

Cyber Security for OT people

Eric Lebeau, Product Line Manager

May 9, 2023



Powering Business Worldwide

© 2023 Eaton. All rights reserved.

Agenda

- Information security basics
- NERC CIP overview
- Networking Fundamentals
- Securing the Network Architecture
- Cryptography and its applications



The Threat



Powering Business Worldwide

© 2023 Eaton. All rights reserved.

Hack on Saudi Aramco hit 30,000 workstations, oil firm admits

First hacktivist-style assault to use malware?

By John Leyden, 29th August 2012

[What you need to know about cloud backup](#)

Analysis Saudi Aramco said that it had put its network back online on Saturday, 10 days after a malware attack flooded 30,000 workstations at the oil giant.

In a [statement](#), Saudi Arabia's national oil firm said that it had "restored all its main internal network services" hit by a malware outbreak that struck on 15 August. The firm said its core business of oil production and exploration was *not* affected by the attack, which resulted in a decision to suspend Saudi Aramco's website for a period of a few days, presumably as a precaution. Corporate remote access services were also suspended as a result of the attack.

Oil and production systems were run off "isolated network systems unaffected by the attack, which the firm has pledged to investigate. In the meantime, Saudi Aramco [promised](#) to improve the security of its network to guard against fresh assaults.

Saudi Aramco has restored all its main internal network services that were impacted on August 15, 2012, by a malicious virus that originated from external sources and affected about 30,000 workstations. The workstations have since been cleaned and restored to service. As a precaution, remote

RELATED STORIES

Syrian net access falls down some stairs, doing OK now

Egyptian navy captures divers trying to cut undersea internet cables

Baby got .BAT: Old-school malware terrifies Iran with del *.*

Saudi Aramco: Foreign hackers



Powering Business Worldwide

http://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis/

© 2023 Eaton. All rights reserved.

#1: The ransomware attack on Colonial Pipeline

Who was affected: In 2021, the largest petroleum pipeline in the United States was hit with a ransomware attack, cutting off gas supply across the East Coast.

The cost: The hackers demanded a \$4.4 million ransom in bitcoin, which was later partially recovered by the Department of Justice.

How they did it: Using credentials included in a batch of logins found on the dark web, threat actors hacked into Colonial Pipeline's system through a VPN.

The takeaway: Signing up for dark web monitoring, which can be automated through Dashlane, means that you'll be notified if your passwords show up as part of a data leak. This gives organizations the opportunity to [change passwords](#) and logins, preventing hackers from gaining access to company networks. Our password manager also helps to eliminate reused passwords; Dashlane will notify employees and admins if a password is weak or has been used for another account.

#2: The hack of a water treatment plant

Who was affected: In February of 2021, hackers tried to poison the water supply of a small water treatment plant in Florida.

The cost: Luckily, an employee was able to stop the attack once they realized the system was being manipulated—but the threat actors still gained access to the system.

How they did it: The hackers logged in to the treatment plant's supervisory control and data acquisition system (SCADA) remotely. The system ran on an unsecured version of Windows, and employees connected to the remote-access software through one password they all shared. The company also neglected to use a firewall for employees to connect.

The takeaway: Shared passwords can be a culprit of breaches and hacks, especially if those passwords are shared through unsecured methods. Dashlane allows employees to share passwords securely through the browser and mobile app to access a shared account, and employees should be discouraged from sharing a single password to access a remote desktop. Instead, each employee should have their own login, and connect through a firewall.

<https://www.dashlane.com/blog/real-world-examples-of-hacks-and-breaches-in-the-utilities-and-energy-industry>



Powering Business Worldwide

Montreal · Updated

Pro-Russian group claims responsibility for cyberattack against Hydro-Québec



Attacks are retribution for Canada's support for Ukraine, expert says



[Matthew Lapierre](#) · CBC News · Posted: Apr 13, 2023 8:29 AM EDT | Last Updated: April 13



No critical Hydro-Québec systems were attacked, says the utility. (Paul Chiasson/The Canadian Press)

Cyber is a top priority

Cyber certainly has the attention of CEOs. In **PwC's 25th Annual Global CEO Survey**, 44% of energy, utilities and resources CEOs ranked cyber threats as a “top three” concern, only slightly edged out by health risks (45%) and climate change (49%). But given this importance, the CISO often doesn't have a direct line to the CEO. The CISO's most frequent interactions are with the Chief Information Officer (CIO), the Chief Technology Officer (CTO) and the Chief Risk Officer (CRO), according to PwC's **2022 Global Digital Trust Insights Survey**.

Utility companies most at risk of cyberattack – Moody's

Water and power companies are attractive targets for hackers, even though the rewards can be relatively low.

By Ryan Morrison



Utility companies and hospitals are coming under increasing risk of [cyberattack](#), according to a report by credit ratings agency Moody's. In its first update to the [Cyber Risk Heatmap](#) since 2019, the agency found water companies were among the most at risk of any sector. While the financial reward for attacking a water or electricity company was relatively low, they often have minimal security measures in place, making them attractive targets.

Home » Survey: 56 percent of utilities have faced a cyberattack in the last year

« XCEL ENERGY GETS GREENLIGHT FOR EV PILOTS AFTER OPPOSITION DISMISSED IN MINNESOTA

MASSACHUSETTS UTILITY ACCEPTING SOLAR PROGRAM ENROLLMENT »

Survey: 56 percent of utilities have faced a cyberattack in the last year

Published on October 15, 2019 by [Jaclyn Brandt](#)



The utility industry may be more vulnerable to cybersecurity threats than previously realized, according to a new report by Siemens and the Ponemon Institute.

The report, “[Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?](#)”, looked at how prepared utilities are for future attacks, as well as offering solutions to create a more secure power grid.



Security and reliability

“End-to-end security encompasses not only deliberate attacks but also inadvertent actions. [...] often more damage is done by carelessness, equipment failures and natural disasters than by those deliberate attacks. [...]

many of the same measures that could be used against deliberate attacks can be used against inadvertent actions. Therefore, it is useful and cost-effective to address both types of security threats with the same types of security measures.”

IEC 62351-7 5.1.1 Scope of end-to-end security

Exploiting Product Vulnerabilities

Process control once was much simpler

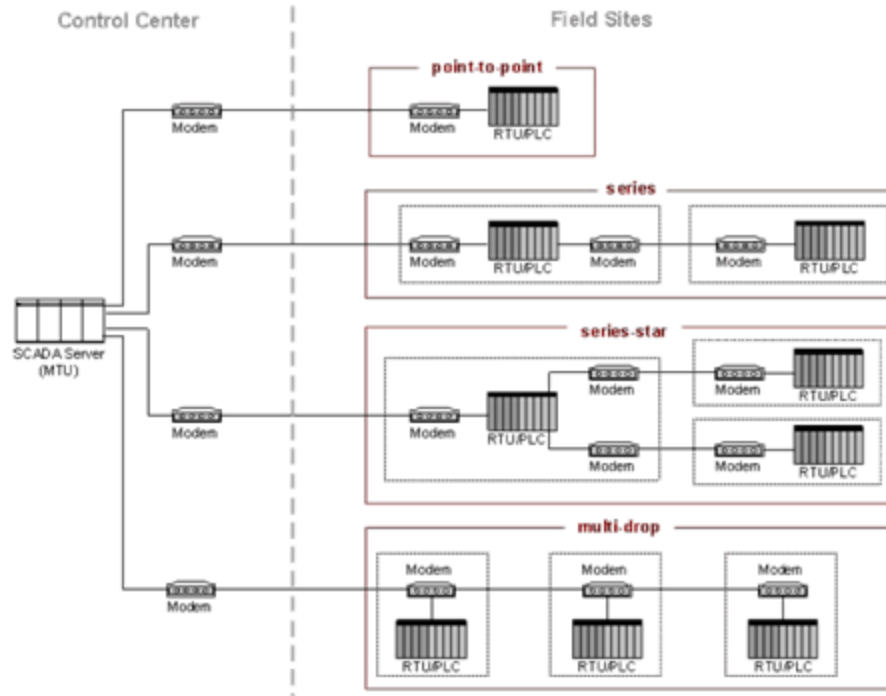
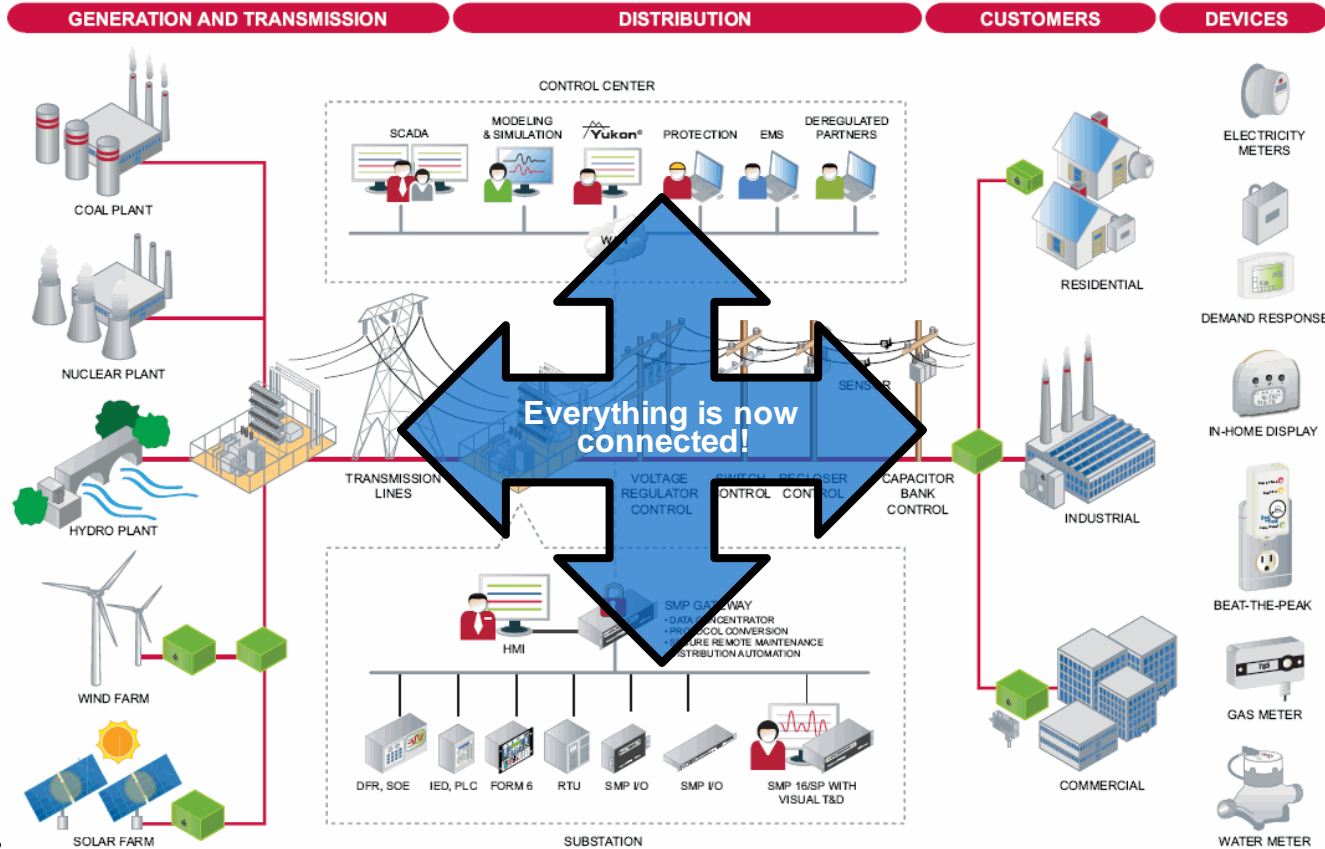


Figure 2-3. Basic SCADA Communication Topologies

NIST 800-82 Guide to Industrial Control Systems (ICS) Security

The Smart Grid utility is more complex



Control systems are at risk

- Traditional systems used **serial** devices connected through dedicated modems with proprietary protocols – **security through obscurity**
- Manufacturers replaced the serial wire by **networking capability** to improve connectivity – often without considering robustness and security
- Systems are increasingly based on **standard protocols**: TCP/IP, OPC, ICCP, DNP3, IEC 61850. Often with little or no security built-in.
- Control systems are increasingly being connected to the enterprise network, and thus indirectly to the Internet.
- Field devices are now subject to many of the same vulnerabilities as computers – 15 years ago... without patches or upgrades.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

[HOME](#)[ABOUT](#)[ICSJWG](#)[INFORMATION PRODUCTS](#)[TRAINING](#)[FAQ](#)

Control Systems

[Home](#)[Calendar](#)[ICSJWG](#)[Information Products](#)[Training](#)[Recommended Practices](#)[Assessments](#)[Standards & References](#)[Related Sites](#)[FAQ](#)

ICS-CERT Advisories

Advisories provide timely information about current security issues, vulnerabilities, and exploits.

[\[change view\]: Advisories by Vendor](#)



- ICSA-15-076-01 : XZERES 442SR Wind Turbine Vulnerability
- ICSA-15-076-02 : Honeywell XL Web Controller Directory Traversal Vulnerability
- ICSA-14-350-02 : Johnson Controls Metasys Vulnerabilities
- ICSA-15-071-01 : Schneider Electric Palco DS-NVs Buffer Overflow Vulnerability
- ICSA-15-069-04A : Elipse E3 Process Control Vulnerability (Updates A)
- ICSA-15-069-01 : Cimon CmnView DLL Hijacking Vulnerability
- ICSA-15-069-02 : ABB HART Device DTM Vulnerability
- ICSA-15-069-03 : SCADA Engine BACnet OPC Server Vulnerabilities
- ICSA-15-041-02 : GE Hydran M2 Predictable TCP Initial Sequence Vulnerability
- ICSA-15-064-01 : Siemens SIMATIC HMI Basic, SINUMERIK, and Ruggedcom APE GHOST Vulnerability
- ICSA-15-064-02 : Siemens SIMATIC ProSave, SIMATIC CFC, SIMATIC STEP 7, SIMOTION Scout, and STARTER Insufficiently Qualified Paths
- ICSA-15-064-03 : Siemens SPC Controller Series Denial-of-Service Vulnerability
- ICSA-15-064-04 : Siemens SIMATIC S7-300 CPU Denial-of-Service Vulnerability
- ICSA-15-064-05 : Siemens SPCanywhere App Vulnerabilities
- ICSA-14-353-01-SupplementA : Network Time Protocol Vulnerabilities (Supplement Update A)
- ICSA-15-062-01 : MICROSYS PROMOTIC Stack Buffer Overflow
- ICSA-15-057-01 : Network Vision IntraVue Code Injection Vulnerability
- ICSA-15-055-01 : Software Toolbox Top Server Resource Exhaustion Vulnerability
- ICSA-15-055-02 : Kepware Resource Exhaustion Vulnerability



Powering Business Worldwide



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Advisory (ICSA-13-291-01B)

[More Advisories](#)

DNP3 Implementation Vulnerability (Update B)

Original release date: April 09, 2014 | Last revised: April 10, 2014

OVERVIEW

This updated advisory is a follow-up to the updated advisory that was published November 21, 2013, on the NC

Adam Crain of Automatak and Chris Sistrunk, Sr. of ICS-CERT reported a vulnerability to ICS-CERT that was evident in numerous implementations. ICS-CERT emphasizes that the vulnerability is not with the DNP3 protocol.

