DNS Operational Experiences in JPRS/.JP

- DNS itself, IPv6, IDN, ENUM -

February 22, 2005
APRICOT 2005 Tutorial

Yasuhiro Orange Morishita <yasuhiro@jprs.co.jp>
Japan Registry Services Co., Ltd. (JPRS)

Targets / Objectives

- Targets
  - – DNS operators/engineers/administrators
    - Especially, TLD DNS operators/engineers
- Objectives
  - – By telling our operational experiences, for helping the DNS server operation
  - – Discussions about them for our past, current and future works

Today’s topics

Technical overview of the following topics and operational experiences in JPRS/.JP

- DNS itself
- DNS related issues
  - IPv6
  - IDN
  - ENUM

DNS

Review: What’s DNS?

Basic (traditional) functions

- Translating/binding between “Domain Name” and “IP address”
  - “Mapping” and “Inverse Mapping”
    - www.apricot.net → 202.12.29.22
    - 202.12.29.22 → nori2.apnic.net
- Email routing
  - Mail Exchange (MX)
  - Identifying a mail exchange for specified domain

Applied functions

- RBL (Realtime Blackhole List)
  - Publishing the “bad” IP addresses of hosts (open mail relays, proxies)
- ENUM (Telephone Number Mapping)
  - Translating E.164 numbers into names/services
- SPF (Sender Policy Framework)
  - Authorizing Use of Domains in email
- And there are so many approaches/usages...
  - AutoID, Cryptographic key, etc...

Review: the features of DNS

- A “Distributed” directory services
- A tree structured name space
  - Domain name space
- Widely deployed
- Low costs (for clients :-)
- Needs “**Internet Registry**”

The role of the Internet Registry

- Administrating “the resources”
  - Domain name registration
  - IP address allocation/assignment
- Managing DNS and WHOIS
- The Internet registry has responsibility in DNS management as well as resources management

A brief history of .JP

- In 1986, .JP was delegated to Jun Murai
- In 1991, JNIC was founded to provide a framework for operation of the .JP
- In 1993, JNIC reorganized itself as Japan Network Information Center (JPNIC)
- In 1997, JPNIC obtained approval from 4 governmental ministries to operate as a corporate body
- In 2002, .JP redelegated to JPRS

A brief history of .JP – in the DNS side

- In the beginning, getting the Worldwide Internet Reachability from Japan was not easy
  - “Domestic IP networks” vs “Worldwide reachable”
- Therefore, JPNIC managed the “3 series” of .JP DNS servers until 1995
  - Series A: Servers for “outside of Japan”
    - Registering only “worldwide reachable” .JP domains
  - Series B: Servers for “domestic”
    - Registering all domains in .JP
  - Series C: Servers for “merged”
    - For referring as “DNS resolver” from “worldwide reachable” hosts in Japan
- Current .JP DNS servers derived from “Series A”

A brief history of .JP DNS servers

- In those days, the important factor of “Series A” is “Reachability from outside of Japan”
- Therefore, JPNIC selected 6 servers
  - 1 server for JPNIC itself, as primary server
  - The organizations which have the “dedicated line for oversea”, as secondary servers
    - 3 servers in “academic” Internet (BITNETJP/JOIN, SINET, WIDE)
    - 2 servers in “commercial” Internet (IIJ, SPIN)
  - All servers were started “voluntary based”
- In 1996, JOIN resigned .JP secondary for closing dedicated line to USA
- In 1999-2002, 1 .JP secondary server added for referring outside of Japan hosted by NTT America Inc. (ns-jp.ntt.net)
- In 2001, Internationalized Domain Name (**IDN**) started in .JP
- In 2003, unification of DNS server hostnames (A.dns.jp ～ F.dns.jp)
- In 2003, established **ENUM** trial Japan (ETJP)
- In 2004, **IP Anycast** technology introduced in .JP DNS
- In 2004, ICANN registered **IPv6** address for glue of .JP DNS

.JP DNS servers – the current

- burdened “The history”
  - A little bit similar to root servers
    - Started as voluntary based
    - Derived from “Reachability” (especially from outside of Japan)
    - The balance between academic and commercial
- The current framework
  - JPRS has the responsibility for managing .JP DNS
  - JPRS organizes “JP DNS managers” for .JP DNS servers’ operation
    - Current member: JPRS, JPNIC, IIJ, SINET, SPIN, WIDE

Recent topics in .JP DNS

- Unification of server hostnames (in 2003)
- Changing the location of E.dns.jp (in 2003)
- Changing IP address and AS number for A.dns.jp and E.dns.jp (in 2003-2004)
- Introducing IP Anycast in A.dns.jp and D.dns.jp (in 2004)

Unification of hostnames (in 2003)

- Hostnames of .JP DNS servers are unified to [A-F].dns.jp on June-August 2003
  - Primary server
    - A.dns.jp: operated by JPRS
  - Secondary servers
    - B.dns.jp: formerly ns0.nic.ad.jp
    - C.dns.jp: formerly dns0.spin.ad.jp
    - D.dns.jp: formerly ns0.iij.ad.jp
    - E.dns.jp: formerly ns.wide.ad.jp
    - F.dns.jp: formerly ns-jp.sinet.ad.jp
- To allocate the payload for more IPv6 glue
- To simplify the relation of delegation
  - “dns.jp” zone itself is now delegated to [A-F].dns.jp

Changing the location of E.dns.jp (in 2003)

- E.dns.jp is former ns.wide.ad.jp
  - Operated by WIDE Project
- Moved the physical location
  - Outside of Tokyo (Osaka area)
- To enhance robustness of .JP DNS service
  - To provide extra redundancy to survive .JP DNS service in the case of serious disasters in Tokyo

