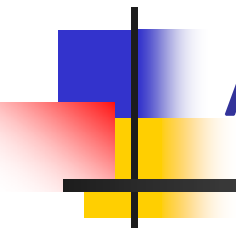
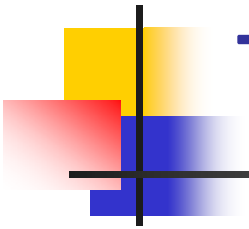


Approaches to Multi6

An Architectural View of Multi6 proposals

Geoff Huston

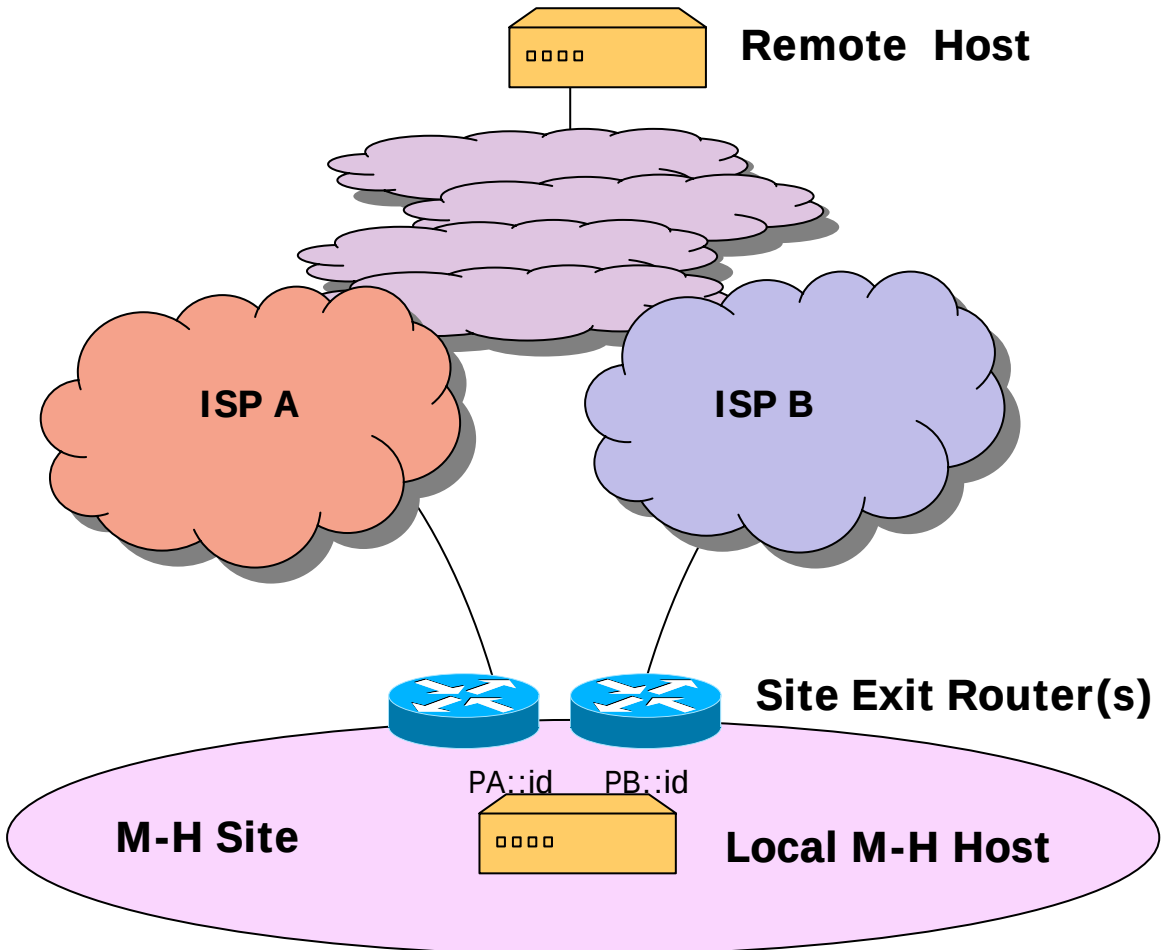
March 2004



The Objective

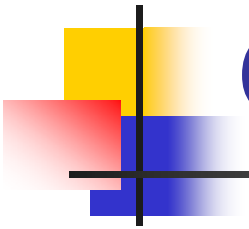
- The desire is to generate a taxonomy of approaches to multi-homing in V6
- The taxonomy is to be based on an architectural analysis of the solution space
- Individual approaches can then be analysed against this architectural taxonomy