The research showed that some implementations of DNP3 have vulnerabilities. ICS-CERT wants to bring greater awareness to developers and users of DNP3 implementations.

This vulnerability can be exploited remotely (over a network) to execute arbitrary code on a serial-based implementation).

Below is a nonexhaustive list of advisories that ICS-CERT has issued regarding DNP3 implementations producing patches or updates to mitigate the reported vulnerabilities.

DNP3 IMPROPER INPUT VALIDATION VULNERABILITY

Advisory Number	Vendor
ICSA-13-282-01A	Alstrom
ICSA-13-297-01	Catapult Software
ICSA-13-346-01	Cooper Power Systems
ICSA-13-346-02	Cooper Power Systems/Cybetec
ICSA-13-337-01	Elecsys
ICSA-13-297-02	GE
ICSA-13-161-01	IOServer
ICSA-13-213-03	IOServer
ICSA-13-226-01	Kepware Technologies
ICSA-13-213-04A	MatrikonOPC
ICSA-13-352-01	NovaTech
ICSA-14-098-01	OSISoft
ICSA-14-006-01	Schneider Electric
ICSA-14-014-01	Schneider Electric
ICSA-13-219-01	Schweitzer Engineering Laboratories
ICSA-13-234-02	Software Toolbox
ICSA-13-252-01	SUBNET Solutions
ICSA-13-240-01	Triangle MicroWorks



Powering Business Worldwide

US-CERT and ICS-CERT Transition to CISA in Feb 2023

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



AMERICA'S CYBER DEFENSE AGENCY

Search

Topics ▾ Spotlight Resources & Tools ▾ News & Events ▾ Careers ▾ About ▾

REPORT A CYBER ISSUE

[Home](#) / [News & Events](#)

SHARE: [f](#) [t](#) [in](#) [e](#)

Filters

What are you looking for?

Sort by (optional)

Release Date ▾

APPLY

Advisory Type +

Release Year +

Cybersecurity Alerts & Advisories

[View Cybersecurity Advisories Only](#)

MAY 04, 2023 ■ ALERT

[CISA Releases One Industrial Control Systems Advisory](#)

MAY 02, 2023 ■ ICS ADVISORY | ICSA-23-122-01

[Mitsubishi Electric Factory Automation Products](#)

MAY 02, 2023 ■ ALERT

[CISA Releases One Industrial Control Systems Advisory](#)

MAY 01, 2023 ■ ALERT

[CISA Urges Organizations to Incorporate the FCC Covered List Into Risk Management Plans](#)



Powering Business Worldwide

ICS Advisory Project

The dashboard displays the following information:

- Summary:** 2,414 CISA ICS Advisories, 485 Vendors, and 1,928 Products.
- Search:** Search by Vendor (Vendor dropdown) and Search by ICS Advisory Alert Code (text input).
- Product Search:** Search by Product (Product dropdown) and Select date range (date range dropdown).
- Vendor Headquarters:** A bar chart showing the top countries: Germany, United States, and Taiwan.
- Map:** A world map showing Vendor Headquarters Location with a 'Country' dropdown menu.
- Table:** A table listing 9 advisories with columns for Alert Code, Release Date, CISA ICS Advisory, Vendor, Product, and Vendor HQ.

	Alert Code	Release Date	CISA ICS Advisory	Vendor	Product	Vendor HQ
1.	ICSA-23-122-01	2 May 2023	Mitsubishi Electric Factory Automation Products	Mitsubishi Electric	Factory Automation (FA) Products	Japan
2.	ICSM-23-117-01	27 Apr 2023	Illumina Universal Copy Service	Illumina	Universal Copy Service (UCS)	United States
3.	ICSA-23-115-01	25 Apr 2023	Keyight N8844A Data Analytics Web Service	Keyight Technologies Inc.	N8844A Data Analytics Web Service	United States
4.	ICSA-23-115-02	25 Apr 2023	Scada-LTS Third Party Component	Scada-LTS	Scada-LTS	Open-source
5.	ICSA-23-110-01	20 Apr 2023	INEA ME RTU	INEA	ME RTU	Slovenia
6.	ICSA-23-108-02	18 Apr 2023	Schneider Electric Easy UPS Online Monitoring Software	Schneider Electric	APC Easy UPS Online Monitoring Software, Schneider Electric Easy UPS Online Monitoring Software	France
7.	ICSA-23-108-01	18 Apr 2023	Omron CSCJ Series	Omron	SYSMAC CS/CJ Series	Japan
8.	ICSA-23-103-01	13 Apr 2023	Siemens Adaptec maxView Application	Siemens	Adaptec maxView Application	Germany
9.	ICSA-23-103-08	13 Apr 2023	Siemens Mendix Forgot Password Module	Siemens	Mendix Forgot Password Module	Germany

Footer: Created by Dan Ricci | Follow the ICS Advisory Project on Twitter @AdvisoryICS | © 2023 ICS Advisory Project | Send question or comments about the ICS Advisory Project to: icsadvisoryproj@icsadvisoryproject.com | Privacy | Looker Studio

<https://www.icsadvisoryproject.com/ics-advisory-dashboards>

Information Security Basics

There is no “Magic” Solution



“Magic” security gate



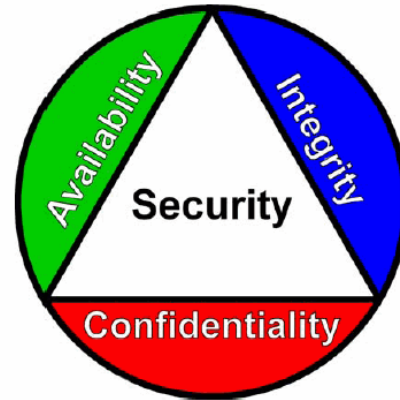
Powering Business Worldwide

Securing Systems

- No system can be 100% secure.
- The protective measures must be based on the value of the assets we need to protect.
- Security must not prevent the organization from meeting its business objectives.
- To protect their critical systems from internal and external threats, organizations need to implement an **Information Security Program** that addresses:
 - People
 - Policies
 - Procedures
 - Technologies

Information Security Concepts

- The term **information security** means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide –
 - **Confidentiality**
 - **Integrity**
 - **Availability**



Confidentiality

- **Confidentiality** consists of ensuring that the desired resource is only accessible to the desired person or system, under the desired conditions.
- Key principles are:
 - **Identification**
 - **Authentication**
 - **Authorization**



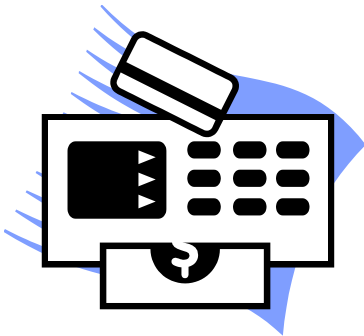
Authentication

- **Authentication** confirms the identity of a person.
- Authentication factors are:
 - Something you **know**, such as a password
 - Something you **have**, such as a card
 - Something you **“are”**, such as a fingerprint



Two-Factor Authentication

- Two-factor, or “strong”, authentication consists of combining two factors for increased assurance:
 - An ATM card with a secret PIN.
 - A password and a random number provided by a security token
 - A password and a thumbprint.



Availability

- **Availability** consists of ensuring that resources are accessible when needed by an authorized party.
- Key measures:
 - Prevent the disruption of service and productivity.



Integrity

- **Integrity** consists of ensuring that the desired resource contains accurate information and performs precisely as intended.
- Keys measures:
 - Prevent unauthorized modification of systems and information, whether intentional or unintentional.
 - **Non-repudiation** - Tie an action to an actor, and prevent an actor from denying (repudiating) an action.
 - Non-repudiation can be ensured by strong authentication.

IT vs. OT

- The main focus of Information Technology (IT) is to ensure the **confidentiality** and the **integrity** of the data using rigorous access control and data encryption.
- In Operations Technology (OT), the main focus is **safety**, then **availability**, and **integrity** of data.
- Enterprise security protects the data residing in the servers from attack.
- Control system security protects the ability of the facility to safely and securely operate, regardless of what may befall the rest of the network.









Powering Business Worldwide

Protecting control systems requires a layered,
“defense in depth” approach.

© 2023 Eaton. All rights reserved.

IT Availability

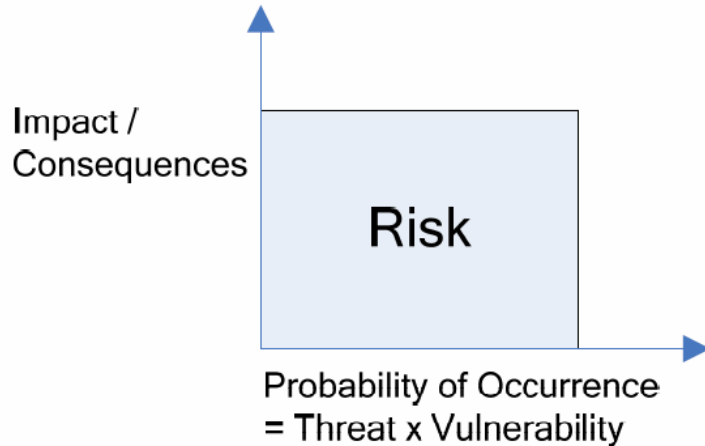
 IT Planned Maintenance Notice	
 Application / Service Impacted:	Full Service Outage: SAP Production Systems
 ACTIVITY PLAN:	<ul style="list-style-type: none">The annual SAP support package upgrade of our SAP production systems will begin on 4/14/23 at 8:00 pm EST and is scheduled to be completed by 4/16/23 at 3:00am EST.<ul style="list-style-type: none">Please note this outage potentially affects any system that relies on a connection to the SAP production systems for functionality. This includes Order Center, RT-ODS, ACL, and SAP Ariba.
 USER GROUP IMPACTED:	Enterprise
 LOCATION(S) IMPACTED:	Global
 CURRENT WORK DETAIL:	Change Status: <u>COMPLETE (Successful)</u> Activity Complete: Saturday 15-Apr-23 7:00 PM (ET)

Process Control Availability

- The lifecycle of process controls systems is different from IT systems –
 - **Continuity of service** is key business goal.
 - Process control is **designed for the long term** – up to 30 years.
 - Once started, **never stops** – few planned outages.
 - Outages are expensive – lost revenue.
 - Configuration never changes – change requires an outage.
 - Operator training is critical to keep system running smoothly – changes are expensive.
 - Maintenance updates – require an outage.

Risk analysis

Risk-based assessment



- **Risk management** is “the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations’ missions.”
- **Threat** is “the potential for a threat-source to successfully exercise (accidentally trigger or intentionally exploit) a specific vulnerability”
- **Vulnerability** is “a Weakness that can be accidentally triggered or intentionally exploited.”

Source: NIST 800-30

Microsoft Threat Modeling - STRIDE threat types

Desired Property	Threat	Definition
Authentication	S poofing	Impersonating something or someone else
Integrity	T ampering	Modifying code or data without authorization
Non-repudiation	R epudiation	The ability to claim to have not performed some action against an application
Confidentiality	I nformation Disclosure	The exposure of information to unauthorized users
Availability	D enial of Service	The ability to deny or degrade a service to legitimate users
Authorization	E levation of Privilege	The ability of a user to elevate their privileges with an application without authorization

Policies, Procedures, Guidelines, and Standards

Lexicon

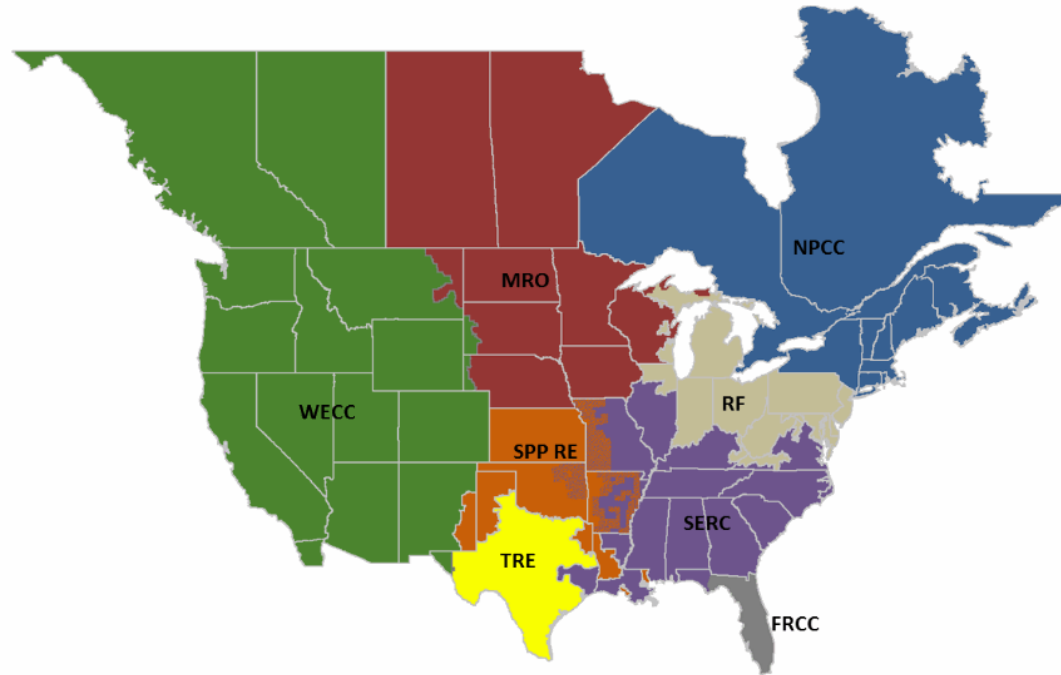
- **Policies** address the who, what, and why. Policies direct the accomplishment of objectives by providing procedures or actions that must be carried out.
- **Procedures** address the how, where, and when. Provide detailed steps to follow for operations.
- **Standards** specify uniform use of specific technologies or parameters. Typically refer to specific hardware and software.
- A **baseline** is a more specific implementation of a standard.
- A **guideline** recommends a way of doing something.

