H.323 を用いた TV 会議と Fire Wall との問題

内藤茂樹

分子科学研究所 技術課

(Check Point Certified Security Engineer 2000)

概要

独立法人化に向けて、統合される核融合科学研究所と国立天文台との間で頻繁に会議が行われてきたが、各機関が地理的に離れているために TV 会議 System を利用することになった。そこで岡崎機構では分子科学研究所電子計算機室で保有している Polycom 社製 View Station を使用した。実際に接続テストをしたところ、30 分程度で接続が切れてしまう現象が発生し、岡崎機構の Fire Wall(NOKIA IP740)が疑われたが、Fire Wall の log には特に問題は見あたらなかった。そこで、電子計算機室で保有する 2 台の View Station を使って、View Station 間の通信 packet を monitoring し、原因を追及した。

今回はその結果と業者からの回答を踏まえ、Fire Wall を挟んで TV 会議を導入する際の注意点を発表する。

1　発生した問題

実際に行われた TV 会議で発生した問題について説明する。

1.1　TV 会議の状況

岡崎国立共同研究機構と、核融合科学研究所、国立天文台がそれぞれ保有する Polycom 社製 View Station を使って画像と音声データを送受信し、同時に Microsoft 社製 NetMeeting を使って data の遣り取りを行っている。どちらも使用している protocol は H.323 である。基本的に View Station/NetMeeting 共に核融合科学研究所から各機関の機器へ call している。概要でも述べたとおり、View Station では 30 分程度で切断される問題が発生しているため、その都度 call し直す運用を余儀なくされている。

1.2　問題の内容

30 分程度で通信が切断されるという現象が起きているのは、3 機関のうち岡崎機構のみである。この現象は、特に何か操作した瞬間に切れるというわけではなく、ただ接続して画像/音声を流しているだけで切れてしまう。また逆に何か操作していれば切れないかと言うとそうでも無い。そして核融合科学研究所と国立天文台間では発生しない。また岡崎機構から call しても他機関から call しても現象は変わらない。なお View Station の firmware を version up したところ、問題の発生時間が 2 時間程度となった。

この現象は再現性があり必ず発生するので途中の経路が疑われ、その中でも岡崎機構の Fire Wall ではないかと推測された。ただしこの Fire Wall で設定されている time out 時間は、TCP が 3600 秒(1 時間)であり UDP が 40 秒である。従って 30 分程度という時間は Fire Wall による time out では無い。なお H.323 で使われる protocol の中で、TCP のものは現在 10800 秒(3 時間)に設定されている。

2　H.323 について

View Station では動画/音声の配信に H.323 を使用している。H.323 は複数の protocol からなり、Call Control として H.225、Media Control として H.245、動画/音声の codec 及び転送方式として RTP を使用する。H.225/H.245

は TCP であり、動画/音声の転送は UDP である。実際の通信は、まず H.225 にて Call Control Channel を開く。H.225 の TCP port number は 1720 である。続いてその Channel を利用して、H.245 により端末同士の能力情報交換、master/slave の決定、RTP stream 用の channel の確立を行うための Media Control Channel を開く。H.245 の TCP port number は動的に決定される。そして RTP stream による通信が開始される。RTP の UDP port number は動的に決定される。従って全ての通信は H.225 で開いた Channel を基にして行われる。

3　調査

岡崎機構の Fire Wall は Nokia 社製 IP740 であり、その Fire Wall engine は Check Point 社製 FireWall-1 である。この Fire Wall-1 は Stateful Inspection を特徴とする。これは Service(使用する port 番号等)を定義しておけば、その Service の通信の状態を終了まで追跡し制御するもので、予め遷移後の high port を開けておく必要がない。そのため Security が高く管理もしやすいのであるが、その反面 log 情報に乏しく今回のように通信途中に問題が発生した場合、その瞬間に何があったかを把握することが困難である。そこで電子計算機室が所有する 2 台の View Station 間で TV 会議を行い、その両側で packet monitoring し、通信が途絶えたときの状況を把握することにした。今回の調査では packet monitoring を行うのに Ethereal を用いた。

3.1　調査方法

調査中 Fire Wall の設定を頻繁に変更する可能性があるため、岡崎機構職員が常時使用している IP740 を使うわけにはいかなかった。そこで普段は利用者のいない岡崎カンファレンスセンター用の Fire Wall である Nokia IP330 を使わせて貰った。この IP330 に搭載されている Fire Wall engine は、IP740 と同じである。この IP330 の両側に dump Hub を設置し、それぞれに View Station と Ethereal 用の PC を接続した。これで Fire Wall 越しの View Station 間の通信内容を monitoring することが出来る。また比較のために通信経路に Fire Wall を挟まない場合の通信内容も monitoring した。

