An Evaluation of the Effectiveness of ECN with Fallback on the Internet

Linzhi ZOU†, Nonmember, Kenichi NAGAOKA††, and Chun-Xiang CHEN†(a), Members

SUMMARY In this paper, we used the data set of domain names Global Top 1M provided by Alexa to analyze the effectiveness of Fallback in ECN. For the same test server, we first negotiate a connection with Not-ECN-Capable, and then negotiate a connection with ECN-Capable, if the sender does not receive the response to ECN-Capable negotiation from the receiver by the end of retransmission timeout, it will enter the Fallback state, and switch to negotiating a connection with Not-ECN-Capable. By extracting the header fields of the TCP/IP packets, we confirmed that in most regions, connectivity will be slightly improved after Fallback is enabled and Fallback has a positive effect on the total time of the whole access process. Meanwhile, we provided the updated information about the characteristics related to ECN with Fallback in different regions by considering the geographical region distribution of all targeted servers.

key words: congestion control, explicit congestion notification, fallback, effectiveness, connectivity

1. Introduction

The study of TCP congestion control is of great significance to ensure the stability and effectiveness of the Internet.

The mainstream congestion control algorithms are mainly divided into two categories, one is based on packet loss, such as TCP Tahoe, TCP Reno, TCP NewReno [1], CUBIC [2], the other is based on delay, such as TCP Vegas [3] and BBR [4] (BBR is based on delay and the bandwidth of the bottleneck link). However, both have their shortcomings. The former packet loss based scheme will cause the waste of network resources and deteriorate the utilization of network bandwidth. On the other hand, the algorithm based on delay is less aggressive than that based on packet loss, so fairness will be affected.

ECN (Explicit Congestion Notification) is another hopeful approach in which the intermediate routers also participate in congestion control. Combining ECN with AQM (Active Queuing Management) [5], the sender can be notified of the impending congestion in the network by marking packets instead of discarding them, then the sender can actively slow down the transmission rate of TCP to improve the network performance.

Many studies have been done since ECN was proposed. [6] and [7] evaluated the effectiveness of ECN and the benefits of using ECN are summarized in [8]. [9] used a new response strategy in ECN and got improved throughput and reduced fluctuations. [10] used packet capture and traceroute tools to evaluate the congestion safety and fairness of using ECN.

[11], [12] and [13] have given some statistical evaluations on the state of ECN on the Internet. All results show that ECN has not been deployed widely. Moreover, [13] have indicated that the ECN-Capable rates corresponding to different top-level domains are different, which means that when exploring the characteristics related to ECN, it is necessary to take the distribution of test servers into account.

Through the previous works, it is clear what restricts the use of ECN can be narrowed down on two reasons. First, all the routers along the path are required to support ECN. However, there are still many obsolete routers, some of which are incapable of identifying the IP header supporting ECN and may even mangle the ECN field in IP header [10]. Second, some administrative boundaries among networks may block the negotiation of TCP connections supporting ECN. Therefore, if ECN is enabled as default setting at the sender, it is possible that some connections cannot be established.

To show the objective facts with regard to ECN, [12] evaluated the connectivity when using ECN negotiation, but it only obtained the results without considering geographical distinction. Furthermore, [13] analyzed the connectivity and the marginal risk of ECN by comparing ECN-Capable negotiation with Not-ECN-Capable negotiation. However, these works have been conducted based on top-level domains without considering the geographical distribution of the fully qualified domain name (FQDN). Some FQDNs of the targeted servers do not truly correspond to the geographical region (hereafter, the term “region” means geographical region) where the servers are distributed. For example, a server of which FQDN ends with .jp may be distributed out of Japan. So the results based on top-level domains can not represent the actual states with the geographical regions. [14] specified an ECN path capability probing process to check whether the IP layer also supports ECN on the premise that the TCP layer has already given an answer to support ECN. But it is still unclear how the TCP layer supports ECN in different regions.

To provide robust connectivity and mitigate the risk [13] when ECN is enabled, RFC 3168 [15] recommends fallback to non-ECN negotiation if the initial SYN ACK
ECE connection attempt fails, and gives a simple operation scenario of it. The Fallback mechanism is theoretically supposed to stimulate ISPs or vendors to install and enable ECN in their equipment. But how well would the connectivity be improved by Fallback, and how would the connection time change after Fallback is activated? Based on the authors’ knowledge, there have been few studies concerning these issues so far except [16]. [16] did empirical study of the effectiveness of Fallback on the ECN. However, it partially evaluated the effectiveness of Fallback only under the consideration of top-level domains, which has the same shortcomings as in [13]. To reveal the whole state with regard to ECN with Fallback, it is required to take the region distribution of the targeted servers into account, and the impact of Fallback on connection time should be evaluated in details.

