Module 8.0

EdgeMarc & EdgeView Advanced Functions



edgewater NETWORKS

Module 8.0: Performance Objectives

1. In this module, attendees follow pre-defined scripts to complete advanced EdgeMarc configuration. The emphasis is on completing pre-defined settings tasks and demos of functionality.

Module 8.0: Hands On Labs

- Lab 1: Demo & Settings for Advanced Topuics
- Traffic Shaping – config settings
- Firewall setup with Proxy Arp Demo
- WAN Failover config & Demo
- High Availability – Demo
- VoIP Survivability – Config and Demo

Module 8.0 Lessons

- Lesson 1.0: Traffic Shaping
- Lesson 2.0: Firewall Deployment
- Lesson 3.0: WAN Failover
- Lesson 4.0: High Availability
- Lesson 5.0: VoIP Survivability

Lesson 8.1: Traffic Shaping

- Understanding QoS options
- EdgeMarc LAN/WAN VoIP prioritization options

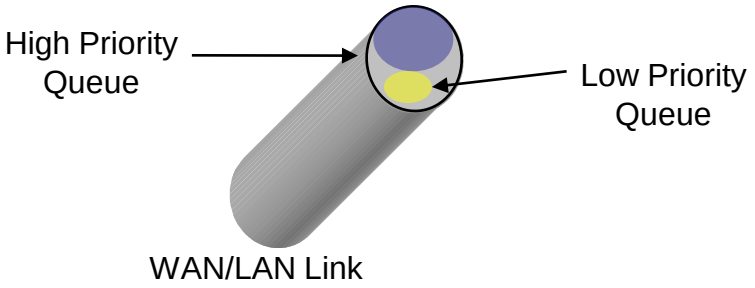
Lesson 8.1: Traffic Shaping

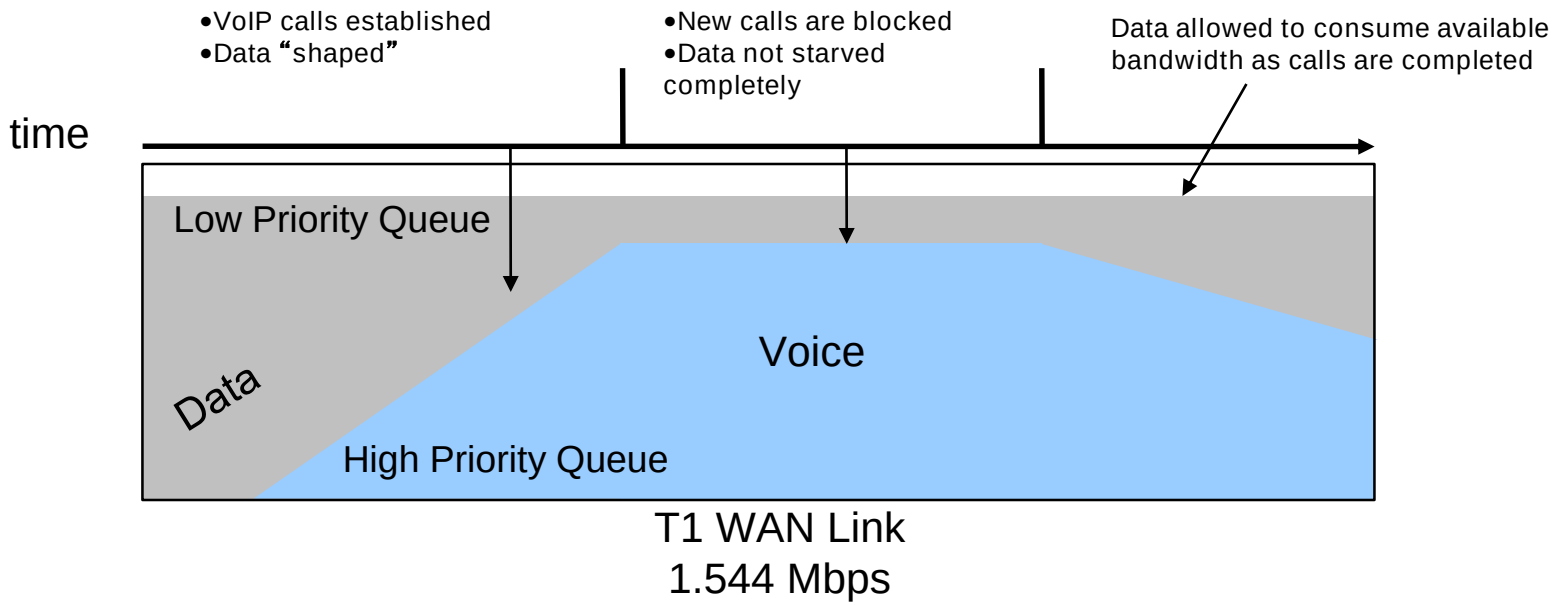
- Class based queues
  - Voice & Signaling are high priority. Everything else is low priority.
  - Traffic Scheduler to service the queues
  - Traffic Shaper to rate limit low priority traffic
- TOS / Diffserv packet marking on LAN and WAN.
  - High-priority TOS value is re-written to 0xb8 (Diffserv AF46)
  - Low-priority TOS value is re-written to 0x00
- TCP congestion management
  - TCP acknowledgements to WAN are delayed to push back on inbound data traffic
  - Proved effective in field. Allows inbound voice to avoid high jitter

Lesson 8.1: Traffic Shaping - Access Link

Single Device to Manage Bandwidth and Improve Quality

- Traffic shaping—dynamic voice prioritization
- Call Admission Control—no oversubscription
- Diffserv marking and policing
- Up to 8 class of service queues

