Recommendations for Pueblo City County Library Network Optimization

Pueblo City County Library District (PCCLD) submitted a Request for Proposal (RFP) asking for Network Assessment and Analysis services. PCCLD specifically requested the following conditions be accommodated:

- Local Area Network Performance (wired and wireless)
- Wide Area Network Performance (all branch locations)
- Discovery & reports of any TCP/IP, DNS/DHCP, and other network protocols issues. The network assessment should analyze performance throughput, errors and retry rates. It can include monitoring tools to gather network performance data for the LAN and WAN. In addition, configuration and general network health data for all relevant network devices should be collected using the appropriate GUI and/or CLI tools.

  The techniques employed should include:

  - Physical-layer analysis: Perform an automated network discovery and develop and/or verify network map. Examine data captured by protocol analyzers and identify physical errors related to networking devices.
  - Network design and configuration analysis: Collect device configuration information. Compare design and configuration data against best practices.
  - Network utilization analysis: Examine network utilization for WAN and Internet access connections.
  - Security vulnerability analysis & recommendations: Basic security assessment and recommendations to include switch and interface security as well as VLAN security (e.g. public access versus staff access).

Flair Data Systems (Flair) won the award. Flair conducted a detailed analysis and assessment for PCCLD. Flair specifically makes the following recommendations for optimizing PPCLD's network:

Finding: PCCLD currently utilizes a mixture of WAN connections involving Layer 2 and Layer 3 connections. This has required extending IP addressing and routing across the WAN links, as well as allows for undesirable communications such as broadcasts to be present on the WAN links. This can contribute to sub-optimal performance as well as unnecessary processing of packets/information by the network infrastructure equipment.

Recommendation: Configure all WAN connections as Layer 3. This will require re-addressing all sites to a more streamlined IP schema as shown in the accompanying document "PCCLD Proposed VLAN-IPAddress-Subnetting Template.xlsx". This will allow for summarized routing between sites, thus reducing the size of routing tables and minimizing processing overhead on network infrastructure equipment. Also, by connecting each of the branches and IDF's to the core via port aggregation, PCCLD will enjoy higher throughputs as well as redundancy. This will also lend to splitting routing functionality into separate Virtual Routing and Forwarding (VRF) instances to segment the Staff network from the Public network. This requires some additional explanation:

- We'd have to rearchitect the WAN links. I verified with SECOM that the SONET ring services will support the re architecture on our side without ISP hardware replacement. There may be some config changes that need to be made on their part, there may not be.
- You'd have to make some changes to your AD structure, in affect building a "Staff" zone and a "Patrons" zone
- All traffic between zones (Staff <-> Patrons) would have to come back to the main site to traverse a centralized firewall policy (which we'd put in place on your ASAs). To that end, you'd want to think of how you are serving up various services (e.g. DNS, DHCP, File Services, Print Services) to see what would need to be changed/what you'd want to leave the same.

Finding: In many of the IDF closets, multiple switches are connected directly back to the core switch, or are daisy-chained together, or both. This is a sub-optimal design and can lead to management complexity as well as potential performance problems.

Recommendation: In all multi-switch closets, replace daisy-chained switches with stacked switches. In the case of the IDF's at Rawlings, these replacement switches would be the Cisco Catalyst WS-C2960X-48FPD-L switch(es). If you do not desire to have 10 Gbs uplinks, then we can utilize the Cisco Catalyst WS-C2960X-48FPS-L model.

In the case of the remote branches, in order to route effectively across the WAN, the new switches would be the Cisco Catalyst WS-C3650-48FD stackable switch(es), or the Cisco Catalyst WS-C3650-48FS model if you don't desire to have 10 Gbs uplinks. These would be connected back via Layer 3 port aggregation to provide higher throughputs and redundancy.

Finding: Current IP addressing does not scale well, nor does it lend itself to route summarization between branches.