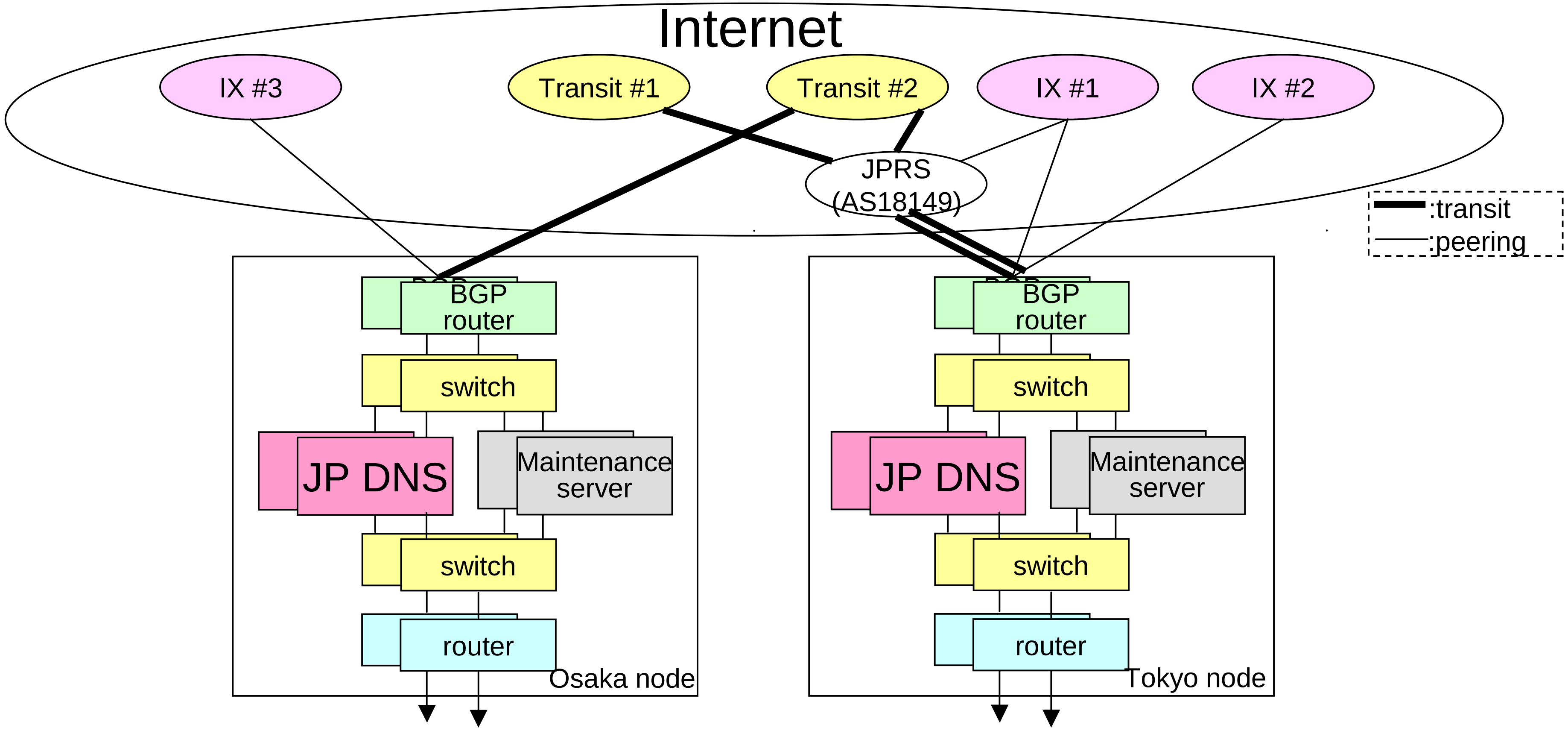
Changing IP address and AS number of A.dns.jp and E.dns.jp (in 2003-2004)

- Changed the IP address and AS number
  - Provider independent (PI) address and its own AS number
    - Detached from organization network itself
    - Only for DNS infrastructures
    - To acquire multiple transits

Introducing IP Anycast in A.dns.jp and D.dns.jp (in 2004)

- A.dns.jp and D.dns.jp are now in IP Anycast mesh
  - A.dns.jp, by BGP anycast
  - D.dns.jp, by IGP anycast

