Securing the Border Gateway Protocol (S-BGP)

Dr. Stephen Kent

Chief Scientist - Information Security

BBN
TECHNOLOGIES
A Verizon Company

Outline

- BGP security concerns & requirements
- Securing BGP UPDATE messages
- PKI design
- Repository design
- Impact of S-BGP on routers
- Making S-BGP a reality
- Questions

BGP Security Issues

- BGP is the critical infrastructure for Internet, the basis for all inter-ISP routing
- Benign configuration errors affect about 1% of all routing table entries at any time
- The current system is highly vulnerable to human errors, and a wide range of malicious attacks
  - links
  - routers
  - management stations
- MD5 MAC is rarely used, perhaps due to lack of automated key management, and it addresses only one class of attacks

The Basic BGP Security Requirement

- For every UPDATE it receives, a BGP router should be able to verify that the owner(s) of the NLRI authorized the first AS to advertise the address block(s) and that each subsequent AS in the path has been authorized by the preceding AS to advertise a route to the addresses in question
- This requirement, if achieved, allows a BGP router to detect and reject unauthorized route advertisements *, irrespective of what sort of attack resulted in the bad advertisements

*re-advertisement of authorized but withdrawn routes is still possible within the lifetime of a route attestation

Derived Security Requirements

- Verification of address space “ownership”
- Verification of Autonomous System (AS) ownership
- Binding a BGP router to the AS(s) it represents
- Verification of UPDATEs
- Route withdrawal authorization
- Integrity and authenticity of all BGP traffic on the wire

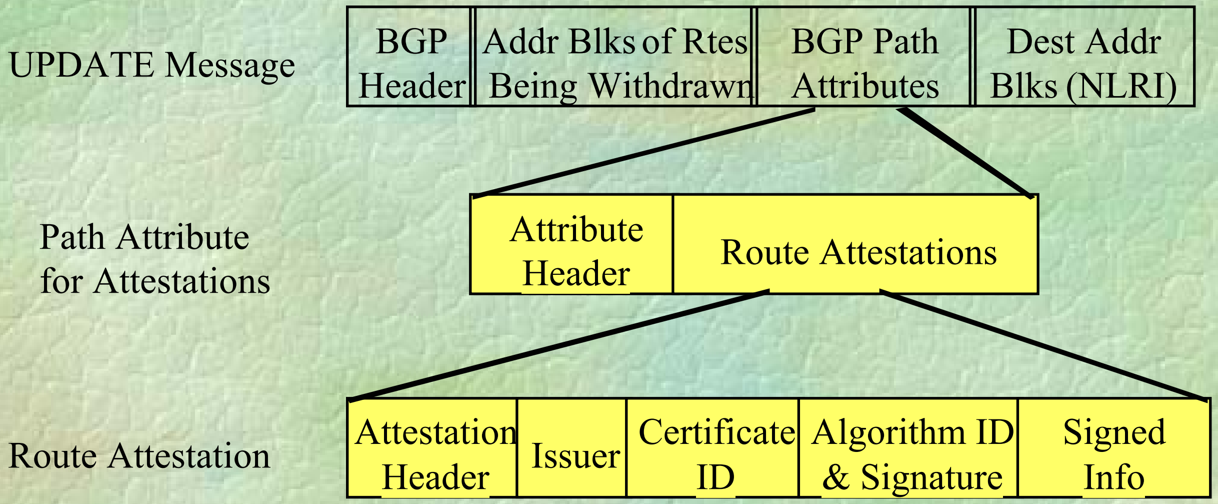
S-BGP Design Overview

- **IPsec**: secure point-to-point router communication
- **Public Key Infrastructure**: an authorization framework for all S-BGP entities
- **Attestations**: digitally-signed authorizations to advertise specified address blocks
- Validation of UPDATEs based on a new path attribute, using PKI certificates and attestations
- **Repositories** for distribution of certificates, CRLs, and address attestations
- Tools for ISPs to manage address attestations, process certificates & CRLs, etc.