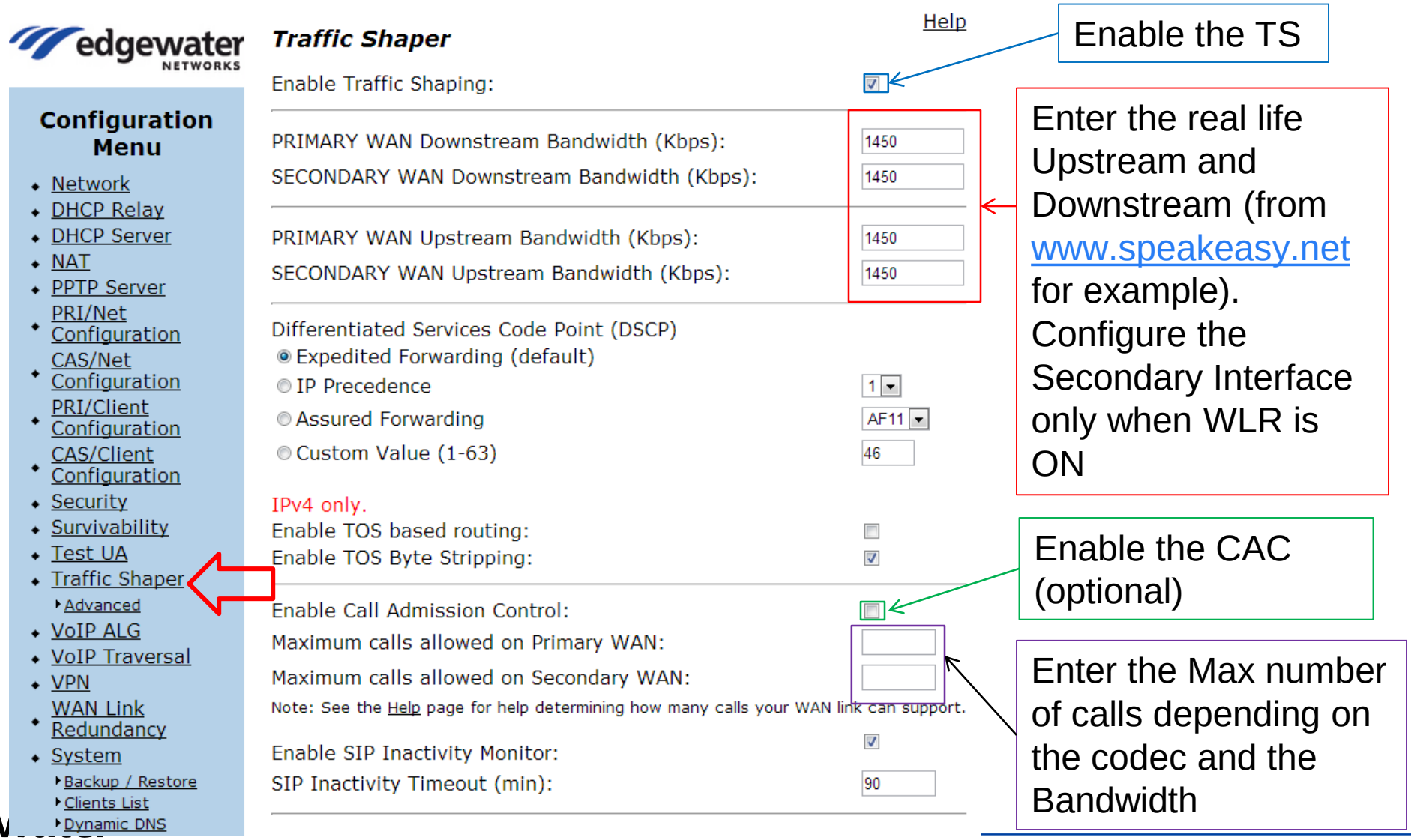




Lesson 8.1: Traffic Shaping – Bandwidth Management

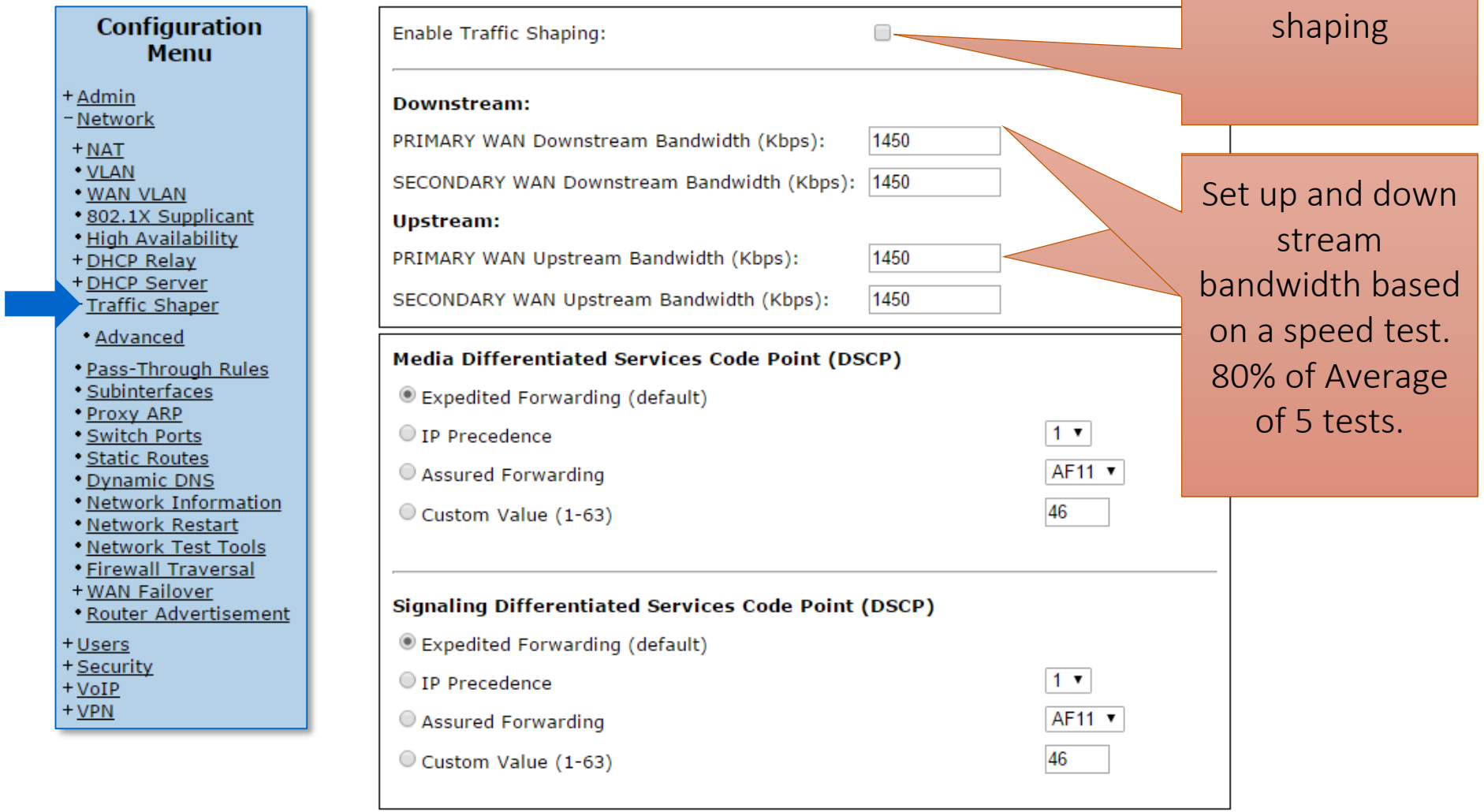
- Call Access Control (CAC)
- Configure maximum allowed calls
- Send “Bandwidth Exceeded” signaling message at call n+1 (inbound or outbound)
- This value is configured in the VoIP ALG page
- Working together with automatic classing, queuing and traffic shaping, CAC ensures the WAN link will not be over subscribed by having too many RTP streams requiring WAN access.

Lesson 8.1: Traffic Shaping - Configuration

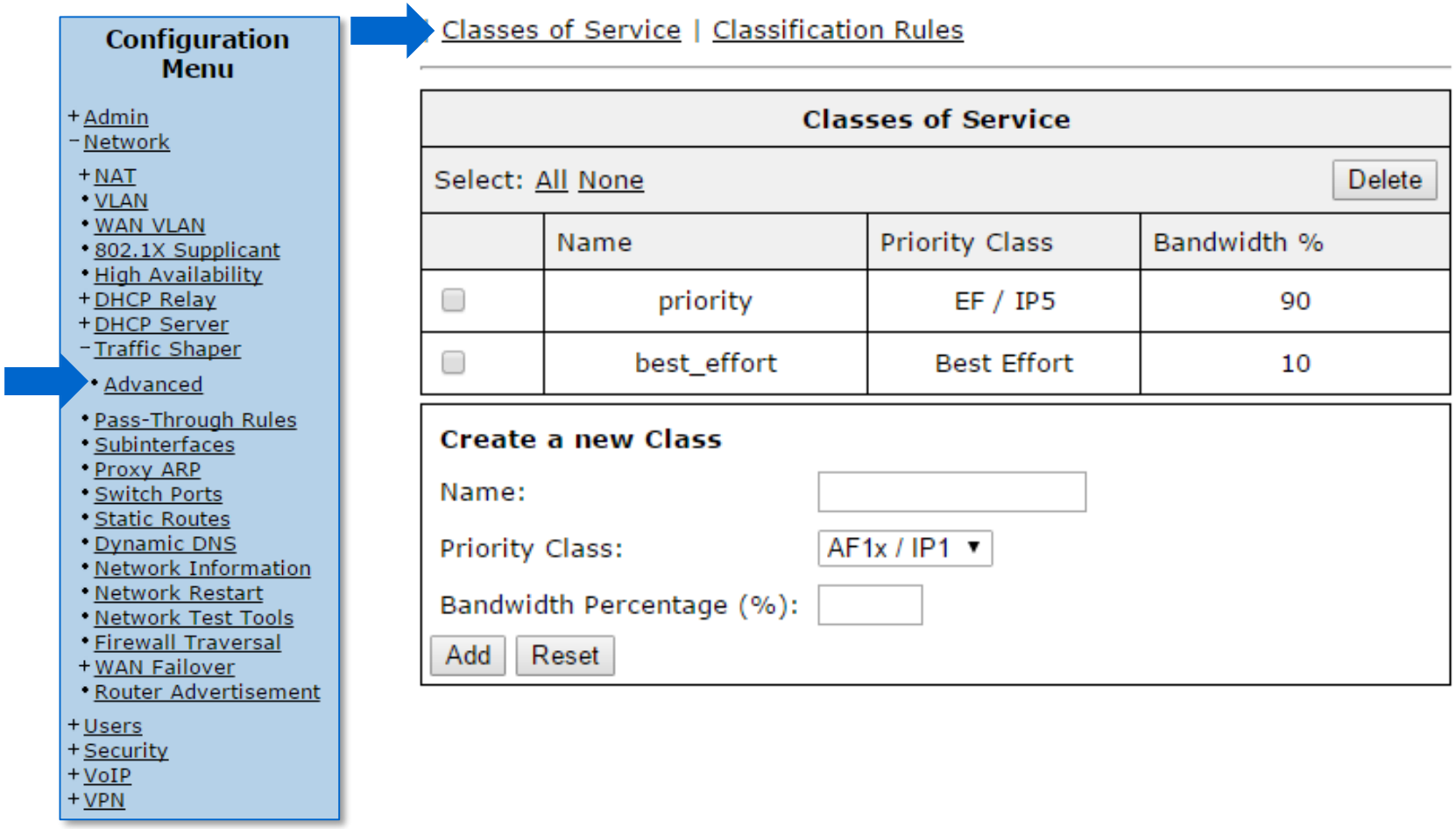


Company Confidential

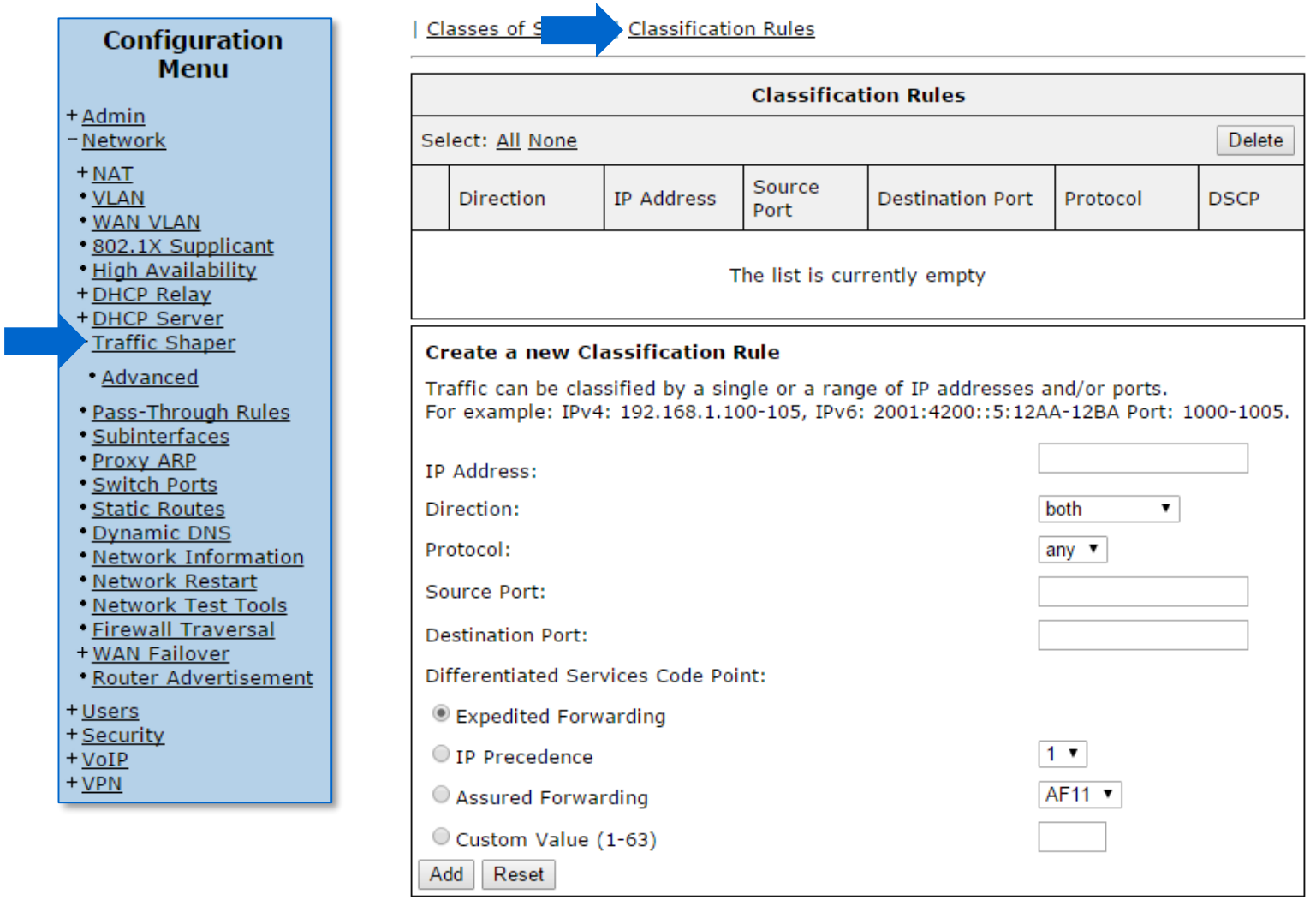
Lesson 8.1: Traffic Shaping - Configuration



