه UDP (سرآیند بعلاوه داده) و یک checksum را می‌چسباند و بلافاصله قطعه حاصل را به لایه شبکه می‌دهد

Connectionless

unreliable data transfer : فرستنده نمی‌تواند مطمئن باشد که پیامی که به دست سوکت UDP اش داده است را فرآیند گیرنده دریافت خواهد کرد. همین طور پیام‌ها می‌توانند بدون حفظ ترتیب ارسال به گیرنده برسند

کنترل ازدحام ندارد : سمت ارسال UDP می‌تواند داده‌ها را با هر نرخی که می‌خواهد به لایه شبکه زیر خود پمپ کند

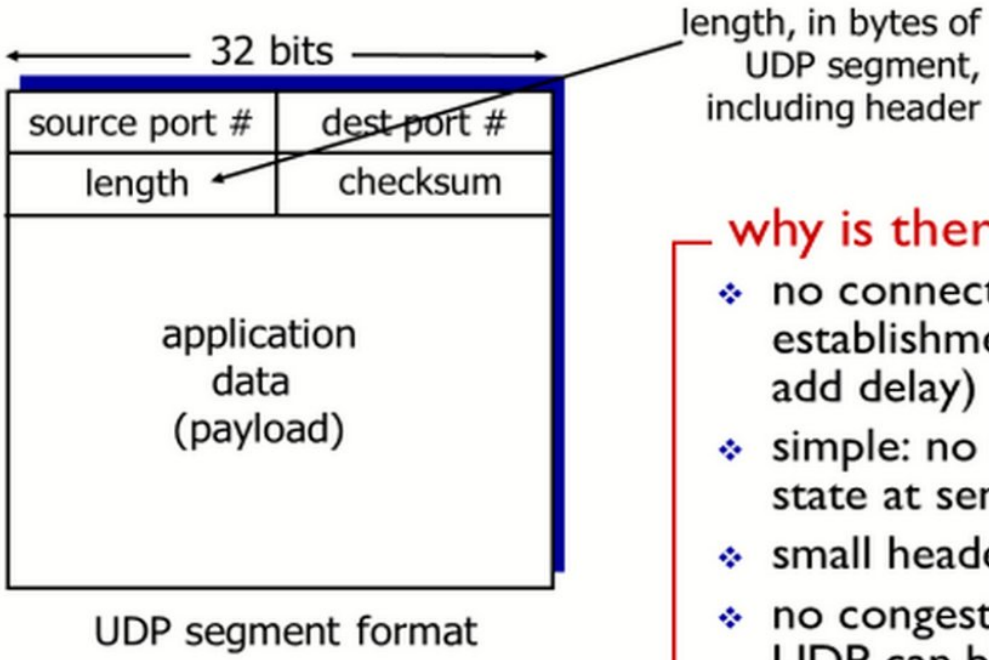
نکته: UDP همچنین کنترل جریان، همزمانی، گارانتی گذردهی، امنیت را ارائه نمی‌کند

نکته: برنامه‌هایی که از UDP بعنوان پروتکل انتقال استفاده می‌کنند نیز می‌توانند انتقال داده قابل اطمینان داشته باشند

- در این برنامه‌ها، برنامه نویسان باید سازکارهای تصدیق دریافت و ارسال مجدد را خودشان پیاده‌سازی کنند
- در اینصورت محدودیت‌های نرخ ارسال که کنترل ازدحام TCP اعمال می‌کند را نخواهیم داشت

Scanned with CamScanner

UDP: segment header



UDP segment format

why is there a UDP?

- no connection establishment (which can add delay)
- simple: no connection state at sender, receiver
- small header size
- no congestion control: UDP can blast away as fast as desired

وقتی TCP هست چرا UDP؟

کنترل بیشتر برنامه‌های کاربردی بر زمان ارسال پیام‌ها

- اگر از UDP استفاده کنید همین که لایه کاربرد پیام خود را به UDP بدهد، UDP آن را در یک قطعه UDP می‌پیچد و به لایه شبکه می‌فرستد ولی TCP ممکن است مجبور شود پیامی که از لایه کاربرد می‌گیرد را به علت اینکه می‌خواهد اندازه سگمنت به یک میزانی برسد در بافرش بگذارد و فعلا ارسال نکند، همین طور در گیرنده نیز اگر قسمتی از بایت های یک سگمنت نرسیده باشد تا رسیدن آن بایت ها سگمنت را به لایه کاربرد تحویل نمی‌دهد
- TCP تا زمانیکه از رسیدن یک قطعه به مقصد مطمئن نشود به ارسال آن ادامه خواهد داد و هیچ اهمیتی به زمان نمی‌دهد، حال آنکه برنامه‌های کاربردی real time به حداقلی از نرخ ارسال نیاز دارند و تاخیر زیاد در دریافت بسته‌ها را نمی‌پسندند و در عوض از دست رفتن بعضی از بسته‌ها در ازای دریافت به موقع برایشان مطلوب‌تر است

نداشتن زمان setup اولیه

عدم نیاز به نگهداری اطلاعات اتصال:

- TCP برای پیاده‌سازی سرویس انتقال داده قابل اطمینان و مکانیزم کنترل ازدحام نیاز دارد اطلاعات اتصال شامل بافرهای ارسال و دریافت، پارامترهای کنترل ازدحام و پارامترهای عدد توالی و عدد تصدیق را در سیستم‌های انتهایی نگهداری کند. UDP هیچ کدام از این کارها را انجام نمی‌دهد
- وقتی که برنامه روی UDP اجرا می‌شود سرور می‌تواند همزمان تعداد بیشتری کلاینت فعال و ساپورت کند

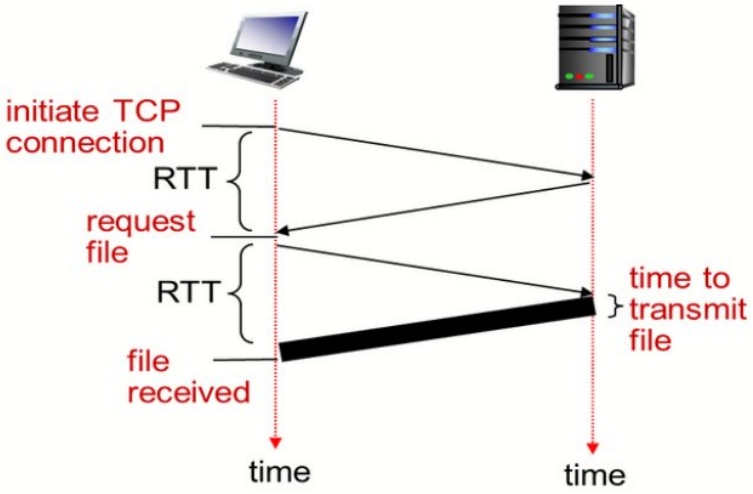
سربار پروتکل UDP از TCP کمتر است

- هر سگمنت TCP دارای سرآیند ۲۰ بایتی و هر سگمنت UDP دارای سرآیند ۸ بایتی است

Scanned with CamScanner

سوال: اگر بخواهید یک انتقال از مشتری به سرور را با حداکثر سرعت ممکن انجام دهید از UDP استفاده می‌کنید یا TCP و چرا؟

پاسخ : از UDP استفاده می‌کنیم چون با استفاده از UDP انتقال می‌تواند در یک RTT کامل شود، در UDP مشتری درخواست انتقال و به سوکت UDP سرور ارسال می‌کند و سرور پاسخ را به سوکت UDP میزبان بر می‌گرداند. درحالی که با استفاده از TCP حداقل دو RTT نیاز است، یکی برای برقراری اتصال TCP و یکی برای مشتری تا درخواستش را ارسال کند و برای سرور تا پاسخ را برگرداند



ویژگی‌های برخی از برنامه‌های شبکه

با توجه به ویژگی های هر یک از این برنامه ها متوجه می‌شویم که برای هر یک از اینها بهتر هست که در لایه انتقال TCP استفاده شود یا UDP

Application	Data Loss	Throughput	Time-Sensitive
File transfer/download	No loss	Elastic	No
E-mail	No loss	Elastic	No
Web documents	No loss	Elastic (few kbps)	No
Internet telephony/ Video conferencing	Loss-tolerant	Audio: few kbps–1Mbps Video: 10 kbps–5 Mbps	Yes: 100s of msec
Streaming stored audio/video	Loss-tolerant	Same as above	Yes: few seconds
Interactive games	Loss-tolerant	Few kbps–10 kbps	Yes: 100s of msec
Instant messaging	No loss	Elastic	Yes and no

Scanned with CamScanner

پروتکل‌های لایه کاربرد و انتقال بکار رفته در برخی از برنامه‌های شبکه

پروتکل RIP برای به هنگام سازی جدول‌های فروادینگ روترها از UDP استفاده می‌کند، چون به هنگام سازی این جداول به دفعات زیاد و هر ۵ دقیقه یکبار ارسال می‌شود اگر یکی از این بسته‌ها گم بشود چون چند دقیه بعد بسته جدید به هنگام سازی می‌رسد تلاش برای ارسال یک بسته به هنگام سازی که زمان آن گذشته تلاش بی ثمری است

Application	Application-Layer Protocol	Underlying Transport Protocol
Electronic mail	SMTP	TCP
Remote terminal access	Telnet	TCP
Web	HTTP	TCP
File transfer	FTP	TCP
Remote file server	NFS	Typically UDP
Streaming multimedia	typically proprietary	UDP or TCP
Internet telephony	typically proprietary	UDP or TCP
Network management	SNMP	Typically UDP
Routing protocol	RIP	Typically UDP
Name translation	DNS	Typically UDP

پروتکل‌های لایه کاربرد و انتقال بکار رفته در برخی از برنامه‌های شبکه

SNMP (Simple Network Management Protocol) (پروتکل مدیریت شبکه) : برنامه های مدیریت شبکه معمولا در شرایطی که شبکه دچار ازدحام شده است و انتقال مطمئن داده کار سختی است اجرا می شوند، بنابراین استفاده از UDP به استفاده از TCP در این شرایط ارجحیت دارد.

DNS: برای اجتناب از تاخیری که فاز اتصال اولیه به ما تحمیل می کند از UDP استفاده می کند

برنامه های کاربردی چند رسانه ای که شامل تلفن اینترنتی، ویدیو کنفرانسینگ و استریمینگ هستند

- تلفات بسته ها را تحمل می کنند
- رابطه خوبی با ساز و کار کنترل ازدحام ندارند
- بنابراین این برنامه ها تمایل دارند از UDP استفاده کنند اما چون بعضی از شرکت ها ترافیک UDP را با استفاده از Firewall ها مسدود می‌کنند استفاده از TCP بعنوان پروتکل انتقال برای برنامه های چند رسانه ای در حال افزایش است

نکته: برخی از برنامه‌های تلفن اینترنتی (مثل اسکایپ) ابتدا سعی می‌کنند که از طریق UDP ارتباط برقرار کنند ولی اگر نشد به عنوان روش پشتیبان از TCP استفاده می‌کنند

نکته: وجه اشتراک پروتکل‌هایی که از TCP استفاده می‌کنند این است که در برنامه‌های کاربردی آنها انتقال فایل داریم معمولا یا اینکه می‌خواهیم از دور چیزی را کنترل کنیم و وجه اشتراک پروتکل هایی که از UDP استفاده می‌کنند این است که برنامه های کابردی آنها یا نسبت به loss حساس نیستند و یا کارهای پریودیک انجام می‌دهند و یا میخواهند سریع باشند و یا میخواهند کارشان سبک باشد

سوال: UDP برای چه کاربردی مناسب است؟

۱) SMTP ۲) Telnet ۳) HTTP ۴) FTP ۵) VOIP

Scanned with CamScanner

UDP و TCP از کدامیک از چهار گروه سرویسی که لایه انتقال می‌تواند ارائه کند استفاده می‌کند

	انتقال داده قابل اطمینان	تضمین گذردهی	همزمانی: تضمین تحویل داده‌ها در بازه زمانی مشخص(تضمین تاخیر و جیتر)	تضمین امنیت
TCP	دارد	ندارد	ندارد	ندارد
UDP	ندارد	ندارد	ندارد	ندارد

- ایجاد امنیت در TCP
  - داده‌ها در TCP و UDP بدون هیچ رمزنگاری به لایه پایین‌تر داده می‌شود
  - SSL در لایه کاربرد پیاده‌سازی می‌شود و سرویس امنیت را برای TCP به ارمغان می‌آورد
  - SSL برای کانکشن‌های TCP، رمزنگاری، صحت داده و end-point authentication را مهیا می‌کند
  - اگر برنامه‌ای بخواهد از سرویس‌های SSL استفاده کند باید کدهای SSL را به برنامه‌های سمت مشتری و سرویس دهنده ضمیمه کند
  - UDP نه خودش امنیت دارد و نه SSL را می‌شناسد

دسته‌بندی(انواع ویژگی‌های) پروتکل‌های لایه کاربرد

- **پروتکل‌های لایه کاربرد را می‌توان به دسته‌های زیر تقسیم کرد**

1. بدون حالت (Stateless) یا Stateful (با نگهداری حالت، با حالت، حالت مند)
2. پایدار(Persistent) یا گذرا (non-persistent)
3. In_band یا out_of_band
4. Push protocol یا pull protocol
5. نوع پیام‌ها

Stateless or Stateful protocol

Stateless: سرور هیچ اطلاعاتی از وضعیت مشتریان نگهداری نمی‌کند

Stateful: سرور اطلاعات وضعیت مشتری‌ها را نگه داری می‌کند بنابراین در ارجاعات بعدی یوزرها آنها را می‌شناسد و سابقه آنها را دارد

- پروتکل‌هایی که حالت را نگه می‌دارند پیچیده هستند زیرا
  - حالت‌های قبلی (پیشینه گذشته) باید نگهداری شود
  - اگر سرور یا کلاینت کرش کند دید و تفکر آنها بعد از کرش در مورد حالت سیستم ناسازگار خواهد بود با آنچه که در قبل بوده و بنابراین باید عملیات تطبیق انجام شود

Scanned with CamScanner

دسته‌بندی‌های پروتکل‌های لایه کاربرد(ادامه)

پایدار، ماندگار، مانا، مداوم(Persistent) یا گذرا، غیر ماندگار(non-persistent)

Non-Persistent and Persistent Connections

یک پروتکل لایه کاربرد برای ارسال و دریافت پیام‌هایش می‌تواند از اتصال‌های TCP پایا یا گذرا استفاده کند

non-persistent : اگر برنامه برای مبادله هر زوج درخواست و پاسخ از یک اتصال TCP جداگانه استفاده کند گوییم برنامه از اتصال گذرا استفاده کرده است، پس از هر زوج درخواست TCP قطع میشود

Persistent : اگر برنامه برای مبادله تمامی درخواست‌ها و پاسخ‌ها فقط از یک اتصال استفاده کند گوییم برنامه از اتصال پایدار استفاده کرده است، TCP ماندگار است

نکته: استفاده از اتصال گذرا سربار بیشتری را تحمیل می‌کند چون به ازای هر درخواست باید یک کانکشن TCP برقرار کنیم و پس از پاسخ به آن درخواست باید آن کانکشن TCP را ببندیم

In_band یا out_of_band

In_band : اگر در پروتکلی پیام‌های کنترلی و داده‌ها از طریق یک کانکشن مبادله شوند، گویند مبادله اطلاعات کنترلی در آن پروتکل in_band هست

out_of_band : اگر سیگناهای کنترلی و داده ها طریق اتصال‌های جداگانه‌ای رد و بدل شوند می‌گوییم مبادله اطلاعات کنترلی در آن پروتکل out_of_band است

نکته: فلش دو طرفه در شکل‌های بالا نشان می‌دهد که ارتباط full duplex است.

Push protocol یا pull protocol

Pull protocol : ماشین گیرنده پیام (فایل) یک اتصال(TCP) به ماشین سرویس دهنده ایجاد می‌کند

Push protocol : ماشین فرستنده پیام(فایل) یک اتصال(TCP) به ماشین گیرنده ایجاد می‌کند

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

DNS (Domain Name System)

جایگاهی بسته ها در اینترنت بر اساس شماره IP ابدا و مقصد انجام می‌شود و قبلا صحبت کردیم که چرا به آدرس IP نیاز داریم، اما انسان ها خیلی برایشان راحت‌تر است که وقتی می‌خواهیم با یک جایی ارتباط برقرار کنیم نام اش را به خاطر بسپاریم به‌جای یک شماره آی پی ۴ بایتی.

سوال - چرا از همین نام ها برای ادرس دهی بسته ها در شبکه استفاده نکنیم؟

به ۲ علت:

۱- اینکه ما نام یک هاست را بدانیم، این نام هیچ اطلاعاتی در مورد اینکه مکان این هاست در کجا قرار دارد به ما نمی دهد

توجه) البته از روی نام هایی که به کد کشورها ختم می‌شوند شاید بتوان حدس زد که سرور در چه کشوری است.

۲- روترها با پردازش نام هاست ها مشکل دارند چون طول نام ها می‌تواند متغیر باشد

در عوض آدرس های IP
- هم routable هستند و هم ساختار سلسله مراتبی دارند
- و هم طول ثابت دارند که برای روترها مناسب است

نتیجه: بنابراین ما انسان ها دوست داریم از نام ها استفاده کنیم، همچنین دوست داریم در شبکه از IP استفاده کنیم ⇐ پس آمدند برای شماره های IP نام های قابل فهمی در نظر گرفتند پس نیاز به سرویسی داریم که بتواند نام میزبان ها را به آدرس IP تبدیل کند

نکته) سلسله مراتبی بودن آدرس IP به اینصورت است که هرچه از سمت چپ به راست برویم در آدرس IP اطلاعات دقیق تری از مکان هاست مورد نظر بدست می آوریم

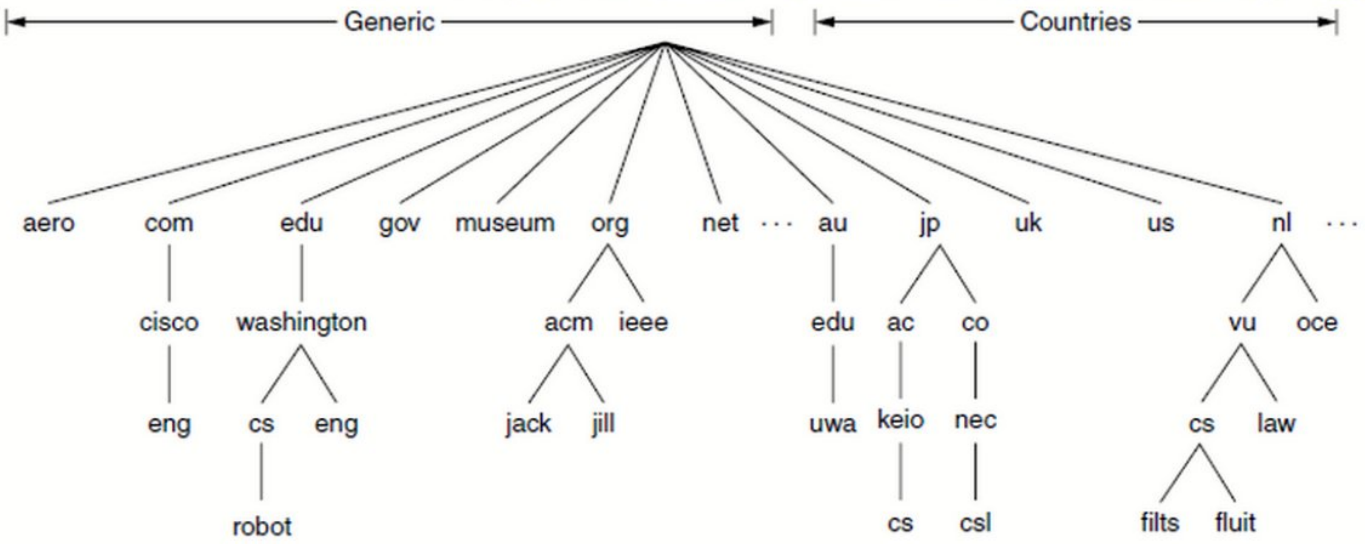
نکته: به این عمل که کسی نام را بدهد و آدرس IP بخواهد می‌گویند Resolve کردن. در اصطلاح می‌گوییم DNS، lookup می‌شود یا DNS، Resolve می‌شود

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

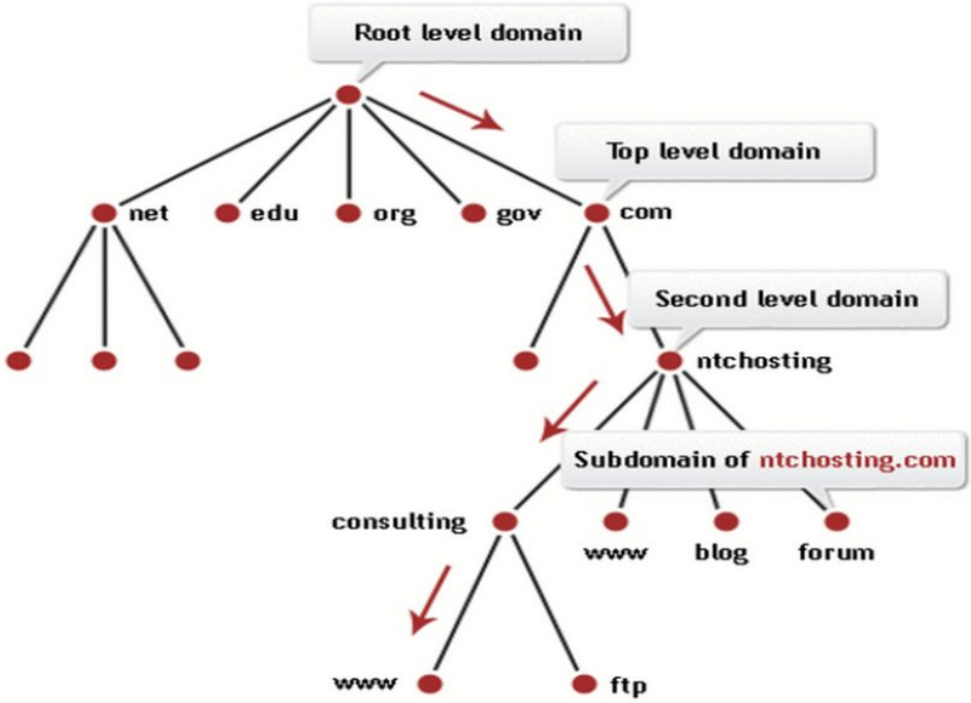
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

- برای راه اندازی سیستمی که یوزرها به آن سیستم نام ها را بدهند و آدرس IP آن نام ها را بگیرند ابتدا نیاز شد تا یک ساختار درختی برای نام ها (دادن نام ها) ایجاد شود. ساختار درختی یعنی یک نام یکسری قسمت هایی دارد که می توان با مشاهده این قسمت ها به یکسری از ویژگی ها پی برد

* یکی از مزایا تعریف نام ها بصورت درختی و سلسله مراتبی این است که تعریف نام ها مانند در هر زیرشاخه ای به نهادهای زیر مجموعه آن شاخه مربط می شود. برای این منظور در هر لول مدیری برای آن لول تعریف می شود، این ساختار درختی بصورت زیر است



A portion of the Internet domain name space

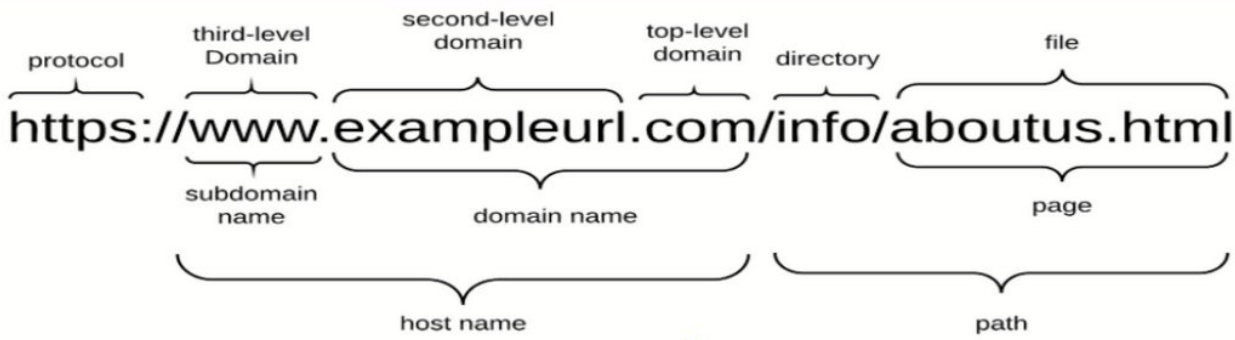


سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

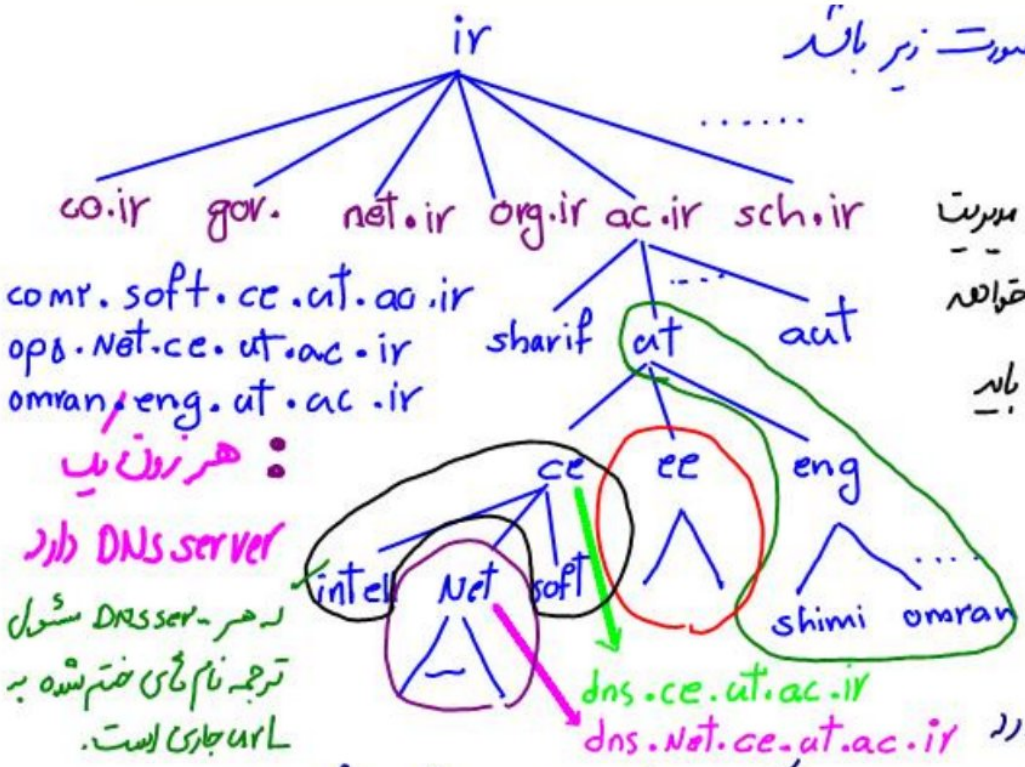
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

رامین رضوی



- نام های تیر ir می‌تواند بصورت زیر باشد



هر زون یک DNS server دارد

که هر DNS server مسئول ترجمه نام های ختم شده به URL جاری است.

تا الان ما کلیا فقط نیروی نام دادیم با مدیریت توزیع شده، حالا وقتی کلیا یوزری خواهد به یک اسمی داده بفرستد چگونه باید آدرس آی پی آن را پیدا کند؟

برای این منظور باید یک دیتا بیسی داشته باشیم که نام و آدرس ها مربوط به آن را نگه دارد

حال سوال پیش می‌آید که آیا این دیتا بیس مرکزی باشد یا توزیع شده باشد؟

مشکلات پایگاه داده مرکزی

۱- single point of failure: اگر این دیتا بیس از کار بیفتد کل اینترنت دیگر کار نمی‌کند

۲- این سرور overload خواهد شد = حجم ترافیک بسیار بالایی به سمت این سرور می‌آید که در نتیجه این سرور را غیر قابل استفاده خواهد کرد

۳- اکثر یوزرها فاصله زیادی با این Data base خواهد داشت ← باعث ایجاد RTT بالا می‌شود

۴- تعمیر و نگهداری چنین Data base ای در عمل غیر ممکن است

راه حل: ایجاد یک پایگاه داده توزیع شده و سلسله مراتبی

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

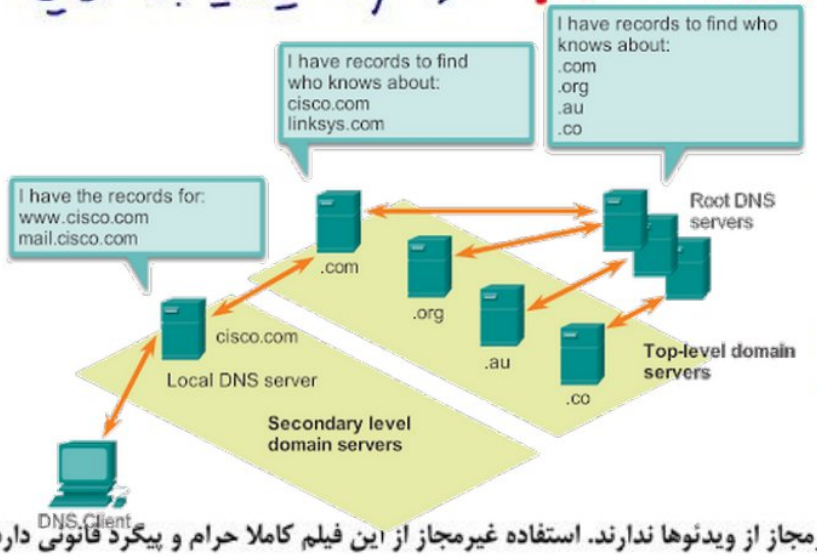
- سرورهای DNS بصورت سلسله مراتبی در دنیا توزیع شده اند، این سرورهای DNS را می‌توان حدوداً به ۴ دسته تقسیم کرد. توجه کنید که هیچ سرور DNS ای به تنهایی اطلاعات نگاشت آدرس به IP تمامی هاست های روی اینترنت ندارد

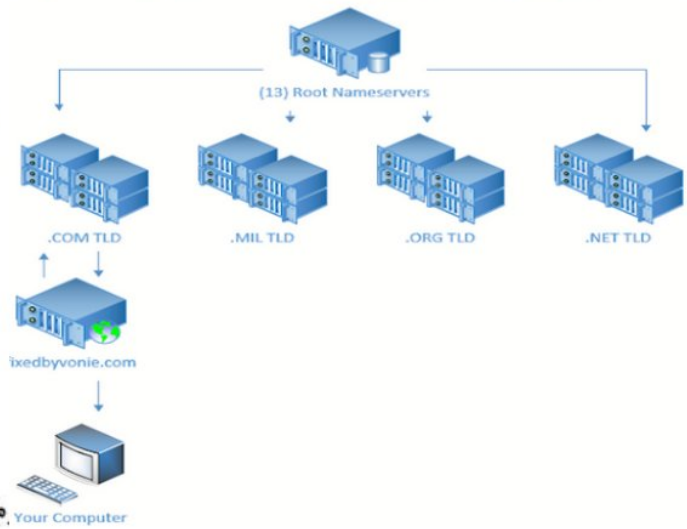
۱- Root DNS servers : در دنیا ۱۳ عدد از این سرورها وجود دارد که از A تا M نام گذاری شده اند. اکثر این سرورها در آمریکا قرار دارند. هریک از این سرورها برای ایجاد امنیت reliability، شکلی متشکل از چندین سرور است. بنابراین تعداد واقعی این سرورها بیش از ۳۰۰ عدد است. RDS ها آدرس سرورهای TLD را دارند

۲- Top level Domain(TLD) servers : این سرورها مسئول دامنه‌های سطح بالا موضوعی مانند com، edu، net و... و همچنین مسئول دامنه‌های سطح بالا کشوری مانند ir، uk و... هستند. TLD server ها آدرس سرورهای سرپرستی را دارند

۳- Authoritative DNSservers: هر شرکتی (هرکس) که بخواهد هاست های خود را مثلاً سایت خود را (سرویس دهنده وب) روی اینترنت قرار بدهد باید دسترسی به رکوردهای DNS اش را در دسترس عموم قرار بدهد. سرور DNS سرپرستی سروری است که این رکوردها را در خود نگه میدارد، حال شرکت ها یا باید سرور سرپرستی اختصاصی برای خودشان راه اندازی کنند و یا باید این کار را به یک سرور سرپرستی عمومی محول کنند. این سرورها آدرس سرورهای محلی را دارند

۴- Defual name server= local DNS server : هر Isp یک یا چندتا از این





مجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

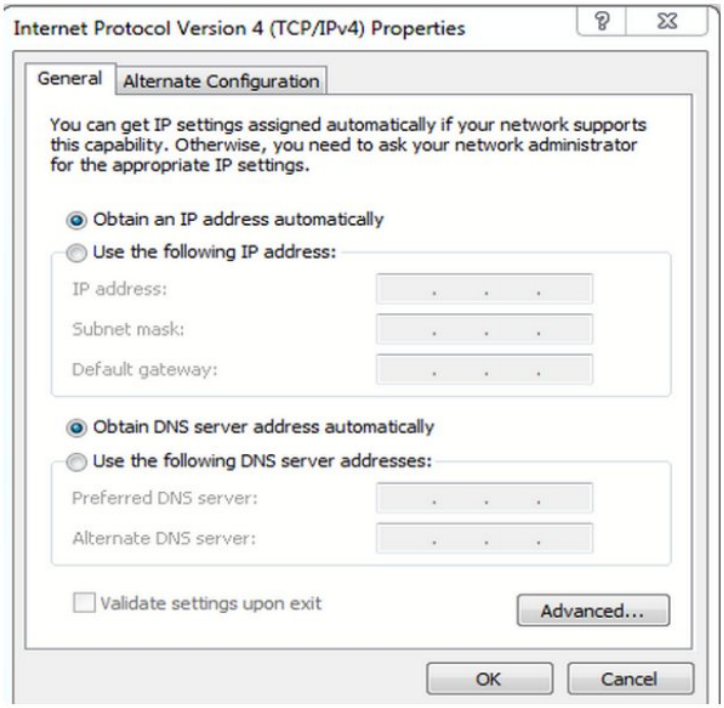
Scanned with CamScanner

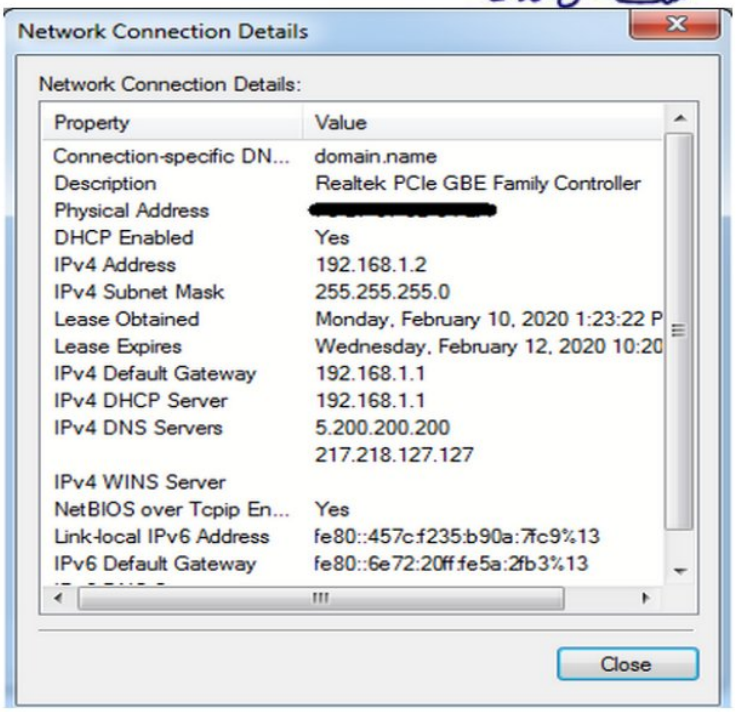
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

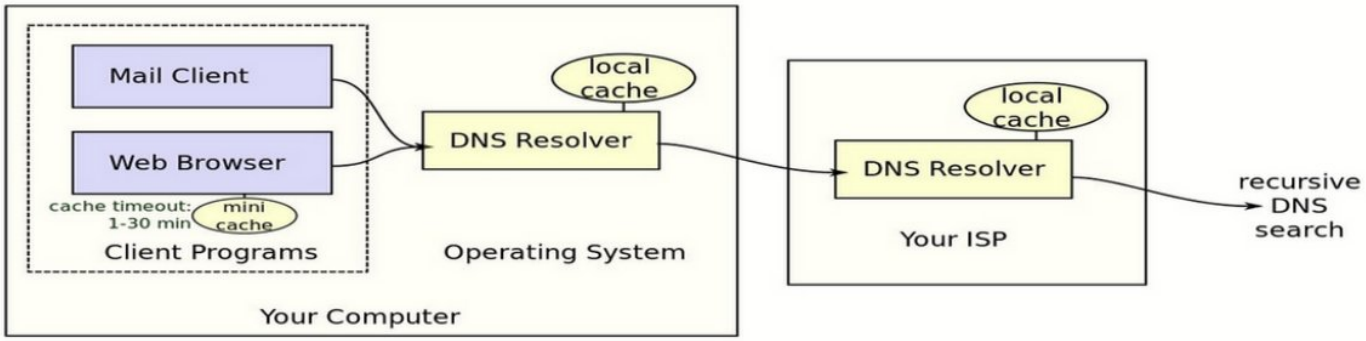
شبکه های کامپیوتری

رامین رضوی

هنگامی که یک برنامه کاربردی یک پرس وجوی DNS را درخواست می‌کند، ابتدا کنش کامپیوتر میزبان جستجو می‌شود و اگر نگاشت آدرس به آی پی وجود داشته باشد که نتیجه به App داده می‌شود ولی اگر این نگاشت درکش نباشد این پرس وجود DNS (DNS query) به local DNS server داده می‌شود، بنابراین جزء الزامات اولیه فرآیند تبدیل نام به آدرس این است که برای هر کامپیوتر متصل به اینترنت مشخص شده باشد که آگر آدرس Ip یک نام را بلد نیست باید local DNS server را در چه آدرسی پیدا کند. این آدرس را می‌توانید در پنجره وضعیت کارت شبکه خود مشاهده کنید. وقتی به یک Isp وصل می‌شوید Isp از طریق DHCP آدرس Ip یکی از local DNS server های خودش را اتوماتیک برای ما ست می‌کند.







Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

حال وقتی پرس وجو DNS به دست local DNS server می‌رسد، این سرور کش خودش را نگاه می‌کند و اگر نگاشت مورد نظر را داشت آن را به یوزر ارسال می‌کند، در غیر اینصورت از این جا به بعد ۲ روش وجود دارد. قبل از اینکه این ۲ روش را توضیح بدهیم نیاز است تا با انواع پرس وجوی DNS آشنا شوید

یک پرس وجوی DNS می‌تواند به ۲ صورت باشد (ارسال درخواست‌های DNS دو مدل دارد)

۱- recursive query : وقتی یک درخواست DNS به یک سرور می‌دهیم و از آن می‌خواهیم تا به نیابت از ما نگاشت نام به آدرس را برای ما پیدا کند

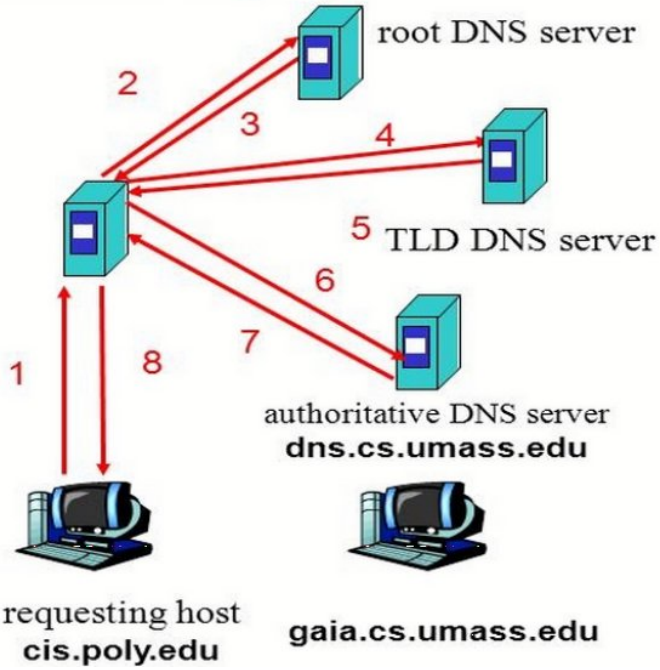
۲- Iterative query : وقتی خود یک سرور بدست آوردن نگاشت نام به آدرس را برعهده می‌گیرد و خود یک سرور DNS query های لازم را به سطوح مختلف سرورهای DNS ارسال می‌کند

الگوریتم های (روش‌های) جستجو DNS :

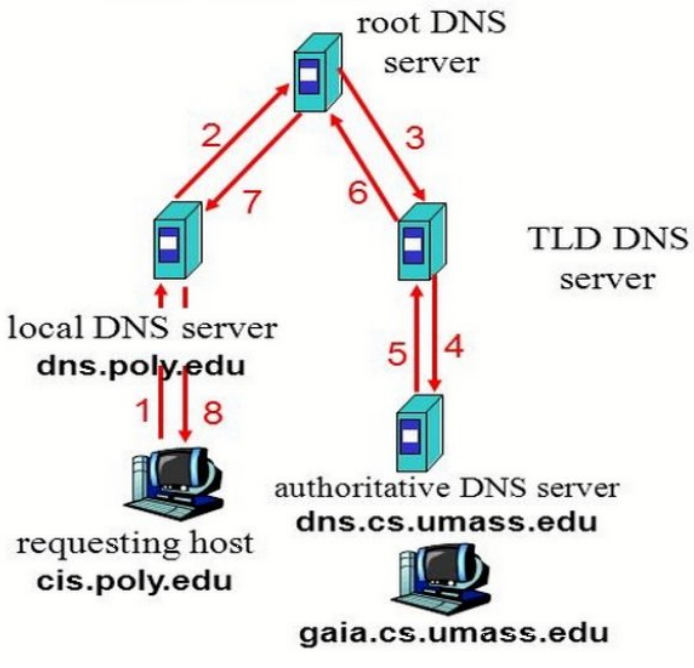
در هر ۲ روش زیر query اول که client به سمت local DNS server ارسال می‌کند از نوع بازگشتی است.

DNS name resolution

iterative query



recursive query



Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

رامین رضوی

محاسبه تاخیر DNS در روش بازگشتی (شکل سمت راست)

$delay_{DNS} = RTT_1 + RTT_2 + RTT_3 + RTT_4$

محاسبه تاخیر DNS در روش تکراری (شکل سمت چپ)

$Delay_{DNS} = RTT_1 + RTT_2 + RTT_3' + RTT_4'$

نکته: روش بازگشتی از روش تکراری سریعتر است و در عمل از روش بازگشتی استفاده می‌شود

m.Tokyo root server

در این شکل اگر از روش تکراری به جای آدرس IP باشیم چند بار از اقیانوس عبور خواهیم کرد.

آمریکا و اروپا

اقیانوس هند

LDS

حافظه نهان در DNS

هر سرور DNS نگاشت ها را به اندازه یک زمان مشخص (TTL) برای خودش کش می‌کند پس از این زمان نگاشت مد نظر معتبر نیست و دور ریخته می‌شود

استرالیا (سیدنی)

نکته) چون مراجعه به سرورهای TDL از طرف کاربران زیاد است در اکثر اوقات آدرس این سرورها در کش local DNS server ها وجود دارد و بنابراین اکثر پرس وجوهای DNS سراغ سرورهای DNS ریشه نمی‌روند

کامپیوتری که می‌خواهد یک نام به خودش اختصاص بدهد باید چه کند

این کامپیوتر باید IP آدرس و نام خودش را به DNS ای که به آن وصل هست بدهد و آن DNS هم باید یک entry جدید در لیست mapping نام به IP ها پیش اضافه کند

نکته) اگر در زمان نگاشت نام به IP در یکی از سرورهای DNS، یک هاست به یکباره IP خودش را عوض کند دیگر دسترسی به آن میزبان میسر نخواهد بود تا زمانیکه تمامی TTL ها منقضی بشوند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

نکته) سیستم DNS از دو بخش تشکیل شده است .
۱ـ پایگاه داده توزیع شده و سلسله مراتبی
۲ـ یک پروتکل لایه کاربرد که با استفاده از این پروتکل میزبان ها و سرورهای DNS باهم صحبت می‌کنند

نکته) پروتکل DNS روی UDP اجرا می‌شود و از پورت ۵۳ استفاده می‌کند

نکته) پروتکل های HTTP ، FTP و SMTP برای تبدیل نام مقصدهایشان به آدرس IP از پروتکل DNS استفاده می‌کنند

نکته) DNS یک تاصیر اولیه به برنامه هایی که از آن استفاده می‌کند اضافه می‌کند

نکته) درست است که DNS یکی از پروتکل های لایه کاربرد است چون هم اولاً با مدل client_server بین دو Host ارتباط برقرار می‌کند ، دوماً برای ارسال پیام های DNS بین هاست ها از پروتکل UDP لایه انتقال ان که در زیرش است استفاده می‌کند ولی برخلاف برنامه هایی همچون وب و ایمیل و ... کاربر هرگز با DNS ارتباط مستقیم ندارد و برنامه های کاربری دیگرهستند که از DNS استفاده می‌کنند

مثال) به محض اینکه شما در مرورگرتان یک URL وارد کنید ، مرورگر Host name را از URL استخراج می‌کند و آن را به برنامه DNS (برنامه سمت client) می‌دهد ، البته خود مرورگر هم کش دارد و اگر در کش اش نباشد Host name را به DNS client می‌دهد ، حال اگر در کش DNS client هم نگاشت وجود نداشته باشد ، DNS client یک query برای local DNS server ارسال می‌کند ، پس پس از آن که LDS نگاشت را پیدا کرد ، IP مورد نظر را به DNS client میدهد ، DNS client نیز این IP را به مرورگر میدهد ، حال مرورگر یک اتصال Tcp به پورت ۸۰ سرور HTTP ان که در آن آدرس IP قرار دارد ایجاد می‌کند .

نکته) DNS سرویس های دیگری نظیر ۱ـ Host aliasing ۲ـ Mail server aliasing ۳ـ Load distribution

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

نکته: یک اتصال Tcp می‌تواند ماندگار (persistent) یا Non persistent باشد. اگر یک برنامه برای مبادله هر تعداد درخواست و پاسخ از یک اتصال Tcp جداگانه استفاده کند و پس از دریافت هر پاسخ Tcp را قطع کند می‌گوییم که برنامه از اتصال گذرا استفاده کرده و اگر برنامه برای مبادله تمامی تعداد ها درخواست، پاسخ از یک اتصال Tcp استفاده کند می‌گوییم که برنامه از اتصال Tcp ماندگار استفاده کرده

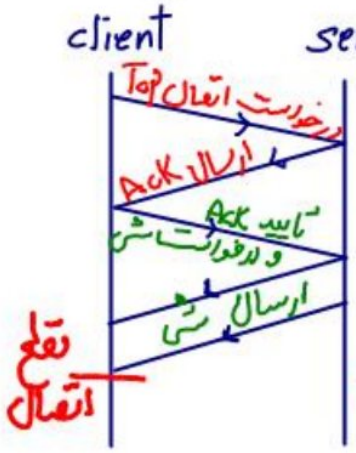
حال گفتیم وقتی کاربر روی یک لینک کلیک می‌کند و صفحه‌ای را می‌خواهد مرورگر باید برای هر یک از اشیا درون صفحه یک پیام درخواست HTTP جداگانه به سمت سرور ارسال کند، حال این درخواست ها می‌توانند **بصورت سری یا موازی به سمت سرور ارسال شود**، سری به این صورت است که تا جواب یک درخواست HTTP دریافت نشده است درخواست HTTP دیگری به سمت سرور ارسال نمی‌کند کلاینت و موازی به اینصورت است که کلاینت درخواست های HTTP موازی را به سمت سرور ارسال می‌کند

نکته ۱- گذرا یا ماندگار بودن اتصال های Tcp مستقل از ارسال درخواست های HTTP بصورت سری یا موازی است

نکته ۲- در HTTP ای که از اتصالات گذرا استفاده می‌کند روال ارسال هر درخواست HTTP بصورت زیر است

ایجاد اتصال Tcp ← ارسال درخواست HTTP ← دریافت پاسخ HTTP (دریافت شی) ← قطع اتصال

برای ایجاد سرعت این دو باهم ادغام می‌شود



* پس در HTTP با استفاده از اتصال گذرا برای هر object باید connection را باز کنیم و سپس ببندیم.

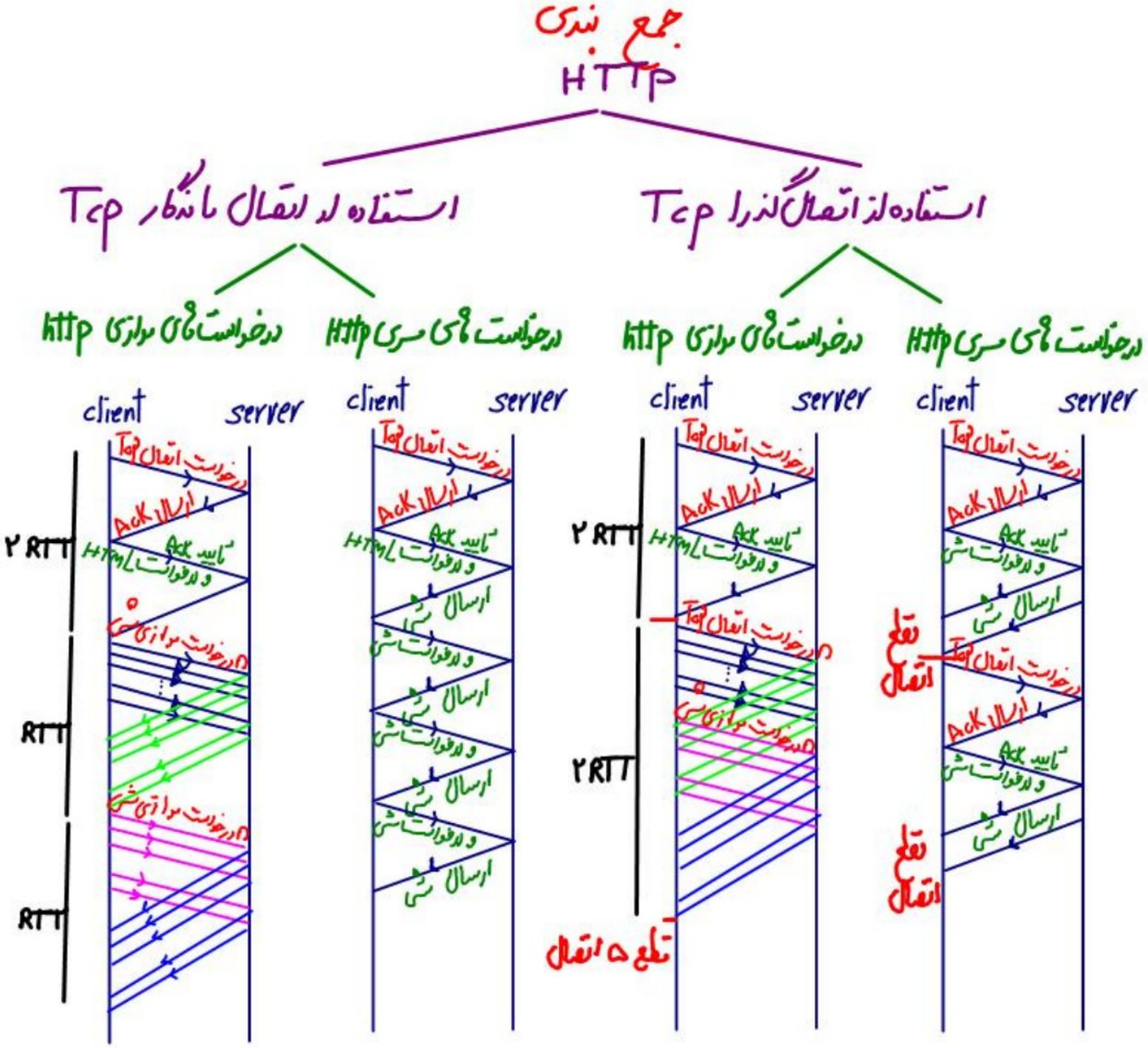
هر شی ← یک درخواست http ← هر درخواست http روی یک اتصال Tcp

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

جمع بندی HTTP



نکته ۱: HTTP بصورت پیش فرض از اتصال پایا Tcp و درخواست های موازی http استفاده می‌کند و اگر در مورد درجه موازی سازی صحبتی نشد، درجه را بصورت پیش فرض بی نهایت بگیرید

نکته ۲: در HTTP ۱ که از اتصال گذرا Tcp استفاده می‌کند اگر در مورد سری یا موازی بودن درخواست های http صحبتی نشد بصورت پیش فرض سری در نظر بگیرید

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Non-persistent HTTP

- مراحل انتقال یک صفحه وب از سرویس دهنده وب به مشتری وب
- فرض کنید این صفحه از یک فایل HTML پایه و ۱۰ تصویر JPEG انجام شده است
- فرض کنید URL فایل HTML پایه بصورت زیر است:

`www.someSchool.edu/someDepartment/home.index`

1a. HTTP client initiates TCP connection to HTTP server (process) at www.someSchool.edu on port 80

1b. HTTP server at host www.someSchool.edu waiting for TCP connection at port 80. "accepts" connection, notifying client

2. HTTP client sends HTTP *request message* (containing URL) into TCP connection socket. Message indicates that client wants object someDepartment/home.index

3. HTTP server receives request message, forms *response message* containing requested object(/someDepartment/home.index), and sends message into its socket

time

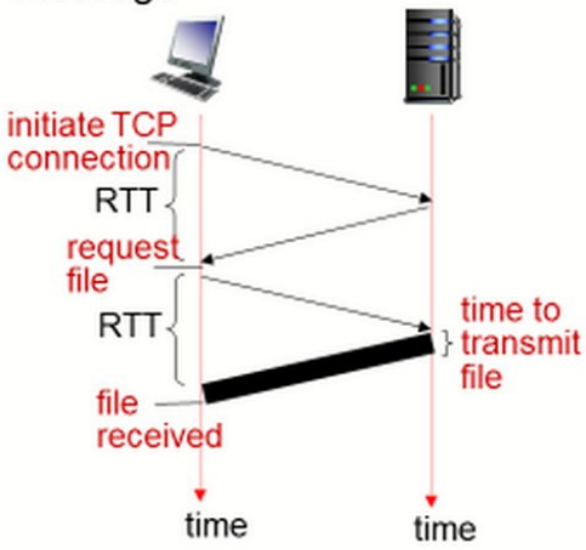
Non-persistent HTTP (cont.)

4. HTTP server closes TCP connection. But TCP doesn't actually terminate the connection until it knows for sure that the client has received the response message

5. HTTP client receives response message and terminate TCP connection. response message containing html file, displays html. Parsing html file, finds 10 referenced jpeg objects

6. Steps 1-5 repeated for each of 10 jpeg objects

time



- برای انتقال این صفحه ۱۱ اتصال TCP ایجاد کردیم

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

نکته ۳: می دانیم که به ازای هر اتصال Tcp در هر دو سمت مشتری و سرور سربار داریم از یرا هر اتصال Tcp به بافرها و متغیرهای خاص خود نیاز دارد، بنابراین چون HTTP ای که از اتصال Tcp گذرا استفاده می‌کند برای درخواست هر شیء یک اتصال Tcp باز می‌کند، ما برای هر شیء این سربارها را داریم.

نکته ۴: یک سرور در هر لحظه به هزاران مشتری سرویس می‌دهد، حال اگر این مشتری ها از http با اتصال Tcp گذرا استفاده کنند، چون معمولا مرورگرها برای دریافت اشیا درخواست های زیادی را بصورت موازی ارسال می‌کنند بنابراین سربار بسیار زیادی به سرور تحمیل می‌شود

نکته ۵ - به جای واژه موازی واژه خط لوله نیز استفاده می‌شود

نکته ۶ - وقتی http از اتصال پایدار Tcp استفاده می‌کند و یک صفحه را دریافت می‌کند، حال می‌تواند از همین اتصال Tcp برای دریافت صفحات دیگر همان وب سایت روی همان سرور نیز استفاده کند

نکته ۷ - در حالتی که از اتصال پایدار استفاده می‌کنیم، سرور تا کلاینت درخواستی نداشته باشد اتصال را قطع نمی‌کند و فقط زمانی این اتصال Tcp را می‌بندد که کلاینت برای مدتی هیچ درخواستی نداره باشد، این زمان روی سرور قابل پیکربندی است، بنابراین در این حالت یک کلاینت مجبور نیست که بصورت مداوم درخواست شیء داشته باشد و یک کلاینت به محض اینکه با یک یا چند درخواست شیء مواجه بشود، درخواست ها را ارسال می‌کند و تایم برقراری اتصال اولیه را ندارند.

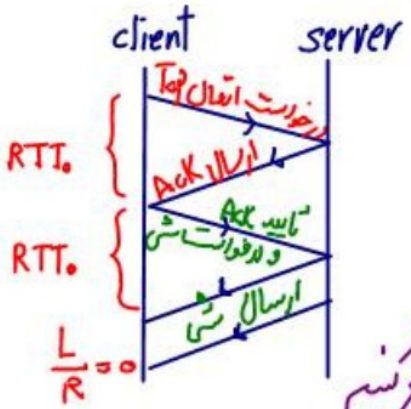
تست ۱ - فرض کنید در مرورگر وب خود روی یک لینک برای رفتن یک صفحه جدید کلیک کرده اید همچنین فرض کنید که آدرس IP مرتبط با URL سایت مورد نظر شیء روی میزبان محلی شما کش نشده است، بنابراین برای یافتن آدرس IP یک جستجو DNS نیاز خواهید داشت. فرض کنید که میزبان شما برای دریافت آدرس IP از DNS، n سرور DNS را ملاقات کرده باشد. این ملاقات های پیاپی هر یک زمان RTT را در پی خواهد داشت. حال فرض کنید که صفحه وب

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

مربوط به این لینک شامل دقیقاً یک شی است که آن شی نیز یک متن بسیار کوچک HTML است.
اگر RTT_0 نشان دهنده زمان رفت و برگشت بین میزبان محلی و سروری باشد که شی ما روی آن است مطلوبست محاسبه زمان دریافت این صفحه وب در صورتی که زمان انتقال شی صفر باشد؟

پاسخ: در سوال به این اشاره نشده که از DNS بازگشتی استفاده کرده است یا از DNS تکراری ولی با توجه به اینکه گفته میزبان برای یافتن آدرس IP ، n سرور DNS را ملاقات می‌کند می‌فهمیم که روش تکراری مد نظرش است. بنابراین برای یافتن آدرس IP زمان $\sum_{i=1}^{n} RTT_i$ نیاز است



$$\text{زمان کل} = \sum_{i=1}^{n} RTT_i + 2RTT_0$$

نکته ۱: چون صفحه ما فقط شامل یک شی است فرقی نمی‌کند که انتقال گذرا است یا ماندگار

نکته ۲: DNS هر مدلی که باشد باید RTT هایی که برای DNS میدهند را جمع کنیم (مگر اینکه سوال خاصی مطرح کنند)

نکته ۳: دقت کنید که ما فقط RTT_0 را در ۲ ضرب می‌کنیم و RTT_1 تا RTT_n را در ۲ ضرب نمی‌کنیم زیرا درخواست های DNS از پروتکل UDP استفاده می‌کنند و UDP فاز برقراری اولیه انتقال را ندارد و بنابراین هر درخواست DNS به یک RTT نیاز دارد

تست ۲) اگر در تست قبل فایل HTML به ۸ شی بسیار کوچک روی همان سرور ارجاع بدهد با فرض اینکه پروتکل HTTP از انتقال گذرا استفاده کند و درخواست های HTTP بصورت سری باشند، زمان دریافت صفحه را محاسبه کنید؟

پاسخ:

$$\sum_{i=1}^{n} RTT_i + 9 \times 2 \times RTT_0$$

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

رامین رضوی

تست ۳ ـ اگر در تست ۲ طول فایل HTML برابر L_0 بایت و طول L_1 تا L_8 بایت باشد و تاخیر بین کلاینت و سرور برابر R باشد زمان دریافت صفحه وب چقدر می‌شود

$$\sum_{i=1}^{n} RTT_i + 9 \times 2 \times RTT_0 + \sum_{i=0}^{8} \frac{L_i \times 8}{R}$$

تست ۴ : تست دو را با فرض اینکه HTTP از اتصال گذرا استفاده کند و مرورگر برای ارسال موازی ۵ درخواست HTTP پیکربندی شده باشد، سوال را حل کنید

$$\sum_{i=1}^{n} RTT_i + 6RTT_0$$

$6RTT_0$ = ۲ تا از این برای دریافت فایل HTML پایه است، ۲ " " " " ۵ شی اول بصورت موازی است و دوتا " " " " ۳ " دیگر " " "

تست ۵: اگر در تست قبل درجه توازن ۴ باشد جواب — چه می‌شود؟ جواب همین می‌شود

" ۶: " " " " " ۳ " " " " چه؟

$$\sum_{i=1}^{n} RTT_i + 8RTT_0$$

تست ۷ ـ اگر در تست ۴ طول فایل HTML برابر L_0 بایت و طول L_1 تا L_8 بایت باشد و تاخیر بین کلاینت و سرور برابر R باشد زمان دریافت صفحه وب چقدر می‌شود

$$\sum_{i=1}^{n} RTT_i + 6RTT_0 + \sum_{i=0}^{8} \frac{L_i \times 8}{R}$$

تست ۹) اگر فایل HTML به ۸ شی بسیار کوچک روی همان سرور ارجاع بدهد و از اتصال ماندگار استفاده شود، زمان لود صفحه وب چقدر می‌شود؟

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

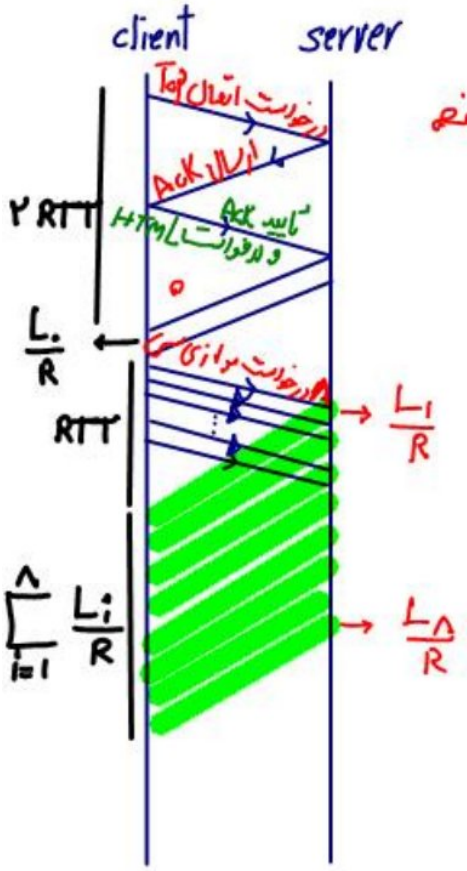
@konkurcomputer
www.konkurcomputer.ir

چون در مورد سری یا موازی بودن صحبتی نکرده بصورت پیش فرض موازی با درجه توازن ∞ در نظر میگیریم

$\sum_{i=1}^{n} RTT_i + 3RTT_0$

$2RTT_0$ برای دریافت فایل HTML و سپس در لحظه کلاینت ۸ درخواست http را بصورت موازی ارسال میکند که در یک RTT دریافت میکند

تست ۱۰ - اگر در تست قبل طول اشیا را در نظر بگیریم چه می شود؟



زمان دریافت صفحه $= \sum_{i=1}^{\infty} RTT_i + 3RTT_0 + \sum_{i=0}^{\infty} \frac{L_i \times 8}{R}$

تست ۱۱: تست ۹ را با فرض آنکه درخواست ها http سری ارسال شود حل کنید

تاخیر کل $= \sum_{i=1}^{\infty} RTT_i + 10RTT_0$

تست ۱۲ - در تست قبل طول اشیا را اگر در نظر بگیریم در انتها نیز $\sum \frac{L_i \times 8}{R}$ خواهیم داشت

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

تست کنکور آی تی ۹۲ سراسری

- فرض کنید شخصی در مرورگر وب خود برای دریافت یک صفحه وب بر روی یک لینک کلیک می‌کند، اگر آدرس IP مربوط به این URL در میزبان بصورت محلی وجود داشته باشد، و فایل HTML مربوط به این لینک دارای ۸ شی باشد درصورتیکه زمان رفت و برگشت بین سرویس دهنده و سرویس گیرنده 100 ms و زمان ارسال اشیا ناچیز باشد با پروتکل Non-persistent HTTP و persistent HTTP از زمانیکه شخص روی لینک کلیک می‌کند تا زمانی‌که صفحه وب را بطور کامل دریافت می‌کند چند میلی ثانیه است؟

۱) ۹۰۰-۱۸۰۰ ۲) ۳۰۰-۹۰۰ ۳) ۳۰۰_۱۸۰۰ ۴) ۱۰۰-۳۰۰

حل : برای Non-persistent HTTP داریم :

$$9 \times 2RTT_0 = 18 \times 100\ ms = 1800\ ms$$

برای persistent HTTP داریم

$$3RTT_0 = 3 \times 100\ ms = 300\ ms$$

تست کنکور آی تی ۹۴ سراسری

- کاربری با استفاده از یک مرورگر وب اقدام به دریافت یک صفحه وب می‌کند. صفحه وب شامل یک فایل HTML و ۹ شی(فایل) است. اندازه هر فایل مساوی و ۵۰۰۰ بایت است. مرورگر وب از (Non-persistent) HTTP 1.0 استفاده می‌کند. وب سرور اجازه حداکثر ۵ ارتباط TCP همزمان به یک کلاینت را می‌دهد. چنانچه گذردهی شبکه بین کاربر و وب سرور 10^6bps باشد، زمان لازم برای دریافت این صفحه بر حسب ثانیه چقدر است؟(زمان رفت و برگشت بین کلاینت و سرور را ۰.۱ ثانیه در نظر بگیرید)

۱) ۱ ۲) ۱.۲ ۳) ۱.۴ ۴) ۱.۵

حل : با $2RTT_0$ بعلاوه $\frac{L}{R}$ مشتری فایل HTML را دریافت می‌کند، سپس از ۹ شی باقیمانده ۵ شی را در $2RTT_0$ دیگر و سپس ۴ شی باقیمانده را در $2RTT_0$ دیگر دریافت می کند

زمان روی خط گذاشتن این ۱۰ شی از طرف سرور هم برابر است با $10 \times \frac{L}{R}$

بنابراین زمان کل لازم برای دریافت این صفحه برابر خواهد بود با:

$$6RTT_0 + 10 \times \frac{L}{R} = 6 \times 0.1\ s + 10 \times \frac{5000 \times 8\ bit}{10^6 bps} = 0.6\ s + 0.4\ s = 1\ s$$

Scanned with CamScanner

تست کنکور آی تی ۹۵ سراسری

- فرض کنید یک برنامه سرویس گیرنده بعد از پیدا کردن آدرس IP کامپیوتر سرویس دهنده می‌خواهد یک صفحه وب که اندازه فایل اصلی آن ۲۰۰ کیلوبیت و اندازه هر یک از ۳ تصویر قرار گرفته در آن ۳۰۰ کیلو بیت است را از طریق پروتکل HTTP غیر مداوم (Non-Persistent HTTP) که مجاز به ایجاد اتصال موازی نیز است دریافت کند. اگر زمان رفت و برگشت(RTT) ۲۰۰ میلی ثانیه، نرخ ارسال هر اتصال ۱۰ مگابیت بر ثانیه و اندازه پیام‌های GET ناچیز باشد، تاخیر دریافت کامل این صفحه وب به میلی ثانیه چقدر است؟

1) ۲۱۲۰
2) ۱۶۵۰
3) ۱۲۵۰
4) ۸۲۰

پاسخ : اندازه فایل HTML پایه را ۲۰۰ کیلو گرفته و گفته ۳ تا شی داریم هر کدام به اندازه ۳۰۰ کیلو بیت

توجه: گفته که نرخ هر اتصال ۱۰ مگابیت هست و نگفته که نرخ خط ۱۰ مگابیت هست. یعنی وقتی ما ۳ تا اتصال موازی برقرار کنیم سه تا ۱۰ مگ یعنی ۳۰ مگ داریم.

ما می‌توانیم یک ۳۰۰ کیلو در نظر بگیریم ولی ۱۰ مگابیت در نظر بگیریم و یا ۳ تا ۳۰۰ کیلو در نظر بگیریم ولی ۳۰ مگ در نظر بگیریم:

$$200ms + 200ms + 200ms + 200ms + \frac{200kbit}{10Mbit} + \frac{300kbit}{10Mbit} = 850\text{ms}$$

تست کنکور آی تی ۹۶ سراسری

- فرض کنید یک صفحه وب شامل یک فایل HTML به اندازه ۱۰ کیلوبایت و ۲ فایل یکی به اندازه ۱۵ و دیگری ۲۰ کیلوبایت. کاربری مایل به مشاهده این صفحه وب است. اگر زمان ایجاد ارتباط بین مرورگر وب و وب سرور 1RTT=7ms و گذردهی این ارتباط 1Mbps باشد، آنگاه زمان دریافت وب چند میلی ثانیه است؟ فرض کنید HTTP در حالت non-persistent و با قابلیت ارتباط موازی کار می‌کند. کیلو را ۱۰۰۰ و مگا را ۱۰۰۰۰۰۰ در نظر بگیرید.

1. ۳۸۸
2. ۳۸۱
3. ۷۳
4. ۶۶

پاسخ: $4 \times 7ms + \frac{45 \times 1000 \times 8bit}{1000000\ bit} = 28 + 360 = 388$

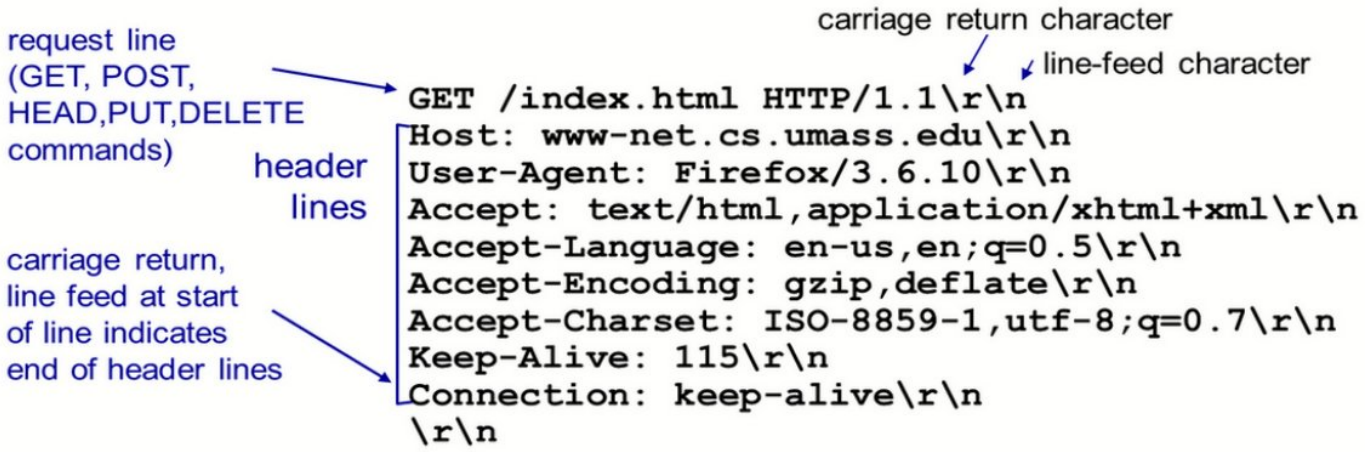
Scanned with CamScanner

فرمت پیام‌های HTTP

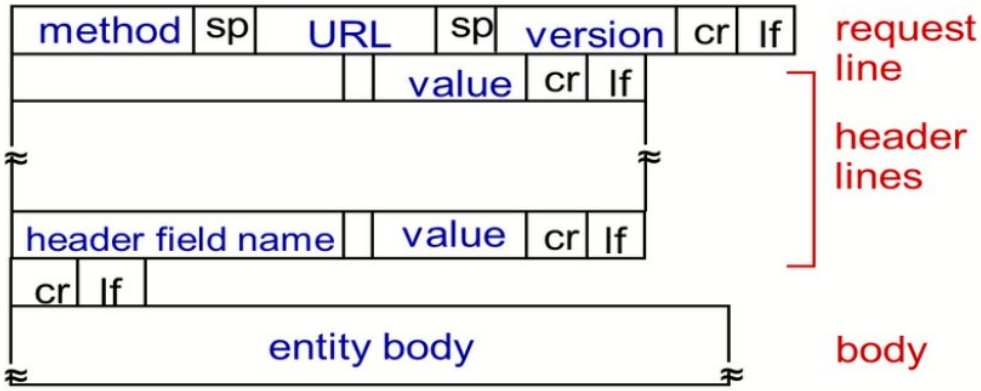
- دو نوع پیام HTTP وجود دارد: ۱) پیام درخواست HTTP ۲) پیام پاسخ HTTP
- پیام‌های درخواست و پاسخ HTTP بصورت کد اسکی ۷ بیتی کد می‌شوند (هر کاراکتر با ۷ بیت کد می‌شود) و قابل خواندن و فهم توسط انسان‌ها است

HTTP request message

- تعداد خطوط پیام درخواست HTTP محدودیتی ندارد، خط اول یعنی request line در پیام درخواست اجباریست و خطوط بعدی که به آنها خطوط سرایند یا هدر می‌گویند اختیاری است
- در انتهای هر خط کاراکترهای کنترلی سر خط (carriage return) و خط بعد (line feed) استفاده می‌شود، همچنین بعد از خط آخر و قبل از body دو جفت از اینها گذاشته می‌شود



فرمت کلی یک پیام درخواست HTTP



فیلد **version** : ورژن **http** که مرورگر ما از آن استفاده می‌کند را بیان می‌کند

فیلد متد می‌توان موارد رو به رو باشد: **GET,POST,HEAD,PUT,DELETE**

متد **GET**: مرورگر وب با این متد، شی گفته شده در فیلد **URL** را از سرویس دهنده درخواست می‌کند، اگر متد ما **GET** باشد، **body** خالی است

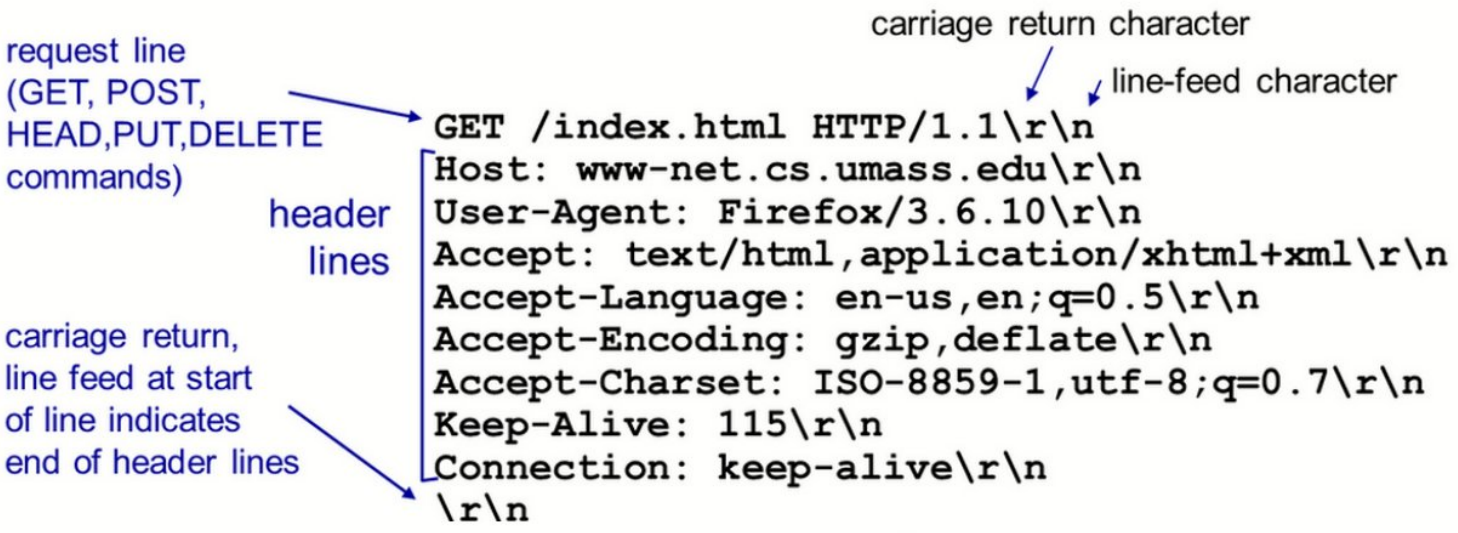
متد **POST** : برای فرستادن فرم‌هایی که فیلدهای آن توسط کاربر پر می‌شود به سرور استفاده می‌شود، سرور نیز بر اساس این اطلاعات پاسخ خواهد داد، مثلا وقتی در گوگل چیزی را می‌خواهیم سرچ کنیم استفاده می‌شود. در صورت استفاده از این متد اطلاعات فیلدهای فرم در قسمت **body** پیام درخواست قرار می‌گیرد

نکته : با **GET** نیز می‌توان اطلاعات فرم‌ها را به سرویس دهنده فرستاد، در این حالت مرورگر اطلاعات را به جای بدنه باید در انتهای **URL** بگذارد

متد **HEAD** : برنامه نویسان برای عیب یابی برنامه هایشان از این متد استفاده می‌کنند، سرویس دهنده در پاسخ به این فقط یک پیام پاسخ **HTTP** بدون شی درخواستی برمی‌گرداند

متدهای **PUT** و **DELETE** : به درد آپلود یا دیلت یک شی از روی سرور می‌خورد(مثلا کسی می‌خواهد سایتش را آپدیت کند)

Scanned with CamScanner



خط Host: میزبانی که شی درخواستی روی آن قرار دارد را مشخص می‌کند

سوال: وقتی کلاینت به همین سرور یک اتصال TCP برقرار کرده چه نیازی به این خط است؟ این خط برای پروکسی سرور (وب کش) نیاز است

خط User-Agent: نوع مرورگر کلاینت را مشخص می‌کند، دلیل استفاده از این سرآیند آن است که یک سرویس دهنده معمولا ویرایش‌های مختلفی از هر شی برای هر مرورگر دارد

خط Connection: مرورگر با این خط به سرور می‌گوید که اتصال پایا (keep-alive) می‌خواهد یا گذرا (close) مثلا اگر `connection: close` بود، مرورگر به سرویس دهنده می‌گوید که او می‌تواند بعد از فرستادن شی درخواست شده اتصال را ببندد

Method types در ورژن‌های مختلف HTTP

HTTP/1.0:

- GET
- POST
- HEAD
  - asks server to leave requested object out of response

HTTP/1.1:

- GET, POST, HEAD
- PUT
- uploads file in entity body to path specified in URL field
- DELETE
  - deletes file specified in the URL field

Scanned with CamScanner

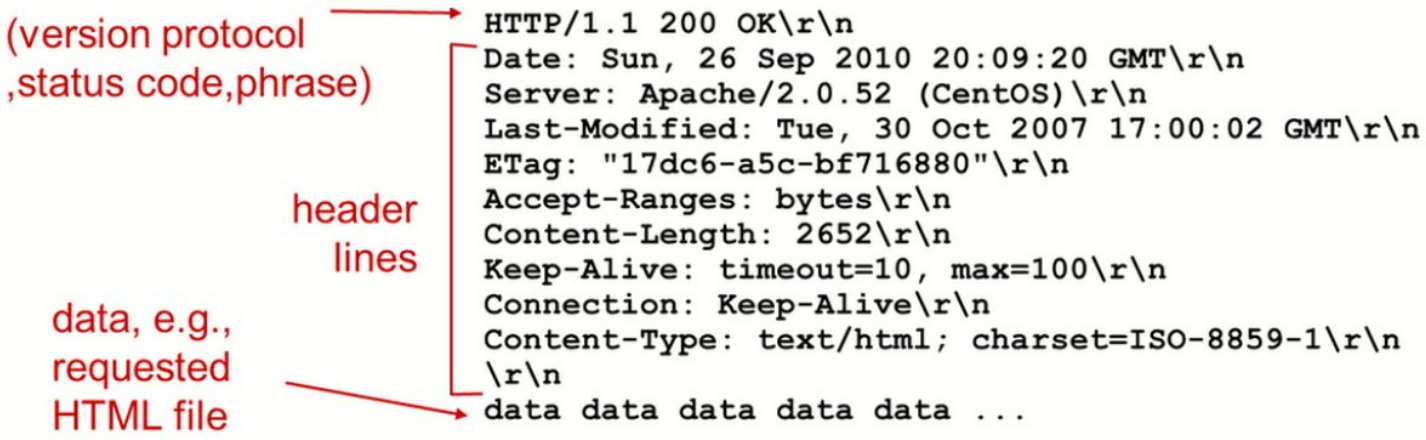
سوال:

پیام ASCII زیر توسط Wireshark وقتیکه مرورگر در حال ارسال یک پیام HTTP GET بوده capture شده، به سوالات زیر پاسخ دهید؟

```
GET /cs453/index.html
HTTP/1.1<cr><lf>Host:gaia.cs.umass.edu<cr><lf>User-Agent:
Mozilla/5.0 (Windows;U; Windows NT 5.1; en-US; rv:1.7.2)
Gecko/20040804 Netscape/7.2 (ax) <cr><lf>Accept:ext/xml,
application/xml, application/xhtml+xml,
text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
<cr><lf>Accept-Language:en-us,en;q=0.5<cr><lf>Accept-
Encoding: zip,deflate<cr><lf>Accept-Charset: ISO-8859-1,utf-
8;q=0.7,*;q=0.7<cr><lf>Keep-Alive: 300<cr><lf>Connection:keep-
alive<cr><lf><cr><lf>
```

1. آدرس تقاضا شده توسط مرورگر چیست؟ http://gaia.cs.umass.edu/cs453/index.html
2. نسخه HTTP که مرورگر استفاده می‌نماید چیست؟ HTTP/1.1
3. مرورگر متقاضی ارتباط پایدار است یا ناپایدار؟ persistent connection
4. **آدرس IP میزبانی که مرورگر روی آن اجرا شده چیست؟** این اطلاعات هیچ وقت در یک پیام HTTP وجود ندارد، برای بدست آوردن IP نیاز به دیتاگرام‌های IP ای که سگمنت‌های TCP ای که درخواست HTTP GET را حمل می‌کند نیاز داریم
5. چه نوع مرورگری این پیام را شروع کرده و چرا نوع مرورگر درون پیام درخواست HTTP احتیاج است؟ Mozilla/5.0

پیام پاسخ HTTP



خط وضعیت ۳ فیلد دارد، ۱) فیلد ورژن پروتکل HTTP ای که سرور استفاده می‌کند ۲) کد وضعیت ۳) پیام وضعیتی که متناظر است با کد وضعیت و آن را توصیف می‌کند

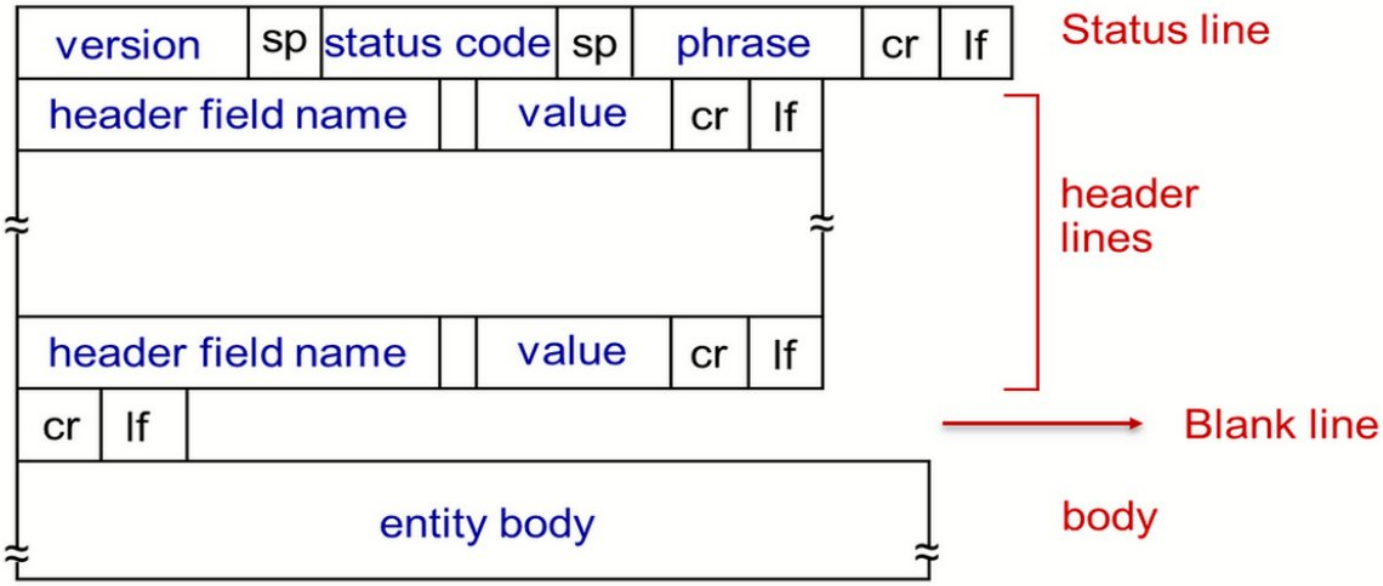
Date : تاریخ و زمان ایجاد و ارسال **پیام پاسخ HTTP** توسط سرور را بیان می‌کند، نشان می‌دهد در چه تاریخ و زمانی سرور این فایل را از فایل سیستم خود گرفته است و در داخل پیام پاسخ قرار داده و آن را فرستاده است

Last-Modified : تاریخ و زمان ایجاد یا آخرین تغییر فایل شی مورد نظر را مشخص می‌کند و **کاربرد این سرآیند برای اطلاع از آپدیت بودن یا نبودن یک شی در ۱) کش کلاینت و ۲) پروکسی سرور است**

Content-Type: نوع شی توسط این سرآیند تعیین می‌شود نه پسوند نام آن فایل

Scanned with CamScanner

فرمت کلی یک پیام پاسخ HTTP



نکته: یک مرورگر وب چگونه سرآیندهایی که در پیام می‌گذارند را تعیین می‌کنند

1. نوع ویرایش‌شان
2. تنظیمات کاربر در مرورگر و وب سرور
3. مرورگر و وب سرور آیا در کش خود نسخه‌ای از شی مورد نظر را دارند

معنی کدهای وضعیت در پاسخ HTTP

- **کد وضعیت و مفهوم متناظر با کد:** این دو در خط اول پاسخ HTTP می‌آیند و مشخص کننده نتیجه درخواست پیام **http** ای است که کلاینت برای سرور ارسال کرده است
- در زیر برخی از این کدها را آورده‌ایم

200 OK

Request succeeded and the information is returned in the response.

