Network &Security
TECHNOLOGIES

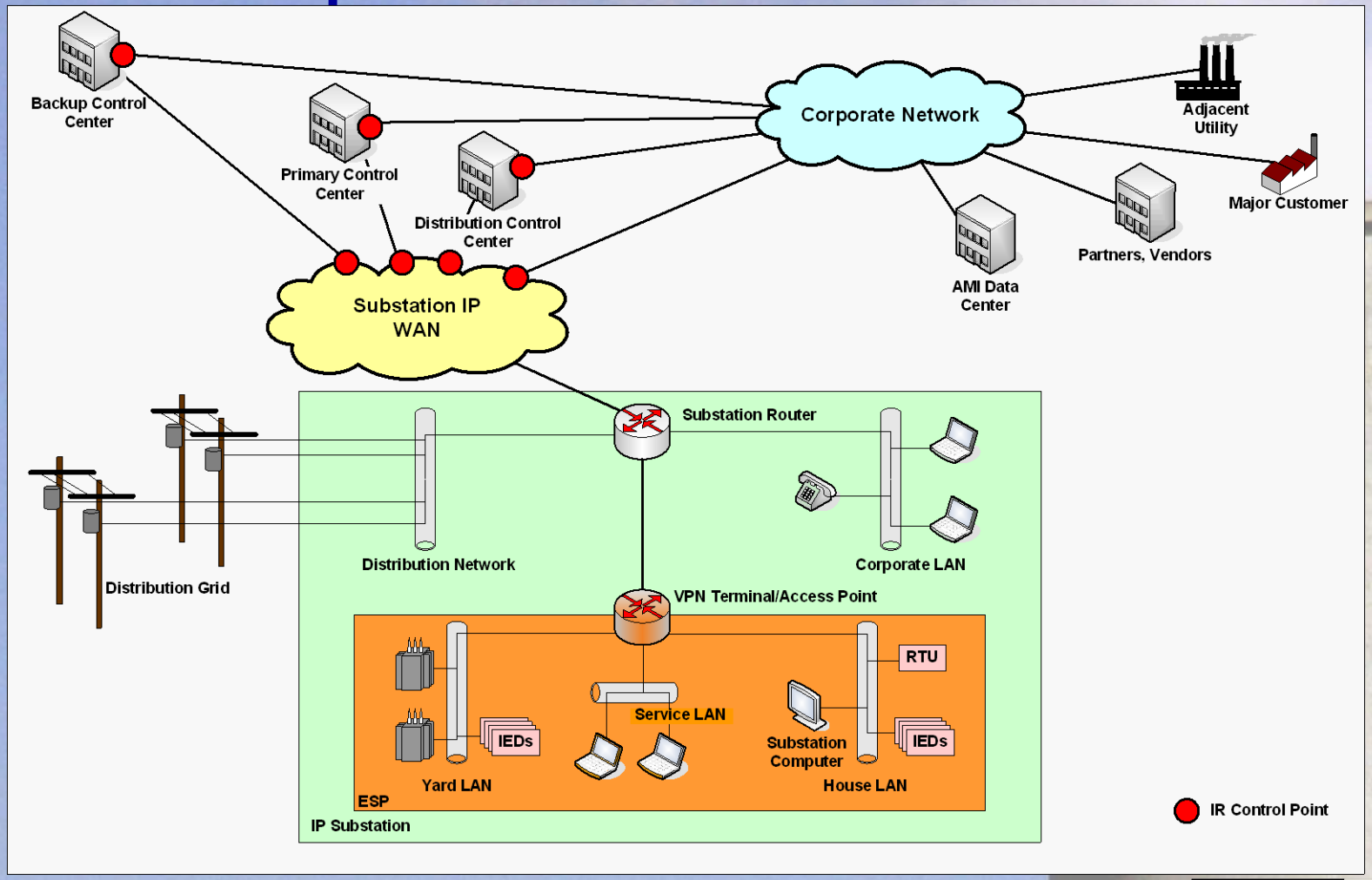
Best Practices in Grid Security

Jeff Kimmelman
Principal Consultant and CTO
Network & Security Technologies
jkimmelman@netsectech.com
978-897-0131

Introduction

- N&ST works with BES participants since 2003 to secure SCADA and control systems.
- We work with more than 30 asset owners:
  - Small, medium, large
  - Metropolitan, regional, multi-state
  - Generation, transmission, load serving
- Primarily 2 types of projects:
  - Security compliance – Documentation, gap analysis, remediation
  - Secure networks and systems – Design and deployment

