

**State Data Center
Secure Network Shared Services
Architecture Project**

Technical Forum Notes and Handouts

8/28/07

Table of Contents

1.	MESSAGE FROM ARCHITECTURE TEAM.....	3
2.	TECHNICAL FORUM NOTES/Q&A.....	4
3.	WHAT IS IT ARCHITECTURE? – PRESENTATION SLIDES	6
4.	SECURE NETWORK ARCHITECTURE TECHNICAL FORUM – PRESENTATION SLIDES	9
5.	NETWORK DIAGRAM HANDOUT	15

1. Message from Architecture Team

The SDC architecture team wants to thank all the customers who came to the Secure Network Shared Service Architecture Technical Forum on August 28, 2007. We appreciate the candid feedback and remain committed to sharing information about architecture strategy and direction as early as possible with our customers. We ask that customers be patient with our ability to answer detailed questions about how we will deploy specific technology in each agency.

As mentioned at the forum, the SDC intends to introduce architecture concepts by each domain area (server, network, storage, etc). Agency specific technical implementation planning sessions will follow these general introduction sessions as the state rolls out projects for each technology architecture deployment.

You should feel free to contact any member of the architecture team if you have questions about the materials contained in this packet.

Sarah Miller:	Business Architect	503-373-0765
Kurtis Danka:	Technical Architect	503-373-2043
Claudia Light:	Project Manager	503-373-2091

We look forward to continued partnership as we work together to build the future.

2. Technical Forum Notes/Q&A

**Network Shared Services Architecture Overview
Technical Forum Notes
Tuesday, August 28, 2007 10:00AM – 12:00PM
DAS East, Mt Mazama Room**

Presenters:

Sarah Miller	Business Architect	503-393-0765
Kurtis Danka	Technical Architect	503-373-2043
Claudia Light	Project Manager	503-373-2091

Attendance: 38

Agencies Represented: DAS, DHS, DOR, OHCS, ODE, ODOT, OMD, OSL, Treasury, SDC

Agenda

Introductions/Overview – Sarah Miller

The forum is an attempt to provide a general overview of the consolidated architecture strategy in regards to network as well as security from a network perspective. A similar session has been held for distributed systems and will subsequently be held for security and storage that will break down individual strategic plans for each. Individual Agency planning meetings will also be held to discuss strategies and agency business requirements.

Architecture Project – Claudia Light

The current project is an 18 month – 2 year project that creates a “next-generation” architecture plan to standardized systems at the SDC. The goal is to create a repeatable process for system design.

What is IT Architecture.ppt

This presentation provides a broad picture of what IT architecture is in relation to the SDC Consolidation project. The presentation discusses architecture definitions, how SDC is approaching architecture planning in order to develop processes for standards through discovery and analysis. Deliverables from this process will include standard system descriptions, guidelines for the design of new processes and implementation road maps for each domain area.

Server Architecture Overview – Kurtis Danka

Secure Network Systems Technical Forum Architecture Presentation.ppt

This presentation provides an overview of the current State network and the planned State network. It also discusses key features and definitions of technologies required to implement a secure network including MPLS, IPSec and network intrusion detection.

Network Architecture Diagram.pdf – Frank Hoonhout

This document provides visual representation of the planned Enterprise Network design and how it securely connects to the SDC Network design through the use of standardized technologies.

Q&A

Q. What is the overall implementation strategy? Will the SDC use end-of-life maintenance as a guideline?

A. We currently have a CISCO assessment underway to learn about CISCO network equipment and configurations. Once that is complete, we will be able to upgrade current equipment to the same release. We have identified critical areas and several hundred end of life devices that need replacing. This will be at least a year long project. We will be working with agencies individually to make sure replacements or upgrades take place within network maintenance windows but we expect some exceptions pending evaluation of business requirements. We are also currently in negotiations with a provider to implement a gigabit backbone with redundancy statewide.

