**The Internet at Sea: Advanced Routing Protocol Techniques for Maintaining Robust Connectivity Aboard Research Vessels**

**INTRODUCTION**

Keeping research vessels connected to the Internet, especially at sea via satellite, is an ongoing challenge. Due to the extreme dynamic nature of ship position and heading, weathersea state, satellite occlusion due to ship superstructure, as well as transitioning between geostationary satellites, the logistics of achieving a consistent and cost-effective Internet communications presence aboard a vessel are complex. We have overcome these obstacles by presenting consistent, stable interfaces and multiple routes between a shipboard and land-based router.

**EXAMPLE OF A HYBRID SETUP**

One link is a route-reflected, direct-routing setup (HiSeasNet-IOR). The other is a generically tunneled setup thr

**G O A L S**

In order to present a stable Internet presence aboard a moving vessel:

- Integrate any and all mobile Internet Service Provider (ISP) links available such that all available links may be used in an ISP selection process. Example ISP links are HiSeasNet (HiSeasNet, 1500 VSW), FleetBroadband (FBB, Ship to Ship to Shore Wireless Access Protocol [SWAP], 3G data plans (temporary for foreign port calls, or permanent for regional vessels), Foreign visitors’ networks (wire or WiFi, E.G. shoreyards or other UNOLS plans).

- Seamless fail-over between ISP links during link outages.
  - User experience is enhanced when downloads, real-time video feeds, and performance-enhancing tunnels may all be maintained, despite a sudden change of ISP. This creates a stable ship/shore communications environment, much like a terrestrial ISP.
  - By unifying all mobile connections to the HSN router, preserve performance-enhancing features such as Carrier-grade routing protocols, seamless fail-over between ISPs eliminates the need for any specialized solution.

- Always use preferred path when available.
  - Cost and speed are key issues. Any shore-based link when a ship is at a pier is likely to have better throughput, latency and packet delivery characteristics than satellites.
  - HiSeasNet has a more predictable usage model than FBB. Therefore, to be fair to the user, tailored logic in place to use the “right” link when multiple are available.

- Tailor ingress/egress to a rate suitable for each link, E.G. throttle FBB rate so that it can both remain usable, yet endure sustained use without causing undue budget overruns, or prevent ‘chaty’ protocols from hogging any one link’s bandwidth.

- Ability to operate through a third party ISP to the HSN earth station.
  - Ability to route from a third-party site, so normal UNOLS vessels’ routing may be handed invisibly, and as effective, as well as simple as direct routing (E.G. Indian Ocean Region [IOR] ISPS).

- Automatically route when moving between HSN leased satellites. Use a “hands-off” routing setup, so that only the radio gear need be adjusted.

**TECHNICAL CONSIDERATIONS**

- **The Maximum Transmission Unit (MTU) must be accounted for on each link.** Ethernet standard MTU is 1500 Bytes, but most ISPs use slightly less than this. Should the MTU be mismatched, packet fragmentation issues may render the link unusable. If the MTU is too small, the extra packets make a less efficient link. If paying per bit across this link, this is an issue.

- The link should avoid additional packet overhead across the satellite whenever possible. Therefore, MTU should be accounted for on each link.

- Where direct routing is not practical, tunneling can help. At the sacrifice of a little MTU. Static Generic Routing Encapsulation (GRE) is effective, easy to setup, stable, and incurs minimal overhead per packet (24 bytes), it requires a static setup on both ends and is the least flexible.

- GRE/Tunnel Resolution Protocol (NHRP) allows an arbitrary raw link to become routable to a static ISP. This is more flexible, but it does not work with any Network Address Translation (NAT) setup.

- IPsec tunneling protocols are most useful for encrypting all traffic, and can originate from arbitrary ISP addresses. Use of this technique, however, it has more overhead (48 bytes) and is more complex to troubleshoot.

**FUTURE DIRECTIONS**

- Fully explore IPsec, for better NAT traversal mechanisms. This allows for secure, more reliable tunneling over arbitrary ISPs.

- Explore alternate routing setups:
  - Combining route premises for better more throughput through multiple ISPs, as available/practical
  - Explore Enhanced Interior Gateway Routing Protocol (EIGRP) instead of BGP for faster route convergence (less disruptive triggering) when mobile links are failing often/quickly

- Use different BGP Autonomous System (AS) processes, to take advantage of long lasting eBGP dampening — so that we do not use a buddy healing link until it has stabilized for 15+ minutes.

- Tailor traffic Quality of Service (QoS) on a per-tunnel basis, to suit particular tunnel’s needs. E.G. allow bursts, but limit over throughput of a FBB tunnel to something that will not result in burdensome link that when used continuously for days.

- Incorporate a shore-side, web filtering interception proxy. This offers high-level HTTP traffic shaping and blacklisting of HTTP traffic — our largest consumer — on a per-link basis, to invisibly suit the practical needs and limits of each link.

- Incorporate Cisco Performance Routing service into the automated route choosing mechanism. Using this technology, a 3G link that is barely in-range (thus performing poorer than a 3G link) should not be chosen over a satellite link that is stable.

- Add shore-side authenticating Captive Portal. This will allow user-level control and user-level documentation of link use.

**A P P R O A C H**

Together, the following components allow a pair of routers to dynamically decide which routing path to use in order to forward packets.

Quick decision-making is critical as one or more paths disappear. Should a router be colocated in a non-HSN teleport, we also have the ability to use BGP to inform multiple earth station routers of various paths available for a particular ship. The dynamic nature of this setup, allows us to seamlessly populate our satellite links as the ship approaches land, using cellular modems, land lines, or WiFi hotspots.

**REFERENCES**

- Fuchsstadt, Germany
- MTU 1500
- Cisco 281
- VHF
- FBB
- Smartphone
- Unsatellite
- ISP
- NA
- UNOLS
- NAT
- GRE
- MTU
- NHRP
- GRE

**CONTACT INFORMATION**

Joe C. Meyer (meyer@ucsd.edu), Shipboard Technical Support – Scripps Institution of Oceanography

Steve Foley (sfoley@ucsd.edu), Institute of Geophysics and Planetary Physics – Scripps Institution of Oceanography

**Example of a hybrid setup. One link is a route-reflected, direct-routing setup (HiSeasNet-IOR). The other is a generically tunneled setup through FleetBroadband. Two or more links to the same router provide robust, redundant underway Internet connectivity.**