WXXM Public Facing in a WXXM Private Environment

AIXM/WXXM Conference

Steve Olson
Meteorological Development Laboratory
Office of Science and Technology
NOAA's National Weather Service

August 30-31 and September 1, 2011

Table of Contents

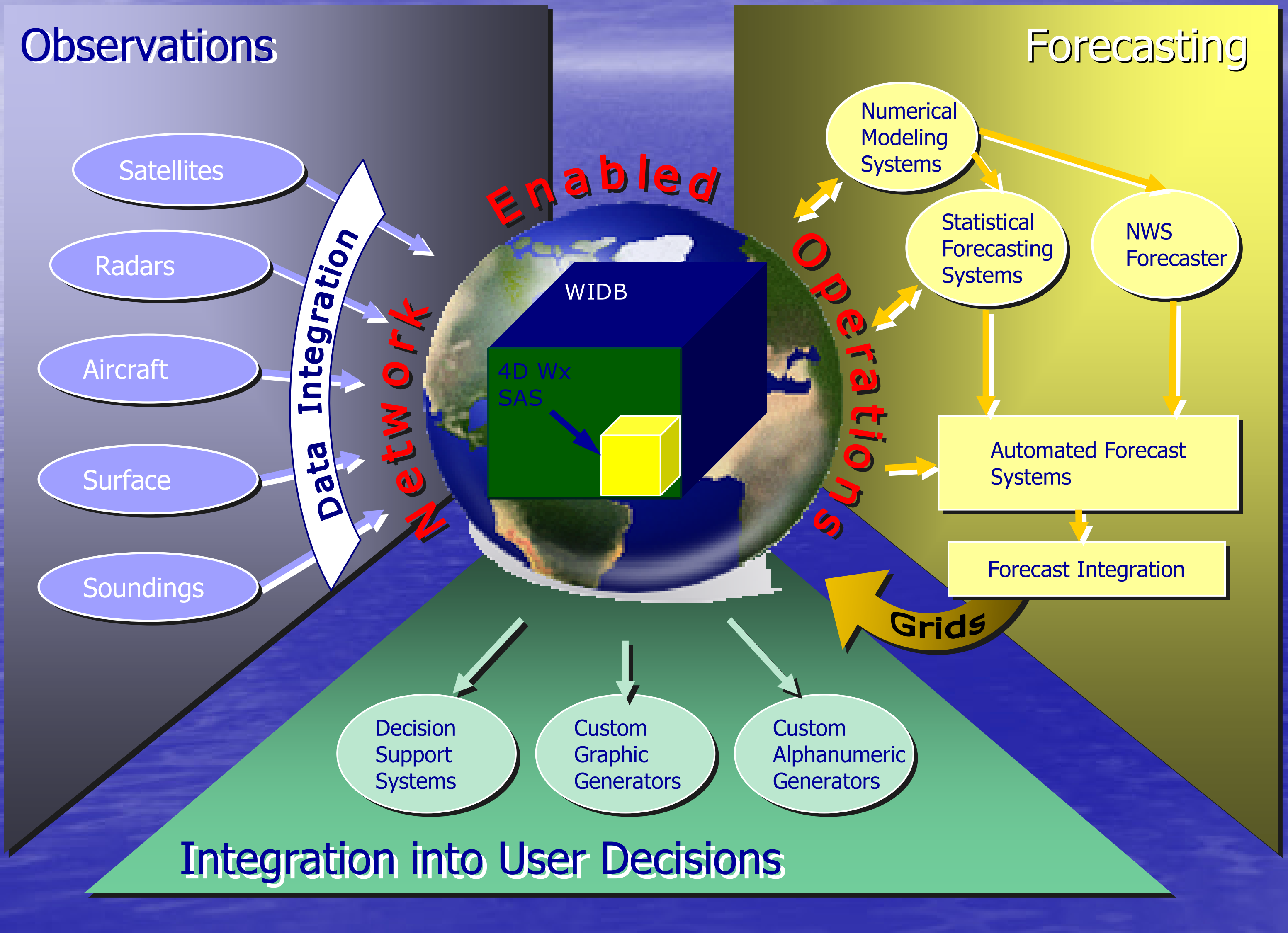
- Acknowledgements
- Conceptual Model of NextGen's 4-D Weather Cube
- Accessing the 4D Weather Cube
- Current MDL NextGen Web Services Setup
- MDL NextGen Infrastructure supporting FAA
- What changes are required for MDL/NWS to support a public facing side to Web Services?
- Adding Security as a service
- Public facing side to MDL's Web Services

