Southwest Arkansas Telephone Cooperative
Network Management Practices

Introduction

This disclosure applies solely to the broadband services offered by Southwest Arkansas Telephone. SWAT may revise this disclosure from time to time without notice by posting a new version to the SWAT website at http://www.swat.coop . In the event of a conflict between any subscriber agreement or the Acceptable Use Policy and this disclosure, the terms of the subscriber agreement or Acceptable Use Policy shall govern. This disclosure does not create enforceable rights in the subscriber or any third party edge provider.

Southwest Arkansas Telephone Coop (SWAT) operates a robust and modern IP network, which serves 7 exchanges in Arkansas and 1 in Texas. Over this IP network we provide a variety of services including Voice, Video and Broadband Internet. SWAT operates 3 network edge locations forming our connection to the outside world for Internet access. SWAT operates with a N+1 redundancy philosophy, which is the foundation for providing both a resilient service as well as a built in spare capacity pool in emergencies or unforeseen capacity demands.

Core Network Overview

SWAT utilizes a 10Gig core network to transport all services. Traffic is segmented into separate virtual routing and forwarding implementations based on service category (network management, voice, video, data, etc) however no prioritization or discrimination of forwarding traffic is performed, either within a service type or between service categories.

Distribution Network Overview

SWAT utilizes 10 and 1Gig distribution rings to transport all services. Traffic is segmented into separate virtual routing and forwarding implementations based on service category (network management, voice, video, data, etc) however no prioritization or discrimination of forwarding traffic is performed, either within a service type or between service categories.

Access Network Overview

SWAT operates 2 separate access networks with 3 service types:

- A PPPoE authenticated, DSL only network
  - This is our legacy network, which is being overbuilt by our unified access network.
  - This network transports strictly Broadband Internet and performs no prioritization or discrimination of forwarding traffic.
  - Bandwidth packages available range from 1.5Mbit to 3Mbit.
- A unified access network supporting Voice, IPTV and Broadband Internet.
  - This access network supports both ADSL2+ deployments as well as FTTH (both GPON and ActiveEthernet).
  - Bandwidth packages available range from 1.5Mbit to 100Mbit

- The access network, “last mile” does prioritize certain Non-BIAS data services (specialized services) above Broadband Internet. Specifically;
  - IP Voice
  - IPTV (if the customer subscribes to this service)

Network Edge Overview

Currently SWAT operates 3 network edge locations (Internet drains), these locations are:

- (2) in Dallas Texas
- (1) in Arkadelphia, Arkansas

SWAT has contracted sufficient capacity at each location to ensure that loosing any location or the largest link between locations would not cause congestion under normal peak load conditions.

SWAT does not discriminate, prioritize or block any legitimate forwarding traffic at our network edge locations.

General Network Principles

SWAT, as much as reasonably possible, designs and operates its network based off of the following guiding principles:

- Where at all feasible, sufficient external bandwidth must be secured to allow the largest edge location to fail or the largest inter-site link to fail and still not suffer congestion during normal peak load utilization.
- The core and distribution networks should focus on forwarding traffic at the highest possible rates with no prioritization or traffic discrimination. For security purposes network traffic should be categorized into discreet service types and segmented via separate VRF and VLAN segments. Specifically this references segmenting management traffic, ILEC voice traffic, IPTV traffic and Broadband Internet traffic.
  - The access network is directly facing the customer. The last mile loop is a dedicated resource to a specific customer however because of last mile technology constraints it has the highest potential for congestion. SWAT does prioritize certain Non-BIAS data services (specialized services) above Broadband Internet. Specifically;
    - IP Voice
    - IPTV (if the customer subscribes to this service)
- All subscriber Broadband Internet packages should be provisioned slightly larger than advertised to allow for protocol overhead so that the customers expectations are exceeded whenever possible.
- Maintaining the security of the network is a top priority as such we will operate with commonly accepted security best practices.

Network Practices

Non-Discrimination Practices

With the exceptions listed under security practices, SWAT does not apply any prioritization, rate limiting or blocking based on source, destination, protocol or port. SWAT reserves the right (but does not undertake the responsibility) to block or degrade content, applications and services that are unlawful, that may violate the rights of third parties (e.g., copyright infringement) or that may pose a harm to our network or other customers.

