



WHITE PAPER

SECURE OPTICAL NETWORKING

INTRODUCTION

Once largely the domain of service providers, optical technology is today helping numerous government and military agencies, research institutions, and enterprises to meet their growing bandwidth and availability requirements. This widespread adoption can be largely attributed to the expanded capabilities of next-generation optical platforms. Offering integrated IP services, storage-extension capabilities, and support for video applications, next-generation platforms provide an attractive solution for deploying highly available, high-speed, multiservice infrastructures. These platforms not only bring tremendous flexibility and improved network efficiency—they also offer the opportunity to take a more coordinated, consistent, and proactive approach to optical networking security.

In the past, optical networking equipment was often protected simply by being kept in locked cages or facilities with restricted physical access. But because today's optical platforms are deployed in more open environments and more closely integrated with the rest of an organization's network, physical protection alone is not enough. Integrated optical and IP environments demand new security considerations beyond the inherent security benefits of optical technology. Organizations must ensure that optical platforms are part of an end-to-end network security strategy, and are just as protected as the rest of the network.

Cisco Systems® has a longstanding reputation as a global leader in network security. Cisco® developed the SAFE Blueprint, a comprehensive framework for defending networks, and has incorporated robust security technologies and features into all Cisco network devices, including optical platforms.

This paper describes the security requirements of optical networks, and the ways in which the Cisco ONS Family of optical network platforms meets the demanding requirements of government agencies, service providers, and enterprises.

THE NEED FOR SECURITY IN OPTICAL NETWORKS

Today's organizations recognize the ever-growing sophistication of network attacks, and are constantly evolving networks and security technologies to thwart them. However, security considerations for optical networks have historically been treated differently than copper networks.

In the past, optical networks were segregated from more open copper networks. Today, the optical-provisioning paradigm has shifted, as optical networks have become more integrated with IP. This shift has provided tremendous advantages. By bringing A-to-Z, "point-and-click" provisioning; automatic network discovery; and other traditional IP features to optical platforms, organizations can now provision optical wavelengths with the same ease and flexibility they would use to provision traditional Ethernet or voice services. However, this paradigm shift also exposes optical networks to new vulnerabilities, including:

- *Increased exposure*—Optical platforms used to be behind a firewall or in a physically secure cage. Now, they may be accessible through the Internet and vulnerable to the same types of attacks as any other network element.
- *Increased interdependence with IP networks*—Previously, optical networks were managed separately from the rest of the copper network. Today, they are integrated, and must be just as secure as every other network element.

- *Greater demand for access from outside parties*—Partners and customers of today’s service providers, enterprises, and government agencies may be given limited management access to the network, enabling a variety of new efficiencies. This accelerates the need for stronger authentication and authorization procedures, and increasingly sophisticated security-policy management to provide tiered levels of access.
- *Rapidly changing workforce*—Organizations face constant fluctuations in the individuals and systems that require access to parts of the network. Organizations must be able to quickly and comprehensively change, add, or remove access.

SECURITY CONCERNS IN DIFFERENT ENVIRONMENTS

When it comes to security features of network elements, all organizations share some basic security requirements. A secure optical network must support:

- Strong identification, authorization, and access-control tools
- Sophisticated logging to provide an audit trail
- Support for new and emerging security standards such as Kerberos, public key infrastructure (PKI) certification, and IEEE 802.11X
- Support for secure communications protocols such as Secure Shell (SSH) Protocol and HTTPS
- Advanced policy-management tools to support a wide range of users and access levels
- Simplified integration with other security services, technologies, and management systems that may be operating within the environment

However, as use of optical network elements has expanded beyond service providers to government agencies and enterprises, these different environments also demand unique security considerations.

SECURITY REQUIREMENTS FOR OPTICAL NETWORKS

To provide a secure solution for service providers, government and military agencies, and enterprises, optical networks should support several critical security features. These include authentication, authorization, and accounting (AAA); authentication protocols such as RADIUS and TACACS/TACACS+; as well as compliance with GR-815 standards.

Authentication, Authorization, and Accounting

The most basic level of protection an optical network must provide is a means of establishing the identity of an individual or system attempting to access the network, and applying the policies that control what that user is authorized to do. This process, along with the process of keeping track of a user’s activity on the network, is referred to as authentication, authorization, and accounting, or AAA. The SAFE Blueprint also refers to a fourth “A,” address management. Address management services provide a means to map IP addresses to individual identities.