301 Moved Permanently

requested object moved, new location specified later in this response message (Location:), and The client software will automatically retrieve the new URL

400 Bad Request

request msg not understood by server

404 Not Found

requested document not found on this server

505 HTTP Version Not Supported

- فرستنده از یک ورژن **http** ای استفاده می‌کند که توسط سرور مورد نظر ساپورت نمی‌شود

Scanned with CamScanner

سوال

- درستی و نادرستی عبارات زیر را مشخص کنید

1. یک صفحه وب که شامل مقداری متن نوشتاری و سه تصویر می‌باشد، برای دریافت این صفحه مشتری یک پیام درخواست http ارسال می‌کند و چهار پیام پاسخ دریافت خواهد کرد

پاسخ : اشتباه است . به ازای هر شی مشتری باید یک درخواست جدا ارسال کند

2. دو صفحه وب مجزا از **یک سایت** که بر روی یک سرور قرار دارند می‌توانند بر روی یک اتصال پایدار برای یک یوزر ارسال بشوند

پاسخ : یک مشتری که به یک وب سرور متصل شده است اگر از اتصال Tcp ماندگار استفاده کند می‌تواند در لحظات مختلفی از زمان پیج‌هایی که روی آن سرور وجود دارد را درخواست کند (ماندگار یعنی اتصال قطع نشود و ما بتوانیم صفحات جدیدی را روی همان اتصال دریافت کنیم)

3. با یک اتصال گذرا بین یک مرورگر و سرور ممکن است یک اتصال TCP واحد، دو پیام درخواست HTTP مجزا را حمل کند

پاسخ :خیر. در اتصال گذرا برای هر تقاضا نیاز به یک ارتباط جدید داریم

3. با یک اتصال گذرا بین یک مرورگر و سرور ممکن است یک سگمنت TCP واحد، یک جفت پیام درخواست و پاسخ HTTP را حمل کند

پاسخ : بله

4. سربار DATE در پیام پاسخ HTTP نمایانگر زمان آخرین تغییر پیام در بخش پاسخ دهنده است

پاسخ : خیر DATE بیانگر زمان ایجاد و ارسال پیام توسط سرویس دهنده است

5. پیام‌های پاسخ HTTP هرگز دارای بدنه خالی نخواهند بود

پاسخ : نادرست است. اگر پیام درخواست دارای متد HEAD باشد پیام پاسخ http ارسالی دارای بدنه خالی خواهد بود

cookies

نکته: ویژگی بدون حالت بدون HTTP باعث شده که سرورها بتوانند همزمان به هزاران اتصال TCP پاسخ دهد

اما در بسیاری از مواقع یک وب سایت نیاز دارد که اطلاعات کاربران خود را نگه دارد، برای این منظور پروتکل HTTP از کوکی استفاده می‌کند

کوکی برای ۴ مورد زیر می‌تواند استفاده بشود

user session state (Web e-mail) ، recommendations،shopping carts ،Authorization

نکته: با استفاده از کوکی است که سایت می‌توانند one click shoping داشته باشند

نکته: عده‌ای کوکی را نقض حریم خصوصی خود می‌دانند

نکته: در واقع به کمک کوکی می‌توان یک لایه نشست روی پروتکل بدون حالت HTTP ایجاد کرد

بسیاری از وب سایت ها از کوکی استفاده می‌کنند این کار چهار مولفه دارد

1. یک خط سرآیند کوکی در پیام پاسخ HTTP
2. یک خط سرآیند کوکی در پیام درخواست HTTP
3. یک فایل کوکی که روی سیستم کاربر نگهداری می‌شود و توسط مرورگر یوزر مدیریت می‌شود
4. یک پایگاه داده پشتیبان در سروری که وب سایت مد نظر روی آن است

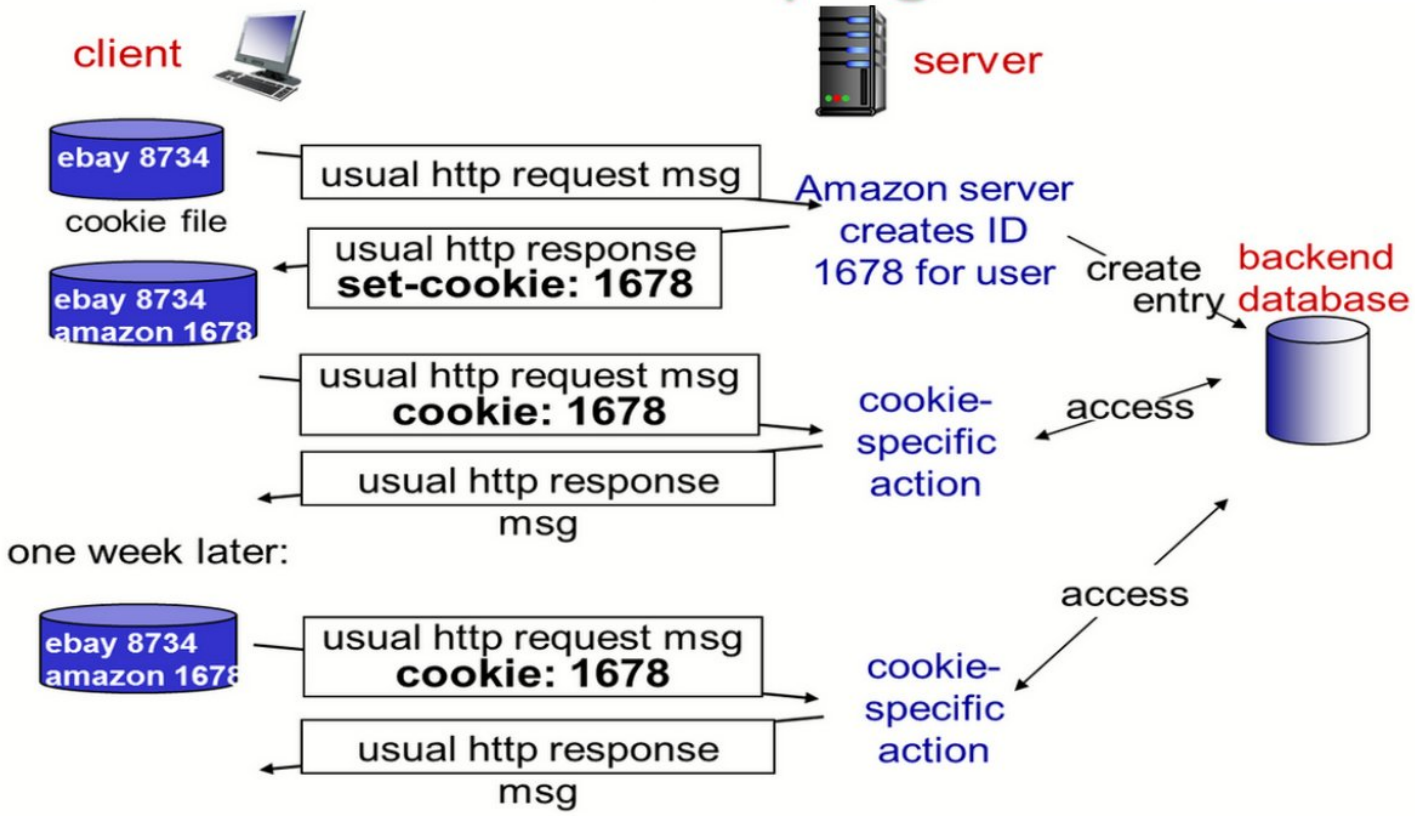
- در واقع پیام‌های HTTP حالت (state) را حمل می‌کنند

مثال :

- سوزان همیشه از طریق کامپیوتر شخصی‌اش به اینترنت متصل می‌شود
- فرض کنید برای اولین بار از یک سایت تجاری دیدن می‌کند
- زمانیکه اولین درخواست HTTP به سایت می‌رسد، سایت موارد زیر را ایجاد می‌کند
  - یک آی دی واحد برای یوزر
  - یک سطر برای این آی دی در پایگاه داده پشتیبان خودش

Scanned with CamScanner

Cookies: keeping "state"

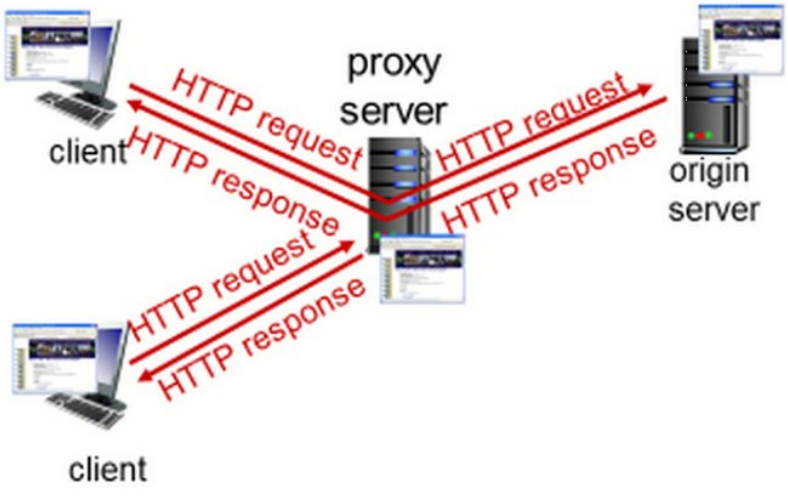


نکته: هر بار که در یوزر میخواهد به یک سایت مراجعه کند ابتدا مرور گر به فایل کوکی مراجعه می‌کند و اگر در فایل ID آن سایت را پیدا کرد یک خط سرآیند بصورت ... :cookie در پیام درخواست http اضافه می‌کند

Web caches (proxy server)

هدف : پاسخ دادن به درخواست‌های کاربران بدون درگیر کردن سرور مقصد

- مرورگرهای وب را می‌توان طوری پیکربندی کرد که تمامی درخواست‌های HTTP خود را ابتدا به یک Web cache بدهند
  - اگر شی در کش باشد، کش شی را بر می‌گرداند
  - اگر شی در کش نباشد، کش شی را از سرور مقصد درخواست می‌کند و پس از دریافت شی، آن را به یوزر ارسال می‌کند



- شبکه‌های توزیع محتوا با نصب حافظه‌های نهان در مناطق مختلف دنیا بخش زیادی از ترافیک اینترنت را بصورت محلی در آورده‌اند

Scanned with CamScanner

حافظه نهان هم نقش مشتری و هم نقش سرور را بازی می‌کند

- نقش سرور هنگامیکه درخواست‌های اصلی را از مرورگر مشتری می‌گیرد و به آن پاسخ می‌دهد
- نقش مشتری هنگامیکه درخواست‌های خودش را به سرور مقصد می‌فرستد

نکته: بطور معمول کش توسط ISP ها نصب و پیاده‌سازی می‌شوند(دانشگاه‌ها، شرکتهای بزرگ)

مزایای web caching چیست؟

1. **کاهش زمان پاسخ برای درخواست‌های مشتری**
   - پهنای باند بین مشتری و کش معمولا خیلی بیشتر از پهنای باند بین مشتری و سرور مقصد است
2. **کاهش ترافیک لینک‌های دسترسی موسسات بزرگ**
   - موسسات نیازی ندارند به سرعت پهنای باندشون و ارتقا بدهند که کاهش هزینه و در بر دارد
3. **کاهش ترافیک اینترنت**
   - افزایش کارایی تمامی برنامه‌ها

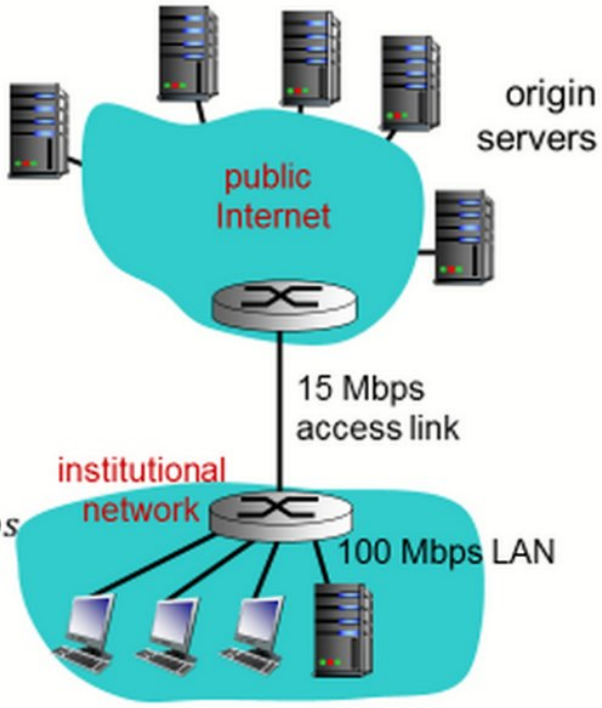
Caching example

assumptions:

- avg object size: 1 Mbits
- avg request rate from browsers to origin servers:15/sec
- avg data rate to browsers: 15 Mbps
- RTT from edge router to any origin server: 2 sec
- access link rate: 15 Mbps

consequences:

- LAN utilization: 0.15 ← $15\ Mbps \div 100\ Mbps$
- access link utilization = 1 → $15Mbps \div 15Mbps$ *problem!*
  - با نزدیک شدن شدت ترافیک به ۱ تاخیر لینک دسترسی به سمت دقیقه میل می‌کند
- total delay = Internet delay + access delay + LAN delay
  = 2 sec + minutes + msec



نکته : معمولا گلوگاه یک سازمان تو LAN سازمان و تو اینترنت نیست و در لینک دسترسی اون سازمان هست

Scanned with CamScanner

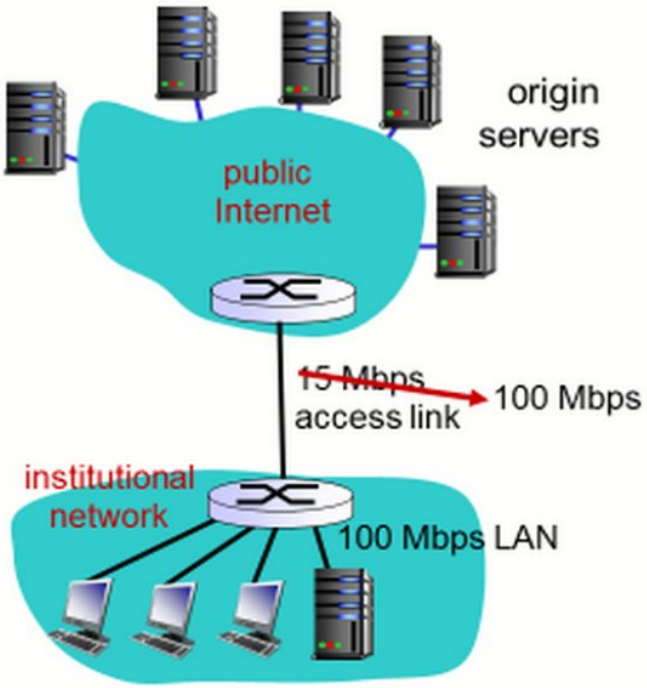
Caching example: faster access link

assumptions:

- avg object size: 1 Mbits
- avg request rate from browsers to origin servers: 15/sec
- avg data rate to browsers: 15 Mbps
- RTT from institutional router to any origin server: 2 sec
- access link rate: ~~15 Mbps~~ → 100 Mbps

consequences:

- LAN utilization: 0.15
- access link utilization = ~~1~~ → 0.15
- total delay = Internet delay + access delay + LAN delay
  = ~~2 sec + minutes~~ → msecs + msecs



Cost: increased access link speed (not cheap!)

Caching example: install local cache

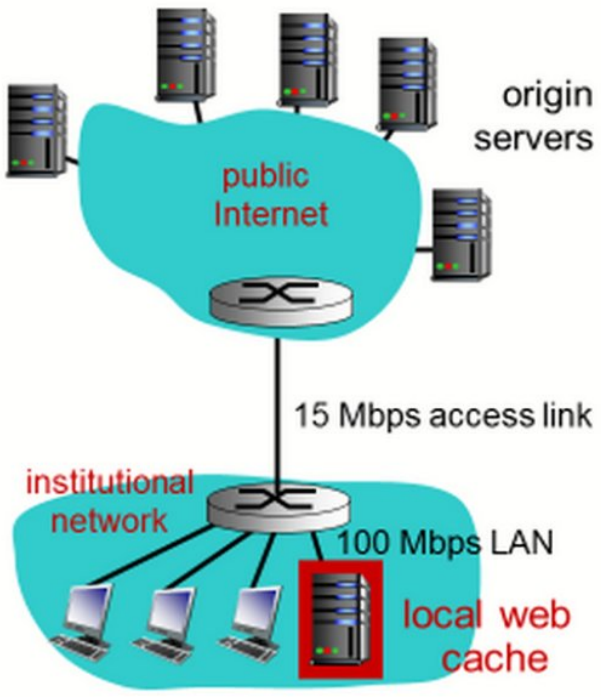
assumptions:

- avg object size: 1 M bits
- avg request rate from browsers to origin servers: 15/sec
- avg data rate to browsers: 15 Mbps
- RTT from institutional router to any origin server: 2 sec
- access link rate: 15 Mbps

consequences:

- LAN utilization: 0.15
- access link utilization = ?
- total delay = ?

How to compute link utilization, delay?

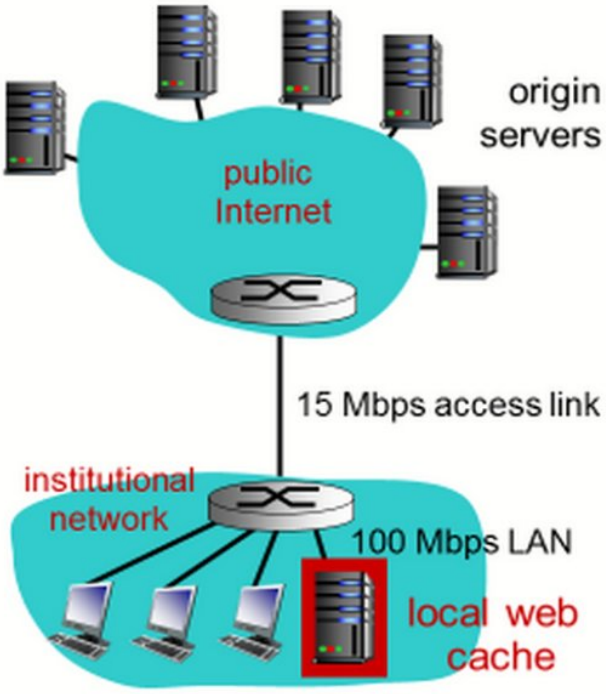


Cost: web cache (cheap!)

Scanned with CamScanner

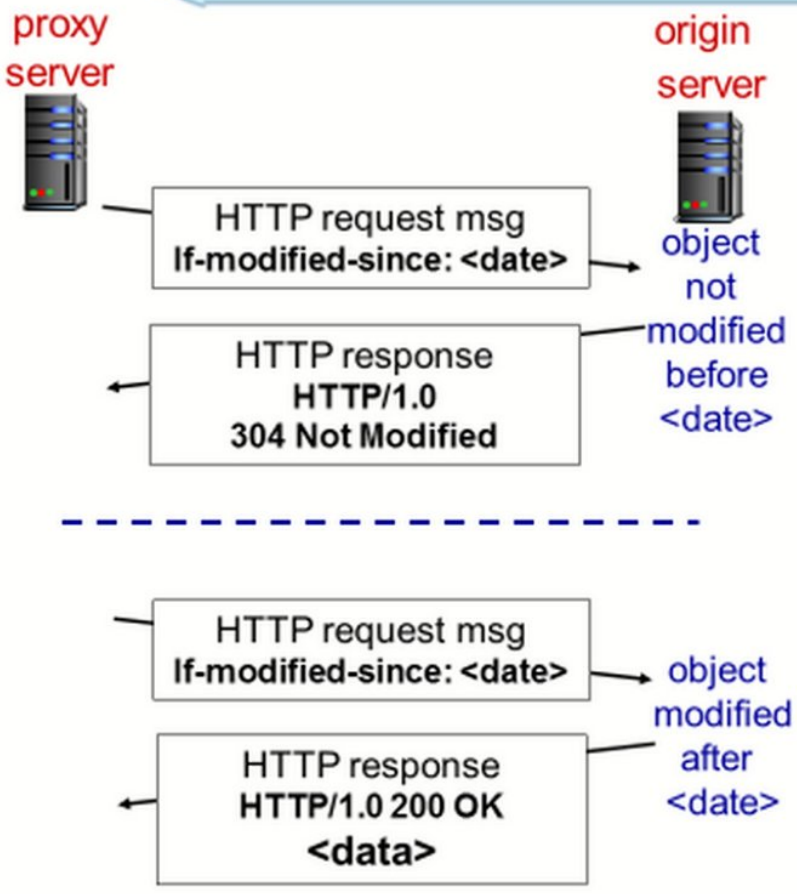
Caching example: install local cache

- *Calculating access link utilization, delay with cache:*
- suppose cache hit rate is 0.4
  - 40% requests satisfied at cache, 60% requests satisfied at origin



- access link utilization:
  - 60% of requests use access link
- data rate to browsers over access link = 0.6*15 Mbps = 9 Mbps
  - utilization = 9/15 = .6
- total delay
  - = 0.6 * (delay from origin servers) +0.4 * (delay when satisfied at cache)
  - = 0.6 (2.01) + 0.4 (~msecs)
  - = ~ 1.2 secs
  - less than with 100 Mbps link (and cheaper too!)

Web caches (proxy server) continue

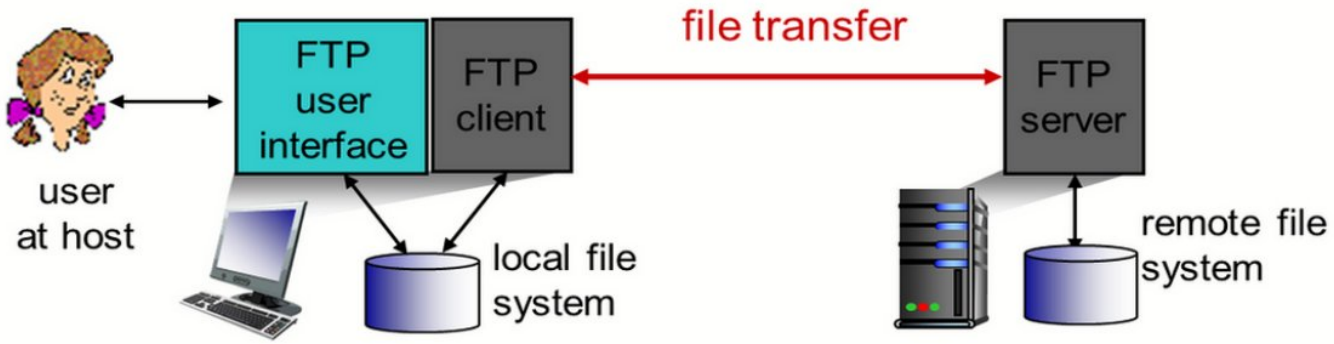


- وقتی شی ای را از سروری درخواست می‌کنیم و کش آن اطلاعات را دارد، همیشه این نگرانی وجود دارد که نکند اطلاعات درون کش آپدیت نباشد
- پروتکل HTTP مکانیزمی به نام GET شرطی (Conditional GET)دارد که اجازه می‌دهد تا حافظه‌های نهان از آپدیت بودن اشیایی که دارند مطمئن شوند
- برای آنکه پیام درخواست HTTP از نوع GET شرطی تلقی شود باید
  1. از متد GET استفاده کنیم
  2. در پیام درخواست از خط هدر If-Modified-Since استفاده شود

Scanned with CamScanner

FTP: the file transfer protocol

- یک فایل سرور راه دور وجود دارد که می‌توانیم فایل‌ها را از آن بخوانیم یا در آن بنویسیم
- تعاملات کاربر با FTP از طریق یک FTP user agent (عامل کاربر FTP) انجام می‌شود، کاربر ابتدا hostname (نام میزبان)، remote host (میزبان دور) را وارد می‌کند که در اثر این FTP client process روی local host با FTP server process در میزبان دور یک اتصال TCP برقرار می‌سازد
- سپس کاربر در اکثر موارد باید یوزرنیم و پسورد خود را وارد کند
  - این اطلاعات بعنوان بخشی از پیام FTP روی این اتصال TCP ارسال می‌شود
- در صورت مجاز دانستن این کاربر توسط سرور، کاربر می‌تواند فایل بگیرد یا بفرستد
- کلاینت/ سرور مدل
  - کلاینت : سمتی که ایجاد انتقال را آغاز می‌کند
  - سرور : میزبان دور (remote host)



- FTP برای انتقال یک فایل از دو اتصال TCP موازی استفاده می‌کند،یک اتصال کنترل و یک اتصال داده
- بنابراین مبادله اطلاعات کنترلی در FTP **خارج باندی** است
- کاربر FTP روی پورت ۲۱ یک اتصال کنترل TCP با سرور ایجاد می‌کند
- روی همین اتصال کنترلی مشتری با وارد کردن یوزرنیم و پسورد احراز هویت می‌شود
  - فرمان‌های تغییر دایرکتوری در سرور و فرمان‌هایی برای جابجا کردن فایل بین دو میزبان از طریق همین اتصال انتقال می‌یابد
- وقتی سرور فرمان انتقال فایل را از مشتری دریافت کند روی پورت ۲۰ یک اتصال داده TCP به مشتری ایجاد می‌کند
- بعد از ارسال یک فایل، سرور اتصال دیتا را می‌بندد و برای ارسال هر فایل در همان نشست یک اتصال داده جدید باز می‌شود
  - **اتصال کنترلی در FTP ماندگار و اتصال داده در FTP گذرا است**
  - **در طول یک نشست** سرور FTP اطلاعات کاربران را نگهداری می‌کند
    - تعداد نشست‌های همزمان در سرور FTP محدود می‌شود

Scanned with CamScanner

تست

- سرور FTP اطلاعات حالت کاربران را به چه صورت نگه می‌دارد؟

1. بصورت همیشگی حالت را نگه می‌دارد(Stateful)
2. اصلا اطلاعات را نگهداری نمی‌کند(Stateless)
3. با استفاده از سرویس دهنده پروکسی اطلاعات وضعیت را نگهداری می‌کند
4. در طول نشست اطلاعات حالت را نگهداری می‌کند(Session State)

تست کنکور آی تی ۹۳ سراسری

- فرض کنید ۱۰ کلاینت با استفاده از پروتکل FTP بطور همزمان در حال دریافت فایل هایی با حجم زیاد از یک فایل سرور هستند و لینک گلوگاه لینک متصل به سرور است، اگر یکی از کلاینت ها از برنامه Download manager استفاده کند که بطور همزمان ۹ اتصال همزمان TCP باز می کند، سرعت دانلود این کلاینت نسبت به قبل چند برابر خواهد شد؟

۱) ۲ ۲) ۴ ۳) ۵ ۴) ۱۰

حل : اگر تعدادی مشتری از نقاط مختلف به یک سرور با پروتکل TCP متصل شود و همه آنها داده زیادی را از سرور بخواهند، TCP بعلت خواصی که دارد که در فصل بعد بررسی می شود باعث می‌شود که پهنای باند سرور بصورت مساوی بین مشتری‌های سرور تقسیم شود

اگر فرض کنیم هر ۱۰ کلاینت بصورت مجزا هر کدام با یک اتصال TCP به سرور متصل می‌شوند، به هر کدام از کلاینت‌ها $\frac{1}{10}$ از پهنای باند سرور می‌رسد ($\frac{1}{10}R_s$) اما در این سوال اینطور نیست، در این سوال به این صورت است که ۹ کلاینت هر کدام با یک TCP به سرور متصل می‌شوند و یک کلاینت(مثلا کلاینت دهم) خود به تنهایی با ۹ اتصال TCP به سرور متصل می‌شود، بنابراین ۱۸ اتصال TCP به سرور خواهیم داشت که سهم هر یک $\frac{1}{18}$ از پهنای باند سرور خواهد بود، کلاینت مورد نظر در حالت عادی $\frac{1}{10}$ از پهنای باند سرور را در اختیار داشت ولی در حالت جدید از $\frac{9}{18}$ پهنای باند سرور استفاده می‌کند، بنابراین خواهیم داشت:

$$\frac{1}{10}R_s \times X = \frac{1}{2} \times R_s \rightarrow X = 5$$

FTP commands, responses

- فرمان‌های FTP از مشتری به سرویس دهنده و پاسخ آنها از سرویس دهنده به مشتری روی اتصال کنترلی و با فرمت اسکی ۷ بیتی منتقل می‌شوند
- فرمان‌های FTP همگی چهار حرفی هستند

Scanned with CamScanner

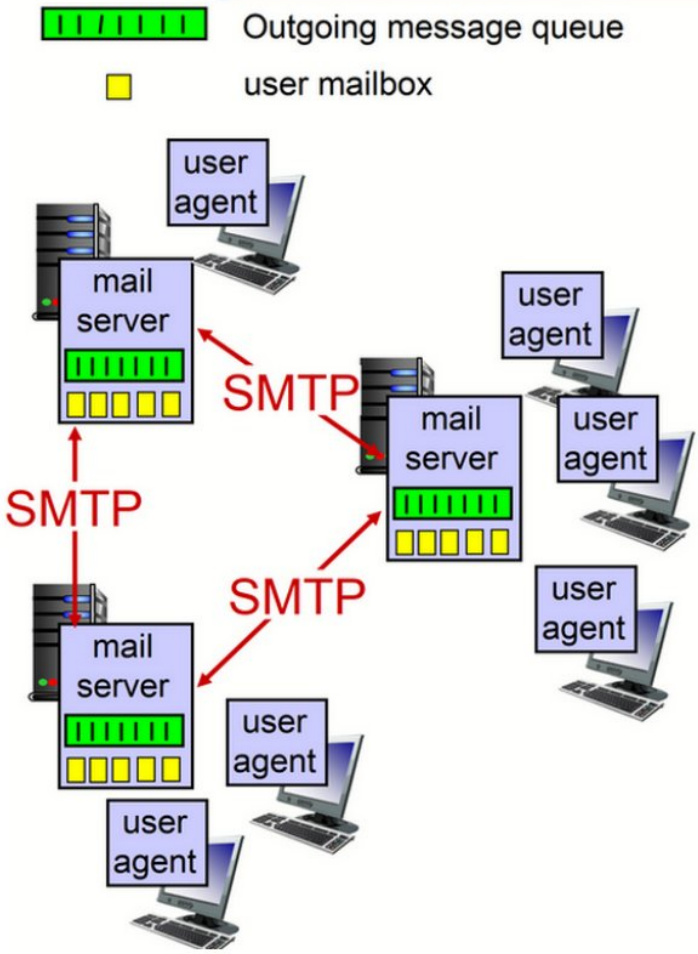
- *sample commands:*
- sent as ASCII text over control channel
- **USER *username***
- **PASS *password***
- **LIST** return list of file in current directory
- **RETR filename** retrieves (gets) file
- **STOR filename** stores (puts) file onto remote host

- *sample return codes*
- status code and phrase (as in HTTP)
- **331 Username OK, password required**
- **125 data connection already open; transfer starting**
- **425 Can't open data connection**
- **452 Error writing file**

- **RETR:** مشتری از سرویس دهنده می‌خواهد تا فایل مشخص شده را برایش بفرستد. سرویس دهنده برای ارسال این فهرست از یک اتصال داده جدید و غیرپایا استفاده می‌کند
- **STOR:** با این فرمان مشتری فایل مشخص شده از کامپیوتر خود را به سرویس دهنده می‌فرستد تا در دایرکتوری جاری سیستم راه دور ذخیره شود، مشتری برای ارسال این فایل یک اتصال داده جدید و غیرپایا به سرویس دهنده ایجاد می‌کند
- هر فرمانی که کاربر روی اتصال کنترل می‌فرستد با یک پاسخ FTP از طرف سرویس دهنده همراه است

Scanned with CamScanner

Electronic mail



- سیستم میل سه جز اصلی دارد
  1. عامل کاربر (user agent)
  2. سرویس‌دهنده پست (mail server)
  3. پروتکل ساده انتقال نامه کاربر (SMTP:simple Mail Transfer Protocol)
- هر گیرنده یک mailbox (صندوق پستی) روی یکی از میل سرورها دارد
- نامه فرستنده توسط عامل کاربر فرستنده به میل سرور فرستنده ارسال می‌شود، سپس در صف نامه‌های خروجی میل سرور فرستده در انتظار ارسال قرار می‌گیرد، سپس میل سرور فرستنده این نامه را به میل سرور گیرنده می‌فرستد، و این پیام در صندوق پستی گیرنده روی میل سرور گیرنده قرار می‌گیرد، حال هر وقت گیرنده بخواهد نامه‌های خود را بخواند عامل کاربر گیرنده این پیام را از صندوق پستی‌اش که روی میل سرور گیرنده وجود دارد بازیابی می‌کند

Electronic mail(count)

User Agent

- بهش mail reader هم می‌گویند
- تولید، ویرایش، خواندن پیام‌های میل
- *مثل* Outlook(microsoft), Thunderbird(mozila), iPhone mail client
- پیام‌های وارد شده و خارج شده روی میل سرورها ذخیره می‌شوند

mail servers

- *mailbox : شامل پیام‌های ورودی کاربرها*
- *message queue of outgoing : (صف نامه‌های خروجی) : ارسال پیام‌های میل*
- *پروتکل SMTP : بین میل سرورهاست برای ارسال پیام‌های ایمیل*
  - *سمت مشتری: روی میل سرور فرستنده اجرا می‌شود، وقتی میل سرور پیامی را به میل سرور دیگری ارسال می‌کند بعنوان مشتری SMTP عمل می‌کند*
  - *سمت گیرنده: روی میل سرور گیرنده اجرا می‌شود، وقتی میل سرور پیامی را از میل سرور دیگری دریافت می‌کند بعنوان سرور SMTP عمل می‌کند*
- میل سرورها هر دو بخش را همزمان اجرا می‌کنند
- چون یک سرور گاهی نقش فرستنده و گاهی نقش گیرنده را بازی می‌کند

Scanned with CamScanner

SMTP

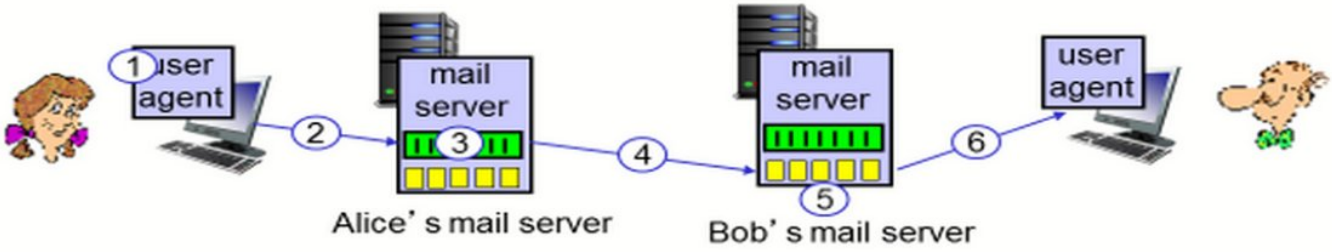
- میل سرور فرستنده پیام‌ها را با استفاده از SMTP به میل سرور گیرنده می‌فرستد
- SMTP برای ارسال مطمئن ایمیل‌ها از کلاینت به سرور از TCP استفاده می‌کند
- ارسال مستقیم : SMTP برای ارسال ایمیل از هیچ میل سرور میانی بعنوان میل سرور واسط استفاده نمی‌کند و یک اتصال TCP مستقیم بین میل سرور مبدا و مقصد برقرار می‌شود
- انتقال پیام از مشتری SMTP به سرور SMTP سه فاز دارد (پس از برقراری اتصال TCP)

1. handshaking (greeting)
   - دستداد لایه کاربرد. مشتری SMTP قبل از ارسال نامه خود را به سرور SMTP معرفی می‌کند همچنین موارد زیر را به سرویس دهنده SMTP می‌گوید
     1. آدرس ایمیل ارسال کننده میل
     2. آدرس ایمیل دریافت کننده میل
2. ارسال پیام میل
3. بستن اتصال
   - اگر سرویس دهنده پست فرستنده چندین پیام به همین مقصد داشته باشد، همه آنها را روی همین اتصال TCP می‌فرستد، یعنی SMTP از اتصال ماندگار TCP استفاده می‌کند

- command/response interaction (like HTTP, FTP)
  - commands: ASCII text
  - response: status code and phrase
- در SMTP نه تنها سرآیند نامه‌ها بلکه بدنه آنها نیز باید اسکی ۷ بیتی باشند، بنابراین عامل کاربر باید قبل از ارسال ایمیل محتویات چندرسانه‌ای باینری ایمیل را بصورت اسکی ۷ بیتی در آورد، در مقصد نیز باید عکس این عمل اتفاق بیفتد
- HTTP محدودیتی برای ارسال داده‌های غیرنوشتاری ندارد

Scenario: Alice sends message to Bob

1) Alice uses UA to compose message "to" bob@someschool.edu
2) Alice's UA sends message to her mail server; message placed in message queue
3) client side of SMTP opens TCP connection with Bob's mail server
4) SMTP client sends Alice's message over the TCP connection
5) Bob's mail server places the message in Bob's mailbox
6) Bob invokes his user agent to read message



Scanned with CamScanner

Sample SMTP interaction

```
S: 220 hamburger.edu
C: HELO crepes.fr
S: 250  Hello crepes.fr, pleased to meet you
C: MAIL FROM: <alice@crepes.fr>
S: 250 alice@crepes.fr... Sender ok
C: RCPT TO: <bob@hamburger.edu>
S: 250 bob@hamburger.edu ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like ketchup?
C: How about pickles?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 hamburger.edu closing connection
```

- سرویس دهنده SMTP در پاسخ به هر فرمان مشتری SMTP پیامی شامل یک عدد و مقداری توضیحات (اختیاری) را بر می‌گرداند

SMTP در مقایسه با HTTP

1. SMTP همیشه از اتصال‌های ماندگار استفاده می‌کند، حال آنکه HTTP می‌تواند از هر دو نوع اتصال گذرا و ماندگار استفاده کند
2. HTTP: Pull protocol و SMTP: Push protocol است
   - Pull protocol : ماشین گیرنده پیام(فایل) یک اتصال(TCP) به ماشین سرویس دهنده ایجاد می‌کند
   - Push protocol : ماشین فرستنده پیام(فایل) یک اتصال(TCP) به ماشین گیرنده ایجاد می‌کند
3. در SMTP هم سرآیند پیام‌ها و هم بدنه پیام باید بصورت اسکی ۷ بیتی ارسال شوند، اما در HTTP بدنه می‌تواند اسکی نباشد
4. در HTTP هر شی در یک پیام پاسخ جداگانه به مشتری ارسال می‌شود در حالی که در SMTP چندین شی در قالب یک پیام واحد به گیرنده فرستاده می‌شود

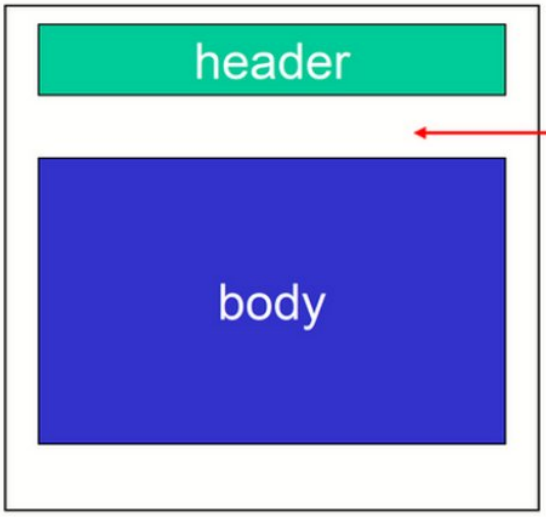
Scanned with CamScanner

فرمت پیام‌های نامه

- مانند HTTP هر خط هدر شامل یک متن قابل خواندن بصورت زیر است

```
Keyword : value
```

- در هدر پیام برخی از keyword ها اجباری و برخی اختیاری هستند
  - اجباری : From : و To :
  - اختیاری : Subject :



- بعد از سرآیندهای پیام یک خط خالی می‌آید و بعد بدنه نامه

- فرمان‌های SMTP (مثل From وTo) بخشی از فرآیند دستداد در پروتکل SMTP هستند در حالی که خطوط سرآیند جزئی از پیام ایمیل محسوب می‌شوند

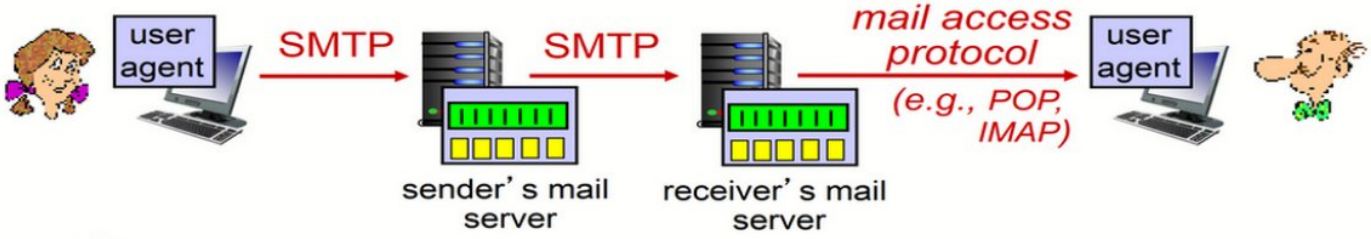
پروتکل دسترسی نامه(Mail access protocols)

- چرا ما نیاز به میل سرورهای سمت فرستنده و گیرنده داریم؟ و چرا عامل‌های کاربر ما مستقیما با هم ارتباط برقرار نمی‌کنند؟
  - دلیل وجودی میل سرور سمت گیرنده : اگر کامپیوتر مقصد خاموش باشد فرستنده نمی‌تواند هر ۳۰ دقیقه یکبار ایمیل را دوباره ارسال کند، در اینصورت همیشه باید آنلاین باشد، بنابراین میل سروری سمت گیرنده می‌گذاریم
  - دلیل وجودی میل سرور سمت فرستنده : اگر سمت فرستنده میل سرور نگذاریم، عامل کاربر فرستنده هیچ راهی برای ارسال پیام‌هایش به یک میل سرور خاموش سمت گیرنده نخواهد داشت

Scanned with CamScanner

پروتکل دسترسی نامه(ادامه)

- عامل کاربر گیرنده نمی‌تواند از پروتکل SMTP برای برداشتن(گرفتن) ایمیل‌های خود از روی میل سرورش استفاده کند، چون SMTP ، Push protocol است نه Pull protocol
- پروتکل دسترسی نامه
  - POP (Post Office Protocol) :
    - authorization, download(transaction), update
  - IMAP (Internet Mail Access Protocol) : قابلیت‌های بیشتری از جمله دستکاری پیام‌های ذخیره شده بر روی سرور را در اختیار قرار می‌دهد
  - HTTP : gmail, Hotmail, Yahoo! Mail



POP3 protocol

- مشتری یک اتصال TCP روی پورت ۱۱۰ به میل سروراش برقرار می‌کند
- بعد از برقراری این اتصال POP3 وارد یک فاز سه مرحله‌ای می‌شود
  1. Authorization
  2. download(transaction) : در این مرحله عامل کاربر می‌تواند:
     - ایمیل‌ها را بازیابی می‌کند
     - پیام‌هایی که می‌خواهد حذف شود را علامت گذاری کند
     - آمار پیام‌ها مانند اندازه پیام‌های موجود در صندوق پستی را استخراج کند
  3. update
     - در این مرحله سرویس دهنده پیام‌های علامت گذاری شده برای حذف شدن را حذف خواهد کرد
- عامل کاربر می‌تواند با استفاده از POP3 جعبه پیام درون میل سرورش را به دو صورت پیکربندی کند
  1. download and delete
  2. download and keep
- مدل دانلود و حذف POP3
  - شخص نمی‌تواند ایمیل‌اش را مجددا از روی کلاینت دیگری جز آن کلاینتی که در ابتدا ایمیل را با آن دانلود کرده بخواند
- مدل دانلود و نگهداری POP3
  - میل سرور پیام‌های شخص را روی خودش نگه می‌دارد
  - بنابراین می‌توان کپی از ایمیل ها را در کلاینت‌های مختلف داشت
- سرور POP3 هیچ اطلاعات حالتی را از یک نشست POP3 به نشست دیگر منتقل نمی‌کند

Scanned with CamScanner

POP3 protocol

authorization phase

- client commands:
  - `user`: declare username
  - `pass`: password
- server responses
  - `+OK`
  - `-ERR`

transaction phase, client:

- `list`: list the size of each of the stored messages
- `retr`: retrieve message by number
- `dele`: delete
- `quit`

```
S: +OK POP3 server ready
C: user bob
S: +OK
C: pass hungry
S: +OK user successfully logged on

C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: <message 1 contents>
S: .
C: dele 1
C: retr 2
S: <message 1 contents>
S: .
C: dele 2
C: quit
S: +OK POP3 server signing off
```

IMAP

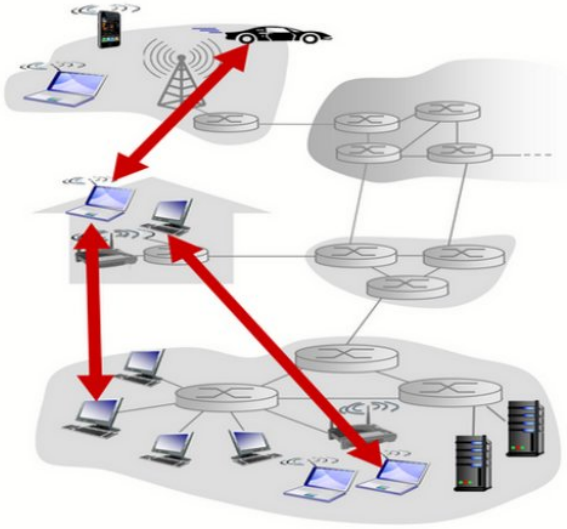
- بعد از POP3 یک ورژن پیشرفته تری بنام IMAP درست شد که این امکان را ایجاد می‌کند که ما روی کامپیوترمان یک Directory structure درست کنیم و ایمیل‌هایمان را در یک Directoryهایی بگذاریم و بعد به محض اینکه این کار را کردیم تو سرور هم همین اتفاق بیفتد، و هر کار که در Directoryهای گیرنده می‌کنیم در دایرکتوری‌های روی سرور هم همین اتفاق می‌افتد که معنی‌اش این هست که یک کپی ای از هرچه که ما در گیرنده داریم توی سرور هم باشد
- حال اگر با کلاینت‌های دیگری به میل سرور وصل شویم عین همون چیزی که تو کلاینت قبلی داشتیم تو کلاینت جدید هم خواهیم داشت
- سرور IMAP اطلاعات حالت را ین نشست‌های متوالی نگه می‌دارد
  - نام فولدرها
  - هر پیام متعلق به چه پوشه‌ای است
- IMAP به یوزرها اجازه میده تا ایمیل‌هایشان را درون فولدرها سازماندهی کنند
- عامل کاربر می‌تواند فقط بخشی از پیام‌ها را درخواست کند، یا تعدادی از ایمیل‌ها را دریافت کند
  - این مورد در لینک‌های با پهنای باند کم بین کاربر و میل سرور سودمند است

Web-Based E-Mail

- کاربران از طریق HTTP به صندوق پستی‌شان دسترسی پیدا می‌کنند
- وقتی کاربر می‌خواهد ایمیلی را از صندوق پستی‌اش بخواند، ایمیل با پروتکل HTTP از میل سرور به مرورگر کاربر فرستاده می‌شود
- وقتی یک کاربر بخواهد ایمیلی را بفرستد این پیام با پروتکل HTTP از مرورگر او به میل سرور او ارسال می‌شود

Scanned with CamScanner

P2P applications



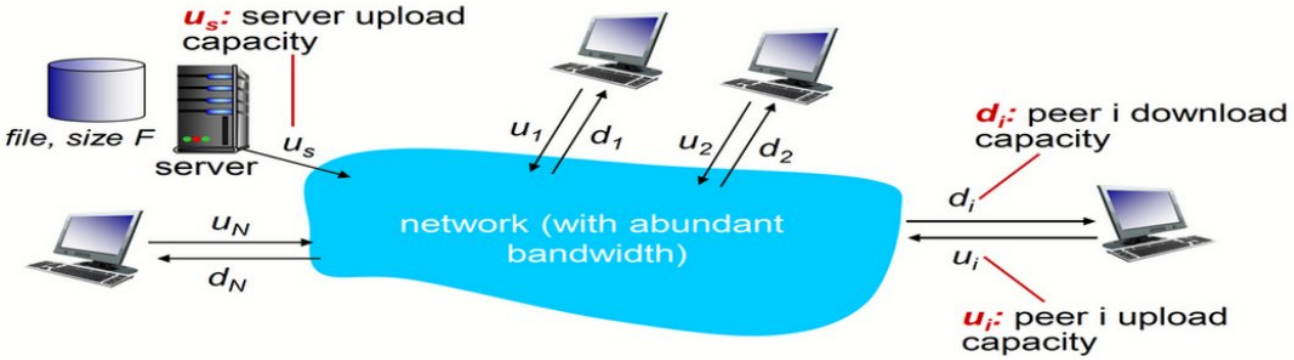
- نودها بطور متناوب متصل می‌شوند و امکان دارد آدرس IP شان را عوض کنند
- میزبان‌ها بطور خودسرانه با یکدیگر ارتباط برقرار می‌کنند
- مدیریت پیچیده
- نودها می‌توانند on یا off باشند

examples

- file distribution (BitTorrent)
- Streaming (KanKan)
- VoIP (Skype)

File distribution: client-server vs P2P

- سوال : چه زمانی طول می‌کشد تا فایلی با اندازه F از یک سرور روی N تا نود توزیع بشود؟
  - نرخ آپلود و دانلود نودها محدود است
  - فرض می‌کنیم که هسته اینترنت پهنای باند نامحدودی دارد
  - سرور و کلاینت‌ها هیچ برنامه‌تحت شبکه دیگری را اجرا نمی‌کنند



زمان توزیع فایل در مدل client-server

- زمان توزیع فایل: زمان لازم برای دریافت کپی فایل توسط N نود (نظیر)
- در این معماری هیچ نظیری به توزیع فایل کمک نمی‌کند
- زمان ارسال سرور : سرور باید پشت سر هم N کپی از فایل را آپلود کند
  - زمان ارسال یک کپی : F/u_s
  - زمان ارسال N کپی : NF/u_s
- نظیر : هر کلاینت باید فایل کپی را دانلود کند
  - D_{min} کمترین نرخ دانلود نظیرها
  - نظیر نمی‌تواند فایل را در زمانی کمتر از F/d_{min} دریافت کند

زمان توزیع فایلی با اندازه F روی N کلاینت با مدل client-server $= D_{c\text{-}s} \geq max\{NF/u_s, F/d_{min}\}$

increases linearly in N

Scanned with CamScanner

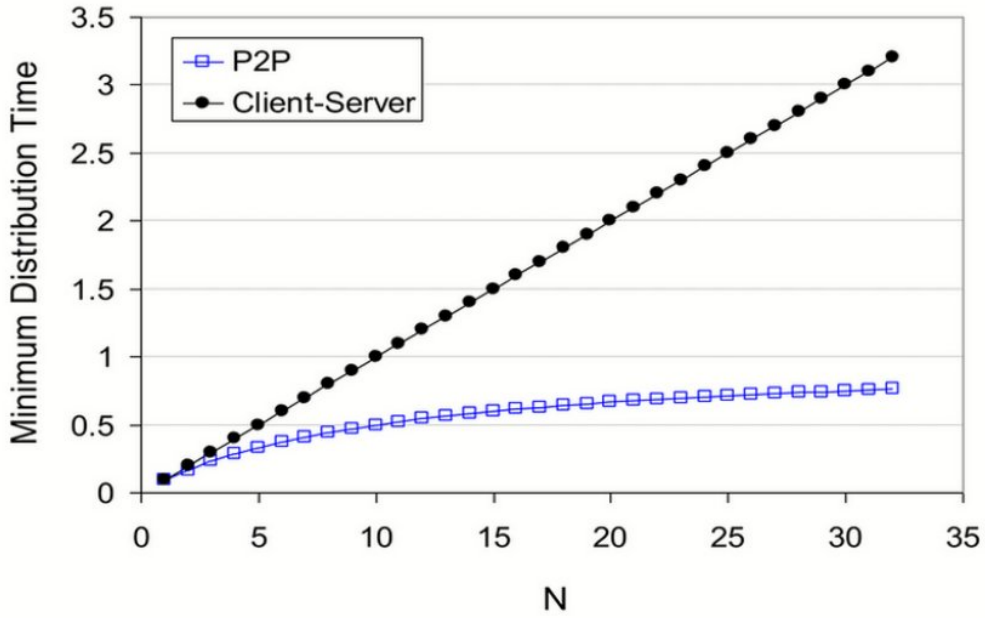
زمان توزیع فایل در مدل P2P

- زمان ارسال سرور : باید حداقل یکبار فایل را آپلود کند
  - زمان ارسال یک کپی: F/u_s (کمترین زمان توزیع حداقل این مقدار خواهد بود)
- نظیر : نظیری که کمترین نرخ دانلود را دارد نمی‌تواند فایل را در زمانی کمتر از F/d_{min} دریافت کند (کمترین زمان توزیع حداقل این مقدار خواهد بود)
- ظرفیت آپلود کل سیستم برابر است با :
  - $u_s + \Sigma u_i$
- در مجموع NF بیت در این سیستم جابجا می‌شود
  - کمترین زمان توزیع ($NF/(u_s + \Sigma u_i)$ خواهد بود

زمان توزیع فایلی با اندازه **F** روی **N** کلاینت با مدل **P2P** : $D_{P2P} > max\{F/u_s, F/d_{min}, NF/(u_s + \Sigma u_i)\}$

Client-server vs. P2P

client upload rate = u, F/u = 1 hour, $u_s = 10u$, $d_{min} \geq u_s$

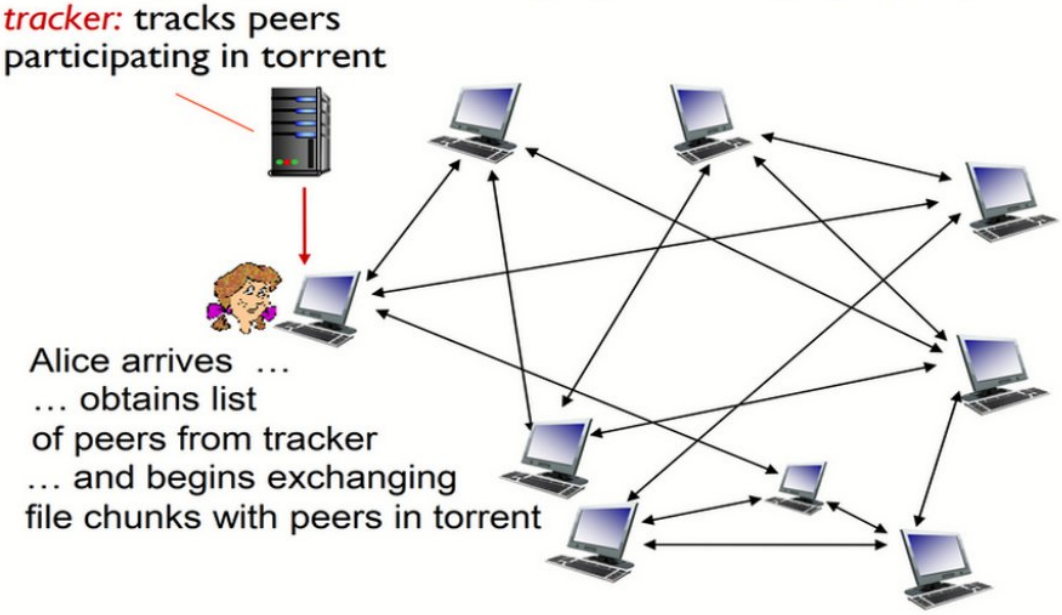


- در معماری client-server با افزایش تعداد N زمان توزیع بصورت خطی افزایش می‌یابد، ولی در معماری P2P به ازای هر تعداد نظیر این زمان هرگز از یک ساعت فراتر نمی‌رود
- برنامه‌های کاربردی P2P می‌توانند خود مقیاس پذیر باشند

Scanned with CamScanner

P2P file distribution: BitTorrent

- تورنت : مجموعه تمامی نظیرهایی که در توزیع یک فایل مشخص شرکت می‌کنند
- فایل به قطعاتی به اندازه یکسان ۲۵۶ کیلو بایتی تقسیم می‌شوند
- نظیرها داخل تورنت این قطعات را ارسال و دریافت می‌کنند
- یک نظیر همزمان که در حال گرفتن قطعات خودش هست، قطعات مورد نیاز نظیرهای دیگر را ارسال می‌کند



P2P file distribution: BitTorrent

- هر تورنت یک گره بنام Tracker دارد که اطلاعات تمامی نظیرهای فعال در تورنت را نزد خود دارد
- هنگامی‌که یک نظیر به تورنت می‌پیوندد
  - هیچ قطعه‌ای از فایل را ندارد، اما قطعات را در گذر زمان از نظیرها جمع آوری می‌کند
  - خود را نزد Tracker ثبت می‌کند و در فواصل معین حضور خود در تورنت را به آن اطلاع می‌دهد
  - سپس Tracker از مجموعه نظیرهای این تورنت زیرمجموعه‌ای را بصورت تصادفی انتخاب می‌کند و آدرس IP آنها را برای نظیر می‌فرستد
  - این نظیر سعی می‌کند با نظیرهای این لیست اتصال TCP برقرار کند
    - به نظیرهایی که این نود موفق می‌شود با آنها اتصال TCP برقرار کند neighboring peers گفته می‌شود
- یک نظیر ممکن است در طول زمان نظیرهایی که با آنها قطعه رد و بدل میکند را عوض کند
- نظیرها می‌آیند و می‌روند

Scanned with CamScanner

درخواست و ارسال قطعات فایل

درخواست قطعات

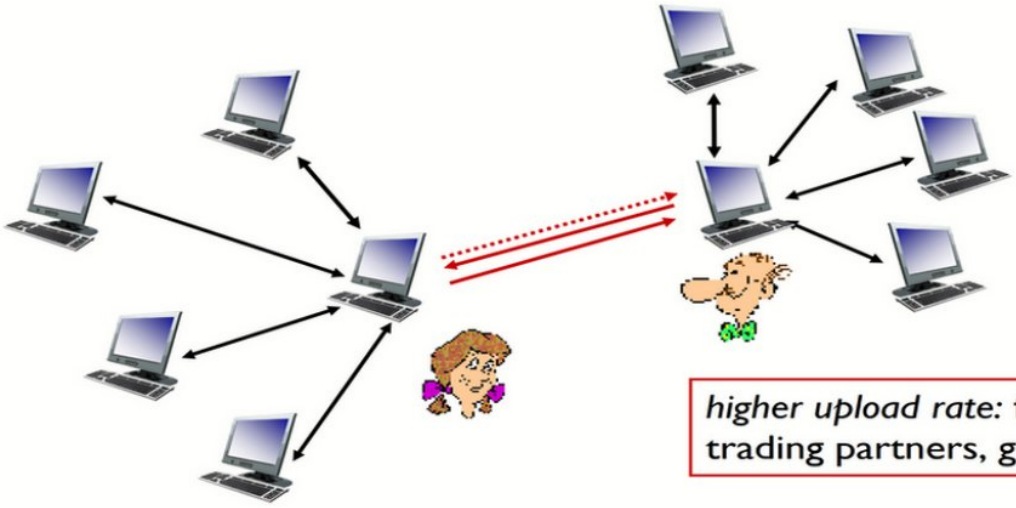
- در هر لحظه از زمان نظیرهای مختلف مجموعه‌ای از قطعات مختلف را دارند
- در فواصل منظم درخواست کننده از نظیرها می‌پرسد که چه قطعاتی را دارند
- درخواست کننده با الگوریتم RAREST FIRST قطاتی که ندارد را از نظیرها درخواست می‌کند
- با این روش قطعات نایاب با سرعت بیشتری بین نظیرها مبادله می‌شود

ارسال قطعات : tit-for-tat

- نظیری که قصد ارسال دارد قطعات را به چهارتا از نظیرهایی که در حال حاظر بیشترین نرخ ارسال به آن را دارند ارسال می‌کند
  - دیگر نظیرها را نادیده می‌گیرد (choke می‌کند)
  - ۴ تای برتر هر ۱۰ ثانیه یکبار مجدد محاسبه می‌شود
- هر ۳۰ ثانیه یکبار یک نظیر شانسی انتخاب می‌کند
  - optimistically unchoke(خوشبینانه نامسدود)
  - ممکن است به جمع ۴ تای اول بپیوندد

tit-for-tat

(1) Alice "optimistically unchokes" Bob
(2) Alice becomes one of Bob's top-four providers; Bob reciprocates
(3) Bob becomes one of Alice's top-four providers



higher upload rate: find better trading partners, get file faster !

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

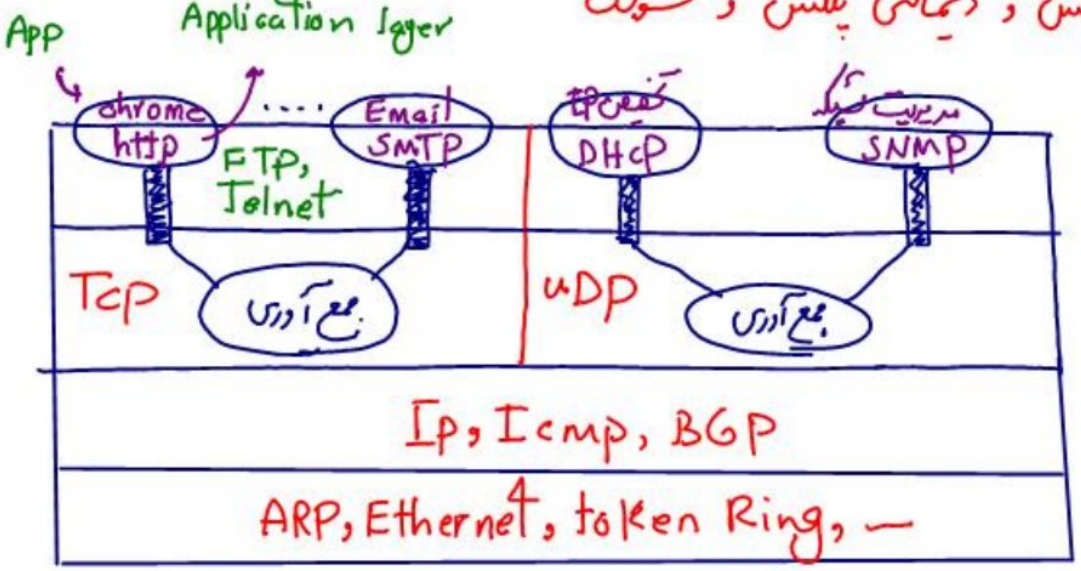
@konkurcomputer
www.konkurcomputer.ir

فصل ۳: لایه انتقال

مرور

- وظیفه پروتکل لایه انتقال ایجاد یک ارتباط منطقی بین فرآیندهای برنامه های اجرا شده روی ماشین های شبکه است
- وظیفه پروتکل لایه شبکه ایجاد یک ارتباط منطقی بین Host ها (میزبان ها) است.
- کلیدی ترین سرویس ان که یک پروتکل لایه انتقال باید به لایه App بدهد
  ۱- تحویل داده فرآیند به فرآیند (multiplexing & Demux)
  ۲- تشخیص خطا
- پروتکل Ip که پروتکل لایه شبکه در اینترنت است یک سرویس connection less ، unreliable ان است که نه حداقل گذردهی ، نه حداقل تاخیر و حداقل jitter و نه امنیت را تضمین نمی کند و در واقع یک سرویس best effort را در اختیار لایه بالاتر قرار میدهد ، حال با وجود اینکه لایه شبکه هیچ گارانتی در موارد بالا به ما نمی دهد ، لایه انتقال می تواند سرویس reliable و امن در اختیار لایه بالاتر قرار بدهد . ولی همچنان لایه انتقال نمی تواند حداقل گذردهی و تاخیر و jitter را تضمین کند

حالتی پکلس و دیمالتی پلکس و سوکت



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

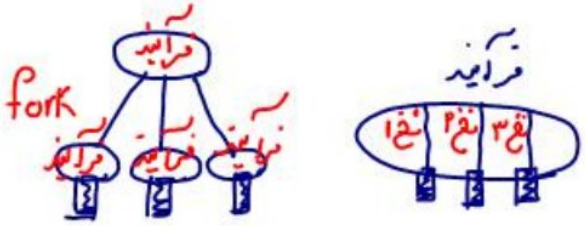
- یک App (فرآیند) وقتی می‌خواهد یک داده را به لایه انتقال بدهد یک چیزی درست می‌کند به اسم سوکت و به هر سوکت یک شناسه خاص اختصاص داده می‌شود

سوکت - دریچه‌ای است که یک فرآیند یا یک نخ، داده‌های خود را از آنجا به لایه انتقال میدهد و یا داده‌های دریافتی را در مقصد از لایه انتقال می‌گیرد

* حال بعنوان مثال وقتی در یک مرورگر چند تب باز می‌کنیم، مرورگرها به ۲ صورت می‌تونند عمل کنند

۱- فرآیند اصلی به ازای هر تب با استفاده از fork یک فرآیند فرزند ایجاد می‌کند

۲- " " " یک نخ درست می‌کند



نکته) به هرحال هر تب چه یک فرآیند جداگانه باشد و چه یک نخ جدا سوکت جداگانه و شماره سوکت خودش را دارد

نکته - یک فرآیند می‌تواند یک یا چند سوکت داشته باشد

نکته - هر سوکت باید یک شناسه منحصر به فرد داشته باشد تا لایه انتقال بداند که در مقصد داده را به کدام فرآیند لایه App تحویل بدهد. ← برای ایجاد یک شناسه منحصر به فرد برای هر سوکت نیاز شد تا شماره پورت مبدا و مقصد هم اضافه شود.

نکته: شماره پورت ۱۶ بیتی است، بنابراین رنج شماره پورت بین ۰ تا $2^{16}-1$ است یعنی ۰ تا ۶۵۵۳۵ (۶۴K).

* شماره پورت‌های ۰ تا ۱۰۲۳ (۰ تا ۱K) به برنامه‌های معروف معمولاً سمت سرور اختصاص دارند و به اینها well Known می‌گویند

نکته: شماره پورت‌های معمول (۱K تا ۶۴K) به ۲ صورت می‌تواند به یک سوکت داده شود

۱- بصورت اتوماتیک و توسط OS (لایه انتقال)

۲- بصورت دستی، و با استفاده از متد bind

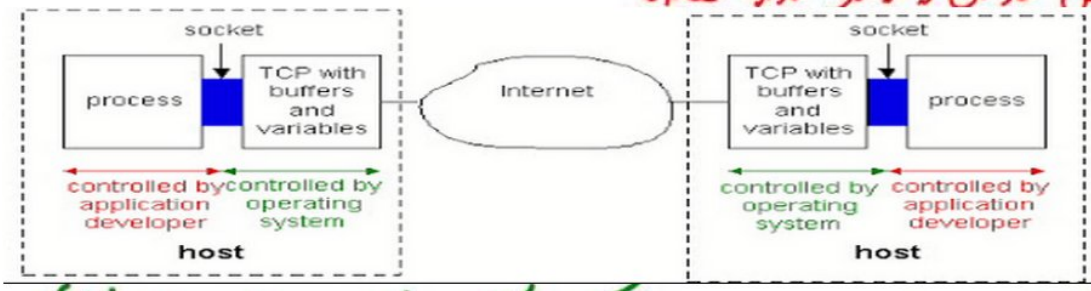
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

نکته: سوکت در واقع یک واسط برنامه نویسی است که برنامه های شبکه با آن نوشته می شوند، یعنی همین به سوکت Api (Application programming interface) یا واسط برنامه نویسی کاربردی) نیز می گویند

یک سوکت دو سمت دارد: ۱- سمت لایه کاربرد سوکت ۲- سمت لایه انتقال سوکت

- در سمت لایه کاربرد سوکت هم چیز تحت کنترل برنامه نویس است
- بر ... انتقال ... برنامه نویس کنترل ناچیزی دارد. در این سمت برنامه نویس فقط کنترل ۲ مورد را می تواند داشته باشد ۱- از کدام پروتکل انتقال استفاده کند ۲- تعیین برخی از پارامترهای لایه انتقال مثل حداکثر حجم بافر و حداکثر اندازه قطعه ها



برنامه هایی که از Tcp و UDP استفاده می کنند چگونه به کلاینت های خود سرویس می دهند

UDP: شروع یک اتصال UDP با client است، اما سرویس دهنده UDP باید از قبل به صورت یک فرآیند روی سرور در حال اجرا باشد تا مشتری بتواند تماس را شروع کند. در برنامه هایی که از پروتکل UDP استفاده می کنند، برنامه سمت سرور **نمی خوابد** روی درخواست های client های مختلف هیچ کنترلی داشته باشد، بنابراین سرور **نیازی ندارد** که بین اینها تمایزی قائل شود و سرور UDP هم درخواست ها را به یک چشم می بیند. بنابراین برای سرور UDP فرقی نمی کند که درخواست ها از کامپیوتر A آمده است یا B.

Tcp: شروع یک اتصال Tcp با client است، اما سرویس دهنده Tcp باید از قبل به صورت یک فرآیند روی سرور در حال اجرا باشد تا مشتری بتواند تماس را شروع کند. در برنامه هایی که از پروتکل Tcp استفاده می کنند، برنامه سمت سرور **می خوابد** روی تک به تک درخواست های client های مختلف کنترل داشته باشد، بنابراین سرور **نیاز دارد** که بین اینها تمایز قائل شود

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

به همین علت است که :

* یک سوکت app با دو شش‌ضلعه مشخص می‌شود ① آدرس Ip مقصد
② شماره پورت مقصد

* یک سوکت Tcp با چهار مشخصه مشخص می‌شود ① و ② شماره پورت فرآیندهای مبدا و مقصد
③ و ④ Ip های مبدا و مقصد

همچنین به همین علت است که در Tcp :
به ازای هر سوکت بافر و متغیرهای کنترلی آن در client و server نگهداری می‌شود (داریم)

نحوه برقراری ارتباط مشتری و سرویس دهنده در یک برنامه Tcp

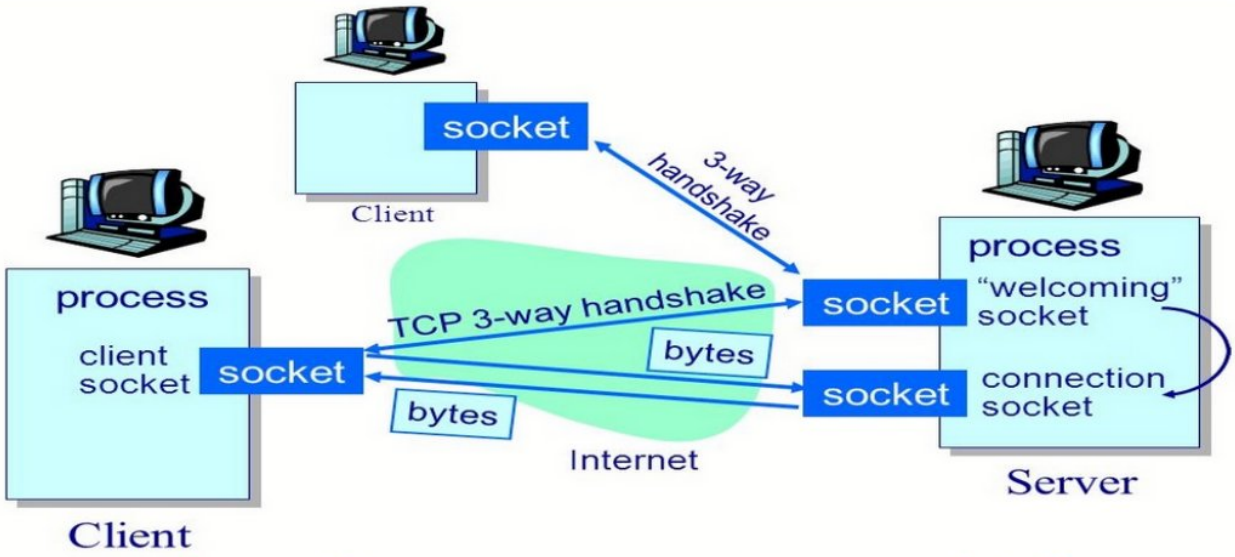
سرویس دهنده Tcp قبل از درخواست مشتری بصورت یک فرآیند روی سرور در حال اجرا است
همچنین یک سوکت به نام welcoming socket (سوکت پذیرنده) برای دریافت و اگر صلاح دانست پذیرش ارتباط آغازین مشتری دارد.
وقتی مشتری می‌خواهد یک ارتباط Tcp را با سرور ایجاد کند یک segment درخواست برقراری اتصال به سمت سرور ارسال می‌کند در این segment ، شماره پورت مقصد شماره پورت سوکت پذیرنده و همچنین SYNbit = 1 و همین طور یک شماره ترتیب رندم برای قطعه قرار داده شده است
حال وقتی os سروری که فرآیند سرویس دهنده روی آن در حال اجرا است این قطعه را می‌گیرد با توجه به شماره پورت بسته آن را به یکی از فرآیندهایی که هنگی روی پورت های پذیرنده‌شان منتظر دریافت درخواست اتصال هستند ارسال می‌کند و فرآیند سرویس دهنده اگر صلاح دانست یک سوکت جدید برای این اتصال به نام connection socket ایجاد می‌کند و یک پاکت (مشخصه) با استفاده از ع پارامتری که تبلا گفتیم به این سوکت می‌دهد ، حال پس از این وقتی سایر segment ها به لایه انتقال می‌رسند لایه انتقال با بدست آوردن این مشخصه ، segment را به سوکت مربوط دیمالتی پلکس می‌کند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

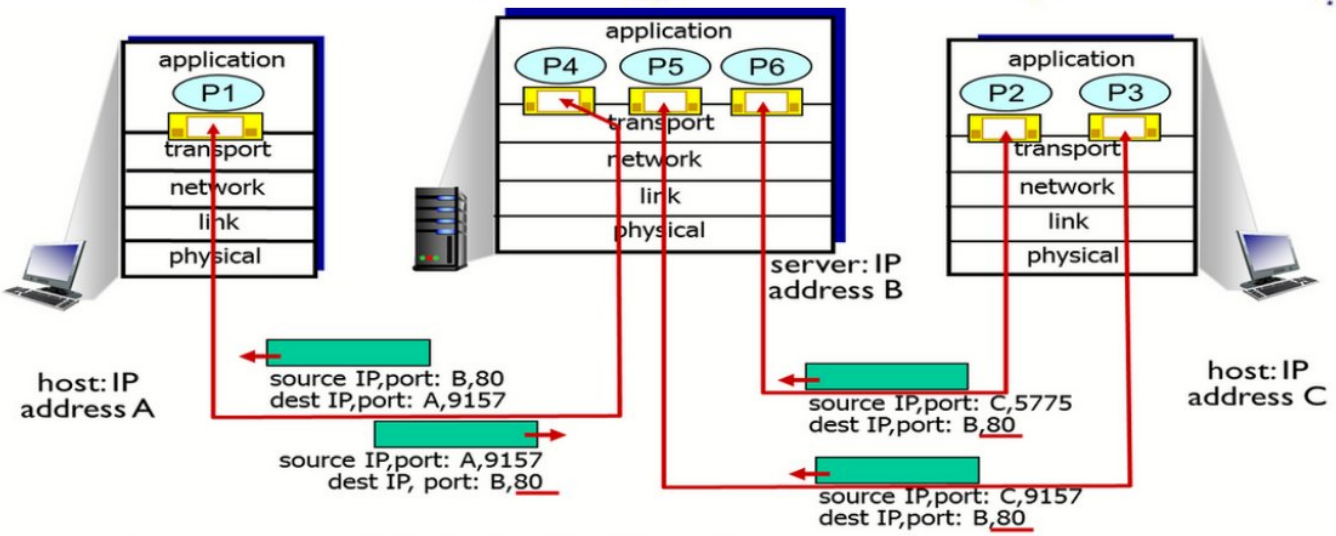
شبکه های کامپیوتری

رامین رضوی



حال بررسی می‌کنیم که چرا TCP به چهار پارامتر برای مشخص کردن هر سوکت نیاز دارد

فرض کنید دو کلاینت A و C و یک سرور B داریم، هر دو کلاینت A و C، از سرور B صفحات وب را می‌خواهند. کلاینت C ۲ درخواست و کلاینت A ۱ درخواست دارد



three segments, all destined to IP address: B,
dest port: 80 are demultiplexed to *different* sockets

سوال ۱- آیا سرور می‌تواند بین این سه انتقال فقط با استفاده از IP و شماره پورت مقصد تمایز قائل شود؟ خیر. در این مثال هر ۳ درخواست IP و پورت مقصد شان یکسان است

سوال ۲- آیا سرور می‌تواند بین این سه درخواست با استفاده از IP و شماره پورت مقصد و همچنین IP مبدا تمایز قائل شود؟ خیر- چون در اینصورت نمی‌توان بین P_2 و P_3 تمایز قائل شد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

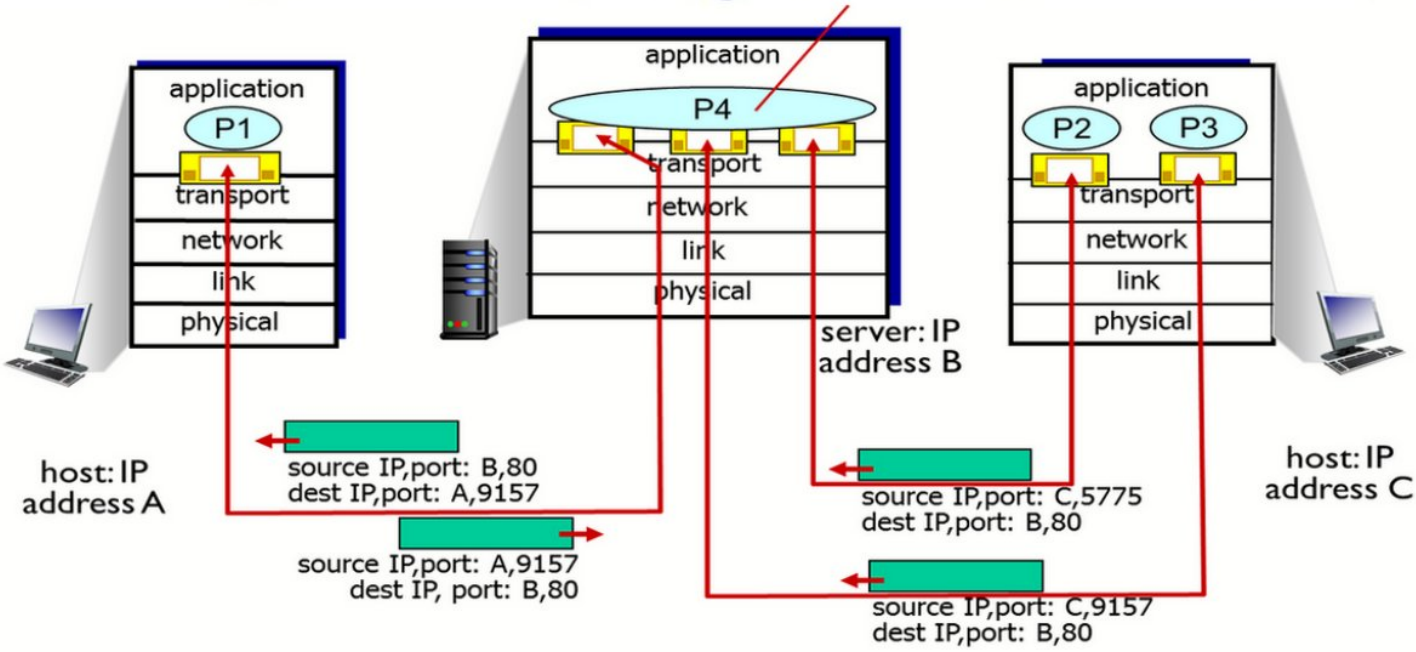
@konkurcomputer
www.konkurcomputer.ir

سوال ۳ - آیا سرور می‌تواند بین این سه درخواست با استفاده از IP و شماره پورت مقصد و همچنین پورت مبدا تمایز قائل شود؟ خیر - چون در اینصورت نمی‌توان بین P_1 و $P_{2,3}$ تمایز قائل شد

نتیجه: برای تفکیک اتصالات Tcp نیاز هست که هر سوکت با ۴ مولفه مشخص شود

نکته ۱: برخلاف UDP در شبکت Tcp ورودی به یک سرور که دارای آدرس IP یا پورت مبدا متفاوت هستند، اما IP و پورت مقصد یکسان دارند به ۲ سوکت مختلف هدایت می‌شوند البته شبکت های Tcp درخواست برقرار اتصال این ۲ پروسس به یک سوکت هدایت می‌شوند

نکته ۲) لزوما بین سوکت های اتصال و فرآیندهای سرویس دهنده تناظر یک به یک برقرار نیست، اتفاقا در سرویس دهنده های وب امروزی این چنین است و در این سرویس دهنده ها یک فرآیند دایم که برای هر درخواست جدید مشتری ها یک نخ جدید با یک سوکت اتصال جدید می سازد

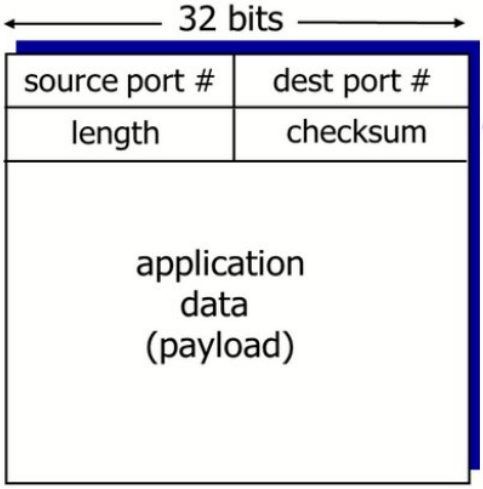


نکته ۳ - در وب بهتر است Http از اتصال Tcp پایا استفاده کند، زیرا ایجاد و بستن سوکت ها به تعداد دفعات بسیار بالا (به ازا هر جفت درخواست / پاسخ) باعث افت شدید کارایی سرور می‌شود

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

UDP Header



UDP segment format

هدر UDP هشت بایت است که از ۴ تا ۲ بایت تشکیل شده.

