Case Studies of Using the Gigabit-compatible Protocol Checker as a Troubleshooting Tool for Home IP Systems

Abstract

This article introduces case studies of using the gigabit-compatible protocol checker as a troubleshooting tool for home Internet protocol (IP) systems. It is the thirteenth in a bimonthly series on the theme of practical field information about telecommunication technologies. This month's contribution is from the Network Interface Engineering Group, Technical Assistance and Support Center, Maintenance and Service Operations Department, Network Business Headquarters, NTT EAST.

1. Introduction

Customer needs are changing as access lines become faster and a wide range of application services come to be provided. There is demand for high-quality Internet protocol (IP) services with even higher levels of reliability than in the past. However, the range of configuration patterns for IP equipment within customers' residences has been growing. As a result, the Technical Assistance and Support Center has been receiving many inquiries concerning faults having low reproducibility, such as ones that occur once a day or once a week, as well as enquiries about unusual faults for which a solution cannot be found without analyzing the packets flowing in the customer's home network.

This article presents case studies of using the gigabit-compatible protocol checker, which can easily capture the packet data needed for fault analysis.

2. Overview of gigabit-compatible protocol checker

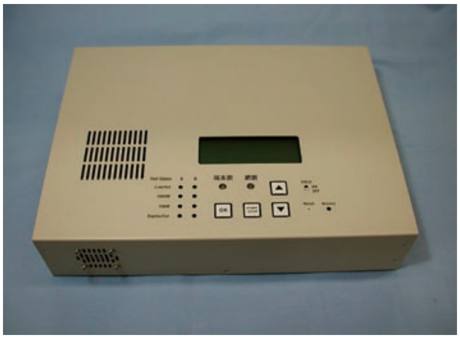


Fig. 1. External view of gigabit-compatible protocol checker.

The gigabit-compatible protocol checker (**Fig. 1**) [1] has two local area network (LAN) ports for mirroring and one LAN port for management. It can be installed within the Ethernet segment in a residence as a packet-capture tool that obtains packet data and stores it in a built-in memory. Although it is compact, it provides long-term file acquisition and storage so it is effective for low-reproducibility faults because it can capture data when the fault reappears; the captured data can be analyzed using a LAN analyzer such as Wireshark. Its main functions are: support for packet capture at about 200 Mbit/s over gigabit Ethernet, an operation panel for starting and stopping packet capture without the need to attach a personal computer (PC), and support for remote control from a maintenance center and automatic transfer of data.

