



Packet Manipulation with MikroTik Firewalls

By Rick Frey



About the Presenter

► Rick Frey

- 20+ years in IT & Communication Industries
- Designed and implemented a wide array of networks all of the world
- Introduced to the MikroTik product line in 2008
- Areas of Focus:
 - Wireless services integration
 - ISP Solutions
- Certifications
 - Certified –MTCNA, MTCRE, MTCTCE, MTCWE, MTCT



Upcoming Training Opportunities

- | | | |
|----------------|-------------|----------------|
| ▶ April 27-30 | Dallas, TX | MTCTCE & MTCWE |
| ▶ May 25-29 | Atlanta, GA | MTCNA & MTCRE |
| ▶ Jun 8-12 | Kansas City | MTCNA & MTCRE |
| ▶ Jun 29-Jul 2 | Omaha, NE | MTCWE & MTCTCE |
| ▶ Jul 6-10 | Little Rock | MTCNA & MTCTCE |
| ▶ Jul 20-24 | Phoenix, AZ | MTCNA & MTCRE |
| ▶ Aug 17-21 | Norfolk, VA | MTCNA & MTCRE |
| ▶ Aug 24-28 | D.C. | MTCNA & MTCRE |
| ▶ Sep 7-11 | Dallas, TX | MTCNA & MTCWE |
| ▶ Sep 21-25 | Albuquerque | MTCNA & MTCRE |

