



BruNet NETWORK & **SECURITY**

BY

Pg Hj Zuhairi bin Pg Hj Jamaludin
Head of BruNet Technical Services
Jabatan Telekom Brunei



BruNet NETWORK & SECURITY

The topic covers 4 Major Parts:

- Introduction
- **BruNet** Network
- **BruNet** Security
- Conclusion



INTRODUCTION



INTRODUCTION

- ESTABLISHED IN OCTOBER 1995, WITH COLLABORATION WITH UBD
 - Dialup: 14.4kbps
 - Lease-line service.
 - 1 Uplink to Singapore, Initially 384kbps then upgraded to 2Mbps
 - 1 Server for WWW, Email, FTP, Newsgroup

- UPGRADED IN 1996
 - Dialup: 28.8kbps and 33.6kbps
 - 8Mbps upstream to Singapore
 - 1 Server for WWW, Email, FTP, Newsgroup

- **BruNet** EXPANSION IN 1998
 - ISDN Introduced
 - 56kbps (FLEX)
 - 14Mbps upstream to Singapore
 - Dedicated Servers (WWW, Email etc)



INTRODUCTION

- In 2000
 - Broadband Introduced
 - 2nd Upstream 45Mbps to USA

- In 2003
 - Revamp entire **BruNet** Network
 - Upstream Singapore upgraded to 45M + USA still 45M

- In 2004
 - New Upstream to HongKong with 45Mbps (total 135Mbps)