- فیلد طول قطعه (length) طول کل قطعه شامل payload و هدر را نشان می دهد و چون ۱۶ بیت است بنابراین حداکثر سایز قطعه UDP 2^{16} Byte = ۶۴KB است.
- فیلد طول قطعه، برحسب بایت است.

فیلد checksum در UDP: (جمع کنترلی UDP)

تمامی محتوا قطعه شامل هدرش را با استفاده از جمع مکمل ۱ جمع می کنیم، در جمع مکمل یک کری مجددا با حاصل جمع می شود. جمع ها بصورت دو بایتی انجام می شود. ابتدا دو بایت اول با دو بایت دوم جمع می شود و حاصل به وجود می آید، سپس دو بایت بعدی با حاصل جمع می شود و الی آخر پس از بدست آوردن جمع نهایی checksum می شود مکمل یک این جمع، که به همراه سگمنت ارسال می شود، حال دریافت کننده تمامی بایت ها سگمنت باهم جمع زده می شود و اگر حاصل ۲ بایت تمام ۱ شد حاصل را درست می گیریم و در غیر اینصورت حاصل را غلط می گیریم

مثال: جمع کنترلی سه کلمه ۱۶ بیتی زیر را بدست آورید

۱- ۰۱۱۰۰۱۱۰۰۱۱۰۰۰۰۰
۲- ۰۱۰۱۰۱۰۱۰۱۰۱۰۱۰۱
۳- ۱۰۰۰۱۱۱۱۰۰۰۰۱۱۰۰

ابتدا ۱ و ۲ را جمع می کنیم

```
  0 1 1 0 0 1 1 0 0 1 1 0 0 0 0 0
+ 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
-----------------------------------
  1 0 1 1 1 0 1 1 1 0 1 1 0 1 0 1
```

← جمع کننده مکمل ۱: یعنی اگر کری داشتیم کری را مجددا با حاصل جمع می کردیم

```
  1 0 1 1 1 0 1 1 1 0 1 1 0 1 0 1
+ 1 0 0 0 1 1 1 1 0 0 0 0 1 1 0 0
-----------------------------------
1 0 1 0 0 1 0 1 0 1 1 0 0 0 0 0 1
↳ 1
-----------------------------------
  0 1 0 0 1 0 1 1 0 0 0 0 0 1 0
```

مشخص است که جمع یک عدد با مکمل یک اش برابر تمام ۱ می شود، بنابراین وقتی دریافت کننده هم را جمع می زنیم باید تمام ۱ شود

⇐ مکمل ۱ این می شود checksum

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

* وکنش گیرنده UDP نسبت به بسته های خراب به نحوه پیاده سازی اش بستگی دارد و ۲ وکنش داریم
۱. بسته خراب را دور می اندازد
۲. " " " به همراه یک اخطار به فرآیند لایه کاربرد مقصد تحویل می دهد

چگونگی انتقال داده قابل اطمینان روی بستر نامطمئن

- در یک انتقال داده قابل اطمینان ما می خواهیم ۱- بسته ها حتما به مقصد برسند و loss نداشته باشیم ۲- بسته هایی به به مقصد تحویل داده می شوند خطا نداشته باشند و error نداشته باشند ۳- قطعات تکراری را به مقصد تحویل ندهیم (No replicate) ۴- قطعات را به ترتیب به مقصد بدهیم
- طراحی یک پروتکل انتقال داده قابل اطمینان و آشنایی با ملزومات آن فقط برای لایه انتقال مهم نیست و برای لایه های App و Data link هم مهم است

* ما می خواهیم آهسته آهسته به سمت طراحی پروتکلی برای این منظور بگیریم که هر ۴ مورد بالا را انجام بدهد برای همین کم کم فرضیات متعی را به پروتکل ابتدایی مان اضافه می کنیم و کم کم پروتکل مان را کامل می کنیم

در مرحله اول که خود شامل ۵ بار طراحی تا رسیدن به نسخه نهایی است ما می خواهیم یک پروتکل stop & wait یا Alternate bit (پروتکل بیت تناوبی یا بیت متناوب) بسازیم، در این پروتکل فرستنده یک بسته را می فرستد و تا وقتی از رسیدن یا نرسیدن آن مطمئن نشود (ack یا nak اش بهرستی به گیرنده نرسد) کاری نمی کند، اگر Ack بسته ارسالی برسد این روش بسته جدید را ارسال می کند و اگر به گیرنده NAK برسد و یا Ack و NAK خراب برسد و یا time out رخ بدهد فرستنده بسته ارسال شده قبلی را مجددا ارسال می کند

نکته) چون پروتکل ما S&W است از ۴ حالت بدی که می تواند برای بسته ها رخ دهد، حالتی که ترتیب بسته ها در گیرنده بهم بریزد را در این ۵ ورژن نخواهیم داشت

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

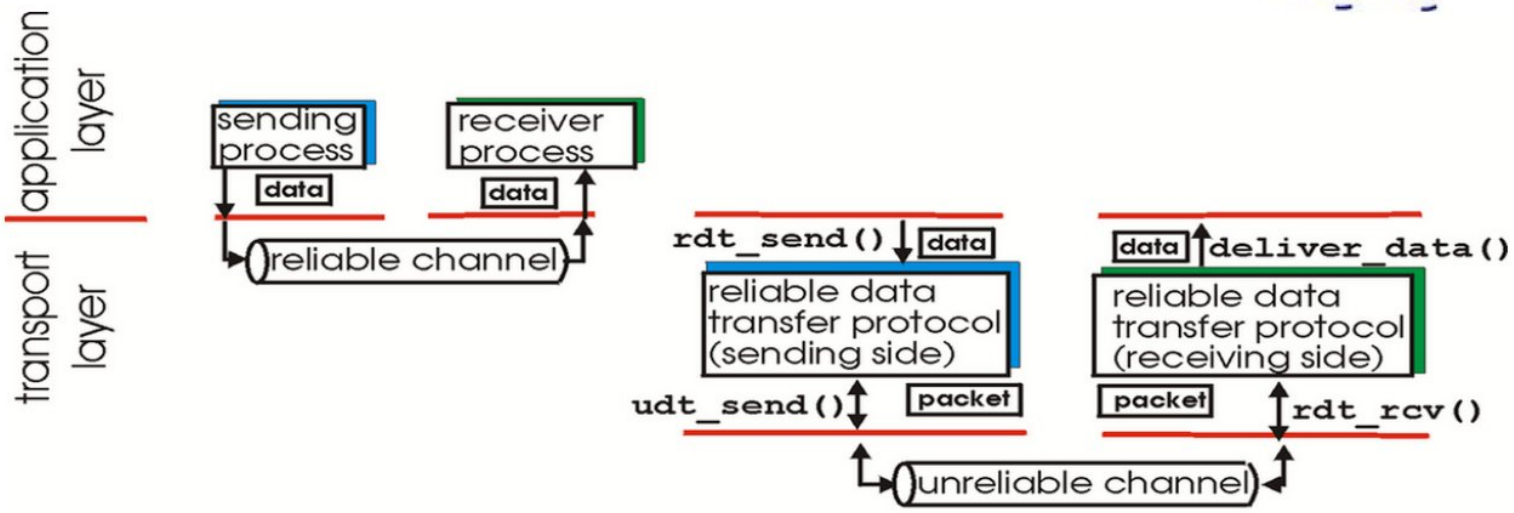
نکته) با توجه به توضیحات داده شده در پروتکل SAW اندازه بافر فرستنده و گیرنده ۱ بسته بالا کافی است.

قانون ۱ : این قانون کلی است : در هر لایه گیرنده باید بسته ها را به ترتیب تحویل لایه بالاتر دهد

پروتکل یک لایه چگونه پروتکل لایه دیگر را صدا می زند و به آن داده می دهد

- در فرستنده هر لایه بالاتر لایه پایین تر را صدا میزند و در گیرنده هر لایه پایین تر لایه بالاتر را صدا می زند

- در شکل b در سمت گیرنده لایه شبکه با تابع rdt_rcv() بسته ها را به لایه انتقال می دهد و لایه انتقال اگر بسته ها درست و به ترتیب بود آنها را با استفاده از تابع deliver_data() تحویل پروسس گیرنده میدهد



(a) provided service (b) service implementation

شروع به طراحی پروتکل SAW

* ما ۳ فرض به داریم : ۱- بسته ها دچار خطا شوند ۲- بسته ها گم شوند ۳- replicate

به ترتیب این فرض ها ب را در نظر می گیریم

ورژن ۱ : rdt 1.0 : فرض می کنیم کانال زیرین مطمئن باشد ⇐ نتیجه : نیازی نیست

بررسی کنترل خطا کاری کنیم ، پس نه نیاز به checksum داریم نه نیاز به اینکه گیرنده Ack یا NAK بدهد ، همچنین در اینجا چون بسته ارسالی قطعا درست به مقصد می رسد replicate نیز در گیرنده نداریم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

در این ورژن فقط مالتی پلکسینگ و دیمالتی پلکسینگ لایه انتقال را مشاهده می کنیم.
همچنین در اینجا فرض کردیم که فرستنده با هر سرعتی بسته ها را ارسال کند گیرنده می تواند آنها را بدون مشکل دریافت کند بنابراین نیازی به کنترل جریان نداریم و گیرنده لازم نیست در این خصوص به فرستنده

sender receiver

ورژن ۲: rdt ۲٫۰ : فرض می کنیم داده ای که فرستنده به گیرنده می فرستد می تواند دچار خطا بشود ولی داده ای که گیرنده به فرستنده می فرستد (Ack و NAK) خراب نمی شود

نتیجه: برای داده ها ارسال نیاز به checksum داریم، همین طور نیاز داریم که گیرنده به فرستنده Ack و NAK بدهد. روی Ack و NAK نیاز نیست checksum بذاریم. همچنین replicate نداریم ← زیرا یا بسته درست به گیرنده رسیده است که گیرنده آن را به لایه بالاتر میدهد و به فرستنده Ack می فرستد و Ack هم سالم به دست فرستنده می رسد و بنابراین فرستنده بسته بعدی را می فرستد و یا بسته با خطا به گیرنده رسیده که گیرنده آن را دور می اندازد و به فرستنده NAK میدهد و NAK سالم به فرستنده می رسد و فرستنده مجددا بسته را ارسال می کند

نکته ۱: خطا روی یک بسته می تواند در هنگام عبور یک بسته از روی لینک ها در تبادل و یا هنگام ذخیره شدن در روترها رخ بدهد

نکته ۲: در حالتی که بسته ها دچار خرابی می شوند ما نیاز داریم که گیرنده بتواند خطا را تشخیص بدهد و درست یا غلط رسیدن بسته ها به خودش را به فرستنده اعلام کند و فرستنده نیز امکان ارسال مجدد برای گیرنده را داشته باشد که به این ساز و کار ارسال مجدد می گویند، در شبکه به پروتکل هایی که از این روش استفاده می کنند پروتکل های ARQ (Automatic Repeat request protocol) (پروتکل درخواست تکرار خودکار) می گویند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

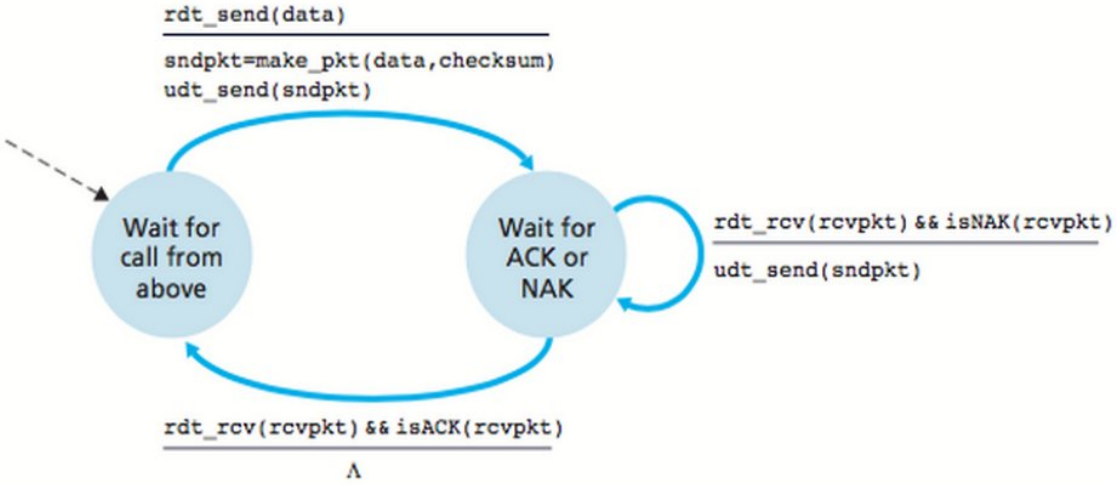
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir
شبکه های کامپیوتری
رامین رضوی

یک پروتکل ARQ برای مقابله با error باید ۳ تا قابلیت را داشته باشد

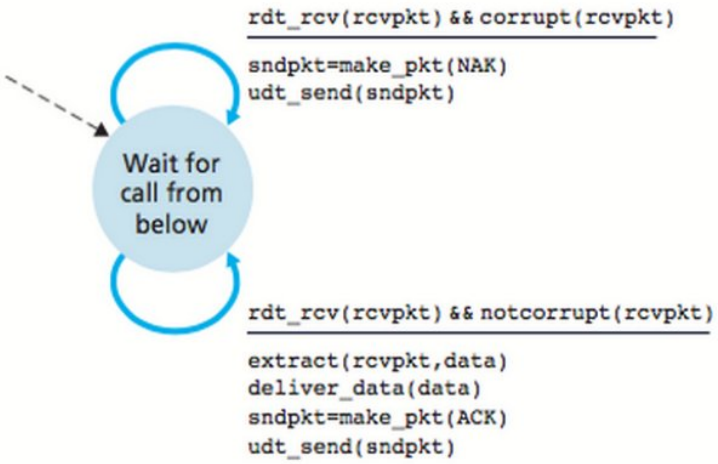
۱- تشخیص خطا دریافت کننده (error detection) ← مثلا استفاده از checksum

۲- بازخورد گیرنده به فرستنده (feedback) ← استفاده از ACK, NAK یا شماره دار

۳- ارسال مجدد: تصحیح رو به عقب (BEC) : درصورت اینکه NAK برای فرستنده بیاید فرستنده باید مجددا بسته را ارسال کند



a. rdt2.0: sending side



b. rdt2.0: receiving side

rdt2.0–A protocol for a channel with bit errors

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

ورژن ۳ ـ rdt 2.1 : Ack و NAK نیز می‌تواند خراب بشود ← نتیجه : برای Ack و NAK نیز باید checksum بگذاریم ⇐ برای مقابله با Ack و NAK خراب فرستنده چه راه کاری دارد ؟ ۳ راه کار متصور است که نشان می دهیم دو راه کار ایراد دارد

۱ـ با فرستادن NAK به گیرنده بهش بگوییم چه گفتی و دوباره بیام اث (Ack یا NAK ات) را ارسال کن ، اما اگر NAK ای که ما نیز به سمت گیرنده می فرستیم خراب شود ، این بار گیرنده با NAK به ما می گوید چه گفتید و بنابراین ممکن است در لوپ بیفتیم .

۲ـ استفاده از تصحیح خطا رو به جلو (پیش رونده) (FEC) ، مثل کد همینگ یا ...

این روش دو عیب دارد ۱ـ سربار زیادی دارد ، مثلا در parity که BEC است بایران تمامی بیت ها یک بیت اضافه می کنیم ولی در همینگ برای ۴ بیت ۳ بیت افزونگی اضافه می کنیم

۲ ـ اگر loss رخ بدهد این روش کار نمی کند (درست است که در این ورژن loss نداریم ولی در ورژن های بعدی می خواهیم loss را اضافه کنیم پس باید حواسمان به این مورد نیز باشد)

*۳ـ اگر از گیرنده بسته ای گرفتیم که نه Ack بود نه NAK بسته ای که فرستاده بودیم را مجددا ارسال کنیم ، اما این رهیافت مشکل اساسی جدیدی بنام Dublicate packet (Replicate) به وجود می آورد ← چطور ؟ چگونه ؟

فرض کنید فرستنده یک بسته بدون شماره را به گیرنده می فرستد و گیرنده آن را دریافت می کند و آن را به لایه بالاتر میدهد و یک Ack برای فرستنده ارسال می کند ، در اینصورت گیرنده منتظر بسته جدید است . حال فرض کنید که این Ack در وسط راه دچار خطا می شود (یا در ورژن بعدی که loss داریم گم می شود ، وقتی loss داریم برای مقابله با loss تایمر می گذاریم و در این حالت تایمر time out می کند و فرستنده بسته را مجددا ارسال می کند) و با خطا به دست فرستنده می رسد ، در اینصورت فرستنده دوباره بسته بدون شماره قبلی را برای گیرنده ارسال می کند ، در اینصورت گیرنده این بسته را بعنوان یک بسته جدید می گیرد و آن را به لایه بالاتر تحویل می دهد ، در صورتیکه این بسته تکراری بوده و داده یک داده تکراری به لایه بالا و تلقی کردن آن بعنوان یک داده جدید بسیار مضر است .

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

برای حل این مشکل یک فیلد جدید به نام sequence number به بسته‌های داده اضافه می‌کنیم، در اینصورت گیرنده با نگاه کردن به این فیلد می‌تواند تشخیص بدهد که بسته دریافتی حاوی داده جدید است یا یک بسته تکراری است.

برای مشخص کردن شماره ترتیب باید سعی کنیم که تا می‌توانیم تعداد بیت کمتری در نظر بگیریم تا هدر کوچک بماند و سربار زیاد نشود

در سناریو گرفتن یک فیلد 1 بیتی بعنوان عدد توالی بسته‌ها کافی است چون در سناریو گیرنده فقط کافی است که بفهمد بسته‌ای که گرفته جدید است یا بسته قبلی است

مثلاً اگر شماره بسته فعلی که گیرنده دریافت کرده 0 باشد ← 0 باشد ← می‌فهمد بسته تکراری است
اگر شماره بسته بعدی که دریافت می‌کند 1 ← 1 ← 1 ← جدید است

نکته: توجه کنید که تعداد بیت sn را با تعداد شماره آن اشتباه نگیرید

حال اتفاق قبلی که باعث بروز خطا شد را مجددا بررسی می‌کنیم

فرستنده فریم شماره 0 را می‌فرستد و گیرنده بسته 0 را می‌گیرد و آن را به لایه بالاتر تحویل میدهد و یک Ack برای فرستنده می‌فرستد و منتظر دریافت فریم شماره 1 می‌شود، حال Ack خراب شده به فرستنده می‌رسد (یا loss می‌شود و time out رخ میدهد)، بنابراین فرستنده مجددا فریم 0 را می‌فرستد، حال گیرنده فریم 0 را دریافت می‌کند اما چون این فریمی نیست که گیرنده انتظارش را دارد، این بسته را دور می‌ریزد و مجددا یک Ack به فرستنده می‌فرستد

قانون ۲: در سناریوهایی که از Ack و NAK استفاده می‌کنیم نه از Ack شماره دار، اگر گیرنده یک بسته خارج از ترتیب دریافت کند، بسته را دور می‌اندازد و Ack برای فرستنده ارسال می‌کند

نکته: در سناریوهایی که از Ack و NAK استفاده می‌کند فرستنده در ۲ صورت بسته قبل را مجددا ارسال می‌کند
① دریافت NAK ② دریافت یک Ack یا NAK اشتباه * توجه: فعلا loss نداریم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

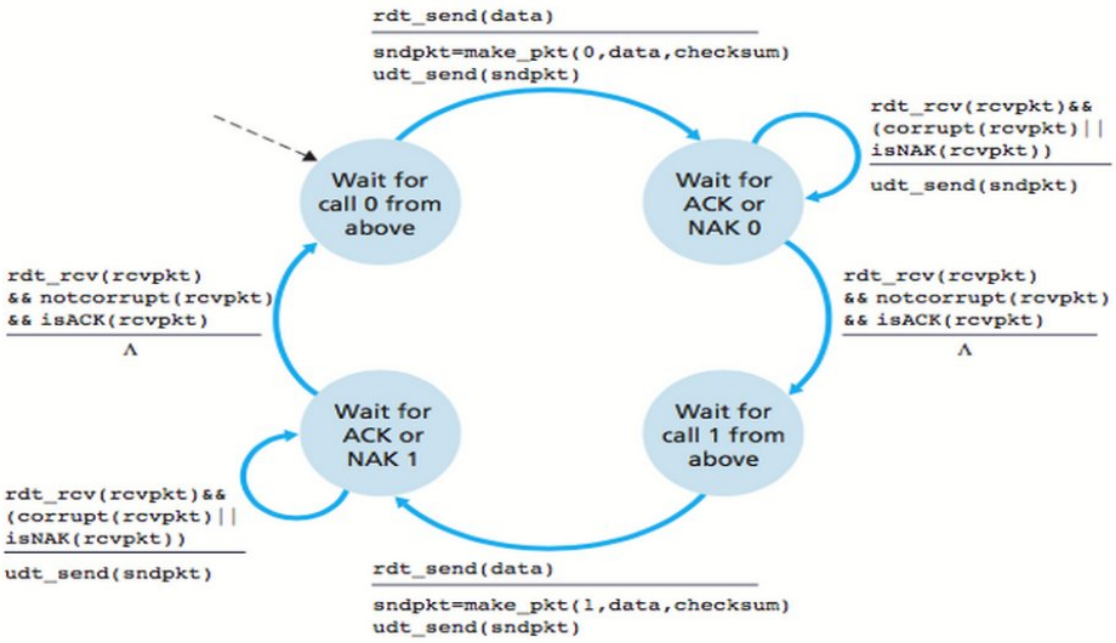
رامین رضوی

نکته) فرستنده تا زمانی که ACK یک بسته را دریافت نکند بسته را در بافرش نگه می‌دارد و به محض اینکه ACK را دریافت کرد بسته را از بافرش پاک می‌کند، البته راس به این نکته اشاره نکرده

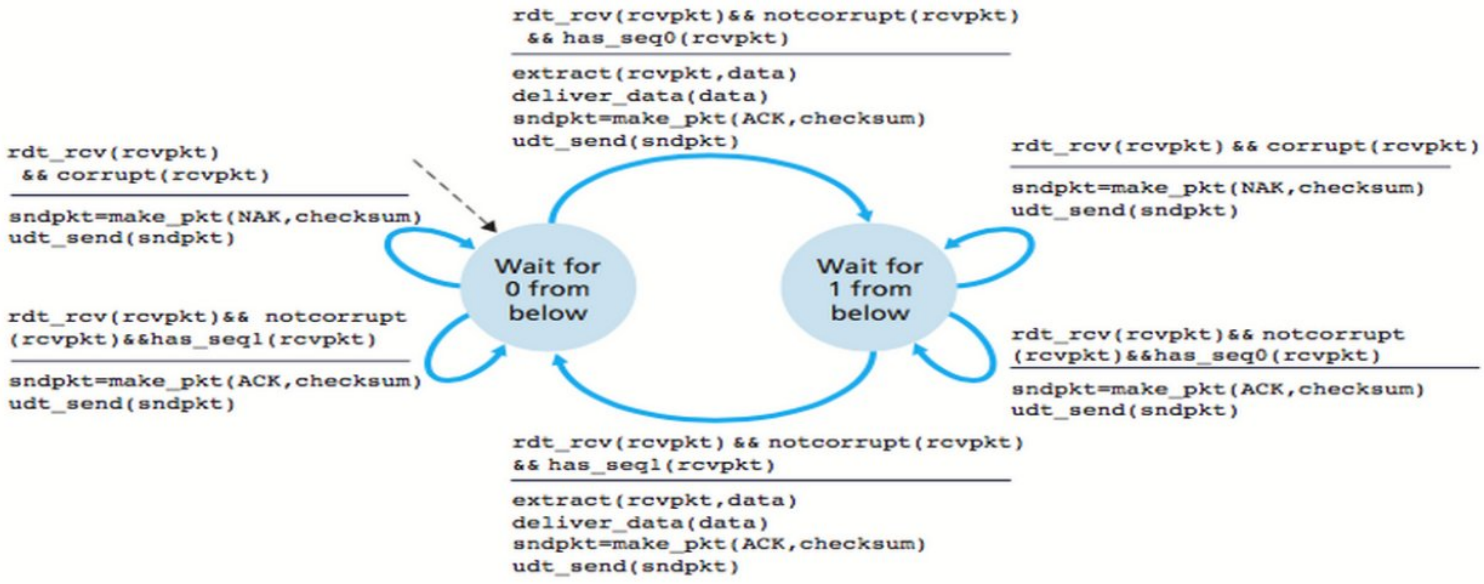
نکته) در این ورژن از ACK و NAK استفاده کردیم، در حالی نیازی نداریم که از ACK و NAK شماره دار استفاده کنیم چون در حالی تا تکلیف یک بسته مشخص نشود سراغ بسته بعدی نمی‌رویم

نکته) گیرنده وقتی که از ACK و NAK استفاده می‌کنیم در ۲ حالت ACK برمی‌گرداند

① یک بسته تکراری دریافت کند ② یک بسته جدید سالم دریافت کند



rdt2.1 sender



rdt2.1 receiver

Scanned with CamScanner

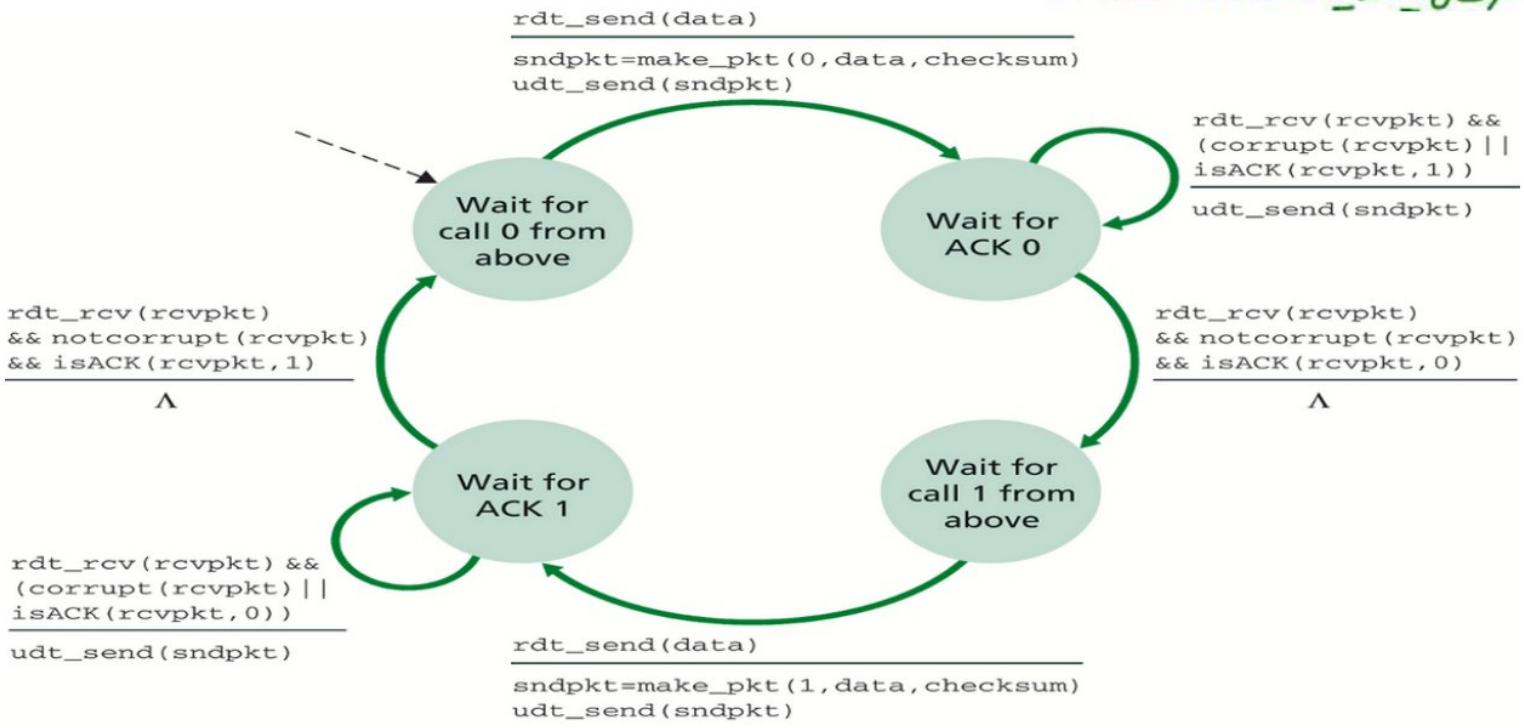
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

ورژن ۲.۲ rdt : فرضیات مان مثل rdt۲.۱ است فقط به جای NAK , AcK از AcK شماره دار استفاده می کنیم

گیرنده با این کار همیشه اعلام می کند که تا کجا را درست گرفته

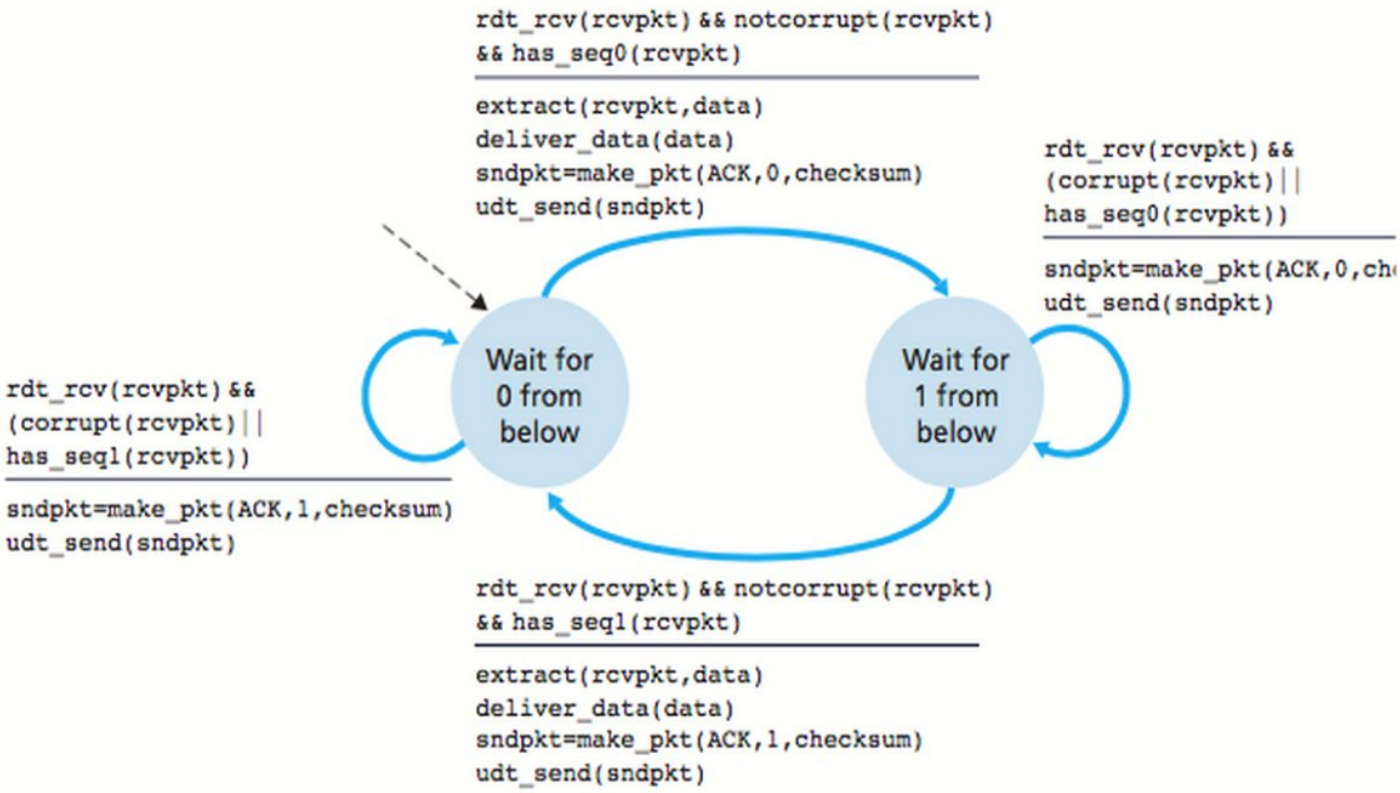
در اینجا گیرنده یک بسته درست با هر شماره ترتیبی را بگیرد Ack با همان شماره را به سمت فرستنده می فرستد ، منظور از درست بودن در اینجا این است که بسته سالم باشد و هم نیت که متعلق به همان بسته که گیرنده منتظرش است . حال اگر گیرنده بسته ای دریافت کند که خطا داشته باشد (corrupt باشد) AcK با شماره NOT آن چیزی که منتظرش است را به سمت فرستنده ارسال می کند ، در واقع دارد Ack آخرین بسته ای که سالم بهش رسیده را برای فرستنده ارسال می کند. فرستنده نیز به این صورت پیاده سازی می شود که اگر فرستنده Ack ای هم شماره با آن چیزی که منتظرش هست را دریافت کند می رود برای ارسال نیم بعدی و اگر یک بسته اشتباه دریافت کند یا Ack ای با شماره ای خلاف آن چیزی که منتظرش هست را بگیرد ، بسته قبلی را مجددا ارسال می کند

قانون ۳ : در این پروتکل فرستادن (توسط گیرنده) و یا گرفتن (توسط فرستنده) AcK خارج از ترتیب به معنا فرستادن و یا گرفتن NAK است . ارسال یا دریافت Ack با شماره تکراری برابر با ارسال یا دریافت NAK است .



rdt2.2 sender

Scanned with CamScanner



rdt2.2 receiver

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

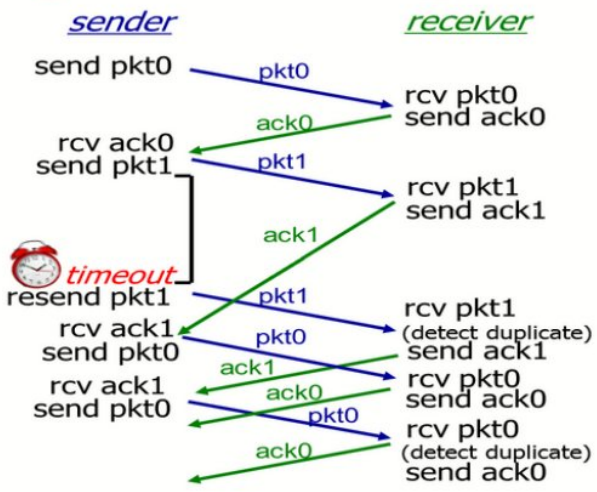
ورژن ۶ : rdt3 : امکان به وجود آمدن loss نیز وجود دارد ← ممکن است بسته ارسالی فرستنده loss شود و اصلا به گیرنده نرسد و بنابراین گیرنده نیز ACK ای برنمی گرداند، یا ممکن است بسته به گیرنده برسد و ACK هم بدهد و این ACK در وسط راه گم بشود ← **نتیجه: باید از timer در فرستنده برای هر بسته استفاده کنیم**

* با این کار بار تشخیص و حل مشکل loss شدن بسته ها را بر دوش فرستنده می گذاریم
- یکی از چالش های قرار دادن تایمر این است که تایمر مکلومن مان را روی چه عددی تنظیم کنیم، در تنظیم تایمر باید به نکات زیر توجه کنیم

۱- عدد تایمر باید بزرگتر از min زمان RTT باشد
۲- " " کوچکتر " max " " " ← تخمین حدالثر تاخیر دشوار است
۳- تنظیم تایمر روی مقدار حدالثر اصلا درست نیست ← هم بسته ها که بدترین حالت را تجربه می کنند با این کار تاخیر انتها به انتها خیلی زیاد می تواند بشود

نکته: وقتی یک بسته time out می شود فرستنده آن بسته را مجددا ارسال می کند در اینصورت ممکن است با مشکل دریافت بسته تکراری در گیرنده مواجه شویم که البته چون seq# داریم مشکلی پیش نمی آید (ACK دو تلفنی شبکه گیر کرده و بعد از time out می رسد)

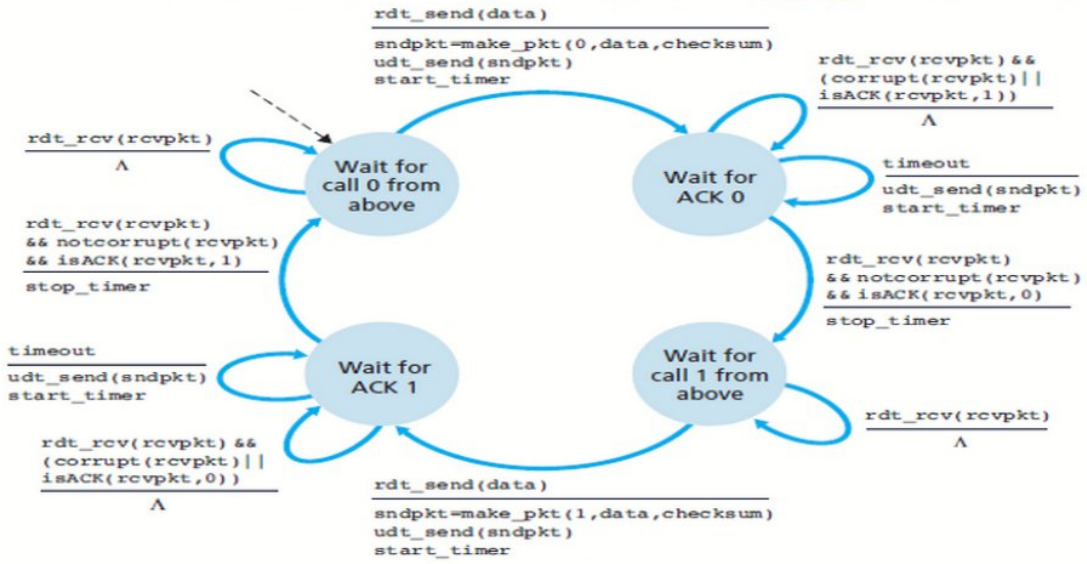
نکته: در این ورژن اگر فرستنده بسته ack را خراب دریافت کند و یا یک ACK خارج از ترتیب دریافت کند همانجا بسته را ارسال مجدد نمی کند و صبر می کند تا time out رخ دهد و وقتی time out رخ میدهد بسته مجددا اتوماتیک ارسال می شود، دلیل این امر را در این شکل می بینید: اولین ack1 که به فرستنده می رسد، فرستنده منتظرش بوده، چون برای pkt1 اولی تایمرمان منقضی شده بود و pkt1 را دوباره فرستاده بودیم فرستنده فکر می کند این ack1 اولی برای pkt1 دومی است، حال به هرحال فرستنده منتظر ack1 بوده و ack1 رسیده بنابراین pkt0 را ارسال می کند بعد یکدفعه مجددا ack1 می آید، خب ما چون منتظر ack0 هستیم این



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند
Scanned with CamScanner

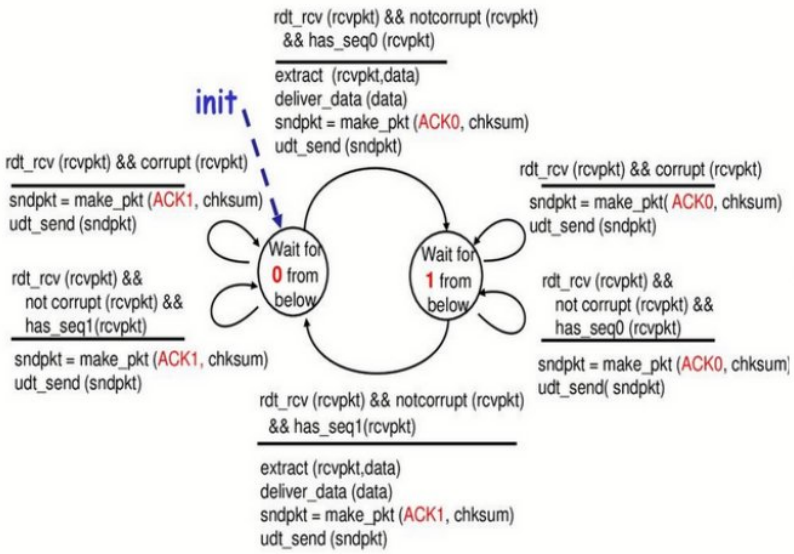
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir
MSc-PhD Computer-IT
شبکه های کامپیوتری
رامین رضوی

ACK1 رسیده برای فرستنده یک ACK خارج از ترتیب محسوب می‌شود. تا حالا ما ACK خارج از ترتیب را به معنا NAK می‌گرفتیم و بسته را مجددا ارسال می‌کردیم، تا حالا فکر می‌کردیم که ACK خارج از ترتیب فقط به این علت رخ میدهد که یا بسته خراب به گیرنده می‌رسد و یا بسته تکراری اما الان می‌فهمیم می‌تواند ACK1 ای باشد که ما فکر می‌کردیم گم شده ولی با تاخیر به فرستنده رسیده است. حالا اگر ما با این ACK مثل قبل رفتار کنیم و همان حالا که دریافت اش می‌کنیم ارسال مجدد انجام بدهیم طبق شکل صفحه قبل همه چی بهم میریزد بنابراین در جاهایی که time out داریم وقتی یک ACK خارج از ترتیب به ما می‌رسد آن قدر می‌ایستیم تا time out رخ بدهد (در واقع هیچ کاری نمی‌کنیم تا تکلیفمان مشخص بشود) و سپس بسته را مجددا ارسال می‌کنیم

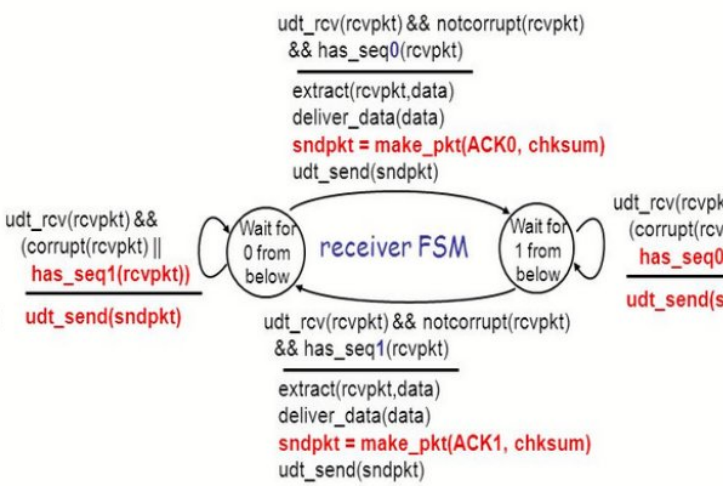


rdt3.0 sender

rdt3.0 : Receiver



rdt3.0: receiver FSM

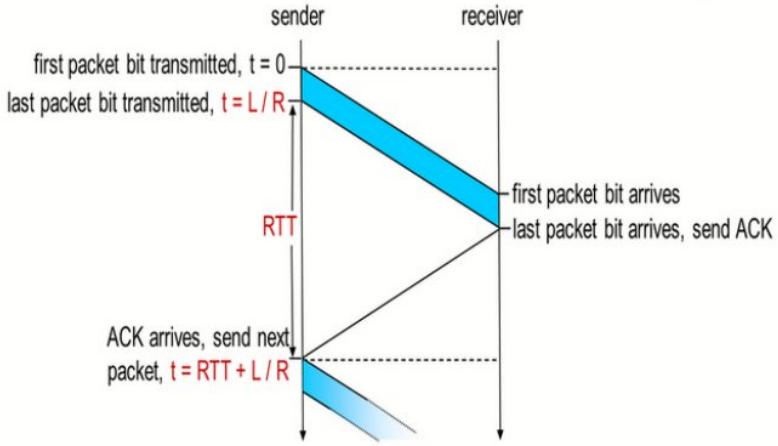


Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

* در اینجا طراحی پروتکل rdt 3.0 به پایان می‌رسد. پروتکل rdt 3.0 یک ایراد اساسی دارد که باید آن را حل کنیم، ایراد پروتکل rdt 3.0 این است که بهره وری (U) آن یا گذردهی (T) آن بسیار پایین است به خصوص زمانی که فاصله بین فرستنده و گیرنده زیاد باشد

بهره وری rdt 3.0



$$U_{sender} = \frac{L/R}{RTT + L/R}$$

با توجه به فرمول $U_{rdt3.0}$ مشخص است که بهره وری به ۲ علت می تواند پایین باشد

۱ـ زیاد بودن فاصله $(RTT) = \frac{d}{s}$

۲ـ کوچک بودن $d_{trans} = \frac{L}{R}$

کوچک بودن طول بسته — بزرگ بودن R

توجه) خروجی بهره وری (زمان کل) می‌شود از زمان شروع ارسال اولین بیت تا زمان دریافت اولین ACK

* ما نمی توانیم راندمان rdt 3.0 را درست کنیم چون خیلی وقت ها فاصله فرستنده و گیرنده و همین طور اندازه بسته دست ما نیست بنابراین باید روش مان را عوض کنیم

سوال: فرض کنید یک فرستنده که در ساحل شرقی ایالات متحده قرار دارد می‌خواهد برای گیرنده‌ای که در ساحل غربی آمریکا است داده ارسال کند، اگر تاخیر انتشار بین فرستنده و گیرنده 15ms باشد و اندازه بسته ها 1000 بایت و نرخ انتقال خط 1Gbps باشد بهره وری و گذردهی را اگر از روش توقف و انتظار استفاده کنیم محاسبه کنید

$$U_{rdt3.0} = \frac{\frac{1000 \times 8}{10^9}}{\frac{1000 \times 8}{10^9} + 2 \times 15 \times 10^{-3}} = 0.00027 = 2.7 \times 10^{-4}$$

$$T = R \times U = 10^9 \text{ bps} \times 2.7 \times 10^{-4} = 270 \times 10^3 = 270 \text{ Kbps}$$

نرخ بیتی موثری که از کانال استفاده می‌شود $270 \frac{Kb}{s}$ است درحالی که خط ما $1 \frac{Gb}{s}$ است!

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

نکته) اگر بگویند بهره وری فرستنده یا گیرنده یا کانال ارتباطی جواب همین می‌شود، زیرا ما به هرجای خط که نگاه کنیم (ابتدا خط، انتها خط یا وسط خط یا هرجا) در $\frac{L}{R}$ از $RTT+\frac{L}{R}$ شغول است

گفتیم باید روشمان را عوض کنیم:

باید از روش pipeline یا همان continious ARQ یا همان sliding window استفاده کنیم

در این روش فرستنده می‌تواند پنجره‌اش از بسته‌ها را ارسال کند بدون اینکه هنوز بسته‌ها Ack برگشته باشد. به بسته‌هایی ارسالی که هنوز Ack آنها برنگشته in_flight می‌گوییم

$$U_{pip} = w \times \frac{\frac{L}{R}}{\frac{L}{R}+RTT} \leq 1$$

در این حالت بهره وری (راندمان) برابر است با:

نکته) حد کثر راندمان می‌تواند 1 باشد، بنابراین اگر راندمان از 1 بیشتر شد آن را برابر 1 بگیرید

* هنگامی که از پروتکل‌های خط لوله‌ای استفاده می‌کنیم (یعنی وقتی پنجره ارسال داریم)

اولا: رنج # seq باید افزایش پیدا کند: زیرا بسته‌های زیادی in flight هستند که دریافت آنها توسط گیرنده تایید نشده

دوما: در فرستنده حتما باید بافر داشته باشیم

↳ بسته به اینکه از چه روشی استفاده می‌کنیم در گیرنده ممکن است بافر (پنجره دریافت) داشته باشیم یا نداشته باشیم (منظور از نداشتن یعنی فقط به اندازه 1 بسته بافر داریم)

Go-Back-N selective repeat OR reject

* تفاوت اصلی GBN و SR

در GBN گاهی اوقات یک بسته خارج از ترتیب به گیرنده می‌رسد و علیرغم اینکه بسته سالم است چون قانونی داریم مجبوریم این است که ما نمی‌توانیم یک بسته خارج از ترتیب را تحویل لایه بالاتر بدهیم و همین طور در گیرنده GBN بافر نداریم این بسته‌ها را دور می‌اندازیم و هر بسته خارج از ترتیبی که دریافت می‌کنیم Ack آخرین بسته‌ای را که درست

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

گرفته ایم را به فرستنده ارسال می کنیم اما در روش SR بسته های خارج از ترتیب دریافت شده توسط گیرنده که درست هستند در گیرنده بافر می شوند تا وقتی ناقصی ها کامل شدند همه را به یکباره به لایه بالاتر و به ترتیب تحویل بدهد

نحوه کار GBN

۱ Ack در روش GBN بصورت تجمعی است (cumulative) یعنی وقتی فرستنده یک بسته Ack با شماره ترتیب n بگیرد به این معناست که تمامی بسته هایی با شماره ترتیب کمتر مساوی n با درستی به گیرنده رسیده است واضح است که باید از Ack تجمعی در GBN استفاده شود، چون در GBN یک بافر داریم و بسته ها یکی یکی به لایه های بالاتر تحویل داده می شوند، بنابراین اگر گیرنده بسته n را تحویل لایه بالاتر بدهد به این معنا است که تمامی بسته های کمتر از n را هم به لایه بالاتر تحویل داده است.

۲ گیرنده هر بسته خارج از ترتیبی که دریافت کند، Ack آخرین بسته ای را که درست دریافت کرده می دهد

۳ اگر یک بسته در راه گم یا خراب بشود (دقت کنید در مورد Ack صحبت نمی کنیم) فرستنده GBN این بسته و تمام بسته های بعد از آن را مجددا ارسال می کند

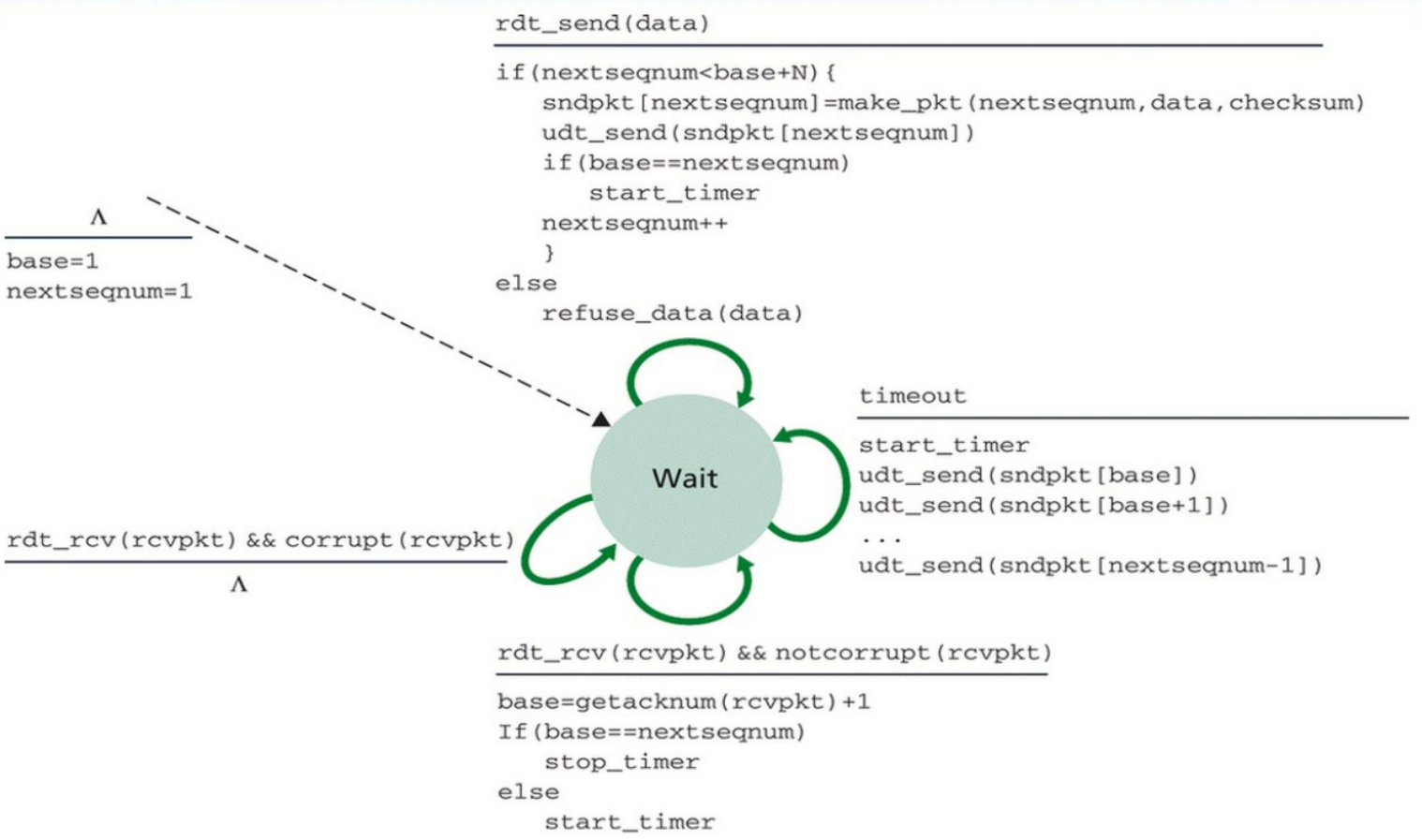
لـ بطور دقیق تر ما همیشه فقط برای بسته اول پنجره تایمر نگه می داریم و اگر این تایمر منقضی شود بسته های از base تا nextseqnum - 1 را مجددا ارسال می کنیم

لـ با توجه به این طرز کار فرستنده، بافر کردن بسته های خارج از ترتیب در گیرنده سودی نخواهد داشت چون یکبار دیگر همه این بسته های خارج از ترتیب به سمت گیرنده ارسال می شوند

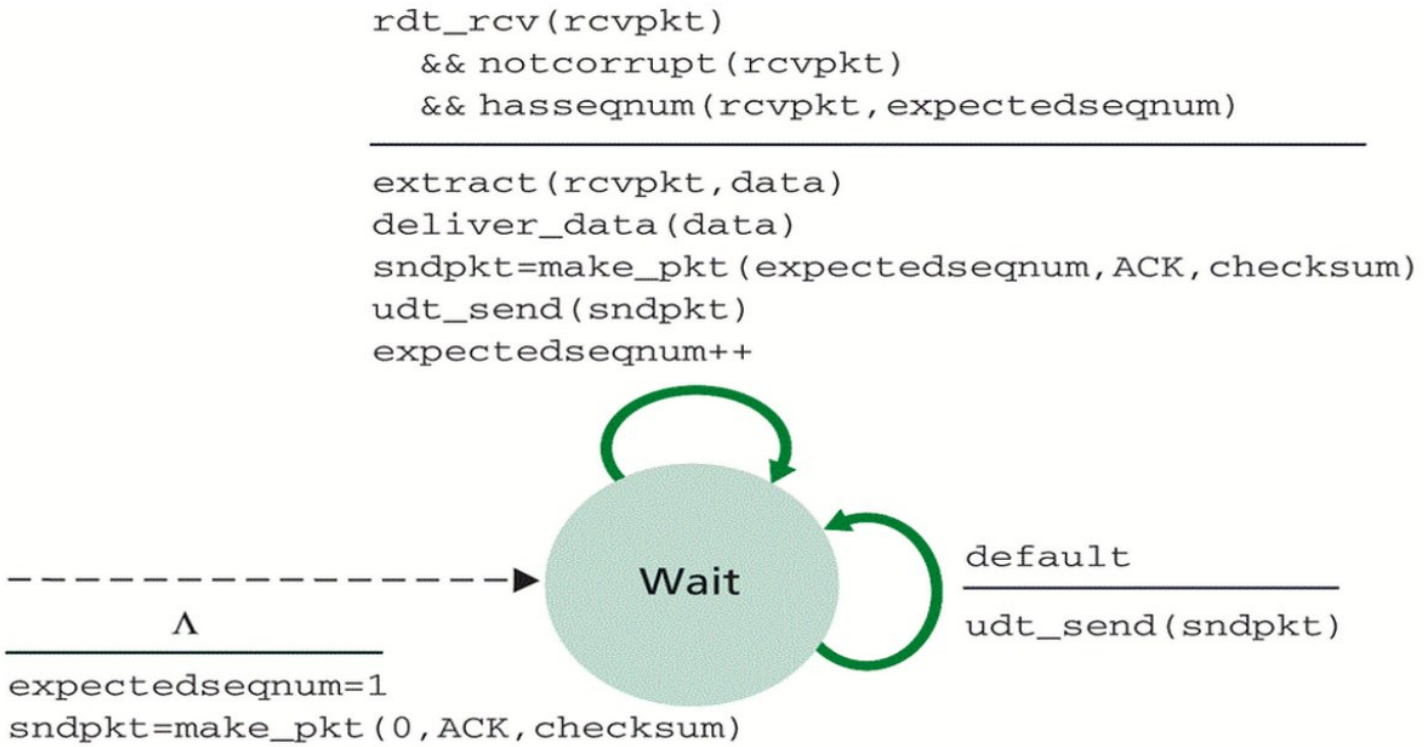
لـ اما نگه داشتن بسته های خارج از ترتیب یک مزیت هم دارد! OD (در واقع بافر کردنشان یک حسن دارد)، ممکن است در ارسال مجدد بسته های خارج از ترتیب، این بسته ها خراب بشوند، بنابراین فرستنده برای بار سوم مجبور می شود این بسته ها را ارسال کند

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir
شبکه های کامپیوتری
رامین رضوی



Extended FSM description of GBN sender



Extended FSM description of GBN receiver

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

selective Repeat

در GBN اگر اندازه پنجره ارسال و حاصلضرب تاخیر در پهنا باند بزرگ باشد بهره وری پایین خواهد بود، اگر پهنا باند و تاخیر بخواهد بزرگ باشد می‌توانند تاخیر یا پهنا باند یا هر دو بزرگ باشد، حال اگر تاخیر زیاد باشد یعنی RTT زیاد است و چون طول پنجره ما هم بزرگ است بنابراین تعداد بسته‌هایی که فرستنده می‌فرستد و هنوز Ack شان نیامده زیاد است (Ack ها خیلی دیر می‌رسند) در اینصورت اگر یکی از بسته‌ها گم شود اولا فرستنده دیر متوجه می‌شود دوما فرستنده تعداد بسته‌های زیادی را مجددا ارسال می‌کند (چون پنجره ارسال مان بزرگ است). اگر هم پهنا باند بزرگ باشد بنابراین $\frac{L}{R}$ کوچک می‌شود و بنابراین بسته‌ها با سرعت ارسال می‌شوند و اگر پنجره بزرگ باشد، تعداد بسته‌های سیار به سرعت روی کانال قرار می‌گیرند و اگر تاخیر زیاد باشد اینجا زمان زیادی منتظر Ack خواهند بود به همین علت سراغ SR می‌رویم

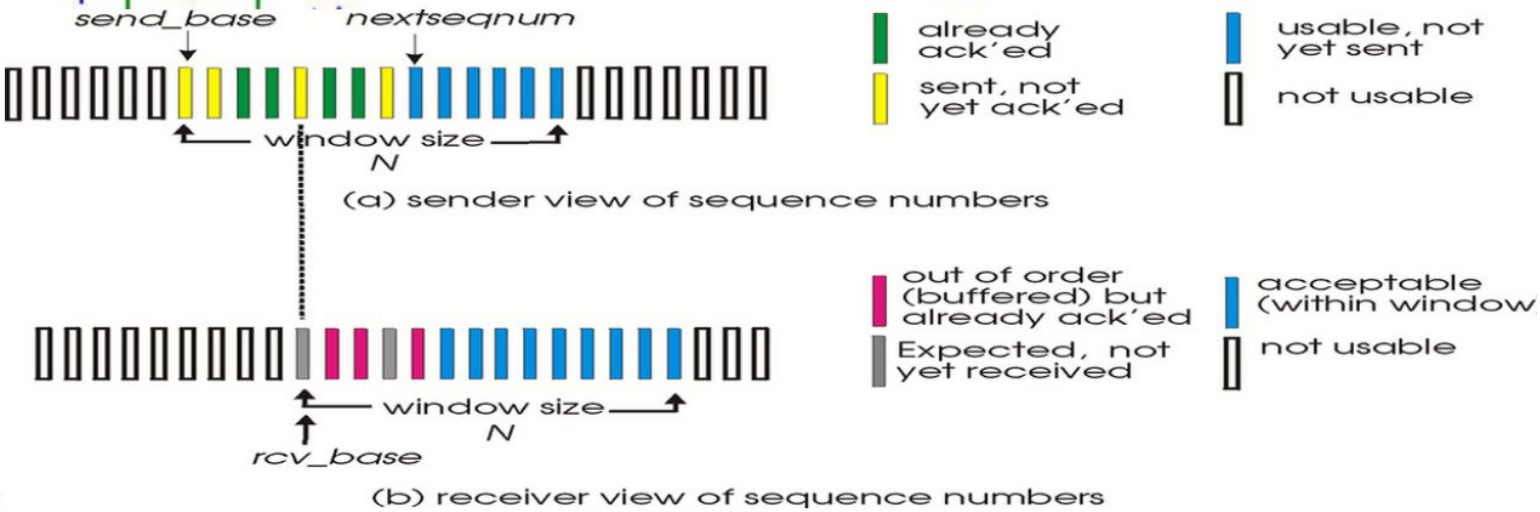
نکته) در SR هم پنجره ارسال داریم و هم پنجره دریافت. این ۲ پنجره لزوما با هم انطباق ندارند اگر فرستنده دیگر از آنچه که بدرستی دریافت شده یکسان نیست

نکته) در SR اولا هر بسته در گیرنده بصورت انفرادی Ack می‌شود و Ack تجمعی نداریم، ثانیا هر بسته ای که در فرستنده ارسال می‌شود timer خودش را دارد

time out = ۵۰ s

بسته	لحظه ارسال	time out
۰	۱۰	۶۰
۱	۲۳	۷۳
۲	۵۰	۱۰۰

لـ یک تایمر سخت افزاری داریم و سایر تایمرها منطقی (مجازی) هستند زمان time out همه بسته‌ها از طریق یک جدول محاسبه و لحاظ می‌شود



Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

فرستنده SR :

* اگر فرستنده Ack دریافت کند در بازه [sendbase, sendbase+N] فرستنده بسته مربوط به آن را بعنوان بسته ای که گیرنده بدرستی دریافت کرده علامت میزند . اگر فرستنده Ack بسته اول پنجره ارسال اش را بگیرد (sendbase) sendbase را تا جایی که به یک بسته تصدیق نشده برسد جلو می برد

سوال : مگر می شود فرستنده Ack باشماره خارج از بازه ای که گفتیم دریافت کند ؟ بله ، Ack می تواند برای بسته ای قبل از اولین بسته پنجره ارسال فرستنده باشد ! چطور ؟ گیرنده Ack یک بسته را میدهد ولی قبل از اینکه این ack به فرستنده برسد ، ۵ ثانیه بعد ، حالا فرستنده دوباره بسته را ارسال میکند و بعد از آن ack مانده در راه به فرستنده می رسد ، حال فرض کنید فرستنده پنجره را جلو می برد ، پس پس از گذشت یک زمان Ack بسته ای که دوباره ارسال کرده ایم به فرستنده می رسد که این Ack خارج از پنجره است و فرستنده نیازی نیست به این Ack محل دهد

گیرنده SR

* اگر در گیرنده بسته ای دریافت کردیم که در بازه [rcv-base, rcv-base+N-1] بود چه قبلا این بسته را گرفته باشیم و چه نگرفته باشیم این بسته را Ack می کنیم ، سپس اگر این بسته قبلا دریافت نشده بود آن را در بافر نگه داریم ، حال اگر این بسته اولین بسته پنجره دریافت گیرنده بود (seq # = rcv-base) آنگاه این بسته تا جایی که به اولین بسته بافر نشده برسیم به لایه بالاتر تحویل داده می شود

سوال : چطور ممکن است گیرنده بسته ای را در پنجره بالا دریافت کند که قبلا آن را بافر کرده است ؟ بسته قبلا توسط گیرنده دریافت و بافر شده است و Ack آن به فرستنده ارسال شده است اما Ack در میان راه گم شده و یا خراب به فرستنده رسیده است ، بنابراین فرستنده مجددا این بسته را ارسال میکند در اینصورت وقتی این بسته مجددا به گیرنده می رسد ، گیرنده فقط نیاز است این بسته را Ack کند و نیاز نیست این بسته را بافر کند ، به هر حال گیرنده باید خیال فرستنده را از رسیدن این بسته راحت کند

* اگر گیرنده یک بسته در بازه [rcv-base -N, rcv-base-1] دریافت کند ، گیرنده باز باید این را Ack کند

مثال بالا برای این هم خوب است ، فقط فرض کنید وقتی در بار اول گیرنده بسته را می گیرد پنجره اش را هم جلو می برد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

شماره ترتیب لازم در روش های GBN و SR و SfW

پروتکل	اندازه پنجره فرستنده	اندازه پنجره گیرنده	تعداد شماره ترتیب لازم
stop & wait	۱	۱	۲
SR	w	w	۲w
GBN	w	۱	w+۱

توجه) تعداد بیت لازم می‌شود سقف $\log_2$ تعداد شماره ترتیب لازم

مثال: فرض کنید w برابر ۴ باشد، بسته‌های متوالی ارسالی در روش های مختلف با شماره‌های زیر ارسال می‌شوند

SfW = ... و ۳ و ۲ و ۱ و ۰

SR = ... و ۷ و ۶ و ۵ و ۴ و ۳ و ۲ و ۱ و ۰ و ... و ۷ و ۶ و ۵

GBN = ... و ۴ و ۳ و ۲ و ۱ و ۰ و ۴ و ۳ و ۲ و ۱ و ۰

دلیل نیاز داشتن w+۱ شماره ترتیب در GBN

در مثال بالا فرض کنید فرستنده ۴ بسته با شماره های ۰ تا ۳ ارسال کرده است و هم این ۴ بسته بدرستی به گیرنده رسیده است و گیرنده نیز ACK های این ۴ را داده و اکنون منتظر بسته با شماره ۰ است در اینجا تعداد شماره ترتیب لازم را ۴ گرفته ایم تا نشان دهیم با ۴ نمی شود. حال فرض کنید هر ۴ تا ACK گم می‌شود در اینصورت بسته ۰ در فرستنده time out می‌کند و بنابراین هر ۴ بسته ۰ و ... و ۳ مجددا ارسال می‌شود وقتی این بسته ها به گیرنده می‌رسد، گیرنده اینها را بعنوان بسته جدید می‌بیند!

اما اگر w+۱ شماره ترتیب داشته باشیم مشکل حل می‌شود

گیرنده SR

۳ و ۲ و ۱ و ۰

فرستنده ۴ و ۳ و ۲ و ۱ و ۰ و ۴ و ۳ و ۲ و ۱ و ۰

در اینجا وقتی ۰ تا ۳ تکراری به گیرنده می‌رسد، حالا در اینجا اصلا مهم نیست که گیرنده فکر می‌کند که اینها داده جدید هستند یا تکرار قبلی ها هستند چون در هر صورت گیرنده منتظر بسته ۴ است و هر بسته ای بجز ۴ بگیرد ACK۳ را میدهد. با همین مثال می‌توان فهمید که برای SR به ازای ۲w عدد برای # ی نیاز داریم، چون وقتی ۰ و ۱ و ۲ و ۳ تکراری به گیرنده می‌رسد اگر #s را w+۱ بگیریم، گیرنده SR اینها را بعنوان داده جدید باور می‌کند و ACK هم اینها را می‌فرستد و حالا فرستنده ۴ را

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
شبکه های کامپیوتری
رامین رضوی
@konkurcomputer
www.konkurcomputer.ir

بفرستند ، در اینصورت وقتی ٤ به گیرنده می‌رسد گیرنده ٤، ٥ و ١و٢و٣ را تحویل لایه بالاتر می‌دهد و در این صورت Duplicate رخ نمیدهد . درصورتی که اگر تعداد #s ٤ را ٢٥ می‌گرفتیم این مشکل پیش می‌آمد

٠و١و٢، ٣، ٤، ٥، ٦، ٧

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

Tcp

۱- Tcp یک پروتکل اتصال گرا است ← اشاره به دستداد اولیه و ست کردن یکسری پارامتر و گرفتن بافر

۲- در Tcp حالت مدار فقط در سیستم های انتهایی حفظ می‌شود بنابراین
- روترها و سوئیچ های میانی اطلاعات اتصال های Tcp را نگه نمی دارند
- روترها هیچ درکی از اتصال های Tcp ندارند و فقط دیتاگرام ها را می بینند نه اتصال ها را

۳- Tcp یک سرویس دو طرفه (full duplex) ارائه می کند

۴- " یک اتصال نقطه به نقطه (point to point) و اتصال Broadcast, multicast ندارد

۵- Tcp از Ack تجمعی استفاده می کند و این Ack به بایت ها اشاره می کند و گیرنده Ack اولین بایتی را به فرستنده می دهد که تا قبل از آن بایت را درست گرفته است.

۶- در Tcp برای هر سگمنتی که ارسال می‌شود یک seq# در نظر گرفته می شود که این seq# شماره اولین بایت درون قطعه است و seq# در ابتدا دو طرف اتصال بصورت تصادفی انتخاب می‌شود

۷- در Tcp همانند UDP برای تشخیص خطا از checksum استفاده می‌شود ولی در اینجا از BEC و مکانیزم ارسال مجدد استفاده می‌شود

۸- در Tcp برای مقابله با loss از مکانیزم Timer استفاده می‌شود، و مانند GBN برای هر بسته ارسالی یک تایمر ندارد و فقط برای اولین بسته ارسال شده هنوز تصدیق نشده تایمر دارد. البته وقتی تایمر منقضی می‌شود فقط آخرین بسته ای که هنوز تصدیق نشده را می فرستیم و مجددا تایمر را با دو برابر مقدار Run می‌کنیم

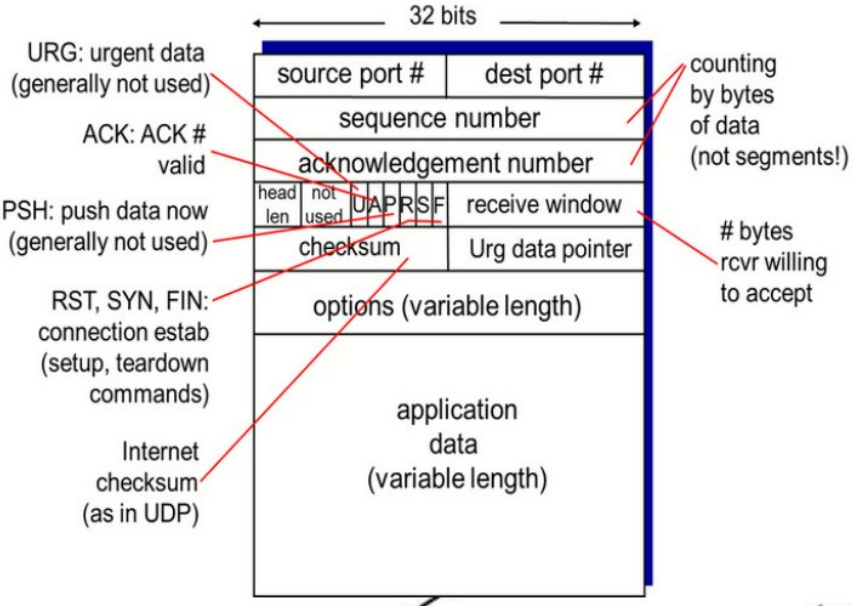
۹- در Tcp از Ack شماره دار استفاده می‌شود و NAK نداریم

۱۰- در Tcp شبیه SR در گیرنده بافر داریم و بسته های خارج از ترتیب را بافر می‌کند، البته در RFC های Tcp تصمیم این که با بسته های خارج از ترتیب چه کنیم بر عهده برنامه نویسی که Tcp را پیاده سازی می‌کند گذاشته شده است و گیرنده می‌تواند بسته های خارج از نوبت را دور بیندازد ولی در عمل از روش اول استفاده می‌شود

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

توضیح هدر Tcp



- باتوجه به فیلد option در هدر Tcp که گاهی از این فیلد برای توافق بر سر مواردی نظیر MSS و یا ضریب تغییر اندازه پنجره استفاده می‌شود هدر Tcp می‌تواند بین ۲۰ تا ۶۰ بایت باشد.

