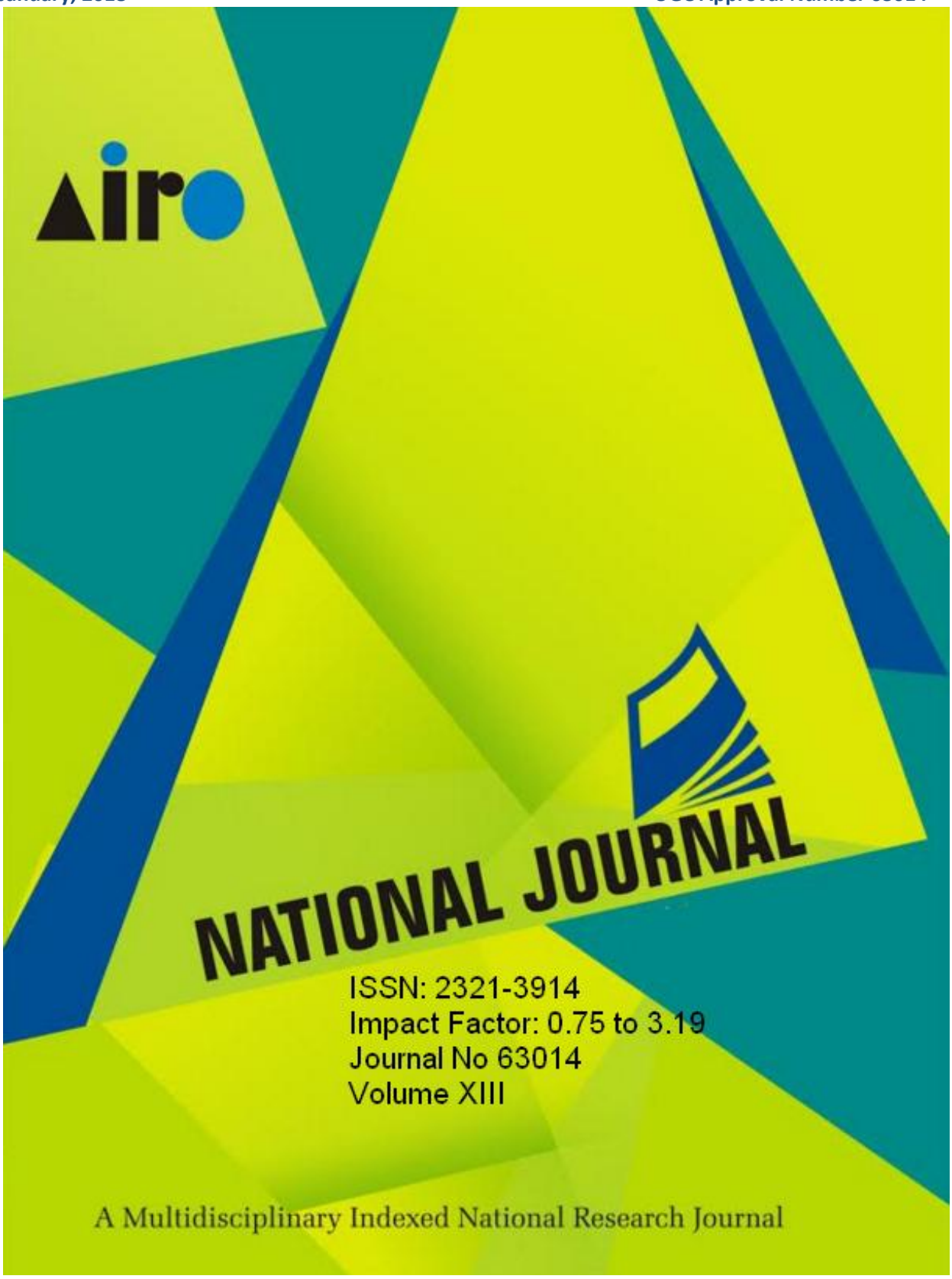
Airo
NATIONAL JOURNAL
ISSN: 2321-3914
Impact Factor: 0.75 to 3.19
Journal No 63014
Volume XIII
A Multidisciplinary Indexed National Research Journal