AAA capability is supported by AAA servers in the network. Network elements use protocols such as RADIUS and TACACS+ to communicate with AAA servers and respond to user requests for access.

The most complex aspect of AAA is authentication, the process of verifying the identity of a user requesting access. The standard model for authenticating users relies on three factors, referred to as the “three Ws”:

- *What you know*, such as a PIN or password
- *What you have to gain access*, such as a digital token, public key certificate, or smartcard
- *Who you are*, established using a fingerprint, voice, or DNA

Most organizations strive for “two-factor” authentication, though many organizations, especially government and military agencies, are increasingly using biometrics to support all three factors.

Authentication and Authorization Protocols

When an individual or system attempts to gain access to an optical network element, that network element uses a service such as RADIUS or TACACS+ to communicate with authentication and authorization systems and apply security policies.

RADIUS

RADIUS is a client/server protocol that enforces broad-based access control and identity policies for users attempting to access network elements. It combines authentication and authorization into a single service, and has been widely used throughout the networking industry.

In a RADIUS system, a RADIUS server receives client connection requests, authenticates the user, and then returns the configuration information that allows the client to deliver services to the user. A RADIUS server can also act as a proxy client to other RADIUS servers or other authentication servers.

Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. User passwords are sent encrypted between the client and RADIUS server to eliminate the possibility that a password could be intercepted on an unsecured network.

In addition to providing basic RADIUS support, an optical network should support RADIUS for all management interfaces, including Cisco Transport Controller, Transaction Language 1 (TL1), FTP, VxWorks, Telnet, etc.

TACACS/TACACS+

The TACACS protocol and its newest version, TACACS+, are Cisco proprietary protocols that enforce access control and identity policies for administrative network access and configuration functions. TACACS+ provides similar capability to RADIUS, with a few important differences.

Where RADIUS combines authentication and authorization into a single step, TACACS+ breaks down the process into the three separate AAA functions. This provides greater flexibility for incorporating separate, stronger authentication services, such as Kerberos. TACACS+ also supports a wider range of protocols and user-privilege levels than RADIUS. And TACACS+ provides greater confidentiality by encrypting the entire client/server transmission (including username, authorized services, and accounting information), whereas RADIUS encrypts only the password.

Optical networks must support RADIUS and/or TACACS/TACACS+ capability to provide the most options and flexibility for securing network assets.

Compliance with GR-815 Standards

In addition to supporting strong AAA services and protocols, the Cisco ONS Family of network platforms complies with GR-815 standards. While GR-815 was designed specifically to meet the security needs of service providers, network platforms that are GR-815-compliant provide enhanced protection in government or enterprise environments.

GR-815 security features include:

- *Identity and authentication services* for individuals or systems requesting access
- *Enhanced confidentiality* through cryptographic services
- *System access control* to manage communication sessions with the network, including login protection, connection-oriented communications, connectionless communications, and emergency entry
- *Resource access control* to deny users access to network elements without proper authorization

- *Audit log tools* to configure and manage audit trail services
- *Data integrity services* that confirm that communications have not been altered or destroyed in an unauthorized manner
- *System integrity tools* for managing reliability of a network element, including maintaining acceptable levels of service if a security breach occurs
- *Continuity of service tools* for addressing threats that can cause a network element to be taken out of service or perform at a reduced level
- *Security administration tools* for proper use and management of network-element security features, including overriding vendor defaults, ensuring appropriate backup procedures, managing security databases, and generating security audits
- *Nonrepudiation tools* for communicating with networks that require irrefutable proof that a message has been sent or received
- *Password services* that provide greater flexibility to manage password functions

Government and Military Agencies

Growing numbers of government agencies are using or considering using optical networking systems, including the Defense Information Systems Agency (DISA), agencies within the Department of Homeland Security, and even civilian agencies such as the Centers for Disease Control and Prevention. For a government or military organization, the cost of a security breach is more than just lost revenues and productivity. It represents a threat to critical services and, potentially, national security.

In addition to the basic security requirements, government and military networks require the strongest trust and identity services, including support for advanced identifiers, such as biometrics. Government networks, especially for the military, have global footprints and support hundreds of critical information services, so optical networks must integrate security services into a unified, manageable system. That means supporting unified directory services and the ability to configure and disable individual services on any network element. Government and military networks must also provide the flexibility to segregate “black,” or secure and encrypted networks, from more open, nonsensitive “red” networks. The use of RADIUS in these networks provides the security that keeps them secure.