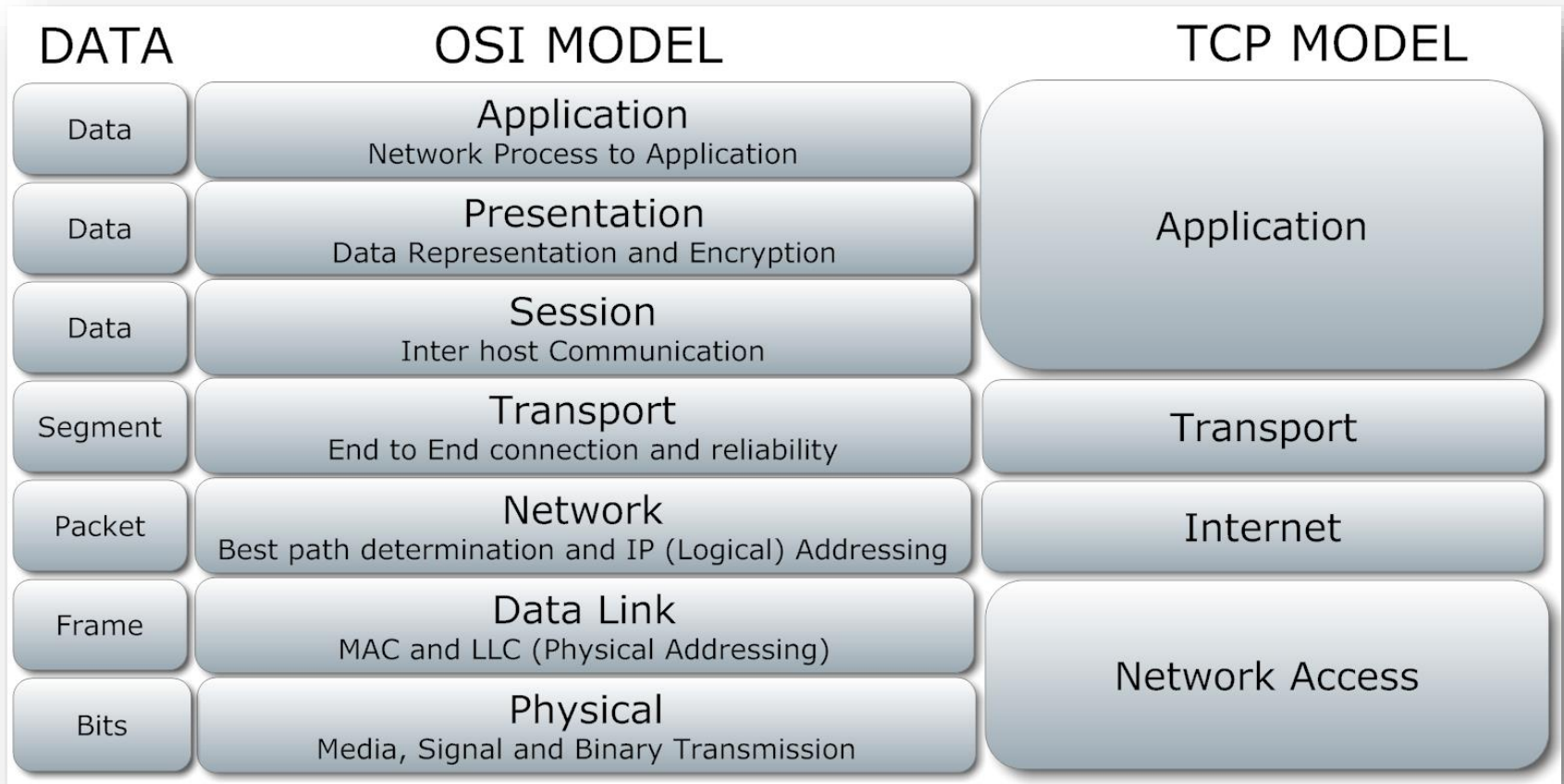


Objectives

- ▶ Explain what/ how much of a Layer 2 Frame can be manipulated
- ▶ Explain what parts of the Layer 2 Frame can be filtered against
- ▶ Explain what/ how much of the Layer 3 Packet can be manipulated
- ▶ Explain what parts of the Layer 3 Packet can be filtered against
- ▶ Explanation of the firewall rules that apply

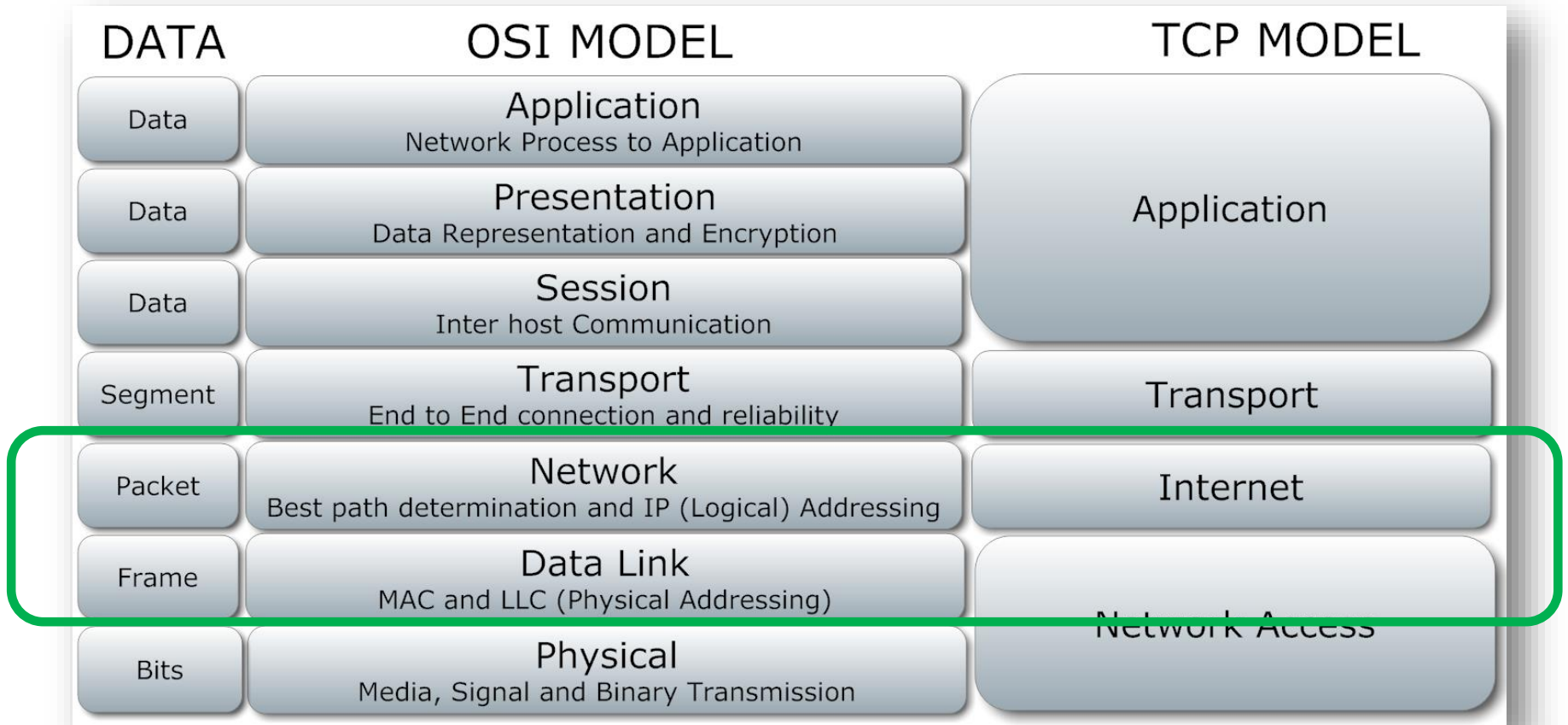


Networking Models





Networking Models





Layer 2 Ethernet Frame

Layer	Preamble	Start of frame delimiter	MAC Destination Address	MAC Source Address	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame Check Sequence (32-bit CRC)	Interpacket Gap
	7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46(42 min with 802.1Q tag)–1500 octets	4 octets	12 octets
Layer 2 Ethernet frame	← 64–1518(1522) octets →								
Layer 1 Ethernet packet	← 72–1526(1530) octets →								



