TNC interfaces enable dynamic differentiation and access control enforcement for a wide variety of users in mixed-use environments.

Enterprises are occupied by a wide variety of users, including visitors, partners, contractors, employees, and privileged employees. Networking and security devices from multiple vendors interoperate using TNC-based technology to provide appropriate access for each user based on their identity, endpoint compliance, role, and behavior.

- The Great Bay Beacon appliance acts as a MAP Client, publishing endpoint profiling and behavior monitoring information to the MAP; other network devices can leverage that information to detect MAC or IP spoofing of unmanaged endpoints and enable intelligent, responsive access control decisions.
- The Juniper Networks IC Series Unified Access Control Appliance, the policy management server at the heart of Juniper’s Unified Access Control solution, acts as a TNC Policy Decision Point (PDP), providing user authentication and endpoint health checking and provisioning policy to the network devices acting as enforcement points. The IC Series also acts as a TNC Metadata Access Point (MAP), providing a clearinghouse for information about connected endpoints.

A variety of TNC interfaces underlie this intelligent, dynamic, responsive network access control:

- IF-PEP enables provisioning of appropriate access for each user while ensuring consistent access control across wired and wireless connections.
- IF-TNCCS and IF-IMC / IMV enable endpoint integrity checking; implementations can range from a full supplicant to a lightweight dissolving agent.
- IF-MAP enables integration of network intelligence from additional security systems to add a behavioral consideration to the access decision.
TNC interfaces enable location, identity, endpoint health, and behavior-based access control decisions for users in an enterprise environment, along with detection and remediation of illicit activity such as data leakage by an endpoint.

Enterprise environments require a high degree of control over user access to critical application and information resources. Integration of traditional NAC with other security technologies such as data leak prevention can ensure protection not only of the network itself but of the data it contains.

- The Lumeta IPsonar acts as a TNC Metadata Access Point (MAP) Client, detecting data leaks and publishing that information to the TNC Metadata Access Point (MAP); other network devices can use that information to prevent unauthorized "backdoor" Internet connections that bypass network access controls.

- The Juniper Networks IC Series UAC Appliance, the policy management server at the heart of Juniper’s Unified Access Control solution, acts as a TNC Policy Decision Point (PDP), providing user authentication and endpoint health checking and provisioning policy to the network devices acting as enforcement points. The IC Series also acts as a MAP, providing a clearinghouse for information about connected endpoints.

A variety of TNC interfaces underlie this integration of physical security, configuration management, network intelligence, and access control:

- IF-PEP enables dynamic admission control and assignment of endpoints to the appropriate VLAN.
- IF-MAP enables data leak prevention, configuration management, and correlation of physical access privileges with network access privileges.
IF-MAP enables dynamic protection for interconnections between a control system network and an enterprise network.

Interconnectivity of industrial control systems, such as Supervisory Control And Data Acquisition (SCADA) systems, with enterprise IT networks is increasing, driven by considerations from cost to management to monitoring. With this increased access comes increased risk; operating systems that can't be patched due to operational considerations are exposed to infection from indirect connections to untrusted networks, and protocols never designed for security are accessible to attackers. Network security components implementing TNC standards provide isolation and protection.

- SCADAnet Endboxes overlay a process control network onto an enterprise network, proxy network transport security for Programmable Logic Controllers (PLCs) and Human Machine Interfaces (HMIs), and act as Policy Enforcement Points for the process control network.
- The Juniper Networks IC Series UAC Appliance, the policy management server at the heart of Juniper’s Unified Access Control solution, acts as a MAP, providing a clearinghouse for information about connected endpoints.
- The Great Bay Beacon appliance acts as a MAP Client, publishing endpoint profiling and behavior monitoring information to the MAP; other network devices can leverage that information to detect MAC or IP spoofing of unmanaged endpoints and enable intelligent, responsive access control decisions.

A TNC interface underlies this protection of the interconnection between a process control network and an enterprise network:

- IF-MAP enables coordination of configuration, behavioral, location, and policy information between provisioning applications, policy management and enforcement devices, and network intelligence / visibility components.