Airo National Research Journal

Volume XIII, ISSN: 2321-3914
January, 2018

UGC Approval Number 63014

USAGE OF INTERNET PROTOCOL IN COMMUNICATION AND NETWOKING

Divya Shree

Assistant Professor (Resource Person),

Department of computer science and engineering,

UIET, MDU, Rohtak

Abstract

The Internet protocols are the world's most popular open-system (nonproprietary) protocol suite because they can be used to communicate across any set of interconnected networks and are equally well suited for LAN and WAN communications. The Internet protocols consist of a suite of communication protocols, of which the two best known are the Transmission Control Protocol (TCP) and the Internet Protocol (IP). The Internet protocol suite not only includes lower-layer protocols (such as TCP and IP), but it also specifies common applications such as electronic mail, terminal emulation, and file transfer. This paper provides a broad introduction to specifications that comprise the Internet protocols. Discussions include IP addressing and key upper-layer protocols used in the Internet. Specific routing protocols are addressed individually in Part 6, Routing Protocols.

Keywords: *Internet, Protocol, Layer*

Introduction

Internet protocols were first developed in the mid-1970s, when the Defense Advanced Research Projects Agency (DARPA) became interested in establishing a packet-switched network that would facilitate communication between dissimilar computer systems at research institutions. With the goal of heterogeneous connectivity in mind, DARPA funded research by Stanford University and Bolt, Beranek, and

Newman (BBN). The result of this development effort was the Internet protocol suite, completed in the late 1970s. TCP/IP later was included with Berkeley Software Distribution (BSD) UNIX and has since become the foundation on which the Internet and the World Wide Web (WWW) are based.

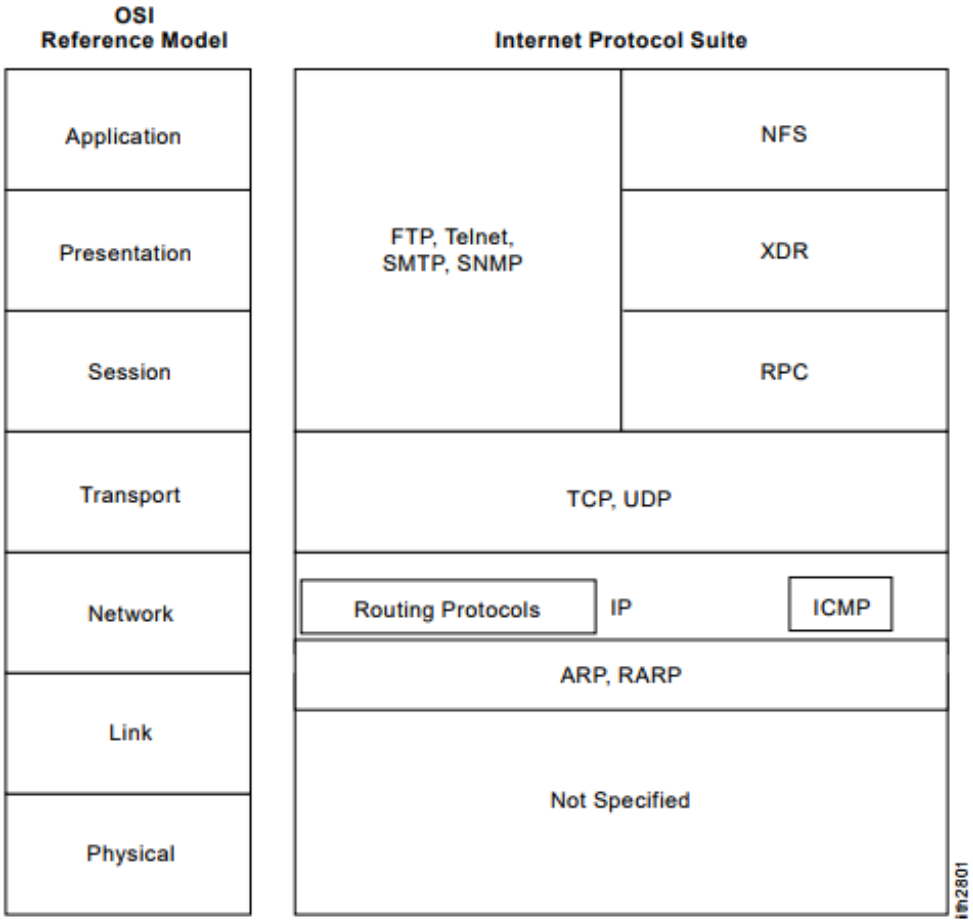

Figure 1: Internet protocols span the complete range of OSI model layers.

The Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed. IP is documented in RFC 791 and is the primary network-layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols. IP has two primary responsibilities: providing connectionless, best-effort delivery of datagrams through an internetwork; and

providing fragmentation and reassembly of datagrams to support data links with different maximum-transmission unit (MTU) sizes.

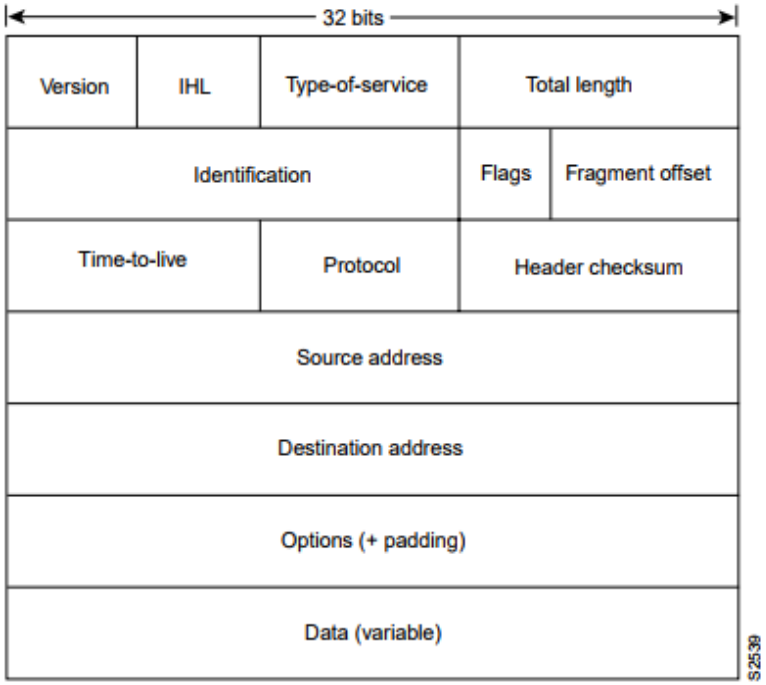

Figure 2: Fourteen fields comprise an IP packet

IP Addressing

As with any other network-layer protocol, the IP addressing scheme is integral to the process of routing IP datagrams through an internetwork. Each IP address has specific components and follows a basic format. These IP addresses can be subdivided and used to create addresses for subnetworks, as discussed in more detail later in this chapter.

Each host on a TCP/IP network is assigned a unique 32-bit logical address that is divided into two main parts: the network number and the host number. The network number identifies a network and must be assigned by the Internet Network Information Center (InterNIC) if the network is to be part of the Internet. An Internet Service Provider (ISP) can obtain blocks of network addresses from the InterNIC and can itself assign address space as necessary. The host number identifies a host on a network and is assigned by the local network administrator.

IP Address Format

The 32-bit IP address is grouped eight bits at a time, separated by dots, and represented in decimal format (known as dotted decimal notation). Each bit in the octet has a binary weight (128, 64, 32, 16, 8, 4, 2, 1). The minimum value for an octet is 0, and the maximum value for an octet is 255.

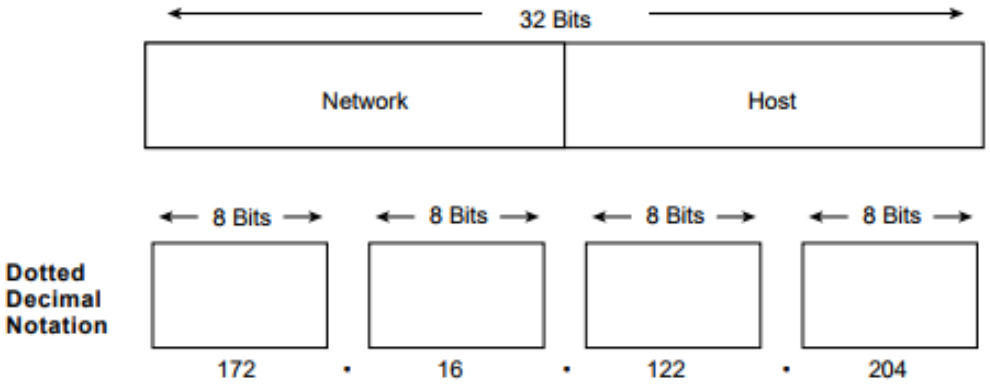

Figure 3: An IP address consists of 32 bits, grouped into four octets

The class of address can be determined easily by examining the first octet of the address and mapping that value to a class range in the following table. In an IP address of 172.31.1.2, for example, the first octet is 172. Because 172 falls between 128 and 191, 172.31.1.2 is a Class B address. Figure 30-5 summarizes the range of possible values for the first octet of each address class.

