NexTech 2015

Secure Routing

J. William Atwood

Distinguished Professor Emeritus
Computer Science and Software Engineering
Concordia University

Course overview

- Internet Standards
  - Standards Development Organizations
- Routing
  - Motivation
  - Architecture
  - Different approaches
- Security
  - Motivation, Responsibility, Threats
  - Validation: Content and Transport Path
  - Examples

..2

- ❑ Network Device Configuration
  - Approaches
  - Layers
- ❑ Routing and Security: KARP
  - Goals
  - Threats and Designs
  - Proposals
- ❑ The future
  - More layers

Communications Standards Development Organizations

- Institute of Electrical and Electronic Engineers (IEEE)
  - Hardware Standards
- Internet Engineering Task Force (IETF)
  - Internet Standards (Request for Comments)
- International Telecommunications Union – Telecommunications (ITU-T)
  - Telephony Standards (Recommendations)

- A strong liaison exists among these bodies

Standardization Scope

- The IETF does *not* standardize transmission hardware (we leave that to organizations such as the IEEE and the ITU) and does not standardize specialized application layer protocols. For example, we leave HTML and XML standards to the World-Wide Web Consortium. But the IETF *does* standardize all the protocol layers in between, from IP itself up to general applications such as email and HTTP.

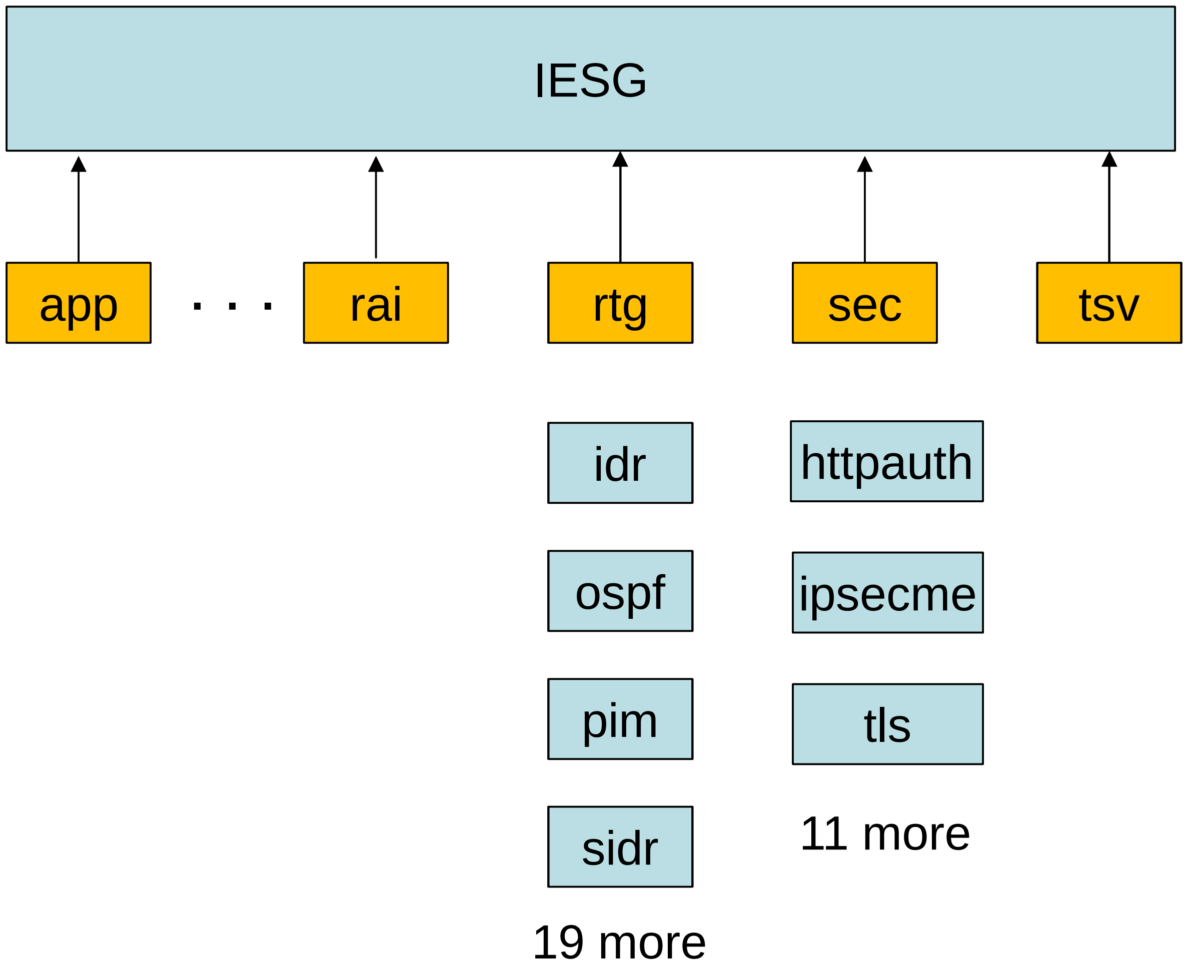
IETF Structure

- Eight Areas
  - Applications (app)
  - General (gen)
  - Internet (int)
  - Operations and Management (ops)
  - Real-time Applications and Infrastructure (rai)
  - Routing (rtg)
  - Security (sec)
  - Transport (tsv)