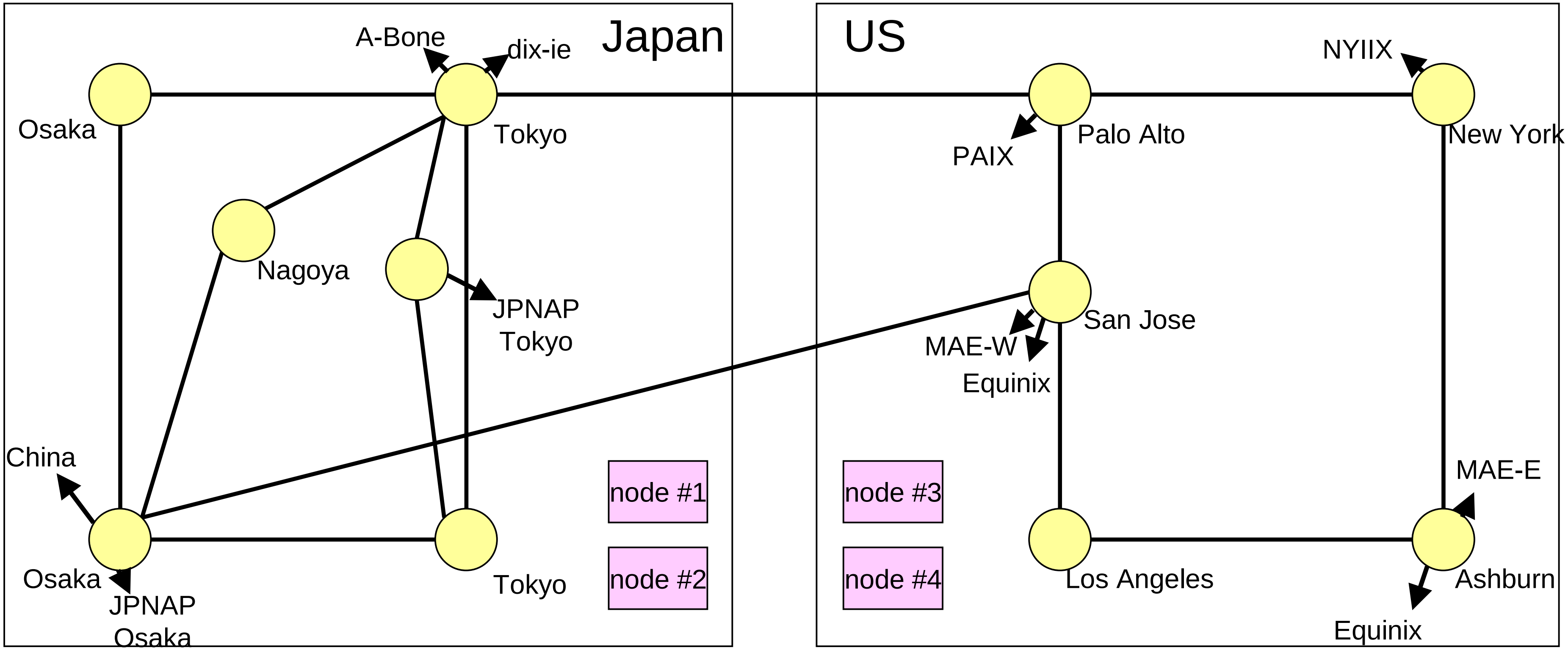
Technical details of A.dns.jp



Technical details of A.dns.jp (cont.)

- Operated by JPRS
- BGP Anycast
  - We have both IPv4 and Ipv6 address, but IP Anycast is introduced in IPv4 address only
- Nodes are located in Tokyo and Osaka
- Fully-duplicated system
  - DNS servers
  - BGP routers
  - Switches
  - Maintenance servers
  - Local routers
  - Remote console servers
- All servers are active and load-shared
- Automatically switched upon system failure

Technical details of D.dns.jp



Technical details of D.dns.jp (cont.)

- Operated by IIJ (Internet Initiative Japan Inc.)
- IGP Anycast
- Two nodes are located in Japan, other two nodes are located in USA (East and West)
- All nameserver nodes are connected to IIJ backbone network
- IIJ has its own global IP backbone and external connection points in Japan and USA

IPv6

Review: What's IPv6?

- The primary purpose: to solve the problem of the shortage of IP addresses
- IPv6 has 128 bits length address
  - IPv4 has only 32 bits

What we need for IPv6 – in the DNS and Registry side

- Two independent DNS issues
  - Capability of processing IPv6 related DNS resource records
  - Capability of processing IPv6 DNS packets (aka IPv6 “transport”)
- Registry/Registrar issue
  - The Internet Registries and Registrars must process registrant’s IPv6 related requests

Capability of processing IPv6 related DNS resource records

- IPv6 related DNS resources records (RRs)
  - AAAA record for mapping
  - IP6.ARPA domain for inverse mapping
    - IP6.INT also should support for compatibility
- Current almost of all DNS server implementations support them
  - BIND 9 and 8
  - NSD
  - djbdns
    - original version supports AAAA itself, and unofficial patch supports writing AAAA easier
  - Nominum’s ANS

Capability of processing IPv6 DNS packets (aka IPv6 “transport”)

- For supporting this, both DNS “authoritative” server and “cache” server have capability for IPv6
- DNS “authoritative” server
  - Prepare for “IPv6 capable DNS server box”
  - Both “a separated server” and “dual-stack” are acceptable
    - It is an operational issue
- DNS “cache” server
  - Prepare for “IPv4 and IPv6 capable DNS server box”
  - DNS “cache” server needs iterative query for each DNS “authoritative” servers
  - DNS “authoritative” servers may support “IPv4 only” or “IPv6 only”
  - And currently, there are no IPv6 addresses in root zone cache
  - Therefore, it must support “dual stack” connectivity
- Current almost of all DNS server implementations support IPv6 transport
  - BIND 9 and 8
  - NSD
  - djbdns with unofficial patch
  - Nominum’s ANS/CNS

Our experiences – IPv6 related work

- In 1999, I sent a bug fix of BIND 8 to ISC for AAAA glue treatment on zone transfer
  - And this is stay alive in the current BIND 8 source...

```
(In ns_xfr.c of current BIND 8.4.6)

 /* for IPv6 glue AAAA record transfer */
                /* patched by yasuhiro@nic.ad.jp, 1999/5/23 */
                foreach_rr(gdp, gnp, T_AAAA, class, DB_Z_CACHE)
                        if (sx_addrr(qsp, fname, gdp) < 0) {
                                /*
                                 * Rats.  We already sent the NS RR, too.
                                 * Note that SXL_GLUING is being left on.
                                 */
                                return (-1);
                        }
```

- In 2000, .JP supported IPv6 AAAA registration for DNS server address (aka “glue”)

Our experiences – IPv6 related work (cont.)

- In 2002, JPRS requested to IANA for registering IPv6 address for .JP DNS servers
- In 2004, IANA registered IPv6 address for .JP DNS servers (this is the first in the world)
- Currently, there are 4 IPv6 ready DNS servers in .JP
  - {A, D, E, F}.dns.jp

IPv6 and DNS packet size issue

- IPv6 provides large address space
- But this increases DNS packet size, too
- Original DNS supports 512 octets as maximum size for UDP transport, and it exceeds, packet is truncated and fallback to TCP
  - It increases the DNS load
- EDNS0 (RFC 2671) can increase UDP payload
- In IPv6 environment, DNS server should support EDNS0 function
  - It is similar to DNSSEC issue

IDN

Review: What’s IDN?

