White Paper

Securing the Wiring Closet with Cisco Catalyst Switches

Deploying comprehensive network security in the wiring closet is critical to the resiliency of the entire LAN.

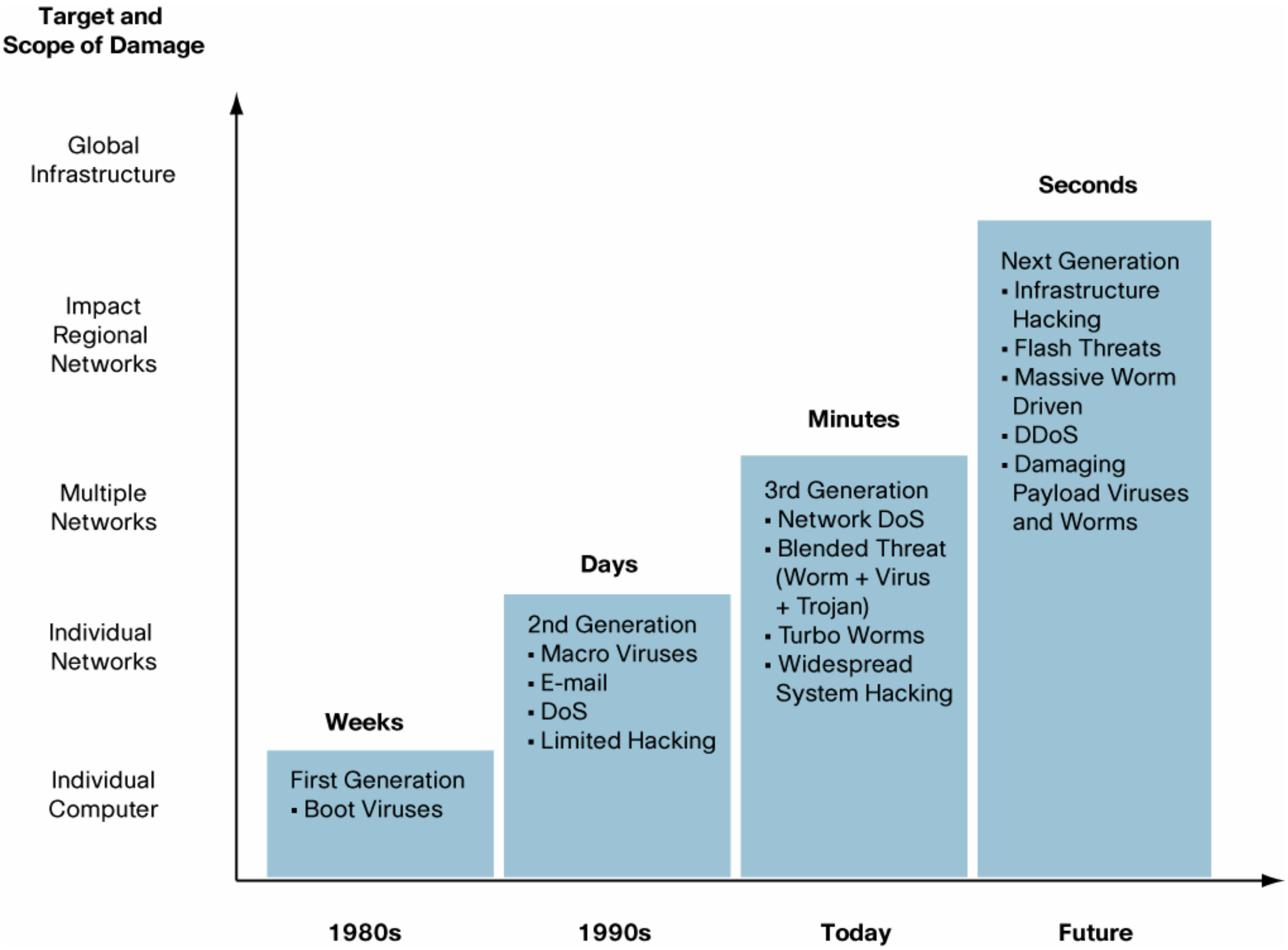
As enterprises continue to rapidly deploy more applications on their IP network to gain the efficiencies of a single, converged network, the demands on the network—and in the wiring closet itself—intensify. The entire network is becoming more critical to business productivity as businesses rely increasingly on their converged networks to securely and reliably deliver a growing number of business-critical, real-time applications.

