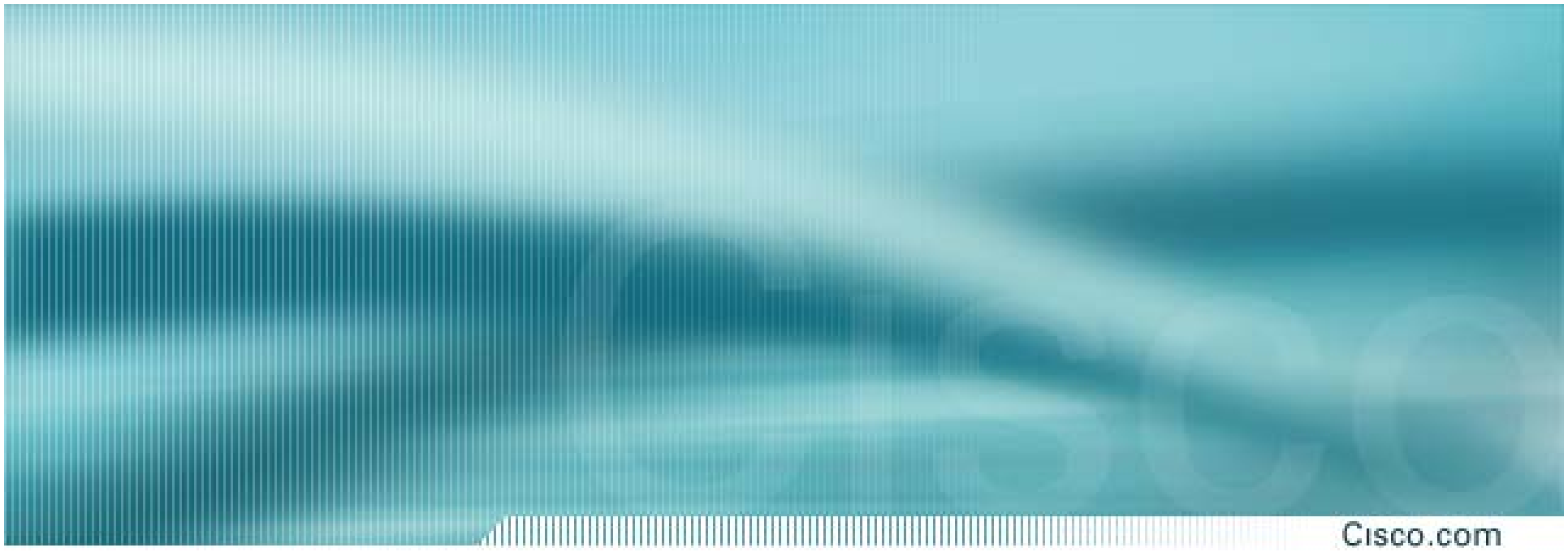


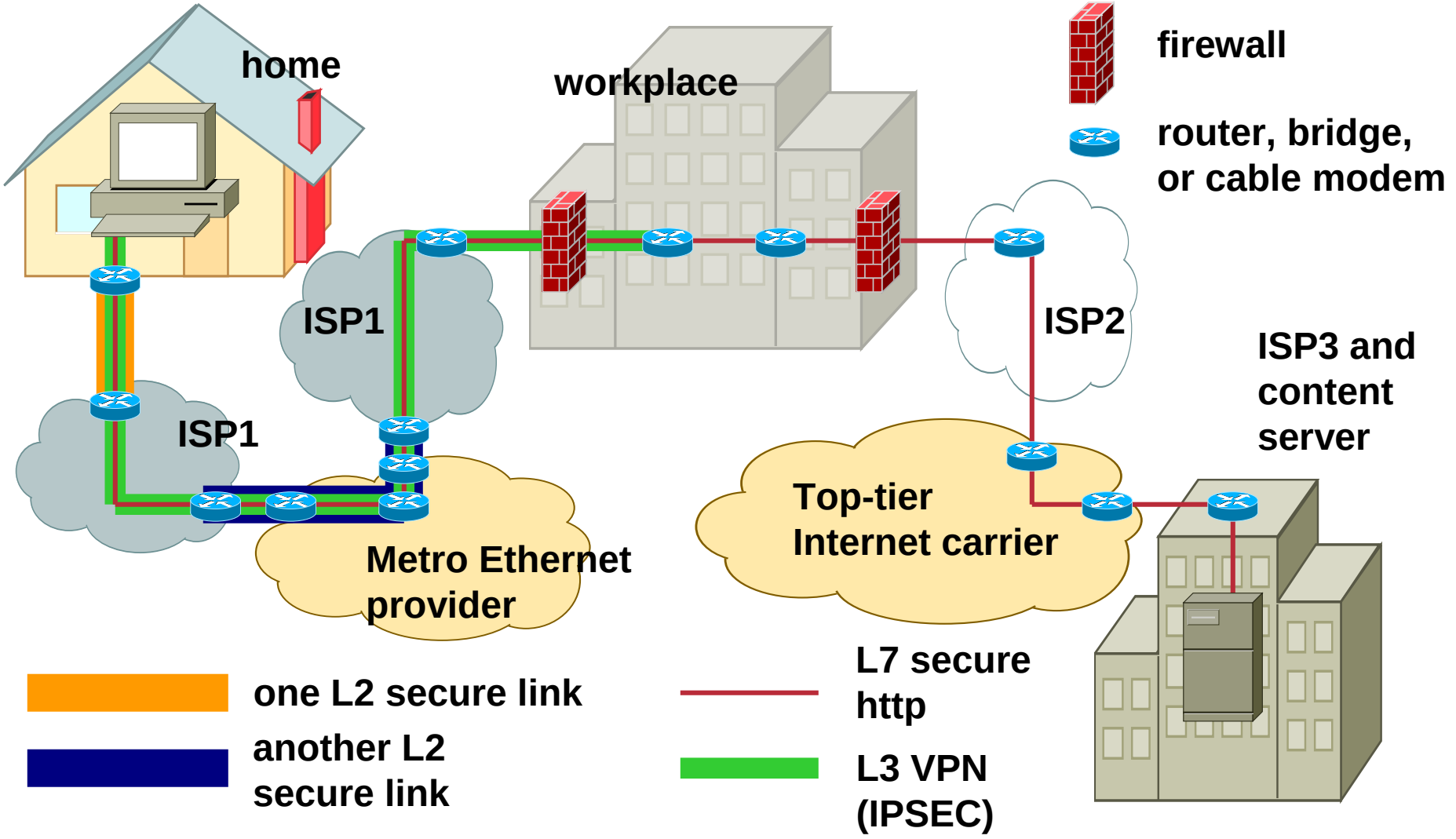
Security for 802 Access Networks: A Problem Statement

Norman Finn, Cisco Systems

Why bother with Link Layer security? Why not just use IPSEC?

- There are many protocols that are not securable via Layer 3: NetBEUI, Spanning Tree, Link Aggregation, GxRP, DHCP, ARP, IPX, …
- The organization legally or practically responsible for the solution may not have Layer 3 access to the endpoints.
- An L2 secure link is “lighter”, i.e. involves fewer protocol elements, than an L3 secure link.
- Security provides value-add for Layer 2 carriers.

