Advanced Security Features for Catalyst 3750-E and 3560-E Series Switches

Ramesh: Hello, everyone. I’m Ramesh Bijor, Product Marketing Manager for Network Systems at Cisco Systems. Thanks for tuning in to this edition of the LAN switching update. This session is one in a series of LAN switching podcasts where we talk about business and deployment considerations in focused 5- to 10-minute topics.

Today’s session is on the advanced security features of the new Catalyst 3750-E and 3560-E Series Switches.

With me today is Greg Beach, Manager, Product Management at Cisco for the Catalyst 3K switches.

Welcome, Greg.

Greg: Thanks, Ramesh, Glad to be here.

Ramesh: Securing the wiring closet seems to be a focus for a lot of enterprises today. What do you think is causing this change in focus in the wiring closet?

Greg: The need for network security has never been greater. Until very recently, network security in the wiring closet was often limited merely to physical security.

With the advent of increasingly sophisticated attacks and new worms and viruses that spread in a matter of minutes, these policies needed to change.

Because most internal security attacks are launched from the wiring closet, its LAN infrastructure presents a critical first line of defense against security attacks in an enterprise LAN. The Catalyst 3750-E and 3560-E switches help achieve this defense using their advanced security features.

Ramesh: What kind of security attacks can be launched from the wiring closet, Greg?

Greg: The most common attacks that are launched from the wiring closet fit in two main categories: denial-of-service attacks and man-in-the-middle attacks.

Now, denial-of-service attacks can interrupt the entire enterprise network. Denial-of-service attacks can be maliciously launched or unknowingly introduced in the network by an infected PC. Man-in-the-middle attacks allow a hacker to snoop and intercept LAN traffic, compromising network privacy.

Ramesh: So, how can businesses prevent against denial-of-service attacks?

Greg: The first line of defense against denial-of-service attacks is to ensure that malicious users cannot gain access to the network and that devices which are permitted access to the network conform to corporate security policies. This is achieved through Advanced Security features of the Catalyst 3750-E and 3560-E and Cisco Identity-Based Networking Services, or IBNS, and Cisco’s Network Admission Control [NAC] capabilities.

Ramesh: And how do these switches support Identity-Based Networking Services [IBNS] and Network Admission Control [NAC]?

Greg: IBNS is all about combining security and mobility. Authentication and validation occur when a host requests access to the network. The Catalyst 3750-E and 3560-E switches support the standard 802.1x protocol as well as Cisco extensions and enhancements to that standard to allow dynamic, port-based security, providing user authentication. 802.1x with an access control list or VLAN assignment allows for specific identity-based security policies regardless of where the user is connected. This ensures, for example, that I can't get access to your salary, which might be in the HR server.

Ramesh: Ok, how about network admission control?

Greg: Network admission control is all about eliminating or reducing the threat of a virus. Network admission control assesses the endpoint devices, such as a desktop computer or laptop. This assessment might involve ensuring that the device has the latest security patch. This is done in order to prevent the host from accessing the network and pushing that virus onto the network.

Ramesh: Greg, earlier you mentioned man-in-the-middle attacks. How do 3750-E/3560-E switches help prevent against those attacks?

Greg: Ramesh, these switches do not allow a hacker to snoop and intercept LAN traffic, which compromises network privacy.

The 3750-E and 3560-E switches have three features that mitigate man-in-the-middle attacks. The first one is DHCP Snooping. This helps prevent malicious users from spoofing a DHCP server and sending out bogus addresses. The second one is Dynamic ARP Inspection, or DAI. This helps prevent hackers from exploiting the insecure nature of the ARP protocol. And lastly, the third one is IP Source Guard. This helps prevent malicious users from spoofing or taking over another user's IP address.

Ramesh: As always, this is great information. It sounds like 3750-E/3560-E switches definitely have an advantage with the advanced security features. Greg, how can I get more information?

Greg: Well, that's a great question. We have more materials that address both technical issues and business benefits, such as a data sheet, an FAQ, PowerPoint presentations: all these things are at our Website at http://www.cisco.com/go/3750-E.

Ramesh: Thanks, Greg, Well, that wraps it up for today. Thanks for listening, everyone. Stay tuned for another session on the latest in switching news.

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA 05/07