- Internationalized Domain Name
- Extending the domain name space
  - Example: 日本語.jp
- Increasing usability of Internet, especially non-English language people
  - Example
    - Famous person’s web pages (人名辞典.jp)
    - Product campaigns (生茶.jp)

What we need for IDN – in the DNS and Registry side

- IETF makes “Internationalizing Domain Names in Applications (IDNA)” architecture for IDN standard (RFC 3490)
- It requires **no** DNS protocol extensions
- But there are many operational issues for deployment of IDN

What we need – introducing IDN

- Character sets and variants which can be registered
  - Especially, “homograph attacks” issue
  - Described later
- Making the registration policy
  - Sunrise period
  - Priority registration policy
    - Trademarks and Trade names
  - Dispute Resolution Policy (DRP)

IDN in .JP

- Available characters
  - Hiragana, Katakana, Kanji
    - The selection is based on JIS (Japanese Industry Standard)
  - Several marks regarded as a Kana or a Kanji
    - ・ヽヾゝゞ〃仝々〆〇ー
- Variants
  - No variants defined
  - In our draft, draft-yoneya-jachar-00.txt: “… However in the name, especially in the proper noun, those aren't interexchangable because of their own identity. Actually, there is no official Kanji variants table in Japan.”

Our experiences in IDN

- In 2001, JPRS started IDN service in .JP
  - RACE-based encoding
- In 2003, JPRS migrated to IDN standards (RFCs)-compatible Japanese JP domain name registration

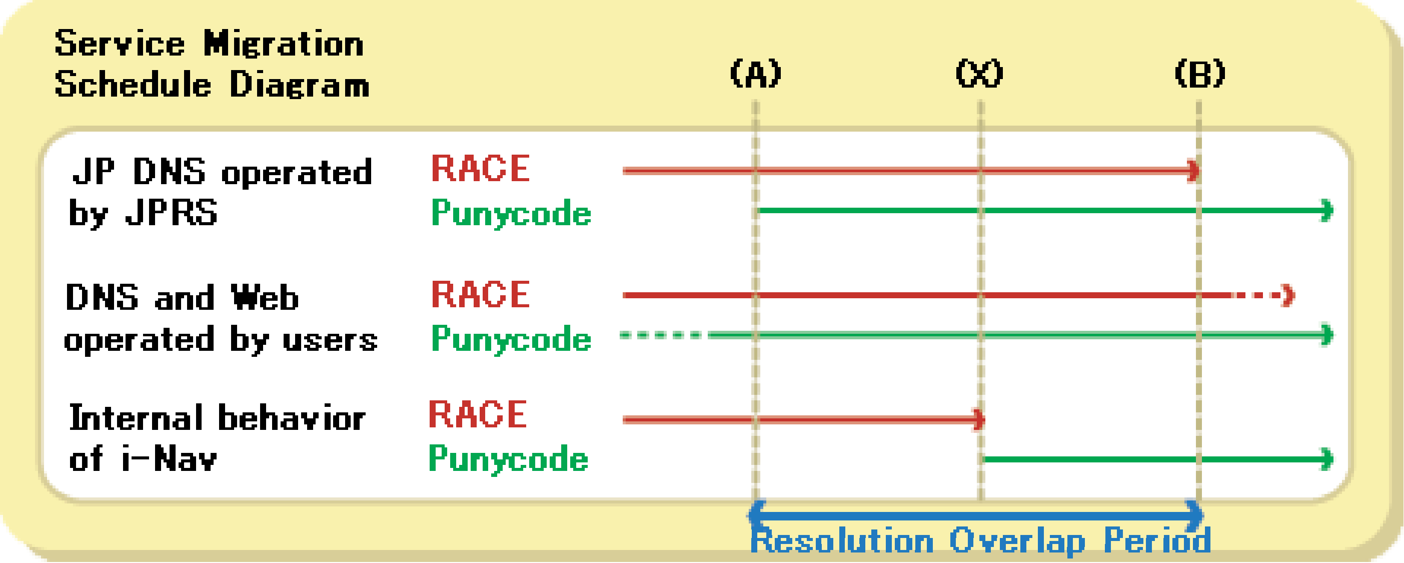
Our experiences – Resolution Overlap Period

- We made “Resolution Overlap Period”
  - Both NS records of Punycode and RACE on .JP DNS servers during ROP (as seen below)
  - To enhance smooth migration of DNS and/or Web server settings from RACE to Punycode

```
; 日本レジストリサービス.jp
; Punycode
xn--vckfdb7e3c7hma3m9657c16c.jp.             IN NS ns1.jprs.co.jp.
                                             IN NS ns1.jprs.co.jp.
; RACE
bq--3bs6kzzmgdwdbobqxeymqmhkgc2tb7bq2myls.jp. IN NS ns1.jprs.co.jp.
                                             IN NS ns2.jprs.co.jp.
```

Resolution Overlap Period

- (A) Starting ROP – on July 10, 2003
- (X) i-Nav^{TM} IE plug-in is changed into Punycode version – on July 30, 2003
- (B) Termination of RACE support – on September 3, 2003


Service Migration Schedule Diagram
(A)
(X)
(B)
JP DNS operated by JPRS
RACE
Punycode
DNS and Web operated by users
RACE
Punycode
Internal behavior of i-Nav
RACE
Punycode
Resolution Overlap Period