NERC CIP

FERC, ERO, NERC and CIP

- The Energy Policy Act of 2005 gave the U.S. **Federal Energy Regulatory Commission** (FERC) authority over the reliability of the **bulk electric power system** (and the owners, users, and operators of bulk power system assets).
- EAct 2005 explicitly defines the term **reliability** standard **to include cybersecurity**.
- Industry-developed standards must be approved by FERC and, once approved, are enforced by an **Electric Reliability Organization** (ERO) approved by FERC.
- In 2006, the **North American Electric Reliability Corporation** (NERC) officially became the ERO.
- NERC developed the **Critical Infrastructure Protection** (CIP) standards to address the security of the bulk electric system.

NERC 8 regional entities



NERC Cyber Security History

- 07/2003 Urgent Action 1200
- 01/2008 Critical Infrastructure Protection (CIP) Standards Version 1, Order 706
- 09/2009 CIP Version 2
- 03/2010 CIP Version 3,
- 04/2012 CIP Version 4, did not get implemented
- 11/2013 CIP Version 5 + revisions...call it version 6 – enforced July 2016
- 07/2017 : CIP-013 - Supply Chain Risk Management
- 08/2018 : CIP-012 – Communication between Control Centers

The NERC CIP Standards enforced today

- **The Critical Infrastructure Protection Standards** provide a **cyber security framework** for the identification and protection of Critical Cyber Assets to support reliable operation of the **Bulk Electric System**:
 - CIP-002-5.1a Critical Cyber Asset Identification
 - CIP-003-8 Security Management Controls
 - CIP-004-6 Personnel and Training
 - CIP-005-7 Electronic Security Perimeter(s)
 - CIP-006-6 Physical Security
 - CIP-007-6 Systems Security Management
 - CIP-008-6 Incident Reporting and Response Planning
 - CIP-009-6 Recovery Plans for Critical Cyber Assets
 - CIP-010-4 Configuration Change Management and Vulnerability Assessments
 - CIP-011-2 Information Protection
 - CIP-012-1 Communication between Control Centers
 - CIP-013-2 Supply Chain Risk Management

Cyber Assets

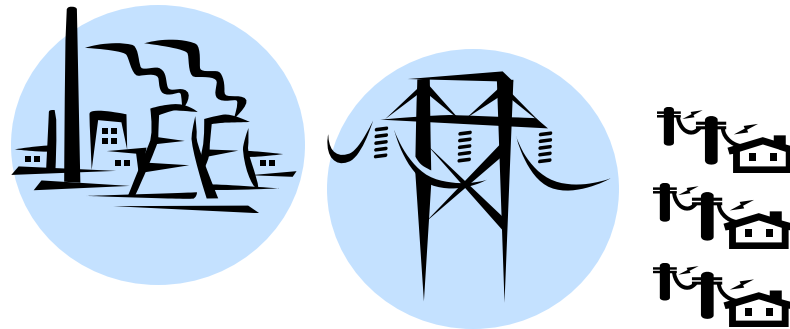
- **Cyber Assets** – Programmable electronic devices including the hardware, software, and data in those devices.
- **BES Cyber Assets** – Cyber Assets that can impact the reliable operation of the Bulk Electric System within 15 minutes if rendered unavailable, degraded, or misused..
- **BES Cyber System** – One or more BES Cyber Assets logically grouped to perform one or more reliability tasks.

Associated Cyber Assets

- **Electronic Access Control or Monitoring Systems (EACMS)** – Electronic Access Points, Intermediate Devices, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.
- **Physical Access Control Systems (PACS)** – authentication servers, card systems, and badge control systems.
- **Protected Cyber Assets (PCA)** – file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems, to the extent they are within the ESP.

CIP-002-5.1a Critical Asset Identification

- *Purpose* : To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.



CIP-002-5.1a Evolving CIP

- The definition of critical assets has evolved to take into account the impact on the reliability of the power system.
 - CIP V4 replaced **risk-based assessment methodology** with **bright-line criteria**, i.e. hard numbers: *“1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.”*
 - CIP V5 introduces **impact levels**: High, Medium and Low, and a 15 minute time window.

“BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise.”

CIP-002-5.1a BES Cyber System Categorization

- Control Centers and backup Control Centers
- Transmission stations and substations
- Generation resources
- Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements
- Special Protection Systems that support the reliable operation of the Bulk Electric System
- For Distribution Providers, Protection Systems Facilities, systems and equipment for the protection or restoration of the BES
 - Underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) systems
 - Special Protection System or Remedial Action Scheme
 - Blackstart Resources and Cranking Paths and initial switching requirements

Typical BES Cyber Assets

Table 1: Cyber Assets Typically Evaluated as BES Cyber Assets		
Control Centers	Transmission Station/Substation	Generation Plants
Application servers	Intelligent Electronic Devices (IED) / protective relay	Programmable Logic Controller (PLC)
Data servers	Remote Terminal Unit (RTU)	Distributed Control System (DCS)
HMI workstations	Programmable Logic Controllers (PLC)	HMI workstation
Data acquisition	Data concentrator	Application server
Data interchange	Meter / indicator	Data server
Computer networking	Tap changer	Computer networking
Communication processing	HMI workstation	Intelligent Electronic Device (IED)/ relay
Precision time device	Computer networking	Remote Terminal Unit (RTU)
	Communications processing	

CIP-003-8 Security Management Controls

Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

- Implement policies to support CIP-004 to CIP-011 Objectives (approved every 15 calendar months)
- Implement Low Impact Controls
- Identify a CIP Senior Manager responsible for CIP Compliance Program

CIP-004-6 Personnel & Training

Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

- Quarterly Security Awareness that reinforce cybersecurity practices for personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems
- Training completion before granted access to applicable cyber assets, to be renewed every 15 months.
- Personnel Risk Assessment (PRA) – identity confirmation and seven year criminal history records check
- Access Management - Process to authorize based on need and to revoke access upon termination of action within 24h

CIP-005-7 Electronic Security Perimeter(s)

Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

- Electronic Security Perimeters:
 - All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.
 - All External Routable Connectivity must be through an identified Electronic Access Point (EAP).
 - Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.
 - Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications

CIP-005-7 Electronic Security Perimeter(s) (cont.)

- Interactive Remote Access Management
 - Utilize Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.
 - Utilize encryption that terminates at an Intermediate System.
 - Require multi-factor authentication
 - Have one or more methods for determining and disabling active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)

CIP-006-6 Physical Security of BES Cyber Systems

Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

- Operational and procedural controls to restrict physical access
- Physical access controls, monitoring of physical access, alert & alarm
- Physical access logging
- Visitor escort procedures

CIP-007-6 Systems Security Management

Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

- Enable only necessary ports (logical and physical) and services
- Security Patch Management
 - Evaluate security patches, at least every 35 days
 - Take action within 35 days of evaluation
- Deploy method(s) to deter, detect, or prevent malicious code
- Security Event Monitoring
 - Log events (retain for at least 90 days)
 - Generate alerts for security events
 - Review log summary or sampling every 15 days

CIP-007-6 Systems Security Management (cont.)

- System Access Control
 - Interactive user access authentication
 - Identify all enabled default, generic, shared accounts
 - Identify individuals who have authorized access to shared accounts
 - Change known default passwords
- For password-only authentication for interactive user access
 - Minimum password length and complexity
 - Update passwords at least once every 15 months
 - Limit attempts or generate alerts

CIP-008-6 Incident Reporting and Response Planning

Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

- Establish Cyber Security Incidents Response Plan
- Test each Cyber Security Incident Response Plan every 15 calendar months.
- Use the plan. Retain records of reportable incidents. Document deviations.
- 90 days after a test or an event or 60 days after change in roles&responsibilities: document lessons learned, update the plan, communicate.
- Notify the Electricity Information Sharing and Analysis Center (E-ISAC)

CIP-009-6 Recovery Plans for BES Cyber Systems

Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

- Develop a recovery plan – identify roles and responsibilities of responders and conditions for activation of the plan
- Backup and storage of information used for recovery
- Testing every 15 months
 - Recovery from an incident
 - Paper drill or table top, or
 - Operational exercise
- Testing every 36 months
 - Operational Exercise
 - High Impact BES Cyber Systems only
- Document lessons learned, update, communicate

CIP-010-4 Configuration Change Management and Vulnerability Assessments

Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

- Establish a baseline Configuration
 - OS or firmware version
 - Application software version
 - Logical network accessible ports
 - Security patches applied.
- Authorize and document changes within 30 days of completing the change
- Configuration Monitoring for High Impact BES Cyber Systems at least every 35 days
- Vulnerability Assessment every 15 months

CIP-011-2 Information Protection

Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

- Methods to identify BES Cyber System Information.
 - Information that could be used to gain unauthorized access or pose a security threat to the BES Cyber System.
- Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.
- Prior to reuse or disposal take action to prevent the unauthorized retrieval of BES Cyber System Information.

CIP-012-1 Communication between Control Centers

Purpose: To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.

- Develop and implement a plan to mitigate risks posed by unauthorized disclosure and modification of real-time data between control centers
 - Identify security protection
 - Where to apply security protection
 - Identify responsibilities

CIP-013-2 Supply Chain Risk Management

Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

- Develop and implement a supply chain cyber security risk management plan for high and medium impact BES Cyber Systems.
 - Vendor notifications management – incident, access, vulnerabilities
 - Software integrity and authenticity of software patches
 - Controls for vendors-initiated Interactive remote access
- Review the plan and obtain CIP Senior Manager approval every 15 months

NERC CIP: The devil is in the details...

- NERC CIP standards:
 - <https://www.nerc.com/pa/Stand/Pages/default.aspx>

Networking Fundamentals

OSI and TCP/IP Network Layers

OSI	Layer	TCP/IP	Protocols
Application	7	Application	DHCP, DNS, FTP, HTTP, LDAP, NTP, POP, SMTP, SNMP, SSH, Telnet, TLS/SSL
Presentation	6		
Session	5		
Transport	4	Transport (TCP)	TCP, UDP, ...
Network	3	Internet (IP)	IPv4, ICMP, IPsec
Data Link	2	Network	Ethernet, L2TP, PPP, ARP
Physical	1		

The Open Systems Interconnection (OSI) model (ISO/IEC 7498-1) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO).

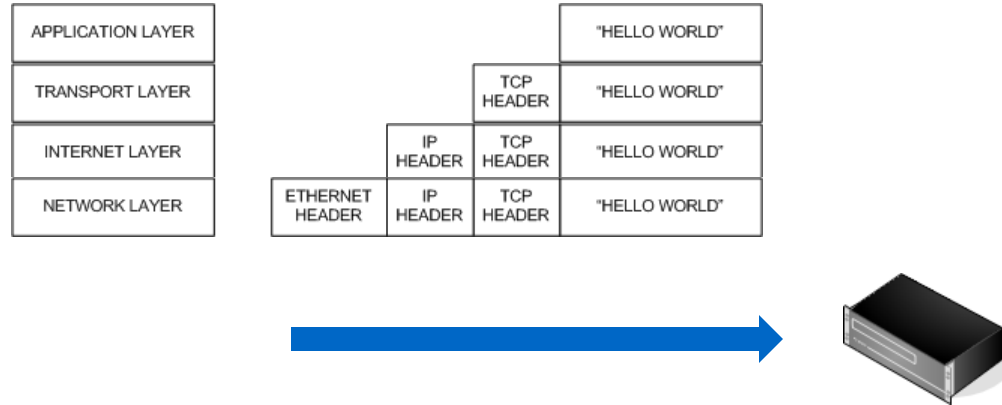
wikipedia



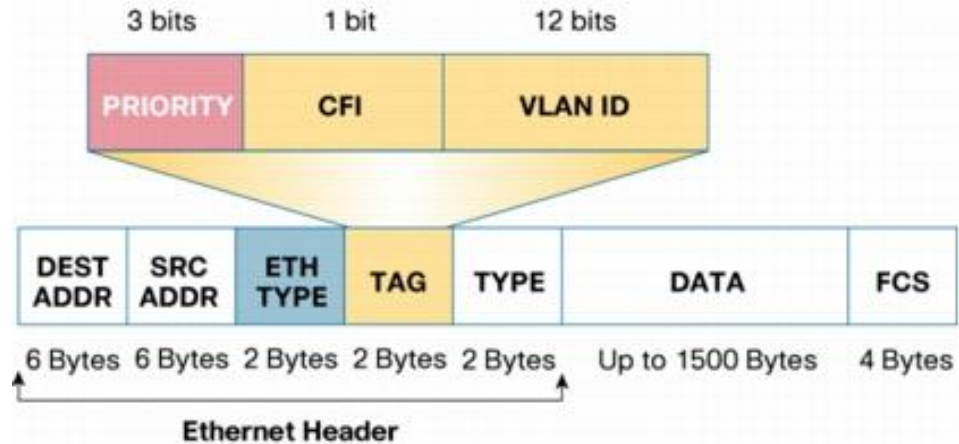
Powering Business Worldwide

© 2023 Eaton. All rights reserved.