Layer 2 vs. Layer 3 vs. Layer 7 Security



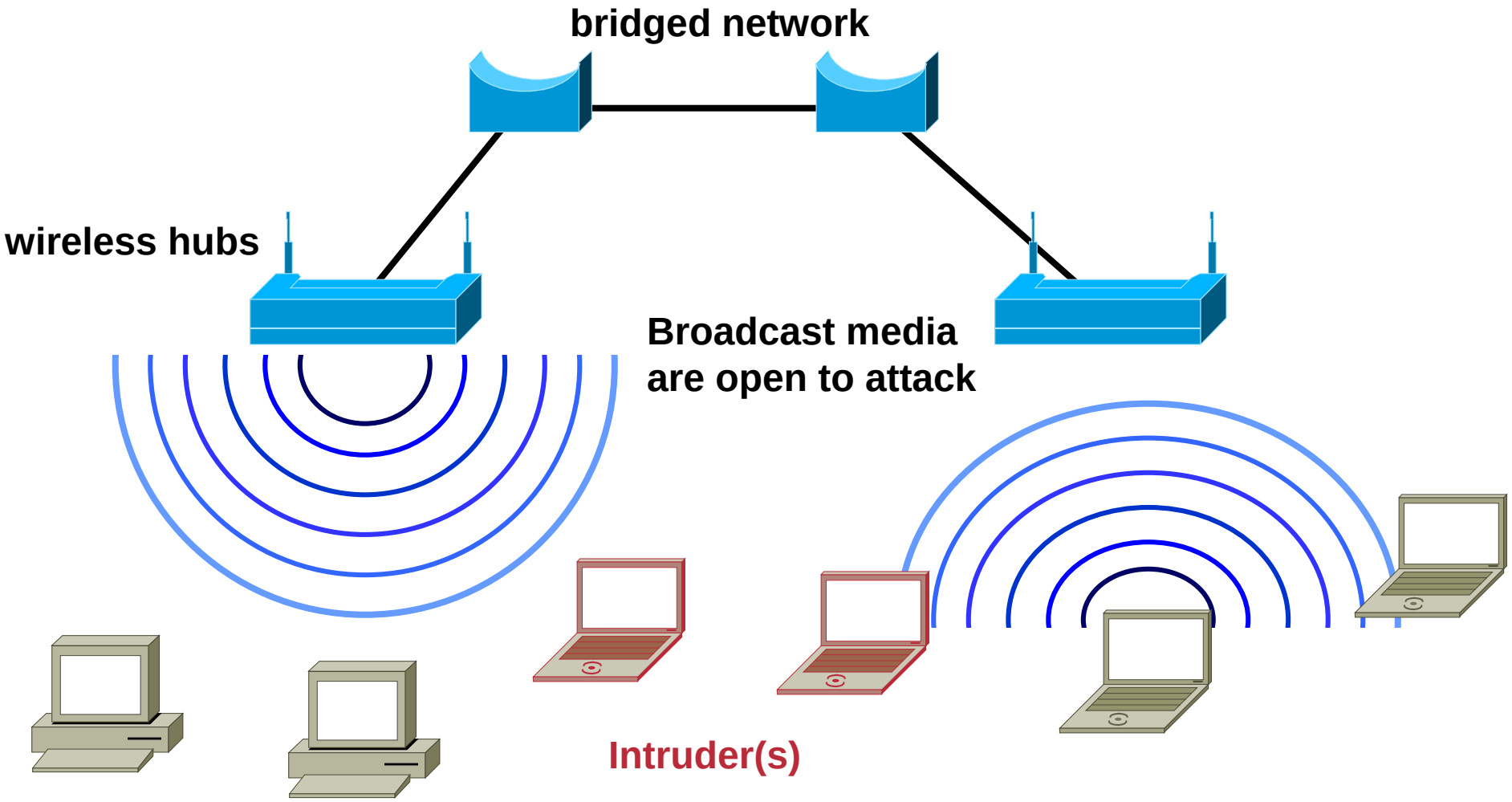
There is no one answer to all security problems.

- Why, today, do I run https over VPN/IPSEC over secure Docsis?
- https protects my credit card number across the big-I Internet.
- VPN/IPSEC connects my PC to a point behind my company firewall.
- Docsis prevents my neighbors from stealing my cable bandwidth.
- Three different scopes of responsibility, three different sets of requirements: a triply-encrypted packet.

