HP WORLD 2004
Solutions and Technology Conference & Expo

Internet Services on HP-UX New Features and Future

Ebenezer Schubert/Senthil Kumar
Hewlett-Packard

Agenda

- Internet Services Features and Future
  - DHCPv6 – New on HP-UX
  - BIND
  - Sendmail – Anti Spamming in HP-UX
  - Multimedia Server Platform
  - Secured Internet Services
  - HP-UX IPv6 Routing
  - Q & A

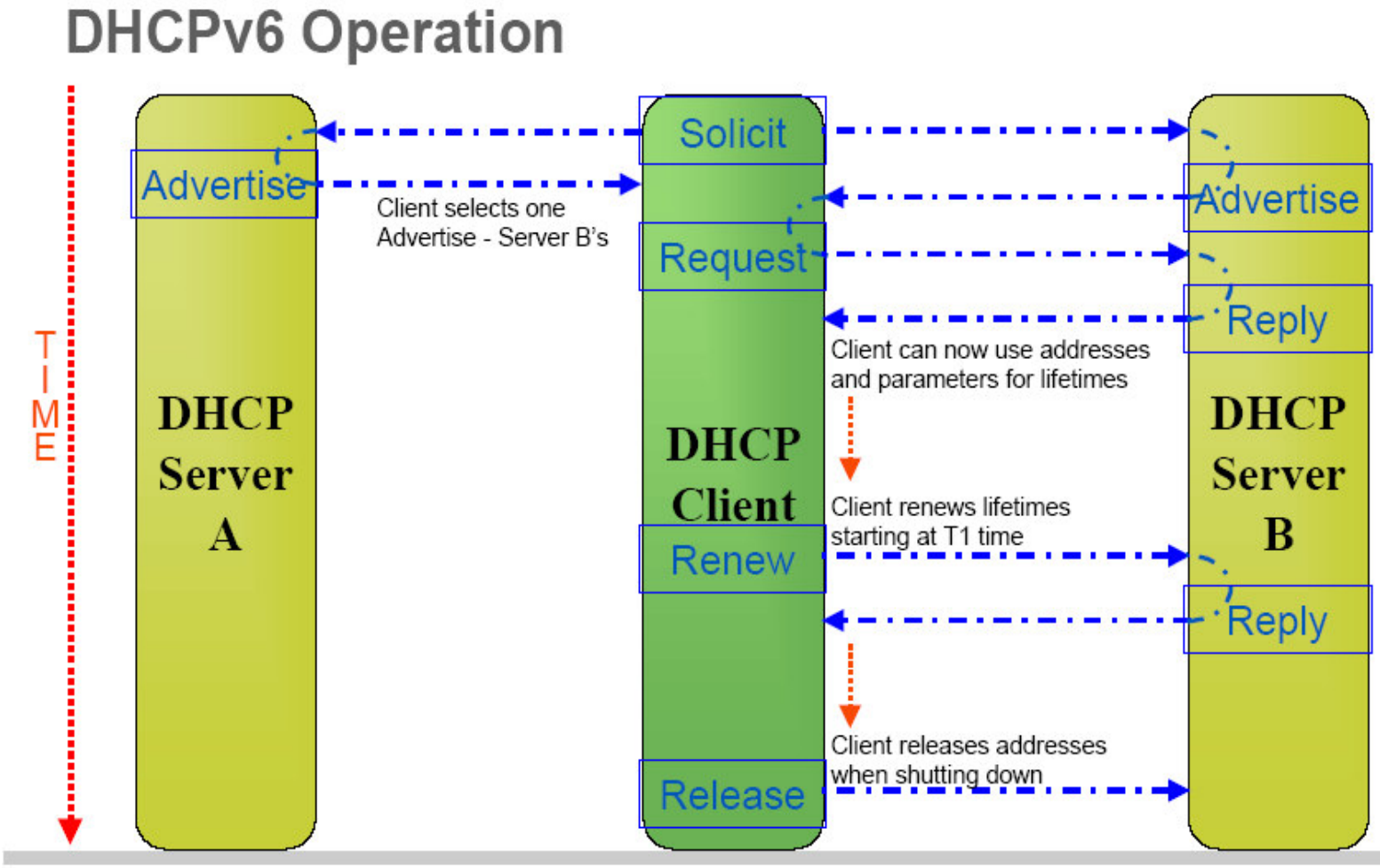
DHCPv6 Features

- Supports IPv6 addressing and configuration needs.It is the “stateful” auto-configuration protocol for IPv6.
- HP-UX DHCPv6 server is a multi threaded code and provides better performance.
- New Flexible packet format.
- 16-bit option space, 16-bit option lengths.
- Uses encapsulation (some messages/options encapsulate others).

DHCPv6 Features

- Client may obtain many addresses (not just one)
- Inherently supports Renumbering using server initiated message exchange (RECONFIGURE)
- Inherently supports Authentication.
- Globally Unique IDs for Client and Server – DUID
- Supports multiple prefixes for a link.
- Supports DNS, SIP and NIS Configuration using DHCPv6

DHCPv6 Basic Messages



DHCPv6 Future Roadmap

- Dynamic DNS support
- Time Configuration Support for DHCPv6
- Remote boot support in DHCPv6

BIND9 FEATURES

- Backend support for ENUM
- Support for EDNS
- IPv6 Support
- Security - TSIG & DNSSEC
- Dynamic Update
- Notify
- Incremental Zone Transfer
- Forwarders
- Support for Views

Security - TSIG

- BIND 9 introduced a new mechanism for securing DNS messages called Transaction Signatures.
- TSIG uses shared secrets and a one-way hash function to authenticate DNS messages, particularly responses and updates.

Security - DNSSEC (DNS-Security Extensions)

- The DNS Security Extensions (RFC 2535), use public key cryptography to enable zone administrators to digitally sign their zone data, thereby proving its authenticity.
- BIND implements KEY,SIG and NXT RR types to support DNSSEC.
- Also BIND distribution provide a set of tools for the key manipulation (dnssec-keygen,dnssec-keycreate,dnssec-makekeyset,dnssec-signzone)