IP Subnet Addressing

IP networks can be divided into smaller networks called subnetworks (or subnets). Subnetting provides the network administrator with several benefits, including extra flexibility, more efficient use of network addresses, and the capability to contain broadcast traffic (a broadcast will not cross a router). Subnets are under local administration. As such, the outside world sees an organization as a single network and has no detailed knowledge of the organization's internal structure. A given network address can be broken up into many subnetworks. For example, 172.16.1.0, 172.16.2.0, 172.16.3.0, and 172.16.4.0 are all subnets within network 171.16.0.0. (All 0s in the host portion of an address specifies the entire network.)

Subnet masks use the same format and representation technique as IP addresses. The subnet mask, however, has binary 1s in all bits specifying the network and subnetwork fields, and binary 0s in all bits specifying the host field.

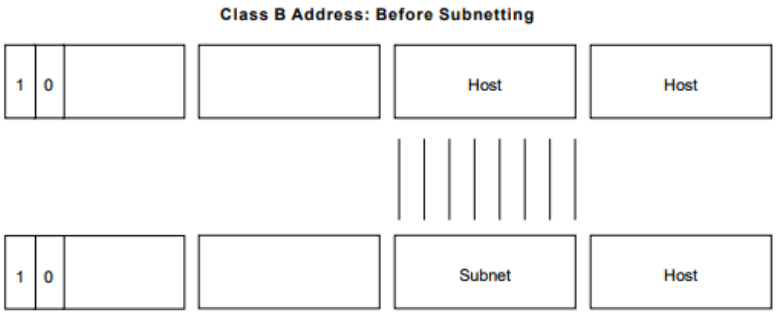

Figure 4: Bits are borrowed from the host address field to create the subnet address field

The default subnet mask for a Class B address that has no subnetting is 255.255.0.0, while the subnet mask for a Class B address 171.16.0.0 that specifies eight bits of subnetting is 255.255.255.0. The reason for this is that eight bits of subnetting or 28 – 2 (1 for the network address and 1 for the broadcast address) = 254 subnets possible, with 28 – 2 = 254 hosts per subnet. The subnet mask for a Class C address 192.168.2.0 that specifies five bits of subnetting is 255.255.255.248.With five bits available for subnetting, 25 – 2 = 30 subnets possible, with 23 – 2 = 6 hosts per subnet.

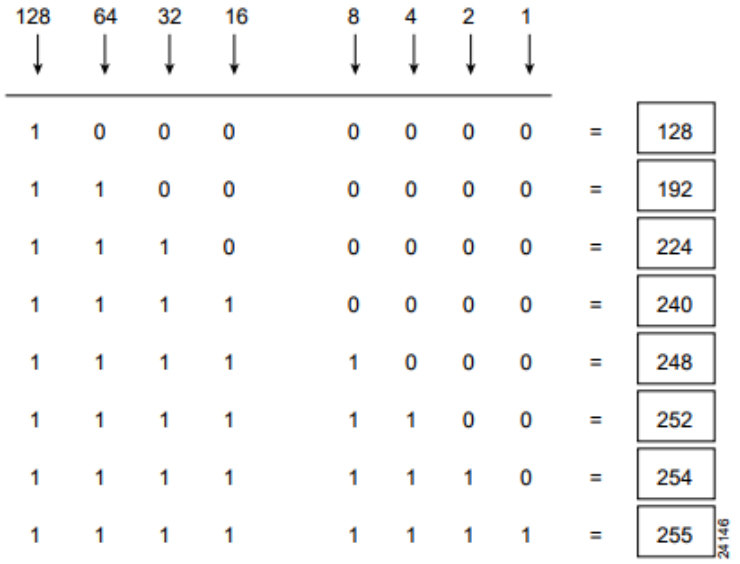

Figure 5: Subnet mask bits come from the high-order bits of the host field

The router performs a set process to determine the network (or more specifically, the subnetwork) address. First, the router extracts the IP destination address from the incoming packet and retrieves the internal subnet mask. It then performs a logical AND operation to obtain the network number. This causes the host portion of the IP destination address to be removed, while the destination network number remains. The router then looks up the destination network number and matches it with an outgoing interface. Finally, it forwards the frame to the destination IP address.