- فیلد header length (طول سرآیند): این فیلد طول هدر را برحسب 4B (۳۲ بیت) نشان میدهد بنابراین عددی است بین ۵ تا ۱۵

نکته) فیلد طول قطعه در UDP اندازه کل قطعه برحسب بایت را بیان می‌کرد

نکته) با استفاده از فیلد checksum و فلگ AcK، AcK number انجام می‌شود BEC

فلگ ها: ۶ تا فلگ داریم

RST، SYN و FIN: برای فاز برقراری اتصال و قطع اتصال استفاده می‌شود

PSH (push): به گیرنده می‌گوید که این داده مهم است و آن را فورا به لایه بالاتر تحویل بده

URG (urgent): یک بودن این بیت به گیرنده اعلام می‌کند که داده‌ای درون سگمنت تا جایی که urgent data pointer نشان میدهد اضطراری است

AcK: اگر ۱ باشد یعنی بسته حاوی AcK است که piggy back شده است و یک بودن فلگ AcK نشان دهنده این است که فیلد شماره AcK (عدد تصدیق) معتبر است

Seq# (عدد توالی) و AcK# (شماره AcK)

نکته) Seq# در دو طرف اتصال Tcp در فاز برقراری اتصال بصورت رندم انتخاب می‌شود

دلیل ⇐ زیرا پس از قطع اتصال میان دو کاست ممکن است هنوز قطعه‌هایی از آن اتصال در شبکه سرگردان باشند، حال انتخاب Seq# تصادفی باعث می‌شود احتمال اشتباه شدن قطعه‌های سرگردان با قطعه‌های جدید به حداقل برسد دقت کنید که Seq# عدد بسیار بزرگی است

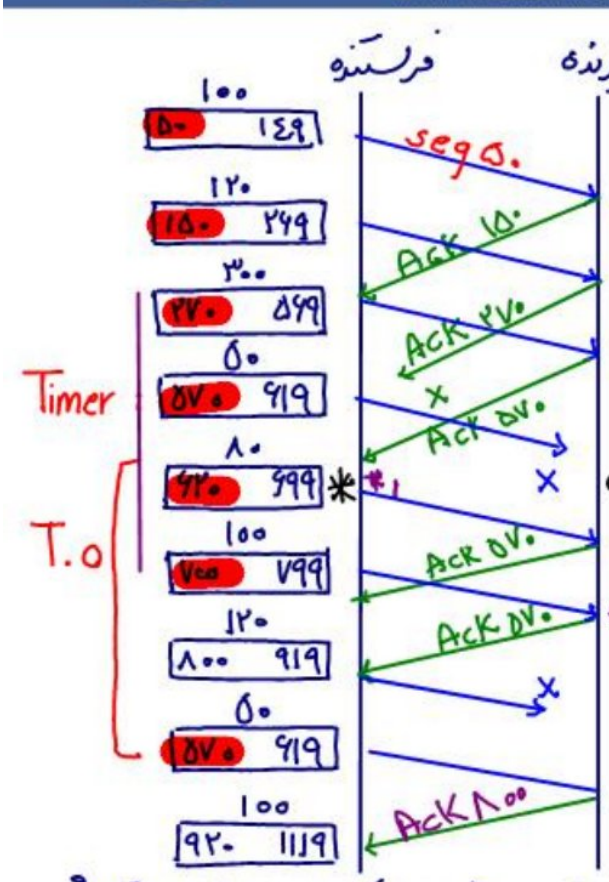
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir
MSc-PhD Computer-IT



*۱ : فرستنده می فهمد که گیرنده تا بایت ۵۶۹ را بدرستی دریافت کرده و الان منتظر بایت ۵۷۰ به بعد است

*۲ : تا بایت ۷۹۹ درست به گیرنده رسیده است اما گیرنده با گرفتن هر بسته خارج از ترتیب Ack بایت اول بسته ای که منتظرش هست را میدهد

* اینجا sendBase = ۵۷۰ است دقت کنید چون یک بسته گم شده هی ack SB می آید، حال اگر یک ack مثل ۷ بیاید که $y > SB$ آنگاه SB آپدیت می شود به ۷

نکته ۱ : یکی از اصلاحیه های پیشنهادی Tcp بنام تصدیق گزینشی به گیرنده Tcp اجازه میدهد تا به جای تصدیق تجمعی بتوان شبیه SR قطعه های خارج از ترتیب را Ack بدهد

نکته ۲. اگر بخواهیم هر قطعه ارسال شده هنوز تصدیق نشده یک تایمر داشته باشد، مدیریت این تایمرها بسیار زمانبر و به سیستم تحمیل می کند بنابراین Tcp برای همه قطعه های ارسال شده هنوز Ack نشده فقط یک تایمر ارسال مجدد در نظر می گیرد

Tcp در دو صورت ارسال مجدد انجام میدهد ۱) وقوع T.o ۲) دریافت ۳ تکراری ack

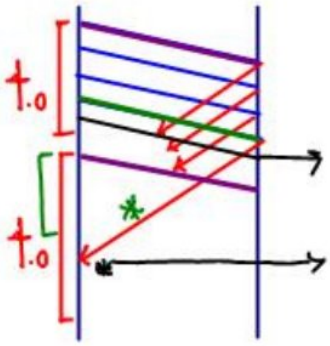
۱) بررسی T.o بصورت دقیق تر

وقتی Tcp یک سگمنت را به لایه IP میدهد اگر این سگمنت اولین سگمنت پنجره ارسال اش باشد تایمر را برایش استارت می کند ← بنابراین تایمر متعلق است به قدیمی ترین قطعه تصدیق نشده حالا اگر این تایمر منقضی بشود، Tcp فقط همین بسته را مجددا ارسال می کند (سگمنت با کوچکترین seq # را) و بعد پس از هر بار انقضا این تایمر، زمان تایمر را دو برابر می کند. بنابراین زمان انقضا تایمر پس از هر ارسال مجدد بصورت نمایی رشد می کند. حال اگر قبل از T.o یک Ack بیاید که $y > SB$ باشد آنگاه Tcp برای قطعه ای که شماره ترتیب اش y است مقدار TimeoutInterval را جدیدا محاسبه کرده قرار می دهد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

نکته) علاوه بر زمانی که یک ACK جدید دریافت می‌کنیم و در این حالت TimeoutInterval جدید را قرار می‌دهیم زمانی که سگمنتی که می‌خواهیم ارسال کنیم کوچکترین سگمنت است برای آن TimeoutInterval جدید را قرار می‌دهیم



در اینجا sendbase=y می‌شود و حالا اگر بسته دیگری پس از بسته سبز ارسال کرده بودیم، تایمر با مقدار جدید T.O.I برای آن استارت می‌شد ولی فکر کنید تا زمانیکه این ack می‌رسد بسته دیگری ارسال نشده، بنابراین در اینجا sendBase = Nextseqnum می‌شود و تایمر متوقف می‌شود حال اگر پس از این سگمنت دیگری بخواهیم ارسال کنیم با مقدار جدید T.O.I تایمرش را ست می‌کنیم

حال چرا Tcp پس از هر بار T.O، T.O.I را دو برابر می‌کند

۱- زیرا وقتی T.O رخ میدهد که در شبکه ازدحام باشد (ازدحام است که باعث دیر رسیدن بسته‌ها و گم شدن آنها و در نتیجه رخ دادن T.O می‌شود) بنابراین ما T.O.I را زیاد می‌کنیم تا مجدداً سریع (الکی) منقضی نشود و مادوباره مجبور بشیم بسته را ارسال کنیم و اوضاع را بدتر کنیم. بنابراین پس از T.O که نشانه بروز ازدحام است فرستنده نباید بر ارسال مجدد قطعه‌ها خود با همان آهنگ قبلی اصرار کند

۲- دو برابر کردن T.O.I باعث می‌شود که قطعه‌ها بجری که منتظر دریافت تصدیق آنها هستیم دچار انقضا زودرس (premature t.o) نشوند

مثلاً در همان مثال بالا فرض کنید اگر t.o.I را دو برابر نمی‌کردیم تصدیق * پس از t.o به ما می‌رسید

نکته) در هنگام شروع مقدار T.O.I را برابر ۱ ثانیه می‌گیرند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

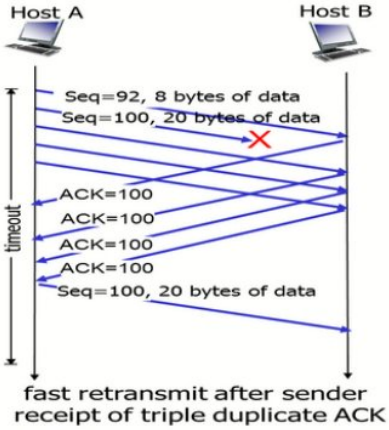
② دریافت ۳ ACK تکراری Fast Retransmit

گاهی اوقات T.O.I می تواند بزرگ باشد بنابراین وقتی یک بسته گم می شود، اگر بخواهیم منتظر T.O آنشویم تا مجددا این بسته را ارسال کنیم این کار باعث افزایش تاخیر انتها به انتها می شود، برای همین فرستنده Tcp راه کار دیگری نیز برای تشخیص احتمال گم شدن بسته ها دارد، اگر فرستنده Tcp برای یک قطعه خاص ۳ ACK تکراری دریافت کند دیگر منتظر T.O نمی شود و بلافاصله یک ارسال مجدد سریع انجام میدهد

نکته ۱: در شبکه ترتیب رسیدن بسته ها به گیرنده می تواند بهم بخورد، بنابراین گیرنده ممکن است برای سگمنتی که منتظرش هست ۳ ACK تکراری هم بدهد ولی بعد از آن، آن سگمنت برسد، بنابراین ارسال ۳ تصدیق از طرف گیرنده و یا دریافت ۳ ACK توسط فرستنده قطعا به معنای از دست رفتن یک بسته نیست

نکته ۲: دلیل اینکه فرستنده نیز با دریافت اولین ACK تکراری مجددا ارسال نمی کند و تا دریافت ۳ ACK تکراری صبر می کند نیز همین مورد است

نکته ۳: وقتی فرستنده ۳ ACK تکراری دریافت می کند و fast retransmit می کند به تایمر دست نمی زند



نکته ۴: تا الان فرض می کردیم که وقتی یک سگمنت in order به گیرنده می رسد، گیرنده بلافاصله ACK آن را برمی گرداند ولی در واقعیت این طور نیست و ۲ حالت در این جا داریم:

۱- گیرنده قطعا می داند که منتظرش است و تمام سگمنت های قبل از این را ACK داده است: در اینصورت ۵۰۰ میلی ثانیه صبر می کند، اگر در این مدت سگمنت in order ای نرسید ACK دوی را می دهد و اگر نرسید ACK اولی را می دهد

۲- گیرنده قطعا می داند که منتظرش است اما سگمنت قبلی منتظر ارسال ACK است: ارسال بلافاصله یک

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

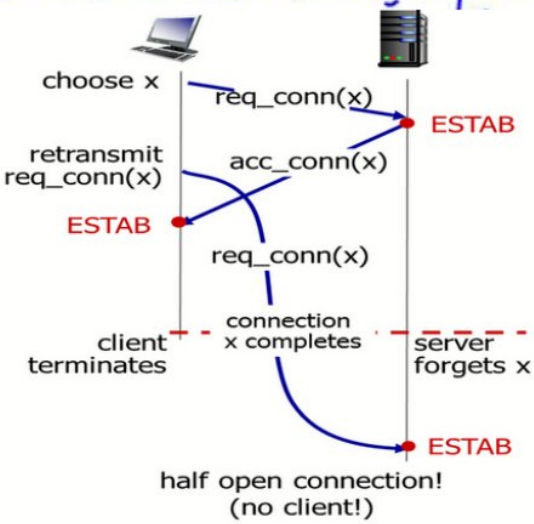
Ack تجمیعی که هر ۲ سگمنت را Ack می کند

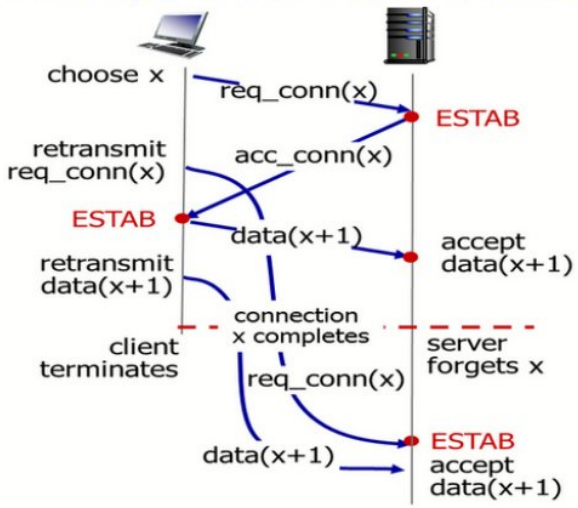
نکته ۵: اگر گیرنده یک سگمنت خارج از نوبت دریافت کند چه این سگمنت شکاف ما را پر کند چه نکند گیرنده بلافاصله Ack مربوطه را میدهد

نکته ۶: نه با رخ دادن T.O و نه با دریافت ۳ Ack تکراری توسط فرستنده نمی توان با قطعیت گفت که سگمنت loss شده است.

مدیریت اتصال Tcp

2-way handshake- در شبکه جواب نمی دهد، چون در شبکه بسته‌های داده و Ack ممکن است گم بشوند و یا با تاخیر برسند و در نتیجه ما ارسال مجدد داریم که این کار ممکن است باعث بروز اشکال شود



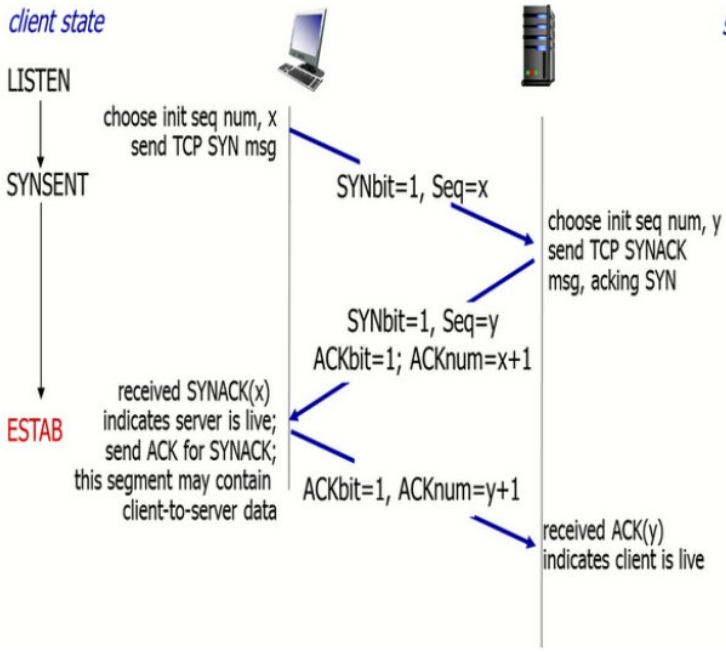


مراحل برقراری اتصال

۱- ارسال بسته SYN segment توسط فرستنده
این قطعه حاوی هیچ دیتا ای نیست

۲- ارسال بسته SYNACK segment یا connection granted segment توسط گیرنده
این قطعه نیز حاوی داده لایه کاربرد نیست

با دریافت قطعه SYN segment، سرور با فرخ و تنظیم‌های Tcp را به این اتصال تخصیص می دهد



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیر
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

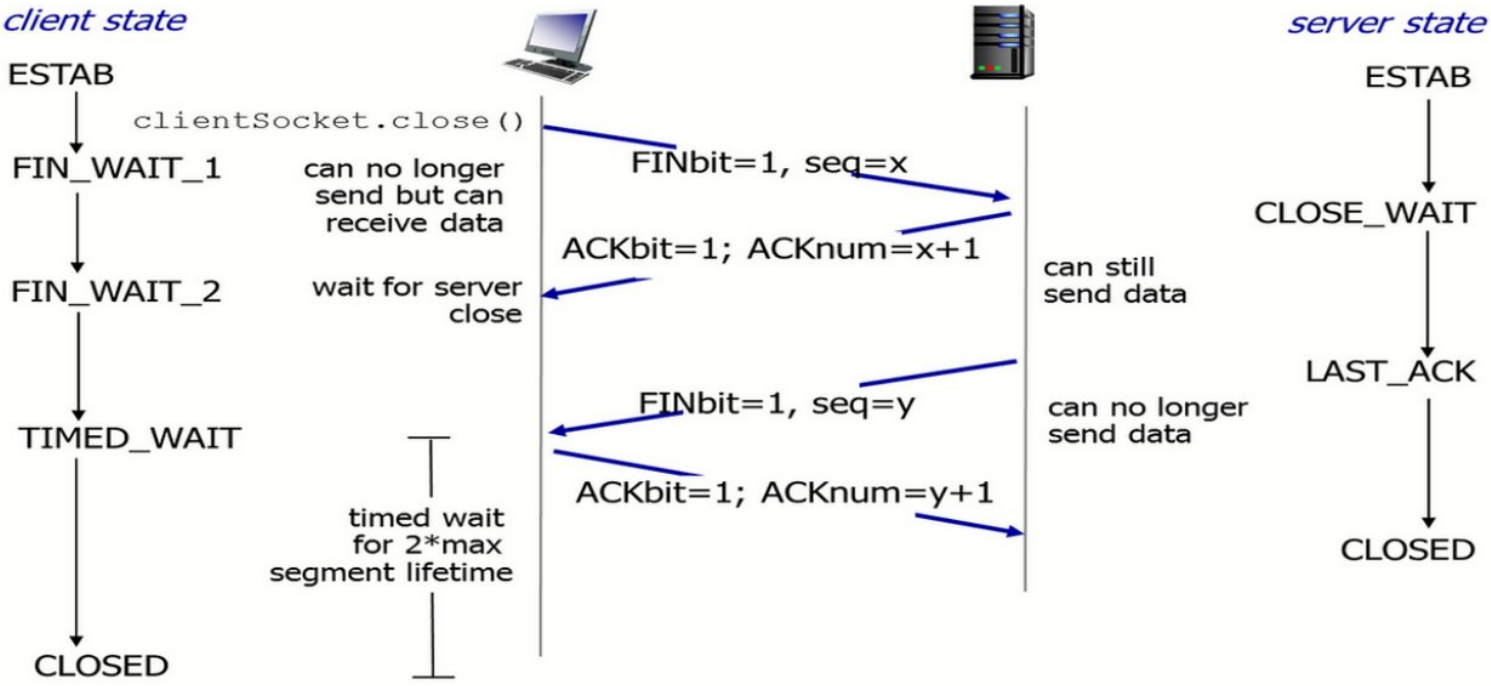
۳- حال کلاینت با دریافت سگمنت SYNACK بافرها و متغیرهای Tcp را به این اتصال تخصیص می‌دهد و یک ACK برای سرور ارسال می‌کند، در این بسته بیت SYN=0 است و همچنین این بسته می‌تواند حاوی داده باشد، با دریافت سگمنت SYNACK از سرور فرستنده وارد حالت ESTABLISH می‌شود و تا زمانی که شنودی در این حالت است می‌تواند سگمنت‌های Tcp دارای داده برنامه کاربری را برای سرور ارسال کند

توجه) دقت کنید که سرور با دریافت قطعه SYN segment وارد حالت ESTABLISHED نمی‌شود و وقتی که ACK بسته SYNACK را دریافت کند وارد حالت فوق می‌شود

نکته: گفتیم قبل از کانکشن سرور باید یک پورت را باز کند و گوش کند، حال تا زمانیکه کلاینت درخواستی نداده می‌گوییم این کانکشن passive است (passive open) connection passive و وقتی درخواست می‌آید می‌گوییم کانکشن active است

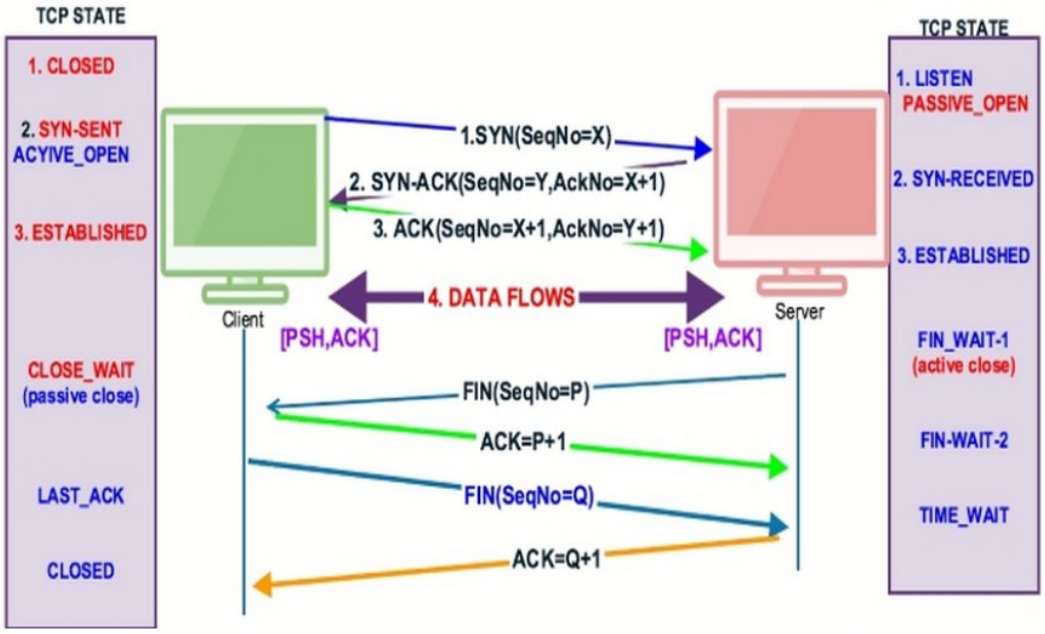
قطع اتصال در Tcp

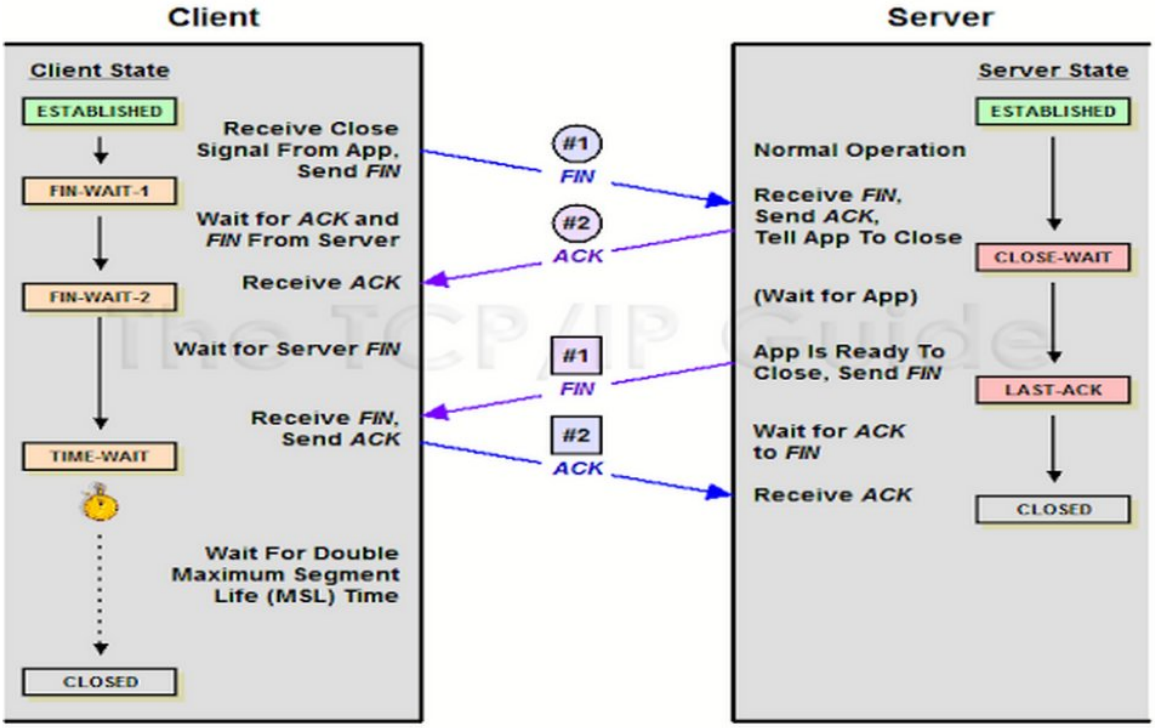
یک اتصال Tcp را هرکدام از دو طرف آن می‌توانند قطع کنند، برای قطع مانند 3-way hand- شبیه برادران اتصال نداریم و یک جفت از two-way han- داریم. هر سمتی که درخواست قطع اتصال را بدهد از آن به بعد می‌تواند از طرف مقابل دیتا دریافت کند ولی دیگر نمی‌تواند Data ال را از لایه App اش برای ارسال به طرف مقابل قبول کند ← منظور دیتا لایه App است.

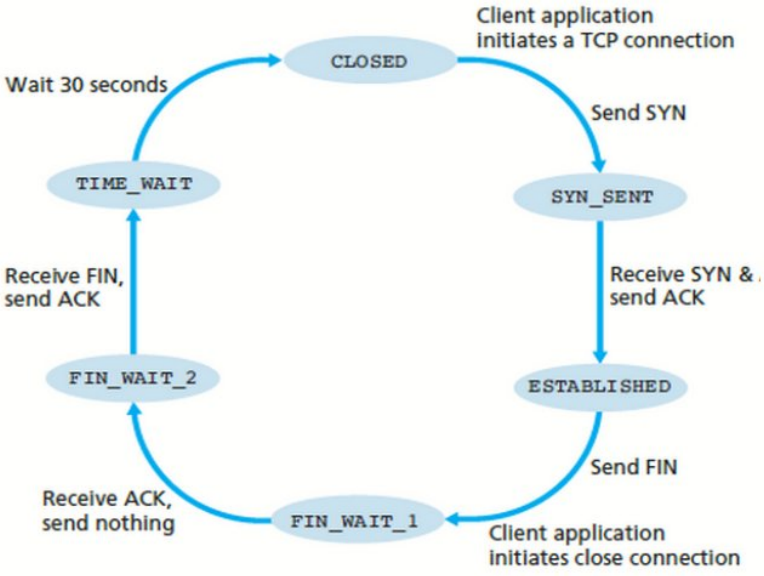


Scanned with CamScanner

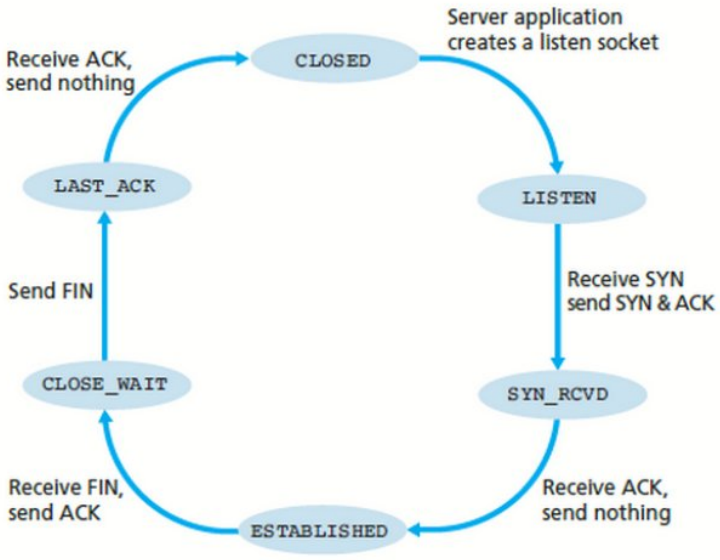
TCP Three Way Handshake/DATA FLOW/CLOSE SEQUENCE







A typical sequence of TCP states visited by a client TCP



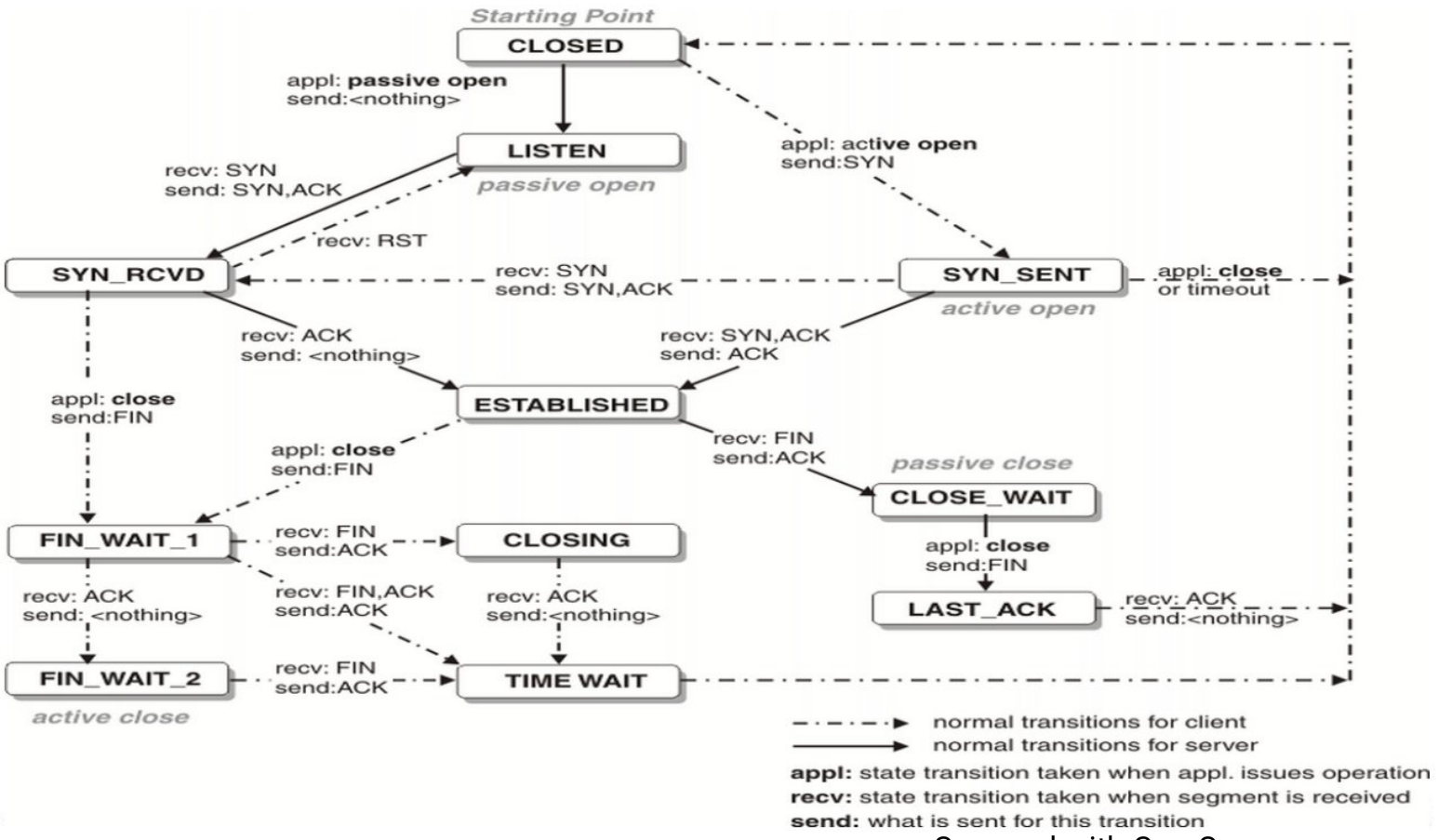
A typical sequence of TCP states visited by a server-side TCP

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir
شبکه های کامپیوتری
رامین رضوی

Table 154: TCP Connection Termination Procedure

Client			Server		
Start State	**Action**	**Transitions To State**	**Start State**	**Action**	**Transitions To State**
ESTABLISHED	**Client Close Step #1 Transmit:** The application using TCP signals that the connection is no longer needed. The client TCP sends a segment with the *FIN* bit set to request that the connection be closed.	*FIN-WAIT-1*	*ESTABLISHED*	At this stage the server is still in normal operating mode.	—
FIN-WAIT-1	The client, having sent a *FIN*, is waiting for it to both be acknowledged and for the serve to send its own *FIN*. In this state the client can still receive data from the server but will no longer accept data from its local application to be sent to the server.	—	*ESTABLISHED*	**Client Close Step #1 Receive and Step #2 Transmit:** The server receives the client's *FIN*. It sends an *ACK* to acknowledge the *FIN*. The server must wait for the application using it to be told the other end is closing, so the application here can finish what it is doing.	*CLOSE-WAIT*
FIN-WAIT-1	**Client Close Step #2 Receive:** The client receives the *ACK* for its *FIN*. It must now wait for the server to close.	*FIN-WAIT-2*	*CLOSE-WAIT*	The server waits for the application process on its end to signal that it is ready to close.	—
FIN-WAIT-2	The client is waiting for the server's FIN.	—	*CLOSE-WAIT*	**Server Close Step #1 Transmit:** The server's TCP receives notice from the local application that it is done. The server sends its *FIN* to the client.	*LAST-ACK*
FIN-WAIT-2	**Server Close Step #1 Receive and Step #2 Transmit:** The client receives the server's *FIN* and sends back an *ACK*.	*TIME-WAIT*	*LAST-ACK*	The server is waiting for an *ACK* for the *FIN* it sent.	—
TIME-WAIT	The client waits for a period of time equal to double the maximum segment life (MSL) time, to ensure the *ACK* it sent was received.	—	*LAST-ACK*	**Server Close Step #2 Receive:** The server receives the *ACK* to its *FIN* and closes the connection.	*CLOSED*
TIME-WAIT	The timer expires after double the MSL time.	*CLOSED*	*CLOSED*	The connection is closed on the server's end.	
CLOSED	The connection is closed.		*CLOSED*	The connection is closed.	



Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

نکته: معمولاً کلاینت که ارتباط را شروع کرده تمام کننده ارتباط نیز هست.

نکته: اصطلاحی داریم به نام graceful close و می‌گوییم Tcp terminate connection gracefully و یعنی این معناست که در دومین جفت از two-way han — وقتی کلاینت سگمنت FIN را از سرور گرفت و Ack داد سریع ارتباط را نمی‌بندد و یک تایمر به اندازه ۲ برابر MSL (Maximum segment lifetime) روشن می‌کند و پس از آن کانکشن را close می‌کند، این کار ۲ دلیل دارد

۱ـ اگر داده‌ای از قبل در شبکه مانده است برسد چون بسته‌ها out of order هستند در شبکه

۲ـ اگر Ack نهایی‌اش که کلاینت به سرور می‌دهد گم بشود، سرور دوباره برای کلاینت FIN را می‌فرستد، حال کانکشن مشتری باید باز باشد تا بتواند FIN بعدی را بگیرد و Ack آن را بدهد

وقتی قطعه‌ای به یک سرور می‌رسد که آن سرور هیچ سوکتی برای آن ندارد این به آن معناست

۱ـ در Tcp: فرض کنید یک قطعه Tcp ای به سرور می‌رسد که با توجه به شماره پورت و Ip های مبدا و مقصد آن بسته با هیچ کدام از سوکت‌ها در حال اجرا روی گیرنده مچ نیست (مثلاً در سروری، روی سروری روی پورت ۸۰ در حال اجرا نیست) در اینصورت مقصد (سرور) یک قطعه به فرستنده می‌فرستد که در آن فلگ RST به ۱ ست شده است با دریافت این قطعه توسط فرستنده، فرستنده متوجه می‌شود که سرور هیچ سوکتی برای این App (قطعه) ندارد و دوباره آن را ارسال نمی‌کند

۲ـ در UDP: در صورتی که اتفاق بالا رخ بدهد، مقصد یک دیتاگرام مخصوص Icmp به فرستنده برمی‌گرداند

تخمین T.o.I

ـ RTT به علت ماهیت شبکه نوسان دارند، بنابراین برای محاسبه T.o.I نیاز داریم که یک میانگین از RTT های سگمنت‌ها قبلی بگیریم و یک Estimated RTT محاسبه کنیم، حال در محاسبه این میانگین باید به نکات زیر توجه کنیم:

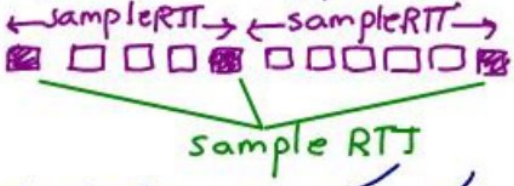
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

رامین رضوی

۱- برای تمام قطعه‌هایی ارسال شده نمی‌آیند RTT را محاسبه کند و میانگین بگیرند و در هر RTT یک قطعه را انتخاب می‌کند و به آن sample RTT می‌گویند و زمان رفت و برگشت آن را محاسبه می‌کند



& sample RTT فاصله زمانی بین تحویل یک قطعه به لایه Ip و دریافت Ack آن از لایه Ip

۲- در شبکه نمونه‌های جدید وضعیت فعلی شبکه را بهتر منعکس می‌کنند تا نمونه‌های قدیمی‌تر بنابراین لازم است که یک میانگین نمایی وزن دار بگیریم (exponential weighted moving average)(EWMA)

۳- Tcp هرگز یک قطعه‌ای که ارسال مجدد قطعات قبلی است را بعنوان sampleRTT انتخاب نمی‌کند زیرا قطعه‌ای که ارسال مجدد می‌شود نیز ممکن است مسیر خوبی را طی نکند تخمین درستی به ما ندهد

$$\text{Estimated RTT(new)} = (1-\alpha)\,\text{Estimated RTT(old)} + \alpha \times \text{sampleRTT}$$

RTT تخمینی یا RTT میانگین

$1-\alpha = \frac{7}{8} = 0.875$

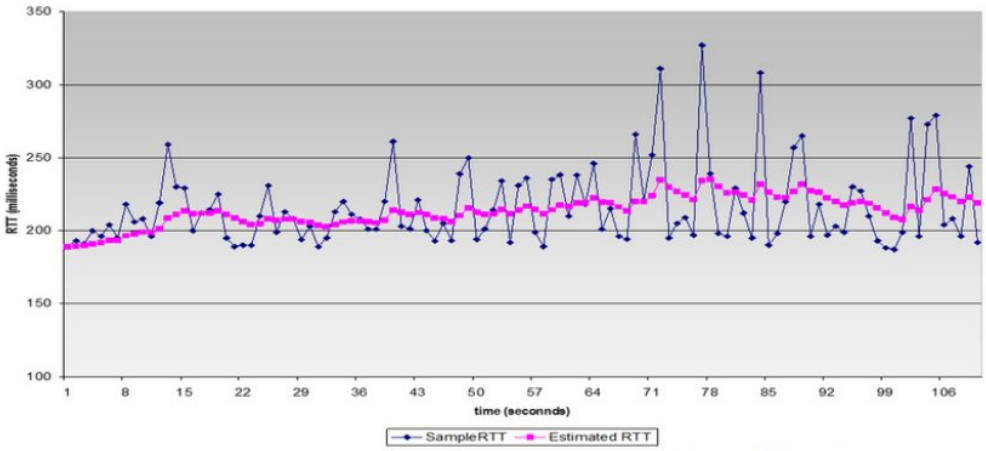
$\alpha = \frac{1}{8} = 0.125$

فقط به نمونه فعلی $\frac{1}{8}$ کل وزن را داده‌ایم و به تمام نمونه‌های قبلی $\frac{7}{8}$ وزن را داده‌ایم

* با توجه به شکل صفحه بعد متوجه می‌شوید که هم sampleRTT و هم Estimated RTT نوسان می‌کنند ولی نوسانات RTT تخمینی به اندازه نوسانات sampleRTT نیست و نوسانات شدید sampleRTT با در نظر گرفتن EstimatedRTT به جای sampleRTT برطرف خواهد شد، اما هرچه قدر مطلق اختلاف بین sampleRTT و EstimatedRTT در یک لحظه بیشتر باشد (انحراف معیار لحظه‌ای) به این معناست که EstimatedRTT ما تخمین خوبی نیست و انحراف‌مان خیلی زیاد است، حال برای بهبود این تقریب باید یک مقدار تخمینی دیگر به RTT تخمینی‌مان اضافه کنیم، حال خود انحراف لحظه‌ای هم این در حال تغییر است، بنابراین باید یک میانگینی از انحرافات بدست بیاوریم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir



$$DevRTT(new) = \underbrace{(1-\beta)}_{\frac{3}{4}=0.75} DevRTT(old) + \underbrace{\beta}_{\frac{1}{4}=0.25} |EstimatedRTT(new) - SampleRTT|$$

میزان انحراف آخرین نمونه از میانگین تخمینی قبلی

$$TimeoutInterval = EstimatedRTT(new) + 4 \times DevRTT(new)$$

کنترل جریان در Tcp

اگر برنامه کاربردی متناظر با یک اتصال Tcp دریافت کننده در خواندن داده های دریافتی فرستنده کند عمل کند، ممکن است بافر دریافت گیرنده سر ریز کند، برای جلوگیری از این کار و تطبیق دادن سرعت ارسال داده فرستنده با سرعت دریافت داده گیرنده Tcp گیرنده در هر قطعه ای که برای فرستنده ارسال می کند میزان فضا آزاد بافرش را در فیلد rwnd هدر Tcp قرار می دهد به این مقدار پنجره دریافت گیرنده (Receive window) می گویند.

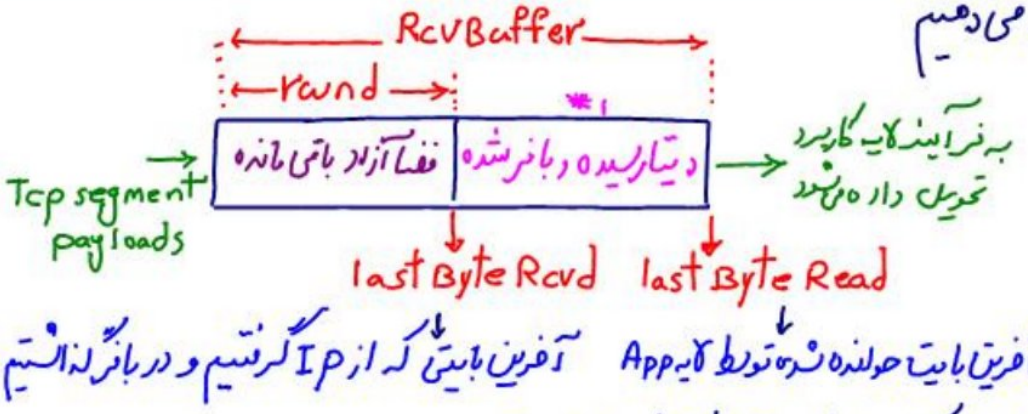
نکته ۱: کنترل جریان و کنترل ازدحام هر دو عمل یکسانی انجام می دهند و هر دو نرخ ارسال فرستنده را کند می کنند اما هدف آنها بسیار متفاوت است.

نکته ۲: توجه کنید که Tcp یک پروتکل full duplex است و هر ۲ طرف می توانند هم داده ارسال و دریافت کنند، بنابراین هر طرف پنجره دریافت مستقل خودش را دارد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

در زیر بافر دریافت گیرنده را نشان می دهیم



*1 داده هایی که هنوز تحویل لایه کاربرد نداریم

آخرین بایت دریافت شده توسط لایه App — آخرین بایتی که از IP گرفتیم و در بافر گذاشتیم

توجه: مشخص است که lastByteRcvd بزرگتر از lastByteRead است

- Tcp فرستنده اجازه ندارد باعث سرریز شدن این بافر شود، بنابراین باید تعداد بایت های درون بافر کوچکتر مساوی اندازه بافر باشد:

شرط سرریز نشدن بافر گیرنده

$$\underbrace{lastByteRcvd - lastByteRead}_{\text{تعداد بایت های درون بافر}} \leq \underbrace{RcvBuffer}_{\text{اندازه بافر}}$$

$$Receive\ window = rwnd = RcvBuffer - [lastByteRcvd - lastByteRead]$$

فضا خالی باقیمانده — حجم کل بافر — داده های درون بافر

گیرنده مقدار rwnd را با هر پیامی که به فرستنده می دهد در هدر Tcp قرار می دهد، فرستنده همیشه تعداد بایت های تصدیق نشده خود را (بایت های in-flight) کمتر از rwnd نگه می دارد

در فرستنده $lastByteSend - lastByteAck \leq rwnd$

نکته ۱: در شروع کار $rwnd = RcvBuffer$ است

نکته ۲: گیرنده وقتی برای فرستنده سگمنت ارسال می کند که یا داده ای برای ارسال به فرستنده داشته باشد یا بخواهد Ack خالی برایش ارسال کند، حال فرض کنید بافر دریافت گیرنده پر شود و مقدار rwnd=0 را به فرستنده گزارش بدهد، همچنین پس از ارسال این بسته، دیگر داده ای برای ارسال به فرستنده نداشته باشد، در اینصورت با وجود آنکه گیرنده پس از مدتی بافرش خالی می شود ولی نمی تواند این امر را به اطلاع فرستنده برساند و بنابراین فرستنده قفل می شود برای حل این مشکل فرستنده Tcp به این شکل رفتار می کند که پس از دریافت rwnd=0 همچنان به ارسال سگمنت های بدون داده به گیرنده ادامه میدهد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

چون گیرنده مجبور است این سگمنت ها را Ack کند در نتیجه مقدار جدید rwnd در هدر این بسته های Ack به فرستنده اعلام می شود

کنترل ازدحام

با توجه به اینکه لایه شبکه به لایه انتقال در راستای کنترل ازدحام کمک کند یا نه، روش های کنترل ازدحام به ۲ دسته تقسیم می شود

۱- end-to-end congestion control

- شبکه هیچ فیدبک صریحی نمی دهد وقتی ازدحام رخ میدهد
- ازدحام توسط مشاهداتی نظیر loss و تاخیر توسط end systems تشخیص داده می شود
- Tcp از این رهیافت برای کنترل ازدحام استفاده می کند

۲- network assisted congestion con-

در این روش روترهای میانی با روش هایی به فرستنده ها اعلام می کنند که ازدحام وجود دارد و در نتیجه فرستنده ها واکنش مناسب را نشان می دهند

روش های مطلع کردن هاست ها توسط روترها

① choke packet (بازخورد مستقیم شبکه)

زمانی که یک روتر تشخیص می دهد که یکی از لینک های خروجی اش دچار ازدحام شده است، این روتر (لایه شبکه روتر) یک بسته کنترلی به نام choke packet (بسته خفه کننده) بصورت مستقیم برای هاست آدرس های Ip که دارند روی این لینک ازدحام ایجاد می کنند ارسال می کند

② Hop by hop choke packet

برای سریعتر کردن روش اول می گویند هر روتر بیاید به روتر قبلی اش یک پیام choke packet بفرستد و با این پیام به روتر قبلی بگوید که من دچار ازدحام هستم می شه شما بار ترافیکی تو کم کنی؟ و حالا اگر خود این روتر هم دید که مبدا ایجاد آن ترافیکی نیست که دارد ازدحام ایجاد می کند، این کار را با روتر قبلی اش انجام میدهد، یعنی هر روتر به روتر قبلی می گوید نرخ ات را پایین بیاور

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

③ warning bit (بازخورد شبکه از طریق گیرنده)

استفاده از warning bit در هدر Ip : اگر یک روتر ببیند که یک لینک اش دچار ازدحام شده است می تواند در هدر بسته های Ip که از آن لینک خارج می شوند یک بیتی را set کند که نشان دهنده ازدحام باشد، حال وقتی این بسته ها به مقصدهای خودشان می رسند اگر مقصد دید که آن بیت ست شده است یک فیدبک به مبدا اش ارسال می کند و به مبدا می گوید که x٪ نرخ ات را پایین بیاور حال تمامی کسانی که از آن روتر و از آن لاین شلوغ روتر دارند بسته ارسال می کنند این فیدبک را دریافت می کنند و نرخ شون را پایین می آورند

وقتی به یک روتر می گوییم ترافیک ات را پایین بیار آن روتر چگونه این کار را می تواند بکند؟

۱ـ به روتر قبلی بگوییم نرخ اش را کم کند

۲ـ اگر صفی با طول مناسب دارد بسته ها را مدت بیشتری در صف اش نگه دارد به این شکل بطور موقت نرخ خروجی را کاهش می دهیم.

به هر حال باهمه کارهای بالا صف خروجی یک روتر ممکن است پر شود، چون لینک خروجی دارد از چندین لینک ورودی داده می گیرد، حالا در صورت پر شدن صف خروجی یک لینک چاره اش جز دور ریختن بسته ها نداریم که بنابراین بحث Buffer management مطرح می شود

load shedding : اگر تصمیم گرفتیم بسته ها را دور بریزیم چه بسته هایی را دور بریزیم؟

این کار می تواند تابع زمان رسیدن بسته ها باشد و یا تابع اهمیت آنها . ۲ روش اول تابع زمان رسیدن بسته ها است و روش سوم تابع اهمیت آنها

۱ـ بسته های جدیدی که وارد می شوند را دور بریزیم : مناسب کارهایی که تایمینگ در آنها خیلی مهم نیست مثل انتقال فایل

۲ـ بسته های قدیمی را دور بریزیم : مناسب کاربردهای real time ، در این کاربردها احتمال به درد نخوردن بسته های قدیمی خیلی بالاتر از بسته های جدید است.

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

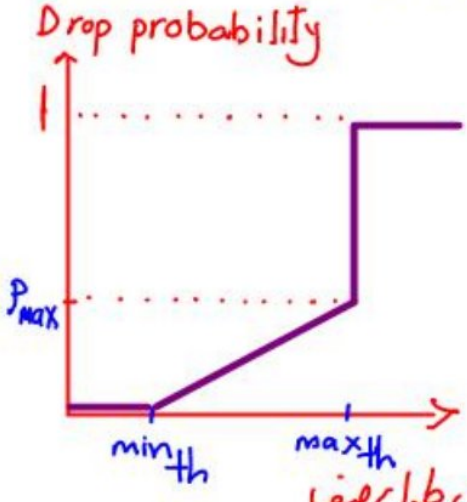
۳_ use packet priority . دور ریختن بسته ها نیاز نیست فقط تابع زمان رسیدن بسته ها باشد

- در پروتکل IP بخشی از هدر IP بنام Type of service مشخص می‌کند که یک بسته متعلق به چه کلاسی از سرویس های QoS است . برخی از روترها به این فیلد توجه می‌کنند
- در شبکه ATM نیز یک بیت در هدر لایه ATM وجود دارد بنام CLP (cell loss priority) که مشخص می‌کند اهمیت cell ها را (scalable coding : لایه base و enhance را گفتیم می‌کنیم با این بیت)

قانون : محاسبات نشون داده که وقتی شبکه دارد به سمت ازدحام پیش می‌رود ، بهتر است بسته ها را قبل از رسیدن به ازدحام Drop کنیم

در راستای قانون بالا روشی داریم بنام Random early detection

این روش می‌آید و در هر لحظه متوسط تعداد بسته هایی که در صف وجود دارد را محاسبه می‌کند ، حال با توجه به نمودار روبه رو و یا راستاخیی که قبلا محاسبه شده اگر این میانگین از min_{th} کمتر باشد روتر هیچ بسته ای را Drop نمی‌کند و اگر میانگین طول صف بین min_{th} و max_{th} باشد با یک احتمال و بصورت تصادفی تصمیم می‌گیرد که بسته آن را Drop کند یا نکند ، هرچه میانگین طول صف به max_{th} نزدیک تر باشد این احتمال بالاتر است و اگر میانگین طول صف بزرگتر مساوی max_{th} شود بسته ها را دور می‌ریزد و یا آنها را علامت می‌زند



نکته) در شبکه های virtual circuit یکی از راه ها پرهیز (جلوگیری کردن) از ازدحام استفاده از Admission control است ، گاهی اوقات به این call admission control (cac) می‌گویند . cac به اینصورت است که در ابتدا که یک client ها درخواست ارسال ترافیک را به یک مقصدی به یک نودی میدهد ، آن نود بررسی می‌کند تا ببیند می‌تواند الزامات مورد نیاز مشتری را پاسخ بدهد در مدار circuit هم مثل تلفن این را داریم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

کنترل ازدحام در Tcp

نرخ فرستنده Tcp در هر لحظه تابع دو چیز است ۱- کنترل جریان ۲- کنترل ازدحام

- مکانیزم کنترل جریان با استفاده از rwnd برای پنجره ارسال فرستنده Tcp محدودیت ایجاد می‌کند

حال مکانیزم کنترل ازدحام نیز درست فرستنده Tcp با متغیر cwnd (congestion control) که بصورت دینامیک آن را تغییر می‌دهد، محدودیت دیگری را روی پنجره ارسال فرستنده اعمال می‌کند

بنابراین در فرستنده باید: تعداد بسته‌های in-flight از رابطه زیر پیروی کند

$$LastByteSend - LastByteAck \leq \min\{rwnd, cwnd\}$$

* حال اگر فرض کنیم که اندازه بافر دریافت گیرنده Tcp نامحدود باشد یعنی $Rwnd = \infty$ در نتیجه عامل محدود کننده فقط cwnd خواهد بود

* cwnd تعداد بایت‌هایی را نشان میدهد که ما در هر RTT می‌توانیم ارسال کنیم، بنابراین حداکثر نرخ ارسال فرستنده Tcp در هر ثانیه برابر است با:

$$\text{نرخ ارسال} = \frac{\text{میزان داده ارسالی}}{\text{زمان ارسال}} = \frac{cwnd}{RTT} \ \frac{Byte}{s} \xrightarrow{\text{برحسب بیت}} \text{Bit rate} = 8 \times \frac{cwnd}{RTT}$$

- در Tcp ما داریم پنجره ارسال مان را به cwnd محدود می‌کنیم بنابراین در واقع داریم نرخ ارسال مان را در هر RTT محدود می‌کنیم

الگوریتم کنترل ازدحام Tcp داراى ۲ یا ۳ فاز بسته به مدل اش دارد

Tahoe (تاهو)

۱- slow start (شروع آهسته)
۲- congestion avoidance (اجتناب از ازدحام)

Reno

۱- slow start
۲- congestion avoidance
۳- fast Recovery

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

گفتیم cwnd بصورت دینامیک تغییر می‌کند، چگونه؟

۱- Tcp با دریافت هر Ack اندازه cwnd (پنجره ازدحام) را زیاد می‌کند، اما اینکه چقدر این پنجره را زیاد می‌کند به این بستگی دارد که در چه فازی باشد

۱- در فاز slow start : با دریافت هر Ack به اندازه یک MSS (اندازه هر بسته را یک MSS می‌گیریم پس می‌توانیم بگوییم به اندازه یک بسته) cwnd را زیاد می‌کند

* نتیجه این کار این می‌شود که در هر RTT اندازه cwnd دو برابر می‌شود.

اثبات: باید ببینیم در هر RTT چند Ack دریافت می‌کنیم، برای این منظور باید ببینیم در هر RTT چند بسته ارسال می‌کنیم، ما در هر RTT، cwnd بایت ارسال می‌کنیم، داده‌ها ارسالی را بصورت بسته‌هایی با سایز MSS بایت ارسال می‌کنیم، بنابراین

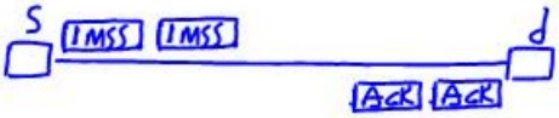
تعداد بسته‌های ارسالی در یک RTT = تعداد Ack‌های دریافتی در یک RTT $= \frac{cwnd}{MSS}$

حال به ازای هر Ack به میزان MSS به cwnd می‌افزاییم، بنابراین در یک RTT داریم:

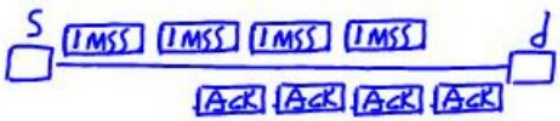
$$cwnd(new) = cwnd(old) + \frac{cwnd}{MSS} \times MSS$$

اگر متوجه نشدید به شکل زیر توجه کنید

$t=0$: cwnd = 1MSS
+1MSS



$t=RTT$: cwnd = 2MSS
+2 "



$t=2RTT$: cwnd = 4MSS
+4 "

۲- در فاز congestion avoidance

در هر RTT کلا یک MSS به پنجره ارسالمان (یعنی cwnd) اضافه می‌شود، بنابراین برای

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

اینکه این اتفاق بیفتد باید به ازای هر Ack به میزان $\frac{MSS}{cwnd} \times MSS$ تا به cwnd اضافه کنیم

سوال: این مقدار چگونه بدست آمد؟

میزانی که می‌خواهیم پنجره cwnd را در یک RTT زیاد کنیم

تعداد ack دریافتی در یک RTT

$\frac{cwnd}{MSS}$	$1 MSS$
1	?

$$\Rightarrow ? = \frac{MSS}{cwnd} \times MSS$$

مثال: فرض کنید که پنجره ارسال در ابتدا یک MSS است و تا ۶۴MSS در فاز slow start خواهیم بود و سپس وارد فاز congestion avoidance می‌شویم، نشان دهید چطور پس از یک RTT اندازه پنجره ارسال ۶۵ MSS می‌شود؟

slow start = ۱, ۲, ۴, ۸, ۱۶, ۳۲, ۶۴ MSS

۶۴ بسته در یک RTT به سمت مقصد ارسال می‌شود بنابراین ۶۴ تا ack در یک RTT به سمت شما می‌آید

به ازای هر Ack چقدر cwnd را اضافه کنیم $= \frac{MSS}{64\,MSS} \times MSS = \frac{1}{64} MSS$

$$64 \times \frac{1}{64} MSS = 1\ MSS$$

پس از یک RTT $= 64\,MSS + \underbrace{\frac{1}{64} MSS + \frac{1}{64} MSS + \cdots + \frac{1}{64} MSS}_{64 \times \frac{1}{64} MSS = 1\ MSS} = 65\,MSS$

- $\frac{1}{64} MSS$: پس از دریافت ack اول
- $\frac{1}{64} MSS$: دریافت ack دوم
- $\frac{1}{64} MSS$: پس از دریافت Ack ۶۴ام

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

توضیح فازها

۱- slow start : وقتی ارتباط Tcp شروع می‌شود، Tcp با کمترین نرخ ممکن یعنی 1mss شروع به ارسال می‌کند، پس در ابتدا مقدار cwnd را به اندازه 1mss مقداردهی می‌کند، پس با دریافت هر ack، cwnd را به اندازه یک mss زیاد می‌کند که این بدان معنی است که در هر RTT اندازه پنجره ارسال اش را دو برابر می‌کند حال این کار را تا زمانی ادامه می‌دهد که یکی از ۳ اتفاق زیر رخ بدهد

۱- به حد آستانه برسد (ssthresh) ← در اینصورت وارد فاز CA می‌شود

	Tahoe	Reno
۲- Time out رخ بدهد	پنجره ارسال به مقدار 1mss ست می‌شود و وارد فاز SS می‌شود	پنجره ارسال به مقدار 1mss ست می‌شود و وارد فاز SS می‌شود
۳- دریافت 3-Dup-Ack	//	پنجره ارسال از راس: ssthresh+۳ / سایر: ssthresh شروع می‌شود و به یکباره فاز CA را اجرا می‌کند

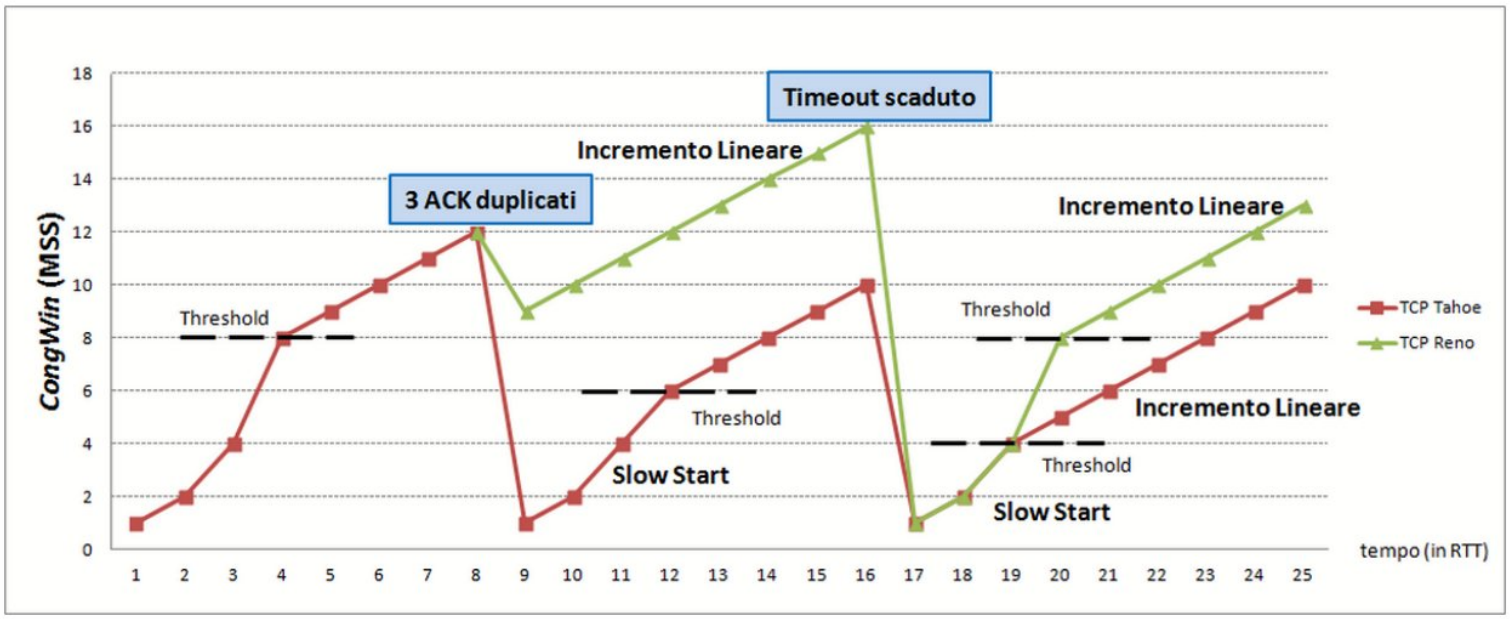
۲- congestion avoidance: در این فاز در هر RTT به اندازه یک mss اندازه پنجره ارسال را زیاد می‌کنیم تا T.O رخ دهد یا Ack تکراری فرستنده دریافت کند، که در اینصورت مانند شماره ۲ و ۳ با او رفتار می‌کنیم

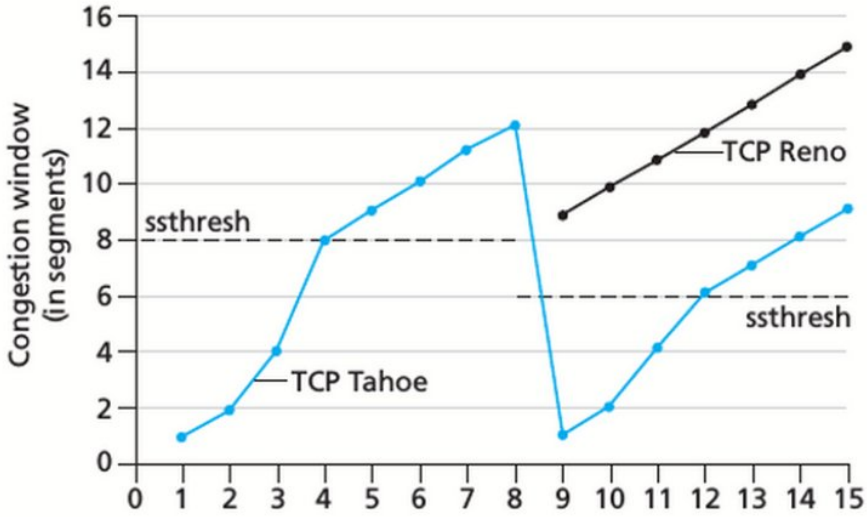
تعیین حد آستانه (ssthresh)

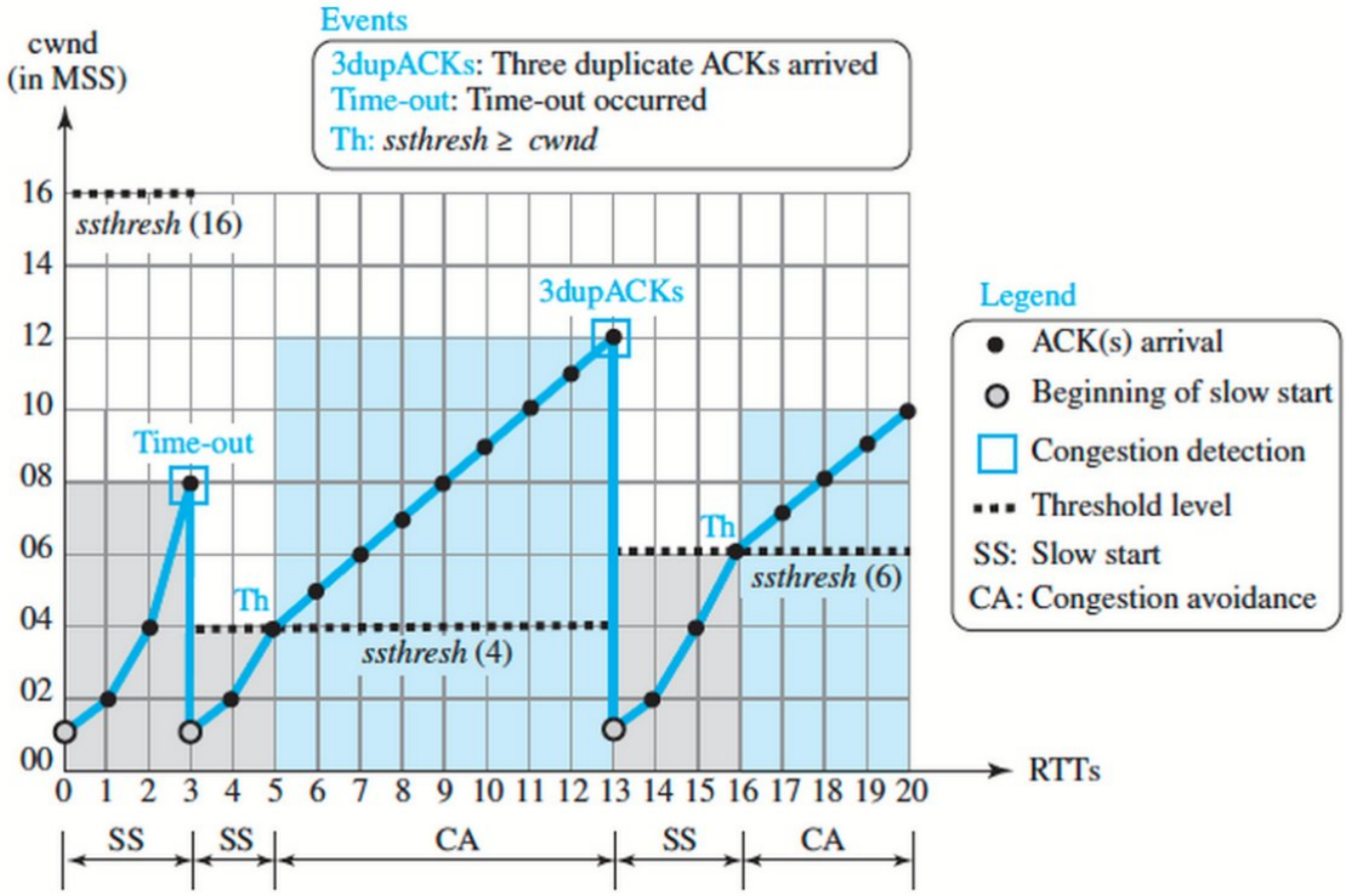
در لحظاتی که T.O رخ بدهد و یا Ack تکراری توسط فرستنده دریافت شود، مقدار حد آستانه را برابر نصف اندازه پنجره ارسال (cwnd) قرار می‌دهیم.

$$ssthresh = \frac{cwnd}{2}$$

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

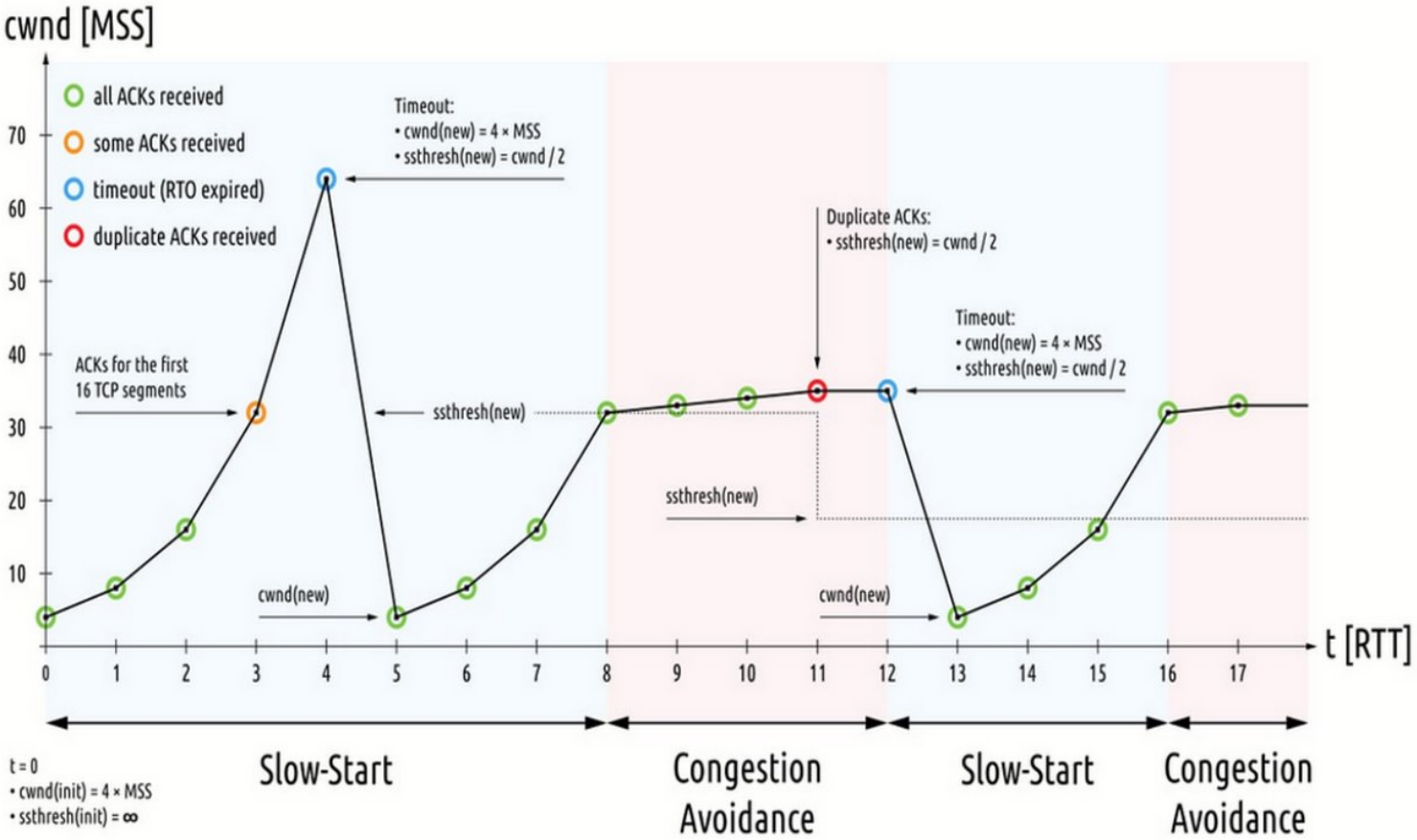






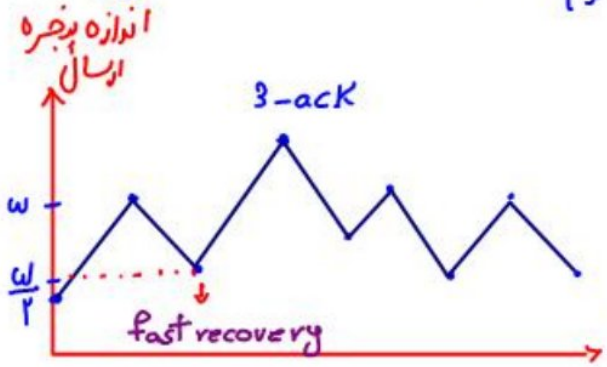
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir



گذردهی در کنترل ازدحام نسخه رنو

- برای محاسبه گذردهی ۲ فرض را نادیده می‌گیرند : ۱- فرض می‌کنند نیاز slow start نداریم
۳- T.O نداریم و فقط سه ACK تکراری می‌تواند رخ بدهد



پنجره ارسال همیشه دارد بین w و w/2 بالا و پایین می‌رود
بنا براین میانگین پنجره ارسال حدوداً $\frac{3}{4}w$ است
بنا براین متوسط پنجره ازدحام (cwnd) = $0.75W$
و بنابراین میانگین گذردهی (متوسط نرخ ارسال) = $\frac{0.75W}{RTT}$
(برای یک اتصال)

* گذردهی میانگین برای هر اتصال که loss داشته باشیم و نرخ loss را به ما بدهند

$$\frac{1.22 \times MSS}{RTT \times \sqrt{L}}$$

↳ تعداد loss

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

مروری بر ATM

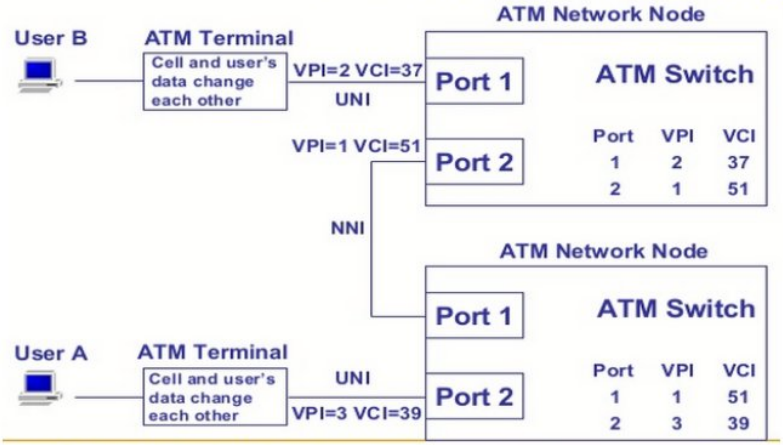
- از اهداف مهم طراحی پروتکل استک ATM این بود که یک شبکه ای درست کنیم که بتواند هم به وین وهم به ویدیو وهم دیتا با کیفیت خوب سرویس بدهد، چون الزامات یک شبکه پکت بین ان که بخواهد به وین سرویس بدهد با الزامات یک شبکه پکت بین ان که بخواهد به دیتا سرویس بدهد خیلی فرق می کند این شبکه پیچیده می شود

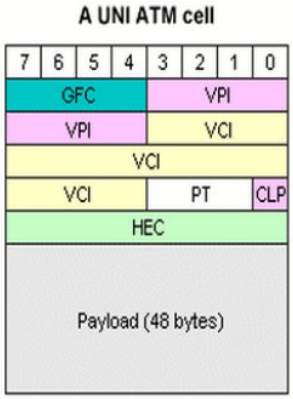
نکته) ATM connection در end point دو مدل می تواند باشد

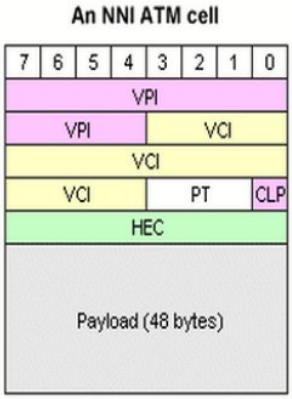
۱. user interface : یعنی در آفرخط می توانند یک یوزر به ATM وصل باشد که امروزه خیلی این حالت را نداریم، چون صحبت کردن با شبکه و چانه زدن برای پهنای باند و ... کار ساده ای برای user نیست

۲. Network inter- : یعنی اتصال Network به Network

سرانجام ATM در داخل شبکه وبین سوئیچ های شبکه در قالب NNI (network-network int-) وبین user و شبکه با یک تغییر جزئی در قالب UNI (user-network interface) باشد، بنابراین هدر سلول های ATM یکی از این ۲ فرمت زیر را می توانند داشته باشند







یک سلول ATM، ۵۳ بایت است که ۵ بایت اول اش (۴۰ بیت اول دش) هدر سلول است. بایت آخر این ۴۰ بیت HEc (Header error check) است که به دور پیدا کردن سر و ته یک سلول در یک استریم می خورد، همچنین error check HEc چهار بایت اول را انجام می دهد

GFc (Generic Flow control) : ۴ بیت است و وقتی استفاده می شود که user قصد اتصال به شبکه را دارد و مجموعا برابر ۵ است و برای کنترل ترافیک در شبکه هایی با توپولوژی Ring و Bus مجموعا کابرد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

CLP (cell loss priority) : اگر این بیت ۰ باشد یعنی این سلول مهم است و اگر ۱ باشد یعنی مهم نیست.

نکته) در IPV6 بیشتر از این دو لول داریم که آزادی عمل بیشتری به ما می‌دهد

نکته) در مالتی مدیا وقتی از scalable coding استفاده می‌کنند برای لایه پایه از ۰ و برای لایه بهبود از ۱ استفاده می‌کنند

نکته) حتی وقتی در مالتی مدیا single layer که می‌کنند می‌توان anchor picture (P, I) را ۰ و B picture را ۱ گرفت (از تصاویر B هیچ‌گاه بعنوان تصویر مرجع برای فشرده سازی تصاویر بعدی استفاده نمی‌شود)

نکته) وقتی در صف سوئیچ های ATM ازدحام به وجود می‌آید، یکی از راه‌ها این است که cell هایی که CLP=1 دارند را حذف کنند

PTI (payload type identifier) : این فیلد سه بیت است و مشخص می‌کند که payload چه نوع سلولی است، زیرا سلول های مختلفی داریم در ATM. در عین حال وقتی که این سلول ها داده یونزی هستند اطلاعاتی در مورد ازدحام در شبکه روی بیت وسط PTI که نام آن EFCI است ثبت می‌شود

EFCI (Explicit Forward congestion indication) : وقتی سلول ها داده دارند از سوئیچ های ATM عبور می‌کنند، اگر سوئیچ روی آن پورت خروجی آن دچار ازدحام بود این بیت را ۱ می‌کند، حالا وقتی یک سلول به دست گیرنده می‌رسد، گیرنده با نگاه کردن به این بیت می‌تواند متوجه شود که این سلول در هنگام عبور از شبکه ازدحام را تجربه کرده است یا نه

نکته) سمت چپ ترین بیت PTI اگر ۰ باشد بدین سلول داده‌ها یونزی است و اگر ۱ باشد دیتاها کنترلی است.

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir
شبکه های کامپیوتری
رامین رضوی

PTI	Cell type
000	User data cell, EFCI = 0, AUU = 0
001	User data cell, EFCI = 0, AUU = 1
010	User data cell, EFCI = 1, AUU = 0
011	User data cell, EFCI = 1, AUU = 1
100	OAM cell
101	OAM cell
110	Resource Management cell (RM-cell)
111	Reserved

ATM service categories

سرویس های مختلفی را در اختیار مشتریان قرار میدهد، این سرویس ها به قرار زیر هستند ATM

Real time
non Real time

۱- CBR
۲- VBR
۳- ABR
۴- UBR
۵- ABT (ATM Block Transfer)

CBR: اگر به یک قول بدهیم که سرویس CBR بهش می دهیم یعنی گارانتی می کنیم که Delay، rate و jitter ان که بهت قول دادم را حتما بهت می دهم بنابراین در CBR به سرویسی که برای user رزرو کرده ایم برای هیچ متغیر دیگری دست نمی زنیم همچنین درصد سل هایی که مفقود می شوند

VBR: به کاربر اجازه میدهد که بصورت میانگین $n \frac{mb}{s}$ را داشته باشد. بنابراین کاربر بعضی وقت ها می تواند نرخ بیشتری را ارسال کند و بعضی وقت ها نرخ کمتری

- همانند باند را برای هر دو مدل real time VBR, non Real time VBR گارانتی می کنیم ولی در real time VBR برای Delay و jitter هم سعی می کنیم گارانتی بدهیم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

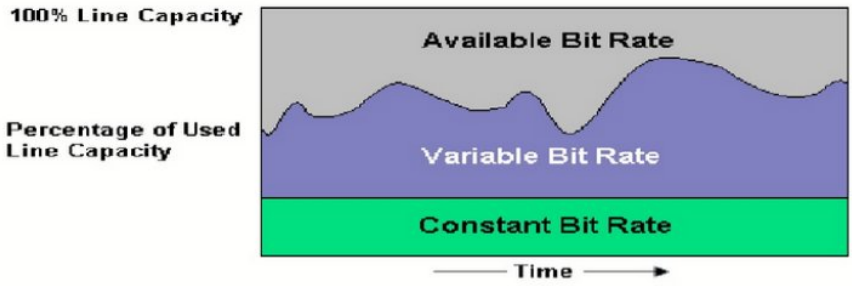
minimum cell rate(MCR)

ABR : شبکه به یوزر به یک اندازه حداقلی قول می دهد ولی اگر فضا اضافه داشت بخش اجازه میده تا هری از این ظرفیت اضافه استفاده کند ، حالا شبکه با دادن فیدبک هی مستمر به یوزر ، یوزر را از اینکه چقدر ظرفیت اضافه دارد و یوزر چقدر می تواند نرخ ارسال را زیاد کند مطلع می کند . با این روش در زمان هایی که سرویس VBR دارد از rate کمتری استفاده می کند ، رسورس باقی مانده را سرویس ABR به نحو احسنت استفاده می کند . در ادامه سرویس ABR را بیشتر باز می کنیم

(unspecified bit rate) UBR : هیچ چیزی را گارانتی نمی کند و می گوید هرچقدر که جایی وجود داشته باشم بهت اختصاص می دهم

نکته) اگر برحسب زمان به ترافیک شبکه ATM نگاه کنیم سرویس CBR نرخ ارسال ثابت است ، سرویس VBR برحسب زمان نرخ ارسال کم و زیاد می شود ، آن بخش هایی که نسبت به ظرفیت کل شبکه خالی می ماند ابتدا در اختیار ABR و اگر ABR از هم آن استفاده نکرد در اختیار UBR قرار می گیرد

ATM Capacity Allocation



	ATM Service Category					
		VBR				
Attribute	CBR	Real-time	Non-real-time	ABR	UBR	ABT
Cell loss ratio	Specified[a]	Specified[a]	Specified[a]	Specified[b]	Unspecified	Specified[c]
Cell transfer delay and delay variation	Specified	Specified	Unspecified	Unspecified[d]	Unspecified	Specified
Peak cell rate	Specified	Specified	Specified	Specified[e]	Specified[d]	Specified
SCR/MBS	Not applicable	Specified	Specified	Not applicable	Not applicable	Specified[f]
Real-time control via RM cells	No	No	No	Yes	No	Yes

[a] For CBR and VBR, the cell loss ratio may be unspecified for CLP=1 cells.
[b] Cell loss ratio is minimized for sources that adjust their cell flow in response to control information.
[c] For conforming blocks, the cell loss ratio is comparable to that for CBR. Block loss ratio is specified.
[d] Peak cell rate is not subject to CAC and UPC procedures.
[e] Represents the maximum rate at which the source may ever send. The momentary maximum allowed rate is subject to control information.

