TATA COMMUNICATIONS

Internet Security & DNS Security

New Delhi

11Feb’2008

shailesh.gupta@vsnl.co.in

TATA

Contents

Tata Group - Brief

Internet Security

- Best Practices
- Brief on Tata Communications NW
- Security Implementations in Tata Communications NW
- DDOS attacks – Key learning & Mitigation Process/tool improvement

DNS Security

- Best Practices
- Brief on Tata Communications DNS architecture
- Security implementations in Tata Communications DNS
- DOS attack – Key learning & Mitigation Process/toll improvement

References
Q&A
Thanks

TATA

India's *largest business Group*

Diverse businesses in *7 sectors*

Revenues equivalent to *3.2% of India's GDP*

International income 38% of Group revenue

Operations in *over 80 countries*

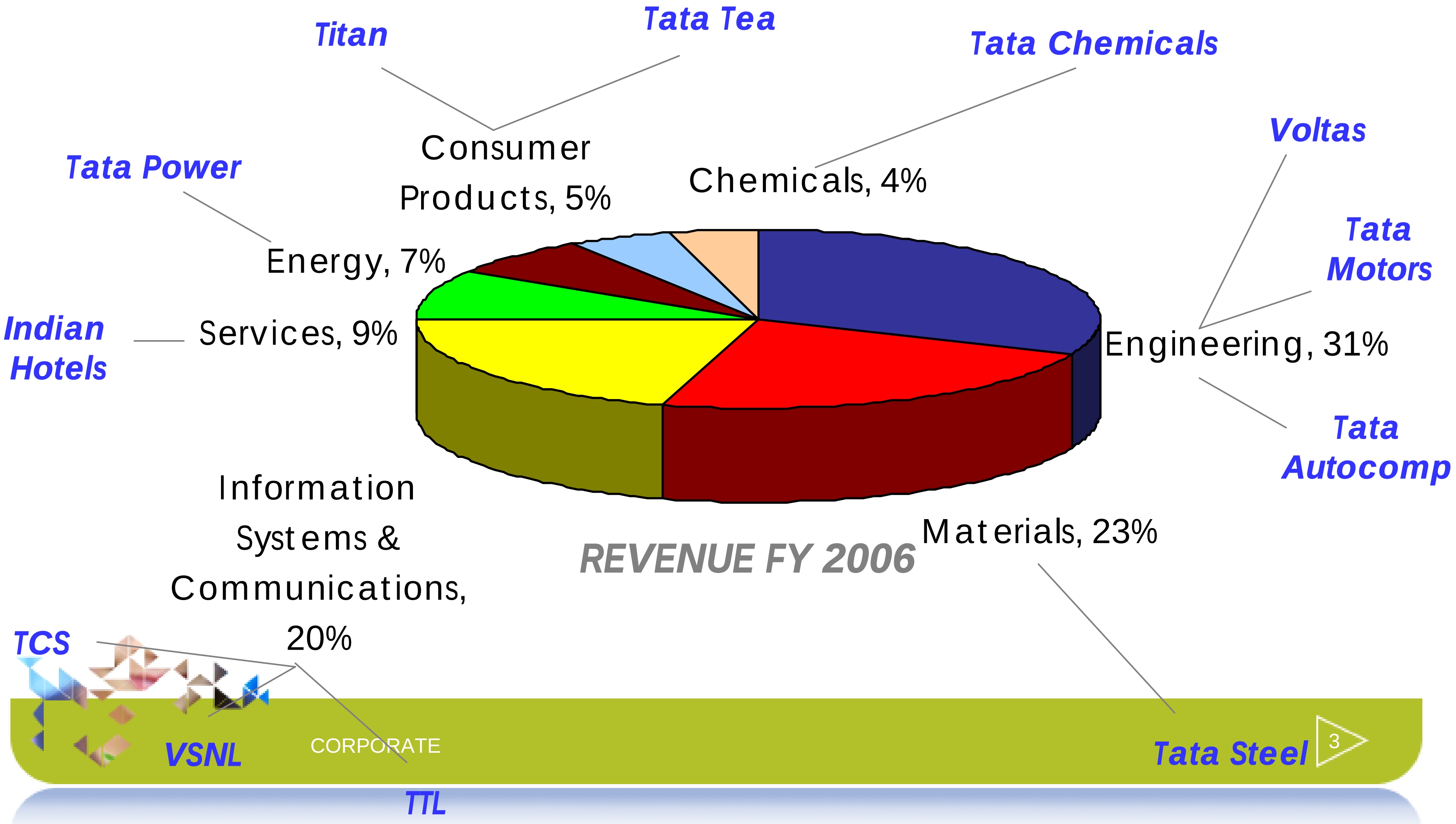
Products and services *exported to 85 countries*

Largest employer in private sector *over 289,500 employees*

Group revenue *FY 2007: Rs 129,994 cr / $ 28.8 bn*

Group profit *FY 2007: Rs 12,574 cr / $ 2.8 bn*

Tata Group Business Sectors



REVENUE FY 2006

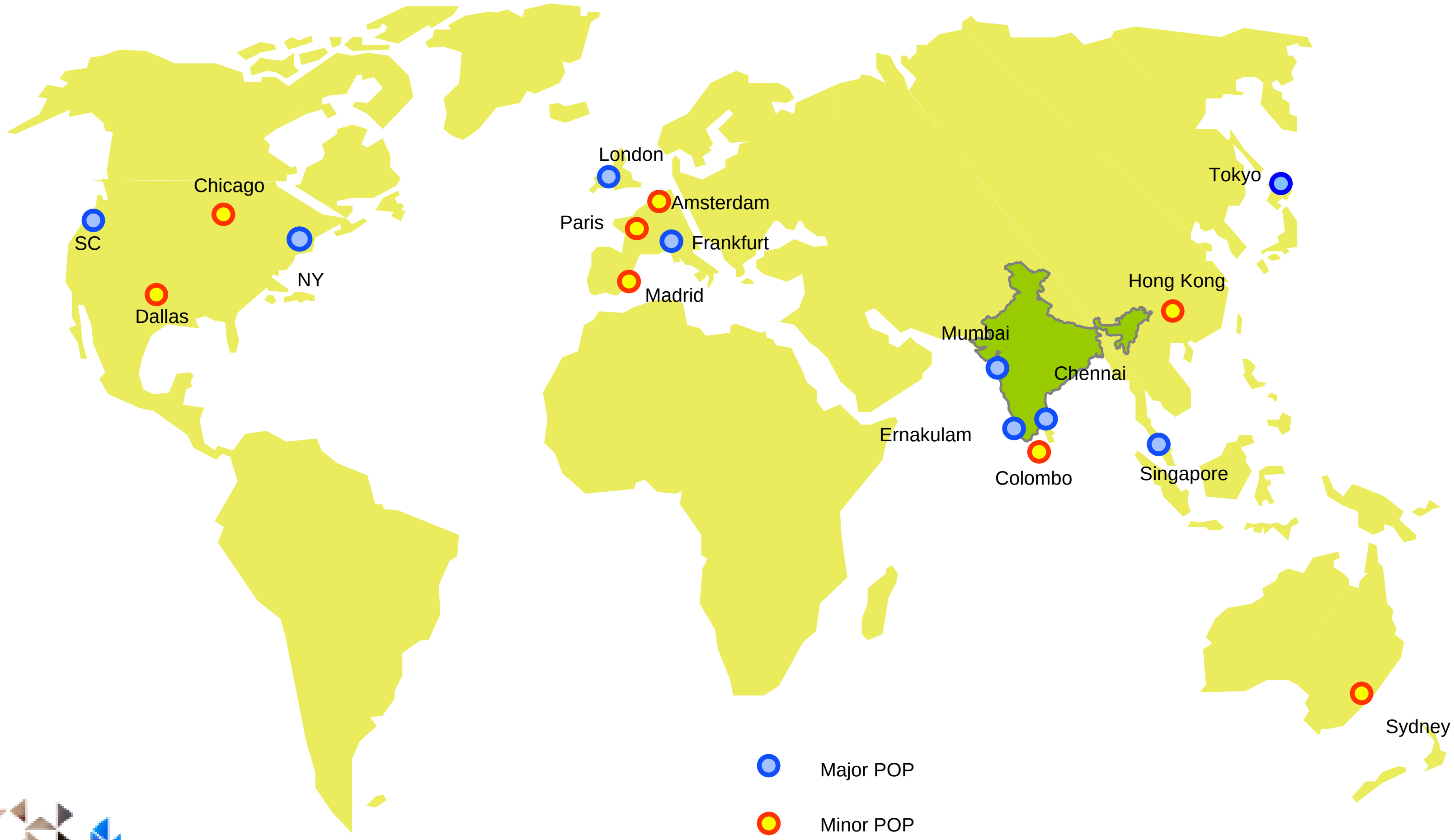
VSNL MPLS network

VSNL MPLS network is a best-in-its-class MPLS network designed to deliver the most advanced MPLS services across a variety of access mechanisms.

The VSNL MPLS network has been built as three distinct networks which rides on super core:

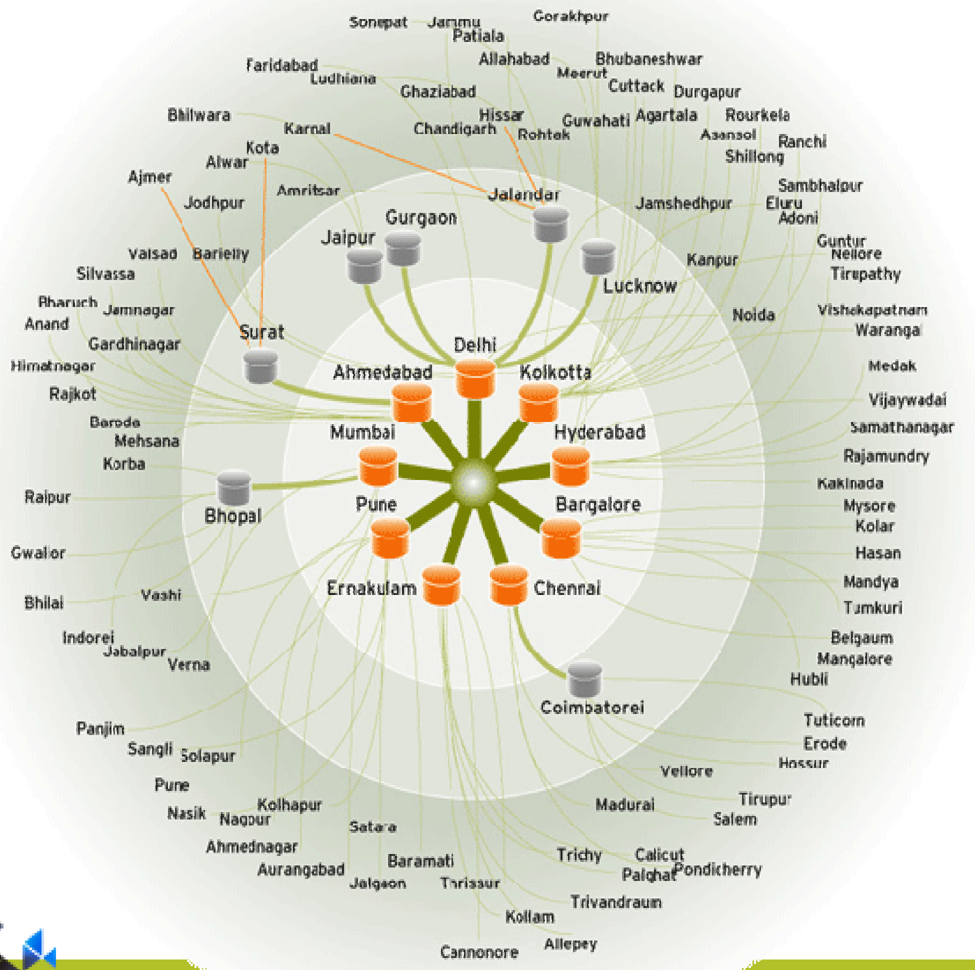
- Metro Ethernet Network across 8 cities,
- 100 PoP network across 116 cities and
- International network across 14 international locations