Securing UPDATE messages

- A secure UPDATE consists of an UPDATE message with a new, optional, transitive path attribute for route authorization
- This attribute contains a signed sequence of route attestations
- This attribute is structured to support both route aggregation and AS sets
- **Validation of the attribute verifies that the route was authorized by each AS along the path and by the address space owner**

An UPDATE with Attestations



UPDATE Message

BGP Header | Addr Blks of Rtes Being Withdrawn | BGP Path Attributes | Dest Addr Blks (NLRI)

Path Attribute for Attestations

Attribute Header | Route Attestations

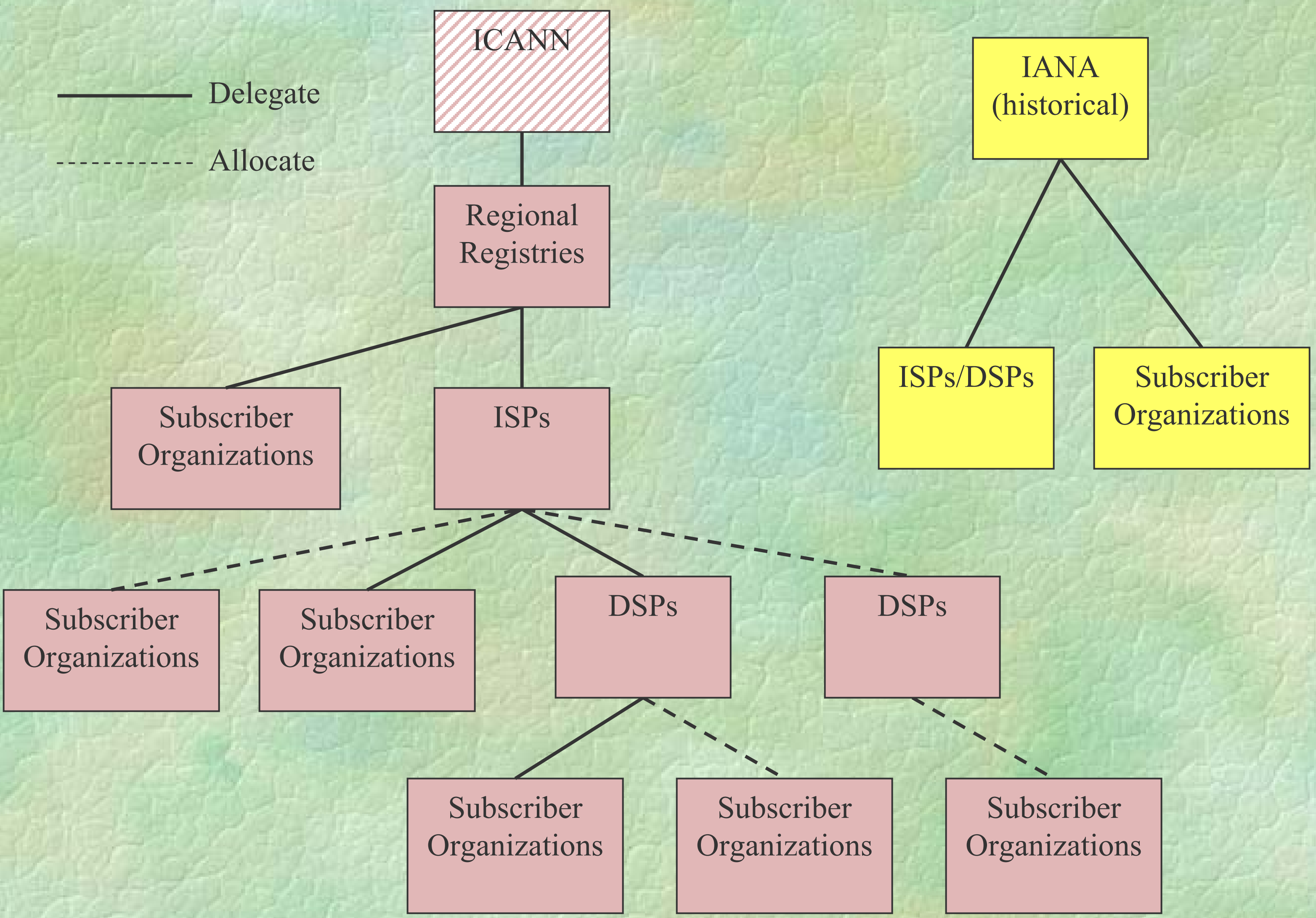
Route Attestation

Attestation Header | Issuer | Certificate ID | Algorithm ID & Signature | Signed Info

