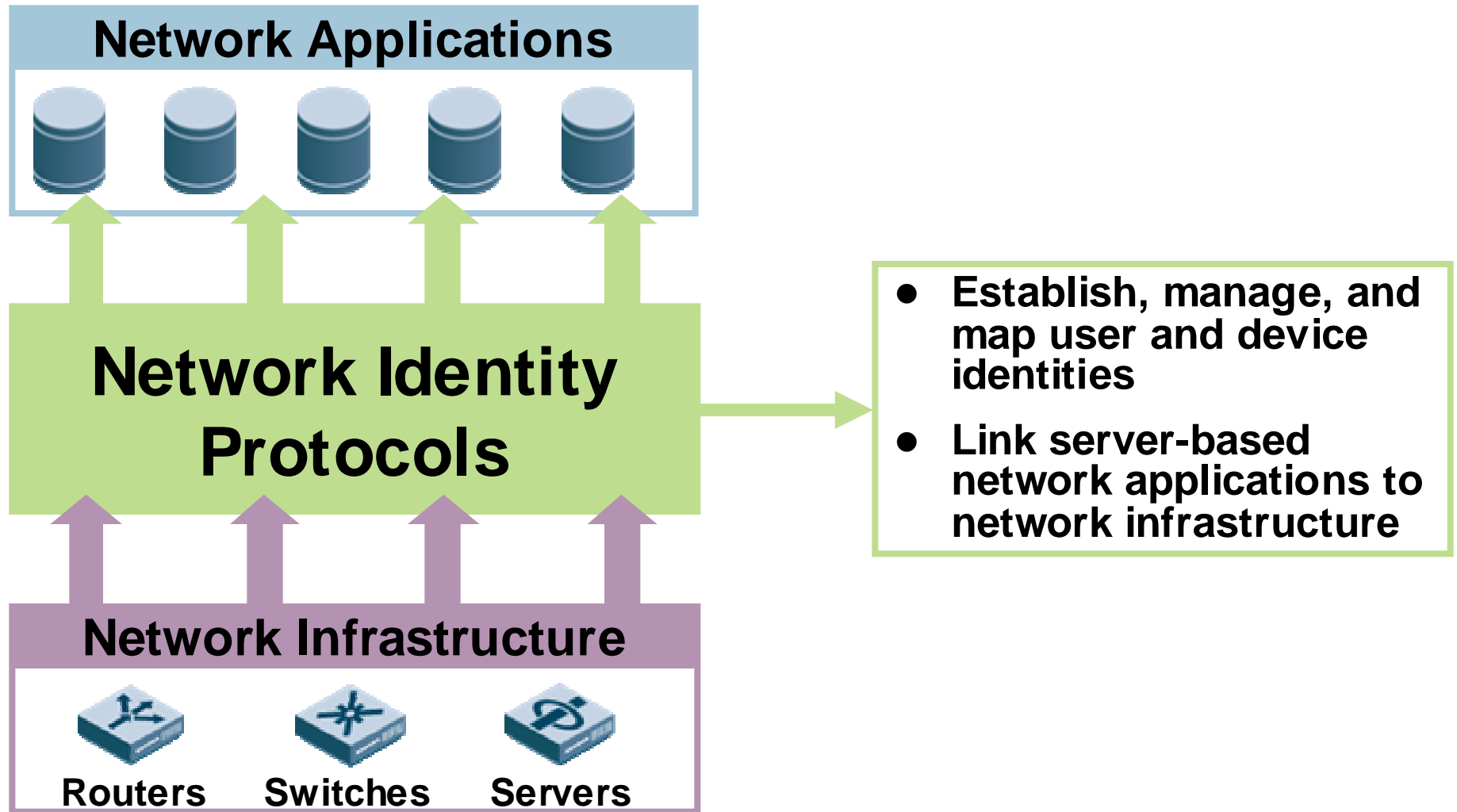




## **Network Identity: Unlocking the Value of Web Services**

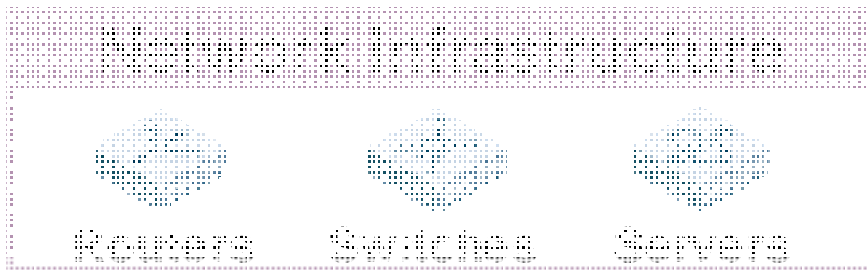
***Cricket Liu***

***Vice President of Architecture, Infoblox***





## Network Identity Protocols



### DNS

- Maps hostnames to IP addresses and vice versa
- Maps email destinations to mail servers
- Maps phone numbers to URIs (ENUM)