International MPLS Network



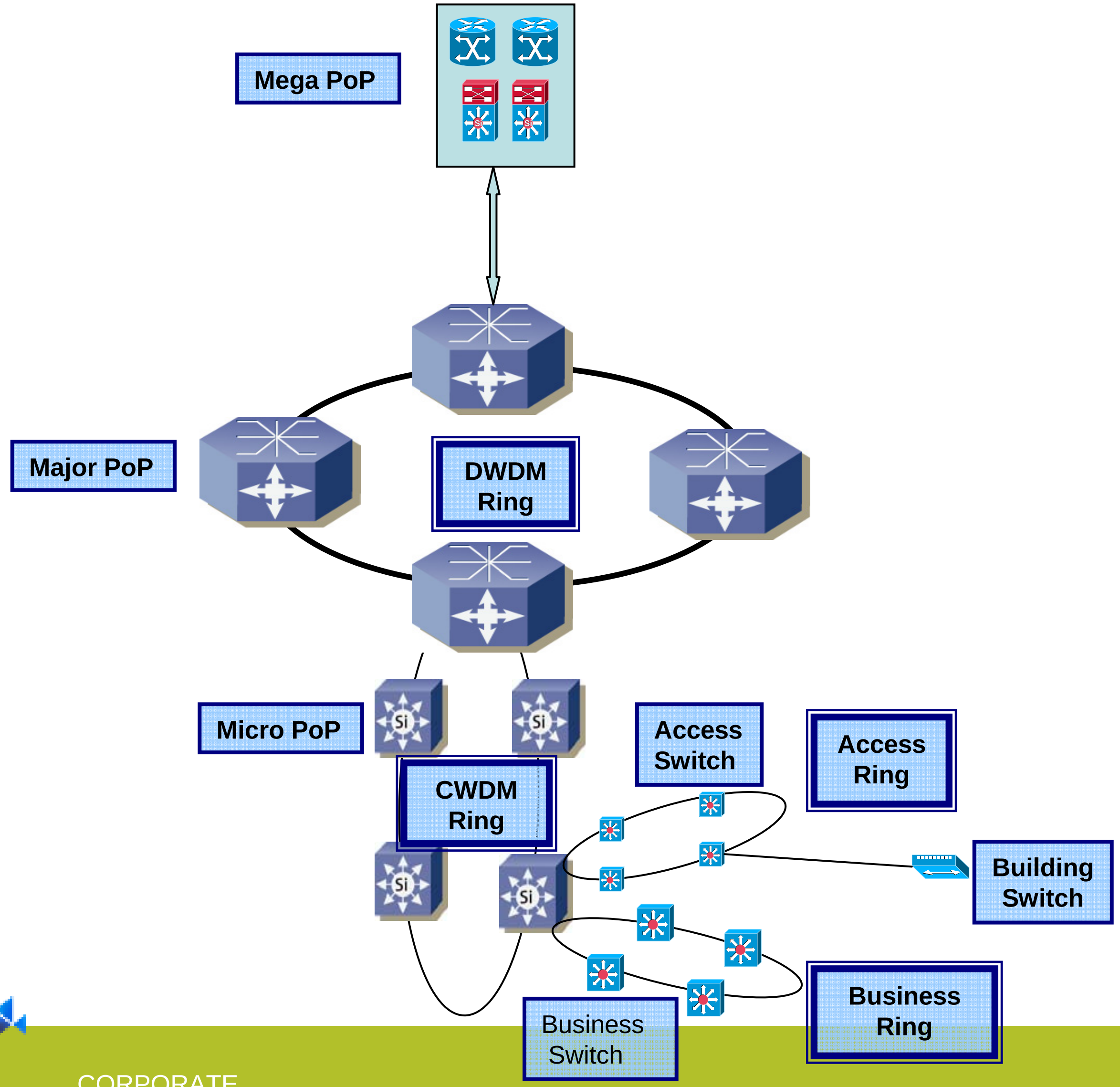
VSNL India MPLS VPN Footprint (116 Locations)

Its all about connectivity … ….All Over India



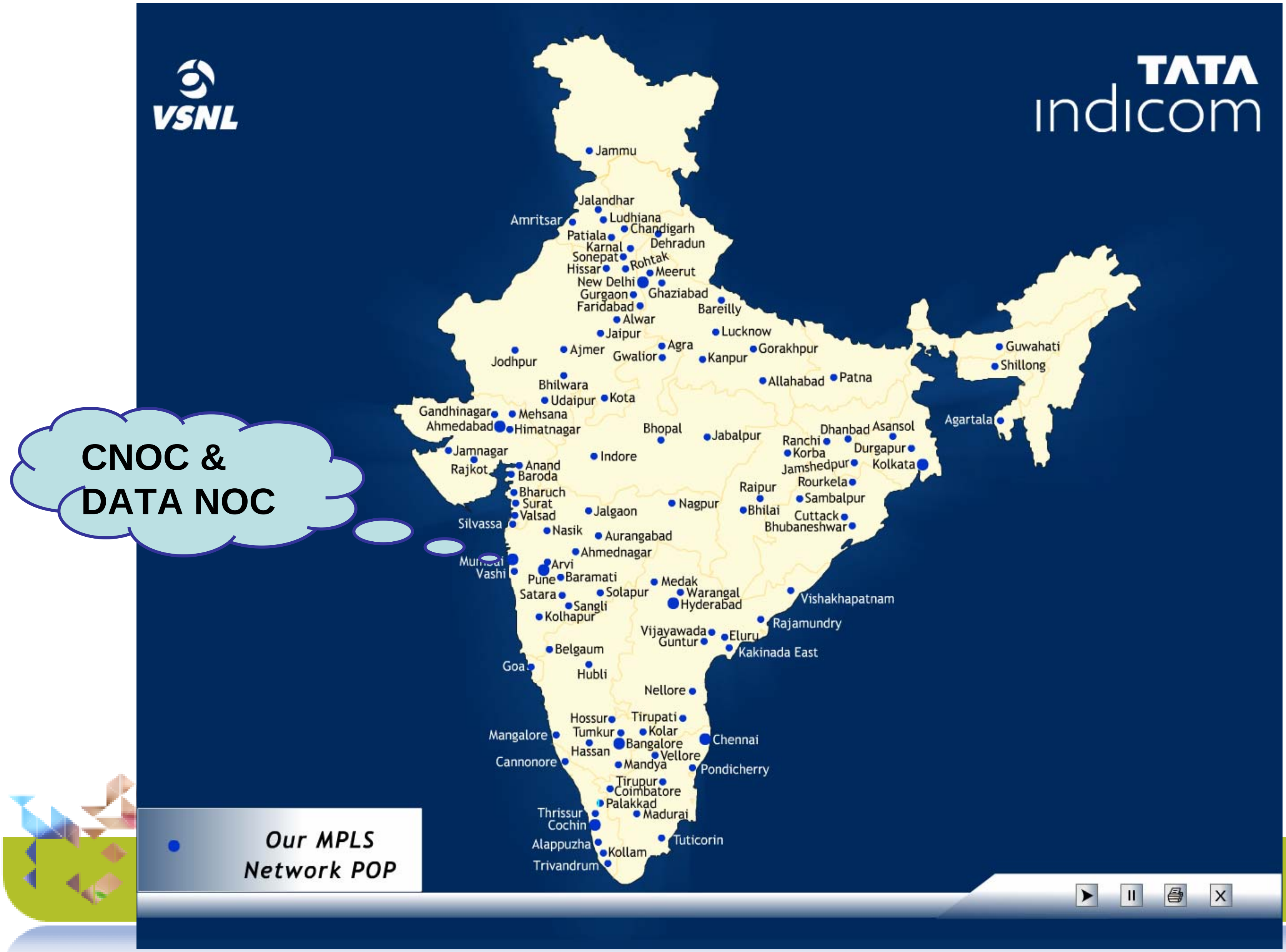
- ▪116 location across the the India.
- ▪3-tier Hierarchical topology for better management.
- ▪9 Big Tier 1 cities including 4 metros
- ▪6 Major Tier 2 cities.
- ▪101 Tier 3 cities

Network Diagram – Metro E



TATA COMMUNICATIONS

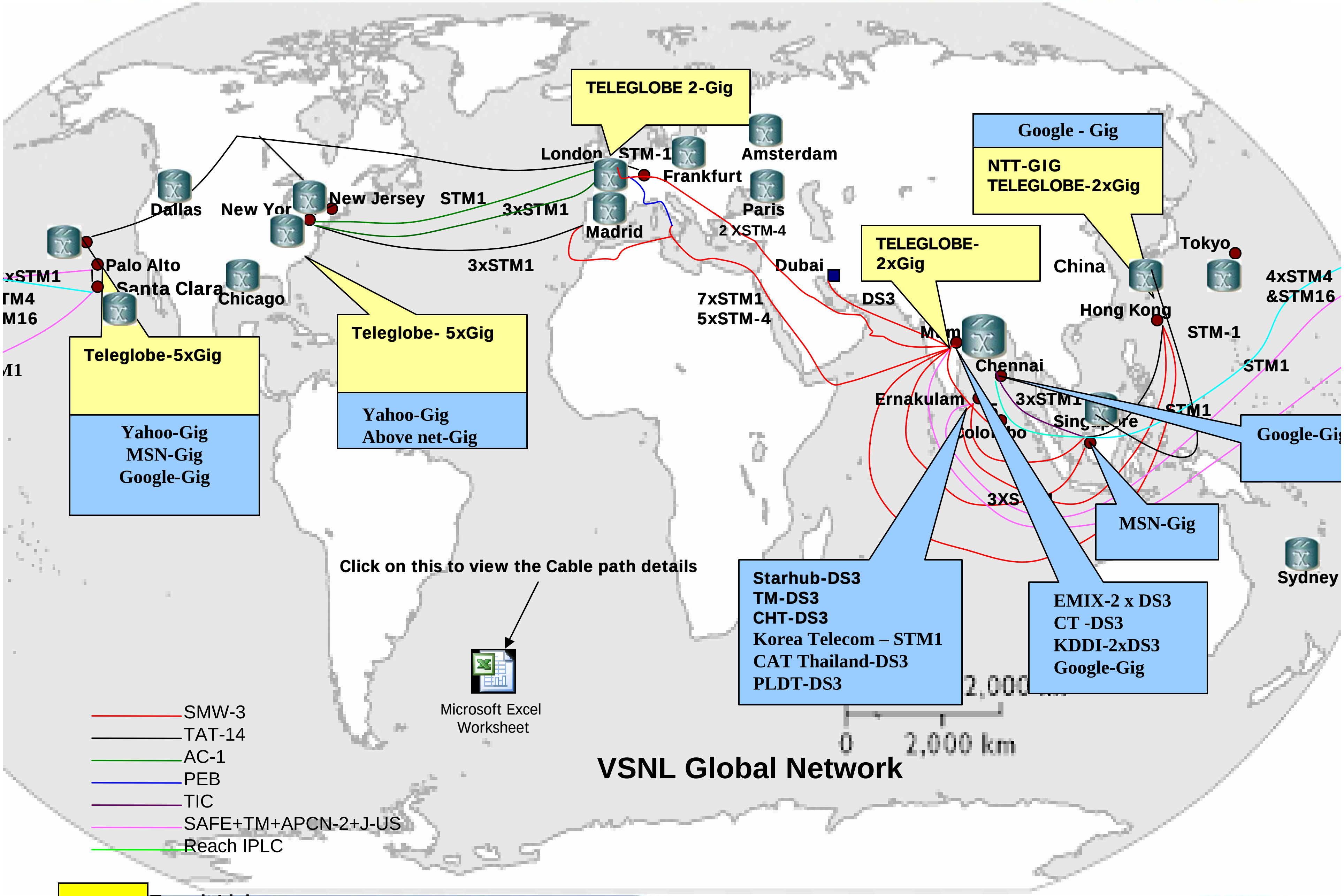
VSNL India MPLS VPN Footprint: India Map View



CNOC &
DATA NOC

● Our MPLS Network POP

INTERNATIONAL TRANSIT / PEERING BW



TELEGLOBE 2-Gig

Google - Gig

NTT-GIG
TELEGLOBE-2xGig

TELEGLOBE-
2xGig

Teleglobe- 5xGig

Yahoo-Gig
Above net-Gig

Teleglobe-5xGig

Yahoo-Gig
MSN-Gig
Google-Gig

Google-Gi

MSN-Gig

Starhub-DS3
TM-DS3
CHT-DS3
Korea Telecom – STM1
CAT Thailand-DS3
PLDT-DS3

EMIX-2 x DS3
CT -DS3
KDDI-2xDS3
Google-Gig

Click on this to view the Cable path details

Microsoft Excel
Worksheet

VSNL Global Network

SMW-3
TAT-14
AC-1
PEB
TIC
SAFE+TM+APCN-2+J-US
Reach IPLC

🟨 Transit Link

🟦 Peering Link

Highly Resilient Network

- **Gateway Locations**
  - Major Gateway locations at New York, Palo Alto, Santa Clara, London, Honk Kong and Mumbai.
  - 33% capacity is available in SMW-3, SMW-4 & TIC and 1% on SAFE cable system. It ensures that optimum latency is available for Premium customers in case of any cable system/Gateway failures.

- **Core Network Element**

  VSNL has got dual core routers (GSR) in all its important locations and has got dual aggregation layer at mega POPS.

- **Provider Edge Routers**
  - There are multiple PE routers available within the POP to take care of box failure. In case of any box failure customers can be migrated to alternate router with minimal down time and the customer's last mile can be terminated in two different PE, if the customer has dual local loop to achieve high uptime.

