Introduction

Rogers Cable Inc. undertook to completely overbuild the existing Excite@Home infrastructure over a very short period of time due to the business discontinuance of our incumbent supplier. All aspects of the infrastructure were impacted, and the entire service delivery mechanism was transitioned to Rogers Cable's own set of platforms that served more than 500,000 customers.

Details of the transition steps will be discussed first. Secondly, some of the key architecture principles and methods are described. Specific examples of redundancy and fault tolerance aspects are presented along with the intrinsic security features architected and built into the platforms. Thirdly, the operational challenges of managing this newly built infrastructure are described.

Network Overbuild Transition

Excite@Home provided all aspects of the data service delivery for Rogers Cable customers, including regional routing platform, provisioning platform, Internet services platform, content, and exterior transit connectivity. The objective was to completely replace the existing set of platforms and to complete the overbuild in less than a month. This was a rather tall order to accomplish, and was even more challenging to maintain services to our customers during this exercise.

Fortunately, Rogers Cable managed to conclude this transition exercise in the required time period and with minimal impact to the customers. This was only possible through company-wide focus, executive support, careful planning, orchestrated execution, and sheer hard work of literally hundreds of individuals.

The transition was executed in three broad steps.

1. First Phase
    - Build Rogers Cable Regional Network Centers (RNC) that house the IP Network Services (IPNS): DHCP, DNS, TFTP, TOD, HTTP cache
    - Build Rogers Cable Internet Services platform (RISP)
    - Build a stub network and exterior connectivity and connect to the RISP
    - Activate the roger.com email domain in parallel with home.com
2. Second Phase
    - Complete the IP Network build to all sites under Rogers own AS
    - Connect the RNCs to the new IP Network
    - Migrate customers to use the Rogers IPNS located in the three RNCs
3. Third Phase
    - Transition all CMTS elements in all sites to the new IP Network
    - Commence routing announcements under Rogers' own AS
    - Deactivate Excite@Home platforms

The first phase transitioned the IP network services required for provisioning control and to activate the Internet Services that were built to provide all services such as email, news, and personal web space. A stub network was constructed to connect the customers to the RISP and provide access to the rest of the Internet. The RISP was used to activate the subscribers' email domain under rogers.com in parallel to the existing home.com email.

The second phase completed the deployment of Rogers Cable Broadband IP Network (RCBIN) across all serving areas called Primary Hubs (PHUBs), consisting of a core, several regional backbones, access network, RNCs, and the Rogers Cable Management IP Network (RCMIN). Three RNCs were built to serve roughly 1/3 of the customer base, and they provided the key network services to the modems and subscriber CPE such as DHCP and DNS. The RNCs and the IPNS were built before the emergency transition started as part of an overall repatriation plan. However, this plan was superseded when the business continuance transition was necessary.

The third phase moved all of the CMTS elements to the newly built IP network by reconfiguring the CMTS relay agent to use Rogers IPNS (DHCP). One exception was the LANcity legacy platform that was flash cut due the platform's reliance on the regional router as the DHCP relay agent. After all CMTS elements were transitioned, Rogers began to make routing announcements and coordinated the withdrawal of Rogers' routes from Excite@Home announcements. All Excite@Home routers were then deactivated. Transit peering bandwidth was increased to handle the total transferred load. At the same time, aggressive private peering connections were arranged to reduce and control the transit bandwidth costs.

Internet services transition was orchestrated very closely with Excite@Home over a period of several weeks. The email, news and personal web pages were migrated to the Rogers RISP with a series of service deactivation-activation from Excite@Home to Rogers RISP. A set of 'dummy' servers were deployed to handle the numerous error messages that were alarmed to the subscribers as the services were transitioned, and was kept active until subscribers migrated off the Excite@Home specific-built browser. No service transition of this scale goes without a hitch, but such mechanisms as dummy servers and the careful handling and coordination of the transition greatly reduced the volume of calls and minimized service interruptions to our customers.

Another major challenge in the transition was introducing a management network and the necessary tools required to operate the newly built platforms. An emergency set of tools was quickly prototyped and used for the initial transition period. After the business continuance task was met, significant amount of energy was poured into building and strengthening the management infrastructure and the required tools and processes. More about the management and operational aspect are described later.

Architecture

A clearly articulated architecture of platforms is the fundamental principle from which all designs, policies, processes, and procedures are built. Rogers took a systems-level approach to the development of the architecture of the customer delivery network (RCBIN), the management and provisioning network (RCMIN), the IP Network Services platform and the associated RNCs, and the Internet Services platform (RISP).

A careful analysis and assessment is crucial to identify the key policies applied to the function of each platform and/or application, the interfaces, and the flow of information across the interfaces. Primary drivers of the assessment are functional hierarchy, scalability, availability and redundancy, manageability, flexibility, security, control points and cost.

Although the emergency rebuild situation allowed the introduction of many of the key desired architectural features and characteristics, it was by no means a ‘green field’ opportunity. Several important pre-established dimensions constrained the architecture and design. For example, the grouping of customers to HFC segments and its aggregation to individual PHUB locations was already set. However, the main constraint was the availability and path of the transport layer (and physical fiber) that, collectively with the severe time restriction, dictated the overall architecture and deployment.

Rogers Cable Broadband IP Network

The RCBIN connects the subscriber CPE to the provisioning and network services platform (at the RNC) and carries customer traffic to/from the Internet and to the Internet services platform (RISP). This network was built with three functional network layer hierarchy: core, distribution and access layers. This approach allows separation of functions to specific layers, provides modularity to facilitate network changes and growth, and reduces operational complexity and improves problem isolation.

The Core is composed of the four largest PHUBs in Rogers, arranged in a physical ring of multiple OC-48 POS infrastructure. The Core provides the main ingress/egress points for the Rogers customers base. The remainder of PHUBs are grouped into the Regional Backbone networks connected in an open ring that lands on the Core at two different locations to provide failure protection.

The Distribution Layer is located at all individual PHUB locations, and it represents the demarcation point between the access and core layer of the network. This layer provides a control point to effect policy-based connectivity. Functions implemented at this layer include address or area aggregation, routing between access and core, CMTS aggregation and connectivity, broadcast/multicast domain definition and limitation, and security measures (reverse path forwarding is a function of this layer).

The third tier in the network hierarchy is the Access Layer, and this layer provides access to the rest of the upstream network. The layer consists of switches (Layer 2 or Layer 3 enabled) and the individual CMTS elements. At this layer, the HFC serving areas and the associated CMTS/CM platforms are segmented into networks. This layer provides many control functions as well such as DHCP relay agent for provisioning and authentication, ACL and subscriber access control, and blocking of broadcast forwarding.

Rogers Cable Management IP Network

A logically separate management network (RCMIN) was incorporated to all network elements for provisioning transactions and for management visibility, access, and control. The RCMIN is a mediated control layer that provides access to and control of service-delivery network elements and servers. Two primary planes of flows through RCMIN are management traffic and provisioning transactions.

Tunnels and firewalls are used to connect to the management port of all network elements and to the RNC for management and provisioning transactions. Console port access is also implemented to allow access during failures and diagnostics, either through the native RCMIN or via dial-up. Secured VPN for staff provides a third tier of access for problem resolution and maintenance window activity from remote locations. The RCMIN also house the Management Core Services (MCS) to support the activities of the Network Operations staff. Services include Radius AAA, TACACS+ AAA, DNS, DHCP, syslog, and configuration repository.

The RCMIN is also the gateway for the provisioning flows. It is the gateway between the RCBIN elements and subscribers and the back-office billing system, which is located within the Rogers Enterprise Network (REN). A well-defined perimeter was built to interface these two networks, and is strictly managed to established policies. Customer order entries are propagated from the billing system to a provisioning workflow engine that generates pre-established set of transactions that are pushed out to the IPNS platform to fulfill the orders.

Redundancy and Reliability

The network architecture incorporated many facets of redundancy and fault tolerance to minimize service interruptions and to maximize service reliability. Careful analysis was conducted to optimize the greatest amount of fault protection against cost and scope of the failure impact. Such trade-off and optimization is a key and necessary exercise to conduct to ensure the service delivery infrastructure meets the service and business requirements. The objective was to ensure that there are no single points of failure in the Core, Regional Backbone, upstream connectivity (transit and private peers), and IPNS connectivity.

The Core network layer of the RCBIN was built in a ring topology, with each Core site possessing two GSR-class routers for fault tolerance. All the other sites (PHUBs) were connected in a 'petal' arrangement that connected to the Core layer in two different core sites. This composition provided fault tolerance for the regional backbone networks. Only a few of the small PHUBs sites were connected using a stub connection to minimize the cost.

At the system level, reliability was achieved through routing mechanism such that any fiber path or interface failures will trigger the packet delivery on the opposite path. For example, if one of the core GSR failed, then the routing advertisement will stop from the failed unit and will cause the other working router to assume the traffic away from the failed unit. At the distribution layer, if one of the Layer 2 aggregation elements fail, then those CMTS platforms that have routing intelligence use the routing protection mechanism to by-pass the failed element; and for those CMTS platforms that do not have the routing capability, HSRP is used to achieve the equivalent fault tolerance.

