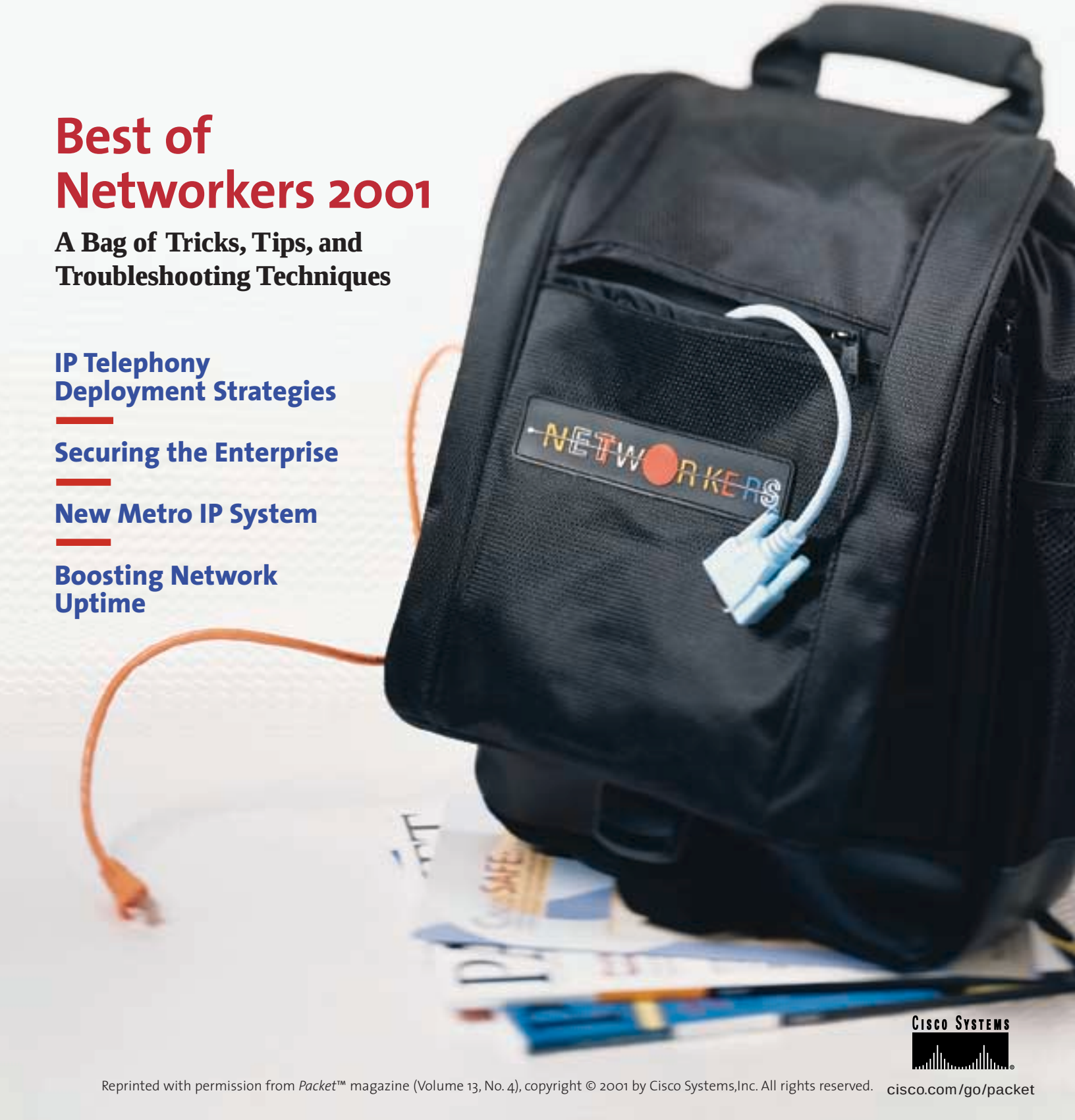
PACKET™

CISCO SYSTEMS USERS MAGAZINE

FOURTH QUARTER 2001



Best of Networkers 2001

A Bag of Tricks, Tips, and Troubleshooting Techniques

IP Telephony Deployment Strategies

Securing the Enterprise

New Metro IP System

Boosting Network Uptime

Cisco Systems

cisco.com/go/packet

Standards Updates

New Option for Authenticated DHCP

Co-authored by Cisco Technical Lead Ralph Droms, RFC 3118 was recently approved as a standards-track protocol by the Internet Engineering Task Force (IETF). RFC 3118 defines a new Dynamic Host Configuration Protocol (DHCP) option that adds authentication to DHCP.