Q. The key features slide, shows consolidated internal and external DNS, please explain that in more detail.

A. Each agency has its own internal DNS servers and in some cases an external DNS server. We are currently looking at DNS appliances that agencies can log into and manage IP addressing and DNS zones. We will work with each agency for migration into the appropriate DNS servers.

Q. Have you planned a test of these appliances in a lab environment, focusing on disjoining DNS from Active Directory and then integrating with a DNS appliance?

A. Yes, after we have selected the vendor, we will run full tests before implementing them in the new environment. The ability to successfully integrate with Active Directory and other appliances is part of our product evaluation and selection process.

Q. DMV has many records and other data that has restricted access. According to the network diagram it looks as though other Agencies may have more exposure in the shared services environment, specifically RACF and Active Directory. How will the SDC minimize exposure?

Management of data will still be done at the agency level. In regards to data transmission over the network, we are leveraging a shared network system but using technologies to route traffic securely through the use of MPLS, VLANS, and other controls. MPLS enforces logical separation, and we will have the ability to encrypt over public networks where required. The shared services environment will maintain separation through the use of security controls, such as firewall service modules in each row. Standardizing the network and reducing complexity will allow more effective security measures to be utilized.

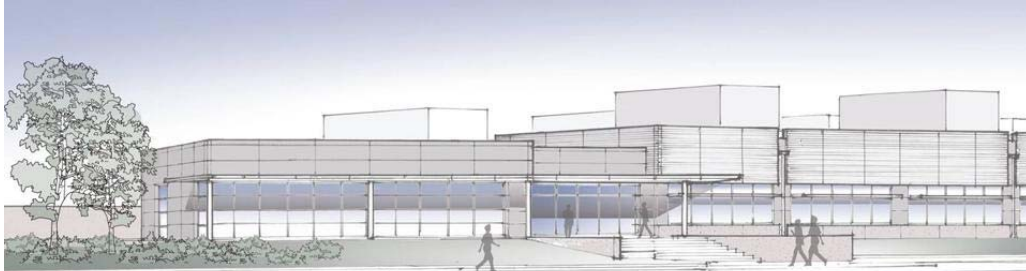
Q. From LaGrande, it currently takes 3 hops to reach the SDC. How many hops will it require through new plan?

A. The plan for LaGrande is to have a dedicated fiber connection and a managed network through the use of a network POP. LaGrande will connect to Portland directly. There is a separation of fiber which will create two different entry points. In most cases, the hop count will be reduced through the use of MPLS. All routers managed by SDC will be MPLS enabled. A feature of MPLS is that it does NOT show up in a customer' IP trace route, except for the ingress router and egress router of the MPLS network.

Q. What will the impact be on latency? Will you provide diagrams showing router locations?

A. We are currently evaluating a 3rd party tool to diagnose response times on applications. MPLS will not be visual on network diagrams. Due to security concerns, detailed network maps will generally not be available to customers. The proper troubleshooting steps if an agency should experience timing issues would be to contact the SDC.

3. What is IT Architecture? – Presentation Slides



State Data Center Consolidation Architecture Project What is IT Architecture?



August 28, 2007

What is IT Architecture?

- A Visio diagram
- A set of constraints
- A process for reviewing proposed projects
- A wager that there will be future benefit to following a direction
- Another word for design



Like the six blind men describing the elephant, each of these descriptions is partially true, but not the complete picture.

What Is IT Architecture?

- Architecture (in Greek αρχή = first and τέχνη = craftsmanship)
- Architecture is the translation of business strategy into technical strategy. unknown
- The organizational structure of a system or component, their relationships, and the principles and guidelines governing their design and evolution over time. (IEEE 610.12)
- In the computer industry, this nerd word is used to describe the overall design and style of a type of computer or of a network of computers, and the way in which its elements work together. Examples include Windows, Macintosh, Unix, or Internet designs.
www.techwriter.co.nz/nerd-ad.html

What We Mean by IT Architecture

“Architecture is essentially a planning discipline that offers sound guidance for the design of new processes or complex systems. Architecture follows a process of discovery and analysis to recommend changes in the form of a recommended ‘road map.’