Lesson 8.1: Traffic Shaping - Advanced - COS



Lesson 8.1: Traffic Shaping - Advanced - Classification Rules



Lesson 8.2: Firewall Traversal & Proxy ARP

- Deployment models using Proxy ARP
- Firewall Traversal settings

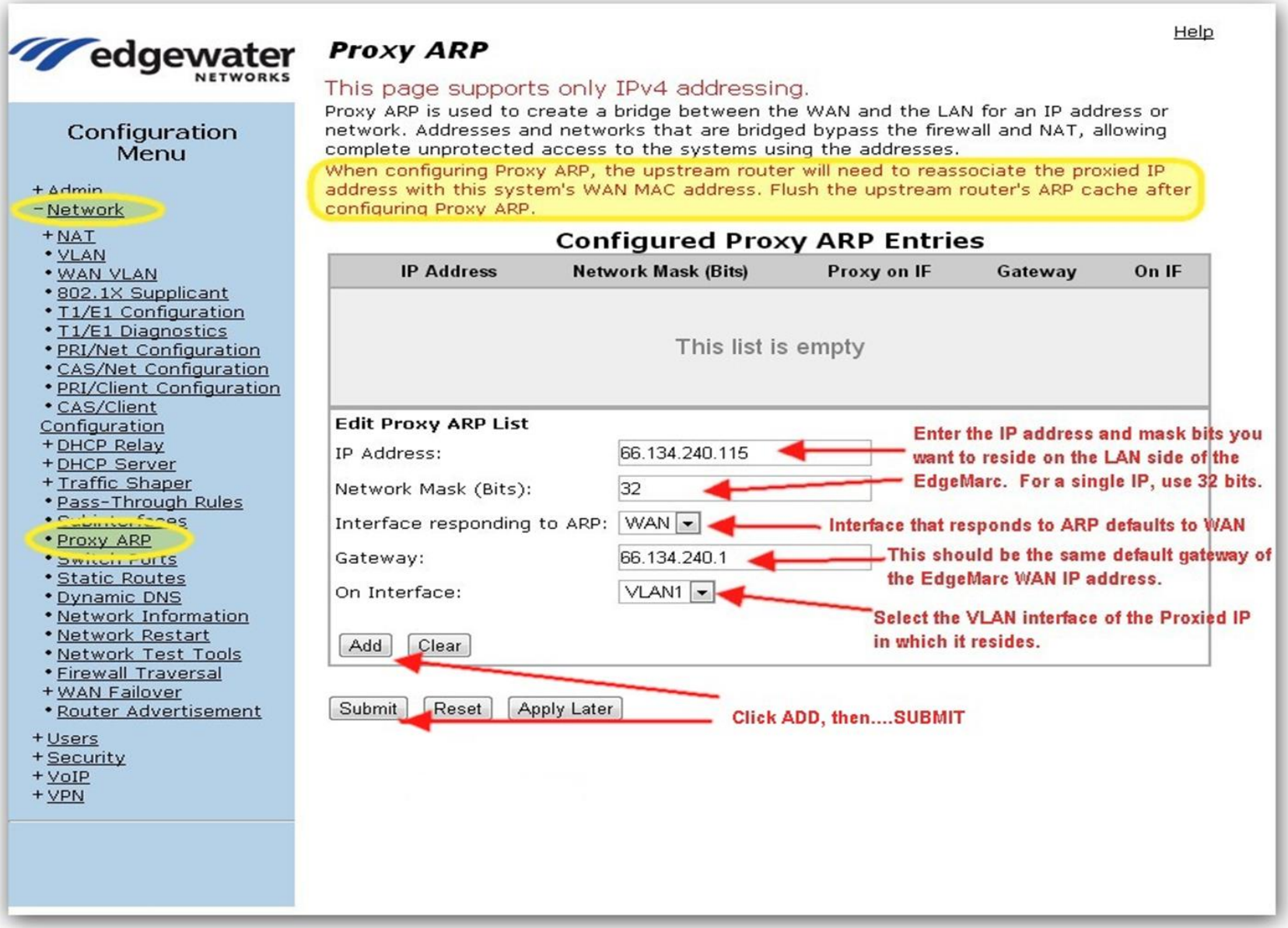
Lesson 8.2: Firewall Traversal

- Using EdgeMarc Firewall Traversal options
- Internal Client, External Server, Remote Client

Lesson 8.2: Firewall Traversal & Proxy ARP

- Proxy Arp is used when you want to assign a LAN side device, a Public IP address, which is on the same subnet as the WAN IP address
- In this example, the EdgeMarc WAN IP address is 66.134.240.114/255.255.255.0 with a default gateway of 66.134.240.1.
- And customer wants 66.134.240.115 on the LAN side server.

Lesson 8.2: Firewall Traversal & Proxy ARP



Lesson 8.2: Firewall Traversal & Proxy ARP

- When you ping the Proxied IP address from a remote computer. The incoming icmp request should contain a destination MAC address of the EdgeMarc eth1 interface. If the destination MAC address does not match eth1 MAC address, the upstream router needs to clear its ARP cache. If customer have cable modem, customer need to power cycle the cable modem.
- Use tcpdump with option “e” to see the destination MAC address.

Lesson 8.2: Firewall Traversal & Proxy ARP

- # tcpdump -nei eth1 -s0 icmp
- tcpdump: listening on eth1
- 01:34:29.937686 0:3:6d:f6:2c:b4 a8:70:a5:0:26:53 0800 75: 24.49.104.166 > 66.134.240.115: icmp: echo request

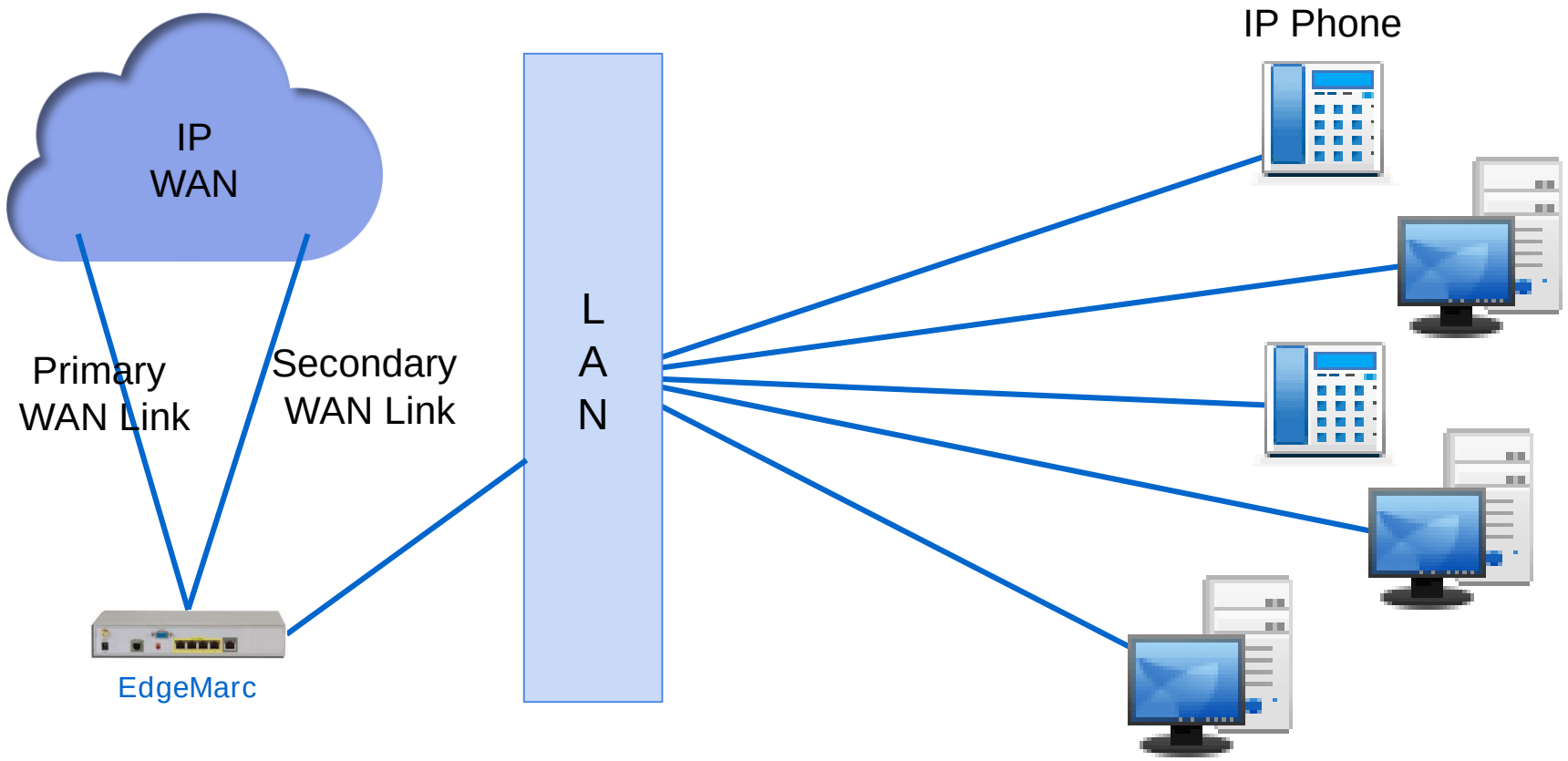
Lesson 8.2: Firewall Traversal & Proxy ARP

