

Secure Network Interface Controller

Acadia's Secure Network Interface Controller (SNIC) provides a robust hardware solution to secure critical network infrastructure at the workstation. It provides methods to securely authenticate and authorize hardware, users, and applications onto the intranet using industry-standard protocols such as 802.1X and SSL/TLS. Additionally, on-board monitoring and control functionality enables network operators to remotely administer the workstation and collect accounting information using industry-standard interfaces and protocols.

Deploying SNICs provides a high degree of resiliency against malicious users and code, since only authenticated/authorized hardware is permitted to access the network. Additionally, since all security and administration functions reside in hardware, the system is highly resistant to hacking. It can withstand viruses, worms, "rootkits," Denial of Service (DoS) attacks, and other security threats, enabling network administrators to monitor and control the network interface over dedicated control channels, even if the operating system itself is compromised.

Extensible FPGA-based Hardware Platform:

- i. Hardware platform provides resiliency against security threats such as viruses, worms, "rootkits," and malicious users which can compromise traditional software-based security approaches.*
- ii. Field-upgradable, reprogrammable hardware platform can dynamically adapt to changing network deployment scenarios and can be upgraded to support new security protocols/standards.*

Multi-level "AAA" network security for physical interface, user, and applications.

- i. Authentication*
Controls access. (802.1X, RADIUS, X.509 certificates with PKI)
- ii. Authorization*
Grants specific services, based on authentication. (QoS, encryption, filtering, etc.)
- iii. Accounting*
Tracks consumption of network resources in real-time. (bandwidth usage statistics, port monitoring, etc.)

Management Interface provided through standardized Management Information Base (MIB).

- i. Compatible with network management software and existing network infrastructure.*
- ii. Remote monitoring and control of device, including real-time traffic shaping and filtering.*

Specifications:

Host Interface:

- PCI Express 1.1 (x8, x4, x1)
- MSI and legacy interrupts
- DMA

Ethernet:

- 10/100/1000 tri-speed MAC
- Jumbo Frames (9000 b)
- QoS (802.1Q, 802.1p) and Security (802.1X)

IP:

- IP Checksum
- IP Segmentation Offload

TCP:

- TCP Checksum
- TCP Segmentation Offload
- Large Receive Offload
- Large Send Offload

UDP:

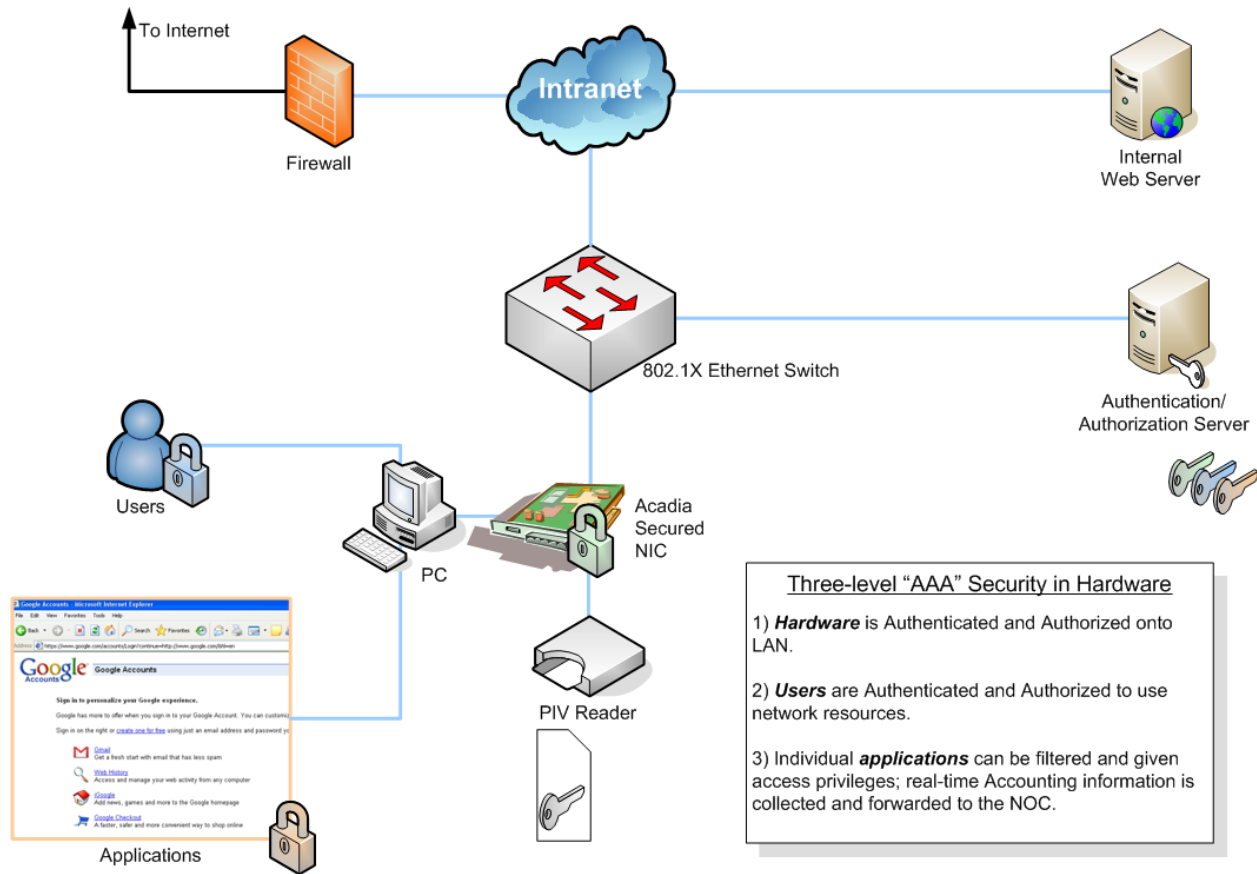
- UDP Checksum
- UDP Segmentation Offload

Security:

- 802.1X/RADIUS Authentication (PAP, CHAP, EAP)
- SSL/TLS RSA handshake algorithm
- On-board, secure storage of X.509 certificates and keys
- Secure Hardware Hash (MD5, SHA-1, SHA-2)
- Real-time packet filtering (port, IP address)
- Integrates with U.S. Government "Smart Card" P.I.V. card readers
- Optional symmetric hardware encryption module (AES)

Management:

- Secure, hardware-based MIB interface
- Remote monitoring/control of network interface
 - Traffic shaping
 - Packet filtering



1. Secure NIC authenticates to Authentication/Authorization server using 802.1X/RADIUS, establishes management control channels for remote monitoring/administration.
2. User authenticates to the PC using PIV card reader.
3. PIV information is sent over a secure channel to Authentication/Authorization server, which authenticates the user and grants authorization to network resources and services according to the user's profile.
4. Network traffic can be filtered by port and IP address to limit access to applications/networks as desired.
5. On-board client certificate and key store enables compatible applications to access secured network resources (e.g. internal web servers).
6. Real-time accounting information is retained on-board and can be transmitted to the Network Operations Center (NOC) for analysis.