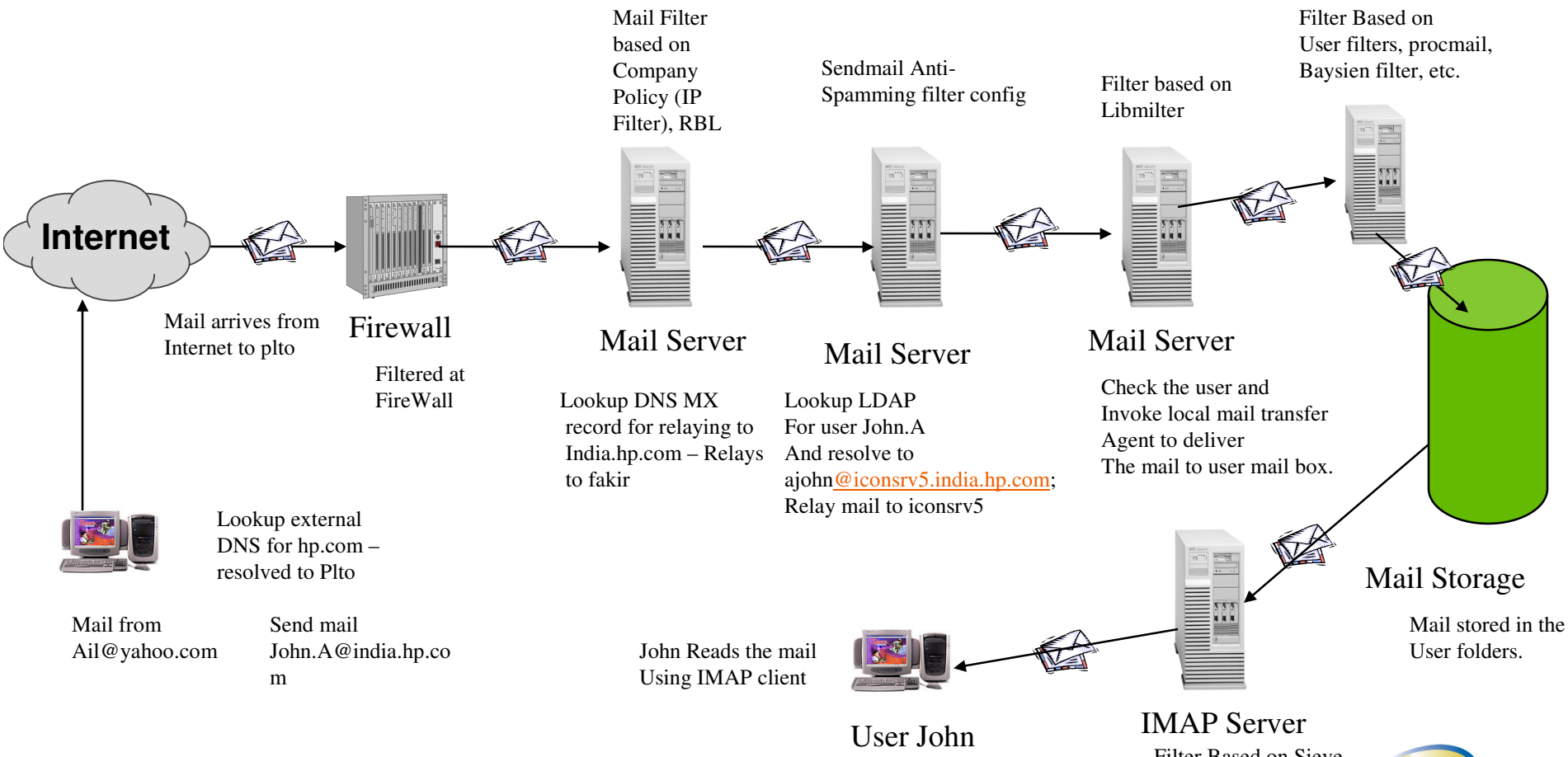
Anti spamming in Sendmail

- Today's e-mail world strives to get rid of unsolicited messages -- Spam.
- HP-UX provides an environment in which unsolicited e-mail is controlled efficiently and effectively.
- Rules to filter unsolicited e-mail
- Rules that include control of blacklist recipients, SMTP headers, message contents and attachments.
- HP-UX anti-spamming features not only reject unsolicited e-mails, they also provide a method to modify or further process the received messages.

Anti spamming in Sendmail

- The dynamic nature of these rules gives customers the flexibility of controlling unsolicited e-mail at various phases of the SMTP transaction and it also allows customers to organize their messages on the server-side itself, which saves bandwidth and the amount of time usually spent transferring messages from the server to a client.

Spam Filter


Internet
Mail arrives from Internet to plto
Firewall
Filtered at FireWall
Mail Filter based on Company Policy (IP Filter), RBL
Mail Server
Lookup DNS MX record for relaying to India.hp.com – Relays to fakir
Sendmail Anti-Spamming filter config
Mail Server
Lookup LDAP For user John.A And resolve to ajohn@iconsrv5.india.hp.com; Relay mail to iconsrv5
Filter based on Libmilter
Mail Server
Check the user and Invoke local mail transfer Agent to deliver The mail to user mail box.
Filter Based on User filters, procmail, Baysien filter, etc.
Mail Storage
Mail stored in the User folders.
IMAP Server
Filter Based on Sieve.
User John
John Reads the mail Using IMAP client
Lookup external DNS for hp.com – resolved to Plto
Mail from Ail@yahoo.com
Send mail John.A@india.hp.com

Messaging future roadmap.

- Scalable & Secure Mail server
- Strong anti-spamming & virus scan solutions (libmitter, sieve).
- Supported access protocols for Mobile access
- Robust message archiving solution
- Instant messaging solution (jabber).
- Kernel based anti-spam filter.

