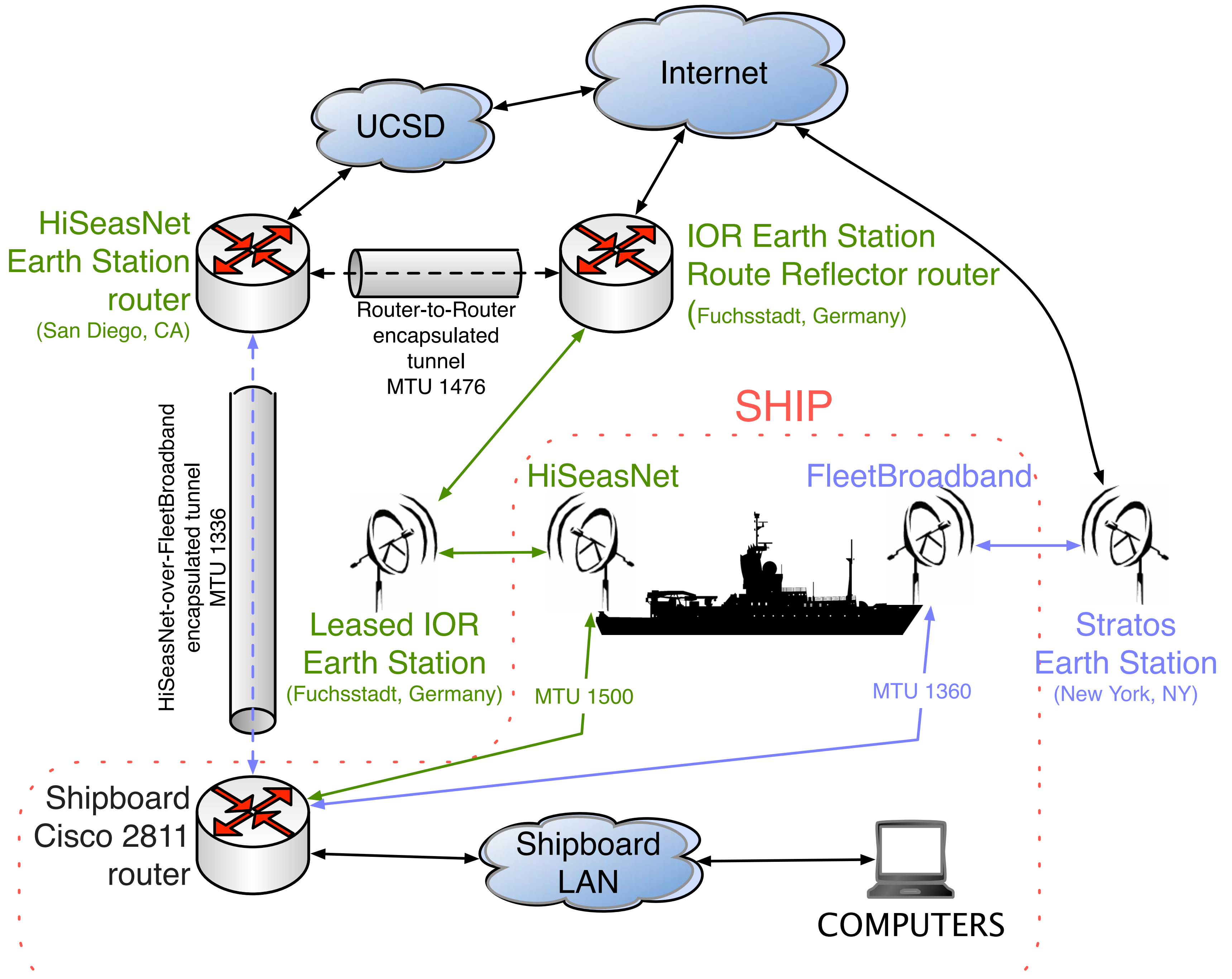
The Internet at Sea: Advanced Routing Protocol Techniques for Maintaining Robust Connectivity Aboard Research Vessels

Jon C. Meyer (jmeyer@ucsd.edu), *Shipboard Technical Support – Scripps Institution of Oceanography*

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

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, weather/sea state, satellite occlusion due to ship superstructure, as well as transiting between geostationary satellites, the logistics of achieving a consistent, constant 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.