For the transit peering, we acquired diverse circuits that terminated at two separate locations (New York and Chicago). For private peering, we were not able to obtain a similar diverse path, but any failed peering traffic would then traverse the transit links. Most recently, however, Rogers established dual ingress/egress points to the Internet via two separate upstream providers to significantly enhance the reliability and to minimize operational cost on the transit links.

The RISP was a unique platform because Rogers outsourced the design, deployment, and management of the services to a service bureau (HP). Rogers interconnected to the RISP demarcation with dual GSR connectivity (with diverse paths) along with the same component-level redundant cards as the core units. Although not directly linked to the network overbuild, the underlying HFC platform is also deployed in a ring topology to address this portion of either fiber or link failures.

At the network component level, each of the GSRs has dual route process modules, dual power supplies, and redundant switch fabric. At the aggregation element that connects all CMTS units at each of the PHUB, there are dual supervisor modules to enhance the system availability. At the facility level, GSR and Layer 2 aggregation units have dual power feeds (distinct UPS per power supply). Fiber conduits are fed into the PHUBs from two different entry points to further minimize common or single points of failure.

The three RNC sites were also heavily protected due to the mission critical nature of the services they provide to the customers. Each RNC has load balancers with diverse paths to the core and to the IPNS servers and applications. Servers are either clustered (TFTP) or load balanced (DNS and HTTP Cache). Key IPNS servers have redundant power supplies, CPU modules, and network interfaces. In some cases, we have redundant servers as well. All systems possess dual, hot-swappable, mirrored disks. Critical databases in the central site are clustered. Wherever possible, back-end application flows were protected against any single server outage. Each RNC also contains a Jumpstart server that can rebuild a catastrophic failure of any server/application by automating the reconstruction of the operating system, all appropriate patches, and the necessary configurations.

The three RNCs were built to handle 2/3 of the peak load requirements such that any one RNC failure will not impact the services to the subscribers. Key services such as DHCP have application ‘keep-alive’ protocol to quickly and seamlessly fail over to the alternate RNC and the TFTP service has failure detection mechanism.

For the management flows, there are multiple links via diverse transport networks to reach the network and server elements. The main connectivity is through encrypted tunnels over the RCBIN and an alternate path via a separate, pre-existing network. Moreover, elements can be also reached through the console port concentrator through native network connection or via dial-up. For the RNCs, there are dual RCMIN routers due to the critical nature of the management flows (diagnostics and provisioning) that must be highly protected.

Security

In any service delivery business, security is a prime technical and business consideration, especially in the Internet industry, for both the provider and customers. A fundamental precept of security is that it is a system property—that is, security must be considered, incorporated and maintained as an intrinsic property of the architecture and design as a whole. Security is not an adjunct that gets bolted to the infrastructure after the platform deployment, or a separate entity with loose interdependency to the service delivery layers.

Security Approach & Methodology

Security management consists of interdependent layers: (bottom-up) network, servers, application, people and processes. Each of the security layers depends on the layer below. Security assessment must be conducted platform by platform, with the recognition of the platforms’ interdependency. This approach ensures that the necessary and appropriate measures are designed and built into the system.

The security assessment starts with the classification of the different threat vectors. Threats from both the external (public) and internal threats (employees) must be accounted for, such as hacks, denial of service, service interruptions, fraud, and vandalism. All threat vectors possess business implications and customer impacts. Knowledge of what threats exist and their potential impact initiates the specific defense strategy formulation.

The next step is then to understand and identify the elements of network interconnection and the elements of server interconnection with the network. Security architecture shape is formed through the grouping and separation of different communities. The community flows are analyzed and appropriate flow rules are created to meet these business requirements. The flow rules are then managed and enforced via frontiers and perimeters as the managed control points.

The different networks (RCBIN, RCMIN, and REN) described in this paper were strictly segregated to establish and to maintain security and control via this mechanism of frontiers and perimeters. Each of the networks has differing security requirements dictated by the nature of services provided and by the flows: the RCBIN by definition faces the customer/public side and thus is least trusted and consequently must be highly defended; the RCMIN is the intermediary that hosts the management and provisioning flows between the RCBIN and the REN, and is treated as medium trust level with lower defense requirements; and the REN is the most trusted network that has the back-office elements.