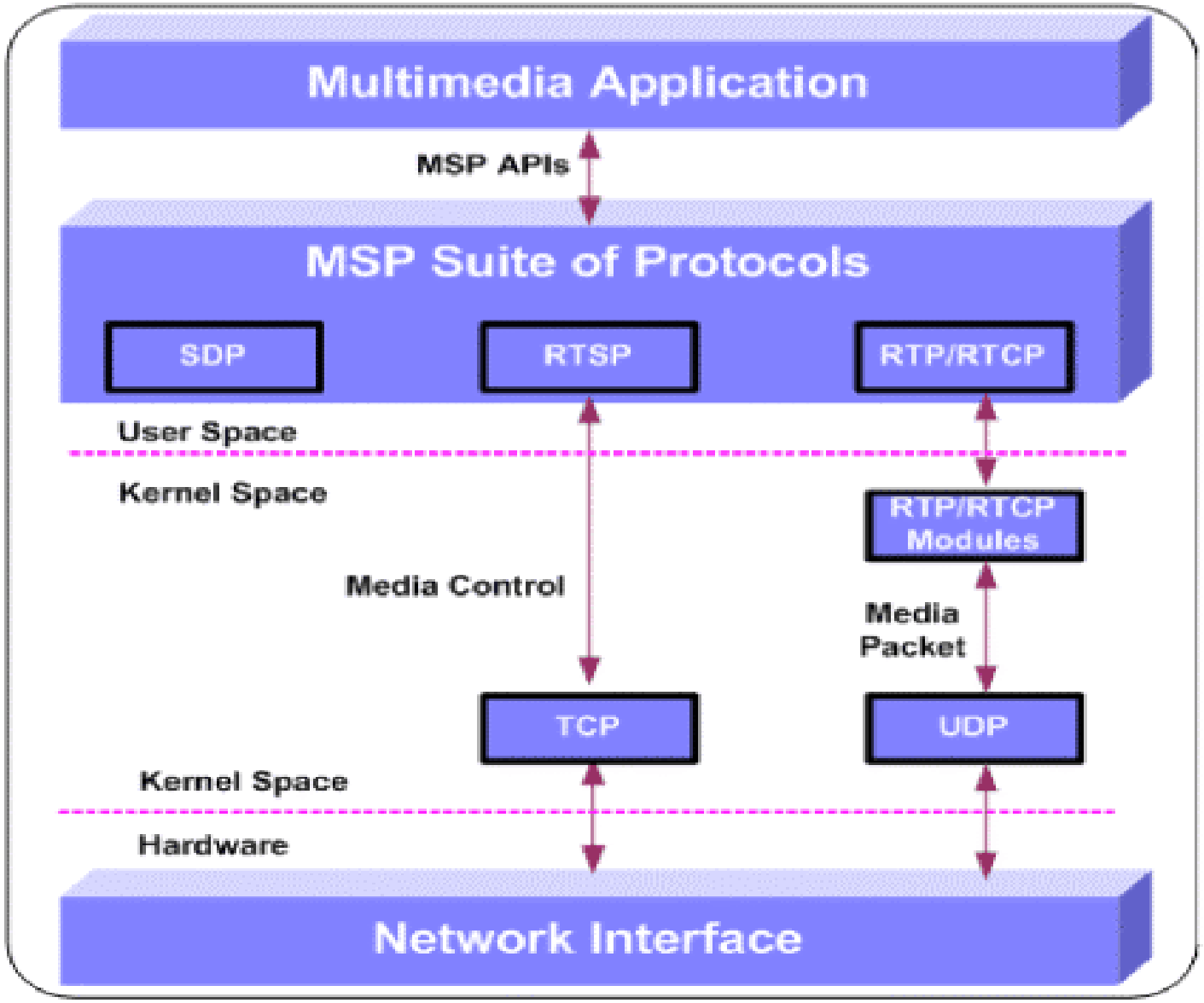
MSP Platform

- Multimedia Streaming Protocols (MSP) enables you to transfer audio and video files to a remote location in real time.
- Unlike the download-and-play mechanism, the multimedia streaming client starts playing the media packets as soon as they arrive, without holding back to receive the entire file.

MSP – What does HP-UX Provide

- The MSP framework for HP-UX multimedia streaming servers comprises libraries required for implementing these protocols and transmitting real-time data.
- These libraries use underlying transport mechanisms, such as TCP and UDP, to deliver services.
- The MSP implementation on HP-UX offers high performance and enables you to take advantage of the scalability, reliability, and high availability of the HP-UX operating system.

MSP Platform



MSP Platform

- Real Time Transfer Protocol (RTP) is a transport protocol that provides end-to-end network transport functions for applications transmitting data with real-time properties, such as interactive audio and video.
- RTP consists of Real-Time Control Protocol (RTCP), a closely linked protocol, which provides a mechanism for reporting feedback on the transmitted real-time data.
- Real Time Streaming Protocol (RTSP) controls the transfer of real-time media data and serves as a network-remote-control for multimedia sessions.
- Session Description Protocol (SDP) describes the general real-time multimedia sessions

MSP Platform

- Download and Use it for Free

http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=MSP

The MSP SDK on HP-UX 11i v1 conforms to the following RFCs:

- RFC 1889 - RTP: A Transport Protocol for Real-Time Applications
- RFC 2326 - Real Time Streaming Protocol (RTSP)
- RFC 2327 - SDP: Session Description Protocol

Secured Internet Services

- Secure Internet Services (SIS) is an optionally enabled mechanism that incorporates Kerberos V5 authentication and authorization for remote access services: ftp, rcp, remsh, rlogin, and telnet.
- The main advantage is that if you are running SIS, your security is enhanced because authorization is no longer required for transmitting a password in a readable form over the network..

What is Kerberos

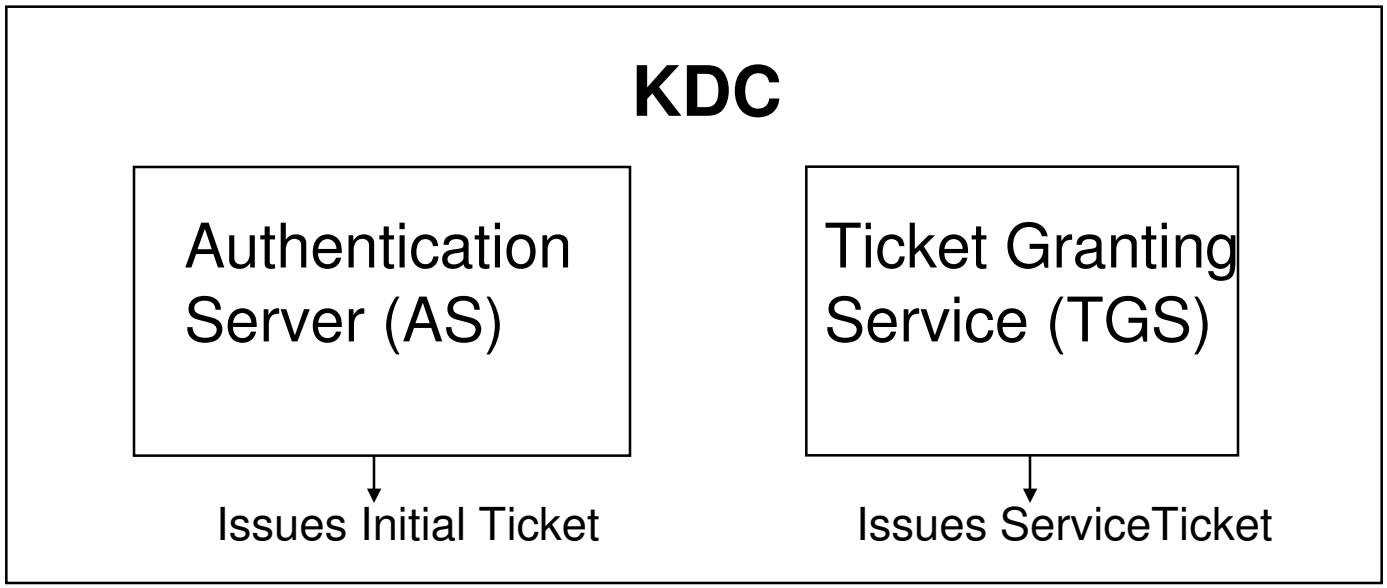
- Kerberos is an authentication protocol designed to allow users and application services to authenticate themselves.
- The Kerberos authentication protocol is based on the Kerberos authentication system developed at MIT

