

## At-A-Glance

### Need for Security in the Wiring Closet

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, security must be heightened in the wiring closet. The wiring closet LAN infrastructure presents a critical first line of defense against security attacks in an enterprise LAN.

With the pervasiveness of mobile devices, employees frequently connect outside of the corporate network and can unknowingly pick up a virus and carry it into the corporate environment, thereby infecting the network. These viruses result in lost productivity and increased operational expenses.

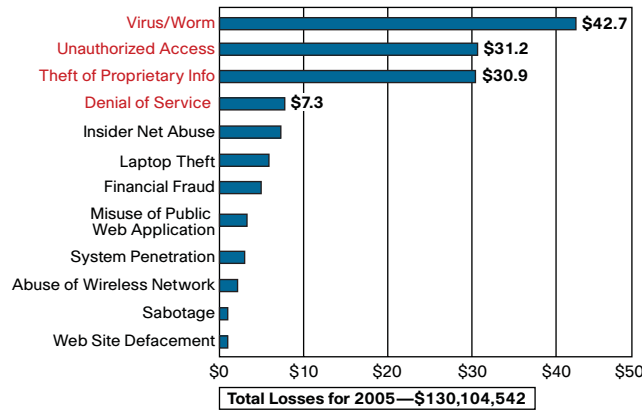
“Tailgaters” can penetrate the physical security of a building by simply walking in behind a trusted employee. They can therefore gain access to the network, intercept confidential data, or intentionally disrupt the network. Today, the skill level required to launch security attacks is minimal. Readily available, menu-based hacker tools are available on the Internet, making sophisticated attacks simple.

Cisco® Catalyst® switches offer rich, industry-leading security features to help mitigate security threats in the wiring closet before they propagate to the rest of the network. These switches deliver the following set of features:

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

According to the 2005 CSI/FBI survey, virus attacks continue to be the source of the greatest financial losses. Unauthorized access, however, showed a dramatic cost increase. See Figure 1 for results of the CSI/FBI survey of losses associated with security incidents.

**Figure 1. Loss Due to Computer Security Incidents**



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

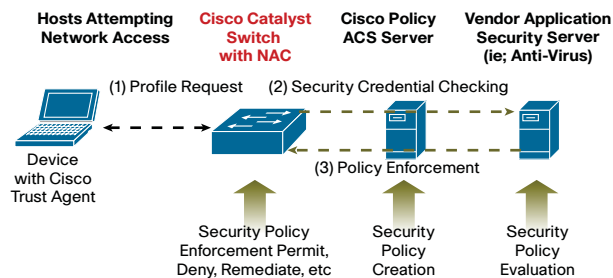
### Trust and Identity

*How do I ensure users and devices connecting to the network are trusted?*

Trust and identity features provide the first line of defense, permitting network access only to trusted users and devices that comply with corporate policy.

- **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 can then help ensure access to the correct network resources.
- **Network Admission Control (NAC)**—Identifies the security compliance of any device (PC, PDA, etc.) attempting to access the network, to make sure that the device meets corporate security policy (for example, having up-to-date software patches, antivirus software, etc.). See Figure 2.

**Figure 2. Network Admission Process with NAC**



### Threat Prevention

*How do I prevent denial-of-service (DoS) attacks?*

DoS attacks flood the network with malicious traffic, shutting out legitimate traffic that the switch needs to process, such as routing updates. This can cause network instability or network crashes.

- **Port Security**—Prevents MAC-based DoS attacks by limits the number of MAC addresses that can transmit from a port.
- **Scavenger Class QoS**—Reprioritizes traffic from systems with abnormally high traffic rates that could be potential DoS attackers.
- **Control Plane Policing**—Controls the type and amount of traffic that is forwarded to the CPU for processing. Prevents CPU overload.
- **NetFlow anomaly detection**—Flow based statistics that identify DoS attacks and apply port-level ACLs to mitigate the attack.

### Data Theft Prevention

*How do I prevent malicious users from intercepting data on the network?*

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.

- **DHCP Snooping**—Ensures that only authorized DHCP servers issue IP addresses; 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 DHCP binding table.
- **IP Source Guard**—Prevents a malicious user from hijacking a neighbor's IP address.

### Summary

Only Cisco Catalyst switches provide these comprehensive set of innovative integrated security features for the wiring closet. Many of these features are free and available across the Cisco Catalyst switching platforms. Enterprises can use these security features in their wiring closet switching infrastructure as an effective first line of defense to identify, respond to, and adapt to security threats before they can cause greater damage across the enterprise.