Internet Engineering Steering Group (IESG)

- Each area has 2 “Area Directors” (ADs), except
  - Routing (3)
  - General (1)
  - Applications (1)
- The IESG membership consists of all the ADs
  - Responsible for the overall management of the IETF

Internet Engineering Steering Group (IESG)



IESG

app · · · rai rtg sec tsv

idr

ospf

pim

sidr

19 more

httpauth

ipsecme

tls

11 more

Routing Area

- 23 Working Groups
  - idr (Inter-Domain Routing)
  - ospf (Open Shortest Path First IGP)
  - pim (Protocol Independent Multicast)
  - sidr (Secure Inter-Domain Routing)
  - . . .
- Three Area Directors

Security Area

- 14 Working Groups
  - httpauth (Hypertext Transfer Protocol Authentication)
  - ipsecme (IP Security Maintenance and Extensions)
  - tls (Transport Layer Security)
  - . . .
- Two Area Directors

Internet Architecture Board

- Provides architectural oversight
  - Series of reports on topics of concern to the entire Internet community
- Acts as an appeals board

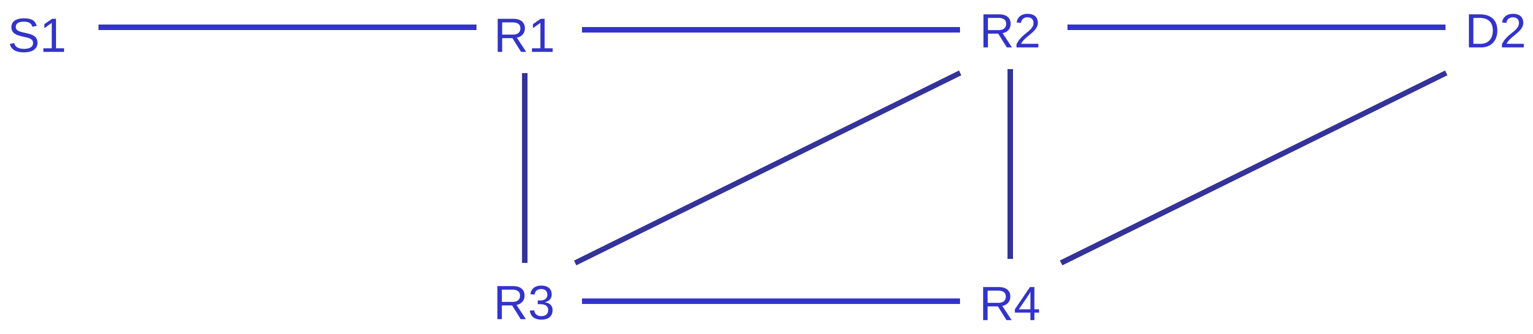
IETF Documents

- An idea starts as an “Internet Draft” (ID)
  - draft-atwood-pim-sm-linklocal
- It is “adopted” by a Working Group
  - draft-ietf-pim-sm-linklocal
- After discussion, it undergoes “Working Group Last Call” (WGLC)
- If it passes WGLC, it is subject to “IETF Last Call”, and review by the IESG (i.e., by ***all*** ADs)
- If it passes scrutiny, it becomes an RFC
  - RFC 5796

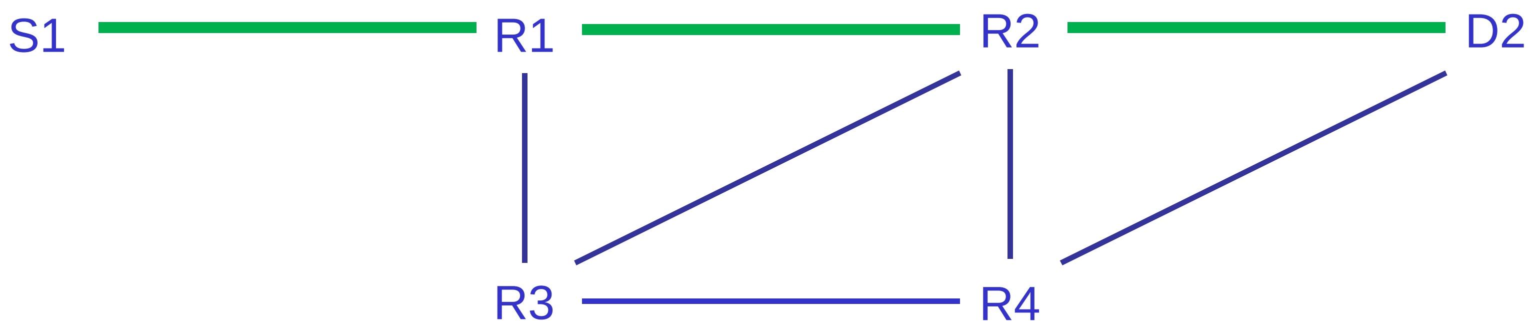
Routing

- Moving a packet from a source to a destination by the least-cost route
- Different definitions of “least cost”
  - Minimum number of hops
  - Factors of policy and charging

