इंटरनेट में सुधार

1. पृष्ठभूमि: दुनिया भर में वास्तविक संचार अवसंरचना बनने के लिए तेजी से अपनाने और इंटरनेट की व्यापक तैनाती के बावजूद, सुरक्षा उल्लंघन के प्रति इसकी भेद्यता के बारे में हमेशा एक चिंता का विषय रहा है। अर्थात्, कॉल का उत्तर देने से पहले ही कॉलर का पता लगाने में सक्षम पारंपरिक पीएसटीएन की तुलना में, इंटरनेट को इतना समय, दिन, महीने या उससे भी अधिक समय क्यों लगता है, बस एक बड़े साइबर हमले के अपराधी का अनुमान लगाना शुरू कर देता है?

इस समस्या का कारण इस तथ्य में निहित है कि मूल IPv4 आधारित इंटरनेट डिज़ाइन में उपयोग किए जा रहे सभी IoT को स्पष्ट और विशिष्ट रूप से पहचानने के लिए पर्याप्त बड़ा पता पूल नहीं था। इस बाधा से गतिशील रूप से निपटने के लिए विभिन्न अंतरिम योजनाएं विकसित की गईं। दुर्भाग्य से, उन्होंने अपराधियों के लिए एकदम सही छलावरण भी प्रदान किया, जबकि आम उपयोगकर्ता खुले में बतख बैठे थे। हालांकि नए संस्करण, IPv6 में सभी IoTs की पहचान करने के लिए पर्याप्त से अधिक पते हैं, फिर भी किसी तरह अंतरिम योजनाओं का उपयोग जारी रहा। इसके अलावा, IPv6, IPv4 की तुलना में अधिक जटिल और महंगा है, जिससे कम-भाग्यशाली क्षेत्रों को IPv6 को अपनाने में कठिनाई होती है। इंटरनेट जैसी लगातार उपयोग की जाने वाली किसी भी बड़ी प्रणाली का पूर्ण प्रतिस्थापन प्रश्न से बाहर है। इस गतिरोध को दूर करने के लिए, एक ऐसी योजना जो वर्तमान प्रथाओं के साथ एक दीर्घकालिक प्रणाली की ओर बढ़ाते हुए सह-अस्तित्व में हो सकती है, एकमात्र यथार्थवादी स्थान है।

2. समाधान: सौभाग्य से, यह पता चला है कि IPv4 एड्रेस पूल का एक महत्वपूर्ण हिस्सा (एक सोलहवां, सटीक होने के लिए), जिसे 240/4 नेटब्लॉक कहा जाता है, शुरुआती दिनों से ही "भविष्य के उपयोग" के लिए "आरक्षित" किया गया है। नतीजतन, वर्तमान इंटरनेट उपकरणों में से कोई भी इसका उपयोग करने में सक्षम नहीं है। यह प्रत्येक मौजूदा IPv4 पते से 256 मिलियन IoT की पहचान करने के लिए राउटर के एक नए वर्ग के लिए इसका उपयोग करने का एक अनूठा अवसर प्रदान करता है। उचित रूप से प्रशासित, पूरी तरह से एंड-टू-एंड एड्रेसेबल दुनिया भर में संचार प्रणाली न केवल प्रत्येक ग्राहक को सभी वांछित सेवाएं प्रदान करती है, बल्कि मौजूदा आईपीवी 4 प्रौद्योगिकी के दायरे में साइबर सुरक्षा भेद्यता के मूल कारण को भी कम करती है।

3. चरणबद्ध परिनियोजन: वर्तमान इंटरनेट सर्वर-क्लाइंट ऑपरेशन मोड के साथ मिश्रण करने के लिए, उपरोक्त दृष्टिकोण को एक डीजेनरेटेड प्रारूप के साथ तुरंत तैनात किया जा सकता है, जिसमें 240/4 नेटब्लॉक का उपयोग किया जाता है जैसे कि यह चौथा निजी नेटवर्क एड्रेस पूल था। 192.168/16, 172.16/12 और 10/8 के अतिरिक्त। इस परिचयात्मक चरण में केवल 240/4 नेटब्लॉक को सक्षम करने की आवश्यकता है, मौजूदा IPv4 डिज़ाइन में कुछ भी संशोधित किए बिना।