Current Services and Features

- ✓ILL, L2 & L3 Services
- ✓Topologies: Full mesh, Hub & spoke, complex
- ✓Last mile access: Serial (PPP, HDLC, FR), Ethernet (WiMAX, EoS port)
- ✓CE-PE Routing: Static, RIP, OSPF, EIGRP, BGP
- ✓Remote access: Dial-up, ISDN, IPSec
- ✓Multicast
- ✓IPv4 & IPv6 enabled Network.
- ✓NNI

Internet Security - Top Ten List

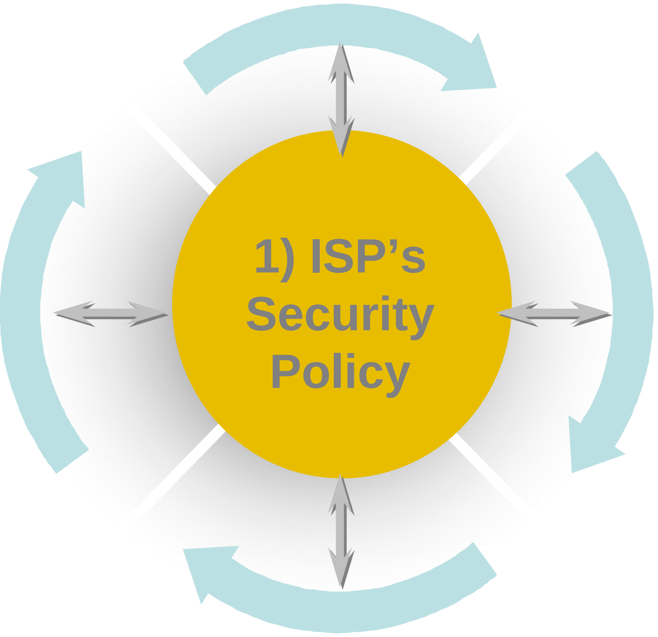
- Prepare your NOC
- Mitigation Communities
- iNOC-DBA Hotline
- Point Protection on Every Device
- Edge Protection
- Remote triggered black hole filtering
- Sink holes
-
- Source address validation on all customer traffic
- Control Plan Protection
- Total Visibility (Data Harvesting – Data Mining)

What Do ISPs Need to Do?

Security incidence are a normal part of an ISP's operations!

2) **Secure Resources**

Firewall, Encryption, Authentication, Audit



1) ISP's Security Policy

5) **Manage and Improve**

Post Mortem, Analyze the Incident, modify the plan/procedures

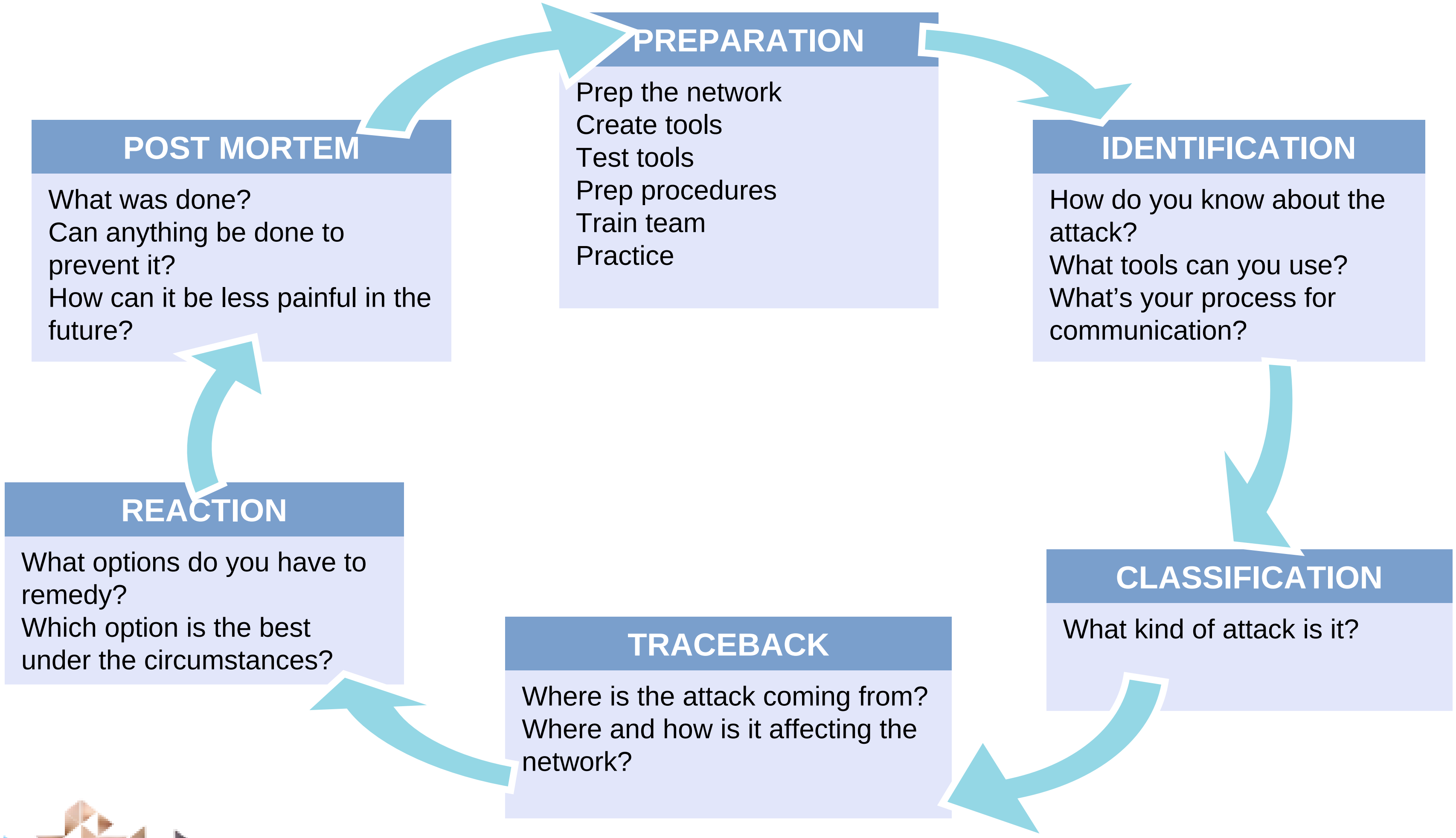
3) **Monitor and Respond**

Intrusion Detection, work the incidence,

4) **Test, Practice, Drill**

Vulnerability Scanning

Six Phases of Incident Response



PREPARATION

Prep the network
Create tools
Test tools
Prep procedures
Train team
Practice

IDENTIFICATION

How do you know about the attack?
What tools can you use?
What’s your process for communication?

CLASSIFICATION

What kind of attack is it?

TRACEBACK

Where is the attack coming from?
Where and how is it affecting the network?

REACTION

What options do you have to remedy?
Which option is the best under the circumstances?

POST MORTEM

What was done?
Can anything be done to prevent it?
How can it be less painful in the future?

Important Points

✓Create your company’s Computer Emergency Response Team

✓Know your peers (neighboring CERTs), build relationships

✓Get on NSP-SEC mailing list and on iNOC Phone

✓Know Each’s Vendors Security Team

✓ Example: psirt@cisco.com, security-alert@cisco.com and www.cisco.com/security to contact Cisco Systems.

✓Be prepared ! Define what to do & whom to contact for various incidents.

“Never underestimate the power of human communications as a tool to solve security problems. Our history demonstrates that since the Morris Worm, peer communication has been *the* most effect security tool.”

Barry Raveendran Greene

Need for Security – ISP NW

VSNL MPLS network is a converged nature as it carries both Internet and MPLS VPN traffic as MPLS switched packets in the core of the network. Hence securing the network from attacks on the Internet and VPN customers is of paramount importance.

Significant increase in the DoS attacks & Various malicious activity on the Internet. These attacks have not only given a negative impact to the users, but also consumed a lot of network resources on the network. In order to minimize the damage caused by these attacks from the Internet as well as the corporate users, VSNL had implemented the following security strategy which is both proactive as well as responsive.

The security policy on the Internet is divided into two areas

- Protecting against Control plane attacks
- Protecting against Data plane attacks

General Security measures Followed in VSNL

- For Accessing Network elements, users have to logon to centralized server through SSH.
- User creation on the servers is done by IT team after recommendation from the HEAD of the Sections.
- Password policy for the users are defined by IT team.
- Enable secret are changed every 2 months and before National holidays, ie NYD, ID & RD.

Turn off unnecessary services and protocols

The philosophy is turn on only the service/ protocol those are required and turn off everything else. Many default built in services of IOS are not needed in a backbone environment and should be turned off.

- no ip finger
- no service pad
- no service udp-small-servers
- no service tcp-small-servers
- no ip bootp server
- no cdp run

All control plane packets except ospf, ldp, bgp, rsvp, ntp, icmp are blocked using infrastructure ACLs wherever the platform supports these.

Turn off interface specific features

Some features on the routers like ip redirects etc can be used to generate DDoS attacks on the Internet. All such services are turned off on the network.

- no ip redirects
- no ip directed-broadcast
- no ip proxy-arp
- no ip unreachables

Control Plane Security ..Contd

Rate limit ICMP packets that should be processed by the device

- the ICMP traffic to be processed by the router be throttled to 100 kbps

Dedicated Bandwidth for control traffic

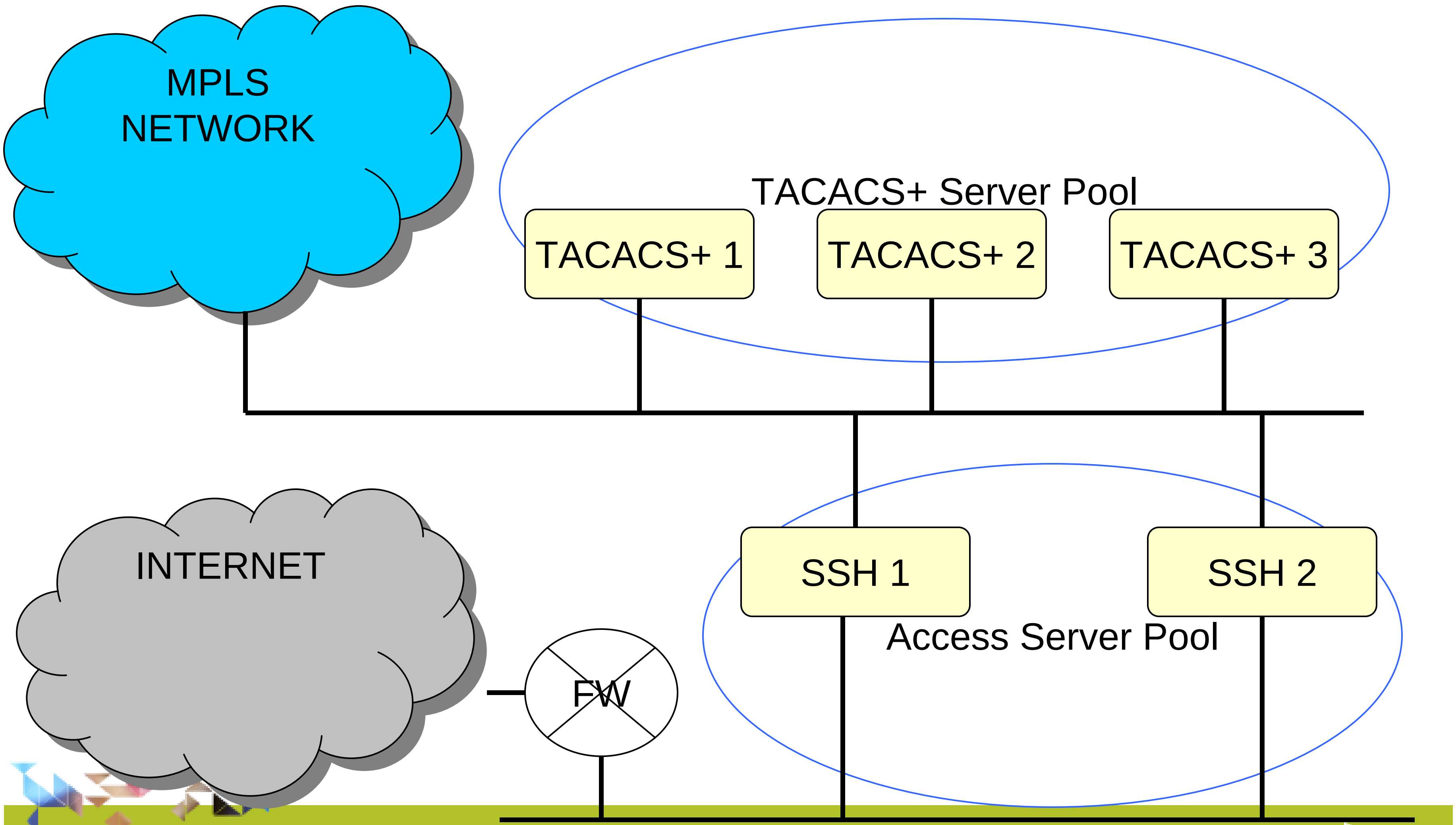
- 2% of the BW on all links is reserved for the network control traffic as a part of the QoS design

Standard ACL on VTY line

- One Local username is allowed with privilege level 15

```
Define the ACL
! permit router originated traceroute
access-list 122 permit icmp any any ttl-exceeded
access-list 122 permit icmp any any port-unreachable
! permit receipt of responses to router originated pings
access-list 122 permit icmp any any echo-reply
! allow pings to router
access-list 122 permit icmp any any echo
! Configure the Class-map
class CoPP-ICMP
   match access-group 122
! configure the policy-map
Policy-map restrict-icmp-packets
Class CoPP-ICMP
police 64000 2000 2000 conform-action transmit exceed-action drop
! Apply the policy to the control-pane
Router(config)# control-plane
Router(config-cp)# service-policy
```

TACACS+ setup



Data Network Equipments are managed by Data NOC(2000+).