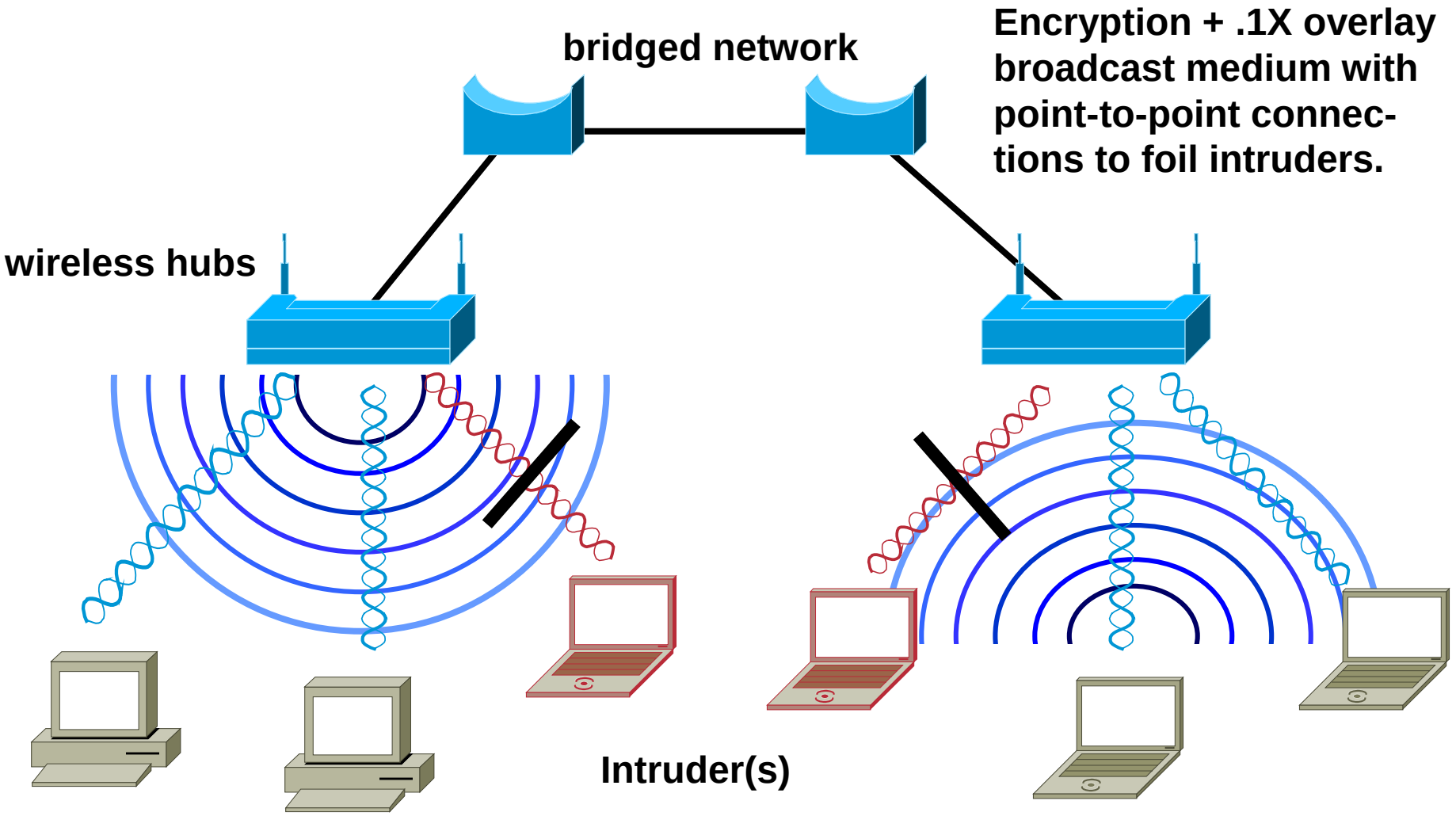
Many groups perceive a need for Layer 2 security

- 802.11 Wireless Access.
- 802.3ah Ethernet in the First Mile Point-to-Multipoint.
- 802.15 Personal wireless networking
- 802.16 Wireless Broadband Access.
- 802.17 Resilient Packet Ring.
- 802.3 CSMA/CD network access using 802.1X.
- 802.1 Metro Ethernet Service Providers

