Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	GN Docket No. 14-28
Protecting and Promoting the Open Internet	)	
In the Matter of	)	
	)	GN Docket No 10-127
Framework for Broadband Internet Service	)	
In the Matter of	)	
	)	GN Docket No. 13-5
Technology Transitions	)	
In the Matter of	)	
	)	GN Docket No. 09-51
A National Broadband Plan for Our Future	)	
In the Matter of	)	
	)	WT Docket No. 13-135
State of Wireless Competition	)	
In the Matter of	)	
	)	WC Docket No. 07-52
Broadband Industry Practices	)	

COMMENTS OF GOLDEN FROG

Matthew A. Henry
henry@dotlaw.biz
W. Scott McCollough
wsmc@dotlaw.biz
MCCOLLOUGH|HENRY PC
1250 S. Capital of Texas Hwy., Bldg. 2-235
West Lake Hills, TX 78746
Phone: 512.888.1112
Fax: 512.692.2522

July 18, 2014

TABLE OF CONTENTS

I.   EXECUTIVE SUMMARY

Since there are no enforceable open Internet rules, broadband Internet access providers are currently throttling and blocking Internet users' traffic. These comments discuss two recent examples that show that users are not receiving the open, neutral, and uninterrupted service to which the Commission says they are entitled.

In the first instance, a customer of Golden Frog's VyperVPN encrypted VPN service has proven that his Netflix traffic is being throttled on Verizon's FiOS service. Colin Nederkoorn recently
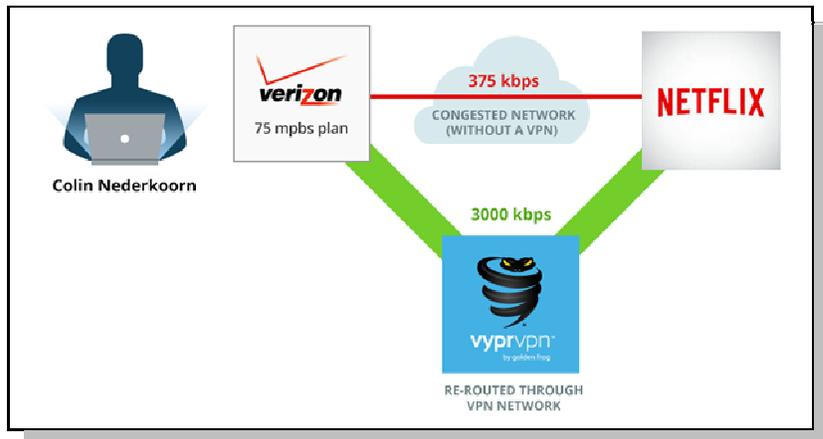
posted a YouTube video of a test he performed on his 75 Mbps service from Verizon that shows his Netflix connection increased from a paltry 375 Kbps to 3000 Kbps when he employed VyprVPN. This is a ten-fold increase that resulted from encrypting his traffic and using VyprVPN's routing. This type of increase in speed is consistent with reports from other customers. Internet access providers are "mismanaging" their networks to their own users' detriment.

In the second instance, Golden Frog shows that a wireless broadband Internet access provider is interfering with its users' ability to encrypt their SMTP email traffic. This broadband provider is overwriting the content of users' communications and actively blocking STARTTLS encryption. This is a man-in-the-middle attack that prevents customers from using the applications of their choosing and directly prevents users from protecting their privacy.
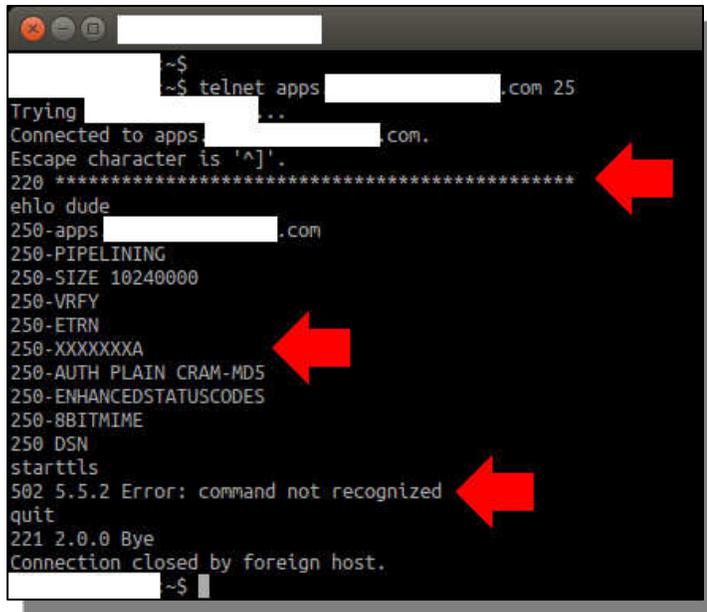
The Commission must establish effective rules that prevent this type of behavior. Unless wireless and wireline broadband access providers receive a strong message that they can no longer throttle and block their users' Internet traffic, these actions will continue, expand, and become the norm. Golden Frog calls on the Commission to truly restore the open Internet, enhance competition, protect user choice, and ensure users can keep nosy Internet access providers from intercepting their private information.