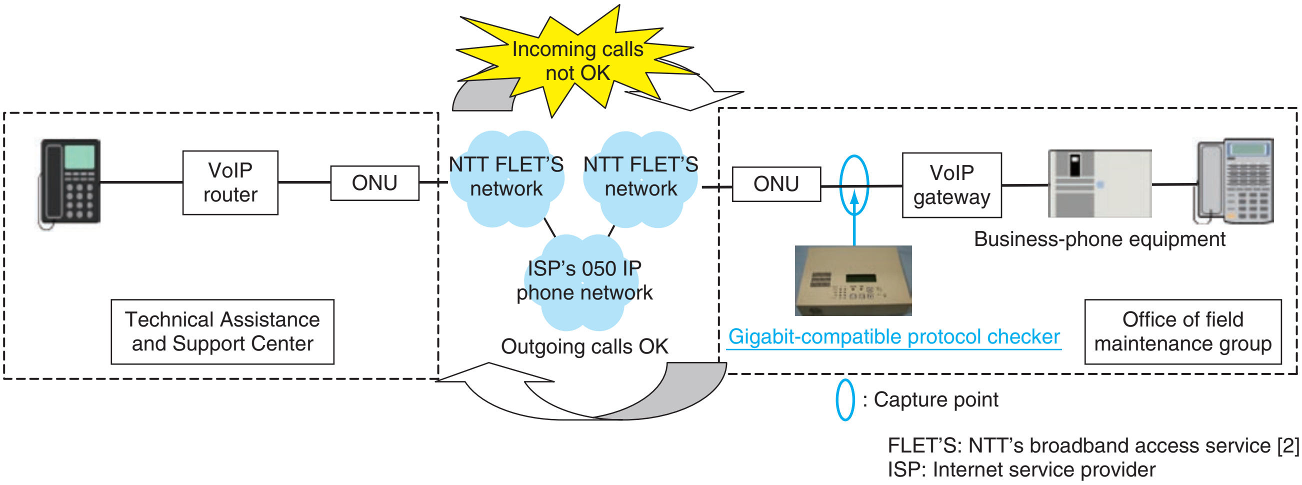

Incoming calls not OK
VoIP router
ONU
NTT FLET'S network
NTT FLET'S network
ISP's 050 IP phone network
ONU
VoIP gateway
Business-phone equipment
Technical Assistance and Support Center
Outgoing calls OK
Gigabit-compatible protocol checker
Office of field maintenance group
: Capture point
FLET'S: NTT's broadband access service [2]
ISP: Internet service provider

Fig. 2. Customer's home configuration and measurement system.

3. Case studies

3.1 Incoming calls disabled on 050 IP phone service

3.1.1 Description of fault

A customer using NTT EAST's B FLET'S service and an ISP's 050 IP phone service upgraded the VoIP-gateway from model A to model B, but then found that incoming calls were disabled even though outgoing calls could be made as usual (VoIP: voice over IP). At the time of the fault, the party making the call simply heard a busy signal although the receiving party (the NTT customer) was not using the line. Even when the new model-B gateway equipment was replaced, the problem persisted.

3.1.2 Inspection method

To troubleshoot this problem, we duplicated the customer's system configuration in the office of a field maintenance group and conducted a test to inspect calls made from the Technical Assistance and Support Center to that office. In this test, we inserted the gigabit-compatible protocol checker between the optical network unit (ONU) and the VoIP gateway in the customer's premises to analyze call conditions at the time of the fault (incoming calls not OK) and we investigated any differences in the session initiation protocol (SIP) sequence for two cases: (1) when the VoIP gateway was model A and (2) when it was model B. The test setup is shown in **Fig. 2**.

3.1.3 Inspection results

We found that calls could be received normally when the VoIP gateway was model A (**Fig. 3**). However, when it was model B, after returning a 100Trying message in response to an INVITE message from the receive-side SIP server, the gateway returned an

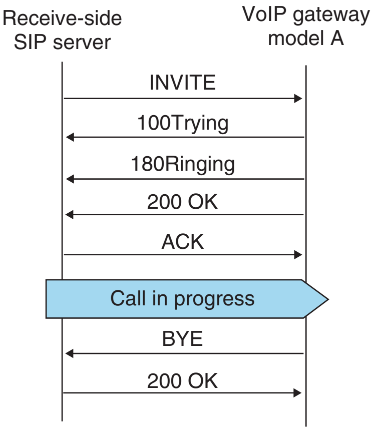


Fig. 3. Incoming-calls OK sequence.

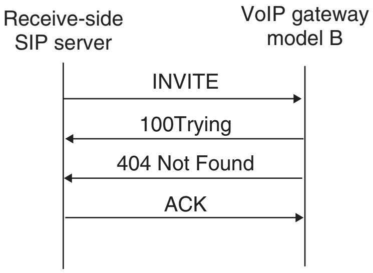
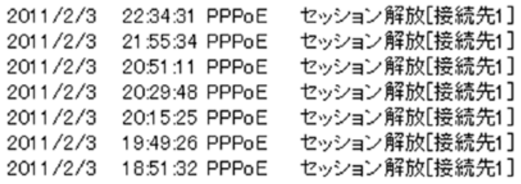


Fig. 4. Incoming-calls not OK sequence.



```
2011/2/3   22:34:31 PPPoE    セッション解放[接続先1]
2011/2/3   21:55:34 PPPoE    セッション解放[接続先1]
2011/2/3   20:51:11 PPPoE    セッション解放[接続先1]
2011/2/3   20:29:48 PPPoE    セッション解放[接続先1]
2011/2/3   20:15:25 PPPoE    セッション解放[接続先1]
2011/2/3   19:49:26 PPPoE    セッション解放[接続先1]
2011/2/3   18:51:32 PPPoE    セッション解放[接続先1]
```

Fig. 5. Router log.