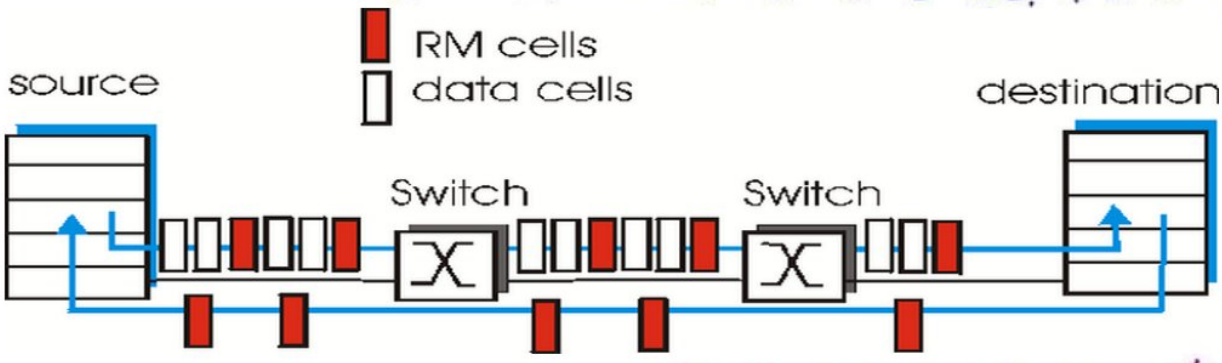
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

ABR

در قسمت قبل گفتیم که شبکه به چه طور فیدبک می‌دهد، حال می‌خواهیم بررسی کنیم که چطور این اتفاق انجام می‌شود. در ATM سلولی داریم بنام Resource management cell (RM) که در PT آن برابر ۱۱۰ است و به اینصورت است که هر ۳۲ سلولی که فرستنده ارسال می‌کند یک سلول RM ارسال می‌کند این سلول در عبور از سوئیچ‌ها شروع به جمع آوری اطلاعات می‌کند و می‌رود تا گیرنده و برمی‌گردد تا فرستنده و با این فرستنده از اطلاعات شبکه آگاه می‌شود



۵۲ بایت یک سل RM بصورت زیر است:

Field	Bytes	Description
Header	1-5	ATM header
ID	6	Protocol ID
Message Type	7	Various control bits (see the list after this table)
ER	8-9	Explicit cell rate
CCR	10-11	Current cell rate
MCR	12-13	Minimum cell rate
QL	14-17	Queue length
SN	18-21	Sequence number
Rsvd	22-52	Reserved
CRC-10	52-53	CRC-10

* بایت message type در آن ۲ بیت هم برای سرویس ABR است

CI (congestion indication): این بیت می‌تواند توسط سوئیچ‌ها و یا مقصد به ۱ ست شود

ست کردن توسط گیرنده: اگر بیت EFCI آفرین سلول داده دریافتی ۱ باشد گیرنده قبل از برگرداندن سلول RM بیت CI را ۱ می‌کند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

بیت NI (No increase) : این بیت نیز هم توسط سوئیچ ها و هم توسط گیرنده می‌تواند ست شود و بدون این بیت نشان می‌دهد که فرستنده می‌تواند سرعت فعلی ارسال اش را حفظ کند و فرستنده لازم نیست که cell rate مجازی که می‌تواند ارسال کند را کاهش بدهد

نکته ۱: این بیت زمانی 1 می‌شود که ازدحام قریب الوقوع پیش بینی می‌شود، بنابراین سوئیچ ها در ازدحام های خفیف تا متوسط از بیت NI و در ازدحام شدید از بیت CI استفاده می‌کند

فیلد ER (explicit rate) : ۲ بایت است، وقتی سل RM از یک سوئیچ رد می‌شود اگر نرخ ارسال اش روی آن لینک کمتر از مقدار درون ER باشد، این فیلد را به این مقدار تغییر می‌دهد، بنابراین وقتی این سلول به گیرنده می‌رسد و گیرنده مجددا این سلول را برای فرستنده می‌فرستد (به این سلول برگشتی backward RM cell می‌گویند) فرستنده متوجه تنگنا شبکه می‌شود و می‌تواند نرخ اش را بر اساس این تنظیم کند

نکته ۲: آهنگ جایگذاری سل های RM در بین سل های داده یک پارامتر قابل تنظیم است

نکته ۳: گیرنده می‌تواند بدون دریافت یک forward RM cell یک backward RM cell تولید کند

نکته ۴: یک سوئیچ می‌تواند یک backward RM cell تولید کند و CI و NI درون آن را ست کند

نکته ۵: با توجه به نکات بالا سل های RM می‌توانند هر دو رویکرد بازخورد مستقیم شبکه (choke packet) و بازخورد شبکه از طریق گیرنده (warning bit) را به ارمغان بیاورند

نکته ۶: در سرویس ABR نرخ ارسال فرستنده با توجه به پارامترهای CI و NI و ER بصورت دینامیک عوض می‌شود

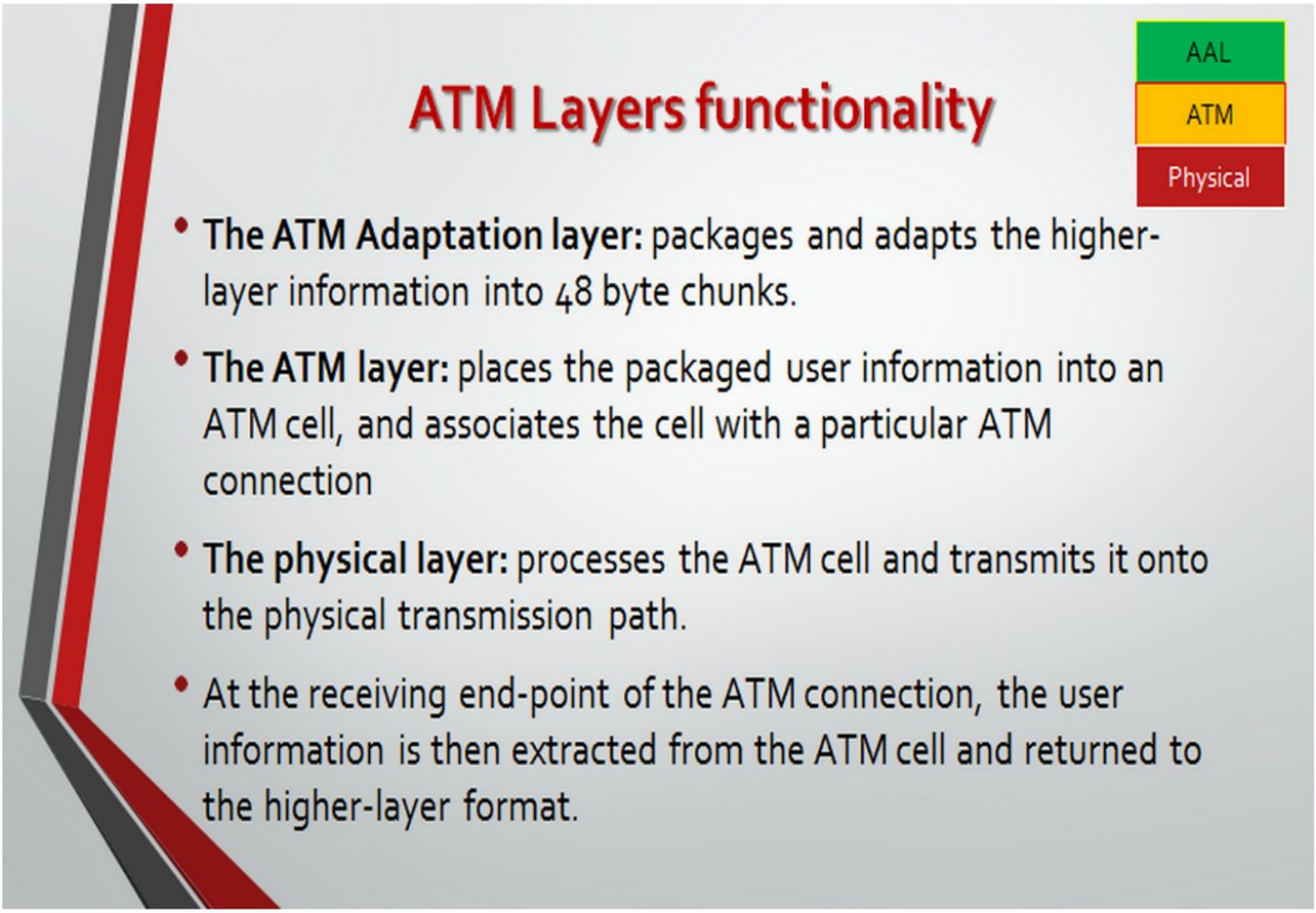
نکته ۷: سرویس ATM ABR با داشتن ساز و کار اعلام ازدحام می‌تواند نرخ ارسال فرستنده را بین MCR و حداکثر آهنگ مجاز تنظیم و کم و زیاد کند، دقت کنید که در ABR ما نرخ MCR را برای هر اتصال تضمین می‌کنیم

نکته ۸: سرویس ABR را می‌توان سرویس کمی بهتر از بهترین تلاش نامید، چون در اینجا هم شبیه IP Delay و Jitter و loss تضمین نمی‌شود

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

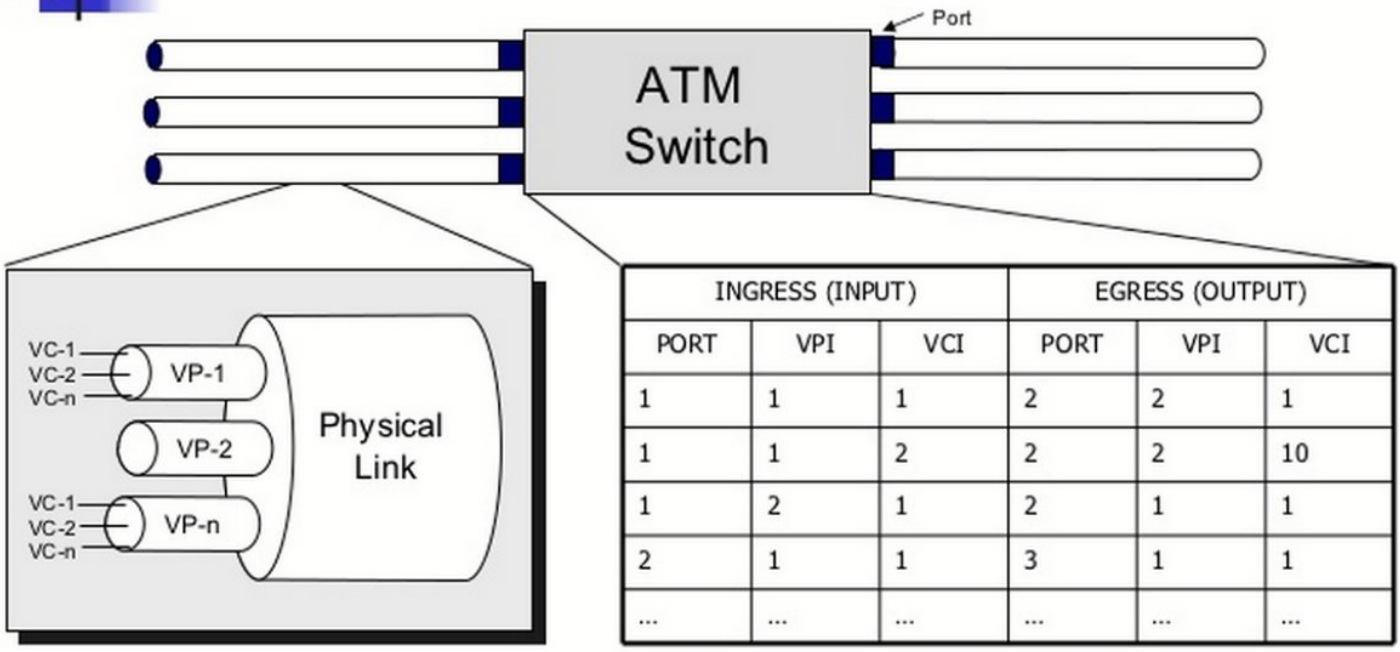
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
شبکه های کامپیوتری
@konkurcomputer
www.konkurcomputer.ir
رامین رضوی

Network Architecture	Service Model	Bandwidth Guarantee	No-Loss Guarantee	Ordering	Timing	Congestion Indication
Internet	Best Effort	None	None	Any order possible	Not maintained	None
ATM	CBR	Guaranteed constant rate	Yes	In order	Maintained	Congestion will not occur
ATM	ABR	Guaranteed minimum	None	In order	Not maintained	Congestion indication provided



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

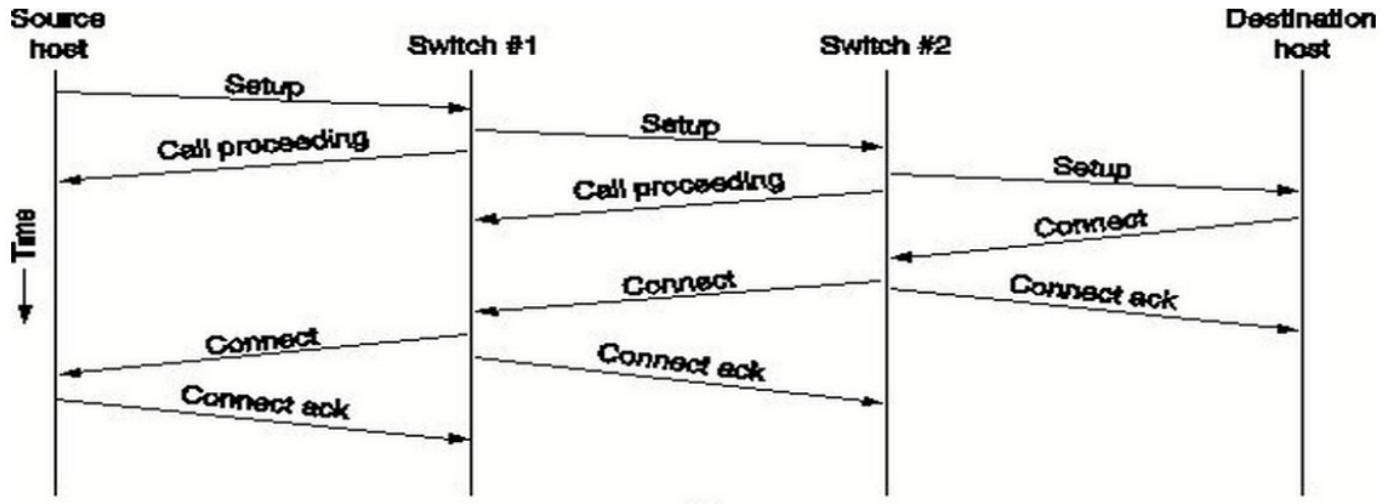
ATM Switching



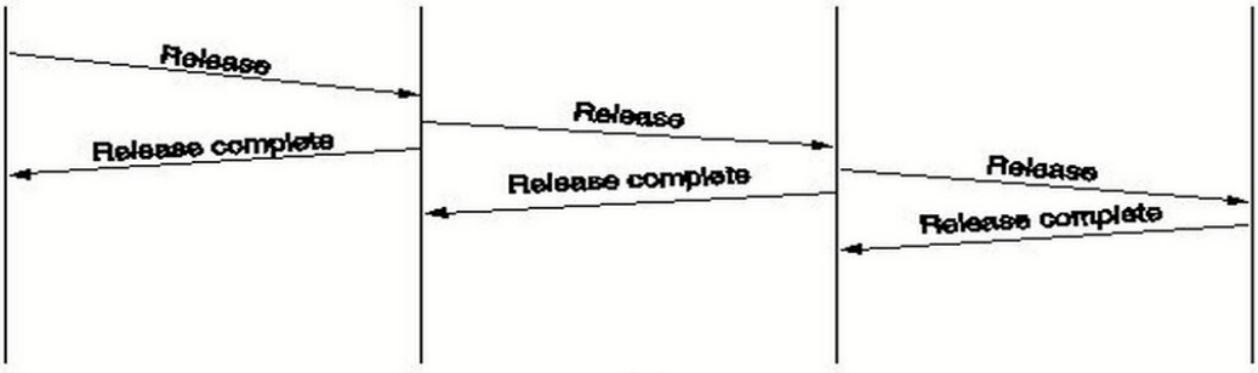
INGRESS (INPUT)			EGRESS (OUTPUT)		
PORT	VPI	VCI	PORT	VPI	VCI
1	1	1	2	2	1
1	1	2	2	2	10
1	2	1	2	1	1
2	1	1	3	1	1
...	...	...	...	...	...

- ATM switch receives ATM cell from a specific virtual channel on a particular input port
- Each ATM cell header contains VPI and VCI information
- The combination of port, VPI and VCI is unique within a switch
- Switch checks its internal routing table (local to the switch) to determine corresponding outgoing VPI and VCI that should be assigned to the cell and the output port on which the cell should be forwarded.
- The switch replaces the incoming VPI/VCI header info with the outgoing VPI/VCI info and sends the cell through the output port to the next device
- The process is repeated across multiple devices until the cell reaches its destination

The Telecom Source

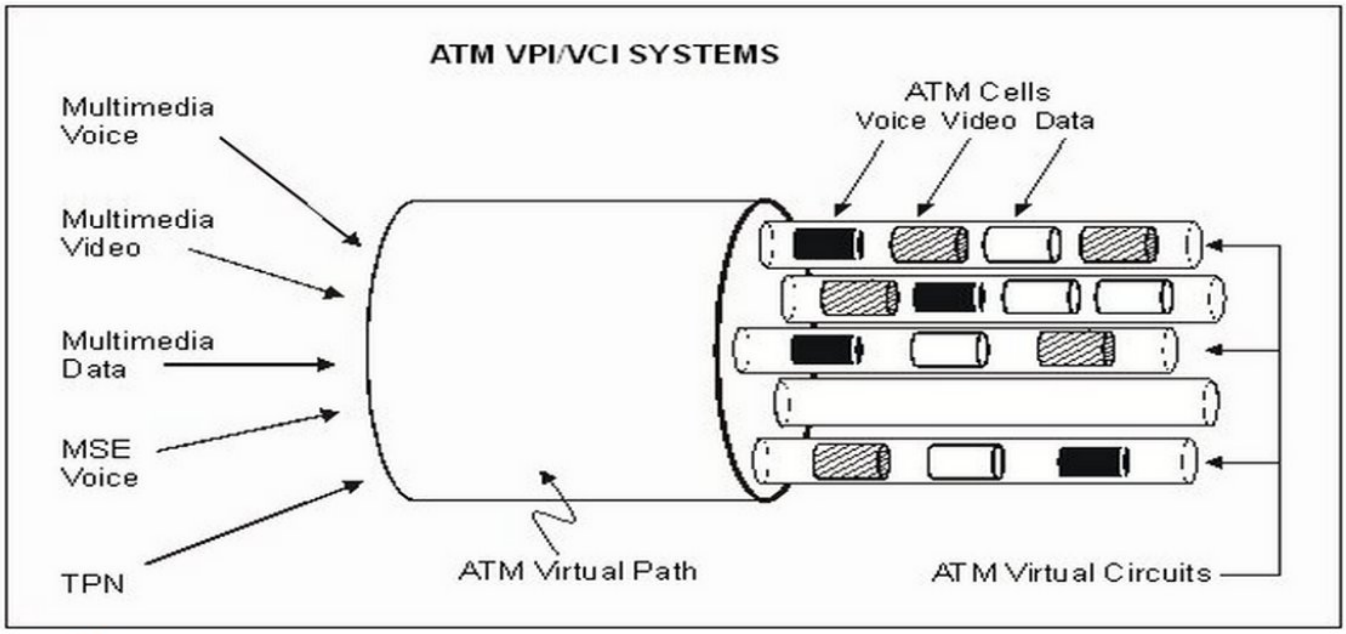


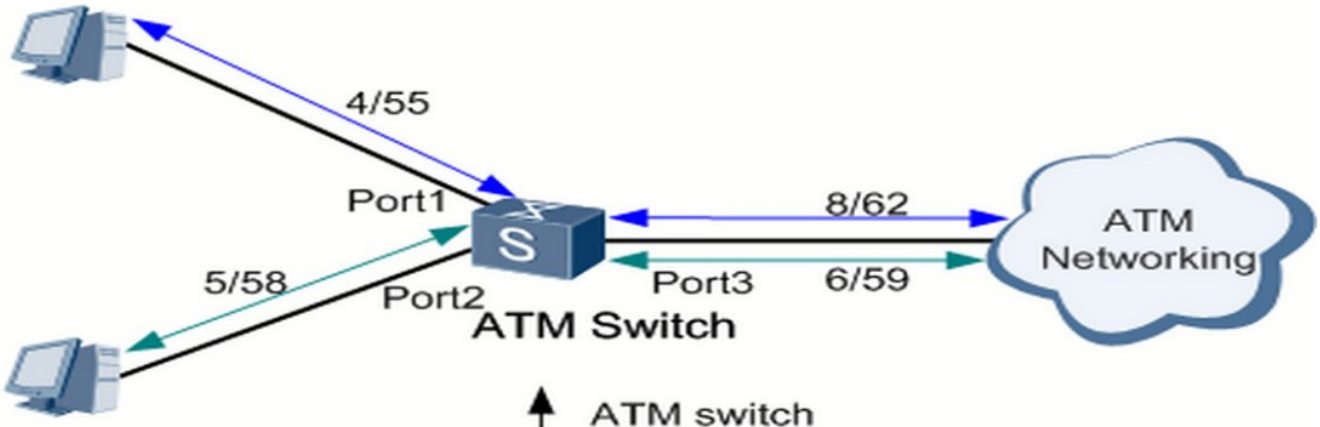
(a)



(b)

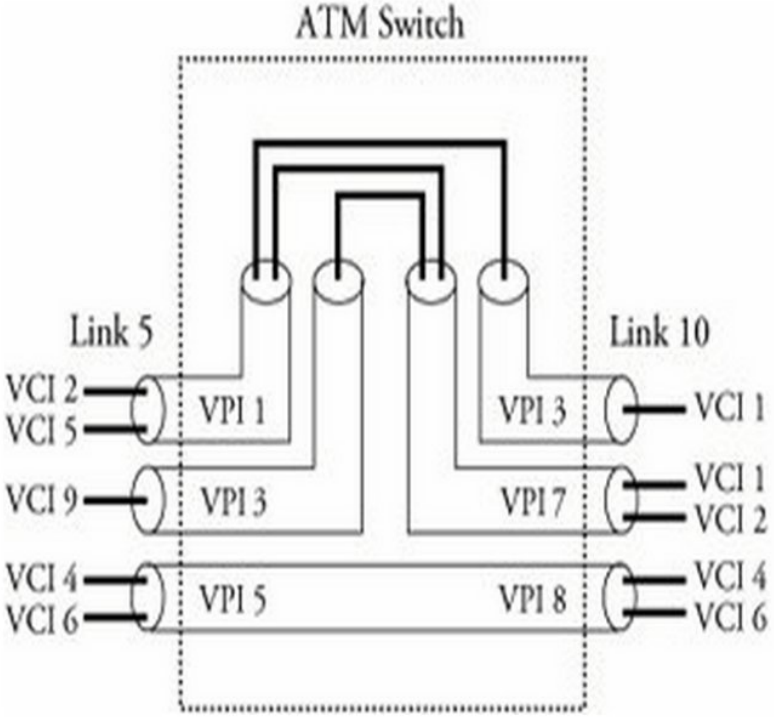
Scanned with CamScanner





ATM switch table

in		out	
port	VPI/VCI	port	VPI/VCI
1	4/55	3	8/62
2	5/58	3	6/59
3	8/62	1	4/55
3	6/59	2	5/58



Routing Table					
Incoming			Outgoing		
Link	VPI	VCI	Link	VPI	VCI
5	1	2	10	3	1
5	1	5	10	7	1
5	3	9	10	7	2
5	5	—	10	8	—

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

رامین رضوی

مهمترین وظایف لایه شبکه

روترها

۱) forwarding (هدایت) : سوئیچ کردن بسته ها

۲) Routing (مسیریابی) : توسط یک الگوریتم ، مسیر مناسب بین فرستنده و گیرنده پیدا می کنند

۳) Addressing : هر روتری که می خواهد در دنیای اینترنت باشد باید یک IP یونیک داشته باشد

منطقی

۴) connection setup : ایجاد و قطع کانکشن در شبکه های مدار مجازی

۵) protocol mapping : اتصال پروتکل های متفاوت لایه پیوند داده کنم

۶) load Balancing : مسیریابی را جوری انجام دهیم که موازنه بار تحقق گردد .

۷) congestion control : گر از کنترل ازدحام شبکه باید استفاده کنیم داریم

Routing : یافتن بهترین مسیر بین فرستنده و گیرنده ، یکی از کارهایی که الگوریتم های مسیریابی می کنند آن است که forwarding table های روترهای شبکه را بصورت پریودیک آپدیت کنند

این مسیریابی می تواند براساس اهداف زیر باشد :

۱) min Delay
۲) Reallbility یا قابلیت اطمینان ← min loss
۳) کوتاهترین فاصله بین فرستنده و گیرنده
۴) اندازه ترین مسیر

مسیریابی از یک لحاظ به ۲ دسته { متمرکز / توزیع شده

توزیع شده ، هم مسیریاب ها باید با همدیگر در مسیریابی شرکت می کنند و هر مسیریاب بخشی از الگوریتم مسیریابی توزیع شده را اجرا می کند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

switching = forwarding = فرستادن و انتقال یک بسته، با توجه به جدول forwarding از یک پورت (لینک) ورودی به یک پورت (لینک) خروجی در داخل یک روتر یا سوئیچ، این کار براساس آدرس مقصد یا یک تگ (شناسه) در مدار مجازی صورت می‌گیرد

توجه: این پورت‌ها فیزیکی هستند

توجه: مسیریابی همه مسیریابی‌ها بین گره مبدا و مقصد را تعیین می‌کند، در واقع برهم‌کنش بین لایه‌ها به گونه‌ای است که مسیریابی است که مسیر دقیق بسته‌ها از مبدا به مقصد را مشخص می‌کند، بنابراین forwarding عملی است در داخل یک روتر یا سوئیچ برای انتقال یک بسته از واسط لینک ورودی به لینک خروجی ولی مسیریابی فرآیندی است مربوط به کل شبکه که مسیر انتها به انتهای بسته‌ها از مبدا به مقصد را تعیین می‌کند

٤) connection setup: این نقطه در شبکه‌های مدار مجازی معنی پیدا می‌کند و در شبکه‌های دیتاگرام معنی ندارد. (این مورد فقط در شبکه‌هایی است که به آن شبکه‌شون connection oriented باشد) در شبکه‌های مدار مجازی قبل از شروع به ارسال داده ما یک فاز اولیه connection setup داریم. یعنی در این شبکه‌ها روترهای بین مبدا و مقصد در ابتدا با هم سیگنال‌هایی کنترلی رد و بدل می‌کنند و سپس یک کانکشن ایجاد می‌کنند که یک مسیر ثابت بین مبدا و مقصد برقرار می‌شود و کلیه منابع رزرو می‌شود. و وقتی ارتباط تمام شد کانکشن را release می‌کنند، شبکه‌های ATM، FrameRelay، mpls و غیره نمونه‌هایی از این شبکه‌ها هستند.

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

کلا یه شبکه چه سرویس هایی می تونه ارائه بده؟ (داریم کلی صحبت می کنیم)

۱) تضمین Delivery بسته ها : (تحویل تضمینی) : بسته حتما به مقصد برسه . البته تضمین نکردم که درست برسه

۲) تضمین دست نخوردن بسته ها

۳) تحویل منظم بسته ها به گیرنده (inorder Delivery)

۴) تضمین Delay

۵) تضمین حداقل پهنای باند

۶) گارانتی حداکثر jitter : فرض کنید دوتا کانکشن داریم ، کانکشن اول داره تاخیرش بین ۱۰ تا ۳۰ هست یعنی میانگین ۲۰ ، کانکشن دوم داره تاخیرش بین ۵۰ تا ۵۲ یعنی میانگین ۵۱ است ! حالا اگر تاخیر برای ما مهم است ما کانکشن اول را می پسندیم ، اما اگر jitter کم برای ما مهم است ، دومی را انتخاب می کنیم . بعضی ها jitter را با استفاده از بافر در مقصد درست می کنند ، اگر در مقصد مثلا در مورد ماشین مدیا کل جریان داده را به اندازه تفاوت بین min و max تاخیر ، به تعویق بیندازیم و باز کنیم ، مشکل jitter حل میشود

برخی از معماری های شبکه

۱) اینترنت : اینترنت پروتکل اینترنت فقط یک سرویس بنام سرویس best effort ارائه می کند

۲) ATM : اتصال های ATM مختلف روی یک شبکه ، می توانند سه از مدل های سرویس دهی مختلف استفاده بکنند ⟵ سرویس ATM CBR
سرویس ATM ABR

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

IP از سوئیچینگ بسته استفاده می‌کند در حالی که ATM از سوئیچینگ مدار مجازی استفاده می‌کند، در IP بسته‌ها از مسیرهای مختلف به سمت مقصد می‌روند و هیچ اتصالی نیز در ابتدا برقرار ایجاد نمی‌شود اما در ATM یک فاز ایجاد اتصال داریم که در این فاز یک مدار مجازی بین مبدا و مقصد ایجاد می‌شود که همین موضوع باعث می‌شود که سرویس‌های IP و ATM خیلی با هم تفاوت کنند

- لایه شبکه در پشته پروتکل اینترنت فقط یک سرویس موسوم به best effort ارائه می‌کند و این سرویس به این گونه است که نه ارسال بسته‌ها، نه تحویل به ترتیب بسته‌ها، نه تأخیر، نه jitter ← تضمین خاصی ندارد همچنین این دیدگاه هم این است که بسته‌ها از مسیرهای مختلف می‌روند. نه پهنای باند، نه ازدحام، نه هیچ‌کدام

- ATM یک مدار مجازی و یک مسیر ثابت بین مبدا و مقصد ایجاد می‌کند. اما مسیر ثابت لزوما به معنا داشتن Delay و jitter ثابت نیست، اما وقتی منابع را رزرو کنیم می‌توانیم jitter و تأخیر را تضمین کنیم.

۲ نوع سرویس ATM ارائه می‌دهد:

۱) سرویس ATM CBR: وقتی نرخ ارسال برنامه‌ها ثابت باشد، یک مدار مجازی بین فرستنده و گیرنده می‌سازیم و مثل آن عمل می‌کند در واقع و به فرستنده و گیرنده یک پهنای باند ثابتی را اختصاص می‌دهد ← یعنی یک مسیر در شبکه برای این اتصال پیدا می‌کند و در تمام آن لینک‌ها به آن اتصال پهنای باند ثابتی را اختصاص می‌دهد. ← پس تأخیر انتها به انتها یک سطح تضمین می‌شود

- jitter تضمین می‌شود
- loss " "
- ازدحام نیز رخ نمی‌دهد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

سرویس ATM ABR : در معماری شبکه ATM ABR ترافیک هر اتصال از نوع VBR است و هر زمان یک min و یک max نرخ ارسال دارد، ATM می آید و برای هر اتصال یک میانگین $\frac{min}{2}$ که خودش با کارهای آماری بدست می آورد رزرو می کند. که ATM از این عدد بیشتر هم با توجه به شرایط شبکه می تواند به آن اتصال بدهد

↓
equivalent capacity

نکته: در ATM برخلاف IP ترتیب تحویل سلول ها هرگز بهم نمی خورد

تکنولوژی: Frame Relay → ATM → mpLs

وجه مشترک هر سه تای اینها این است که هر سه از آتش virtual circuit استفاده می کنند.

مقایسه بین شبکه های مدار مجازی و دیتاگرام

یادمان هست که لایه ی شبکه می تواند دو نوع سرویس اتصال گرا و نا اتصال را در اختیار لایه ی بالاتر از خودش قرار دهد مثل لایه ی اتصال گرا که درخواست به لایه ی App سرویس متصل ارائه دهد از Tcp استفاده می کرد و گفت می خواست که به لایه ی App سرویس نا متصل ارائه کند از Udp استفاده می کرد. بنابراین در لایه ی شبکه نیز ما می توانیم سرویس متصل یا نا متصل ارائه کنیم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

- لایه انتقال سرویس اش از پروسس مبدا است تا پروسس مقصد و می گویند process to process ولی لایه شبکه سرویس که ارائه می دهد از کامپیوتر مبدا است تا کامپیوتر مقصد و می گویند host to host است.

- لایه شبکه یا یک سرویس ناانتصال (connection less) host to host ارائه می کند و یا یک سرویس connection ori- host to host، در هیچ معماری شبکه این دو با هم ارائه نمی شوند

حال می خواهیم در مورد ۲ شبکه صحبت کنیم < شبکه مدار مجازی / دیتاگرام

شبکه مدار مجازی: شبکه کامپیوتری ای که در لایه شبکه فقط سرویس متصل ارائه کند را شبکه مدار مجازی می گویند

شبکه دیتاگرام، " " " " " " " ناانتصال ارائه کند

توجه: سرویس اتصال را لایه انتقال فقط در سیستم های انتهایی پیاده می شوند، در حالیکه سرویس متصل لایه شبکه علاوه بر سیستم های انتهایی در مسیریاب های هسته شبکه نیز پیاده سازی می شوند

virtual circuit Network

شبکه های Frame Relay, ATM, mpLS از نوع شبکه های مدار مجازی هستند و در لایه شبکه از اتصال استفاده می کنند. به اتصال های لایه شبکه مدار مجازی (VC) گفته می شود.

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

یک VC (virtual circuit) شامل سه بخش است

۱- یک مسیر (path) از مبدا به مقصد

۲- شناسه VC (VC number) : به هر لینک مسیر یک شماره داده می‌شود

۳- entries in forwarding table در روترهای روی مسیر

یک مدار مجازی مراحل زیر را از سر می‌گذراند

۱- VC setup : ۱- لایه شبکه مسیر بین مبدا و مقصد را مشخص می‌کند
(برپایی VC) ۰ لینک‌ها و روترهایی که این مدار مجازی از آنها عبور می‌کند

۲- لایه شبکه شماره VC لینک‌های روی مسیر را مشخص می‌کند

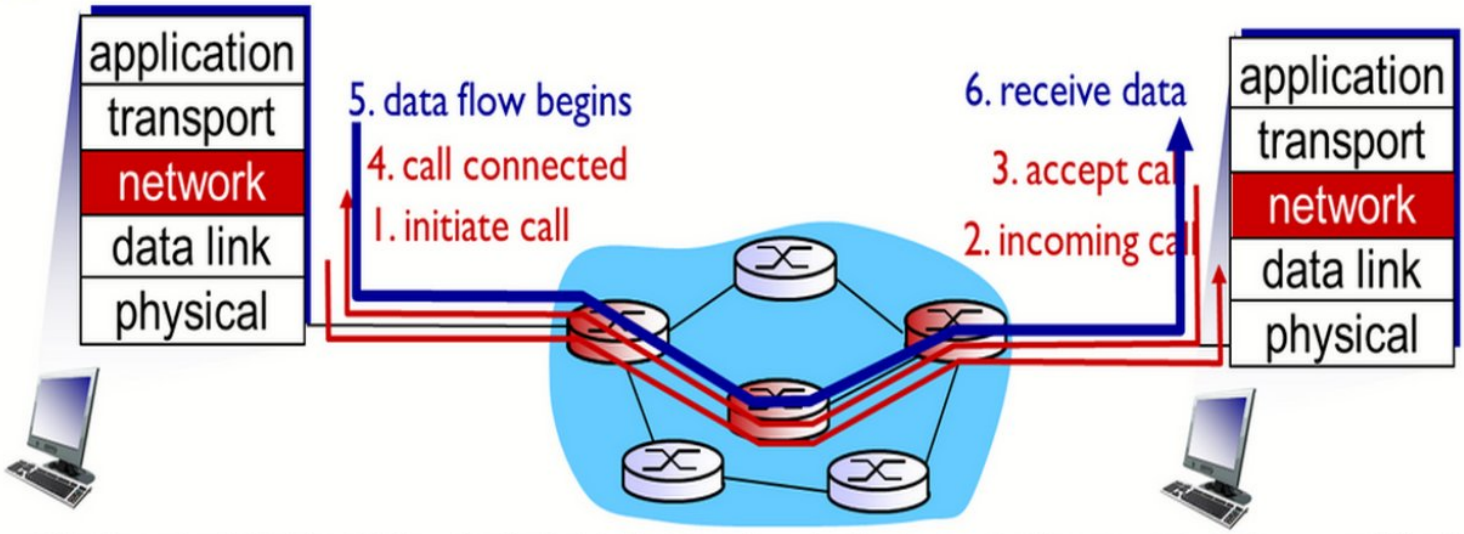
۳- " " مدخل‌های مورد نیاز را به forwarding table های روترهای روی مسیر اضافه می‌کند

۴- اگر لازم باشد منابع لازم در طول مسیر را رزرو می‌کند

۲- تبادل داده : فرستنده و گیرنده روی این VC برای هم دیتا می‌فرستند

۳- VC teardown : ۱- لایه شبکه ابتدا قطع تماس را به سیستم انتهایی اطلاع می‌دهد

۲- مدخل‌های مربوط به این VC از forwarding table های روترهای روی مسیر حذف می‌شوند



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

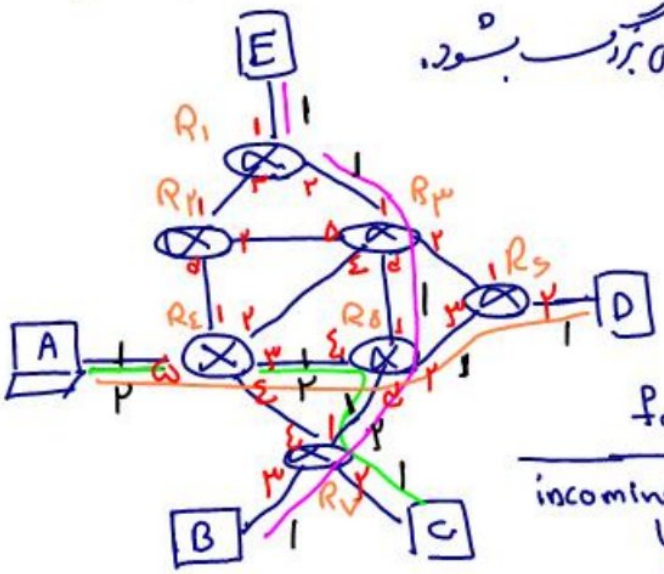
شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

چرا بسته روی تمامی لینک ها مسیر خود از یک شماره VC ثابت استفاده می کند؟

۱) طول فیلد VCI در هدر بسته ها محدود است و همین طور این کار باعث کوچک شدن طول فیلد VCI و بنابراین کمتر شدن سربار در هدر بسته ها می شود. اگر روی یک لینک n تا VC وجود داشته باشد شماره هایی که به VC ها می دهیم از ۱ است تا n و هر لینک مستقل از سایرین شماره گذاری می کند و چون VC ها سوجود روی یک لینک خیلی کمتر از تعداد VC در کل شبکه است، این عدد نمی تواند خیلی بزرگ شود.



انتقال ها:
سبز: A → C
بنفش: E → B
نارنجی: D → A

forwarding table R4

incoming port	VC#	outgoing port	out-VC#
۵	۱	۳	۱
۵	۲	۳	۲

۲) اگر کسی بخواهد شماره منحصر به فرد داشته باشد، باید پیام های زیادی بین تمامی لینک ها در شبکه بین روترها جابجا شود و بنابراین الگوریتمی که بخواهد شماره ها را در دنیا unique کند خیلی پیچیده می شود و تاخیر زیادی هم به ارمغان می آورد.

شبکه های دیتاگرام:

آدرس های IP ۳۲ بیتی هستند، بنابراین ما 2^{32} یعنی ۴ میلیارد آدرس در اینترنت داریم، یک راه برای پیاده سازی forwarding table این است که بیاییم برای هر روتر ۴ میلیارد سطر بذاریم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Datagram forwarding table

Destination Address Range	Link Interface
11001000 00010111 00010000 00000000 through 11001000 00010111 00010111 11111111	0
11001000 00010111 00011000 00000000 through 11001000 00010111 00011000 11111111	1
11001000 00010111 00011001 00000000 through 11001000 00010111 00011111 11111111	2
otherwise	3

Q: but what happens if ranges don't divide up so nicely?

Longest prefix matching

longest prefix matching

when looking for forwarding table entry for given destination address, use *longest* address prefix that matches destination address.

Destination Address Range	Link interface
11001000 00010111 00010*** *********	0
11001000 00010111 00011000 *********	1
11001000 00010111 00011*** *********	2
otherwise	3

examples:

DA: 11001000 00010111 00010110 10100001 — which interface?

DA: 11001000 00010111 00011000 10101010

DA: 11001000 00010111 00011000 10101010 — which interface?

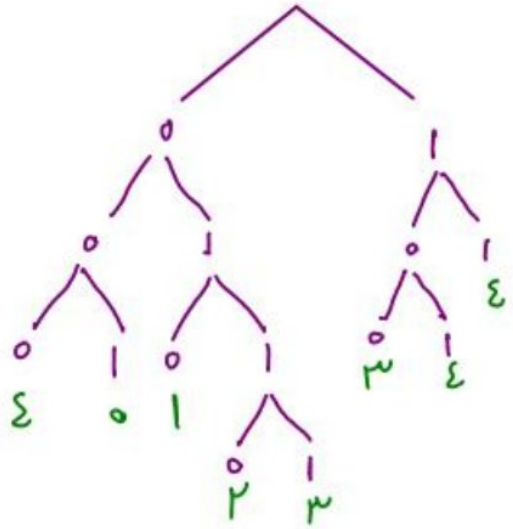
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

سوال: باتوجه به جدول هدایت مربوط به یک روتر که در زیر برایتان آورده‌ایم، رنج IP مقصد بسته‌های خارج شده از پورت ٤ را بدست آورید.

Destination add Rang	link interface
٠٠١	٠
٠١٠	١
٠١١	٢
١٠٠	٣
٠١١١	٣
otherwise	٤



٠٠٠ x — x (٢٩ بیت) ⇒ ٠٠٠٠H - ١FFF H

١٠١ x — x (٢٩ بیت) ⇒ A٠٠٠H - BFFF H

١١ x — x (٣٠ بیت) ⇒ C٠٠٠H - FFFFH

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

اما نیاز ما به این کار نیست و ما پیشوند آدرس ها مقصد را در forwarding table ها خودمان انجام

حال وقتی یک بسته به یک روتر می رسد، روتر طولانی ترین سطر forwarding table را که با آدرس

مقصد بسته مطابقت دارد برای هدایت بسته استفاده می کند، به این قاعده :

longest prefix matching می گویند .

نکته : در شبکه های دیتاگرام، الگوریتم های مسیریابی هستند و forwarding table روترها را آپدیت

می کنند و این کار را در حدود هر 1 دقیقه یکبار انجام میدهند . اما در شبکه های مدار مجازی

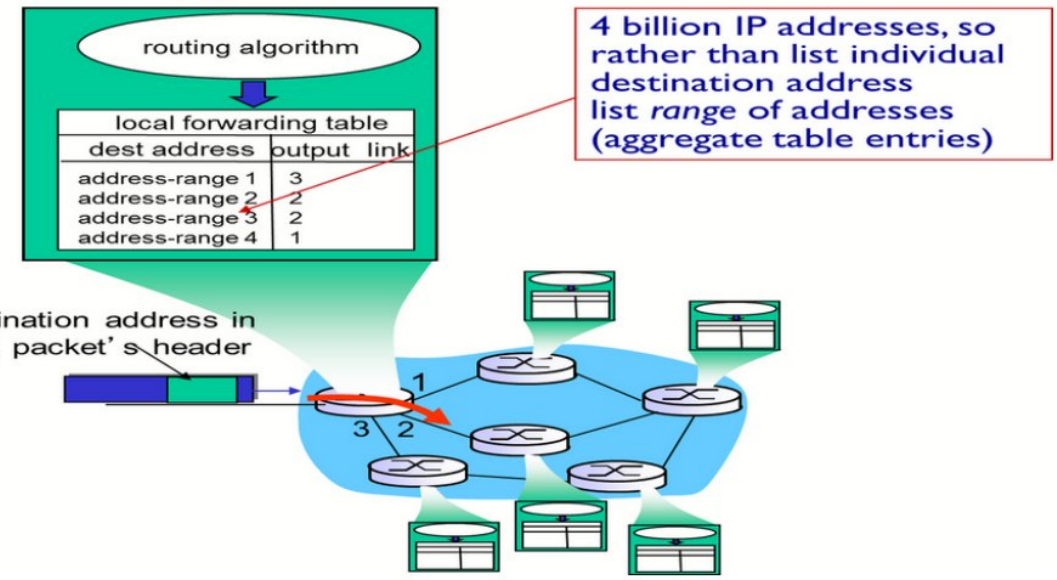
connection close و در فاز connection setup و forwarding table های روترها فقط در فاز

بسته شدن یک اتصال قبلی ← (عبور) ایجاد یک اتصال جدید ← آپدیت می شوند

نکته : می دانیم در شبکه های دیتاگرام، forwarding table روترها در هر لحظه می تواند update شوند

بنابراین ممکن است بسته هایی که مقصدشان یکسان هستند، مسیرهای متفاوتی را در رسیدن

به مقصد طی کنند .

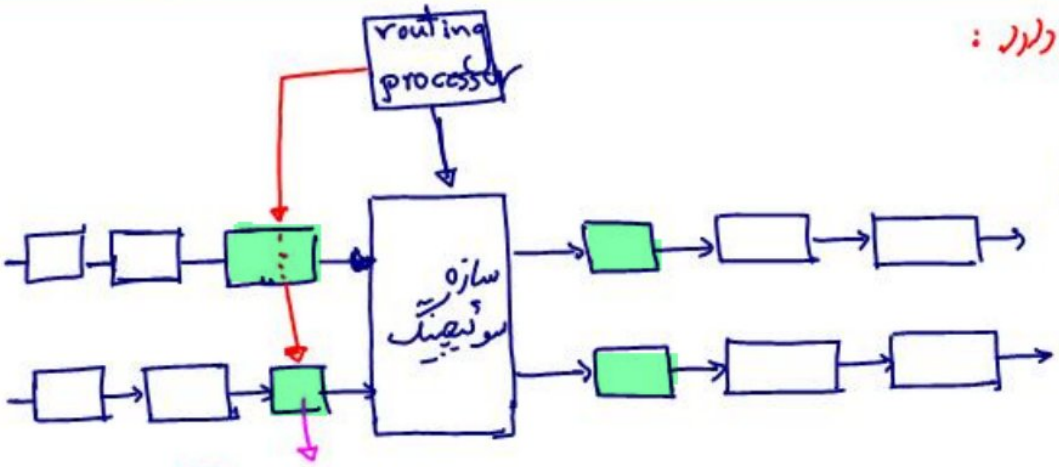


سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

رامین رضوی



درون یک روتر چه چیزهایی وجود دارد :

- حداقل یکی پورت ورودی
- یکی پورت خروجی دارد ، که پورت ها دوطرفه هستند

محل حیتصب و فوارلینگ

* هر پورت ورودی یک cpu بنام forwarding proce- دارد و همین طور یک جدول فوروردینگ برای خودش دارد . البته جدول فواردینگ همه پورت ها مانند هم است. دانشه بالیم

- در لایه شبکه پورت های ورودی و خروجی صف داریم و هردو اینها می توانند پر شوند و در هر دوی توانیم loss بنابراین
- مسیریابی در پورت ها انجام نمی شود ، و هر روتر یک routing processor دارد و این پردازنده برنامه ای درون خودش اجرا می کند ، که در اثر آن با دوترهای دیگر پیغام رد و بدل می کند و در اثر آن برای هر پست تصمیم گیری می کنند که ، rout اش به چه شکلی باشد در واقع forwarding table را می سازند

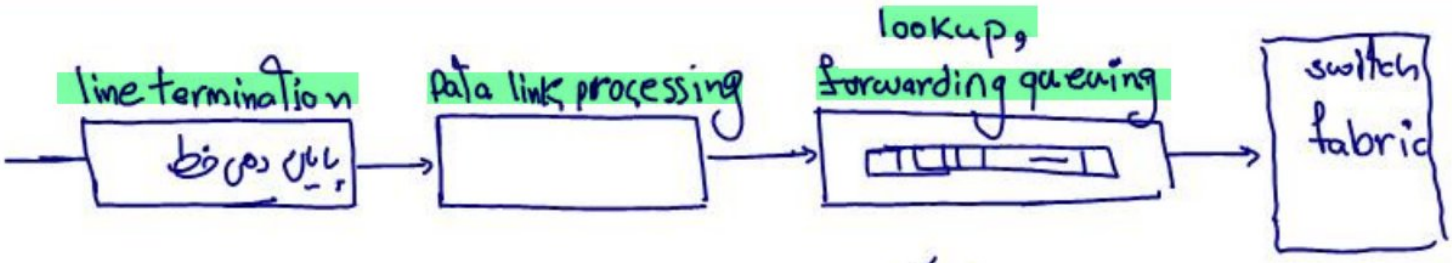
وظایف routing proces :

1) اجرای الگوریتم های مسیریابی
2) نگهداری و ساخت forwarding Table
3) نگهداشتن اطلاعات حالت پورت های متصل به روتر
4) نگهداری جداول مسیریابی
5) کارهای مدیریتی شبکه

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir



* عمل forwarding بسته و نگاه کردن جدول forwar توسط هر پورت forwarding proc بصورت سخت افزاری انجام می شود، چون این کار برروی Data path شبکه قرار دارد (این کار کار Data path ان است) اما صحبت کردن روترها با هم و ساخت جداول هدایت کاری control path ان است و نرم افزاری معمولا انجام می شود.

نکته: بسته ای که از یک سوئیچ رد می شود، همه فایش نیز عوض می شود، چون TTL و برخی دیگر از پارامترهای (فیلدهای) تغییر می کند

switching fabric: سازه سوئیچینگ چه مدل هایی دارد؟

۱) سوئیچینگ از طریق حافظه
۲) " " " باس
۳) " " " یک شبکه میان ارتباطی

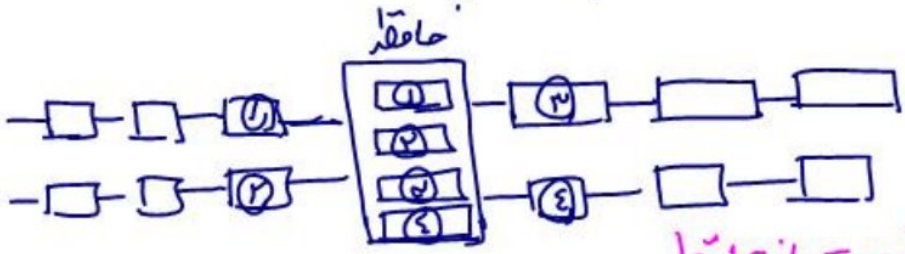
۱) سوئیچینگ از طریق حافظه

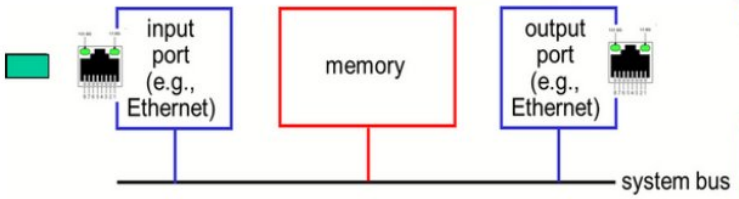
دو حالت را می توانیم برای این دسته بگیریم
۱) یک حافظه و یک cpu مسیریابی داشته باشیم
۲) یک حافظه داشته باشیم و هر پورت ورودی ای پردازنده داشته باشد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

① پورت های ورودی وقتی بسته ای بهشون می رسه، از طریق یک دقیقه نرم افزاری این را به routing process ارجاع می دهند، سپس cpu این بسته را به حافظه منتقل می کند، بعد پردازنده این بسته را از حافظه برمی دارد و با توجه به آدرس مقصد بسته و با توجه به Forwarding Table پورت مقصد را شناسایی می کند و بسته را می گذارد در حافظه مربوط به آن پورت





- در واقع در اینجا ما داریم در یک قسمت از حافظه می نویسیم، بعد می خوانیم و در جای دیگری می نویسیم

② هر پورت ورودی یک cpu داشته باشد که همه این ۴ به حافظه دسترسی داشته باشند، حال هرکدام از اینها بصورت جداگانه آدرس مقصد هر بسته را بدست بیاورند و بروند در حافظه مربوط به پورت مقصد بنویسند (multi processor shared memory)

- چون یک حافظه داریم، حافظه سرعت ما را محدود می کند

- اگر بخواهیم B بسته در ثانیه در این حافظه بنویسیم یا بخوانیم، در هر ثانیه چند بسته را می توان سوئیچ کرد؟
$\frac{B}{2}$ بسته در هر ثانیه. چون هر سوئیچ کردن نیاز به یکبار خواندن و یک بار نوشتن دارد.

سوئیچینگ از طریق باس (گذرگاه)

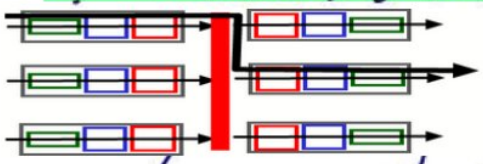
وقتی یک بسته از ورودی میاد، با توجه به اینکه باید به چه پورت خروجی ای هدایت شود، table پورت خروجی رو آن بسته نگه داشته می شود و سپس آن بسته را روی باس می گذاریم، فقط پورتی که این شماره

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

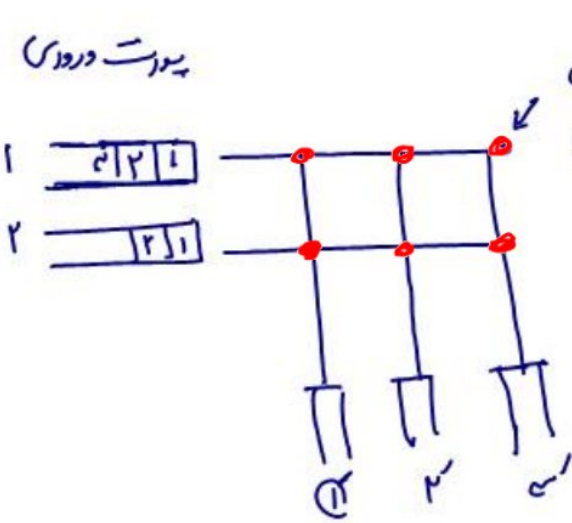
@konkurcomputer
www.konkurcomputer.ir

مختص آن است، آن بسته را برمی‌دارد. مزیت دیش این است که سرعت اش می‌تواند از روش قبلی بیشتر باشد ولی اشکال اش آن است که باز نیز مانند حالت قبل دو تقریبا همزمان نمی‌توانند فروارد شوند؟



۳) سوئیچینگ از طریق شبکه‌های میان ارتباطی:

در اینجا شبکه‌ای بهم پیوسته از باس‌ها استفاده می‌کنیم، با این کار بر محدودیت یک باس غلبه می‌کنیم، این شبکه میانی می‌تواند یک شبکه بهم پیوسته از سوئیچ‌های کوچک باشد، که M پورت ورودی را با N پورت خروجی متصل می‌کند، که به این توپولوژی شبکه میان ارتباطی گفته شده crossbar می‌گویند که switch fabric controller می‌تواند در هر لحظه نقاط تقاطعی که وجود دارد را باز کند یا ببندد



پردازش خروجی: اگر از چند پورت ورودی با نرخ زیاد به یک پورت خروجی هدایت شوند، صف خروجی داران ازدحام می‌شود و صف‌های پورت‌ها خروجی پر می‌شوند

درگیری‌ها تلفات بسته داریم؟ تلفات بسته یا در مسیر بسته‌ها رخ میدهد (روی سیم‌ها و سوئیچ‌ها) و یا در صف‌های پورت‌های ورودی یا خروجی روترها.

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

R_{line} = نرخ ارسال خطوط ورودی و خروجی = $\frac{\text{بسته}}{s}$

N = تعداد پورت های ورودی

N = ~ ~ خروجی

R_{switch} = نرخ اتصال بسته از پورت ورودی به پورت خروجی

if $R_{switch} \geq N \cdot R_{line}$ → احتمال تشکیل صف در پورت های ورودی بسیار اندک است، اما اگر سرعت سازه سوئیچ نسبت به سرعت خطوط ورودی آنقدر سریع نباشد که همه بسته های ورودی را بدون تاخیر از خود عبور دهد آن گاه در ورودی پورت ها ممکن است صف تشکیل شود.

- بارترین این که به یک پورت خروجی وارد می شود دارای نوسان است، حال اندازه بافر خروجی برای کنترل کردن این نوسانات چقدر باشد خوب است؟

برای وقتی که تعداد اتصال Tcp کم است

نرخ بیت (ظرفیت) → ظرفیت لینک لینک خروجی برحسب $\frac{b}{s}$

اندازه بافر خروجی برحسب بیت ← $B = RTT \times C$ ← ظرفیت لینک

تاخیر زمان رفت و برگشت برحسب ثانیه

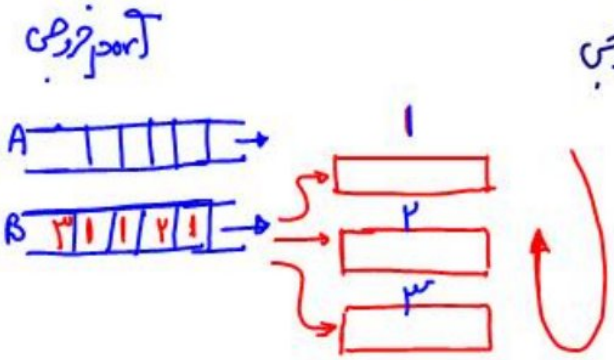
وقتی تعداد زیادی اتصال Tcp داریم؟

$B = \frac{RTT \times C}{\sqrt{N}}$ → تعداد اتصالات Tcp

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

- تعدادی بسته در صف خروجی برای ارسال روی لینک خروجی قرار دارد، حال سوال این است که به چه نحوی اینها را از داخل صف برداریم و روی لینک خروجی بفرستیم؟



برای این منظور یک packet scheduler روی پورت خروجی داریم که به مدل های مختلف می‌تواند این کار را انجا دهد

- first come first served
- weighted for queuing

سیاست هایی که موقع پرشدن صف ها ورودی وجود دارد

الگوریتم های مدیریت فعال صف active queue management

صف پرشده باشد
- (۱) drop tail = قیچی کردن = بعد از پرشدن صف بسته های تازه وارد
- (۲) بسته های وسط صف را دور می اندازیم.

قبل از اینکه پرشود
- RED (Random early detection): قضیه زودرس تصادفی

در RED یک min_{th} و یک max_{th} و در هر لحظه از زمان یک میانگین وزنی از طول صف محاسبه می شود

میانگین طول صف خروجی =
- $\leq min_{th}$: بسته ها ورودی پذیرفته می شوند
- $min_{th} \leq median \leq max_{th}$: بصورت رندم بسته ها را دور می اندازد یا دور می اندازه و فقط مارک دار شون می کنند
- $> max_{th}$: بسته ها ورودی دور انداخته می شوند، یا مارک دار می شوند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

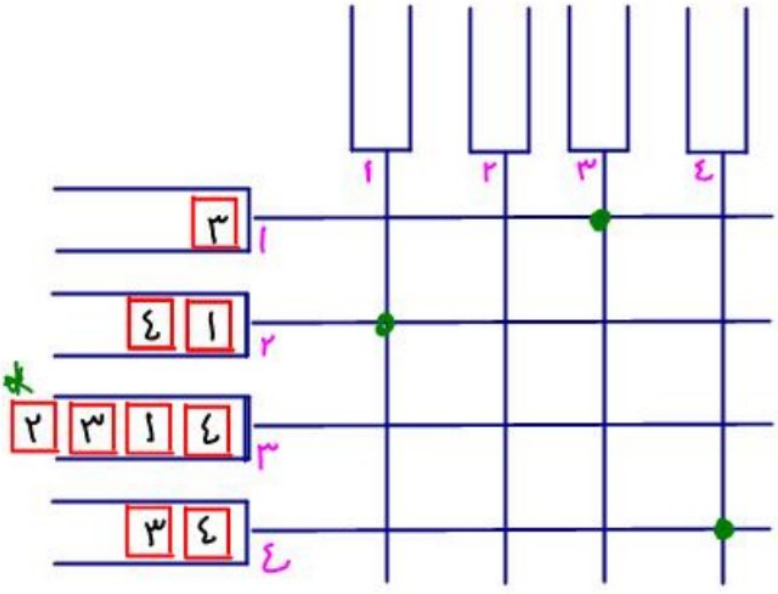
HoL (head-of-the-line blocking)

HoL یعنی یک بسته وارد شده به یکی از پورت های ورودی دیگر با وجود آزاد بودن پورت خروجی که می‌خواهد به آن برود، مجبور شود در صف بماند زیرا بسته ای در سر صف پورت ورودی متعلق به این بسته وجود دارد که سر صف را مسدود کرده است و منتظر است تا به پورت خروجی اش ارسال شود

نکته) در یک crossbar switch، ماتریکس سوئیچ می‌تواند چندین بسته را بطور همزمان از ورودی به خروجی سوئیچ کند به شرط آنکه مقصد این بسته ها یک پورت خروجی واحد نباشد، اما اگر ۲ بسته که در سر صف دو ورودی مجزا هستند بخواهند به یک پورت خروجی واحد بروند، باید یکی از این ۲ بسته منتظر بماند تا دیگری سوئیچ شود

نتیجه: سازه سوئیچینگ در هر لحظه فقط ۱ بسته را می‌تواند به ۱ پورت مشخص ارسال کند

به شکل زیر توجه کنید



* آن در لحظه اول بسته شماره ۲ که در صف ورودی پورت ۳ است می‌تواند ارسال شود ولی ۴ جلو آن را گرفته

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

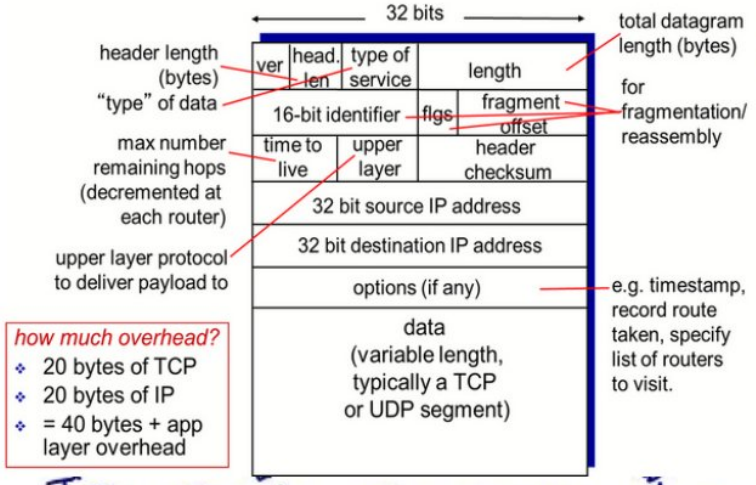
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

لایه شبکه به سه دسته تقسیم می‌شود

- پروتکل IP
- پروتکل های مسیریابی: مسیر حرکت یک بسته از مبدا به مقصد را تعیین می‌کند و وظیفه پروتکل های مسیریابی محاسبه جدول Forwarding.
- گزارش خطا و مبادله پیام های سطح بالا کنترلی بین روترها

پروتکل IP: آدرس دهی، ویژگی بسته های IP، پردازش بسته های دیتاگرام



قالب دیتاگرام ها:

Header length: طول هدر را مشخص می‌کند، هدر معمولا 20 بایت است، مانند هدر Tcp مگر اینکه option داشته باشیم

Type of service: با این فیلد خواستند Qos را اعمال کنند. ۸ بیت است و با توجه به این فیلد روترها بین دیتاگرام های IP می‌توانند اولویت گذاری کنند (بسته های real time اولویت شون مشخص می‌شود)

Datagram length: طول سرآیند + طول داده ها برحسب بایت

۱۶ بیت هست، بنابراین اندازه دیتاگرام حداکثر می‌تواند 2^{16} Byte = 64KB باشد که البته MTU این را محدود می‌کند

TTL = زمان حیات = hope count

upper layer protocol: پروتکل لایه بالاتر را مشخص می‌کند که چیست. در واقع این فیلد مشخص می‌کند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

که داده دیتاگرام را باید host به چه پروتکلی در لایه بالاتر تحویل دهد. روترها باید به این فیلد توجهی نمی‌کنند

Head checksum: خطا موجود در دیتای دیتاگرام را بررسی می‌کند و فقط وجود یا عدم وجود خطا در هدر دیتاگرام را چک می‌کند. بنابراین IP کنترل خطا ندارد. این کار را برای این می‌کند که اگر هدر بسته خراب بود، بیخوده بسته را تا مقصد حمل نکند. این فیلد در هر روتر بصورت مستقل محاسبه می‌شود

fragmentation (قطعه قطعه کردن بسته های IP)

ما در لایه انتقال segmentation و reassembly داشتیم، پس چه نیازی به قطعه قطعه کردن هست؟ چون شاید در وسط شبکه نیاز بشود که بسته ها را بشکونیم، چون وسط شبکه دیگه لایه انتقال نداریم، بنابراین این وظیفه به عهده روترها می‌افتد.

- اگر عمل شکستن بسته ها و سر هم کردن آنها در مبدا و مقصد صورت گیرد به آن segmentation و reass- می‌گوییم و اگر توسط روترهای میانی صورت گیرد به آن fragmentation می‌گوییم

توجه: لایه شبکه مبدا و لایه شبکه تمامی روترهای موجود در مسیر بین مبدا و مقصد می‌توانند بسته‌هایی که بخشوندی رسیده را کنار بگذارند و بسته مقصد ارسال کنند، ولی فقط لایه شبکه مقصد است که می‌تواند این تکه‌ها را هم بچسباند و به لایه انتقال تحویل دهد.

- وقتی تکه‌های مربوط به بسته‌های مختلف به مقصد می‌رسد، مقصد چطوری باید بفهمد که کدام تکه‌ها متعلق به بسته A است؟ برای این منظور در یک فیلد شناسه ۱۶ بیتی در هدر IP استفاده می‌کنیم

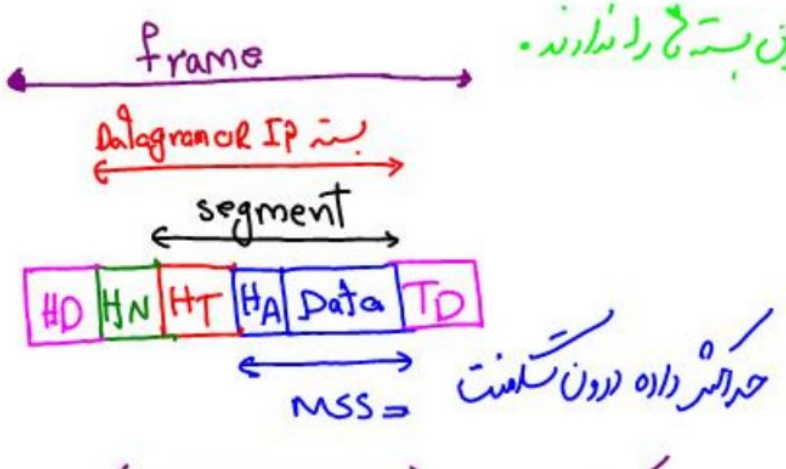
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

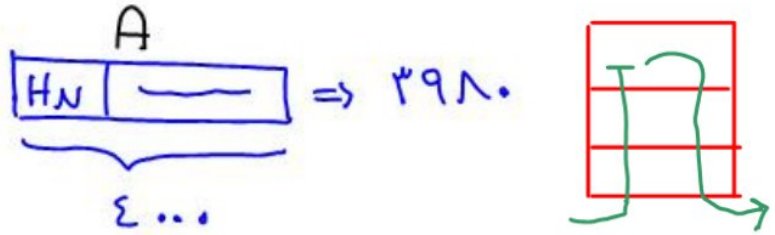
@konkurcomputer
www.konkurcomputer.ir

ویرایش اینیله بخصوص قطعه چندم هستیم از یک فیلد ۱۳ بیتی دیگر به نام آفست قطعه سازی استفاده می‌کنیم

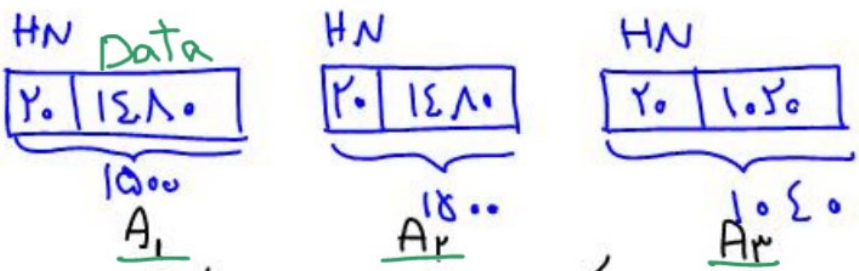
* در ویرایش جدید IP روتر اجازه خرد کردن بسته ها را ندارند.



سوال) یک بسته IP به اندازه ۴۰۰۰ بایت وارد یک روتر شده، حال می خواهیم، از روی لینکی آن را به سمت مقصد بفرستیم که MTU اش برابر ۱۵۰۰ بایت. پرچم ها و آفست تکه سازی هر بسته خروجی از این روتر چند است؟



۳۹۸۰ | ۱۴۸۰
۲۹۶۰ | ۲
۱۰۲۰



یک مثال دیگر برایتان می‌زنم قطعه ها ادامه دارند یا اینکه قطعه ای که مقصد دریافت کرده آخری است یعنی قطعه ادامه دارند و ۰ یعنی تکه آخری است.

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

fragment offset : این فیلد می‌گوید که دیتایش از کدام بایت به بعد دیتا اصلی است .

* دربسته اول می‌گوییم که من از بایت ۰ به بعد هستم . ۰ - ۱۴۷۹
۱۸۵ " " دوم " " " " ۱۴۸۰ " ۲۹۵۹ - ۱۴۸۰
۳۷۰ " " سوم " " " " ۲۹۶۰ " ۳۹۷۹

۱۸۵ × ۸ = ۱۴۸۰

* اندازه بسته ها می‌توانه ۲^۶ × ۲^۱۰ B ← ۶۴KB ، IP در حد ۲^۱۶B = ۶۴KB بنابراین با ۱۶ بیت می‌توان بایت های درون یک بسته را آدرس دهی کرد ، ولی فقط ۱۳ بیت است .

	fragment offset	flag	شناسه	
A_1	۰	۱	۷۷۷	۱۴۸۰
A_2	۱۸۵	۱	۷۷۷	۱۴۸۰
A_3	۳۷۰	۰	۷۷۷	۱۰۲۰

آدرس دهی IP V4 :

آدرس های IP ، ۳۲ بیتی هستند ، این ۳۲ بیت را به این شکل بیان می‌کنند که ۸ بیت ، ۸ بیت جدا می‌کنند و هر ۸ بیت را به صورت دهدهی نمایش می‌دهند و با یک dot کنار هم می‌نویسند

11000001 | 01000000 | 00001001 | 00000111 = ۱۹۳.۶۵.۹.۷

* هر وسیله (کارت شبکه) که به اینترنت متصل است باید یک IP منحصر بفرد در دنیا داشته باشد ، البته به جز host و Device هایی که پشت NAT هستند .

۱۹۲.۱۶۸.۰.۰ — ۲۰۲۰ — X — ۲۵۴.۱۲۶.

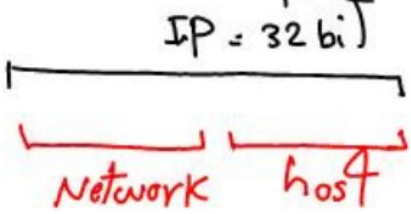
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

رامین رضوی

- مانند خواهیم آدرس ها را بصورت fix اختصاص بدهیم و می خواهیم سلسله مراتبی باشد



به این ترتیب ایده دسته بندی IP به کلاس های مختلف به وجود آمد (class ful IP)

کلاس های مختلفی داریم که تفاوت بودن بایت سمت چپ کلاس های IP متفاوتی را از ما ایجاد می کند

	بایت چپ	بایت اول	Net تعداد بیت	Host تعداد بیت
A کلاس	0 | 7 bit	1 - 126	۸	۲۴
B "	10 | 6 bit	128 - 191	۱۶	۱۶
C "	110 | 5 bit	192 - 223	۲۴	۸
D "	1110 | 4 bit	224 - 239		
E "	1111 | 4 bit	240 - 254		

Net Host ID

198.103.121.10

ok بیت چپ آی پی شبکه را مشخص می کند (Network) و قسمت راست IP، هاست های آن شبکه را مشخص می کند (Host ID)

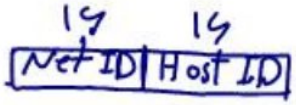
آدرس اول با توجه به آدرس شبکه می دهیم

تو شبکه مورد نظر و بس می دهیم سراغ هاست مورد نظر

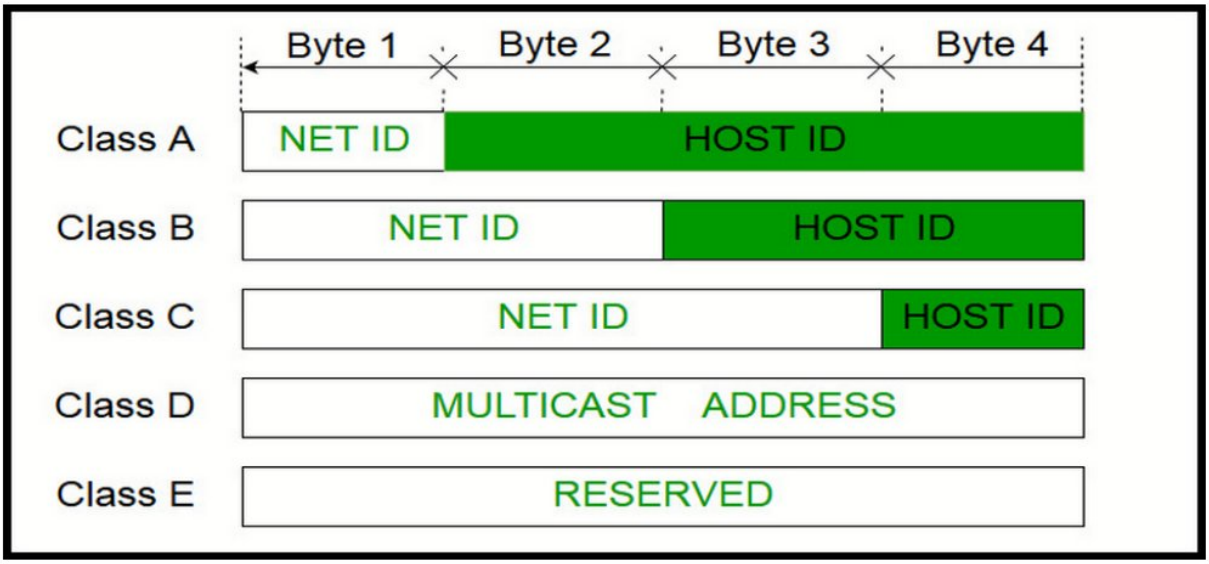
ok تعداد بیت هایی که به Network و host نسبت می دهیم در کلاس های مختلف متفاوت است

تعداد هاست های درون هر شبکه = تعداد شبکه

	تعداد شبکه	تعداد هاست
A کلاس	$2^7 - 2$	$2^{24} - 2 \simeq 16$ million
B "	2^{14}	$2^{16} - 2 = 65534$
C "	$2^{21} \simeq$ ۲ میلیون	$2^8 - 2 = 254$



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner



Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

Address Class	RANGE	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Reserved for Multicasting
E	240.0.0.0 to 254.255.255.255	Experimental

Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback testing.

IP Address Classes

Class	First Bits	First Byte Values	Network ID Bits	Host ID Bits	Number of Networks	Number of Hosts
A	0	1 - 126	7	24	126	16,777,214
B	10	128 -191	14	16	16,384	65,534
C	110	192 - 223	21	8	2,097,152	254

Private IP Address Range – **Special purpose**

Class	Network Address
A	10.0.0.0 through 10.255.255.255
B	172.16.0.0 through 172.31.255.255
C	192.168.0.0 through 192.168.255.255

وقتی دوتا IP مختلف در شبکه می خواهند باهم ارتباط برقرار کنند، باید در forwarding table های روترهای درون شبکه مشخص شود که چطور می شود به یک IP رسید، به همین دلیل یک IP و یا یک بلاک از IP ها را که یک شرکت می گیرد هزینه دارد، ولی اگر یک شرکت نخواهد درون یک ساختمان بین سیستم های خودش مدیریت و سوییچینگ بگذارد (یا یک دانشگاه) و یک شبکه داخلی برای خودش درست کند که یک ارتباط درون شبکه ای داشته باشد اولاً چرا باید هزینه بدهد؟ دوما چرا باید IP را با هماهنگی از یک ارگان بگیرد سوما در اینصورت IP کم می آید

به همین علت یکسری از آدرس های IP را بعنوان آدرس private OR invalid OR unregister را آزاد گذاشتند تا هر کس که می خواهد براحتی از اینها استفاده کند

نکته: آدرس های private در اینترنت قابلیت مسیریابی ندارند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

- یک آدرس IP می‌تواند نمایانگر یک هاست در شبکه باشد یا معرف یک شبکه باشد و یا نشان دهنده هم یا تعدادی از نودهای شبکه باشد

در مجموعه ای از آدرس های IP که یک شبکه را تشکیل می دهند، دو آدرس وجود دارد که آدرس های خاصی محسوب می شوند

۱- NET ID : IP ای که معرف (بیان گر، نشان دهنده) یک شبکه است

برای محاسبه NET ID به قسمت Network آی پی دست نمی زنیم و تمام بیت های مربوط به قسمت هاست را ۰ می کنیم (بعدا متوجه می شوید که در واقع با Network mask دارم and میکنیم)

۲- Broadcast address : این IP نشان دهنده همه نودهای درونی شبکه خودمان است. وقتی در داخل شبکه خودمان می‌خواهیم یک پیام ای را Broadcast کنیم از این IP برای بسته های پیام استفاده می کنیم

برای محاسبه BA یک شبکه به قسمت Network دست نمی زنیم و تمام بیت های هاست را ۱ می کنیم

نکته مهم: آی پی های NET ID و Broadcast Add، IP هایی هستند که ما نمی توانیم اینها را بعنوان آدرس معتبر به هاست هایمان تخصیص بدهیم

مثال: شبکه ای که آدرس IP ۲۱۰.۲۲۰.۱۲.۲۳ در آن وجود دارد را در نظر بگیرید، حال موارد زیر را محاسبه کنید

۱- class — C

۲- Net ID — 210.220.12.0

۳- اولین آدرس IP این شبکه — 210.220.12.1

۴- آخرین " " " " — 210.220.12.254

۵- Broadcast addr — 210.220.12.255

۶- تعداد آدرس های IP در دسترس — $2^8 - 2 = 254$

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

رامین رضوی

زیرشبکه (subnet)

مثال: یک آدرس کلاس A که بایت سمت چپ آش ۷۰ است

۰۱۰۰۰۱۱۰ . . . . .

70.0.0.0

⋮

70.255.255.255

چه رنجی از IP ها را (Host ها را) پوشش می دهد

70.123.10.240 : یک IP Host درون این شبکه

سوال) Network mask شبکه چیست؟

255.0.0.0

چطور روتر تشخیص می دهد که یک آی پی متعلق به شبکه است LAN اش است یا خیر

70.123.10.240
AND 255.0.0.0
70.0.0.0 → روتر چک می کند

* اگر تمام آدرس های درون این شبکه را با Network mask این شبکه AND کنیم جواب برابر 70.0.0.0 می شود پس اگر UI IP را با Network mask این شبکه AND کنیم و جواب برابر 70.0.0.0 نشد، گوییم آن IP متعلق به آن شبکه نیست.

* اگر Network mask شبکه n را با تمام IP های درون شبکه n AND کنیم جواب برابر Net ID می شود

نکته: Net mask یک کلاس IP به اینصورت صحبت است که باید به تعداد Net های آن کلاس ۱ بگذاریم و بقیه بیت ها را ۰ بدهیم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

دانشگاه تهران

$2^6 \times 2^{10} = 64K$

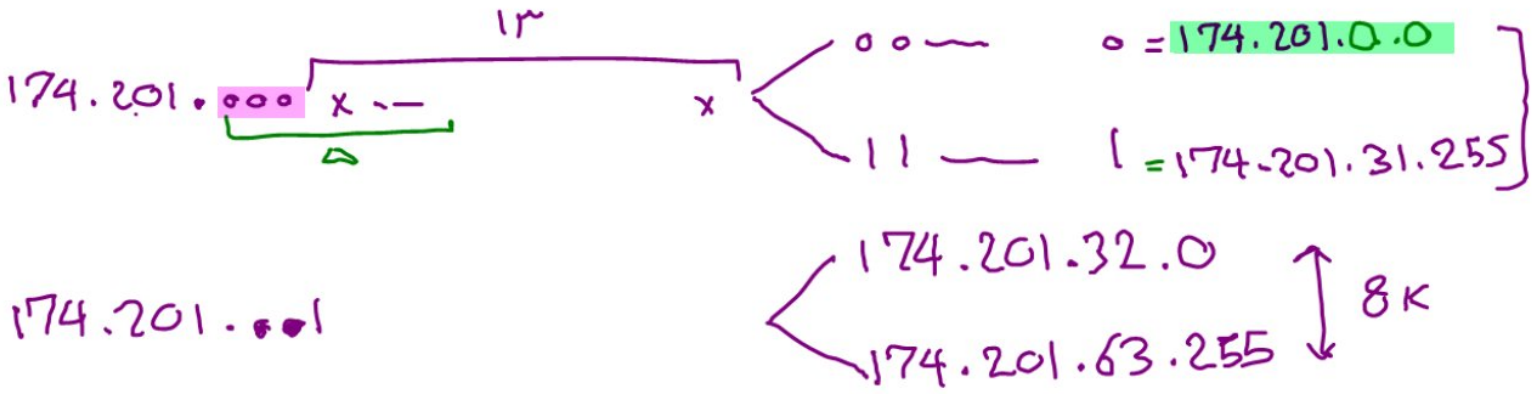
تهران

IP class; B ⇒ 174.201. (16 | 16 → 3 | 13)

دانشگاه تهران ۶۴ تا زیر شبکه

دانشگاه تهران Net ID: 174.201.0.0

Broadcast Address: 174.201.255.255



174.201.001

174.201.32.0

174.201.63.255

8K

010

011

100

101

110

174.201.224.0

174.201.255.255

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

رامین رضوی

* Network mask برای کلاس های مختلف بصورت زیر است :

A کلاس : 255.0.0.0

B " : 255.255.0.0

C " : 255.255.255.0

زیرشبکه : subnet تقسیم شبکه به چند شبکه

B کلاس IP

Net ID	Host ID
16 Bit	16 Bit

↓

دانشگاه تهران بیاید Host ID به ۲ قسمت تقسیم کند

فرض کنید دانشگاه تهران یک IP کلاس B گرفته است ، بنابراین می تواند 2^{16} تا host داشته باشد حال دانشگاه تهران می گوید ۱۶ بیت را به ۲ قسمت می کنم ، این تقسیم روی بیت ها را با قیمانده می تواند متقارن یا نامتقارن انجام شود . فرض کنید دانشگاه تهران این قسمت را تقسیم کرده به ۲۵۴ (۲-۲۵۶) زیرشبکه که هرکدام ۲۵۴ تا host دارد .

IP دانشگاه تهران : 132.66.0.0 → Host ID

Net ID

↓

subnet ID = دانشکده ها

متغیر

↓

دانشکده کامپیوتر : 132.66.7.0

" عمران : 132.66.23.0

" مدیریت : 132.66.14.0

Netmask = 255.255.0.0

SubNet mask = 255.255.255.0

مثال : 132.66.23.186 سوال : این IP در دانشگاه تهران است ؟

132.66.23.186

AND 255.255.0.0

132.66.0.0 → Net ID

چک می کنیم با

132.66.23.186

AND 255.255.255.0

132.66.23.0 → دانشکده عمران

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

حال می‌خواهیم IP را عنید متقارن تقسیم کنیم؟ دانشگاه تهران می‌بیند که ۵۰ تا زیر شبکه دارد می‌گوید شبکه دانشگاه تهران را به ۵۰ زیر شبکه بشکنیم که هر زیر شبکه به‌جای اینکه ۲۵۴ تا host داشته باشد ۱۰۰۰ تا host باشد.

دقت کنید باید شرط $50 \times 1000 \leq 2^{16}$ باشد

$2^{16} = 65K$

دانشگاه تهران می‌گوید باید ۶ بیت برای subnet ID بهم اختصاص بدهم.