Historically, network managers have focused on ensuring that the core and distribution layers of the network were well designed, because these were the primary aggregation points in the network. During a failure, these points could impact large numbers of users. With increasing network security threats launched from the wiring closet, however, the wiring closet has now become the new front line of defense to prevent attacks and ensure the health of the entire network. This paper provides an overview of some of the primary security threats in the wiring closet and how Cisco® Catalyst® switches can help mitigate these security threats before they impact the network.

Until very recently, network security in the wiring closet was often limited merely to physical security (for example, preventing someone from gaining access to the switch) or to turning off Ethernet ports when not in use. With the advent of increasingly sophisticated worms and viruses that spread in a matter of minutes, those policies need to change.

Figure 1 shows how the spread and speed of attacks have changed over the years.

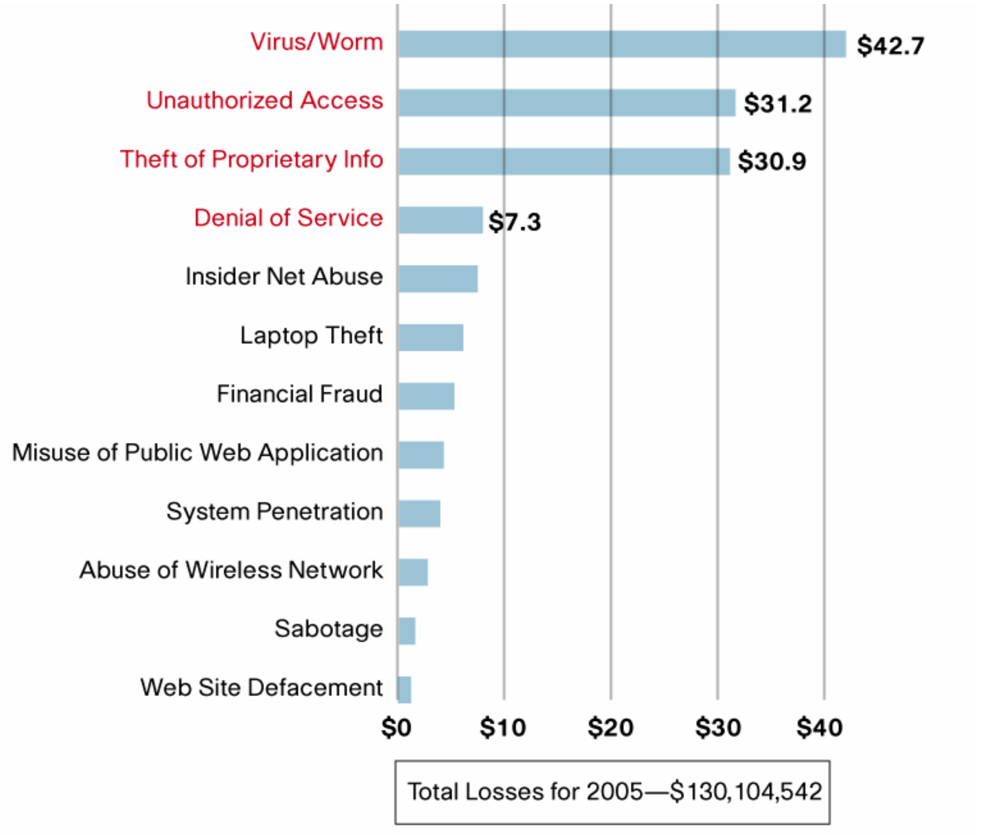
Figure 1. Understanding Security Attacks—Past, Present, and Future



New network viruses and worms appear almost weekly. To protect against these “zero hour” attacks that spread in seconds, the switching infrastructure in the wiring closet must play a significant role in the overall security strategy of an enterprise. In addition to protecting against worms or viruses that attack the switch or network itself, enterprises also need to protect their data as it flows over the LAN. Easy-to-use, menu-based network sniffing tools are readily available on the Web that allow interception of voice and data traffic from the network.