Routing Structures

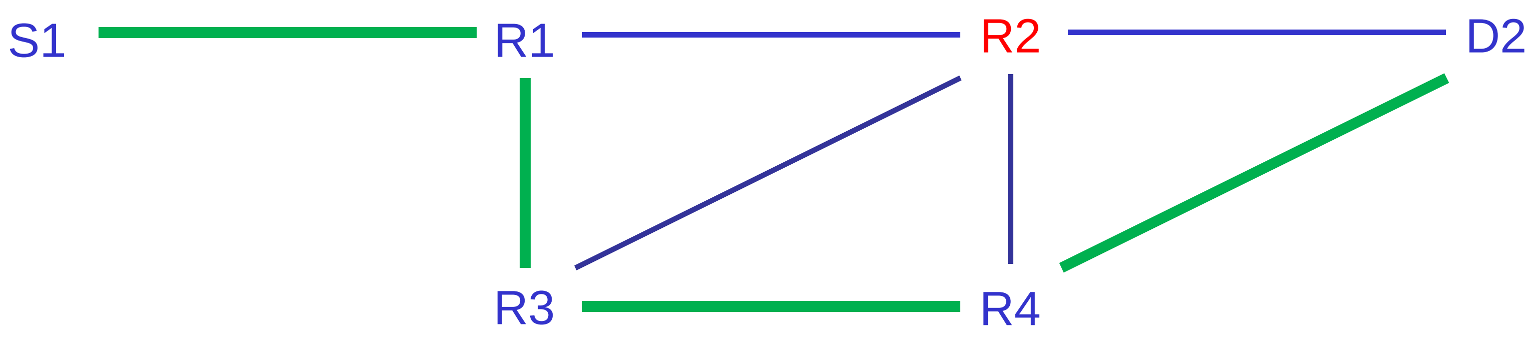


Routing Structures



Shortest path: S1 – R1 – R2 – D2

Routing Structures



Shortest path avoiding R2: S1 – R1 – R3 – R4 – D2

Forwarding Information Base (FIB)

- At each router, need to determine where to send an incoming packet
  - Forwarding Information Base (aka Forwarding Table)
    - Local environment: few entries
    - Global Internet: 350, 000 entries
    - Very hard to look up quickly
- The task of a routing protocol is to fill the FIB with the appropriate entries
  - Obtain information from “peers”
  - Apply policies to get the “best” next router

Autonomous Systems

- Global Internet is large
  - Need for “local control” of parts of it
  - An Autonomous System is a part of the Internet with a “common routing policy”
  - Routing is at two levels:
    - Inter-AS
    - Intra-AS
  - Intra-AS routing tends to be “shortest path”
  - Inter-AS routing is policy-based

Different approaches to routing

- ❑ Intra-AS routing
  - Interior Gateway Protocols (IGPs)
    - OSPF, IS-IS
  - All under one “administration” (more or less)
  - Shortest-path routing
- ❑ Inter-AS routing
  - Exterior Gateway Protocols (EGPs)
    - BGP
  - Many policy or contractual issues
  - Preferred routing tends to be defined by lawyers, not network personnel

Example routing protocols

- Border Gateway Protocol (BGP)
  - E-BGP
  - I-BGP
- Open Shortest Path First (OSPF)
- Routing Information Protocol (RIP)
- Static routing
- Protocol Independent Multicast (PIM)

Border Gateway Protocol

- BGP provides inter-AS routing
- Routing packets are carried by TCP, since the “neighbors” can be quite far away
- BGP is specified by IDR WG
- Validity of BGP information is specified by SIDR WG

Open Shortest Path First

- Routing packets are (normally) link-local (i.e., not forwarded beyond the local subnet)
- They are carried directly by IP
- They are multicast to the neighbors
- OSPF is specified by the OSPF WG

Routing Information Protocol

- A very early routing protocol
- Limited in scope, so RIP is used only in “small” routing domains.
  - Limit on the “diameter” of the routing graph
- Simpler than OSPF

Static Routing

- The Forwarding Table entries on a device are specified manually.
- Typically, static routing is used for end hosts.
  - An entry for “other hosts on the same network segment”
  - An entry for “the rest of the world” (i.e., a default gateway)
- Can be useful for large, structured networks, where little or no change is expected over time

Protocol Independent Multicast

- PIM is “independent” of the underlying unicast routing protocol, although it assumes the existence of a unicast Routing Information Base (RIB)
- Various “flavors”:
  - PIM-SM (Sparse mode)
  - PIM-SSM (Source-specific mode)
  - PIM-DM (Dense mode)
  - BIDIR-PIM (Bidirectional)

PIM…2

- The routing packets are normally link-local
- They are carried directly by IP
- They are multicast
- Some special PIM packets are sent unicast

Security

- Justification
  - IAB Workshop on “Unwanted Internet Traffic”
    - Section 8.1 “A simple risk analysis would suggest that an ideal attack target of minimal cost but maximal disruption is the core routing infrastructure.”
    - Section 8.2 calls for “[t]ightening the security of the core routing infrastructure”.
  - We will explore why this is not happening