Address Resolution Protocol (ARP) Overview

For two machines on a given network to communicate, they must know the other machine's physical (or MAC) addresses. By broadcasting Address Resolution Protocols (ARPs), a host can dynamically discover the MAC-layer address corresponding to a particular IP network-layer address. After receiving a MAC-layer address, IP devices create an ARP cache to store the recently acquired IP-to-MAC address mapping, thus avoiding having to broadcast ARPS when they want to recontact a device.

If the device does not respond within a specified time frame, the cache entry is flushed. In addition to the Reverse Address Resolution Protocol (RARP) is used to map MAC-layer addresses to IP addresses.

RARP, which is the logical inverse of ARP, might be used by diskless workstations that do not know their IP addresses when they boot. RARP relies on the presence of a RARP server with table entries of MAC-layer-to-IP address mappings.

Internet Routing

Internet routing devices traditionally have been called gateways. In today's terminology, however, the term gateway refers specifically to a device that performs application-layer protocol translation between devices. Interior gateways refer to devices that perform these protocol functions between machines or networks under the same administrative control or authority, such as a corporation's internal network. These are known as autonomous systems.

Exterior gateways perform protocol functions between independent networks. Routers within the Internet are organized hierarchically. Routers used for information exchange within autonomous systems are called interior routers, which use a variety of Interior Gateway Protocols (IGPs) to accomplish this purpose. The Routing Information Protocol (RIP) is an example of an IGP. Routers that move information between autonomous systems are called exterior routers. These routers use an exterior gateway protocol to exchange information between autonomous systems. The Border Gateway Protocol (BGP) is an example of an exterior gateway protocol.

IP routing protocols are dynamic. Dynamic routing calls for routes to be calculated automatically at regular intervals by software in routing devices. This contrasts with static routing, where routers are established by the network administrator and do not change until the network administrator changes them. An IP routing table, which consists of destination address/next hop pairs, is used to enable dynamic routing. An entry in this table, for example, would be interpreted as follows: to get to network 172.31.0.0, send the packet out Ethernet interface 0 (E0). IP routing specifies that IP datagrams travel through internetworks one hop at a time. The entire route is not known at the onset of the journey, however. Instead, at each stop, the next destination is calculated by matching the destination address within the datagram with an entry in the current node's routing table.

ICMP Messages

ICMPs generate several kinds of useful messages, including Destination Unreachable, Echo Request and Reply, Redirect, Time Exceeded, and Router Advertisement and Router Solicitation. If an ICMP message cannot be delivered, no second one is generated. This is to avoid an endless flood of ICMP messages. When an ICMP destination-unreachable message is sent by a router, it means that the router is unable to send the package to its final destination. The router then discards the original packet. Two reasons exist for why a destination might be unreachable. Most commonly, the source host has specified a nonexistent address.

Less frequently, the router does not have a route to the destination. Destination-unreachable messages include four basic types: network unreachable, host unreachable, protocol unreachable, and port unreachable. Network-unreachable messages usually mean that a failure has occurred in the routing or addressing of a packet.

Host-unreachable messages usually indicates delivery failure, such as a wrong subnet mask. Protocol-unreachable messages generally mean that the destination does not support the upper-layer protocol specified in the packet. Port-unreachable messages imply that the TCP socket or port is not available. An ICMP echo-request message, which is generated by the ping command, is sent by any host to test node reachability across an internetwork.

The ICMP echo-reply message indicates that the node can be successfully reached. An ICMP Redirect message is sent by the router to the source host to stimulate more efficient routing. The router still forwards the original packet to the destination. ICMP redirects allow host routing tables to remain small because it is necessary to know the address of only one router, even if that router does not provide the best path. Even after receiving an ICMP Redirect message, some devices might continue using the less-efficient route.

TCP Sliding Window

A TCP sliding window provides more efficient use of network bandwidth than PAR because it enables hosts to send multiple bytes or packets before waiting for an acknowledgment. In TCP, the receiver specifies the current window size in every packet. Because TCP provides a byte-stream connection, window sizes are expressed in

bytes. This means that a window is the number of data bytes that the sender is allowed to send before waiting for an acknowledgment. Initial window sizes are indicated at connection setup, but might vary throughout the data transfer to provide flow control.