RNC Security Description

A good example of the layered defense constructed is the manner in which the RNC was constructed from the network security perspective. The RNC hosts the IPNS to the customers and thus a ‘nuclear missile silo’ approach was taken to survive extreme and direct attacks. Specifically, only specific protocols were activated and flows from known source addresses were allowed into the RNC servers. All non-essential, unnecessary processes on the specific servers were shut down, installing the minimum packages required per application function. Each server in the RNC handles only one application/process to minimize failure recovery time and to support ease of capacity upgrades. All relevant security patches were also applied and maintained. Failure at a single RNC was backed up with other RNC units. This represents the customer facing interfaces on the RCBIN.

On the back-office facing side in the RNC (the RCMIN), all servers have a server-to-server only connection with a firewall in between (RCMIN frontier), transitioning into the central site server domain. This transition represents a layered defense mechanism with increasing security the deeper a flow traverses the interfaces from the public side to the back-office side. Another frontier (firewall) is established between the RCMIN and REN, inline with the security architecture of increasing layers of defense and security control points. In essence, the frontiers were deployed to manage flows explicitly from lower to higher security levels. Higher to lower flow was permitted, but flows from low to high security levels were minimized or eliminated.

From the user policy perspective, access to servers was strictly limited by blocking unauthorized user access and/or visibility of network elements, provisioning systems and management systems. Those users that do require access, such Network Operations, each have individual accounts that must be authenticated and logged for all activities using AAA and Radius facilities. In addition, tiered privilege levels with standard command sets per privilege level were established to meet individual departments’ role and accountability.

Other security rules and principles applied include:

- Limit the number of systems accessing the network elements directly;
- Mediate business systems' interaction with network elements;
- Business systems interact with provisioning or management systems;
- Only provisioning/management systems access the network elements;
- Document configuration change requests to ensure policies can be traced back to initiating business requirements;
- Validate any security change request for compliance to security architecture.

Operation Setup and Challenges

Since the repatriation of all the services from Excite@Home in January 2001, Rogers Cable has been exploring different network management models to operate its extensive IP networks covering Ontario, New Brunswick, Newfoundland, and the four data centers hosting the various Internet and Network Services Applications. The operations of the Rogers Internet Services Platform (RISP) including POP/SMTP mail, WebMail, NNTP news, Personal Web Space, and Member Services are out-sourced to Hewlett Packard Canada (then Compaq Canada) Managed Services division. All the rest are operated internally by Rogers' personnel.

At the end of this paper, we will touch briefly on the operations of the HP-managed RISP. First, let us look at how the IP Backbone network and Internet Network Services platform are run and operated by Rogers' staff. These network services include: DHCP for CPE and modems, authoritative DNS for rogers.com domain, caching DNS, TFTP and TOD for modems, and HTTP caching. Rogers has decided to adopt the ISO FCAPS model of operations. The FCAPS model will be reviewed in the following sections, which also describe how we realize this model in Rogers. For details about this model, please refer to M.3400 TMN Management Functions, an ITU-T publication.

FCAPS

ISO FCAPS is an acronym for a model of network management objectives. There are a total of five levels: “F” stands for fault-management, “C” stands for configuration management, “A” stands for accounting, “P” stands for performance management, and “S” stands for security management.

For Fault Management, network and systems outages are discovered and restored by the Service Management Center (SMC). Potential problems are identified and steps are taken to keep them from occurring or recurring. As a result, the network and systems are kept operational and downtime is minimized. Backup and restore procedures are documented and exercised by SMC personnel to ensure minimum MTTR (Mean Time To Restore).

With more than 650K customers, it is important that timely communication be given to the Customer Care group when an outage occurs, so that they can in turn speak intelligently to customer inquiry. We have established an efficient notification process by which alert messages will be posted to the affected CRM (Customer Relationship Management) accounts within 15 minutes of the outage. The prerequisite for this notification process to be successful is an accurate topology database that maps every customer to network and system elements. This allows all customer accounts affected by such element failure to be easily identified and retrieved. Using ANI (Automatic Number Identification) feature, an informational message can also be automatically played back to the affected customers when they call to inquire about the service outage. Our experience shows that this notification process can effectively reduce by 50% such calls hitting a live agent, thus reducing the overall operating cost.

For Configuration Management, operation of the network and system is monitored and controlled. Hardware, firmware, and software changes, including the addition of new equipment and applications, modification of existing systems, and removal of obsolete systems and programs, are coordinated. An inventory of equipment and software is kept and updated regularly.