Main steps

- ❑ Increase the security mechanisms and practices for operating routers
- ❑ Clean up the Internet Routing Registry [IRR] repository, and securing both the database and the access, so that it can be used for routing verifications
- ❑ Create specifications for cryptographic validation of routing message content
- ❑ Secure the routing protocols’ packets on the wire

Responsible parties

- OPSEC
  - ***Operational Security Working Group***
- Liaison with those running the IRRs globally

- SIDR
  - ***Secure Inter-Domain Routing Working Group***
- KARP
  - ***Keying and Authentication for Routing Protocols Working Group***

Security is not just technical

- OPSEC
  - Operational (non-cryptographic) security considerations
- Liaison
  - Convincing others to act in concert
- SIDR
  - Validating the ***content*** of the messages
- KARP
  - Validating the ***exchanges*** themselves (“on the wire”)

Generic Security Threats: RFC 4593

- Generic Routing Protocol Threat Model
  - Threat sources
  - Threat consequences
- Generally Identifiable Routing Threat Actions
  - Deliberate exposure
  - Sniffing
  - Traffic analysis
  - Spoofing
  - Falsification

Issues with Existing Cryptographic Protection: RFC 6039

  - Weaknesses of MD5 and SHA-1 are discussed
  - Technical and management issues are identified

- Protocols reviewed
  - Open Shortest Path First Version 2 (IPv4)
  - Open Shortest Path First Version 3 (IPv6)
  - Intermediate System to Intermediate System Routing Protocol
  - Border Gateway Protocol (BGP-4)
  - Routing Information Protocol (RIP)
  - Bidirectional Forwarding Detection (BFD)

Validating the Contents: SIDR

- BGP is specified by IDR WG
- BGPsec is specified by SIDR WG
- Goal is to permit validation of the ***contents*** of the exchanges
- BGP uses TCP-MD5 or TCP-AO to ensure that the exchanges are authentic and have not been altered

BGPsec

- An extension to BGP that provides improved security for BGP routing
- Motivation
  - BGP does not include mechanisms that allow an AS to verify the legitimacy and authenticity of BGP route advertisements
  - Vulnerability analysis RFC 4272
  - Resource Public Key Infrastructure (RPKI) provides a first step

RPKI

- Resources
  - AS number
  - IP address
- RPKI certificates issued to holders of resources provide a binding
  - AS number <-> IP address
- and a cryptographic key to verify a digital signature

Route Origination Authorization

- ROA allows holders of IP address resources to authorize specific ASes to originate routes (in BGP) to these resources
- Data extracted fro valid ROAs can be used by BGP speakers to determine whether a received route was actually originated by an AS that is authorized to originate that route
- RFC 6483
- RFC 7115

Local Policy

- Prefer a route that can be validated using RPKI data
- Can protect from certain mis-origination attacks
- Little or no protection from a sophisticated attacker
  - Append authorized origin AS to an illegitimate AS path
- draft-ietf-sidr-bgpsec-threats

BGPsec extension

- ❑ Add BGPsec router certificate
- ❑ Binds an AS number to a public signature verification key
- ❑ Private key is held by (one or more) BGP speakers within the AS
- ❑ BGP speaker signs on behalf of its AS
- ❑ Relying party can then verify that a given BGP signature was produced by a BGP speaker belonging to a given AS

Goal

- Use signature to protect the AS path data in BGP update messages
- So that a BGP speaker can assess the validity of the AS path data in the update message that it receives

BGPsec Operation

- Core of BGPsec is a new optional (non-transitive) attribute called BGPsec_Path
  - AS path data
  - Sequence of digital signatures, one for each AS in the path
  - draft-ietf-sidr-bgpsec-protocol
  - New signature is added each time an update message leaves an AS
  - Any tampering with AS path data or NLRI in the BGPsec_Path can be detected

Negotiation of BGPsec

- Separate for address family
- Separate for each direction

Update signing and validation

- Outline in draft-ietf-sidr-bgpsec-overview
- Specific details in draft-ietf-sidr-bgpsec-protocol

Validating the Exchanges

- Security is specified in each Protocol Specification
- These specifications cover
  - Authenticity of sender
  - Integrity of the packet

Current practice

- No security
  - Never activate the security features of the routing protocol
- -OR-
- Install and forget
  - Put a shared key in place
  - Leave it unchanged for 5 years or more, until the router is replaced

Why?

- Operational Issues
  - Changing an active key requires coordinating both ends of the link
- Key rollover is a disaster
  - Usually results in breaking (and re-establishing) an adjacency
  - User data packets are lost during this process
- The (potential) loss of revenue from the lost packets is seen as more of a problem than the (potential) fallout from a security breach

On-the-wire Security Methods

- Security is achieved at various levels, depending on the Routing Protocol
- Typical Approaches
  - Authentication Trailer
  - IPsec
  - TCP-MD5, TCP-AO

Authentication Trailer

- A field, appended to the Routing Protocol packet, that permits authentication of the source of the packet.
- Based on calculating
  - A Message Digest (e.g., MD5) -or-
  - A Hash-based Message Authentication Code (HMAC)
- over the RP packet and a (shared) key
- This provides authentication and integrity verification