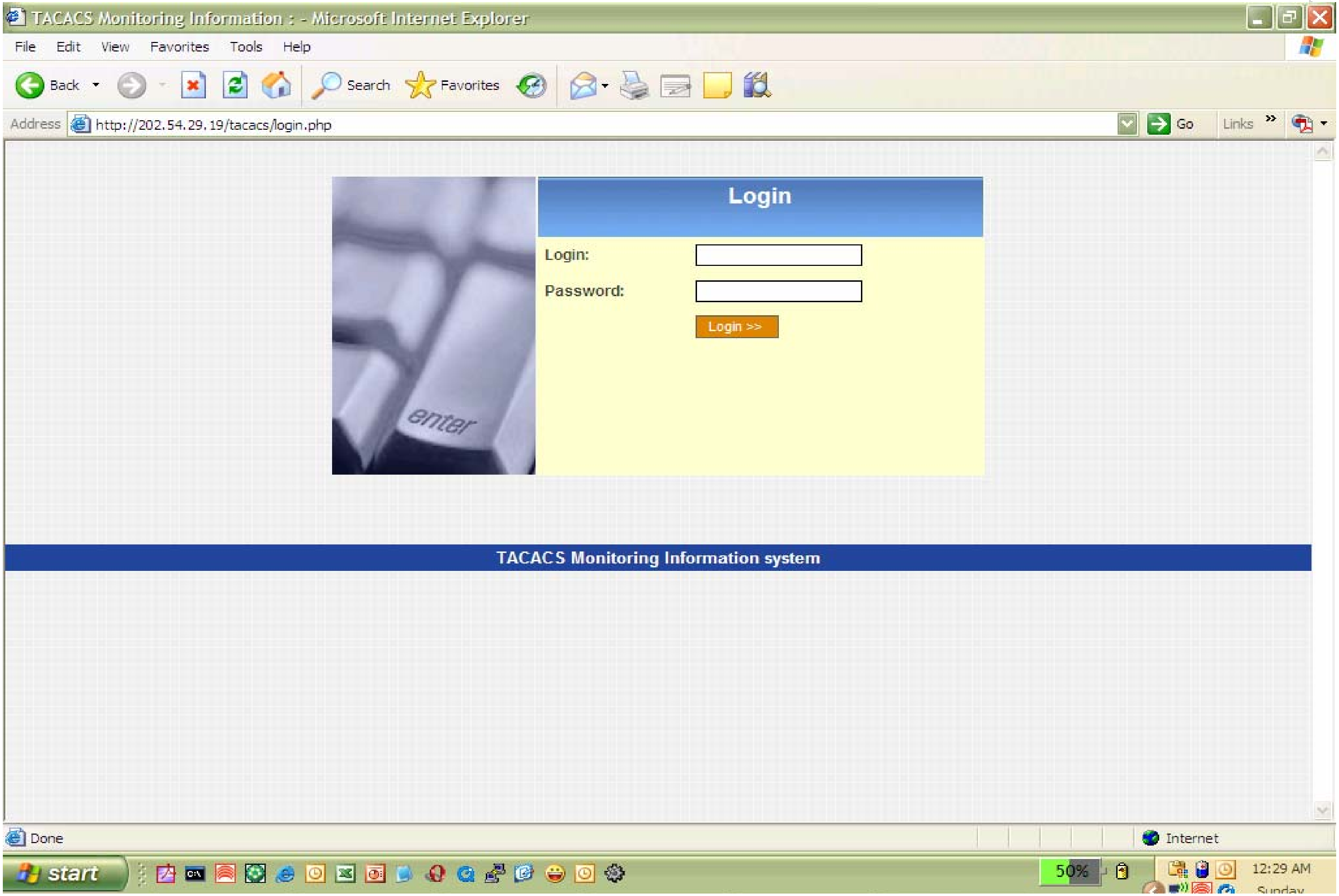
Users and Devices are segregated into the various groups as per the teams they belong to.

Access to devices are required by members of other teams in addition to Data NOC. E.g.

- SOC team requires visibility for all the PEs for supporting the Customers.
- Retail teams require access for the SSG and BRAS on the network to support the Retail customers.

Sample Access rights

						Configuration Access		
	Level	Access To	Show	Trace	Ping	Partial	Control Plane	Full
Data	L1	All Devices	Y	Y	Y	Y		
	L2	All Devices	Y	Y	Y	Y	After CM Process	
	L3	All Devices	Y	Y	Y	Y		
	L4	All Devices	Y	Y	Y	Y		Y
SOC	L1	All Edge Devices	Y	Y	Y			
	L2	All Edge Devices	Y	Y	Y			
	L3	All Edge Devices	Y	Y	Y	Y		
TM	L1	All Edge Devices	Y					
	L2	All Edge Devices	Y					
	L3	Region Edge Devices	Y					
Branch Data	L1	Region Edge Devices	Y	Y	Y			
	L2	Region Edge Devices	Y	Y	Y	Y		
	L3	Region Edge Devices	Y	Y	Y	Y		
P&I		All Edge Devices	Y	Y	Y			
Access-HQ		All SSG's & FWSM	Y			Y		
Branch Access		Regional SSG's & FWSM	Y			Y		



TACACS Monitoring Information : - Microsoft Internet Explorer

Address http://202.54.29.19/tacacs/login.php

Login

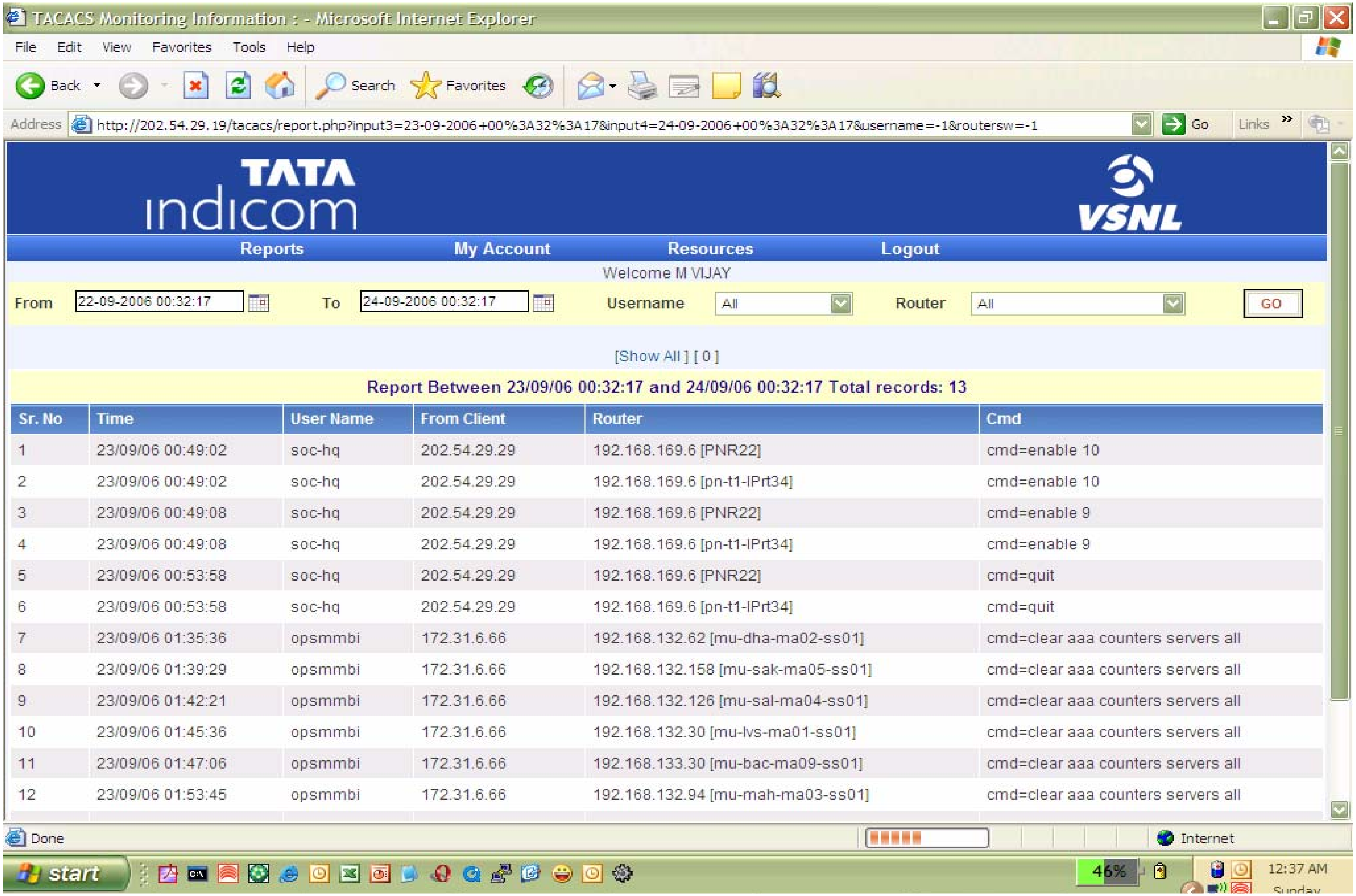
Login:

Password:

TACACS Monitoring Information system

TATA COMMUNICATIONS

TACACS Online Monitoring System-Logs



http://202.54.29.19/tacacs/report.php?input3=23-09-2006+00%3A32%3A17&input4=24-09-2006+00%3A32%3A17&username=-1&routersw=-1

Welcome M VIJAY

From 22-09-2006 00:32:17 To 24-09-2006 00:32:17 Username All Router All

[Show All] [0]

Report Between 23/09/06 00:32:17 and 24/09/06 00:32:17 Total records: 13

Sr. No	Time	User Name	From Client	Router	Cmd
1	23/09/06 00:49:02	soc-hq	202.54.29.29	192.168.169.6 [PNR22]	cmd=enable 10
2	23/09/06 00:49:02	soc-hq	202.54.29.29	192.168.169.6 [pn-t1-IPrt34]	cmd=enable 10
3	23/09/06 00:49:08	soc-hq	202.54.29.29	192.168.169.6 [PNR22]	cmd=enable 9
4	23/09/06 00:49:08	soc-hq	202.54.29.29	192.168.169.6 [pn-t1-IPrt34]	cmd=enable 9
5	23/09/06 00:53:58	soc-hq	202.54.29.29	192.168.169.6 [PNR22]	cmd=quit
6	23/09/06 00:53:58	soc-hq	202.54.29.29	192.168.169.6 [pn-t1-IPrt34]	cmd=quit
7	23/09/06 01:35:36	opsmmbi	172.31.6.66	192.168.132.62 [mu-dha-ma02-ss01]	cmd=clear aaa counters servers all
8	23/09/06 01:39:29	opsmmbi	172.31.6.66	192.168.132.158 [mu-sak-ma05-ss01]	cmd=clear aaa counters servers all
9	23/09/06 01:42:21	opsmmbi	172.31.6.66	192.168.132.126 [mu-sal-ma04-ss01]	cmd=clear aaa counters servers all
10	23/09/06 01:45:36	opsmmbi	172.31.6.66	192.168.132.30 [mu-lvs-ma01-ss01]	cmd=clear aaa counters servers all
11	23/09/06 01:47:06	opsmmbi	172.31.6.66	192.168.133.30 [mu-bac-ma09-ss01]	cmd=clear aaa counters servers all
12	23/09/06 01:53:45	opsmmbi	172.31.6.66	192.168.132.94 [mu-mah-ma03-ss01]	cmd=clear aaa counters servers all

Control Plane Security - Cont..

Authentications for protocols

- All protocols on the network like OSPF, BGP, LDP are authenticated between the network devices with MD5 authentication.

SNMP authentications

- SNMP communities are configured on all devices and an ACL is in place in each router to allow only authorized SNMP servers respond to the SNMP requests.

Max-routes limit inside E-BGP & VPNs

- The maximum number of routes that can be present in a EBGP & MPLS VPN is restricted to 500 as a standard practice. This limit is increased on a per customer basis as required at a premium if business so considers fit.
  - Route-leakage is avoided.

Control Plane Security - Cont..