Example: 802.11
Everyone hears everything



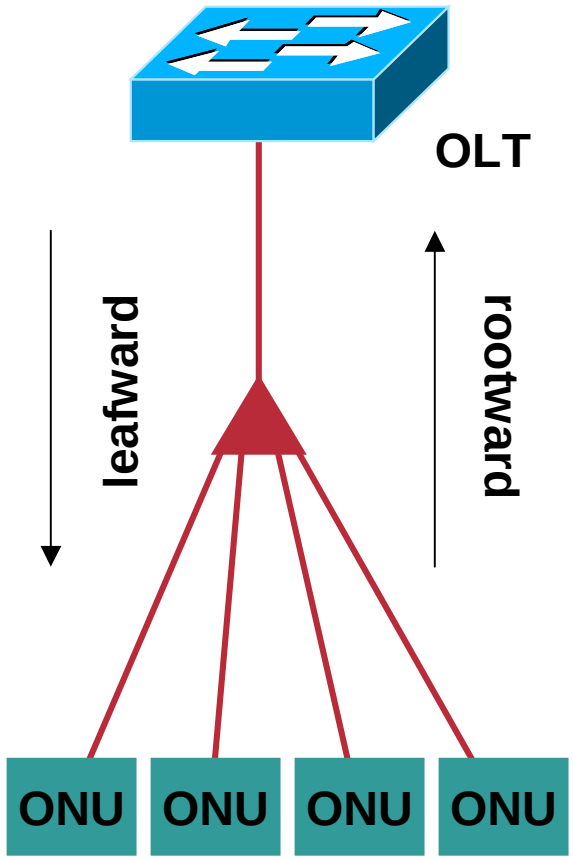
802.11: Closing the gate



802.11

- Felt the first need, generated the first answer.
- Leveraged 802.1X to prevent unauthorized use of an access point.
- Separated the data streams of the authorized users of a single hub.
- Used encryption to create point-to-point connections.
- Found that authorization and secure session setup was vulnerable to attack.
- Is developing a new solution, 802.11i.

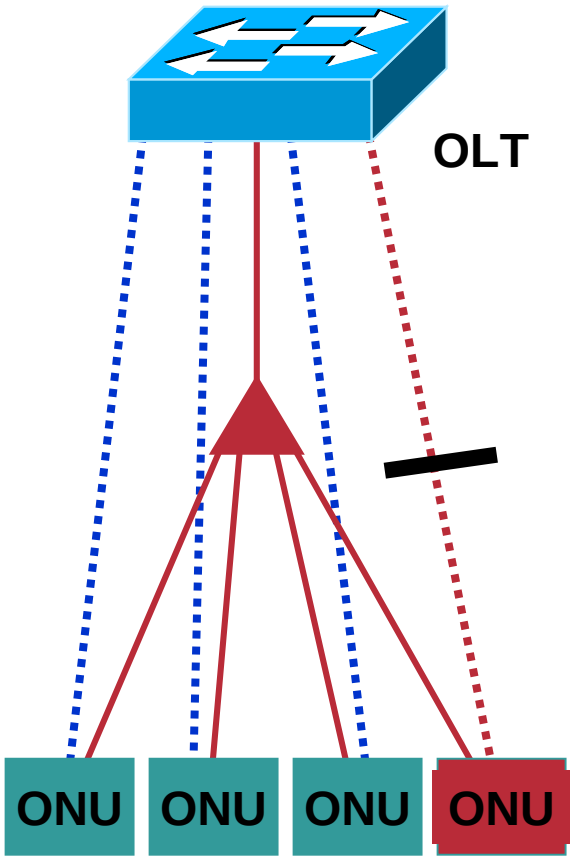
802.3ah Ethernet Passive Optical Network: EPON



Leafward traffic is seen by all ONUs, and normally, filtered by the ONU-ID In the preamble.

Rootward traffic is seen only by the OLT, assuming that the fiber is not tapped. ONUs are Time Division Multiplexed.

802.3ah Protecting leafward traffic



Encrypting all traffic ensures that attacker can neither eavesdrop nor masquerade as another ONU (or OLT!).

Link operation traffic, e.g. time slot allocation, must be protected.

Any new link level management, e.g. OAM, must be protected.

