INCIDENT REPORT

INFORMATION TECHNOLOGY SERVICES

Incident Report – March 7, 2017

Incident #2017-190

Campus Wide Network Outage

Summary

On Tuesday March 7, at approximately 4:35pm, a campus-wide network outage was reported. By 5:00pm, the senior network team was called to diagnose and remediate the problem.

Analysis revealed that the problem was complex in nature and the outages were intermittent but widespread. At 6:12pm, it was deemed necessary to engage the vendor (Cisco). Accessing the required Cisco team was difficult, which slowed diagnosis of the issue.

Between 7:30 and 10:30pm, both teams identified a network loop as the cause of the outage. Removing all connected switches and systematically reconnecting the switches one at a time uncovered the source of the loop. Further log analysis of the core network equipment pointed to a specific Vlan as the source of the problem and the widespread network instability.

Impact

Campus wide network connectivity was either degraded or unavailable in some cases across campus for approximately 4 hours. Both services/applications and users being able to login were affected.

Root Cause

A network layer two spanning tree loop caused the problem. A rogue network device plugged incorrectly into the network caused the offending loop (a network cable plugged into a wall jack while the other end was inadvertently plugged into another wall jack). This “loop” caused all network core equipment to utilize 100% of its CPU, which then slowed the whole network down, making it unavailable.

Resolution

1. All network connections to buildings were disconnected.
2. Buildings were systematically reconnected to the network until the one causing the problem was located.

3. The entire network was then connected and the offending building was left disconnected. This allowed the rest of the network to stabilize.

Communications (Internal)

ITS monitoring flagged the issue and the ITS network team were then alerted. ITS engaged Cisco support services to help and then continued troubleshooting the issues until resolved.

ITSPP Communications (External)

A campus-wide notification was posted at 5:09pm including a message to the ITS Twitter account. The notification was posted to the ITS website and emailed to appropriate lists using the ITS Notification Tool. Updates were posted periodically as work continued. The final update was posted when the network was fully operational at 10:30pm.

Lessons Learned

1. No offsite access to key documentation
2. There is a need to improve remote access to network equipment.

Action Items

1. Store key documentation in off site location
2. Upgrade and maintain system used to remote access to network equipment.