
# Case Communications Xmas 2006 Newsletter

**Case Communications Xmas 2006 Newsletter**

**In this Issue:**



**Archives**

**Read the back issues**

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

**Subscribe FREE**

**Sign-up for the newsletter**

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe/Unsubscribe]**

**Feedback**

**Tell us your thoughts**

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/Enquiry]**

## Welcome,

Welcome to Case Communications December 2006 Newsletter. With the short month and festive season in mind we have kept this newsletter shorter and a little more light hearted than usual.

We wish all our readers a very Merry Xmas and Propserous New Year

### Flatulence prompts jet to make emergency landing

An American Airlines flight made an emergency landing on Monday after a passenger with severe gas problems struck matches to mask the odour of flatulence, an official said.
**[More]**

### An Overview of STUN

STUN (Simple Traversal of User Datagram Protocol (UDP)
**[More]**

### Case Communications provide Selex Communications with Radio Over IP equipment.

When SELEX-Communications, a Finmeccanica company, won a contract to provide a Radio Trunked Network in Romania, they spoke to Case Communications about using the Case's KMX technology, which the two companies had so successfully used in their Radio Trunked Network previously.
**[More]**

### The Japanese use RFID to track their children

The authorities in the Japanese city of Osaka decide tracking is best way to protect kids
**[More]**


Case Communications Xmas 2006 Newsletter



**Archives**

**Read the back issues**

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

**Subscribe FREE**

**Sign-up for the newsletter**

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe/ Unsubscribe]**

**Feedback**

**Tell us your thoughts**

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/ Enquiry]**

# Flatulence prompts jet to make emergency landing

An American Airlines flight made an emergency landing on Monday after a passenger with severe gas problems struck matches to mask the odour of flatulence, an official said.

The flight from Washington to Texas landed at Nashville airport, in the south-eastern state of Tennessee, after passengers alerted the crew about the smell of burning sulfur, Lynne Lowrance, spokeswoman for the Nashville International Airport Authority said.

She said all 99 passengers and their luggage were taken off the plane and searched, and an unlucky canine team was brought in to sniff the aircraft for explosives.

After intense questioning by the FBI, a woman passenger admitted to lighting matches on board the aircraft to conceal her gas, Lowrance said.

"For a long time she did not admit to striking matches and I think that was just out of embarrassment," she said. "She did finally admit to it saying she had a medical problem about excessive gas."

The unidentified woman was not charged but "American did ban her from flying on their airline for a very long time," Lowrance said.

Story courtsey of

The Sydney Morning Herald


Case Communications Xmas 2006 Newsletter

**Case Communications Xmas 2006 Newsletter**

**In this Issue:**



**Archives**

**Read the back issues**

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

**Subscribe FREE**

**Sign-up for the newsletter**

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe/ Unsubscribe]**

**Feedback**

**Tell us your thoughts**

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/ Enquiry]**

# An Overview of STUN

STUN (Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)) is a network protocol allowing a client behind a NAT (or multiple NATs) to find out its public address, the type of NAT it is behind and the internet side port associated by the NAT with a particular local port. This information is used to set up UDP communication between two hosts that are both behind NAT routers. The protocol is defined in RFC 3489.

STUN is a client-server protocol. A VoIP phone or software package may include a STUN client, which will send a request to a STUN server. The server then reports back to the STUN client what the public IP address of the NAT router is, and what port was opened by the NAT to allow incoming traffic back in to the network.

The response also allows the STUN client to determine what type of NAT is in use, as different types of NATs handle incoming UDP packets differently. It will work with three of four main types: Full Cone, Restricted Cone, and Port Restricted Cone. (In the case of Restricted Cone or Port Restricted Cone NATs, the client must send out a packet to the endpoint before the NAT will allow packets from the endpoint through to the client.) STUN will not work with Symmetric NAT (also known as bi-directional NAT) which is often found in the networks of large companies. With Symmetric NAT, the IP address of the STUN server is different than that of the endpoint, and therefore the NAT mapping the STUN server sees is different than the mapping that the endpoint would use to send packets through to the client. For details on the different types of NAT, see network address translation.