- # ifconfig eth1
- eth1 Link encap:Ethernet HWaddr A8:70:A5:00:26:53
- inet addr:66.134.240.114 Bcast:66.134.240.255 Mask:255.255.255.0
- inet6 addr: fe80::aa70:a5ff:fe00:2653/64 Scope:Link
- UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
- RX packets:139235 errors:0 dropped:0 overruns:0 frame:0
- TX packets:799 errors:0 dropped:0 overruns:0 carrier:0
- collisions:0 txqueuelen:1000
- Base address:0x3600

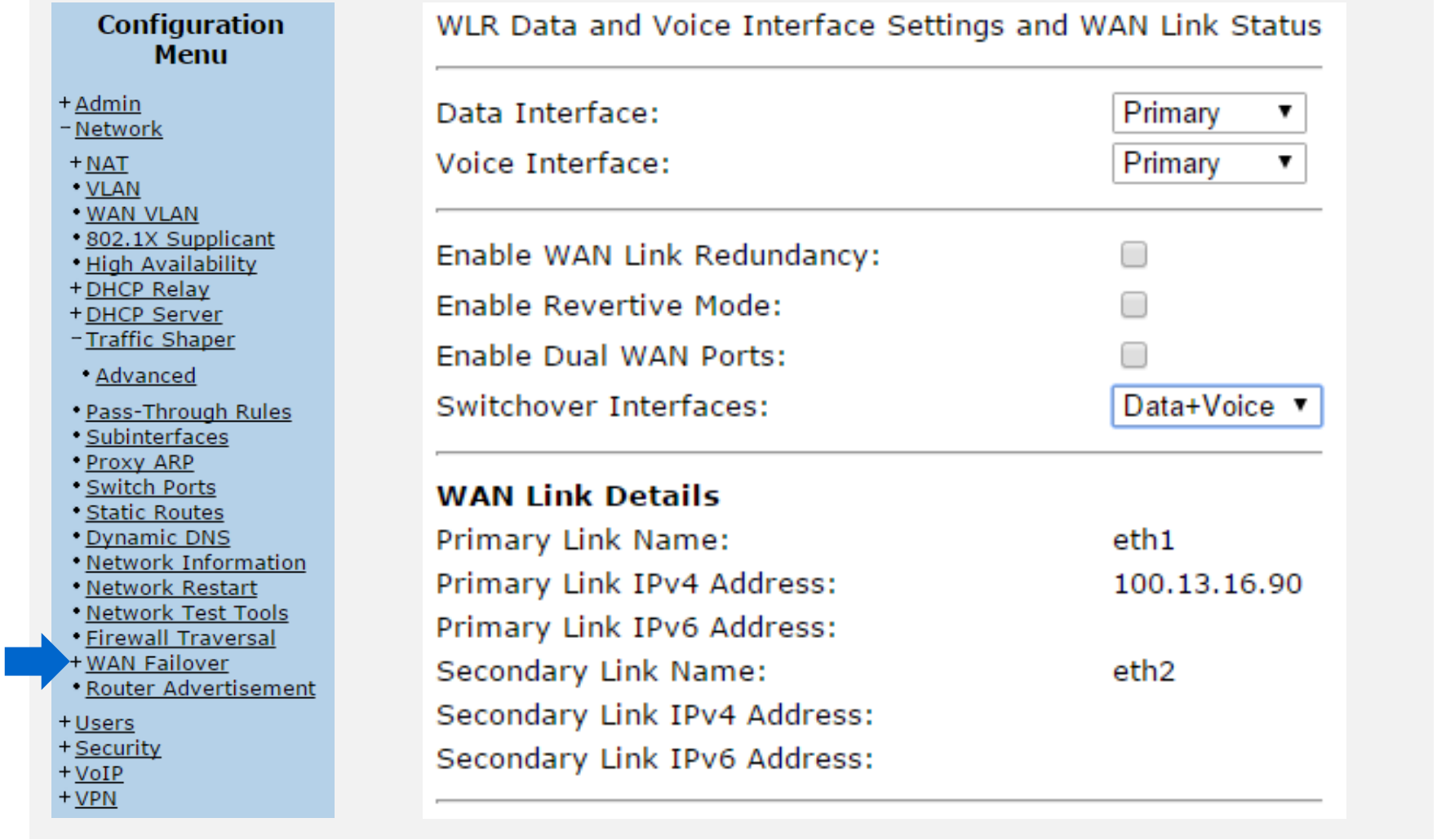
Lesson 8.3: WAN Link Redundancy

- Understanding Voice & Data options for WAN fail over
- Primary vs Secondary WAN links
- Configuring WAN Failover using revertive mode