An Architecture for a Secure Operations Network

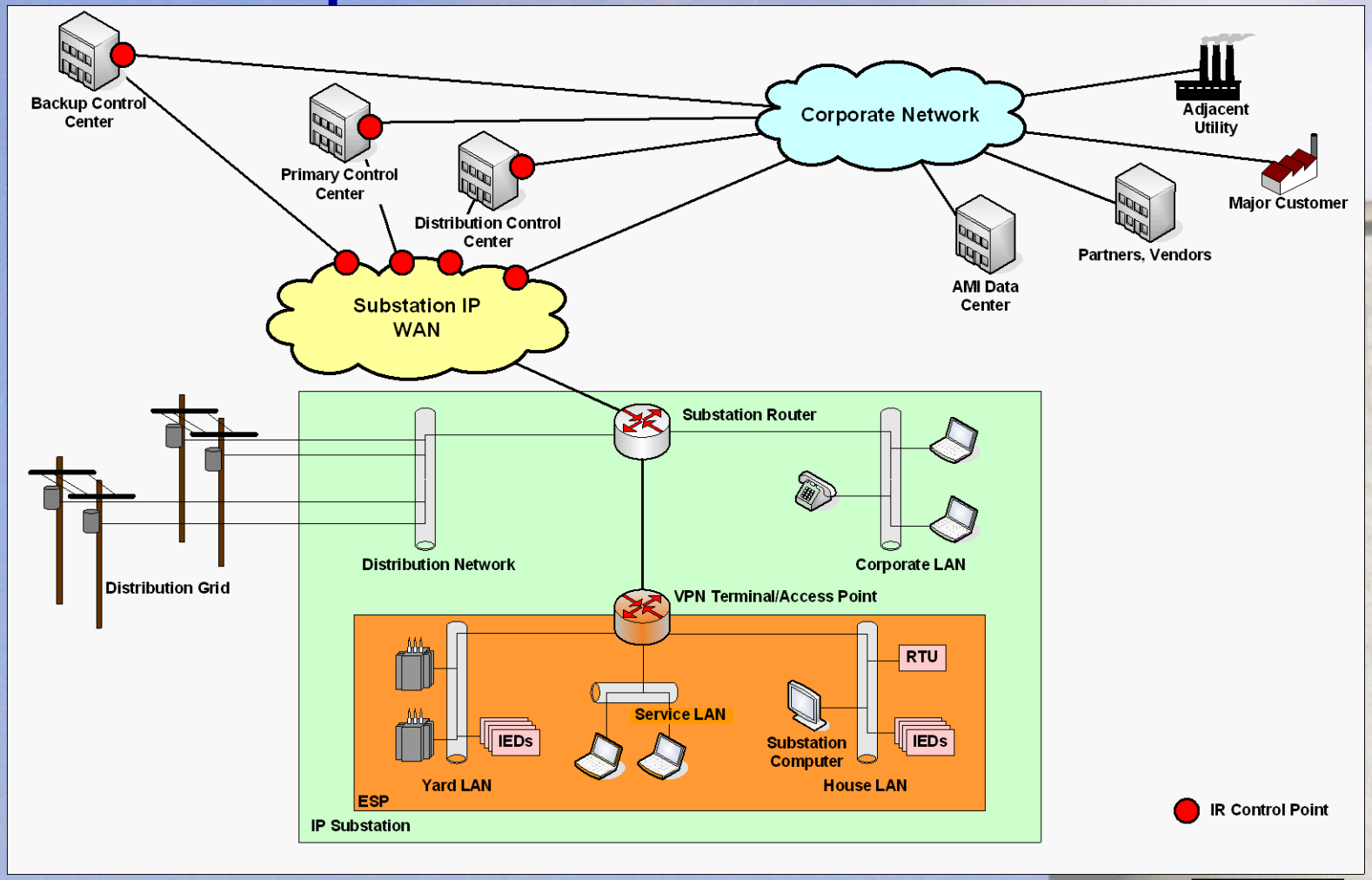


Network & Security Technologies

1. Restrict the Substation Network

- Identify all user communities.
- Limit dispatch access points.
- Profile traffic.
- Duplicate legacy serial strategy for WAN links:
  - Own the network (if possible).
  - Use VPN technology to enforce traffic separation.

