CONF42

Network Incidents:

What to Know Before the Chaos Strikes!

Maksim Kupriianov

What Is A Network Incident?

Unexpected event that disrupts or degrades critical network services, impacting their availability, integrity, or performance.

What Are The Critical Network Services?

- Infrastructure Services (DNS, DHCP, Routing, VPN, NTP/PTP);
- Security Services (Firewalls, IDS/IPS, Certificate centers, physical access control);
- Directory Services (User management, Authentication, Authorization);
- Cloud & container orchestration;
- Web Services (traffic load balancers, web servers, CDN).

Why Network Incidents Are So Disruptive?

- Cascading failures.
- Loss of monitoring and diagnostic tools.
- Downtime affects multiple stakeholders.
- Difficulty in Triage.
- Time-consuming troubleshooting.
- Increased security risks.
- Reduced business operations.

Examples Of Network Incidents

- Cloudflare Outage (July 2020) – **20 minutes**
- Google Cloud Outage (December 2020) – **50 minutes**
- Microsoft Azure and Teams Outage (March 2021) – **3 hours**
- Fastly CDN Outage (June 2021) – **1 hour**
- Facebook Outage (October 2021) – **6 hours**
- Amazon Web Services (AWS) Outage (December 2021) – **6 hours 30 mins**

In the IT world, network incidents are as certain as sunrise

The Anatomy of a Network Incident

The Initial Trigger

Every network incident begins with a trigger, which could be:

- Hardware failures
- Software issues
- Human error
- Security breaches
- External factors
- Market-related events

Immediate Effects

The immediate aftermath includes:

- Service outages
- Alert storms
- User complaints

Cascading Failures

Network incidents rarely remain isolated:

- Interdependent systems fail
- Traffic bottlenecks
- Resource exhaustion

Loss of Visibility and Control

Key challenges arise in managing the incident:

- Inaccessible monitoring tools
- Remote access issues
- Communication breakdown

Increased Security Risks

The incident may expose the network to additional threats:

- Firewall bypasses
- Exploitable weakness

Incident Response Challenges

Teams face multiple obstacles:

- Stress and pressure
- Prioritization dilemmas
- Communication with stakeholders

- Network incidents have multiple triggers
- Interconnectedness magnifies impact
- Loss of visibility complicates response

Preparation:
Fortify Before the Storm

Key Steps to Take Before an Incident Strikes

Implement redundant infrastructure and backups

- Network redundancy
- Out-of-band management network
- Data backups
- Failover systems

Key Steps to Take Before an Incident Strikes

Conduct regular system audits and health checks

- Network assessments
- Hardware maintenance
- Capacity planning

Subset of monitoring tools and dashboards must be accessible out-of-band!

Key Steps to Take Before an Incident Strikes

Develop comprehensive documentation and playbooks

- Network documentation
- Incident response playbooks
- Knowledge base

Keep a fresh copy outside of your network!

Test It: Fire Drills for Your Network

- Conduct regular drills and simulations
- Evaluate and update response plans
- Ensure team preparedness

- Preparation is an ongoing process
- Have a backup plan
- Fire regular drills
- Benefits outweigh costs