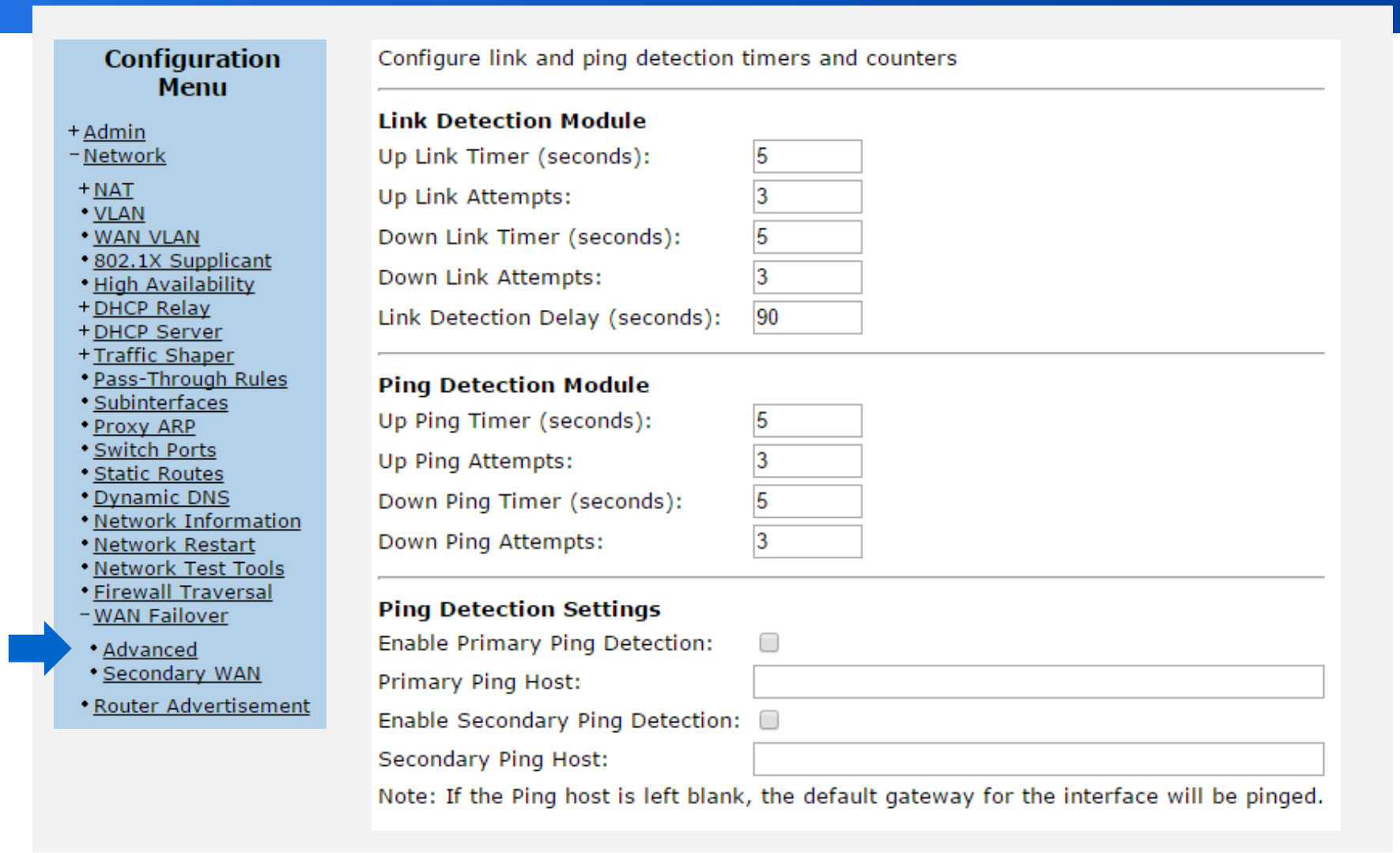
Lesson 8.3: WAN Link Redundancy



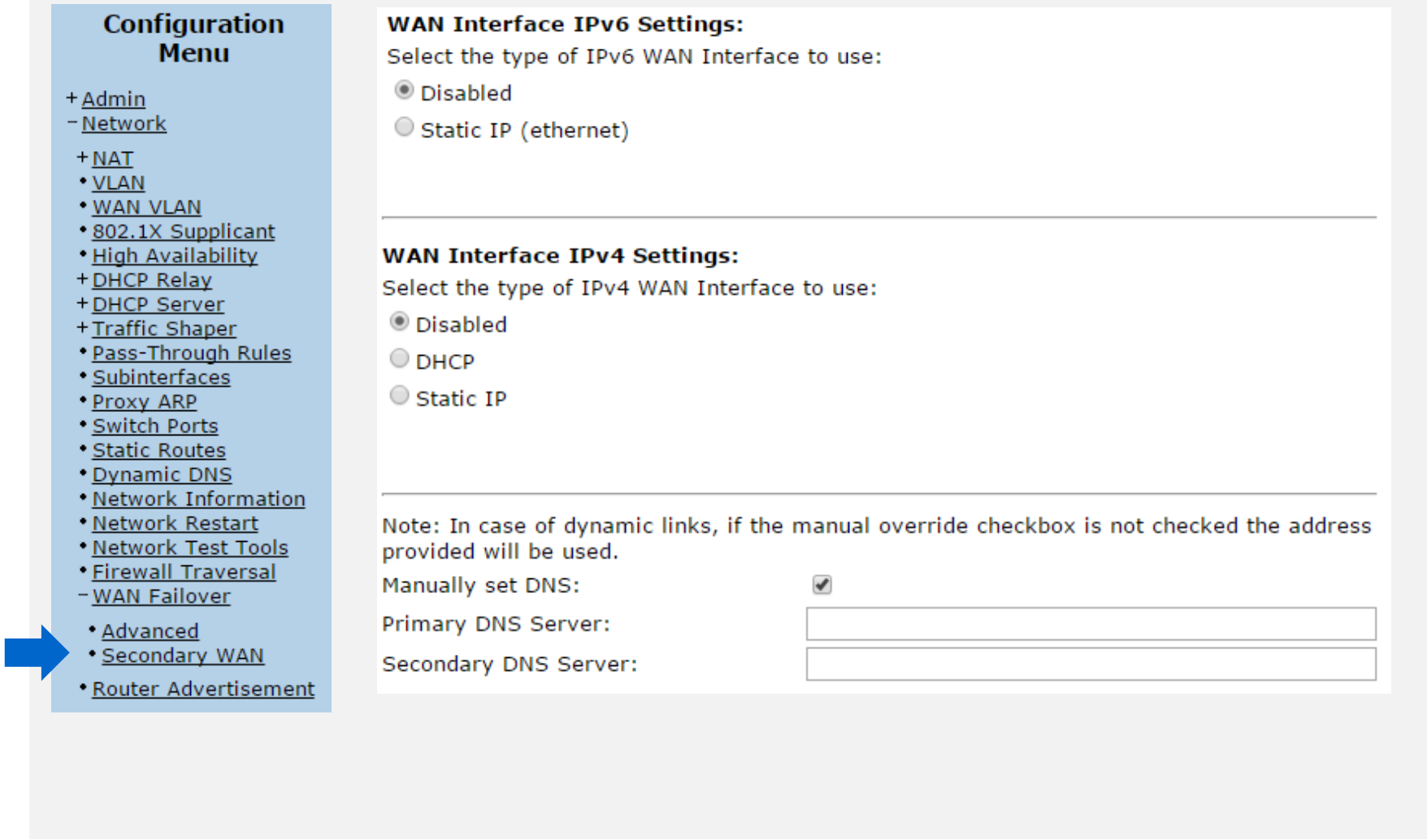
Lesson 8.3: WAN Link Redundancy



Lesson 8.3: WAN Link Redundancy



Lesson 8.3: WAN Link Redundancy



Lesson 8.4: High Availability

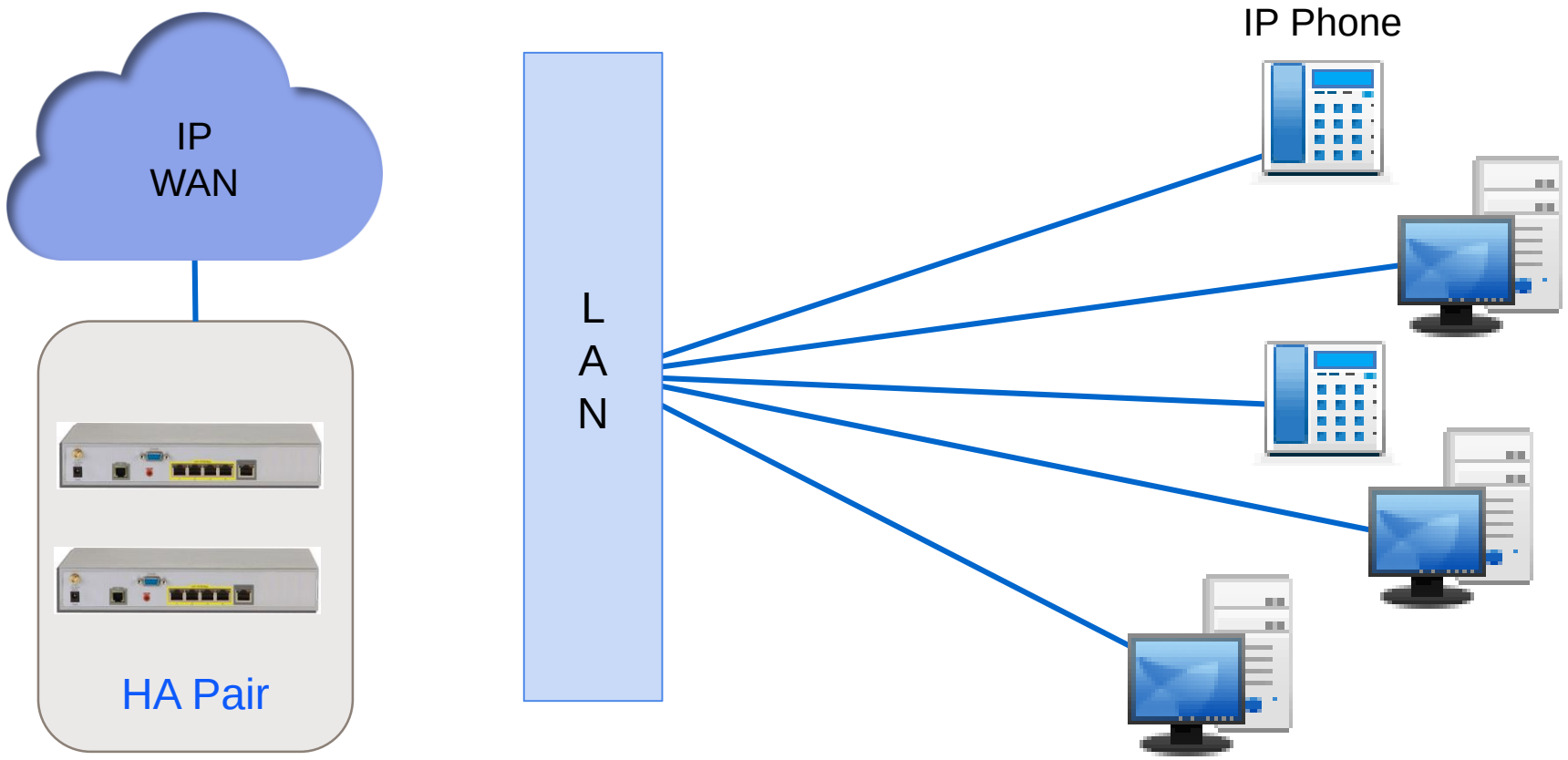
- Configuring HA
- IPv4 vs IPv6 configuration

Lesson 8.4: High Availability

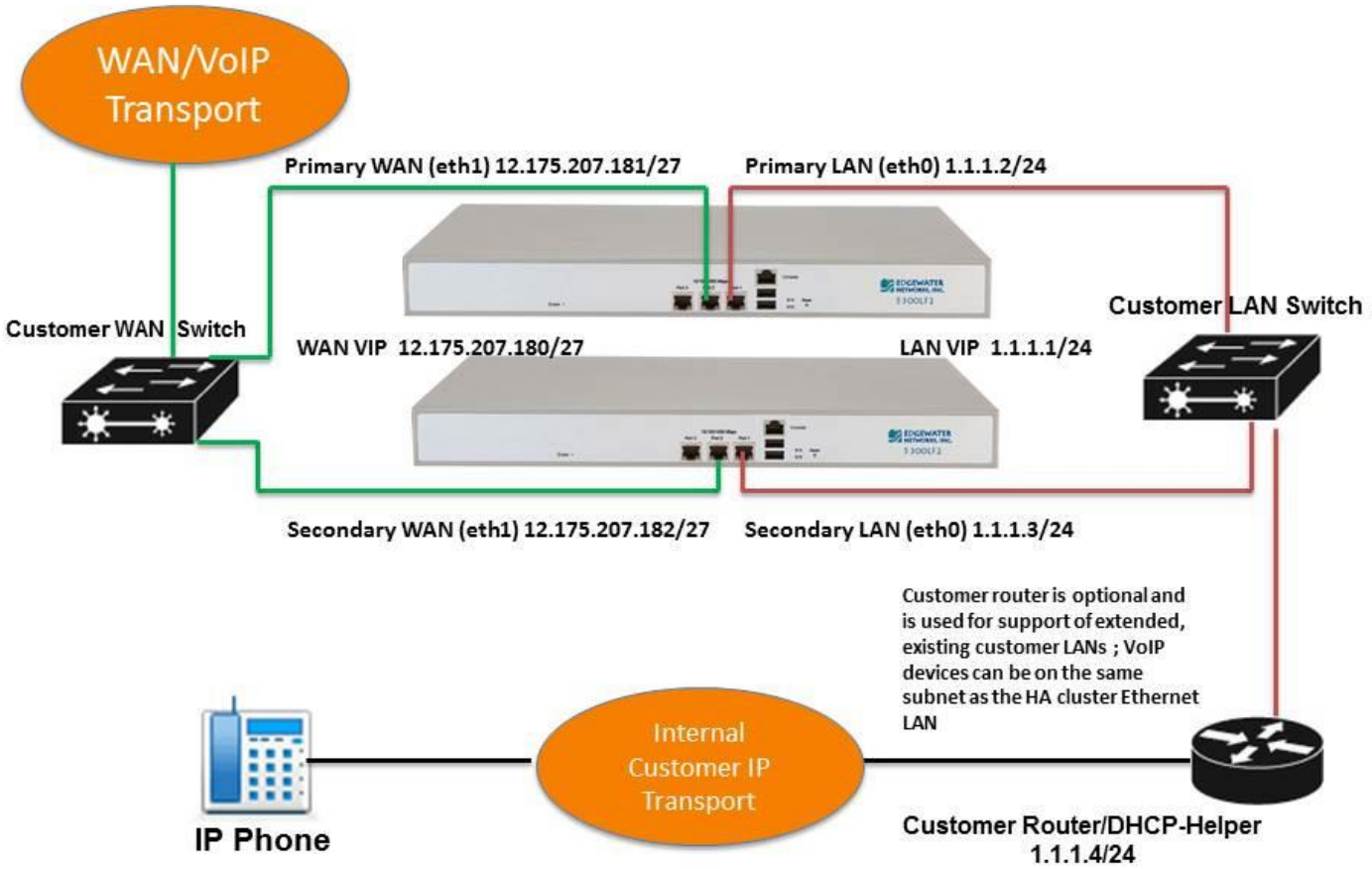
- HA is designed to remove any single point of failure in the network configuration:
  - Physical
  - Data link
  - Network routing
  - ALG
    - B2BUA is not HA compliant
  - Hot failover