Once a client has discovered its external addresses, it can relate it to its peers. If the NATs are full cone then either side can initiate communication. If they are restricted cone or restricted port cone both sides must start transmitting together.

Note that using the techniques described in the STUN RFC does not necessarily require using the STUN protocol; they can be used in the design of any UDP protocol.

Protocols like SIP use UDP packets for the transfer of sound/video/ text signaling traffic over the Internet. Unfortunately as both endpoints are often behind NAT, a connection cannot be set up in the traditional way. This is where STUN is useful.

An example of a well-known VoIP application that uses STUN is Google Talk, which interoperates with STUN servers situated in Google's datacenters.

The STUN server is contacted on UDP port 3478, however the server will hint clients to perform tests on alternate IP and port number too (STUN servers have two IP addresses). The RFC states that this port and IP are arbitrary.

STUN uses the following algorithm (adapted from RFC 3489) to discover the presence of NAT gateways and firewalls:

Where the path through the diagram ends in a red box, UDP communication is not possible. Where the path ends in a yellow or green box, communication is possible.

**STUN DEFINITION**

STUN (Simple Traversal of UDP through NATs (Network Address Translation)) is a protocol for assisting devices behind a NAT firewall or router with their packet routing

**Note:** The STUN RFC states: *This protocol is not a cure-all for the problems associated with NAT.*

- STUN enables a device to find out its public IP address and the type of NAT service its sitting behind
- STUN operates on TCP and UDP port 3478.
- STUN is not widely supported by VOIP devices yet.

- STUN may use DNS SRV records to find STUN servers attached to a domain. The service name is _stun._udp or _stun._tcp

**Definitions (from the RFC)**

**STUN Client:** A STUN client (also just referred to as a client) is an entity that generates STUN requests. A STUN client can execute on an end system, such as a user's PC, or can run in a network element, such as a conferencing server.

**STUN Server:** A STUN Server (also just referred to as a server) is an entity that receives STUN requests, and sends STUN responses. STUN servers are generally attached to the public Internet

**Various types of NAT (still according to the RFC)**

**Full Cone:** A full cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

**Restricted Cone:** A restricted cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Unlike a full cone NAT an external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X.

**Port Restricted Cone:** A port restricted cone NAT is like a restricted cone NAT, but the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P.

**Symmetric:** A symmetric NAT is one where all requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used.

Furthermore, only the external host that receives a packet can send a UDP packet back to the internal host.

**Closing words ( from the RFC)**

The problems with STUN are not design flaws in STUN. The problems in STUN have to do with the lack of standardized behaviours and controls in NATs. The result of this lack of standardization has been a proliferation of devices whose behaviour is highly unpredictable, extremely variable, and uncontrollable. STUN does the best it can in such a hostile environment Ultimately, the solution is to make the environment less hostile, and to introduce controls and standardized behaviours into NAT. However, until such time as that happens, STUN provides a good short-term solution given the terrible conditions under which it is forced to operate.


Case Communications Xmas 2006 Newsletter

**Case Communications Xmas 2006 Newsletter**

**In this Issue:**



**Archives**

**Read the back issues**

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

**Subscribe FREE**

**Sign-up for the newsletter**

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe/ Unsubscribe]**

**Feedback**

**Tell us your thoughts**

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/ Enquiry]**

# Case Communications provide Selex Communications with Radio Over IP equipment.

When SELEX-Communications, a Finmeccanica company, won a contract to provide a Radio Trunked Network in Romania, they spoke to Case Communications about using the Case's KMX technology, which the two companies had so successfully used in their Radio Trunked Network previously.

Their customer liked the Time Division Multiplexing technology, but asked if it was possible to provide a technology that was more 'Future-Proof' and also highly cost effective.

Case Communications saw their Viper (Voice Over IP Router) as being the ideal platform for connecting the Radio Base stations to the main switch site, as it was both Future Proof, highly flexible and cost effective.

A Radio Trunked network has different requirements to VoIP (Voice Over-IP), which meant the standard Viper routers would require several changes to make the system operate successfully with Radio. Some of these changes are;

· Radio has no call 'set up' or 'tear down'; the channels are 'Always-On'.