II.   DESCRIPTION OF GOLDEN FROG

Golden Frog GmbH[1] is a global service provider committed to developing applications and services that provide an open and secure Internet experience, while preserving and enhancing user privacy. Golden Frog owns and operates a global network with private server

---

[1] Golden Frog is a member of the Internet Infrastructure Coalition (i2Coalition), and supports the comments submitted by the i2Coalition. Like i2Coalition, Golden Frog believes that a preferable course of action is to return to Open Access, and if this is done the Commission need not and should not directly regulate Internet access.

clusters in North America, South America, Europe, Asia and Oceania with users in over 195 countries. Golden Frog owns and manages 100% of its own servers, hardware and network to ensure the highest levels of security, privacy and service delivery. Golden Frog's founders are Internet veterans who have owned and operated Internet businesses since the dawn of the public Internet in 1994.

Golden Frog created VyprVPN – a secure personal VPN service – to help users protect themselves against efforts by commercial or governmental third parties to monitor, access and intercept confidential, privileged or private information. VyprVPN provides encrypted connections to the Internet to protect user privacy and security. Like other VPN providers, Golden Frog uses standards-based VPN protocols. Unlike other VPN providers, Golden Frog writes 100% of its supporting software, manages its own network, and owns the hardware enabling it to deliver the fastest VPN speeds in the world. VyprVPN has desktop applications for Windows and Mac and recently launched mobile apps for iOS and Android.

Dump Truck is Golden Frog's second product. Dump Truck provides secure online storage that allows users to safely store, sync, share and access all of their files from anywhere and on any device. All data uploaded to Dump Truck is encrypted in transit and then encrypted with per-user keys while stored. Golden Frog does not rely on third parties to store user data or use data deduplication to inspect user data. Dump Truck for Mac and Windows automatically syncs all files to the desktop. Dump Truck mobile apps for iOS and Android allow easy access to files while on the go. The Dump Truck Web App provides access to files from any web browser and access to advanced features such as public sharing, activity feeds, and more.

II.   VPNs PROTECT PRIVACY AND SHOW THAT INTERNET ACCESS PROVIDERS ARE THROTTLING TRAFFIC

Golden Frog's original purpose for VyprVPN was to protect privacy and facilitate a truly open Internet. Even before the Snowden revelations, we were aware of the extent to which both government and other commercial interests were inspecting traffic and monitoring domestic communications. Indeed, our sister company Data Foundry predicted this would occur in multiple prior filings with the Commission.[2] When the Commission and others chose to proceed despite Data Foundry's cautioning, our founders decided to deploy a product that would defeat monitoring efforts. At the same time, several other countries were also spying on their citizens and denying access to Internet applications, content, services, uses, sources/destinations or devices. Golden Frog was formed, and VyprVPN was born. Users worldwide can now access the full Internet and maintain privacy using our encryption tools.