Kerberos System Building Blocks

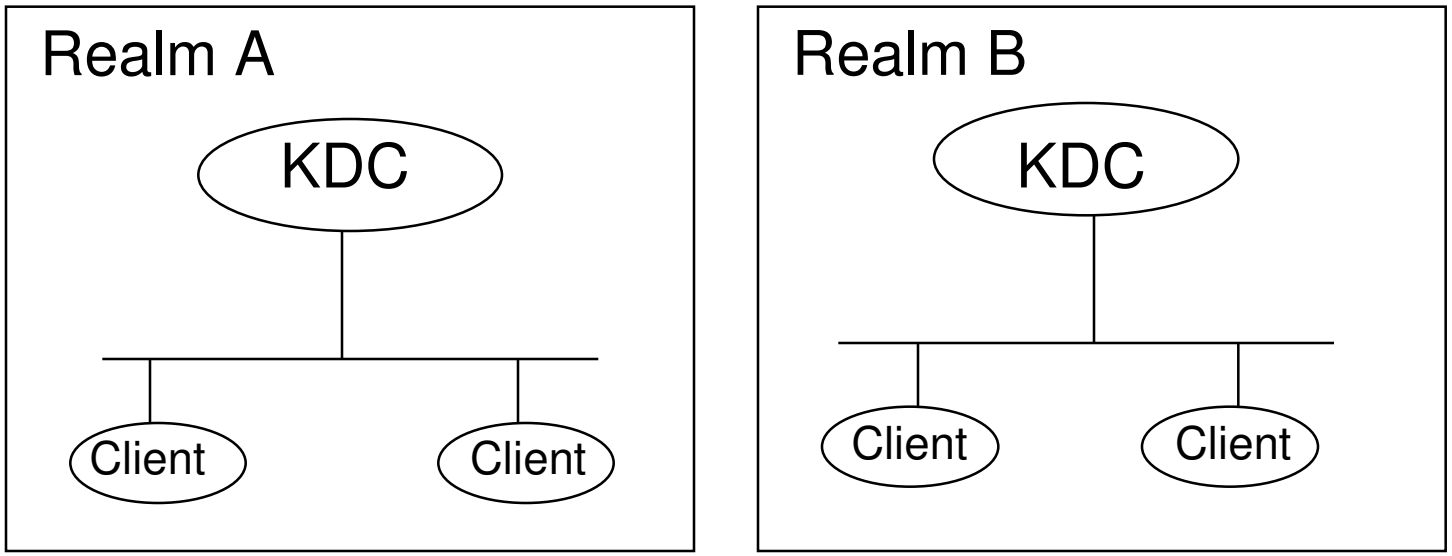
- Key Distribution Center
- Realm
- Principal
- Tickets

Key Distribution Center

This comprises of:



Realm



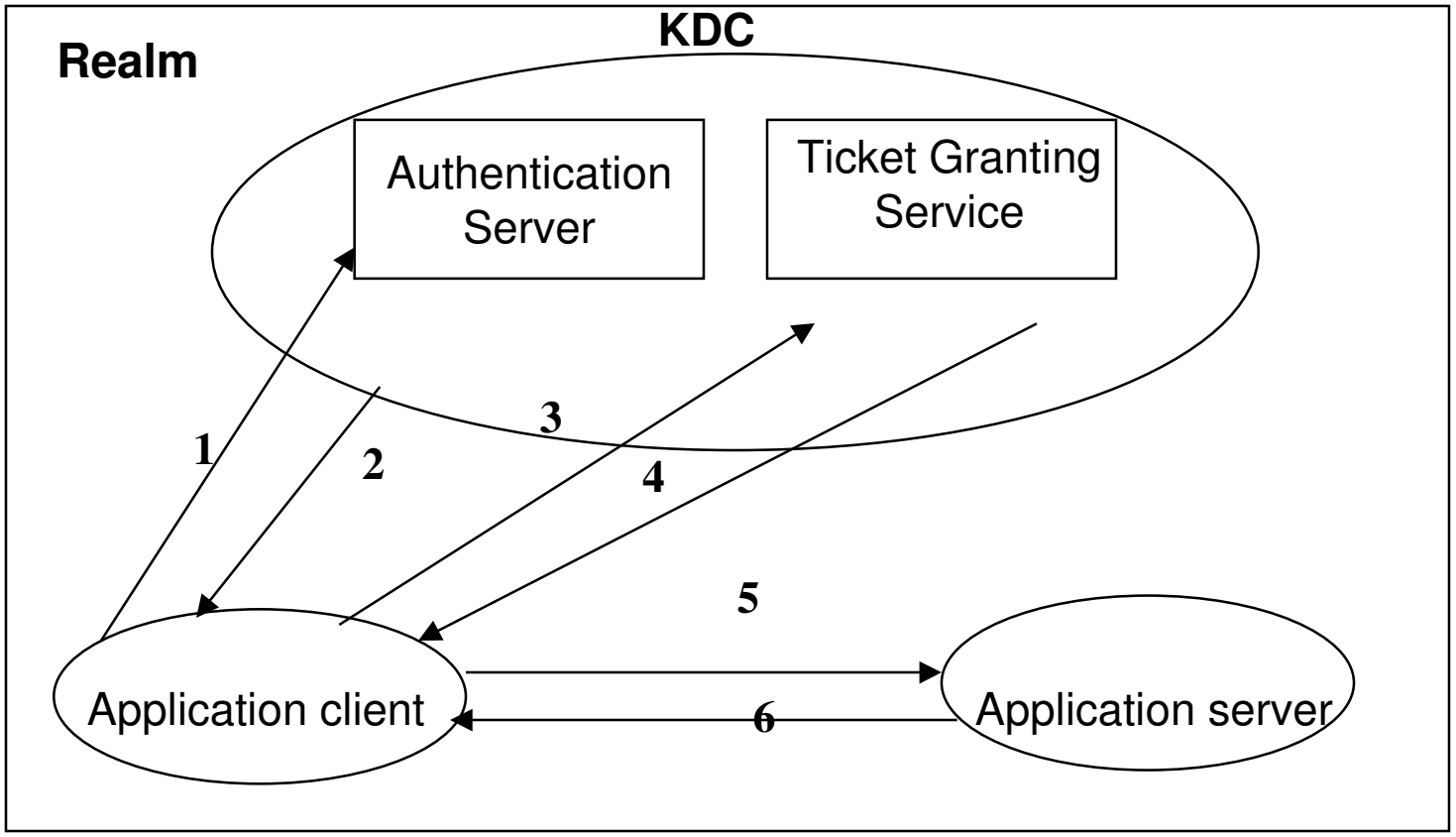
Principals

- Principals are unique names for users or services and are created in the Kerberos database
  - **User Principal** – A user principal is associated with a user
  - **Service Principal** – A service principal is associated with a particular service
  - **Special Principals** - Principals created automatically when the Kerberos database is created

Tickets

- A ticket is a record that helps a client to authenticate itself to a server.
- The two types of tickets are:
  - Ticket Granting Ticket (TGT) – An initial ticket obtained from the Authentication Server (AS) and later used to allow a client to obtain Service Tickets
  - Service Ticket – A ticket obtained from the Ticket Granting Service (TGS) to access the other services across the network

How Kerberos Works?