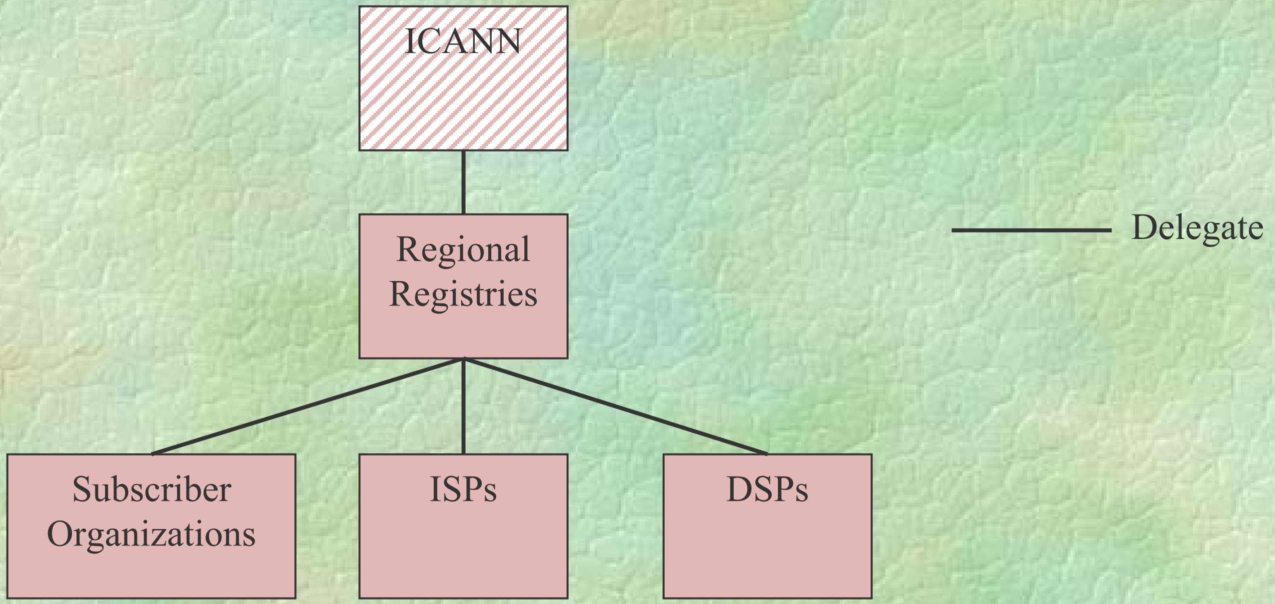
A PKI for S-BGP

- Certificates identify owners of AS numbers and address blocks
- Address blocks in certificates are used to verify address attestations
- Address attestations and AS # certificates are inputs to UPDATE verification
- Other certificates are used for management of repository access control, IPsec (IKE), etc.
- PKI design uses a multi-rooted tree, rooted at regional registries, with delegation to national registries, ISPs, DSPs, subscribers