Sending a Message Through the Stack



Layer 2: Ethernet Packet

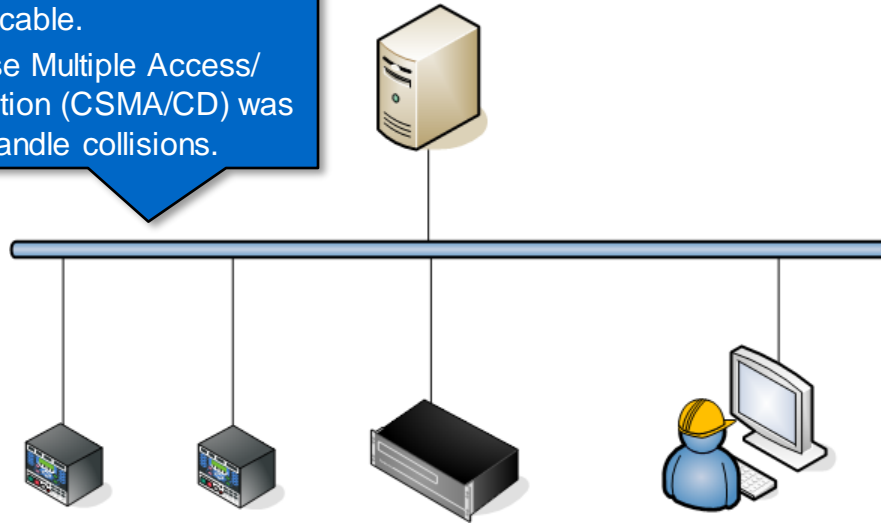


Broadcast address has all bits set to "1".

Ethernet Network Logical Representation

Originally, all devices were connected to the same coaxial cable.

Carrier Sense Multiple Access/ Collision Detection (CSMA/CD) was used to handle collisions.

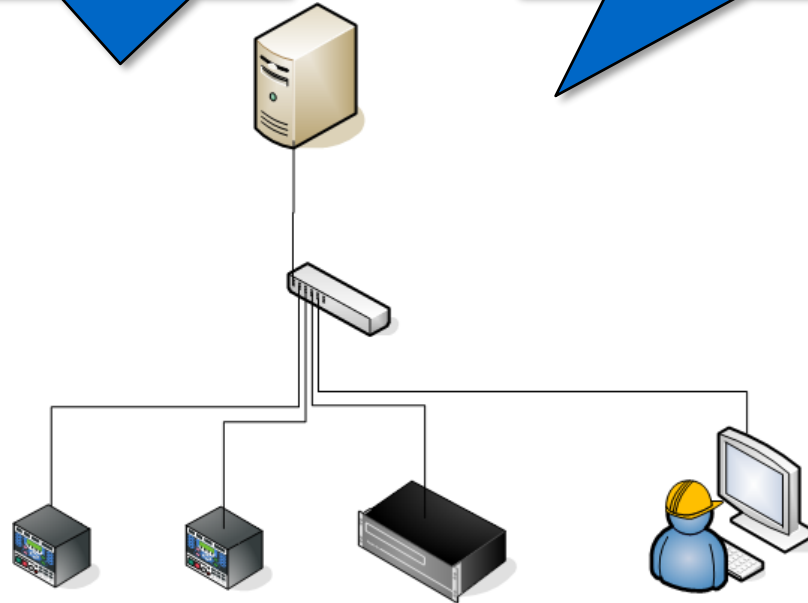


Each device has a built-in 48 bit physical Media Access Control (MAC) address. Messages are put on the wire and visible to all devices. The device chooses to process messages addressed to it.

Ethernet Network Physical Representation

A hub simply replaces the shared cable. Every packet is sent to every port.

A switch keeps track of MAC addresses and sends messages to the appropriate port only.



Managed Switches

- **Unmanaged** switches are plug-and-play.
- **Managed** switches provide the capability to modify the way they process data:
 - Turn particular port range on or off
 - Priority settings for ports
 - MAC filtering and other types of "port security" features
 - SNMP monitoring of device and link health
 - VLAN settings
 - 802.1X network access control

Network Devices

- A **hub** replicates messages to all ports. Each port sees every message on the network. Sniffing messages is easy. No confidentiality. No longer used.
- A **bridge** connects two network segments. It keeps track of MAC addresses and forwards messages not on its segment to the other segment.
- A **switch** combines the function of the hub and the bridge. It learns the MAC address on each port and forwards messages to the correct port. Unknown addresses are forwarded to other segments. Sniffing messages is much more difficult.
- **Hubs and switches** handle messages at layer 2, Ethernet.
- **Routers** handle messages between networks, at layer 3, the TCP/IP layer.

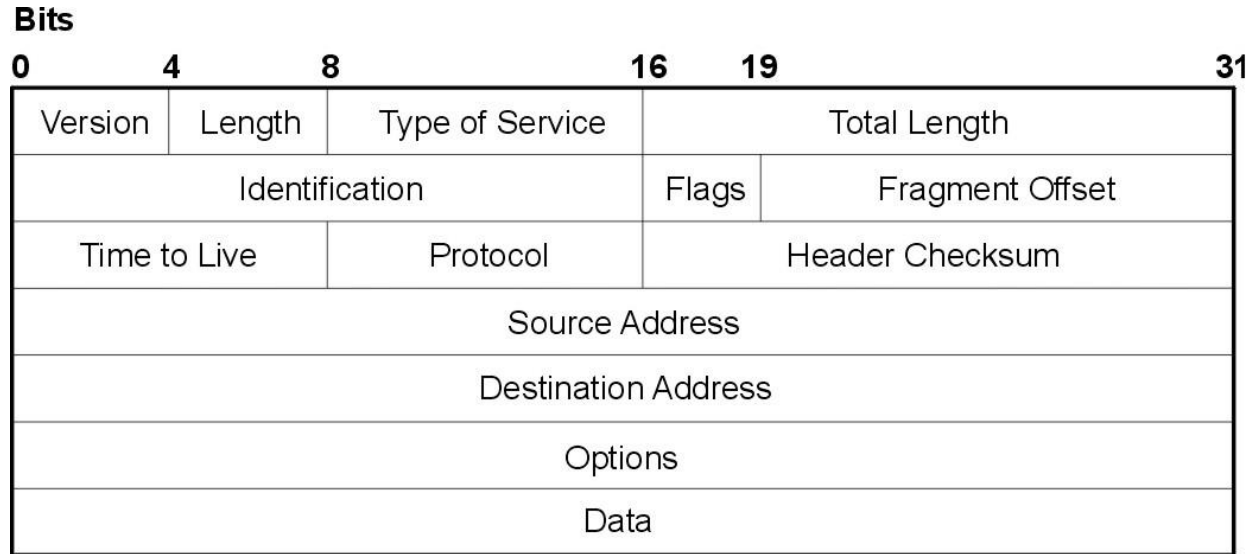
VLANs

- VLANs are used to partition a network in multiple domains.
- Domains are isolated so that packets can only pass between them via routers.
- VLANs provide a level of security by providing the capability to isolate network segments.
- VLANs provide a means of controlling broadcast messages.

Layer 3: IP – adding addressing

OSI	Layer	TCP/IP
Application	7	Application
Presentation	6	
Session	5	
Transport	4	Transport (TCP)
Network	3	Internet (IP)
Data Link	2	Network
Physical	1	

IP Packets



Broadcast destination address has all bits set to "1".

IP Addressing

- Each node on an IP network has a unique IP address
- The address is composed of two parts:
 - The network address
 - The host address
- Addresses are 32 bits and denoted as 4 four numbers separated by periods:
 - 10.135.21.204

Subnets and the Default Gateway

- The leftmost part of the IP address is the network address
- The **subnet mask** provides a method of identifying the network and host address, e.g.
 - 255.255.255.0 network address is leftmost 24 bits.
 - Host address is thus rightmost 8 bits
 - There can be 254 different host addresses in this network segment. Addresses 0 and 255 are reserved.
 - Any IP address with a different network address will need to be routed to the other network segment.
 - Note: This subnet can also be represented by adding /24 after the address, i.e. 10.135.21.204/24
- The **default gateway** is the address of the router.

Private Network Addressing

- There are not enough addresses available to connect every single device to the public Internet.
- But, not every device needs to be connected to the public Internet.
- The following addressing ranges are reserved for private networks and are not routed to the Internet:
 - 10.0.0.0 to 10.255.255.255
 - 172.16.0.0 to 172.31.255.255
 - 192.168.0.0 to 192.168.255.255
- These addresses require **Network Address Translation (NAT)** in order to access other networks

Mapping IP addresses to MAC addresses

- Each individual device on the network handles mapping IP addresses to MAC addresses.
- The device can obtain its IP address dynamically using the BOOTP or DHCP protocols.
- In automation networks, IP addresses are generally **static** and preconfigured.
- To determine a MAC address from an IP address, the device broadcasts an **Address Resolution Query** (ARP protocol).

ARP “spoofing” or “cache poisoning” consists of redirecting traffic to the attacker by sending fake ARP messages.



Name resolution and DNS

- Control systems typically use **static IP** addresses
- In order to use names, a name resolution service is necessary
 - “hosts” file
 - Microsoft NetBIOS/WINS
 - Domain Name System (DNS) to map names like www.eaton.com to IP addresses
 - DNS is based on a hierarchy of name servers.

IPv6

- IPv4 provides an addressing capability of 2^{32} or approximately 4.3 billion addresses
- This was not a concern as TCP/IP originally was a research project.
- An IPv6 address is 128 bits, for an addressing capability of 2^{128} or approximately 3.4×10^{38} addresses
- The standard size of a subnet in IPv6 is 2^{64} addresses
- IPv4 and IPv6 will continue to operate simultaneously
- Modern operating systems support dual IP stacks
- Other transition approaches are supported such as tunneling and proxying

Layer 4: TCP and UDP – transporting data

OSI	Layer	TCP/IP
Application	7	Application
Presentation	6	
Session	5	
Transport	4	Transport (TCP)
Network	3	Internet (IP)
Data Link	2	Network
Physical	1	

UDP

- **User Datagram Protocol (UDP)** sends out packets but does not guarantee delivery.
- Used when speed of delivery is more important (VoIP, video) than loss of a packet.
- Assumes that the network is reliable.
- Supports multicasting.

UDP Header

The port number identifies a service or application running on the destination server.

Source Port	Destination Port
Length	Checksum
Data	

UDP Applications and Ports

- Domain Name System (DNS) 53
- Boot Protocol (BOOT/DHCP) 67 and 68
- Trivial File Transfer Protocol (TFTP) 69
- Network Time Protocol (NTP) 123
- NetBIOS over TCP/IP (NBT) 137-139
- Simple Network Management Protocol (SNMP) 161 and 162
- Network File System (NFS) 162

Transmission Control Protocol (TCP)

- Most common protocol
- Connection oriented
- Provides guaranteed packet delivery
- Supports flow control
- Supports large amount of data per packet

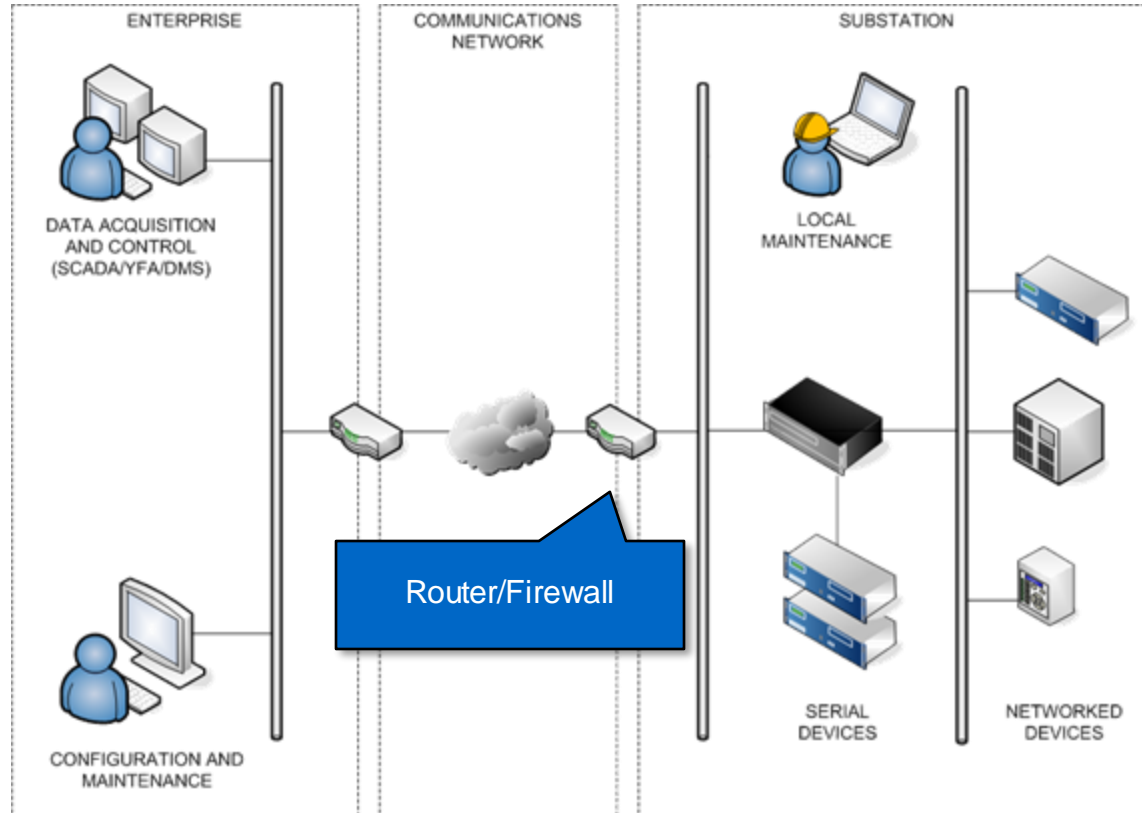
TCP Header

Source Port		Destination port	
Sequence Number			
Acknowledgement Number			
Offset HL	Reserved	Flags	Window
Checksum		Urgent Pointer	
Options			
Data			

TCP Applications and Ports

- File Transfer Protocol (FTP) 20 and 21
- Telnet 23
- Simple Mail Transfer Protocol (SMTP) 25
- Domain Name System (DNS) 53
- Hyper Text Transfer Protocol (HTTP) 80
- Post Office Protocol (POP) 110
- HTTP Secure (HTTPS) 443

