APNIC Training

Introduction to Internet Operation

28 January 2010 – Dhaka, Bangladesh

15 South Asian Network Operators Group (SANOG) Conference

SANOG

In conjunction with ISPAB

APNIC
Asia Pacific Network Information Centre

Introduction

- Presenters
  - Nurul Islam Roman
    - Technical Training Officer
    - nurul@apnic.net
  - Jeffrey Tosco
    - Training Office
    - jeffrey@apnic.net

Assumptions & Objectives

Assumptions

- Entry/Mid level engineers working in ISP/service provider network
- Are not familiar or up-to-date with technology detail
- Has not got advance experience to work with network equipment
- Are interested in Internetworking technologies

Objectives

- To provide an understanding of current Internet protocols
- To provide a working knowledge of the procedures managing Internet
- To keep up updated knowledge of future Internet technology

Overview

- Introduction to Internet Operation
  - Internet Protocols – some revision
  - IP addressing basic
  - IP Routing basic
  - Introduction to DNS & RevDNS
  - Infrastructure Security Fundamental

APNIC Asia Pacific Network Information Centre

Overview

- Introduction to Internet Operation
  - **Internet Protocols – some revision**
  - IP addressing basic
  - IP Routing basic
  - Introduction to DNS & RevDNS
  - Infrastructure Security Fundamental

APNIC Asia Pacific Network Information Centre

Signal, Data and Information

- Data is transmitted over a physical network as a sequence of binary digits (bits - 0s and 1s).
- The "sending" process involves the source device generating a pattern of signals (voltages, light patterns, wavelengths).
- The pattern of signals generated represents the sequence of bits making up the data.
- These signals can be "read" by any device attached to the same physical network.
- "Reading" means identifying the signals to receive the same pattern of bits as generated by the sender.

APNIC Asia Pacific Network Information Centre

What is Protocols

- All data is transmitted in the same way irrespective of what the data refers to, whether it is clear or encrypted.
- The data communication protocols define the structure or pattern for the data transferred – this gives it its meaning.
- The Protocols define
  - *functions* or *processes* that need to be carried out in order to implement the data exchange and the
  - *information* required by these processes in order for them to accomplish this

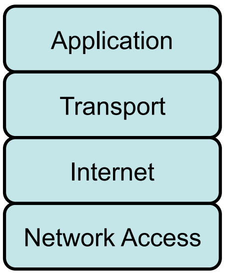
The OSI Model

Application	Access to the network
Presentation	Manipulate data (Translate, encrypt)
Session	Manage sessions (connections)
Transport	Provide reliable delivery
Network	Internetwork - move packets from source to destination
Data Link	Configure data for direct delivery by physical layer
Physical	Physical delivery - electrical specs etc

Protocol Models

- In the late 1970s the ISO (International Standards Organisation) introduced a model defining the functions for data communications between two computers in a 7 layer model - The OSI (Open System Interconnection) Model
- Not a protocol but a framework intended to facilitate the design of protocols for inter-computer communication.
- Defines the processes required at each of the modularised layers
- OSI is “protocol independent”

The Four Layers of TCP/IP

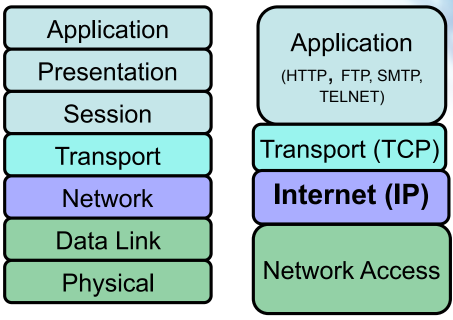


TCP/IP and the OSI Model

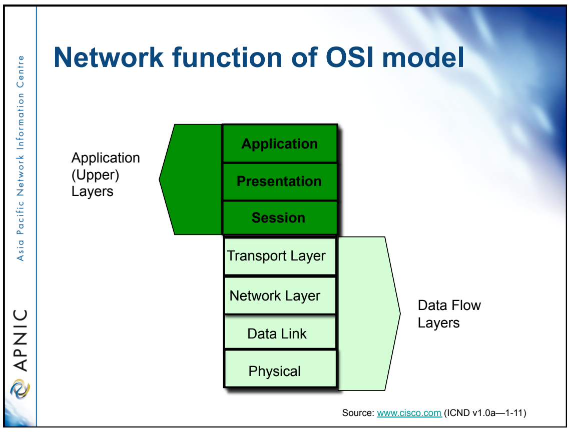
- TCP/IP was created before the OSI model
- It is a layered protocol implementation
- Its layers do not match the OSI model exactly, but the processes defined in the OSI model are contained in the TCP/IP layers

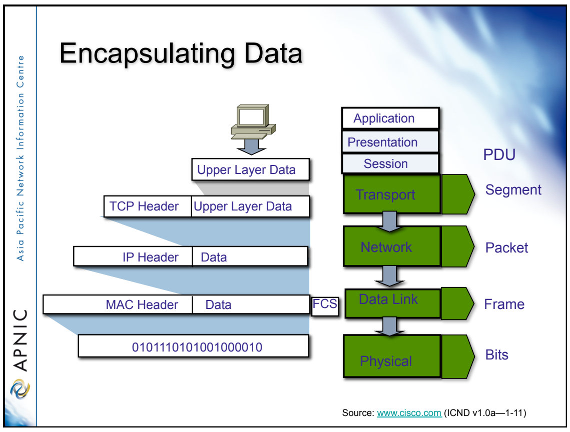
APNIC Asia Pacific Network Information Centre

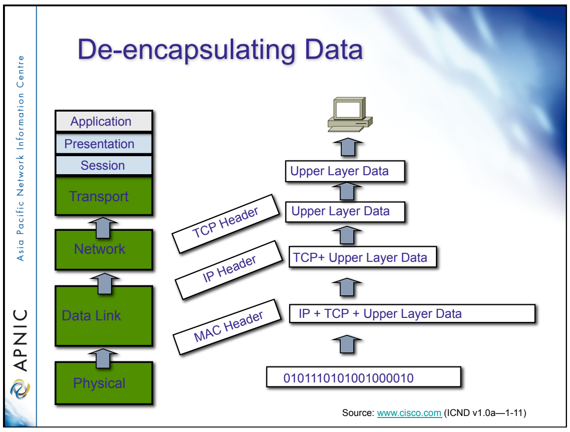
The OSI Model and TCP



APNIC Asia Pacific Network Information Centre


Network function of OSI model
Asia Pacific Network Information Centre
APNIC
Application (Upper) Layers
Application
Presentation
Session
Transport Layer
Network Layer
Data Link
Physical
Data Flow Layers
Source: www.cisco.com (ICND v1.0a—1-11)


Encapsulating Data
Asia Pacific Network Information Centre
APNIC
Upper Layer Data
TCP Header
Upper Layer Data
IP Header
Data
MAC Header
Data
FCS
0101110101001000010
Application
Presentation
Session
Transport
Network
Data Link
Physical
PDU
Segment
Packet
Frame
Bits
Source: www.cisco.com (ICND v1.0a—1-11)


De-encapsulating Data
Asia Pacific Network Information Centre
APNIC
Application
Presentation
Session
Transport
Network
Data Link
Physical
Upper Layer Data
TCP Header
Upper Layer Data
IP Header
TCP+ Upper Layer Data
MAC Header
IP + TCP + Upper Layer Data
0101110101001000010
Source: www.cisco.com (ICND v1.0a—1-11)