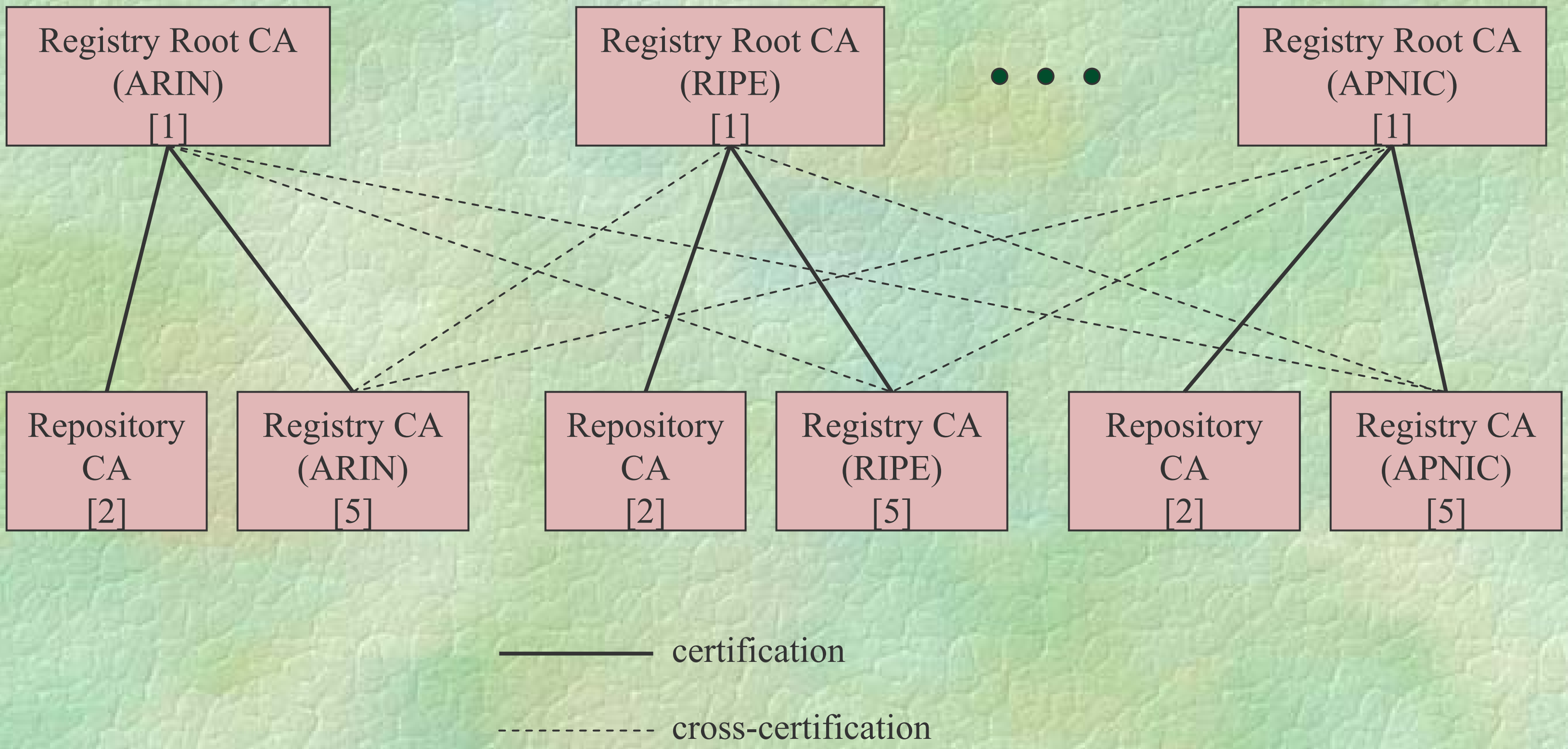
Address Delegation and Allocation



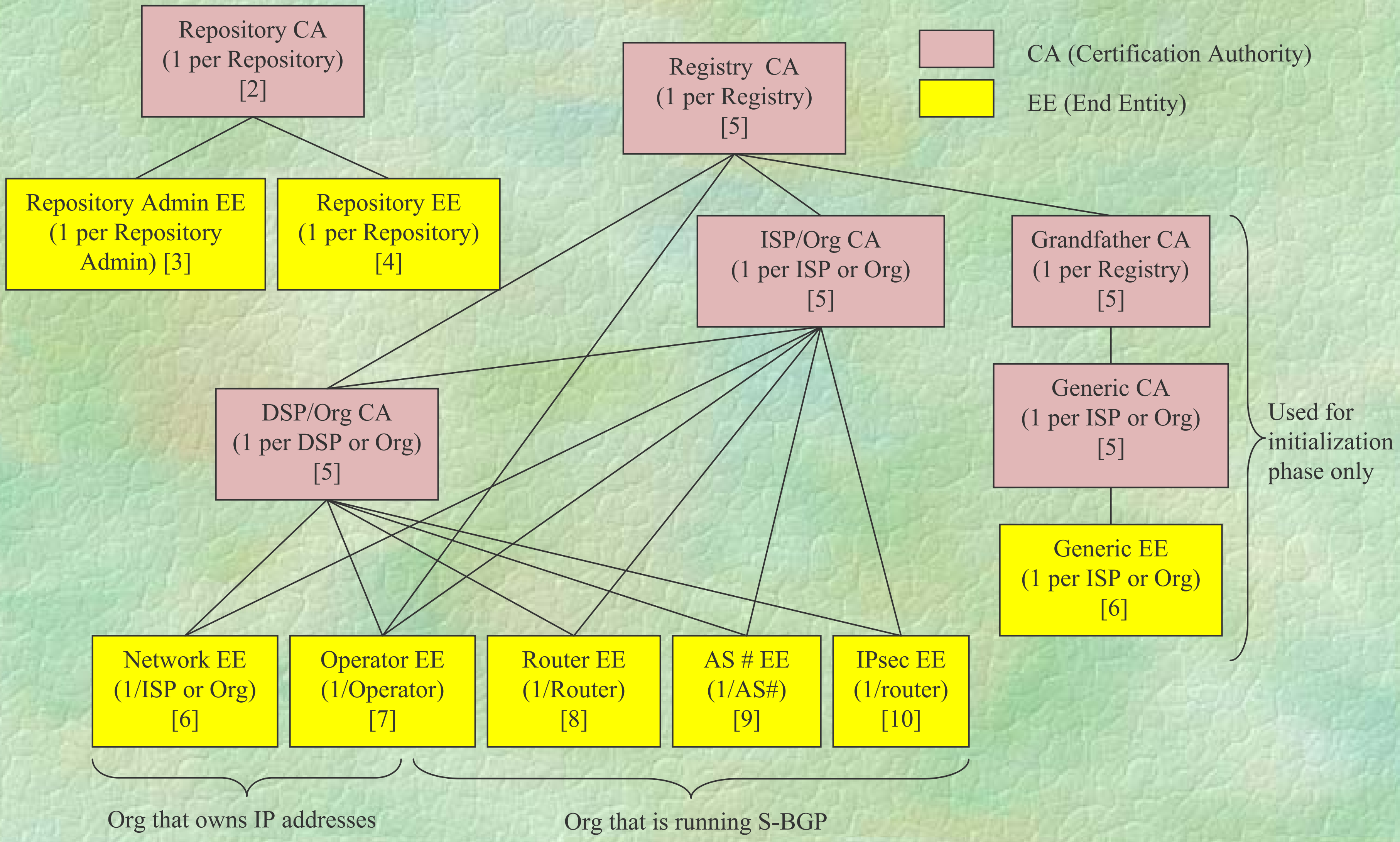
AS Number Delegation Hierarchy



S-BGP PKI: Top Tiers



S-BGP PKI: Registry "Branch"



S-BGP PKI Repositories

- Cannot fit certificates, CRLs, and address attestations in UPDATEs (redundant & too big)
- Solution: use servers at highly available, directly accessible (not routed) sites, e.g., NAPs
- ISPs/DSPs/ORGs upload own new data, download full database, on a daily basis
- NOCs process downloads, send extracts to S-BGP routers, so routers never parse certificates, etc.
- Repositories impose access controls to counter DoS attacks on the digitally signed data they hold, support loose replication among sites