This paper gives Fallback a comprehensive explanation, the contributions are shown as follows: (1) We have confirmed that Fallback can improve the connectivity and has a positive impact on the connection time. These two points provide ISPs or vendors with high stimulation to popularize the deployment of ECN in the current network environment. (2) We have quantified the ECN-Capable rates, Fallback rates and the impact of initial retransmission timeout (RTO) on the Fallback rates in different regions. These results show the updated information about the characteristics related to ECN with Fallback, and also can be used as a comparison in the future with the rapid development of the Internet today. (3) We have obtained the packet loss rate of ECN-Capable negotiation and Not-ECN-Capable negotiation respectively. These results are analyzed by directly measuring the servers distributed on the Internet, which demonstrates the actual facts of the effectiveness of ECN.

The rest of this paper is organized as follows. Section 2 explains working principle of ECN. Section 3 describes data set and methodology of measurement. Section 4 demonstrates ECN-Capable rates and Fallback rates among regions. Section 5 presents the analytical results of effectiveness of Fallback. Concluding and outlook are given in Sect. 6.

2. Working Principle of ECN

In order to support ECN, some modifications need to be made in IP and TCP header. The two rightmost bits of the TOS (Type of Service) field in IP header are redefined as the ECN field. The combination of the two bits yields 4 values: 00 indicates that the sender does not support ECN, 01 and 10 indicate ECN support, 11 indicates the impending congestion in the network. The two rightmost bits of the Reserved field in TCP header are modified to CWR (Congestion Window Reduced) and ECE (ECN-Echo), respectively [15].

The general working process of ECN is as follows: (1) When the intermediate router receives a packet belong to a ECN-Capable TCP connection, it determines whether ECN field should be set to 11 based on the current network conditions (for packets that have been set to 11 in ECN field, no longer need to set but continue forwarding). (2) After receiving the packet with ECN field set to 11 in IP header, the TCP receiver sets ECE bit to 1 when sending ACK packet and sets ECE bit of subsequent ACK packets to 1. (3) When the sender receives the ACK packet with ECE bit set to 1, it must reduce its transmission rate and sets CWR bit to 1 when sending next packet. (4) When the receiver receives the packet with CWR bit set to 1, ECE bit of subsequent ACK packets will no longer be set. And the process described above will be repeated when another packet with ECN field set to 11 is received.

3. Data Set and Methodology of Measurement

3.1 Data Set

In order to evaluate the effectiveness of ECN with Fallback, we are going to practically measure the servers distributed on the Internet. To do so, we need a dataset which includes as many entries of the targeted servers as possible. Ideally, the targeted servers should cover the whole Internet, but collecting and testing all the servers on the Internet are almost impossible and unnecessary. Hence, we use a well-known domain names list, published by Alexa Global [17], which includes one million entries of major top domain names and has been widely used by researchers in the related field [18].

Since web servers are the most accessed servers on the Internet and when they are the official web servers of some organizations, they are able to be accessed by HTTP (or HTTPS, Hypertext Transfer Protocol Secure) client almost without any restrictions. Though there are many other kinds of servers on the Internet, such as mail servers, database servers, and so on, testing other types of servers that operate on other protocols is not easy and probably is not allowed. Therefore, We only consider the major web servers as the targeted servers.

We download the Global Top 1M domain names from Alexa [17], and translate every entry in the domain names list to FQDN of the corresponding entry by adding the most popular prefix www. to the head of ever entry [13], then we use Google public DNS (8.8.8.8) to look up the IPv4 (or IPv6) address of every FQDN. After removing the FQDNs which have same IP address, there were 508122 unique FQDN entries left. Then we used the IP geolocation data provided by MaxMind company to analyze the geographical region distribution of the address of each FQDN. We took the top 100000 entries and all these 508122 FQDNs as the targeted web servers in June 2019 and December 2019, respectively. And the analysis in this paper is almost based on the measurement done in December 2019.

We show the results of 31 regions in which the number of FQDNs ending with the top-level domain of this region in unique FQDN entries are greater than 2500 or the number of the targeted web servers distributed in this region are greater than 2500.
3.2 Methodology of Measurement

Two kinds of hosts (called sender) are used in this work (CentOS 6.10 with the customized Linux Kernel 4.9.80 and Fedora Core 30 supporting ECN and Fallback) to perform the testing.

The operations of the test tools used in this work comply with HTTP in accordance with the Fallback example scenario in RFC 3168 [15]. The processes of measurement in sequence are illustrated in Fig. 1.

We first negotiate an HTTP connection with Not-ECN-Capable, of which SYN flag is set only. Then we negotiate an HTTP connection with ECN-Capable to the same server, of which SYN, ECN, CWR flags are set. If the sender does not receive the response to ECN-Capable negotiation from the receiver by the end of retransmission timeout, it will enter the Fallback state, and switch to negotiating a connection with Not-ECN-Capable. When these two negotiations are finished, pick up the IP address of the next FQDN entry and repeat the above procedures. In addition, if a server has IPv4 and IPv6 addresses, we perform two tests and the procedures of IPv6 are same to IPv4.

Note that, Fig. 1 shows the general process. The packets transmitted in some connections may only be a part of it. Moreover, in Not-ECN-Capable negotiation, the response to Not-ECN-setup SYN packet is Not-ECN-setup SYN-ACK packet. And in ECN-Capable negotiation, if the server does not support ECN, the response to ECN-setup SYN packet is Non-ECN-setup SYN-ACK packet.

In order to distinguish the test results clearly, we make a unified description and definition of the situation that will occur in the connection process.

Let \( N_1 \) be the number of targeted web servers, which reply to these two negotiations (Not-ECN-Capable negotiation and ECN-Capable negotiation) at least once. We call them valid servers. Let \( N_2 \) be the number of targeted web servers, which do not reply to either of these two negotiations. We call them invalid servers.

Here we list all possible connection situations in Not-ECN-Capable negotiation and ECN-Capable negotiation separately.

In the Not-ECN-Capable negotiation, after sending the Not-ECN-setup SYN packet, one of the following two situations will occur: (1) The sender receives Not-ECN-setup SYN-ACK packet from the receiver (note that Not-ECN-Capable negotiation is the system’s default way to negotiate a connection, the maximum number of negotiations for establishing a connection to the same server is 3, so the sender has 3 chances to receive the response). The number of such connections is expressed as \( N_{11} \). (2) The sender does not receive any response from the receiver within 3 times of negotiations. The number of such connections is expressed as \( N_{12} \).

In ECN-Capable negotiation, after sending ECN-setup SYN packet, one of the following three situations will occur: (1) The sender receives ECN-setup SYN-ACK packet from the receiver, that means the receiver is ECN-Capable. The number of such connections is noted as \( N_{21} \). (2) The sender receives Non-ECN-setup SYN-ACK packet from the receiver, that means the receiver is not ECN-Capable. The number of such connections is noted as \( N_{22} \). (3) By the end of the retransmission timeout, the sender does not receive any response from receiver. If Fallback is disabled, the sender gives up this negotiation and test next entry. If Fallback is enabled, the connections in case (3) will enter the Fallback state, and negotiate a connection with Not-ECN-Capable, that is, the sender send Not-ECN-setup SYN packet. Note that the connections in case (2) will not enter the Fallback state, since the sender received the response from the receiver, that means the connection has been successfully established. After entering the Fallback state, there may be two situations that are same with the situations in Not-ECN-Capable negotiation, and the numbers of such connections are noted as \( N_{31} \) and \( N_{12} \), respectively.

We use tcpdump to collect TCP/IP packets regarding to all above procedures and use the tool we developed to extract the key information from the header fields of TCP/IP packets.

4. ECN-Capable Rates and Fallback Rates

In this section, we show the updated information about the characteristics related to ECN with Fallback in each region by analyzing the ECN-Capable rates, Fallback rates and the impact of the initial RTO value on Fallback rates.

4.1 ECN-Capable Rates

Fallback is a part of ECN technology. Only when the sender does not receive the response to ECN-Capable negotiation from the receiver by the end of retransmission timeout (in this case, the receiver is considered as not ECN-Capable), it will enter the Fallback state. So we first analyze ECN-Capable rates when Fallback is enabled.

ECN-Capable rate is defined by the proportion of the targeted web servers that are ECN-Capable to the valid servers. According to the definition in Sect. 3.2 it can be calculated by \( \beta_{ecn} = \frac{N_{21}}{N_1} \).

ECN-Capable rates classified by regions are illustrated
in Fig. 2. We can know that in IPv4, for most regions in Europe and North America, their ECN-Capable rates are nearly 90%, which indicates that these regions have a good network environment to support ECN. Therefore, we suggest that ISPs in these regions enable ECN as default setting. However, as for East Asia, the ECN-Capable rates of all regions are less than 80%, which shows that their ECN environment is not very ideal. And the ECN-Capable rates in China, Taiwan and South Korea are even lower than 70%, we suggest that ISPs in these regions open or update equipment that prevent ECN from being enabled, so as to provide a better ECN-Capable environment. Moreover, the ECN-Capable rates of IPv6 are higher than that of IPv4 in most regions, and some regions even reach 100%. However, the ECN-Capable rates of IPv6 are still low in Australia, Spain, Turkey and Taiwan. With the gradual popularization of IPv6, we also suggest that ISPs in these regions increase the deployment of ECN to provide a better supporting environment for IPv6.

4.2 Fallback Rates

Then we analyze the Fallback rate of each region. Intuitively, the connection toward the regions with lower ECN-Capable rate is more likely to enter the Fallback state, while the connection toward the regions with higher ECN-Capable rate is less likely to enter the Fallback state. Here we present the Fallback rates among regions and compare them with ECN-Capable rates.

We tested the targeted web servers under the same data set in June 2019 in three different places: PUH (Prefectural University of Hiroshima, Japan), NIT, IC (National College of Technology, Ishikawa College; Ishikawa, Japan), Chongqing China. We use this result to present the Fallback rates among regions and compare them with ECN-Capable rates.