Layer 2 Ethernet Frame

Layer	Preamble	Start of frame delimiter	MAC Destination Address	MAC Source Address	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame Check Sequence (32-bit CRC)	Interpacket Gap
	7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46(42 min with 802.1Q tag)–1500 octets	4 octets	12 octets
Layer 2 Ethernet frame	← 64–1518(1522) octets →								
Layer 1 Ethernet packet	← 72–1526(1530) octets →								

Portion which can be captured for analysis

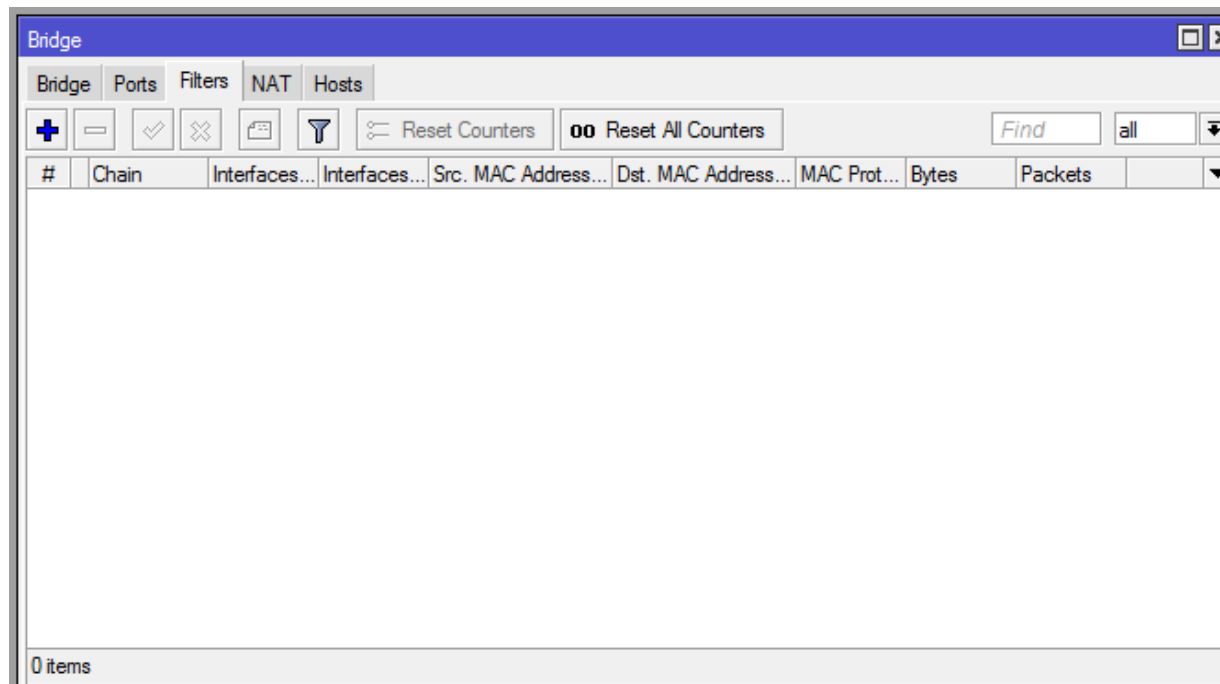


Filtering the Layer 2 Packet with the Bridge Firewall



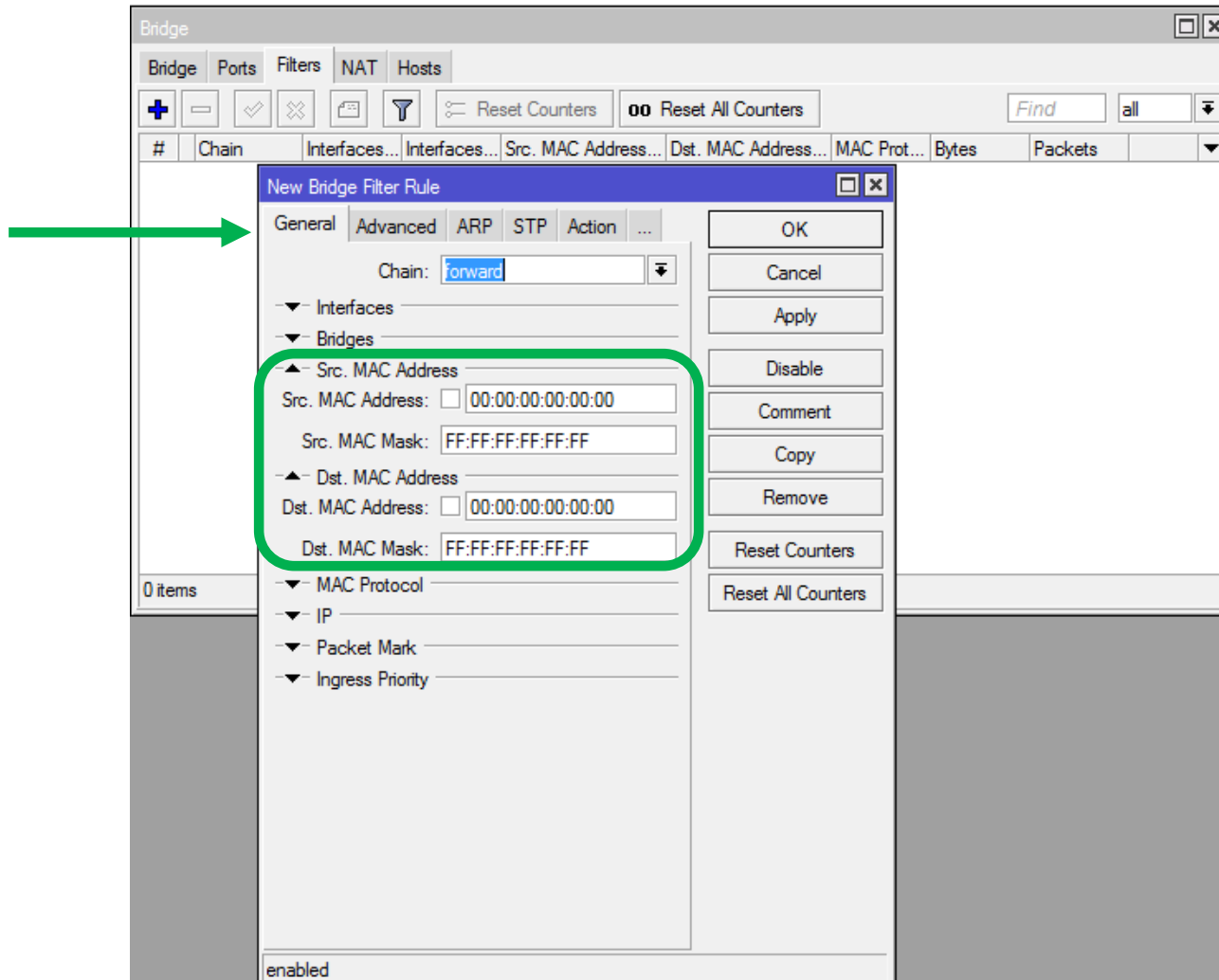
Bridge Filters & NAT

- ▶ Both the Filters & NAT tabs have the same filtering options. Only the actions are different.