This process results in two kinds of architecture deliverables: system descriptions and guidelines. The specific tangible products can be described in four outputs:

- The *current state* description
- The *future state* description
- *Principles*
- *Design guidelines* in the form of standards, reference models and patterns”

Source: *Creating a Business Architecture: Where Does it Lead You?* By Bill Rosser, Gartner, Inc., 11/30/06, ID number: G00144983

Why We Need Architecture

“In any architecture, structure and function come together to guide the engineering of a system (or building) that meets needs and serves a purpose. In IT enterprise architecture, that purpose is to provide supporting systems to further the goals of enterprise business strategy.”

Source: Key Components for Building Your Architecture by Jeff Comport, Gartner, Inc., 8/13/02, ID number: AV-17-4818

“All architecture is design but not all design is architecture. Architecture represents the significant design decisions that shape a system, where significant is measured by the cost of change.

Source: Grady Booch, <http://www.booch.com/architecture/blog.jsp?archive=2006-03.html>

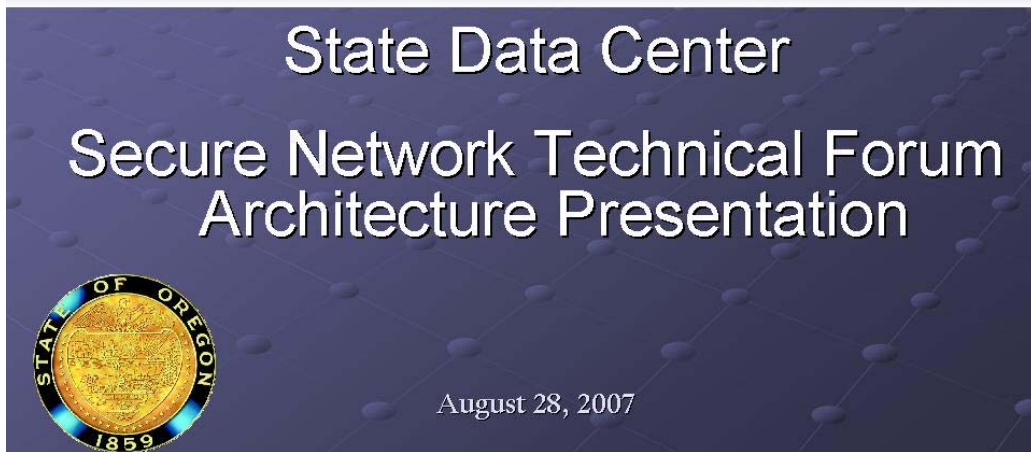
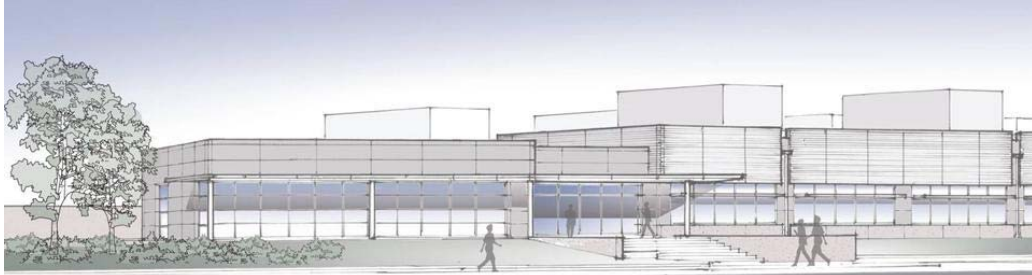


IT Architecture – the Big Rocks

“For years we have been using the ‘big rocks’ metaphor. If we place several big rocks in a large jar, then add pebbles, and last add sand, we fit them all into our jar. And yes, we could even add water. The point is not that we can always ask the developer to do more! The point is that if we start with the same sand, add the pebbles, and then try to add the big rocks, we cannot fit them all in the jar. To fit them all in, we must start with the big rocks. Architecture is about getting the big rocks in place first. But what are the ‘big rocks’? The architectural elements – the components and their relationships, yes. And architectural mechanisms addressing cross-cutting concerns or systemic properties, yes. Big rocks bear a high cost of change, yes.”

