

Chapter 14

Asymmetric Extended Route Optimization (AERO)

Fred L. Templin

Association for Computing Machinery (ACM), USA

ABSTRACT

Modern enterprise networks must accommodate mobile devices such as cell phones, tablets and laptop computers. When a mobile device moves to a new access network, it often receives a new Internet Protocol (IP) address. This can disrupt communication sessions and create challenges for locating and tracking mobile assets. The enterprise network should therefore provide each mobile device with a stable IP address or prefix that never changes, but this requires a new mobility architecture. Asymmetric Extended Route Optimization (AERO) supports mobility by modeling the enterprise network as a virtual link through a process known as encapsulation. The AERO system tracks mobile devices through control message signaling and an efficient routing system. AERO maintains optimal routes for roaming devices so that performance is maximized and congestion points are avoided. This chapter describes the AERO system for accommodating mobile devices within enterprise networks.

INTRODUCTION

The Internet was designed long before the advent of modern mobile networked devices. The Internet Protocol (IP) therefore includes no provisions for a device to move between different network points of attachment while still maintaining a stable IP address or prefix. Instead, each mobile device is assigned an IP address that is topologically-inferred, i.e., bound to its current access network point of attachment. This address is called a Topologically-Fixed Address (TFA). If the device moves to a new access network, it must relinquish its former TFA

address and obtain a new one. In some instances, this may disrupt ongoing communication sessions and complicate mobile device tracking. A means of maintaining a stable IP address or prefix across mobility events would therefore result in a more flexible architecture.

In addition to the mobility challenges, the Internet is currently undergoing growing pains since there are now billions of networked devices worldwide with many more on the way. This exponential growth has exhausted the IP version 4 (IPv4) (Postel et al., 1981) address space that is physically constrained to support at most 4 bil-

lion addresses. To remedy this address run-out condition, the Internet Engineering Task Force (IETF) has designed IP version 6 (IPv6) (Deering & Hinden, 1998) with sufficient address space for the foreseeable future. Moreover, mobile devices often require not just a single address but a mobile network prefix that can address multitudes of additional devices and services. Since all public IPv4 prefixes have already been consumed (and since private IPv4 addresses are not routable outside the enterprise) this can only be cleanly accommodated by the expanded address space offered by IPv6.

Modern enterprise networks appear as Autonomous Systems (ASes) in the Internet's Border Gateway Protocol (BGP) routing system (Rekhter, Li, & Hares, 2006), but they are internally organized as an Internet unto themselves. These enterprise networks have an internal routing system and addressing architecture that must be capable of providing pervasive connectivity to ensure the smooth operation of enterprise services. More and more, mobile enterprise network devices connect through multiple diverse wireless (e.g., Wireless LAN or "WLAN") and wired-line (e.g., Ethernet) access technologies. However, each time the mobile device transitions from one access network to another it receives a new TFA and discontinues the use of its old TFA. Without specific mitigations, this can disrupt ongoing communication sessions and can make tracking and locating devices based on IP address challenging.

It has long been known that a technique called tunneling can present a mobile device with a stable Topology-Independent Address (TIA) (or TIA prefix) even if its TFA changes frequently. Tunneling involves the encapsulation of an inner IP packet with a TIA source and/or destination address within an outer IP header that uses TFA addresses. The enterprise network routing system then bases its packet forwarding decisions on the outer TFA address instead of the inner TIA address, i.e., the TFA and TIA address spaces are kept separate. Tunneling introduces additional header bytes that reduce the amount of space available for user

data and consume network bandwidth resources. However, tunneling is seen in widespread and ever-growing use throughout the Internet since the benefits often outweigh the costs.

Tunnels have an ingress endpoint and one or more egress endpoints, but the discovery of an egress endpoint nearest the packet's destination (also known as "route optimization") is required to provide optimum performance and reduce network cost. The selection of an egress endpoint must also be securely coordinated with mobility events to defeat encapsulation-based attacks. Asymmetric Extended Route Optimization (AERO) was therefore designed to address these needs.

The following sections present the AERO routing, addressing and mobility management system. The reader will be introduced to the features that make AERO a natural fit for mobility management and address stability in enterprise networks. AERO is based on a Non-Broadcast, Multiple Access (NBMA) tunnel virtual link model, where all nodes appear as neighbors the same as if they were attached to the same physical link. Enterprise networks will increasingly need to provide support for mobility, route optimization, IPv6 transition, multiple interfaces, security, traffic engineering and many others. They can therefore benefit from adopting the AERO technology as part of their long-term architectural evolution.

BACKGROUND

The NBMA tunnel virtual link model is not new. It was introduced in "6over4" (Carpenter & Jung, 1999), where multicast mapping between the IPv6 and IPv4 multicast address spaces were also required. Since many enterprise networks still do not support multicast, however, a unicast-only variant was introduced in ISATAP (Templin, Gleeson & Thaler, 2005). However, these approaches only connect hosts (not routers) and do not support mobility. Their applicability has therefore been limited primarily to experimental use. Other

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/asymmetric-extended-route-optimization-aero/131371

Related Content

Real Living with Virtual Worlds: The Challenge of Creating Future Interactive Systems

Kirstie L. Bellman (2005). *Developing Future Interactive Systems* (pp. 1-39).

www.irma-international.org/chapter/real-living-virtual-worlds/8258

Black Nerds, Asian Activists, and Caucasian Dogs: Online Race-based Cultural Group Identities within Facebook Groups

Jenny Ungbha Korn (2015). *International Journal of Interactive Communication Systems and Technologies* (pp. 14-25).

www.irma-international.org/article/black-nerds-asian-activists-and-caucasian-dogs/136849

Categorizing Live Streaming Moderation Tools: An Analysis of Twitch

Jie Cai and Donghee Yvette Wohn (2019). *International Journal of Interactive Communication Systems and Technologies* (pp. 36-50).

www.irma-international.org/article/categorizing-live-streaming-moderation-tools/237231

Connecting Real and Virtual Neighbors: The Interplay between Physical Space, Civic Journalism, and Online Community

Robin Blom, Jonathan S. Morgan, Paul Zube and Brian J. Bowe (2013). *International Journal of Interactive Communication Systems and Technologies* (pp. 1-15).

www.irma-international.org/article/connecting-real-and-virtual-neighbors/105653

The Use of 'Stalking Horse' Evaluation Prototypes for Probing DTV Accessibility Requirements

Mark Springett and Richard Griffiths (2007). *Interactive Digital Television: Technologies and Applications* (pp. 131-147).

www.irma-international.org/chapter/use-stalking-horse-evaluation-prototypes/24511