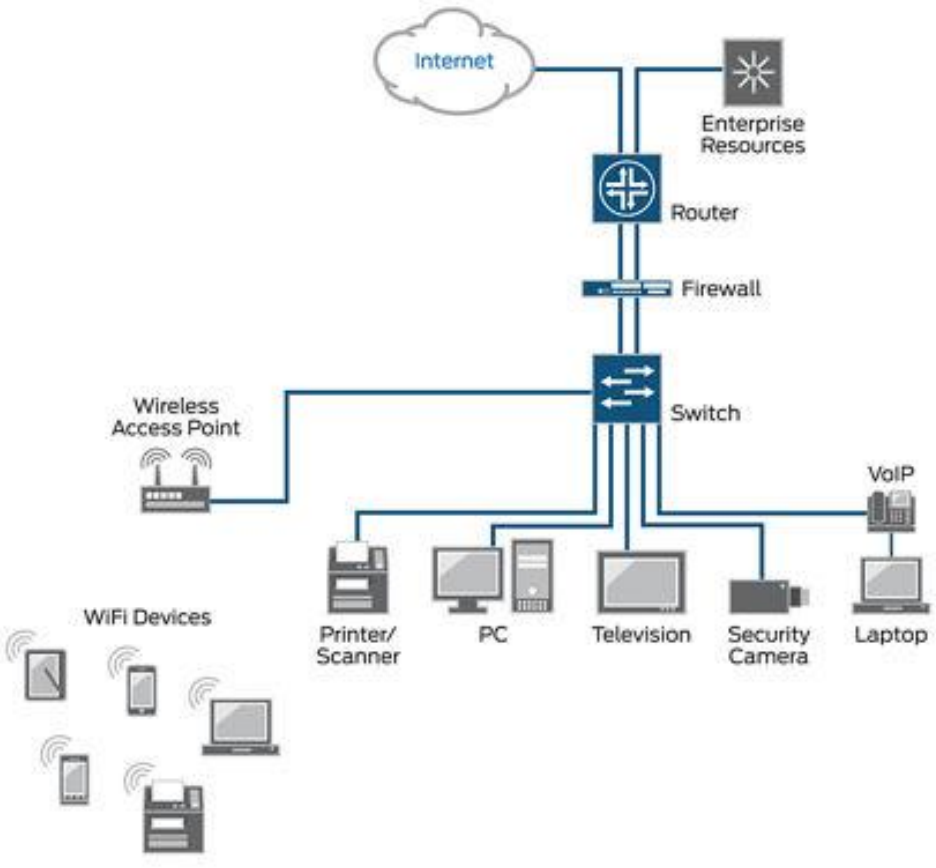
What is 802.1X Network Access Control (NAC)?

802.1X network access control (NAC) enables administrators to provide uniform access control across wired and wireless networks. It is widely deployed on campus and branch enterprise networks, and is comprised of two major elements:

- **802.1X protocol**—An IEEE standard for port-based network access control (PNAC) on wired and wireless access points. 802.1X defines authentication controls for any user or device trying to access a LAN or WLAN.
- **NAC**—A proven networking concept that identifies users and devices by controlling access to the network. NAC controls access to enterprise resources using authorization and policy enforcement.

Problems 802.1X Network Access Control Address

The impact of wireless network access, mobility, bring your own device (BYOD), social media, and cloud computing on enterprise network resources is huge. This expanded mobility increases exposure to network threats and digital exploitation, as shown in the following figure. Using 802.1x helps you improve your ingress security in this type of environment while lowering your total cost of ownership.



What Can You Do with 802.1X Network Access Control?

There are many ways to deploy a NAC, but the essentials are:

- Pre-admission control—Blocks unauthenticated messages.
- Device and user detection—Identifies users and devices with pre-defined credentials or machine IDs.
- Authentication and authorization—Verifies and provides access.
- Onboarding—Provisions a device with security, management, or host-checking software.
- Profiling—Scans endpoint devices.
- Policy enforcement—Applies role and permission-based access.
- Post-admission control—Enforces session termination and cleanup.

802.1X provides L2 access control by validating the user or device that is attempting to access a physical port.

How Does 802.1X Network Access Control Work?

The 802.1X NAC operation sequence is as follows:

1. **Initiation**—The authenticator (typically a switch) or supplicant (client device) sends a session initiation request. A supplicant sends an EAP-response message to the authenticator, which encapsulates the message and forwards it to the authentication server.

2. **Authentication**—Messages pass between the authentication server and the supplicant via the authenticator to validate several pieces of information.

3. **Authorization**—If the credentials are valid, the authentication server notifies the authenticator to give the supplicant access to the port.

4. **Accounting**—RADIUS accounting keeps session records including user and device details, session types, and service details.

5. **Termination**—Sessions are terminated by disconnecting the endpoint device, or by using management software.

https://www.juniper.net/us/en/research-topics/what-is-802-1x-network-access-control.html