1. Request for TGT
2. Receive TGT
3. Request for Service Ticket
4. Receive Service Ticket
5. Request for a Service
6. Receive authenticator (optional)

Reference

- RFC 1510 - The Kerberos Network Authentication Service (v5)
- MIT Kerberos V5 UNIX User's Guide

  http://www.nrl.navy.mil/ccs/help/kerberos/kerb-user-guide.html
- Kerberos: An Authentication Service for Open Network Systems

  ftp://ftp.pdc.kth.se/pub/krb/doc/kerberos.ps

Secured Internet Services

The following steps describe how to use SIS:

- Identify yourself to the Security Server, also known as the KDC (Key Distribution Center), by issuing the kinit command:
  - **kinit user_name@realm_name**
- To identify yourself to an HP DCE Security Server, you would generally use the dce_login command rather than kinit. To identify yourself to an HP Praesidium/Security Server (P/SS), use the dess_login command.

Secured Internet Services

- Start any service (ftp, rcp, remsh, rlogin, or telnet) using the same method with which you start the non-secure version of the service. The following example starts ftp:
  - **ftp remote_host_name**
- If you are using SIS, ftp does not prompt for a user name and password.
- After working with the secure session, issue the kdestroy command to remove the credentials that you have accumulated during the session:
  - **kdestroy**

Secured Internet Services

- If the SIS product is installed and enabled on your system, you can refer to the following man pages for more information:
- For information common to all the Secure Internet Services, including warning and error messages, type man 5 sis at the HP-UX prompt.

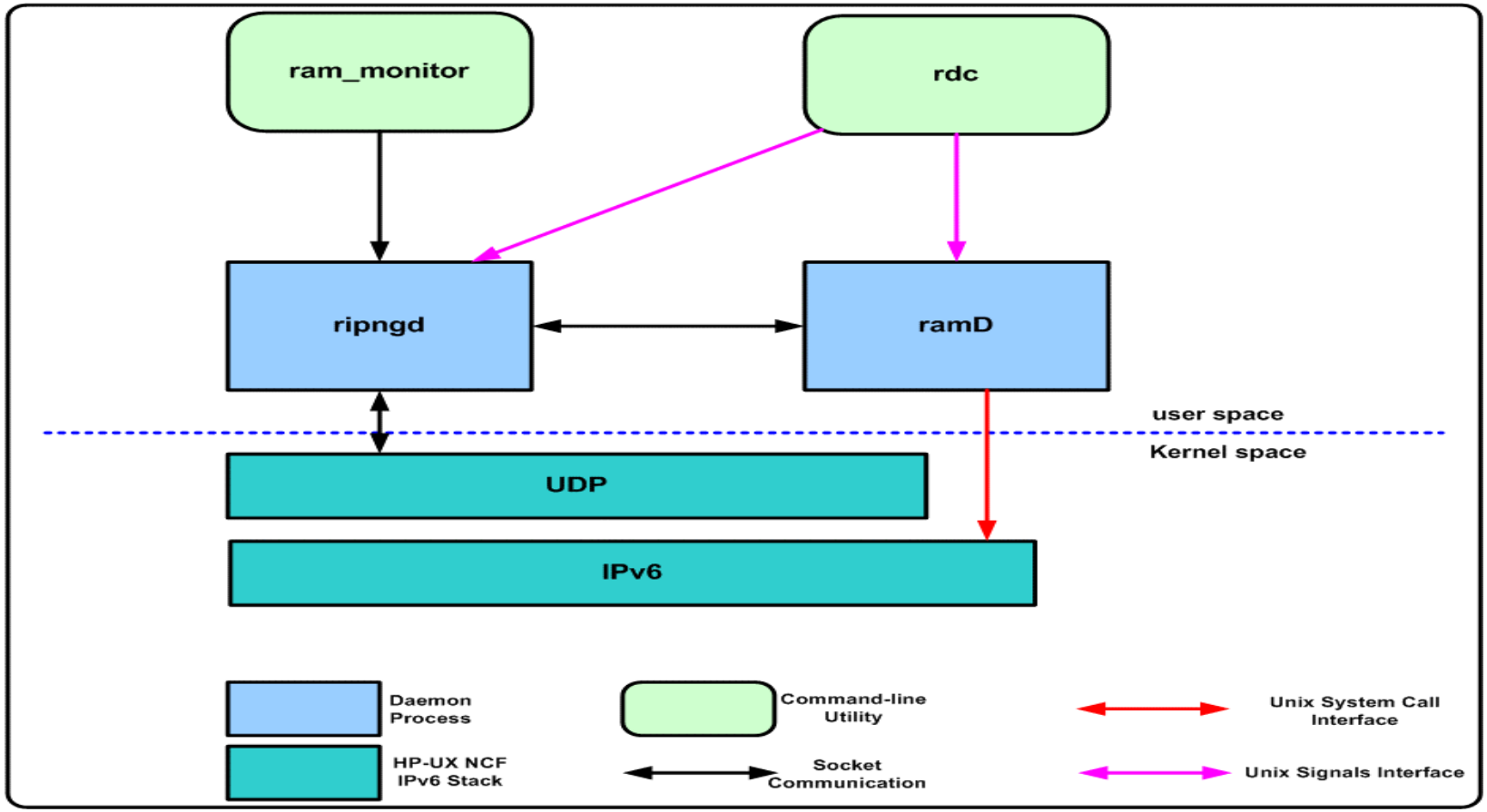
Secured Internet Services

- For information specific to individual services, type man 1 ftp, man 1M ftpd, man 1 rcp, man 1 remsh, man 1M remshd, man 1 rlogin, man 1M rlogind, man 1 telnet, man 1M telnetd, or man 5 sis at the HP-UX prompt.
- For information on some common Kerberos utilities, type man 1kinit, man 1 klist, man 1 kdestroy, man 1M krbval, man 8sec k5dcelogin, man 1M inetsvcs_sec, or man 4 inetsvcs at the HP-UX prompt.