The Problem Space



Functional Goals

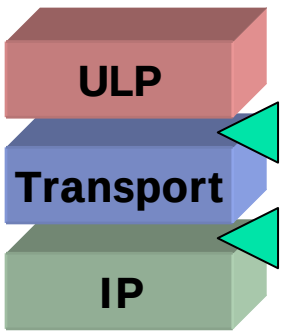
- RFC3582 enumerates the goals as:
  - Redundancy
  - Load Sharing
  - Traffic Engineering
  - Policy
  - Simplicity
  - Transport-Layer Surviveability
  - DNS compatibility
  - Filtering Capability
  - Scaleability
  - Simplicity
  - Legacy compatibility
- draft-lear includes some 30 additional questions relating various aspects of the proposals in the areas of:
  - Interaction with routing
  - Aspects of an ID/Locator split, if used
  - Changes to packets on the wire
  - Names, Hosts, endpoints and the DNS



Generic Approaches:

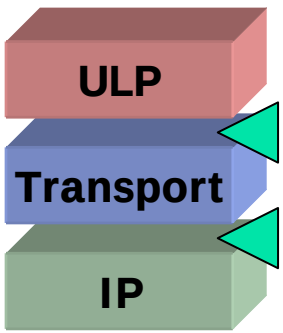
- Insert a new level in the protocol stack (identity element)
  - New protocol element
- Modify the Transport or IP layer of the protocol stack in the host
  - Modified protocol element
- Modify the behaviour of the host/site exit router interaction
  - Modified forwarding architecture

New Protocol Element



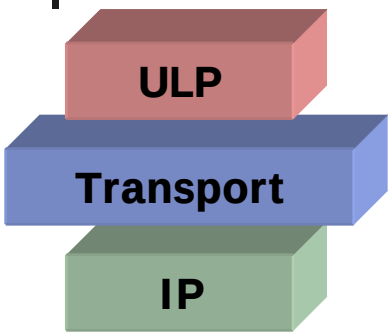
- Define a new Protocol element that:
  - presents an identity-based token to the upper layer protocol
  - Allows multiple IP address locators to be associated with the identity
  - Allows sessions to be defined by an identity peering, and allows the lower levels to be agile across a set of locators

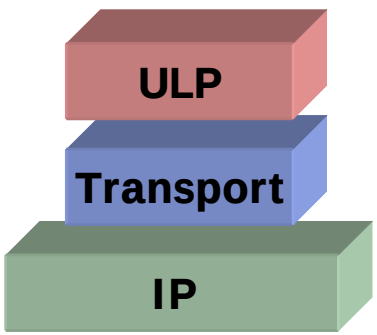
Protocol Element Implementation



- "Conventional"
  - Add a wrapper around the upper level protocol data unit and communicate with the peer element using this "in band" space
- "Out of Band"
  - Use distinct protocol to allow the protocols element to exchange information with its peer
- "Referential"
  - Use a reference to a third party point as a means of peering (e.g. DNS Identifier RRs)

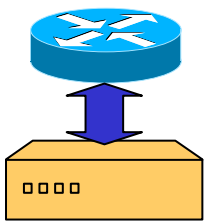
Modified Protocol Element Behaviour





- Alter the Transport Protocol to allow a number of locators to be associated with a session
  - *e.g.* SCTP
- Alter the IP protocol to support IP-in-IP structures that distinguish between current-locator-address and persistent-locator-address
  - i.e. MIP6