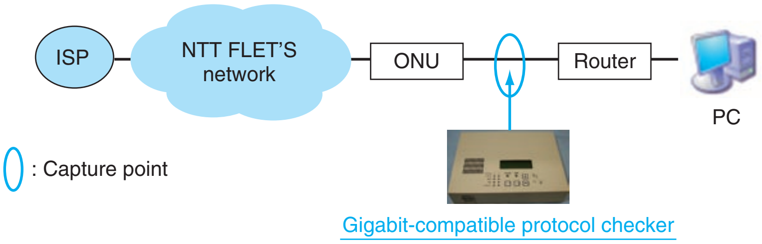


Fig. 6. Customer's home configuration and measurement system.

error "404 Not Found" (**Fig. 4**). This error is returned whenever the called party cannot be detected, which means that the model-B VoIP gateway had judged that the terminal targeted by the incoming call did not exist.

3.1.4 Cause of fault

The results of this inspection led us to consider that although the model-B VoIP gateway received the dial-in number contained in the INVITE message, it could not recognize the terminal targeted by it and returned "404 Not Found". When the model-B VoIP gateway was designed, no assumptions were made about the provider of the 050 IP telephone services; consequently, the maintenance manual did not describe how to set the additional dial-in numbers for a particular provider. This lack of settings caused this problem.

3.1.5 Countermeasure and results

We solved this problem by creating settings for additional dial-in numbers in the model-B VoIP gateway. We also concluded that no problems occurred with incoming calls in the model-A VoIP gateway because it does not refer to settings of additional dial-in numbers in the INVITE message of the ISP's 050 IP phone service.

3.2 Occasionally slow Internet access

3.2.1 Description of fault

A customer using a FLET'S optical line reported that Internet access slowed down sometimes. Upon checking the customer's router log, we found frequent occurrences of the message "PPPoE[*1] session released" (**Fig. 5**). Even when the router and ONU were replaced and the accommodation line was changed, the problem remained.

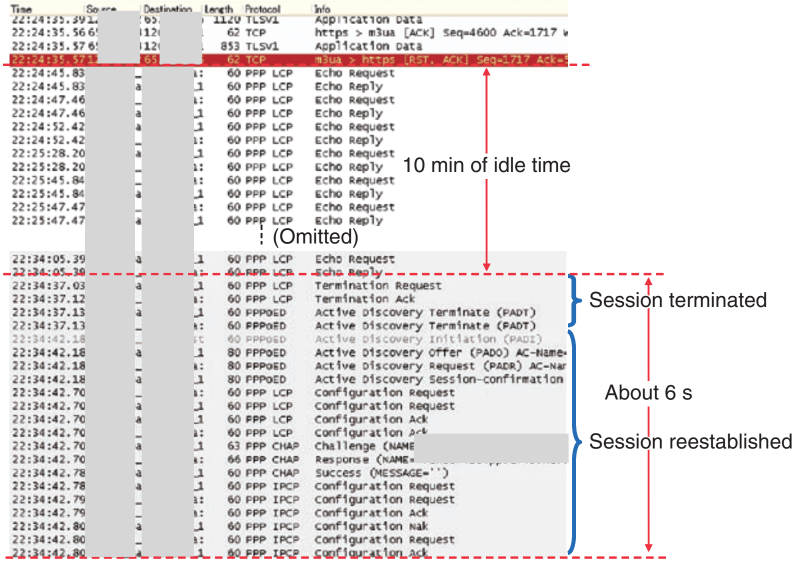
3.2.2 Inspection method

We inserted the gigabit-compatible protocol checker between the ONU and router installed in the customer's residence and proceeded to capture and analyze packets. The system configuration at that time is shown in **Fig. 6**.

3.2.3 Inspection results

Upon analyzing the router log and data captured at the time of this phenomenon, we found that the reception of a PPP (point-to-point protocol) Termination Request from the network side was followed by a PPPoE Active Discovery Termination (PADT) request. Furthermore, upon checking the packet data captured at times other than when this phenomenon occurred, we found that in all cases the reception of a PPP Termination Request was preceded by an idle state with the Internet service provider (ISP) lasting about 10 minutes (**Fig. 7**).