IPsec

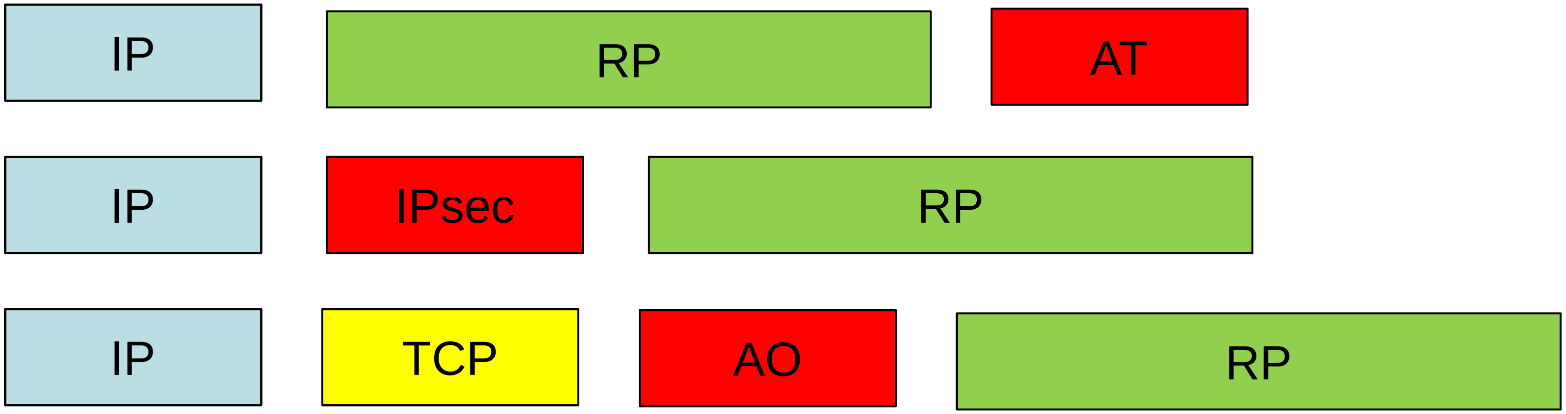
- IP Security (IPsec)
  - IPsec is a general purpose system, that provides security for all kinds of IP packets. It uses two headers (additions to the IP packet) called Encapsulating Security Payload (ESP) and Authentication Header (AH)
  - The AH is a field, part of the IP Header, that provides authentication of the source of the packet
  - The ESP is a field, part of the IP Header, that provides authentication of the source and confidentiality of the contents for a particular IP packet
  - Both ESP and AH ensure integrity

TCP-MD5 and TCP-AO

- TCP-MD5 is an extension to TCP that provides authentication of the source, using an MD5 hash
- TCP-AO is an extension to TCP that provides superior authentication compared with TCP-MD5.
- These are both achieved by adding to the TCP header
- Extended TCP is used by routing protocols that need security and the properties of TCP

Comparison

- Authentication Trailer
- IPsec
- TCP-AO (or TCP-MD5)



IP RP AT

IP IPsec RP

IP TCP AO RP

Examples

List of Protocols that use specific techniques

Routing Protocol	Key Scope	Communication Type	Security Feature	Standard
BGP	Peer Keying	Unicast	OoB	TCP-AO
RIPv2	Group keying	Multicast	Built-in	AT
OSPFv2	Group keying	Both	Built-in	AT
OSPFv3	Group keying	Both	Built-in	AT
OSPFv3	Group keying	Both	OoB	IPsec
PIM-SM	Group keying	Multicast	OoB	IPsec

AT: Authentication Trailer
OoB: Out of Band
Both: Unicast and Multicast

Router Configuration

- Manual
- Simple Network Management Protocol (SNMP)
- XML forms
  - See Nitin’s thesis
- NETCONF and YANG

Manual configuration

- Walk up to the router
  - Use a “console” (Terminal, DEC VT220)
- Access a router remotely
  - Use ssh to access a “virtual console” on the router
  - Depends on unicast routing already working, so this is only useful for “changes”.

Simple Network Management Protocol

- Provides the ability to read the state of a network device, and to set a new state.
- Originally had no security
- Acquired some security features over time, but they were very primitive

NETCONF

- IETF Standard for Network Configuration
- Basic set of operations for configuration
  - Install
  - Manipulate
  - Delete
- Client-Server Architecture: Remote Procedure Call
  - get, get-config, edit-config, copy-config, delete-config
  - Uses XML encoding

NETCONF..2

- Multiple Logical Datastores
  - writable-running, startup, candidate
  - Each represents a possible configuration state
  - Each can be configured independently, locked and unlocked, to ensure safe manipulation and consistency of the configuration data
- No specific data-modeling language
  - Private solutions
  - XACML