Company Confidential

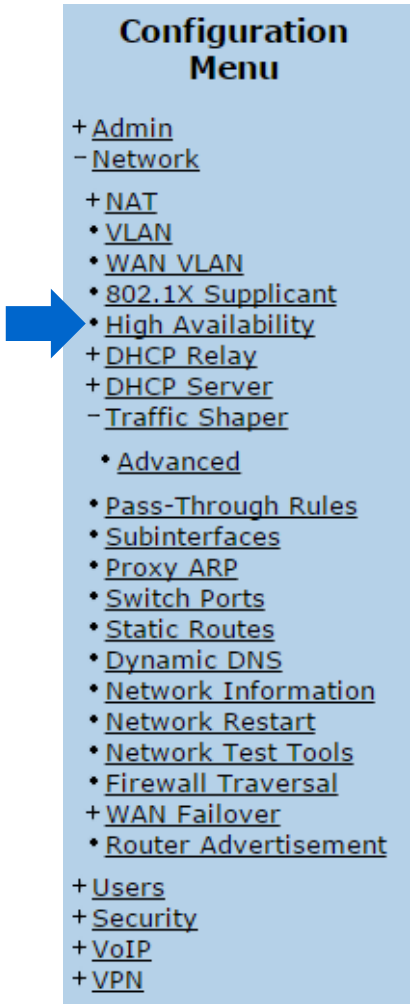
Lesson 4.4: High Availability Architecture