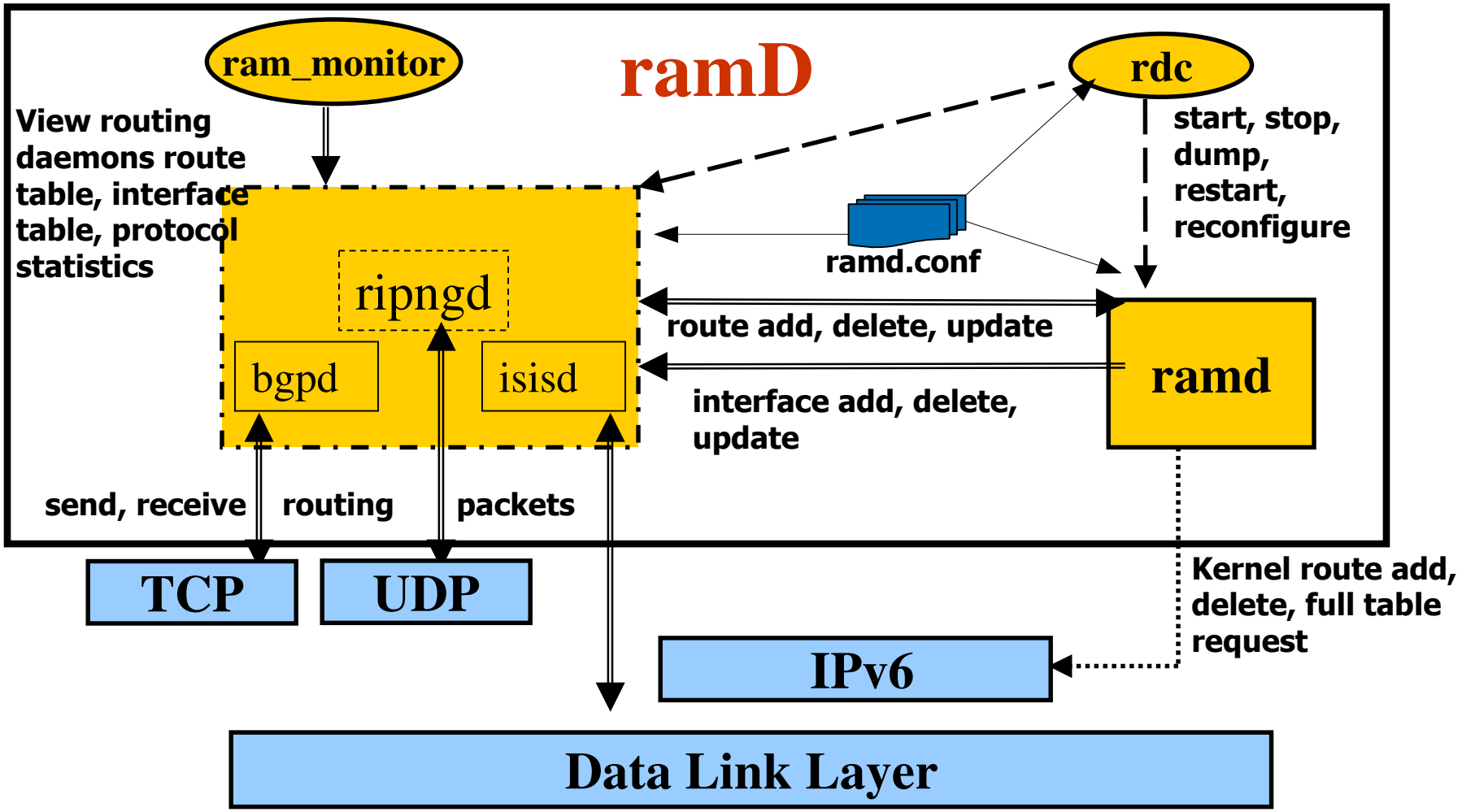
Router Administration Manager (ramD)

- It is the routing daemon that handles the following Internet Protocol version6 (IPv6) routing protocols.
  - BGP4+
  - RIPng
  - IS-IS for IPv6

RAMD Architecture



Route Administration Manager Daemon (ramD) Architecture



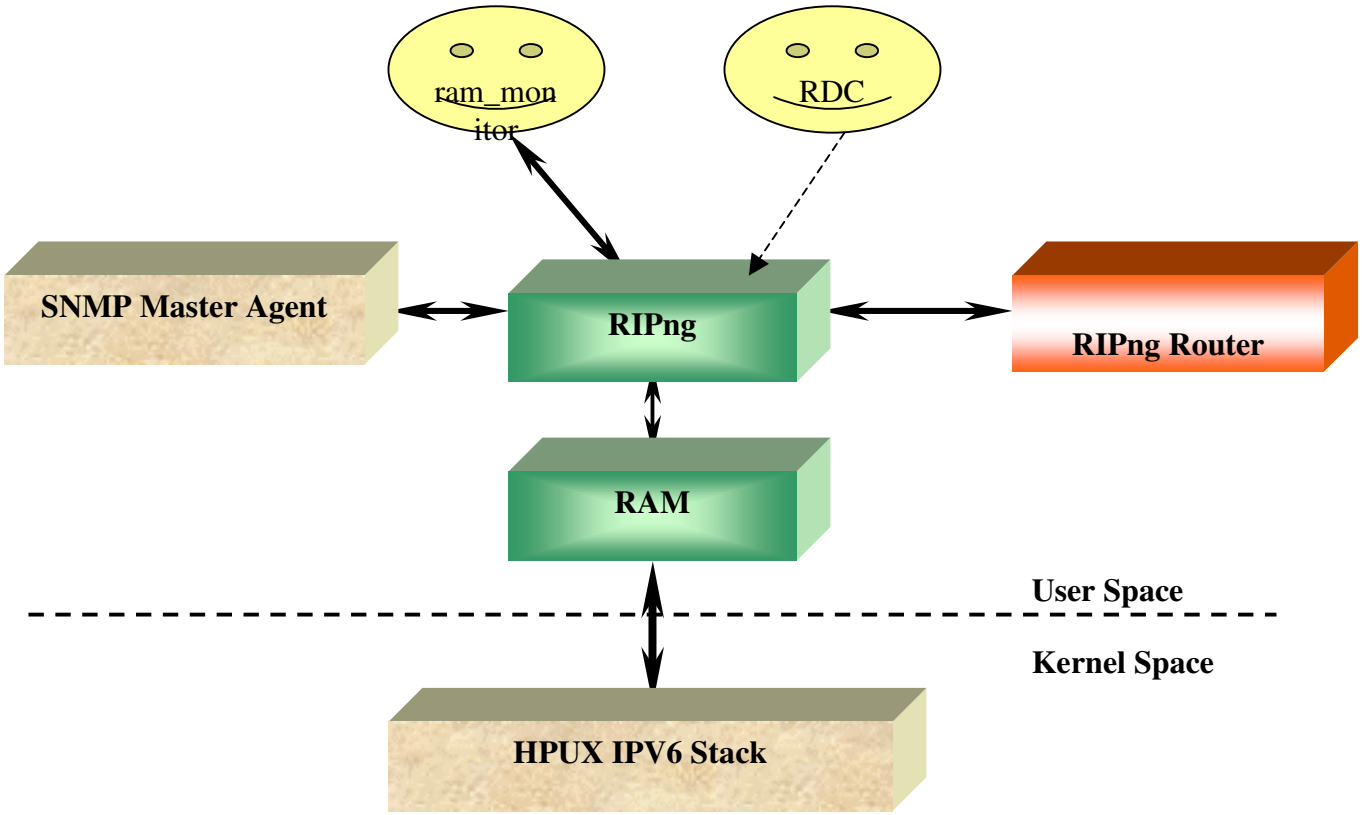
RIPng (RIP – Next Generation)

