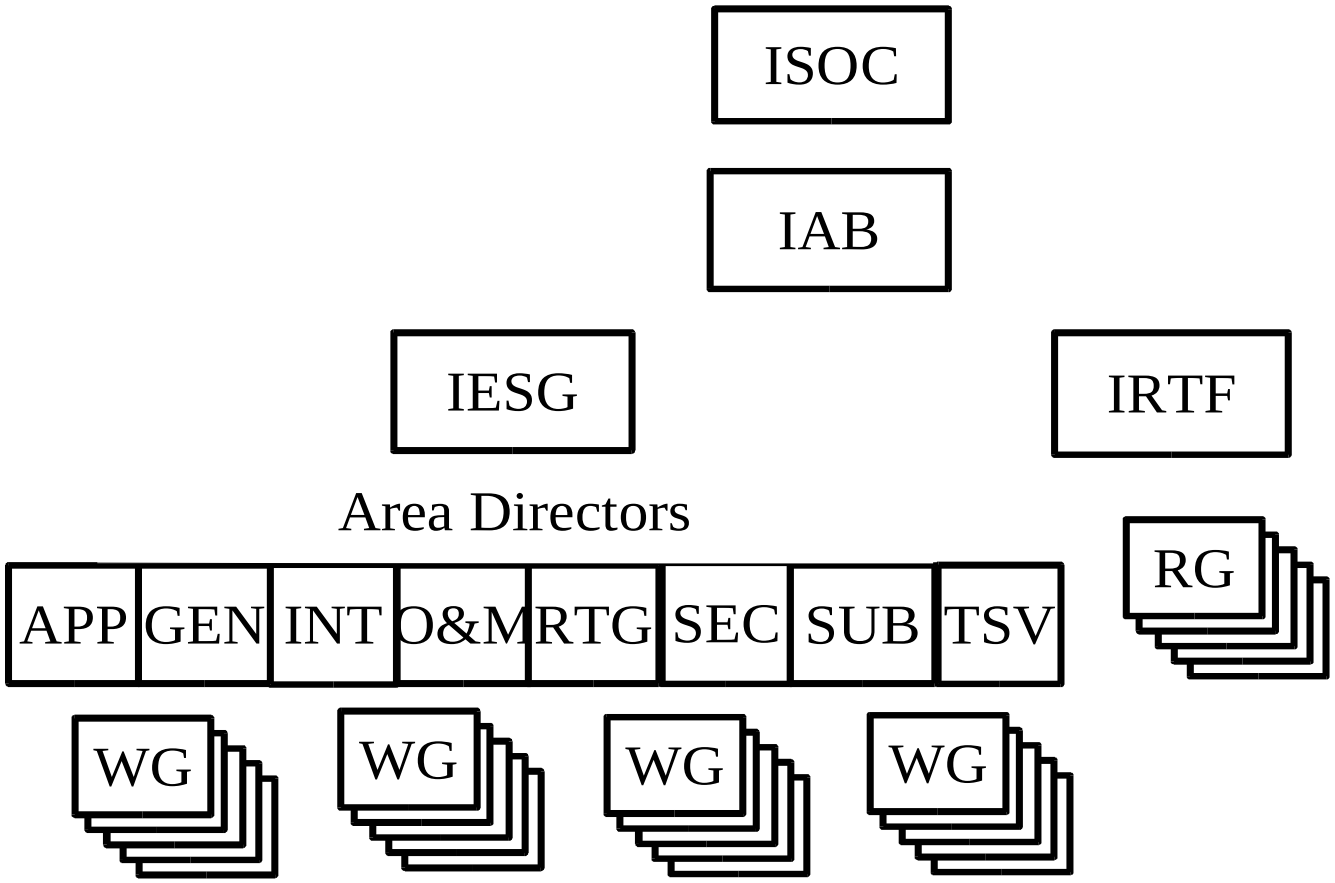
IETF Overview

Erik Nordmark
erik.nordmark@sun.com
Sunlabs Europe

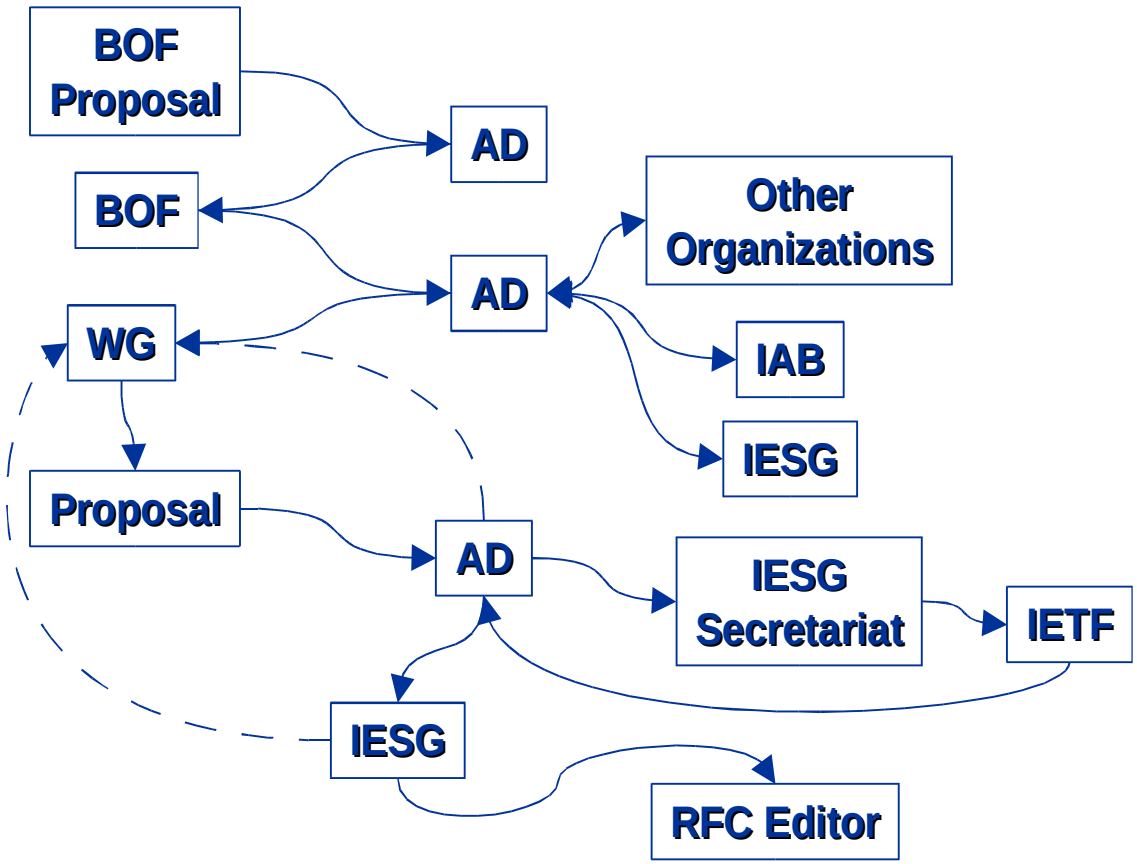
The IETF Organization



How does the IETF work?

- Mailing lists per WG
  - For most discussion
- Internet-Drafts
  - Ideas (good and bad), WG documents, etc.
- Meetings 3 times per year
  - For face to face time, cross WG discussions
  - About 2000 people
- Some WGs also have interim meetings

The IETF Process



Not all RFCs are standard

- Standards track
  - Proposed standard
  - Draft standard
  - Standard
- Best current practice (BCP)
- Experimental
- Informational
- Historic