Routers and Firewalls



Routers

- A router is a device that forwards data packets between computer networks.
- A router is connected to two or more data lines from different networks.
- It generally supports a variety of communications interfaces such as Ethernet, Frame Relay, T1/E1, ADSL, etc.
- When a data packet comes in on one of the lines, the router reads the address information in the packet to determine its ultimate destination.
- Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey.
- Routers and firewalls are often combined

Firewalls

- A firewall is a router with filtering rules
- Filters incoming and outgoing communications
- Protects systems from attack
- Perform Network Address Translation (NAT)
- Encrypts communications for VPN
- Logs and monitors traffic for intrusion detection

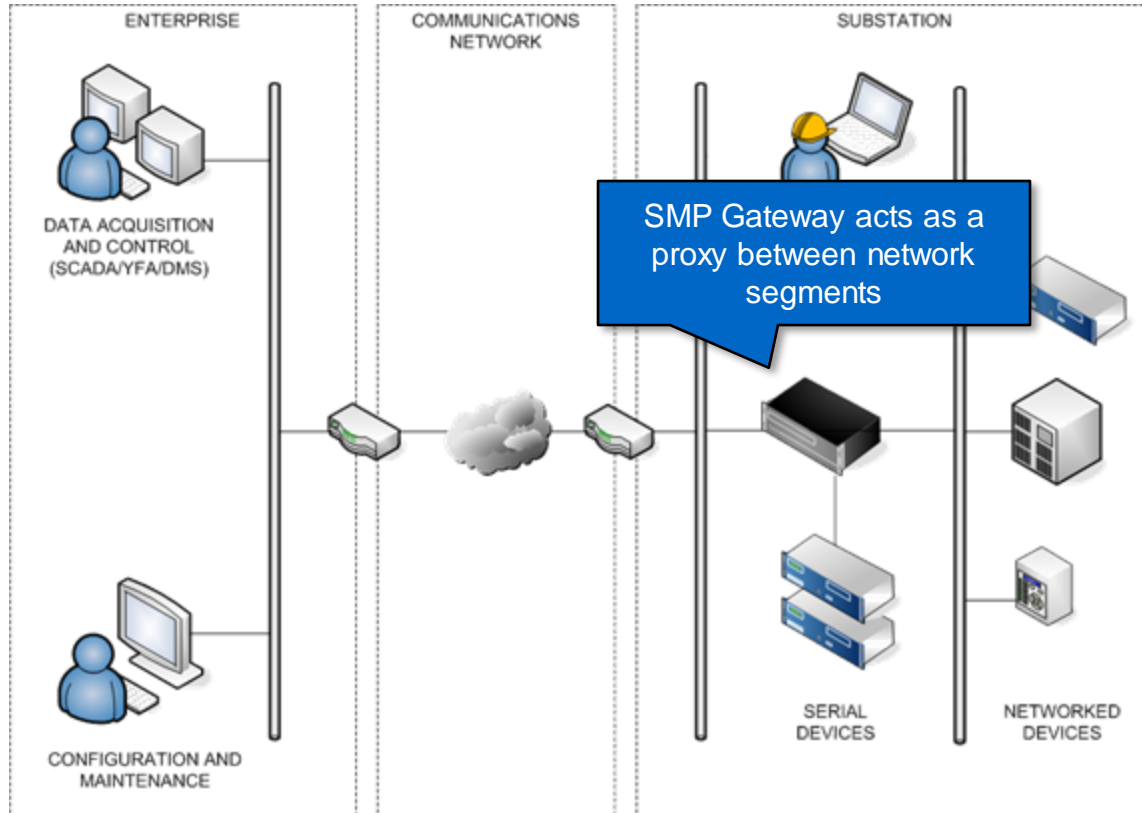
How Firewalls Filter Communications

- The firewall can be set up to block all traffic by default.
- Rules are used to define which packets can go through, based on:
 - Content
 - Source address
 - Destination address
 - Port number
- NERC CIP V5 requires that outgoing traffic must also be filtered
- There is no silver bullet, setting up firewall rules is complex and error prone.

Advanced firewalls can do “deep packet inspection” and filter on content. However, IT firewalls are generally not aware of OT protocols such as MODBUS and DNP3.



Proxy/Application Gateway



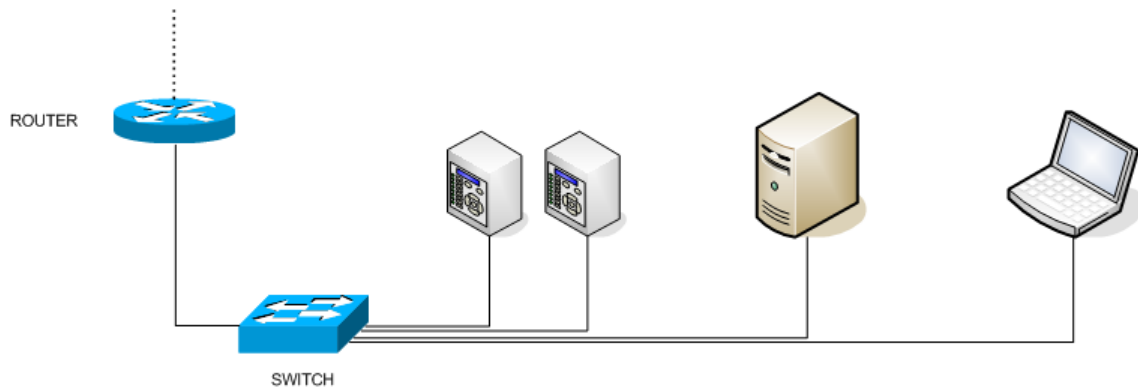
Proxies

- Packet filtering firewalls are fast, but difficult to manage
- Proxies, or application gateways, provide higher security as they only let through well-known traffic:
 - Client connects to proxy
 - Proxy connects to server
 - Client sends a message
 - Proxy intercepts message, tears it down, and validates content
 - Proxy rebuilds the message and sends it to server
- Proxies provide Network Address Translation (NAT)
- Eaton SMP Gateway and IMS Passthrough implement a proxy

Network Address Translation (NAT)

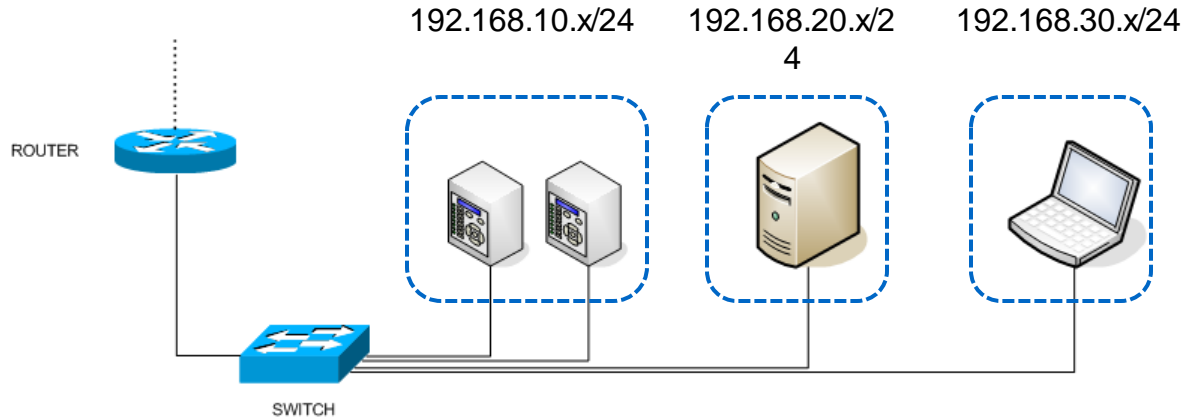
- The following addressing ranges are reserved for private networks and are not routed to the Internet:
 - 10.0.0.0 to 10.255.255.255
 - 172.16.0.0 to 172.31.255.255
 - 192.168.0.0 to 192.168.255.255
- In order to reach a server on the Internet, the private address needs to be replaced by a public address.
- The router performs NAT by replacing the internal address by the public address of the router.
- The Source Port field is use to keep track of the outgoing connection. The external server preserves this value.
- When the router receives the reply, it uses the source port to identify which internal address to substitute.

LAN



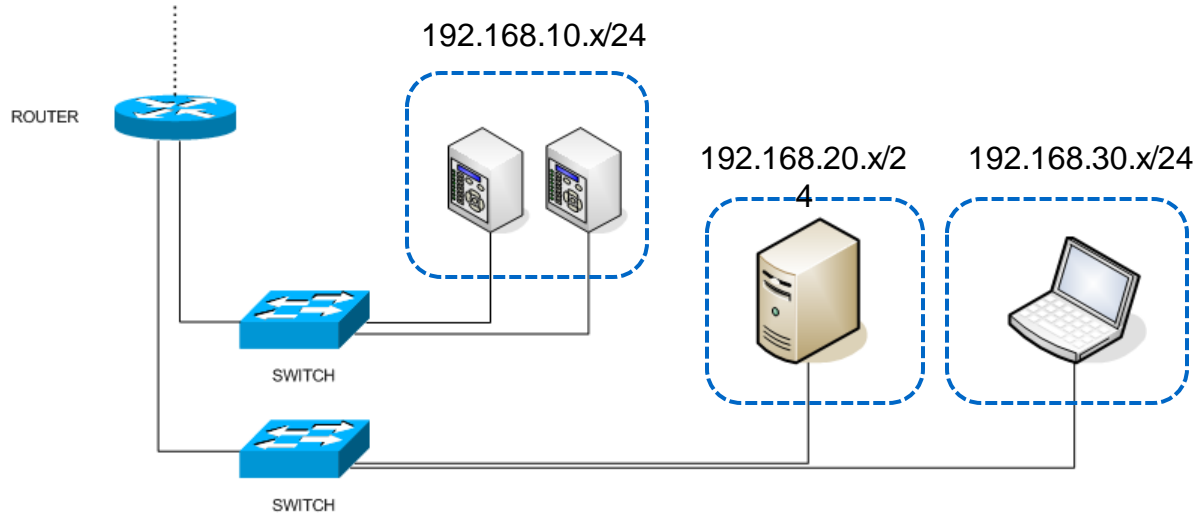
From the Ethernet perspective, every device can talk to every other device.
Ethernet broadcast traffic such as IEC 61850 GOOSE is visible to all devices.

Subnets



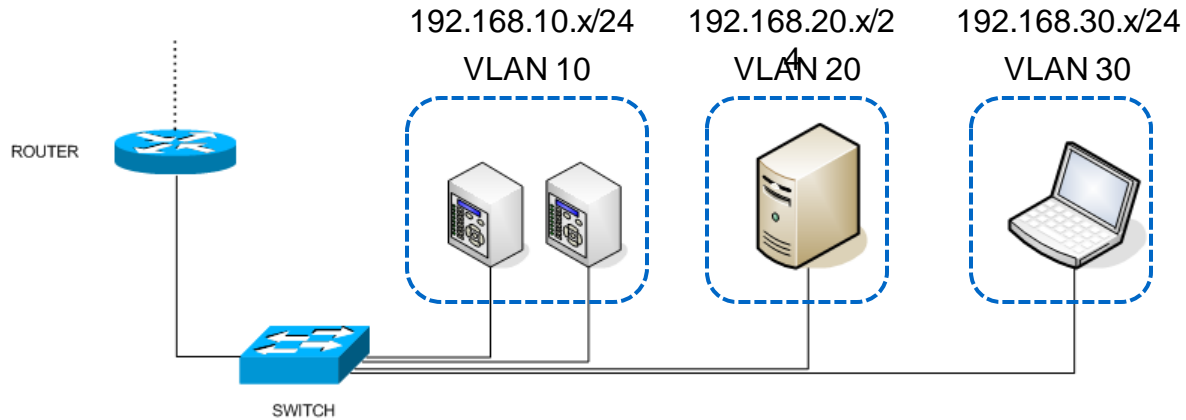
Creating TCP/IP subnets provides a first level of segmentation. Devices can only exchange data with other devices in the same subnet. Data exchanged between subnets must go through the router. However, Ethernet traffic remains visible to all devices.

Physical Segmentation



Using separate switches isolates Ethernet traffic.

VLANs



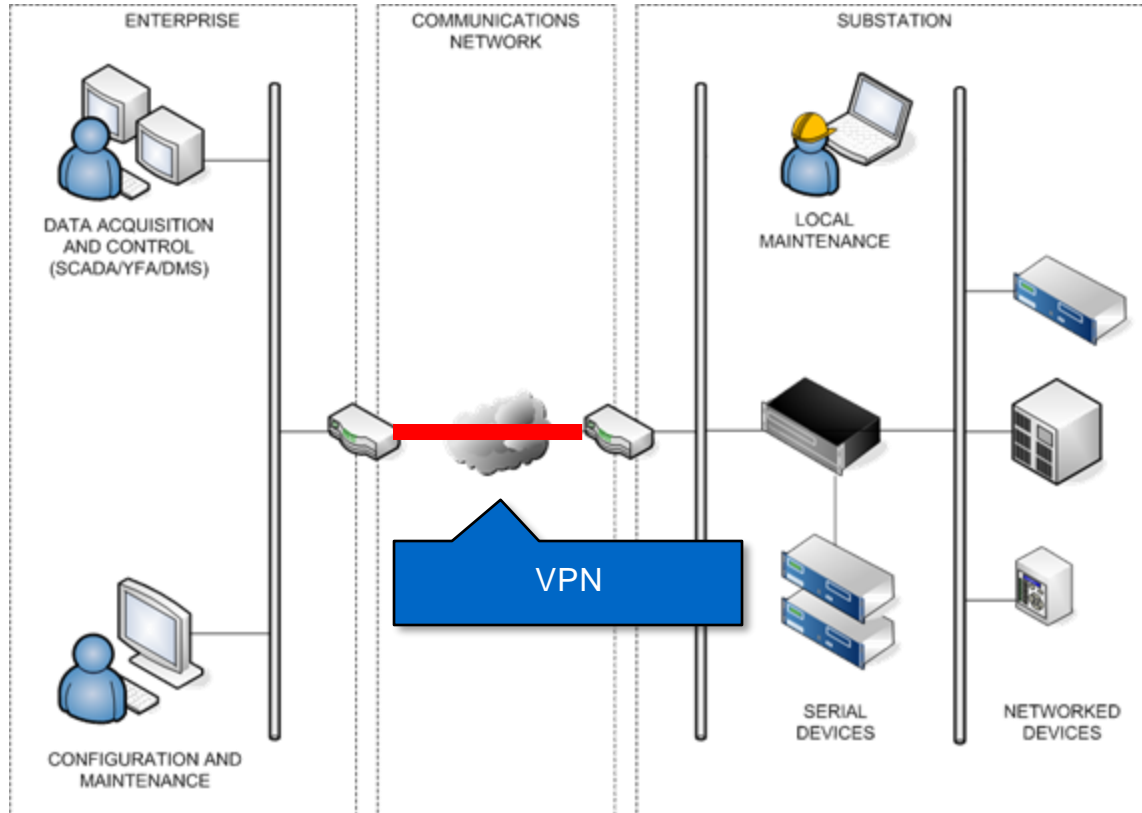
By adding VLANs, Ethernet traffic can only travel between devices in the same VLAN.