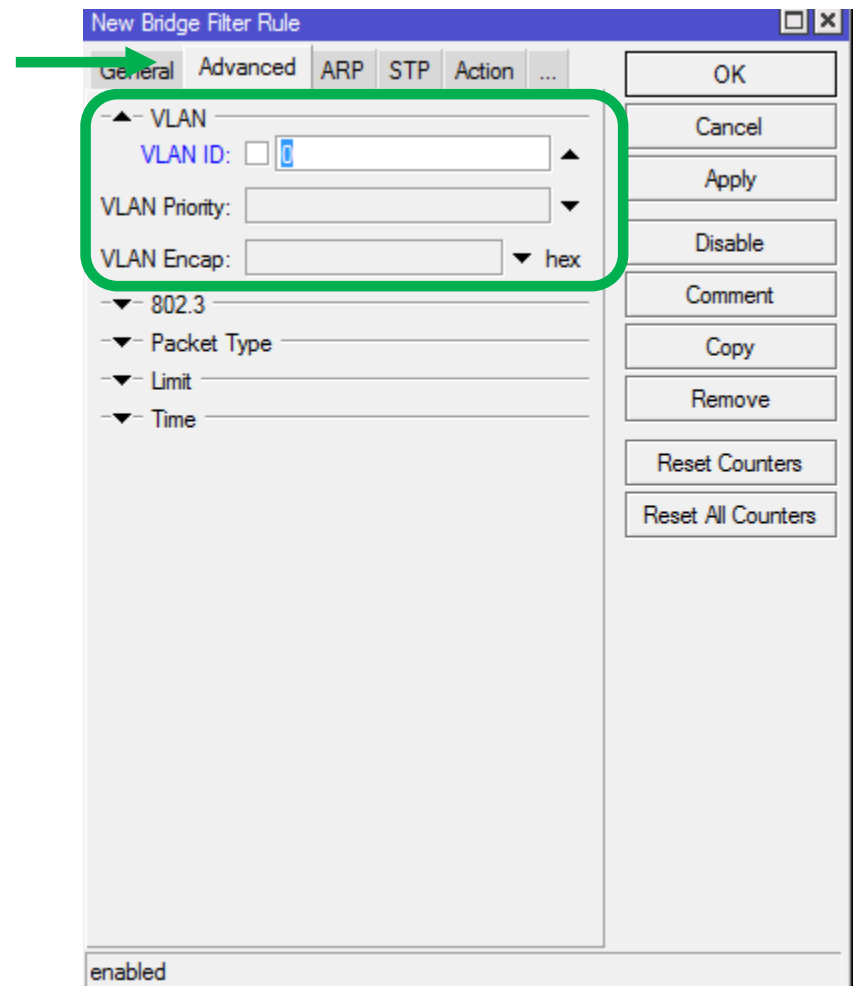
Source / Destination MAC Field





802.1Q Tag Field

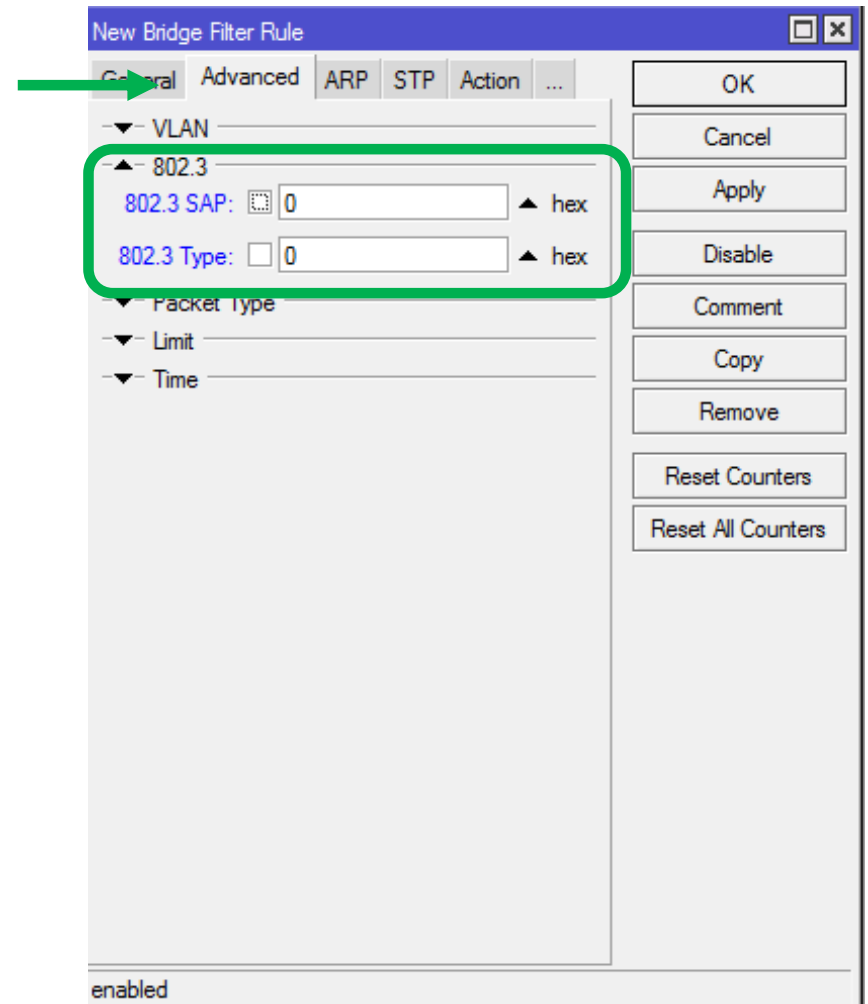
- ▶ **vlan-id** (*integer 0..4095*)
- ▶ **vlan-priority** (*integer 0..7*)
- ▶ **vlan-encap** (*802.2 | arp | ip | ipv6 | ipx | length | mpls-multicast | mpls-unicast | ppoe | ppoe-discovery | rarp | vlan or integer: 0..65535 decimal format or 0x0000-0xffff hex format*)