Device Attachment Rules

SWAT does not restrict what types of devices are eligible to connect to our network, however we can only provide direct end user support for devices for which we are familiar. In addition all attached devices must be capable of making a valid access request (DHCP or PPPoE depending on network segment). At each demarcation we provide a single ethernet port for Broadband Internet and if a subscriber wishes to use multiple devices, the customer will need to provide their own router, which will provide NAT. For residential service, each demarcation point is dynamically assigned a single public IPv4 address. For commercial service, multiple IPs are available if needed.

Security Practices

In an effort to maintain the security of the SWAT network and our subscribers as well as to abide by good Internet Citizenship, SWAT utilizes the following listed security practices, which affect forwarded traffic delivered to our subscribers. In addition to this list, SWAT utilizes multiple other mechanisms to sustain the Confidentiality, Integrity and Availability of the SWAT network, however only those having a direct bearing on customer forwarded traffic are listed here.

Access Network

- Subscriber MAC addresses are tied to a valid authentication request (for PPPoE) or validated DHCP request (utilizing option 82 tracking). IP addresses that are not properly requested / authenticated are not permitted to pass any traffic.
- Only traffic destined for a valid IP/mac address pairing is terminated to a subscriber, broadcast flooded traffic is not delivered to the end user.
- All ARP requests within the access network are handled via proxy.

- An end subscriber that sustains more than 5 pps of ARP request for a 15 second period is automatically shutdown for 30 seconds. After the 30-second blacklist period the port is automatically re-enabled and the counters reset.
- An end subscriber that sustains more than 30 pps of IGMP traffic on the Broadband Internet service for a 15 second period is automatically shutdown for 30 seconds. After the 30-second blacklist period the port is automatically re-enabled and the counters reset.
- An end subscriber that sustains more than 5 pps of DHCP traffic on the Broadband Internet service for a 15 second period is automatically shutdown for 30 seconds. After the 30-second blacklist period the port is automatically re-enabled and the counters reset.
- DHCP broadcast requests destined to UDP port 67 (attempting to connect to a DHCP server) are not permitted to terminate to a subscriber end point
- In the event of malicious activity, SWAT may implement a temporary block at this network level restricting traffic, which may be harmful to the network as a whole. If such activity is necessary, the affected customer(s) would be contacted and worked with to remove the underlying threat.
- SWAT collects performance characteristics in the aggregate at this level (link level utilization), which allows us to proactively plan in advance proper network scaling.
- If needed, when working with a subscriber to troubleshoot a problem, properly trained staff within SWAT may perform real time traffic analysis of subscriber traffic.

Distribution Network

- In the event of malicious activity, SWAT may implement a temporary block at this network level restricting traffic, which may be harmful to the network as a whole. If such activity is necessary, the affected customer(s) would be contacted and worked with to remove the underlying threat.
- SWAT collects performance characteristics in the aggregate at this level (link level utilization), which allows us to proactively plan in advance proper network scaling.
- If needed, when working with a subscriber to troubleshoot a problem, properly trained staff within SWAT may perform real time traffic analysis of subscriber traffic.

Core Network

- In the event of malicious activity, SWAT may implement a temporary block at this network level restricting traffic, which may be harmful to the network as a whole. If such activity is necessary, the affected

customer(s) would be contacted and worked with to remove the underlying threat.
- SWAT collects performance characteristics in the aggregate at this level (link level utilization), which allows us to proactively plan in advance proper network scaling.
- If needed, when working with a subscriber to troubleshoot a problem, properly trained staff within SWAT may perform real time traffic analysis of subscriber traffic.

Network Edge

- In the event of malicious activity, SWAT may implement a temporary block at this network level restricting traffic, which may be harmful to the network as a whole. If such activity is necessary, the affected customer(s) would be contacted and worked with to remove the underlying threat.
- SWAT collects performance characteristics in the aggregate at this level (link level utilization), which allows us to proactively plan in advance proper network scaling.
- SWAT collects netflow data on all external traffic flows to better understand network attacks.
- If needed, when working with a subscriber to troubleshoot a problem, properly trained staff within SWAT may perform real time traffic analysis of subscriber traffic.
- Traffic entering our network edge from the external side, sourced from an IP address within one of our network ranges is denied.
- Traffic traversing our network edge sourced from RFC1918 address space is denied.
- Traffic traversing our network edge sourced from loopback, link local or 'this' address (as defined in RFC 3330) is denied.