The Internet Area

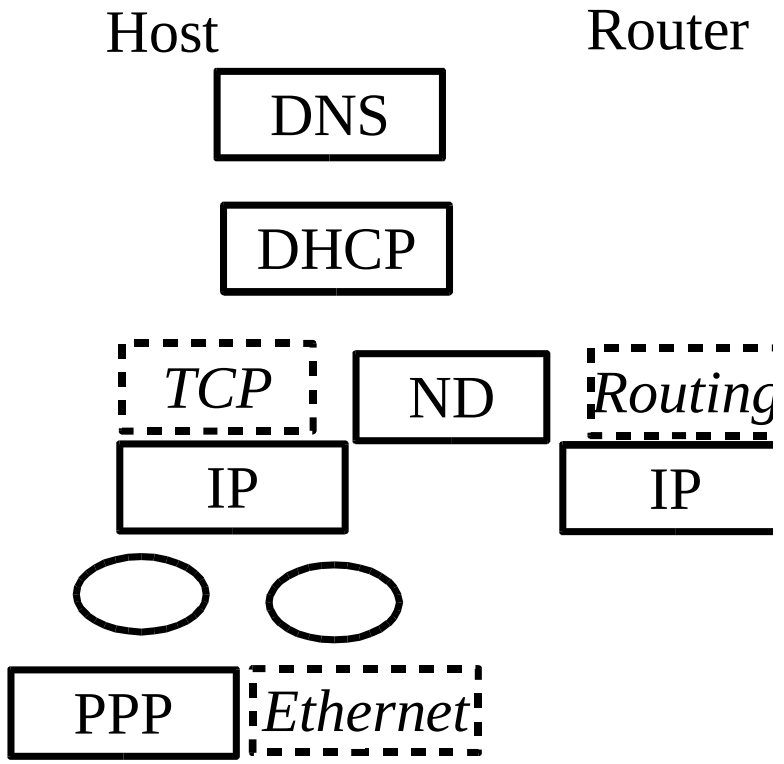
Erik Nordmark
erik.nordmark@sun.com
Sunlabs Europe

Working Groups

- AToM MIB
- Dynamic Host Configuration
- DNS Extensions
- Extensible Authentication Protocol
- Internationalized Domain Name
- Interfaces MIB
- IP over Cable Data Network
- IP over InfiniBand
- IP over Resilient Packet Rings
- IP Version 6 Working Group
- ICMP Traceback
- Layer Two Tunneling Protocol Ext.
- Multicast & Anycast Group Membership
- IP Routing for Wireless/Mobile Hosts
- Protocol for carrying Authentication for Network Access
- Point-to-Point Protocol Extensions
- Zero Configuration Networking
- Network Mobility (under review)
- Secure Neighbor Discovery (under review)

What's in the Internet Area?

- DNS, IDN
- Configuration (DHCP)
- IP layer (IPv6)
- Host-router protocols
- End-to-end IP mobility
- IP over “foo”
  - And MIBs for “foo”
- PPP, L2TP, EAP, PANA



IP Layer Protocols

- IPv6 WG
  - IPv6 work being done throughout the IETF
  - Core pieces in this WG
  - Prefix delegation
    - IPv6 user will get a /48 prefix by default
    - Automate this using a protocol (probably using DHCPv6)
  - MIBs common for IPv4 and IPv6
  - DNS discovery?
- New IPv6 operations (v6ops) WG
  - In Operations and Management Area

Host-to-router protocols

- Multicast and anycast membership (IGMP, MLD)
  - Hosts asking to join multicast groups is well understood
    - Anybody can join and receive packets
    - Leave security to the application protocol
  - Joining an *anycast* group prevents other members from receiving packets
    - Only one (the closest) member receives the packets
    - How to apply access control – who can join?

Host-to-router protocols (contd)

- PANA – protocol for carrying authentication for network access
  - Today's authentication at the edge
    - A device (host or home router) often uses PPP
    - With 802.11 it is likely to use 802.1x
    - And there are cellular standards
    - Hotels with web forms to authenticate and authorize
  - How about a common IP-level protocol for hosts to authenticate to the routers?
  - Use e.g., with Mobile IPv6

Host-to-router protocols (contd)