4. कार्यान्वयन: इस दृष्टिकोण के लिए शायद ही किसी इंजीनियरिंग प्रयास की आवश्यकता होती है। परिनियोजन लागत तुलनीय वर्तमान IPv4 उपकरण के समान है। और, साइबर हमलों जैसे व्यवधानों को कम करने वाली सुव्यवस्थित प्रथाओं के कारण संचालन खर्च कम हो जाएगा:

A. उत्पाद विकास (ProDev): केवल मौजूदा सॉफ्टवेयर कोड अक्षम करें जो 240/4 नेटब्लॉक के उपयोग को अक्षम कर रहे हैं।

B. पूंजीगत व्यय (CapEx): समान हार्डवेयर का उपयोग करके समान सेवा क्षमता के लिए वर्तमान IPv4 उपकरण के समान।

C. संचालन व्यय (OpEx): गतिशील योजनाओं पर निर्भर न होने वाली सुव्यवस्थित प्रथाओं द्वारा कम किया गया।

D. साइबर सुरक्षा: नियतात्मक IoT पहचान (पता) प्रशासन द्वारा बेहतर।

5. प्रस्तावित कार्य:

A. विकास प्रयासों के बिना एक निजी नेटवर्क से इंटरनेट सेवाएं शुरू करने की अंतर्निहित विशेषताओं के साथ, इस प्रस्तावित प्रणाली को किसी भी इच्छुक पार्टी (सरकारी एजेंसियों, व्यवसायों, उद्यमियों, आदि) द्वारा मौजूदा आईपीवी 4 उपकरणों का उपयोग करके उपलब्ध वैध आईपीवी 4 पते से तैनात किया जा सकता है।

B. चूंकि यह दृष्टिकोण सामान्य प्रकृति का है, इसलिए आईटीयू-डी द्वारा इंटरनेट में सुधार के लिए सार्वभौमिक परिनियोजन में इसकी उपयुक्तता के लिए इसकी समीक्षा करने की अनुशंसा की जाती है।

सन्दर्भ:

I. साइबर सुरक्षा भेद्यता स्थिति

https://blog.apnic.net/2021/02/03/the-internet-of-trash/

II. इस प्रस्ताव का एक आसानी से दोहराने योग्य व्यवहार्यता प्रदर्शन।

https://www.avinta.com/phoenix-1/home/RegionalAreaNetworkarchitecture.pdf

III. आईएबी ब्लॉग पर टिप्पणी: प्रोटोकॉल/उत्पाद विकास में अंतिम उपयोगकर्ता की भागीदारी को सुविधाजनक बनाने के लिए इस योजना का प्रस्ताव।

https://blog.apnic.net/2020/08/31/rfc-8890-the-internet-is-for-end-users/

IV आईईटीएफ ड्राफ्ट: इस प्रस्ताव का तकनीकी विवरण

https://datatracker.ietf.org/doc/html/draft-chen-ati-adaptive-ipv4-address-space

V. बौद्धिक संपदा: यूएस पेटेंट संख्या: 11,159,425

शब्दावली, संक्षिप्त नाम और परिवर्णी शब्द:

. CG-NAT: कैरियर ग्रेड नेटवर्क एड्रेस ट्रांसलेशन

. DHCP: डायनेमिक होस्ट कॉन्फ़िगरेशन प्रोटोकॉल

. DNS: डोमेन नाम प्रणाली

. IAB: इंटरनेट आर्कटिक्चर बोर्ड

. IETF: इंटरनेट इंजीनयिरगि टास्क फोर्स

. IoTs: इंटरनेट ऑफ थगि्स

. IPv4: इंटरनेट प्रोटोकॉल संस्करण 4

. IPv6: इंटरनेट प्रोटोकॉल संस्करण 6

. ITU-D: अंतर्राष्ट्रीय दूरसंचार संघ - वकिास क्षेत्र

. PSTN: सार्वजनकि स्वचि्ड टेलीफोन नेटवर्क

. 240/4 नेटब्लॉक: IPv4 एड्रेस पूल 240.0.0.0 से 255.255.255.255 तक, लगभग 256 मलियिन (256M) या एक बलियिन (0.25B) एड्रेस का चौथाई

https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml