[[the most important changes:

- remove item 3 on application development and v4 dependencies (already done)
- remove standardization of mechanisms from item 6
- remove responsibility of existing basic v6 transition mechanisms
- add new milestones and documents

existing issues still:
- "operational/security issue" is still a blurry concept
- should _someone_ be responsible for the protocols? [this is not commonplace at IETF, though]
- the scenarios docs are still there, but they do not trigger any protocol work
]]

Description of Working Group:

The global deployment of IPv6 is underway, creating an IPv4/IPv6 Internet consisting of IPv4-only, IPv6-only and IPv4/IPv6 networks and nodes. This deployment must be properly handled to avoid the division of the Internet into separate IPv4 and IPv6 networks while ensuring global addressing and connectivity for all IPv4 and IPv6 nodes.

The IPv6 Operations Working Group (v6ops) develops guidelines for the operation of a shared IPv4/IPv6 Internet and provides guidance for network operators on how to deploy IPv6 into existing IPv4-only networks, as well as into new network installations.

The v6ops working group will:

1. Solicit input from network operators and users to identify operational or security issues with the IPv4/IPv6 Internet, and determine solutions or workarounds to those issues. This includes identifying standards work that is needed in other IETF WGs or areas and working with those groups/areas to begin appropriate work. These issues will be documented in Informational or BCP RFCs, or in Internet-Drafts.

   For example, important pieces of the Internet infrastructure such as DNS, SMTP and SIP have specific operational issues when they operate in a shared IPv4/IPv6 network. The v6ops WG will cooperate with the relevant areas and WGs to document those issues, and find protocol or operational solutions to those problems.

2. Provide feedback to the IPv6 WG regarding portions of the IPv6 specifications that cause, or are likely to cause, operational or security concerns, and work with the IPv6 WG to resolve those concerns. This feedback will be published in Internet-Drafts or RFCs.

~~3. Publish Informational RFCs that help application developers (within and outside the IETF) understand how to develop IP version-independent applications. Work with the Applications area, and other areas, to ensure that these documents answer the real-world concerns of application developers. This includes helping to identify IPv4 dependencies in existing IETF application protocols and working with other areas and/or groups within the IETF to resolve them.~~

4. Publish Informational or BCP RFCs that identify potential security risks in the operation of shared IPv4/IPv6 networks, and document operational practices to eliminate or mitigate those risks. This work will be done in cooperation with the Security area and other relevant areas or working groups.

5. Publish Informational or BCP RFCs that identify and analyze solutions for deploying IPv6 within common network environments, such as ISP Networks (including Core, HFC/Cable, DSL & Dial-up networks), Enterprise Networks, Unmanaged Networks (Home/Small Office), and Cellular Networks.

   These documents should serve as useful guides to network operators and users on how to deploy IPv6 within their existing IPv4 networks, as well as in new network installations.

6. Identify open operational or security issues with the deployment scenarios documented in (5) and fully document those open issues in Internet-Drafts or Informational RFCs. ~~Work to find workarounds or solutions to basic, IP-level operational or security issues that can be solved using widely-applicable transition mechanisms, such as dual-stack, tunneling or translation.~~

   ~~If the satisfactory resolution of an operational or security issue requires the standardization of a new, widely-applicable transition mechanism that does not properly fit into any other IETF WG or area, the v6ops WG will standardize a transition mechanism to meet that need.~~

~~7. Assume responsibility for advancing the basic IPv6 transition mechanism RFCs along the standards track, if their applicability to common deployment scenarios is demonstrated in (5) above:~~

~~- Transition Mechanisms (RFC 2893)~~

~~- SIIT (RFC 2765)~~

~~- NAT-PT (RFC 2766)~~

~~- 6to4 (RFC 3056 & 3068)~~

~~- This includes updating these mechanisms, as needed, to resolve problems. In some cases, these mechanisms may be deprecated (i.e. moved to Historic), if they are not found to be applicable to the deployment solutions described in (5) or if serious flaws are encountered that lead us to recommend against their use.~~

IPv6 operational and deployment issues with specific protocols or technologies (such as Applications, Transport Protocols, Routing Protocols, DNS or Sub-IP Protocols) are the primary responsibility of the groups or areas responsible for those protocols or technologies. However, the v6ops group will provide input to those areas/groups, as needed, and cooperate with those areas/groups in developing and reviewing solutions to IPv6 operational and deployment problems.

Specifying any protocols or transition mechanisms is out of scope of the WG.

Goals and Milestones:

~~Aug~~

Nov 04 ~~Submit Assisted~~
Adopt IPv6-in-IPv4 Tunneling ~~Requirements to IESG for Info~~
~~Sep 04~~ ~~Publish Enterprise Deployment Solutions~~ **using IPsec** as ~~a~~ WG ~~I-D~~ **item**
Adopt document describing issues with NAT-PT as WG item
Adopt IPv6 Security Overview as WG item
Adopt IPv6 deployment using VLANs as WG item

Dec 04
Adopt ISP IPv6 Deployment Scenarios in Broadband Access Networks as WG item
Adopt IPv6 Network Architecture Protection as WG item

Jan 05
Submit IPv6-in-IPv4 Tunneling using IPsec to IESG for Info
Submit IPv6 deployment using VLANs as WG item

Feb 05
Submit IPv6 Security Overview to IESG for Info
~~Feb 05~~
Submit document describing issues with NAT-PT to IESG for Info
Submit Enterprise Deployment ~~Solutions~~ **Analysiss** to IESG for ~~BCP~~ **Info**

Apr 05 **Submit IPv6 Network Architecture Protection to IESG for Info**

May 05 **Submit ISP IPv6 Deployment Scenarios in Broadband Access Networks to IESG for Info**