- Securing Neighbor Discovery (under review)
  - Neighbor Discovery is the IPv6 version of ARP + router discovery
  - Often we assume that a single link (e.g., Ethernet) is secure
  - What about providing public access on e.g. 802.11?
    - Might not trust everybody else which is on the link
  - Securing 802.11 is not enough
    - Any authenticated node could claim to be the router or do “ARP” spoofing
- Note: only a piece of security puzzle

Mobility

- Mobile IPv6 security solution
  - Don't depend on a global PKI
  - Assume routing infrastructure is reasonably trusted
  - Has resulted in “Return routability” scheme
  - Mobile IPv6 specification is close to done in the WG
- Mobile IP optimizations
  - Localized mobility management
- NAT traversal for Mobile IPv4
  - Tunneling IP in UDP to cross NAT box

Mobility (contd)

- Network Mobility WG being reviewed
  - A network moving as a unit
    - E.g., a personal area network, or a train
    - One or more Mobile Routers attach to the Internet
  - Approach to use tunneling between a home agent and the mobile router
- Later explore how the overhead associated with the tunnels can be removed
  - Known as “Route Optimization”

Configuration

- DHC WG
  - DHCPv6 soon an RFC
  - Deployable authenticated DHCP?
    - RFC 3118 not enough
    - plug&play plus security?
- Zeroconf WG
  - Configuring link-local IPv4 addresses
    - Only useful for communication on a single link
  - Various versions already exists in products

DNS

- Get DNSSEC deployable
  - Implementation feedback on “delegation signer”
  - Opt-in? Wildcard optimization?
  - Make the DNSSEC specifications easier to read
- Local name resolution - part of plug and play
  - Link-local multicast name resolution (LLMNR)
  - Referential integrity issue
    - If www.ietf.org can be resolved locally
    - If www.ietf.org can be resolved using DNS
    - Do they refer to the same?

Internationalized Domain Names

- Separate session this week
- Extend domain names to Internationalized Domain Names
  - Using Unicode 3.0
- ASCII-compatible encoding (ACE) for carrying the names in DNS as well as application protocols
- Applications to be modified to display and handle input of the names in their Unicode form
  - Unmodified applications display www.bq--ndfsj.se

IP over “foo”

- For example, IP over InfiniBand
  - Example of adding IP support after the fact
- Often the link layer has things that IP doesn't need
- Often details don't match what IP needs
  - E.g., multicast model subtly different
  - In this case InfiniBand is being slightly modified by the InfiniBand Trade Association

PPP, L2TP, EAP

- New EAP WG
  - Extensible Authentication Protocol
    - Used by PPP, 802.1x, e.g., for 802.11
  - Refine EAP specification based on implementation and interoperability experience
  - Clarify the state machine
  - Clarify security assumptions
- In the future review some EAP methods e.g., those based on mobile phone SIMs

