Magazine Telephone Company (MAGTEL)

Network Management Practices

[INTRODUCTION 3](#_TOC_250023)

[CORE NETWORK OVERVIEW 3](#_TOC_250022)

[DISTRIBUTION NETWORK OVERVIEW 3](#_TOC_250021)

[ACCESS NETWORK OVERVIEW 3](#_TOC_250020)

[NETWORK EDGE OVERVIEW 4](#_TOC_250019)

[GENERAL NETWORK PRINCIPALS 4](#_TOC_250018)

[NETWORK PRACTICES 5](#_TOC_250017)

[NON-DISCRIMINATION PRACTICES 5](#_TOC_250016)

[DEVICE ATTACHMENT RULES 5](#_TOC_250015)

[SECURITY PRACTICES 5](#_TOC_250014)

[Access Network 5](#_TOC_250013)

[Distribution Network 6](#_TOC_250012)

[Core Network 6](#_TOC_250011)

[Network Edge 6](#_TOC_250010)

[Service Controls 7](#_TOC_250009)

[PERFORMANCE CHARACTERISTICS 8](#_TOC_250008)

[SYSTEM PERFORMANCE 8](#_TOC_250007)

[PERFORMANCE DATA COLLECTED 9](#_TOC_250006)

TERMS AND CONDITIONS OF SERVICE 10

[PRICING 10](#_TOC_250005)

[TERMS AND CONDITIONS 10](#_TOC_250004)

[PRIVACY POLICIES 10](#_TOC_250003)

[REDRESS OPTIONS 10](#_TOC_250002)

[End User 10](#_TOC_250001)

[Edge Provider 10](#_TOC_250000)

# Introduction

This disclosure applies solely to the broadband services offered by Magazine Telephone Company. MAGTEL may revise this disclosure from time to time without notice by posting a new version to the MAGTEL website at <http://www.magtel.com.> 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.

Magazine Telephone Company (MAGTEL) operates a robust and modern IP network, which serves 2exchanges in Arkansas. Over this IP network we provide a variety of services including Voice and Broadband Internet. MAGTEL operates 1 network edge locations forming our connection to the outside world for Internet access. MAGTEL 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

MAGTEL 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, data, etc.) however no prioritization or discrimination of forwarding traffic is performed, either within a service type or between service categories.

## Distribution Network Overview

MAGTEL 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, data, etc) however no prioritization or discrimination of forwarding traffic is performed, either within a service type or between service categories.

## Access Network Overview

MAGTEL operates 2 access network:

* A 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 3Mbit to 16Mbit.
* A fixed wireless access network supporting Broadband Internet.
	+ This access network supports fixed wireless connections
	+ Bandwidth packages available range from 13Mbit to 40Mbit

## Network Edge Overview

Currently MAGTEL operates2 network edge locations (Internet drains), these locations are:

* (1) to Danville, Arkansas

MAGTEL 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.

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

## General Network Principals

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

* 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 reference segmenting management traffic, ILEC voice 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.
* 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

MAGTEL does not apply any prioritization, rate limiting or blocking based on source, destination, protocol or port. MAGTEL 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

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

### Access Network

* Subscriber MAC addresses are tied to a 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.
* 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, MAGTEL 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.
* MAGTEL 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 MAGTEL may perform real time traffic analysis of subscriber traffic.

### Distribution Network

* In the event of malicious activity, MAGTEL 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.
* MAGTEL 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 MAGTEL may perform real time traffic analysis of subscriber traffic.

### Core Network

* In the event of malicious activity, MAGTEL 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.
* MAGTEL 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 MAGTEL may perform real time traffic analysis of subscriber traffic.

### Network Edge

* In the event of malicious activity, MAGTEL 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.

* MAGTEL collects performance characteristics in the aggregate at this level (link level utilization), which allows us to proactively plan in advance proper network scaling.
* MAGTEL 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 MAGTEL 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 MAGTEL network and our subscribers as well as to abide by good Internet Citizenship, MAGTEL utilizes the following listed security practices, which affect Broadband Internet subscribers’ use of MAGTEL provided Internet Services. In addition to this list, MAGTEL utilizes multiple other mechanisms to sustain the Confidentiality, Integrity and Availability of the MAGTEL network, however only those having a direct bearing on customer services are listed here.

* Recursive DNS queries are limited to those sourced from valid MAGTEL IP address ranges. Authoritative DNS queries are answered regardless of source.
* Email relaying is only permitted if sourced from a valid MAGTEL 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 25 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

MAGTEL 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.

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 MAGTEL.

## Performance Data collected

MAGTEL 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 http://www.magtel.com

## Terms and Conditions

A one-time nonrecurring charge applies for the installation of ADSL Access Service. When the customer commits to retain the ADSL-Voice Data service option for a minimum 6-month period, MAGTEL will waive the nonrecurring installation charge. A $35.00 fee will be charged if the ADSL Access Service is permanently disconnected for any reason before the end of the 6-month commitment period other than for an ADSL service conversion, a discontinuance of service within the first 30 days of service, or a discontinuance of service due to a fire, flood, or other occurrence described as an act of God.

## Privacy Policies

* MAGTEL reserves the right to inspect and analyze network traffic to assist in troubleshooting or service recovery as needed.
* MAGTEL 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. 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 magtel@magtel.com. Customers found to be acting in violation of the AUP will receive two warnings and service may be disrupted upon the third complaint.