Internet
UCSD
HiSeasNet Earth Station router
(San Diego, CA)
Router-to-Router encapsulated tunnel MTU 1476
IOR Earth Station Route Reflector router
(Fuchsstadt, Germany)
SHIP
HiSeasNet-over-FleetBroadband encapsulated tunnel MTU 1336
HiSeasNet
FleetBroadband
Leased IOR Earth Station
(Fuchsstadt, Germany)
MTU 1500
MTU 1360
Stratos Earth Station
(New York, NY)
Shipboard Cisco 2811 router
Shipboard LAN
COMPUTERS

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

GOALS

In order to present a stable Internet presence aboard a moving vessel, we need to meet the following goals:

- **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 (HSN)*, *FleetBroadband (FBB)*, *Ship to Ship/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. shipyards or other UNOLS piers).
- **Seamless fail-over between ISP links during link outages.**
  - User experience is enhanced when downloads, realtime data 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 land-based installation.
  - By unifying all mobile connections to the HSN router, preserve performance-enhancing Accelerator tunnel, regardless of ISP link.
- **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 delay variation characteristics than satellite-based links. HSN has a more predictable usage model than FBB. So, there needs to be intelligent, 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 useable, yet endure sustained use without causing undue budget overruns, or prevent "chatty" 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 handled invisibly, and as effectively as practical (E.G. *Indian Ocean Region (IOR)* ISPs).
- **Ability to automatically route when moving between HSN leased satellites.** Use a "hands-off" routing setup, so that only the radio gear need be adjusted.

APPROACH

Together, the following components allow a pair of routers to dynamically decide which routing path to use in short order. 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 between the Internet and ship. The dynamic nature of this setup, allows us to seamlessly supplant our satellite links as the ship approaches land, using cellular modems, land lines, or WiFi hotspots.

- **A ship-based router with multiple connections to multiple ISPs.** Each ISP connection contains a direct link to the HSN router.
- **A combination of direct routing, *Generic Routing Encapsulation (GRE)*, and *Virtual Private Network (VPN)* tunneling.** Use of static real-world IP addresses on the ship's end simplifies setup and minimizes overhead, but is not always available from some ISPs, hence the need for a few different approaches.
- **Networks traditionally advertised solely over HSN are advertised over all available links,** so that each side of the link is concurrently aware of any and all paths to/from the ship. This is done via a dynamic routing protocol such as *Border Gateway Protocol (BGP)*. Use of this dynamic routing protocol to toggle connections between ISPs allows the ship to use the preferred connection (for cost, stability, delay, etc.).
- **Unified routing advertisements mean that shipboard IP addresses are maintained during toggling.** Consistent IP addresses ensure that higher level activity, such as TCP sessions (E.G. downloads, chat clients) and performance-improving devices (E.G. hardware accelerators), invisibly survive a toggle between ISPs.

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 the link, this is an issue.
- **The link should avoid additional packet overhead across the satellite wherever possible.** Therefore, MTU should be a high as practical.
- **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). However, it requires a static setup on both ends and is the least flexible. GRE +Next Hop Resolution Protocol (NHRP) allows an arbitrary real-world IP address to tunnel to a static IP. This is more flexible, but it does not work with any Network Address Translation (NAT) setup. GRE +IPsec tunneling provides the security of encrypting all traffic and, can originate from arbitrary IP addresses, even behind NAT gateways. 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 paths 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 toggling) 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 badly behaving link until it has stabilized for 15+ minutes.
- **Tailor traffic *Quality of Service (QoS)* on a per-tunnel basis, to suit a particular tunnel's needs.** E.G. allow bursts, but limit over throughput of a FBB tunnel to something that will not result in burdensome bill 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 traffic 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 satellite link) would not be chosen over a satellite link that is stable.
- **Add shore-side authenticating Captive Portal.** This would allow user-level control and user-level documentation of link use.