According to the definition in Sect. 3.2, \( N_{22} + N_{31} \) represents the number of targeted web servers that are not ECN-Capable and \( N_{31} \) represents the number of the connections that entered the Fallback state. As for \( N_{32} \), it stands for the number of the invalid servers, because they did not give response to ECN-Capable negotiation (before Fallback) and Not-ECN-Capable negotiation (after Fallback). The Fallback rate can be calculated by \( \beta_{fb} = N_{31}/(N_{22} + N_{31}) \).

The Fallback rates among regions are shown in Fig. 3. It can be seen that, the results tested in PUH are almost consistent with that in NIT, IC, and it is obvious that the Fallback rate toward China is abnormally high (close to 35%), while the Fallback rates toward other regions are all lower than 5%. And it is strange that in the results tested in China, the rate of Fallback toward China is the lowest, while the rates of Fallback toward other regions are much higher than the results tested in Japan.

From Fig. 2, we have already known that the ECN-Capable rates in East Asia, such as, China, Taiwan and South Korea, are relatively low. However, in Fig. 3, the Fallback rates of the other two regions except China are very low. Therefore, the reason for the low ECN-Capable rate in China is different from the other two regions.

Since targeted web servers we tested are exactly the same, we suspect that the possible reason for this phenomenon may be due to the fact that some accesses are inspected in the cross-border gateways in China, which leads the RTT (Round-Trip-Time) to be longer than retransmission timeout. Because of this, some of the negotiations cannot receive SYN-ACK packet from the receiver by the end of retransmission timeout after sending ECN-setup SYN packet, so the rate of Fallback is increased. On the other hand, in China the accesses from domestic connections do not need to go through such gateways, so there is no extra checking time, which makes Fallback rate low.

4.3 The Impact of the Initial RTO Value on the Behavior of Fallback

If the sender does not receive the response to ECN-Capable negotiation from the receiver by the end of retransmission timeout, it will enter the Fallback state. So the initial RTO (Retransmission Timeout) value has a great influence on the Fallback rate. The default value of RTO is 3 s, and RFC 6298 [19] suggests changing this value to 1 s. In order to get the relationship of the initial RTO value on the behavior of Fallback, we carried out tests with the initial RTO set to 1 s and 3 s. The results are shown in Fig. 4, where \( fb = 1 \) means Fallback is enabled, while \( fb = 0 \) means Fallback is disabled. This definition is also applicable to the following figures.

For almost all the regions, the rates of Fallback when
the initial RTO = 1 s are higher than that when the initial RTO = 3 s. This result is consistent with the theory. There are some connections with ECN-Capable negotiation, in which the receiver possibly replied to the ECN-Capable negotiation, but sender did not receive it by the end of retransmission timeout, so it entered the Fallback state. Setting the initial RTO = 3 s will give SYN-ACK packet more time to return to the sender, so the Fallback rate will be reduced.

At the same time, the difference between these two results can be considered as the rate of connections of which RTTs are greater than 1 s and less than 3 s. RFC 6298 [19] shows that more than 97.5% of the connections observed in a large scale analysis were less than 1 second. But from our statistical results, we can see that there are more than 10.39%, 3.69%, and 6.96% of connections toward China, Iran and Romania with RTT bigger than 1 s. Therefore, changing the initial RTO value from 3 s to 1 s proposed in RFC 6298 may have an adverse effect on the access to these regions.

5. The Effectiveness of Fallback

In this section, we present the analytical results with regard to the effectiveness of Fallback.

5.1 The Impact of Fallback on Connectivity

In this section, we show how the Fallback affects the connectivity to IPv4 and IPv6 targeted web servers among regions.

We define connectivity as the ratio of the number of targeted web servers that reply to ECN-setup SYN packet in ECN-Capable negotiation to the number of valid servers. According to the definition in Sect. 3.2, when Fallback is disabled, the connectivity is calculated by $\beta_{11} = (N_{21} + N_{22})/N_1$, and when Fallback is enabled, the connectivity is calculated by $\beta_{11} = (N_{21} + N_{22} + N_{31})/N_1$. From the definition, we can see that Fallback can improve connectivity. Here we quantify the improvement.

It can be seen from Fig. 5 that in IPv4, before Fallback is enabled, all regions except China have very high connectivity (close to 100%). When Fallback is enabled, the connectivity of these regions has been improved, even though the rates of increase are very low. As regards China, the connectivity has been relatively large improved while Fallback is enabled, but the value is still lower than other regions when ECN is disabled. This situation is same to China and India in IPv6 in Fig. 6. But Fallback has almost no effect on the connectivity to IPv6 targeted web servers in most regions.

5.2 The Impact of Fallback on Connection Time

As seen in previous section, Fallback is able to improve the connectivity more or less. However, Fallback is activated if the sender does not receive the response to ECN-setup SYN packet, it will inevitably increase the time of establishing the connection (called establishment time). In this section, we first investigate the impact of Fallback on establishment time.