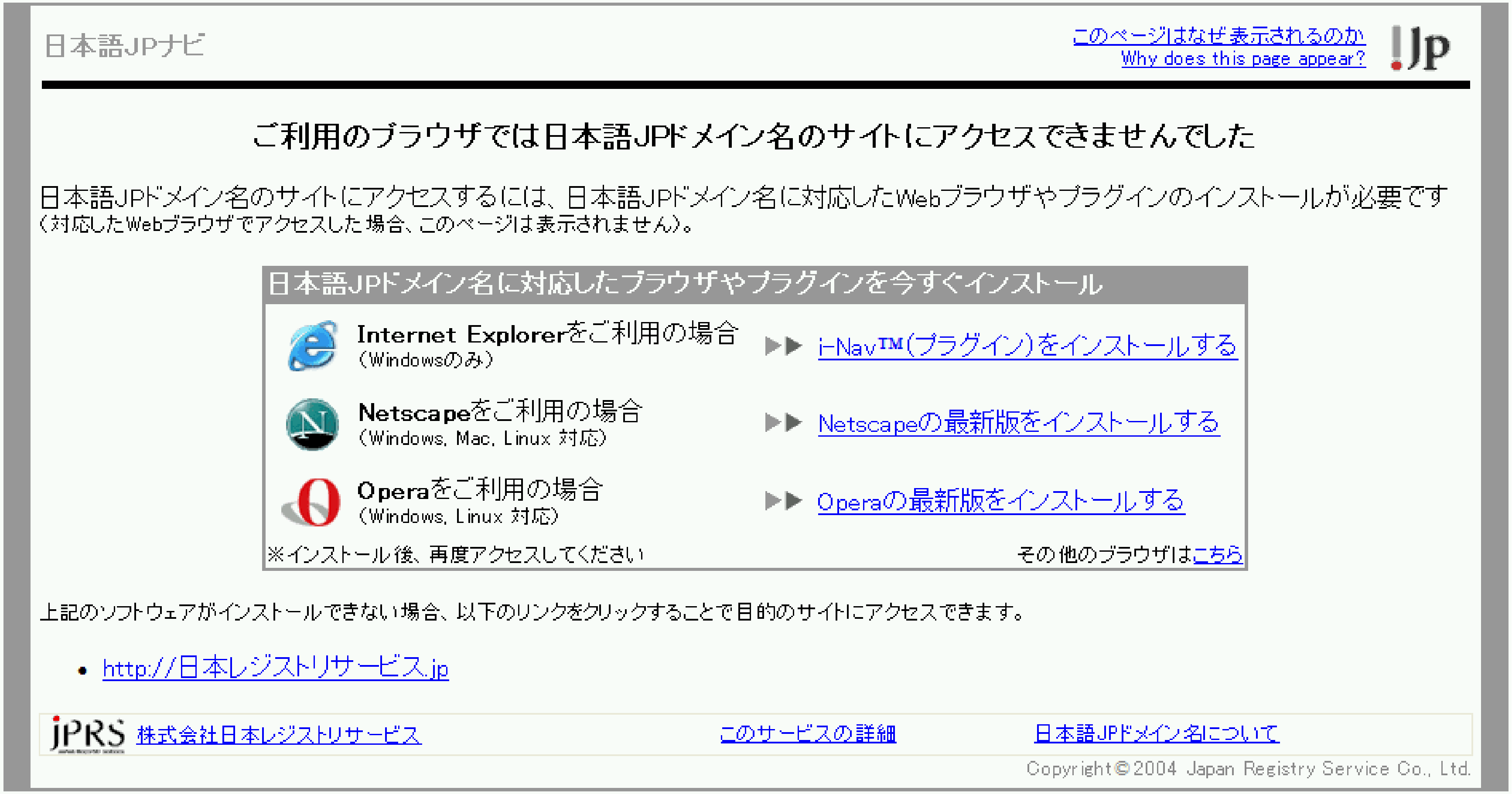
Our experiences – “Japanese JP Navi” service

- In 2004, JPRS started “Japanese JP Navi” service
- Objectives
  - By using DNS
    - Inform users to use IDN-aware Web browsers
    - Decrease 8bit label DNS queries
  - For IDN not-aware web browsers
    - Users happen to see unexpected error, but they can not understand the reason
    - JDN registrants want to utilize their JDN, but it is hard to get understanding of users that JDN/IDN-aware application is required
    - Without deployment of JDN/IDN-aware environment, it continues 8bit label DNS queries

“Japanese JP Navi” service

- Only when JDN registrant wishes, adds UTF-8 encoded JDN onto JP zone
  - Japanese JP-navi is **opt-in**
  - Requires existence of NS
  - Adds A and MX RRs
  - No wildcard RRs
- When users type JDN through JDN/IDN-unaware Web browser, a certain Web page is shown
  - To navigate i-Nav™ plug-in download page
  - To introduce JDN/IDN-aware browsers such as Opera and Netscape Navigator

Example of the navigation page



日本語JPナビ

このページはなぜ表示されるのか
Why does this page appear?

ご利用のブラウザでは日本語JPドメイン名のサイトにアクセスできませんでした

日本語JPドメイン名のサイトにアクセスするには、日本語JPドメイン名に対応したWebブラウザやプラグインのインストールが必要です
（対応したWebブラウザでアクセスした場合、このページは表示されません）。

日本語JPドメイン名に対応したブラウザやプラグインを今すぐインストール

Internet Explorerをご利用の場合
（Windowsのみ） ▶▶ i-Nav™(プラグイン)をインストールする

Netscapeをご利用の場合
（Windows, Mac, Linux 対応） ▶▶ Netscapeの最新版をインストールする

Operaをご利用の場合
（Windows, Linux 対応） ▶▶ Operaの最新版をインストールする

※インストール後、再度アクセスしてください　その他のブラウザはこちら

上記のソフトウェアがインストールできない場合、以下のリンクをクリックすることで目的のサイトにアクセスできます。

- http://日本レジストリサービス.jp

株式会社日本レジストリサービス　このサービスの詳細　日本語JPドメイン名について

Copyright©2004 Japan Registry Service Co., Ltd.