An Architecture for a Secure Operations Network

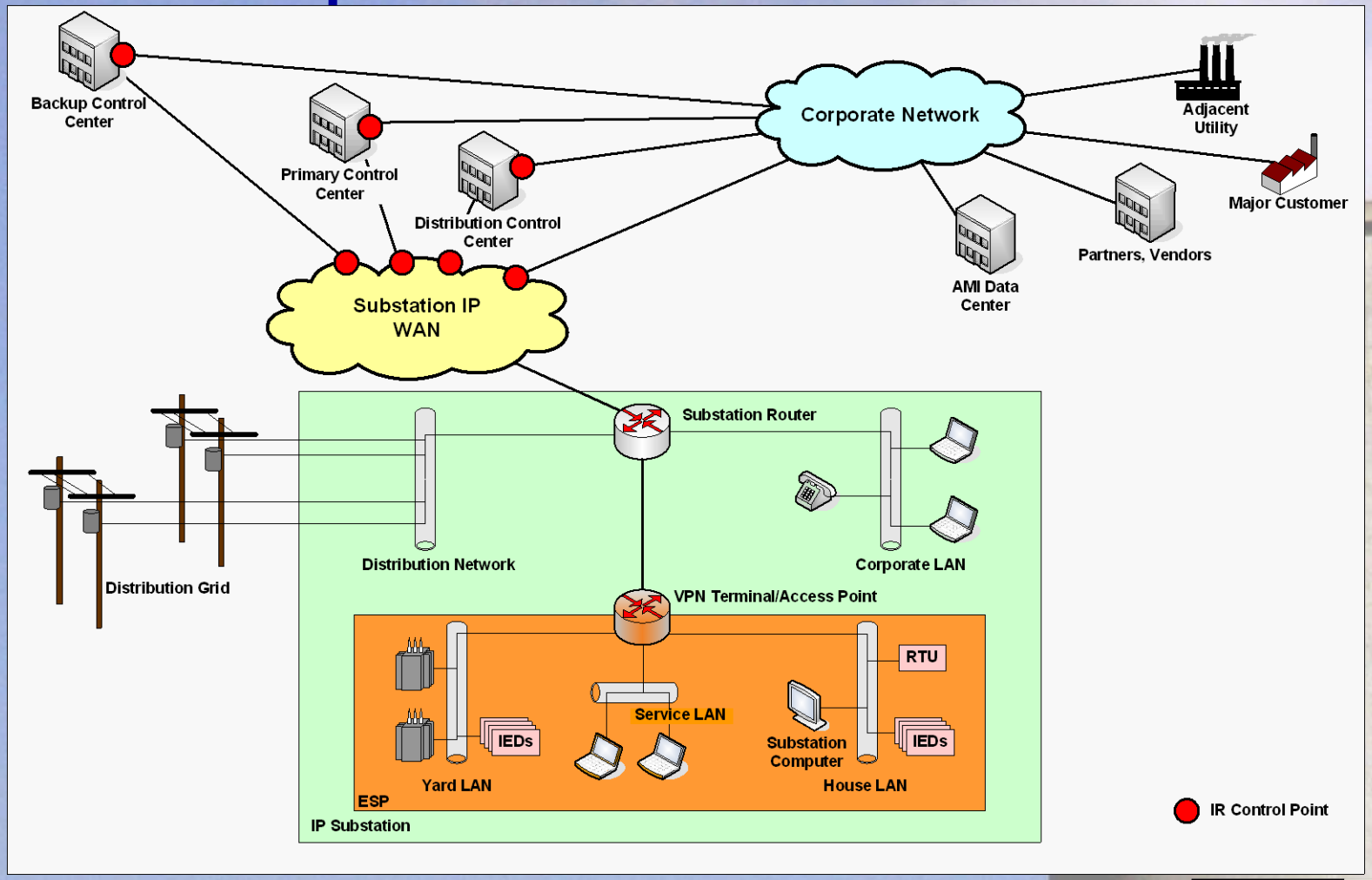


Network & Security Technologies

2. Segregate Traffic in the Substation

- Identify the Electronic Security Perimeter (ESP).
- Prioritize SCADA (i.e., ESP) traffic.
- Standardize equipment configuration.
- Provision access for personnel in attendance.
- Control access and monitor from central management system.
- Include local fail-safe capability.