In Rogers, the Service Management Center is fully accountable for any changes to the production environment. Only this group has enable 15 and root privileges on network and system elements. This is the only group allowed to promote any changes to production. They do so by following a pre-established MOP (Method Of Procedure) for any change. The MOP is a change management document that outlines in great detail all the steps necessary to execute the desired change. It is first reviewed with architecture and engineering groups to ensure completeness and accuracy. An added advantage is that through these review sessions, proper technology know-how can be transferred to SMC personnel that also equip them with the necessary knowledge for performing their ongoing operations and maintenance of the network and systems. Our experience has shown that with this knowledge transfer process in place, the amount of escalations for assistance to the architecture and engineering groups has been drastically reduced.

Accounting, which might also be called the Allocation level, is devoted to distributing resources optimally and fairly among customers. This makes the most effective use of the systems available, minimizing the cost of operation. This level is also responsible for ensuring that users are billed accordingly. It is believed that the launch of Usage Based Billing (UBB) will reshape the amount and type of traffic generated by the end users. This may have a positive impact on the transit cost to the Internet that we incur. In addition, the accounting information can assist in analyzing traffic irregularities and bandwidth bottlenecks. Our Capacity Planning group can leverage the results from these analyses when planning for capacity uplift to ensure end-customer satisfaction.

Performance Management is involved with managing the overall performance of the network and systems. Throughput is maximized, bottlenecks are avoided, and potential performance problems are identified. A major part of the effort is to identify which improvements will yield the greatest overall performance enhancement. Two different aspects of performance measurements can be identified: parametric measurements and end-customer experience measurements. The former set of measurements identify performance issues of the network and system devices themselves, such as CPU and memory utilization, transaction queues, bit error rates, packet losses, etc. The later set is trying to emulate end-customer experience by putting drone machines in strategic locations of the network and measuring response times, latency, download times, etc. of client applications such as email, news, HTTP browsing, DHCP, and DNS. These two sets of measurements are mutually exclusive and equally important in order to analyze the true performance of the services. We are currently evaluating such performance management applications that will be run on the drone machines at the data centers, the headends, and selected customer premises.

With Security Management, the network and systems are protected against hackers, unauthorized users, and physical or electronic sabotage. Confidentiality of user information is maintained where necessary or warranted. The security systems also allow network and system administrators to control what each individual authorized user can (and cannot) do with the system. In order to succeed, a company has to institutionalize security as part of the culture, from the CEO to the front lines.