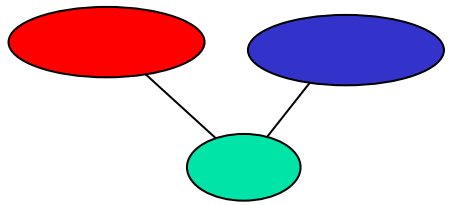
Modified Host / Router Interaction



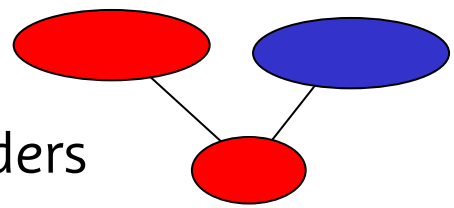
- Modify the interaction between the host and the Site Exit router to allow:
  - Source-based routing for support of host-based site-exit router selection
  - Site Exit router packet header modification
  - Host / Site Exit Router exchange of reachability information

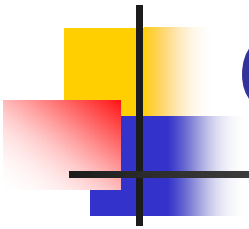
None of the above: Mapping to IPv4 Status Quo to IPv6

- Such as:
  - Obtain a local AS
  - Obtain PI space
  - Advertise the PI space to all upstream providers
  - Follow routing



- Or:
  - Use PA space from one provider
  - Advertise it to all other upstream providers
  - Follow routing

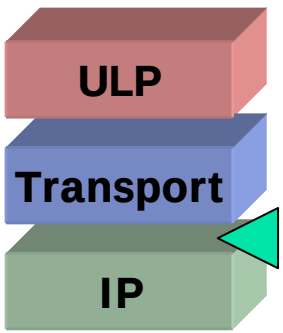




Common Issues

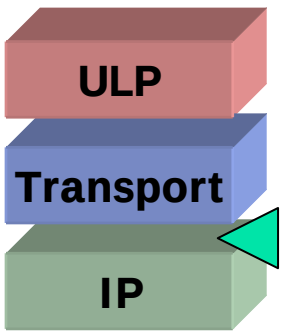
- Host based locator address selection
  - How to pick the “best” source locator for the reverse packet?
  - How to pick the “best” destination locator if there are more than one available?
- Detection of network element failure
  - How to detect reverse path failure?
- Session Persistence
  - How and when to switch locators for active sessions ?

Proposals for a new Protocol Element



- HIP:
  - Shim between Transport and IP layer
  - Presents a stable identity to the transport layer
  - Allows multiple locators to be bound to the identity, and communicates this binding to the remote end (HIP protocol)
  - Allows the local host to switch source locators in the event of network failure to ensure session survivability

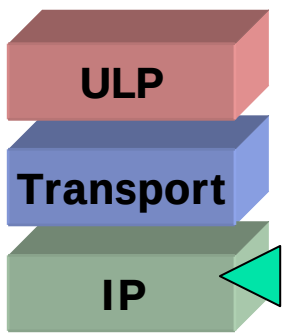
Proposals for a new Protocol Element



- NOID +
- SIM (CBID 128) +
- CB64:
  - Addition of an identifier shim layer to the protocol stack.
  - The identifier / locator mapping may be contained in the DNS (NOID) or may be contained within a protocol exchange (SIM), or a hybrid approach (CB64)
  - Permits Site Exit routers to rewrite source locators on egress
    - (i.e. includes elements of host / Site Exit Router interaction)

Identity Protocol Element Location

- It appears that the proposals share a common approach:
  - Above the IP forwarding layer (Routing)
  - Below IP fragmentation and IPSEC (IP Endpoint)



Proposals for an Identity Protocol Element

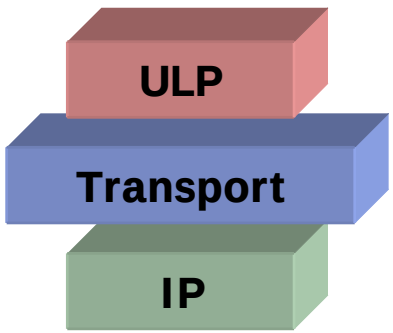
Hierarchically Structured Space

- Use identity tokens lifted from a protocol's "address space"
  - DNS, Appns, Transport manipulate an "address"
  - IP functions on "locators"
  - Stack Protocol element performs mapping
- FQDN as the identity token
  - Is this creating a circular dependency?
  - Does this impose unreasonable demands on the properties of the DNS?
- Structured token
  - What would be the unique attribute of a novel token space that distinguishes it from the above?

