5 Fundamentals of OT Networking

Topics

- Understanding OT Networking
- Types of Networks in OT
- Challenges in OT Networking
- Understanding Network Segmentation
- Air Gaps and Physical Segmentation
- Use of Separate Hardware Vendor Equipment
- Redundancy and Resiliency
- Scalability and Flexibility

Understanding OT Networking

Overview

- Goal: robust and reliable network infrastructure
- Can withstand harsh industrial settings
- Network types
  - LAN, WAN, Fieldbus, Wireless
- Protocols
  - Modbus, DNP3, OPC, PROFIBUS
- Challenges
  - Legacy systems
  - Segmentation
  - Scalability and resiliency

Types of Networks in OT

Types of Networks

- **LANs**
  - Connect devices in a small area
- **WANs**
  - Span larger areas, up to countries or continents
- **Fieldbus** networks
  - Serve a specific area within a factory or plant
  - Connect sensors and actuators to controllers
- **Wireless** networks
  - Serve mobile or difficult-to-reach devices
  - Provide flexibility where cables cannot reach

OT Protocols

- **Modbus**
  - Simple and robust, for industrial devices
- **DNP3**
  - Reliable for critical infrastructure like power grids
- **OPC**
  - Interoperable among different vendor devices
- **PROFIBUS**
  - Fast, deterministic communication in automation systems

Challenges in OT Networking

- Integrating legacy systems
- Network segmentation
  - To contain disruptions or security breaches
- Scalability
- Resiliency

Future of OT Networking

- **Software-Defined Networking (SDN)**
  - Unprecedented control over network traffic
- **Industrial Internet of Things (IIoT)**
  - Brings together thousands of devices
  - Rich data for analytics and decision-making
- **Edge Computing**
  - Process data closer to where it's generated
  - Reduces latency and bandwidth usage

Challenges in OT Networking

Challenges

- **Legacy Systems**
  - May require upgrades or gateways
- **Interoperability**
  - May require standard protocols like OPC-UA or middleware
- **Network Segmentation**
  - Using firewalls, VLANs, and access controls
  - Strike a balance between security and operational needs
- **Scalability and Future-Proofing**
  - Use scalable networking technologies and architecture

Challenges

- **Resilience and Redundancy**
  - Redundant network paths and power supplies
  - Backups
  - Link Aggregation Control Protocol (LACP) or EtherChannels
- **Skills and Expertise**
  - Must understand IT and OT

Understanding Network Segmentation

VLANs (Virtual Local Area Networks)

- A VLAN may contain devices on different physical LANs
- Each VLAN is its own broadcast domain
- This decreases unnecessary traffic and provides some security
- Separate critical systems from the rest of the network
    - Example: separate industrial control systems from corporate IT systems
- Inter-VLAN routing goes through a router or layer 3 switch

Subnetting and VRF

- **Subnetting**
  - Divides a large network into separate portions called subnets
  - Subnets can be used to segregate regions with different security requirements
- **VRF (Virtual Routing and Forwarding)**
  - A physical router creates several virtual routing instances
    - Called **Virtual Private Networks (VPNs)**

PBR (Policy-Based Routing)

- Replaces traditional routing with bespoke policies or criteria
- Dictate specific routes based on source address, packet size, service type, etc.
- Can ensure reliable delivery and lower latency
    - Send all traffic from a certain sensor through a fast path
- Can also balance network loads across multiple links
- Can send sensitive data through encrypted tunnels

ACL (Access Control Lists)

- Enforce security policies based on predefined rules
- Included in routers, switches, and firewalls
- Not foolproof, but part of a defense-in-depth strategy

DMZ (Demilitarized Zone)

- A buffer zone between an internal OT network and an external network
- Has services that should be publicly accessible
  - But separated from the core OT network
- **Example 1: Remote Access Gateways**
  - Provide only one way to reach the Internet from the OT network, for maintenance personnel
  - A VPN in the DMZ

DMZ (Demilitarized Zone)

- **Example 2: Web Servers**
  - Placed in the DMZ, if the web server is hacked, the attacker doesn't have direct access to the OT network
- **Example 2: Multi-Tier DMZ Architecture**
  - One DMZ for external-facing services, like a Web server
  - A second DMZ for internal services used by other departments within the organization
  - This isolates threats and impedes lateral movement

SDN (Software-Defined Networking)

- Separates the system that controls the network (**control plane**)
- From the system that forwards traffic (**data plane**)
- Uses a centralized network controller
  - Programmatically configured and managed, allowing
- **Dynamic Network Configurations**
  - Rapid changes based on changing demands or conditions
- **Enhanced Network Segmentation**
  - Segments can be dynamically adjusted to mitigate the spread of security threats
  -

SDN (Software-Defined Networking)

- **Scalability**
  - SDN is easily reprogrammed for larger or modified network
- **Security Enhancements**
  - A central view of the network
  - Quicker detection of anomalies or suspicious activities
  - Immediate implementation of security policies

Air Gaps and Physical Segmentation

Air Gaps

- Physically isolates a computer or network
- No network interfaces connected to other systems
- Example: Industrial Control System (ICS) with a Safety Instrumented System (SIS)
  - SIS monitors a process and returns it to a safe state if a dangerous condition is detected
  - Often air-gapped to maintain integrity and availability

Physical Segmentation

- Separating networks by using different hardware components
- Separated by a firewall

Use of Separate Hardware Vendor Equipment

Diversity

- Using networking devices and equipment from different manufacturers
- Avoids a single point of failure

Redundancy and Resiliency

Redundancy in Network Design

- Duplicate crucial network components
  - Power supplies, routers, switches, network links
- **Link Aggregation Control Protocol (LACP)**
  - Combines several physical links into one logical link
  - Produces a high-capacity fault-tolerant connection
- **EtherChannels**
  - Merges multiple Ethernet links into one logical channel
- **Spanning Tree Protocol (STP)**
  - Prevents loops in redundant network topologies

Virtual Router Redundancy Protocol (VRRP)

- Creates a virtual router from several physical routers

Scalability and Flexibility

Scalability and Flexibility

- **Scalability**
  - Ability of an OT network to gracefully handle expansion and increased demands
- **Flexibility**
  - An OT network's capability to adapt to changing operational needs
  - New devices, system upgrades, emerging technology
- **Modular Design**
  - Enhances scalability and flexibility

Virtualization and Containerization

- Create virtual machines that are separate from the underlying hardware
- Increases efficient resource allocation
- Dynamic allocation of virtual servers

Edge and Fog Computing

- Locate computation closer to end devices
- Reduces latency
- Enhances scalability and flexibility

The Cloud

- On-demand resources
- Scalability on an elastic basis
- Capacity to rapidly deploy and manage applications

Ch 5