Service Controls

In an effort to maintain the security of the SWAT network and our subscribers as well as to abide by good Internet Citizenship, SWAT utilizes the following listed security practices, which affect Broadband Internet subscribers' use of SWAT provided Internet Services. In addition to this list, SWAT utilizes multiple other mechanisms to sustain the Confidentiality, Integrity and Availability of the SWAT network, however only those having a direct bearing on customer services are listed here.

- Recursive DNS queries are limited to those sourced from valid SWAT IP address ranges. Authoritative DNS queries are answered regardless of source.

- Email relaying is only permitted if sourced from a valid SWAT IP address range or from external source IPs that successfully authenticate.
- Authentication requests for email relaying are denied from some remote locations based on IP address reputation and previous malicious behavior.
- Email messages may not exceed 35 MB in size.
- Our edge spam filtering processes all emails passing through our servers, both inbound and outbound.
- All email accounts have a quota of 1GB of mail storage.

Performance Characteristics

System Performance

SWAT has an ongoing performance-monitoring program, which tracks very closely link utilization, errors, and latency between key nodes on our system. Customers are encouraged to utilize external speed test sites and to report any inconstancies they notice.

At this point, we do not have a speed test program in place that would allow us to track end user performance, however we have done extensive internal testing. Following are our average test results to public speed test servers on the public internet:

DSL

Package	Advertised Download	Advertised Upload	Average Download Test Results	Average Upload Test Results	Latency to test server
1.5Mb	1.5Mb	768kb	1.54Mb	720kb	32.77
4.0Mb	4.0Mb	768kb	4.3Mb	720kb	32.6
6.0Mb	6.0Mb	768kb	6.1Mb	720kb	33.6
10.0Mb	10.0Mb	768kb	10.23Mb	720kb	33.4
20.0Mb	20.0Mb	768kb	20.14Mb	720kb	32.6

FTTH

Package	Advertised Download	Advertised Upload	Average Download Test Results	Average Upload Test Results	Latency to test server
1.5Mb	1.5Mb	1.5Mb	1.83Mb	1.78Mb	8
4.0Mb	4.0Mb	4.0Mb	4.11Mb	4.4Mb	8
6.0Mb	6.0Mb	6.0Mb	6.35Mb	6.57Mb	8
10.0Mb	10.0Mb	10.0Mb	11.55Mb	12.20Mb	8
20.0Mb	20.0Mb	20.0Mb	22.10Mb	23.06Mb	8
50.0Mb	50.0Mb	50.0Mb	51.53Mb	53.3Mb	8

Our service is based on a “best effort” technology, which means that all advertised speeds are an “up to” rating and not a committed information rate. The actual speed a customer will experience while using the Internet depends upon a variety of conditions, many of which are beyond the control of an ISP such as SWAT.

Performance Data collected

SWAT collects and analysis the following performance data:

- Netflow data for all external traffic.
- Per Interface counters for all Core links, Distribution links and Access uplink ports which include:
    - Bits Per Second / Transmit
    - Bits Per Second / Receive
    - Packets Per Second / Transmit
    - Packets Per Second / Receive
    - Errors Per Second / Transmit
    - Discards Per Second / Transmit
    - Errors Per Second / Receive
    - Discards Per Second / Receive
- Per node counters for all Core and Distribution nodes which include:
    - CPU utilization
    - Memory utilization
    - Buffer misses
- Latency statistics between the core network and all distribution and edge nodes.

Terms and Conditions of Service

Pricing

Pricing is available on our website at http://www.swat.coop

Terms and Conditions

All subscribers are required to abide by our AUP, which is available at http://www.swat.coop/files/SWAT%20Allowable%20Use%20Policy-AUP.pdf

To qualify for discounted rates, new customers are required to sign a contract for services which is available for review from our business office, at 870.653.8222

Privacy Policies

- SWAT reserves the right to inspect and analyze network traffic to assist in troubleshooting or service recovery as needed.
- SWAT agrees to treat broadband customer's confidential data with the same level of protection as required under CPNI.

Redress Options

End User:

All service concerns should initially be addressed to the business office at 870.653.8222. Our customer support staff will take ownership of the issue and work with internal resources to resolve any problems.

Edge Provider:

All complaints should be addressed to abuse@swat.coop. Customers found to be acting in violation of the AUP will receive two warnings and service may be disrupted upon the third complaint. Customer information will only be released upon receipt of a bona fide subpoena.