---

[2] Docket 07-52, *In the Matter of Broadband Industry Practices*, Data Foundry Comments, pp. 9-12 and Attachment B (June 16, 2007), available at http://apps.fcc.gov/ecfs/document/view?id=6519529007; Docket 07-52, *In the Matter of Broadband Industry Practices*, Data Foundry Reply Comments (July 16, 2007), available at http://apps.fcc.gov/ecfs/document/view?id=6519558239; Docket 07-52, *In the Matter of Broadband Industry Practices*, Data Foundry Notice of *Ex Parte* and Attachment "Tiered Internet Service Threatens the Privileged and Confidential Nature of Online Communications (October 22, 2008), available at http://apps.fcc.gov/ecfs/document/view?id=6519741393; Docket 07-52, *In the Matter of Broadband Industry Practices*, Data Foundry Notice of *Ex Parte* and Attachment "Broadband Network Management and Net Neutrality: Equal Threats to User Privacy and Security" (October 22, 2008), available at http://apps.fcc.gov/ecfs/document/view?id=6520176853; Docket GN 09-51, *In the Matter of A National Broadband Plan for Our Future*, Data Foundry Comments (June 8, 2009), available at http://apps.fcc.gov/ecfs/document/view?id=6520220238; Docket GN 09-51, *In the Matter of A National Broadband Plan for Our Future*, Data Foundry Reply Comments (July 21, 2009), available at http://apps.fcc.gov/ecfs/document/view?id=7019917828; Docket 07-52, *In the Matter of Broadband Industry Practices* and Docket GN 09-51, *In the Matter of A National Broadband Plan for Our Future*, Data Foundry Notice of *Ex Parte* (October 19, 2009), available at http://apps.fcc.gov/ecfs/document/view?id=7020142373; GN Docket 09-191, *In the Matter of Preserving the Open Internet* and WC Docket 07-52, *Broadband Industry Practices*, Data Foundry Comments (January 14, 2010), available at http://apps.fcc.gov/ecfs/document/view?id=7020378808; NBP Public Notice #29, GN Docket Nos. 09-47, 09-51, and 09-137, Data Foundry Comments (January 23, 2010), available at http://apps.fcc.gov/ecfs/document/view?id=7020383064; GN Dockets No. 09-51 and 09-191 and WC Docket No. 07-52, Data Foundry Notice of *Ex Parte* and Attachment (January 28, 2010), available at http://apps.fcc.gov/ecfs/document/view?id=7020384236; GN Docket No. 10-127, *In the Matter of Framework for Broadband Internet Service*, Data Foundry Comments, pp. 23-35 (July 15, 2010), available at http://apps.fcc.gov/ecfs/document/view?id=7020547123; GN Docket No. 10-127, *In the Matter of Framework for Broadband Internet Service*, Data Foundry Reply Comments, pp. 16-22 (August 12, 2010), available at http://apps.fcc.gov/ecfs/document/view?id=7020706608; ; GN Docket No. 10-127, *In the Matter of Framework for Broadband Internet Service*, Data Foundry Notice of *Ex Parte* (August 25, 2010), available at http://apps.fcc.gov/ecfs/document/view?id=7020809986.

VPNs, however, have another salutary attribute. They defeat Internet access provider throttling through application identification and "special treatment" on the user facing side or purposeful congestion of particular connections on the "Internet" facing side. VyprVPN, in effect, allows Internet access customers to override Internet access providers' privacy invasions and other conduct that inhibits, interferes with or controls user choices regarding applications, content, services, use, source/destination or devices.

VyprVPN users consistently report that their speeds increase when they use VyprVPN. They are effectively using VyprVPN's encrypted connection to boost their speeds, while also protecting their privacy. This demonstrates that there is a market for alternative Internet access providers that do not throttle traffic or invade their users' privacy, and VPNs are proving to be the closest surrogate for real broadband competition

The current controversy over whether Internet service providers are throttling video traffic or purposefully letting traffic become congested on ingress links demonstrates this is so. Several users that suffer degraded video streams when trying to connect to video sites like Netflix or YouTube have discovered that if they employ a VPN, the problem disappears. A recent example was revealed on July 17, 2014.[3] Golden Frog has known about this for quite some time. For example, we blogged about the issue in April, 2014.[4]

Common sense would lead one to believe speeds would inherently slow down due to the encryption overhead. But activity at the network layer explains why there is increased speed

---

[3] *See* Colin Nederkoorn's Blog, Verizon made an enemy tonight, http://iamnotaprogrammer.com/Verizon-Fios-Netflix-Vyprvpn.html; John Brodkin, 'Verizon made an enemy': FiOS customer mad that Netflix works better on VPN, 75Mbps Verizon FiOS service isn't good enough to stream Netflix smoothly, Ars Technica (July 18, 2014), available at http://arstechnica.com/information-technology/2014/07/verizon-made-an-enemy-fios-customer-mad-that-netflix-works-better-on-vpn; Ben Popper, How one man bypassed internet congestion and fixed his Netflix streaming, On today's internet, the shortest route is sadly not always the best, The Verge (July 18, 2014), available at http://www.theverge.com/2014/7/18/5916153/netflix-verizon-vpn-streaming-congestion-speed.