According to the 2005 CSI/FBI survey in the United States, *"Virus attacks continue to be the source of the greatest financial losses. Unauthorized access, however showed a dramatic cost increase …"* See Figure 2 for results of the CSI/FBI survey of losses associated with security incidents.

Figure 2. Loss Due to Computer Security Incidents



Source: CSI/FBI Computer Crime and Security Survey 2005 639 Respondents

The four most costly security incidents listed in Figure 2 are commonly launched from the wiring closet. This new reality requires a renewed focus on security as an integral part of the wiring closet switches. Cisco Catalyst switches offer numerous innovative security features and tools, many of them integrated into the Catalyst software at no additional cost, that help protect and mitigate these top four threats. These integrated features are presented in this document in three categories:

- **Trust and identity**—Prevent unauthorized users and devices from accessing the network
- **Threat prevention**—Prevents virus and worms from disrupting or disabling the network
- **Data-theft prevention**—Prevents data theft such as man-in-the-middle attacks

1.0 TRUST AND IDENTITY

The first line of defense in the campus or branch LAN is to determine who or what is accessing the network, which resources these users should be able to access, and the state of the device attempting to access the network. A “tailgater” can penetrate the physical security of the building by simply walking in behind a trusted employee. When inside, such tailgaters can attach a laptop or other device to the network and intercept confidential information or launch attacks.

Cisco Systems® offers a comprehensive suite of capabilities to help ensure that trust and identity are maintained within the switched network. Trust and identity comprise two fundamental components:

- **Identity-Based Networking Services (IBNS), using 802.1X**, identify and validate the network user or device prior to granting physical access to the network. They then help ensure access to the correct network resources.
- **Network Admission Control (NAC)** identifies the security or compliance of the device attempting to access the network to make sure that the device meets corporate security policy. For example, the device should have the latest OS patch and correct version of antivirus software.

1.1 Identity-Based Networking Services Using 802.1X

The IBNS feature provides one of the first lines of network security defense in the wiring closet. Generally, when users have access to network ports, they can plug into the network and gain unimpeded access to the corporate LAN. But what if the person accessing the network port is unauthorized, such as a visitor or a tailgater who snuck into the building? Depending on their intent, intruders can launch several types of disruptive network attacks when they have uncontrolled access to the network.

Much like companies that require employees to log into applications such as e-mail with a user ID and password, the 802.1X standard uses similar principles to authenticate users and allow access into the network. Cisco has added extensions to 802.1X, resulting in a more robust security feature referred to as IBNS. After it authenticates a user, IBNS can restrict access to various parts of the network depending on the corporate security policy. For example, IBNS might allow users from the engineering department to access the corporate network, but restrict them from the finance and HR portion of the network. Another powerful feature of IBNS is *guest VLAN*. With this feature, visitors or business partners who do not have a valid ID and password can be automatically placed into a restricted VLAN that only permits access to the Internet. This allows partners or visitors to access their data over the Internet while protecting the corporate network and assets.

802.1X is an IEEE protocol that operates through a Cisco Catalyst switch positioned between end stations and a RADIUS server such as the Cisco Secure Access Control Server (ACS). When the end station first connects to an Ethernet port, the Catalyst switch queries the end station for login credentials. If the end station supports 802.1X, it then replies with its credentials (username and password) and the Catalyst switch forwards that information to the Cisco Secure ACS server for authentication. Upon successful authentication, the Catalyst switch enables the port and allows access to the networked resources. Based on the information provided by the Cisco Secure ACS, the Catalyst switch can also enable other policies such as placing users in a particular VLAN while restricting access to other confidential areas of the network. If the client does not support 802.1X or does not authenticate correctly, the client can be placed in a guest VLAN or denied access completely. In situations where the device attempting to access the network does not support an 802.1X client, Catalyst switches support *MAC Authorization*, which allows devices to gain access based on their MAC address if they are defined in the Cisco Secure ACS.

Not only does 802.1X validate users when accessing the network, but in the same way it can also validate network devices that support 802.1X, wireless access points for instance. This prevents employees from connecting rouge access points that compromise network security.