RRs address onto .JP

- A and MX RRs for UTF-8 encoded JDN and with www

```
xn--wgv71a119e.jp. NS        ns. xn--wgv71a119e.jp.
日本語.jp.            A         10.10.10.10
                      MX 10     not-exist.jp.
www.日本語.jp.        A         10.10.10.10
                      MX 10     not-exist.jp.
```

    - AAAA is currently not provided

- Basically, 4 RRs are added per domain
  - In maximum, 12 RRs are added if the JDN includes alphabet
    - To support compatible characters of alphabets

ASCII	“JPRS会社.jp”
Full-width (Upper case)	“ＪＰＲＳ会社.jp”
Half-width (lower case)	“ｊｐｒｓ会社.jp”

  - If JDN includes digit and/or hyphen, 8 RRs are added

ASCII	“123-会社.jp”
Full-width	“１２３－会社.jp”

Treatment of SMTP

- Due to A RR addition, SMTP connection is expected
    - To avoid receiving E-Mail, add MX RR which does not exist to make immediate error
- There are MTAs that try to connect A if connect to MX failed (RFC2821 violation)
    - No SMTP service provided
        - Not to record any connection
    - RFC2821 incompliant MTAs will retry for a several days
- SMTP connection may be rare (our assumption)
    - MTA will cause error during address format checking

Our experiences – DNS survey before starting “Japanese JP Navi”

- UTF-8 8bit label treatment in DNS
- 8bit is permitted as the DNS protocol, but there are few operational experiences
  - Cite from RFC1035, 3.1 Name space definitions

    Although **labels can contain any 8 bit values** in octets that make up a label…
- Target of survey on UTF-8 8bit label treatment on DNS servers
  - Authoritative server
    - BIND, which is used as authoritative server of .JP DNS
  - Cache server
    - BIND, dnscache and Windows DNS service, which is widely used in Japan

Our survey – Items of the 8bit label

- Can contain A and MX RRs
- Can zone transfer
- Can hold a lot of 8bit labels
- Can hold a long label (up to 63 octets)
- No influence to 7bit queries
- 8bit label and its masked 7bit label are distinguished completely
  - Both authoritative and cache server

Our results – 8bit label survey

- No problems were found for authoritative servers used in .JP DNS
  - Also no problems were found for NSD, tinydns (djbdns) and other versions of BIND
- No problems were found for **all** BIND (as a cache) available from ISC’s ftp site
  - Works fine even on BIND Version 4.8.3
  - Excluded non release (alpha, beta and RC) versions of BIND 9 series to decrease target (for time constraints)
- No problems were found for dnscache (djbdns)
- No problems were found for Windows DNS service (Windows 2000, 2000 SP4 and 2003) if 8bit label is UTF-8
  - Another encodings were not responded
- No problems were found for SOHO routers (NAT boxes) as far as availed

Current hot topic - Homograph attack

- Regarding “Phishing Fraud”
- Example:
  - http://www.paypal.com/ (correct URL)
  - http://www.p а ypal.com/ (This is Cyrillic character “ а ”)
- This is not Nameprep’ed / unified in IDN/Unicode specification

Homograph attack – cont.

- We already published a comment about this
  - "About Recent Articles Regarding Phishing Using Homographs among IDNs" - Countermeasures Already in Place, and .JP Follows Them -
  - http://jprs.co.jp/en/topics/050214.html
- We explained the following viewpoints
  - Root of the Problem
  - Existing Countermeasures Applied to IDN Registration by Domain Name Registries
  - Measures already taken in Japanese .JP domain name registration from its beginning
- Our summary
  - "In summary, the problem is rooted in IDN registration policies of each registry, but not in IDN-aware applications such as browsers. Japanese JP domain name, introduced taking into consideration of the above possible problems, can be used without too much worry."

ENUM

Review: What's ENUM?

- Telephone Number Mapping
- Translating E.164 numbers into names / services
- Example of E.164 number translation (described as RFC 2916)
  1. See that the E.164 number is written in its full form, including the countrycode IDDD. Example: +46-8-9761234
  2. Remove all non-digit characters with the exception of the leading '+'. Example: +4689761234
  3. Remove all characters with the exception of the digits. Example: 4689761234
  4. Put dots (".") between each digit. Example: 4.6.8.9.7.6.1.2.3.4
  5. Reverse the order of the digits. Example: 4.3.2.1.6.7.9.8.6.4
  6. Append the string ".e164.arpa" to the end. Example: 4.3.2.1.6.7.9.8.6.4.e164.arpa
- This is very similar to inverse mapping of domain name

Layer of ENUM services and standards

Communication service (multiple carriers)

Authentication, Social Security

Communication service (single carrier)