Acknowledgements

The following individuals have contributed significantly to this work:

- Mark Oberfield
- Daniel Gilmore
- James Wantz
- Po Li

A Conceptual Model of the 4-D Weather Cube



Observations

Satellites

Radars

Aircraft

Surface

Soundings

Data Integration

Network Enabled Operations

WIDB

4D Wx SAS

Forecasting

Numerical Modeling Systems

Statistical Forecasting Systems

NWS Forecaster

Automated Forecast Systems

Forecast Integration

Grids

Decision Support Systems

Custom Graphic Generators

Custom Alphanumeric Generators

Integration into User Decisions

Accessing 4-D Weather Cube Data is a 2 step Process

1. "Data Discovery" → Registry/Repository (Reg/Rep)
2. "Retrieval" → Data Access Service (WCS/WFS/WMS)

NWS offers Reg/Rep, WCS and WFS Web Services

Current MDL NextGen Web Services Setup

- Registry/Repository (RegRep) Web Service
  - ebXML-based app built by Wellfleet Software
  - Uses ISO standards 19115 and 19139
  - License supporting clustered systems. Uses standard port defined by NextGen
  - Clustered VM systems (VMware ESXi)
    - Dedicated and separate Postgres & RegRep VM clusters
  - MDL has metadata for 28 NDFD and NDGD weather grids for our WCS, and a single metadata for our WFS guidance TAFs.

Current MDL NextGen Web Services Setup (Cont'd)

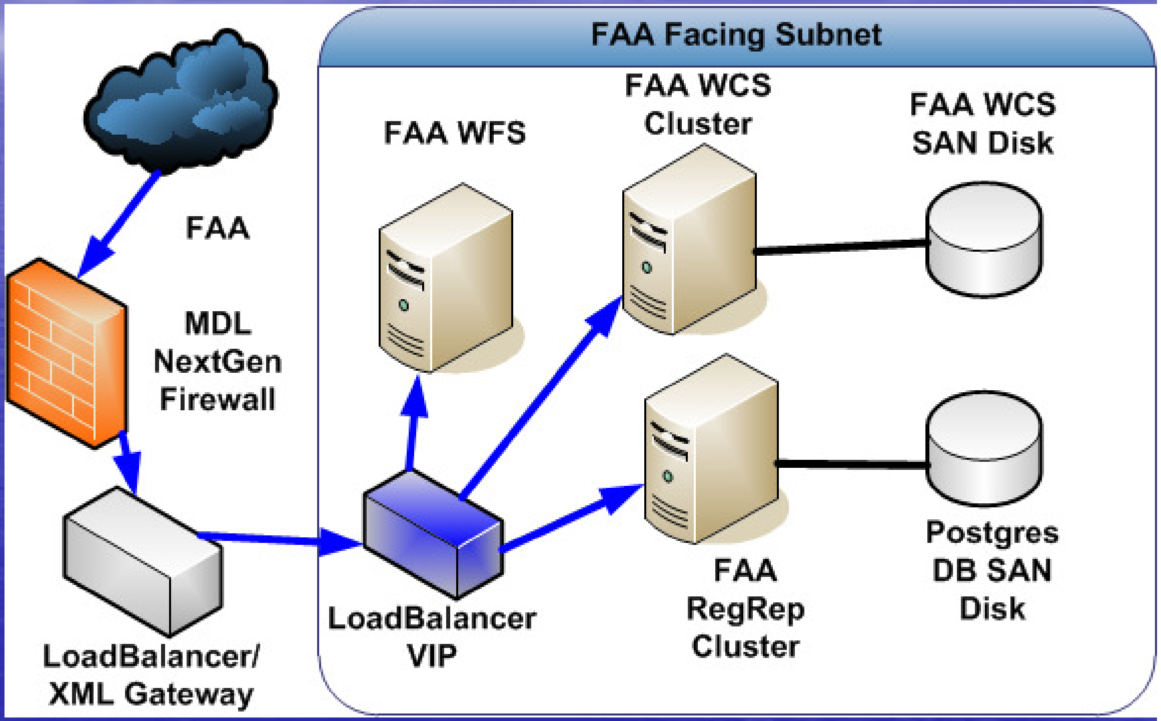
- Web Coverage Service Reference Implementation (WCSRI)
  - Java-based app built by NCAR featuring: Apache Fuse Servicemix, ActiveMQ (JMS), and database (postgres)
  - Supports SOAP/REST-based queries, http/https, pub/sub, KVP for getCapabilities
  - Clustered VM systems (VMware ESXi)
  - Load balancer in front of WCS services.