5.2.1 Establishment Time

We selected those IPv4 FQDNs which replied response to the sender regardless of using ECN-Capable negotiation or Not-ECN-Capable negotiation from the test done in December, then analyzed the impact of Fallback on establishment time.

The blue data in the Fig. 7 represents the establishment time with Not-ECN-Capable negotiation, that is, the time from sending Not-ECN-setup SYN packet to receiving Not-ECN-setup SYN-ACK packet. The orange data represents the establishment time with ECN-Capable negotia-
tion, that is, the time from sending ECN-setup SYN packet to receiving the response, that is, ECN-setup SYN-ACK or Non-ECN-setup SYN-ACK or Not-ECN-setup SYN-ACK packet (described in Sect. 3.2). Note that, in the last case, the establishment time includes the retransmission timeout.

We first pay attention to Not-ECN-Capable negotiation. Since the source of the connection is from Japan, so the establishment time of the connection toward the targeted web servers distributed in Japan is the lowest, which is consistent with the fact. Starting from Japan, these times to connect to the targeted web servers distributed in Asian regions are basically under 200 ms, but there are relatively big differences in different regions. For example, the establishment times to Singapore, Hong Kong, Taiwan and South Korea are roughly 100 ms, while the establishment times to Thailand and India are close to 200 ms. The establishment times to European regions are basically within 250 ms to 300 ms, and we can see that the establishment times to the regions within Europe are almost the same, which shows that the European network environment is relatively stable. The establishment times to American regions are shorter in the United States and Canada, which are less than 200 ms, while Brazil and Colombia are close to 300 ms. In Oceania region, the establishment time to Australia is about 200 ms. China, Iran, and South Africa have the longest establishment times in all regions, which are close to 400 ms. However, under ECN mechanism, the sender can be notified of the impending congestion in the network by marking packets instead of discarding them, so the packet loss can be mitigated. Since packet loss will cause retransmission, which reduces the throughput efficiency of the network. Because of existence of the Fallback, the more effective congestion mechanism ECN can be activated at first. Thus when analyzing the impact of Fallback on connection time, the influence of ECN can not be ignored. For this reason, we carried out the following tests and compared the packet loss rate of ECN-Capable negotiation and Not-ECN-Capable negotiation in the whole connection process (including data transmission phase) among regions.

5.2.2 Packet Loss Rate

We tested all web servers in unique FQDN entries ten times based on the regions they distributed. Take Japan for example, the number of targeted web servers is 13227, expressed by $N_{total\_Japan}$. The results tested are shown in Table 1.

RRT1_OK means the connections in which the sender received Not-ECN-setup SYN-ACK packet after sending the Not-ECN-setup SYN packet. According to the definition in Sect. 3.2, $N_{11}$ can represent this number.

RRT2_OK means the connections in which the sender received ECN-setup SYN-ACK or Non-ECN-setup SYN-ACK packet after sending the ECN-setup SYN packet. Note that when counting this number, the connections entered the Fallback state cannot be included, because after entering the Fallback state, the received packet is Not-ECN-setup SYN-ACK. According to the definition in Sect. 3.2, this number is calculated by $N_{21} + N_{22}$. We pay attention to the change of RRT2_OK in these ten tests. There are 11512 targeted web servers replied to ECN-Capable negotiation at most, and 11501 targeted web servers replied to ECN-Capable negotiation at least. Since our tests are continuous, it means, within the test period, the state of the targeted web server side can be considered unchanged. Therefore, the change of $max(N_{21} + N_{22}) - min(N_{21} + N_{22}) = 11$ connections’ behavior can only be caused by the change of network environment, and the main reason is due to packet loss. So we consider the value of $\alpha_2 = \frac{max(N_{21} + N_{22}) - min(N_{21} + N_{22})}{N_{total\_Japan}}$ as an approximation of the packet loss rate in the network.