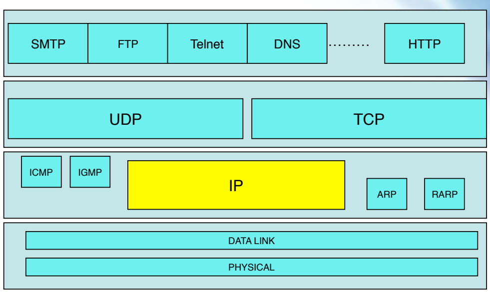
Packets

- A packet then contains a set of data made of the various headers from each layer including the data generated by the application layer.
- The packet is "built" during a sending process when each layer determines the information needed for its tasks, and adds this header information
- The layer will then take this information, with any other data it might have received from a higher layer, and pass it as one set of data to a lower layer.
- This process is then repeated and is called *encapsulation*

Internet Protocol (IP)

- IP is an unreliable, connectionless delivery protocol
  - A best-effort delivery service
  - No error checking or tracking (no guarantees – Post Office)
  - Every packet treated independently
    - Can follow different routes to same destination
  - IP leaves higher level protocols to provide reliability services (if needed)
- IP provides three important definitions:
  - basic unit of data transfer
    - specifying exact format of the headers
  - routing function
    - choosing path over which data will be sent
  - rules about delivery
    - how IP datagrams should be processed
    - how to deal with unusual events (errors)

TCP/IP Protocol Structure



From Forouzan

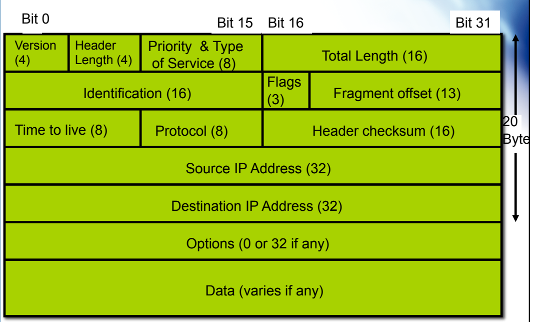
IP Datagram format

- That part of a packet containing the IP headers and the data from the higher layers passed to the IP layer are called ***datagrams***
- IP specifies the header information for the data it requires for its tasks - information needed for routing and delivery
  - eg source and destination IP addresses
- It has nothing to do with higher layer headers or data and can transport arbitrary data

Datagram header	Datagram data area

Asia Pacific Network Information Centre
APNIC

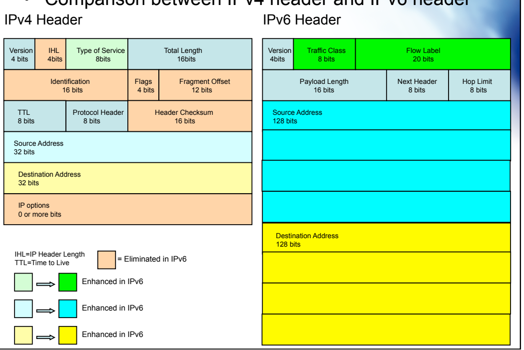
IPv4 Datagram header fields



Asia Pacific Network Information Centre
APNIC

IPv6 header

- Comparison between IPv4 header and IPv6 header



Asia Pacific Network Information Centre
APNIC

Questions?

Overview

- Introduction to Internet Operation
  - Internet Protocols – some revision
  - **IP addressing basic**
  - IP Routing basic
  - Introduction to DNS & RevDNS
  - Infrastructure Security Fundamental

Overview

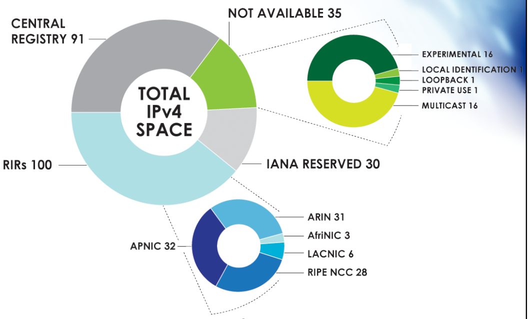
- IP addressing Issues and solution
- Variable Length Subnet Mask (VLSM)
  - Written exercise : VLSM calculation
- Summarisation of routes
- Classless InterDomain routing (CIDR)
- Internet registry IP management procedure
  - Written exercise : Route summarisation

IP Addressing issues

- Exhaustion of IPv4 addresses
  - Wasted address space in traditional subnetting
  - Limited availability of /8 subnets address
- Internet routing table growth
  - Size of the routing table due to higher number prefix announcement
- Tremendous growth of the Internet

APNIC Asia Pacific Network Information Centre

How many IPv4 IANA pool available



Source : Internet Number Resource Report - Number Resource Organization (NRO)

APNIC Asia Pacific Network Information Centre

IP addressing solutions

- Subnet masking and summarization
  - Variable-length subnet mask definition
  - Hierarchical addressing
  - Classless InterDomain Routing (CIDR)
  - Routes summarization (RFC 1518)
- Private address usage (RFC 1918)
  - Network address translation (NAT)
- Development of IPv6 address

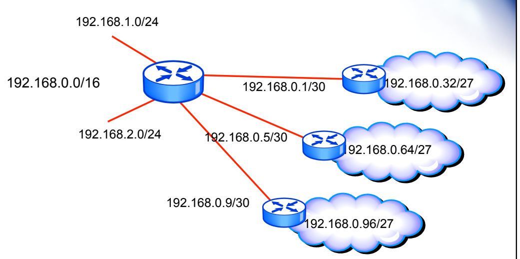
APNIC Asia Pacific Network Information Centre

Variable Length Subnet Mask

- Allows the ability to have more than one subnet mask within a network
- Allows re-subnetting
  - create sub-subnet network address
- Increase the routes capability
  - Addressing hierarchy
  - Summarisation

Calculating VLSM example

- Subnet 192.168.0.0/24 into smaller subnet
  - Subnet mask with /27 and /30 (point-to-point)



Calculating VLSM example (cont.)

- Subnet 192.168.0.0/24 into smaller subnet
  - Subnet mask with /30 (point-to-point)

Description	Decimal	Binary
Network Address	192.168.0.0/30	x.x.x.000000**00**
1st valid IP	192.168.0.1/30	x.x.x.000000**01**
2nd valid IP	192.168.0.2/30	x.x.x.000000**10**
Broadcast address	192.168.0.3/30	x.x.x.000000**11**

Calculating VLSM example (cont.)

- Subnet 192.168.0.0/24 into smaller subnet
  - Subnet mask with /27

Description	Decimal	Binary
Network Address	192.168.0.32/27	x.x.x.000**00000**
Valid IP range 192.168.0.33 - 192.168.0.62		x.x.x.000**00001**
		x.x.x.000**00010**
Broadcast address	192.168.0.63/30	x.x.x.000**11111**

Calculating VLSM example (cont.)