During the Incident: Staying Calm in the Chaos

Immediate Actions When Everything Goes Dark

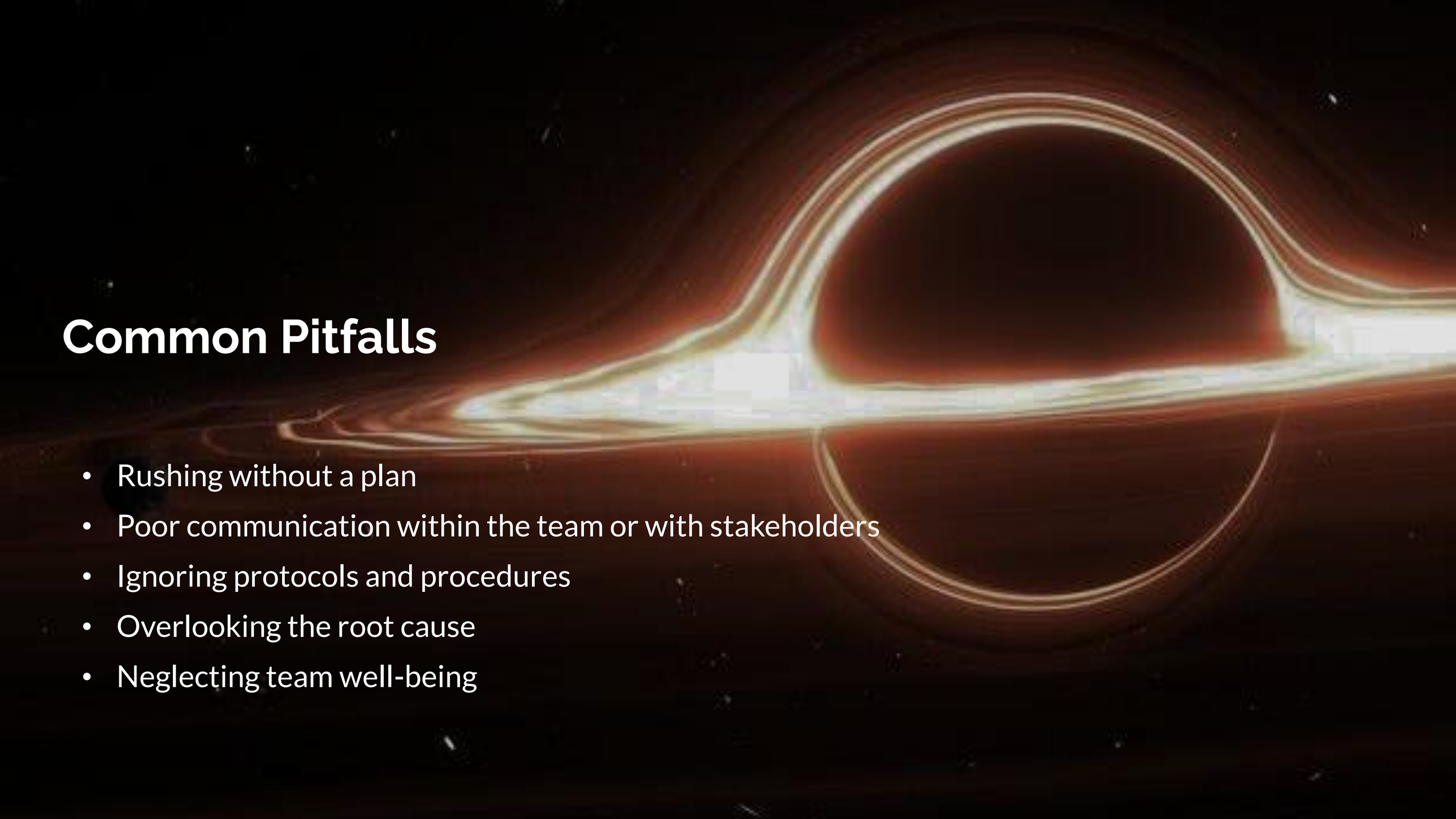
- STAY CALM
- Gather initial information
- Establish incident command
- Secure a communication channel
- Inform stakeholders

Prioritize: What to Fix First

- Identify critical services
- Determine the root cause
- Develop an action plan and follow it

Communicate: Keep Everyone Informed

- Establish a communication protocol with regular updates
- Inform affected parties
- Maintain open lines within the team
  - Share findings
  - Ask for help
  - Create an activity log
- Stay positive!



Common Pitfalls

- Rushing without a plan
- Poor communication within the team or with stakeholders
- Ignoring protocols and procedures
- Overlooking the root cause
- Neglecting team well-being

- Stay calm and positive
- Effective communication is critical
- Teamwork matters
- Prioritize actions
- Avoid the pitfalls

Post-Incident:
Learn and Improve

- Analyze what went wrong
- Create a feedback loop
- Building resilience

Thank You For Your Attention!

Any questions?