

APPLICATION NETWORK ARCHITECTURE

Even the best applications in the world will suffer if they're built on a sub-optimal network architecture.

The key is to understand an application's characteristics and then design the network around it. From databases and servers to network appliances and routing, every component impacts the performance and stability of an application. Distributed applications (e.g., mobile, web) perform best when they take advantage of geographic awareness through AnyCast and GSLB. The removal of single points of failure on the network provides better disaster recovery and reduces downtime for the end-user; redundant servers in a load-balanced configuration provides fault tolerance during a hardware failure.

Relevant Technologies and Vendors

- A10 Networks AX Series
- F5 BIG-IP
- Spirent
- ApacheBench
- Extrahop
- Gigimon
- ApacheBench

Reference Case

Architected a solution for NewAOL (AOL's download complex) to utilize 6 geographically distributed locations. Tuned servers to accelerate download speeds for HTTP and FTP protocols. Worked with Sun Microsystems to make modifications to their FTP software to handle more concurrent users (16k/server) and add specialized functionality.

APPLICATION SECURITY

For some, application security is an after-thought ... often after they've already experienced a security incident.

Applications must be designed with security in mind, which includes the network it runs over and the servers it runs on. From a systems operations perspective, this means updating operating systems and services with the latest security patches; designing and implementing host-based access controls; and configuring hosts and services to restrict unnecessary functions. From a network operations perspective, this means detecting hostile traffic (e.g., probes and bot-net activity) and then mitigating its impact.

Relevant Technologies and Vendors

- Wireshark
- Intrusion Detection System
- Gigimon
- Nessus
- Load Balancer TCL Scripting
- Firewalls and ACLs

Reference Case

A large multi-service organization suffered a 4-hour distributed denial of service attack (DDOS) against their caching DNS. To secure the application afterwards, a rate limiting feature was designed and implemented by A10 Networks. Fourteen AX Series load balancers with this feature enabled were then installed in the DNS complex.

WEB APPLICATION OPTIMIZATION

Nothing is more frustrating to a user than a slow web site for a product or service they really want. Speed, reliability, and stability are hallmarks of a superior web system.

Optimization opportunities are present in every web system, and tuning activities that require little or no financial investment bring the greatest ROI. The process is straight forward: document the web system; perform an analysis of the servers, network, and application; and evaluate these findings against standards and best practices. Network protocol analysis provides detailed information about the application and its traffic, highlighting issues and risks. Low-effort solutions include web server performance tuning, server-side caching, and the addition of expiration headers. Sample complex solutions include the tuning of Application Delivery Controllers (ADC), enabling advanced features such as gzip compression and HTTP header/response control, implementing DNS based GSLB, and introducing web acceleration appliances.

Relevant Technologies and Vendors

- HTTPWatch
- tcpdump
- Wireshark
- Extrahop
- Gigimon
- A10 Networks AX Series
- F5 BIG-IP
- F5 Web Accelerator
- Content Delivery Networks
- Apache
- Squid

Reference Case

Evaluated Time Warner Cable's Residential Customer Portal (rr.com) for performance optimization opportunities. Formulated recommendations and reviewed it with the responsible web development team. Engineered new load balancer configuration to increase speeds. Web site response times decreased from 14 seconds to 8 seconds.

NETWORK PROTOCOL ANALYSIS

Protocol analysis is more than just a rule set and some tools; it's a philosophy that you apply to any client-server application. Packets have characteristics, behaviors, and data, and protocol analysis can be used to find performance degradations, determine security issues, and provide information for capacity planning exercises. As a foundation of technology architecture, protocol analysis allows architects to have a real view into how applications work and how to optimize them to work better. Since network and systems information is encoded within packets, even a single packet can provide insight into a situation. Details in a malformed packet help architects identify the part of the packet flow that introduced the error, an essential process of network, systems, and application troubleshooting.

Relevant Technologies and Vendors

- Wireshark
- tcpdump
- tcptrace
- HTTPWatch
- Niksun NetVCR
- Extrahop
- Coradiant
- Gigimon

Reference Case

AOL's internal monitoring tool determined that a percentage of AIM.com web requests were not being served by the application. Performed forensics analysis by utilizing a Niksun NetVCR for packet capture. Determined that the Foundry layer-4 switch was not properly tracking user sessions. Worked with the vendor to perform root cause analysis and then validated 9 revisions of the switch code in production until the issue was resolved.

SYSTEMS ARCHITECTURE

Systems architecture is about building the house in which an application will live. The process involves turning business requirements into a set of functional requirements from which engineers and administrators will implement a production system. An architect works with the product manager or business stakeholder to understand the scope of the application and the objectives that have to be met. A system is then designed that will meet those goals, keeping in mind the challenges and limitations of scalability, reliability, security, performance, and cost. Ease of maintenance is essential, as is the total cost of ownership. Architects are also exploring innovation opportunities within systems design by utilizing or combining the same set of technologies in new ways.

Relevant Technologies and Vendors

- UNIX (Solaris 6 - 10, HP-UX), Linux (Red Hat Enterprise, CentOS, Fedora, Slackware, Debian), BSD
- Host-based Services (Web, DNS, Mail, Syslog, Caching)
- Host and Service-Based Security
- Storage Area Networks
- Backup Systems
- Monitoring Solutions
- Custom-built Intrusion Detection Systems

Reference Case

Upgraded AOL's internal NFS complex by designing a new architecture to match updated business requirements. The new system was 5x larger and 2x faster than the previous version.

TRAINING

Training is the primary method by which technical architects convey their expertise to engineers and administrators. The key reason to train technical staff is so that they are more knowledgeable and better prepared to meet the challenges that they have to deal with on a day to day basis. Training is applicable in any stage of an application's life cycle, whether it be to understand a new application design or to understand how to use an application analysis appliance to solve a security issue. While superior training requires an instructor who has extensive knowledge of and experience with the subject matter, equally important is the ability to effectively convey that knowledge to students so that they understand the concepts as well as their practical applications.

Relevant Technologies and Vendors

- Network Protocol Analysis
- Network Troubleshooting
- Load Balancers (A10 Networks, F5)
- Gigimon
- Application Analysis Appliances (Extrahop, Coradiant)
- Protocol Analysis Appliance (Niksun NetVCR)
- Web Performance Tuning
- Linux Administration

Reference Case

Was invited to teach a class to the Mail Anti-Abuse Working Group (MAAWG) at their Fall 2009 meeting. The requested topic was basic protocol analysis. Objectives included the acquisition of packet captures, basic Wireshark and tcpdump filtering, and isolating elements within packet traces.

DESIGNING AND IMPLEMENTING TECHNOLOGY ARCHITECTURE SOLUTION SETS BASED ON STANDARDS, BEST PRACTICES, AND REAL WORLD EXPERIENCE.