ISP Network Security Challenges

Chris Morrow
UUNET/VerizonBusiness

What is network security?

- Enterprise Security
  - One firewall
  - One 'untrusted network' connection
  - Well defined border
  - Well defined and limited 'services'
  - Limited user base, trusted user base

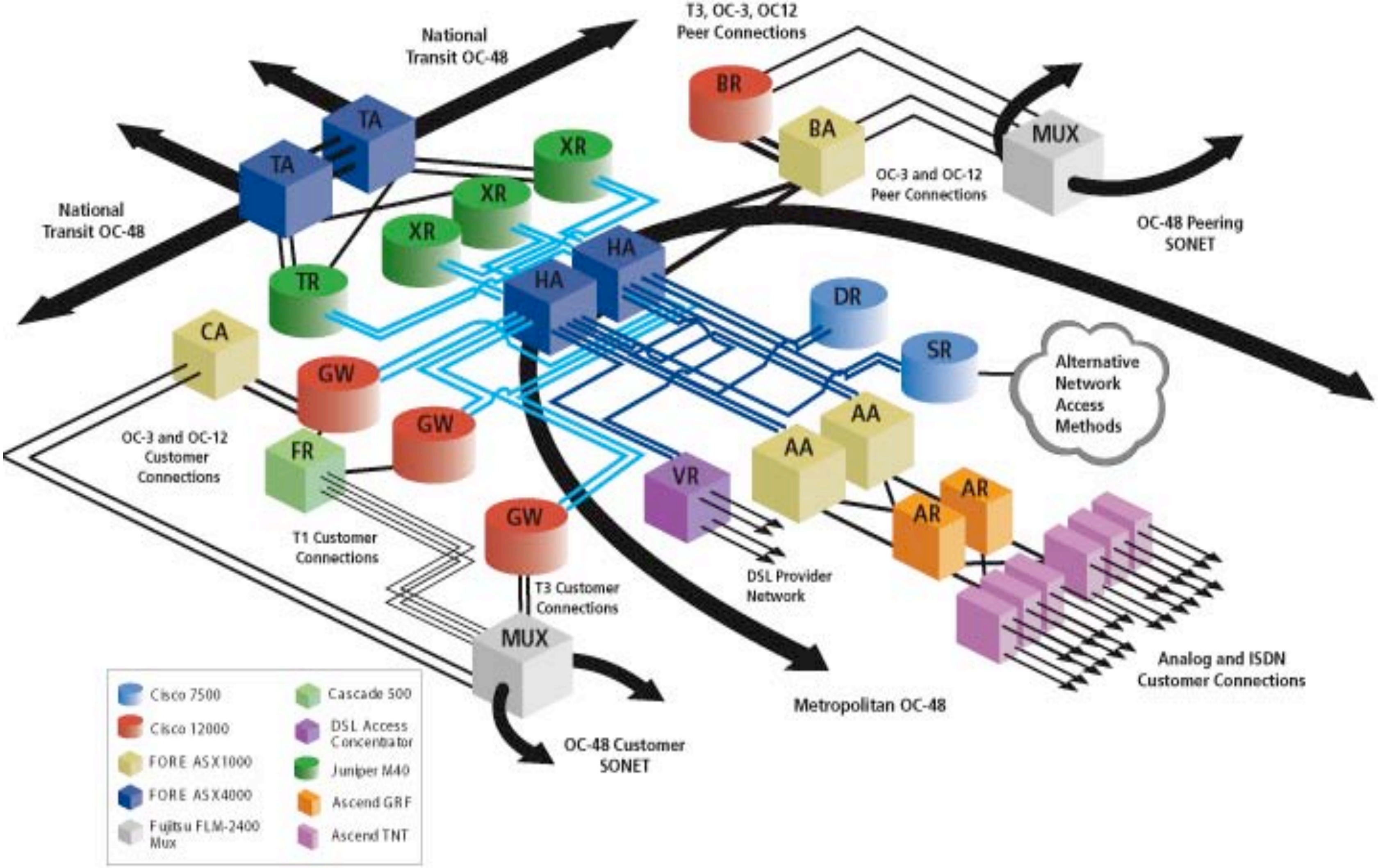
What is network security?

- ISP Security
  - We are the 'Internet'
  - We have 100,000 'Internet connections'
  - Borders defined by 'customer' or 'peer' boundaries
  - 'Services' are both software and traffic based
  - No trust in the users, ever
  - Availability is job #1