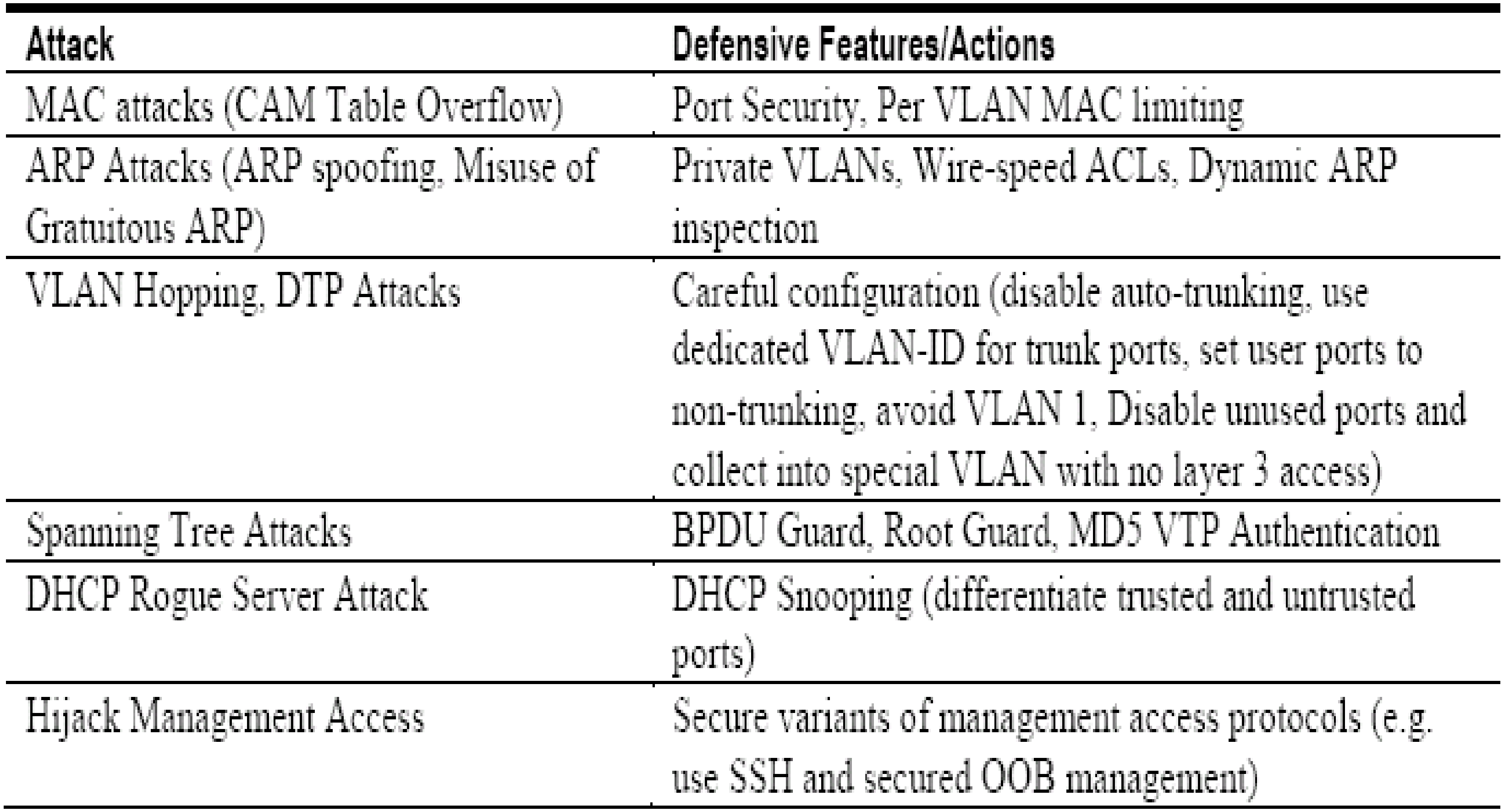
BGP dampening for eBGP customers

- dampening is done only for IPv4

BGP filter lists on all BGP peers

- BGP filters are used on all eBGP sessions with other Autonomous systems to remove specific routes from being accepted/ advertised to BGP peers.
- Block all martians/ boguns/ RFC 1918 addresses/ default route from being advertised or received on the eBGP sessions.
- Accept only customer Registered routes
- Remove all communities associated with the incoming route advertisements and tag them with communities that make sense on our network.
  - Details regarding communities and routing policies are available in the VSNL BGP Policy document.

L2 security



Attack	Defensive Features/Actions
MAC attacks (CAM Table Overflow)	Port Security, Per VLAN MAC limiting
ARP Attacks (ARP spoofing, Misuse of Gratuitous ARP)	Private VLANs, Wire-speed ACLs, Dynamic ARP inspection
VLAN Hopping, DTP Attacks	Careful configuration (disable auto-trunking, use dedicated VLAN-ID for trunk ports, set user ports to non-trunking, avoid VLAN 1, Disable unused ports and collect into special VLAN with no layer 3 access)
Spanning Tree Attacks	BPDU Guard, Root Guard, MD5 VTP Authentication
DHCP Rogue Server Attack	DHCP Snooping (differentiate trusted and untrusted ports)
Hijack Management Access	Secure variants of management access protocols (e.g. use SSH and secured OOB management)

Complete Interface Config

```
interface FastEthernetx/y
 description Residential Customer X interface
 switchport mode access
 switchport access VLAN 1100
 switchport protected
 switchport port-security maximum 5
 switchport port-security violation restrict
 switchport port-security aging time 5
 switchport port-security aging type inactivity
 spanning-tree portfast
 spanning-tree guard root
 IP dhcp snooping limit rate 10
 no IP dhcp snooping trust
 storm-control broadcast level 5.00
 storm-control multicast level 5.00
 storm-control action trap
 no cdp enable
 no shutdown
```

Blocking user-user L2 communication

Limiting number of MAC addresses learnt

forwarding state from a blocking state

customer switch should not be STP root switch

10 DHCP message per second rate limit

Storm control commands

Data Plane Security

- **Access List**

  ACLs are the most common option for enforcing a policy at the data plane. However, ACLs are not scalable and hence must not be used if the implementation is done in software or the performance is not line rate.

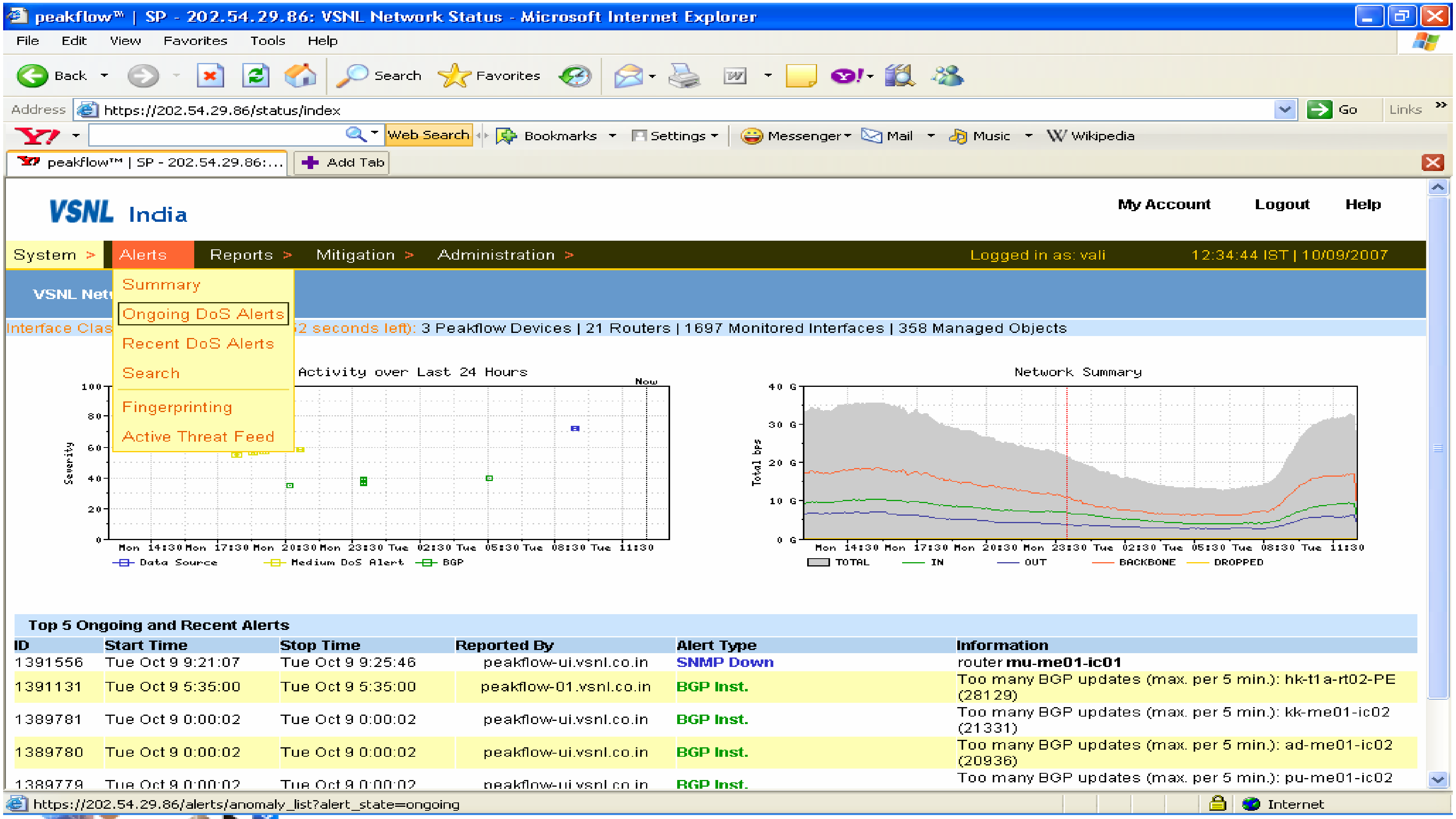
- **Black Holing traffic from upstream providers**

Unicast Reverse path forwarding are used where customer is single-homed

DOS/DDOS attack detection and mitigation

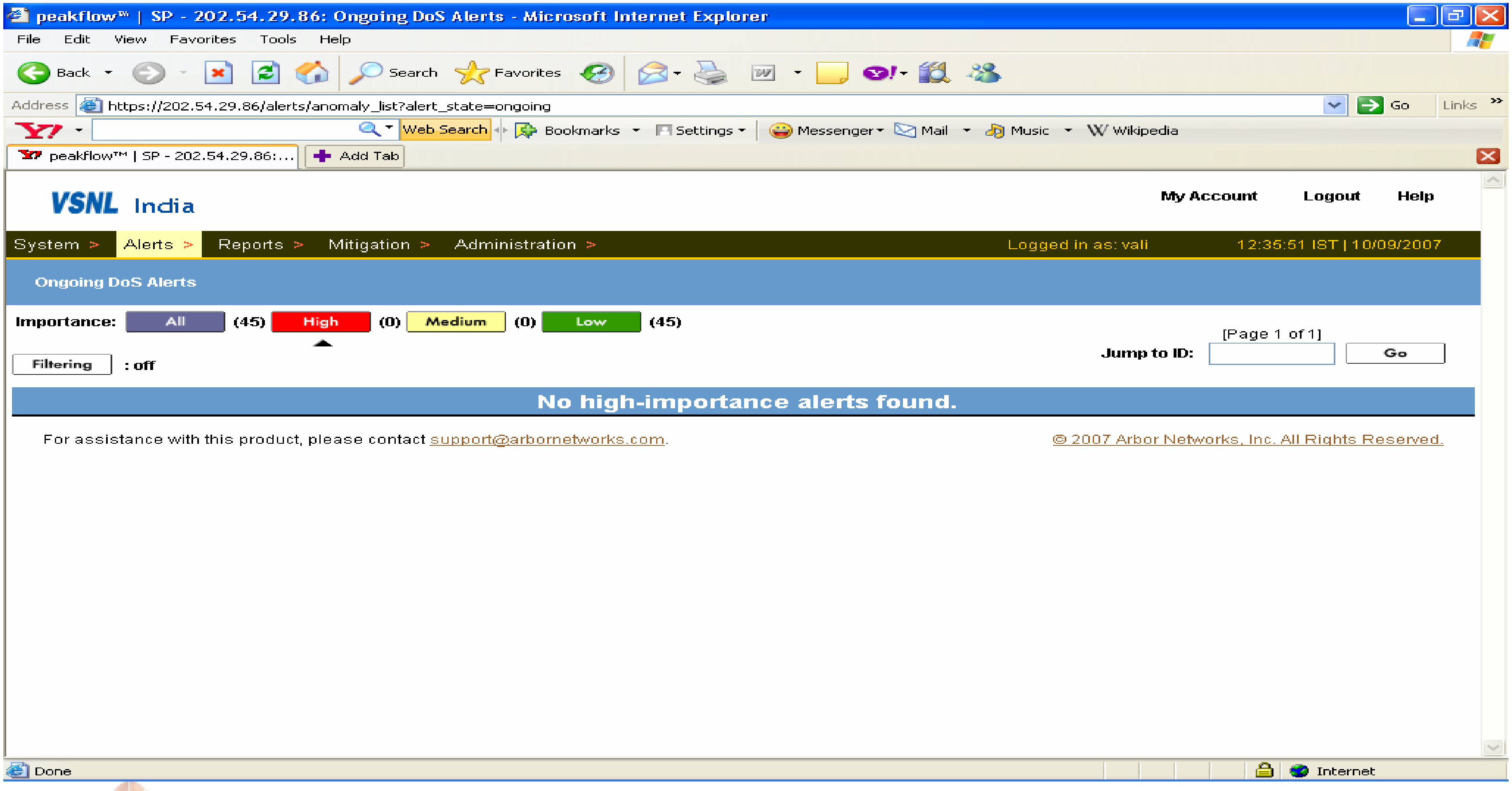
DOS and DDOS attacks are being monitored through ARBOR which raises the alarm for any happening DOS/DDOS attack in the network. Depending upon the nature of the attack it categorizes the attack as low medium and high as shown in the snap shot. Once the source/destination of the attack is being identified RTBF(Remote triggered black hole filtering) is used to black hole the traffic to safe guard the network (All the GW and aggregate routers in VSNL network are pre configured for RTBF).