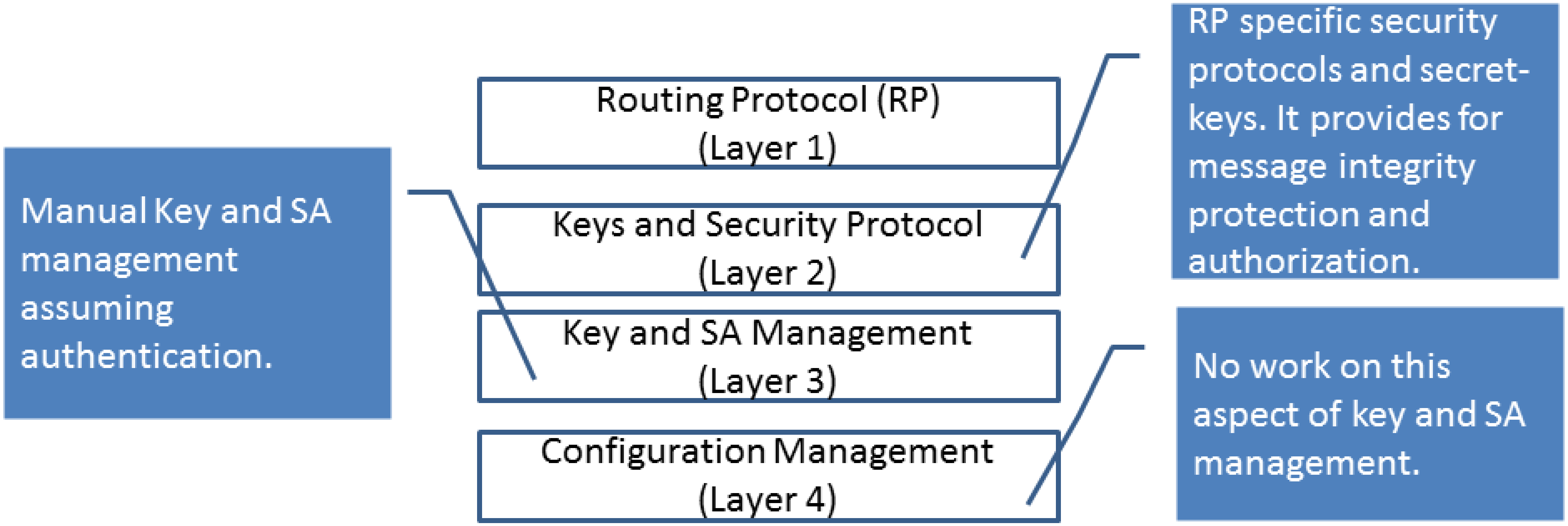
Extensible Access Control Markup Language

- Expression of authorization policies in XML against objects that are themselves defined in XML.
  - Core schema
  - Corresponding namespace
- Extensible
  - Can define IP address, port number, device identity, etc. when required.
- Based on XML
  - Easy to extend, hard to reach consensus on extensions

Data Modeling Language

- XML
  - Not really suitable
- YANG
  - Hierarchical
  - Modular
  - Designed for NETCONF
  - Modules are reusable, extensible, and importable
  - Derived types
  - Can be translated into an equivalent XML
  - Supports versioning

Layers of Configuration Management



Routing Protocol (RP) (Layer 1)

Keys and Security Protocol (Layer 2)

Key and SA Management (Layer 3)

Configuration Management (Layer 4)

Manual Key and SA management assuming authentication.

RP specific security protocols and secret-keys. It provides for message integrity protection and authorization.

No work on this aspect of key and SA management.

Routing and Security

- Routing Protocol documents tend to have poor or outdated “Security Considerations”
- All IETF documents have to be reviewed by the Security Directorate (part of the Security Area)
- Problem: How to ensure progress on the security side, without “scaring” the Routing Area personnel
- Joint agreement between the Security ADs and the Routing ADs

Keying and Authentication for Routing Protocols

- Charter Goals
  - The KARP working group is tasked to work with the routing protocol working groups in order to improve the communication security of the packets on the wire used by the routing protocols. This working group is concerned with message authentication, packet integrity, and denial of service (DoS) protection. At present, this charter explicitly excludes confidentiality and non-repudiation concerns.

KARP..2

- Determine current threats to the routing protocol operation, and define general requirements for cryptographic authentication of routing protocols. A primary source for this document should be draft-lebovitz-karp-roadmap, although RFC 4393 may also be useful.
- Identify deficiencies of each routing protocol in scope, and specify mechanisms that bring them in line with the general requirements. These are referred to as protocol gap analysis documents.
- Define one or more frameworks describing the common elements for modern authentication in routing protocols.

KARP..3

- Publish guidance on how to create a gap analysis for routing protocols.
- Publish guidance on guidance to operators on how to create and use integrity keys used with routing protocol message authentication.
- Specify automated key management needs for routing protocols.

KARP Documents

- Overview, Threats, and Requirements
  - Summary
- Design Guide
  - Summary
- Gap Analyses
  - Analyses of specific routing protocols
- Proposals for Automated Key Management
  - Case1: unicast exchanges
  - Case 2:multicast exchanges

Overview, Threats, and Requirements: RFC 6862

- Overview
  - KARP scope
  - Incremental approach
  - Goals
  - Non-goals
  - Audience

Overview, Threats, and Requirements: RFC 6862

- Threats
  - Review of specific threats to routing protocols
  - Threat sources
  - Threat actions in scope
  - Threat actions out of scope
- Requirements
  - For work phase 1
  - Update to a routing protocol’s existing transport security

Design Guide: RFC 6518

- ❑ Categorizing routing protocols
- ❑ Consider the future existence of a Key Management Protocol
- ❑ Roadmap
- ❑ Routing protocols in categories
- ❑ Supporting incremental deployment
- ❑ Denial-of-service attacks
- ❑ Gap analysis
- ❑ Security Considerations