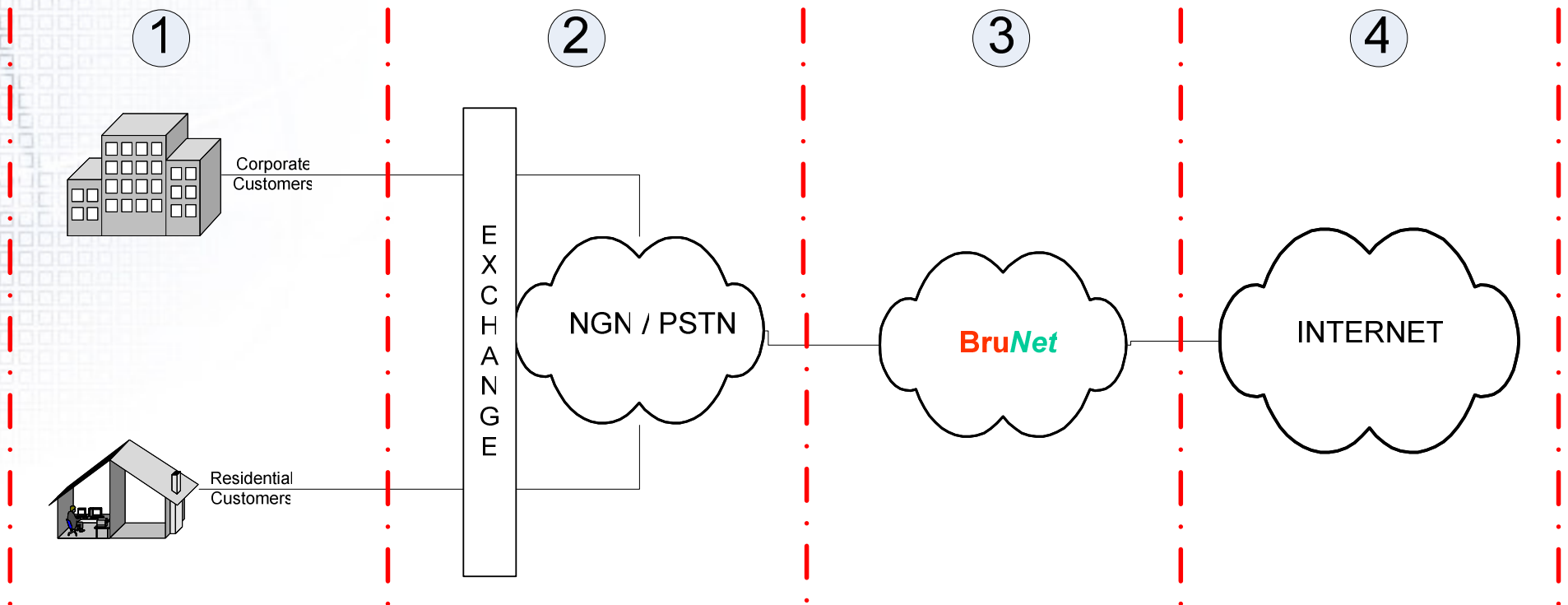


BruNet NETWORK



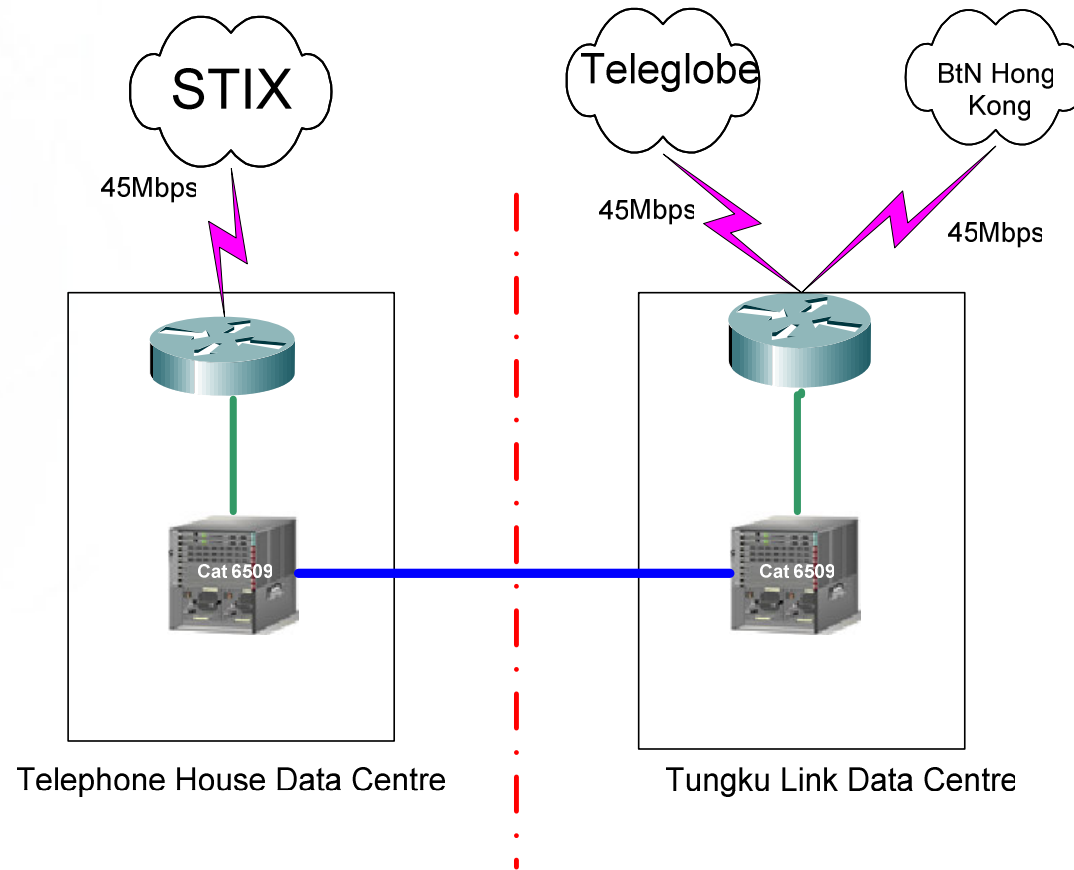
BruNet NETWORK - Overview

INTERNET CONNECTIVITY DIAGRAM





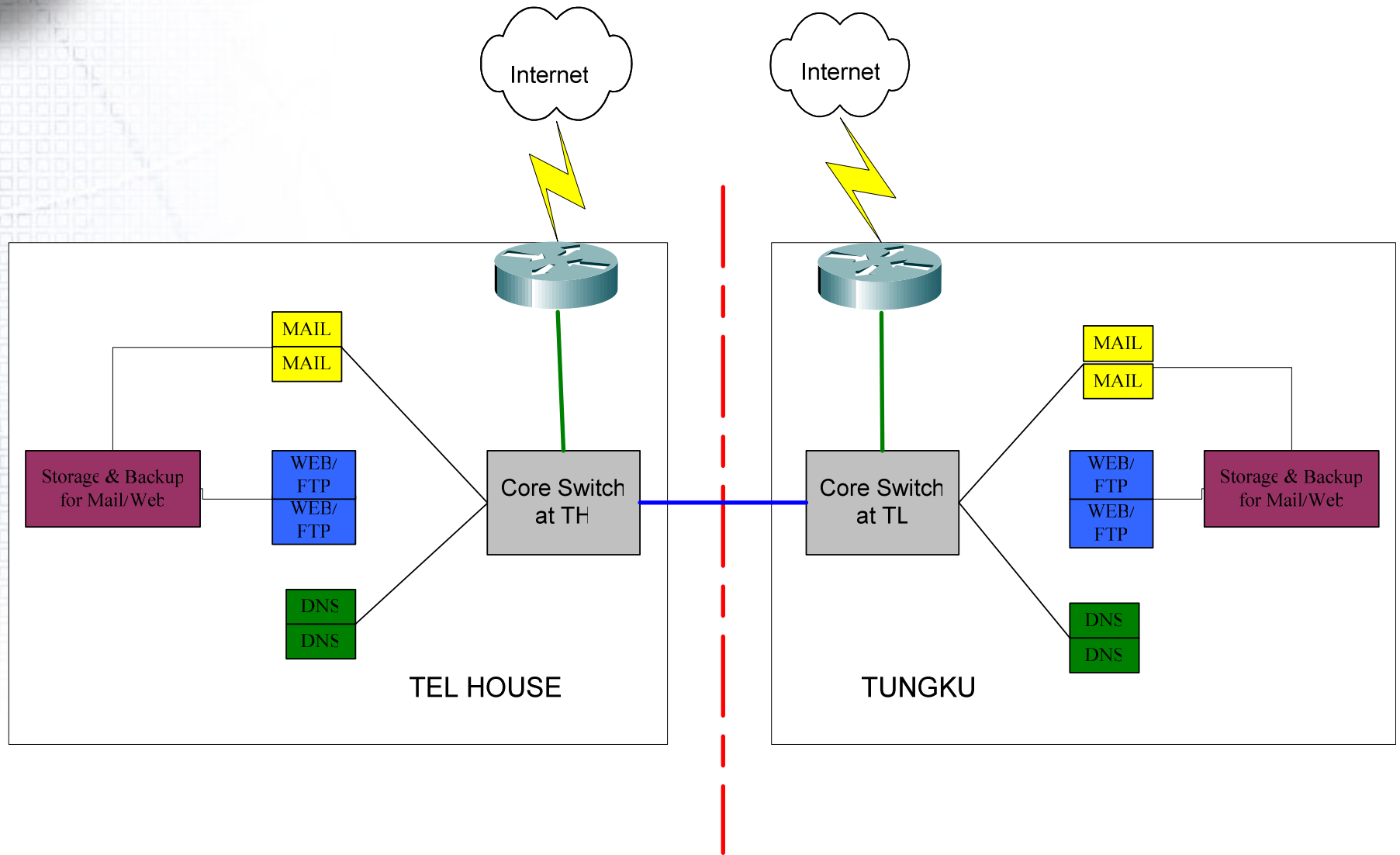
BruNet NETWORK - Core Network



BruNet Core Network Setup



BruNet NETWORK - ISP Services





BruNet NETWORK - Services

➤ ACCESS SERVICE

- Dialup
- Broadband-ADSL (Espeed)
- Leased-Lines
- Hot Spot-WiFi (BlinkZONE)

➤ VALUE ADDED

- WebHosting (Personal & Corporate)
- eMail
- Domain Name (com.bn, gov.bn, edu.bn org.bn)
- Co-location
- Banner Advertising
- Virtual Email

➤ For more info Visit: www.brunet.bn



BruNet SECURITY



BruNet SECURITY

BruNet SECURITY

- Data Center - Physical Security
- Network Security
- Security Threats
- Future Security Initiatives



BruNet SECURITY

DATA CENTER - PHYSICAL SECURITY

1. Two (2) BruNet DRC Sites at Different Geographical Location
2. DRCs are Restricted Area
3. Security Door Access (BIOMETRIC)
4. CCTV
5. Fire Protection System (FM200)





BruNet SECURITY

NETWORK SECURITY

1. Firewall
2. IDS
3. Network Element Filtering (Router, Coreswitch, Servers)
4. SMTP Security (Anti Relay, Anti Virus & Anti Spam)
5. Redundant Servers
6. Authentication/Password



BruNet SECURITY – Network Security

➤ FIREWALL

- BruNet's first line of Defence.
- Purpose of having Firewall is to protect BruNet resources from being use by users from other network.
- Basically it controls who goes in and out of BruNet network.
- Security logs can be used as forensic evident.
- All critical servers (Web, Email & Radius) are behind Firewall.
- Less-critical servers are placed in DMZ (Demilitarized Zone).
- However, it does not provide protection against email Viruses.



BruNet SECURITY – Network Security

➤ INTRUSION DETECTION SYSTEM (IDS)

- BruNet's second line of Defence.
- Simple Analogy: Firewall is a “Secure Door Access”, while IDS is your “Burglar Alarm”.
- Monitor, analyze and detect suspicious activities
- Recognize abnormal activity pattern
- To provide security logs for BruNet Security Team to act upon.
- IDS is “reactive” in nature



BruNet SECURITY – Network Security

➤ NETWORK ELEMENT FILTERING

- Router :
 - ❖ *Route filtering (use by BruNet IP)*
 - ❖ *Packet filtering (validity of Source)*
 - ❖ *Rate Limiting (eg ICMP)*
- CoreSwitch
 - ❖ *Apply Access Control Lists (ACL)*
- Servers
 - ❖ *Apply Access Control Lists (ACL)*



BruNet SECURITY – Network Security

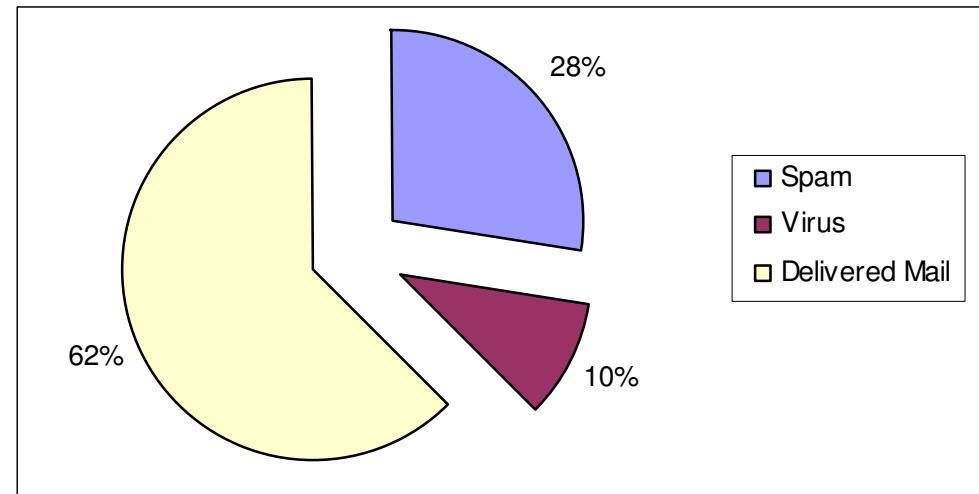
➤ SMTP SECURITY

- Anti Relay:
 - *It only allows sending email from any .bn domain.*
- Anti Virus:
 - *Eliminates email virus/worm from reaching BruNet email users Inbox.*
- Anti Spam:
 - *Reduces SPAM reaching BruNet customers*

➤ SPAM Filtering Effectiveness:

- Was 70% in 2002.
- Now reduced to 30%
- Due to Evolving nature of SPAM

➤ JTB is Looking at a more Advance Anti-Spam System





BruNet SECURITY – Security Threats

WHAT ARE SECURITY THREATS THAT AN ISP
(eg BruNet) ENCOUNTER?

- Hacking
- Virus/Worms
- SPAM
- Dos/DDos
- Spoofing
- Phishing
- Modem Hijacking

*Continue



BruNet SECURITY – Security Threats

*Continue

- Phishing :
 - Scheme to trick customers into giving-out their details
 - Usually in the form of email, disguised as coming from a Financial Institution (eg Bank), requesting customer details by claiming Updating its record.
- Modem Hijacking
 - Customer Visit “Funny” website, eg Adult, Gaming and Gambling.
 - By pressing a button, A DIALLER automatically installed onto customer PC:
 - Terminate connection to local ISP
 - Establish an IDD call to a remote server.
 - Customer will be charged with IDD call, caused by the DIALLER.



BruNet SECURITY – Security Threats

WHAT CAN BE DONE TO REDUCE IMPACT FROM SECURITY THREATS?

- First of all, BruNet as well as other ISPs, cannot eliminate entirely the security threats.
- However, BruNet can minimize impact from security threats via IDS, Firewall, SMTP security and other security measures.
- BruNet also actively participates in dialogue lead by AiTi (Brunei Industry Regulator) with regards to SPAM issue.
- Identified Security Breach will be acted upon depending on severity of attack, ranging from simple warning to service suspension.
- Uplink providers also help in blocking DDos attack from overseas.
- BruNet customers can reduce risk further by:
 - Installing Client-based Anti-spam, Anti-Virus & Anti-SpyWare
 - Installing Personal Firewall
 - Following safe Internet Practice



BruNet SECURITY – Future Security Enhancement Project

- DRC expansion Project
 - Improve Network Resilience
 - Improve Security Measure (Advance Analysis tool)
 - Human Resource Development

- Enhance BruNet Security:
 - Intrusion Prevention System (IPS)
 - Host based IDS
 - Host based Firewall

- Traffic Management System (with build-in security features)
 - Control - To Avoid DoS attack and SYN flood.

- Looking at a more advance Anti-Spam System



CONCLUSION



CONCLUSION

- In summary, I quote a remark by Mr Vinton Cerf, a Senior VP of Technology Strategy at MCI (taken from Telecom Asia Magazine):

“What I call cyber hygiene, the notion that security is everyone’s business and that everyone using a computer in an organization should set aside a little time everyday to tending to security matters. If everyone did that there’d be a lot fewer problems”



THANK YOU



➤ For Enquires or Complaints about JTB Internet Services:

- Call : **121** (toll free number)
- e-Mail : 121@brunet.bn