Ethernet Type Field

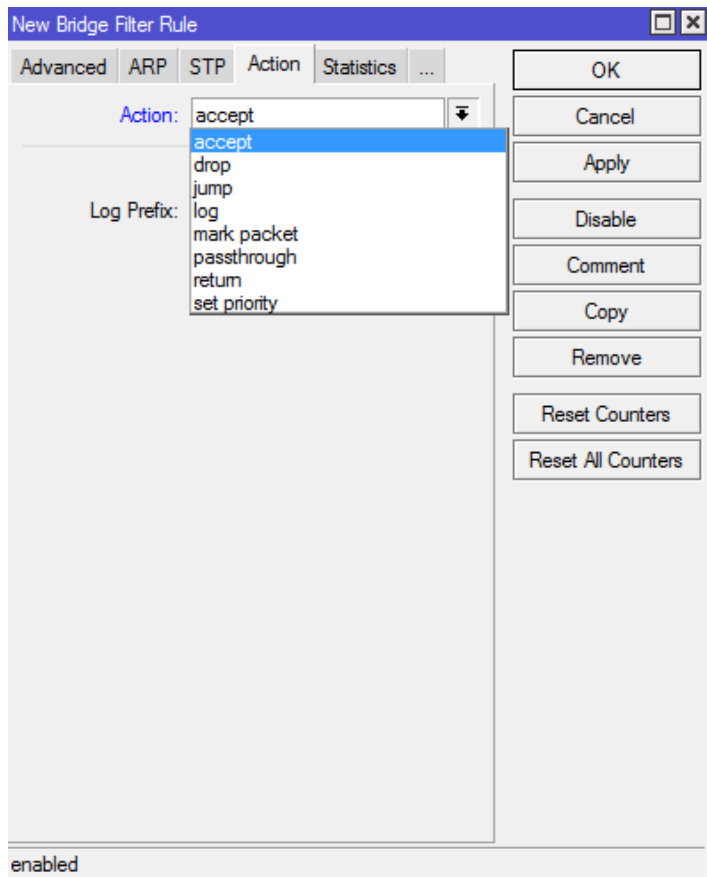
- ▶ **802.3-sap** (*integer*)
 - ▶ Example: 0xAA
- ▶ **802.3-type** (*integer*)
 - ▶ Example: 0x809B