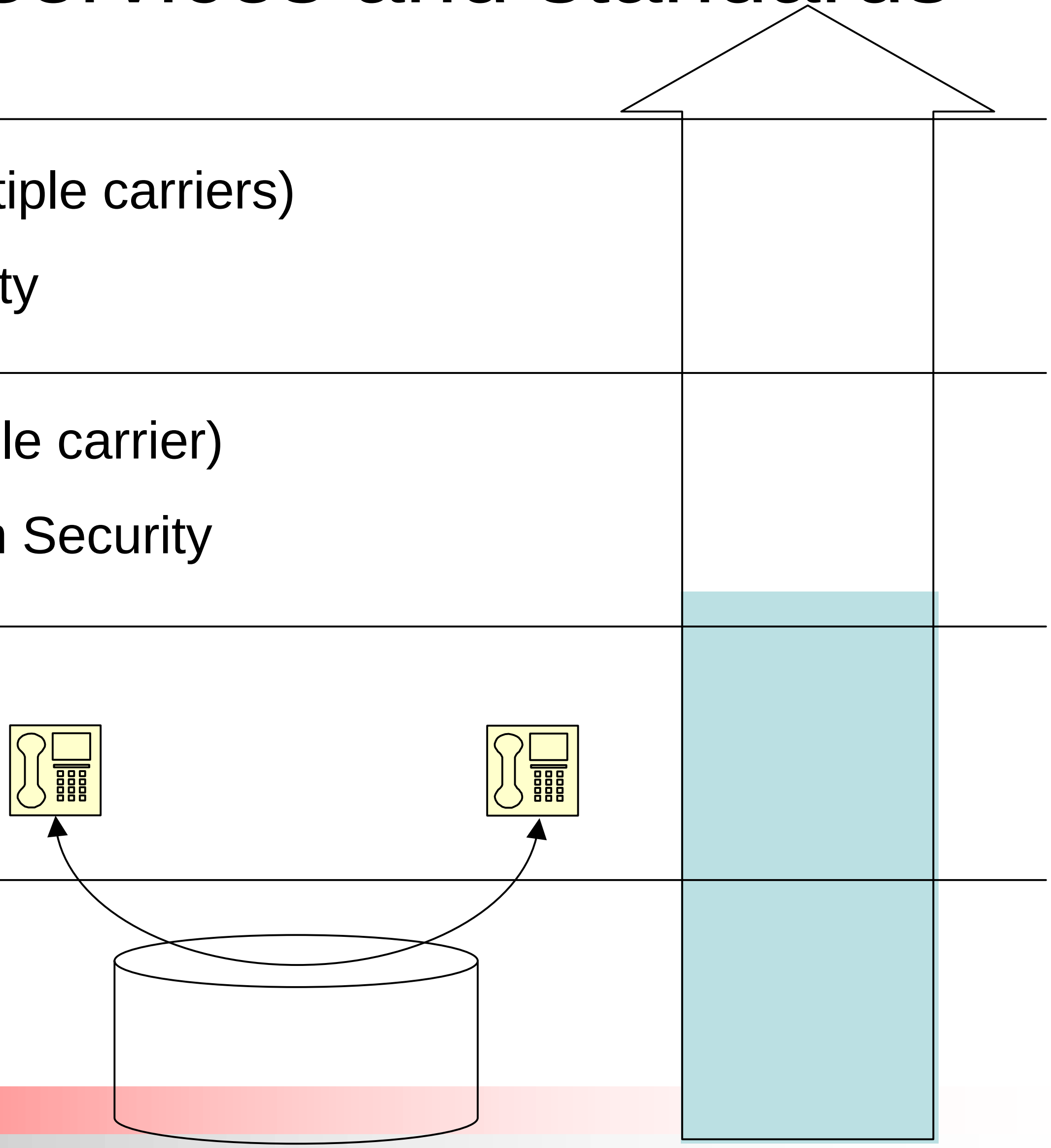
Provisioning, Communication Security

Applications/Terminals

SIP, Mail, Web, etc.

Infrastructure

ENUM DNS



DNS structure design for ENUM

- Depends on what model to select
  - User ENUM / Operator ENUM
  - Requirements (such as Number-Portability?)
- Typical requirements for Tier1 DNS:
  - Handling of large zone
    - even over 100M entries (if all the numbers are held in Tier1)
  - Scalability and stability
  - Performance
- Typical requirements for Tier2 DNS:
  - Capability for frequent update
  - EDNS0 support
    - To hold a number of NAPTR RRs for a single E.164 number that may exceed 512 octets in one DNS packet

Considerations on DNS

- Typical ENUM services like Web, Mail, SIP also lookup DNS
  - Web: Hyper-links (A)
  - Mail: sending (MX, A), receiving (PTR)
  - SIP: service protocol (D2U/D2T NAPTR), service location (SRV), sip server (A)
- The number of DNS queries will increase when ENUM is deployed
- Users are nervous about service quality
  - Users don’t care where the bottle neck is

Our experiences – ENUM study group

- Established in September 2002
  - http://www.nic.ad.jp/en/enum/index.html
- Objectives
  - Understanding the ENUM technology : desk work
  - Studying the implementation and operation of the ENUM–based system, and related matters
  - Finding political/regulatory issues related to ENUM-based implementation and operation
  - Finding technological issues related to ENUM
  - Clarifying pros and cons in ENUM usage
- Final report
  - Published in May 2003
    - http://www.nic.ad.jp/en/enum/ENUMReport.pdf

Our experiences – ENUM Trial Japan (ETJP)

- Established on 17 September 2003
  - http://etjp.jp/english/index.html
- Purpose
  - Perform ENUM trials to ensure functioning and feasibility of basic technical facility
  - Demonstration of technology for international use
  - Accumulation and sharing of know-how about ENUM
  - DNS operation for ENUM Trial
  - Feasibility test of communication applications (device, software) using ENUM
  - Feasibility test of communication services
- Results
  - Technical verification
    - Communication devices and software provided by participants
    - Communication services
  - Clarification and consideration of relevant issues

ETJP organization

- Participants
  - Companies, organizations, and individuals who hope to contribute to ETJP activities
  - Number of members: 45 (as of 21 February 2005)
- Officers
  - Chairman
    - Shigeki Goto
      Japan Network Information Center (JPNIC) / Waseda University
  - Vice chairman
    - Hirofumi Hotta
      Japan Registry Services Co., Ltd. (JPRS)
    - Yoshiki Ishida
      WIDE Project

ETJP working groups

- Privacy and Security WG
  - Objective
    - Discuss data treatment policy in each phase of trial and then publish guidelines
  - Milestone
    - Jan 2004: First draft, request for comments
    - Feb 2004: Second draft
    - Mar 2004: Publish guideline
- DNS WG
  - Objective
    - Definition of possible ENUM DNS models in Japan, their requirements and evaluation criteria, then evaluate current DNS implementations
  - Milestone
    - Feb 2004: Definition of possible ENUM DNS models, requirements, evaluation criteria
    - Mar 2004: Build Testbed, evaluation
    - Apr 2004: publish reports of the evaluation