[4] *See* Golden Frog Blog, Infographic: Netflix vs. Comcast – The Peering Problem, (April 25, 2014) © 2014 Golden Frog, GmbH, available at http://www.goldenfrog.com/blog/netflix-vs-comcast-the-peering-problem.

despite the additional overhead. A VPN provider that operates its own server infrastructure, is multi-homed, and that runs its own network can control the router and dynamically use uncongested routes to users.[5] Attachment A provides an illustration. The Internet access providers are using Deep Packet Inspection to identify the application, content, service, use, source/destination or device based on access provider preferences, rather than user preferences. Proxies and encryption allow the user to override the Internet access provider's "traffic management" and shaping.

Of particular interest in the example from July 17 is that this consumer was able to utilize the same Internet access to achieve full throughput of his Netflix service by using a VPN to control the route through which Netflix flowed. This demonstrates that his Internet access provider has sufficient bandwidth to fulfill his request, but the provider chooses to not properly manage the network in order to provide their customer the bandwidth that was advertised and contracted. Instead, he had to take further action and utilize a VPN service, in the hopes that the route through his Internet access provider to the VPN service was on an uncongested link.

The Internet access providers may claim that alternatives such as VyprVPN provide the sort of technological or competitive market responses available on the Internet that make rules unnecessary. While it is true that these are in fact technological and competitive market responses, the very same Internet access providers who make that claim can throttle or block VPNs, proxies or encryption if the Commission imposes no effective rules. As the i2Coalition observed in its comments on pages 37-49, the current proposed rules do not prevent them from

---

[5] The large Internet access providers could use similar network management techniques avoid congestion on ingress and egress traffic, but they choose to not do so. If they had any competition or a true desire to actually fulfill the contracts they formed with their users they would add capacity as needed and use real management rather than opportunistically attacking traffic they do not like or want to tax.

interfering with encryption services. Without enforceable rules, Netflix throttling may be the problem of today and encryption blocking the problem of tomorrow.

We turn now to a demonstration that broadband Internet access providers have already started blocking their users' efforts to encrypt.

III. ENCRYPTION BLOCKING IS OCCURRING TODAY AND THE PROPOSED RULES WOULD NOT STOP IT

As a result of *Verizon v. FCC*, broadband Internet access providers are no longer subject to any no-blocking or anti-discrimination rules.[6] They are completely free to interfere with their customers' use of the Internet at will. The dominant Internet access providers repeatedly protest that rules against blocking and unreasonable discrimination need not be reinstated because there is no evidence any is occurring or will occur, and they can be trusted to act properly without any rules. The NPRM, however, sets out actual empirical evidence supporting the stated concerns by listing a series of acts by fixed and mobile Internet access provider that directly support those concerns.[7] Our Netflix example above provides further evidence of an Internet access provider failing to perform proper network management in the best interest of fulfilling the service sold to a large number of customers.

The purpose of these comments is to provide new evidence that blocking is occurring today, and therefore demonstrate that there are still problems to be solved and effective rules are required. Golden Frog has recently discovered that at least one broadband service provider is blocking the use of a common email encryption technology. Specifically, this provider is using network equipment to block the STARTTLS command from enabling the encryption of SMTP (Simple Mail Transfer Protocol) traffic.

---

[6] *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014).

[7] *Protecting and Promoting the Open Internet*, Notice of Proposed Rulemaking, 2014 FCC LEXIS 1689 (2014) at ¶¶ 6, 26, and 39-53.

STARTTLS is an extension to SMTP that allows an SMTP server and client to use TLS (Transport Layer Security) to provide private, encrypted, and authenticated communication over the Internet. This gives users the ability to protect some or all of their communications from eavesdroppers and attackers. SMTP [RFC2821] servers and clients routinely communicate in the clear over the Internet.[8] In many cases, this communication goes through one or more routers that are not controlled or trusted by either entity. An untrusted router might allow a third party to monitor or alter the communications between the server and client.[9]

STARTTLS allows a client to initially make a clear connection but then initiate a request to the server to switch to an encrypted connection. The initial connection is in the clear, so any entity in the middle – including the Internet access provider – can see the connection requests and associated header and control information, including the connection set up requests. It is possible for an Internet access provider to interpret the request and control information, and to even change the content requests from the client or responses from the server. This includes the client request to initiate an encrypted session, or the server response to that request.