- Subnet 192.168.0.0/24 into smaller subnet
  - Subnet mask with /27

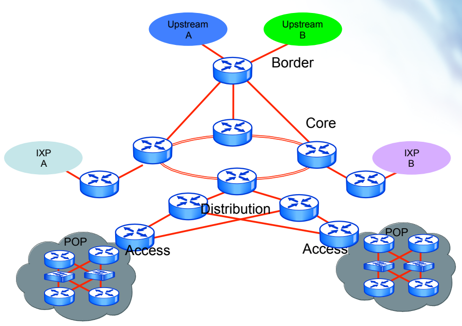
Description	Decimal	VSLM	Host	Host range
1st subnet	192.168.0.0/27	**x.x.x.000**	**00000**	0-31
2nd subnet	192.168.0.32/27	**x.x.x.001**		31-63
3rd subnet	192.168.0.64/27	**x.x.x.010**		64-95
4th subnet	192.168.0.96/27	**x.x.x.011**		96-127

n = 5 (n is the remaining subnet bits)
2n – 5 = 30 host per subnet

Addressing Hierarchy

- Support for easy troubleshooting, upgrades and manageability of networks
- Performance optimisation
  - Scalable and more stable
  - Less network resources overhead (CPU, memory, buffers, bandwidth)
- Faster routing convergence

Addressing Hierarchy example



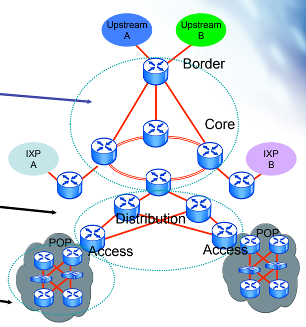
Addressing Hierarchical (cont.)

Network Number
192.168.0.0/16

Core
192.168.32.0/19

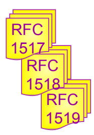
Distribution/Core
192.168.32.0/21

Access/Distribution
192.168.48.0/21



Classful and classless

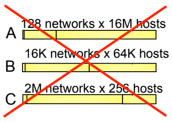
- Classful *(Obsolete)*
  - Wasteful address architecture
    - network boundaries are fixed at 8, 16 or 24 bits (class A, B, and C)
- **Classless** Best Current Practice
  - Efficient architecture
    - network boundaries may occur at any bit (e.g. /12, /16, /19, /24 etc)
- CIDR
    - Classless Inter Domain Routing architecture
  - Allows *aggregation* of routes within ISPs infrastructure



Classless & classful addressing

Best Current Practice

Classful



Obsolete
- *inefficient*
- *depletion of B space*
- *too many routes from C space*

Classless

Addresses	Prefix	Classful	Net mask
...	...	...	...
8	/29		255.255.255.248
16	/28		255.255.255.240
32	/27		255.255.255.224
64	/26		255.255.255.192
128	/25		255.255.255.128
256	/24	1 C	255.255.255.0
...	...	...	...
4096	/20	16 Cs	255.255.240.0
8192	/19	32 Cs	255.255.224
16384	/18	64 Cs	255.255.192
32768	/17	128 Cs	255.255.128
65536	/16	1 B	255.255.0.0
...	...	...	... *

* See back of slide booklet for complete chart

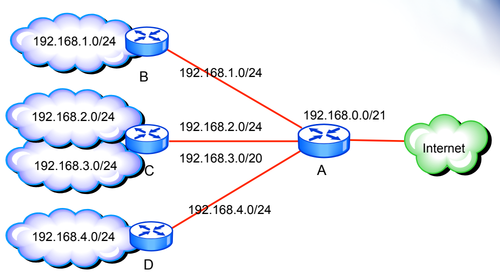
- Network boundaries may occur at *any* bit

Prefix routing / CIDR

- Prefix routing commonly known as classless inter domain routing (CIDR)
  - It allows prefix routing and summarisation with the routing tables of the Internet
- RFCs that talks about CIDR
  - *RFC 1517* Applicability statement for the implementation of CIDR
  - *RFC 1518* Architecture for IP address allocation with CIDR
  - *RFC 1519* CIDR : an address assignment and aggregation strategy
  - *RFC 1520* Exchanging routing information access provider boundaries in a CIDR environment

CIDR solution advantage

- CIDR offers the advantages reducing the routing table size of the network by summarising the ISP announcement in a single /21 advertisement

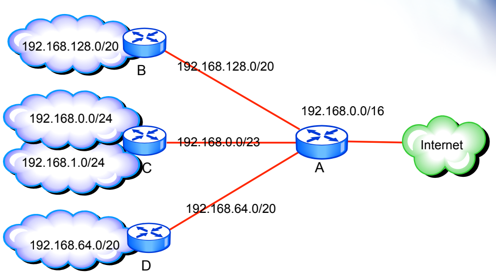


Route summarisation

- Allows the presentation of a series of networks in a single summary address.
- Advantages of summarisation
  - Faster convergence
  - Reducing the size of the routing table
  - Simplification
  - Hiding Network Changes
  - Isolate topology changes

Summarisation example

- Router C summarises its networks (2 x/24) before announcing to its neighbors (routers B and D)
- Router A combined the networks received from B, C, D and announce it as single /16 routing to Internet



Route summarisation

- Subnet 192.168.0.0/24 and 192.168.1.0/24 combining then to become a bigger block of address “/23”

Network	Subnet Mask	Binary
192.168.0.0	255.255.255.0	x.x.0000**0000.x**
192.168.1.0	255.255.255.0	x.x.0000**0001.x**
Summary	192.168.0.0/23	x.x.0000**0000.x**
192.168.0.0	255.255.254.0	x.x.0000**0000.x**

Configuring summarisation

- Manual configuration is required with the use of newer routing protocols
  - Each of the routing protocols deal with it in a slightly different way
- All routing protocols employ some level of automatic summarisation depending on the routing protocol behavior (be cautious about it)

APNIC Asia Pacific Network Information Centre

Manual summarisation

- Manual summarisation uses by OSPF are more sophisticated.
  - Sends the subnet mask including the routing update which allows the use of VLSM and summarisation
- Performs a lookup to check the entire database and acts on the longest match

APNIC Asia Pacific Network Information Centre

Discontiguous networks

- A network not using routing protocol that support VLSM creates problem
  - Router will not know where to send the traffic
  - Creates routing loop or duplication
- Summarisation is not advisable to network that are discontiguous
  - Turn off summarisation
    - Alternative solution but understand the scaling limitation
    - Find ways to re-address the network
  - Can create disastrous situation

APNIC Asia Pacific Network Information Centre

Questions?

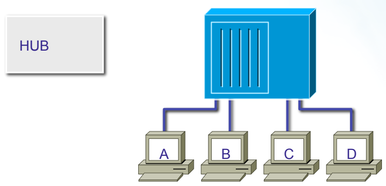
Overview

- Introduction to Internet Operation
  - Internet Protocols – some revision
  - IP addressing basic
  - **IP Routing basic**
  - Introduction to DNS & RevDNS
  - Infrastructure Security Fundamental

Objectives

- To be able to gain knowledge about the foundation of the routing protocols
- Classify the difference between a classful and classless routing architecture
- Compare distance vector and link-state protocol operation
- Describe the information written inside the routing table

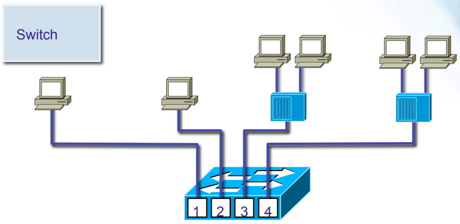
Routing Fundamental Physical Layer



- All workstation will be in the same collision domain
- All workstation will be in the same broadcast domain
- Workstations will share the total bandwidth

Source: www.cisco.com (ICND v1.0a—1-11)