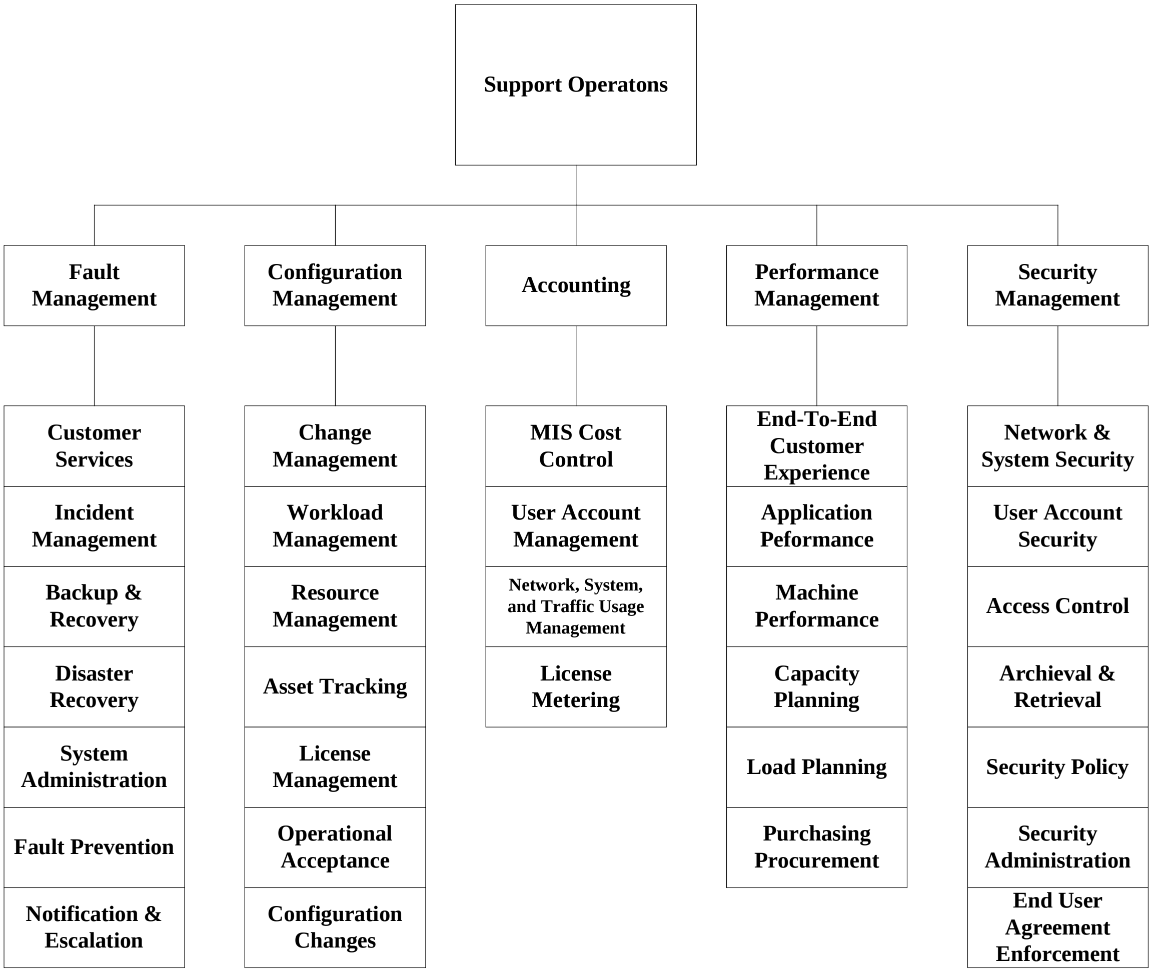
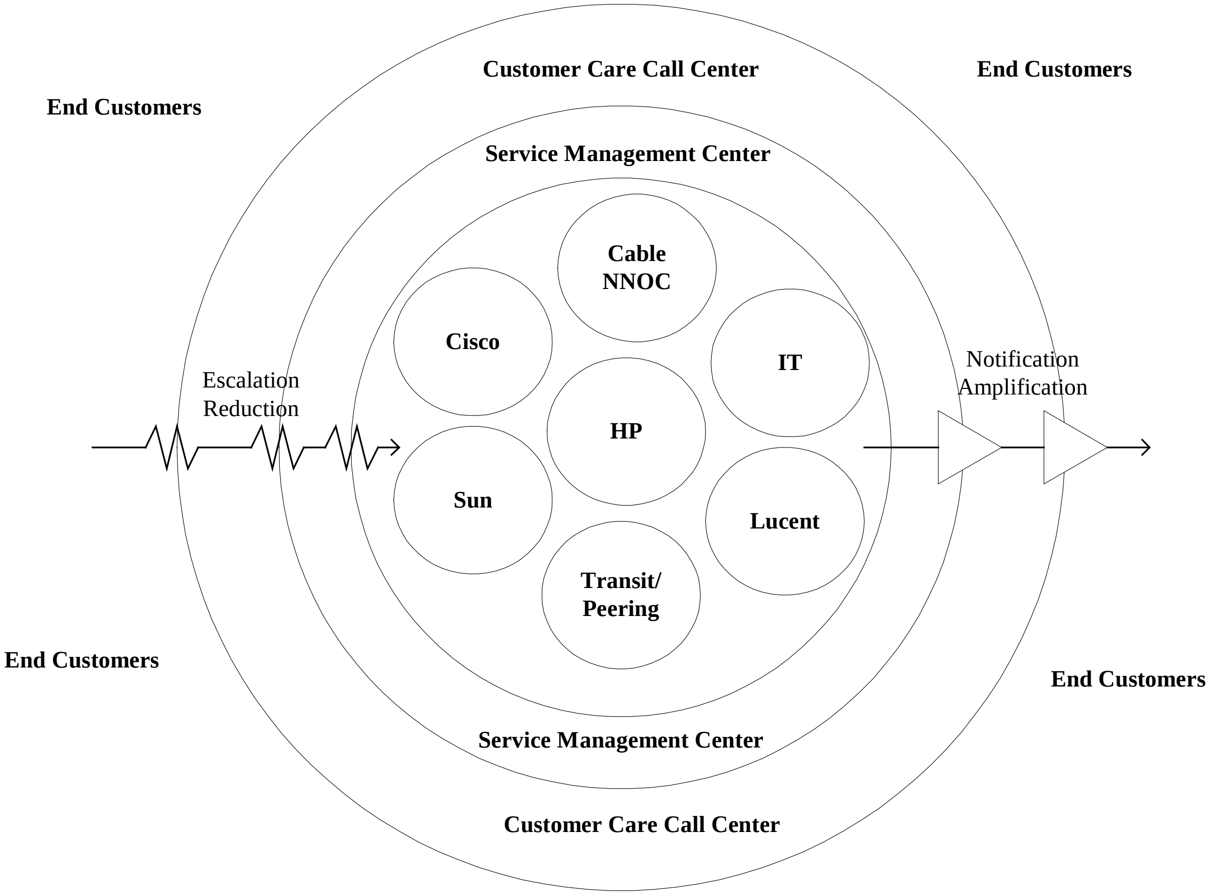