Arbor is also capable of handling other attacks like BGP hijacking. In which the attacker may announce VSNL prefix as his own and drag the traffic for that particular prefix towards him (though this is controlled through proper filters on neighbors but additional feature present in the system)


peakflow™ | SP - 202.54.29.86: VSNL Network Status - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
https://202.54.29.86/status/index
Go
Links
Web Search
Bookmarks
Settings
Messenger
Mail
Music
Wikipedia
peakflow™ | SP - 202.54.29.86:...
Add Tab
VSNL India
My Account
Logout
Help
System >
Alerts
Reports >
Mitigation >
Administration >
Logged in as: vali
12:34:44 IST | 10/09/2007
VSNL Netw
Summary
Ongoing DoS Alerts
Recent DoS Alerts
Search
Fingerprinting
Active Threat Feed
Interface Clas
2 seconds left): 3 Peakflow Devices | 21 Routers | 1697 Monitored Interfaces | 358 Managed Objects
Activity over Last 24 Hours
Now
Severity
100
80
60
40
20
0
Mon 14:30 Mon 17:30 Mon 20:30 Mon 23:30 Tue 02:30 Tue 05:30 Tue 08:30 Tue 11:30
Data Source
Medium DoS Alert
BGP
Network Summary
Total bps
40 G
30 G
20 G
10 G
0 G
Mon 14:30 Mon 17:30 Mon 20:30 Mon 23:30 Tue 02:30 Tue 05:30 Tue 08:30 Tue 11:30
TOTAL
IN
OUT
BACKBONE
DROPPED
https://202.54.29.86/alerts/anomaly_list?alert_state=ongoing
Internet

Top 5 Ongoing and Recent Alerts

ID	Start Time	Stop Time	Reported By	Alert Type	Information
1391556	Tue Oct 9 9:21:07	Tue Oct 9 9:25:46	peakflow-ui.vsnl.co.in	**SNMP Down**	router **mu-me01-ic01**
1391131	Tue Oct 9 5:35:00	Tue Oct 9 5:35:00	peakflow-01.vsnl.co.in	**BGP Inst.**	Too many BGP updates (max. per 5 min.): hk-t1a-rt02-PE (28129)
1389781	Tue Oct 9 0:00:02	Tue Oct 9 0:00:02	peakflow-ui.vsnl.co.in	**BGP Inst.**	Too many BGP updates (max. per 5 min.): kk-me01-ic02 (21331)
1389780	Tue Oct 9 0:00:02	Tue Oct 9 0:00:02	peakflow-ui.vsnl.co.in	**BGP Inst.**	Too many BGP updates (max. per 5 min.): ad-me01-ic02 (20936)
1389779	Tue Oct 9 0:00:02	Tue Oct 9 0:00:02	peakflow-ui.vsnl.co.in	**BGP Inst.**	Too many BGP updates (max. per 5 min.): pu-me01-ic02


peakflow™ | SP - 202.54.29.86: Ongoing DoS Alerts - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://202.54.29.86/alerts/anomaly_list?alert_state=ongoing Go Links
Web Search Bookmarks Settings Messenger Mail Music Wikipedia
peakflow™ | SP - 202.54.29.86:... Add Tab
My Account Logout Help
System > Alerts > Reports > Mitigation > Administration >
Done Internet

VSNL India

Logged in as: vali 12:35:51 IST | 10/09/2007

Ongoing DoS Alerts

Importance: All (45) High (0) Medium (0) Low (45)

[Page 1 of 1]

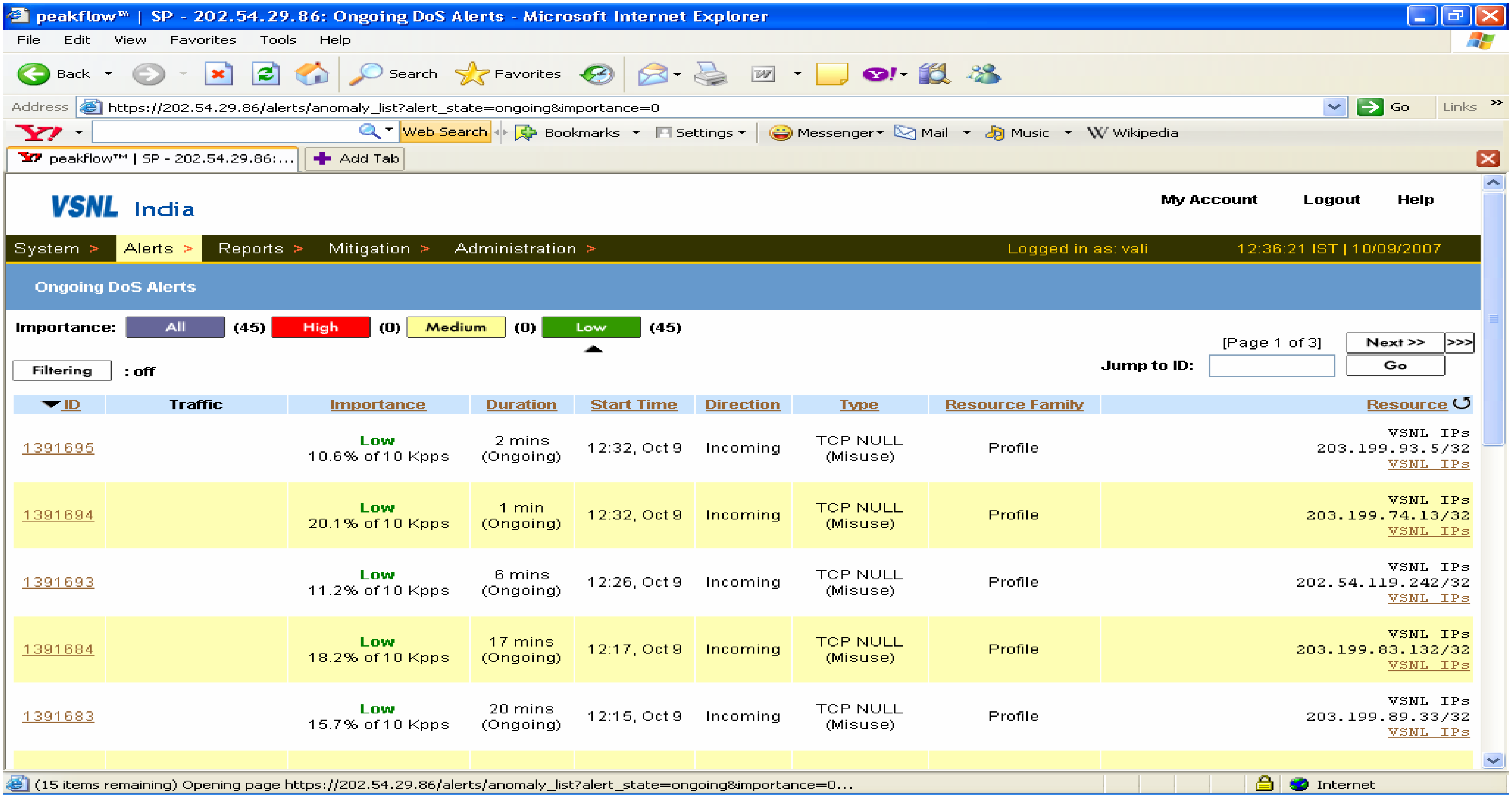
Filtering : off

Jump to ID: Go

No high-importance alerts found.

For assistance with this product, please contact support@arbornetworks.com.

© 2007 Arbor Networks, Inc. All Rights Reserved.



peakflow™ | SP - 202.54.29.86: Ongoing DoS Alerts - Microsoft Internet Explorer

Address https://202.54.29.86/alerts/anomaly_list?alert_state=ongoing&importance=0

VSNL India

Logged in as: vali 12:36:21 IST | 10/09/2007

Ongoing DoS Alerts

Importance: All (45) High (0) Medium (0) Low (45)

Filtering : off

[Page 1 of 3] Next >> >>>

Jump to ID: Go

ID	Traffic	Importance	Duration	Start Time	Direction	Type	Resource Family	Resource
1391695		Low 10.6% of 10 Kpps	2 mins (Ongoing)	12:32, Oct 9	Incoming	TCP NULL (Misuse)	Profile	VSNL IPs 203.199.93.5/32 VSNL IPs
1391694		Low 20.1% of 10 Kpps	1 min (Ongoing)	12:32, Oct 9	Incoming	TCP NULL (Misuse)	Profile	VSNL IPs 203.199.74.13/32 VSNL IPs
1391693		Low 11.2% of 10 Kpps	6 mins (Ongoing)	12:26, Oct 9	Incoming	TCP NULL (Misuse)	Profile	VSNL IPs 202.54.119.242/32 VSNL IPs
1391684		Low 18.2% of 10 Kpps	17 mins (Ongoing)	12:17, Oct 9	Incoming	TCP NULL (Misuse)	Profile	VSNL IPs 203.199.83.132/32 VSNL IPs
1391683		Low 15.7% of 10 Kpps	20 mins (Ongoing)	12:15, Oct 9	Incoming	TCP NULL (Misuse)	Profile	VSNL IPs 203.199.89.33/32 VSNL IPs

(15 items remaining) Opening page https://202.54.29.86/alerts/anomaly_list?alert_state=ongoing&importance=0...

Internet

Network Audit - SYSLOG

- Central Syslog server is available and all devices are configured to dump the error/ log messages to this server.

- Routine audits are conducted on the logs generated to identify any malicious activity on the network in a timely manner.

- With Help of CM Process, TACACS Based Authentication & Centralized Syslog servers it is easy to keep the track of the events taking place in the network.

TATA COMMUNICATIONS

Tata Communications - IP Network
DDoS Mitigation

New Delhi

TATA

DDoS Identification – Arbor PeakFlow

- IP Traffic (Net Flow) being monitored through at all AS interconnects with Peers.

- Net Flow is being collected by Arbor System PeakFlow Devices.

- Arbor keeps monitoring the flows and has configured profiles which are said as a DOS Attack.

- Any Flow which exceeds the limits set is identified as a DOS and an Alert Generated.

  - Alert has the Source IP, Destination IP along with the Ports being used.
  - It has the Packet per Second rate of traffic.
  - It has the Bits per Second rate of traffic.

DDoS Mitigation - RTBHF

- Upon receipt of an Alert from the Security Helpdesk from Arbor, IP NOC analyses the same.
- If the Alert is Impacting the Infrastructure of VSNL action is initiated on the same.
- All IP gateways and regional IP ICGs have been configured with Remote Triggered Black Hole Filtering (RTBHF).
- The IP under attack is advertised to the Internet as a /32 route with the RTBHF Community of VSNL network. (4755:666)
- With this all IP Gateways block any traffic destined to the IP and drop the same to Null.
- The same is also advertised to our upstream AS (6453) with RTBHF community of 6453 set on the same. (64999:0)
- 6453 inturn receives this and drops any traffic destined to this IP in its network edge itself.

DDoS Mitigation – After Steps

➢For the destination IP Blocked, the owner of the IP is informed via concerned customer facing teams.

➢If the source IP is a specific IP / range, a complaint is lodged with the Abuse ID of the registrar of the IP address.

➢The IP is released after the destination machine is traced and checked for any compromise which could attract the attack.

Recent DOS Attacks on 4755

1. Attack towards Pune.

- Impact – High CPU Utilization (100%) on pn-t1-IPrt33
- Cause DOS Attack towards 59.163.64.190/32 and 203.197.88.52/32
- Used RTBHF to block the first IP. And then second. CPU reduced to normal.
- Later first IP removed from Block-hole as it was not causing high CPU impact.

2.

Attack toward Nasik

- Impact – Overutilization of Nasik Backbone links. Services to Nasik degraded.
- Cause : DOS attack towards 59.165.154.195/32
- Used RTHF to block the IP.
- Utilization dropped back to normal.