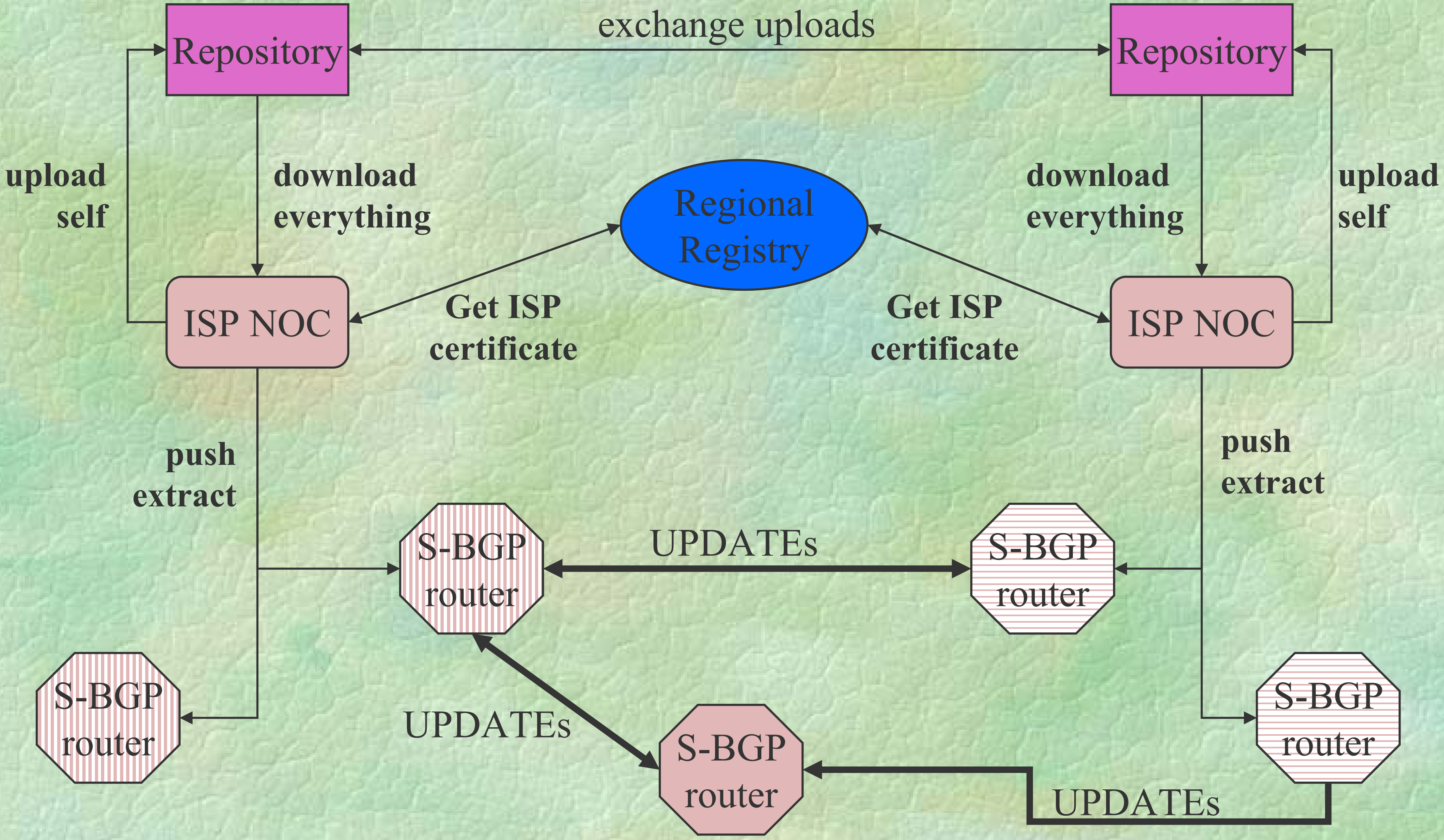
S-BGP NOC Software

- Software to help ISPs manage data required by S-BGP
  - Mini-RA facility for managing organization, router, and operator certificates, generating address attestations
  - Software for uploading & downloading certificates, CRLs, and address attestations to/from repositories
  - Software for validating certificates and address attestations and producing extract for download to routers
- Policy management
  - Software to configure S-BGP routers to know which AS’s implement S-BGP

Impact on BGP Routers

- Processing:
  - Digital signature validation & generation is a new burden on the same CPU that executes BGP, but analysis and limited experiments suggest it's tolerable
- Storage
  - LOCRIBs and ADJRIBs grow to store route attestations
  - Also need to store extracted file of certificates and address attestations
  - Many routers lack enough memory for **full** deployment of S-BGP, but ancillary PC used with multi-hop BGP can address this problem in the near term
  - To speed up restarts, prefer disk backup for RIBs

S-BGP System Interactions



Who Needs to Do What for S-BGP to Become a Reality?

- S-BGP PKI
  - Regional Registries and ISPs need to act as Certification Authorities, issuing certificates to the organizations to whom they have delegated portions of IP address space
  - Repositories must be deployed for S-BGP PKI data
- S-BGP protocol implementation
  - Router vendors need to offer S-BGP software in router products (<u>with enough memory and non-volatile storage</u>)
  - **OR** an ancillary device that implements S-BGP and connects to existing BGP routers needs to be offered
- ISPs need to acquire, deploy, and manage S-BGP products

http://www.ir.bbn.com/projects/sbgp

Any More Questions?