Routing fundamental Data Link Layer



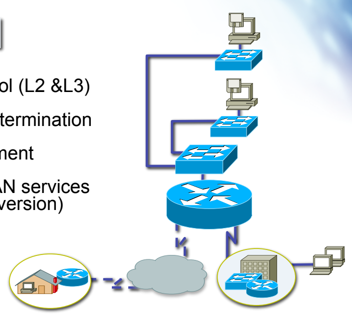
- Each port will have its own collision domain
- All ports will be in the same broadcast (LAN) domain

Source: www.cisco.com (ICND v1.0a—1-11)

Routing fundamental Network Layer

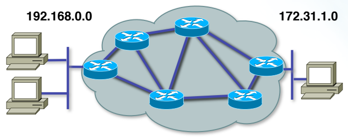
Router

- Broadcast control (L2 &L3)
- Optimal path determination
- Traffic management
- Connects to WAN services (Protocol conversion)



Source: www.cisco.com (ICND v1.0a—1-11)

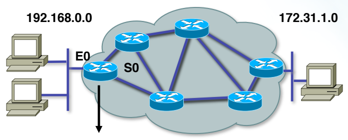
What is Routing?



- To route, a router needs to know:
  - Destination addresses
  - Sources it can learn from
  - Possible routes
  - Best route
  - Maintain and verify routing information

Source: www.cisco.com (ICND v1.0a—1-11)

What is Routing? (cont.)



Network Protocol	Destination Network	Exit Interface
Connected	192.168.0.0	E0
Learned	172.31.1.0	S0

Routed Protocol: IP

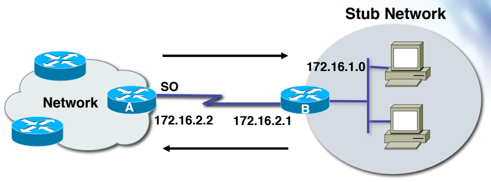
Routers must learn destinations that are not directly connected

Static and Dynamic Routing

- Static Route
  A route that a network administrator enters into the router manually

- Dynamic Route
  A route that a network routing protocol adjusts automatically for topology or traffic changes

Static Routing

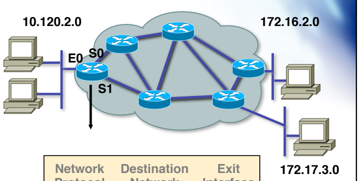


Configure unidirectional static routes to and from a stub network to allow communications to occur.

Source: www.cisco.com (ICND v1.0a—1-11)

Dynamic Routing

- Routing protocols are used between routers to determine paths and maintain routing tables.
- Once the path is determined a router can route a routed protocol.



Network Protocol	Destination Network	Exit Interface
Connected	10.120.2.0	E0
RIP	172.16.2.0	S0
IGRP	172.17.3.0	S1

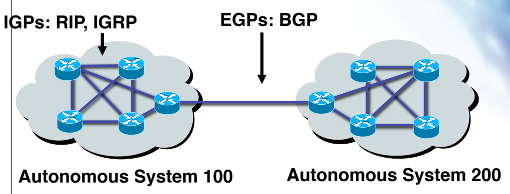
Routed Protocol: IP
Routing protocol: RIP, IGRP

Source: www.cisco.com (ICND v1.0a—1-11)

What is a dynamic routing protocol?

- A set of rules defined to facilitate the exchanges of routing information between routers (Layer 3 device) inside networks
- Build routing tables dynamically to let the route find its path in a network having more than one path to a remote network.
- Maintains the devices connectivity within the network about the available network connections.

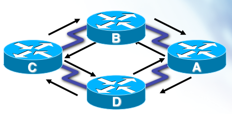
Interior or Exterior Routing Protocols

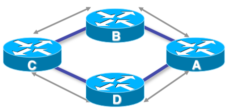


- An autonomous system is a collection of networks under a common administrative domain
- IGPs operate within an autonomous system
- EGPs connect different autonomous systems

Classes of Routing Protocols

Distance Vector





Link State

Routing protocol behavior

- Mechanism to update Layer 3 routing devices, to route the data across the best path
- Learns participating routers advertised routes to know their neighbors
- Learned routes are stored inside the routing table

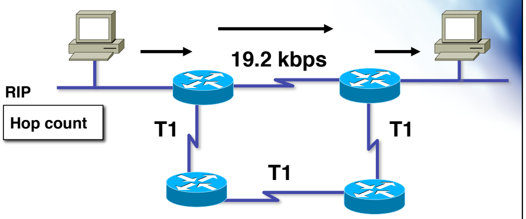
Distance Vector Routing Protocol

- Pass periodic copies of routing table to neighbor routers
- Accumulate metric on every router (I.e Hop count)

61

APNIC Asia Pacific Network Information Centre

Distance Vector—Best Route selection

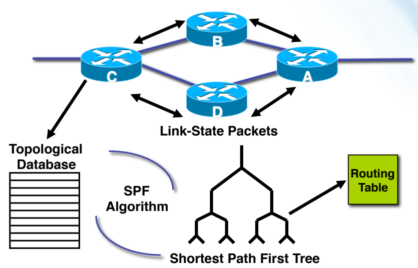


Information used to select the best path for routing

Source: www.cisco.com (ICND v1.0a—1-11)

APNIC Asia Pacific Network Information Centre

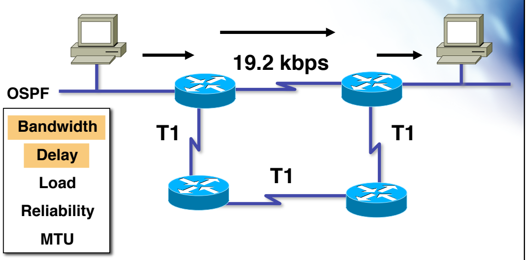
Link-State Routing Protocols



After initial flood, pass small event-triggered link-state updates to all other routers

Source: www.cisco.com (ICND v1.0a—1-11)

Link State—Best Route selection



Information used to select the best path for routing

Source: www.cisco.com (ICND v1.0a—1-11)

Distinction between *routed* and *routing* protocols

- Routed protocols
  - Layer3 datagram that carry the information required in transporting the data across the network
- Routing protocols
  - Handles the updating requirement of the routers within the network for determining the path of the datagram across the network

Routing and *routed* protocols

Routed protocol	Routing protocol
AppleTalk	RTMP, AURP, EIGRP
IPX	RIP, NLSP, EIGRP
Vines	RTP
DecNet IV	DecNet
IP	RIPv2, OSPF, IS-IS, BGP and (Cisco Systems proprietary) EIGRP,

Metric field

- To determine which path to use if there are multiple paths to the remote network
- Provide the value to select the best path
- But take note of the administrative distance selection process ☺

Routing protocol metrics

Routing protocol	Metric
RIPv2	Hop count
EIGRP	Bandwidth, delay, load, reliability, MTU
OSPF	Cost (the higher the bandwidth indicates a lowest cost)
IS-IS	Cost

Administrative distance

- Is the method used for selection of route priority of IP routing protocol, the lowest administrative distance is preferred
  - Manually entered routes are preferred from dynamically learned routes
    - Static routes
    - Default routes
  - Dynamically learned routes depend on the routing protocol metric calculation algorithm and default metrics values the smallest metric value are preferred

Administrative distance chart (Cisco)