Data exchanged between subnets and VLANs must go through the router.

The industry best practice is to use VLANs and subnets together.

Securing the Link to the Substation

VPNs – Protecting Data in Transit



Virtual Private Networks (VPN)

- A VPN ensures the **confidentiality** of data in transit.
- The VPN acts as a tunnel between two networks.
- VPNs operate at Layer 2 and Layer 3 of the stack.
- Data is encrypted at one end and decrypted at the other end.
- **IPSec** is the industry standard for VPNs.
- It is typically implemented between two routers.
- The routers typically share a “secret” to ensure mutual authentication.
- The tunnel can be used by malware as well as legitimate traffic.

Authentication and Authorization

Authentication and Authorization

- **Active Directory (AD)** is a directory service for Windows domain networks.
- An AD **domain controller** authenticates and authorizes all users and computers in a Windows domain type network.
- **Security Support Provider Interface (SSPI)** is a Microsoft Windows API used to perform a variety of security-related operations such as authentication.
- **Kerberos** is a computer network authentication protocol which works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.
- The **Lightweight Directory Access Protocol (LDAP)** is an application protocol for accessing and maintaining distributed directory information services over an IP network.
- **Remote Authentication Dial In User Service (RADIUS)** is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service.
- RADIUS servers refer to external sources — commonly SQL, Kerberos, LDAP, or Active Directory servers — to verify the user's credentials.

Role Based Access Control

- Role Based Access Control (RBAC) is an approach to restricting system access to authorized users.
- Roles are created for various job functions.
- Permissions to perform certain operations are assigned to specific roles.
- Users are assigned to roles, e.g. administrator, engineer, technician, operator
- RBAC makes it easier to manage authorization

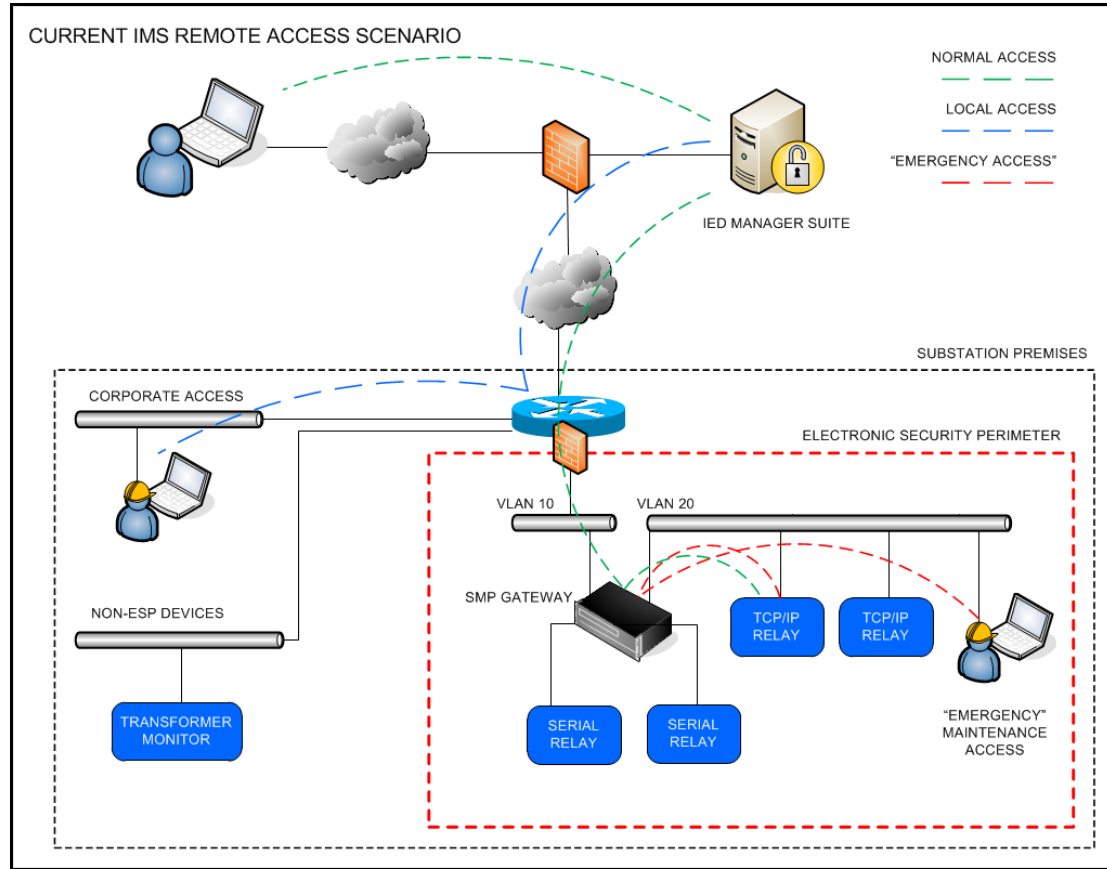
DNP3 user roles

Value	Name	Permissions						
		Monitor Data	Operate Controls	Transfer Data Files	Change Config	Change Security Config	Change Code	Local Login
<0>	VIEWER	Yes	No	No	No	No	No	No
<1>	OPERATOR	Yes	Yes	No	No	No	No	No
<2>	ENGINEER	Yes	No	R/W/D	Yes	No	No	Yes
<3>	INSTALLER	Yes	No	R/W	Yes	No	Yes	Yes
<4>	SECADM	No	No	No	No	Yes	Yes	Yes
<5>	SECAUD	Yes	No	R	No	No	No	Yes
<6>	RBACMNT	Yes	No	D	Yes	Roles only	No	No
<7 ..32767>	RESERVED	For future use.						
<32768 ..65535>	PRIVATE	Defined by external agreement. Not guaranteed to be interoperable.						



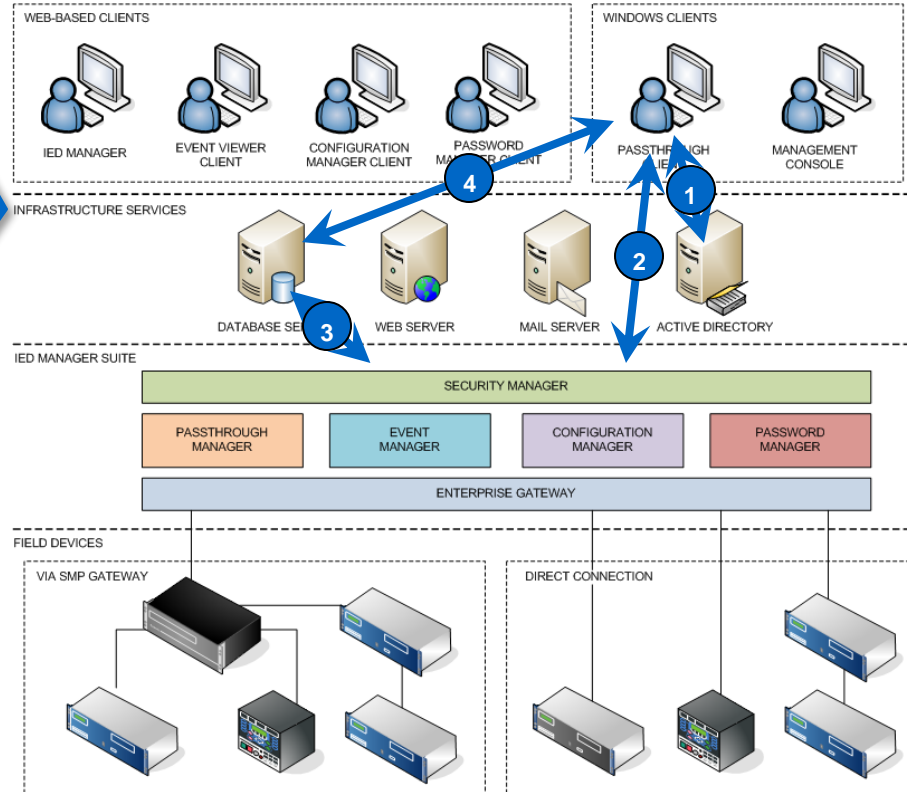
NERC CIP secure remote access

Secure Remote Access



IMS Passthrough Manager

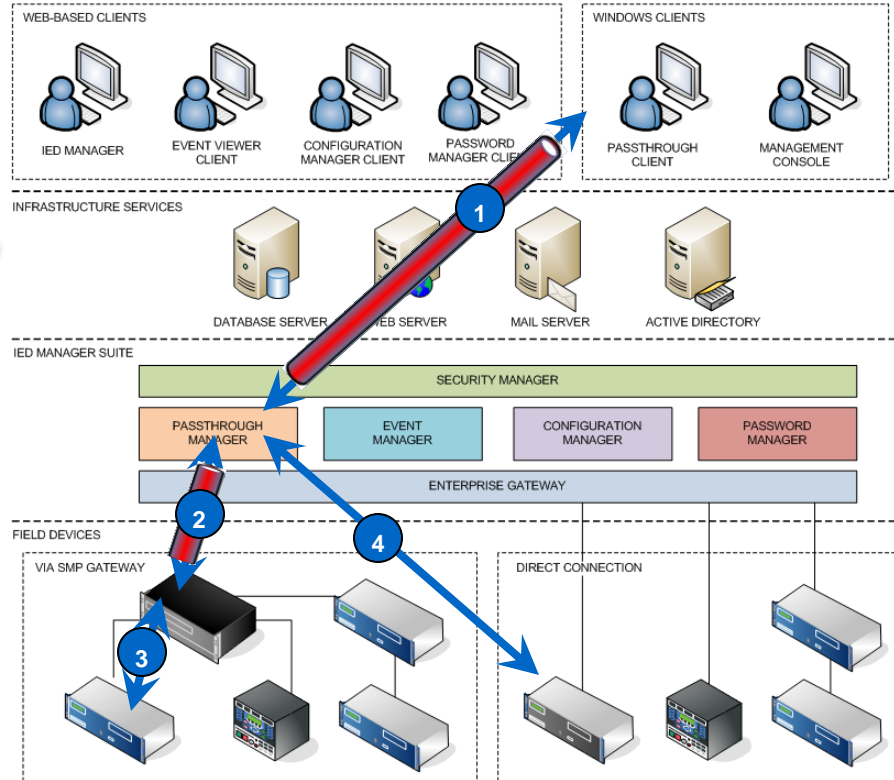
1. User logs in to Windows and is authenticated by Active Directory
2. Passthrough Client forwards Windows session ticket to Security Manager
3. Looks up permissions and IEDs in database
4. Forwards and displays list of authorized devices



Passthrough Manager

1. Passthrough Client sets up an encrypted link to server
2. Server sets up an encrypted link to SMP Gateway
3. Gateway connects to device
4. Alternatively, server connects directly to device

Client captures all data from application and forwards to IED via server. Server performs auto-login and command filtering



Logging and Monitoring

Intrusion Detection Systems (IDS)

- IDS reports attacks against monitored systems
- It analyzes traffic and generates alerts
- Uses signature or protocol analysis
- Required in NERC CIP V5 for control centers
- The challenge is achieving a good balance between:
 - True positive and False positives
 - True negatives and False negatives

Signature Analysis

- The IDS generates alerts based on:
 - Protocol, address and port information
 - Payload contents (deep packet inspection)
 - Traffic flow analysis
 - Fields in the packet
- IDS is a valuable security technology for control systems as the network traffic is very predictable.
- IDS does not work with encrypted data!

Security Information and Event Management (SIEM)

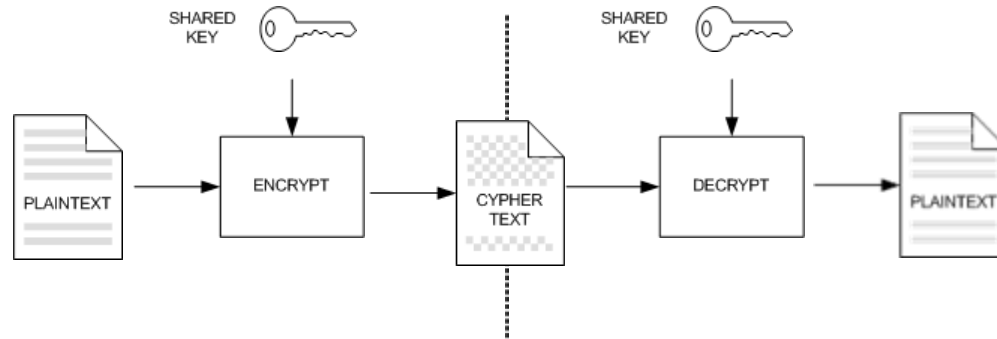
- The industry standard for message logging is **Syslog**.
- SIEM solutions capture logging messages to provide real-time analysis of security alerts generated by network hardware and applications.
 - Data aggregation
 - Correlation
 - Alerting
 - Dashboards
 - Compliance
 - Retention

Symmetric Cryptography

Terminology

- A **cipher** is a method that encrypts or disguises text.
- The **plaintext** or clear text, is the original message before **encryption**.
- The **ciphertext** is the encoded version of the message.
- **Encryption** is the process of transforming **plaintext** to **ciphertext**.
- **Decryption** is the opposite.

