

VOCORD AntiFraud

Fraud Counteraction System for Network Providers

The goal of fraud counteraction in a transit network

The architecture of transit network and the building technologies applied fully determine the attitude towards organization of a fraud counteraction system in this network. The following factors can explain the complexity of the solution for this problem:

1. There are no commutation centres in SDH network. All communication centres and all multiplexers are in fact commutation centres.
2. Technical capabilities of the network equipment allow to organize channels with quite wide interface (joint) range. As the clients of a transit provider can order organization of a channel with almost any of the possible joint types, the provider must support all these interface types.
3. According to the business model defined by recently introduced in RF "Rules of Providing Long Distance Telephony Services" and "Rules of Providing IP telephony Services", a transit provider has to make contracts on affiliation of local network providers to his network with mentioning of the service types that a local network provider has a right to use. I.e. according to the "Rules" a local provider has to get corresponding licenses and different terms of affiliation to a transit network for different service types.

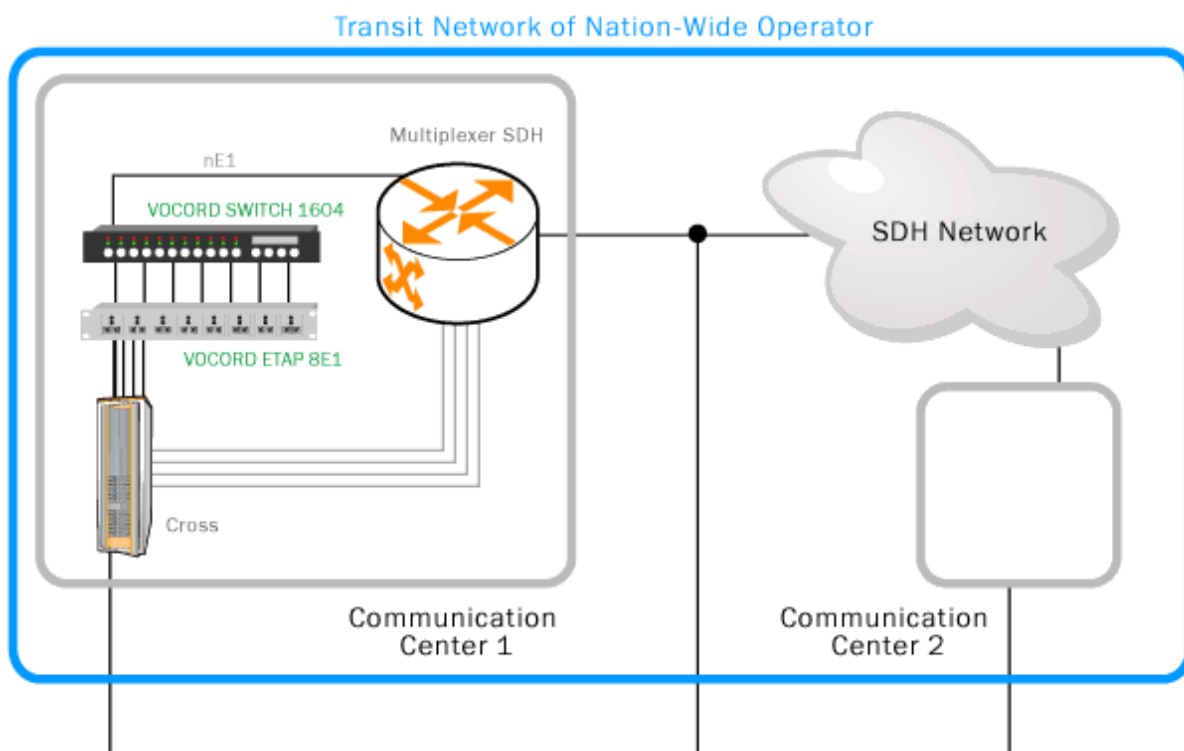


Consequently, a transit provider MUST control that the local provider fulfills the terms of affiliation contract:

1. Make affiliation contracts with local operators only for those services that he has licenses for.
2. Control the list of services ("communication services") that are carried out on the channel leased by the affiliated provider.
3. Have objective technical control facilities.

Solving the problem of fraud counteraction in a transit network

To solve the problem of fraud counteraction in a transit network a mobile deployable software-hardware system VOCORD AntiFraud is offered. Let us look through a typical startup and operation circuit for VOCORD AntiFraud SHS:



On a communication centre of a transit operator a block of non-destructive VOCORD ETAP branchers is set; they are serially connected to all channels that come to a multiplexer.

Let us assume that we need to organize control of a leased channel between “X-Telecom” and “Y-Infocom”. Branched traffic is transmitted to a channel commutation device VOCORD Switch, which is operated remotely and allows to chose any incoming channel from the Monitoring Centre and direct it to the outgoing channel. Then the traffic from the VOCORD Switch output is directed through free (reserved) multiplexer interfaces over the transit network of the operator to the Monitoring Centre. In the Monitoring Centre all the branched traffic is analyzed on the VOCORD AntiFraud HSS within the period of time needed; during this operation structure of the branched traffic, data and service types of the channel are determined.

As a result of processing the “measurements” VOCORD AntiFraud reports the structure of the telecommunication traffic:

- Number of transmitted bytes for each protocol group;
- For telematic IP telephony services a complete report is given as a list of IP telephony connections with mentioning “A” and “B” telephone numbers and other identifiers;
- For telematic short message services a complete report is given as a list of SMS connections with mentioning “A” and “B” telephone numbers and other identifiers.

Main capabilities of VOCORD AntiFraud HSS

- synchronous recording of signals of 1....8 channels simultaneously;
- automated analysis of structured and unstructured streams G.703;
- random selection of groups of time intervals for data traffic analysis;
- automated selection of most probably used telephony signaling protocols: ISDN PRI, SS7 (subsystem ISUP), R2, CC5;
- automated selection of transport protocol for transmission of IPv4 packets: Cisco HDLC, FrameRelay, PPP;
- estimation of the number of SMS transmission sessions in GSM networks with interactions between operators (ASE-SMS);
- decoding of IP telephony sessions according to H.323 v.2 standards and SIP.