TATA COMMUNICATIONS

DNS Security

New Delhi

TATA

DOMAINS AND DELEGATIONS

The Domain Name System uses a tree (or hierarchical) name structure. At the top of the tree is the root followed by the Top Level Domains (TLDs) then the domain-name and any number of lower levels each separated with a dot.

NOTE: The root of the tree is represented most of the time as a silent dot ('.')

Top Level Domains (TLDs) are split into two types:
Generic Top Level Domains (gTLD) .com, .edu, .net, .org, .mil etc.
Country Code Top Level Domain (ccTLD) e.g. .us, .ca, .tv , .uk etc.

Country Code TLDs (ccTLDs) use a standard tw

The following figure shows this:

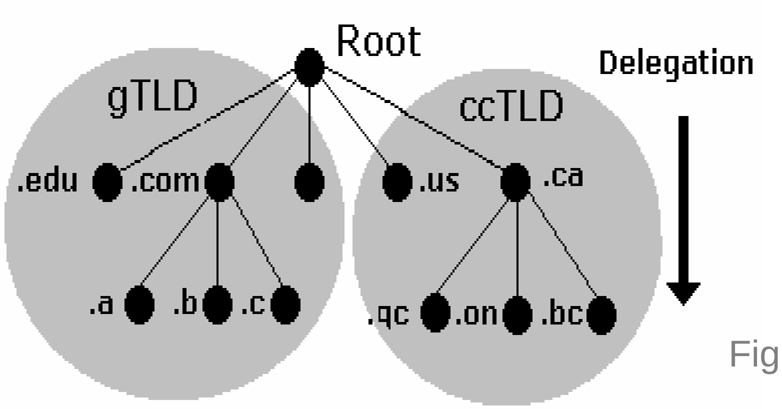


Fig 1.1

Authority and Delegation

The concepts of Delegation and Authority lie at the core of the domain name system hierarchy.

The Authority for the root domain lies with **Internet Corporation for Assigned Numbers and Names (ICANN).** Since 1998 ICANN, a non-profit organization, has assumed this responsibility from the US government.

The gTLD's are authoritatively administered by ICANN and delegated to a series of accredited registrars. The ccTLD's are delegated to the individual countries for administration purposes.

Figure 1.1 above shows how any authority may in turn delegate to lower levels in the hierarchy, in other words it may delegate anything for which it is authoritative. Each layer in the hierarchy may delegate the authoritative control to the next lower level.

Countries with more centralized governments, like India and others, have opted for functional segmentation in their delegation models e.g. .co = company, .ac = academic etc.).

DNS ORGANISATION AND STRUCTURE

The Internet's DNS exactly maps the 'Domain Name' delegation structure described above. There is a DNS server running at each level in the delegated hierarchy and the responsibility for running the DNS lies with the AUTHORITATIVE control at that level.

The Root Servers (Root DNS) are the responsibility of ICANN but operated by a consortium under a delegation agreement. ICANN created the Root Servers Systems Advisory Committee (RSSAC) to provide advice and guidance as to the operation and development of this critical resource. The IETF was requested by the RSSAC to develop the engineering standards for operation of the Root-Servers. This request resulted in the publication of RFC 2870.

There are currently (mid 2003) 13 root-servers world-wide. The Root-Servers are known to every public DNS server in the world.

The TLD servers (ccTLD and gTLD) are operated by a variety of agencies and registrars under a fairly complex set of agreements by Registry Operators.

The Authority and therefore the responsibility for the User (or 'Domain Name') DNS servers lie with the owner of the domain. In many cases this responsibility is delegated by the owner of the Domain to an ISP, Web Hosting Company or increasingly a registrar. Many companies, however, elect to run their own DNS servers and even delegate the Authority and responsibility for sub-domain DNS servers to separate parts of the organisation.

When any DNS cannot answer (resolve) a request for a domain name from a host e.g. example.com the query is passed to a root-server which will direct the query to the appropriate TLD DNS server which will in turn direct it to the appropriate Domain (User) DNS server.

Recursive Query

In a recursive query a DNS server will, on behalf of the client (resolver), chase the trail of DNS across the universe to get the real answer to the question. The journeys of a simple query such as 'what is the IP address of xyz.example.com' to a DNS server which supports recursive queries but is not authoritative for example.com could look something like this:

1. Resolver on a host sends query 'what is the IP address of xyz.example.com' to locally configured DNS server.
2. DNS server looks up xyz.example.com in local tables (its cache) - not found
3. DNS sends query to a root-server for the IP of xyz.example.com
4. The root-server replies with a referral to the TLD servers for .com
5. The DNS server sends query 'what is the IP address xyz.example.com' to .com TLD server.
6. The TLD server replies with a referral to the name servers for example.com
7. The DNS server sends query 'what is the IP address xyz.example.com' to name server for example.com.
8. Zone file defines a CNAME record which shows xyz is aliased to abc. DNS returns both the CNAME and the A record for abc.
9. Send response abc=x.x.x.x (with CNAME record xyz=abc) to original client resolver. Transaction complete.

DNSSEC - Best practices

- **Provide redundant DNS services**

Yes (For every primary server allocated region wise we provide a secondary server for redundancy)

- **Use separate servers for advertising & resolving**

Yes**. All regional are only resolver**

- **Limiting DNS interface access for resolution**

Yes (ACL's are used for limiting the same), IP pool based ACL

- **Restricting and Securing zone replication**

Yes, Maser to Slave

- **Restrict Dynamic updates**

Yes, not enabled

DNSSEC - Best practices …Contd

- **Prevent cache corruption**

By limiting the number of recursive clients 3000 to 5000.

- **Disable recursion**

We allow recursive queries on the resolver but by limiting the number of recursive clients.

- **Filter traffic to name server**

Yes, by running only the required software on the DNS server and allowing only DNS related TCP and UDP packets on port 53.

- **Run the services with least privileges**

The main configuration files /etc/named.conf and /etc/rndc.conf are protected by giving only read and write permission to the owner. And rndc service is configured to listen on localhost on port 953 and is restricted for access from the localhost only. Access control on this port is implemented via TSIG keys and a new private key of 128 bit of algorithm hmac-md5 is generated to control access.

DNSSEC - Best practices …Contd

➢**Source address validation**

Yes (ACL's are used for limiting the same)

➢**Further we have eliminated single points of failure in the DNS infrastructure by having redundant secondary servers to counter DoS attacks.**

➢**Restricted zone transfers to only our own known slave DNS servers, thus preventing hackers from listing the contents of zones and others from taxing name server's resources.**

➢**Protected against spoofing by restricting the addresses to only few clients, the name server will respond to recursive queries from.**

VSNL's DNS Infrastucture

The mid-range Sun Fire V440 [4 CPU, 8 GB RAM] with SunOS 5.9 at Delhi, Chennai, Kolkata, Bangalore, Mumbai and Pune with a failover to Mumbai and being shared with Radius cache applications on the same servers are used.

Region Wise DNS Server Allocation :

Location	Primary	Secondary
MUMBAI	ns4.vsnl.com (202.54.29.5)	ns1pn.vsnl.com (202.54.10.2)
DELHI & Other NORTHERN regions	ns1del.vsnl.com (202.54.15.30)	ns4.vsnl.com (202.54.29.5)
KOLKATA & Other EASTERN regions	ns1kol.vsnl.com (202.54.9.1)	ns4.vsnl.com (202.54.29.5)
CHENNAI	ns1chn.vsnl.com (202.54.6.60)	ns4.vsnl.com (202.54.29.5)
PUNE, AHMEDABAD & Other WESTERN regions	ns1pn.vsnl.com (202.54.10.2)	ns4.vsnl.com (202.54.29.5)
B'LORE, HYDERABAD, ERNAKULAM, VIZAG & Other SOUTHERN regions	ns1bgl.vsnl.com (202.54.12.164)	ns4.vsnl.com (202.54.29.5)

Other VSNL’s DNS servers

DNS Server	Use
dns.vsnl.net.in (202.54.1.30)	For VSNL Infrastructure domains, IP's and few old customers
ns3.vsnl.com (203.197.12.42)	For VSNL Infrastructure domains, IP's and few old customers
MMB4 (202.54.1.18)	For few old customers
ns5.vsnl.com (202.54.49.10)	New secondary server
corpdns (202.54.1.64)	For ILL customers
corpdns1 (202.54.1.63)	For ILL customers

Dos Attack on ns1chn.vsnl.com on December 15, 2006:

It was found that the IP 211.5.176.136 of Japan Network Information Center was querying ns1chn.vsnl.com DNS server continuously for the PTR entry 37.229.17.61.in-addr.arpa at an average rate of 1000 hits/min

Log details are as below:

```
16803  Dec 15 10:27:30.791 queries: info: client 211.5.176.136#1024: query:
37.229.17.61.in-addr.arpa IN PTR
16804  Dec 15 10:27:30.805 queries: info: client 211.5.176.136#1024: query:
37.229.17.61.in-addr.arpa IN PTR
16805  Dec 15 10:27:30.813 queries: info: client 211.5.176.136#1024: query:
37.229.17.61.in-addr.arpa IN PTR
```

So the IP 211.5.176.136 was blocked in ns1chn.vsnl.com DNS server, after which the named process utilization on it has been reduced from 50% to 35%.

Mitigation and Securing DNS

Upgradation of BIND :

The Bind application has been upgraded from version 9.2.3 to latest stable version 9.3.x with the required security and logging.

Rndc Service:

Also rndc service has been configured on all the DNS servers, which allows one to administer the named daemon with command line statements.

So in case if one wants to reload the DNS configuration file “named.conf”, one need not require to stop and start the named process, but instead one can simply reload it by the command “rndc reload” or “rndc reconfig”.

This will reduce the frequent restart of the named process causing the unavailability of the DNS service for few seconds.

Proactive Monitoring of named process load for any attack :

References

1. www.cisco.com/security
2. VSNL Metro Ethernet LLD
3. VSNL DNS LLD

Q & A

?

Our Inspiration

Mr. Ratan N Tata

We must be bold in our actions.

We must always lead – we must never follow!

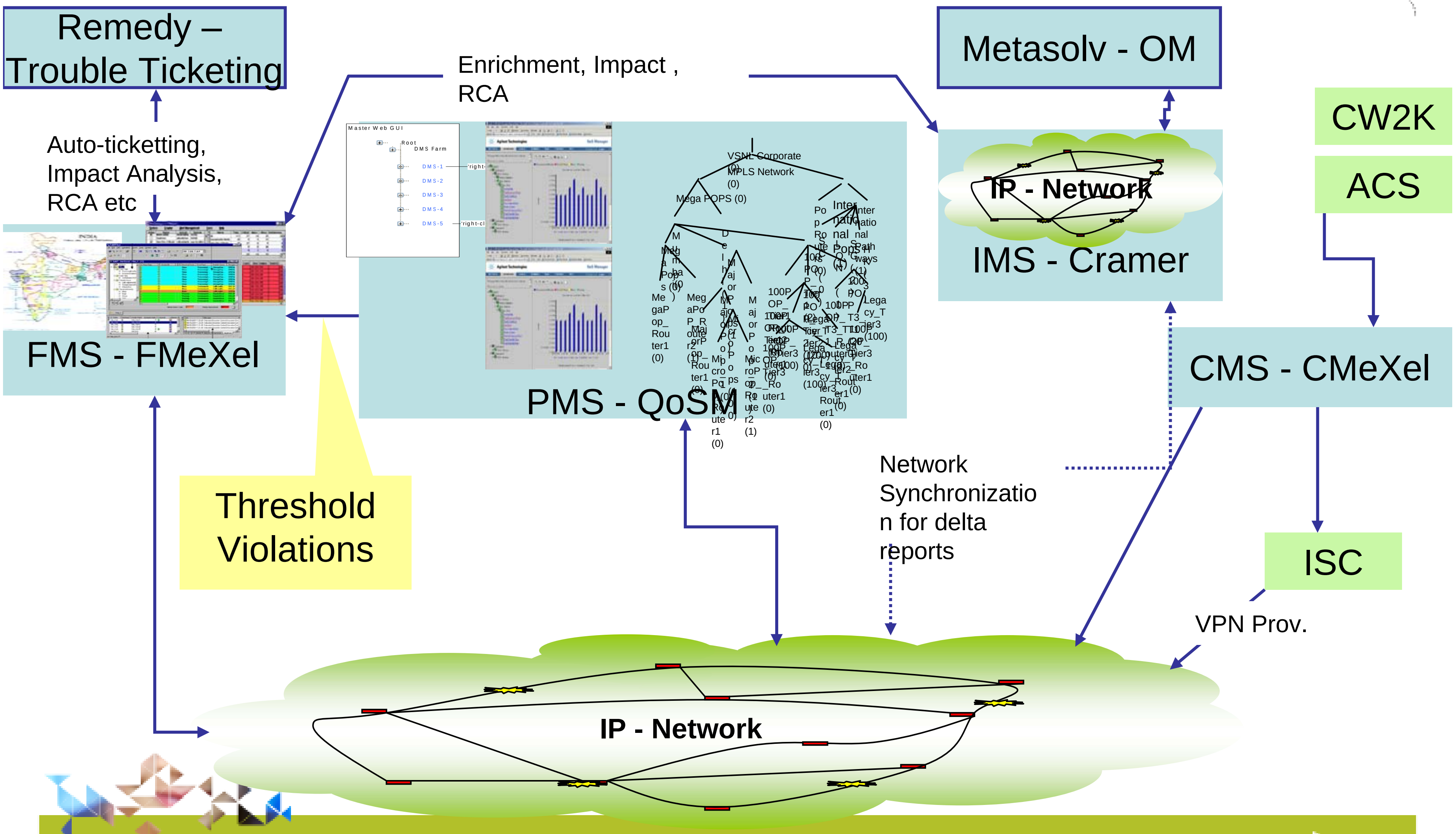
TATA COMMUNICATIONS

Thank you

New Delhi

TATA

CNMS - Proposed Architecture for IP



Remedy – Trouble Ticketing

Enrichment, Impact , RCA

Metasolv - OM

CW2K

ACS

Auto-ticketting, Impact Analysis, RCA etc

IMS - Cramer

FMS - FMeXel

PMS - QoSM

CMS - CMeXel

Threshold Violations

Network Synchronizatio n for delta reports

ISC

VPN Prov.