Symmetric Cryptography



ALICE



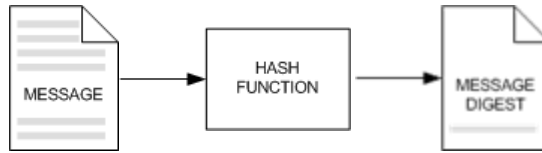
BOB

Symmetric Cryptography Standards

- 1977 – Data Encryption Standard (DES) adopted as FIPS 46 federal standard for unclassified data.
 - 56-bit key
 - In 2008, it was demonstrated that DES could be broken in less than a day through brute force.
- 1999 – FIPS 46-3 standard recommends the use of Triple DES (TDES or 3DES) for increased security.
 - With 2 keys, effective strength of 80 bits
 - With 3 keys, effective strength of 112 bits and approved for use until 2029
- 2001 – FIPS 197 Advanced Encryption Standard (AES)
 - 128, 192, or 256 bit keys
 - 128 bit key is approved for use beyond 2030

Hashing and Message Integrity

Message Integrity



Message Authentication
Code
(MAC)

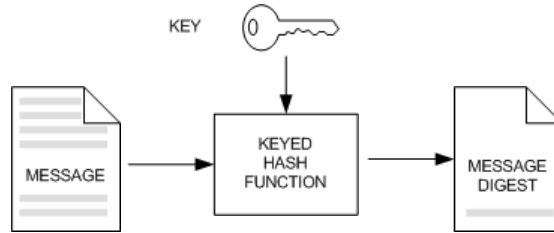
Message Authentication Codes

- Checksums and Cyclic Redundancy Check (CRC) designed to detect common communications errors.
- CRC is fast, but not designed to provide security. Easy to generate two messages with same value.
- Cryptographic hashes are slower, but it is extremely difficult to generate two messages with same hash.
- MD5 (Message-Digest algorithm 5) is widely used and generates a 128 bit digest. It is no longer considered secure.
- MD5 is widely used to store passwords and to validate the authenticity of data files.

Message Authentication Codes (cont.)

- SHA-1 replaced MD5 and produces a 160 bit digest. However, weaknesses have been identified and it is no longer acceptable for signature verification.
- SHA-2 defines four functions to replace SHA-1: SHA-224, SHA-256, SHA-384 and SHA-512.
- SHA-224 is approved for use until 2029.
- SHA-3 has been approved as a dissimilar alternative to SHA-2.

Message Integrity and Authentication



Hashed-based Message
Authentication Code
(HMAC)

Hash-based Message Authentication Code (HMAC)

- The Hash-based Message Authentication Code (HMAC) algorithm uses a key as part of the hashing process.
- HMAC algorithm is designed to be used with any hash function.
- HMAC with key greater than 112 bits, but shorter than 128 bits is acceptable until 2030.
- After 2030, key should have more than 128 bits.

Asymmetric Cryptography

Solving the Key Management Challenge: Asymmetric Cryptography

- In **symmetric** cryptography both parties share a secret key used to encrypt and decrypt messages.
- In **asymmetric** cryptography, keys come in pairs.
- A message encrypted with one key can only be decrypted using the other key.
- One key is known as the **public key** and can be widely shared.
- The other key, known as the **private key**, is kept in a secure location.
- The sender of a message can use the intended receiver's public key to encrypt the message.
- Only the intended receiver with the appropriate private key will then be able to decrypt the message.

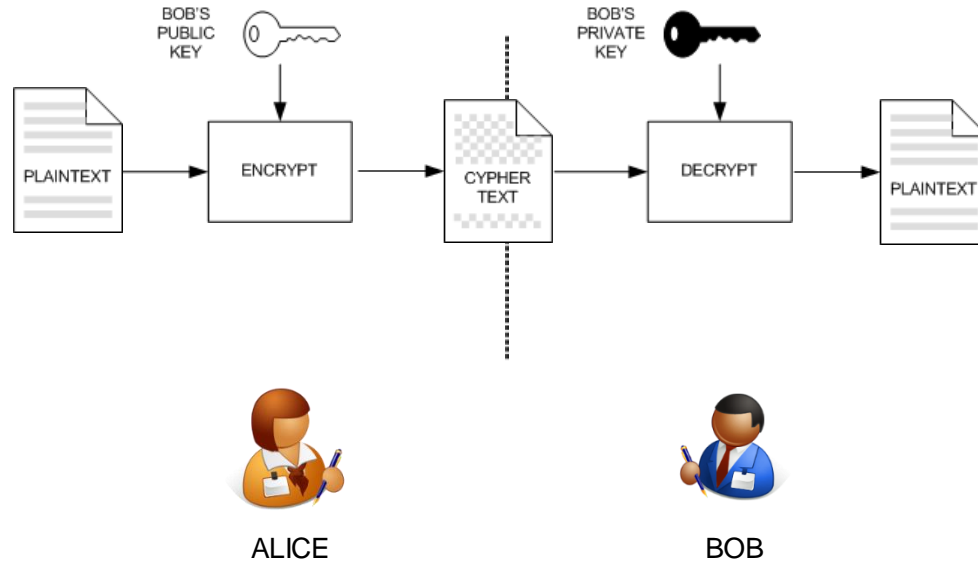
Rivest, Shamir and Adleman (RSA)

RSA performs the generation of a public/private key pair as follows:

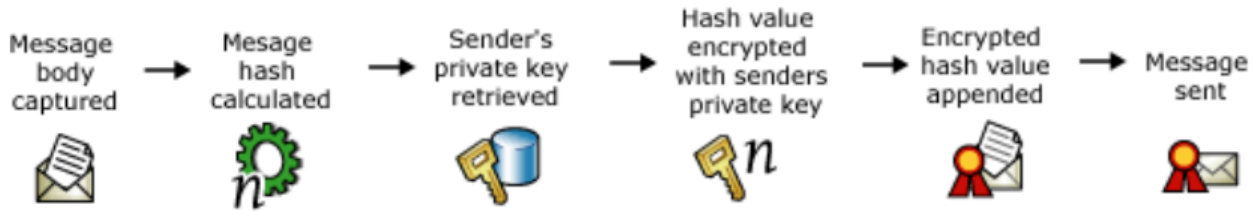
Two large primes, p and q are used to compute their product $n = pq$, where n is called the modulus. A number is chosen, e , which is less than n and relatively prime to $(p-1)(q-1)$, which means e and $(p-1)(q-1)$ have no common factors except 1. Another number is chosen, d , such that $(ed - 1)$ is divisible by $(p-1)(q-1)$. This is the inverse of e and means that $ed = 1 \pmod{(p-1)(q-1)}$.

The values e and d are called the public and private exponents, respectively. The public key is the pair (n, e) and the private key is (d) .

Asymmetric Cryptography

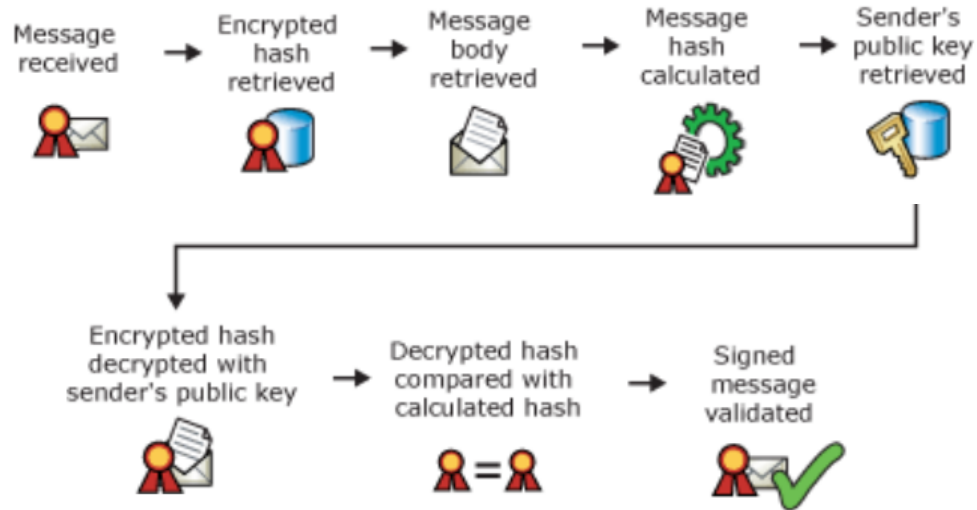


Digital Signatures



ALICE

Validating a Digital Signature



BOB

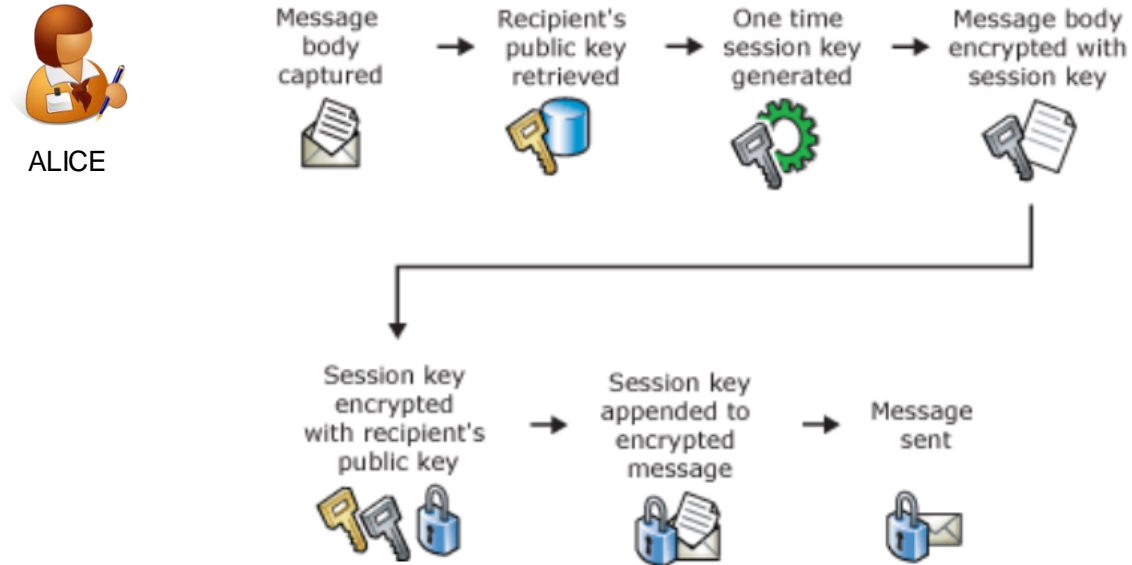


Powering Business Worldwide

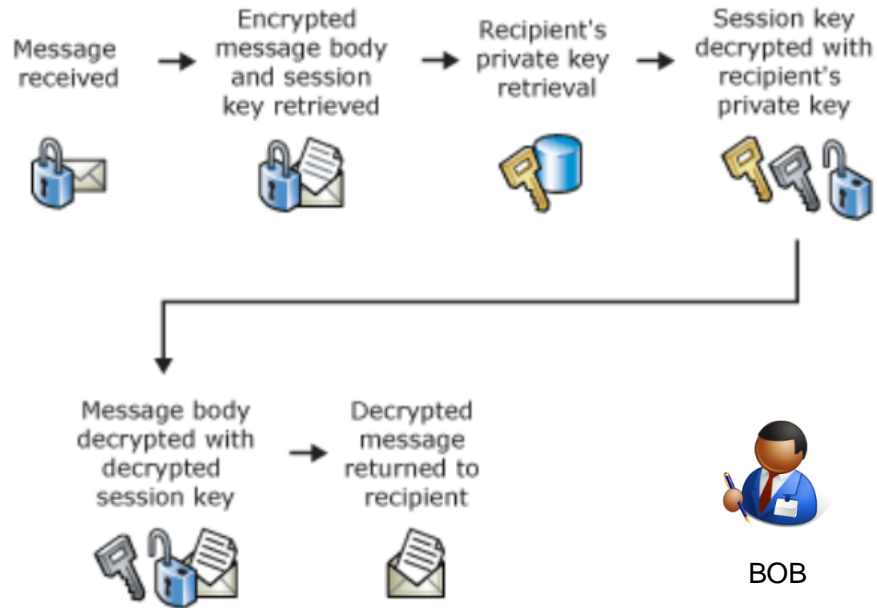
Understanding Public Key Cryptography
[http://technet.microsoft.com/en-us/library/aa998077\(v=exchg.65\).aspx](http://technet.microsoft.com/en-us/library/aa998077(v=exchg.65).aspx)

© 2023 Eaton. All rights reserved.