### DHCP

- Assigns IP addresses to MAC addresses
- Assigns configuration parameters to computers

### RADIUS

- Authenticates users
- Maintains user accounting

### LDAP

- Authenticates users
- Maintains directory information for users, computers, and software

## Network Applications



## Network Identity Protocols

## Network Infrastructure



Routers



Switches



Servers

Nearly all current networked applications rely on at least one of these protocols

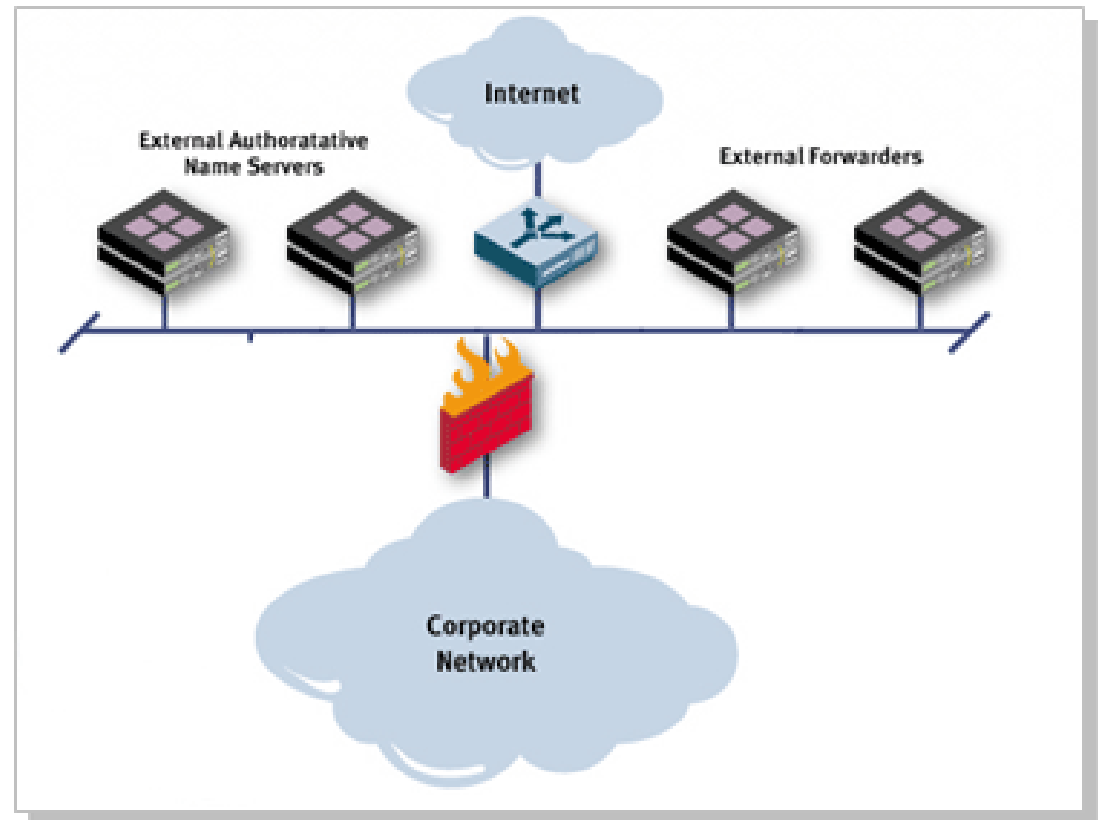
All future networked applications will rely on at least one of the protocols

Some of these networked applications are critical

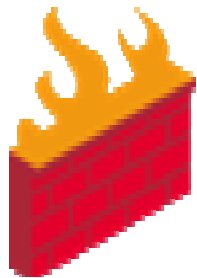
- VoIP relies on DHCP and will rely on DNS (with ENUM)
- VPN and dialup access typically rely on RADIUS or LDAP

**Just like other types of infrastructure...**

- Their reliability must be guaranteed
- Their security must be safeguarded
- They must be managed across the entire enterprise



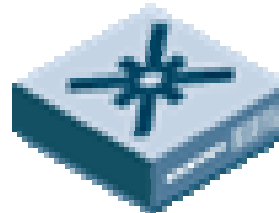
**We've been thinking about other TCP/IP services this way for years....**



**Firewalls**



**Routers**

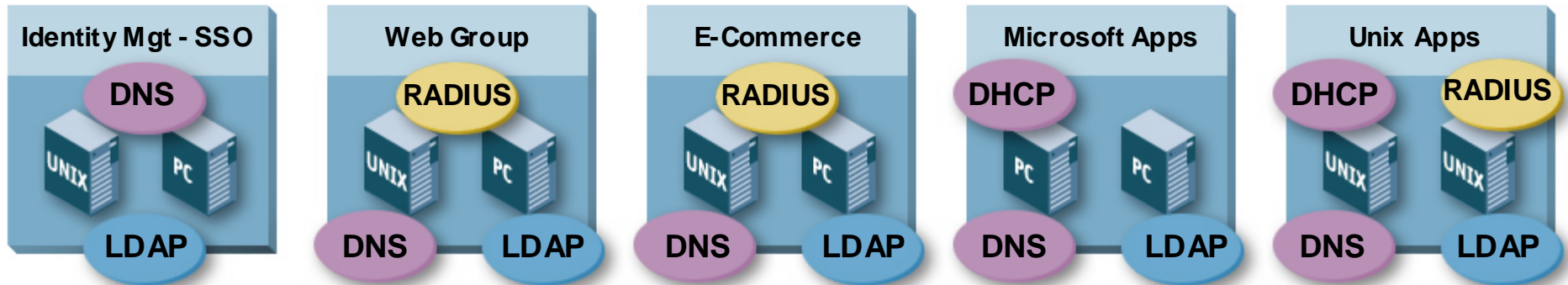


**Switches**

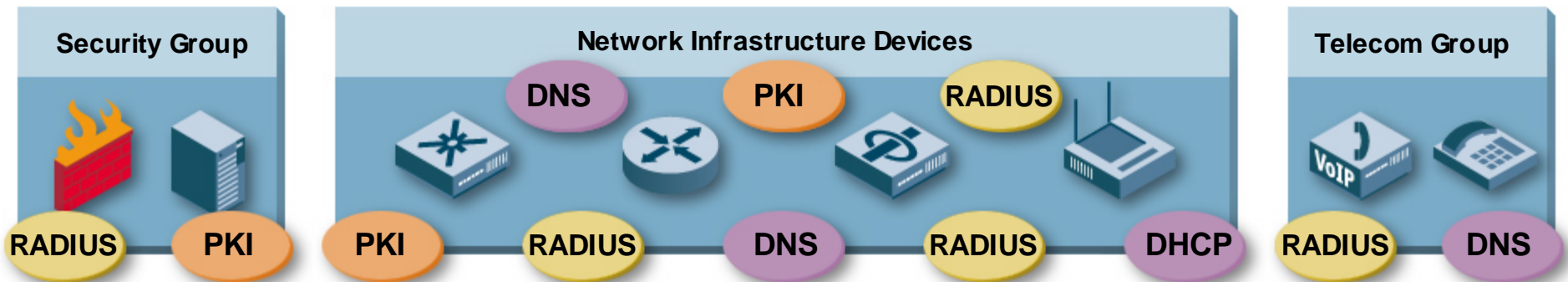


**Remote  
Access Servers**

# Problems with Network Identity Protocols: Balkanized Management



- ✗ Duplication of administrative effort
- ✗ Uneven administration across OS platforms
- ✗ Poor communication and coordination between groups of administrators
- ✗ Difficulty deploying tools across platforms
- ✗ Difficulty implementing certain designs or features
- ✗ Interoperability problems
- ✗ Lack of clear accountability
- ✗ Support issues





## Organizations often have no DNS architecture

- Just network diagrams showing where name servers are physically connected to the network
- Sometimes the diagrams will also show the operating system and software version each name server runs
- Less often there's a map showing which name servers are authoritative for which zones
- There's rarely a name resolution diagram
- and almost never all of the above
- Sometimes, the problem isn't that the architecture is undocumented... it's that it's unknown



- Frequently there's no monitoring of the service at all
- Some network monitoring platforms ping the hosts running name servers periodically
  - Some even send the name servers a simple query
- Few actually check that the name server is authoritative for the zones delegated to it

**Many organizations--to their credit--run DNS infrastructure based on the latest version of BIND**

**However..**

**Most of these organizations also have no commercial support for BIND**

## Network infrastructure protocols should be...

- Run on a common hardware and OS platform
- Run on a controlled set of software versions
- Monitored for responsiveness and correct configuration
- Commercially supported

A stable network requires...	Appliances offer...
A common hardware and OS platform	A common hardware platform
A controlled set of software versions	Simple upgrades to the OS platform and protocol engine
Monitoring for responsiveness and correct configuration	SNMP for monitoring and reporting
Commercial support	Vendor support

Appliances	Custom Solutions
Ease of use – simple installation and management	Maximum flexibility
Stable and secure services	A level of customization, integration, or control that is difficult to provide using appliances
Few infrastructure changes	Often requires infrastructure changes
Reduced requirement for substantial DNS expertise	Requires substantial DNS and product expertise
Cost-effective – one appliance vs. the cost of a server <i>and</i> software <i>and</i> the operating expense of implementation and ongoing maintenance	Can be expensive

**After you get back from N+1, examine your network and make sure:**

- You work to consolidate management of your network identity protocols, to a single organization with clear responsibility and accountability for the service
- You consolidate to a manageable number of platforms, including hardware, OS, and software.
- You produce a documented architecture for each of the network identity protocols you rely on
- You monitor each of these protocols
- You ensure that you have commercial support