Current MDL NextGen Web Services Setup (Cont'd)

- Web Feature Service (WFS)
  - Java-based app built by LL/MIT featuring: Apache Tomcat, ActiveMQ (JMS), and database (derby)
  - Supports SOAP/REST-based queries, http/https, pub/sub, KVP for getCapabilities
  - Single VM system (VMware ESXi)

Current MDL NextGen Infrastructure supporting the FAA

- Have a dedicated subnet for NextGen specific activities separate from the rest of MDLNet infrastructure
- MDL NextGen infrastructure currently only supports connections to and from FAA, GSD and AWC.
- MDL NextGen communication specifics:
  - Use existing infrastructure to peer to NOAANet
  - Point to point connection from NOAANet to FAA Research Enclave covering 3 TCP port ranges
  - 3 TCP ports are forwarded to internal NAT load balancer service interface.
  - Firewall only allows specific IP addresses to traverse through our infrastructure
  - XML Gateway protects the application layer.



NWS vision: Make 4D Weather cube the new geospatial dissemination method

- It's the NWS goal to leverage the 4D weather cube concept (which has aviation focus) and apply it to ALL NWS products.
- Make this the new method for public dissemination of geospatial data!
- MDL is paving the early way to support the public facing side

How do we get there?

Public Facing Web Services Requirements

- Extend NextGen 4D wxcube rqmt (aviation focused) to broader spectrum of MDL weather products.
- Compartmentalize public facing system to allow for segmenting from FAA/OPSnet network developed for NextGen.
- Different IP address than the FAA to expose for the systems/services with separate routing and firewall rules
- Use the XML Gateway to set up a virtual WSDL. The Gateway would then be capable of distinguishing FAA traffic from general public traffic
- Public systems must be unable to access FAA
- Must be capable of supporting REST, SOAP and KVP-based queries

Adding Security as a Service

- A vendor device that provides a central point for security, which means you can offload your security requirements for the applications
- Can inspect and/or reject all requests and responses based on security criteria; such as virus scanning, known malicious content, sql injections, etc.
- Can provide load balancing, combine WDSLs, redirection/translation of requests, user authentication, encryption, document signing, document validation, etc.
- Add XACML access control policies (ACP) on RegRep systems
- Juniper SSG security device capable of packet inspection in place as firewall
- Fully FIPS 140.2 compliant