| Test | Packets | $P_{01}$ | $P_{\text{Not ECN}}$ | $P_{02}$ | $P_{\text{ECN}}$ | $P_{03}$ | $P_{\text{Not ECN}}$ | $P_{04}$ | $P_{\text{ECN}}$ | $\gamma_1$ (%) | $RTT1_OK$ | $RTT2_OK$ |
|------|---------|-----------|---------------------|--------|-----------------|--------|---------------------|--------|-----------------|---------------|-----------|-----------|
| test1 | 261025  | 9495      | 8458               | 11     | 5783            | 1.0592 | 37252               | 14     | 0.0376          | 11524         | 11510     | 11510     |
| test2 | 262224  | 9482      | 8311               | 15     | 5773            | 0.9987 | 38246               | 18     | 0.0474          | 11522         | 11508     | 11508     |
| test3 | 263143  | 9496      | 8101               | 8      | 5789            | 0.9084 | 39028               | 6      | 0.0154          | 11521         | 11512     | 11512     |
| test4 | 263136  | 9492      | 8138               | 7      | 5785            | 0.9249 | 38742               | 3      | 0.0077          | 11517         | 11509     | 11509     |
| test5 | 264166  | 9485      | 8004               | 5      | 5770            | 0.8846 | 38089               | 13     | 0.0341          | 11514         | 11510     | 11510     |
| test6 | 263168  | 9491      | 8001               | 6      | 5778            | 0.8802 | 38158               | 24     | 0.0629          | 11517         | 11510     | 11510     |
| test7 | 263093  | 9487      | 7998               | 7      | 5770            | 0.8833 | 37793               | 17     | 0.0450          | 11519         | 11511     | 11511     |
| test8 | 261251  | 9491      | 8017               | 10     | 5780            | 0.8846 | 37896               | 4      | 0.0106          | 11522         | 11510     | 11510     |
| test9 | 263104  | 9493      | 7961               | 4      | 5782            | 0.8638 | 38161               | 10     | 0.0262          | 11513         | 11509     | 11509     |
| test10| 261474  | 9503      | 8016               | 7      | 5795            | 0.8787 | 38040               | 6      | 0.0158          | 11508         | 11501     | 11501     |

![Fig. 7](image-url) Establishment times, IPv4.
As far as RTT1_0K is concerned, the value of \( a_1 = \frac{\text{max}(N_{11}) - \text{min}(N_{11})}{N_{\text{max}} - N_{\text{min}}} \) does not represent the packet loss rate. As described in Sect. 3.2, Not-ECN-Capable negotiation is the system’s default way to negotiate a connection, the maximum number of negotiations for establishing a connection to the same server is 3. So even if the Not-ECN-setup SYN packet is lost within the network, the sender can still make it up for it by retransmission, so \( a_1 = \frac{\text{max}(N_{11}) - \text{min}(N_{11})}{N_{\text{max}} - N_{\text{min}}} \) represents the probability of encountering three-times packet loss in the same connection.

When ECN and Fallback are enabled, ECN-setup SYN packet will not be retransmitted, because after encountering packet loss, the sender enters the Fallback state, and the retransmitted packet is Not-ECN-setup SYN, so only \( a_2 \) can be used as the parameter reflecting the packet loss rate.

Since the time we measured is only the time from sending the SYN packet to the receiving SYN-ACK packet (establishment time), the packet loss rate measured by the above method is only the packet loss rate during the connection establishment phase.

Then we analyzed the data packets captured by Wire-shark in these ten tests, and obtained the packet loss rate of the entire connection process using Not-ECN-Capable negotiation and ECN-Capable negotiation, respectively.

As for Not-ECN-Capable negotiation in Table 1. Let \( P_{01} \) be the total number of Not-ECN-Capable (ECN field in IP header is 0) IPv4 packets related to all connections in a test and let \( P_{02} \) be total number of Not-ECN-Capable retransmitted IPv4 packets related to all connection in a test. So \( P_{02}/P_{01} \) means the retransmission rate of IPv4 packets with Not-ECN-Capable.

Since the retransmission is almost caused by packet loss, it is suitable to take the retransmission rate as the packet loss rate. However, \( P_{02}/P_{01} \) is not enough to stand for packet loss rate. As shown in Sect. 3.2, in our test FQDN entries, there exit some invalid servers, the packets related to these servers should not be considered. Through analysis, we found that, among the targeted web servers distributed in Japan, there are 1665 servers, which give no response to Not-ECN-Capable negotiation and ECN-Capable negotiation in this ten consecutive tests, so these 1665 servers are invalid servers. Let \( P_{\text{none}, \text{all}} \) be the total packets related to these 1665 targeted web servers in a test. Let \( P_{\text{none}, \text{re}} \) be the retransmitted packets related to these 1665 targeted web servers in a test.

Moreover, some retransmission are due to the entering of the Fallback state, that is, the sender did not receive the response to ECN-Capable negotiation, after entering the Fallback state, the Not-ECN-setup SYN packet is sent. Unlike other retransmitted packets, one of the reason for such retransmission is may because the packet is not lost but the sever does not reply for ECN-Capable negotiation. As we can not distinguish the specific retransmission reason of such packets, we calculate the packet loss without considering such packets. The number of such packets, expressed by \( P_{fb} \), is equal to the number of connection which entered the Fallback state in a test (\( N_{11} \)).

So, the specific way to calculate the packet loss rate using Not-ECN-Capable negotiation in a test is \( \gamma_1 = \frac{P_{02} - P_{\text{none}, \text{re}} - P_{fb}}{P_{02} - P_{\text{none}, \text{all}} - P_{fb}} \). Considering ten tests, let the packet loss rate using Not-ECN-Capable negotiation, expressed by \( e_1 \), equal to the average of \( \gamma_1 \).

As for ECN-Capable negotiation, let \( P_{03} \) be the total number of ECN-Capable (ECN field in IP header is not 0) IPv4 packets related to all connections in a test. Let \( P_{04} \) be total number of ECN-Capable retransmitted IPv4 packets related to all connection in a test. Note that ECN field in IP header always is 0 during the establishment phase, the ECN-Capable packet only exits in data transmission phase after the connection is established. So \( \gamma_2 = \frac{P_{04}}{P_{03}} \) is the retransmission rate of IPv4 packets with ECN-Capable in data transmission phase in a test. In order to get the whole packet loss rate of the entire connection process using ECN-Capable negotiation, we need to add \( a_2 \) to \( \gamma_2 \). Considering ten tests, let the packet loss rate using ECN-Capable negotiation, expressed by \( e_2 \), equal to the average of \( (\gamma_2 + a_2) \).

Then we got the results of the packet loss rate by using ECN-Capable negotiation and Not-ECN-Capable negotiation, respectively. For comparison, we ranked Fig. 8 according to the difference between \( e_1 \) and \( e_2 \).

It can be seen from the statistical results in Fig. 8 that among Not-ECN-Capable negotiation, the connection toward Bulgaria has the lowest packet loss rate, with a value of 0.3848% and the connection toward China has the highest packet loss rate, with a value of 11.3650%. Among ECN-Capable negotiation, the connection toward Japan has the lowest packet loss rate, with a value of 0.1134% and the connection toward China has the highest packet loss rate, with a value of 4.6236%.

For 60% of the regions, using ECN-Capable negotiation will result in lower packet loss rate than Not-ECN-Capable negotiation. Then let us focus on regions with large difference. There are 4 regions, Vietnam, South Korea, Russia and Singapore, in which the packet loss rates of ECN-Capable negotiation are 50% higher than that of Not-ECN-Capable negotiation. So as for these 4 regions, Not-ECN-Capable negotiation is a better way to avoid packet loss. There are 16 regions, China, Ukraine, United States, Hong Kong, Japan, Ireland, Thailand, Italy, Turkey, Spain, etc.
France, Canada, United Kingdom, Australia, Poland and Germany, in which the packet loss rates of Not-ECN-Capable negotiation are 50% higher than that of ECN-Capable negotiation. So for these 16 regions, ECN-Capable negotiation is a better way to avoid packet loss.

From the above analysis, we have verified that ECN-Capable negotiation is generally more effective than Not-ECN-Capable negotiation.

In combination with the Figs. 7 and 8, we make a conclusion that although the Fallback mechanism will increase the time for establishing the connection, it is more likely to bring lower packet loss rate. As the time increased to establish connection is relatively small, which is far less than the retransmission time after packet loss, we assess that Fallback has a positive effect on the total time of the whole access process.

6. Concluding and Outlook

Congestion control on the Internet has been a challenge for a long time. Researchers have been working hard to deal with it and constantly developing new schemes. Having to take the compatibility with the current Internet and ease of implementation into consideration, they have proposed most of their schemes based on packet-loss or packet-delay or the combination. Furthermore, these schemes cannot reflect the timely congestion state on the Internet. So ECN has been the most promising scheme yet, which has been recognized by the Internet industry.

To show the latest state concerning ECN with Fallback and to provide helpful references to ISPs and vendors, in this paper, we analyzed the effectiveness of Fallback and quantified the characteristics related to ECN in different regions by doing an experimental measurement. We used the one million domain name entries provided by Alexa, and made up the dataset of the targeted web servers.

For the same targeted web server, we first negotiated a connection with Not-ECN-Capable, and then negotiated a connection with ECN-Capable, if the sender did not receive the response to ECN-Capable negotiation from the receiver by the end of retransmission timeout, it would enter the Fallback state, and switched to negotiating a connection with Not-ECN-Capable.

We got the conclusions as following. (1) European and North American regions have higher ECN-Capable rates, and the regions with lower ECN-Capable rates are mostly distributed in East Asia. (2) The rates of Fallback among different regions are a bit different, and the Fallback rate toward China has opposite features to other regions. (3) In most regions, connectivity will be slightly improved after Fallback is enabled and Fallback has a positive effect on the total time of the whole access process. (4) The value of initial RTO has a strong impact on the Fallback rate toward China, Iran and Romania, as there is still a relatively large rate of connection with RTT in the range of 1 s to 3 s in these regions.

In this work, the dataset of the targeted servers we used only contains the major web servers obtained from the 1M top domain provided by Alexa. The results suitably reflect the state of ECN with Fallback at these servers. In the future work, we will collect the dataset that cover more minor servers and make the results more universal.

Acknowledgments

The authors would like to thank the editor and anonymous reviewers for their helpful comments and suggestions, which improved this paper.