Source: Architect: What's in a Name? by Ruth Malan, April 2006
<http://www.bredemeyer.com/Architect/WhatsInAName.htm>

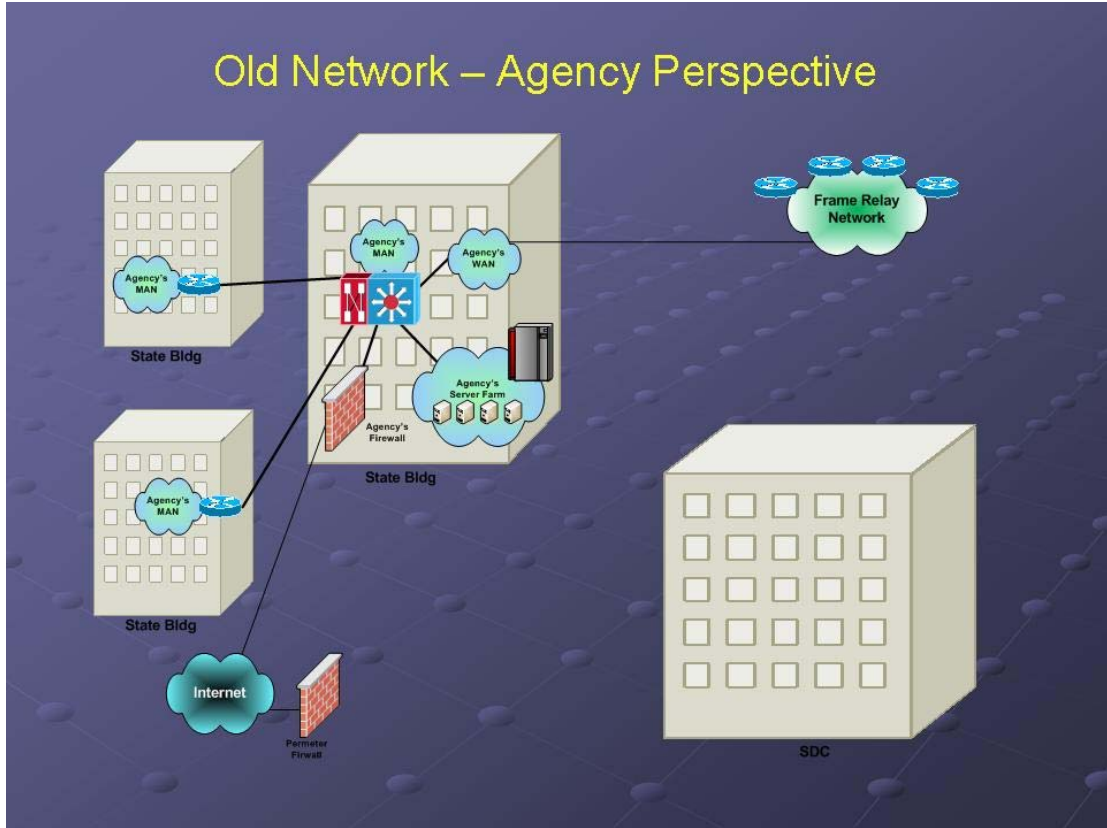
4. *Secure Network Architecture Technical Forum – Presentation Slides*



