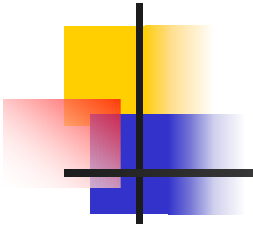
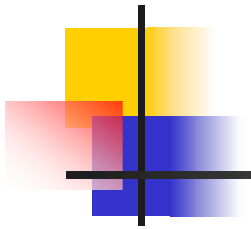
Security Framework for Provider Provisioned Virtual Private Networks



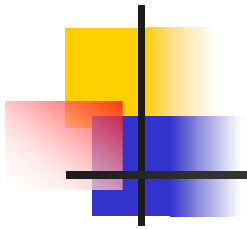
draft-fang-ppvpn-security-framework-00.txt

luyuanfang@att.com
mbehring@cisco.com
fabio@lucent.com
mduffy@quarrytech.com
paul.hitchen@bt.com
paul.night@nortelnetworks.com



Motivations

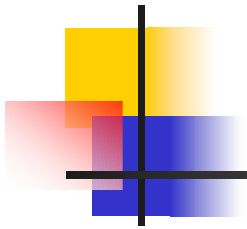
- Security is an intrinsic attribute of PPVPN services
  - In Atlanta, security framework identified as an area that needs to be addressed in PPVPN
- PPVPN users have well-defined security expectations that are specific of the PPVPN service
- PPVPN services raise the bar on required security in the network infrastructure
- Pressing need to define general security framework, user requirements, and corresponding provider requirements for PPVPNs
- Framework can be used to analyze security properties of specific PPVPN solutions and as a guideline for different implementation techniques



Status

Version .00

- Immediate goal is to achieve consensus on scope/organization of the document
  - Requesting feedback from the WG
- Content in many places still in preliminary form, will be expanded/refined in the next version



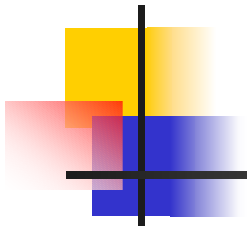
Draft Outline

- Introduction
- PPVPN Security Reference Model
- Security Threats
  - Attacks on the Data Plane, Attacks on the Control Plane
- Defensive Techniques
  - Cryptographic techniques, Sender Authentication, Access Control techniques, Use of Dedicated and Shared Infrastructure, Service Provider Quality Control Processes
- Monitoring, Detection, and Reporting of Security Attacks
- User Security Requirements
  - Isolation, Protection, Confidentiality, Authentication, Integrity, Anti-Replay, [Non-repudiation]
- Provider Security Requirements
  - Protection within the Core Network, Protection on the User Access Link, General Requirements for PPVPN Providers

Open Issues (Please Comment)

Scope of the document:

- To what extent do we define security requirements?
  - WITHIN the scope of the document is to identify the user and provider requirements for different levels of security
    - NOTE: A specific technology may or may not meet all these requirements
  - NOT within the scope of the document is to propose specific mechanisms/solutions/implementation to meet security requirements
- Should we include analysis of specific technologies?
  - e.g., RFC2547, Virtual Router, IPSec VPNs, Layer 2 PPVPNs
  - Check list of specific technologies against the identified user and provider requirements
  - Could be part of this document, or could be a separate draft, or could be part of each individual technology drafts
    - If it is part of this document, it is easier to make it consistent. Also, less risk of delaying progress of existing document



Next Steps/Goals

- Converge on scope
- Identify PPVPN-specific security issues that require additional work
- The goal is to make this draft a reference document for other drafts proposing specific security mechanisms/solutions
- This draft does not intend to stop existing documents from moving forward