132.66 . [6 bit] [10 bit] → $2^{10} - 2 = 1022$

Net ID | subnet ID | Host ID

ماچند دانشکده می‌توانیم داشته باشیم؟ $2^6 - 2 = 62$

ولی ۵۰ تا داریم پس بقیه هدر می‌رود

سوال) در این حالت subNet mask و Net mask چیست؟

Net mask: 255.255.0.0

subnet mask: 255.255.11111100 . 00000000

255.255.252.0

دانشکده کامپیوتر = 132.66.28.0/22

یکی از تست دانشکده کامپیوتر = 132.66.00011101.01101001

یکی دیگر = 132.66.00011100.10001101

AND = 255.255.11111100.00000000

132.66.00011100.00000000

= 132.66.28.0

* هر IP را با subnet mask AND بشود و برابر 132.66.28.0 شود یعنی در دانشکده کامپیوتر است

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir

سوال) اگر subnet mask شبکه ای که در کلاس B است بصورت زیر باشد، چند تا زیر شبکه داریم و هر زیر شبکه چند تا هاست دارد؟

255.255.241.0/20

255.255.1111 0000 . 0000 0000

↓

۴ بیت آخر مقدار آی پی هاش اینجا نشان داده شده

تعداد زیر شبکه ها = $2^4 - 2$

تعداد هاست های هر زیر شبکه = $2^{12} - 2$

البته ما چند تا زیر شبکه داریم. ۲- می کنیم

اگر اینگونه دسته بندی کردن IP ها باعث هدر رفتن IP ها می شود.

در کلاس A ، ۱۶ میلیون هاست داریم

" " B ، ۶۵۵۳۴ " "

حال یکی اگر ۲ میلیون هاست داشته باشد مجبور است IP کلاس A را بگیرد، و ۱۴ میلیون IP بلا استفاده می ماند و در واقع IP ها تلف می شود

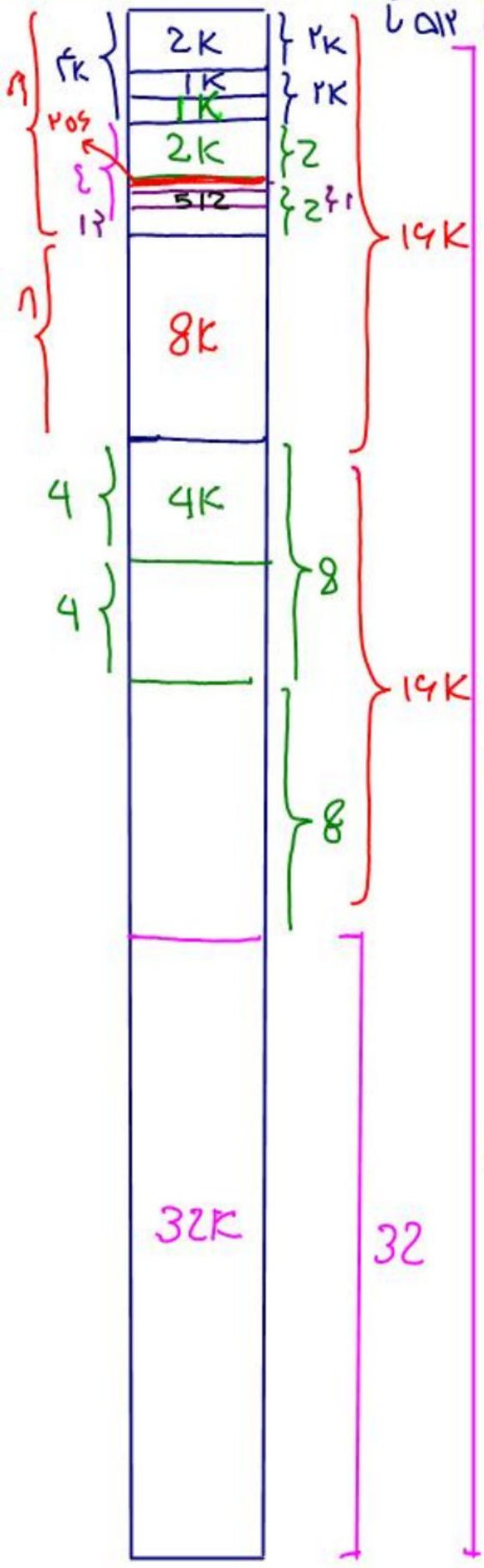
حال راه حل این مشکل این است که کلاس ها را حذف کنیم، برای این کار از CIDR استفاده می کنیم

classless inter domain routing

- هر مقدار آدرس که می خواهید اختصاص بدهید، اول چک کنید که آیا در فضای خالی که دارید جا می شود یا خیر، اگر جا می شد به نحوی که گفته می شود آن را در اولین فضای خالی از بالا قرار دهید، اما اگر این مقدار آدرس بزرگتر از میزان فضای خالی باقیمانده بود، میزان فضای قبلی را بایه تا مقداری که به دو برابر مقدار IP درخواست شده است بزرگ کنید و بعد نیمه دوم اش را به مقدار IP درخواستی اختصاص دهید.

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.


2K
1K
1K
2K
512
8K
4K
4K
32K
14K
14K
32
64
8
8
8
4
4
4
2
2
2

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

سازمان 2 : VSIP سازمان 2 از 210.36.8.0 شروع می‌شود و چون 1K می‌خواهیم

به سازمان 2 بدهیم، ($1K = 2^{10}$) 10 بیت سمت راست این IP می‌تواند متغیر باشد

210.36.00001 000.00000000 = 210.36.8.0

rang ↕ — سازمان 2 ↕

210.36.00001 011.11111111 = 210.36.11.255

subnet mask = 255.255.252.0

Network ID = 210.36.8.0

نگذری نامیں = 210.36.8.0/22

1K آی پی آزاد:

210.36.00001100.00000000

rang ↕

210.36.00001111.11111111 = 210.36.15.255

سازمان 3 : 4K آی پی می‌خواهد:

210.36.16.0 = Net ID

210.36.0001 0000.00000000

12 bit

rang ↕

210.36.0001 1111.11111111 = 210.36.31.255

subnet mask = 255.255.240.0

Net ID: 210.36.16.0

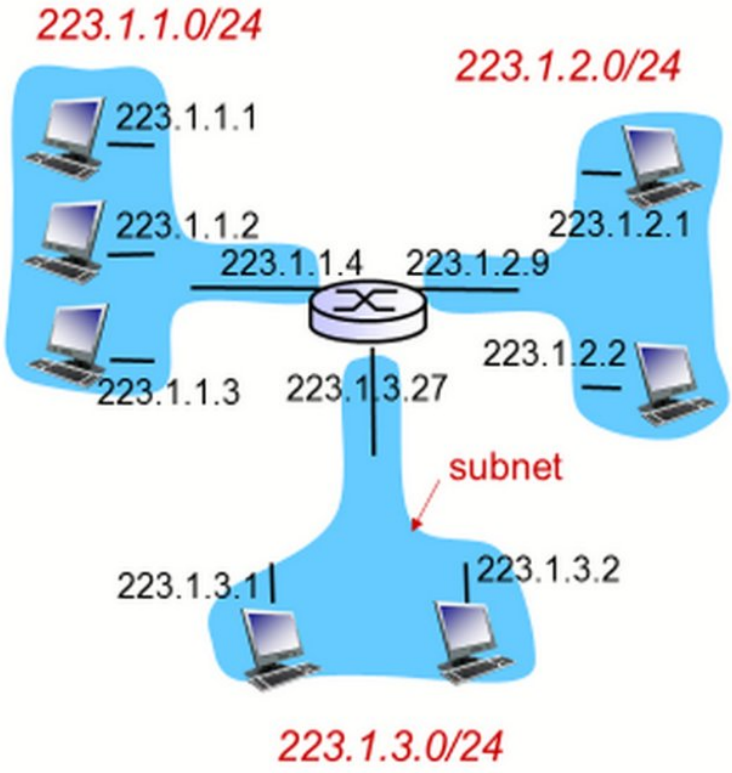
نگذری نامیں = 210.36.16.0/20

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

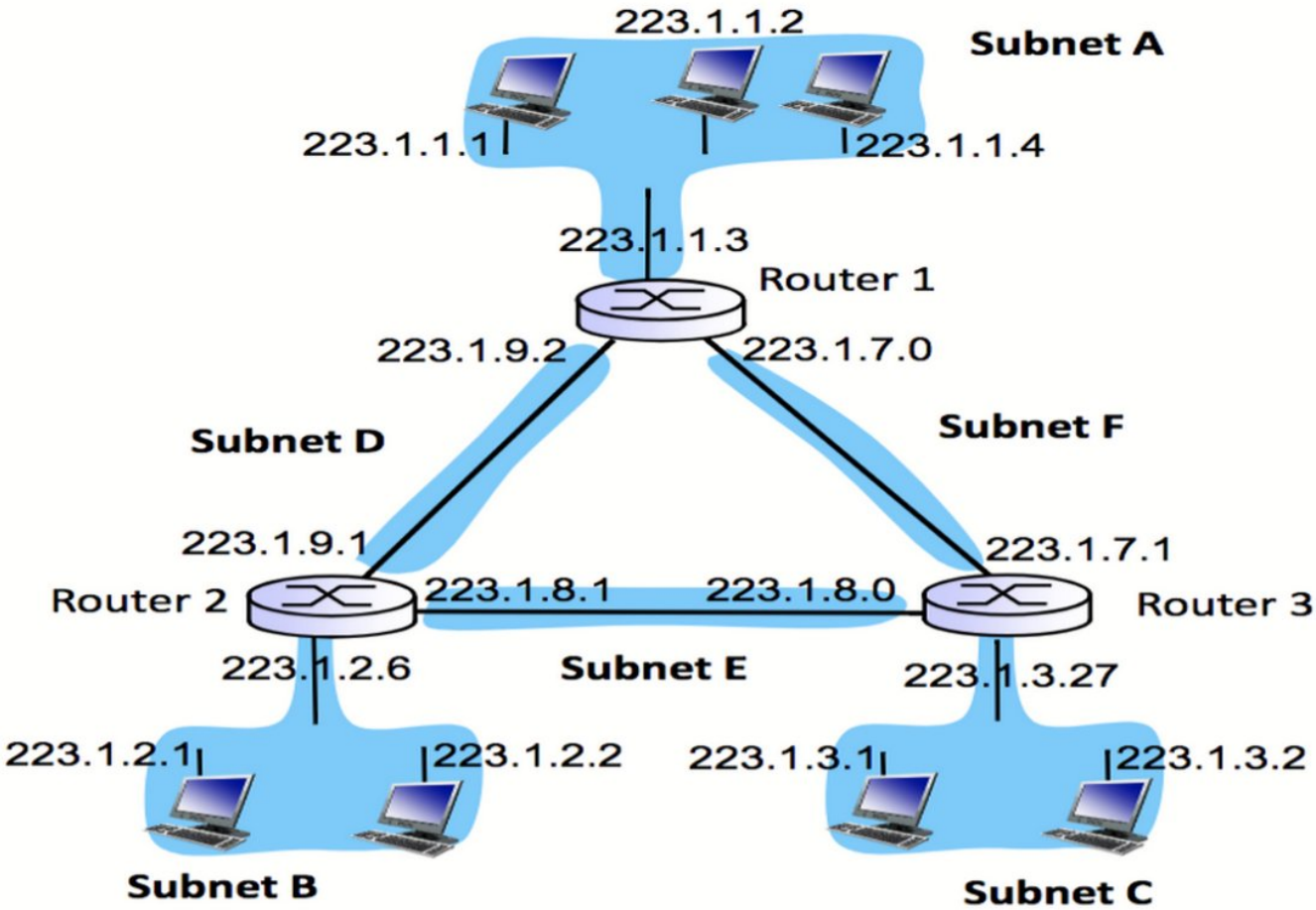
Subnets

recipe

- to determine the subnets, detach each interface from its host or router, creating islands of isolated networks
- each isolated network is called a *subnet*



subnet mask: /24



Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

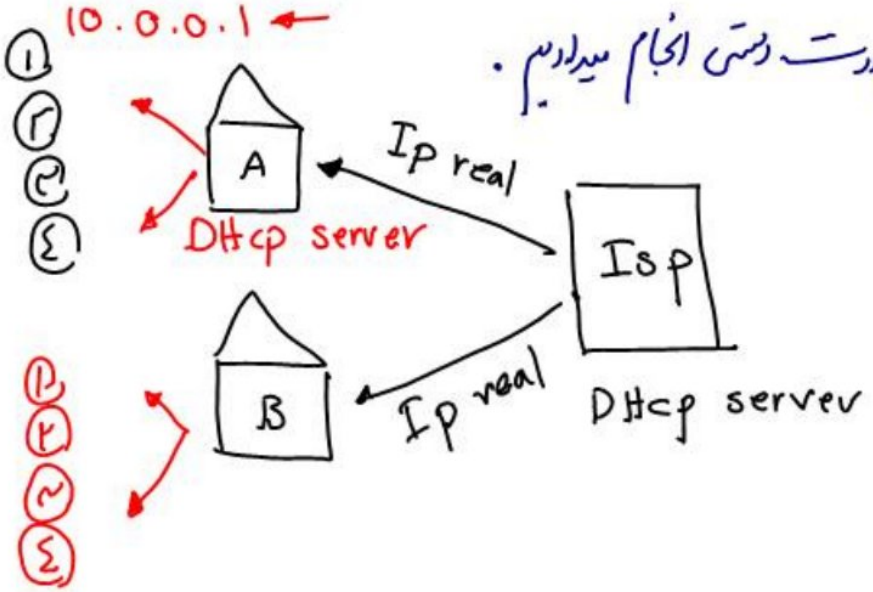
نکته: ماهر آدرس Ip را به یک کارت شبکه می دهیم، مثلا یک روتر به تعداد پورت هایش کارت شبکه دارد و بنابراین ما باید به تعداد پورت هایش بهش Ip بدیم.

زیر شبکه: جزیره هایی که به واسطه جدا کردن کارت شبکه ها از کارت ها و روتر ها به وجود می آید

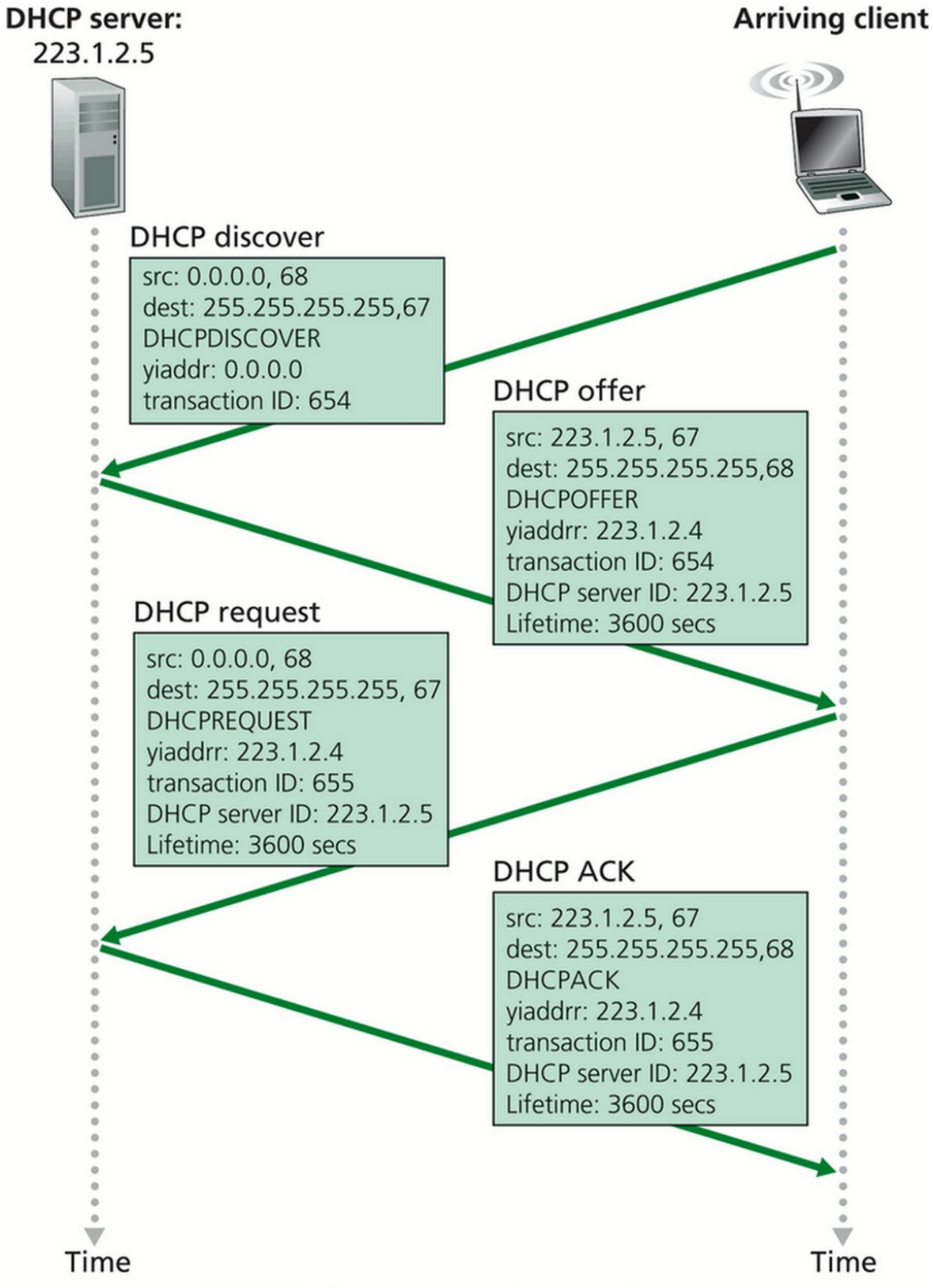
DHcP: (Dynamic Host configuration protocol) پیکر بندی دینامیک هاست ها

DHcp به هاست ها آدرس Ip اتوماتیک می دهد، مثلا من یک رنجی از Ip را دارم، یک DHcp server میذارم، بعد یک ماشین ام که روشن می شود و میاد با A، یک DHcp request میده و DHcp سرور بهش یکی از آدرس هایی را که در اختیار دارد تخصیص می دهد و اگر آن Host خاموش شود آن Ip، release می شود و DHcp می تواند آن را به Host دیگری بدهد.

اگر DHcp نبود باید این کار را بصورت دستی انجام میدادیم.



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner



DHCP client-server interaction

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

نکته: DHCP چه اطلاعاتی را می‌تواند به Host بدهد؟ آدرس IP، subnet mask (آدرس زیرشبکه)، Default gateway، آدرس DNS محلی

برعکس مشتری و سرویس دهنده DHCP

یک Host جدید برای گرفتن IP از DHCP باید یک فرآیند ۴ مرحله‌ای را طی کند

۱) شناسایی سرویس دهنده DHCP: اولین کاری که یک هاست تازه وارد باید انجام بدهد یافتن یک سرور DHCP برای گرفتن اطلاعات مورد نیازش است، چون آدرس DHCP server را نمی داند برای پیدا کردن DHCP و یک پیام با نام DHCP discover message (پیام شناسایی DHCP) داخل یک بسته UDP به پورت ۶۷ پرواز می‌کند، پس در اثر دریافت این پیام توسط DHCP server تمام DHCP هایی که در زیرشبکه ما وجود دارند، خودشون را به هاست تازه وارد معرفی می‌کنند.

۲) پیشنهادهای سرورهای DHCP به هاست تازه وارد: وقتی سرورهای DHCP یک پیام شناسایی DHCP دریافت می‌کنند، یک بسته با نام DHCP offer mess- به مقصد پورت ۶۸ برای همه هاست‌های آن زیرشبکه Broadcast می‌کنند (آدرس IP را برای برودکست 255.255.255.255 می‌گذارند)

۳) درخواست DHCP: Host تازه وارد از بین پیشنهادهای دریافتی یکی را انتخاب می‌کند و یک پیام DHCP request message با شماره پورت مقصد ۶۷ را Broadcast می‌کند تا به دست سرور هاکه انتخاب کرده برسد و همان پارامترهایی را که از DHCP انتخاب گرفته بود را به آن برگرداند

۴) تصدیق (DHCP) سرور DHCP یک پیام DHCP ack message را Broadcast می‌کند

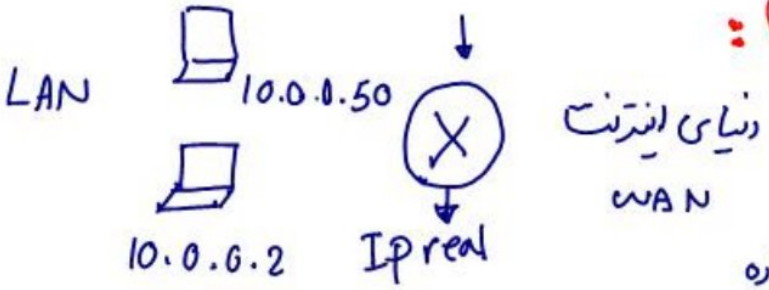
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

تا به مقصد مورد نظر برسد و با این پیام به Host می گوید من، این Ip را برای تو ارسال کردم.

NAT (Network address translation):



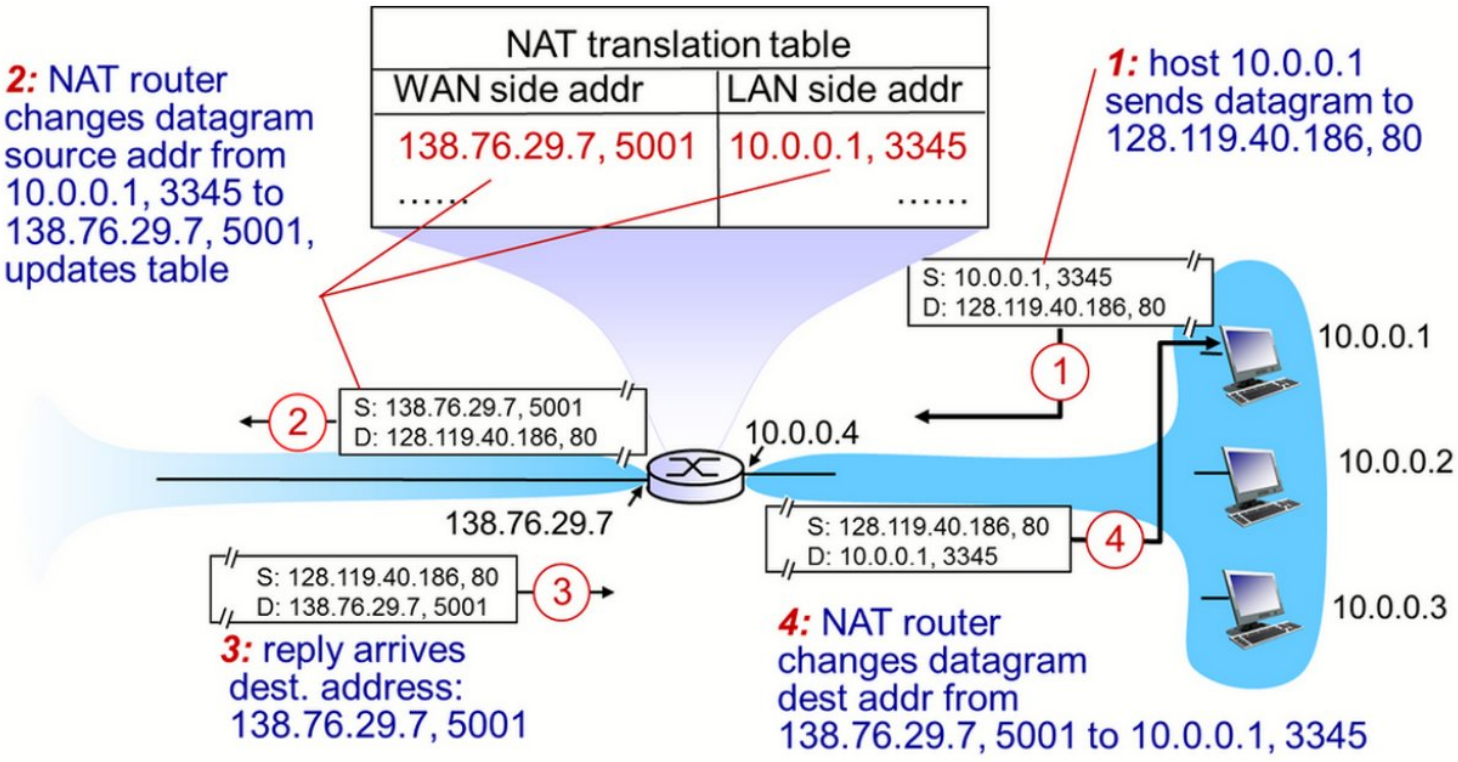
IPV4 تمام شد و جلوگیری یکسری آدرس را دادند بدین که همه بتوانند در شبکه محلی شون از آنها استفاده کنند، اما این آدرس ها ممکن است توسط خیلی از هاست ها در دنیا استفاده شود، حالا این Ip های محلی است و سراسری نیست و بنابراین این هاست ها نمی توانند با این Ip ها در دنیای اینترنت فعالیت کنند پروتکل NAT این ماجرا را برای ما حل می کند و کاری می کند که آدرس های این هاست ها real شود و این کار را با استفاده از شماره پورت که در لایه انتقال در بسته ها می گذاریم حل می کند.

از سمت LAN یک router، NAT می گذاریم که یک جدول تبدیل NAT درون اش داریم، هر بسته ای که به روتر می رسد، روتر آدرس Ip مبدا بسته و آدرس پورت مبدا را عوض می کند و آدرس Ip خودش و همین طور یک شماره پورت جدید برای آن می گذارد و در جدول تبدیل NAT این موارد را نگه می دارد.

در واقع روتر یک جدول برای ترجمه می سازد و همه Host هایی که از سمت LAN بهش وصل شده اند را از طریق شماره پورت شون تشخیص می دهد. آدرس Ip همه این هاست ها از نظر دنیای واقعی یکی است

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

NAT: network address translation



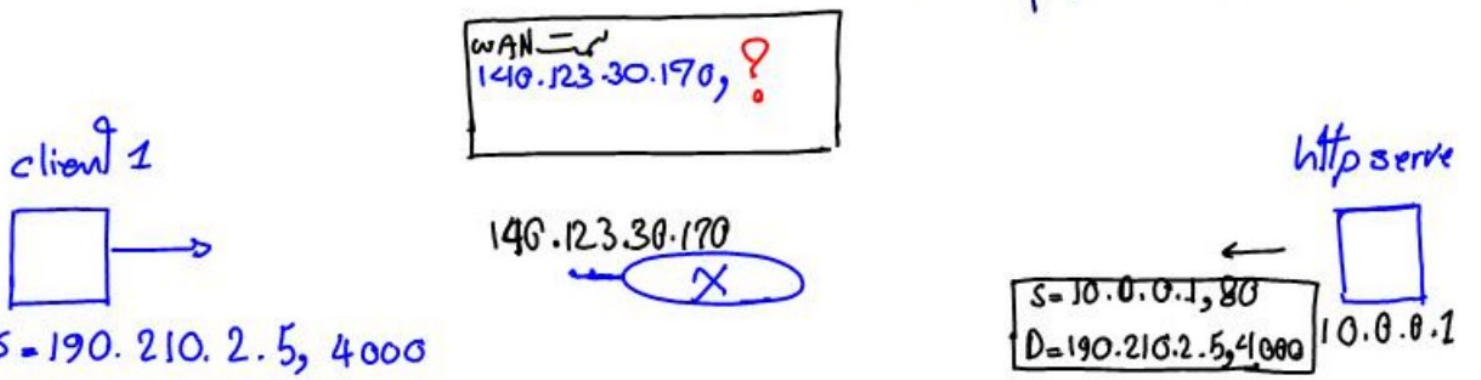
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

مشکلات NAT :

۱) سرور نمی تواند پشت NAT ، چون Ip سرور باید real باشد و همه آن Ip را بشناسند تا بتوانند به مقصد آن پیام ارسال کنند



۲) شماره پورت فقط برای آدرس دهی فرایندها (پروسس ها) است ، نه برای آدرس دهی host ها ولی NAT از شماره پورت برای آدرس دهی host ها استفاده می کند

فرار می کنیم این بود که host ها را با آدرس Ip تفکیک کنیم و پروسس ها را با پورت

۳) روترها قرار بود فقط بتوانند تا لایه سه به بسته ها دست بزنند و به هدر لایه انتقال کاری نداشته باشند (چون شماره پورت در هدر لایه انتقال است)

۴) اصل ارتباط انتها به انتها می گوید دو تا host باید بتوانند بدون آنکه نودهای میانی آدرس Ip و شماره پورت مبدا و مقصد را دستکاری کنند با همدیگر صحبت کنند ، NAT اصل ارتباط end to end را نقض می کند ، قرار بود لایه انتقال فقط در host مبدا و مقصد باشد ، قرار بود لایه انتقال end to end باشد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

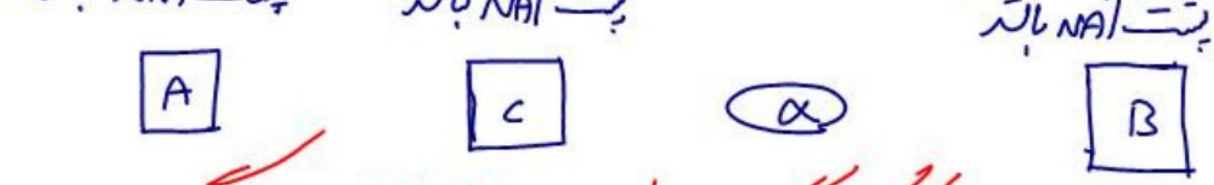
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

- گفتیم سرور نمی‌تواند پشت NAT بیاید، خب چون ما معمولاً به سرورها Real IP اختصاص میدهیم
این موضوع برای ما هم نیست و مشکلی برای ما ایجاد نمی‌کند، اما این موضوع وقتی که ما از برنامه های p2p
استفاده می‌کنیم مشکل ایجاد می‌کنیم. چون در برنامه های p2p وقتی A و B با هم تبادل دیتا می‌کنند
هر دو اینها می‌توانند پشت NAT قرار گیرند، حال در p2p گاهی اوقات A کلاینت و B سرور است
و گاهی A سرور و B کلاینت است، حالا مشکل یکی از اینها پشت NAT هست و می‌خواهد نقش
سرور را بازی کند، مشکلی که گفتیم را خواهیم داشت. یعنی اگر B پشت NAT باشد نمی‌تواند
بعنوان یک سرویس دهنده عمل کرده و اتصال های Tcp را قبول کند

برای رفع این مشکل باید از یک سرور میانی که آدرس Ip واقعی دارد استفاده کنیم و هر ۲ کلاینت
A و B به آن متصل شوند

* اگر هر ۲ تا است A و B پشت NAT باشند و یا یکی از آنها پشت NAT باشد باز هم می‌توانیم
ارتباط p2p اینها را برقرار کنیم.



* فقط A برای ارتباط با B از C کمک می‌گیرد، این کار به ۲ شرط می‌تواند صورت گیرد

① C پشت NAT نباشد
② B یک اتصال Tcp به C داشته باشد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir
MSc-PhD Computer-IT

- حال A توسط C از B پیغام داده تا مستقیما یک ارتباط TCP با خودش (A) برقرار کنه، بعد از برقراری این ارتباط TCP، A و B می‌تونند مبادله دیتا رو شروع کنند (P2P)، به این کار وارونگی ارتباط (connection reversal) می‌گویند، که با این کار از NAT عبور می‌کنند

* C کلا نباید پشت NAT نباشد.

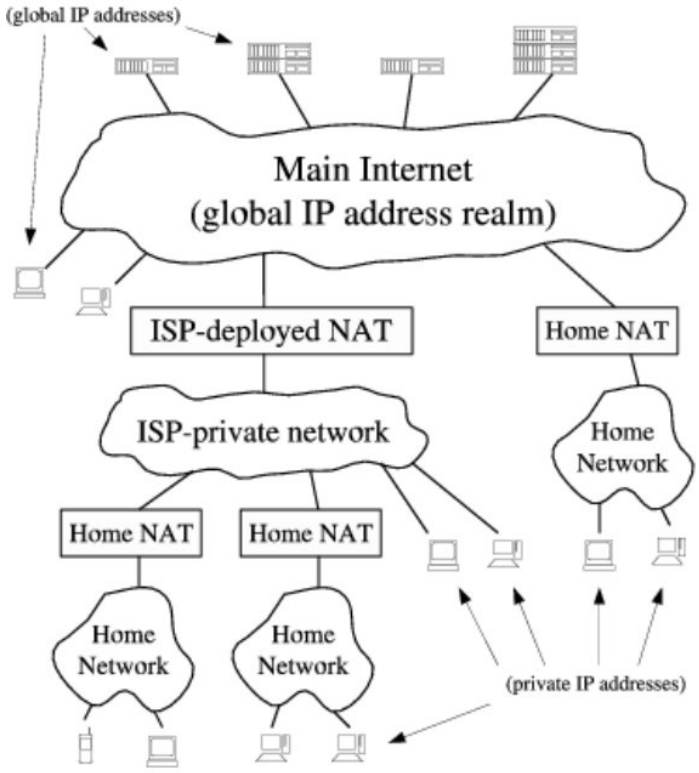
۱. مقدمه

همانطور که می‌دانید اعضای شبکه مستقیما با هم در ارتباط نیستند. از این رو هر عضو شبکه برای برقراری ارتباط با عضوی دیگر مجبور است بسته‌اش را از مسیری بگذراند که شامل اعضای میانی است. کار برخی از این اعضای میانی، صرفا مسیریابی است و بسته را بدون تغییر به گره‌ی بعدی انتقال می‌دهند. اما اعضایی هم وجود دارند که بسته را بازرسی و فیلتر کرده و در برخی مواقع آن را تغییر می‌دهند. به طور کلی به این اعضا Middle Box می‌گوییم.

حالت خاصی از Middle Boxها، Network address translation (NAT)ها هستند. این اعضاء آدرس مبدا و یا مقصد را تغییر می‌دهند، بنابراین گره‌هایی که پشت NAT قرار دارند، از دید اعضای دیگر شبکه آدرس متفاوتی دارند و بعضاً ممکن است دو گره شبکه یک آدرس داشته باشند. مشکلی که اینجا پیش می‌آید این است که اگر دو همتا [۱] بخواهند یک ارتباط همتا به همتا [۲] ایجاد کنند و به یکدیگر بسته بفرستند، چگونه آدرس همدیگر را پیدا کنند و به نوعی محدودیت‌های NAT را دور بزنند. روش‌های مختلفی برای اینکار وجود دارد و به طور کلی به این مساله NAT Traversal می‌گویند.

ساختار شبکه را در حالت کلی می‌توان به شکل زیر در نظر گرفت:

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner



شکل ۱: ساختار کلی شبکه ـ منبع شکل

۲. مقدمه‌ای بر NAT

امروزه استفاده از NATها بسیار رایج شده است و اکثر همتاها پشت چند لایه از NAT قرار دارند. کار مهم NAT این است که آدرس و یا درگاه بسته‌ی وارد شده را تغییر داده و یا ترجمه کند و سپس بسته را به گره بعدی بدهد. NATها با توجه به نوع عملکردشان به چند دسته تقسیم می‌شوند که رایج‌ترین آن‌ها Outbound NAT است. این نوع از NATها در حالت عادی برای بسته‌های وارد شده آدرس محلی را به آدرس عمومی ترجمه می‌کنند. اما آدرس بسته‌هایی که از خارج وارد می‌شوند را تنها در صورتی به آدرس محلی تبدیل می‌کنند که از قبل نشستی [۳] با این آدرس از داخل شبکه محلی ایجاد شده باشد. Outbound NAT خود به دو زیر دسته تقسیم می‌شود:

- Basic NAT: تنها آدرس را ترجمه می‌کنند
- Network/Port Translation (NAPT): که هم آدرس و هم درگاه را ترجمه می‌کنند و این امکان را می‌دهند تا همزمان چند همتا از یک آدرس عمومی روی درگاه‌های مختلف استفاده کنند .

متاسفانه اکثر حالت‌های NAT باعث می‌شود اگر هر دو همتا پشت NATهای جدا باشند، هیچ کدام نتوانند با دیگری نشستی ایجاد کنند، زیرا NAT همتای مقابل بسته وارد شده از خارج را دور می‌ریزد و در نتیجه تنها حالت

[۳] یک نشست یا Session در پروتکل UDP و TCP از یک چهارتایی (Local IP, Local Port, Remote IP, Remote Port) تشکیل می‌شود.

Scanned with CamScanner

ممکن برای برقراری ارتباط این است که یک همتا شروع کننده نشست باشد و همتای دیگر پشت NAT نباشد. برای برقراری ارتباط بین دو همتای پشت NAT باید از روش‌هایی مانند UDP Hole Punching است.

۳. مقدمه‌ای بر UDP Hole Punching

روش Hole Punching یکی از روش‌هاییست که برای عبور از NAT استفاده می‌شود. ایده کلی این روش کمک گرفتن از یک کارگزار شناخته شده برای دو همتا است. ابتدا لازم است هر دو همتا با کارگزار یک نشست درست کنند. در این زمان، کارگزار به ازای هر همتا دو آدرس و دو درگاه نگهداری می‌کند. یکی آدرس و درگاهی است که خود همتا بسته را با آن فرستاده بود که به آن اطلاعات محلی می‌گوییم. دیگری آدرس و درگاهی است که کارگزار هنگام دریافت بسته در سرآیندهای بسته می‌بیند که به آن اطلاعات عمومی می‌گوییم. اطلاعات محلی را باید خود همتاها بفرستند زیرا پس از عبور از NAT دیگر قابل شناسایی نیست. اما اطلاعات عمومی از سرآیندها معلوم است. پس از این کارگزار تمام اطلاعات هر همتا را برای دیگری می‌فرستد. هر کدام از همتاها با هر دو اطلاعات محلی و عمومی تلاش به برقراری یک نشست جدید می‌کنند. هر نشستی که زودتر انجام شد، همان را ادامه می‌دهند.

برای مثال فرض کنید دو همتای A و B داریم که هر دو پشت NATاند و کارگزاری مانند S وجود دارد که پشت NAT نیست و هر دو A و B از قبل با S یک نشست UDP ایجاد کرده‌اند. حال A در تلاش است تا با B یک نشست UDP ایجاد کند. پس مراحل زیر را انجام می‌دهند:

۱. A آدرس B را نمی‌داند، پس از S میپرسد.

۲. S بسته ای به A شامل آدرس و درگاه محلی همچنین آدرس و درگاه عمومی B می‌فرستد. به طور همزمان اطلاعات A را نیز به B می‌فرستد تا هر دو همدیگر را بشناسند.

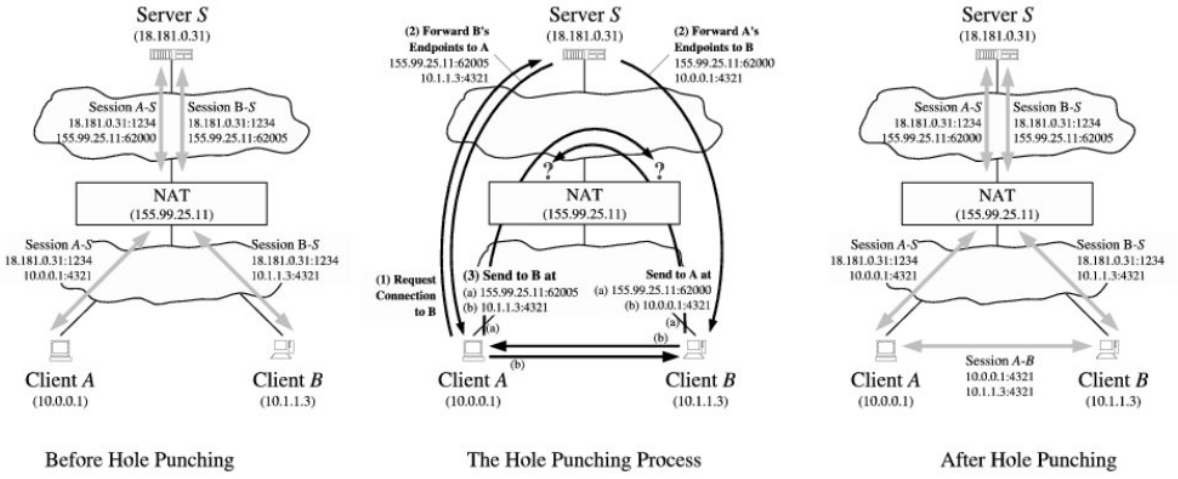
۳. هنگامی که A اطلاعات را از S دریافت کرد، به هردو آدرس محلی و عمومی B بسته اش را می‌فرستد و منتظر می‌شود تا یکی از این دو آدرس جوابش را بدهند و با آن ارتباط را ادامه دهد. به طور موازی B نیز هنگامی که بسته را دریافت کرد، به هر دو آدرس محلی و عمومی A بسته را می‌فرستد و منتظر می‌شود تا از یکی پاسخ بگیرد.

با توجه به سناریو بالا، سه حالت مختلف برای A و B پیش می‌آید که در ادامه به بررسی آن‌ها می‌پردازیم.

۱.۳. NAT مشترک

در این حالت هر دو همتا پشت یک NAT مشترک هستند. همانطور که در شکل می‌بینید، دو همتا پس از دریافت اطلاعات از S، از طریق آدرس عمومی و محلی یکدیگر تلاش به برقراری ارتباط می‌کنند. در اینجا چون هر دو در یک شبکه محلی هستند، مسیر محلی زودتر شکل می‌گیرد و در نتیجه نشست از طریق ارتباط محلی برقرار می‌شود.

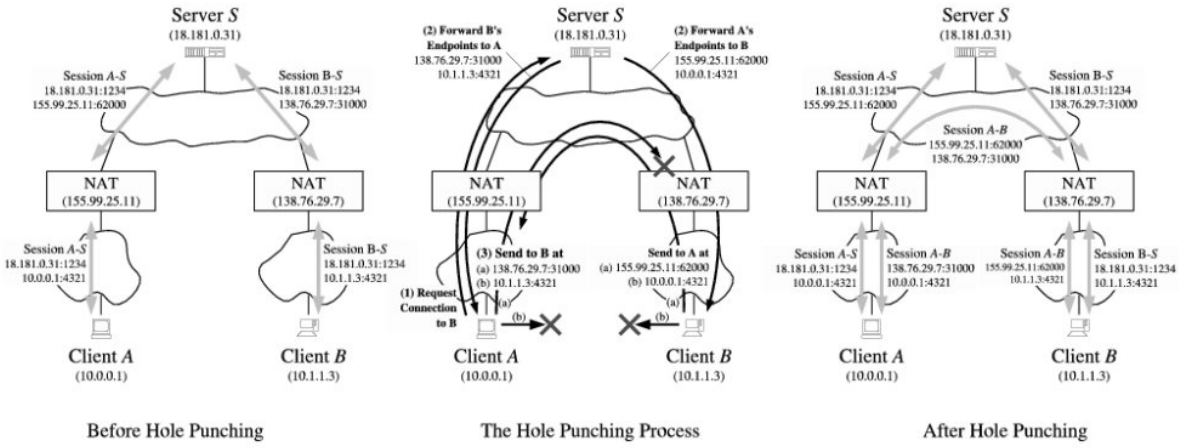
Scanned with CamScanner



شکل ۲: برقراری ارتباط در حالت NAT مشترک ـ منبع شکل

۲.۳. NAT متفاوت

در این حالت دو همتا پشت NATهای متفاوت هستند و نمی‌توانند از طریق اتصالات محلی با هم ارتباط برقرار کنند. اما هنگامی که A درخواست خود را به آدرس و درگاه عمومی B ارسال می‌کند، یک خانه جدید در NAT مربوط به A ایجاد می‌شود که شامل آدرس و درگاه محلی A و آدرس و درگاه عمومی B است. اگر B از قبل مشابه همین درخواست را برای آدرس و درگاه عمومی A ارسال کرده باشد، جدول NAT مربوط به B نیز یک خانه شامل اطلاعات عمومی A و اطلاعات محلی B دارد و بسته به مقصد می‌رسد. در غیر این صورت این بسته دور ریخته می‌شود ولی هنگامی که B بسته‌اش را ارسال می‌کند، از هر دو NAT عبور می‌کند. مشاهده می‌شود که در هر صورت ارتباط دو طرفه ممکن خواهد بود.



شکل ۳: برقراری ارتباط در حالت NAT متفاوت ـ منبع شکل

Scanned with CamScanner

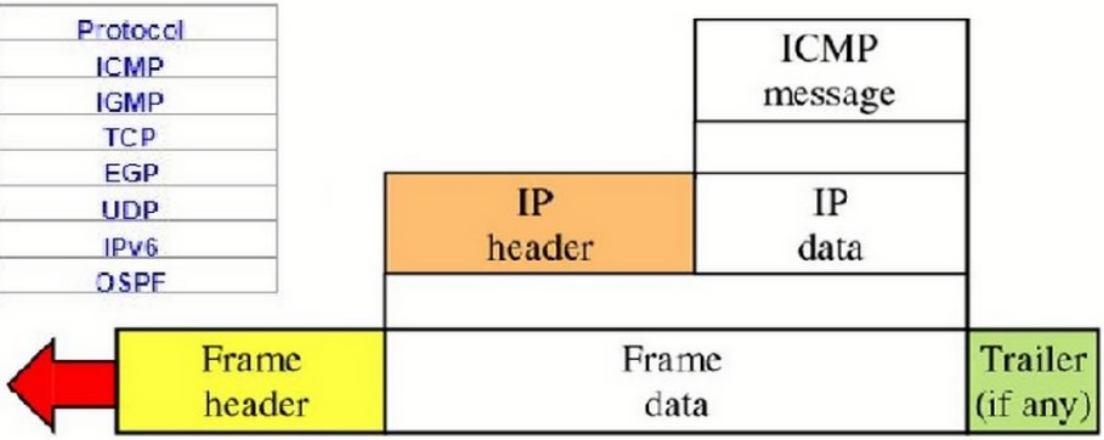
(Internet control message protocol): Icmp

این پروتکل برای مبادله اطلاعات کنترلی بین Host ها و روترها به کار می‌رود، Icmp بالای IP قرار می‌گیرد زیرا پیام‌های Icmp دقیقاً مثل پیام‌های UDP و TCP جدول داده دارند و پیام‌ها در IP حمل می‌شوند

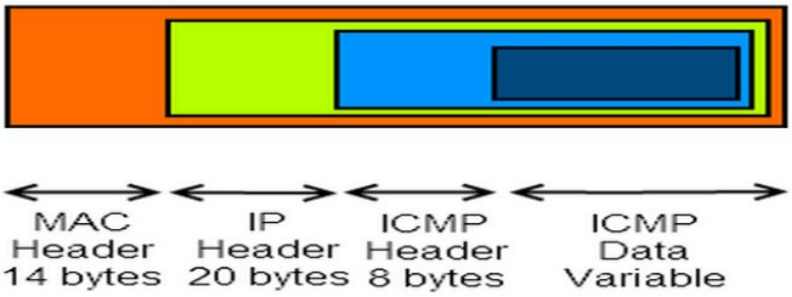
ICMP encapsulation

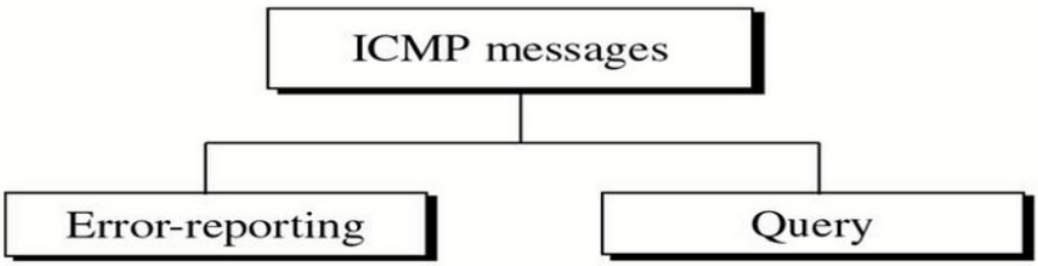
- The value of the protocol field in the IP datagram : 1

Value	Protocol
1	ICMP
2	IGMP
6	TCP
8	EGP
17	UDP
41	IPv6
89	OSPF



ICMP Packet Overview





Type	Message
3	Destination Unreachable
4	Source Quench
11	Time Exceeded
12	Parameter problem
5	Redirection

Type	Message
8 or 0	Echo request or reply
13 or 14	Timestamp
17 or 18	Address Mask
10 or 9	Router Sollicitation/Adv

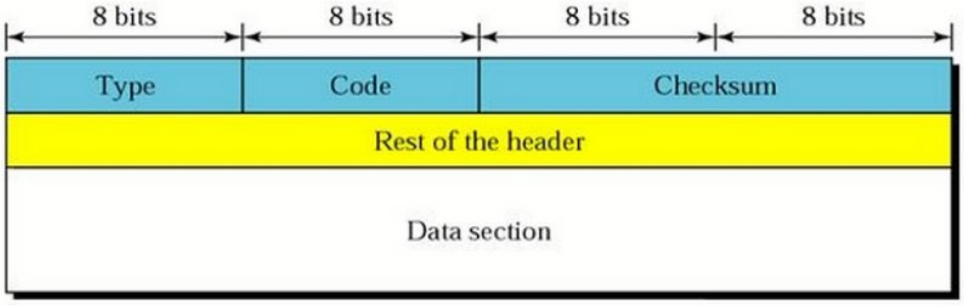
Scanned with CamScanner

type	*code*	Description	Query	Error
0	0	echo reply (Ping reply, Chapter 7)	•	
3		destination unreachable:		
	0	network unreachable (Section 9.3)		•
	1	host unreachable (Section 9.3)		•
	2	protocol unreachable		•
	3	port unreachable (Section 6.5)		•
	4	fragmentation needed but don't-fragment bit set (Section 11.6)		•
	5	source route failed (Section 8.5)		•
	6	destination network unknown		•
	7	destination host unknown		•
	8	source host isolated (obsolete)		•
	9	destination network administratively prohibited		•
	10	destination host administratively prohibited		•
	11	network unreachable for TOS (Section 9.3)		•
	12	host unreachable for TOS (Section 9.3)		•
	13	communication administratively prohibited by filtering		•
	14	host precedence violation		•
	15	precedence cutoff in effect		•
4	0	source quench (elementary flow control, Section 11.11)		•
5		redirect (Section 9.5):		
	0	redirect for network		•
	1	redirect for host		•
	2	redirect for type-of-service and network		•
	3	redirect for type-of-service and host		•
8	0	echo request (Ping request, Chapter 7)	•	
9	0	router advertisement (Section 9.6)	•	
10	0	router solicitation (Section 9.6)	•	
11		time exceeded:		
	0	time-to-live equals 0 during transit (Traceroute, Chapter 8)		•
	1	time-to-live equals 0 during reassembly (Section 11.5)		•
12		parameter problem:		
	0	IP header bad (catchall error)		•
	1	required option missing		•
13	0	timestamp request (Section 6.4)	•	
14	0	timestamp reply (Section 6.4)	•	
15	0	information request (obsolete)	•	
16	0	information reply (obsolete)	•	
17	0	address mask request (Section 6.3)	•	
18	0	address mask reply (Section 6.3)	•	

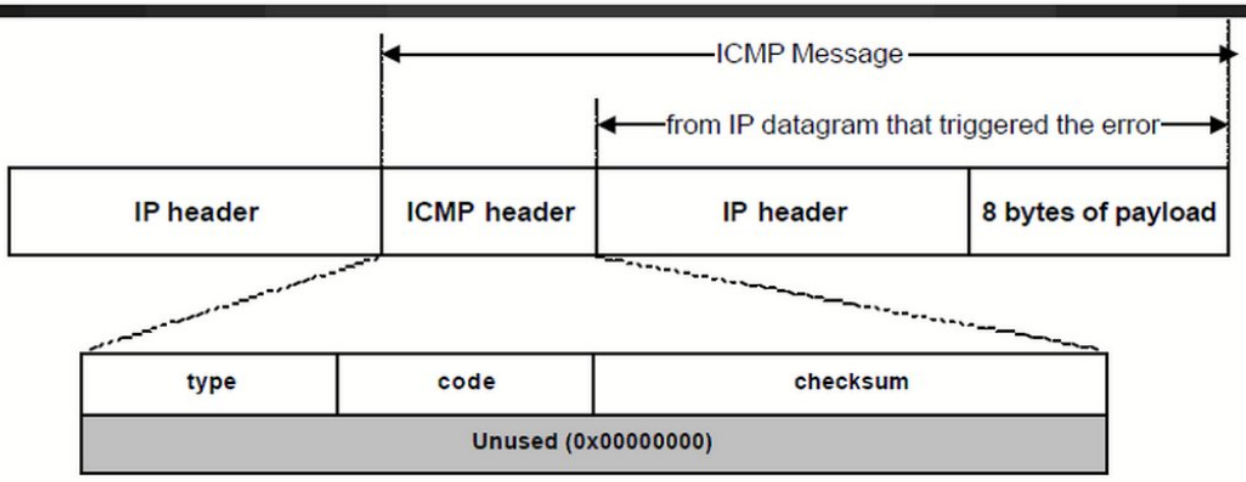
Scanned with CamScanner

Message Format

- An ICMP message has an 8-byte header and a variable-size data section
- The general format of the header is different for each message type, but the first 4 bytes are common to all
- The first field, ICMP type defines the type of the message and the Code field specifies the reason for the particular message type
- The rest of the header is specific for each message type
- The data section in error messages carries information for finding the original packet that had the error
- In query messages, the data section carries extra information based on the type of the query



ICMP Error message



- ICMP error messages include the complete IP header and the first 8 bytes of the payload (typically: UDP, TCP)

Scanned with CamScanner

• **Type 3**: when a router cannot route a datagram, or a host cannot deliver a datagram, the datagram is discarded and the sender is notified through ICMP message type 3.

•**Type 4**: when a router or a host discard a datagram due to congestion in the path from source to destination. Thus the sender is notified on the error and quenched to slow down the transmission.

• **Type 11**: to notify the sender when a router discard a datagram with TTL =0 and/or when all fragments did not reach the destination within a certain time window.

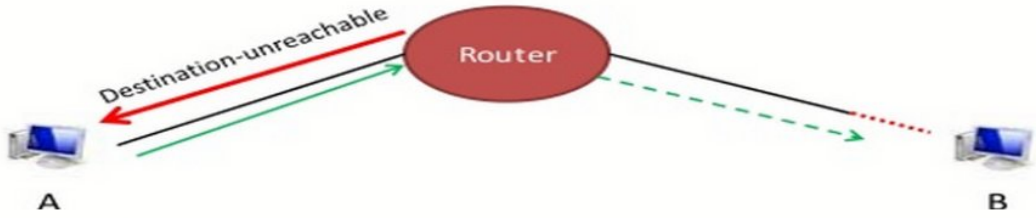
• **Type 12**: to notify the sender when a router or any host discarded a datagram because there is an error/ missing info from any field of the datagram.

• **Type 5**: to notify the sender when he sends a datagram to the wrong router. The receiving router will forward the datagram to the correct router and notify the host to update his routing table.

- **Error-reporting message**

destination-unreachable message

ICMP header	Type=3	Code=0-15	Checksum
	Rest of Header=unused (all zero)		
Data	IP header and first 8 bytes of original datagram's data		



❑ Source Quench

- **is designed to add a kind of flow control to the IP**
  - **IP does not have a flow-control mechanism embedded in the protocol**
- **when a router or host discards a datagram due to congestion, it sends a source-quench message to the sender of the datagram**
  - **making slow down the sending process**

Scanned with CamScanner

Type: 4	Code: 0	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

source-quench message

ICMP header	Type=4	Code=0	Checksum
	Rest of Header=unused (all zero)		
Data	IP header and first 8 bytes of original datagram's data		

Time exceeded

- Whenever a router receives a datagram whose time-to-live field has the value of zero, it discards the datagram and sends a time-exceeded message to the original source
- When the final destination does not receive all of the fragments in a set time, it discards the received fragments and sends a time-exceeded message to the original source

- In a time-exceeded message, code 0 is used only by routers to show that the value of the time-to-live field is zero. Code 1 is used only by the destination host to show that not all of the fragments have arrived within a set time

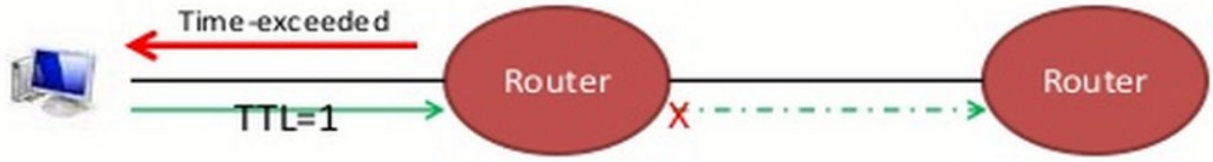
- Time-exceeded message format

Scanned with CamScanner

time-exceeded message

ICMP header	Type=11	Code=0 or 1	Checksum
	Rest of Header=unused (all zero)		
Data	IP header and first 8 bytes of original datagram's data		

- Code=0, TTL count exceeded
- Code=1, Fragment reassembly time exceeded



Parameter-problem

- **A parameter-problem message caused by ambiguity in the header part can be created by a router or the destination host**
- **Code 0 : error or ambiguity in one of the header fields**
  - **the value in the pointer field points to the byte with the problem**
- **Code 1 : the required part of an option is missing. In this case, pointer is not used**

parameter-problem message

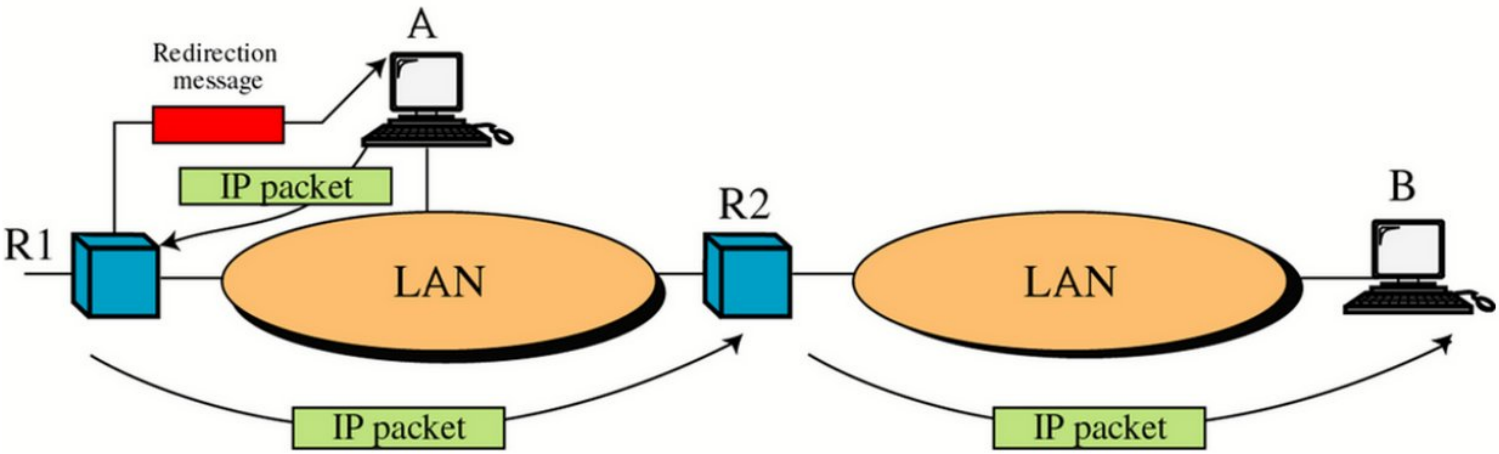
ICMP header	Type=12	Code=0,1,2	Checksum
	index	unused (all zero)	
Data	IP header and first 8 bytes of original datagram's data		

- Code=0, Pointer indicates the error
- Code=1, Missing a required option
- Code=2, Bad length

Scanned with CamScanner

Redirection

- A host usually starts with a small routing table that is gradually augmented and updated. One of the tools to accomplish this is the redirection message.
- A redirection message is sent from a router to a host on the same local network.



Redirection message format

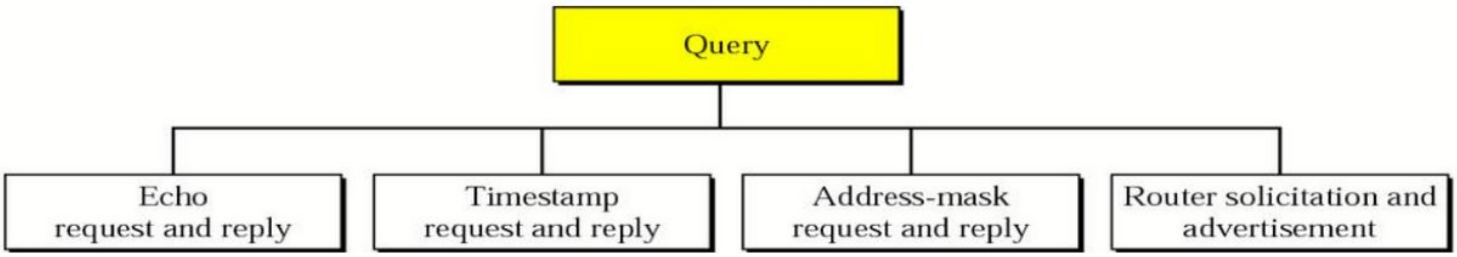
Type: 5	Code: 0 to 3	Checksum
IP address of the target router		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

- Code 0 : redirection for the network-specific route
- Code 1 : redirection for the host-specific route
- Code 2 : redirection for network-specific route based on specific type of service
- Code 3 : redirection for the host-specific route based on the specified type of service

Scanned with CamScanner

Query

- ICMP can also diagnose some network problems through the query messages, a group of four different pairs of messages
- In this type of ICMP message, a node sends a message that is answered in a specific format by the destination node.



Echo Request and Reply messages

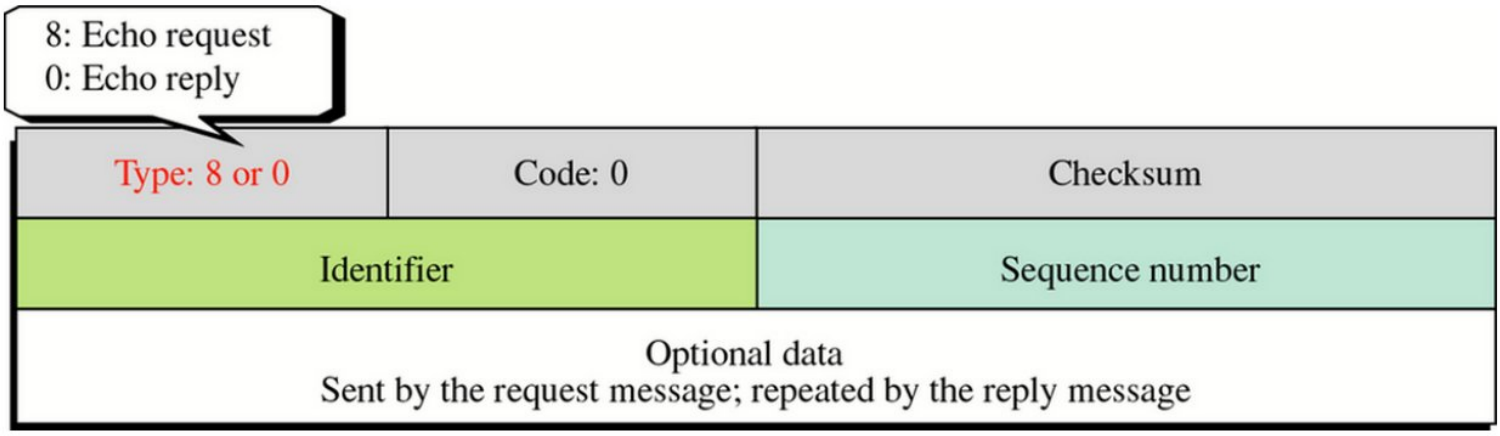
- designed for diagnostic purpose
- the combination of echo-request and echo-reply messages determines whether 2 systems (hosts or routers) can communicate with each other
- An echo-request message can be sent by a host or router. An echo-reply message is sent by the host or router which receives an echo-request message
- Echo-request and echo-reply message can be used by network managers to check the operation of the IP protocol

Echo-request and echo-reply messages can test the reachability of a host. This is usually done by invoking the ping command

Identifier and sequence number fields are not formally defined by the protocol and can be used by the sender

Echo-request and echo-reply message

Scanned with CamScanner



- **The identifier field**
  - defines a group of problems
  - ex) process ID that originated the request
- **The sequence number field**
  - keeps track of the particular echo request messages sent
- **At the user level**
  - Invoking the packet Internet groper (ping) command

- **Timestamp Request and Reply**
  - 2 machines (routers or hosts) can use the timestamp-request and timestamp-reply messages to determine the round-trip time needed for an IP datagram to travel between them
  - can used to synchronize the clocks in two machines
  - Three timestamp fields are each 32 bits long
    - holding a number representing time measured in milliseconds from midnight in Universal Time
      - Cannot exceed 86,400,000 = 24 x 60 x 60 x 1,000

Scanned with CamScanner

- **Timestamp-request and reply message format**

13: request
14: reply

Type: 13 or 14	Code: 0	Checksum
Identifier		Sequence number
Original timestamp		
Receive timestamp		
Transmit timestamp		

  - **original timestamp field : clock at departure time**
  - **receive timestamp field : at the time the request was received**
  - **transmit timestamp field : at the time the reply message departs**

- **The formulas for computing the one-way or round-trip time required for a datagram to go from a source to a destination and then back again.**
  - **Sending time = value of receive timestamp – value of original time stamp**
  - **Receiving time = time the packet returned – value of transmit timestamp**
  - **Round-trip time = sending time + receiving time**

- **Timestamp-request and timestamp reply message can be used to measure the round-trip time between a source and a destination machine even if their clocks are not synchronized**

Scanned with CamScanner

Example

- Value of original timestamp : 46
- Value of receive timestamp : 59
- Value of transmit timestamp : 60
- Time the packet arrived : 67

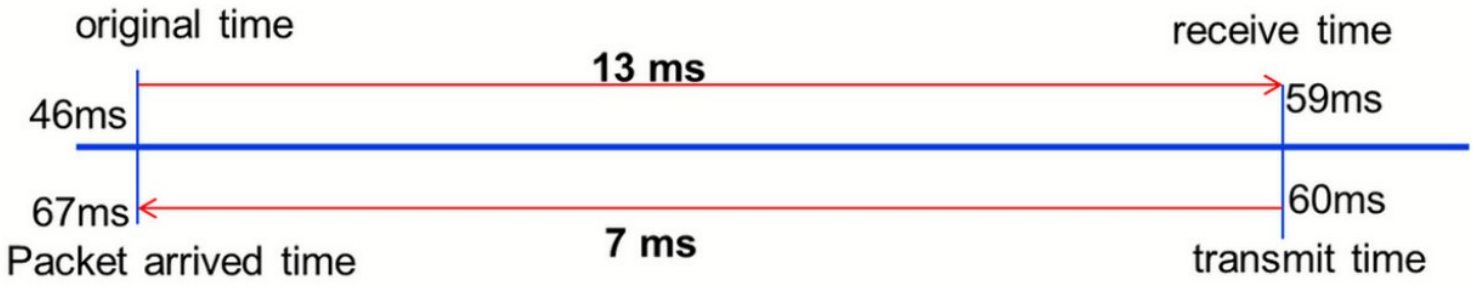
Sending time = 13 ms

Receiving time = 7 ms

Round-trip time = 20 ms

Synchronizing clocks between two machines

- Time difference = receive timestamp – (original timestamp field + oneway time duration)
- In previous example,
  - Time difference = 59 – (46 + 10) = 3



Address Mask Request and Reply

- for differentiating among network address, subnetwork address and host ID
- example, a host may know its 32-bit IP address as

  10011111.00011111.11100010.10101011
- left 20 bits are network and subnetwork addresses and remaining 12 bits are Host ID. In this case, following mask

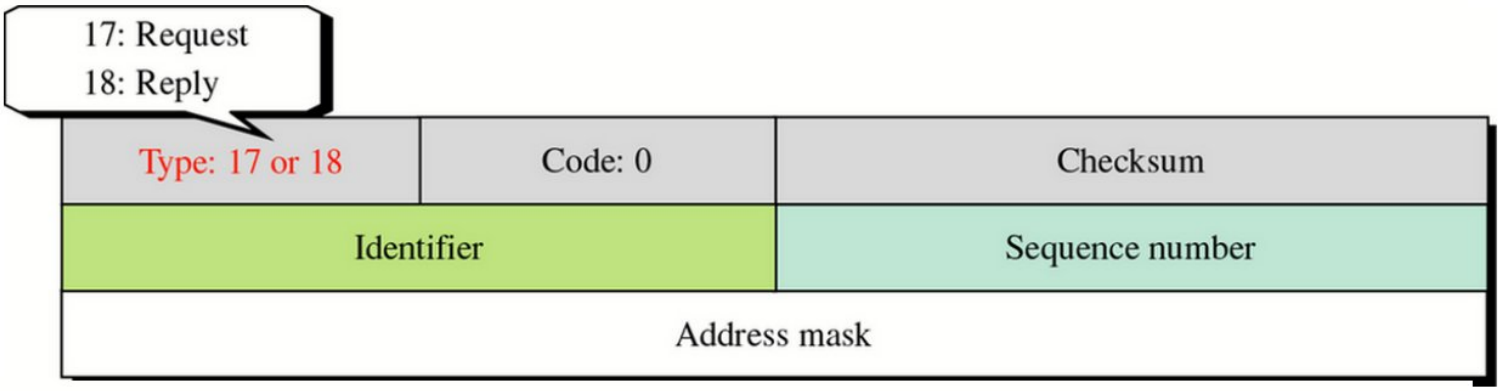
  11111111.11111111.11110000.00000000

Netld and subnetid → 10011111.00011111.1110

Host ID → 0010.10101011

Scanned with CamScanner

- To obtain its mask,
  - A host sends an address-mask-request message to a router on the LAN. (unicast or broadcast)
  - If the host knows the address of the router, it sends the request directly to the router, if not, it broadcasts the message.



- Masking is needed for diskless stations at start-up time.
- When a diskless station comes up for the first time
  - it may ask for its full IP address using RARP protocol
  - after receiving its IP address, it may use the address mask request and reply to find out which part of the address defines the subnet
- Router Solicitation and Advertisement
  - A host that wants to send data to a host on another network needs to know the address of routers connected to its own network.
    - the host should know if the routers are alive and functioning
    - A host can broadcast (or multicast) a router-solicitation message.
    - The router or routers that receive the solicitation message broadcast their routing information using the router-advertisement message.
      - A router can also periodically advertise router-advertisement messages even if no host has solicited

Scanned with CamScanner

Router-solicitation message format

Type: 10	Code: 0	Checksum
Identifier		Sequence number

Router-advertisement message format

- lifetime field : showing the number of seconds that entries are considered to be valid
- address preference level defines the ranking of the router
  - preference level 0 : default router
  - preference level 80000000_{16} : the router should never be selected as the default router

Type: 9	Code: 0	Checksum
Number of addresses	Address entry size	Lifetime
Router address 1		
Address preference 1		
Router address 2		
Address preference 2		
• • •		

یکی از پیام های معروف Icmp پیام ping است. ما وقتی می خواهیم تست کنیم که یک Host ای در شبکه هست یا نیست از پیام ping استفاده می کنیم. پیام ping توسط آیه ۲ تولید می شود. مثلاً اگر می خواهیم چک کنیم که به اینترنت وصل هستیم یا خیر می زنیم

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

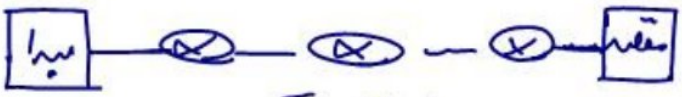
@konkurcomputer
www.konkurcomputer.ir

ping 4.2.2.4 ← آدرس DNS مرکز است

به این پیام می‌گویند Icmp echo request و این پیام توسط ساخته می‌شود، ماشین مقصد این پیام را دریافت و پیام echo reply را ارسال می‌کند. اگر کسی را می‌خواهیم (ماشینی که می‌خواهیم) ping کنیم باشد خودش پیام echo reply به ما می‌دهد و اگر نباشد، روترهای میانی پیام‌های دیگری را به سمت مبدا ping کننده می‌فرستند.

نکته: برنامه Traceroute که کارش نشان دادن مسیر (یعنی IP روترهای بین مبدا و مقصد) یک host به هر host دیگر همین طور اسم روترها، IP روترها، فاصله روترها از هم است از Icmp استفاده می‌کند

- برای این منظور برنامه Tracrout ماشین مبدا به تعداد هریک از روترها در طول مسیر و همین طور ماشین مقصد بسته‌های udp دیدست مقصد ارسال می‌کند (به تعداد اینها فرض بر ۳) و زمان رفت و برگشت هرکدام را محاسبه می‌کند



N-1 روتر

و این بسته‌ها را به گونه‌ای خاص تولید می‌کند

مبدا TTL بسته‌ها را 1 می‌گذارد، که در واقع این بسته برای روتر اول است، TTL بسته دوم را دو می‌گذارد (در واقع این بسته برای روتر دوم است) و به همین طور وقتی بسته مخصوص هر روتر به آن می‌رسد چون TTL اش به ۰ می‌رسد، روتر آن را دور می‌اندازد و یک پیام Icmp که نشان می‌دهد

تعداد بسته‌هایی که برنامه Trace- مبدا می‌فرستد = 3(N-1+1)
↑ Host

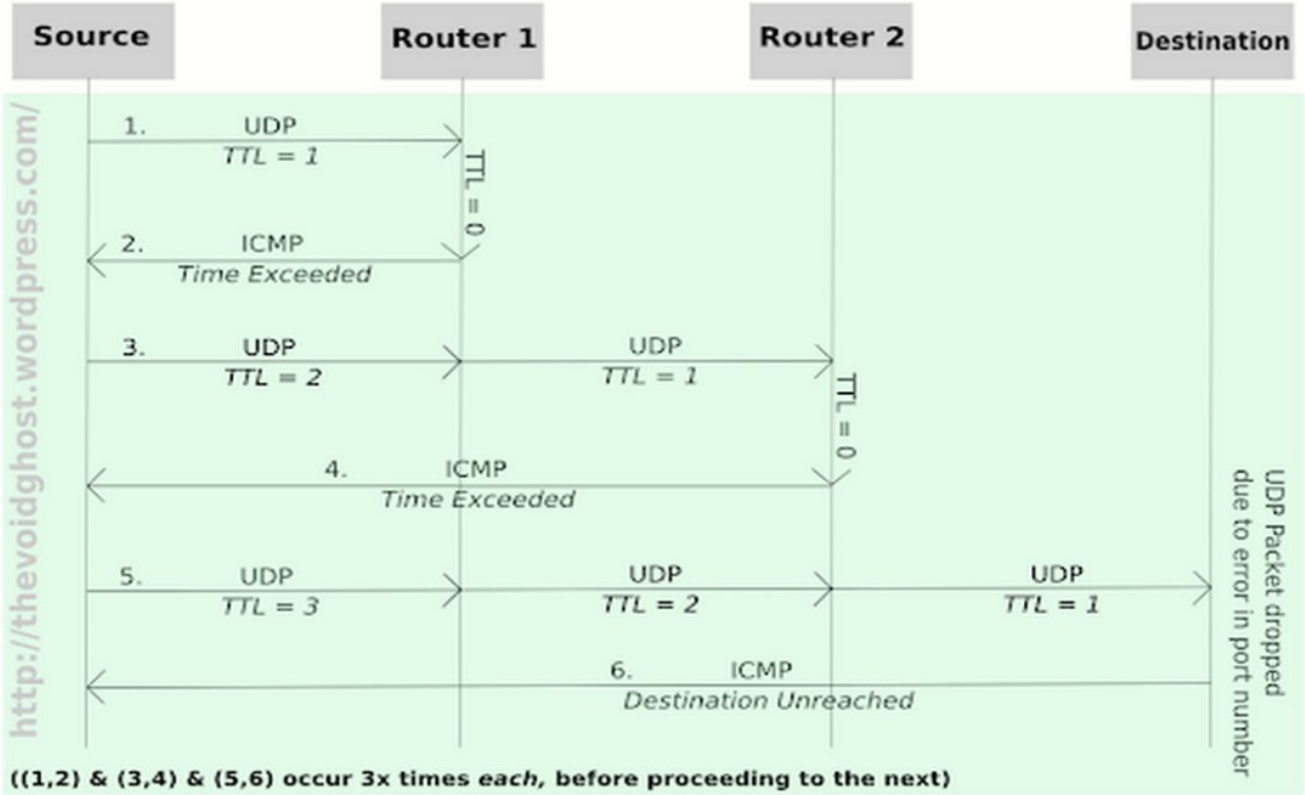
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

منتقلی شده است را برای مبدا ارسال می‌کند، یک پیام Icmp error نوع ۱۱ کد ۰ به ماشین مبدا ارسال می‌کند؛ حال با دریافت این پیام به ماشین مبدا، ماشین مبدا (برنامه Traceroute) می‌تواند با استفاده از تایمری که برای هریک از این پیام‌ها اشارت زده بوده، زمان رفت و برگشت را محاسبه کند و نصف این زمان را بعنوان فاصله بین خودش و روتر مربوطه اعلام کند

سوال - برنامه Traceroute ماشین مبدا از کجا می‌فهمد که چه زمانی باید فرستادن قطعه‌های UDP را متوقف کند؟

برنامه Traceroute به ترتیب سربسته با TTL=1 و سپس سربسته با TTL=2 و ... ارسال می‌کند و این کار را تا زمانی ادامه می‌دهد تا یکی از این قطعات به میزبان مقصد برسد، حال وقتی یکی از این بسته‌ها به میزبان مقصد می‌رسد چون هیچ فرآیندی در میزبان مقصد منتظر این قطعه UDP نیست، میزبان مقصد یک پیام Icmp error نوع ۳ و کد ۳ (port unreachable) به ماشین مبدا برمی‌گرداند و هاست مبدا با دریافت این پیام می‌فهمد که دیگر نیازی به ارسال بسته‌هایی با TTL بزرگتر نیست



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

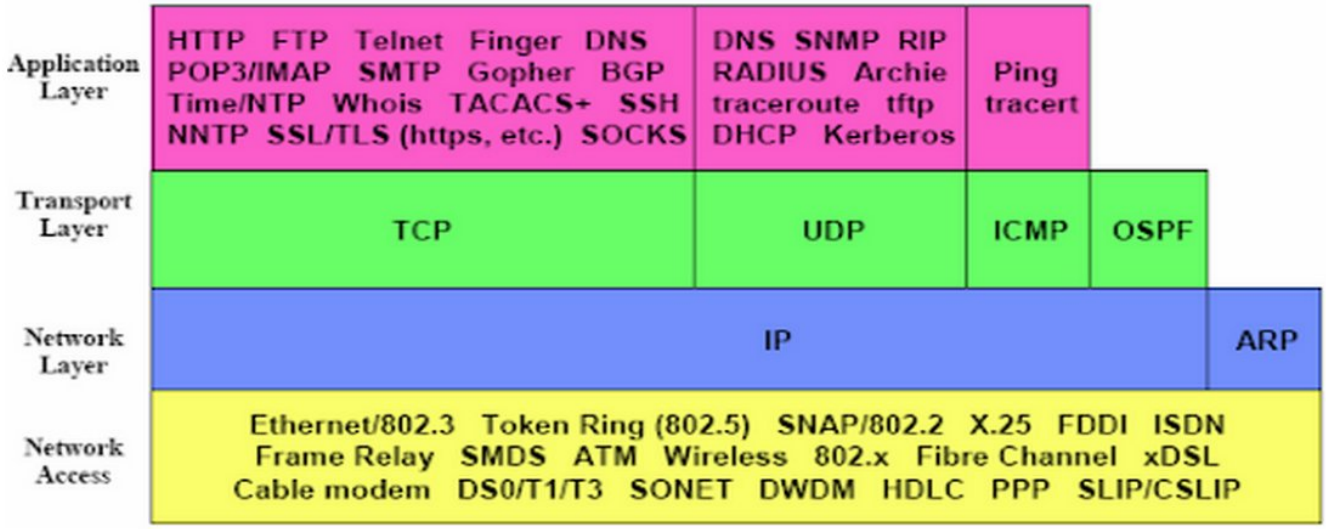
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

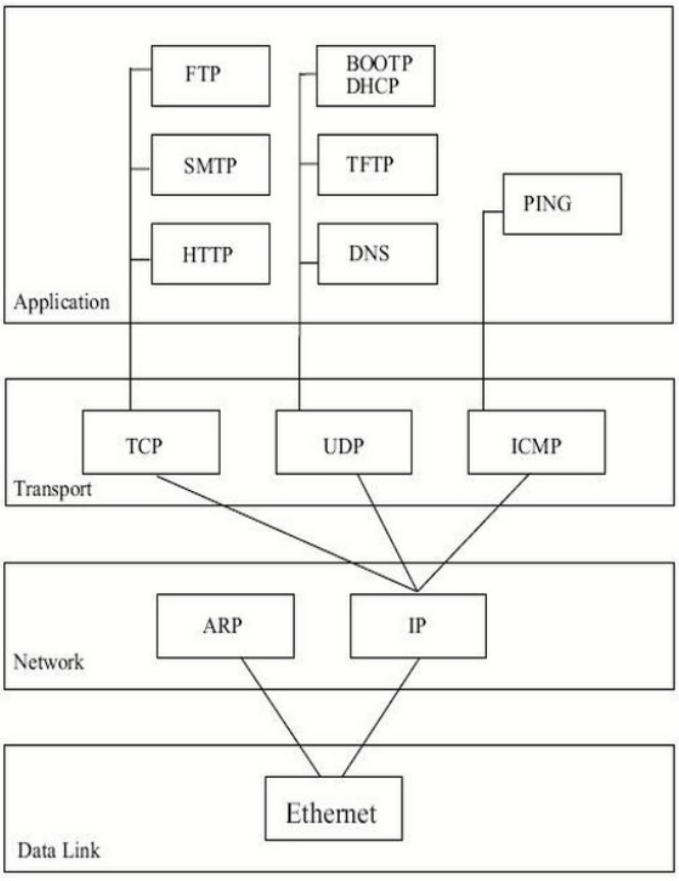
شبکه های کامپیوتری

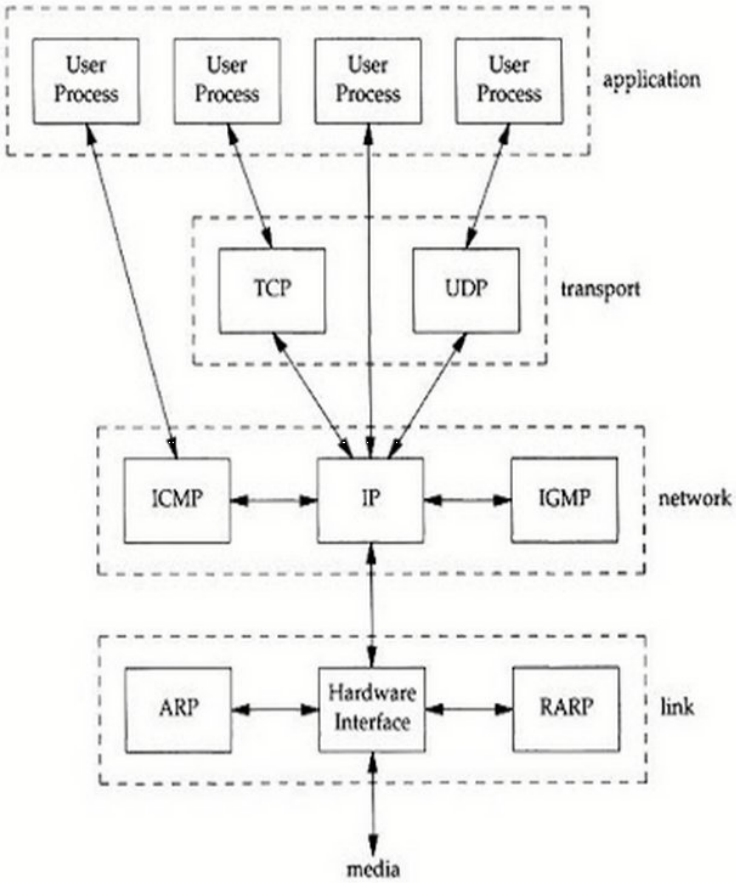
رامین رضوی

نکته: برنامه tracert برای windows است و برنامه traceroute مختص linux است.