A window size of zero, for instance, means "Send no data." In a TCP sliding-window operation, for example, the sender might have a sequence of bytes to send (numbered 1 to 10) to a receiver who has a window size of five. The sender then would place a window around the first five bytes and transmit them together. It would then wait for an acknowledgment. The receiver would respond with an ACK = 6, indicating that it has received bytes 1 to 5 and is expecting byte 6 next. In the same packet, the receiver would indicate that its window size is 5. The sender then would move the sliding window five bytes to the right and transmit bytes 6 to 10.

The receiver would respond with an ACK = 11, indicating that it is expecting sequenced byte 11 next. In this packet, the receiver might indicate that its window size is 0 (because, for example, its internal buffers are full). At this point, the sender cannot send any more bytes until the receiver sends another packet with a window size greater than 0.

REFERENCES

[1] Akiki, P.A., Bandara, A.K., and Yu, Y. Using Interpreted Runtime Models for Devising Adaptive User Interfaces of Enterprise Applications. Proceedings of the 14th International Conference on Enterprise Information Systems, SciTePress (2012), 72–77.

[2] Akiki, P.A., Bandara, A.K., and Yu, Y. RBUIS: Simplifying Enterprise Application User Interfaces through Engineering Role-Based Adaptive Behavior. Proceedings of the 5th ACM SIGCHI Symposium on Engineering Interactive Computing Systems, ACM (2013), 3–12.

[3] Akiki, P.A., Bandara, A.K., and Yu, Y. Cedar Studio: An IDE Supporting Adaptive Model-Driven User Interfaces for Enterprise Applications. Proceedings of the 5th ACM SIGCHI Symposium on Engineering Interactive Computing Systems, ACM (2013), 139–144.

[4] Appert, C. and Beaudouin-Lafon, M. SwingStates: Adding State Machines to the

Swing Toolkit. Proceedings of the 19th Annual ACM Symposium on User Interface Software and Technology, ACM (2006), 319–322.

[5] Balme, L., Demeure, R., Barralon, N., Coutaz, J., Calvary, G., and Fourier, U.J. Cameleon-RT: A Software Architecture Reference Model for Distributed, Migratable, and Plastic User Interfaces. Proceedings of the 2nd European Symposium on Ambient Intelligence, Springer (2004), 291– 302.

[6] Baresi, L. and Ghezzi, C. The Disappearing Boundary Between Development-time and Run-time. Proceedings of the FSE/SDP Workshop on Future of Software Engineering Research, ACM (2010), 17–22.

[7] Bencomo, N., Sawyer, P., Blair, G.S., and Grace, P. Dynamically Adaptive Systems are Product Lines too: Using Model-Driven Techniques to Capture Dynamic Variability of Adaptive Systems. Proceedings of the 12th International Conference on Software Product Lines, Lero Int. Science Centre, University of Limerick (2008), 23–32.

[8] Blouin, A. and Beaudoux, O. Improving Modularity and Usability of Interactive Systems with Malai. Proceedings of the 2nd ACM SIGCHI Symposium on Engineering Interactive Computing Systems, ACM (2010), 115–124.

[9] Blouin, A., Morin, B., Beaudoux, O., Nain, G., Albers, P., and Jézéquel, J.-M. Combining Aspect-Oriented Modeling with Property-Based Reasoning to Improve User Interface Adaptation. Proceedings of the 3rd ACM SIGCHI Symposium on Engineering Interactive Computing Systems, ACM (2011), 85–94.

[10] Blumendorf, M., Lehmann, G., and Albayrak, S. Bridging Models and Systems at Runtime to Build Adaptive User Interfaces. Proceedings of the 2nd ACM SIGCHI Symposium on Engineering Interactive Computing Systems, ACM (2010), 9–18.

[11] Blumendorf, M., Lehmann, G., Feuerstack, S., and Albayrak, S. Executable Models for Human-Computer Interaction. Interactive Systems. Design, Specification, and Verification, Springer-Verlag (2008), 238–251.

[12] Botterweck, G. Multi Front-End Engineering. In H. Hussmann, G. Meixner and D. Zuehlke, eds., Model-Driven Development of Advanced User Interfaces. Springer (2011), 27–42.