ABSTRAK

Najira Duwila,

Studi Strategi Mitigasi Untuk Transisi Jaringan IPV4 ke Jaringan IPV6

Kata Kunci: IPV4, IPV6, Keamanan

IPv4 dikembangkan pada tahun 1981 dan digunakan untuk membuat interkoneksi antar jaringan yang berbeda. Setelah tiga versi, IP mendapatkan nomor versi berikutnya 4 dan kemudian IPv4 dinyatakan sebagai IPv4 ke komunitas internet. Versi pertama IPv4 pada umumnya digunakan untuk memastikan bahwa dua komputer atau dua perangkat jaringan dapat terhubung satu sama lain. Karena ada perluasan dengan kemajuan yang terus berkembang dalam jaringan dan mekanisme internet. internet telah menjadi alat kerja yang sangat penting, yang memungkinkan kita berkomunikasi secara efektif dan secara virtual.

IPv6 tidak sepenuhnya berbeda dari IPv4. Perbedaan antara IPv4 dan IPv6 ada di lima bidang utama, pengamatan dan perutean, keamanan, terjemahan alamat jaringan, beban kerja administrative dan dukungan untuk perangkat seluler. IPv6 juga menyertakan fitur penting, sekumpulan kemungkinan rencana migrasi dan transisi dari IPv4. Sejak 1994, lebih dari 30 RFC IPv6 telah diterbitkan. Mengubah IP berarti mengubah lusinan protocol dan konversi internet, mulai dari bagaimana alamat IP disimpan dalam DNS (sistem nama domain) dan aplikasi, hingga bagaimana datagram dikirim dan dirutekan melalui Ethernet,PPP, Token RING.

Keamanan selalu menjadi isu penting dalam setiap arsitektur jaringan, IPv6 menawarkan fitur keamanan bawaan dengan *header ekstensi* untuk meningkatkan mekanisme keamanannya. Terlepas dari peningkatan IPv6 ini, ada beberapa ancaman jaringan yang terganggu kerena beberapa jenis serangan baru. Keamanan jaringan adalah masalah yang penting, terutama ketika berali ke *NGN* virtual dan selama hubungan jaringan IPv4 dan IPv6. Beberapa jenis serangan mempengaruhi kedua arsitektur IPv4 dan IPv6 dan tidak membeda-beda kan penampilan, beberapa contoh serangan semacam itu adalah serangan yang mengendus, serangan banjir, serangan *man in the middle* dan serangan lapisan aplikasi.

ABSTRACT

Najira Duwila,

Studi Strategi Mitigasi Untuk Transisi Jaringan IPV4 ke Jaringan IPV6

Keywords: IPV4, IPV6, Security

IPv4 was developed in 1981 and is used to create interconnections between different networks. After three versions, IP gets the next version number 4 and then IPv4 is declared as IPv4 to the internet community. The first version of IPv4 was generally used to ensure that two computers or two network devices could connect to each other. Because there is expansion with ever-growing advances in internet networks and mechanisms. The internet has become a very important work tool, allowing us to communicate effectively and virtually.

IPv6 is not completely different from IPv4. The differences between IPv4 and IPv6 are in five main areas, monitoring and routing, security, network address translation, administrative workloads and support for mobile devices. IPv6 also includes important features, a set of possible migration and transition plans from IPv4. Since 1994, more than 30 IPv6 RFCs have been published. Changing IP means changing dozens of internet protocols and conversions, from how IP addresses are stored in DNS (domain name systems) and applications, to how datagrams are sent and routed via Ethernet, PPP, RING tokens.

Security is always an important issue in any network architecture, IPv6 offers built-in security features with extension headers to enhance its security mechanisms. Despite these IPv6 improvements, there are several threats of disrupted networks due to several new types of attacks. Network security is an important issue, especially when switching to virtual NGNs and during IPv4 and IPv6 network connections. Some types of attacks affect both IPv4 and IPv6 architectures and do not differ in appearance, some examples of such attacks are sniffing attacks, flooding attacks, man in the middle attacks and application layer attacks.