[*1] PPPoE: Point-to-point protocol (PPP) over Ethernet; a protocol specifically for establishing, setting, and terminating a PPP session between an access concentrator and a terminal device on an Ethernet network.



```
Time        Source      Destination  Length Protocol  Info
22:24:35.39 [redacted]  [redacted]   1120 TLSv1       Application Data
22:24:35.56 [redacted]  [redacted]     62 TCP         https > m3ua [ACK] Seq=4600 Ack=1717 W
22:24:35.57 [redacted]  [redacted]    853 TLSv1       Application Data
22:24:35.57 [redacted]  [redacted]     62 TCP         m3ua > https [RST, ACK] Seq=1717 Ack=
22:24:45.83 [redacted]  [redacted]     60 PPP LCP     Echo Request
22:24:45.83 [redacted]  [redacted]     60 PPP LCP     Echo Reply
22:24:47.46 [redacted]  [redacted]     60 PPP LCP     Echo Request
22:24:47.46 [redacted]  [redacted]     60 PPP LCP     Echo Reply
22:24:52.42 [redacted]  [redacted]     60 PPP LCP     Echo Request
22:24:52.42 [redacted]  [redacted]     60 PPP LCP     Echo Reply
22:25:28.20 [redacted]  [redacted]     60 PPP LCP     Echo Request
22:25:28.20 [redacted]  [redacted]     60 PPP LCP     Echo Reply
22:25:45.84 [redacted]  [redacted]     60 PPP LCP     Echo Request
22:25:45.84 [redacted]  [redacted]     60 PPP LCP     Echo Reply
22:25:47.47 [redacted]  [redacted]     60 PPP LCP     Echo Request
22:25:47.47 [redacted]  [redacted]     60 PPP LCP     Echo Reply

22:34:05.39 [redacted]  [redacted]     60 PPP LCP     Echo Request
22:34:05.39 [redacted]  [redacted]     60 PPP LCP     Echo Reply
22:34:37.03 [redacted]  [redacted]     60 PPP LCP     Termination Request
22:34:37.12 [redacted]  [redacted]     60 PPP LCP     Termination Ack
22:34:37.13 [redacted]  [redacted]     60 PPPoED      Active Discovery Terminate (PADT)
22:34:37.13 [redacted]  [redacted]     60 PPPoED      Active Discovery Terminate (PADT)
22:34:42.18 [redacted]  [redacted]     60 PPPoED      Active Discovery Initiation (PADI)
22:34:42.18 [redacted]  [redacted]     80 PPPoED      Active Discovery Offer (PADO) AC-Name=
22:34:42.18 [redacted]  [redacted]     80 PPPoED      Active Discovery Request (PADR) AC-Nar
22:34:42.18 [redacted]  [redacted]     80 PPPoED      Active Discovery Session-confirmation
22:34:42.70 [redacted]  [redacted]     60 PPP LCP     Configuration Request
22:34:42.70 [redacted]  [redacted]     60 PPP LCP     Configuration Request
22:34:42.70 [redacted]  [redacted]     60 PPP LCP     Configuration Ack
22:34:42.70 [redacted]  [redacted]     60 PPP LCP     Configuration Ack
22:34:42.70 [redacted]  [redacted]     63 PPP CHAP    Challenge (NAME[redacted]
22:34:42.70 [redacted]  [redacted]     66 PPP CHAP    Response (NAME=[redacted]
22:34:42.78 [redacted]  [redacted]     60 PPP CHAP    Success (MESSAGE='')
22:34:42.78 [redacted]  [redacted]     60 PPP IPCP    Configuration Request
22:34:42.79 [redacted]  [redacted]     60 PPP IPCP    Configuration Request
22:34:42.79 [redacted]  [redacted]     60 PPP IPCP    Configuration Ack
22:34:42.80 [redacted]  [redacted]     60 PPP IPCP    Configuration Nak
22:34:42.80 [redacted]  [redacted]     60 PPP IPCP    Configuration Request
22:34:42.80 [redacted]  [redacted]     60 PPP IPCP    Configuration Ack
```

Fig. 7. Captured data.

3.2.4 Cause of fault

The PPPoE session was terminated when the idle state with the ISP lasted longer than 10 minutes, and it took about 6 seconds for the session to be reestablished. Therefore, we concluded that the customer would have experienced a slow response when attempting to access the Internet during this 6-s period.

3.2.5 Coping

When we contacted the customer's ISP, we were advised that a PPP session is terminated if the idle time exceeds 10 minutes to prevent unnecessary distribution of global IP addresses. We therefore told the customer that the problem was not caused by NTT equipment and we asked the customer to consult with the ISP.

3.3 Failure of LAN communications between fax and PC

3.3.1 Description of fault

A customer with a home fax machine receives images via a FLET'S optical line and uses a function for automatically transferring those images from the fax to a PC via a LAN. The customer reported that this transfer occasionally failed. Replacing devices within the customer's home did not solve the problem.

3.3.2 Inspection method

To examine the image-data transmission conditions between the fax and PC, we inserted a gigabit-compatible protocol checker between the fax and switch in the customer's home and analyzed the captured data. The system configuration at that time is shown in **Fig. 8**.

3.3.3 Inspection results

Upon analyzing the captured data, we found that communications between the fax and PC were conducted in the form of a TCP (transmission control protocol) session. During normal operation, the session was established on the basis of a TCP 3-way handshake[*2] (**Fig. 9**) and communications proceeded without any problems. However, when the fault occurred, no Syn/Ack packets were returned from the PC in response to a Syn packet sent from the fax. As a consequence, no session was established and normal communications were not performed. Data captured during normal operations is shown in **Fig. 10** and data captured when the fault occurred is shown in **Fig. 11**.

3.3.4 Cause of fault

Upon inspecting the customer's PC, we found that the firewall settings of the security software installed on it had been modified from their standard values: the settings closed the TCP port, which disrupted communications.

3.3.5 Countermeasure and results

The firewall settings modified by the customer

[*2] 3-way handshake: A procedure for establishing a connection in TCP. The name derives from the fact that packets are passed three times, as shown in Fig. 9.

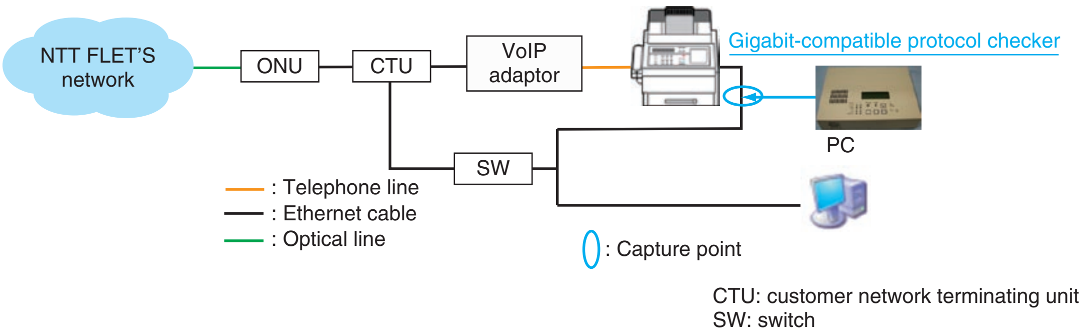


Fig. 8.   Customer's home configuration and measurement system.

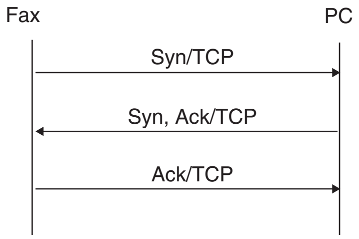
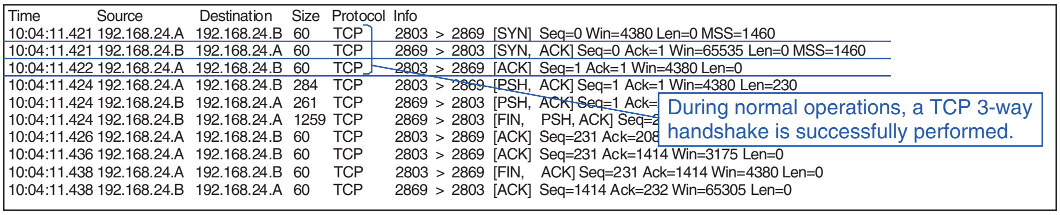


Fig. 9.   TCP 3-way handshake.