Unstructured

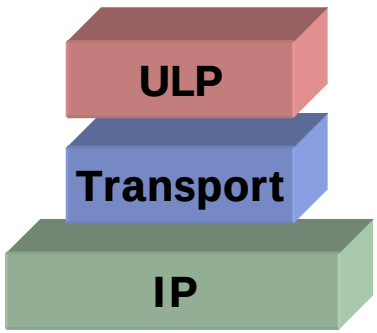
- Unstructured token
  - Allows for self-allocation of identity tokens (opportunistic tokens)
  - How to map from identity tokens to locators using a lookup service?

Proposal for a Modified Transport Protocol



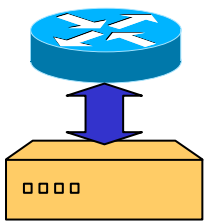
- SCTP:
  - Host-based solution that sets up multiple locators for a session
  - Changes locators on end-to-end heartbeat failure
  - Depends on IPSEC for operational integrity of locator exchange

Proposal for a Modified IP Layer

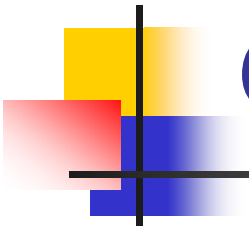


- MIP6:
  - Use one locator as the home address
  - Allow a dynamic switch to an alternate locator as a session surviveability response
  - An instance of a generic approach of packet encapsulation, where the outer encap is the current locator binding and the inner packet is the identifier peering.

Modified Host / Site Exit Router interaction



- Site Exit Anycast proposal
  - Allows local forwarding of outgoing packets to the ‘matching’ site exit router for the selected source address
- Local Site source locator-based forwarding
- Site Exit source address rewriting
  - May be used in combination with locator protocol element proposals
- Have upstream accept all of the site’s sources and use host-based source locator selection

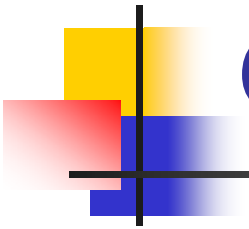


Common Issues

- Picking the ‘best’ source locator

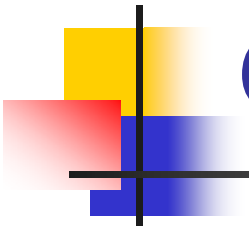
  (how do know what destination works at the remote end?)

  - Use each locator in turn until a response is received
  - Use a identity peering protocol to allow the remote end to make its own selection from a locator set



Common Issues

- Picking the ‘best’ destination locator
  - Longest match
  - Use each in turn
- Picking the ‘best” source / destination locator pair
  - As these may be related choices

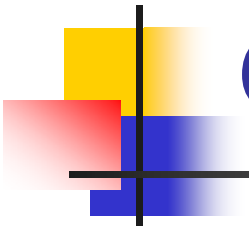


Common Issues

- Detecting network failure

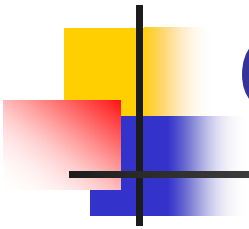
  (How does a host know that its time to use a different source and/or destination locator?)

  - Heartbeat within the session
  - Modified transport protocol to trigger locator change
  - Host / Router interaction to trigger locator change
  - Application timeframe vs network timeframe
  - Failure during session startup and failure following session establishment



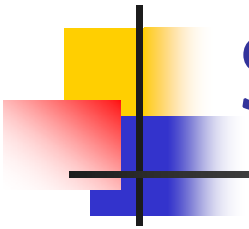
Common Issues

- Session Persistence
  - Use one locator as the “home” locator and encapsulate the packet with alternative locators
  - Set up the session with a set of locators and have transport protocol maintain the session across the locator set
    - Optionally delay the locator binding, or allow the peer dynamic change of the locator pool
  - Use a new peering based on an identity protocol element and allow locators to be associated with the session identity



Common Issues

- Bilateral peer applications vs multi-party applications
  - What changes for 3 or more parties to a protocol exchange?
- Application hand-over and referral
  - How does the remote party identify the multi-homed party for third party referrals?



Security Considerations

- Not considered in the scope of this work
- Worthy of a separate effort to identify security issues in the various proposals following up on threats draft