Service Providers

In addition to protecting against internal and external attacks, service providers must take extra precautions to protect against accidental network-configuration changes that could disrupt service to customers. Service providers also must ensure that configuration policies are tightly controlled to enable faster rollout of new services.

Service provider networks must also comply with Telcordia Technologies’ *General Requirements for Network Element/Network System Security* guidelines, commonly referred to as GR-815. GR-815 provides a standardized set of security features and requirements for any network element used in any service provider network across the industry.

Enterprises

As enterprises have adopted more applications using much bandwidth, such as disaster recovery implementations, they have increasingly turned to optical networks. In an enterprise environment, hundreds of individuals and systems may require access to a given network element, so identity and authentication services, access control, and user-based policy services must be extremely sophisticated. Enterprise optical networks must also allow for fast, comprehensive access changes to support a mobile, constantly changing workforce. Use of applications such as RADIUS and TACACS/TACACS+ provide higher levels of security for the optical products that support these secure applications.

FUNDAMENTALS OF NETWORK SECURITY

While optical networks demand some unique security considerations, the fundamental principles of network security apply to any network environment. The SAFE Blueprint from Cisco provides a comprehensive framework for designing, implementing, and maintaining secure networks. Every network solution from Cisco, including the Cisco ONS Family of optical network platforms, was designed in accordance with the following fundamental network-protection concepts outlined in the SAFE Blueprint:

- A true security solution is a process, not a product. An effective security solution must be able to continually evolve and change to accommodate new threats or requirements.
- All access points of the network are potential targets, and must be protected accordingly.
- A successful security solution requires comprehensive, integrated safeguards throughout the entire network infrastructure.
- Security solutions must be modular in order to be scalable, flexible, and cost-effective.
- A layered, in-depth defense strategy ensures more complete protection and minimizes areas of potential vulnerability.

For more information about the SAFE Blueprint, visit www.cisco.com/go/safe.

Securing Network Platforms

The SAFE Blueprint recognizes that router security is critical in any network. Routers control access from every network to every network, advertise networks, and filter who can and cannot gain access. As a result, they present an extremely attractive target for potential attacks.

The Cisco ONS Family of optical network platforms incorporates best practices for router security described in the SAFE Blueprint. These principles require network platforms to support:

- Locking down of Simple Network Management Protocol (SNMP) and Telnet access to the router, and support for more secure access methods such as SSH Protocol
- User authentication and authorization through services such as RADIUS and TACACS/TACACS+
- Ability to disable unneeded services
- Logging at all appropriate levels to provide a comprehensive audit trail
- Authentication of routing updates
- Integration with security and other features of network switches

The Cisco ONS Family also provides additional security benefits by:

- Combining standard network security services with GR-815 services, providing multiple layers of security on every network element
- Allowing organizations to shut off or turn on access to physical ports on the platform
- Providing additional methods for detecting security breaches, because a properly designed optical network will detect any degradation of optical signals
- Allowing organizations to manage optical security within the same management framework as the rest of the network



THE FUTURE OF NETWORK SECURITY

Optical network users, whether service providers, enterprises, or government and military agencies, have unique and growing security needs. Today's optical networks must provide end-to-end protection that is fully integrated with other security services, technologies, and management systems. To provide the greatest flexibility, optical network elements should support advanced AAA services, and provide multiple layers of protection. Optical network security services should also be scalable and standards-based to ensure that organizations can continually evolve security postures as threats and requirements change.

Cisco Systems offers more than just a secure optical platform. By engineering network elements as part of a comprehensive, broad-based security strategy, Cisco can help organizations ensure that optical networks are just as secure as traditional copper networks, and provide robust, multilayered protection.

Security threats will continue to evolve, and optical networks must evolve with them. Cisco is already building a framework for defending networks against tomorrow's security threats. As part of its vision of the Intelligent Information Network, Cisco is developing a model for integrated, collaborative, and adaptive security services that take advantage of the ubiquitous sensing and control capabilities inherent within the network itself. By engineering optical and other network components as part of a coordinated, consistent, and proactive network environment, Cisco can help organizations build a unified threat-defense system that will reduce windows of network vulnerability and lower security-management burden.

For more information about Cisco optical networking solutions, visit: www.cisco.com/go/optical.

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR
Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia
Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

TH/LW8282 04/05

