輻輳制御

●送信元と送信先との間のルータが輻輳を検知すると、IP ヘッダの ECN フィールドのフラグが立つので、送信先は送信元に輻輳発生を通知するために、TCP ヘッダのコントロールフラグ（SYN、FIN、ACK 等に対してフラグを立てるやつ）の中の ECE（ECN-Echo）フラグを 1 にしてから、送信元にパケットを送る。

●輻輳ウインドウを縮小したことを送信先に通知するため、送信元は TCP ヘッダのコントロールフラグの中の CWR（Congestion Window Reduced）フラグを 1 にしてからパケットを送る。

※輻輳ウインドウの縮小方法は省略

●輻輳ウインドウ：ウインドウサイズまでは受信確認を待たずにデータを送れるが、念のため輻輳が発生しないように、通常は、MSS（Max Segment Size）の 1 倍から徐々に 2,4,8…倍にして、輻輳が発生しない実際のウインドウサイズを探す。この時に使用されるのが輻輳ウインドウである。徐々に輻輳ウインドウを増やすことをスロースタートアルゴリズムという。

●ECN を採用する以前は、RTO（Retransmission Time Out）等によって、輻輳を検知していた。送信したパケットに対する ACK が返ってこない場合、再送するまでの時間が RTO であり、RTT（Round Trip Time：相手に TCP パケットを送信してから、ACK を受信するまでの時間）に基づいて決定される。

●似た言葉である TAT（Turn Around Time）は、システムに処理要求してから結果の出力が終了するまでの時間である。RTT にシリアル化遅延時間を加えると TAT と同じ概念になる。

MTU (Maximum Transmission Unit：最大伝送単位)

FCS (Frame Check Sequence)

CRC (Cyclic Redundancy Check：巡回冗長検査)

SFD (Start Frame Delimiter：Delimiter（区切り符号）)

●イーサネットフレームにおいてデータ部分はデータ本体だけでなく IP ヘッダと TCP ヘッダも含まれる。この時の MTU（IPH＋TCPH＋データ）は 1500 オクテット（バイト）である。

●イーサネットフレームのエラー等をチェックするために FCS にはフレーム全体を特定のビット列（生成多項式）で割った余りである CRC を入れる。

●イーサネットフレームを送る時にはフレームの前にプリアンブルと呼ばれるフィールドが付加され、そのフィールドの最後の 1 オクテットを SFD と呼ぶ。

QUIC (Quic UDP Internet Connections)

●トランスポート層のプロトコル。QUIC を使った HTTP 接続は HTTP/3 (HTTP ver3)として整理。

●UDP をベースに高速伝送を実現する一方、TCP の要素を取り込んで信頼性を高め、TLS の要素を取り込んで暗号化による安全性を高めている。

UDP が送信元 IPA を詐称しやすい理由

●スリーウエイハンドシェイク、つまりコネクション確立フェーズでは、お互いの IPA、ポート番号、シーケンス番号、確認応答番号、ウインドウサイズ等を交換し合うため、この時点で IPA を詐称しても、他のパラメータでボロが出てくるため確立フェーズは失敗する可能性が高い。そして確立フェーズ後の割り込みは、更にハードルが高くなるため、至難の業となるだろう。

TCP wrapper

●UNIX 系 OS に常駐するプログラムで tcpd（TCP デーモン）のこと。

●tcpd は、接続元の IPA 等の情報を元に、外部からの TCP/IP 接続のアクセス制御を行う。

TCP トリビア

●FIN/ACK で返しに ACK で終了であるが、RST/ACK は一方的に送り付けて終了

●一方的と言えば、IPA を DHCP サーバに返す時も、DHCPRELEASE を送りつけて終了

●RTT は転送時間で、シリアル化遅延時間は伝送時間。実効転送速度はウインドウサイズを RTT で割ったもの。

ポートとソケット

●通常、TCP/IP 通信では、1 つの IPA に 2 の 16 乗（65536）のポートで構成される。このポートとは、機器内のサービス（特定プロセスやアプリケーション等）に割り当てられた数値であり、そのポートで物理的にデータを送受信するインターフェースがソケットである