802.3ah EPON summary

- **All leafward traffic is seen by all leaves.**
- **Rootward traffic is invisible to other leaves.**
- **Needs are similar to 802.11, threats are perhaps a subset.**

802.17

- **Is a double fiber packet ring.**
- **Would like to allow different customers' equipment onto a ring.**
- **Ring relay function allows others to see your data.**
- **Thus, has similar eavesdropping and replay threats to 802.11.**
- **Introduces man-in-the-middle threats: attacker can receive your packet and modify it before relaying it.**

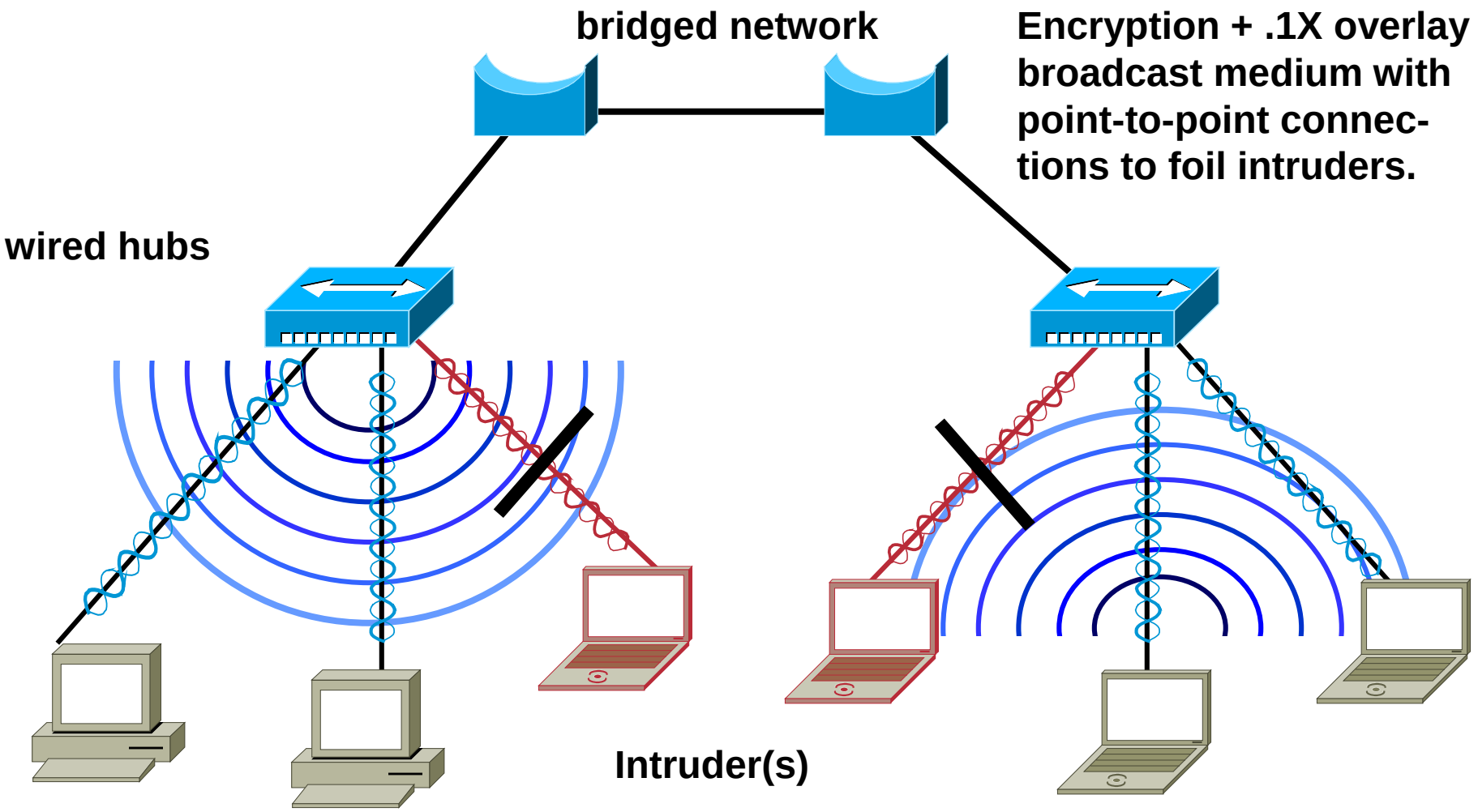
Other dot.groups

- **802.15**
  - **Similar needs to 802.11.**
  - **Much less power transmitted, lower range.**
  - **Much tighter constraints on complexity.**
  - **Has addressed the problem.**
- **802.16**
  - **Similar needs to 802.11.**
  - **Higher power, more range, more directional.**
  - **Has addressed the problem.**

802.3 hubs and 802.1X

- 802.1X assumes point-to-point connections, and explicitly does not address shared media, hubs, or bridges which do not run spanning tree.
- A bridge port attached to a hub is actually similar to an 802.11 access point, from a security standpoint. Everyone sees everything.
- It is easier in 802.3 than in 802.11 for a “man-in-the-middle” to insert a 2-port PC on any line, then eavesdrop, replay, modify, or insert data.
- Using bits in the preamble (as does 802.11) to solve the problem would greatly reduce the appeal of any solution.

General 802.3 solution



Many facets to a secure, interoperable solution

- **Threat analysis: What, explicitly, are you defending against? Accidents? Maliciousness? How much money must an attacker spend in order to defeat your security?**
- **Physical security: Can you prevent physical tampering? Discover it? Do you care?**
- **Authentication: Are you who you say you are?**
- **Authorization: Should you be here at all?**
- **Key establishment: How do you exchange secret keys over an insecure link?**
- **Data exchange: Can you run at wire speed?**

Points of attack

- **Man-in-the-middle:**

  A device with two ports is interposed between two devices which believe they are connected by a point-to-point connection.

- **Snooper:**

  A device can inspect, but not interfere with the transmission of, network traffic.

- **Intruder:**

  Unauthorized attachment to network.

  If one can intrude twice, one can become a man-in-the-middle to the larger network.