Route sources	Default distance
Connected interface	**0**
Static route out an interface	**0**
Static route to a next hop	**1**
External BGP	**20**
IGRP	**100**
OSPF	**110**
IS-IS	**115**
RIP v1, v2	**120**
EGP	**140**
Internal BGP	**200**
Unknown	**255**

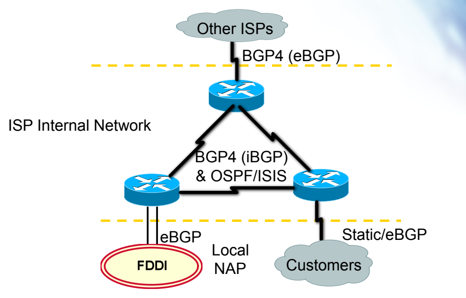
Principles of addressing

- Separate customer & infrastructure address pools
  - Manageability
    - Different personnel manage infrastructure and assignments to customers
  - Scalability
    - Easier renumbering - customers are difficult, infrastructure is relatively easy

Principles of addressing

- Further separate infrastructure
  - ‘Static’ infrastructure examples
    - RAS server address pools, CMTS
    - Virtual web and content hosting LANs
    - Anything where there is no dynamic route calculation
- Customer networks
    - Carry in iBGP, do not put in IGP
      - No need to aggregate address space carried in iBGP
      - Can carry in excess of 100K prefixes

Hierarchy of routing protocols



Source: www.cisco.com (ICND v1.0a—1-11)

Questions?

Overview

- Introduction to Internet Operation
  - Internet Protocols – some revision
  - IP addressing basic
  - IP Routing basic
  - **Introduction to DNS & RevDNS**
  - Infrastructure Security Fundamental

Purpose of naming

- Addresses are used to locate objects
- Names are easier to remember than numbers
- You would like to get to the address or other objects using a name
- DNS provides a mapping from names to resources of several types

APNIC Asia Pacific Network Information Centre

Naming History

- 1970's ARPANET
  - Host.txt maintained by the SRI-NIC
  - pulled from a single machine
  - Problems
    - traffic and load
    - Name collisions
    - Consistency
- DNS created in 1983 by Paul Mockapetris (RFCs 1034 and 1035), modified, updated, and enhanced by a myriad of subsequent RFCs

APNIC Asia Pacific Network Information Centre

DNS

- A lookup mechanism for translating objects into other objects
- A globally distributed, loosely coherent, scalable, reliable, dynamic database
- Comprised of three components
  - A "name space"
  - Servers making that name space available
  - Resolvers (clients) which query the servers about the name space

APNIC Asia Pacific Network Information Centre

DNS Features: Global Distribution

- Data is maintained locally, but retrievable globally
  - No single computer has all DNS data
- DNS lookups can be performed by any device
- Remote DNS data is locally cachable to improve performance

APNIC Asia Pacific Network Information Centre

DNS Features: Loose Coherency

- The database is always internally consistent
  - Each version of a subset of the database (a zone) has a serial number
    - The serial number is incremented on each database change
- Changes to the master copy of the database are replicated according to timing set by the zone administrator
- Cached data expires according to timeout set by zone administrator

APNIC Asia Pacific Network Information Centre

DNS Features: Scalability

- No limit to the size of the database
  - One server has over 20,000,000 names
    - Not a particularly good idea
- No limit to the number of queries
  - 24,000 queries per second handled easily
- Queries distributed among masters, slaves, and caches

APNIC Asia Pacific Network Information Centre

DNS Features: Reliability

- Data is replicated
  - Data from master is copied to multiple slaves
- Clients can query
  - Master server
  - Any of the copies at slave servers
- Clients will typically query local caches

DNS Features: Dynamicity

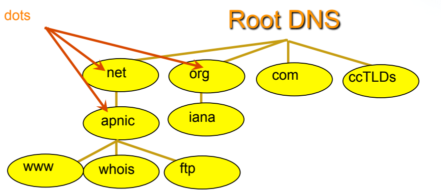
- Database can be updated dynamically
  - Add/delete/modify of any record
- Modification of the master database triggers replication
  - Only master can be dynamically updated
    - Creates a single point of failure

Concept: DNS Names

- How names appear in the DNS
  - Fully Qualified Domain Name (FQDN)
    - `WWW.APNIC.NET.`
  - labels separated by dots
- DNS provides a mapping from FQDNs to resources of several types
- Names are used as a key when fetching data in the DNS

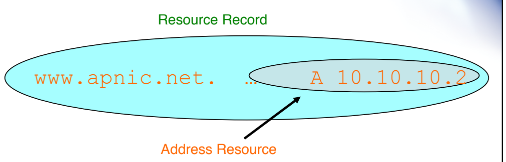
Concept: DNS Names contd.

- Domain names can be mapped to a tree
- New branches at the 'dots'



Concept: Resource Records

- The DNS maps names into data using Resource Records.

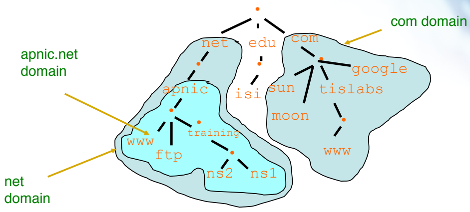


- More detail later

Concept: Domains

- Domains are "namespaces"
- Everything below *.com* is in the com domain
- Everything below *apnic.net* is in the apnic.net domain and in the net domain

Concept: Domains



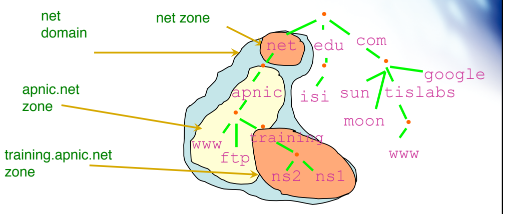
Delegation

- Administrators can create subdomains to group hosts
  - According to geography, organizational affiliation or any other criterion
- An administrator of a domain can delegate responsibility for managing a subdomain to someone else
  - But this isn't required
- The parent domain retains links to the delegated subdomain
  - The parent domain "remembers" who it delegated the subdomain to

Concept: Zones and Delegations

- Zones are "administrative spaces"
- Zone administrators are responsible for portion of a domain's name space
- Authority is delegated from a parent and to a child

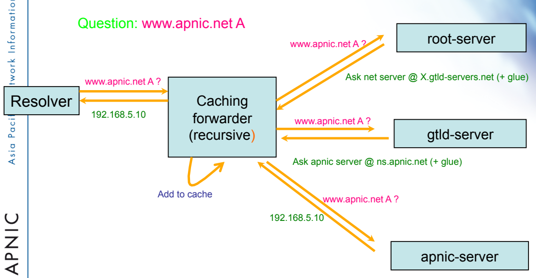
Concept: Zones and Delegations



Concept: Name Servers

- Name servers answer ‘DNS’ questions
- Several types of name servers
  - Authoritative servers
    - master (primary)
    - slave (secondary)
  - (Caching) recursive servers
    - also caching forwarders
  - Mixture of functionality

Concept: Resolving process & Cache



Concept: Resource Records

- Resource records consist of it's name, it's TTL, it's class, it's type and it's RDATA
- TTL is a timing parameter
- IN class is widest used
- There are multiple types of RR records
- Everything behind the type identifier is called rdata

```
www.apnic.net.   3600   IN   A   10.10.10.2
Label            ttl    class type rdata
```