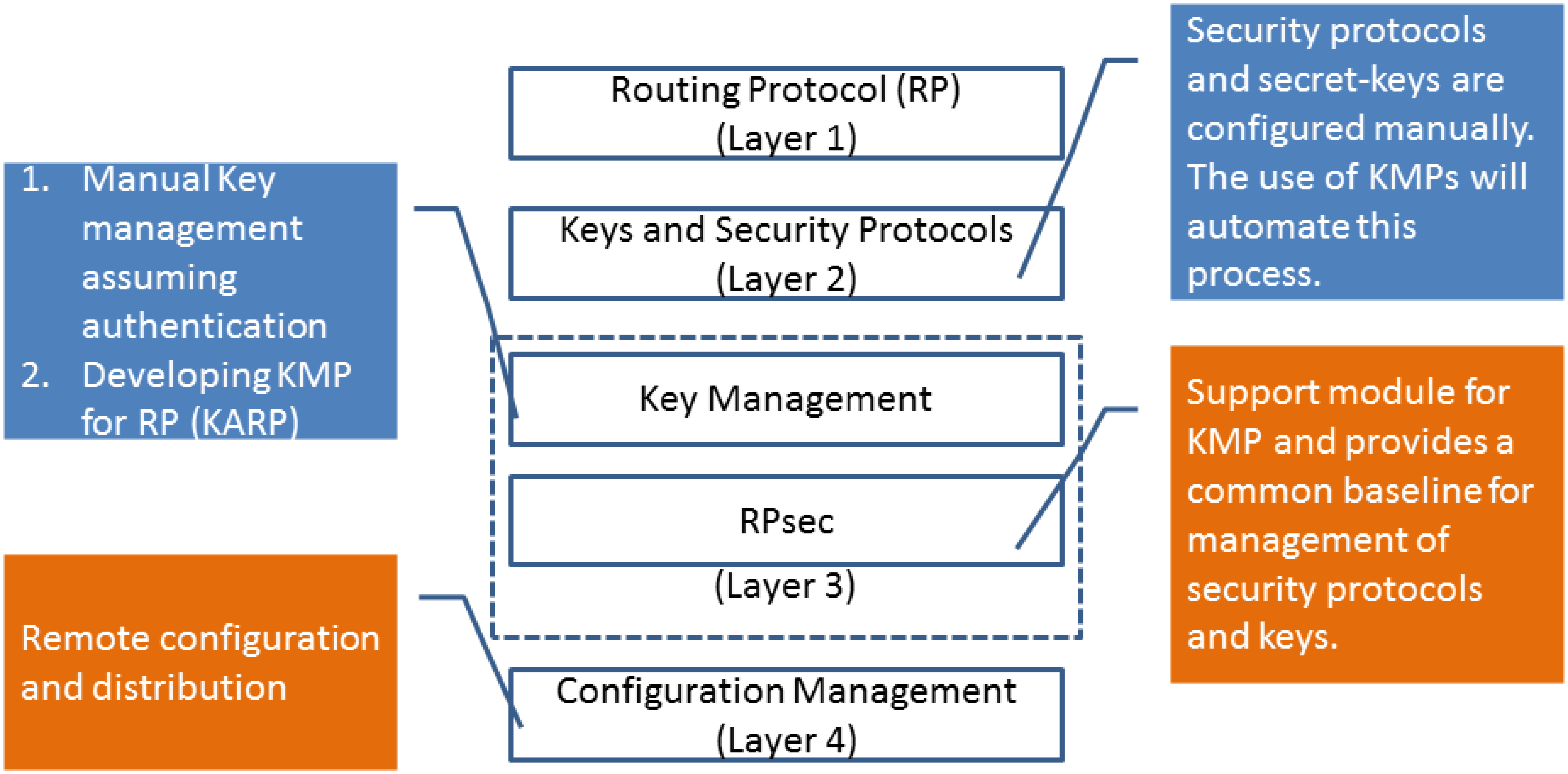
Work phase 1: Routing Protocol Analyses

- RFC 6863
  - Open Shortest Path First
- RFC 6952
  - Border Gateway Protocol (BGP)
  - Label Distribution Protocol (LDP)
  - Path Computation Element Communication Protocol (PCEP)
  - Multicast Source Distribution Protocol (MSDP)
- RFC 7492
  - Bidirectional Forwarding Detection (BFD)

Work phase 2: Automated Key Management Protocols

- RKMP
  - draft-mahesh-karp-rkmp
- MaRK
  - draft-hartman-karp-mrkmp
- G-IKEv2
  - draft-yeung-g-ikev2
- Using G-IKEv2 for Routing Protocols
  - draft-tran-karp-mrmp

Layers of Configuration Management - Revisited



Routing Protocol (RP)
(Layer 1)

Keys and Security Protocols
(Layer 2)

Key Management

RPsec

(Layer 3)

Configuration Management
(Layer 4)