Our experiences – ENUM Client/SDK

- Running under Microsoft Windows
  - Japanese and English version
    - Only different in messages
- ENUM Client
  - Source codes and client binary
- ENUM SDK
  - Runtime libraries (binary)
  - Sample codes (VC++, VB)
- All binaries and source codes are downloadable from JPRS Web site
  - http://jprs.co.jp/enum/software/software.html

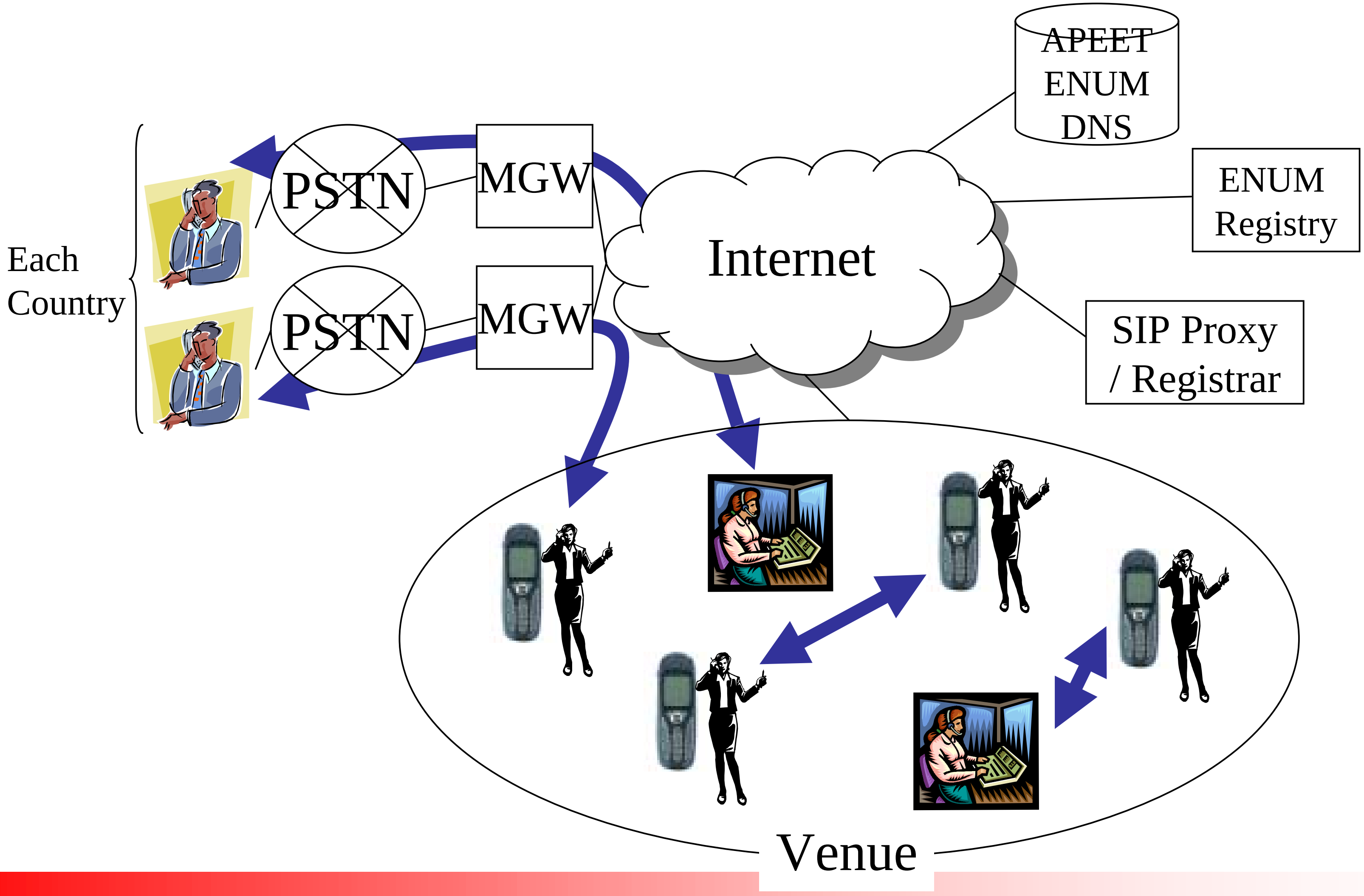
Our experiences - APEET

- Asia Pacific ENUM Engineering Team
- Established on July 19, 2004
  - – http://www.apenum.org/
- APEET operates ENUM-like DNS tree under apenum.org domain
- JPRS is a member of APEET

APEET ENUM/SIP Live Trial in APRICOT 2005

- https://apricot2005.apenum.org/ (Now we are open!)
- As a member of APEET (Asia Pacific ENUM Engineering Team), organized to promote ENUM trials in the region, JPRS offers a live trial (dynamic exhibition) of ENUM/SIP in the venue of APRICOT 2005
- The trial ranges from SIP communication services including overseas transmission and ENUM registration services
- APRICOT participants can join and experience the demonstration through using wireless SIP phones which can be borrowed or purchased at the venue

An image of APEET Live Trial



Conclusions and Future works

- The role of DNS in the Internet is more important
  - Therefore, DNS operators have more responsibility for stable Internet operation
- The demand about “cost” is also important
  - Not only money and server resources but also the human resources
- More usable and stable DNS services are needed
  - For example, updating more frequently the DNS data
- More technical experiences are needed
  - IP Anycast deployment
  - DNS Dynamic Update
  - DNSSEC

Questions / Discussions

JAPAN REGISTRY SERVICES

http://jprs.jp/tech/

Acknowledgements

- This presentation is included the research activities funded by National Institute of Information and Communications Technology (NICT).