Asia Pacific Network Information Centre
APNIC

Example: RRs in a zone file

```
apnic.net. 7200 IN      SOA     ns.apnic.net. admin.apnic.net.
                (
                         2001061501      ; Serial
                         43200   ; Refresh 12 hours
                         14400   ; Retry 4 hours
                         345600  ; Expire 4 days
                         7200    ; Negative cache 2 hours )

apnic.net.           7200  IN    NS     ns.apnic.net.
apnic.net.           7200  IN    NS     ns.ripe.net.

whois.apnic.net.     3600  IN    A      193.0.1.162

host25.apnic.net.    2600  IN    A      193.0.3.25
Label                ttl   class type   rdata
```

Asia Pacific Network Information Centre
APNIC

Resource Record: SOA and NS

- The SOA and NS records are used to provide information about the zone itself

- The NS indicates where information about a given zone can be found

```
apnic.net. 7200  IN   NS    ns.apnic.net.
apnic.net. 7200  IN   NS    ns.ripe.net.
```

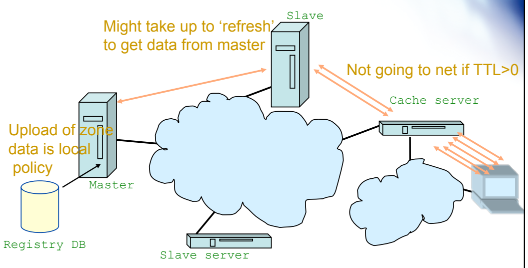
- The SOA record provides information about the start of authority, i.e. the top of the zone, also called the APEX

Concept: TTL and other Timers

- TTL is a timer used in caches
  - An indication for how long the data may be reused
  - Data that is expected to be 'stable' can have high TTLs
- SOA timers are used for maintaining consistency between primary and secondary servers

Places where DNS data lives

- Changes do not propagate instantly



To remember...

- Multiple authoritative servers to distribute load and risk:
  - Put your name servers apart from each other
- Caches to reduce load to authoritative servers and reduce response times
- SOA timers and TTL need to be tuned to needs of zone. Stable data: higher numbers

Performance of DNS

- Server hardware requirements
- OS and the DNS server running
- How many DNS servers?
- How many zones expected to load?
- How large the zones are?
- Zone transfers
- Where the DNS servers are located?
- Bandwidth

Performance of DNS

- Are these servers Multihomed?
- How many interfaces are to be enabled for listening?
- How many queries are expected to receive?
- Recursion
- Dynamic updates?
- DNS notifications

Writing a zone file

- Zone file is written by the zone administrator
- Zone file is read by the master server and it's content is replicated to slave servers
- What is in the zone file will end up in the database
- Because of timing issues it might take some time before the data is actually visible at the client side

First attempt

- The 'header' of the zone file
  - Start with a SOA record
  - Include authoritative name servers and
  - Add other information
- Add other RRs
- Delegate to other zones

Authoritative NS records and related A records

```
apnic.net.       3600 IN NS   NS1.apnic.net.
apnic.net.       3600 IN NS   NS2.apnic.net.
NS1.apnic.net.   3600 IN A    203.0.0.4
NS2.apnic.net.   3600 IN A    193.0.0.202
```

- NS record for all the authoritative servers
  - They need to carry the zone at the moment you publish
- A records only for "in-zone" name servers
  - Delegating NS records might have glue associated

Zone file format short cuts nice formatting

```
apnic.net.        3600  IN SOA NS1.apnic.net. admi
n\.email.apnic.net. (
               2002021301    ; serial
               1h          ; refresh
               30M         ; retry
               1W          ; expiry
               3600 )        ; neg. answ. Ttl

apnic.net.     3600 IN NS   NS1.apnic.net.
apnic.net.     3600 IN NS   NS2.apnic.net.
apnic.net.         3600 IN MX   50   mail.apnic.net.
apnic.net.             3600 IN MX   150  mailhost2.apnic.net.

apnic.net.             3600 IN TXT  "Demonstration and test zone"
NS1.apnic.net.     4500 IN A    203.0.0.4
NS2.apnic.net.     3600 IN A    193.0.0.202
localhost.apnic.net.   3600 IN A    127.0.0.1
www.apnic.net.     3600 IN CNAME IN.apnic.net.
```

Zone file short cuts: repeating last name

```
apnic.net.         3600  IN SOA NS1.apnic.net. admi
n\.email.apnic.net. (
              2002021301 ; serial
              1h     ; refresh
              30M        ; retry
              1W     ; expiry
              3600 )     ; neg. answ. Ttl
               3600 IN NS   NS1.apnic.net.
                   3600 IN NS   NS2.apnic.net.
           3600 IN MX   50   mail.apnic.net.
           3600 IN MX   150  mailhost2.apnic.net.

           3600 IN TXT  "Demonstration and test zone"
NS1.apnic.net.     3600 IN A    203.0.0.4
NS2.apnic.net.     3600 IN A    193.0.0.202

localhost.apnic.net.   4500 IN A    127.0.0.1

NS1.apnic.net.     3600 IN A    203.0.0.4
www.apnic.net.     3600 IN CNAME IN.apnic.net.
```

Zone file short cuts: default TTL

```
$TTL    3600 ; Default TTL directive
apnic.net.       IN SOA NS1.apnic.net. admin\.email.apnic.net. (
               2002021301    ; serial
               1h        ; refresh
               30M       ; retry
               1W        ; expiry
               3600 )    ; neg. answ. Ttl
               IN NS   NS1.apnic.net.
                   IN NS   NS2.apnic.net.
           IN MX   50  mail.apnic.net.
           IN MX   150 mailhost2.apnic.net.

           IN TXT  "Demonstration and test zone"
NS1.apnic.net.     IN A   203.0.0.4
NS2.apnic.net.     IN A   193.0.0.202

localhost.apnic.net. 4500 IN A    127.0.0.1

NS1.apnic.net.         IN A    203.0.0.4
www.apnic.net.     IN CNAME NS1.apnic.net.
```

Zone file short cuts: ORIGIN

```
$TTL    3600 ; Default TTL directive
$ORIGIN apnic.net.
@           IN SOA NS1 admin\.email.apnic.net. (
               2002021301    ; serial
               1h        ; refresh
               30M       ; retry
               1W        ; expiry
               3600 )    ; neg. answ. Ttl
           IN NS   NS1
               IN NS   NS2
       IN MX   50  mailhost
       IN MX   150 mailhost2


       IN TXT  "Demonstration and test zone"
NS1         IN A    203.0.0.4
NS2         IN A    193.0.0.202

localhost 4500 IN A     127.0.0.1

NS1             IN A    203.0.0.4
www         IN CNAME NS1
```

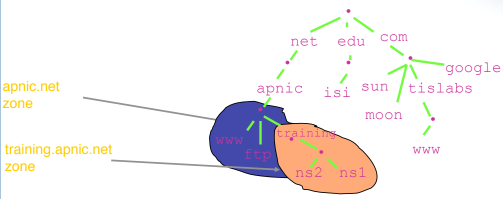
Zone file short cuts: Eliminate IN

```
$TTL    3600 ; Default TTL directive
$ORIGIN apnic.net.
@           SOA NS1 admin\.email.sanog.org. (
                2002021301    ; serial
                1h          ; refresh
                30M         ; retry
                1W          ; expiry
                3600 )      ; neg. answ. Ttl
            NS   NS1
                NS   NS2
        MX   50  mailhost
        MX   150 mailhost2


        TXT  "Demonstration and test zone"
NS1          A    203.0.0.4
NS2          A    193.0.0.202

localhost 4500  A    127.0.0.1

NS1             A    203.0.0.4
www          CNAME NS1
```