DNSSEC Best Practices

▪Provide redundant DNS services

- Use separate servers for advertising & resolving
- Limiting DNS interface access for resolution
- Restricting and Securing zone replication
- Restrict Dynamic updates
- Prevent cache corruption
- Disable recursion
- Turn off glue fetching
- Filter traffic to name server
- Run the services with least privileges
- Source address validation

ME - OVERALL NETWORK TOPOLOGICAL VIEW

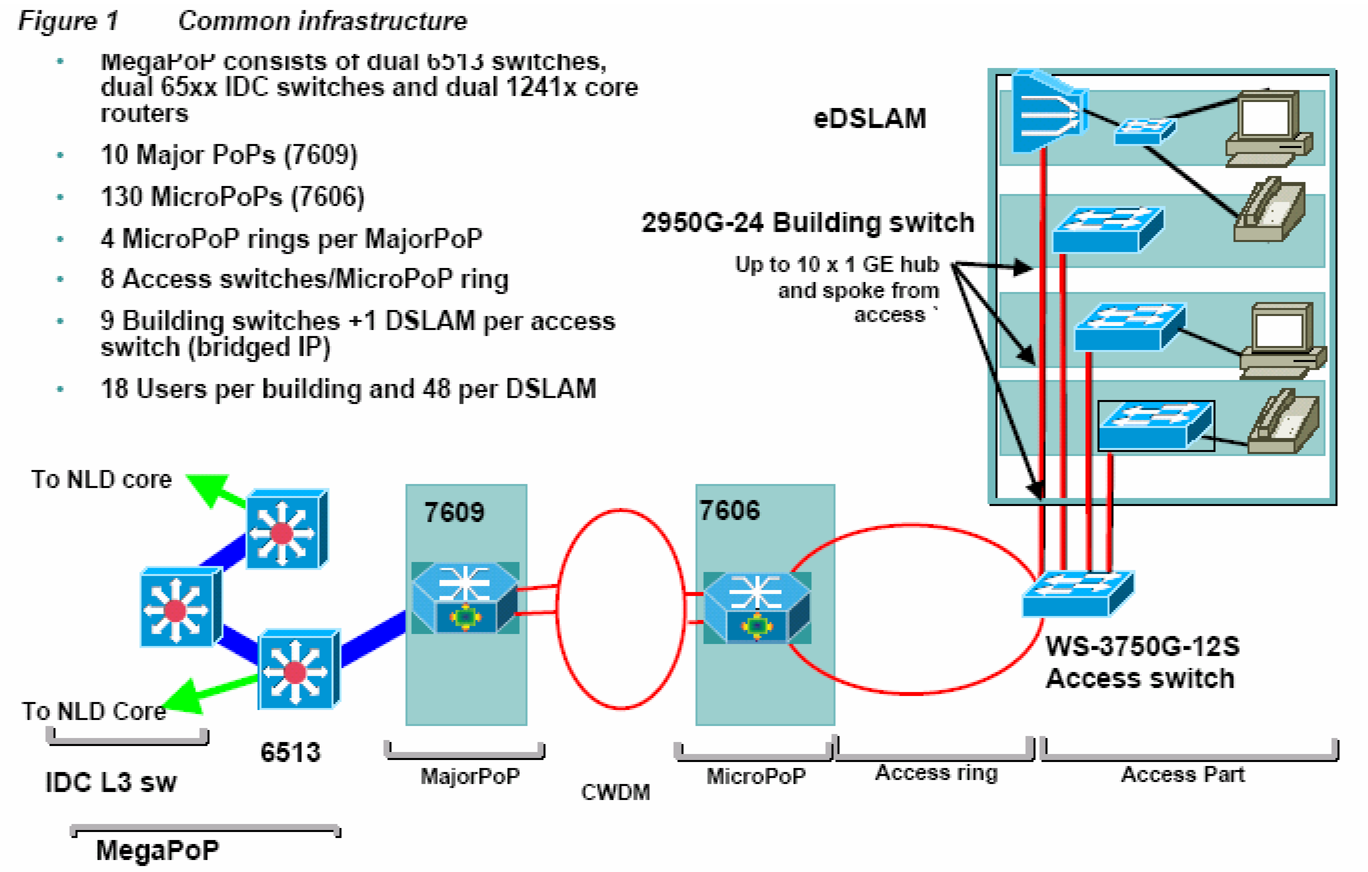


Figure 1 Common infrastructure

- MegaPoP consists of dual 6513 switches, dual 65xx IDC switches and dual 1241x core routers
- 10 Major PoPs (7609)
- 130 MicroPoPs (7606)
- 4 MicroPoP rings per MajorPoP
- 8 Access switches/MicroPoP ring
- 9 Building switches +1 DSLAM per access switch (bridged IP)
- 18 Users per building and 48 per DSLAM

Backbone Capacity Geo Wise

Major Backbone Usage						
	Backbone	Capacity	Usable capacity	In (Mb)	Out (Mb)	G/W % Util
West Coast US (CHN & EKM)	**Backbone**	**8084**	**7592**	**6745**	**1337**	88.84%
East Coast US (MUM)	**Backbone**	**2486**	**2336**	**2158**	**1606**	92.38%
Asia Pacific (CHN & EKM)	**Backbone**	**2798**	**2628**	**1827**	**330**	69.52%
Europe (MUM)	**Backbone**	**1399**	**1314**	**1188**	**1232**	93.76%
Total Major Backbone	**Backbone**	**14767**	**13870**	**11918**	**4505**	85.93%

TATA COMMUNICATIONS

Cable Media Wise Capacity

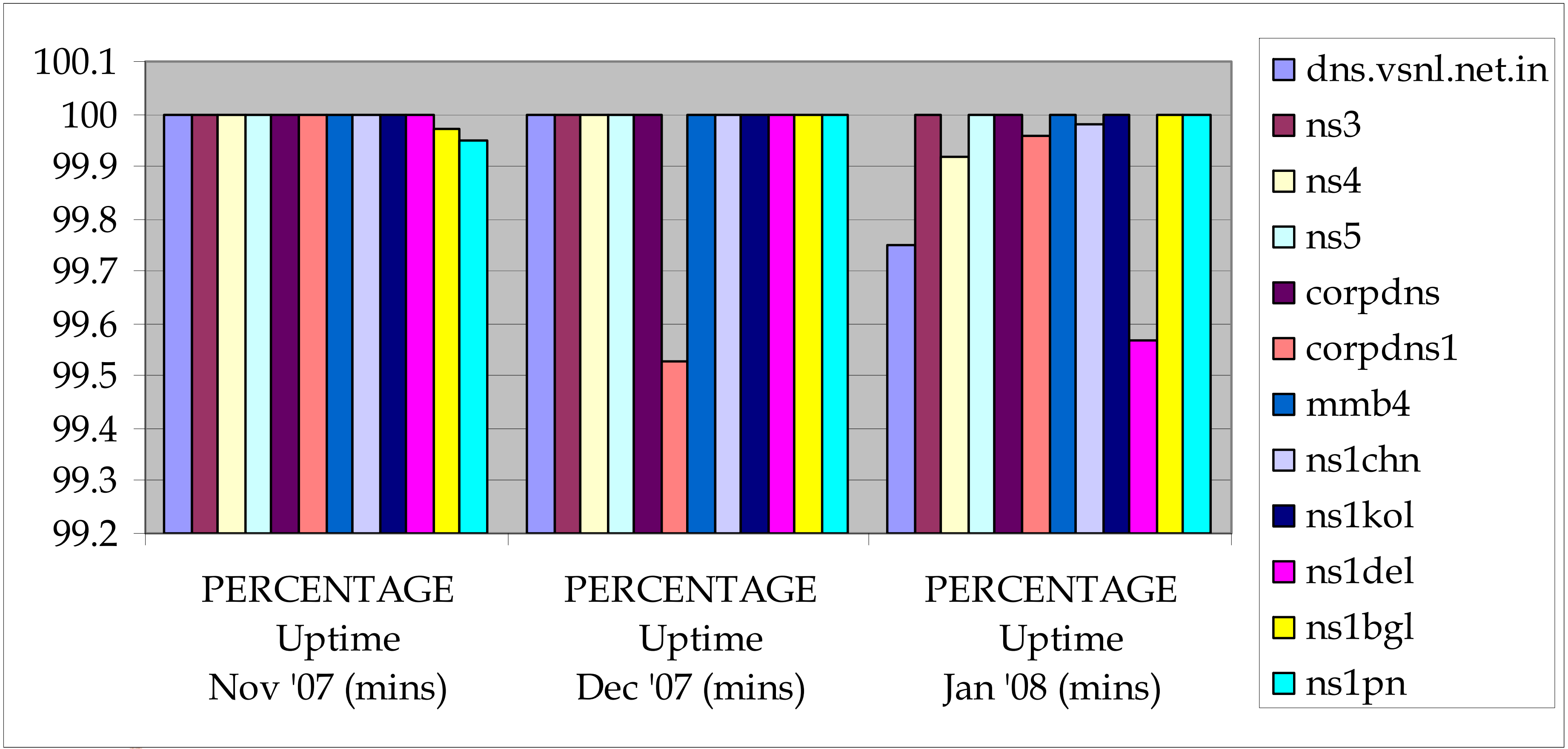
TATA

TOTAL TRAFFIC ON CABLE NETWORK TOWARD INDIA										
Link		Media								
FROM	TO	SMW4	SMW3	SAFE	TIC	TOTAL MB	DS3	STM1	STM4	STM 16
CHENNAI	**SANTA CLARA**				**7464**	7464			**4**	**2**
CHENNAI	**HONG-KONG**				**1399**	1399		**1**	**2**	
CHENNAI	**SINGAPORE**				**155**	155		**1**		
ERNAKULAM	**SANTA CLARA**			**155**		155		**1**		
ERNAKULAM	**Palo Alto**			**465**		465		**3**		
ERNAKULAM	**Hong Kong**		**1244**			1244			**2**	
ERNAKULAM	**STARHUB**		**45**			45	1			
ERNAKULAM	**TM**			**45**		45	1			
ERNAKULAM	**CAT, Thailand**		**45**			45	1			
ERNAKULAM	**TAIWAN**		**45**			45	1			
ERNAKULAM	**Phillipines**		**45**			45	1			
ERNAKULAM	**Korea**		**155**			155		**1**		
MUMBAI	**China Telecom**		**45**			45	1			
MUMBAI	**SINGTEL**		**155**			155				
MUMBAI	**EMIX**	**45**	**45**			90	2			
MUMBAI	**KDDI**		**90**			90	2			
MUMBAI	**London**	**1244**	**622**			1866			**3**	
MUMBAI	**FFT**	**155**				155		**1**		
MUMBAI	**NYC**	**2488**	**1242**			3730		**4**	**5**	
TOTAL FOR IP BACKBONE		3932	3778	665	9018	17393	10	12	16	2
%		22.61	21.72	3.82	51.85					

AS Ratings

ISP	Netconfigs			CAIDA			CIDR		
	17-Jan	24-Jan	7-Feb	17-Jan	24-Jan	7-Feb	17-Jan	24-Jan	7-Feb
VSNL (4755)	25	25	19	54	56	55	112	115	116
TG (6453)	11	10	9	10	14	19	446	439	438
NIB (9829)	62	62	92	379	387	372	102	104	104
Bharti (9498)	24	24	20	51	48	54	90	92	91
Sify (9583)	69	66	69	483	492	494	631	630	634
RIL (18101)	27	27	44	56	57	66	365	363	343

VSNL DNS Server Uptime


PERCENTAGE Uptime Nov '07 (mins)
PERCENTAGE Uptime Dec '07 (mins)
PERCENTAGE Uptime Jan '08 (mins)
dns.vsnl.net.in
ns3
ns4
ns5
corpdns
corpdns1
mmb4
ns1chn
ns1kol
ns1del
ns1bgl
ns1pn