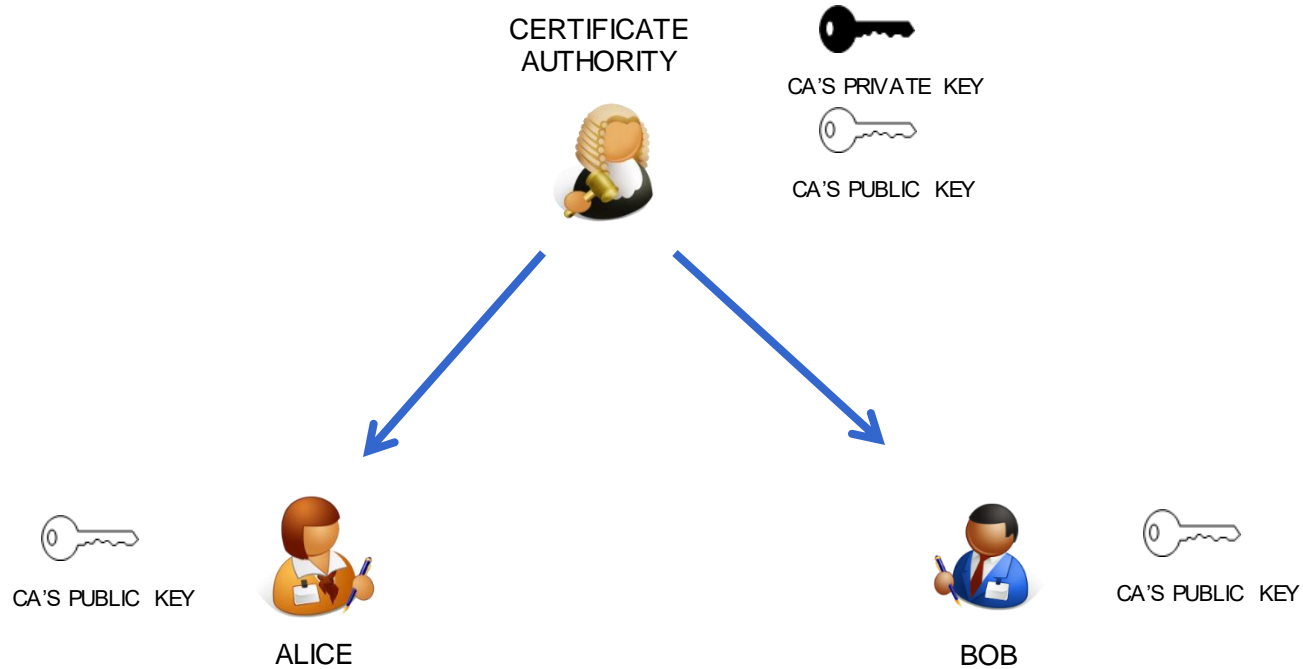
Public Key Cryptography and Message Encryption



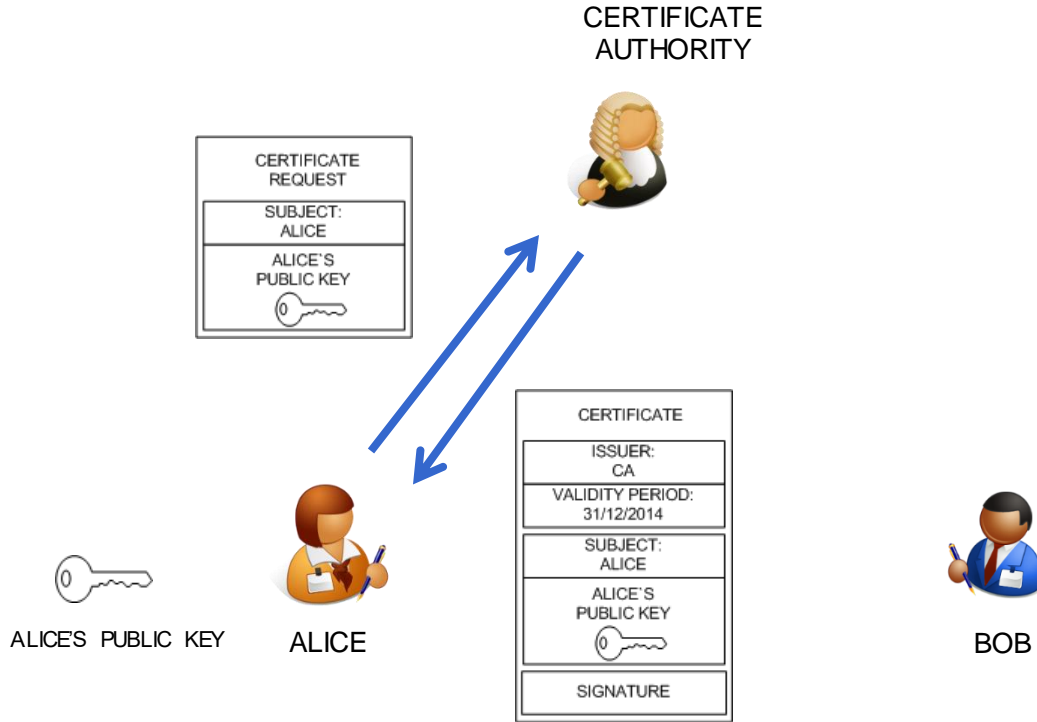
Decrypting the Message



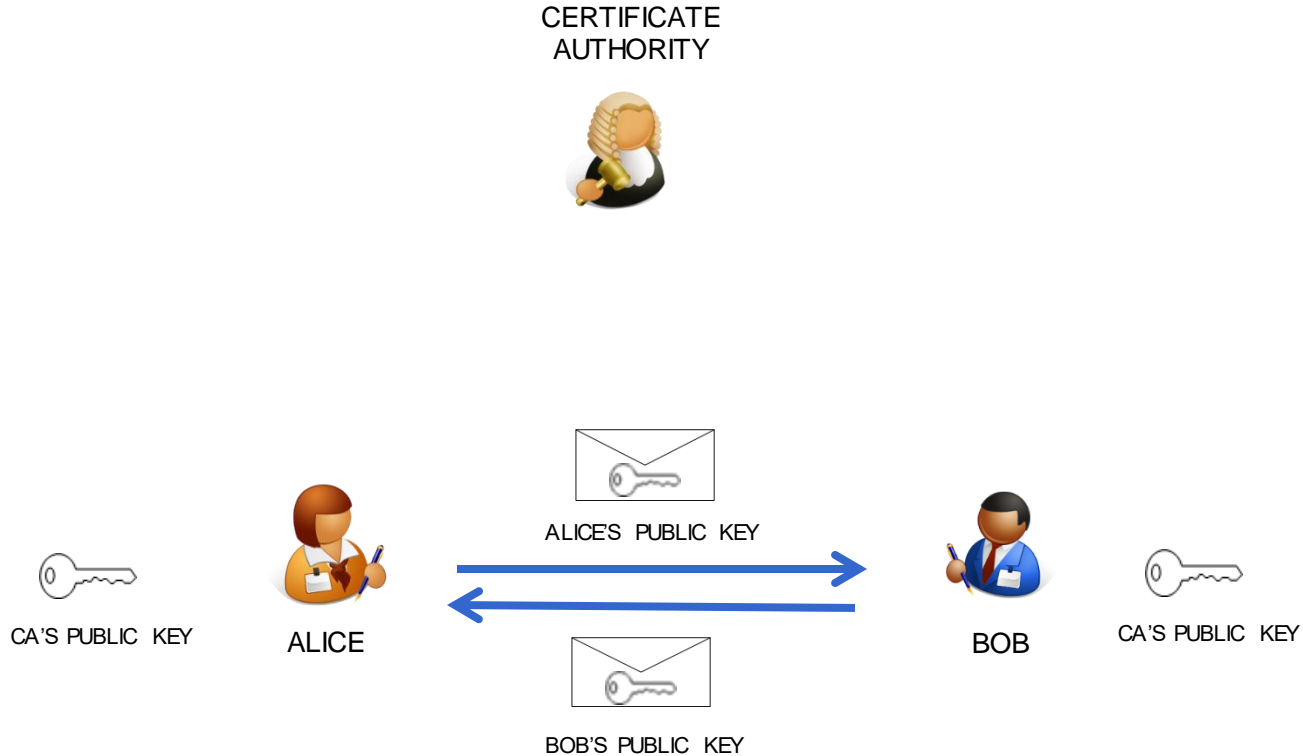
Distributing Public Keys: The Trusted Third Party



Public Key Certificates



The Trust Relationship

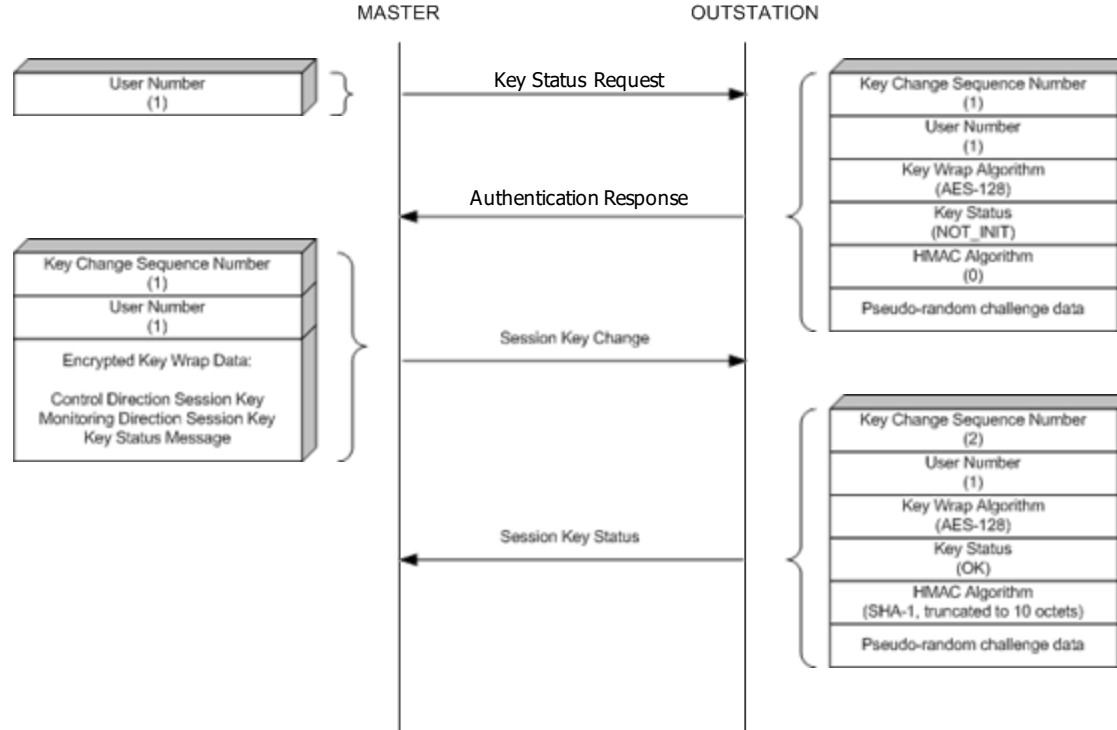


Terminology

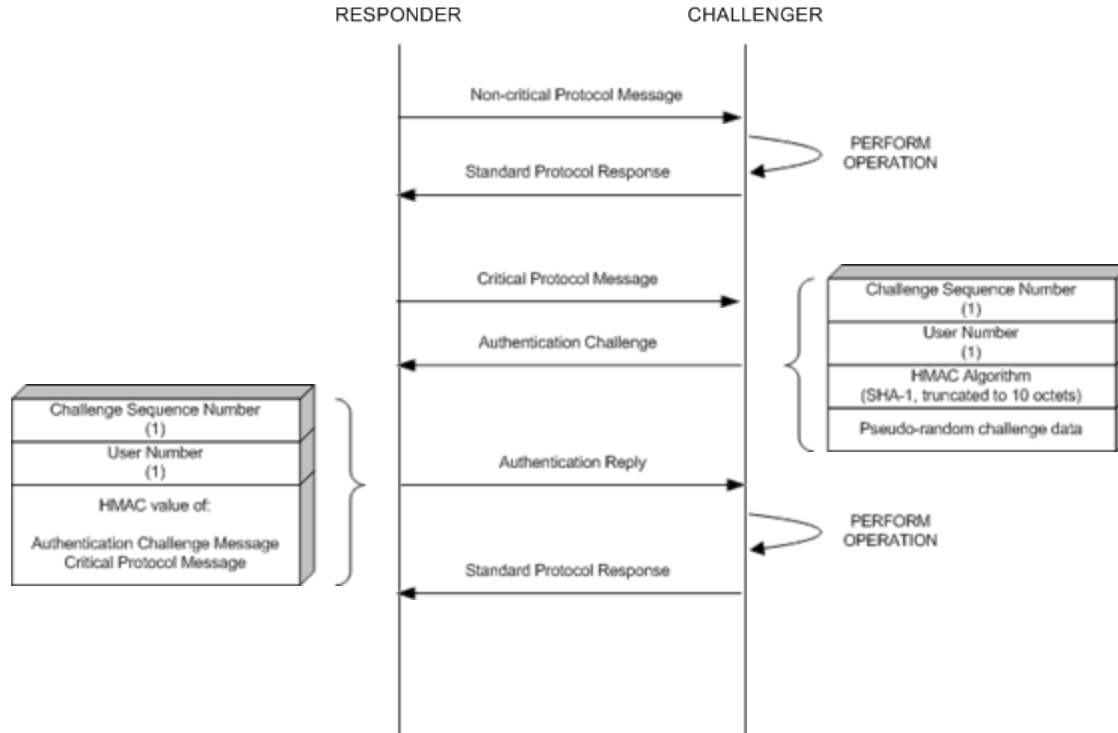
- A **public-key infrastructure** (PKI) is a system for the creation, storage, and distribution of digital certificates.
- **X.509** is an ITU-T standard for a public key infrastructure (PKI). It specifies standard formats for public key certificates, certificate revocation lists, and certification path validation algorithm.
- The **certificate authority** (CA) issues and verifies the digital certificates.
- The **registration authority** (RA) verifies the identity of users requesting information from the CA.
- The **certificate revocation list** (CRL) is a list of certificates that have been revoked and should no longer be trusted.

DNP3 Secure Authentication

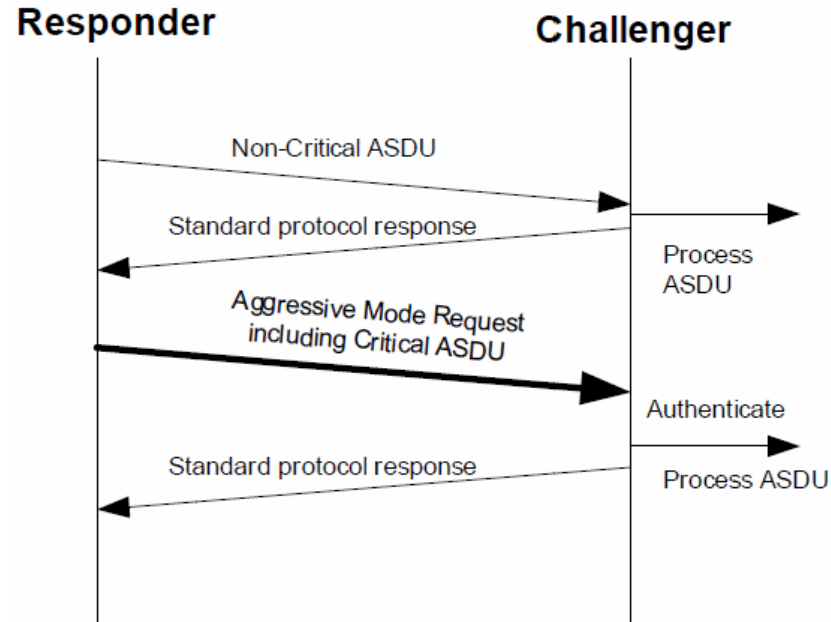
DNP3 Secure Authentication Initial Handshake



DNP3 Secure Authentication Challenge-Response



DNP3 Secure Authentication Aggressive Mode



EATON

Powering Business Worldwide