- IGP – Interior Gateway Protocol
- Belongs to the distance vector class
- Protocol is similar to RIPv2.

RIPng (RIP – Next Generation).

- Important requirement for immediate deployment of IPv6
- Next-hop limit of 15
- Uses UDP port 521and the multicast address ff02::9
- New feature: Next-hop RTE

RIPng Architecture



BGP Protocol Overview

Why BGP ?

- Network scaling
- Multi-homing (connecting to multiple providers)
- Policy discrimination
  Controlling how the traffic flows

BGP Protocol Overview (Contd..)

- IETF RFC 1771 defines Border Gateway Protocol
- Used between Inter & Intra Autonomous System (AS)
- Runs over Transmission control protocol (TCP) port 179
- Uses Autonomous system (AS) path information as metric
- Uses path vector algorithm to determine the best route to as destination
- Learns only IPv6 route information
- Uses the neighboring routers as peers

BGP Protocol Overview (Contd..)

- Exchanges route open, Keep alive,update & notification packets with neighbors

  - Open is used to exchange configuration information and to negotiate common parameters for the peering session.

  - UPDATE messages are used to distribute the routing information

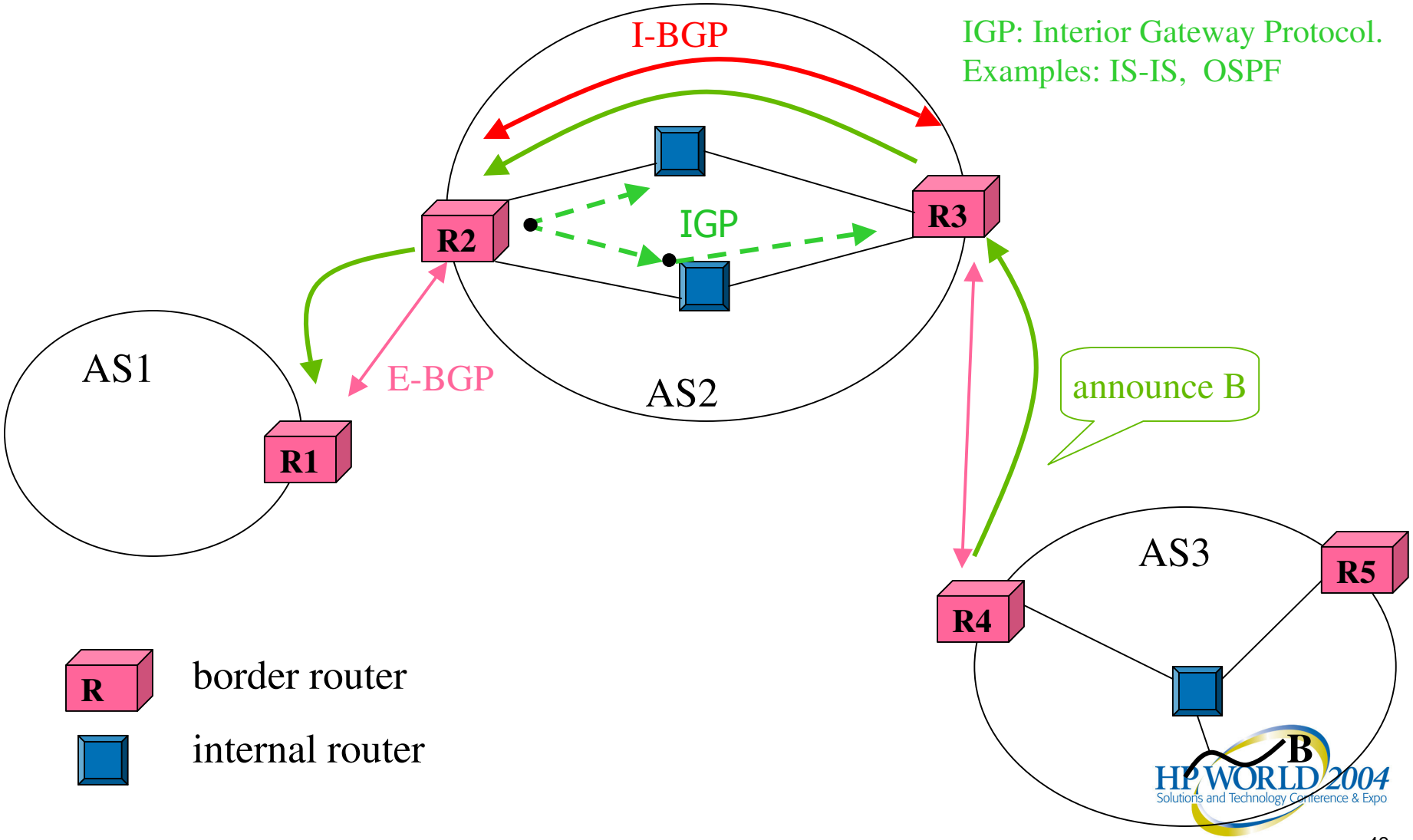
  - KEEPALIVE messages are sent periodically to keep the BGP session alive

  - NOTIFICATION message is sent when BGP detects an error condition , after which the peering session is terminated

BGP Protocol Overview (Contd..)

- Supports MD5 authentication (Message Digest)
- Enforces policy decisions on routes learnt
- Installs the best route in the BGP routing table
- SNMP support.

BGP Protocol Overview (Contd..)