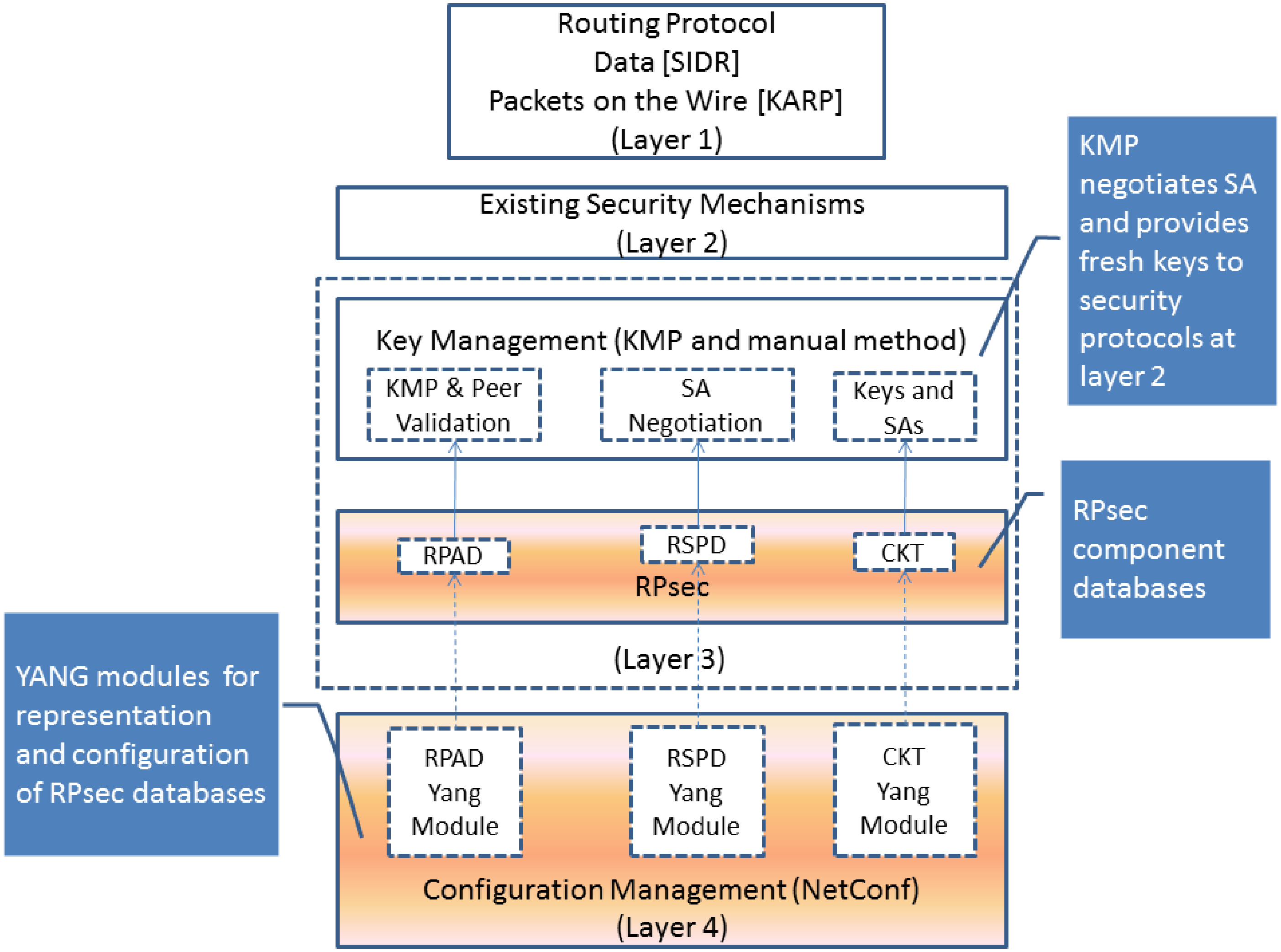
1. Manual Key management assuming authentication
2. Developing KMP for RP (KARP)

Remote configuration and distribution

Security protocols and secret-keys are configured manually. The use of KMPs will automate this process.

Support module for KMP and provides a common baseline for management of security protocols and keys.

Layers of Configuration Management..3



Routing Protocol
Data [SIDR]
Packets on the Wire [KARP]
(Layer 1)

Existing Security Mechanisms
(Layer 2)

Key Management (KMP and manual method)

KMP & Peer Validation

SA Negotiation

Keys and SAs

RPAD

RSPD

CKT

RPsec

(Layer 3)

RPAD Yang Module

RSPD Yang Module

CKT Yang Module

Configuration Management (NetConf)
(Layer 4)

KMP negotiates SA and provides fresh keys to security protocols at layer 2

RPsec component databases

YANG modules for representation and configuration of RPsec databases

Getting the Senior Manager to Understand

- YANG provides a way to model the RPsec databases
- NETCONF provides a way to coherently distribute the configurations (YANG instances) to a set of devices
- Various senior managers have different views of what is important
- How to map from “corporate policies” to individual YANG configurations?

Getting Security Deployed

- Configuration of security is only one aspect of configuration of the overall device
- Any “new” approaches have to fit with existing deployments, and “play nice”
- There has to be a perceived advantage to adding the security, and little or no impact on the existing infrastructure

Thank you!

- Questions?