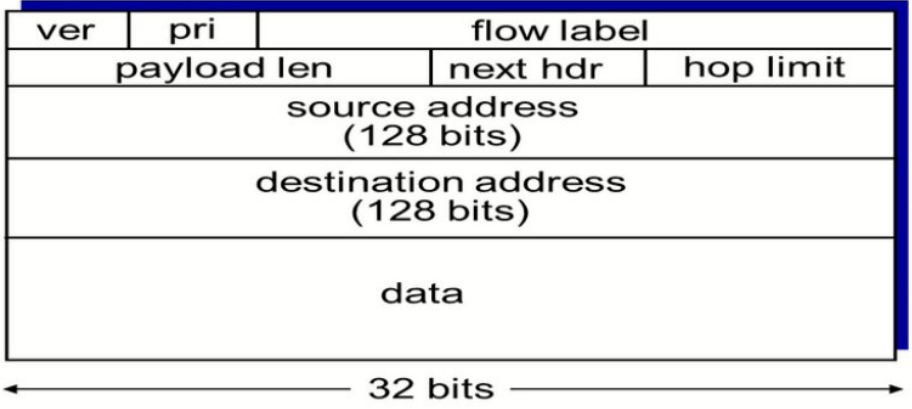
نکته: tracert فقط از Icmp استفاده می‌کند (Icmp echo requests) اما برنامه traceroute از UDP استفاده می‌کند و از Icmp استفاده نمی‌کند (البته این موضوع به توزیع لینوکس هم بستگی دارد)







سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner



IP V6

در IPV6 آدرس های IP ، ۱۲۸ بیتی هستند . طول هدر در IPV6 ۴۰ بایت است و ۲ برابر طول هدر IPV4 است ، البته درصورتیکه IPV4 ، option نداشته باشد

کلاس ترافیک (Traffic class) : این همان Type of servic (نوع سرویس) ای است که در IPV4 داشتیم و مانند آنجا ۸ بیتی است ، با این فیلد می توانیم QOS را ساپورت کنیم

برچسب جریان : یادمان هست که در مدار مجازی جریان داشتیم و با lable کار می کردیم . اما در IP این چنین نبود . این فیلد ۲۰ بیتی است .

در IPV6 می توانیم بین سرویس های انتقال اعداد تصویر و یا ترافیک افرادی که می خواهند اولویت بالاتری بسته هایشان داشته باشد بروال بین منظور پول پرداخت می کنند و سرویس های آنلاین مثل میل و انتقال فایل و سه تفاوت قائل بشویم بصورتی که برای نوع اول جریان از برچسب جریان استفاده کنیم و برای نوع دوم مانند IPV4 عمل کنیم . بنابراین روترها باید بتوانند به جریان ها سرویس های بهتری ارائه بدهند

- بنابراین در IPV6 برچسب زدن به بسته های متعلق به یک جریان خاص که خواسته نوع خاص از سرویس گرفتن را برای آن درخواست کرده ، مانند سرویس های real time و یا QOS ان غیر آنچه که پیش فرض بوده امکان پذیر است .

طول داده : طول محموله داده : این فیلد ۱۶ بیتی بی علامت برای مشخص کردن تعداد بایت های داده است .

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

سرآیند جدید: همان upper layer protocol است که در IPV4 داشتیم و مشخص می‌کند IP باید به چه کسی در لایه بالاتر تحویل بدهد. مثلاً Tcp بدهد یا UDP یا Icmp. این فیلد از همان مقادیر فیلد upper layer pro- در IPV4 استفاده می‌کند

- سقف جهش (Hop limit): همان TTL است

گذر از IPV4 به IPV6:

چگونه می‌توان اینترنت را که بر اساس IPV4 بنا شده است، به سمت IPV6 سوق داد و چه تمهیداتی باید این کار را انجام بدهیم؟

* روترها و سیستم‌هایی که بر اساس IPV6 تولید می‌شوند می‌توانند پیام‌ها و دیتاگرام‌های IPV4 را عبور بدهند، اما عکس آن امکان‌پذیر نیست

چه پیشنهادهایی وجود دارد: ۱) تعیین یک روز مشخص: عملی نیست

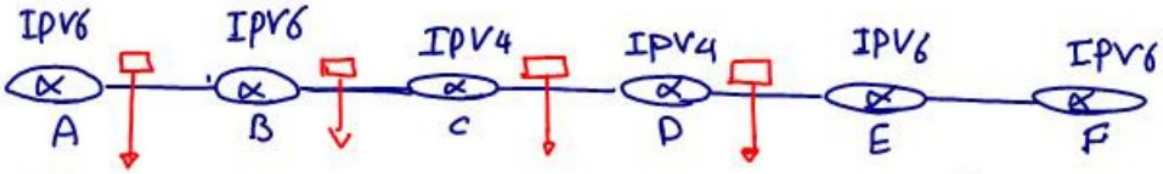
Dual stack approach (۲

Tunneling (۳

۲) رهیافت دوپشته‌ای: هر دستگاه جدیدی که بر اساس IPV6 ساخته می‌شود باید بتواند پروتکل IPV4 را نیز ساپورت کند. بدین Device ها IPV6/IPV4 می‌گویند. یک گره IPV6/IPV4 باید هر دو آدرس IP و زبان ۴ و ۶ را داشته باشد، همین طور باید تشخیص دهد که Device جدید ال که بخش فعال است، Device، IPV4 ای است یا IPV6 است. Device جدید هر چه که باشد باید با زبان خودش با آن صحبت کنیم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir



جریان = x
S = A
D = F
payload

S = A
D = F
payload

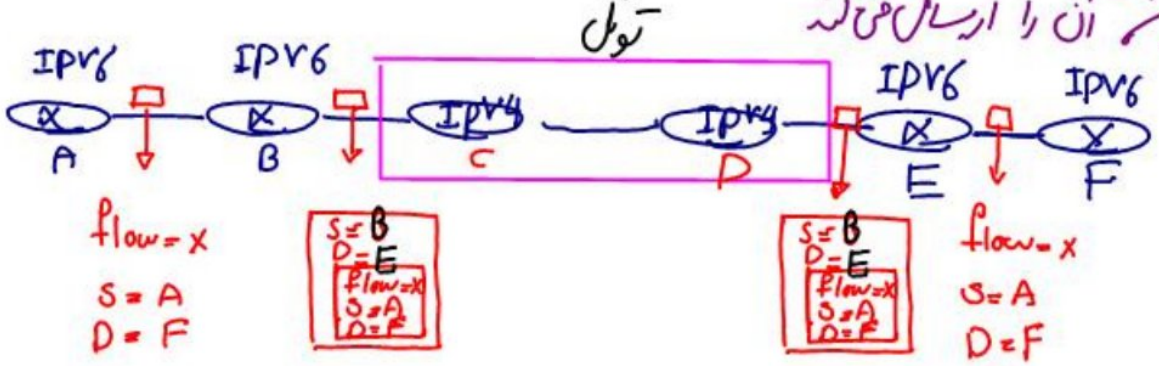
S = A
D = F
payload

flow = ??
S = A
D = F
payload

* وقتی از IPV6 به IPV4 بسته ای را ترجمه می‌کنیم یکسری از اطلاعات از بین می‌رود، مثل برچسب جریان ← بنابراین اگر می خواهیم همه اطلاعاتی را از دست ندهیم باید به سراغ روش ۳ برویم

نکته) اینکه تصمیم گیرنده بعدی از نظر IPV4 یا IPV6 بودن یا نبودن چه است را DNS مشخص می کند

۳) Tunneling approach : (تونل زنی) : وقتی روتر فعلی قرار است یک بسته را به روتر بعدی که IPV4 است ارسال کند، تمام بسته IPV6 را بعنوان دیتا می‌گذارد درون یک بسته IPV4 و به روتر بعدی ارسال می‌کند، به این کار می‌گویند تونل زدن. این بسته به همین صورت جلو می رود تا برسد به یک روتر IPV6 که روتر بعدی آن هم IPV6 است، در اینصورت، روتر ابتدایی هدر IPV4 را می‌کند و دیتا درون آن را ارسال می‌کند



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

ایجاد امنیت در IP:

پروتکل IPsec: IP این نیست و اگر بخواهیم این باشد باید از این پروتکل استفاده کنیم. این پروتکل این ۲ به شکل بکارگسترده ای در VPN ها به کار گرفته می‌شود (شبکه های خصوصی مجازی). این پروتکل با IPV4 و IPV6 سازگار دارد. برخلاف IPV6 و IPV4 برای استفاده از IPsec نیازی به جایگزین کردن این پشته پروتکل در روترها و host ها نیست و این ۲ هاست بخواهند با هم ارتباط برقرار کنند، کافی است، فقط این پروتکل در یکی از این هاست ها وجود داشته باشد و هر Device ها دول میدی توانند IPV4 یا IPV6 باشند

- IPsec برخلاف IP یک پروتکل اتصال گرا است و در ابتدا (اتصال) دو میزبان مبادله مقدار بین خودشان یک نشست برقرار می کنند، حال وقتی این نشست برقرار شد، تمامی قطعات UDP و TCP ارسال شده توسط هاست ها رمزنگاری شده و فیلدهای امنیتی دیگر نیز به آنها اضافه می شود و در مقصد رمزگشایی می شود و به لایه انتقال (UDP یا TCP) تحویل داده می شود.

سرویس های امنیتی که IPsec ارائه می کند عبارت اند از:

۱) قرار داد رمزنگاری: سازوکاری که به ۲ میزبان اجازه میدهد تا بر سر الگوریتم ها و کلیدهای رمزنگاری توافق کنند

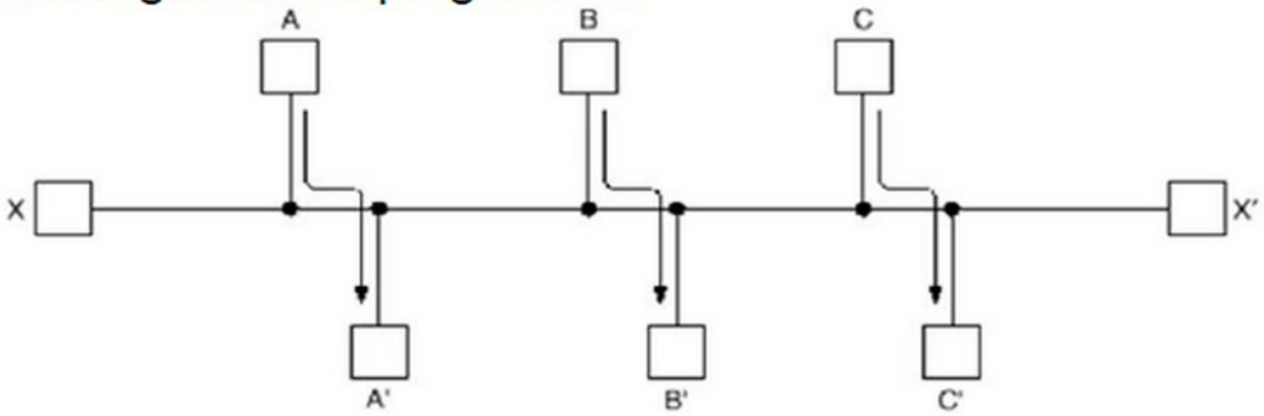
۲) رمزنگاری داده های دیتاگرام: محموله رمزشده فقط توسط Host مقصد قابل رمزگشایی است

۳) صحت داده (جامعیت داده): دیتاگرام ها در مسیر دستکاری نشده باشند

۴) احراز هویت: (شناخت طرفین): مطمئن بشیم طرفین همان کسانی هستند که ادعا می کنند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

- Routing algorithm requirements
  - Correctness
  - Simplicity
  - Robustness: cope with changing topology
  - Stability: converge quickly
  - Fairness: guarantee progression



Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

الگوریتم های مسیریابی :

مسیریابی عبارت است از تعیین مسیرهای مناسب از فرستنده به گیرنده از طریق روترهای شبکه

هدف یک الگوریتم مسیریابی این است که یک مسیر مناسب بین مبدا و مقصد پیدا کند

پروتکل های مسیریابی از یک دیدگاه به ۲ دسته متمرکز و توزیع شده تقسیم می شوند :

۱) الگوریتم های سراسری یا متمرکز : این الگوریتم ها اطلاعات مربوط نحوه اتصال های گره های شبکه و هزینه لینک های بین همه گره ها را بطور کامل دارند . به این الگوریتم ها الگوریتم های حالت لینک Link state algorithm (LS) گفته می شود

۲) الگوریتم مسیریابی غیر متمرکز : محاسبات کمترین هزینه مسیر بین یک گره مبدا تا مقصد بصورت تکرار شونده و توزیع شده انجام می شود . هیچ گره ای اطلاعات کاملی از نحوه اتصال شبکه و هزینه لینک ها در اختیار ندارد و هر گره تنها باید آدرس بهترین مسیر تا مقصد مشروع به مبادله اطلاعات با گره های همسایه خودش می کند و در فرآیندی تکرار شونده به تدریج کمترین فاصله بین خودشان و مقصد را پیدا می کنند

الگوریتم های مسیریابی به ۲ گروه استاتیک و دینامیک تقسیم می شوند

خیلی مواقع در دنیا شبکه های ریتا این فرضیات برقرار نیست. ساده ترین حالتی که این فرضیات برقرار نیست ثابت نبودن ماتریس ترافیک آن است.

۱) Non-adaptive routing or static : (Flooding مثل) توپولوژی شبکه، ظرفیت لینک ها، ماتریس داده ها و ... fix و مشخص است و مسئله این است که مسیریابی را به چه شکل انجام دهیم که به بهترین نحو از منابع آن شبکه استفاده کنیم

۲) Adaptive rou... Dynamic : عنایا تقسیم گیری در مورد مسیریابی به وضعیت شبکه و وضعیتا

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

ترافیک شبکه بستگی دارد. لذا در اینجا اطلاعات سان باید بصورت کاملا پرمودیک بروز رسانی بشود

در الگوریتم های دینامیک تقسیم بندی برای روتینگ می توانند بر اساس موارد زیر باشد

- Distance ۱
- Hop count ۲
- Traffic rate ۳
- congestion ۴

Flooding: ایده این الگوریتم این است که هر روتر بسته ای را که دریافت می کند روی تمامی پورت های دیگرش ارسال کند. بنابراین ما مطمئنیم که بسته به مقصد می رسد.

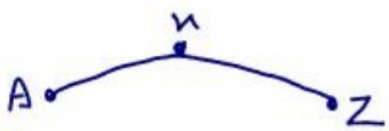
- خیلی ناکارآمد است ـ تعداد زیادی بسته که به مقصد هم نمی رسند تولید می شود
- برای Damp کردن Flooding ایده های بسیاری وجود دارد که یکی از آنها Hope count است

flooding useful for

1) extreme robustness
2) reliable
3) Broad cast
4) Reference algorithm

* Flooding یک بسته را از مبدا به مقصد در حداقل زمان ممکن می رساند و هیچ روشی از این سریعتر نخواهد بود
به همین علت بعنوان مرجع برای مقایسه الگوریتم ها استفاده می شود

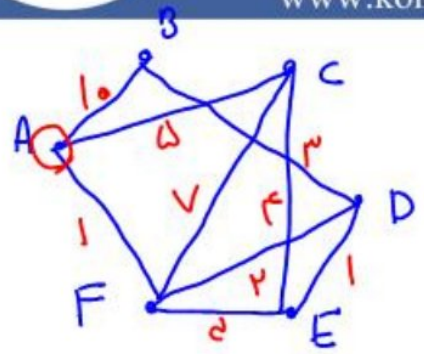
optimality principle:



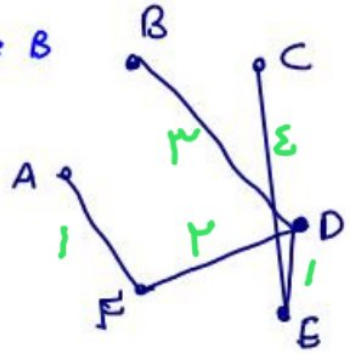
* در شبکه برای هر نودی مثل B یک روتت وجود دارد که این روتت بهترین مسیر رسیدن تمامی نودهای دیگر شبکه به B را نشان می دهد که به این روتت sink tree(B) گویند و B در ریشه این

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

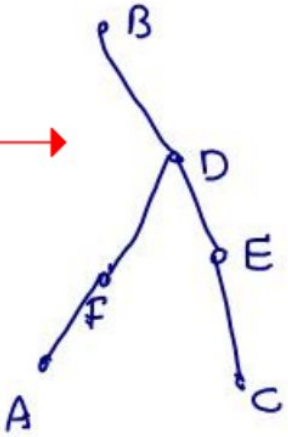
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir



sink tree B



درخت است.



- این درخت حتما حلقه ندارد، یعنی هیچ وقت نمی‌تواند از یک نود به ریشه B دوتا بهترین مسیر پیدا کند
- حریص‌تر برای ارسال یک بسته به سمت مقصد چندین پورت و option دارند، یک روتر بهترین کاری که می‌تواند برای رساندن یک بسته به مقصد انجام بدهد آن است که sink tree مقصد را داشته باشد و در نهایت sink tree را ارسال کند.

نکته: sink tree یک نود می‌تواند ثابت (استاتیک) یا داینامیک باشد، بعنوان مثال اگر شاخص ما به ازدحام ربط داشته باشد، آن‌گاه متریک هر یال به ازدحام ربط دارد و آن وقت بهلکرد نود ها و ترافیک شبکه، متریک هر یال را در طی زمان بصورت داینامیک عوض می‌کند، بنابراین اگر در یک لحظه یک روتر می‌خواهد بهترین مسیر به یک مقصد را پیدا کند باید در همان لحظه sink tree مقصد را بدست بیاورد.

- الگوریتم‌های زیادی برای بدست آوردن sink tree هر نود وجود دارد که یکی از معروف‌ترین آن‌ها را می‌توان دکسترا (دیجسترا) ارائه داد.

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

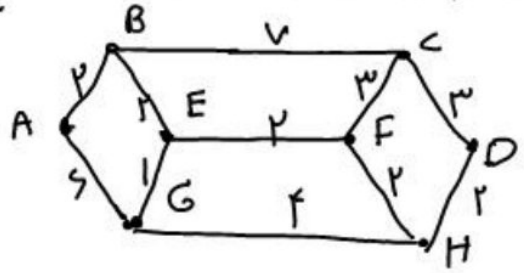
الگوریتم کوتاه‌ترین مسیر (shortest path Algorithm (Dijkstra

یک گراف وزن دار را در نظر بگیرید، وزن یالها مثبت است، هدف یافتن کوتاه‌ترین مسیر بین یک گره تا سایر گره‌ها است. در واقع هدف یافتن sink tree نود A است.

برای بدست آوردن sink tree A یک جدول درست می‌کنیم که در این جدول همه نودهای دیگر را در ستون‌ها می‌نویسیم. یک مجموعه که در ابتدا فقط شامل A است در نظر می‌گیریم

step 1: فاصله همه نودهای مجاور به مجموعه مان (در ابتدا فقط A جز مجموعه مان است) را همراه یالی که از طریق آن به سمت A کوتاه‌ترین مسیر وجود دارد را روی نودهای مجاور به مجموعه مان می‌نویسیم

step 2: سپس از بین نودهایی که مقدار گرفته اند، کوچکترین شان را به مجموعه مان (درخیمان) اضافه می‌کنیم



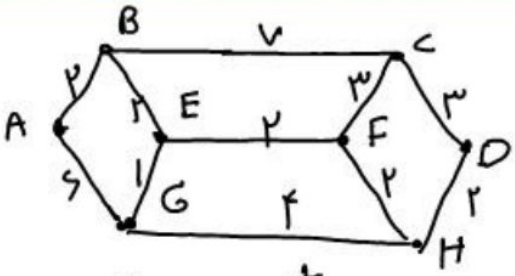
سپس مجددا قدم اول را انجام میدهیم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

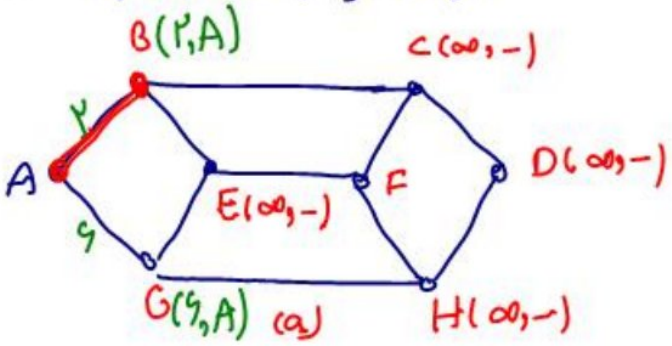
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir
MSc-PhD Computer-IT

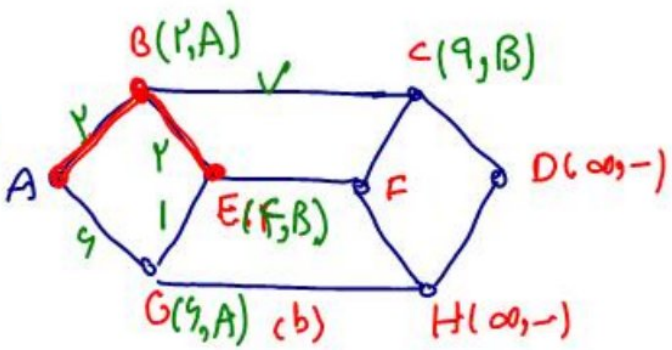
شبکه های کامپیوتری

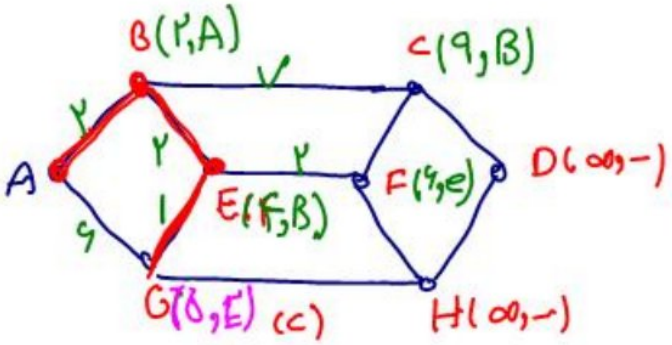
رامین رضوی

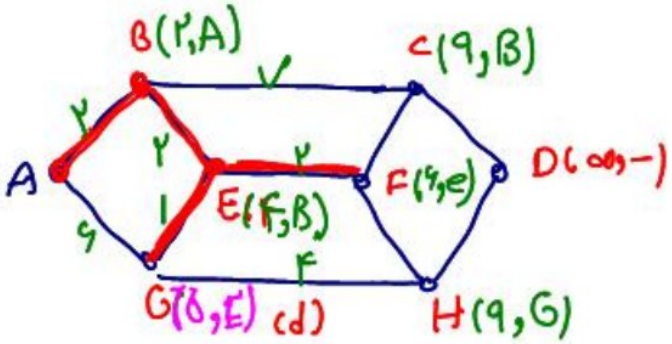


Base set	B	C	D	E	F	G	H
• A	2,A	∞	∞	∞	∞	6,A	∞
1 A,B		9,B	∞	4,B	∞	6,A	∞
2 A,B,E		9,B	∞		6,E	5,E	∞
3 A,B,E,G		9,B	∞		6,E		9,G
4 A,B,E,G,F		9,B	∞				8,F
5 A,B,E,G,F,H		9,B	10,H				
6 A,B,E,G,F,H,C			10,H				
7 A,B,E,G,F,H,C,D							









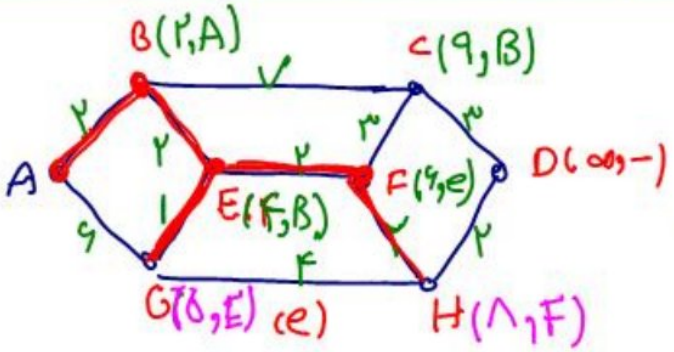
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

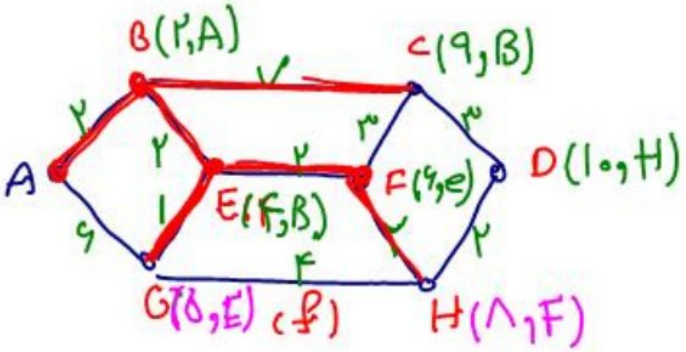
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

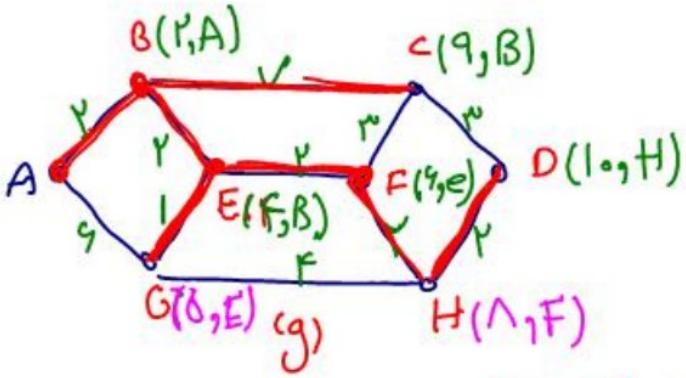
شبکه های کامپیوتری

رامین رضوی

@konkurcomputer
www.konkurcomputer.ir







(DVR) OR (DV) Distance vector Routing

در اینترنت بخش RIP یا (Routing information protocol) می‌باشد

این الگوریتم یک الگوریتم توزیع شده و iterative است ، به این علت توزیع شده است که هیچ روتری در ابتدا گراف شبکه را ندارد یعنی کسی global informa- ندارد ، و الگوریتم دارد روی روترهای مختلف Run می‌شود و بر اساس اجرا الگوریتم روی روترهای مختلف جدول های فوروارد‌ینگ را کامل می‌کند . پارامتر بهینه سازی در این روش تا ضیه لازم برای رسیدن یک بسته از مبدا به مقصد است .

هر روتر باید بردار فاصله‌اش را به دست آورد ، برای اینکار هر روتر بصورت زیر عمل می‌کند هر روتری بعد از روشن شدن اش ، هم فاصله خودش با همسایگان اش را به دست می‌آورد (برای اینکار یک بسته بنام hello به همسایگان اش می‌فرستد و همسایه ها پس از دریافت این بسته را می‌خوانند و نود

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

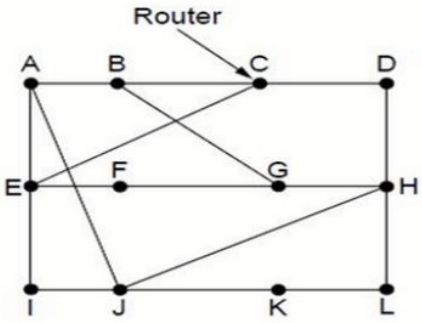
رامین رضوی

می دهند که فاصله اش تا هر کس $\frac{RTT}{2}$ است) و هم به همسایه هایش می گوید در جدول فاصله تون با تونل های دیگر شبکه را به من بدید.

عددی متفاوت نیستند چون فرض شده شبکه پویاست و فاصله بین J و A که الان به دست آمده، ممکن است با فاصله بین A و I که در جدول بردار فاصله A به J داده می شود متفاوت باشد چون این جدول ممکن است برای ۲ دقیقه قبل بوده باشد (در همین حین A یا I نیز می توانند متفاوت باشند)

* هر نودی به وسط مقصدها فقط گام بعدی را از کوتاهترین مسیری که تا این لحظه به دست آورده می داند. هر نودی همگی دیگر اینکه برای به مقصد ۸ از فلان جا برو (از فلان پورتم خارج شو) و لی تا مقصد راه دارد. بنابراین فاصله ها در هر سطر دوتراست، فاصله تا گام بعدی نیست و فاصله تا مقصد است.

Distance Vector Routing



(a)

To	A	I	H	K	New estimated delay from J	Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	—
K	24	22	22	0	6	K
L	29	33	9	9	15	K
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6	New routing table for J	

Vectors received from J's four neighbors

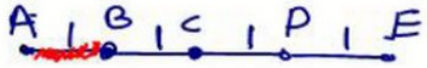
(b)

(a) A network.
(b) Input from *A, I, H, K, and the new routing table* for *J*.

Computer Networks, Fifth Edition by Andrew Tanenbaum and David Wetherall, © Pearson Education-Prentice Hall

Scanned with CamScanner

* DVR با روشی که گفتیم حتما در همه موارد کار نمی کند (در واقع می توان گفت در برخی از موارد stable و همگرا نیست) و به جای همگرا شدن واگرا می شود .



	A	B	C	D	E
ابتدا	∞	∞	∞	∞	∞
1)	1	∞	∞	∞	∞
2)	1	2	∞	∞	∞
3)	1	2	3	∞	∞
4)	1	2	3	4	∞
	3	2	3	4	4
	3	4	3	4	4
	5	4	5	4	6
	5	6	5	6	6

در اینجا فاصله هر نود را تا A بعد از هر آپدیت سوال می خواهیم بنویسیم و به بقیه کاری نداریم

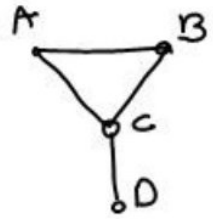
به این مشکل که پیش می آید می گویند شمارش تا بینهایت count to infinity

Scanned with CamScanner

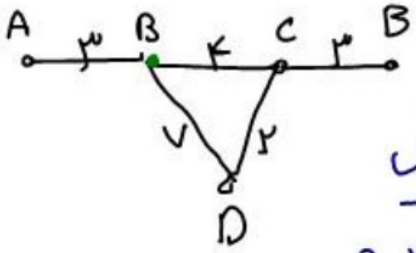
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

برای رفع این مشکل پیشنهاد این است که وقتی B از C پرسید فاصله توی C تا A چند است، C بگه بابا جان من خودم بسته ام را دارم میدم است توی B که تو بدون به A دیگه توی B نسبته تو به من C نده که بدم به A، C به B بگه فاصله من تا A ∞ است.



به این میگن split Horizon Hack
poisened Rerese



باز: با این ایده هم مشکل حل نمی شود.

فکر کنید مسیر A به B قطع میشود، B تا حالا فکر می کرده به A یک مسیر به طول ۳ دارد. C قبلا مسیری به طول ۷ به A داشته، حالا B میگه من یک مسیری به طول ۴ به C داشتم و بعد از اونجا با ۷ میدم به A. یعنی می شود ۱۱ تا. اما با توجه به اینکه C به B می گوید فاصله ام تا A ∞ است این اتفاق دیگر نمی افتد. D یک مسیر به A با فاصله ۹ دارد از طریق C. D به C می گوید مسیرم به A ∞ است و به B می گوید مسیرم به A ۹ است، حالا وقتی لینک A و B حذف شود، B فکر می کند که می تواند از طریق D به A برود در صورتیکه مسیری وجود ندارد.

* دلیل اصلی این مشکل در RIP این است که نودها مشاهداتشون از شبکه فقط محدود است به همسایه هاشون و چون در RIP هیچ نودی به تنهایی هیچ حسی نسبت به توپولوژی شبکه ندارد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

- همینطور که برای حل این مشکل هر نودی باید بداند که توپولوژی شبکه چیست تا هر روتر بتواند sink tree سایر نودها را بدست آورد.

Link state Routing

این الگوریتم چهار تا گام دارد.

1) هر روتر همسایه‌هایش را بشناسد: ارسال Hello packet و گرفتن ID
2) فاصله‌اش را تا آنها اندازه بگیرد
3) به همه نودهای دیگر این اطلاعات را بدهد
4) هر نودی توپولوژی شبکه را بدست بیاورد و shortest paths هزینه را محاسبه از روی توپولوژی بدست بیاورد

* هر روتر بسته‌ای بنام Link state packet تولید و بصورت پریودیک ارسال می‌کند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

- مرتبه الگوریتم LSR، $O(N^2)$ است

- تعداد پیام های مبادله شده $O(nxe)$ است
  - e: تعداد یالها
  - n: تعداد گره ها

*larg memory requirement ~ $O(NK)$

N= number of router

K= network node degree.

مسیریابی سلسله مراتبی

ما در اینترنت از الگوریتم DVR بعلت مشکلاتی که دارد نمی توانیم استفاده کنیم و وقتی تعداد روترهای خیلی بالا برود هرگز همگرا نخواهد شد، از LSR هم نمی توانیم استفاده کنیم چون scalable نیست (هم تعداد پیام ها زیاد رد و بدل می شود و هم سطرهای هر روتر خیلی بزرگ می شود)

در ضمن هرکس در سازمان خودش شاید بخواهد مسیریابی ویژه خود را داشته باشد، برای حل هر ۲ مشکل مقیاس پذیری و استقلال اجرایی روترها را به zone هایی، AS هایی (Autonomous system) تقسیم می کنند، که هر AS تحت تظارت یک ISP یا یک شبکه سازمانی است. هر AS الگوریتم مسیریابی مختص خودش را می تواند داشته باشد که به آن

intra autonomous systems routing algorithm

OR

interior gateway protocol

پروتکل دروازه داخلی

آن AS گفته می شود، RIP، OSPF، Is-Is پروتکل های مسیریابی درون AS هستند. در داخل یک AS

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

تمامی روترها یک پروتکل مسیریابی درون AS واحد را اجرا می‌کنند، اینگونه ما به خود مختاری که در تعریف AS بود می‌رسیم

یک روتر درون AS1 نیازی نیست روترهای دیگر درون سایر AS ها را بشناسد و فقط کافی است که بداند بسته اش را به کدام gateway اش دهد و بنابراین قرارنیست یک مسیریابی بین همه روترهای شبکه اجرا شود و مسیریابی باید بین AS ها انجام شود و چون تعداد AS ها کم است، مشکل مقیاس پذیری را هم حل کرده ایم.

یک روتر می خواهد بسته ای را به سمت مقصد ارسال کند

مقصد داخل همان AS باشد: با مسیریابی داخل AS ها هر روتر بهترین مسیر به سایر روترهای آن AS را می داند.

مقصد خارج از آن AS باشد: AS فقط یک روتر دروازه (gateway) داشته باشد، روتر مبدا بسته را به سمت این روتر ارسال می کند، این gateway هم بسته را به خارج AS ارسال می کند

AS بیش از یک gateway داشته باشد

باید ببینیم بالاخره بسته مان به مقصد، بسته مان را به سمت کدام gateway، AS ما ارسال کنیم

حال یک روتر این اطلاعات را چگونه متوجه می شود؟

هر AS باید بداند که کدام مقصدها (زیرشبکه ها) از طریق AS های همسایه اش قابل دسترسی هستند و این اطلاعات را به تمامی روترهای درون سازمان خود بدهد، بنابراین AS ها باید به کمک همدیگر یک الگوریتم مسیریابی دیگر بنام الگوریتم مسیریابی برون AS (inter AS routing algorithm) اجرا کنند، در

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

واتع تمام AS ها این اینترنت یک پروتکل مسیریابی درون AS واحد بنام BGP4 را اجرا می کنند (و AS ها از طریق gateway هاشون با هم الگوریتم Run را BGP می کنند)

نتیجه گیری) هر روتر اطلاعات هر ۲ پروتکل مسیریابی درون AS و برون AS را دریافت می کند و بر اساس این ۲ forwarding table ها خود را update می کند.

مسیریابی درون AS : RIP ، OSPF ، Is-Is

RIP (Routing information protocol):

RIP یک پروتکل DVR است که از تعداد hop (جهش) بعنوان معیار هزینه استفاده می کند. و تعداد hop بین ۲ ایست تا تعداد زیر شبکه ها طی شده در امتداد کوتاه ترین مسیر از روتر مبدا به زیر شبکه مقصد با احتساب شمارش زیر شبکه مقصد، بجای شمارش هزینه هر لینک را ۱ می گیریم. در الگوریتم DVR هزینه ها را بین هر زوج روتر تعریف کردیم اما در RIP هزینه ها را از روتر مبدا تا زیر شبکه مقصد می گیریم.

شکل ۴ - ۳۴ توضیح داده شده

- در DVR هزینه هر چیزی می توانست باشد، اما در اینجا هزینه ها تعداد گام است.
- قطر هر AS که از الگوریتم RIP استفاده می کند نهایتا باید ۱۵ باشد.
- قسمتی از RIP در لایه App است که روی UDP اجرا می شود، (می شود گفت RIP یک پروتکل لایه App است که روی UDP اجرا می شود ولی پروتکل خاصی است که به forwarding table ها ۲ به

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

پروتکل RIP توسط پروسس بنام Routed در لایه کاربرد اجرا می شود. پروسس Routed با پروسس های Routed روترهای مجاور پیام رد و بدل می کنند.

شکل ۴-۳۹ توضیح داده شد

Routing table = RIP table =>

include both router's distance vector and the router's forwarding table.

این جدول همان شکل ۴-۳۰ است.

شکل ۴-۳۵ و ۴-۳۶ توضیح داده شد.

روترهای همسایه هر ۳۰ ثانیه یکبار جدول مسیریابی خود را با استفاده از پیام پاسخ RIP با هم مبادله می کنند، نام دیگر این پیام همان صورت زیر است.

RIP response message = RIP advertisement

نکته: RIP بیشتر در ISP های رده پایین یا شبکه های سازمانی استفاده می شود

(open shortest path first) OSPF

الگوریتمی است برای مسیریابی درون AS، که معمولا در ISP های رده بالا استفاده می شود. الگوریتم ospf در دل یک پروتکل LS است که از دایکسترا و انتشار اطلاعات به صورت پخشی استفاده می کند.

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

الگوریتم ospf بصورت زیر عمل می‌کند

یک روتر با اطلاعاتی که دارد Broad cast می‌کند تو پولتری کل AS را برای خودشان ایجاد می‌کند پس با استفاده از الگوریتم sink tree خودشان را می‌سازند (در حقیقت کوتاهترین مسیرها به تمامی زیر شبکه های موجود در AS)

- ospf هیچ سیاست از پیش تعیین شده ای برای تعیین وزن لینک ها ندارد و اینکار به عهده مسئول شبکه است.

مسئول شبکه می‌تواند هزینه لینک ها را مثلاً به صورت زیر در نظر بگیرد

تعداد گام (جهش) : وزن هم لینک ها را 1 بگیرد

عکس Bit rate : هرکس که Bit rate اش بزرگتر باشد هزینه اش کمتر می‌شود، آن وقت کوتاهترین مسیر کسی است که پهنای باندش بیشتر است

روتر هایی که از ospf استفاده می‌کنند ۲ چیز را بصورت پریودیک برای هم منتشر می‌کنند

1) اطلاعات مسیریابی خود را
2) بسته حالت لینک را: هر ۳۰ دقیقه یک بار

ospf برای انتشار این اطلاعات، پیام های IP را از طریق لایه انتقال به IP می‌دهد، که IP آنها را منتشر کند. در واقع قسمتی از ospf مثل یک پروتکل لایه انتقال با شماره پروتکل ۸۹ یا ۷۸ در IP قرار دارد.

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

ویژگی های ospf:

1) امنیت: مبادله پیام بین روترهای یک As با احراز هویت باشد. بطور پیش فرض ospf از احراز هویت استفاده نمی کند

2 مدل احراز هویت می توانیم داشته باشیم
- ساده: روترها از یک رمز استفاده می کنند و وقتی به یکدیگر پیام ارسال می کنند این رمز را برای هم بصورت آشکار ارسال می کنند
- پیشرفته: MD5:

MD5) یک کلید مخفی مشترک در روترها پیکربندی می شود، یک روتر وقتی می خواهد پیامی به روتر دیگر بفرستد، دیتایش را با کلیدش که دارد Hash می کند و دیتا و همین طور Hash شده دیتا را برای روتر مقصد ارسال می کند، روتر مقصد این پیام را می گیرد، قسمت دیتا را با کلید خودش Hash می کند و با قسمت Hash شده ای که روتر مبدا برایش ارسال کرده مقایسه می کند، اگر برابر آن Hash شده که به دست آنها رسیده بود، یعنی درست است.

2) پشتیبانی از ارسال بسته ها روی مسیرهای هم هزینه به سمت مقصد

وقتی چند مسیر به سمت مقصد دارای یک هزینه باشند، ospf اجازه می دهد تا از همه اینها استفاده شود

3) پشتیبانی از ارسال پیام ها در چند بخش در کنار پشتیبانی از ارسال پیام ها در تک بخش

4) پشتیبانی از سلسله مراتبی کردن یک As بزرگ. یک As بزرگ را می توان بصورت چندین ناحیه سلسله مراتبی پیکربندی اش کرد. هر ناحیه ospf جداگانه خودرا

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

اجرا می‌کنه.

Broadcast پیام‌های روترهای درون ناحیه i، منحصر برای روترهای درون ناحیه i است، در هر ناحیه روترهای مرزی بنام area border router وجود دارد که مسئول ارسال بسته‌های ارسالی به مقصد خارج آن ناحیه هستند. یک ناحیه هم شامل هم area border router‌ها و شاید روترهای غیر مرزی دیگر بنام ناحیه ستون فقرات داریم (backbone area) که مسئول مسیریابی ترافیک بین ناحیه‌های AS است.

BGP (Border gateway protocol)

BGP بعنوان یک پروتکل مسیریابی برون AS (inter protocol) به AS اجازه می‌دهد تا:

۱) اطلاعات دسترسی به زیرشبکه‌ها را از همسایه‌های مجاورش بیاموزد
۲) این اطلاعات را به تمامی مسیریاب‌های داخلی AS منتشر کند
۳) براساس این اطلاعات و همین طور سیاست AS، روترهای مناسب به زیرشبکه‌ها را مشخص کند

* BGP اجازه می‌دهد هر زیرشبکه وجود و حضورش را به بقیه روترهای اینترنت اعلام و منتشر کند، و BGP این اطلاع را به تمام روترهای همه AS‌ها اینترنت و همین طور اینکه چطور این AS

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

ها می توانند بسته ها را به As مذکور برسانند، می رسانند

- در BGp هر ۲ روتر که می خواهند اطلاعات مسیریابی را با هم مبادله کنند، این اطلاعات را روی یک اتصال Tcp منطقی بنیه پایا و از طریق پورت ۱۷۹ مبادله می کنند. زوج روترها لزوما فیزیکی بهم متصل نیستند

شکل ۴-۴۰ توضیح داده شد

اتصال های Tcp بنیه پایا بین چه کسانی برقرار می شود؟

۱) به ازای هر لینکی که ۲ روتر را در دو As مختلف مستقیما بهم وصل کرد، یک اتصال BGp Tcp بنیه پایا وجود دارد

۲) بین روترهای داخل یک As می توانند اتصالات BGp Tcp وجود داشته باشند

- به روترهای ۲ سر یک اتصال BGp Tcp، BGp peer می گویند
- به مجموعه این اتصال و پیام های BGP ای که روی آن اتصال مبادله می شوند نشست BGP می گویند
- نشست بین دو As مختلف برقرار شده باشد external BGp session (eBGP)
- " " در داخل یک As " " " " internal " (iBGP)

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

- BGP کار می‌کند تا هر AS و تمام روترهای آن AS بفهمد کدام زیرشبکه‌ها از طریق کدام یک از AS‌ها همسایه قابل دسترسی است، دو AS مجاور از طریق پشت BGP بین خود فهرست زیرشبکه‌هایی که هر یک به آنها دسترسی دارند (مستقیم یا غیرمستقیم) را برای هم ارسال می‌کنند، سپس این gateway router هر یک در forwarding table خود یادداشت می‌کنند که چه زیرشبکه‌هایی، با چه آدرس‌هایی از طریق چه AS ای (گام بعدی) قابل دسترسی است حال هر یک از دو gateway router این اطلاعات را از طریق پشت‌های BGP به همه روترهای AS خود ارسال می‌کنند، و این روترها در forwarding table خود یادداشت می‌کنند که چه زیرشبکه‌هایی، با چه آدرس‌هایی از طریق چه AS ای قابل دسترسی هستند

* در BGP زیرشبکه‌ها به صورت پیشوندهای CIDR به روترها و دروازه یا غیره دروازه معرفی می‌شوند، پس هر پیشوند یک یا چند شبکه را مشخص می‌کند

به عنوان مثال فرض کنید 4 زیرشبکه زیر به AS2 متصل هستند

A)	138.16.64/24	138.16.01000000	01000000
B)	138.16.65/24	" " "	01000001
C)	" " 66/ "	" " "	01000010
D)	" " 67/ "	" " "	01000011

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

این ۴ پیشوند را می‌توان در یک پیشوند 138.16.64/22 تجمیع کرد و سپس این پیشوند را به وسیله BGP به AS1 آگهی کرد.

- حال اگر A و B و C در AS2 باشند و D در AS3 باشد. AS2 همچنان می‌تواند 138.16.64/22 را به AS1 آگهی دهد، AS3 نیز می‌تواند پیشوند tight تر 138.16.67/24 را به AS1 آگهی دهد.

چون روترها از قاعده انطباق طولانی ترین مسیر استفاده می‌کنند، مشکلی پیش نمی‌آید

- هر سیستم خودگردان با یک ID منحصر به فرد به نام ASN (autonomous system number) شناخته می‌شود

BGP ۲ مشخصه مهم دارد: ۱) As-path ۲) Next-hop

۱) As-path & یک پیام آگهی (یک پیشوند) می‌خواهد در شبکه حرکت کند، تا همه روتر ها در اینترنت بداند x وجود دارد. این پیام از As مبدا شروع می‌کند و بر ان رسیدن به هر مسیر یابی را طی می‌کند. حال وقتی یک پیشوند می‌خواهد از یک As عبور کند، آن As شماره ASN خود را به مشخصه As-path این پیام Advertisment اضافه می‌کند. در واقع در پیام Advertisment، path را می‌نویسیم و در path لیست As هایی است که پیام از آنها عبور کرده.

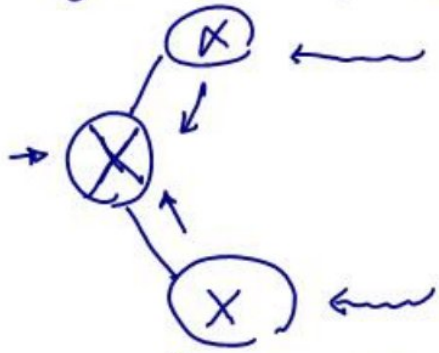
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

کاربردهای As-path:

۱) جلوگیری از تشکیل حلقه (جلوگیری از ارسال بسته محدود توسط یک gateway): اگر پیام آگهی بعضی به gateway ای برسد که ID خودش را درون لیست ببیند، پیام را دور می‌اندازد

۲) برای پیدا کردن مسیرهای جایگزین برای رسیدن به AS زیرشبکه و انتخاب بهترین آنها.



Next-hope: مشخص می‌کند که interface و Next hope کدام است

As-path شروع می‌کند (آدرس IP پورت متصل به gateway دورترین AS بعدی) و هر Next hope به روترها کمک می‌کند تا جداول هدایت خود را بهترین پیکربندی کنند

انتخاب مسیر در BGP:

اگر اطلاعات بیش از یک مسیر به یک مقصد (پیشوند) به یک روتر برسد، آن‌گاه BGP از روتر به ترتیب کارهای زیر را انجام می‌دهد تا فقط یک مسیر باقی بماند:

۱) اولویت تعیین شده توسط local preference value که توسط مدیر AS مشخص می‌شود.

۱ ۲ ۳ ۴ ۵

۱ ۴ ۴

مسیرهای دارای اولویت پایین حذف می‌شوند. حال اگر یک مسیر با اولویت بالا باقی مانده بود که کار تمام است ولی اگر چند مسیر

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

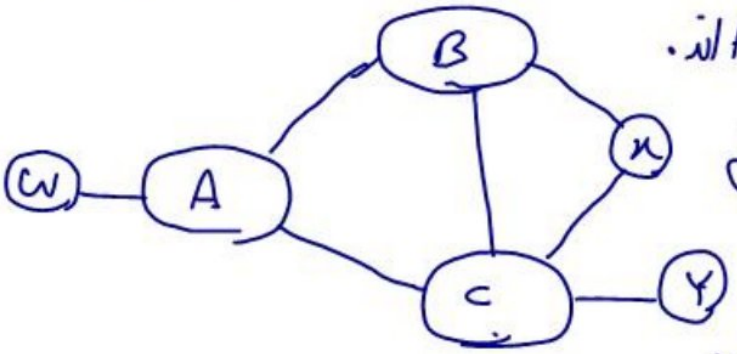
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

با اولویت باقی مانده بود به گام دوم انتخاب مسیر می رویم

۲) از مسیرهای هم اولویت باقیمانده، مسیرهایی که کوتاهترین As-path انتخاب می شود، برای این مرحله از الگوریتم DV استفاده می شود و هر گام یک As در نظر گرفته می شود

۳) از مسیرهای باقیمانده، مسیری که ما را سریعتر از As ای که روش هستیم خارج می کند انتخاب می کنیم

یعنی مسیری را انتخاب کنیم که gateway تری کمتری دارد، یعنی مسیر دارای نزدیکترین روتر Next hop انتخاب می شود. به این فرآیند مسیریابی سیب زمینی داغ می گویند



- همه ارادی که در این شکل هستند As اند.

A, B, C و Isp هستند و W و X و Y سازمان هایی خصوصی هستند به As هایی که بسته هایی که وارد آنها می شود قرار نیست از آنها عبور کنند و به یک As دیگر برسد، یعنی در واقع مقصدهایی شون آن As است

stub می گویند. X و Y و W هستند.

تمام ترافیکی که وارد یک شبکه انتهایی stub Network می شود، باید مقصدهایی آن بسته ها همان شبکه باشد و تمام ترافیکی که از یک شبکه انتهایی خارج می شود باید از همان شبکه منشا گرفته شود

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

X یک multi home - stub است، چون از دو تا Isp سرویس می گیرد.

وقتی می گیم X یک stub است یعنی تمام ترافیکی که از شش خارج می شه باید، X منشاش باشه.

بنابراین باید کاری کنیم که X ترافیک بین B و C را هدایت نکند. چون درست نیست که ترافیک از Isp1 وارد شرکت خصوصی X بشود و بعد از شرکت X وارد Isp2 بشود و بعد از آنجا برود به B.

X این وضعیت را نمی پسندد.

* B زیر شبکه های X را تبلیغ می کند.

C هم همین طور B و A را تبلیغ می کند

۲ غیر از خودش AS دیگری را به C تبلیغ نمی کند

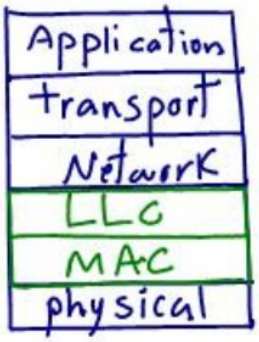
X نمی خواهد نقش واسط را داشته باشد، برای اینکار کافی است X به همسایه های خودش بگوید که هیچ مسیری به هیچ مقصد دیگری به جز خودش ندارد. در واقع X باید جلوی فروارد کردن اینکه روترها بخواهند از خودشون تبلیغات را عبور بدهند را بگیرد

بعبارت دیگر با اینکه X از وجود یک مسیر برای رسیدن به D (مسیر D,C,X) اطلاع دارد (C این اطلاعات را قبلا بهش داده) ولی این مسیر را به B آگهی نمی کند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

فصل Data link layer



LLC : logical link control
- مجموعه دوکار کنترل جریان و کنترل خطا را انجام می دهد

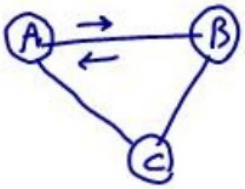
MAC (media access control)

صورت مسئله: ما خیلی از مواقع با این امر مواجه هستیم که یک محیط (کانال) فیزیکی برای انتقال داده ها داریم ولی به جای اینکه یک نفر بخواهد در این کانال دیتایش را ارسال کند چندین نفر می‌خواهند ارسال کنند، حال مسئله می‌شود اشتراک گذاری منابع کانال بین یوزرها، منابع کانال می‌تواند در حوزه زمان یا فرکانس یا کد باشد

نکته: MAC در جاهایی مطرح می‌شود که یوزرها از یک رسانه مشترک استفاده می‌کنند

مثال: بلوتوث، Bas، Token Ring، وایرلس (IEEE 802.11)، wimax

مثال: در شبکه زیر که لینک ها full duplex هستند بحث MAC مطرح نمی‌شود



روش های ارائه دسترسی به کانال (روش های تقسیم منابع بین کاربرها)

۱- روش های استاتیک
۲- " دینامیک

روش استاتیک: منابع کانال بصورت استاتیک بین یوزرها تقسیم می‌شود بصورت TDM یا FDM یا ...

نکته ۱- اگر از روش های استاتیک استفاده کنیم دیگر تصادم اصلا رخ نمی‌دهد

" ۲- در جایی خوب است که کاربرهایی که کانال بینشون share شده از منابعی که در اختیارشون قرار گرفته همه در همه استفاده را بکنند (همه

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

@konkurcomputer
www.konkurcomputer.ir

نکته ۳- اگر کاربرها همیشه دیتا ارسال نداشته باشند این روش موثر نیست، ترافیکی که توسط سیستم‌های کامپیوتری تولید می‌شوند این خاصیت را دارند و اغلب تولید کنندگان ترافیک کامپیوتری $\frac{Peak}{RMS}$ ترافیک شان بسیار بالاست ← متوسط ترافیک

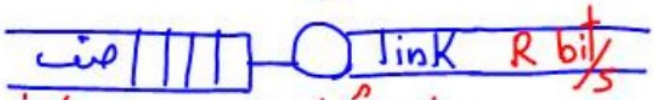
نکته ۴- در نتیجه مؤثر بودن یا نبودن روش‌های استاتیک تا حد بسیار زیادی به ماهیت تولید ترافیک کاربرها بستگی دارد

تخصیص پویا

دسترسی کاربرها به کانال بصورت پویا تعیین (انجام) می‌شود و از قبل مشخص نمی‌کنیم که چه کسی در چه زمانی نوبت اش خواهد بود ولی یک الگوریتم ارائه می‌دهیم که روی هم Run & Device شود و بر اساس آن الگوریتم تعیین می‌شود که چه کسی به کانال دسترسی خواهد داشت

نکته) از منابع بصورت بهینه استفاده می‌شود

سرویس دهنده



M فریم در ثانیه روی خط قرار داده می‌شود

λ فریم در ثانیه وارد صف می‌شود

متوسط تاخیری که فریم ها در چنین صفی مشاهده می‌کنند

$$T = \frac{1}{\mu - \lambda}$$

سوال: n کاربر داریم که همگی می‌خواهند دیتاشون را روی لینک با پهنای باند (share media) حال فرض کنید نرخ ارسال هر کاربر برابر $\frac{\lambda total}{n}$ باشد و میانگین طول بسته L bit باشد حال معلومیت متوسط زمان تاخیر صف و هم چنین میانگین زمان ارسال یک بسته روی لینک در ۲ حالت استاتیک و دینامیک

Dynamic(1

$$\text{میانگین نرخ سرویس دادن} = \frac{1}{\text{میانگین زمان سرویس دادن}}$$

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

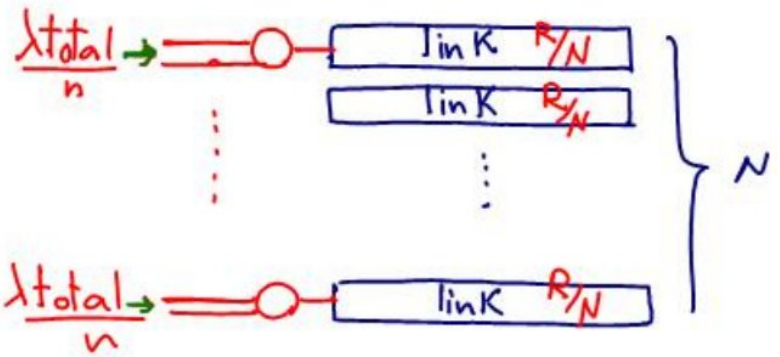
میانگین زمان ارسال یک بسته $= d(trans) = \frac{L_{(mean)}}{R} \Rightarrow \mu = \frac{1}{\frac{L}{R}} = \frac{R}{L}$

در تخصیص پویا کل پهنا باند بین کاربرها share می‌شود

میانگین تاخیر صف $= D(queue\text{-}Dynamic) = \frac{1}{\frac{R}{L} - n \times \frac{\lambda_{total}}{n}} = \frac{1}{\frac{R}{L} - \lambda_{total}}$

استاتیک: پهنا باند را بین هم share می‌کنیم و پهنا باند را بین کاربران تقسیم می‌کنیم

- there will be N channel with a capacity of R/N bits/s for each
- " " " " " streams " an average rate of $\frac{\lambda_{total}}{n}$



* با آمدن رسوس‌ها کانال را بین n تا تقسیم کردیم

میانگین زمان ارسال یک بسته $= \frac{L}{R/N} \Rightarrow \mu = \frac{R}{NL}$

میانگین تاخیر هر صف $D(each\ queue\text{-}static) = \frac{1}{\frac{R}{NL} - \frac{\lambda_{total}}{N}} = \frac{N}{\frac{R}{L} - \lambda_{total}}$

$D(each\ queue\text{-}static) = N \times D(queue\text{-}Dynamic)$

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com

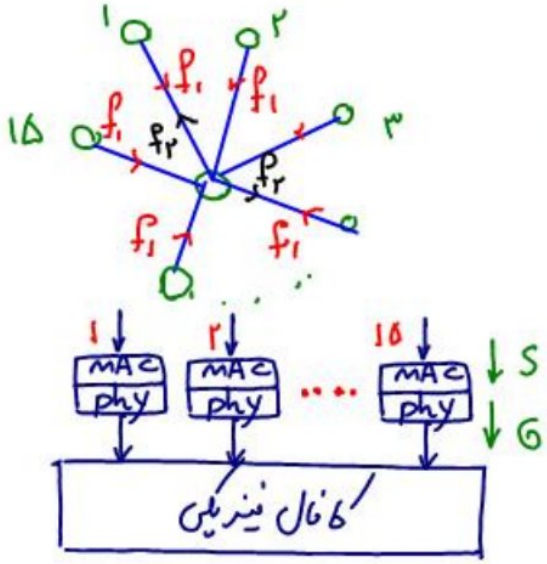
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

نتیجه: اگر نرخ ترافیک وارد شده به صف بزرگ مان CBR باشد این دو تحلیل با هم فرقی نخواهند داشت (زیرا نرخ ورود ترافیک به هرکدام از صف ها کوچکتر هم ثابت می شود) اما در مواقعی که $\frac{Peak}{RMS}$ خیلی زیاد باشد اختصاص دادن منابع کانال بصورت دینامیک خیلی بهتر از استاتیک است

میانگین زمان ارسال بسته در دینامیک $\times N$ = میانگین زمان ارسال یک بسته در استاتیک

ALOHA:

ایده اصلی ALOHA این است که کاربرهای ما هر موقعی که یک فریمی برای ارسال دارند، ارسال کنند، حال اگر دو یا تعداد بیشتری کاربر فریم هایشان با هم تصادم کنند، نودهایی که تشخیص می دهند تصادم برایشان رخ داده است یک زمان رندمی صبر می کنند و سپس مجددا ارسال می کنند



* تعداد فریم هایی که phy رو کانال میگذارد (G) از تعداد فریم هایی که MAC به phy میدهد بیشتر است زیرا re-trans داریم

* اگر لود کانال کم باشد یعنی از S ترافیک خیلی کمی تردد بشود در نتیجه تصادم خیلی کم خواهیم داشت و در نتیجه $S = G$

* S↑ در نتیجه collision↑ در نتیجه re-trans↑ در نتیجه $G > S$

در نهایت می خواهیم ببینیم که چقدر از S فریمی که به MAC داده ایم بصورت موفق ارسال شده

احتمال موفقیت آمیز بودن $\times$ همه باری که رو کانال قرار گرفته = باری که بصورت موفق از کانال عبور کرده

عبور فریم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDF Annotator.com
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
شبکه های کامپیوتری
رامین رضوی
@konkurcomputer
www.konkurcomputer.ir
MSc-PhD Computer-IT

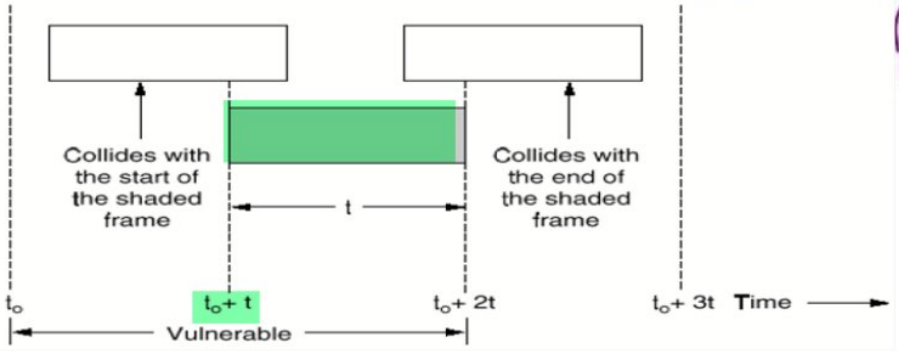
$S = G \times P_0$

اگر تصادم نداشته باشیم یعنی $P_0 = 1$ آن گاه $S = G$

بررسی احتمال collision نداشتن :

می خواهیم ببینیم یک فریم که توسط یک کاربر از N کاربر که تولید می شود در چه صورتی سالم به مقصد می رسد ؟ در صورتی که تمامی station ها انگیر در مدت زمان $2t$ (از t_0 تا t_0+2t) هیچی روی کانال نفرستند

احتمال تصادف نداشتن این فریم برابر است با احتمال خالی بودن کانال به اندازه $2t$ (2 برابر زمان ارسال یک فریم)



اگر یک فرآیند توزیع پواسن داشته باشد با متوسط G ، یعنی این است که احتمال رخ دادن K رخداد در یک بازه زمانی مشخص برابر $P[K]$ است ، درنتیجه احتمال رخ ندادن هیچ رخدادی $P[0]$ ، یک رخداد $P[1]$ و ...

$$P[K] = \frac{G^K e^{-G}}{K!}$$

↳ احتمال تولید K فریم در بازه زمانی t

$P[0] = e^{-G}$ احتمال اینکه هیچ فریمی توسط هیچ station آن در بازه زمانی t تولید نشود

ولنرد زمان = زمان ارسال یک فریم $= \frac{L}{R} = t$

G = متوسط تعداد بسته ای که در ولنرد زمان (t) روی کانال گذاشته می شود توسط همه ایستگاه ها

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDF Annotator.com
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
شبکه های کامپیوتری
رامین رضوی
@konkurcomputer
www.konkurcomputer.ir

میگیم متوسط تعداد فریم هایی که در بازه زمانی ۲ تولید میشوند G باشد آن گاه
" " " " " " " " " " ۲G است

Aloha در

درنتیجه: فرایند پواسن با متوسط ۲G داریم که میخواهیم در بازه زمانی ۲ هیچ کس فریمی تولید نکنه

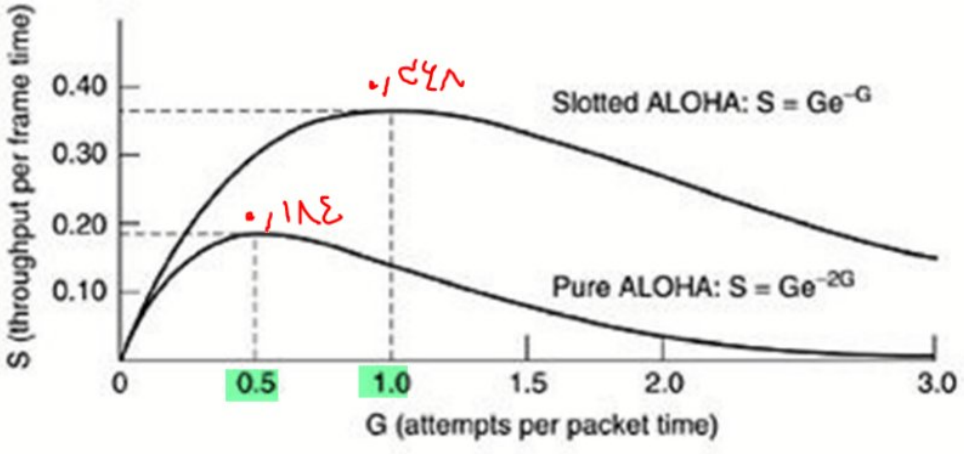
$$P[K] = \frac{(2G)^K e^{-2G}}{K!} \Rightarrow P[0] = \frac{(2G)^0 \times e^{-2G}}{0!} = e^{-2G}$$

$P[K]$: احتمال تولید K فریم در بازه زمانی ۲

احتمال تصادم ندادشتن یک فریم

$$\text{ALOHA efficiency} = S = G \times e^{-2G}$$

ما ۱۰۰ تا فریم ارسال میکنیم ولی مثلا با احتمال ۱/۵ این ۴ درست میرسند، بنابراین ۲۰ بسته در نهایت سالم عبور کرده



جمع بندی: یک الگوریتم MAC ارائه دادیم که متابع کانال را بصورت پویا بین ما تخصیص داد ولی با این الگوریتم حداکثر ۱۸ درصد از ظرفیت کانال ما را بطور متوسط میتوانیم استفاده کنیم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

slotted ALoHA

هر station ای هر زمانی که خواست نتواند ارسال کند و فقط سر یک زمان های خاصی حق داشته باشد که ارسال کند

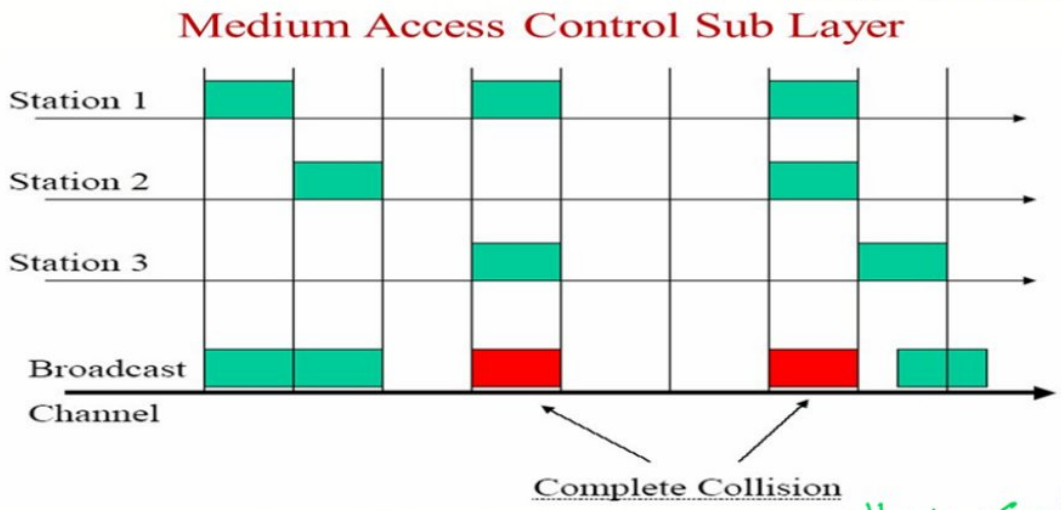


Fig : collisions in Slotted ALOHA

K تعداد کل فریم هایی ارسالی در یک slot به کانال مشترک است

$$P[K] = \frac{G^K e^{-G}}{K!}$$ ← احتمال تولید K فریم در بازه زمانی t

$$P[0] = e^{-G}$$ ← احتمال اینکه هیچ فریمی توسط هیچ station ای در بازه زمانی t تولید نشود

$$\text{slotted ALOHA efficiency} = S = G \times e^{-G}$$

با این تغییر توانستیم تصادم ها را کاهش دهیم و بنابراین efficiency دو برابر شد

$$P_k = e^{-G}(1 - e^{-G})^{k-1}$$

یعنی به این احتمال یک slot خالی است. پس در واقع این نشان میدهد که چه درصدی از slot ها در این سیستم خالی است

Expected number of transmissions E per carriage will be

$$E = \sum_{k=1}^{\infty} kP_k = \sum_{k=1}^{\infty} ke^{-G}(1 - e^{-G})^{k-1} = e^{G}$$

اگر تعداد slot های کل را داشته باشیم می توانیم آن را در این احتمال ضرب کنیم و تعداد اسلات های خالی را در کل زمان محاسبه کنیم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com

G: میانگین نرخ ارسال همه ایستگاه‌ها روی هم رفته در بازه زمانی $\frac{L}{R}$ است.

