Research on Infrastructure Systems and Services

Brent Hoon Kang,
Vikram Sharma,
Gautam Singaraju,
Pratik Thanki
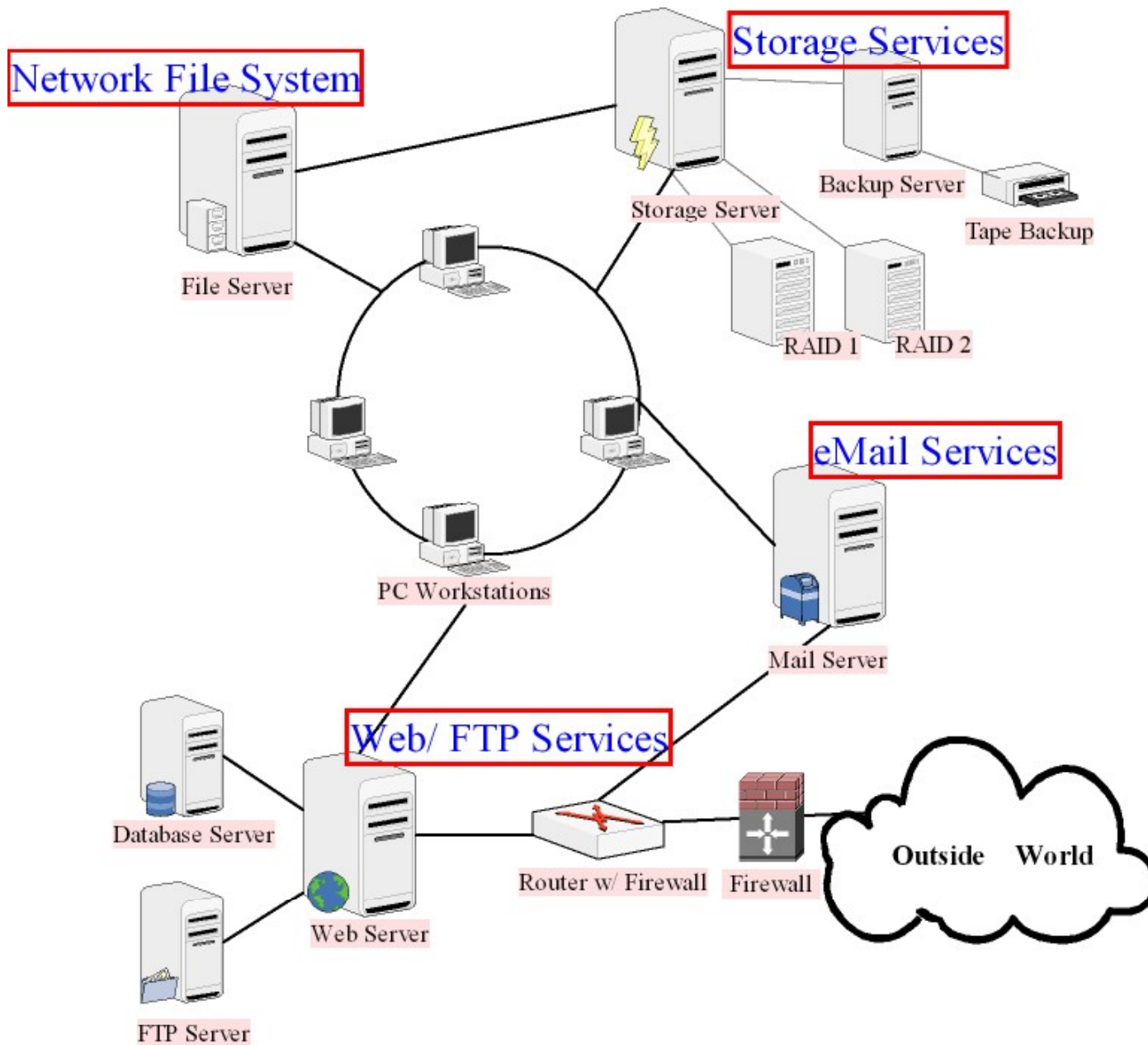
Research on Infrastructure System & Services

Agenda

- Discussion on IT Infrastructure – Systems, Services, their scope and complexity
- We'll talk about challenges in managing IT Infrastructure in a secured and reliable manner
- This talk will showcase the efforts and projects addressing the challenges in infrastructure systems design, implementation, and management.
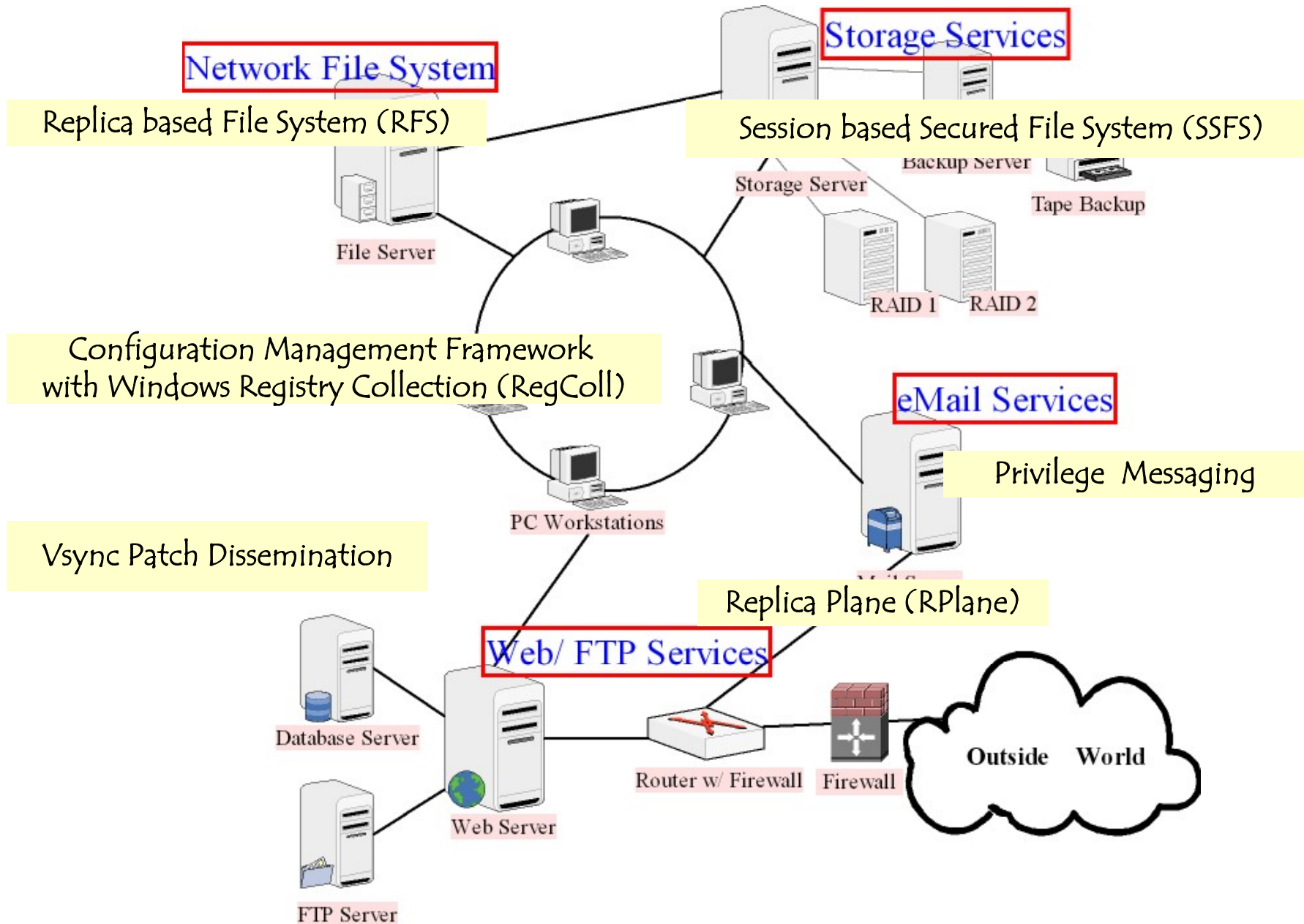
Components of an IT Infrastructure

- IT Infrastructure systems are vital to any organization, services like;
  - Network File Systems
  - Storage Architecture
  - Email Services, and
  - Web Servers

- Infrastructure System and Services Research (ISSR) Lab's current projects –
  - Replica based File System (RFS)
  - Session based Secured File System for Storage Networks (SSFS)
  - Privilege Messaging (P-Messaging)
  - Replica Plane (R-Plane)
  - Version based Patch Dissemination Protocol (Vsync)
  - Configuration Management Framework with Registry Collection (RegColl)

Typical Infrastructure Systems

New Infrastructure Systems Tools

Network File System

Storage Services

Replica based File System (RFS)

Session based Secured File System (SSFS)

Backup Server

Storage Server

Tape Backup

File Server

RAID 1   RAID 2

Configuration Management Framework
with Windows Registry Collection (RegColl)

eMail Services

Privilege Messaging

PC Workstations

Vsync Patch Dissemination

Replica Plane (RPlane)

Web/ FTP Services

Database Server

Router w/ Firewall   Firewall

Outside   World

Web Server

FTP Server

Replica base File Services (RFS) for Personal Computers
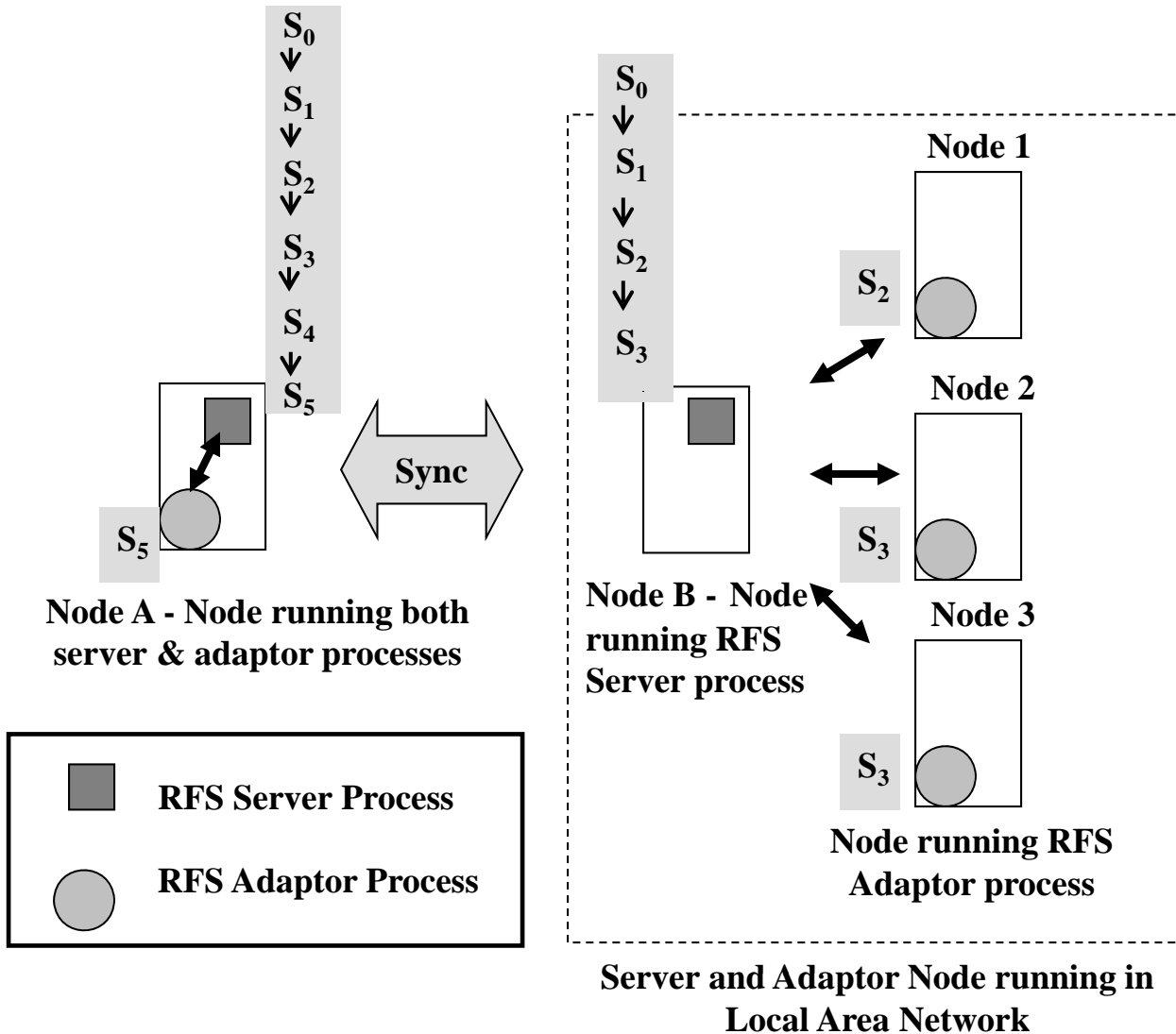
Infrastructure System and Services Research Lab

RFS: A Replica based File Services for Personal Computers

- Current Networked file systems
  - inaccessible during network disconnections.
- Modern personal computers
  - local disk storage in the order of 40 to 250GB.
- Is it possible to utilize local disks to enable users to access remote files regardless of network connectivity?
- Can the personal computer replicate a user's entire home directory stored on the network file server?
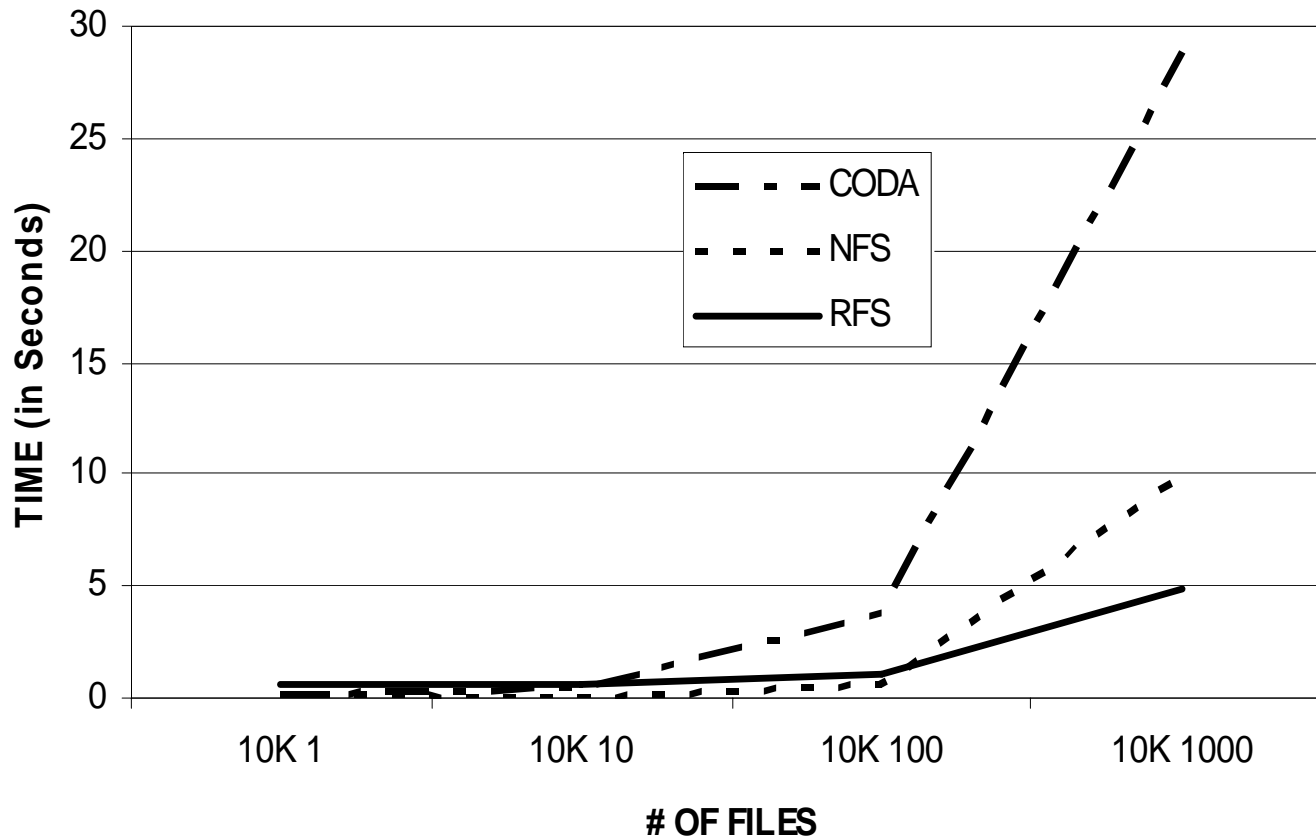- Can we undo or restore the file changes that were made onto remote file servers or local disks?

RFS Implementation

- Our local college's network file system usage
  - about 90% of the users had utilized up to 6.25GB
- RFS supports large local replica
  - Fast and incremental change set and synchronization.
  - Consistency and scalable log management in one data structure.
- RFS uploads files as fast as NFS and Coda,
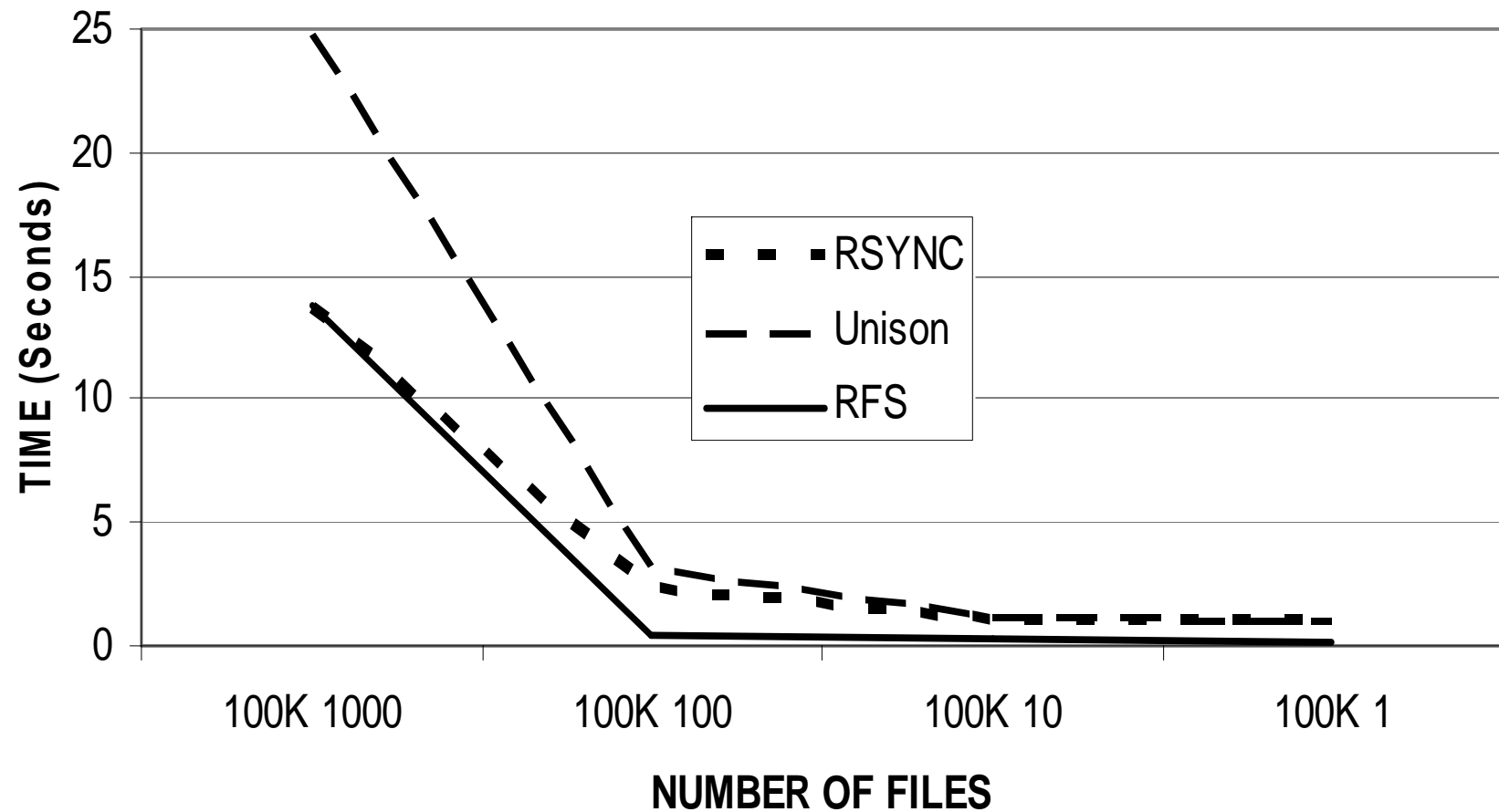- Synchronizes faster than Rsync and Unison.

RFS Architecture

S_0
↓
S_1
↓
S_2
↓
S_3
↓
S_4
↓
S_5

S_5

Node A - Node running both server & adaptor processes

Sync

S_0
↓
S_1
↓
S_2
↓
S_3

Node B - Node running RFS Server process

Node 1

S_2

Node 2

S_3

Node 3

S_3

Node running RFS Adaptor process

Server and Adaptor Node running in Local Area Network

■	**RFS Server Process**
●	**RFS Adaptor Process**

RFS vs. CODA vs. NFS

RFS vs. RSync vs. Unison

Vsync – Unidirectional Version Synchronization Protocol

Infrastructure System and Services Research Lab

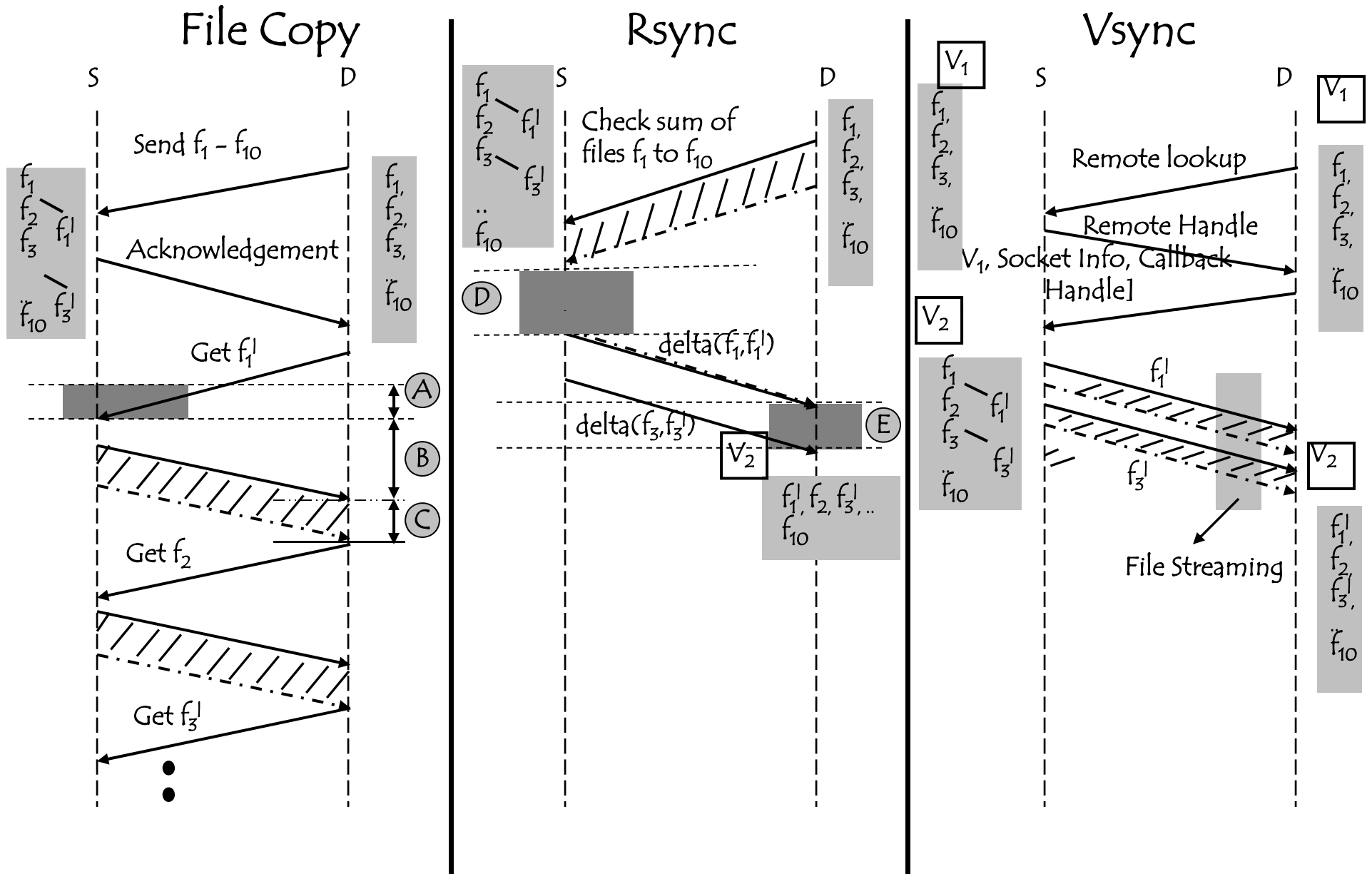# Version based Unidirectional Synchronization for Planet-Lab Nodes (Vsync)

- Motivation
  - Patch release
  - Virus definition update
  - Source tree change dissemination
  - Tool which is faster than Rsync
  - RFS is faster than NFS, CODA and Unison

- Issues
  - High latency of Wide Area Network
  - Substantial overhead of number of round trips of the protocol on these networks

- Changes made on RFS to make Vsync
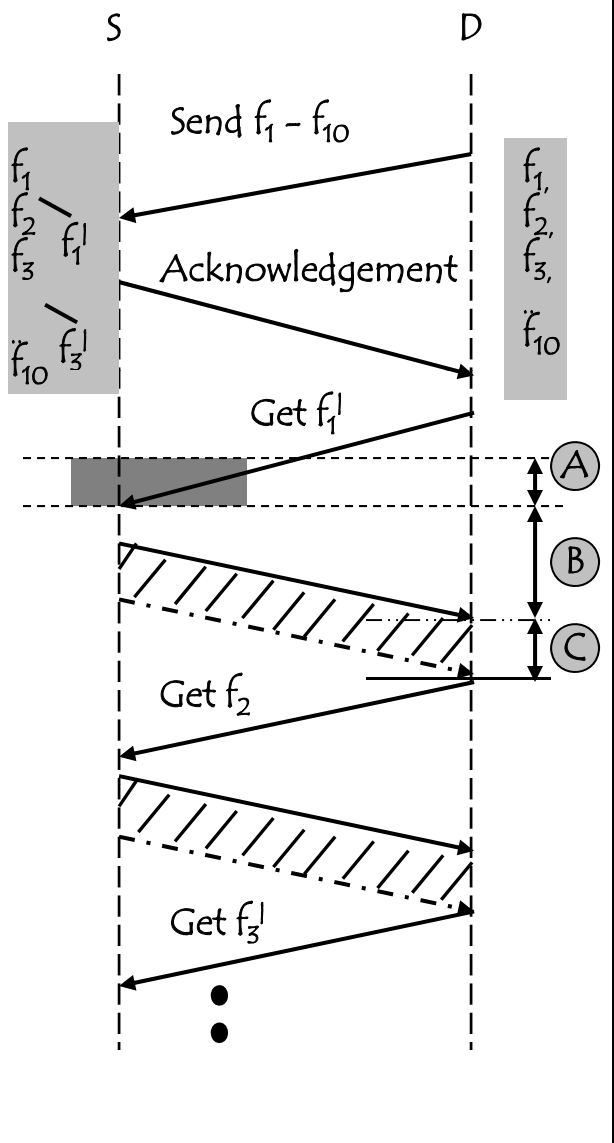 - Number of round-trips were reduced to 2 from 6.

Keys to Vsync protocol

- **One time Change Set generation** – Change Set is generated once (Vsync) against sending checksums all the time (Rsync).

- Combating latency by reducing the number of round trips

- Files are streamed to be synchronized in a threaded manner.

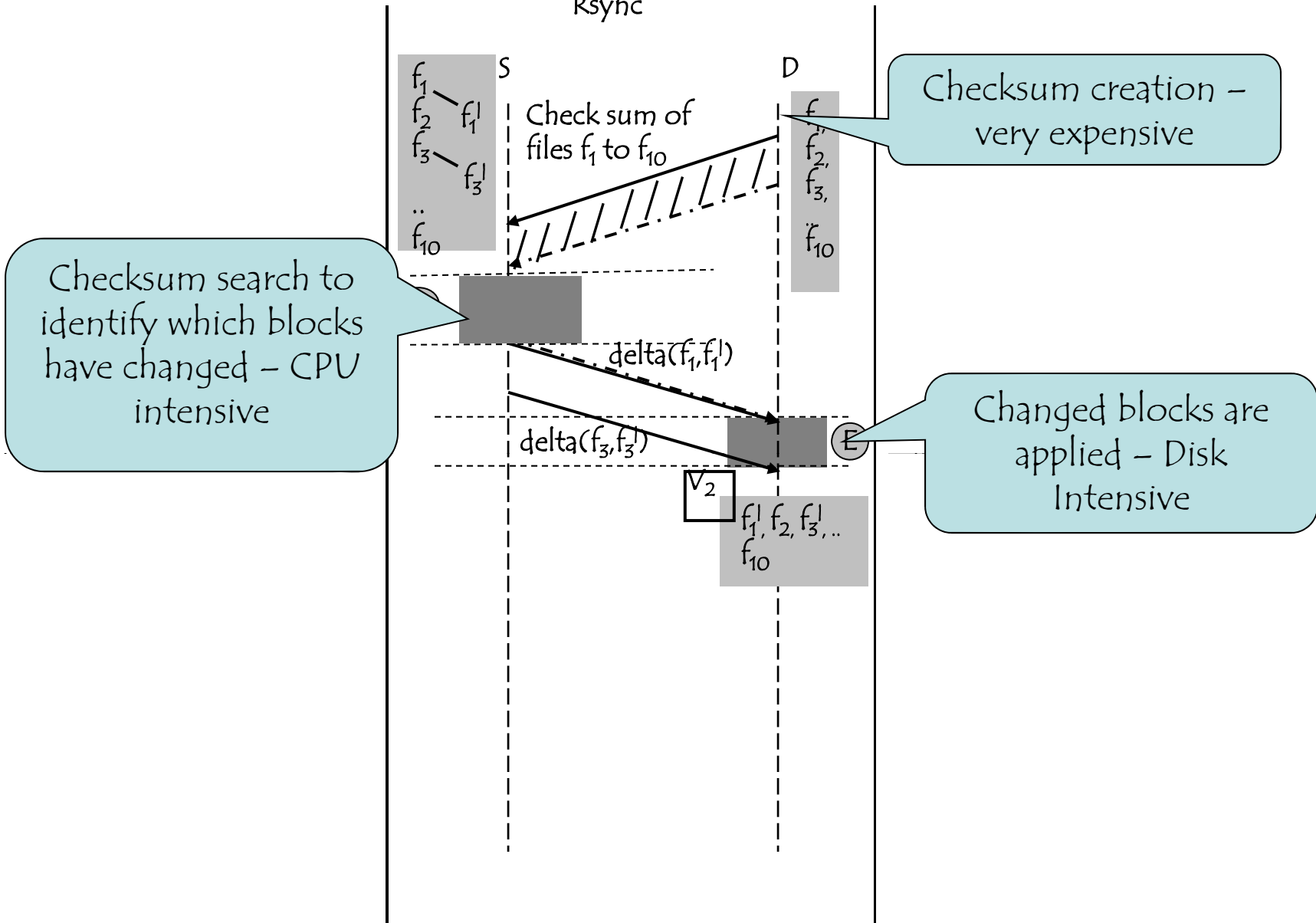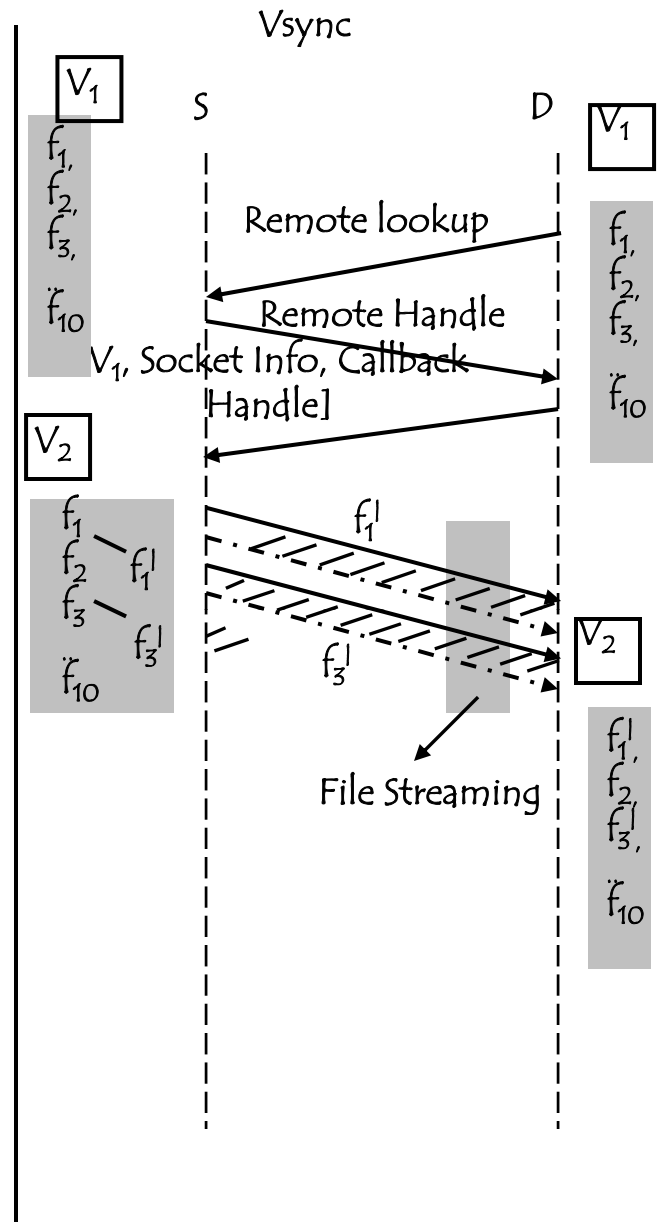# Protocol Round Trip Time Comparison

File Copy

S   D

Send $f_1 - f_{10}$

f_1
f_2 f_1^I
f_3

Acknowledgement

f_{10} f_3^I

$f_1,$
$f_2,$
$f_3,$

f_{10}

Get f_1^I

(A)

(B)

(C)

Get f_2

Get f_3^I

Rsync

f$_1$
f$_2$ — f$_1^|$
f$_3$ — f$_3^|$
..
f$_{10}$

S

Check sum of
files f$_1$ to f$_{10}$

D

f$_{1,}^{}$
f$_{2,}^{}$
f$_{3,}^{}$
..
f$_{10}$

Checksum creation –
very expensive

Checksum search to
identify which blocks
have changed – CPU
intensive

delta(f$_1$,f$_1^|$)

delta(f$_3$,f$_3^|$)

E

Changed blocks are
applied – Disk
Intensive

V$_2$

f$_1^|$, f$_2$, f$_3^|$, ..
f$_{10}$

Vsync

V_1

V_1

S

D

$f_{1,}$
$f_{2,}$
$f_{3,}$

$\ddot{f}_{10}$

Remote lookup

$f_{1,}$
$f_{2,}$
$f_{3,}$

$\ddot{f}_{10}$

Remote Handle

V_1, Socket Info, Callback Handle]

V_2

f_1
f_2 — $f_1^|$
f_3
$f_3^|$

$\ddot{f}_{10}$

$f_1^|$

V_2

$f_3^|$

File Streaming

$f_{1,}^|$
$f_{2,}^|$
$f_{3,}^|$

$\ddot{f}_{10}$

How does Vsync win?

Rsync – Vsync protocol comparison
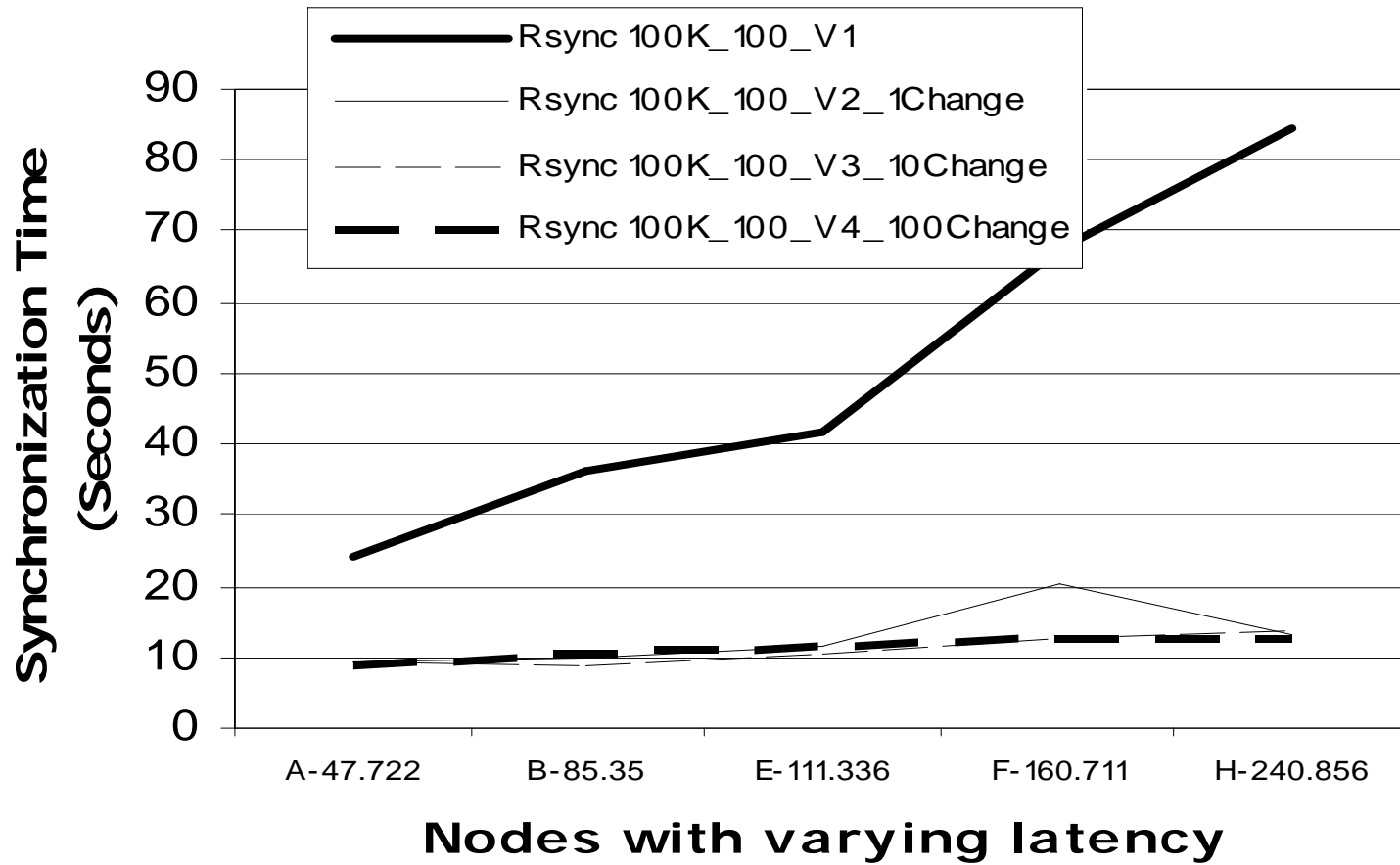
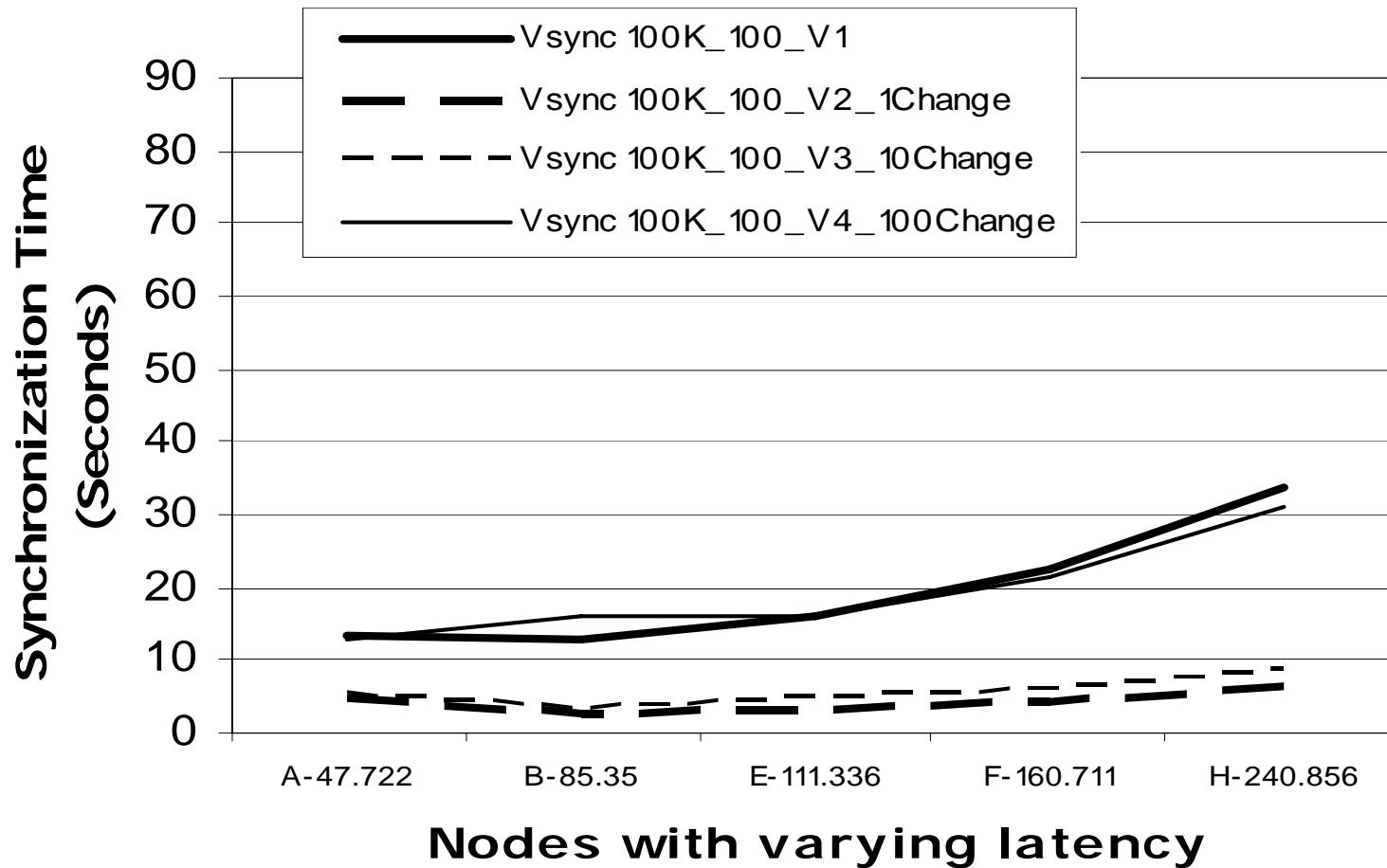| Rsync	Vsync
Exchanging checksums all the time	One time change set generation
Pipelining the files	Parallel streaming the files
# of round trips = 1	# of round trips = 2

Better

Better for less number of files

Better

Rsync synchronization on Planet Lab Nodes

Vsync synchronization on planet lab

Chart legend:
- Vsync 100K_100_V1
- Vsync 100K_100_V2_1Change
- Vsync 100K_100_V3_10Change
- Vsync 100K_100_V4_100Change

Y-axis: Synchronization Time (Seconds) — 0, 10, 20, 30, 40, 50, 60, 70, 80, 90

X-axis: Nodes with varying latency — A-47.722, B-85.35, E-111.336, F-160.711, H-240.856

Conclusion

- ⬩ Vsync provides an efficient replacement to Rsync for <u>update distribution</u> on Wide Area Networks.
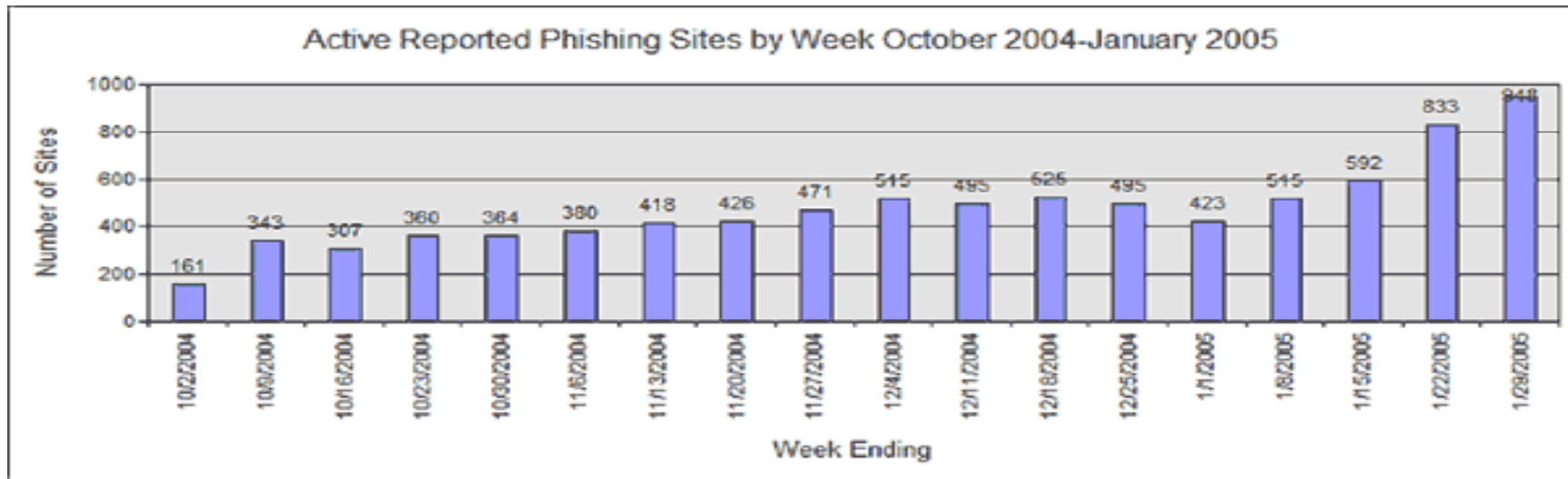
P-Messaging
QoS based Email Infrastructure

Infrastructure System and Services Research Lab

Quiz!

- What do you think were the losses in US alone for fraudulent emails for the fiscal year 2004?
  - $500 Million: Nacha (the electronic payments association)

How serious is unsolicited email?

Active Reported Phishing Sites by Week October 2004-January 2005

- Number of active phishing sites reported in January: **2560**
- Average monthly growth rate in phishing sites July through January: **28%**
- Number of brands hijacked by phishing campaigns in January: **64**
- Number of brands comprising the top 80% of phishing campaigns in January: **7**
- Country hosting the most phishing web sites in January: **United States**
- Contain some form of target name in URL: **25 %**
- No hostname just IP address: **53 %**
- Percentage of sites not using port 80: **9.53 %**
- Average time online for site: **5.8**
- Longest time online for site: **31 days**

Why did spam happen???

- Current Email infrastructure:
    - Unauthorized content creation in your mailbox.
    - No mechanism to validate email addresses.
    - No mechanism to differentiate email from a contact as a 'spam' or 'not-spam'.

- No support for differential email services.

P-Messaging

- P-Messaging, QoS based email infrastructure service, is dependent upon the users' privileges
  - Sender needs to possess the privilege to send the message
  - Receiver needs to honor the privilege to accept the message

- Built upon the current email infrastructure using signature based mechanism.
- Classification based on privilege mechanism allows differential services, i.e., Emails classified based on the privileges.
- For a receiver, out of the four categories:
  - Privilege honored and privilege verified ✅
  - Privilege honored and privilege not verified ❌
  - Privilege not-honored and privilege verified ❌
  - Privilege not- honored and privilege not Verified ❌
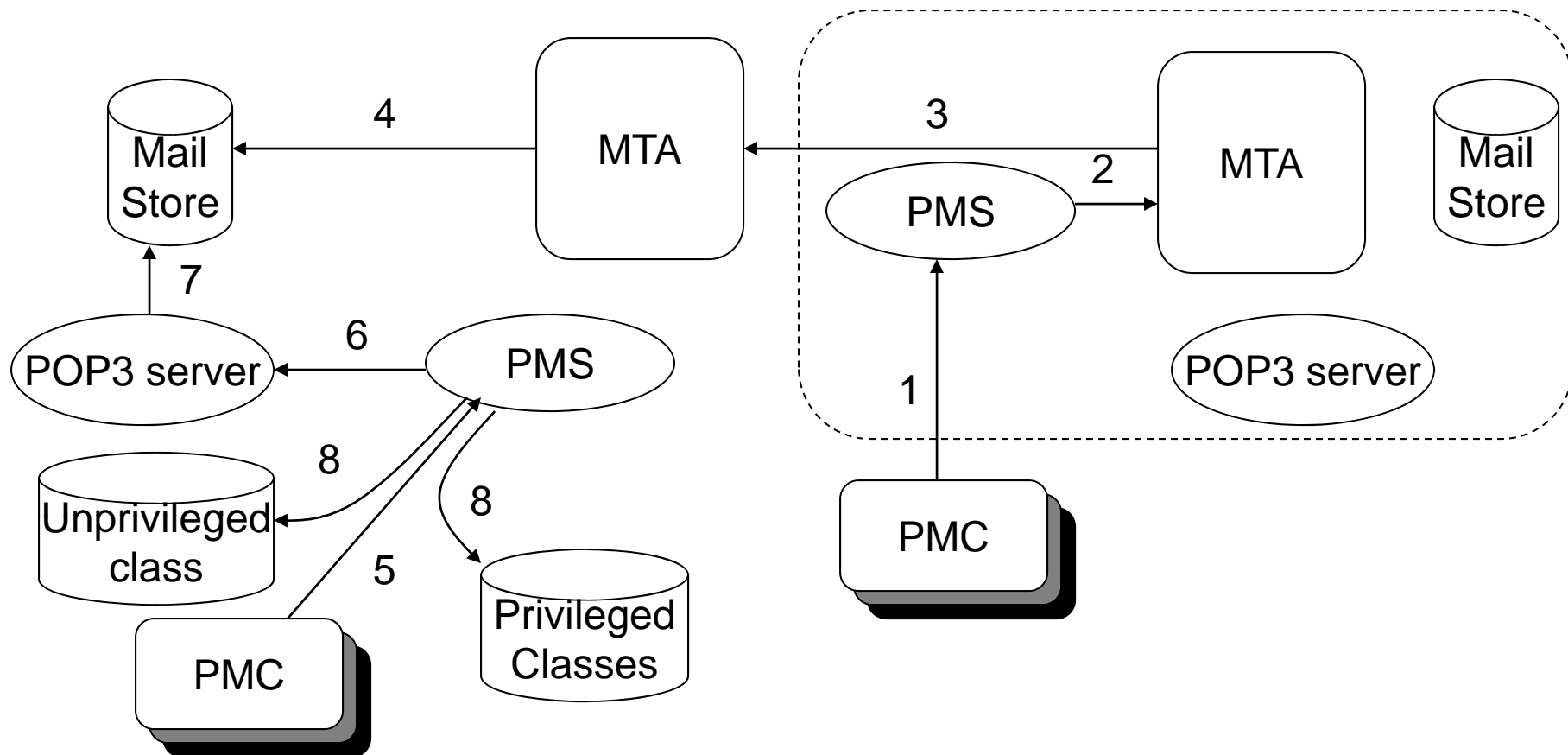
MTA – Message Transport Agent

PMS – Privilege Messaging Service

PMC – Privilege Messaging Clients

1. Message sent (RMI): Signature generation

2-5 SMTP calls [Privilege message]

6. Message download (RMI): Signature verification

Conclusion

- P-Messaging:
    - QoS based messaging mechanism.
    - Revisits the presumptions of the current email infrastructure.
    - Uses current email infrastructure.

- P-Messaging service and Outlook plug-in will soon be available…

Managing the IT Infrastructure

Infrastructure System and Services Research Lab

Management of IT Infrastructure

◇We are now forced to think *systems* not just computers.

◇Infrastructure Systems are agreeable vital , yet there is no **systematic framework** exists to analyze, design and operate these systems

◇The **methodologies and approaches** that are currently used are different for each domain specific infrastructure system and are often are based on <u>ad hoc experiences</u>

◇Is it a *management science* or an *engineering field* or (just) an *administrative job*

Complexity of Infrastructure Systems

◇ The complexity of computer systems is increasing all the time.
Even a single PC today, running Windows NT and attached to a
network approaches the level of complexity that an IBM, Unix
or VAX mainframe had ten years ago.

- Multitasking systems
- Multi User systems
- Complex Networks
- Security of users/network

Problems in IT Infrastructure Mgt.

What people do is _central_ to the whole thing. What are the problems we are facing?

- Lack of standards - software wars

- Rate of development: too slow/too fast

- Old-fashioned network models which do not scale well.

- Need to KNOW and keep track of all kinds of apparently random facts.

Why "Research"!!

- As infrastructure systems have increased in size, scope and complexity, the possibility of **cascading failures** exists between infrastructure systems in different domains

- Infrastructure System management issues are beyond the administrative realm
  - Network & System Design, Analysis, Efficiency and Security,
  - Issues in Network and System administration

  We propose to make these **management** issues to be an **administration science** and an **engineering field**

Research Direction

◇ The proposed research will examine the extent to which common frameworks, analysis approaches and methodologies can be developed for different infrastructure systems.

◇ The objective is to develop a **generalizable systematic approach** for infrastructure planning, implementation, operation and management

What are we trying to achieve?

- Enable **real time control** of the systems, including security, performance and reliability measurement techniques

- Modeling **failure correlations** and **integration dependencies**

- As a result, the infrastructure systems can be transformed from static systems to **dynamic demand responsive** systems.

"If we managed finances in companies the way we manage software…somebody would go to prison."

– Introduction to a workshop on configuration management conducted by Corvus International in 1996

Monitoring the IT Infrastructure

- Monitoring health of IT Infrastructure – We developed a Centralized Registry Framework for Configuration Management, called – RegColl

  (To be published in 19th USENIX LISA 2005 CONFERENCE)

Why?

- Compliance with current legislatures mandating protection of non-public information
- Corporate IT Infrastructure Policy Enforcement - Setting Standards
- System Configuration Management – Maintaining Stable States
- Incident Response – Reporting Requirements
- Most Importantly …. Monitoring health of IT Infrastructure systems

Monitoring system's registry

- System's registry and configuration information
  - offers important insights in deployed software, patches, drivers, etc –
  - analyzed for vulnerabilities, troubleshooting, and compliance standards
  - providing documentation for reporting requirements

RegColl Architecture

4. Compliance & Analysis Point

3. Config. & Registry Repository

2. Collection Server

1. Collection Points

Registry Collector
Primary Collection Server

Policy Enforcement

Audit & Analysis

Registry & Configuration Store

Configuration Management

Laptop . Logs of Registry Snapshots

Incident Response

WkStn1 | Reg_v1,Reg_v2,Conf_v1, …

Primary Server

Fail Over Server

Secondary Server

Networked Systems

Disconnected Systems

Registry Monitor

Workstation-1

Registry Monitor

Workstation-2

Registry Adaptor

Registry Monitor

Desktop

Registry Monitor

Laptop computer

Collection Server
Registry & System
Configuration Information

RegColl Conclusion

◇ We identified that a centralized registry and system configuration repository could incorporate useful facilities for infrastructure system monitoring, including:

- System audit, compliance checks and configuration analysis

- Incident response endorsement and reporting process

- Policy validation and enforcement

- System configuration management

New Infrastructure Systems

Network File System

Replica based File System (RFS)

Storage Services

Session based Secured File System (SSFS)

Backup Server

Storage Server

Tape Backup

File Server

Configuration Management Framework
with Windows Registry Collection (RegColl)

RAID 1   RAID 2

eMail Services

Privilege Messaging

PC Workstations

Vsync Patch Dissemination

Replica Plane (RPlane)

Web/ FTP Services

Database Server

Router w/ Firewall   Firewall

Outside   World

Web Server

FTP Server