Asia Pacific Network Information Centre
APNIC

Delegating a zone (becoming a parent)

- Delegate authority for a sub domain to another party (splitting of *training.apnic.net* from *apnic.net*)



Asia Pacific Network Information Centre
APNIC

Concept: Glue

- Delegation is done by adding NS records:

```
training.apnic.net.     NS ns1.training.apnic.net.
training.apnic.net.     NS ns2.training.apnic.net.
training.apnic.net.     NS ns1.apnic.net.
training.apnic.net.     NS ns2.apnic.net.
```

- How to get to ns1 and ns2… We need the addresses

- Add glue records to so that resolvers can reach ns1 and ns2

```
ns1.training.apnic.net. A 10.0.0.1
ns2.training.apnic.net. A 10.0.0.2
```

Asia Pacific Network Information Centre
APNIC

Concept: Glue contd.

- Glue is 'non-authoritative' data
- Don't include glue for servers that are not in sub zones

```
training.apnic.net.    NS    ns1.training.apnic.net.
Training.apnic.net.    NS  ns2.training.apnic.net.

training.apnic.net.    NS    ns2.apnic.net.
training.apnic.net.    NS    ns1.apnic.net.
ns1.training.apnic.net. A     10.0.0.1
Ns2.training.apnic.net. A  10.0.0.2
```

Only this record needs glue

APNIC Asia Pacific Network Information Centre

Delegating training.apnic.net. from apnic.net.

training.apnic.net

Setup minimum two servers
Create zone file with NS records
Add all training.apnic.net data

apnic.net

Add NS records and glue

Make sure there is no other data from the training.apnic.net. zone in the zone file

APNIC Asia Pacific Network Information Centre

Questions?

APNIC Asia Pacific Network Information Centre

Reverse DNS

Overview

- Principles
- Creating reverse zones
- Setting up nameservers
- Reverse delegation procedures

What is 'Reverse DNS'?

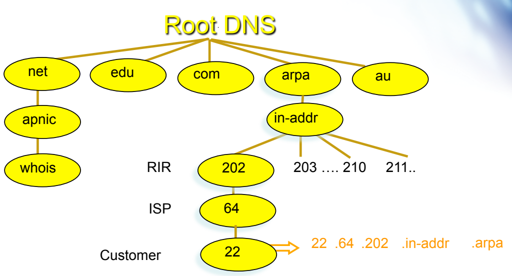
- 'Forward DNS' maps names to numbers
  - svc00.apnic.net -> 202.12.28.131
- 'Reverse DNS' maps numbers to names
  - 202.12.28.131 -> svc00.apnic.net

Reverse DNS - why bother?

- Service denial
  - That only allow access when fully reverse delegated eg. anonymous ftp
- Diagnostics
  - Assisting in trace routes etc
- SPAM identifications
- Registration responsibilities

Principles – DNS tree

- Mapping numbers to names - 'reverse DNS'



Creating reverse zones

- Same as creating a forward zone file
  - SOA and initial NS records are the same as normal zone
  - Main difference
    - need to create additional PTR records
- Can use BIND or other DNS software to create and manage reverse zones
  - Details can be different

Creating reverse zones - contd

- Files involved
  - Zone files
    - Forward zone file
      - e.g. db.domain.net
    - Reverse zone file
      - e.g. db.192.168.254
  - Config files
    - <named.conf>
  - Other
    - Hints files etc.
      - Root.hints

Start of Authority (SOA) record

```
<domain.name.>      CLASS   SOA     <hostname.domain.name.>
 <mailbox.domain.name> (
      <serial-number>
                        <refresh>
                         <retry>
                         <expire>
                        <negative-caching> )
```

253.253.192.in-addr.arpa.

Pointer (PTR) records

- Create pointer (PTR) records for each IP address

```
131.28.12.202.in-addr.arpa.  IN PTR svc00.apnic.net.
```

or

```
131           IN      PTR            svc00.apnic.net.
```

A reverse zone example

```
$ORIGIN 1.168.192.in-addr.arpa.
@ 3600  IN SOA test.company.org. (
         sys\.admin.company.org.
         2002021301    ; serial
         1h     ; refresh
         30M       ; retry
         1W     ; expiry
         3600 )        ; neg. answ. ttl

   NS  ns.company.org.
   NS  ns2.company.org.

1  PTR    gw.company.org.
      router.company.org.

2  PTR    ns.company.org.
;auto generate:  65 PTR host65.company.org
$GENERATE 65-127 $ PTR host$.company.org.
```

Setting up the primary nameserver

- Add an entry specifying the primary server to the *named.conf* file

```
zone "<domain-name>" in {
type master;
file "<path-name>"; };
```

- <domain-name>
  - Ex: 28.12.202.in-addr.arpa.
- <type master>
  - Define the name server as the primary
- <path-name>
  - location of the file that contains the zone records

Setting up the secondary nameserver

- Add an entry specifying the primary server to the *named.conf* file

```
zone "<domain-name>" in {
type slave;
file "<path-name>";
Masters { <IP address> ; }; };
```

- <type slave> defines the name server as the secondary
- <ip address> is the IP address of the primary name server
- <domain-name> is same as before
- <path-name> is where the back-up file is

Reverse delegation requirements

- /24 Delegations
  - Address blocks should be assigned/allocated
  - At least two name servers
- /16 Delegations
  - Same as /24 delegations
  - APNIC delegates entire zone to member
  - Recommend APNIC secondary zone
- < /24 Delegations
  - Read “classless in-addr.arpa delegation”

RFC 2317

APNIC & ISPs responsibilities

- APNIC
  - Manage reverse delegations of address block distributed by APNIC
  - Process organisations requests for reverse delegations of network allocations
- Organisations
  - Be familiar with APNIC procedures
  - Ensure that addresses are reverse-mapped
  - Maintain nameservers for allocations
    - Minimise pollution of DNS

Subdomains of in-addr.arpa domain

- Example: an organisation given a /16
  - 192.168.0.0/16 (one zone file and further delegations to downstreams)
  - 168.192.in-addr.arpa zone file should have:

```
0.168.192.in-addr.arpa.     NS ns1.organisation0.com.
0.168.192.in-addr.arpa.     NS ns2.organisation0.com.
1.168.192.in-addr.arpa.     NS ns1.organisation1.com.
1.168.192.in-addr.arpa.     NS ns2.organisation1.com.
2.168.192.in-addr.arpa.     NS ns1.organisation2.com.
2.168.192.in-addr.arpa.     NS ns2.organisation2.com.
      :
      :
```

Subdomains of in-addr.arpa domain

- Example: an organisation given a /20
  - 192.168.0.0/20 (a lot of zone files!) – have to do it per /24)
  - Zone files

0.168.192.in-addr.arpa.
1.168.192.in-addr.arpa.
2.168.192.in-addr.arpa.
:
:
15.168.192.in-addr.arpa.