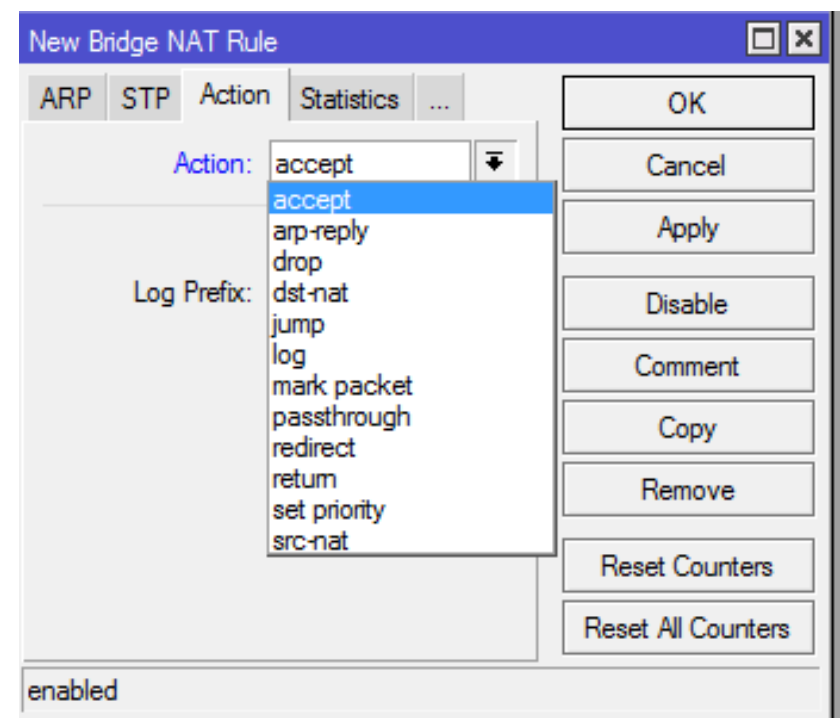


Bridge Firewall Actions

Filter Actions



NAT Actions





Primary Actions for Bridge Firewall

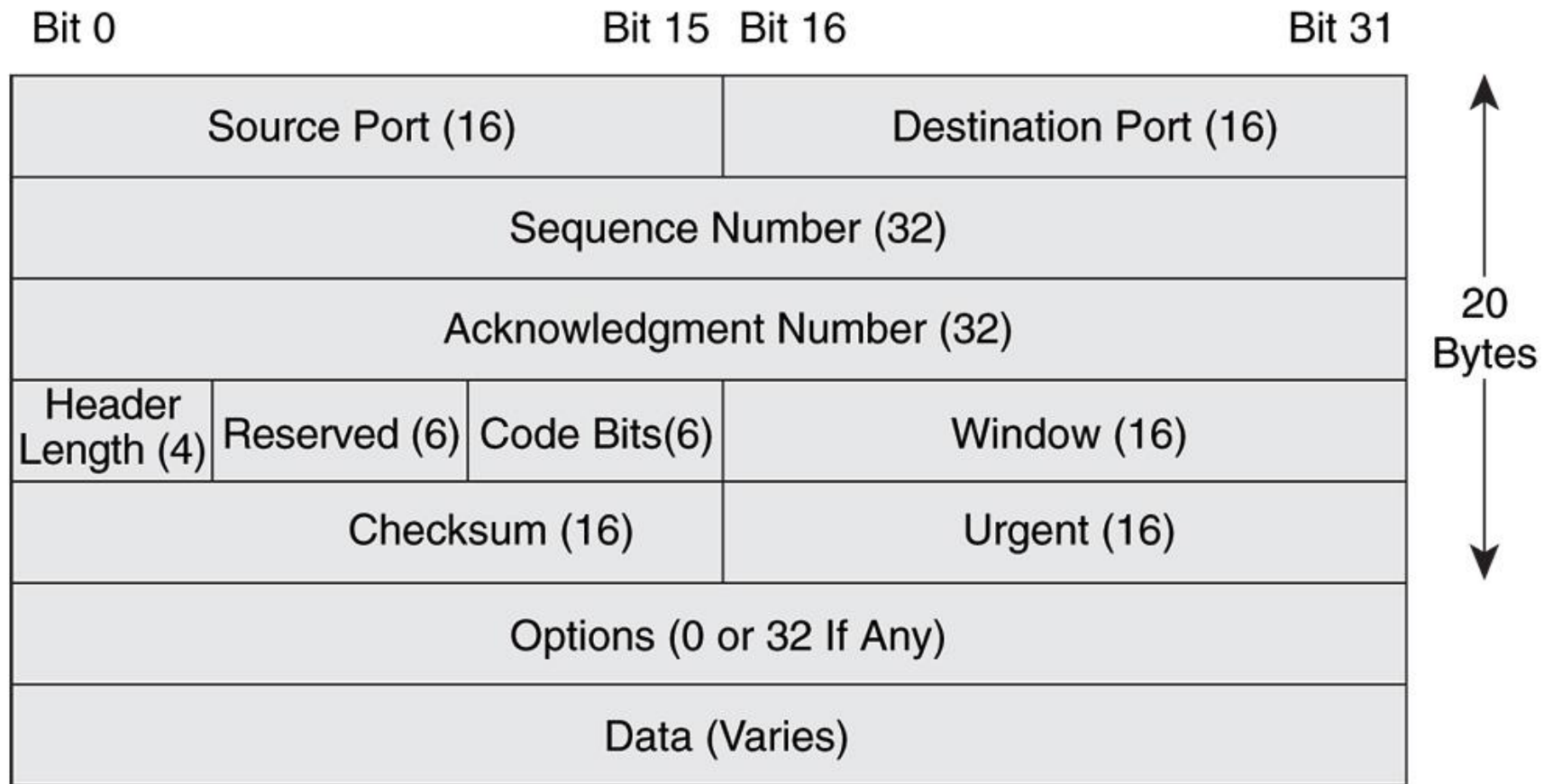
- ▶ Drop
- ▶ Set Priority
- ▶ Src-NAT
- ▶ Dst-NAT



Layer 3 Packets



TCP Header (L2 Frame Payload)





Filtering Layer 3 Packets with the Firewall



Source/ Destination Port Fields

- ▶ Protocol (25 Supported)
- ▶ Src Port
- ▶ Dst Port
- ▶ Any Port

New Firewall Rule

General Advanced Extra Action Statistics

Chain: forward

Src. Address:

Dst. Address:

Protocol: ☐ 6 (tcp)