Figure 1: ISO FCAPS Model

Internet Service Management Center

Let’s look at how Rogers implements the FCAPS model. Internet Service Management Center (SMC) is a group within the Engineering & Network Operations Department dedicated to the ongoing operations, maintenance, administration and provisioning of the networks and systems delivering and supporting the Rogers’ HiSpeed Internet services. The primary mandate for this group is to stabilize the platforms. The following diagram depicts the placement of this group within the organization.


Customer Care Call Center
End Customers
End Customers
Service Management Center
Cable NNOC
Cisco
IT
Escalation Reduction
Notification Amplification
HP
Sun
Lucent
Transit/ Peering
End Customers
End Customers
Service Management Center
Customer Care Call Center

The Internet SMC is composed of the following teams.

7x24 TAC (Technical Action Center)

Working around the clock, this group is accountable for the Fault Management of the network devices, server systems, applications, and the end-to-end services as well. Members of this group have diverse knowledge with the overall operations and inter-working of the various components. Usually CCNA and Sun Solaris Administration I certification are expected skills. The area of responsibilities includes the modems, CMTS', switches, routers, servers, applications, escalations to transit providers, and SLA interface with HP on the RISP platform.

Process consistency is the key success factor for this group. Time-based notification and escalation has been institutionalized to ensure expedited outage restoral by the appropriate groups and also keep interested parties in the company apprised of outage situations.

Extensive use of Network Support Systems is another key component of this operation. All network incidents are tracked by the Remedy ticketing system. A combination of BMC Patrol, SNMPc, and HP OV are used as the proactive surveillance tools, alerting the duty staff of events. Custom-built scripts are then run by the duty operator in order to further diagnose and isolate the problem. Restoral action is either initiated directly by the duty staff, or if it is of a more complicated nature, it will be escalated to the on-call platform specialists.

The mandate for this group is to not miss any outages, and to restore any outages within the pre-defined timeframes. Leveraging the 7x24 nature of this group, a lot of routine / proactive maintenance and auditing tasks can be performed during the quiet times of the shifts. This group also acts as the policeman for change control, making sure any changes to the production systems are properly approved and that personnel is authorized to do the work.

Server & Application Operations

A group of Unix, Database, and Application administrators provide technical support to the TAC. They share the accountability of maintaining the ongoing operations, maintenance and administration of the various Unix servers, databases and applications. This group is composed of senior Unix and database administrators. Currently we have more than 150 Sun servers located in four data centers. While OS and database experiences can be acquired through proper recruitment, there is no easy substitute for acquiring application knowledge other than on-the-job training. The Lucent QIP/VA application is used exclusively for DHCP, DNS, TFTP, TOD network services. Network Appliance's netcache product is our HTTP proxy. Knowledge also has to be gained on the NSS systems, such as the Remedy AR system, BMC Patrol, SNMPc, HP OV and Spectrum. A couple of Perl and SQL programmers in this group are also instrumental in developing customized diagnostic scripts for the TAC. Only this group has root privilege and they are fully accountable for any changes to the production systems.

The challenge for this group is the diverse knowledge required for the hardware, OS, databases and applications. As more products are developed and offered to the end customers, so is the number of applications introduced to operations. This group is projected to have the highest growth in knowledge in the coming years.

IP Network Operations

With more than 50 POPs across the network in Ontario, New Brunswick and Newfoundland, a focus group of Cisco certified professionals (CCNP and CCIE) are charged with the care and feeding of these network devices every day. A lot of redundancy has been built into the design of the core IP backbone and the exit points to the Internet. The most vulnerable elements are the aggregation switches and CMTSs in each POP, which because of economic reasons, are not protected. We found most of the challenge is the timely recovery of network equipment after a failure. A network support maintenance agreement is used to ensure timely delivery of RMA spares to these sites. The economics have been carefully studied to decide whether to outsource the RMA process or stock appropriate spares in our own depots.

It is not surprising to understand most of the outages are human-introduced during construction and changes. In order to minimize these outages, an elaborate change control process has to be institutionalized in the whole company. In Rogers, full operational accountability resides with the Network Operations Department. Therefore any changes to production IP networks can only be executed by the IP Network Operations group. An added benefit of this policy is the enforcement of proper documentation and knowledge being transferred from the architects and designers to this operations group.