· The network needed to support FFSK (Fast Frequency Shift Key) technology.

· Base Station to the main switch communications was via a continuous HDLC stream.

Case Communications developed software to handle the 'Always-on' requirement and used the Viper G.729 compression to compress the radio channel down to 9Kbps. The FFSK channel was supported using 32Kbps ADPC.

A Case Communications Multi-Access Router (A Router designed to handle non IP protocols over IP) was used to transport an HDLC stream between the main switch site and each of the base stations.

Initial testing in the SELEX Communications laboratories proved the technology, and ironed our any problems. One major change was that the equipment was to be installed in remote mountain sites and where the power supply was 24 volts DC and this meant every component of the network had to be developed to support 24 Volts DC.

One other key difference between RoIp and VoIP is 'Silence Suppression. While both systems save bandwidth using silence suppression, its usual to output a sample of background sounds, so the VoIP telephone user knows the circuit is still open, and the person at the remote site has not 'hung up'.

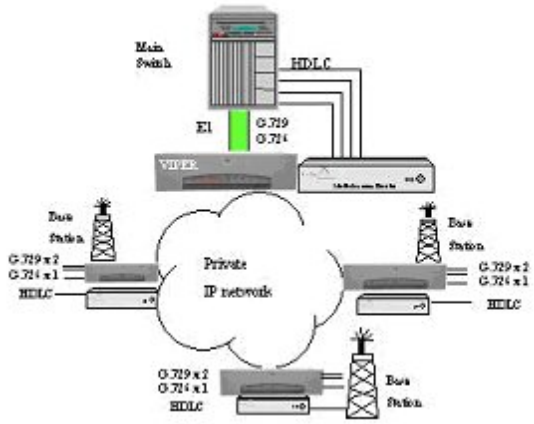
In RoIP this background sound becomes amplified by the Radio system, especially when operating in broadcast mode, where one

channel is copied to multiple other channels, therefore the Viper silence suppression was enabled, but the background sound generation was set to complete silence.

Having proved the technology in the laboratories the entire system was shipped to Romania and installed in the mountains.

The installation went very smoothly and voice quality was comparable to the original KMX TDM system, but at a much lower cost. Typical bandwidth to each site is 59Kbps, with 2 x G.729 channels, 1 x 32 Kbps ADPCM channel and 9600Bps for the HDLC stream. Quality of Service mechanisms provide automatic fragmentation and give high priority traffic priority over less time critical traffic.

The diagram below provides a simplified overview of the Radio Trunked Network, showing a ‘Head-End’ master switch communicating with remote Base Station sites.




The new network continues to roll out and provides a highly cost effective and reliable transport mechanism to support the Romanian Radio Trunked Network.


Case Communications Xmas 2006 Newsletter



**Archives**

**Read the back issues**

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

**Subscribe FREE**

**Sign-up for the newsletter**

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe/ Unsubscribe]**

**Feedback**

**Tell us your thoughts**

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/ Enquiry]**

# The Japanese use RFID to track their children

The rights and wrongs of RFID-chipping human beings have been debated since the tracking tags reached the technological mainstream. Now, school authorities in the Japanese city of Osaka have decided the benefits outweigh the disadvantages and will now be chipping children in one primary school.

The tags will be read by readers installed in school gates and other key locations to track the kids' movements.

The chips will be put onto kids' schoolbags, name tags or clothing in one Wakayama prefecture school. Denmark's Legoland introduced a similiar scheme last month  last month to stop young children going astray.

RFID is more commonly found in supermarket and other retailers' supply chains, however, companies are now seeking more innovative ways to derive value from the tracking technology. US airline Delta recently announced it would be using RFID to track travellers luggage.

**Passports:**
Another controversial application  is soon-to-be mandatory use of RFID in passports. The US is leading the way in deployments and the UK isn't far behind.

As well as the obvious privacy fears that surround such rollouts, experts have questioned how secure the passports are with some claiming to have cracked and cloned them already.