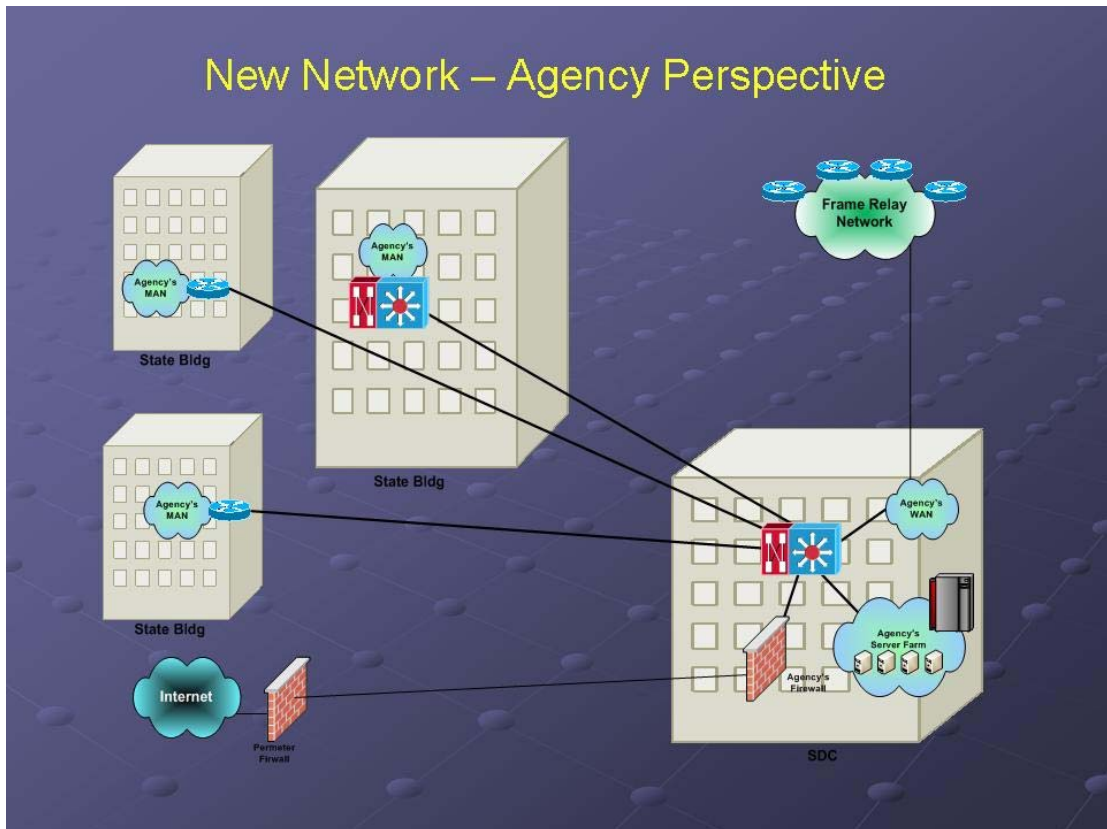
Secure Network Architecture Goals

- Optimal design
- Supportability
- Standards Based
- Simplified Security
- Integrated security and transport design
- One converged network
- High availability

Old Network – Agency Perspective



New Network – Agency Perspective



Technologies to Enable a Secure Network Solution

- MPLS
- IPSec
- Network Intrusion Detection

What is MPLS?

- MultiProtocol Label Switching.
- Allows flexibility to place any network in any security zone
- Ability to share a network segment without compromising security integrity.
- Provides Multi-Protocol Support
 - IPv4, IPv6

What is IPSec?

- Internet Protocol Security.
- Ability to have devices authenticate on a public network.
- Encryption on a public network

Key Features of the SDC Secure Network Architecture

- MPLS Technology
- IPSec
- Redundant State Core Network
- Includes a lifecycle replacement plan
- Flexibility to provide security in all zones
- Standardized Firewall Management
- Monitoring and Intrusion Detection
- Consolidated Internal/External DNS

Putting the Secure in Secure Network

- Security in all zones
- Simplified firewall management

Next Steps

- Salem MAN Ring Implementation
- Continue Implementation of MPLS
- Redundant Backbone Implementation
- Replacement of End of Life Devices
- Security Architecture Implementation
- Firewall Architecture Phased Migration
- Continued focus on IOS Standardization