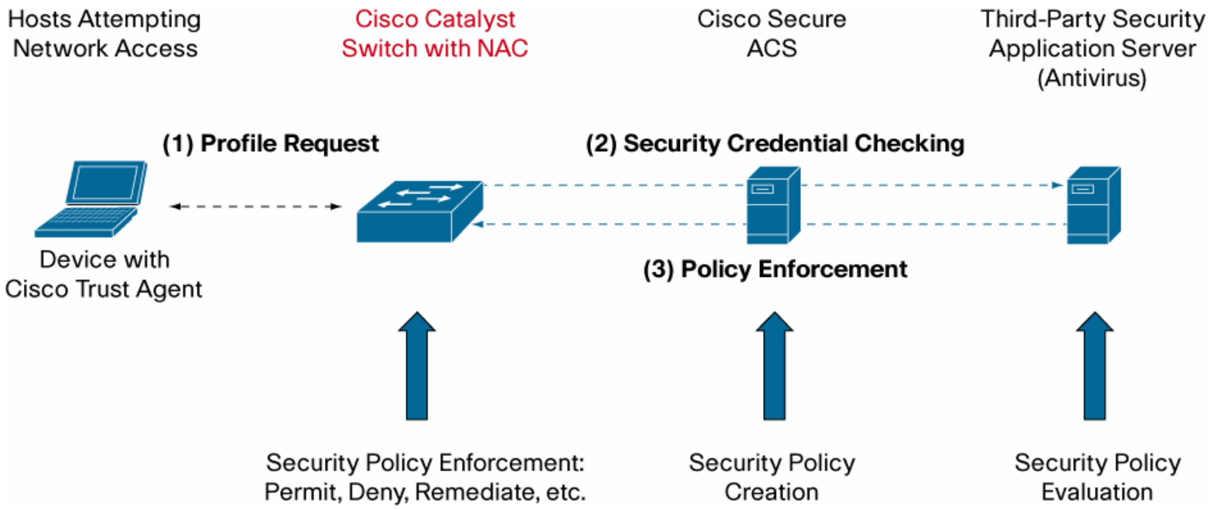
IBNS on Cisco Catalyst switches provides a powerful tool for authenticating users before permitting them access to the corporate network. With the intelligence in the Catalyst switches, IBNS can also provide granular workgroup segmentation depending on company security policy.

1.2 Network Admission Control—NAC

Viruses and worms remain the primary security issue facing organizations today, according to the 2005 CSI/FBI Security Report. The large numbers of annual incidents result in significant financial impact due to downtime, lost revenue, damaged or destroyed data, and loss of productivity. Meanwhile, the pervasiveness of mobile computing has increased these threats. Mobile users are able to connect to the Internet or the office from home or public hotspots—and can easily and often unknowingly pick up a virus and carry it into the corporate environment, thereby infecting the network. Without an accurate way to assess the "health" of a device, even the most trustworthy user can inadvertently expose everyone else on the network to significant risks.

In response, Cisco has developed Network Admission Control (NAC), a comprehensive security solution that brings together leading antivirus, security, and management solutions to help ensure that all devices accessing the network comply with security policy. NAC allows companies to analyze and control all devices coming into the network, such as PCs, laptops, servers, smartphones, and personal digital assistants (PDAs). By ensuring that every endpoint device complies with corporate security policy (that they are running the latest and most relevant security protections, for example), organizations can significantly reduce endpoint devices as a common source of infection or network compromise. Figure 3 shows a high-level overview of NAC.

Figure 3. Overview of Network Admission Control


Hosts Attempting Network Access
Cisco Catalyst Switch with NAC
Cisco Secure ACS
Third-Party Security Application Server (Antivirus)
(1) Profile Request
(2) Security Credential Checking
Device with Cisco Trust Agent
(3) Policy Enforcement
Security Policy Enforcement: Permit, Deny, Remediate, etc.
Security Policy Creation
Security Policy Evaluation

With NAC enabled on the Catalyst switches, whenever an endpoint device attempts to make a network connection, the Catalyst switch automatically requests a security profile of the endpoint device (see Figure 3). The Catalyst switch then forwards the profile information to the Cisco Secure ACS (2). It is then compared to network security policy on the Cisco Secure ACS, and the level of device compliance to that policy determines how the Catalyst switch responds to the request for admission (3). The switch can simply permit or deny access, or it can also quarantine a noncompliant device by redirecting it to a remediation server, where it may be updated with components that will bring it into policy compliance.

By checking the "health" of a device before permitting access to the network, NAC dramatically improves network security by helping ensure that all network devices conform to security policy. Limiting the potential of end devices to introduce worms and viruses into the network enables enterprises to significantly increase network resilience while reducing operating expenses typically related to manually identifying and repairing noncompliant or infected systems.

2.0 PROTECTING AGAINST DoS THREATS IN THE WIRING CLOSET

Denial-of-service (DoS) attacks are a significant and growing threat to businesses worldwide. These attacks, which are often initiated with readily accessible tools and are difficult to detect, can quickly incapacitate a targeted business, costing thousands, if not millions, of dollars in lost revenue and productivity. DoS attacks are often launched from the wiring closet by worms or viruses that have arrived by an employee’s infected device, either intentionally or, most commonly, unknowingly. DoS attacks cause significant network instabilities by overloading network switches. Worms, in particular, can spread alarmingly fast. For example, a recent Structured Query Language (SQL) Slammer Worm doubled every 8.5 seconds. In the span of 3 minutes, it could perform 55 million scans per second, bringing a 1-Gbps link to a standstill in just 1 minute.

DoS attacks flood the network with malicious traffic, thus shutting out legitimate traffic that the switch needs to process, such as routing updates or spanning-tree bridge protocol data units (BPDUs), leading to network instability or actual network crashes. Cisco Catalyst switches provide an array of features in the wiring closet to defend against these disruptive DoS attacks.

- **Port Security**—Used to prevent MAC-based attacks. Lets administrator restrict the number of MAC addresses that can transmit from a switch port.
- **Scavenger Class QoS**—Used to reprioritize traffic from systems with abnormally high traffic rates that could be potential DoS attackers.
- **Control Plane Policing**—Controls the type and quantity of traffic that is forwarded to the CPU for processing.
- **NetFlow Anomaly Detection**—These flow-based statistics identify DoS attacks and apply port-level access control lists (ACLs) to mitigate the attack.

2.1 Port Security

A simple DoS attack can be launched by a PC with shareware software available on the Internet. Armed with such software, a PC can generate tens of thousands of MAC addresses on an Ethernet port. As the switch attempts to learn and store these new addresses, its finite CAM tables (tables that store MAC forwarding information) fill up. When the CAM table is full, the switch cannot learn additional addresses, so the data from new addresses is flooded throughout the Layer 2 VLAN domain. This results in poor network and end-station performance.

To prevent this kind of attack, the Cisco Catalyst switch offers the *Port Security* feature, which limits the number of MAC addresses (user-defined) that can be learned from a given port. If the limit is exceeded, the Cisco Catalyst switch will disable the port to protect the network.

Port Security helps ensure that a limited number of MAC addresses are learned at a given port. In this way, a DoS attack based on MAC flooding can be stopped immediately.

2.2 Scavenger Class QoS

A DoS or worm attack can also flood network links, filling up device buffers and the Ethernet link between switches. This in turn impairs voice quality and slows application performance considerably. Many of these worms scan the network, using many different TCP or User Datagram Protocol (UDP) flows, thereby significantly increasing the volume of flows on the network—a dangerous situation. The remedy is to use the Cisco Catalyst *Scavenger Class QoS* feature, which restricts these flows on a link.

When using Scavenger Class QoS, the Catalyst switch defines scavenger-class traffic as traffic that, over a sustained period of time, bursts or transmits above a defined threshold—something that a properly functioning end station would not do. The first detection is not enough to drop packets, however, because it may be a legitimate burst. It is unlikely, though, that a port would see high user traffic sustained over time. That traffic is then marked as “scavenger” and placed in the lowest-priority queue. The queue is also configured to be shallow, so that queue overflows are frequent. The result is that TCP-based flows are throttled back, and UDP flows are dropped. In this way, voice and other legitimate traffic are protected.

2.3 Control Plane Policing

Besides attacking the forwarding tables of the switch or the links, DoS attacks also target the switch's CPU directly. They accomplish this by sending control information, such as Address Resolution Protocol (ARP) packets, to the CPU for processing. With a finite amount of processing power, the CPU can become overloaded, resulting in real control packets, such as routing updates or BPDUs, being dropped.

Cisco Catalyst switches offer user-defined Control Plane Policing, also known as rate limiting, to help mitigate this type of attack. When Control Plane Policing is enabled on the CPU, excess packets above a certain rate are dropped, ensuring that the CPU can manage (or most likely drop) the malicious packets without failing. This allows the CPU to continue performing normal system tasks—even while under attack.

2.4 NetFlow Anomaly Detection

The speed and unpredictability of DoS attacks require not only that Catalyst switches *react* to attacks, but that they also proactively prevent them in the first place. The purpose of the Cisco *NetFlow Anomaly Detection* feature is to detect worm-related anomalous behavior in the wiring closet early and take action quickly to contain it before it spreads to the rest of the network.

NetFlow is a Cisco technology integrated into Catalyst switches for monitoring network traffic. It provides network administrators with access to detailed traffic-flow information from their data networks. NetFlow data, when used in conjunction with the Cisco Security Monitoring, Analysis and Response System, provides customers with a powerful tool to identify traffic anomalies in the network. It alerts network administrators to quickly identify a potential attack before it impacts the network.

The Cisco Security Monitoring, Analysis and Response System (CS-MARS) builds a detailed network baseline based on the NetFlow traffic statistics from the network. When a DoS attack occurs, baseline traffic thresholds are exceeded, and the system identifies it as an anomaly and can take simple action to alert the network administrator or shut down the port.

The Embedded Event Manager (EEM) feature, available on the Cisco Catalyst 6500 Series Switches can work in conjunction with NetFlow. EEM is a policy-based framework embedded in the switch that monitors important system events and acts when an event is triggered. EEM can trigger immediate action based on anomalous NetFlow traffic.

NetFlow Anomaly Detection provides network administrators an invaluable tool to quickly identify and contain attacks before they spread into the rest of the network.

3.0 DATA THEFT AND MAN-IN-THE-MIDDLE-ATTACKS

Unlike attacks that disrupt the network, many attacks are directed against users and servers—and they often can go undetected. These attacks, often called man-in-the-middle attacks, use common tools that can be downloaded from the Internet and easily launched from the wiring closet. The tools use a variety of mechanisms that allow a malicious user to spy on other employees, managers, or executive staff, resulting in the theft of proprietary information as well as privacy violations.

Cisco Catalyst switches offer a set of integrated features to thwart these attacks from the wiring closet and protect data and user integrity.

- **DHCP Snooping** helps ensure that only authorized Dynamic Host Configuration Protocol (DHCP) servers issue IP addresses; it maintains an IP address/port binding table that is also used by other security features.
- **Dynamic ARP Inspection** intercepts addressing information on the network and validates it with the binding table.
- **IP Source Guard** prevents a malicious user from hijacking a neighbor's IP address.

3.1 DHCP Snooping

One of the techniques hackers use to gain access to private information is to spoof the DHCP server—in effect, to trick user machines into "assuming" that the hacker's PC is the DHCP server. This allows the intruder to give out false DHCP information for the default gateway and name servers (Domain Name System [DNS] and Windows Internet Naming Service [WINS]), which points clients to the hacker's machine. The hacker then becomes the "man in the middle" and is able to gain access to confidential information such as username and password pairs, while the end user is oblivious to the attack.

The DHCP Snooping feature on Catalyst switches allows companies to prevent this type of attack by helping ensure that only defined "trusted" ports on a Catalyst switch can process DHCP requests and issue IP addresses. This prevents all other ports form issuing DHCP addresses, thus mitigating the risk of a rogue DHCP server issuing invalid addresses.

Another important function performed by DHCP Snooping is to build a *DHCP Binding Table* that maps a client's MAC address, IP address, VLAN, and port ID. This table is also used as a foundation for the next two Cisco Catalyst features that further prevent man-in-the-middle attacks.

3.2 Dynamic ARP Inspection

One of the most common man-in-the-middle attacks takes advantage of ARP. By employing easy-to-use and readily available tools, hackers can exploit a security hole in ARP that allows an end station to send out a gratuitous and unsolicited ARP packet. By sending out gratuitous ARP packets, malicious users can spoof either another end station or the default gateway, placing themselves between the user and the true default gateway. This is often referred to as *ARP poisoning*.

ARP poisoning allows malicious users to sit between the innocent user and the default gateway and spy on all data being sent on the network by the user. The problem is that neither the default gateway nor the end user is aware that this attack is taking place. Therefore, malicious users can continue spying on private information for as long as they want, allowing them time to access passwords, e-mail messages, transactions—even IP voice calls.

Cisco Catalyst switches offer a feature called *Dynamic ARP Inspection* (DAI) to stop this attack. DAI intercepts all incoming ARP packets and examines them for proper MAC-to-IP bindings. This is done by using the DHCP binding table created by the DHCP Snooping feature. If an ARP packet arrives on a port, it is matched against the DHCP binding table. If a match is found, the ARP packet is permitted to proceed; if no match is found in the DHCP binding table, the ARP packet is dropped.

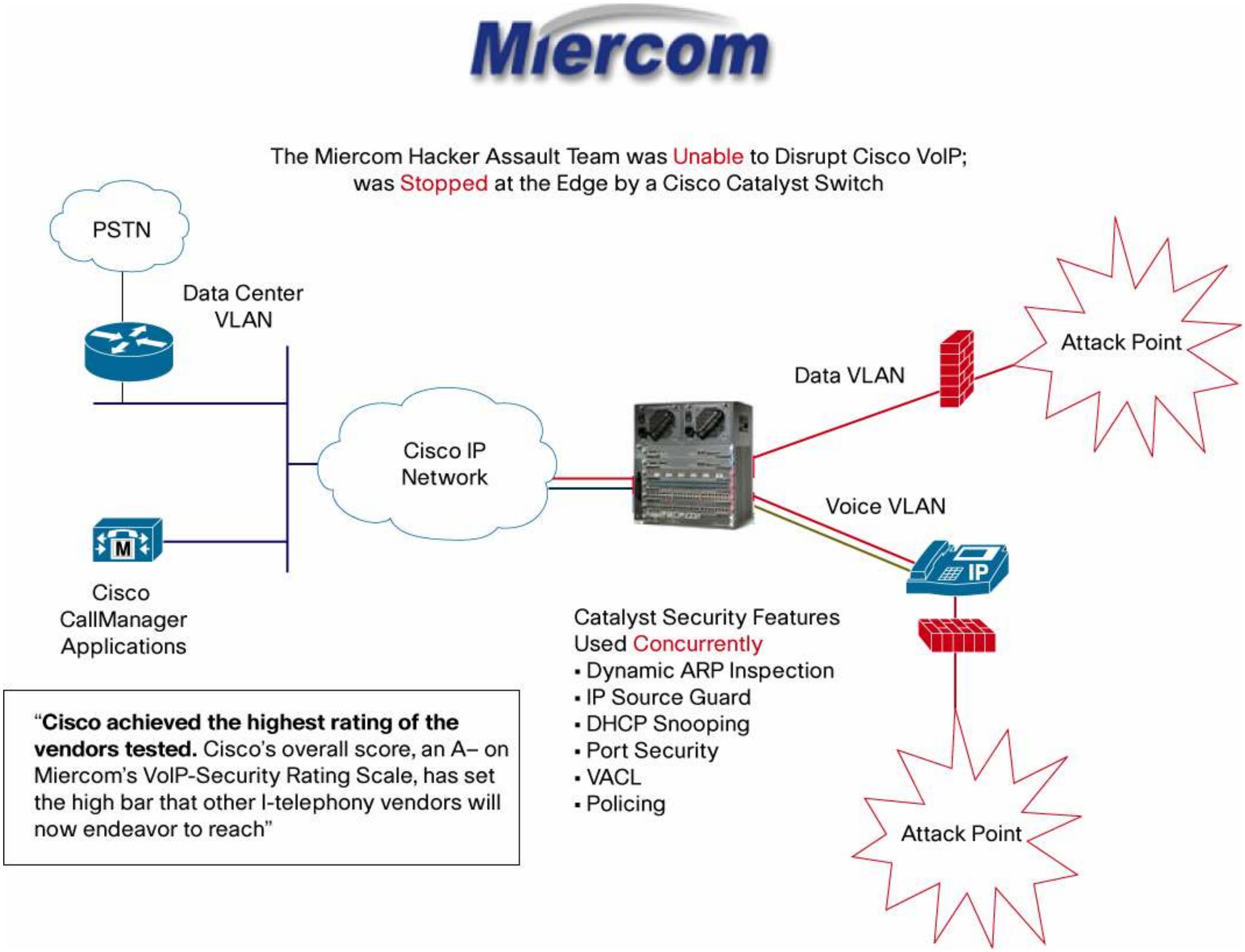
3.3 IP Source Guard

Another potential threat to privacy is the spoofing of an innocent user's IP address. This enables a malicious user to appear to be on another subnet and, therefore, to bypass an access control list (ACL) that might restrict computers on the malicious user's actual network.

IP Source Guard takes advantage of the DHCP binding table created during DHCP Snooping to check the binding of an IP address to a MAC address, its port, and its associated VLAN. It does this by automatically configuring an ACL on the switch port that limits the port to only transmit traffic that originates from the authorized IP address for that port. If a device attempts to transmit data with an altered IP address, the Catalyst switch will disable the port.