نکته مهم: اگر n تا ایستگاه داشته باشیم و هر ایستگاه با نرخ $\frac{frame}{s}$ λ ارسال کند و طول میانگین فریم‌ها L بایت و نرخ ارسال روی کانال مشترک R بایت بایت باشد G برابر خواهد بود با:

فرض $\frac{L}{R} = 1$

چند فریم در 1 ثانیه روی کانال گذاشته می‌شود $= n\lambda \frac{frame}{s} \Rightarrow G = n\lambda \times \frac{L}{R}$

چند بسته ارسال می‌کنیم	زمان
$n\lambda$	1s
$G = n\lambda \times \frac{L}{R}$ ؟	$\frac{L}{R}$ s

	احتمال موفقیت	S یا U	بازه آسیب‌پذیری	G(Umax)	(U یا S) max
ALoha	e^{-2G}	$G \times e^{-2G}$	$\frac{2L}{R}$	۰/۵	۰/۱۸۴
slow Alow	e^{-G}	$G \times e^{-G}$	$\frac{L}{R}$	۱	۰/۳۶۸

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

carrier sense multiple Access protocol (CSMA)

الگوریتم هایی هستند که بعنوان CSMA شناخته می شوند، ایده این الگوریتم ها این است که سخت افزار ها بتوانند وجود یا عدم وجود سیگنال دیگری را در یک مدیا مشترک تشخیص بدهد هر station مستقلا تشخیص دهد که آیا فرد دیگری دارد از کانال استفاده می کند یا خیر

نکته) این سرویس ان است که لایه phy می تواند ارائه دهد

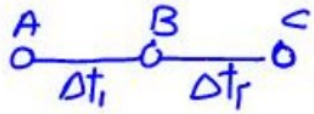
۲) این ویژگی می تواند جلو بسیاری از تصادم ها را بگیرد

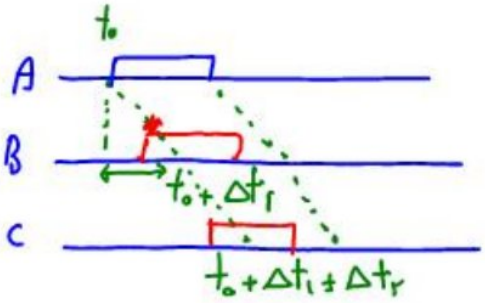
نسخه های CSMA :

۱- 1-persistent OR persistent : لایه شبکه یک فریم را به MAC میدهد حال لایه MAC کانال را بررسی می کند، اگر کانال اشغال باشد، بصورت پیوسته کانال را sense می کند تا کانال خالی شود و به محض اینکه خالی شد فریم را ارسال می کند، اما اگر دید کانال خالی است فریم را ارسال می کند سپس چک می کند که آیا تصادفی رخ داده یا نه اگر تصادف ان رخ نداده باشد می رود ابتدا فلوچارت اما اگر تصادف رخ داده باشد، بسته را بطور کامل ارسال می کند و بعد برمی گردد و یک زمان رندم صبر می کند و بعد دوباره شروع می کند به sense کانال و سپس ادامه ماجرا

۲ حالت برای تصادم قابل تصور است : ۱- چند نفر که دارند به کانال گوش میدهند و کانال شغول است بعد از آزاد شدن همگی با هم ارسال می کنند

۲- ما تاخیر بین نودها را در نظر نگرفتیم



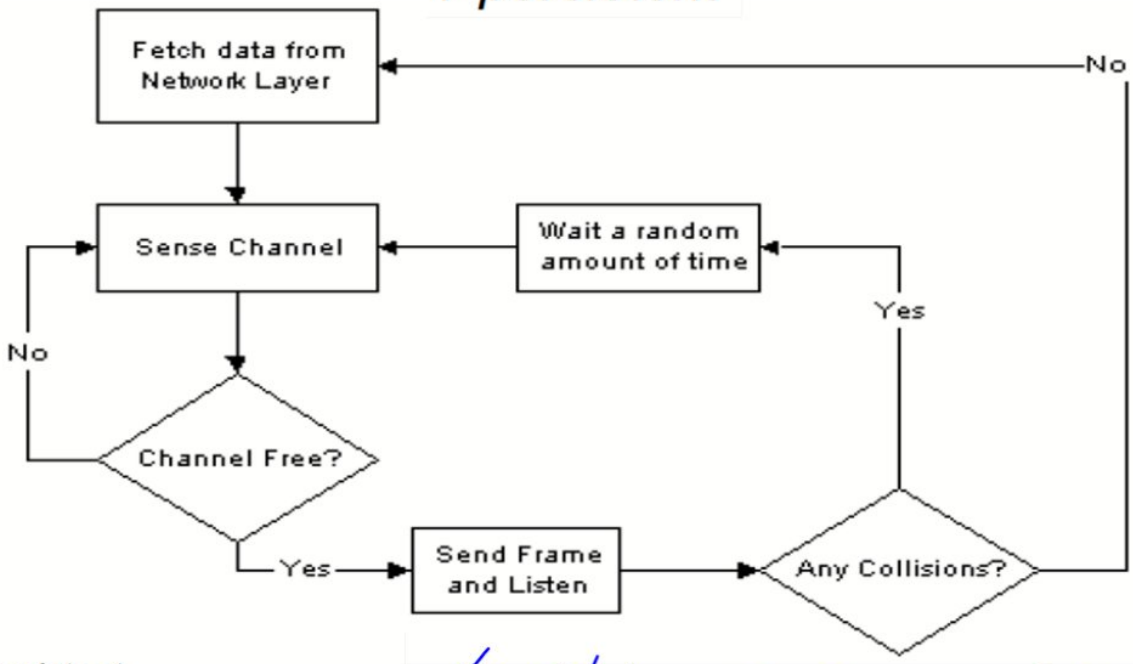


نکته - در 1-persistent وقتی ۲ نفر به کانال گوش می کنند و هر ۲ کانال را مشغول می بینند، یک گارانتی تصادم خواهیم داشت

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

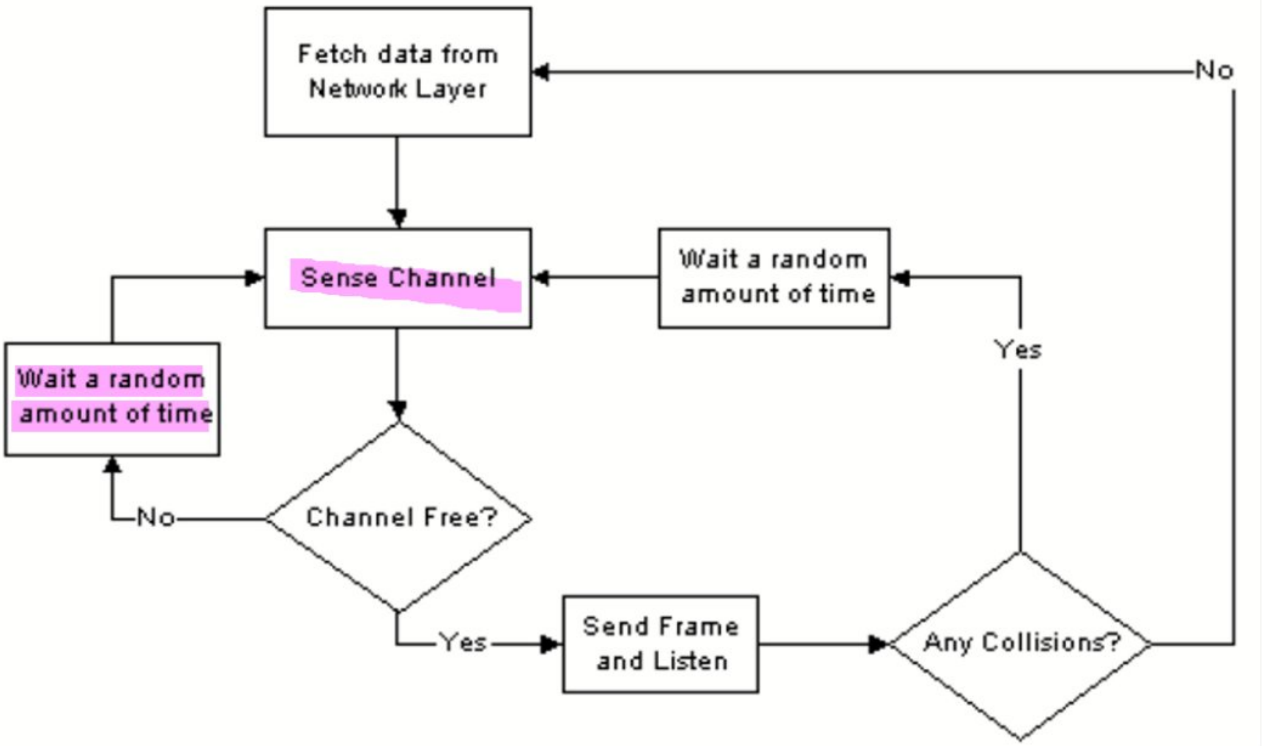
Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir
شبکه های کامپیوتری
رامین رضوی

1-persistent



- *Non-persistent*:
  - Sense channel; if idle, transmit
    If not idle, wait a random period before sensing the channel
  - Better utilisation, however, longer delays

اگر کانال آزاد نباشد همون‌جا وا نمی‌ایستیم و دائما کانال را چک کنیم، یک زمان رندم صبر می‌کنیم و بعد دوباره کانال را sense می‌کنیم.
تصادم در این روش کمتر از 1-persistent هست ولی Delay در ارسال اتفاق می‌افتد



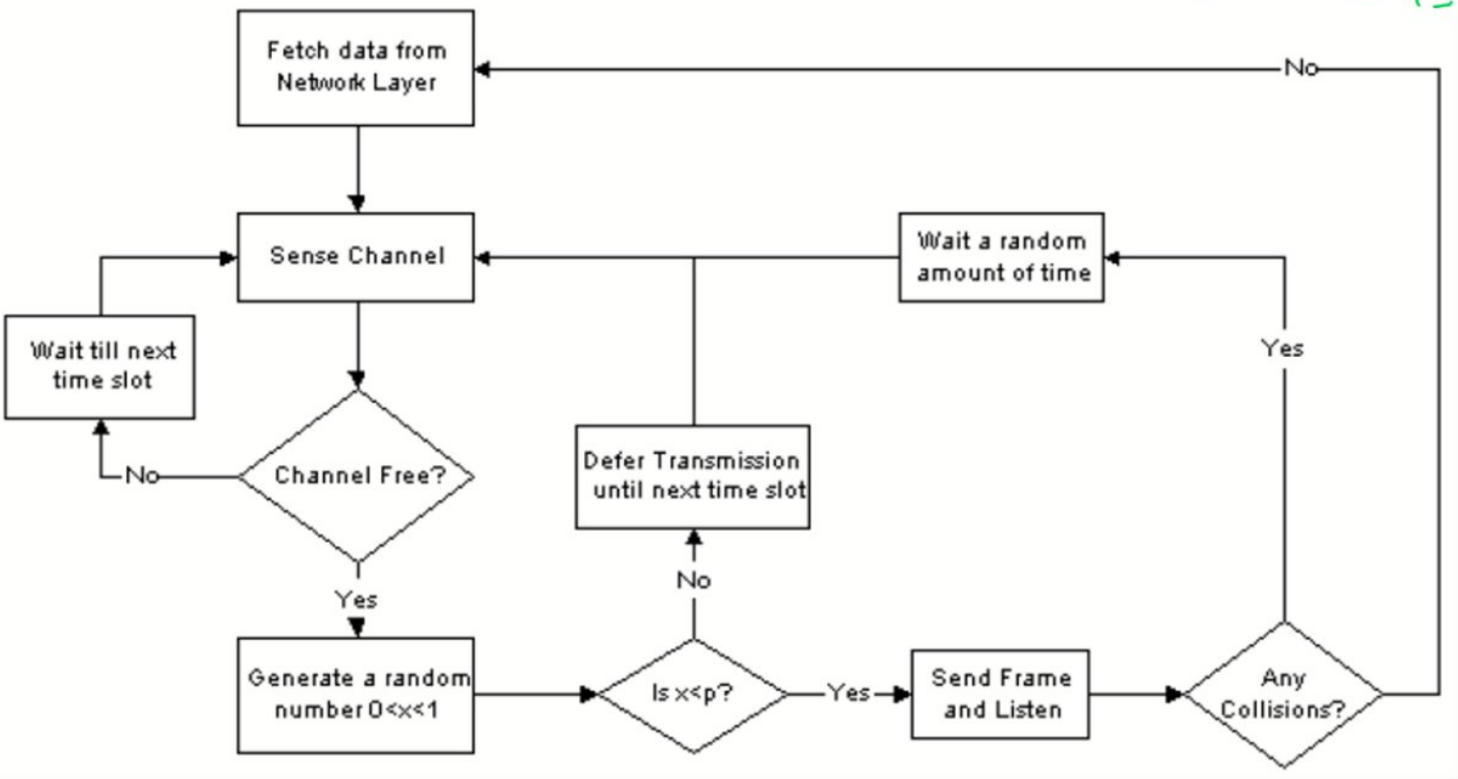
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDF-Annotator.com

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

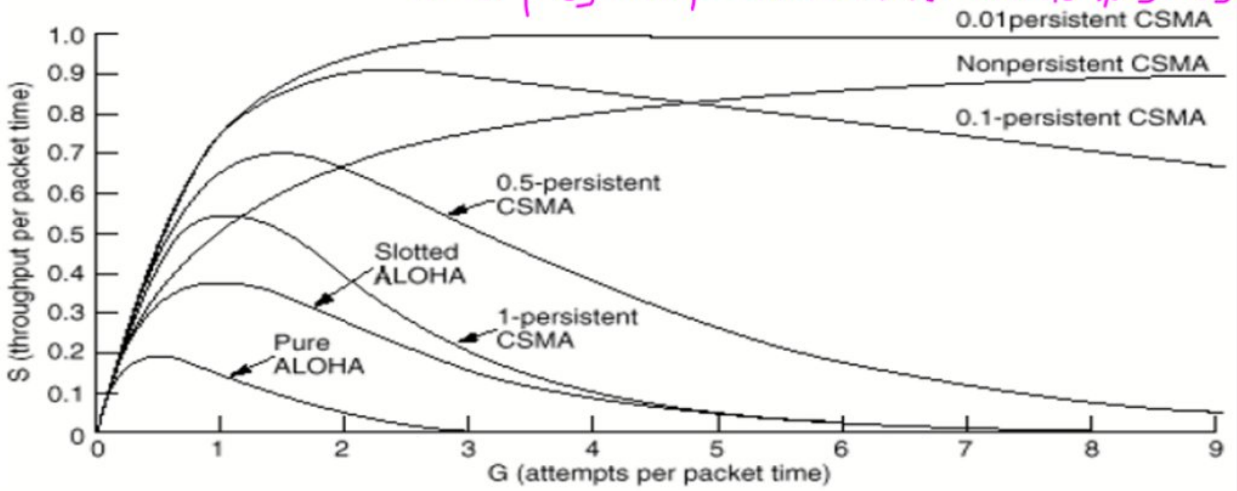
- ***P-persistent:***
  - Sense channel, if idle, transmit with probability p, defer With probability 1-p to the next slot.
  - If next slot idle repeat the same algorithm
  - If busy the first time, wait till next time slot and try again

پس از اینکه کانال را خالی دید یک عدد رندم بین ۰ و ۱ تولید می‌کنه و حالا اگر اون عدد رندم از p کمتر باشه ارسال می‌کنه
این روشش در واقع داره خودش بیشتری را برای یک فرستنده ایجاد می‌کنه که هر وقت کانال را خالی دید الزاما فریم اش را ارسال نکنه



Throughput of ALOHA and CSMA

یعنی از هر ۱۰۰ دفعه‌ای که کانال را خالی می‌بینند یک بارش و ارسال می‌کنه و ۹۹ دفعه ارسال نمی‌کنه ، در واقع داره خیلی تایفید ایجاد می‌شود ولی تصادف هم داره خیلی کم می‌شه



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

Scanned with CamScanner

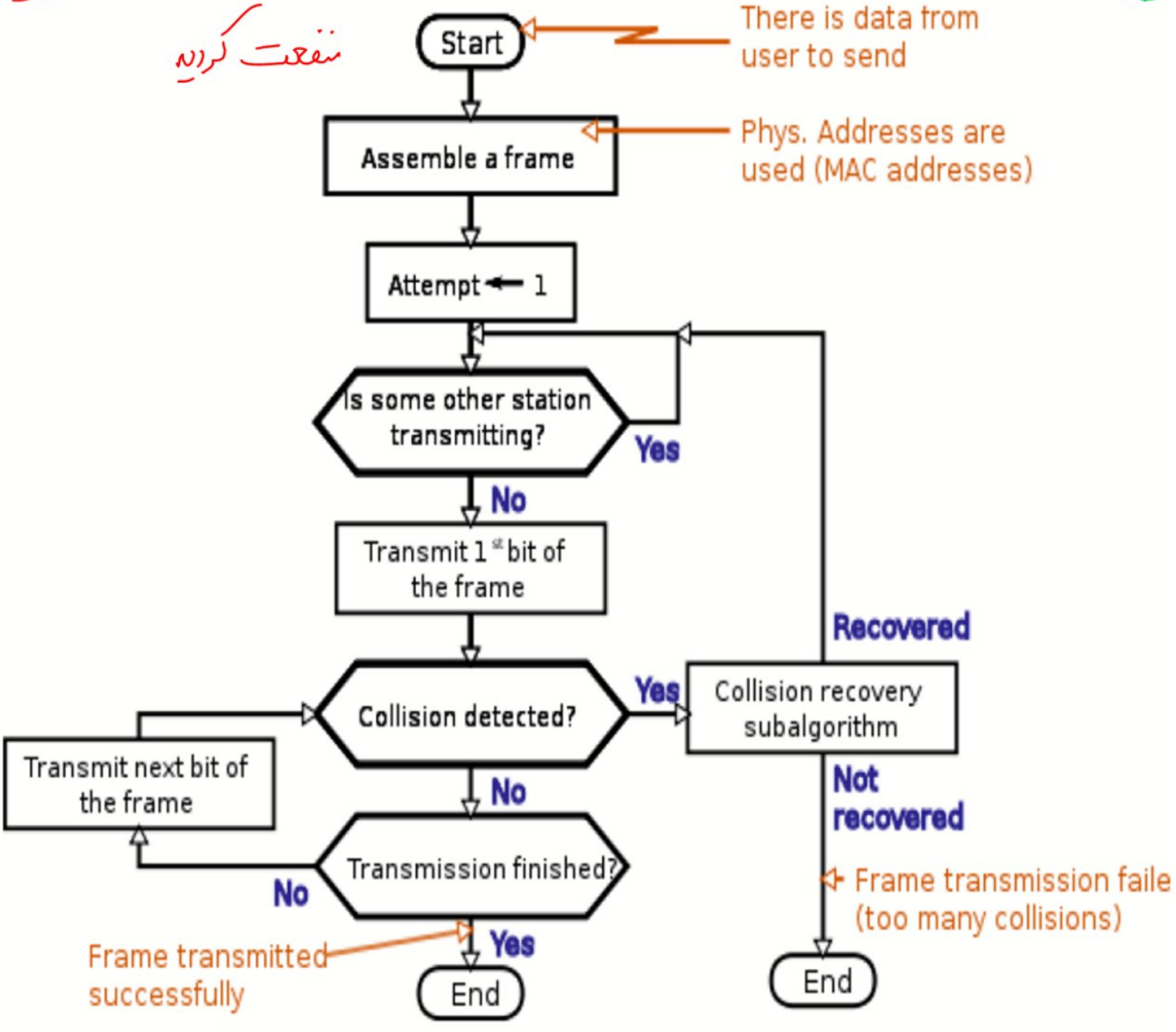
Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com

CSMA with Collision Detection

- Idea: *stop directly after detecting collision and wait for a random period*

هر نودی موقعی که فریم را ارسال می‌کند کماکان به کانال گوش می‌کند، حال اگر در حین ارسال متوجه تصادم شد، بقیه فریم آن را ارسال نمی‌کند

* هر وقت جلو ضرر را بگیرید منفعت کردید

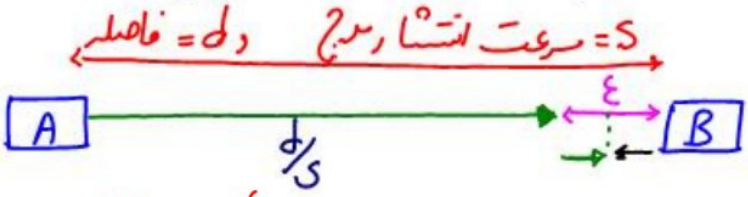


Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

قانون: یک فرستنده تا زمانی که در حال ارسال یک بسته است می‌تواند به کانال گوش کند و فقط در طی این زمان است که اگر متوجه حضور سیگنال دیگری شود متوجه تصادم می‌شود (اکی)

الگوریتم‌هایی که براساس CD هستند اگر بخواهند خوب کار کنند باید شبکه تاخیر انتشار را در نظر بگیرند



فرض کنید A و B می‌خواهند برای هم داده ارسال کنند (مدیا مشترک (شلوغ) Bus در اترنت)

اگر ε لحظه قبل از اینکه دیتا A به B برسد، B نیز شروع به ارسال کند

B کی متوجه تصادم می‌شود؟ $\frac{\varepsilon}{2}$ پس از تصادم

ε " " اینکه بسته را ارسال کرده

A " " " ؟ $\frac{\varepsilon}{2} - d/s$ پس از تصادم = d/s پس از ارسال بسته اش

$\varepsilon - 2d/s$ " " اینکه بسته را A ارسال کرده = $2d/s$ پس از ارسال

حداکثر بازه زمانی کشف تصادم از لحظه ارسال = $2\,d/s = RTT$
$\max\{\varepsilon, 2d/s\}$

شرط تشخیص تصادم توسط فرستنده

فرستنده A تا وقتی ارسال بسته اش به طول L تمام نشود به خط گوش می‌کند، که $\frac{L}{R}$ طول می‌کشد تا یک بسته روی خط گذاشته شود که در همین مدت زمان به خط گوش می‌کند و بعد از این گوش نمی‌کند بنابراین اگر $\frac{L}{R} \geq RTT$ باشد اگر تصادم رخ دهد می‌فهمد

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
Telegram Channel: @ konkurcomputer [WWW.KONKURCOMPUTER.IR]

۲۹۸

تمرین تالیفی: فرض کنید در یک کانال ماهواره‌ای با نرخ ارسال ۱۰۰Kbps از پروتکل ALOHA استفاده شده است. اگر اندازه فریم‌های ۱۰۰۰ بیت باشد، حداکثر نرخ گذردهی (Throughput) در این سیستم برحسب فریم در ثانیه تقریباً برابر است با:

۱) ۱۸/۴ فریم در ثانیه ۲) ۵۰ فریم در ثانیه

۳) ۱۰۰ فریم در ثانیه ۴) ۳۶/۸ فریم در ثانیه

فرض کن تصادم نداریم

حداکثر تعداد فریمی که در ثانیه می‌توانیم ارسال کنیم $= \frac{100 \times 10^3}{1000} = 100$ frame/s

اگرمن به نحو احسنت از شبکه بتوانم استفاده کنم، یعنی Full ارسال کنم ۱۰۰ فریم در ثانیه می‌توانم ارسال کنم، اما اگر در Aloha حداکثر گذردهی ۰٫۱۸۴ است پس داریم:

۱۰۰ × ۰٫۱۸۴ = ۱۸٫۴

۲۹۹

آی تی ۸۳: کدام‌یک از استانداردهای زیر در مورد پروتکل برای شبکه‌های محلی بی‌سیم است؟

۱) IEEE۸۰۲.۱۱ ۲) IEEE۸۰۲.۱۵ ۳) IEEE۸۰۲.۳ ۴) IEEE۸۰۲.۱۶

وایرلس (wireless man) اترنت بلوتوث وای فای

۳۰۰

آی تی ۸۳: در پروتکل دسترسی به رسانه CSMA/CD اگر طول کانال ۲۵۰۰ متر، سرعت انتشار ۱×۱۰^۸ متر در ثانیه و نرخ ارسال داده ۱۰۰ مگابیت در ثانیه باشد، حداقل اندازه فریم‌ها چقدر است؟

۱) ۳۲ بایت ۲) ۶۴ بایت ۳) ۲۵۶ بایت ۴) ۶۲۵ بایت

$\frac{L}{R} > ۲ \times \frac{D}{S} \Rightarrow L > ۲ \times \frac{۲۵۰۰ \text{m} \times ۱۰۰ \text{Mb/s}}{۱۰۰ \text{m/s}} \Rightarrow L > ۵۰۰۰ \text{ bit}$

$L > \frac{۵۰۰۰}{۸} = ۶۲۵ \text{ Byte}$

۲۰۱

آی تی ۸۵: در توپولوژی باس با پروتکل CSMA/CD فرض کنید طول کانال ۲۵۰۰ متر و نرخ ارسال ۱۰۰ مگابیت در ثانیه باشد. در بدترین حالت پس از شروع به ارسال یک فریم تا لحظه کشف تصادم، چند بیت داده خراب می‌شود (سرعت انتشار امواج در سیم ۲۰۰ هزار کیلومتر در ثانیه فرض شود.)

۱) ۵۰۰۰ بیت ۲) ۲۵۰۰ بیت ۳) ۱۲۵۰ بیت ۴) ۵۰۰ بیت

* یک بیت از لحظه‌ای که ارسال یک بیت را شروع می‌کند تا لحظه‌ای که متوجه تصادم می‌شود

کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیر مجاز از ویدیوها ندارد. استفاده غیر مجاز از این موارد کاملا حرام و پیگرد قانونی دارد

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
Telegram Channel: @ konkurcomputer [WWW.KONKURCOMPUTER.IR]

و بنابراین متوجه می‌شود بسته‌ای که فرستاده تا این لحظه خراب شده است حداکثر $2d_{prop}$ ($2\times\frac{D}{s}$) می‌گذرد

$$2\times\frac{D}{s}=\frac{2\times 2500}{200\times10^3\times10^3}=25\times10^{-6}\ s$$

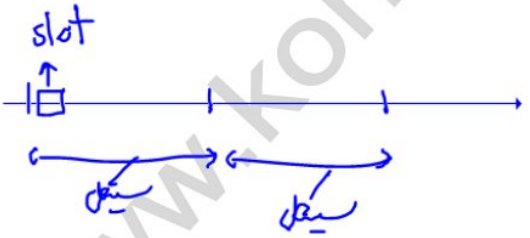
زمان	نرخ ارسال هر ثانیه
25×10^{-6}	100×10^6
?	۲۵۰۰ بیت

۳۰۲ ** آی تی ۸۶: یک روش کنترل دسترسی به رسانه می‌تواند استفاده از مالتی پلکس کردن زمان ثابت باشد. در این روش به هر ایستگاه یک Slot زمانی در هر سیکل اختصاص داده می‌شود. اگر فرض کنیم اندازه هر Slot مدت زمان لازم برای ارسال ۱۰۰ بیت به علاوه تأخیر انتشار انتها به انتها باشد و با در نظر گرفتن این‌که نرخ ارسال داده‌ها ۱۰Mbps، طول کانال ۸km و سرعت انتشار امواج 2×10^8m/s باشد، اگر تعداد ۱۰۰ ایستگاه داشته باشیم حداکثر نرخ ارسال هر ایستگاه چقدر است؟

۱) ۲۰Kbps ۲) ۲۵Kbps ۳) ۱۰۰Kbps ۴) ۵۰Kbps

در هر ثانیه این است؟ به هر ایستگاه در ۱ ثانیه چند تا slot می‌رسد

$$\text{زمان یک slot}=T(slot)=\frac{L}{R}+\frac{d}{s}=\frac{100}{10\times10^6}+\frac{8\times10^3}{2\times10^8}=5\times10^{-5}$$



تعداد کل slot هایی که در ۱ ثانیه داریم $=\frac{1}{5\times10^{-5}}=\frac{1}{5}\times10^5=20\times10^3$ slot/s

تعداد slot هایی که به هر ثانیه می‌رسد در یک ثانیه $=\frac{20\times10^3}{100}=200$

نرخ ارسال هر ثانیه $=200\times100=20$ Kb/s

هر ایستگاه در هر slot می‌تواند ۱۰۰ بیت داده مفید ارسال کند

روش ۲) زمان یک سیکل $=100\times5\times10^{-5}\ s=5\times10^{-3}\ s \Rightarrow R_{host}=\frac{100\ bit}{5\times10^{-3}\ s}=20\ Kb/s$

در هر سیکل ۱ اسلات به هر ثانیه میرسد

* چون سیستم پریودیک است، می‌توانیم نرخ ارسال ثانیه در یک سیکل را محاسبه کنیم

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
Telegram Channel: @ konkurcomputer [WWW.KONKURCOMPUTER.IR]

۳.۳

آی تی ۸۸: ده هزار ایستگاه رزرو بلیط هواپیما، برای استفاده از یک کانال واحد، به روش Slotted Aloha با هم رقابت می‌کنند. هر ایستگاه به طور متوسط ۱۸ تقاضا در هر ساعت خواهد داشت. برش‌های زمانی (time slot) ۱۰۰ میکروثانیه‌ای هستند. گذردهی در این کانال برابر است با:

خودش برش زمانی را داده، یعنی $\frac{L}{R} = ۱۰۰\mu s$

۱) $\frac{۱}{۲۰۰}e^{-\frac{۱}{۲۰۰}}$ ۲) $\frac{۱}{۲۰}e^{-\frac{۱}{۲۰}}$ ۳) $\frac{۱}{۲۰۰}e^{-\frac{۱}{۱۰۰}}$ ۴) $\frac{۱}{۲۰}e^{-\frac{۱}{۱۰}}$

$\frac{L}{R}$ نرخ ارسال هیچ‌کدام از ایستگاه‌ها روی هم در بازه $G = \frac{۱۰۰۰۰ \times ۱۲ \text{ frame} \times ۱۰^{۶} \times ۱۰^{-۶} s}{۱ \text{ h} \to ۳۶۰۰ s} = ۱/۲ \times ۱۰^{-۲}$

گذردهی $S = \gamma = G \times e^{-G} = ۱/۲۰۰ \times e^{-۱/۲۰۰}$

اگر در بازه ۱۶ تا ۱۰ با شد از ۲۰۰ رنج ۱۰۲۴ و ۰۰۰ و ۶۴ استفاده می‌کنیم

۳.۴

آی تی ۸۸: در شبکه Ethernet (استاندارد IEEE ۸۰۳/۳)، هر ایستگاه زمان back off را از رابطه $k \times t_{\text{mini slot}}$ محاسبه می‌کند. اگر ایستگاه A، k را از مجموعه {۰,۱,۲,۳} انتخاب کند. چه تعداد تصادم توسط ایستگاه A تشخیص داده شده است؟

۱) ۱ ۲) ۲ ۳) ۳ ۴)

در اترنت که به یک باس (رسانه مشترک) وصل هستند و برای استفاده از این رسانه مشترک از الگوریتم CSMA/CD استفاده می‌کنند، در اترنت بعد از تشخیص تصادمی که روی Bus اتفاق می‌افتد، برای ارسال مجدد از الگوریتم Binary exponential backoff استفاده می‌کنند

پس از تصادم اول ← یک عدد تصادفی از بازه $[۰, ۱, ۲, ۳]$ به نام K انتخاب کن و پس به مدت زمان $K \times t_{\text{mini slot}}$ صبر کن و بعد مجدد اقدام کن

$t_{\text{mini slot}}$ را اگر ندادند بطور پیش فرض آن را ۵۱۲ بیت بگیرید

۳.۵

آی تی ۸۹: ۳۰۰۰ ایستگاه برای تبادل داده‌ها از یک کانال مشترک با نرخ ارسال ۱۲ مگابیت در ثانیه به روش Pure ALOHA استفاده می‌کنند. اگر طول بسته‌ها ۱۰۰ بایت باشد و هر ایستگاه ۵ بسته در ثانیه ارسال کند، حداکثر گذردهی در این پیوند چقدر است؟

۱) $e^{-۱}$ ۲) $e^{-۲}$ ۳) $۰/۵e^{-۰/۵}$ ۴) $۰/۵e^{-۱}$

$G = n \times \lambda \times \frac{L}{R} = \frac{۳۰۰۰ \times ۵ \times ۱۰۰ \times ۸}{۱۲ \times ۱۰^{۶}} = ۱ \Rightarrow \gamma = G \times e^{-۲G} = ۱ \times e^{-۲}$

کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیر مجاز از ویدیوها ندارد. استفاده غیر مجاز از این موارد کاملا حرام و پیگرد قانونی دارد

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
Telegram Channel: @ konkurcomputer [WWW.KONKURCOMPUTER.IR]

۳۰۶

آی تی ۹۰: فرض کنید در یک کانال ماهواره‌ای با نرخ ارسال ۶۴kbps از پروتکل ALOHA استفاده شده است. اگر اندازه فریم‌ها ۱۰۰۰ بیت باشد، حداکثر نرخ گذردهی (Throughput) این سیستم برحسب فریم در ثانیه تقریباً برابر است با:

۱) ۸ فریم در ثانیه ۲) ۱۲ فریم در ثانیه ۳) ۱۰ فریم در ثانیه ۴) ۱۴ فریم در ثانیه

حداکثر مقدار فریمی که در یک ثانیه می‌توان ارسال کرد درصورتی که این بالا

$= \frac{۶۴ \times ۱۰^۳}{۱۰۰۰} = ۶۴ \text{ frame/s}$

ولی می‌دانیم در Aloha، حداکثر بهره برابر ۰٫۱۸۴ است پس داریم:

$۶۴ \times ۰٫۱۸۴ \text{ frame/s} = ۱۱٫۷۲۰$

۳۰۷

آی تی ۹۱: در شبکه اترنت، از کدام پروتکل برای کنترل دسترسی چندگانه به کانال (MAC) استفاده می‌شود؟

۱) CSMA ۲) CDMA ۳) TDMA ۴) CSMA/CD

اگر چیزی نباشد، Default است

۳۰۸

دکتری آی تی ۹۱: در یک اترنت ۱۰base T، پس از چهارمین تصادم، احتمال آن که یک گره متغیر تصادفی k=۵ را برای عقب‌نشینی انتخاب کند چیست؟ اگر k انتخاب شود، زمان عقب‌نشینی چند میکروثانیه (μs) است؟

$\text{bit time} = \frac{۱}{۱۰ \times ۱۰^۶}$

۱) $۵۱۲, \frac{۱}{۳۲}$ ۲) $۲۵۶, \frac{۱}{۳۲}$ ۳) $۲۵۶, \frac{۱}{۱۶}$ ۴) $۵۱۲, \frac{۱}{۱۶}$

در این تصادم یک بیت K اش را از بین اعداد ۰ و ۳ انتخاب می‌کند

$\text{backoff time}(\mu s) = ۵ \times ۵۱۲ \times \frac{۱}{۱۰ \times ۱۰^۶} = ۲۵۶ \times ۱۰^{-۶} = ۲۵۶ \mu s$

۳۰۹

دکتری آی تی ۹۱: یک شبکه CSMA/CD با نرخ بیت ۱Gb/s و طول کابل ۱km و بدون تقویت‌کننده را فرض کنید. اگر سرعت انتشار سیگنال در کابل ۲۰۰۰۰۰km/s باشد، آن‌گاه حداقل اندازه هر فریم باید چند بایت باشد؟

می‌خواستیم بهره ۱۰۰ Mb/s

۱) ۱۰۰ ۲) ۱۲۵ ۳) ۲۵۰ ۴) ۵۱۲

$\frac{L}{R} > RTT : L > R \times ۲ \times \frac{D}{S} \Rightarrow L > \frac{۱۰^۹ \text{ b} \times ۲ \times ۱۰^۳ \text{ m} \times \text{s}}{\text{s} \times ۲ \times ۱۰^۸ \times ۱۰^۳ \times \text{m}} = ۱۰^۴ \text{ b}$

$L > ۱۰۰۰۰ = ۱۲۵۰$

کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیر مجاز از ویدیوها ندارد. استفاده غیر مجاز از این موارد کاملا حرام و پیگرد قانونی دارد

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com

slotted Aloha

- n تا هست همگی می خواهند روی یک کانال مشترک که نرخ ارسال اش R bit/s است داده ارسال کنند، می دانیم که زمان بصورت slot، slot است و هر slot برابر $\frac{L}{R}$ است تا هست اگر فریمی برای ارسال داشته باشند فقط می توانند در اول هر slot و با احتمال p فریم شان را ارسال کنند، حال اگر تصادم رخ بدهد هر تا هست در هر کدام از slot ها بعد آن فریم را مجددا با احتمال p ارسال می کند

برای Aloha ← $p(1-p)^{2(n-1)}$ = احتمال اینکه تا هست فقط یک فریم را بتواند ارسال کند = احتمال اینکه گره مشخص i در یک slot ارسال کند و سایر گره ها ارسال نکنند

efficiency sA = احتمال اینکه یکی از گره های تا هست موفق بشود = احتمال اینکه یکی از گره ها در یک اسلات ارسال کند و سایر گره ها ارسال نکنند

برای Aloha ← $np(1-p)^{2(n-1)}$ = احتمال اینکه گره n ام موفق بشود یا ... یا احتمال اینکه گره اول موفق بشود

نکته مهم: حال اگر احتمال ارسال هر نود برابر $p=1/n$ باشد آن گاه احتمال اینکه در هر slot یکی از گره ها موفق بشود max می شود ← بنابراین efficiency ما نیز max می شود

برای Aloha: $p=\frac{1}{2n-1}$

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
Telegram Channel: @ konkurcomputer [WWW.KONKURCOMPUTER.IR]

۳۱۰

دکتری آی تی ۹۱: کدام گزینه زیر در مورد بازده حداکثر Slotted Aloha وقتی N گره که هر یک با احتمال p ارسال می‌کنند صحیح است؟

۱) $p(1-p)^{N-1}$ ۲) $(1-1/N)^{N-1}$ ۳) $p(1-p)^{2(N-1)}$ ۴) $(1-1/N)^{2(N-1)}$

efficiency SA: $n \times p \times (1-p)^{n-1}$

حداکثر وقتی رخ میده که هر ایستگاه با احتمال p_n ارسال کنه هربار

$\Rightarrow n \times 1/n \times (1-1/n)^{n-1}$

www.konkurcomputer.ir

۳۱۱ ***

دکتری آی تی ۹۱: دو گذرگاه داریم که چهار کامپیوتر به هر دوی این گذرگاه‌ها متصل هستند. کامپیوترها در حال مبادله بسته‌ها به طول یک ثانیه هستند. زمان به اسلات‌های یک ثانیه‌ای تقسیم شده است. دو ایستگاه با احتمال مساوی هر کدام از گذرگاه‌ها را انتخاب کرده و با احتمال p در شروع اسلات بعدی، ارسال خود را آغاز می‌کنند. به ازای چه مقدار p، نرخ ارسال موفق بسته‌ها ماکزیمم می‌باشد؟ نرخ ارسال موفق ماکزیمم چیست؟

۱) $p(success) = ۰/۱۸, p = \frac{۱}{۴}$ ۲) $p(success) = ۰/۳۶, p = \frac{۱}{۴}$

۳) $p(success) = ۰/۳۶, p = \frac{۱}{۲}$ ۴) $p(success) = ۰/۴۲, p = \frac{۱}{۲}$

کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیر مجاز از ویدیوها ندارد. استفاده غیر مجاز از این موارد کاملا حرام و پیگرد قانونی دارد

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
Telegram Channel: @ konkurcomputer [WWW.KONKURCOMPUTER.IR]

احتمال اینکه گره مشخص‌ی در یک slot ارسال کند و سایر گره‌ها ارسال نکنند $= p(1-p)^3$

$(u^m)' = u' \times m \times u^{m-1}$

احتمال اینکه یکی از گره‌ها موفق شود $= 4 \times p \times (1-p)^3 = 2p \times (1-p)^3$

p چه باشد که این max شود؟ باید از این برحسب p مشتق بگیریم و مساوی ۰ قرار دهیم

$2 \times (1-p)^3 - \frac{1}{2} \times 3 \times (1-p)^2 \times 2p = 0 \Rightarrow 2-p = 3p \Rightarrow p = \frac{1}{2}$

$\text{max efficiency} = 2 \times \frac{1}{2} \times (\frac{1}{2})^3 = \frac{27}{64} = 0.42$

برابر با

۴۱۲

آی تی ۹۱: فرض کنید که کل بار فریم‌های ارسال شده در سیستم Slotted ALOHA باشد. در این صورت چه درصدی از Slotهای زمانی در این سیستم خالی است.

۱) $\frac{1}{e^G}$ ۲) $\frac{1}{e^{2G}}$ ۳) $1-\frac{1}{e^G}$ ۴) $1-\frac{1}{e^{2G}}$

$e^{-G} = \frac{1}{e^G}$

www.konkurcomputer.ir

کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیر مجاز از ویدیوها ندارد. استفاده غیر مجاز از این موارد کاملا حرام و پیگرد قانونی دارد

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
Telegram Channel: @ konkurcomputer [WWW.KONKURCOMPUTER.IR]

۳۱۶) دکتری آی تی ۹۲: در یک شبکه از نوع ALOHA پنج ایستگاه وجود دارد و هر یک ۱۲ فریم در دقیقه تولید می‌کنند و زمان ارسال هر فریم به طور متوسط ۱۰۰ms است. میزبان بار و گذردهی نرمالیزه شبکه و تعداد بهینه ایستگاه‌ها چند است؟

۱) ۰/۱، ۰/۱۴، ۹ ۲) ۰/۰۸۲، ۰/۱، ۹ ۳) ۰/۱، ۰/۰۸۲، ۱۰ ۴) ۰/۱۴، ۰/۱، ۹

$G = \frac{n \times \lambda \times L}{R} = \frac{5 \times 12 \times 100 \times 10^{-3}}{(min)60} = 1/10$

$S = G \times e^{-2G} = 0.1 \times e^{-0.2} \simeq 0.082$

تعداد بهینه ایستگاه، تعدادی است که باعث شود S ماکزیمم شود، می‌دانیم که وقتی S ماکزیمم می‌شود که $G = 1/2$ باشد ← با 25 ایستگاه S ماکزیمم می‌شود

$G = \frac{n \times \lambda \times L}{R} \Rightarrow 1/2 = \frac{n \times 12 \times 100 \times 10^{-3}}{60} \Rightarrow n \simeq \frac{5 \times 10}{2} = 25$

۳۱۷) آی تی ۹۳: ۸ ایستگاه از طریق دو باس سیمی مختلف به هم متصل شده‌اند. فرض کنید که زمان ارسال هر فریم یک ثانیه طول می‌کشد و زمان نیز به اسلات‌های زمانی یک ثانیه‌ای تقسیم شده است. زمانی که یک ایستگاه فریمی برای ارسال دارد به طور تصادفی و با احتمال مساوی یکی از باس‌ها را انتخاب کرده و در زمان شروع اسلات بعدی با احتمال p ارسال می‌کند. مقدار p برای حداکثر شدن نرخ ارسال موفقیت‌آمیز چقدر است؟

۱) $\frac{1}{16}$ ۲) $\frac{1}{8}$ ۳) $\frac{1}{4}$ ۴) $\frac{1}{2}$

احتمال اینکه گره مشخصی در یک اسلات ارسال کند و سایر گره‌ها ارسال نکنند $= p/2 (1 - p/2)^7$

$(u^m)' = u' \times m \times u^{m-1}$

احتمال اینکه یکی از گره‌ها موفق بشود $= 8 \times p/2 \times (1 - p/2)^7 = 4p \times (1 - p/2)^7$

چه باید p باشد که این max بشود، باید از این برحسب p مشتق بگیریم و مساوی 0 قرار دهیم

مشتق: $4 \times (1 - p/2)^3 - 4p \times 1/2 \times (1 - p/2)^4 \times 7 = 0 \Rightarrow 1 - p/2 = 7/2\, p \Rightarrow 2 - p = 7p$

$p = 1/4$

کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیر مجاز از ویدیوها ندارد. استفاده غیر مجاز از این موارد کاملا حرام و پیگرد قانونی دارد

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
Telegram Channel: @ konkurcomputer [WWW.KONKURCOMPUTER.IR]

۲۱۵) دکتری آی تی ۹۴: در اترنت (Ethernet) برای این‌که فرستنده A از عدم برخورد بسته ارسالی خود با بسته فرستنده B مطمئن شود، ارسال بسته‌اش باید حداقل برای ..... به طول بینجامد (فرض کنید که حداکثر فاصله بین دو گره در این شبکه فاصله بین دو گره AوB باشد).

۱) فاصله زمانی بین دو گره AوB
۲) دو برابر فاصله زمانی بین دو گره AوB
۳) سه برابر فاصله زمانی بین دو گره AوB
۴) بیش از سه برابر فاصله زمانی بین دو گره AوB

۲۱۶) آی تی ۹۴: یک شبکه محلی با روش دسترسی به رسانه CSMA/CD را در نظر بگیرید. اگر طول شبکه یک کیلومتر، نرخ ارسال ۱۰۰ مگابیت بر ثانیه، سرعت انتشار ۲۰۰ متر بر میکروثانیه، و سربار هر فریم ۲۵ بایت باشد، حداقل طول فیلد داده باید چند بایت است؟

۱) ۵۰
۲) ۱۰۰
۳) ۲۲۵
۴) ۴۵۰

$\frac{L}{R} > 2 \times \frac{D}{S} \Rightarrow L > \frac{2 \times 100 \times 10^6 \times 10^3}{200 \times 10^6} = 1000\,bit \Rightarrow L > \frac{1000}{8} = 125B$

طول داده درون فریم $> 125 - 25 = 100$

۲۱۷) آی تی ۹۵: ۱۰۰۰۰ ایستگاه برای ارسال اطلاعات خود از یک کانال مشترک با روش دسترسی Slotted ALOHA استفاده می‌کنند. اگر هر ایستگاه ۱۸ ارسال در یک ساعت داشته و اندازه هر برش زمانی (time slot) ۱۰۰ میکروثانیه باشد، بار کانال برحسب تعداد ارسال در هر برش زمانی برابر است با:

۱) ۰/۰۰۵
۲) ۰/۰۱۰
۳) ۰/۰۱۵
۴) ۰/۰۲۰

$G = \frac{n \times \lambda \times L}{R} = \frac{10000 \times 18 \times 100 \times 10^{-6}}{3600\,s} = \frac{1}{200}\,\frac{f}{slot} \xrightarrow{\times 5/5} \frac{5}{1000}$

کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیر مجاز از ویدیوها ندارد. استفاده غیر مجاز از این موارد کاملا حرام و پیگرد قانونی دارد

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
Telegram Channel: @ konkurcomputer [WWW.KONKURCOMPUTER.IR]

۳۱۸ دکتری آی تی ۹۶: یک شبکه خطی اترنت به طول ۲km را در نظر بگیرید. فرض کنید سرعت انتشار موج الکترومغناطیس $۲\times۱۰^{۸}m/s$ و نرخ ارسال شبکه ۱۰Mbps است. حداقل اندازه‌ای که برای فریم لازم است تا مطمئن شویم CSMA/CD در این شبکه به درستی کار می‌کند، چند بیت است؟

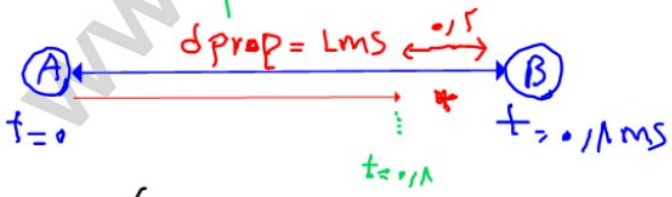
۱) ۱۰۰ ۲) ۱۵۰ ۳) ۲۰۰ ۴) ۲۵۰

$\frac{L}{R} > ۲\times D/S \Rightarrow L > \frac{۲\times۱۰\times۱۰^{۶}\times۲\times۱۰^{۳}}{۲\times۱۰^{۸}} \rightarrow ۲۰۰ bit$

۳۱۹ مهندسی کامپیوتر ۹۷: شبکه‌ای را که در آن امکان برخورد (collision) بسته‌ها وجود دارد و پروتکل CSMA/CD فعال است را در نظر بگیرید. در این شبکه زمان انتشار (propagation) بین نود A و نود B یک میلی‌ثانیه (mSec) است. در لحظه $t = ۰$ نود A بسته‌ای را با نرخ ۴ مگابیت بر ثانیه ارسال می‌کند و در لحظه t=۰/۸msec نود B بسته‌ای را با نرخ ۴ مگابیت بر ثانیه ارسال می‌کند. به ترتیب از راست به چپ حداقل اندازه بسته A چند بایت باشد که A متوجه برخورد شود و حداقل اندازه بسته B چند بایت باشد که B متوجه برخورد شود؟

۱) ۱۰۰۰-۱۰۰۰ ۲) ۱۴۰۰-۶۰۰ ۳) ۹۰۰-۱۰۰ ۴) ۶۴-۶۴

* کلا نکته کلیدی این است که هر جا است تا وقتی سیگنال تصادم بهش می‌رسه باید به ارسال داده ادامه بده



طول بسته‌ای که A می‌فرسته: $\frac{L_A}{R} > ۰/۹ms\times۲ \Rightarrow L_A > \frac{۴\times۱۰^{۶}\times۹\times۱۰^{-۴}\times۲}{۱۰\times۸} = ۹۰۰B$

و B هم: $\frac{L_B}{R} > ۰/۲ms \Rightarrow L_B > \frac{۴\times۱۰^{۶}\times۲\times۱۰^{-۳}}{۱۰\times۸} = ۱۰۰B$

کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیر مجاز از ویدیوها ندارد. استفاده غیر مجاز از این موارد کاملا حرام و پیگرد قانونی دارد

Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

شبکه های کامپیوتری

رامین رضوی

فصل کنترل:

ما دوتا چیز تو کنترل خطا داریم ⟨ (۱ تشخیص خطا (error detection
(۲ تصحیح خطا (error correction

نیاز به اتفاق نظر داریم برای هرکدام از این موارد

ما خیلی باید خطا را تصحیح کنیم، به همدوش می‌توانیم خطا را دریافت کنیم

۱) تصحیح خطا رو به جلو، تصحیح خطا پیش رو. forward error correction

می‌آییم اطلاعات اضافی به همراه دیتا به گیرنده ارسال می‌کنیم و گیرنده از روی اطلاعات اضافی خطا را تشخیص می‌دهد و می‌تواند آن را تصحیح کند مانند کدهمینگ

۲) تصحیح خطا رو به عقب، تصحیح خطا پس رو backward error correction

گیرنده از روی بیت‌های اضافه خطا را تشخیص می‌دهد و به فرستنده یا با NAK یا با ACK می‌گوید بسته را دوباره ارسال کن

همینگ:

- فاصله همینگ دو کد c_1 و c_2 برابر تعداد بیت‌های متفاوت دو کد است.

$c_1 = 10101$ $\quad D(c_1, c_2) = 4$

$\oplus\ c_2 = 11001$

$01011 \Rightarrow w(\text{حاصل}) = 4$

- وزن یک کد برابر تعداد یک‌های آن کد است

$w(c_1) = 3$ و $w(c_2) = 3$

- نکته: نحوه دوم بدست آوردن فاصله همینگ آنه: دو کد را باهم XOR می‌کنیم و بعد وزن حاصل XOR را بدست می‌آوریم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

نکته: فاصله همینگ مجموعه کدهای valid ما برای ارسال، برابر است با min فاصله همینگ میان دو به دو اعضای مجموعه.

$C_1, C_2, C_3, C_4 = \{000, 011, 101, 110\}$

$D(C_1, C_2) = 2$
$D(C_1, C_3) = 2$
$\vdots$

min اینجا را عنوان فاصله همینگ مجموعه اعلام می‌کنیم

چرا min را به دست می‌آوریم؟
چون این دو کدی که نسبت به هم min فاصله همینگ را دارند خطرناک‌ترین قسمت هستند، زیرا اگر یکی از این دو کد معتبر ارسال شود با کمترین خطا به کد معتبر دیگر تبدیل می‌شود و ما در گیرنده حتی قادر به تشخیص وقوع خطا نمی‌شویم

نکته: حداکثر تعداد خطاهای قابل تشخیص (detection) d در یک مجموعه کد که دارای فاصله همینگ D است از فرمول زیر به دست می‌آید

$d = D - 1$

نکته: حداکثر تعداد خطاهای قابل تصحیح (correction) (c) توسط گیرنده (FEC)

$c = \left\lfloor \frac{D-1}{2} \right\rfloor$ → قدرت تصحیح

- زوج parity: اگر همه بیت‌های دیتا را با هم XOR کنیم و حاصل را به دیتا اضافه کنیم و سپس ارسال کنیم، این کار را می‌گویند parity زوج (با احتساب خود parity) و فاصله همینگ parity زوج ۲ است.

$d = 2 - 1$ → ۱ بیت خطا را می‌توان تشخیص داد

* وقتی می‌گوئیم که فاصله همینگ در یک کد را به دست آورید همیشه سعی کنید مثال بزنید و عدد گذاری بکنید، مثلاً در اینجا مثالی برای داده ۲ بیتی می‌زنیم و بعد min فاصله همینگ دو به دو کدهای معتبر را به دست می‌آوریم

$c = \left\lfloor \frac{2-1}{2} \right\rfloor = 0$

	۰۰	۰۱	۱۰	۱۱
۰۰		۱	۱	۲
۰۱	۱		۲	۱
۱۰	۱	۲		۱
۱۱	۲	۱	۱	

$\Rightarrow minTotal = 2$

راه‌حستی برای کدهای خطی: min وزن کدهای معتبر

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com

منظور از کد خطی کدی است که ترکیب آن با XOR دیتا الفبای باینری یا کپی دیتا اصلی باشد و همین طور کدی با وزن و هم داشته باشیم

- وقتی در even parity می‌گوییم فاصله همینگ‌مان ۲ است، یعنی ۲ بیت خطا قابل تشخیص نیست، زیرا یک کد معتبر دوباره به یک کد معتبر تبدیل می‌شود و این بدترین اتفاقی است که در کنترل خطا می‌تواند رخ بدهد، چون گیرنده نه تنها نمی‌تواند بفهمد در کجا خطا رخ داده بلکه اصلا متوجه رخ دادن خطا نمی‌شود و داده را معتبر و درست می‌بیند

- در even parity که فضا کدها بصورت زیر خواهد بود

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

که کدهای معتبر را با رنگ سبز و کدهای نامعتبر را با رنگ قرمز مشخص کرده‌ایم.

حال متوجه می‌شویم که چرا ما می‌توانیم ۱ بیت خطا را تشخیص بدهیم ولی نمی‌توانیم تصحیحش بکنیم

- فرض کنید فرستنده که ۰۰۰ را ارسال کرده و گیرنده که ۰۰۱ را که کدی نامعتبر است دریافت کرده، حال گیرنده متوجه خطا می‌شود اما از کجا می‌خواهد بفهمد که کدی که ارسال شده ۰۰۰ بوده یا ۱۱۰ یا ۱۰۱؟

چون که نامعتبر ۰۰۱ رسیده به گیرنده سه کد معتبر با فاصله همینگ ۱ دارد، گیرنده نمی‌تواند بگوید که ۰۰۱ به کدام یک شبیه‌تر است.

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDF Annotator.com
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

(longitudinal Redundancy check) LRC - (Block checksum char) BCC

↓ طولی

که تا این کد می‌خواهیم ارسال کنیم را زیر هم می‌نویسیم، بعد XOR بیت‌های هر ستون را بدست می‌آوریم (دو روش داریم) parity ستونی انجام میدهیم.

زوج یا فرد

	P	b_6	b_5	b_4	b_3	b_2	b_1	b_0
	0	1	0	1	0	1	1	0
	1	0	1	0	0	1	0	0
	1	0	1	1	0	0	1	1
	0	1	0	0	1	0	0	1
	0	0	1	1	0	1	1	1
	0	0	1	1	1	0	1	1

فاصله همینگ در checksum به فاصله همینگ در parity است و بنابراین 2 است. چون در CS اگر 2 خطا در یک ستون رخ بدهد قابل تشخیص نیست

ماتریس را طولی یا ستونی

در روش checksum هر ستون را به صورت modul-2 جمع میزنیم، یعنی بعد از هر جمع کردن 2 را دور می‌اندازیم، این روش جمع کردن معادل همان XOR کردن است

= checksum

زوج یا فرد

نکته: checksum را همراه دیتا می‌فرستیم، بعد گیرنده نیز همین کار را انجام میدهد و checksum را بدست می‌آورد و بعد با این checksum با متناب می‌کند

نکته: قدرت تشخیص خطا این روش 1 بیت، ایشون قدرت تصحیح خطا را ندارد

$$d = D - 1 \Rightarrow D = 1 + 1 = 2$$

— روش توازن دوبعدی

علاوه بر توازن افقی، طولی یا ستونی، از بیت‌های توازن عمودی (vertical) سطری یا عرضی استفاده می‌کنیم، به بیت‌های توازن عمودی VRC (Vertical Red— check) میزنی گویند

با حیدره با 7 انجام می‌گیرد.

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com

- این روش روش هرمینگ خطایی را Detect می‌کند و این روش تا ۱ بیت را تصحیح می‌تواند درست کند

فاصله همینگ توازن دو بردار ۴ است $\rightarrow D_{min} = 4 \Rightarrow d = D - 1 \Rightarrow 3 = D - 1 \longrightarrow d = D - 1$

نکته: این که همیشه ۵ بیت خطا را تشخیص می‌دهد.

بررسی بیشتر کد توازن ۲ بعدی:

تعداد خطا	تشخیص	تصحیح	توضیحات
۱	✓	✓	
۲	✓	✗	بدترین حالت به این صورت است که هر ۲ خطا در یک سطر یا یک ستون باشند
۳	✓	گاهی	بدترین حالت به این صورت است که هر ۳ خطا به صورت مثلثی باشد. اگر خطا مثلثی نباشد به اشتباه یک بیت درست را خراب می‌کند
۴	✗	✗	بدترین حالت به این صورت است که ۴ خطا بصورت مربعی یا مستطیلی رخ بدهد
۵	✓	✗	امکان تصحیح اشتباه وجود دارد

△ △ △ ○ ✗
○ ○ ○ △ ✓
✗ ✗ ✗ ✓

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDF Annotator.com
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
@konkurcomputer
www.konkurcomputer.ir

اگر ۱ بیت خطا رخ بدهد که همینگ نه تنها تشخیص اش میدهد بلکه به درستی تصحیح اش میکند، اما اگر ۲ بیت خطا رخ بدهد و مابقی نه باشیم تشخیص میدهد خطا رخ داده ولی در تصحیح اش گند میزند

همینگ: همینگ می خواهد علاوه بر تشخیص خطا تصحیح نیز انجام دهد، همینگ به این منظور طوری ستون ها را ایجاد میکند که حداقل فاصله همینگ اش باید ۳ باشد ← وقتی فاصله همینگ دو کد همینگ ۳ باشد ۲ خطا باعث می شود گیرنده گند بزند

$$t = \left\lfloor \frac{D_{min}-1}{2} \right\rfloor \rightarrow D_{min} = 3$$

نکته: حداقل اقرونلی ۲ اگر بخواهیم یک کدی که داراش m بیت داده اصلی و ۲ بیت اقرونلی دارد یک بیت خطا را تصحیح کند چقدر می تواند باشد؟

$$\overbrace{m+2}^{n}+1 \leq 2^2$$

هرکد n بیتی که $n = m+2$ است اگر بخواهد ۱ بیت خطا را تصحیح کند

- هرکد n بیتی که بخواهد K بیت خطا را تصحیح کند، حداقل اقرونلی اش r از رابطه زیر بدست می آید

$$\text{تصحیح ۱ بیت خطا} = \binom{n}{1} + 1 \leq 2^r$$

$$\text{تصحیح ۲ بیت خطا} = \binom{n}{1} + \binom{n}{2} + 1 \leq 2^r$$

$$\text{تصحیح K بیت خطا} \rightarrow \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{K} + 1 \leq 2^r$$

داده ها با ۱۰ بیتی

۱۲۰ تا $\binom{10}{1}$ ، ۴۵ تا $\binom{10}{2}$ ، $10 + \frac{10.9}{2!} + \frac{10.9.8}{3!} + 1 \leq 2^r \Rightarrow 176 \leq 2^r$

$\min r = 8$ ← تا ۱ بیت می توانیم خطا را تصحیح کنیم

کوچکترین r ای که در این رابطه صدق کند مرتبه min اقرونلی

نکته) هرچه m نسبت به r بزرگتر باشد بهره وری بیشتر (ارزش کمتر) ان خواهیم داشت.

در ۱ بیت تصحیح

$m = 1 \rightarrow r = 2$ ، $\frac{1}{3}$ ، $n = 2$

$m = 1000 \rightarrow r = 10$ ، $\frac{1000}{1010}$ ، $n = 1010$

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

کدهای خطی: کدخطی یک داده m بیتی را گرفته (که m بیت اطلاعاتی اصلی ماست) و یک کلمه n بیتی تولید می‌کند، بنابراین $r=n-m$ بیت افزونگی مازاد تشخیص و تصحیح خطاست. و به این کد تولید شده می‌گوییم کدخطی رده (n,m) (n: کل، m: main Data)

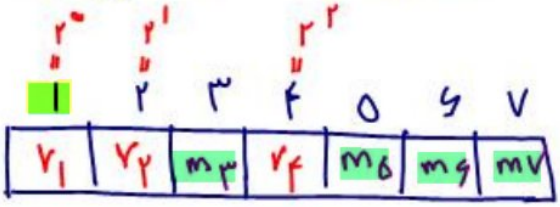
- همینگ برای ۴ بیت داده اصلی از ۳ بیت افزونگی استفاده می‌کند. بنابراین همینگ یک کدخطی از رده (۷,۴) محسوب می‌شود. فرمت کلی همه کدهای همینگ: $(2^r-1, 2^r-1-r)$

$r=2 \rightarrow (3,1)$

- افزونگی‌های کدهای خطی بصورت xor (even parity) از روی داده‌های اصلی ساخته می‌شود

سوال - کدخطی (۷,۴) را با روش همینگ درست کنید.

۷ بیت می‌داریم از شماره‌های ۱ تا ۷. بیت‌هایی که توانی از ۲ هستند، افزونگی هستند و بقیه دیتای اصلی هستند



r_i: با استفاده از xor و m_i به طریق خاص بدست می‌آیند. بیا و اندیس‌های m را بصورت توانی از ۲ بنویس، حال m_i در محاسبه r_i هایی با عدد‌های ۱ بدست آمده استفاده می‌شود.

$m_3 = 1+2$

$m_5 = 1+4$

$m_6 = 2+4$

$m_7 = 1+2+4$

$r_1 = m_3 \oplus m_5 \oplus m_7$

$r_2 = m_3 \oplus m_6 \oplus m_7$

$r_4 = m_5 \oplus m_6 \oplus m_7$

۱۰۰۰ ۱۰۱ → ۰۱۰۰ ۱۰۱

توجه) کد همینگ گفت ۱ بیت خطا رخ بدهد درست کار می‌کند

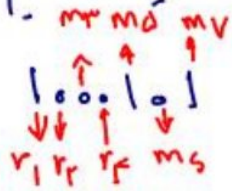
اگر r_1 و r_2 دچار خطا بشوند آن وقت ما اشتباهاً فکر می‌کنیم که m_3 خراب شده درصورتیکه r_1 و r_2 خراب شده‌اند

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDF Annotator.com
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

سوال - کدی دریافت کردیم در مقصد، اگر از همینگ استفاده کرده باشیم آیا کدی که دریافت کردیم درست است؟ اگر درست نیست، درست اش چیست؟



$r_1 = m_3 \oplus m_5 \oplus m_7 \rightarrow 1 \stackrel{?}{=} 0 \oplus 1 \oplus 1 \rightarrow X$: غلط

$r_2 = m_3 \oplus m_6 \oplus m_7 \rightarrow 0 = 0 \oplus 0 \oplus 1 \rightarrow$ غلط

$r_4 = m_5 \oplus m_6 \oplus m_7 \rightarrow 0 = 1 \oplus 0 \oplus 1 \rightarrow$ ✓

$r_4\ r_2\ r_1 = 0\ 1\ 1 = 3$

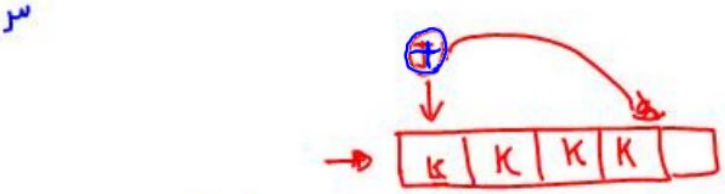
خطا در بیت سوم

تعاقب افتاده

روش ۲: اندیس بیت هایی که ۱ هستند را با هم XOR کنیم

در اینصورت عدد بدست آمده اندیس بیت خطادار را نشان می دهد.

۱ = ۰ ۰ ۱
۵ = ۱ ۰ ۱
۷ = ۱ ۱ ۱ ⊕
۰ ۱ ۱ → سوم خطادار



K=۲

۰۰ ۰۰ ۰۰ ۰۰ ... = ۰
۰۱ ۰۱ ۰۱ ۰۱ = ۱ → D
۱۰ ۱۰ ۱۰ ۱۰ = ۵
۱۱ ۱۱ ۱۱ ۱۱ = ۸

* اگر که غیر همینگ خطی بدهند و فاصله همینگ را ندانند باید بصورت زیر عمل کنیم

۱) همه کدهای معتبر را تولید می کنیم
۲) وزن همه کدها را بدست می آوریم
۳) min وزن غیر ۰ ها برابر فاصله همینگ است.

CRC: (cycle Redundancy check) یا کدهای چند جمله ای (polynomial code)

- در این روش هر عدد دودویی متناظر با چند جمله ای در نظر گرفته می شود
- مثلا چند جمله متناظر با عدد ۱۱۰۰۱ برابر است با: $x^4 + x + 1$

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.

- در این روش فرستنده و گیرنده بر سر یک چند جمله‌ای مولد به اسم G(x) توافق می‌کنند (generator polynomial)

G(x) یک چند جمله‌ای است که با 1 شروع می‌شود و با 1 ختم می‌شود و معمولاً

فرض کنید تعداد بیت‌های G(x) برابر n باشد

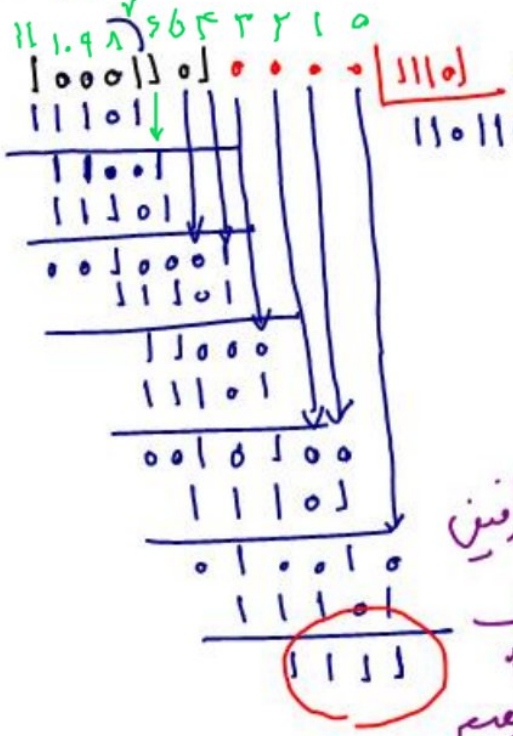
روال توزیع کلمه ارسال شده در فرستنده CRC:

۱) ابتدا n-1 بیت 0 به سمت راست داده اصلی اضافه می‌کنیم، انگار D را n-1 بیت به سمت چپ شیفت می‌دهیم

۲) عدد بدست آمده را بر G(X) تقسیم modulo 2 می‌کنیم (در این نوع تقسیم به مقدار اعداد کاری نداریم و به تعداد ارقام کار داریم و اعداد را از هم تفریق نمی‌کنیم و XOR می‌کنیم)

۳) باقیمانده تقسیم که باید حداکثر n-1 بیت باشد را به جای همان n-1 بیت 0 ای که سمت راست داده گذاشته بودیم قرار می‌دهیم و کل را فرستنده آن را ارسال می‌کند بدست می‌آید (در واقع داریم باقیمانده n-1 بیتی بدست آمده را با مقسوم XOR می‌کنیم)

مثال: می‌خواهیم داده 1000 1101 را با روش CRC و مولد



ارسال کنیم $G(x) = x^4+x^3+x^2+1$ ← درجه G(x) برابر مقدار بیت‌های آن است

4 3 2 1 0
G(x) = 1 1 1 0 1

این داده را فرستنده ارسال می‌کند → 1000 1101 1111

گیرنده این داده را دریافت می‌کند و این را بر G(x) مورد توافق آنها تقسیم می‌کند، حال اگر باقیمانده 0 شود خطا نداریم ولی در غیر اینصورت خطا داریم. ولی با این کار نمی‌توانیم مکان خطاها را مشخص کنیم

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com

تقسیم بالا را با استفاده از چند جمله‌ای G نیز می‌توانستیم انجام بدهیم ؛

$x^{11} + x^{7} + x^{6} + x^{4}$ | $x^4+x^3+x^2+1$

$x^{11} + x^{10} + x^{9} + x^{7}$ | $x^7+x^6+x^4+x^3+x+1$

$x^{10} + x^{9} + x^{7} + x^{4}$

$x^{10} + x^{9} + x^{8} + x^{6}$

$x^{8} + x^{4}$

$x^{8} + x^{7} + x^{6} + x^{4}$

$x^{7} + x^{4}$

$x^{7} + x^{6} + x^{5} + x^{3}$

$x^{6} + x^{3}$

$x^{6} + x^{4} + x^{3} + x$

$x^{4} + x$

$x^{4} + x^{3} + x^{2} + 1$

$x^3 + x^2 + x + 1 \Rightarrow$ 1111

عبارت 4 بی که با هم برابر هستند با هم خط می‌خورند و سایر عبارات باقی می‌ماند، این خاصیت XOR است

7 6 5 4 3 2 1 0

1 1 0 1 1 0 1 1

تا جایی تقسیم را ادامه می‌دهیم که دیگر نتوان به x^4 تقسیم کرد، یعنی بزرگترین درجه‌ای که می‌ماند از x^4 کوچکتر بشود

* تقسیم D بر G ممکن است در ابتدا کار به ما باقیمانده ≠ 0 بدهد، حالا با این کار که وقتی r را به D اضافه می‌آوریم می‌آوردیم و این را با D، XOR می‌کنیم، در واقع داریم از D مقدار باقیمانده را کم می‌کنیم، بدان همین در مقصد باید تقسیم داده ارسالی بر G(x) باقی مانده آن 0 بدهد)

نکته) در روش CRC نقطه خطاهایی قابل تشخیص نیست که E(x) مضربی از G(x) باشد مثلاً E(x) = G(x) باشد که این بدان معناست که از سمت راست داده ارسالی نقطه همان بیت‌ها با متناظر با آن‌ها G(x) خراب بشوند و بیت‌های متناظر با 0 های G(x) هم خراب نشوند

مثلاً در مثال بالا که $G(x) = x^4+x^3+x^2+1$ یا 11111 و داده ارسالی برابر 1000110 است D(x) = 1000110 0000 بیت

1000110000010 | 11101

$E(x) = x^2 \times G(x) = x^6+x^5+x^4+x^2$ ← 1 1 1 0 1 0 0

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com

نکات CRC

۱- سمت راست $G(X)$ (بیت LSB اش) همیشه ۱ است

۲- کد CRC تعداد بیت های خطا و همین طور محل وقوع خطا را مشخص نمی کند، فقط بخ دادن (وقوع) خطا را تشخیص می دهد.

۳- تمامی خطاهای تک بیتی قابل شناسایی است

۴- اگر $G(X)$ بر $x+1$ بخش پذیر باشد تمام خطاهای فرد قابل شناسایی است

۵- اگر $G(X)$، حداقل ۳ از جمله داشته باشد تمام ۱-۲ بیتی قابل تشخیص است

(تا یک در $G(X)$ وجود داشته باشد)

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDF Annotator.com
سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به
استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز
از این فیلم کاملا حرام و پیگرد قانونی دارد.
MSc-PhD Computer-IT
@konkurcomputer
www.konkurcomputer.ir

گیرنده با ارسال NAK یا ACK مدارش میگوید مجدد برای من ارسال کن

پیاده سازی سازی CRC با shift Register

ما میخواهیم باقیمانده ای که باید به سمت راست داده مان اضافه کنیم را بدست آوریم، تا آن را به سمت راست داده مان اضافه کنیم و آن را ارسال کنیم، برای این منظور با توجه به G(x) سخت افزار (شیفت رجیستر) زیر را می سازیم، و داده مان را به همراه بیت های ۰ ای که سمت راست اش چسبانده ایم را از با ارزش ترین بیت اش از سمت راست مدارش که ساختیم یک بیت یک بیت وارد می کنیم در نهایت داخل رجیستر ها موجود در سخت افزار باقیمانده تقسیم Data ما به G(x) وجود دارد

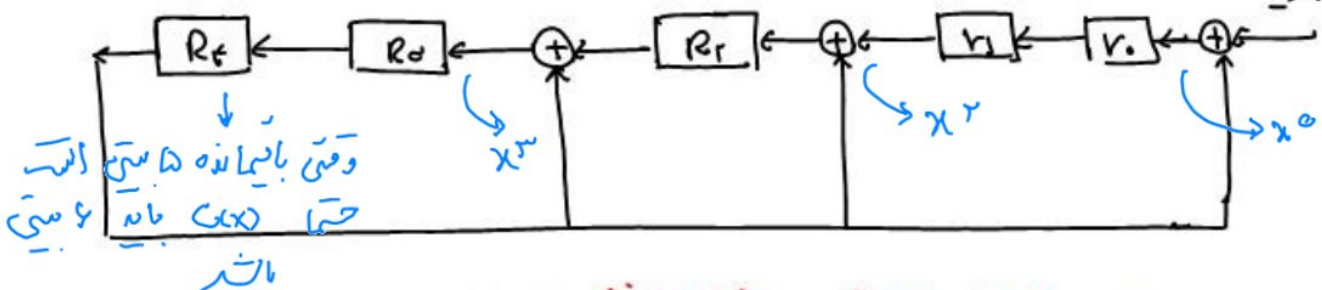
بنابراین اگر G(x) ما ۶ رقمی است، باید شیفت رجیستری بسازیم ۵ رقمی.

باقیمانده ۵ رقمی است

مثال: برای $G(x)=1011101$ شیفت رجیستر طراحی کنید ← $G(x)=x^5+x^4+x^3+1$

رقم آخر را در نظر نگیرید

* به جز جمله آخر به زبان هر ۱ در عدد دودویی G(x)، یک XOR قبل از بیت متناظر با آن قرار میگیرد.



- فعال / سه استیبل ۵۳. محتوا و احتمال خواب شدن یا نشدن بسته در مسیر.

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.

احتمال از دست رفتن (یا نرسیدن) یک بسته در مسیر

در یک مسیر شامل n لینک متوالی، اگر احتمال مفقود شدن بسته در هر لینک برابر p باشد و این احتمال بر روی هر لینک مستقل از دیگر لینک ها باشد، آن گاه داریم:

احتمال دریافت موفقیت آمیز بسته توسط گیرنده : $(1-p)^n$

احتمال مفقود شدن بسته در طول مسیر = سالم رسیدن بسته − کل = $1-(1-p)^n$

* حال اگر یک بسته در مسیر رسیدن به دست مشتری مفقود شود فرستنده دوباره آن را ارسال می کند، حال برای آنکه یک بسته با موفقیت به مشتری برسد

① هر بسته بطور میانگین $\frac{1}{(1-p)^n}$ بار توسط فرستنده ارسال می شود

② " " " " " " " " " " " " " " " " " " مجدد می شود $\frac{1}{(1-p)^n} - 1$

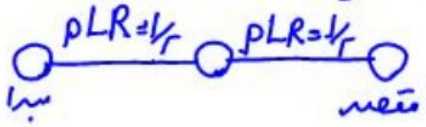
یا راه دوری از آمار : در یک آزمایش برنولی داریم : میانگین تعداد ارسال = $\frac{1}{\text{احتمال موفقیت}}$

آزمایش برنولی : اگر هر بار انجام آزمایش مستقل از نتایج بدست آمده از دفعات قبلی فقط و فقط به یکی از دو پیشامد موفقیت یا شکست با احتمال ثابت p و $p-1$ منجر شود

* در این حالت پدیده ای که احتمال موفقیت اش p است را باید $\frac{1}{p}$ بار تکرار کنیم تا به اولین موفقیت برسیم

مثال) چند بار یک سکه را پرتاب کنیم تا به اولین شیر برسد؟ ممکن است خوش شانس باشیم و بار اول شیر بیاید یا ممکن است بد شانس باشیم و هزار بار بیندازیم و خط بیاید حالا سوال این است که بطور میانگین چند بار باید بیندازیم تا اولین شیر بیاید

سوال- با توجه به شکل زیر PLR کل را بدست آورید؟



سایت کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیرمجاز از ویدئوها ندارند. استفاده غیرمجاز از این فیلم کاملا حرام و پیگرد قانونی دارد.
Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
Telegram Channel: @ konkurcomputer [WWW.KONKURCOMPUTER.IR]

۳۲۰

آی تی ۸۶: برای بالا بردن اطمینان در انتقال داده‌ها، به جای یک بیت توازن از کدی استفاده می‌کنیم که یک بیت توازن برای بیت‌های فرد و یک بیت توازن برای بیت‌های زوج دارد. فاصله همینگ این کد چقدر است؟

۱) ۲ ۲) ۳ ۳) ۴ ۴) ۵

۳۲۱

مهندسی کامپیوتر ۸۶: در یک ماتریس دو بعدی با بیت‌های توازن دو بعدی با ۴ سطر و ۳ ستون، با فرض وقوع هم‌زمان چهار خطا، احتمال کشف نشدن خطا چقدر است؟

۱) $\frac{۲}{۵۵}$ ۲) $\frac{۴}{۵۵}$ ۳) $\frac{۳}{۱۳۲}$ ۴) $\frac{۹}{۱۳۲}$

۳۲۲

آی تی ۸۸: یک روش کدگذاری قدیمی در ارسال رادیویی استفاده از کدهای با تعداد بیت "۱" برابر است. در کد ۲ از ۵، فقط ۲ بیت از کلمه کد ۵ بیتی "۱" می‌باشد. در صورتی که از کدهای ۲ از ۵ استفاده شود. احتمال عدم تشخیص خطا در گیرنده برابر کدام است؟

۱) $\frac{۷}{۳۲}$ ۲) $\frac{۸}{۳۲}$ ۳) $\frac{۹}{۳۲}$ ۴) $\frac{۱۰}{۳۲}$

www.konkurcomputer.ir

کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیر مجاز از ویدیوها ندارد. استفاده غیر مجاز از این موارد کاملا حرام و پیگرد قانونی دارد

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
Telegram Channel: @ konkurcomputer [WWW.KONKURCOMPUTER.IR]

۳۲۳ تست تالیفی: کدی ایجاد کردیم که برای ما عمل تشخیص و تصحیح خطا را انجام دهد، این کد برای هر K بیت داده، یک کلمه کد به طول ۳K بیت تولید می‌کند. کلمه کد شده ارسالی به این صورت تولید می‌شود که K بیت اول اطلاعات، K بیت بعدی تکرار اطلاعات و K بیت بعدی نیز تکرار اطلاعات است. حداقل فاصله همینگ در این کلمه کد چقدر است؟

۱) ۲ ۲) ۳ ۳) ۴ ۴) ۵

روش ۱) که خطی است

K=۲

۰۰ ۰۰ ۰۰	۰
۰۱ ۰۱ ۰۱	۳
۱۰ ۱۰ ۱۰	۳
۱۱ ۱۱ ۱۱	۶

$\Rightarrow min = ۳$

روش ۲)

۰۰ ۰۰ ۰۰
۰۱ ۰۱ ۰۱] D=۳

روش ۳) گیرنده چطور خطا را تشخیص میدهد؟ گیرنده سه تا که K بیتی می‌گیرد، اگر این سه تا شبیه هم بود می‌گوید خطایی نداریم ولی اگر یکی از اینها فرق داشت خطا را detect میکند

فرستنده: ۰۰ ۰۰ ۰۰ → گیرنده: ۰۰ ۰۰ ۱۰۰ است خطا ✓
" : " " : ۰۰ ۰۱ ۰۱ " ۲ " ✓ ⇒ d=۲ ⇒ D=۳
" " ۰۱ ۰۱ ۰۱ (valid) " ۳ نمی‌تواند (d=D-۱)

۳۲۴ تست تالیفی: کدی ایجاد کردیم که برای ما عمل تشخیص و تصحیح خطا را انجام دهد، این کد برای هر K بیت داده، یک کلمه کد به طول ۲K+۱ بیت تولید می‌کند. کلمه کد ارسالی به این صورت تولید می‌شود که K بیت اول اطلاعات، K بیت بعدی Not اطلاعات و بیت آخر XOR، K بیت دوم است. حداقل فاصله همینگ در این کلمه کد چقدر است؟

۱) ۲ ۲) ۳ ۳) ۴ ۴) ۵

توجه کنید: این که خطی نیست و اگر از راه ۱ بروید تست را غلط می‌زنید

روش ۲)

K=۲ ⇒ ۰۰ ۱۱ ۰
۰۱ ۱۰ ۱] D=۳

روش ۳) اخطا رخ بدهد؟ هرجا رخ بدهد می‌فهمد

۱ خطا ؟ " " ۲ " } d=۲ ⇒ D=۳
۲ " ؟ " " ۳ "

قابل تشخیص نیست

K=۲
۰۰ ۱۱ ۰ →
۰۱ ۱۰ ۱
۱۰ ۰۱ ۱
۱۱ ۰۰ ۰

کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیر مجاز از ویدیوها ندارد. استفاده غیر مجاز از این موارد کاملا حرام و پیگرد قانونی دارد

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
Telegram Channel: @ konkurcomputer [WWW.KONKURCOMPUTER.IR]

۳۲۵

مهندسی کامپیوتر ۸۸: یک کد تشخیص خطا k بیت اطلاعات را به صورت زیر به ۲K+۱ بیت تبدیل می‌کند.

K بیت اول بیت‌های اطلاعات است.

K بیت دوم تکرار بیت‌های اطلاعات است.

بیت آخر XOR بیت‌های اطلاعات است.

حداقل فاصله همینگ در این کد چقدر است؟

۱) ۳ ۲) ۵ ۳) ۴ ۴) ۶

روش ۱)

K=۲ ⇒

۰	۰	۰	۰
۰	۱	۱	۳
۱	۰	۱	۳
۱	۱	۰	۴

⇒ min=۳ ⇒ D=۳

روش ۲)

K=۴

۰۰۰۰ ۰۰۰۰ ۰

۰۰۱۰ ۰۰۱۰ ۱] D=۳

۳۲۶

آی تی ۸۹: در یک کد خطی (۳، ۶) بیت‌های چک‌کننده (check bits) به صورت زیر محاسبه می‌شوند.

$b_4=b_1+b_2$

$b_5=b_1+b_3$

$b_6=b_2+b_3$

توجه) نگفته مقاومش از جمع چیست، پس بصورت پیش فرض آن را modvle-2 می‌گیریم

حداقل فاصله همینگ در این کد چقدر است؟

b_1	b_2	b_3	b_4	b_5	b_6	w
۰	۰	۰	۰	۰	۰	۰
۰	۰	۱	۰	۱	۱	۳
۰	۱	۰	۱	۰	۱	۳
۰	۱	۱	۱	۱	۰	۴
۱	۰	۰	۱	۱	۰	۳
۱	۰	۱	۱	۰	۱	۴
۱	۱	۰	۰	۱	۱	۴
۱	۱	۱	۰	۰	۰	۳

۱) ۴ ۲) ۵ ۳) ۲ ۴) ۳

کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیر مجاز از ویدیوها ندارد. استفاده غیر مجاز از این موارد کاملا حرام و پیگرد قانونی دارد

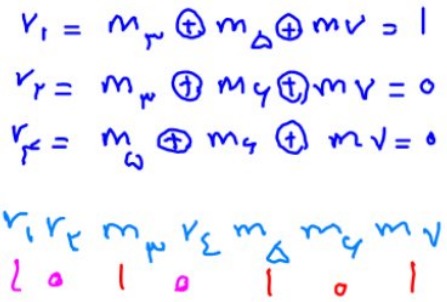
Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
Telegram Channel: @ konkurcomputer [WWW.KONKURCOMPUTER.IR]

۲۷ تی

آی تی ۸۷: می‌خواهیم با استفاده از کد همینگ پیام‌های ۴ بیتی داده را به نحوی ارسال کنیم که گیرنده بتواند هر خطای یک بیتی را تشخیص و تصحیح کند. بدین منظور تعداد بیت‌های چک‌کننده موردنیاز چقدر است؟ اگر پیام 1101<-- باشد، کد تولید شده ارسالی چیست؟

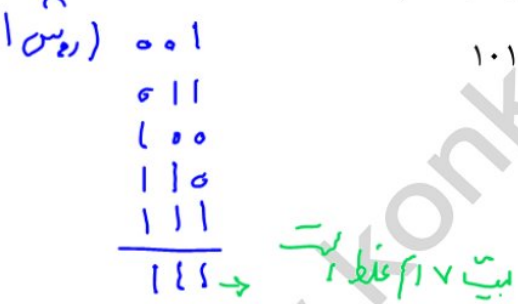
۱) ۲ بیت و ۱۰۱۰۱۰ ۲) ۲ بیت و ۱۱۰۱۰۱ ۳) ۳ بیت و ۱۰۱۰۱۰۱ ۴) ۳ بیت و ۱۱۰۱۰۱۱



۲۸ تی

آی تی ۹۵: یک کد همینگ ۷ بیتی با مقدار ۱۰۱۱۰۱۱ به گیرنده می‌رسد. مقدار صحیح این کد چیست؟

۱) ۱۰۱۱۰۰۱ ۲) ۱۰۱۱۰۱۱ ۳) ۱۰۱۱۰۱۰ ۴) ۱۰۱۱۱۱۱



۲۹ تی

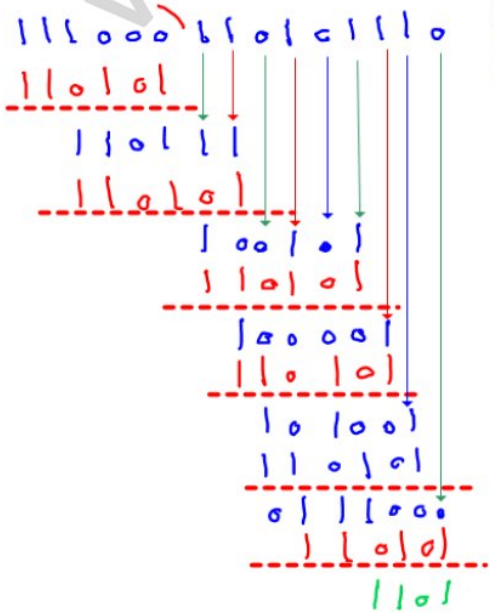
مهندسی کامپیوتر ۸۳: پیغام ۱۱۱۰۰۰۱۱۰۱۰۱۱۱۰ از طریق یک کانال دریافت شده است. هر گاه کد استفاده شده دارای ۵ بیت CRC و چند جمله‌ای مولد $g(x)=1+x^2+x^4+x^5$ باشد. کدام‌یک از موارد زیر صحیح است:

۱) خطا وجود ندارد.

۲) خطا وجود دارد و ۱ بیتی است.

۳) خطا وجود دارد و ۳ بیتی است.

۴) خطا وجود دارد ولی تعداد بیت‌های آن مشخص نیست.

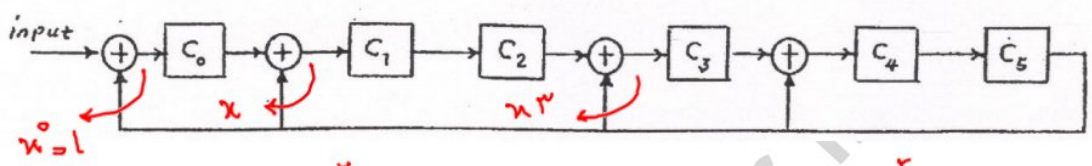


کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیر مجاز از ویدیوها ندارد. استفاده غیر مجاز از این موارد کاملا حرام و پیگرد قانونی دارد

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
Telegram Channel: @ konkurcomputer [WWW.KONKURCOMPUTER.IR]

۳۳۰ مهندسی کامپیوتر ۸۳: در یک سیستم تشخیص خطا به روش CRC از شیفت رجیستر مطابق شکل استفاده شده است. چند جمله‌ای مولد این CRC چیست؟



۱) $x^6+x^4+x^3+x+1$ ۲) x^5+x^3+x+1 ۳) $x^5+x^3+x^2+x+1$ ۴) $x^6+x^5+x^3+x+1$

۳۳۱ مهندسی کامپیوتر ۹۱: فرستنده‌ای پیام‌هایی را به کمک CRC با م ولد $G(x)=x^3+x^2+1$ کد می‌کند و پیام‌های زیر توسط گیرنده دریافت می‌شود. کدام‌یک از گزینه‌های زیر دارای خطاهای بیت است؟

۱) ۰۰۱۱۰۱۱۰ ۲) ۰۱۰۰۱۰۱۱ ۳) ۱۰۱۱۰۱۰۱ ۴) ۱۱۰۱۱۱۰۱

www.konkurcomputer.ir

کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیر مجاز از ویدیوها ندارد. استفاده غیر مجاز از این موارد کاملا حرام و پیگرد قانونی دارد

Scanned with CamScanner

Produced with a Trial Version of PDF Annotator - www.PDFAnnotator.com
Telegram Channel: @ konkurcomputer [WWW.KONKURCOMPUTER.IR]

۳۳۲

مهندسی کامپیوتر ۸۳: یک بسته داده از لایه بالاتر از لایه پیوند به ۱۰ فریم تقسیم شده است و احتمال این‌که هر یک از فریم‌ها صحیح به مقصد برسند ۸۰٪ است. اگر کنترل خطا در لایه پیوند داده صورت نگیرد. این بسته به طور متوسط چند بار باید ارسال شود تا صحیح به مقصد برسد؟

۱) ۱۰ ۲) ۹/۳۱ ۳) ۸/۳۱ ۴) ۷/۳۱

احتمال اینکه هر فریم صحیح به مقصد برسد = ۰٫۸
احتمال اینکه همه ۱۰ فریم صحیح به مقصد برسند = $(۰٫۸)^{۱۰}$
بطور متوسط چند بار ارسال شود تا صحیح به مقصد برسد = $\frac{۱}{(۰٫۸)^{۱۰}} = (\frac{۱۰}{۸})^{۱۰} \simeq ۹٫۳۱$

۳۳۳

مهندسی کامپیوتر ۸۴: در یک شبکه کامپیوتر، لایه پیوند داده‌ها خطاهای انتقال را با درخواست ارسال مجدد برای پیام‌های دریافتی خطادار مرتفع می‌نماید. فرض کنید احتمال دریافت یک پیام به صورت خطادار P باشد و درخواست ارسال مجدد نوین بدون خطا دریافت گردد. تعداد متوسط ارسال یک پیام برای دریافت بدون خطای آن چقدر است؟

۱) $\frac{۱}{۱-P}$ ۲) $\frac{۱}{۱-P^۲}$ ۳) $\frac{۱}{۱-۲P}$ ۴) $\frac{۱}{(۱-P)^۲}$

۳۳۴

مهندسی کامپیوتر ۸۸: یک پیام از لایه بالاتر به ۵ بسته تقسیم شده است. اگر عملیات کنترل خطا در ارسال این بسته صورت نگیرد و احتمال دریافت صحیح بسته در مقصد ۰/۵ باشد، این پیام چند بار باید ارسال شود تا صحیح به مقصد برسد؟

۱) ۴ ۲) ۸ ۳) ۱۶ ۴) ۳۲

احتمال اینکه همه فریم ها درست به مقصد برسد = $\frac{۱}{۲} \times \frac{۱}{۲} \times \dots \times \frac{۱}{۲}$ (۵ بسته) = $\frac{۱}{۳۲}$
بسته چند بار ارسال شود تا موفق برسد = $\frac{۱}{\frac{۱}{۳۲}} = ۳۲$

کافه تدریس و استاد رضوی هیچ رضایتی نسبت به استفاده غیر مجاز از ویدیوها ندارد. استفاده غیر مجاز از این موارد کاملا حرام و پیگرد قانونی دارد

Scanned with CamScanner