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. With authenticated DHCP, a host can verify that a particular DHCP server can be trusted to provide valid configuration information. Additionally, a DHCP server can use the technique described in RFC 3118 to decide whether a request for DHCP information comes from a client that is authorized to use the network.

Among the chief benefits of RFC 3118 is that DHCP clients and servers are able to authenticate one another, so that rogue and possibly malicious DHCP clients and servers cannot mount denial-of-service attacks or gain unauthorized access to an organization's network. For example, an organization with a wireless LAN (WLAN) might use authenticated DHCP to control the assignment of IP addresses to authorized devices on the WLAN. An authenticating DHCP client can confirm the identity of the DHCP server it chooses in an unsecured network environment such as a cable-based Internet service provider (ISP). The proposed standard defines a technique that can provide both entity authentication and message authentication.

To implement RFC 3118 authentication, network administrators must deploy RFC 3118-compatible software on all computers attached to the network and upgrade DHCP servers to support DHCP authentication. Users must also devise an authentication key scheme and distribute the authentication schemes to all authenticated DHCP clients. After upgraded DHCP clients and servers are in place and the keys have been distributed, the DHCP clients will automatically authenticate themselves.

Cisco is fully supporting RFC 3118 in its product roadmap, and Cisco's DHCP servers will be modified to implement authentication as specified in RFC 3118, according to Droms. In addition, all Cisco hardware products that use DHCP for configuration will be modified to add RFC 3118 authentication to the DHCP client code.

For the full text of IETF RFC 3118, "Authentication for DHCP Messages," visit the URL ietf.org/rfc/rfc3118.txt?number=3118. ▲▲

FURTHER READING

For more information on DHCP, visit the following URLs:

- **"Cisco IOS IP and Routing Configuration Guide"—Configuring DHCP chapter: cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt1/1cddhcp.htm**
- **"Using the Cisco IOS DHCP Server on Access Servers"—sample configurations: cisco.com/warp/public/471/dhcp_access.shtml**

Ethernet in the First Mile Standards Take Shape

In July 2001, the IEEE 802.3 Working Group established the IEEE 802.3ah Ethernet in the First Mile (EFM) task force to develop standards using Ethernet as the Layer 2 protocol of choice, to more efficiently and economically deliver broadband services to subscribers. The IEEE standards body prefers the term "first mile" to describe the connections between business and residential subscribers and the public network's central office or point of presence—an area long referred to as the last mile or local loop.

Network engineers from more than 80 companies, including Cisco, are collaborating on the EFM standards, which will support single-mode fiber-optic and voice-grade, twisted pair cabling. Standards will cover three network topologies: point-to-point copper over existing copper lines at speeds of at least 10 Mbps up to at least 750 meters, point-to-point optical fiber over a single fiber at 1000 Mbps up to at least 10 kilometers, and point-to-multipoint fiber at 1000 Mbps up to at least 10 kilometers.

For more information on the IEEE EFM 802.3ah task force standards objectives, visit the URL ieee802.org/3/efm/index.html. The task force and Cisco's related EFM efforts are covered in greater detail on page 17. ▲▲

Mystified by the IETF?

Let RFC 3160 show you the way. From the IETF's humble beginnings, to the role of working groups and RFCs, to understanding the standards process and related organizations, RFC 3160—"The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force"—lays it all out. To get the full text of "The Tao of IETF," visit the URL ietf.org/rfc/rfc3160.txt?number=3160. ▲▲