Golden Frog performed tests using one mobile wireless company's data service, by manually typing the SMTP commands and requests, and monitoring the responses from the email server in issue. It appears that this particular mobile wireless provider is intercepting the server's banner message and modifying it in-transit from something like "220 [servername] ESMTP Postfix" to "200 ********************." The mobile wireless provider is further modifying the server's response to a client command that lists the extended features supported by the server. The mobile wireless provider modifies the server's "250-STARTTLS" response

---

[8] It is possible to establish an encrypted connection at the beginning. SMTPS automatically starts SSL encryption before any SMTP level communication.

[9] RFC 3207, <u>SMTP Service Extension for Secure SMTP over Transport Layer Security</u>, © The Internet Society (2002), available at <u>https://tools.ietf.org/html/rfc3207</u>.

(which informs the client of the server's capacity to enable encryption). The Internet access provider changes it to "250-XXXXXXXA." Since the client does not receive the proper acknowledgement that STARTTLS is supported by the server, it does not attempt to turn on encryption. If the client nonetheless attempts to use the STARTTLS command, the mobile wireless provider intercepts the client's commands to the server and changes it too. When it detects the STARTTLS command being sent from the client to the server, the mobile wireless provider modifies the command to "XXXXXXXX." The server does not understand this command and therefore sends an error message to the client.

The practice in issue and in use by this provider is conceptually similar to the way that Comcast used packet reset headers to block the use of BitTorrent in 2007. The result is that wireless Internet users that wish to protect their email communications with basic encryption protocols cannot do so when on this particular wireless provider's network.

Although the precise technology being used in this instance cannot be determined, the activity resembles a documented feature made available in the Cisco Adaptive Security Appliance (ASA). An ASA purchaser can engage in "ESMTP application inspection," monitor content, and limit commands and responses that that can pass through the system. Cisco's documentation explains that after the ASA purchaser enables ESMTP application inspection, the feature "changes the characters in the server SMTP banner to asterisks." "An SMTP server responds to client requests with numeric reply codes and optional human readable strings. SMTP application inspection controls and reduces the commands that the user can use as well as the messages that the server returns."[10] This is exactly what Golden Frog experienced.

---

[10] The Cisco Adaptive Security Appliance's ability to filter SMTP and ESMTP traffic is documented and explained at http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113423-asa-esmtp-smtp-inspection.html; *see also* http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/I-R/cmdref2/i2.html#pgfId-1765148. Golden Frog is not alleging that the blocking related above is being performed

Attachment B to these comments contains two screenshots that compare a successful STARTTLS session initiation (on a different network) with a failed session on the wireless provider's network. The screenshot of the unsuccessful STARTLLS session shows that an ESMTP banner is being overwritten with asterisks, the STARTTLS extended option is Xed out, and the client command leads to an error message. The result is an inability to establish an encrypted link.

Absent enforceable Commission rules, broadband providers can (and at least one already does) block and discriminate against entirely acceptable Internet uses. In this case, users are not just losing their right to use the applications and services of their choosing, but also their privacy. It is not at clear that this type of encryption blocking would be forbidden for fixed broadband Internet access, under the proposed rules' exception for reasonable network management. This example involves mobile wireless broadband, however, and it is clear that the proposed rules would _**not**_ prohibit the activity. STARTLLS encryption does not constitute "a lawful website" or "an application[] that compete[s] with the provider's voice or video telephony services[.]"[11] The proposed rules on their face do not prohibit mobile broadband Internet access providers from blocking user efforts to maintain privacy through encryption.

IV.   CONCLUSION

The claim that rules banning blocking and unreasonable discrimination are solutions in search of a problem is flatly wrong. There have been problems in the past and there are problems

by a Cisco appliance. The citation and quotations are provided only to provide a technical explanation of how it can be made to occur, and the result. Further, Golden Frog emphasizes that this feature can be important to an Enterprise or private network operator to manage security issues. The problem arises when it is applied by an Internet access provider to conduct a man in the middle attack in order to frustrate a user's efforts to encrypt communications and perhaps even intercept the content of emails the user wants to keep private. In this situation, the Internet access provider is merely "an untrusted router" and "third party" that is able to monitor or alter the communications between the server and client." As RFC 3207 explains that is the very thing the STARTTLS extension is designed to prevent.