3.2　調査結果

2 台の View Station のうち call する側を A、call される側を B とする。Ethereal のデータから、通信開始後凡そ 1740 秒後に H225 の[RST]packet を A、B ともに受信して終了してしまうことが判った。詳しく packet を調査すると、A は約 1740 秒後に Seq.No.を 1 減らした[ACK] packet を B に向けて送信している。次の表は H.225(1720)の TCP stream のみを抜き出して表示したものである。

No.	Time	Source	Destination	Protocol	Info
10	3.554325	A	B	TCP	2778 > 1720 [SYN] Seq=215628286 Ack=0 Win=23360 Len=0
11	3.55899	B	A	TCP	1720 > 2778 [SYN, ACK] Seq=24717819 Ack=215628287 Win=23360 Len=0
12	3.560308	A	B	TCP	2778 > 1720 [ACK] Seq=215628287 Ack=24717820 Win=23360 Len=0
:	:	:	:	:	:
29	4.207428	A	B	TCP	2778 > 1720 [ACK] Seq=**215628452** Ack=24718065 Win=23115 Len=0
183279	1743.339002	A	B	TCP	2778 > 1720 [ACK] Seq=**215628451** Ack=24718065 Win=23115 Len=0
183283	1743.4019	B	A	TCP	1720 > 2778 [**RST**] Seq=24718065 Ack=215628451 Win=0 Len=0

No.29 の packet の Seq.No.が 215628452 なのに対して、No183279 の packet の Seq.No.が 215628451 と 1 減少している。そして No.183283 で A が[RST]packet を受信しているのが判る。

一方 B は約 1740 秒後に、最後に A から受信した packet の Ack.No.から 1 減らした値を Seq.No.とした[ACK] packet を A に向けて送信している。同様に H.225(1720)の TCP stream のみを抜き出してみると、次の表のようになる。

No.	Time	Source	Destination	Protocol	Info
3	2.201679	A	B	TCP	2778 > 1720 [SYN] Seq=215628286 Ack=0 Win=23360 Len=0
6	2.203766	B	A	TCP	1720 > 2778 [SYN, ACK] Seq=24717819 Ack=215628287 Win=23360 Len=0
7	2.206378	A	B	TCP	2778 > 1720 [ACK] Seq=215628287 Ack=24717820 Win=23360 Len=0
:	:	:	:	:	:
22	2.853405	A	B	TCP	2778 > 1720 [ACK] Seq=215628452 Ack=**24718065** Win=23115 Len=0
183466	1742.566138	B	A	TCP	1720 > 2778 [ACK] Seq=**24718064** Ack=215628452 Win=23195 Len=0
183468	1742.628811	A	B	TCP	2778 > 1720 [**RST**] Seq=215628452 Ack=24718064 Win=0 Len=0

No.22 の packet の Ack.No.が 24718065 なのに対して、No.183466 の packet の Seq.No.が 2718064 と 1 減少している。そして No.183468 で B が[RST]packet を受信しているのが判る。

そこで Fire Wall を挟まない状態での H.225 の TCP stream のデータを見てみると、[ACK]packet の Seq.No.が同様に 1 減少しているにもかかわらず、[RST]packet が流れずに通信は問題なく継続されている。

No.	Time	Source	Destination	Protocol	Info
6	3.932917	A	B	TCP	2772 > 1720 [SYN] Seq=98300429 Ack=0 Win=23360 Len=0
7	3.934517	B	A	TCP	1720 > 2772 [SYN, ACK] Seq=109552122 Ack=98300430 Win=23360 Len=0
8	3.935273	A	B	TCP	2772 > 1720 [ACK] Seq=98300430 Ack=109552123 Win=23360 Len=0
:	:	:	:	:	:
24	4.653884	A	B	TCP	2772 > 1720 [ACK] Seq=**98300595** Ack=109552368 Win=23115 Len=0
144558	1742.284449	A	B	TCP	2772 > 1720 [ACK] Seq=**98300594** Ack=109552368 Win=23115 Len=0
144559	1742.285384	B	A	TCP	1720 > 2772 [ACK] Seq=**109552368** Ack=98300595 Win=23195 Len=0
290254	3481.661883	B	A	TCP	1720 > 2772 [ACK] Seq=**109552367** Ack=98300595 Win=23195 Len=0
290255	3481.662792	A	B	TCP	2772 > 1720 [ACK] Seq=**98300595** Ack=109552368 Win=23115 Len=0
433858	5221.343926	A	B	TCP	2772 > 1720 [ACK] Seq=**98300594** Ack=109552368 Win=23115 Len=0
433859	5221.344988	B	A	TCP	1720 > 2772 [ACK] Seq=109552368 Ack=98300595 Win=23195 Len=0
:	:	:	:	:	:

これらのことから[RST]packet を発信しているのは、Fire Wall ではないかと推測された。

4 各社からの回答

以上の調査結果を基に、FireWall-1 の製造元である Check Point 社、View Station の製造元である Polycom 社、そして岡崎機構の Fire Wall の導入業者である NetMarks 社に対して質問を行った。以下にその質問と各社からの回答の要約を提示する。

4.1 Check Point 社

Check Point 社に対しては今回のデータを添付すると共に、Seq.No.が減少した packet を受信した時の Fire Wall-1 の動作について質問した。Check Point 社から「Fire Wall-1 は Seq.No.のチェックをしており、異常があると判断した場合 reset または reject の処理を行う」との回答を得た。これにより、View Station から送信された Seq.No.が 1 減少した[ACK]packet に対して[RST]packet を返しているは、岡崎機構の Fire Wall(Fire Wall-1)であることが確定した。

4.2 Polycom 社

Polycom 社に対しては、View Station が送信する Seq.No.を 1 減少させた[ACK]packet は TCP の規約に反しているのではないかと質問した。Polycom 社から「その[ACK]packet は RFC1122 にある keep-alive である」、「Check point の Fire Wall で View Station の通信が遮断されるのは既に Check Point 社で認識されている問題であり、patch も提供されている」との回答を得た。RFC1122 では「To confirm that an idle connection is still active, these implementations send a probe segment designed to elicit a response from the peer TCP. Such a segment generally contains SEG.SEQ = SND.NXT-1 and may or may not contain one garbage octet of data. Note that on a quiet connection SND.NXT = RCV.NXT, so that this SEG.SEQ will be outside the window. Therefore, the probe causes the

receiver to return an acknowledgment segment, confirming that the connection is still live.」と記述されていて、View Station ではこれを利用しているとの事だった。しかし同じ RFC1122 には「The TCP specification does not include a keep-alive mechanism because it could: (1) cause perfectly good connections to break during transient Internet failures; (2) consume unnecessary bandwidth ("if no one is using the connection, who cares if it is still good?"); and (3) cost money for an Internet path that charges for packets.」とあり、そして「Implementors MAY include "keep-alives" in their TCP implementations, although this practice is not universally accepted. If keep-alives are included, the application MUST be able to turn them on or off for each TCP connection, and they MUST default to off.」と記述されている。keep-alive を実装する場合は on/off の切り替えが可能であり default は off でなければならいならば、View Station が RFC1122 に準拠している以上 keep-alive を off にする方法があるかも知れないと思い、Polycom 社にそのことを質問した。それに対して Polycom 社から「RFC1122 では TCP/IP protocol stack の組込方法について記述されており、View Station の TCP/IP protocol stack は RFC1122 に基準している。この RFC では application の layer がその TCP/IP protocol stack の利用する方法については触れていない。RFC1122 の規格通り、View Station の TCP/IP protocol stack では keep-alive は default で off になっており、通話を行っていない状況では keep-alive を送信しない。View Station の application の layer が必要に応じて(つまり通信中に)keep-alive を on にしている。なお、この keep-alive を application の layer で常時 off にする設定は無い」との回答を得た。View Station の TCP/IP stack が RFC1122 に準拠しているのなら、application 側で keep-alive を使わない設定にすれば Fire Wall の問題も解決するのであるが、そのような機能は無いようである。これにより View Station 側で keep-alive を停止することによって問題解決を図ることが不可能だということが判った。

4.3 NetMarks 社

Polycom 社からの回答より Fire Wall-1 用の patch があることが判ったため、その patch の情報を導入業者である NetMarks 社に尋ねたところ「岡崎機構の Fire Wall-1 の Version である NG fp2 用の patch は無い。NG fp3 用にならpatch がある。」との回答を得た。つまり現状の岡崎機構では今回の問題には対応出来ないことが判明した。

5 まとめ

今回の問題の原因は岡崎機構の Fire Wall1 が TCP の keep-alive に対応していないことにある。従って TV 会議(H.323)以外にも問題が発生する可能性がある。しかし現在岡崎機構でこの問題が発生しているのは Polycom 社製 View Station を使った TV 会議のみであり、他の Service では発生していない。以上のことから、今後 Fire Wall を導入するときには TCP keep-alive に対応しているかどうか確認した方が良い。また TV 会議を導入するときには、Fire Wall 越しの通信についての確認事項の中に、使用する protocol だけではなく TCP keep-alive を使っているかどうかも入れておいた方が良いだろう。また現在では Internet もかなり安定しているので、TCP keep-alive を使わない設定のできるものや、そもそも実装していないものを選べば無用な問題を起こす事もない。

参考文献

[1] 今泉弘幸, “図解雑学 IP 電話”,ナツメ社

Check Point Certified Security Engineer 2000