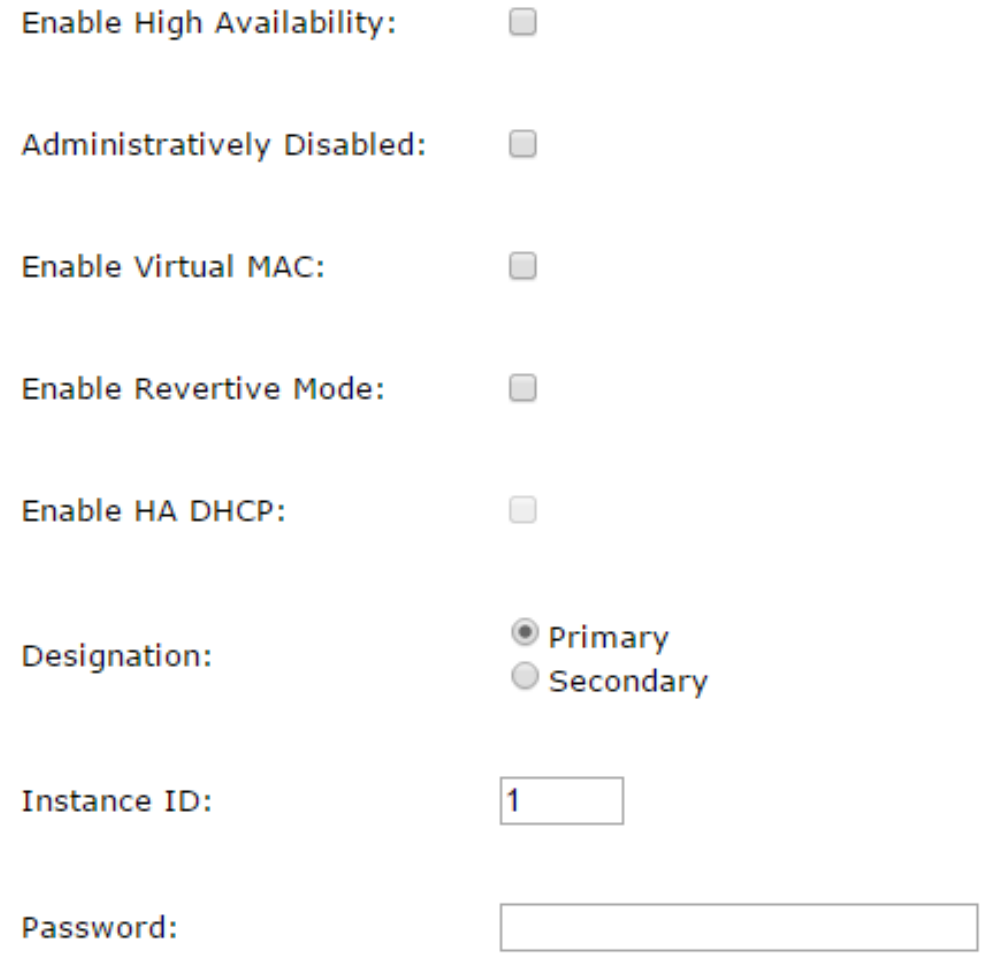


Lesson 8.4: High Availability Architecture

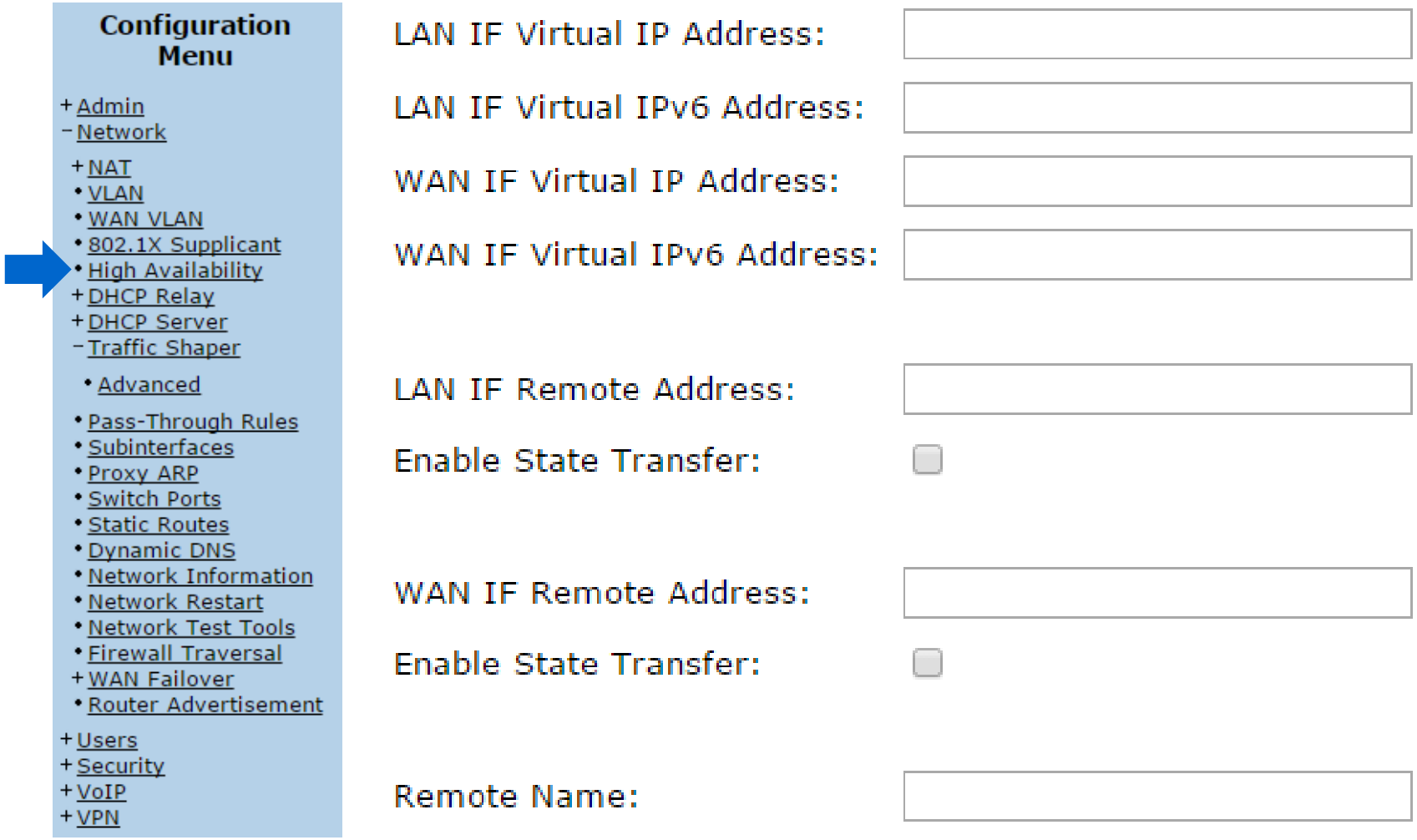


Lesson 8.4: High Availability - Configuration

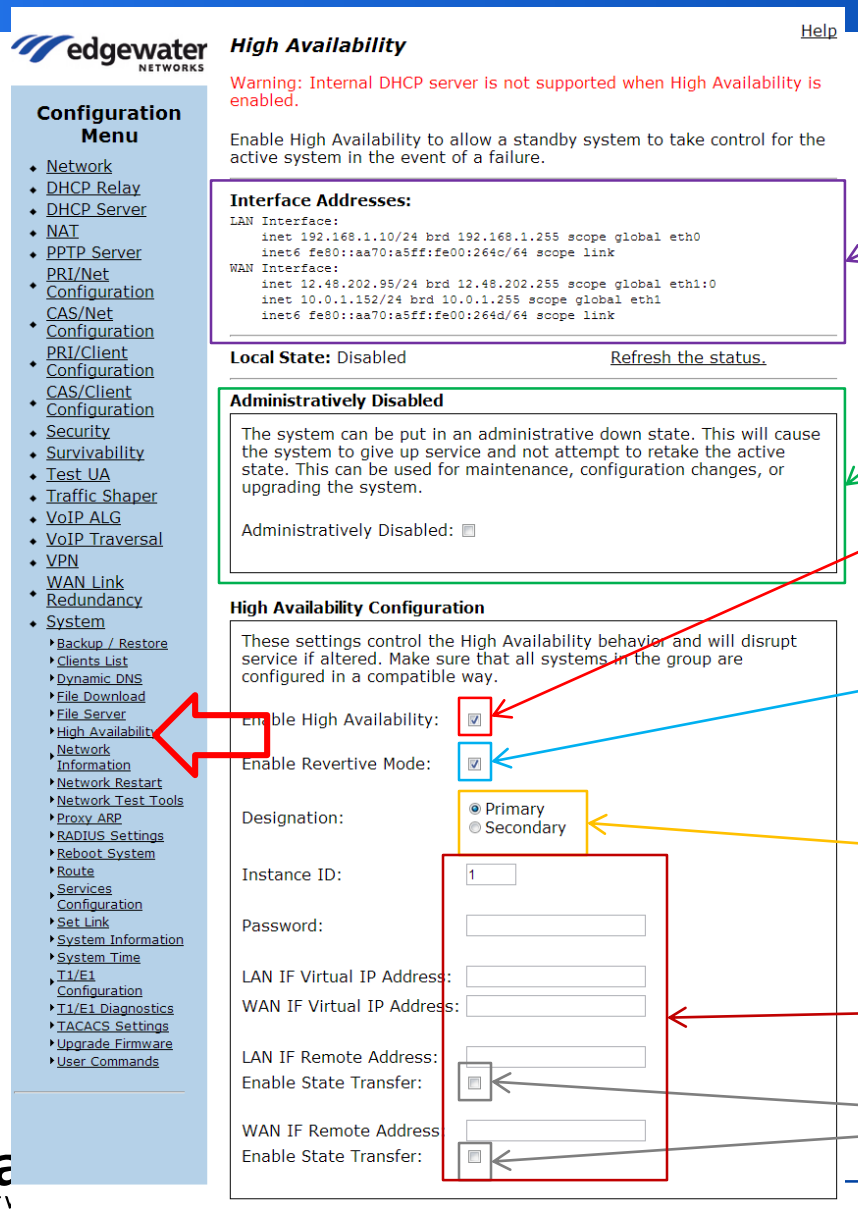




Lesson 8.4: High Availability - Configuration



Lesson 8.4: High Availability – Configuration



List of interfaces

Enabling the maintenance mode

Enabling HA

Enabling a mode where when the primary EM is back up, it is becoming the master of the HA pair again automatically

Configuring the primary versus secondary EM

Configuring the Networking HA

State full configuration

Company Confidential

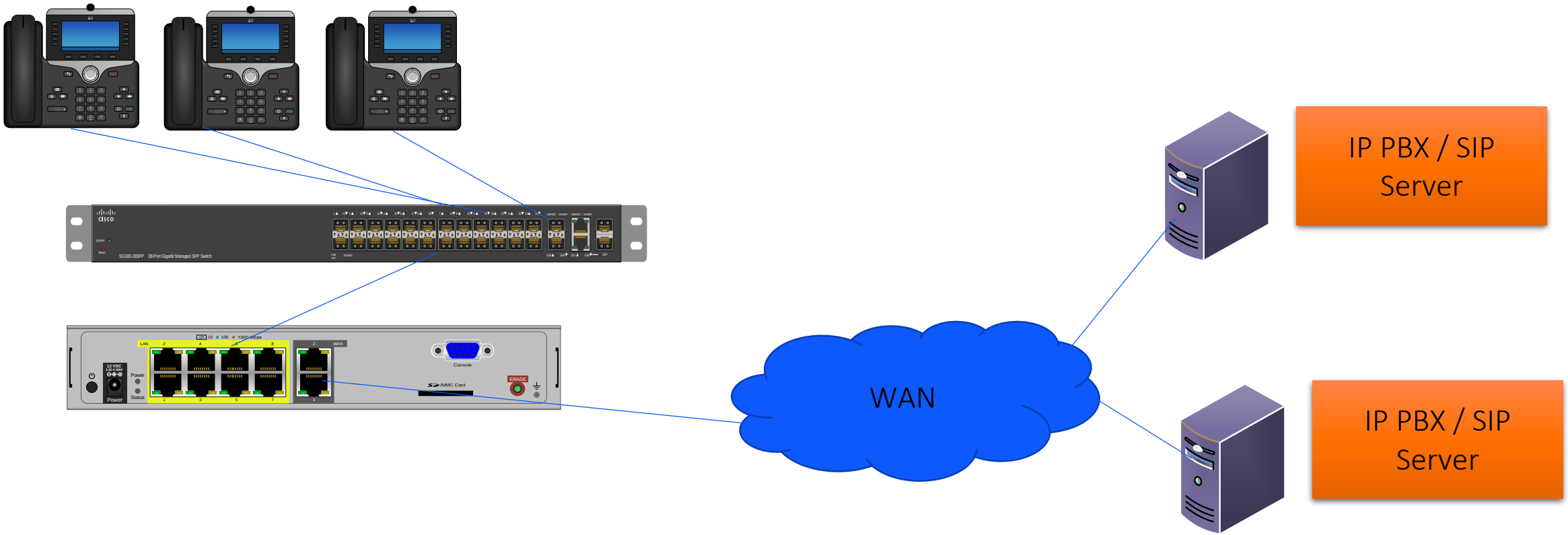
Lesson 8.5: VoIP Survivability

1. Setting up redundant Softswitch / IP PBX configurations
2. WAN Link failure & local call control

Lesson 8.5: VoIP Survivability

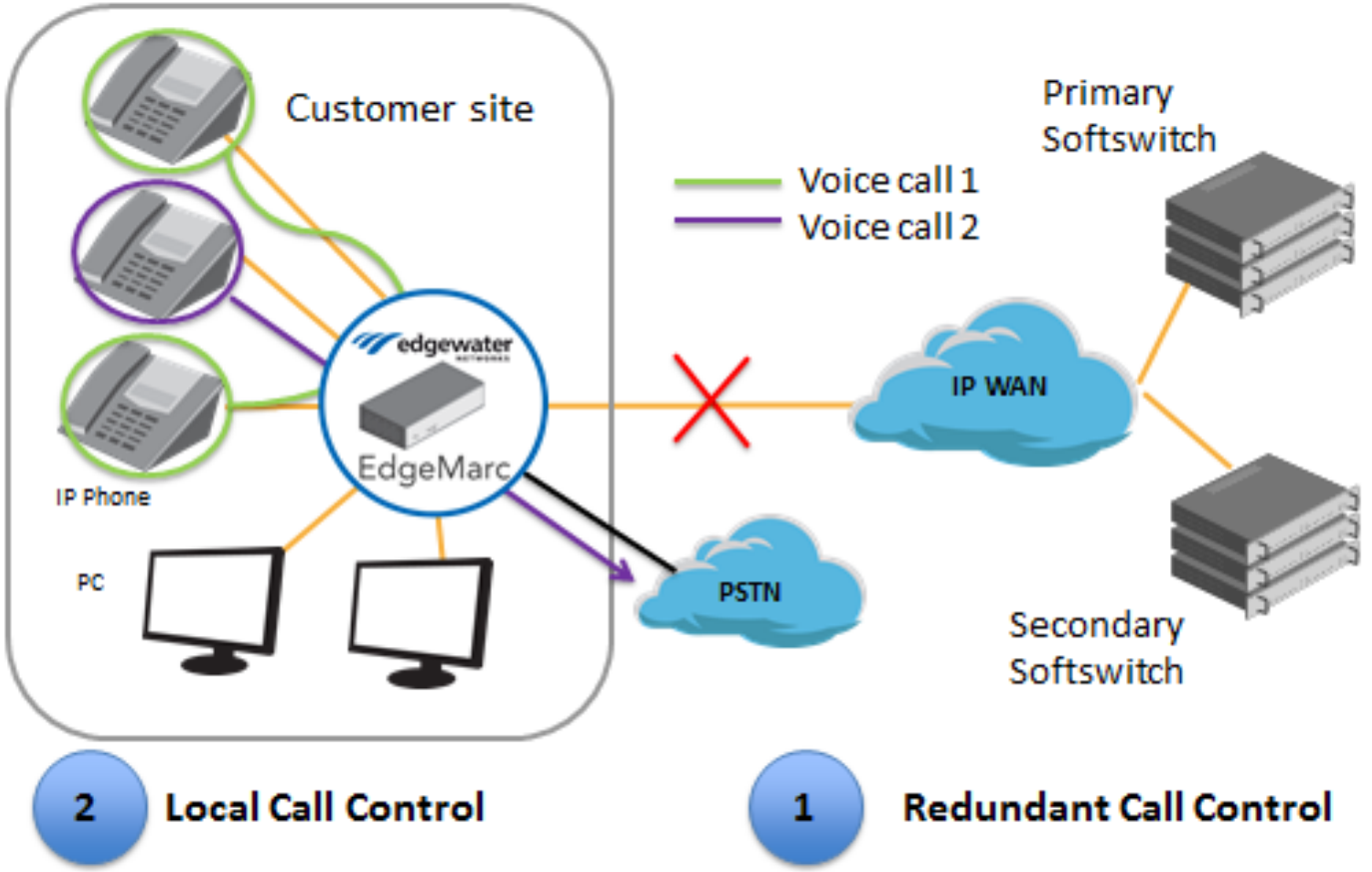
- Survivability is a collection of features that enable the system to extend the availability of VoIP services.
- These features include:
  - Support for redundant Softswitches/IP PBX's
  - Local call control in the event of WAN link failure, softswitch/IP PBX failure, or during periods of network congestion that result in loss of connectivity to a remote Softswitch/IP PBX