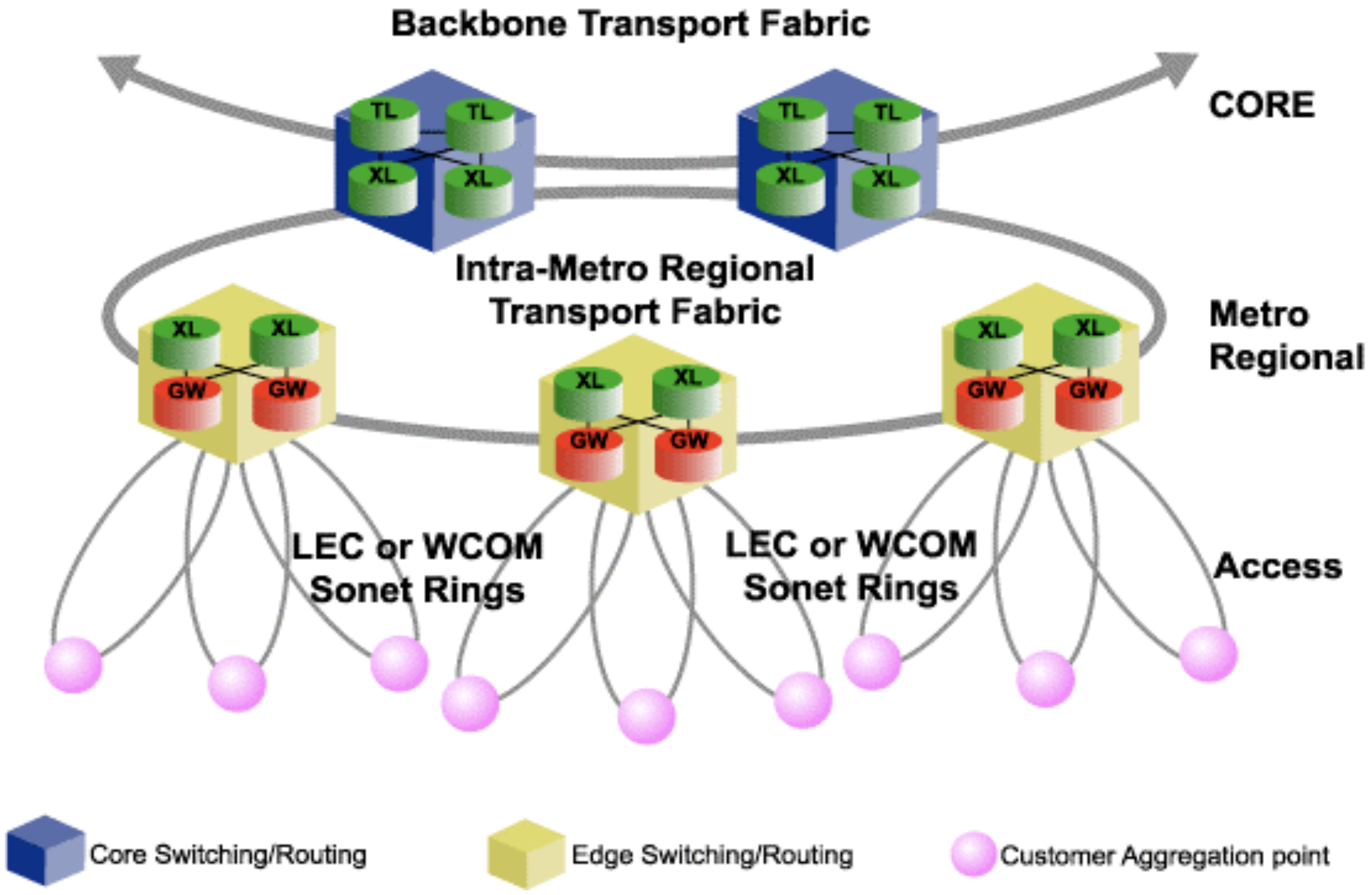
What is an ISP network today?

- Core infrastructure
- Services Aggregation Layer
  - internal services
  - customer services
- Converged Services
  - voip – Voice over IP
  - l2tp – Layer-2 Tunneling Protocol
  - MPLS VPN services

UUNET Network Circa 2000



UUNET Network circa 2004



Basics

- Built for Scale
- Built for Speed
- Consistency of delivery required
- Focus on Security to maintain availability
- Extreme sensitivity to failure

Scale

- Think 1200 interfaces/Router
- Think MPLS
- Think multiple ‘Internet sized 2547 VPN’
- Tomorrow multi-chassis + Logical Router + Virtual Router
- Large, complex, very low tolerance for error

Scale (cont)

- Core functions are critical to business
- Basic IP functionality must work
- What works in an enterprise doesn’t always work for an NSP
- Follow Standards (RFCs) It’s expected
  - work toward standards
- Services are planned according to Standards Compliance

Speed

- Interface speeds are increasing at the edge
- Core interfaces increasingly Shared
- Core interfaces increasingly MPLS
- Core increasingly passing non-native IP services
  - Voice
  - Pseudo-wire services
  - L2TPv3
- Convergence, both protocol and service

Security (general)

- Line Rate ACLS on all interfaces
  - ACLs on all interfaces on all platforms
  - full packet match capability
- Line Rate ACLS on all platforms (core)
  - don’t limit acls to edge platforms, todays core is tomorrows edge (maybe next months edge)
- Label pops on MPLS (not clear that this is truely feasible)
  - to which VPN does this packet belong, 192.168.1.1 isn’t necessarily unique anymore
- TTL filtering in acls and services
  - set outbound ttl/default-ttl
- Auditing usage and changes

Security (network OS)

- Listening Services on all interfaces?
  - define the interface/ip for each service
- SSH Host Keys, do they follow the hardwar or can I move them as part of 'software'?
- Follow RFC’s, don’t artificially limit without a big warning
- Provide knobs when breaking is required
  - allow reasonable behavior with the knob

Threats to Devices

- Passing packets is required, most modern day core devices can do this ‘headless’ for a short period of time
  - hardware tables for lookups
  - non-stop routing
- Queues for RE/RP traffic
  - isis
  - bgp
  - mgmt

Network Threats (cont)

- Worms Viruses can cause
  - unusual traffic patterns
  - excessive traffic
  - unintended traffic

Network Threats (cont)

- Malicious code can cause
  - distributed scan and exploit (unexpected traffic)
  - massive increases in traffic volumes

Life in a Converged World

- Outages are non-existent
- Packet sizes are radically different from I-Mix
- Routing protocol convergence is important
  - loops are outages
  - some services are very non-tolerant of delay
- FCC reportable (?)

Life in a Converged World (cont)

- Security increasingly important
  - Perceived ‘security’ of frame/atm
- CALEA
  - no truck roll
  - intercept at the edge
  - traffic flow for captured traffic
  - authentication of stream
  - verification of stream’s origination

Questions?