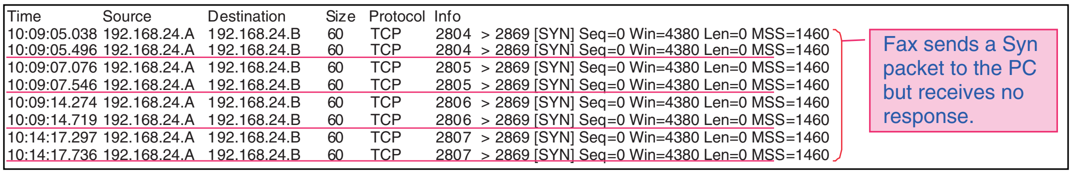


```
Time          Source        Destination   Size  Protocol Info
10:04:11.421 192.168.24.A  192.168.24.B   60    TCP      2803 > 2869  [SYN]  Seq=0 Win=4380 Len=0 MSS=1460
10:04:11.421 192.168.24.B  192.168.24.A   60    TCP      2869 > 2803  [SYN,  ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
10:04:11.422 192.168.24.A  192.168.24.B   60    TCP      2803 > 2869  [ACK]  Seq=1 Ack=1 Win=4380 Len=0
10:04:11.424 192.168.24.A  192.168.24.B   284   TCP      2803 > 2869  [PSH,  ACK] Seq=1 Ack=1 Win=4380 Len=230
10:04:11.424 192.168.24.B  192.168.24.A   261   TCP      2869 > 2803  [PSH,  ACK] Seq=1 Ack=
10:04:11.424 192.168.24.B  192.168.24.A   1259  TCP      2869 > 2803  [FIN,   PSH, ACK] Seq=2
10:04:11.426 192.168.24.A  192.168.24.B   60    TCP      2803 > 2869  [ACK]  Seq=231 Ack=208
10:04:11.436 192.168.24.A  192.168.24.B   60    TCP      2803 > 2869  [ACK]  Seq=231 Ack=1414 Win=3175 Len=0
10:04:11.438 192.168.24.A  192.168.24.B   60    TCP      2803 > 2869  [FIN,   ACK] Seq=231 Ack=1414 Win=4380 Len=0
10:04:11.438 192.168.24.B  192.168.24.A   60    TCP      2869 > 2803  [ACK]  Seq=1414 Ack=232 Win=65305 Len=0
```

During normal operations, a TCP 3-way handshake is successfully performed.

*IP addresses are partially shown. 192.168.24.A: FAX, 192.168.24.B: PC

Fig. 10.   Fax LAN port communications during normal operations.



```
Time          Source        Destination    Size  Protocol  Info
10:09:05.038 192.168.24.A  192.168.24.B    60    TCP       2804  > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
10:09:05.496 192.168.24.A  192.168.24.B    60    TCP       2804  > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
10:09:07.076 192.168.24.A  192.168.24.B    60    TCP       2805  > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
10:09:07.546 192.168.24.A  192.168.24.B    60    TCP       2805  > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
10:09:14.274 192.168.24.A  192.168.24.B    60    TCP       2806  > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
10:09:14.719 192.168.24.A  192.168.24.B    60    TCP       2806  > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
10:14:17.297 192.168.24.A  192.168.24.B    60    TCP       2807  > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
10:14:17.736 192.168.24.A  192.168.24.B    60    TCP       2807  > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
```

Fax sends a Syn packet to the PC but receives no response.

*IP addresses are partially shown. 192.168.24.A: FAX, 192.168.24.B: PC

Fig. 11.   Fax LAN port communications at time of fault occurrence.

were restored to their standard values. This action eliminated the fault.

4. Concluding remarks

This article presented case studies of using a gigabit-compatible protocol checker to troubleshoot faults. Packet analysis is becoming an essential tool for investigating IP-related faults, and it is hoped that the reader has found the case studies described here to be informative and useful.

References

[1] "Gigabit-compatible Protocol Checker," NTT Technical Review, Vol. 10, No. 7, 2012.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201207fa3.html

[2] FLET'S services. http://flets.com/english/