Recommendation: Re-address all branches using a more streamlined IP schema as shown in the accompanying document "PCCLD Proposed VLAN-IPAddress-Subnetting Template.xlsx". This will allow for summarized routing between sites, thus reducing the size of routing tables and minimizing processing overhead on network infrastructure equipment. This will also allow VLAN representation by the 3rd octet and provide a simpler management paradigm throughout the network.

Finding: VLAN Trunking Protocol (VTP) configurations vary between sites. While VTP can be beneficial to reproduce VLANs across trunk links to multiple switches in the Layer 2 network, they also pose a risk if not properly configured and left unsecure.

Recommendation: With the implementation of stacked switches in the branch sites and the Rawlings IDF's, and the fact that VTP won't traverse Layer 3 connections, Flair recommends removing VTP from the branches completely. Since we're replacing daisy-chained switches with stacks, the stacked switches are essentially one large virtual/physical switch, thereby removing the need for VTP.

If VTP is necessary at Rawlings, then Flair recommends implementing VTP version 3 within those switch stacks and the Core. VTP version 3 offers advanced authentication and security options to prevent any inadvertent insertion of another switch which could reconfigure the VTP environment. VTP version 3 also allows for more VLANs to be synchronized should the need arise.

Finding: Public WiFi and Wired subnets are not currently prohibited from accessing other internal LAN resources/subnets.

Recommendation: Implement VLAN ACLs per branch specifying specific connectivity for Public segments, preventing them from accessing internal LAN resources but still allowing for Internet access. If certain resources are required for specific activities on the Public segments, those can be allowed via the VLAN ACLs specifically.

Finding: PCCLD is still using the IPSEC client for remote VPN connectivity.

Recommendation: Upgrade the VPN connectivity solution to AnyConnect/SSL. Cisco has declared End-of-Sale/End-of-Life for their IPSEC client and has discontinued any

development for same. Moving to the AnyConnect solution allows for connectivity with less overhead and the ability to keep current with the solution over time.

Finding: None of PCCLD's network infrastructure gear is covered under Cisco SMARTNet. SMARTNet is Cisco's support policy that allows access to the Technical Assistance Center (TAC), software upgrades, and defective device exchanges beyond hardware warranties. Please refer to accompanying file "PCCLD Network Equipment Support Eligibility Matrix.pdf" for details on specific equipment.

Recommendation: Ideally, all network infrastructure devices should be covered under SMARTNet. If something were to happen to a device PCCLD could enlist troubleshooting support from TAC, upgrade device firmware if necessary, or even get advanced product replacement when needed. At a minimum the core devices in each branch should be covered under SMARTNet.

Finding: Firewall configuration(s) need some attention

Recommendation:

1. Remove old boot system command.
2. Audit Objects/Object groups and remove what's not in use.
3. Audit ACLs and remove whatever isn't in use.
4. Update to latest stable version of ASA and ASDM code
5. Clean up EIGRP config (Remove auto-summary, only network 10.10.90.0/24 and 10.254.254.0/24 should be needed. Make passive interface if no neighbor exists off of DMZ Net.
6. Run SSL test on the URL you are using for VPN and make sure strict encryption mechanisms are employed
7. Clean up any old files in flash
8. Rearchitect internet link. Right now, if your primary internet link goes down, connections initiated from the internet to internal servers will fail because those connections are initiated to the 208.123.148.64/26 space - which would be dead. You have outbound redundancy but not inbound redundancy. To provision for inbound redundancy, you'll need a /24 from your ISP, along with rights to advertise it tied to your own ASN (which you'd need to acquire from ARIN). There are some alternative options, but none of them are as effective as injecting a /24 directly into BGP. *This would require additional hardware. We may be able to repurpose existing hardware but would need to discuss the considerations in person as they are relatively extensive.

Finding: Switch configurations could be better standardized with best practice configurations.

Recommendation: Implement Flair's best practice configurations on all switches. We can provide this information and work with you when you’re ready to move forward with this step.