References

[1] S. Floyd and T. Henderson, “The NewReno modification to TCP’s fast recovery algorithm,” RFC 2582, April 1999.
[2] I. Rhee, L. Xu, S. Ha, A. Zimmermann, L. Eggert, and R. Scheffenegger, “CUBIC for fast long-distance networks,” RFC 8312, Feb. 2018.
[3] L.S. Brakmo and L.L. Peterson, “TCP Vegas: End to end congestion avoidance on a global Internet,” IEEE J. Sel. Areas Commun., vol.13, no.8, pp.1465–1480, Oct. 1995.
[4] M. Claypool, J.W. Chung, and F. Li, “BBR - An implementation of bottleneck bandwidth and round-trip time congestion control for ns-3,” Proc. 10th Workshop on ns-3 (WNS3), pp.1–8, June 2018.
[5] F. Baker and G. Fairhurst, “IETF recommendations regarding active queue management,” RFC 7567, July 2015.
[6] S. Floyd, “TCP and explicit congestion notification,” ACM Computer Communication Review, vol.24, no.5, pp.8–23, Oct. 1994.
[7] J. Hadi Salim and U. Ahmed, “Performance evaluation of explicit congestion notification (ECN) in IP networks,” RFC 2884, July 2000.
[8] G. Fairhurst and M. Welzl, “The benefits of using explicit congestion notification (ECN),” RFC 8087, March 2017.
[9] M. Kwon and S. Fahmy, “TCP increase/decrease behavior with explicit congestion notification (ECN),” IEEE International Conference on Communications, New York, NY, USA, April 2002.
[10] S. Bauer, R. Beverley, and A. Berger, “Measuring the state of ECN readiness in servers, clients, and routers,” Proc. 11th ACM SIGCOMM/USENIX Internet Measurement Conference (IMC 2011), pp.171–180, Berlin, DE, Nov. 2011.
[11] M. Kühlwind, S. Neuner, and B. Trammell, “On the state of ECN and TCP options on the Internet,” International Conference on Passive and Active Measurement, PAM 2013, pp.135–144, 2013.
[12] B. Trammell, M. Kühlwind, D. Boppart, I. Learmonth, G. Fairhurst, and R. Scheffenegger, “Enabling Internet-wide deployment of explicit congestion notification,” Proc. 16th International Conference, PAM 2015, New York, NY, USA, Lecture Notes in Computer Science, vol.8995, pp.193–205, March 2015.
[13] C.-X. Chen and K. Nagaoka, “Analysis of the state of ECN on the Internet,” IEICE Inf. & Syst., vol.E102-D no.5, pp.910–919, May 2019.
[14] M. Kuehlwind and B. Trammell, “A mechanism for ECN path probing and fallback,” draft-kuehlwind-tcpm-ecn-fallback, Internet-Draft, Sept. 2013.
[15] K. Ramakrishnan, S. Floyd, and D. Black, “The addition of explicit congestion notification (ECN) to IP,” RFC 3168, Sept. 2001.
[16] L.Z. Zou, C.-X. Chen, and K. Nagaoka, “An empirical study of the effectiveness of fallback on the ECN,” NOMS 2020, Budapest, Hungary, pp.1–4, April 2020 (DOI: 10.1109/NOMS47738.2020.9110403).
[17] https://s3.amazonaws.com/alexa-static/top-1m.csv.zip
[18] Q. Scheitle, O. Hohlfeld, J. Gamba, J. Jelten, T. Zimmermann, S.D. Strowes, and N. Vallina-Rodriguez, “A long way to the top: Significance, structure, and stability of Internet top list,” IMC ’18.
[19] V. Paxson, M. Allman, J. Chu, and M. Sargent, “Computing TCP’s retransmission timer,” RFC 6298, June 2011.

Linzhi Zou received B.E. degree from Southwest JiaoTong University, Sichuan, China in 2019. He is now studying for the master degree at Prefectural University of Hiroshima, Hiroshima, Japan. His current research interests include the measurement and the management of network environment.

Kenichi Nagaoka received his B.E. and M.E. degrees from Kanazawa University in 1990 and 1992, respectively. From 1992 to 2001, he was an assistant professor and from 2001 to 2013, was an instructor in the department of electronics and information engineering at National Institute of Technology, Ishikawa College. Since 2014, he has been an associate professor at National Institute of Technology, Ishikawa College. His current research interests include performance evaluation of communication networks, QoS on the Internet and educational technology. He is a member of IEICE of Japan and IEEE.

Chun-Xiang Chen received M.E. and Ph.D. degrees from Kanazawa University and Osaka University, Japan, in 1991, 1994, respectively. From 1994 to 1996, he was an assistant professor in the Department of Computer Engineering at Hiroshima City University, Japan. From 1997 to 2005, he was an Associate Professor at Hiroshima Prefectural University. From 2006 to 2007, he was an Associate Professor at Prefectural University of Hiroshima. Since April 2008, he has been a Professor at Prefectural University of Hiroshima, Hiroshima, Japan. His current research interests include performance evaluation of communication networks, congestion control with TCP, multiple-traffic control on multiple-channel systems and QoS on the Internet. He is a member of the IPS, IEICE of Japan and the IEEE Communications society.