Miercom conducted a security test to analyze how secure voice traffic is over an IP network. Figure 4 shows the basic topology of the test. Miercom enabled the man-in-the-middle attack mitigation features discussed previously and attempted to intercept voice traffic. After approximately three days of hacking attempts, Miercom network engineers were unable to intercept the voice traffic. Cisco Catalyst switches received the highest rating of all the vendors tested.

Figure 4. Miercom VoIP Security Test Topology



"**Cisco achieved the highest rating of the vendors tested.** Cisco's overall score, an A– on Miercom's VoIP-Security Rating Scale, has set the high bar that other I-telephony vendors will now endeavor to reach"

Cisco Catalyst switches provide inherent capabilities to stop man-in-the-middle attacks and prevent data and voice traffic interception and theft. To thwart these attacks, enabling these features in the wiring closet is highly recommended to help protect privacy within the network and help mitigate theft of valuable or confidential information.

SUMMARY

The wiring closet switching infrastructure is the first line of defense for campus networks to protect an organization's data, applications, and the network itself —and the features that enable this defense are a critical part of the enterprise-wide Cisco Self-Defending Network. With the innovative integrated security features of the Cisco Catalyst switches, enterprises can use their wiring closet switching infrastructure to effectively identify, respond, and adapt to security threats before they can cause damage across the enterprise.

Table 1 lists the security features that are supported on specific Cisco Catalyst platforms. These features represent a subset of the numerous features that are available on Cisco Catalyst switches. For the purposes of this paper, only primary features are highlighted. For a comprehensive list of features, please see the Cisco Catalyst Switching Guide: http://www.cisco.com/en/US/products/hw/switches/

Table 1. Security Features on Cisco Catalyst Switches

Security Feature	Catalyst 6500 Series	Catalyst 4500 Series	Catalyst 3750/3560 Series
Trust and Identity			
IBNS (802.1X)	Yes	Yes	Yes
MAC Authentication	Yes	Yes	–
NAC	Yes	Yes	Yes
Threat Prevention			
Port Security	Yes	Yes	Yes
Scavenger Class QoS	Yes	Yes	Yes
Control Plane Policing	Yes	Yes	–
NetFlow Anomaly Detection	Yes	Yes	–
Embedded Event Manager	Yes	Yes	–
Data Theft Prevention			
DHCP Snooping	Yes	Yes	Yes
Dynamic ARP Inspection	Yes	Yes	Yes
IP Source Guard	Yes	Yes	Yes

CISCO SYSTEMS

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

Printed in the USA

C11-340443-00 03/06