Lesson 8.5: VoIP Survivability – Redundant SIP Server / IP PBX



Lesson 8.5: VoIP Survivability

- Local dial tone in case of network disruption:
  - Station-to-station
  - Hold
  - Transfer
- 3-way conference
- Outbound/Emergency calls with integrated gateway



Lesson 8.5: VoIP Survivability - Features

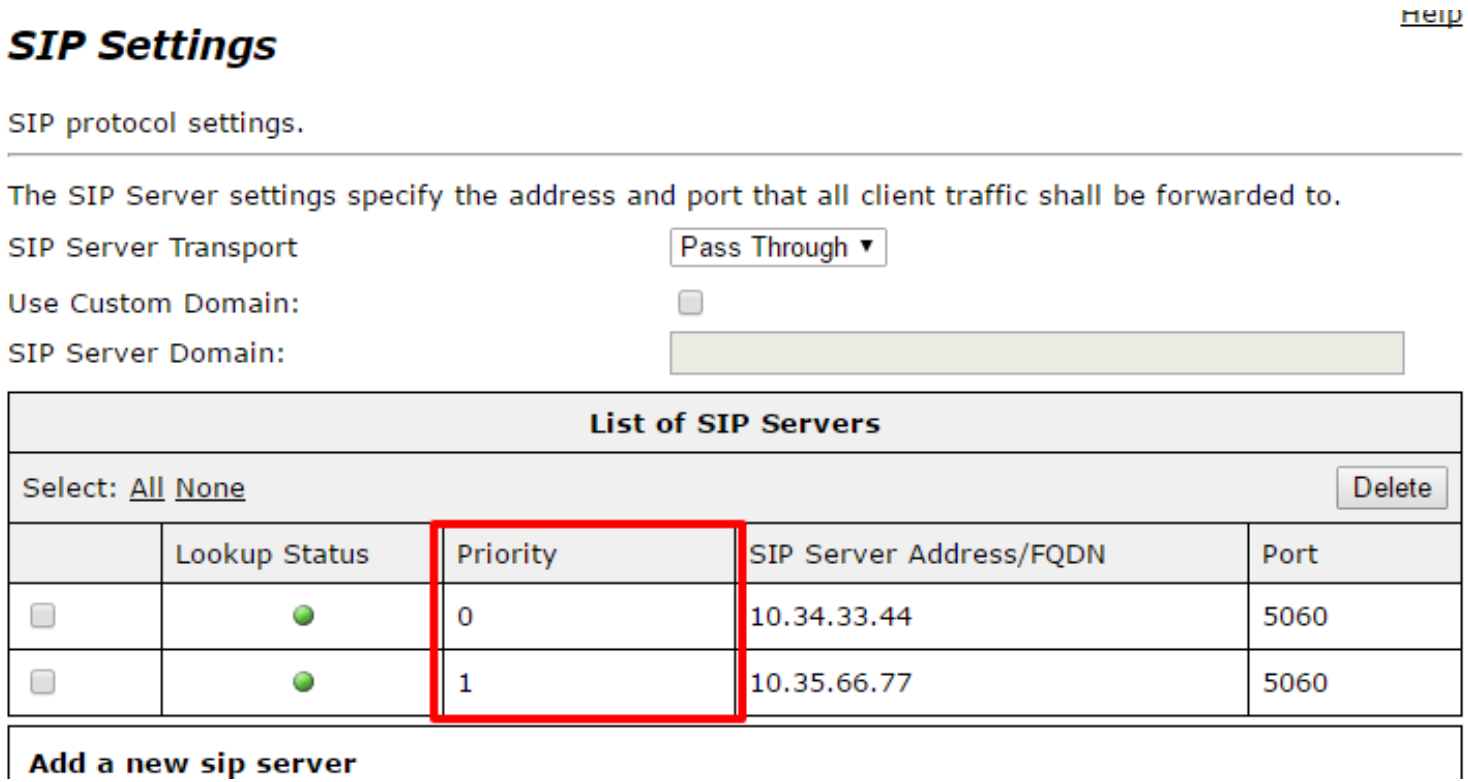
- Available for all EdgeMarc series appliances
- Application layer monitoring of softswitch connectivity
- Automatic failure detection and return of call control
- Support for redundant softswitch servers
- Automatic creation of local dial plan to simplify setup
- Dial plan integration with Softswitch
- Local call switching between SIP user agents and PSTN gateway
- Transfer, hold and conference capability when in local mode (5300 adds voicemail)

Lesson 8.5: VoIP Survivability – Deployment Examples

- EdgeMarc can accommodate very complex survivability implementation architectures.
- See the document in your student materials called “Application_Note-Configuring_Survivability_features”

Lesson 8.5: VoIP Survivability – Basic Configuration

- First step is create a list of SIP Servers that EdgeMarc can prioritize
- Typically two SIP Servers
- Can be manually added to SIP Settings or DNS SRV Record lookup can obtain list of SIP Servers



Help

SIP Settings

SIP protocol settings.

The SIP Server settings specify the address and port that all client traffic shall be forwarded to.

SIP Server Transport: Pass Through

Use Custom Domain:

SIP Server Domain:

List of SIP Servers

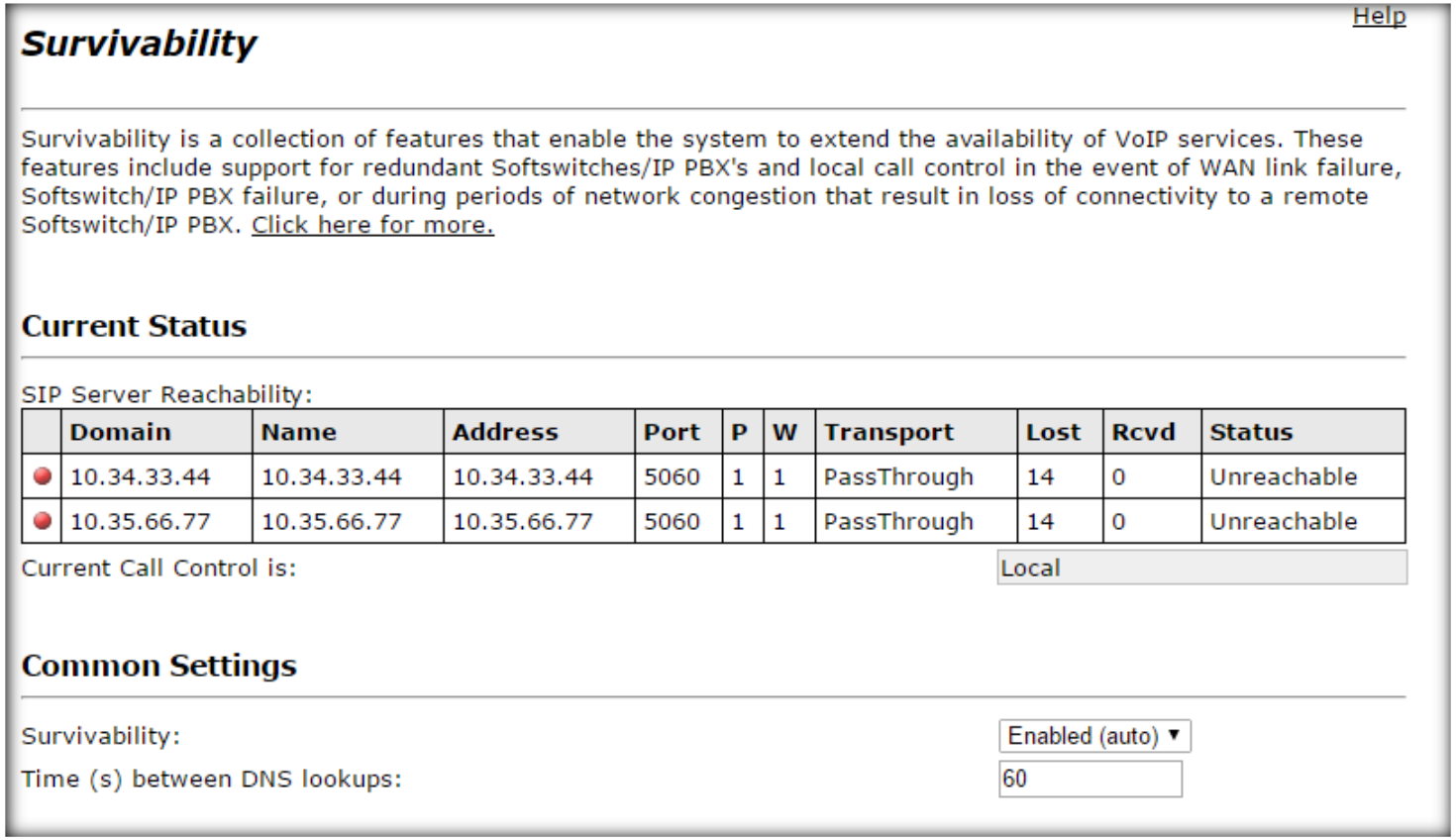
Select: All None — Delete

	Lookup Status	Priority	SIP Server Address/FQDN	Port
☐	●	0	10.34.33.44	5060
☐	●	1	10.35.66.77	5060

Add a new sip server

Lesson 8.5: VoIP Survivability – Advanced Settings

- Walk through the settings on the Survivability Page
- Refer to the Application Note for use case and sample configuration settings



Help

Survivability

Survivability is a collection of features that enable the system to extend the availability of VoIP services. These features include support for redundant Softswitches/IP PBX's and local call control in the event of WAN link failure, Softswitch/IP PBX failure, or during periods of network congestion that result in loss of connectivity to a remote Softswitch/IP PBX. Click here for more.

Current Status

SIP Server Reachability:

	Domain	Name	Address	Port	P	W	Transport	Lost	Rcvd	Status
●	10.34.33.44	10.34.33.44	10.34.33.44	5060	1	1	PassThrough	14	0	Unreachable
●	10.35.66.77	10.35.66.77	10.35.66.77	5060	1	1	PassThrough	14	0	Unreachable

Current Call Control is: Local

Common Settings

Survivability: Enabled (auto)

Time (s) between DNS lookups: 60

Module 8.0: Review

Module 8.0: Quiz