Network Provisioning Operations

Like most MSOs, Rogers has been actively upgrading the HFC and IP networks to support better quality and more types of services. Rebuilding existing nodes to smaller size with shorter cascade may result in different CMTSs feeding the affected customers. IP address allocations have to be carefully tracked and augmented to meet the demand on change. In addition, as sales continue to grow, CMTS and DHCP servers need to be allotted more IP subnets on a day-to-day basis. The process to relieve CMTSs from congestion as the number of customers grows can be very complicated and includes the coordination of many groups.

To support all of these time-sensitive activities, a Network Provisioning Group was formed. Key success factors for this group include quality control (since they are working on a production environment), timely deliverables to meet growth, and cost control. Their work is greatly assisted by our highly accurate and complete configuration and topology databases, which account for all customers, modems, optical nodes, CMTSs, and POPs in the network.

Network Security & Fraud

As with any ISP, managing network security and fraud is a daily activity. With more than 650K Internet users we attract and originate a lot of security incidents. An EUA (End User Agreement) enforcement group has been setup to educate our customers and to protect the brand from being blacklisted by other ISPs. If fraudulent behaviour and/or violation of the EUA is detected, progressive disciplinary actions against the violators are exercised to protect other users and the Rogers brand.

Denial of Service (DOS) attacks and hacker attempts to compromise our network and system devices have to be guarded against. A set of governing network security policies to identify what needs to be protected, and in which manner, should be outlined. Operational procedures for SIRT (Security Incident Response Team) compliance to lawful intercept and warrant requests, etc. can then be established.

HP Managed RISP

As mentioned earlier, Compaq (now Hewlett Packard) Managed Services are engaged to operate some components of the HiSpeed Internet services. A three-year contract has been signed with HP to offer managed services for the day-to-day operations, maintenance, administration and provisioning of our RISP (which includes emails, NNTP, Personal Web Space, Member Services, Provisioning Applications for these services, and Diagnostic Tools on these services for TSRs). This contract is centered on an SLA that specifies the performance levels for each of these services that HP must deliver. In order to meet the SLA, HP established a dedicated Tier 3 and Tier 4 support specialist center on site in the same building where the RISP data center resides. This enables HP specialists to attend to any problems promptly. A QA environment is also available on site in close proximity to the production system. This QA environment allows issues and proposed changes to be tested and analyzed in a captive environment in preparation for promoting them to production.

Moreover, HP has dedicated a group of management staff to look after the RISP data center and the supporting staff. They have a very close working relationship with Rogers operations management. Daily, weekly and monthly meetings are conducted to ensure any issues are promptly raised and addressed. The close proximity of their technical specialists to the data center and of their management staff to Rogers is a big contrast compared with our previous engagement. This mode of operation has proven to be very effective.

Summary

After disengaging from Excite@Home two years ago, Rogers developed the Internet SMC dedicated to run and operate the HiSpeed Internet services. The popular FCAPS model in the telecommunication industry is adopted to provide an operational framework. There is no reason why the same model cannot be applied to other advanced services such as Digital TV and IP Telephony services in the future. The operations of the Email, News, PWS, and Member Services are outsourced to Hewlett Packard under a three-year contractual agreement.

Acronyms

AS	Autonomous System
ANI	Automatic Number Identification
CCIE	Cisco Certified Inter-network Expert
CCNA	Cisco Certified Network Associate
CCNP	Cisco Certified Network Professional
CMTS	Cable Modem Termination System
CRM	Customer Relationship Management
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
EUA	End User Agreement
FCAPS	Fault, Configuration, Accounting, Performance, Security
HFC	Hybrid Fiber Coaxial
IPNS	IP Network Services
MOP	Method Of Procedure
MSO	Multiple System Operator
MTTR	Mean Time To Restore
NNTP	Network News Transfer Protocol
POP	Point Of Presence
PHUB	Primary Hub
PWS	Personal Web Space
QA	Quality Assurance
RCBIN	Rogers Cable Broadband IP Network
RCMIN	Rogers Cable Management IP Network
REN	Rogers Enterprise IP Network
RISP	Rogers Internet Services Platform
RNC	Regional Network Center
SIRT	Security Incident Response Team
SLA	Service Level Agreement
SMC	Service Management Center
TAC	Technical Action Center
TFTP	Trivial File Transfer Protocol
TMN	Telecommunication Management Network
TOD	Time Of Day
UBB	Usage Based Billing