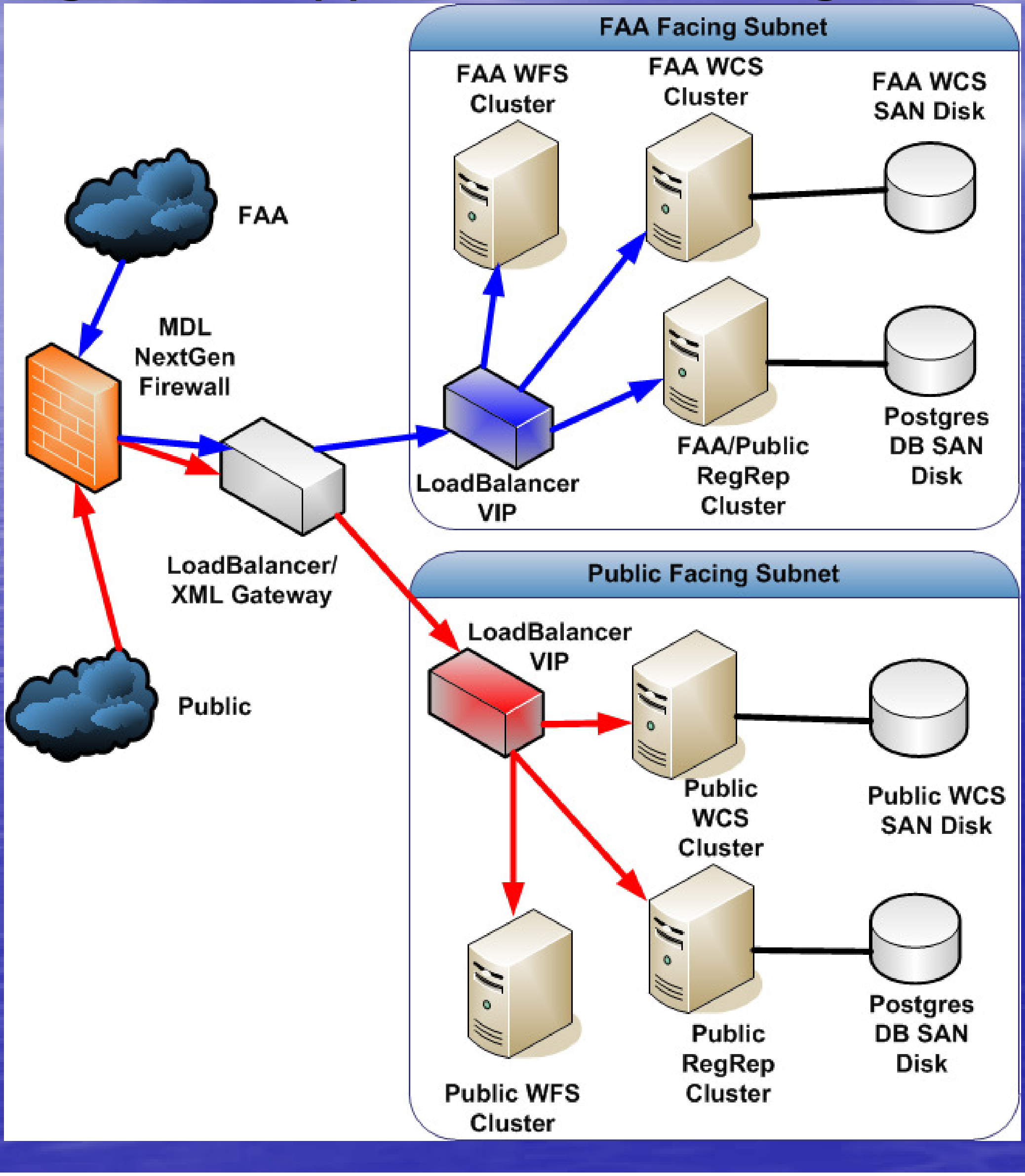
The Public-Facing side to MDL’s Web Services

- New WCS/WFS virtual systems would be created
  - – Have their own dedicated SAN
- New VLAN and subnet created
- New load balancer interface would be created on the new VLAN/subnet
  - – Existing RegRep servers and new WCS/WFS servers would be available via this interface

What the public will see

- Customers will connect to the DNS entry for mdl-nextgen.nws.noaa.gov which will point to the external IP
- The ports for the services will be the only exposure, which will actually be the load balancer

Proposed System Boundary Configuration Changes to support Public-Facing Web Services


FAA Facing Subnet
FAA WFS Cluster
FAA WCS Cluster
FAA WCS SAN Disk
FAA
MDL NextGen Firewall
LoadBalancer VIP
FAA/Public RegRep Cluster
Postgres DB SAN Disk
LoadBalancer/ XML Gateway
Public Facing Subnet
LoadBalancer VIP
Public
Public WCS Cluster
Public WCS SAN Disk
Postgres DB SAN Disk
Public RegRep Cluster
Public WFS Cluster