Src. Port: ☐

Dst. Port: ☐

Any. Port: ☐

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

enabled



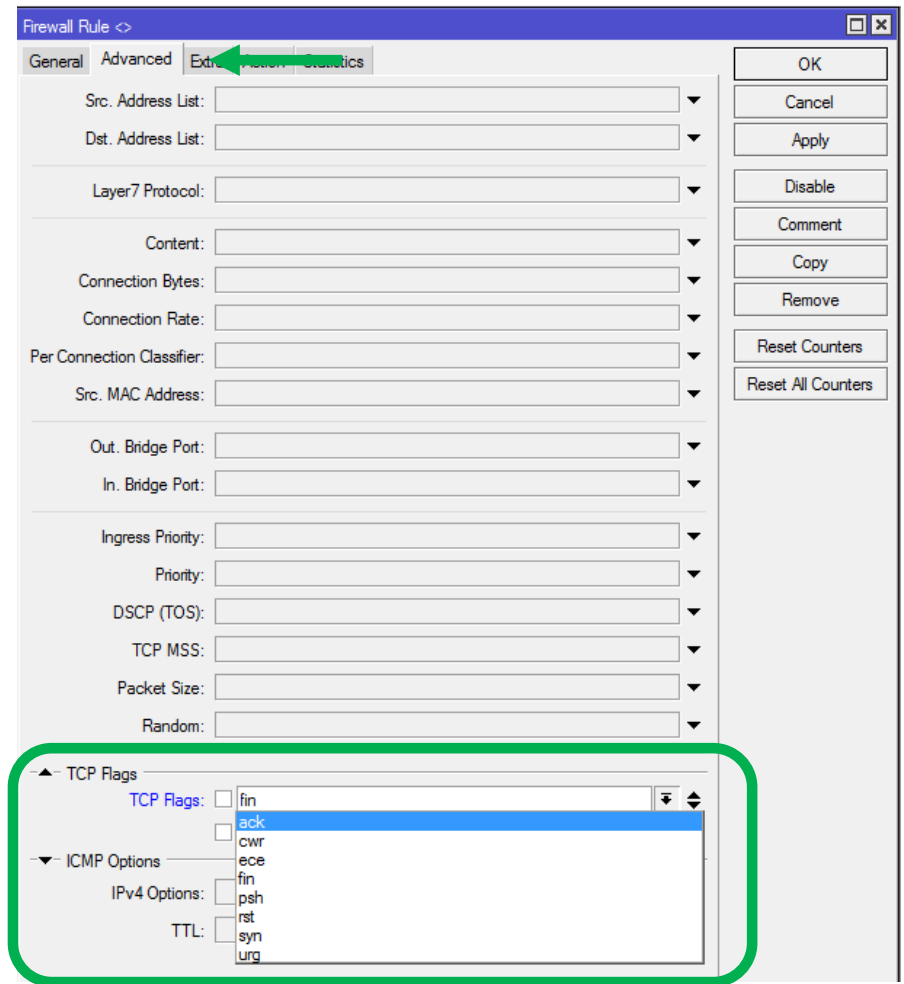
Sequence #, Ack#, Header Len Fields

- ▶ Difficult to match exact values



Code Bits/Flags Field

- ▶ **ack** - acknowledging data
- ▶ **cwr** - congestion window reduced
- ▶ **ece** - ECN-echo flag (explicit congestion notification)
- ▶ **fin** - close connection
- ▶ **psh** - push function
- ▶ **rst** - drop connection
- ▶ **syn** - new connection
- ▶ **urg** - urgent data





Window, Checksum, Urgent Pointer Fields

- ▶ Can not be directly matched against



Options Field

- ▶ 45 Options have been standardized
- ▶ Only is applicable 99% of the time
 - ▶ MSS (Maximum Segment Size)

The screenshot shows the 'Firewall Rule' configuration window with the 'Advanced' tab selected. The 'TCP MSS' field is highlighted with a green box and contains the value '1460-65535'. A green arrow points to the 'Advanced' tab. The window includes various configuration fields such as 'Src. Address List', 'Dst. Address List', 'Layer7 Protocol', 'Content', 'Connection Bytes', 'Connection Rate', 'Per Connection Classifier', 'Src. MAC Address', 'Out. Bridge Port', 'In. Bridge Port', 'Ingress Priority', 'Priority', 'DSCP (TOS)', 'Packet Size', 'Random', 'TCP Flags', 'ICMP Options', 'IPv4 Options', and 'TTL'. The right side of the window has buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters'.



Data Field

- ▶ Can be filtered using the “Content” and/ or Layer 7 Filters
- ▶ Content Filter can be used for any know values not specifically filtered by other rules

The screenshot shows the 'Firewall Rule' configuration window with the 'Advanced' tab selected. A green box highlights the 'Layer7 Protocol' and 'Content' fields. The 'Content' field is currently empty. The 'Action' tab is also visible, showing various options like 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters'.

Firewall Actions



Filters

Firewall Rule <>

General Advanced Extra Action Statistics

Action: accept

Log Prefix: drop

enabled

Drop

Nat

New NAT Rule

General Advanced Extra Action Statistics

Action: accept

Log Prefix: dst-nat

enabled

Src-NAT

Masquerade

Netmap

Redirect

Dst-NAT



Firewall Mangle Actions

- ▶ Change DSCP (TOS)
- ▶ Change MSS
- ▶ Change TTL
- ▶ Clear DF
- ▶ Set Priority
- ▶ Strip IPv4 Options

New Mangle Rule

General	Advanced	Extra	Action	Statistics
			Action:	accept
			Log Prefix:	accept
				add dst to address list
				add src to address list
				change DSCP (TOS)
				change MSS
				change TTL
				clear DF
				jump
				log
				mark connection
				mark packet
				mark routing
				passthrough
				return
				set priority
				sniff PC
				sniff TZSP
				strip IPv4 options



Conclusion

▶ Layer 2 Frames

- ▶ 100% of the 4 visible fields can be filtered
- ▶ 75% can be changed

▶ Layer 3 Packets

- ▶ Most Fields with standard values can be filtered or changed



Questions?