Common theme: Security

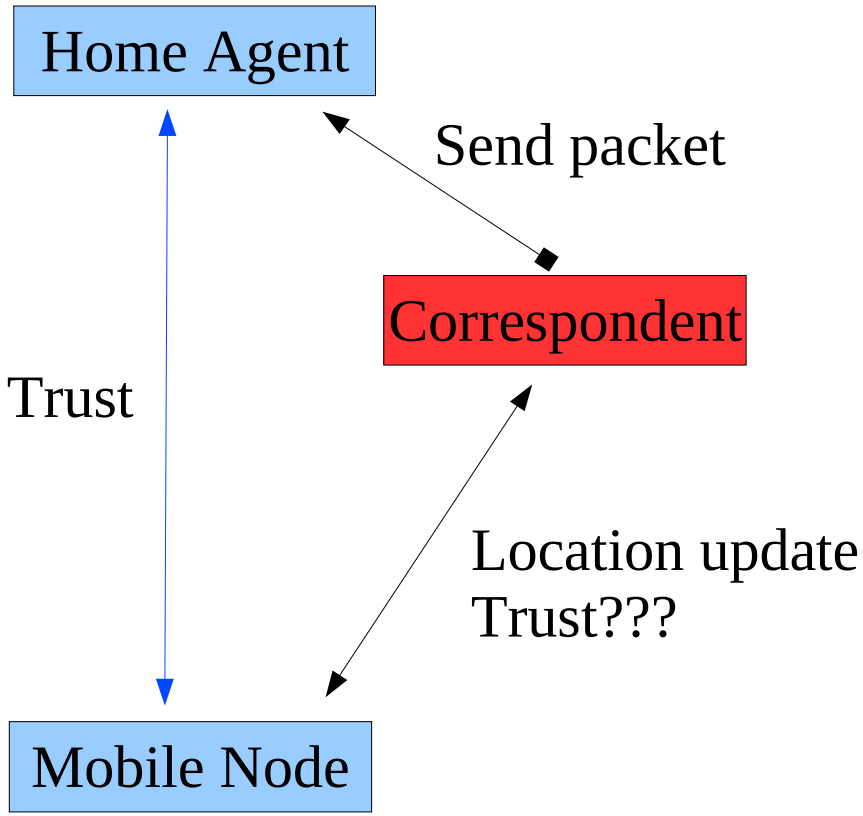
- History in the IETF
  - No security – passwords in the clear
  - Require “Security Considerations” in RFCs
  - Work on getting “tools”
    - Cryptography, IPsec, TLS, IKE, etc.
  - “ Use IPsec” common in RFCs
    - Major fallacy; it ain't that easy
    - Need specifications and interoperability testing
  - But what threats were we concerned with?
  - Who do we trust and not trust?

Security in Practice

- Start with a trust model and threat analysis
  - Attackers on the local link?
  - On-path attackers?
  - Anybody in the Internet?
- Assumptions about security infrastructure
  - A global PKI? Unlikely to ever be deployed
  - Local PKIs
  - No security infrastructure?
- When to use which tool? [IPsec, TLS, ...]

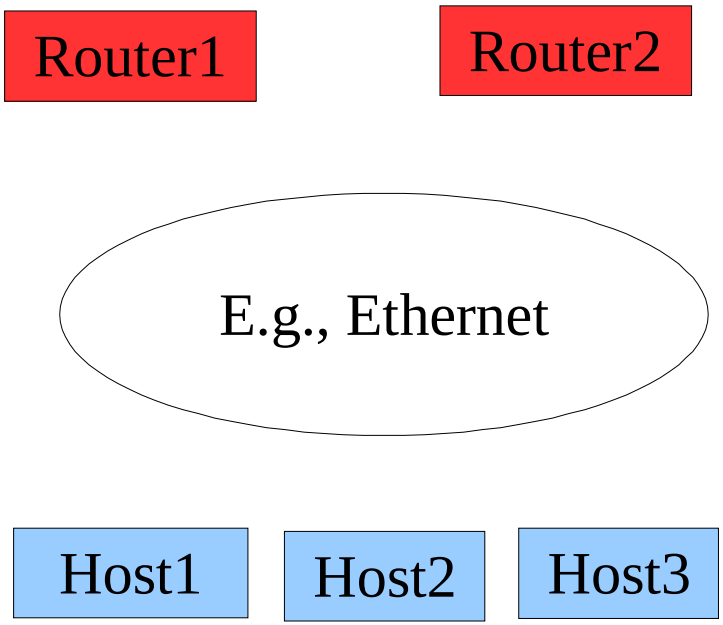
Security Example: Mobile IPv6

- Hard part is correspondent
- Original idea: IPsec + global PKI
- New idea:
  - IPsec between MN and HA
  - Rely on routing being reasonably secure between CN and HA



Example: Neighbor Discovery

- RFC 2462 says “use IPsec”
  - Works but not that useful
- Bootstrapping means automatic key management can't be used
- Hard to know which routers to trust



Robustness in the architecture

- Basic Internet model has soft-state except at the endpoints
  - A router failure doesn't upset the end-to-end connections
- Newer network elements have hard state
  - Firewalls, NAT boxes, some load balancers, etc.
  - Some routing elements are not designed to be easily replicated (e.g., mobile IP home agents)
- Are we building such Single Points of failure into the architecture?