Reverse delegation procedures

- Standard APNIC database object,
  - can be updated through MyAPNIC, Online form or via email.
- Nameserver/domain set up verified before being submitted to the database.
- Protection by maintainer object
- Zone file updated instantly

Creation of domain objects

- If you opt to create the domain objects yourself
  - Either you can use MyAPNIC
  - Or use web/email templates
- Using web/email templates will result in initial errors
  - As the /8 is hierarchically maintained by MAINT-AP-DNS
  - Contact <helpdesk@apnic.net>

Whois domain object

```
domain:      28.12.202.in-addr.arpa
descr:       in-addr.arpa zone for 28.12.202.in-addr.arpa
admin-c:     DNS3-AP
tech-c:      DNS3-AP
zone-c:      DNS3-AP
nserver:     ns.telstra.net
nserver:     rs.arin.net
nserver:     ns.myapnic.net
nserver:     svc00.apnic.net
nserver:     ns.apnic.net
mnt-by:      MAINT-APNIC-AP
mnt-lower:   MAINT-DNS-AP
changed:     inaddr@apnic.net 19990810
source:      APNIC
```

Reverse Zone

Contacts

Name Servers

Maintainers (protection)

APNIC Asia Pacific Network Information Centre

Questions?

APNIC Asia Pacific Network Information Centre

Overview

- Introduction to Internet Operation
  - Internet Protocols – some revision
  - IP addressing basic
  - IP Routing basic
  - Introduction to DNS & RevDNS
  - **Infrastructure Security Fundamental**

APNIC Asia Pacific Network Information Centre

Security for an ISP

- An enterprise network security is relatively simpler comparing to an ISP's
  - Main objective: protecting the enterprise's network from outside intrusions
- An ISP's security concerns are much broader
  - Security measures will affect ISP's network operation
  - But security threats are real and need to be protected against
    - ISPs are very visible targets for malicious and criminal attacks
  - Must protect themselves
  - Must help to protect their customers
  - Must minimise the risk of their customers from becoming problems to others on the Internet

Security for an ISP

- No network is ever fully secure or protected
- There is always a RISK factor
- ISPs need to know how to use tools to build resistance
  - Resist attacks and intrusion attempts to their network
  - Resist long enough for internal security procedures to be activated to track the incident and apply counters

First of all…

- Introduction to security issues
  - Attack type
  - Terms and definitions
  - Security goals and services
- Risk analysis and quantification

Type of Attacks

- Eavesdropping
- Masquerading
- Man-in the middle

Reference: Complete Cisco VPN Configuration Guide

Eavesdropping Attack

- Clear text data exchange between source and destination
- Hackers/attacker will be in the middle (On the network)
- Sniff all clear text packet
- Used tools i.e protocol analyzer, promiscuous LAN card and PC

Reference: Complete Cisco VPN Configuration Guide

Eavesdropping Attack (Cont)

Possible solutions are:

- One time password (OTP) to protect password information (Not other data).
- Data encryption i.e SSL

Reference: Complete Cisco VPN Configuration Guide

Eavesdropping Attack (Cont)

- Two type of encryption
  - Link encryption (L2)
    On point to point link entire frame (PPP /HDLC) in encrypted
  - Packet payload encryption (L3)
    Only Packet payload is encrypted so it could be routed across L3 network or Internet
  - Example encryption RC4, DES, 3DES, AES
- Packet payload/L3 encryption is most common in Internet because only source and destination will do encryption/decryption

Reference: Complete Cisco VPN Configuration Guide

APNIC Asia Pacific Network Information Centre 142

Masquerading Attack

- Hacker/attacker spoof someone's identity
- Change source address (L2 or L3)
- Typically combine with DoS attack
- Use specialized software to generate packet/frame changing IP/MAC address of the originating PC
- Masquerade identity with authorized external source IP/MAC to get access

Reference: Complete Cisco VPN Configuration Guide

APNIC Asia Pacific Network Information Centre 143

Masquerading Attack (Cont)

- To control returning traffic attack might be combined with routing attack
- To initiate DoS attack hacker/attacker use internal address as source of packet
- In L2 network ARP spoofing is used to redirect L2 traffic

Reference: Complete Cisco VPN Configuration Guide

APNIC Asia Pacific Network Information Centre 144

Masquerading Attack (Cont)

- Need packet integrity check to handle masquerading attack
- Common solution is to use hash function
- Hash function use a one way hash with a shared key
- Only the device have the key will be able to create/verify hash value
- Most common hashing functions are MD5, SHA

Reference: Complete Cisco VPN Configuration Guide

Man-in-the Middle Attack

- Attacker can sit in the middle of source and destination and initiate following two types of Man-in-the Middle attacks:
  - Session reply attack
  - Session hijack attack
- For both type of attack hacker need access to the network (i.e LAN/Internet)

Reference: Complete Cisco VPN Configuration Guide

Man-in-the Middle Attack (Cont)

- Session hijack attack

  Attacker insert him in to an established connection between sender and receiver and hijack the connection. Require a specialized TCP sequence number generating software.
- This is much easier in UDP, ICMP protocol (No ACK)

Reference: Complete Cisco VPN Configuration Guide

Man-in-the Middle Attack (Cont)

- To handle these type of attack generate randomize TCP sequence number
- TCP sequence number is 32bit so around 2 billion possible combination. Practically impossible to guess next sequence number.
- VPN is best option to protect this attack.

Reference: Complete Cisco VPN Configuration Guide

APNIC Asia Pacific Network Information Centre 148

Man-in-the Middle Attack (Cont)

- Session reply attacks

  Attacker intercepts traffic from the source to the real destination by combination of spoofing and routing attack. Then pretend to be the real destination, capture all information from source and redirect it to real destination including TCP session reply.
- Attacker use Java or ActiveX script to initiate this attack

Reference: Complete Cisco VPN Configuration Guide

APNIC Asia Pacific Network Information Centre 149

What is Key

- A key is used to protect information.
- A data key can performs a similar function as a password used to protect a user account or a PIN (personal identification number) used with your ATM card.
- Normally, the longer the key, the more secure the protection it can provide.

APNIC Asia Pacific Network Information Centre

Key Types

- There are two basic types of keying solutions:
  - Symmetric
  - Asymmetric

Symmetric Keys

- Symmetric keys use the same single key to provide a security function to protect information
- An encryption algorithm that uses symmetric keys uses the same key to encrypt and decrypt information
- The algorithm used is fairly simple, very efficient and very quick

Symmetric Keys

- Encryption algorithms and standards that use symmetric keying are: DES, 3DES, CAST, IDEA, RC-4, RC-6, Skipjack, and AES.

- MD5 and SHA are examples of hashing functions that use symmetric keying.

Symmetric Keys distribution

- Pre-sharing keys— We can pre-share the keys, out-of-band between the two devices.
- Using a secure connection— We can use either an existing secure, protected connection to send keys across, or create a new protected connection to send keys across.

APNIC Asia Pacific Network Information Centre

154

Asymmetric Keys

- Asymmetric keying uses two keys:
  - Private keys
  - Public keys
- The private key is kept secret by the source to decrypt data sent to it
- The public key is given out to other by the source devices to encrypt the data to be sent to the source

APNIC Asia Pacific Network Information Centre

Asymmetric Keys example

- RSA public keying—to produce digital signatures and to perform encryption
- Digital Signature Algorithm (DSA)
- Diffie-Hellman (DH)— This is used by the Internet Key Exchange (IKE) protocol in IPsec to exchange keying information.

APNIC Asia Pacific Network Information Centre

Questions?

Thank you!