An Architecture for a Secure Operations Network

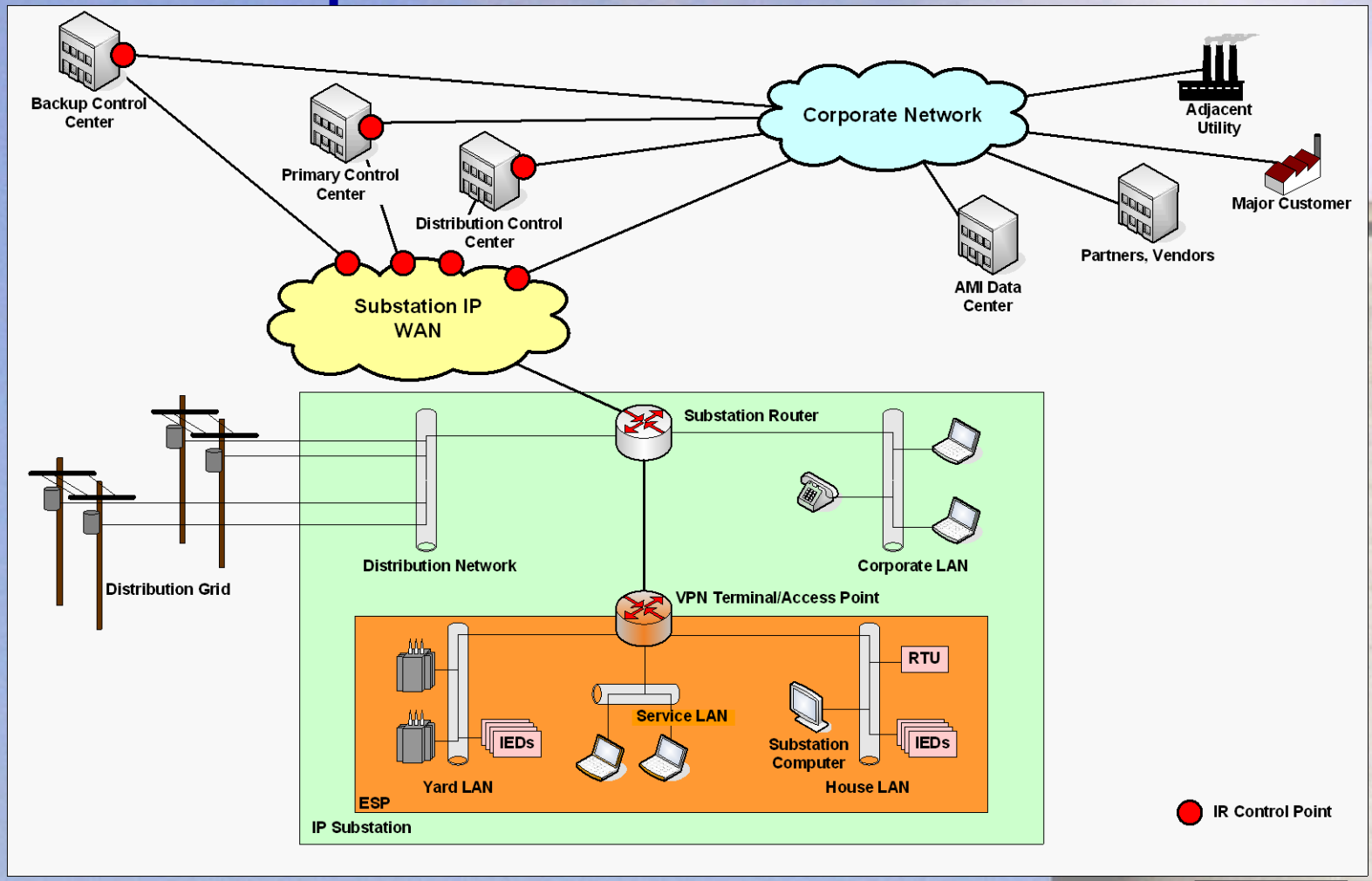


Network & Security Technologies

3. Define Conservative Incident Responses

- Define and maintain strict traffic policies.
- Enforce policy through Active Policy Enforcement (e.g., intrusion detection and prevention).
- Lock out non-essential activity upon detection of an anomaly:
  - Dispatch access points
  - Control center access points
  - Substation access point(s)

An Architecture for a Secure Operations Network



Network & Security Technologies

Summary

- Restrict the substation network.
- Segregate traffic in the substation.
- Define conservative incident responses.

Network &Security
TECHNOLOGIES

Best Practices in Grid Security

Jeff Kimmelman
Principal Consultant and CTO
Network & Security Technologies
jkimmelman@netsectech.com
978-897-0131