Basic operations of attackers

- **Inspect and record sensitive data.**
- **Inject frames that do not belong in the network:**

  new frames;

  previously inspected and recorded frames;

  legitimate or modified frames from another part of the network.
- **Prevent the transmission of legitimate frames.**
- **Modify the contents of otherwise legitimate frames.**

Multicast is an issue

- **For many to receive an encrypted packet sent once, all must have the same key.**
- **This is, perhaps, a more tractable problem at Layer 2 than at Layer 3.**
  - **The connection is more reliable.**
  - **The number of receivers is smaller.**
- **And, perhaps, more important at L2 than at L3.**
  - **At Layer 3, replicator is often sending to multiple links.**
  - **At Layer 2, there is usually no box between sender and receivers to replicate the data.**

High-level similarities

- One thread common to (at least) 802.11, 802.3ah, 802.16, and 802.3 hubs: transform a shared medium into a bundle of (tens of) secure point-to-point links.
- Point-to-point physical links are merely a special case. (And are not always what they seem.)
- Add the man-in-the-middle and you cover all of the dot groups.

High-level similarities

- **Authorization and key exchange are the critical points, because they involve trading information securely across an insecure medium.**
- **We may suppose that 802.11i will provide, at least, a good starting point for a common effort.**

Low level differences

- You may be able to use bits to the preamble to secure the MAC addresses in some dot groups.
- You cannot do that on existing Ethernet links.
- There are potential tricks to encrypt MAC addresses without involving the preamble.
- One must be very careful with encrypted MAC addresses: a bridged network might melt down if encrypted packets “escape” and reach an encryption-unaware device.
- If not adding to preamble, must either extend frame size, fragment/reassemble, or lower MTU.

Summary

Cisco.com

- **We need one 802 group to solve today's link-layer security problems and those to come.**
- **802.11i will likely provide the basis for the solution(s).**
- **The new group must be responsive to the various media groups' needs.**
- **It is not clear whether preamble bits are required to encrypt MAC addresses.**
- **We need the solution yesterday.**
- **But, we need a good solution.**