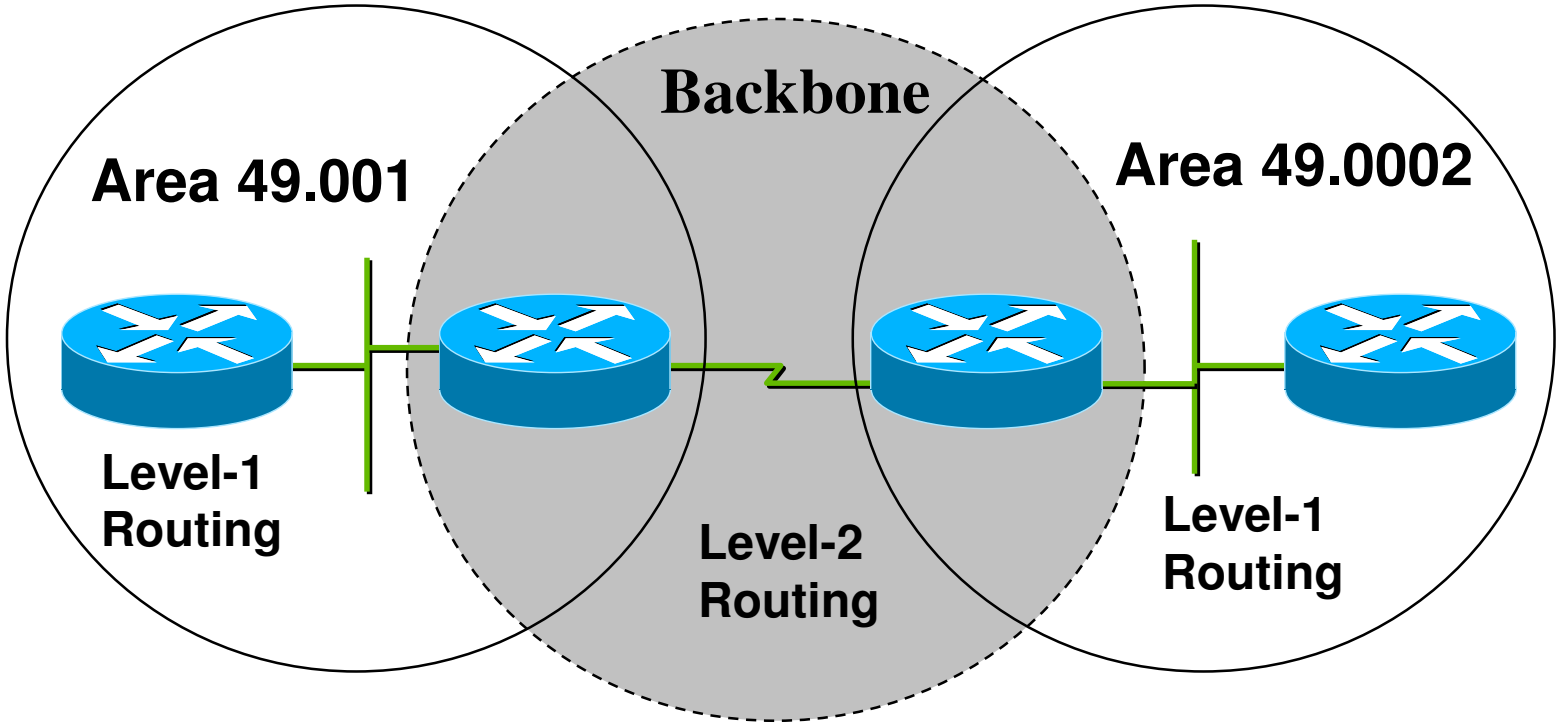
IS-IS Protocol Overview

- Intermediate system (IS) - Router
- IS0 10589 defines the IS-IS routing protocol for Connectionless Network Service (CLNS) traffic. IETF RFC 1195 adds IP support also known as integrated IS-IS. IETF draft RFC draft-ietf-isis-ipv6-03.txt defines support to IPv6 on IS-IS.
- IS-IS was originally devised as a routing protocol for CLNP, but has been extended to include IP routing (Integrated IS-IS)
- Used as a Interior Gateway protocol
- Link state routing protocol that runs over data link layer

IS-IS Protocol Overview (contd..)

- Exchanges route IIH, LSP, CSNP, and PSNP PDUs with neighbors
- Learns only IPv6 route information
- Uses Shortest-Path First Algorithm (SPF) to determine the best route to a destination
- Installs the best route that satisfy particular criteria in the IS-IS routing table
- Supports SNMP

IS-IS Protocol Overview



- Provides a multi-level hierarchy (two-level for IS-IS) called "area routing“
- Routing domain is carved into areas. Routing in an area is level-1. Routing between areas is level-2

IS-IS Protocol Overview

- IS-IS Hello Packets (IIH)
  - Level 1 LAN IS-IS Hello
  - Level 2 LAN IS-IS Hello
  - Point-to-point Hello
- Link State Packets (LSP)
  - Level 1 and Level 2
- Complete Sequence Number packets (CSNP)
  - Level 1 and Level 2
- Partial Sequence Number Packets (PSNP)
  - Level 1 and Level 2

IS-IS Protocol Overview

- Timers used
  - Adjacency Related
    - Hello Timer
    - Holding Timer
  - LSP Related
    - MinLSPTxTimer
    - MinLSPGenTimer
    - MinSPTTimer
    - WaitingTimer
    - SNPTimer
    - MaxAgeTimer
    - ZeroAgeTimer

IS-IS Protocol Limitations

- Does not scale well as more routers are added to the routing domain.

IS-IS for IPv6

- Runs over data link layer
- Uses Shortest Path Algorithm (SPF), also known as Djikstra's algorithm, to compute its routing algorithm by selecting the best path in the network. It builds the shortest path tree by calculating routes to all designated networks. SPF runs over Level 1 and Level 2 database separately
- Send hello packets out on all IS-IS enabled interface to discover neighbors and establish adjacencies.

IS-IS for IPv6

- Routers of IS-IS become neighbors if the hello packets contain information that meets the criteria to form an adjacency. The criteria differs depending on the media that IS-IS uses. The main criteria are matching authentication, IS type and Maximum Transmission Unit (MTU) size
- Builds a Link-State Packet (LSP) that communicates the reachability information to adjacent routers

IS-IS for IPv6

- Floods all adjacent neighbors with LSPs except the router that sent the same LSP. However, there are different forms of flooding and a number of scenarios in which the flooding operation can differ.
- Constructs the link-state database from the LSPs
- Routers provide the best path to ramD for updating the IP routing table

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP

RECOMMENDED TRAINING VENUE FOR THE

HP Certified Professional