[11] _See Protecting and Promoting the Open Internet_, Notice of Proposed Rulemaking, 2014 FCC LEXIS 1689 (2014) at § 8.5.

now. The proposed rules do not resolve all of the problems identified in the NPRM. Further broadband Internet access providers are still interfering with beneficial and privacy-enhancing applications users want to employ. Internet access providers, even with demonstrable available bandwidth, also continue to fail to properly manage the networks to ensure their customer base receives the service levels they have contracted for and paid to receive. The Commission needs to take strong action to protect the Open Internet. The proposed rules fall far short.

Respectfully Submitted,

Matthew A. Henry
henry@dotlaw.biz
W. Scott McCollough
wsmc@dotlaw.biz
MCCOLLOUGH|HENRY PC
1250 S. Capital of Texas Hwy., Bldg. 2-235
West Lake Hills, TX 78746
Phone: 512.888.1112
July 18, 2014   Fax: 512.692.2522

ATTACHMENT A

NETFLIX THROUGH CONGESTED NETWORK COMPARED TO THROUGH A VPN
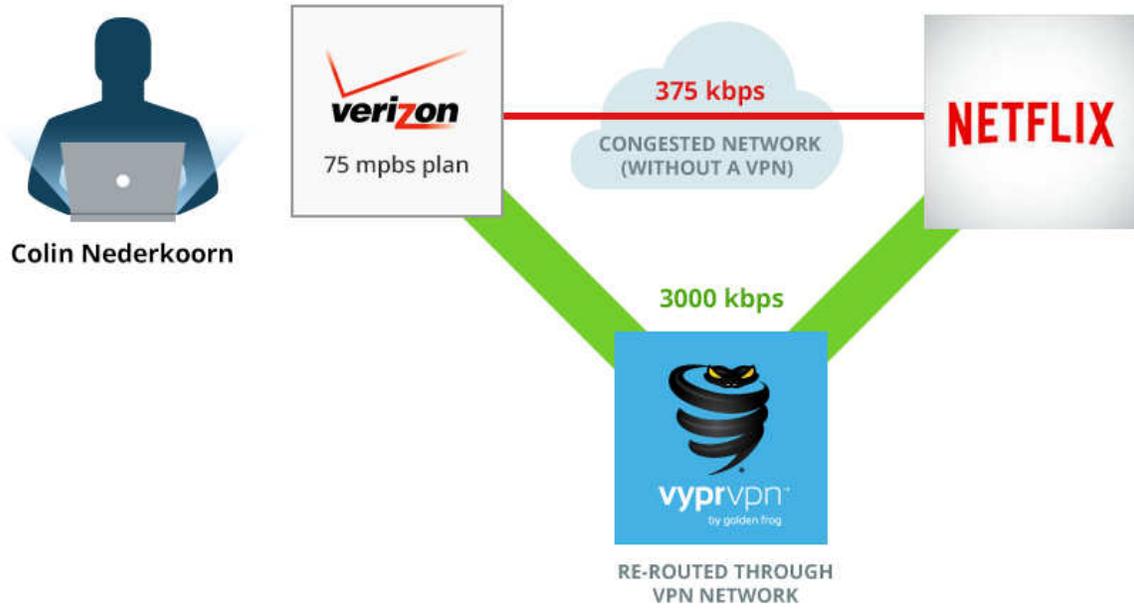
ATTACHMENT B

OVERWRITING STARTTLS ENCRYPTION SESSION INITIATION

A.   Normal STARTTLS Encryption Initiation Response


```
:~$ telnet apps            com 25
Trying         ...
Connected to apps        .com.
Escape character is '^]'.
220 apps            com ESMTP Postfix (Ubuntu)
ehlo dude
250-apps            com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN CRAM-MD5
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
starttls
220 2.0.0 Ready to start TLS
^]close

telnet> close
Connection closed.
        ~$
```

B.   Network-Overwritten STARTTLS Encryption Initiation Response


```
        ~$
        ~$ telnet apps            .com 25
Trying         ...
Connected to apps.        .com.
Escape character is '^]'.
220 *******************************************
ehlo dude
250-apps            .com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-XXXXXXXA
250-AUTH PLAIN CRAM-MD5
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
starttls
502 5.5.2 Error: command not recognized
quit
221 2.0.0 Bye
Connection closed by foreign host.
        ~$
```